



**TECNOLÓGICO
DE MONTERREY®**

Dictámen final sobre Auditoría de Seguridad Información

Reporte de Reconocimiento

Descripción breve

Este documento es un reporte sobre el proceso de reconocimiento de la infraestructura del IEC sobre la cual se efectuó las pruebas y los análisis descritos en otras secciones de todo el trabajo.

Jesús R. González / Juan Arturo Nolasco
jrgonza@gmail.com jnolasco@itesm.mx

Índice

1	Resumen Ejecutivo	4
1.1	Alcance del documento	4
2	Ambiente	4
2.1	Conectividad	4
2.2	Herramientas	4
2.3	Consideraciones	5
3	Descubrimiento	5
3.1	Externo	5
3.1.1	VPNC 189.201.192.30	6
3.2	Interno	8
3.2.1	Red 10.50.1.0	9
3.2.2	Red 10.50.2.0	10
3.2.3	Red 10.50.3.0	10
3.2.4	Red 10.50.4.0 (aun no implementada)	10
4	Anexo I – Descubrimiento del equipo VPNC (189.201.192.30)	12
5	Anexo II Descubrimiento de la red 10.50.1.0	14
5.1	Descubrimiento red	14
5.2	Escaneo red	16
6	Anexo III Descubrimiento de la red 10.50.2.0	49
6.1	Descubrimiento red	49
6.2	Escaneo red	51
7	Anexo IV Descubrimiento de la red 10.50.3.0	97
7.1	Descubrimiento red	97
7.2	Escaneo red	99
8	Anexo V Descubrimiento de la red 10.50.4.0	102

Tabla de Ilustraciones

Ilustración 1 Esquema de conectividad.....	5
Ilustración 2 Traceroute hacia el IEC (desde red TELMEX).....	6
Ilustración 3 Traceroute hacia el IEC (desde red IZZI).....	7
Ilustración 4 Herramienta AngryPing.....	8
Ilustración 5 Herramienta Zenmap	9
Ilustración 6 Descubrimiento red 10.50.1.0.....	10

Versión	Fecha	Descripción
1.0	18 – Mayo – 2017	Resultados del descubrimiento de infraestructura tanto interna como externa del IEC. Análisis de vulnerabilidades

Dictamen elaborado por MsC. Jesús Raúl González Hernández en coordinación con Dr. Juan Arturo Nolasco.

1 Resumen Ejecutivo

Este documento describe las técnicas y metodologías usadas para el descubrimiento de los elementos de la red del IEC para escaneo y análisis.

1.1 Alcance del documento

Este documento solamente incluye los esquemas bajo los cuales se hizo el descubrimiento así como las herramientas y scripts usados para tener completa la lista de elementos de la red que se estarían escaneando para los análisis subsecuentes de vulnerabilidades, riesgo y penetración.

2 Ambiente

Esta sección describe la situación en que se hicieron las actividades de descubrimiento y escaneo de activos dentro de la red del IEC.

2.1 Conectividad

El IEC proporciona un acceso remoto vía VPN el cual se accede a la red para hacer el escaneo. El elemento con el cual se conectó para hacer el escaneo es un VPN Concentrator 3000 el cual recibe túneles de IPSEC y se encuentra en la red pública 189.201.192.30.

El análisis se realizó desde tres redes: Telmex, IZZI y Alestra/Axtel. Los mejores resultados se dieron desde la red de IZZI con la cual se tenía el menor número de saltos. Es por esto que se escogió la red de IZZI y de Alestra para facilitar los tiempos de conexión y evitar problemas con el túnel de IPSEC debido a la cantidad de hosts que hay entre los dos puntos.

2.2 Herramientas

Las herramientas para descubrimiento que se escogieron para poder hacer mejor el trabajo y confirmarlo son:

- **NCAT**– ES una herramienta que mediante comandos de script permite abrir conexiones de tipo TCP/UDP en un host
- **NMAP** – Mapeado de Redes es una herramienta de código abierto para exploración de redes y de seguridad. El objetivo de esta herramienta es el análisis de grandes redes permitiendo consultar al momento de estar escaneando el equipo que sistema operativo, aplicaciones, puertos activos entre otra información.
- **ZENMAP** – Es lo mismo que NMAP pero para versión de Windows.
- **AngryPing** – ES un programa hecho en JAVA con licencia abierta que permite hacer descubrimiento en una red de objetivos mostrando información sobre ellos.
- **TRACERT** – Esta herramienta permite trazar la ruta de paquetes desde el una computadora origen hasta el destino que se está buscando permitiendo encontrar los saltos que da y los tiempos que tarda en llegar.

2.3 Consideraciones

Al momento de hacer los escaneos, el IEC no proporciono datos algunos sobre sus redes ni aplicaciones, solamente proporciono el acceso a la VPN sobre la cual nos debíamos conectar.

Para propósitos del análisis y escaneo que se realiza como parte de las auditorías del IEC; los permisos de flujos de datos hasta antes del 15 de Mayo del 2017 están abiertos para permitir este escaneo. Se nos notificó que en el momento de las elecciones los permisos se modificarán para dar acceso a los sitios de acopio solamente a los servicios y equipos que deban tenerlo, de no ser así, estará bloqueado.

3 Descubrimiento

Para facilitar esta sección se estructura en los descubrimientos externos en la red pública de Internet así como los internos, que son en donde se encuentran los desarrollos en cuestión.

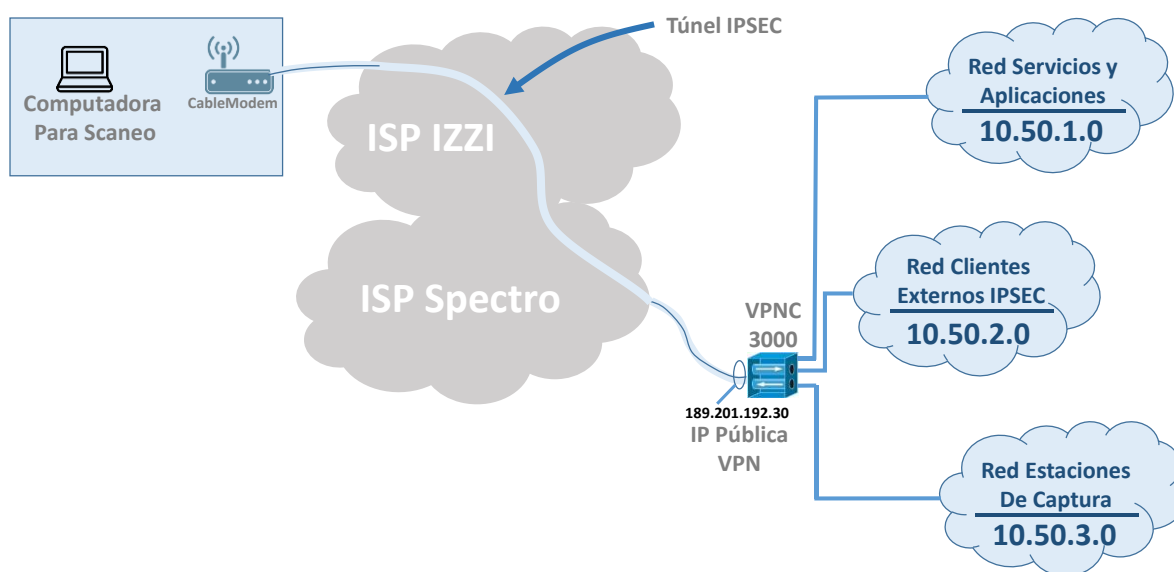


Ilustración 1 Esquema de conectividad

Anteriormente se tenía conexión a SPECTRO como proveedor de servicios, pero previo a las elecciones, habrá un proveedor adicional que pudo conectarse para antes de finalizar mayo del 2017 que es AXTEL/ALESTRA. Todas las sesiones y pruebas de descubrimiento se hicieron mediante un túnel de IPSEC. Se determinó utilizar la red de IZZI ya que de las que se tenía disponible era la que tenía mejor conteo de sitios para alcanzarla.

3.1 Externo

La red externa se escaneo con la dirección 189.201.192.30 dada para la terminación del túnel de IPSEC confirmando la existencia de un VPN Concentrador de CISCO el cual es un terminador de

túneles. La función de este es la conexión de los sitios de acopio remotos, ya sea con escáner o vía Smartphone (fotografía).

3.1.1 VPNC 189.201.192.30

El equipo VPNC 3000 es el terminador de túneles que habilita a los centros de acopio conectarse de vía remota vía IPSEC para subir las actas al sistema vía FTP. El VPNC se encuentra conectado a un proveedor de Internet ubicado en saltillo de nombre SPECTRO.

El descubrimiento se hizo desde rutas de Telmex y de IZZI TELECOM (antes multimedios) encontrando una mejor ruta (menos saltos) vía la red de IZZI TELECOM

Ruta vía TELMEX

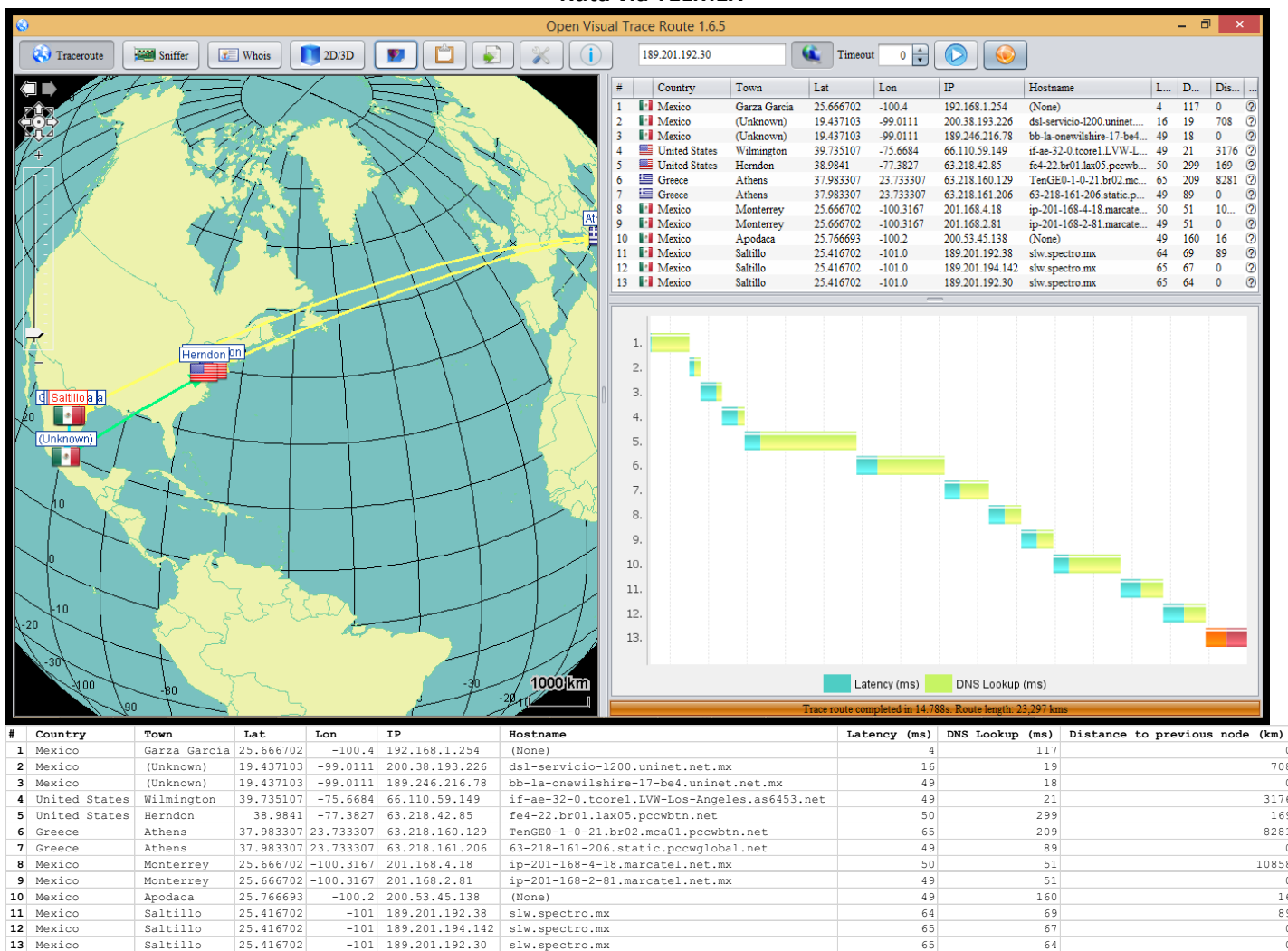
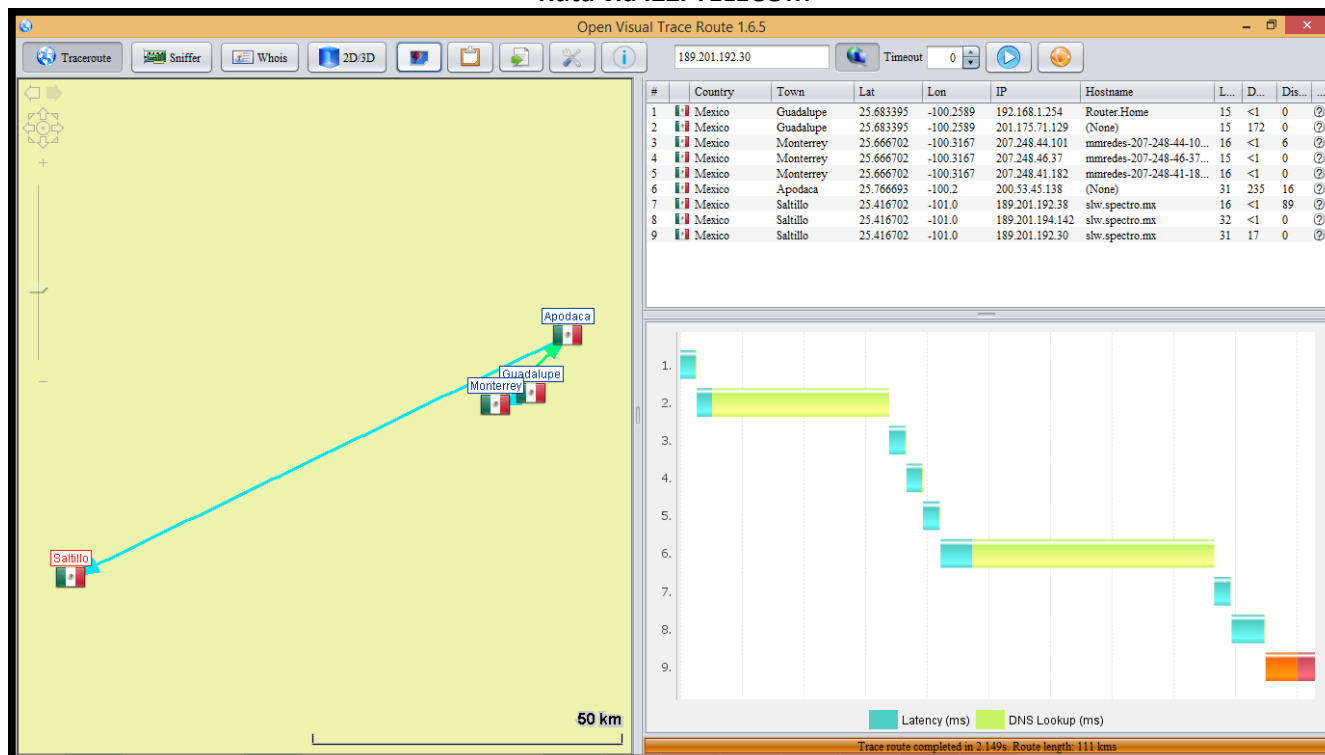


Ilustración 2 Traceroute hacia el IEC (desde red TELMEX)

Por Telmex se tienen que dar más de 13 pasos pasando por varios sitios en EEUU los cuales dificultan y retrasan la negociación del túnel de IPSEC.

La ruta vía IZZI representa menos saltos lo cual facilita y agiliza la conexión vía IPSEC. Esto debe tomarse en cuenta como parte de las rutas por donde se estarán haciendo los feeds a los replicadores de información el día de las elecciones.

Ruta vía IZZI TELECOM



#	Country	Town	Lat	Lon	IP	Hostname	Latency (ms)	DNS Lookup (ms)	Distance to previous node (km)
1	Mexico	Guadalupe	25.683395	-100.2589	192.168.1.254	Router.Home	15	0	0
2	Mexico	Guadalupe	25.683395	-100.2589	201.175.71.129	(None)	15	172	0
3	Mexico	Monterrey	25.666702	-100.3167	207.248.44.101	mmredes-207-248-44-101.multimedios.net	16	0	6
4	Mexico	Monterrey	25.666702	-100.3167	207.248.46.37	mmredes-207-248-46-37.multimedios.net	15	0	0
5	Mexico	Monterrey	25.666702	-100.3167	207.248.41.182	mmredes-207-248-41-182.multimedios.net	16	0	0
6	Mexico	Apodaca	25.766693	-100.2	200.53.45.138	(None)	31	235	16
7	Mexico	Saltillo	25.416702	-101	189.201.192.38	slw.spectro.mx	16	0	89
8	Mexico	Saltillo	25.416702	-101	189.201.194.142	slw.spectro.mx	32	0	0
9	Mexico	Saltillo	25.416702	-101	189.201.192.30	slw.spectro.mx	31	17	0

Ilustración 3 Traceroute hacia el IEC (desde red IZZI)

Durante el final de la auditoría, se le instalo al IEC un enlace de 100Mbps por Alestra/Axtel. No se alcanzó a probar bajo este enlace dado que las pruebas se corrieron desde el enlace de SPECTRO y las limitaciones de tiempo lo impidieron.

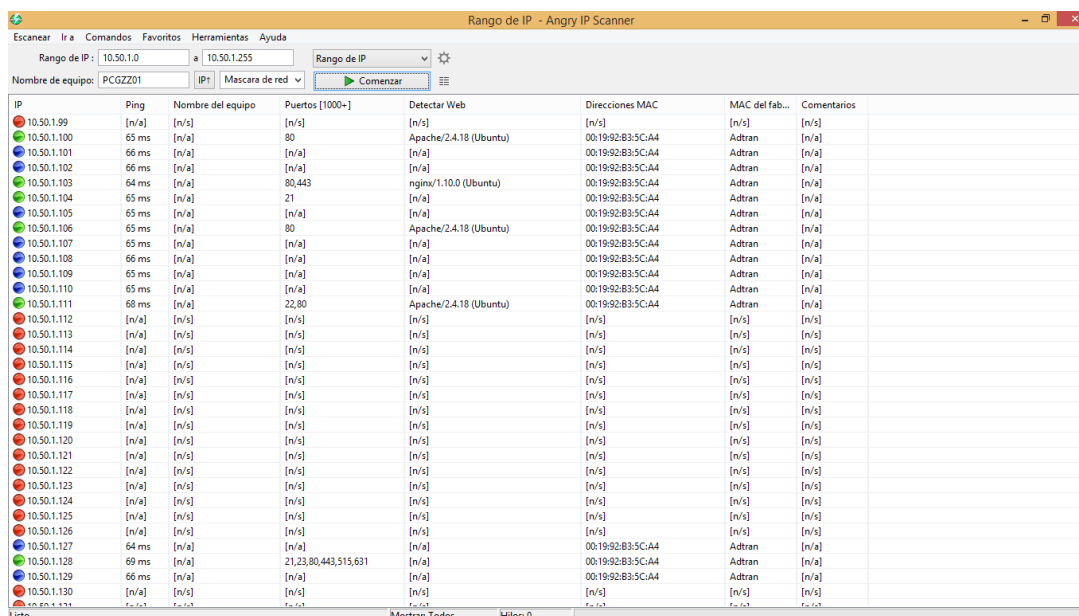
3.2 Interno

Una vez conectados en la red interna, se hizo descubrimiento de tres redes donde se conectan todos los dispositivos involucrados para las elecciones que celebrará el IEC. Las herramientas utilizadas para este descubrimiento fueron NMAP, ANGRYPING, NCAT con las que se pudo descubrir tres redes sobre las cuales opera el IEC

- 10.50.1.0 – En esta red se encuentran los servidores y aplicaciones primarios que contienen los servicios que se estarán usando durante las elecciones para el almacenamiento de archivos/imágenes digitales (las actas de mayoría) que estarán enviando los centros remotos
- 10.50.2.0 – En esta red se encuentra los elementos que se conectan en IPSEC a la red. Desde aquí se hizo el escaneo variando en las direcciones asignadas por el VPN
- 10.50.3.0 – En esta red se encuentran las estaciones de trabajo para captura del centro de acopio principal que se encuentra en Saltillo a donde llegarán las actas digitalizadas ya sea vía escáner o bien vía telefónica por medio de foto.

Las herramientas utilizadas desde la computadora de escaneo, reconocieron las redes para saber cuál equipo estaba conectado y podía responder.

- Angryping – A esta herramienta se le configura la red y su CIDR para que inicie el proceso de ping a dirección y puerto para verificar que está conectado dentro de la red que se le configuro



IP	Ping	Nombre del equipo	Puertos [1000+]	Detectar Web	Direcciones MAC	MAC del fab...	Comentarios
10.50.1.99	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
10.50.1.100	65 ms	[n/a]	80	Apache/2.4.18 (Ubuntu)	00:19:92:83:5C:A4	Adtran	[n/a]
10.50.1.101	66 ms	[n/a]	[n/a]	[n/a]	00:19:92:83:5C:A4	Adtran	[n/a]
10.50.1.102	66 ms	[n/a]	[n/a]	[n/a]	00:19:92:83:5C:A4	Adtran	[n/a]
10.50.1.103	64 ms	[n/a]	80,443	nginx/1.10.0 (Ubuntu)	00:19:92:83:5C:A4	Adtran	[n/a]
10.50.1.104	65 ms	[n/a]	21	[n/a]	00:19:92:83:5C:A4	Adtran	[n/a]
10.50.1.105	65 ms	[n/a]	[n/a]	[n/a]	00:19:92:83:5C:A4	Adtran	[n/a]
10.50.1.106	65 ms	[n/a]	80	Apache/2.4.18 (Ubuntu)	00:19:92:83:5C:A4	Adtran	[n/a]
10.50.1.107	65 ms	[n/a]	[n/a]	[n/a]	00:19:92:83:5C:A4	Adtran	[n/a]
10.50.1.108	66 ms	[n/a]	[n/a]	[n/a]	00:19:92:83:5C:A4	Adtran	[n/a]
10.50.1.109	65 ms	[n/a]	[n/a]	[n/a]	00:19:92:83:5C:A4	Adtran	[n/a]
10.50.1.110	68 ms	[n/a]	[n/a]	[n/a]	00:19:92:83:5C:A4	Adtran	[n/a]
10.50.1.111	68 ms	[n/a]	22,80	Apache/2.4.18 (Ubuntu)	00:19:92:83:5C:A4	Adtran	[n/a]
10.50.1.112	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
10.50.1.113	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
10.50.1.114	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
10.50.1.115	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
10.50.1.116	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
10.50.1.117	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
10.50.1.118	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
10.50.1.119	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
10.50.1.120	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
10.50.1.121	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
10.50.1.122	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
10.50.1.123	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
10.50.1.124	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
10.50.1.125	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
10.50.1.126	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
10.50.1.127	64 ms	[n/a]	[n/a]	[n/a]	00:19:92:83:5C:A4	Adtran	[n/a]
10.50.1.128	69 ms	[n/a]	21,23,80,443,515,631	[n/a]	00:19:92:83:5C:A4	Adtran	[n/a]
10.50.1.129	66 ms	[n/a]	[n/a]	[n/a]	00:19:92:83:5C:A4	Adtran	[n/a]
10.50.1.130	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
10.50.1.131	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]

Ilustración 4 Herramienta AngryPing

- NMAP – En esta herramienta se configuro con una serie de comandos que permitieron descubrir mayor detalle de cada equipo conectado así como escaneo de los primeros 1000 puertos TCP. El comando utilizado para este propósito es: `nmap -T4 -O -A -v -Pn 10.50.X.0/24`
 - X – Es la red que se pretende descubrir, en el caso del IEC se buscó sobre las redes 10.50.1.0/24, 10.50.2.0/24 y 10.50.3.0/24
 - -T4- Tiempo de escaneo entre puertos. Mientras más alto, es más rápido.
 - -O- Habilitar descubrimiento del sistema operativo
 - -A Habilitar detección Sistema operativo, versión y traceroute
 - -v Nivel medio de verbosidad (cantidad de información que ofrece la salida)
 - -Pn – Tratamiento del host como equipo en línea (evitar descubrimiento de hosts)

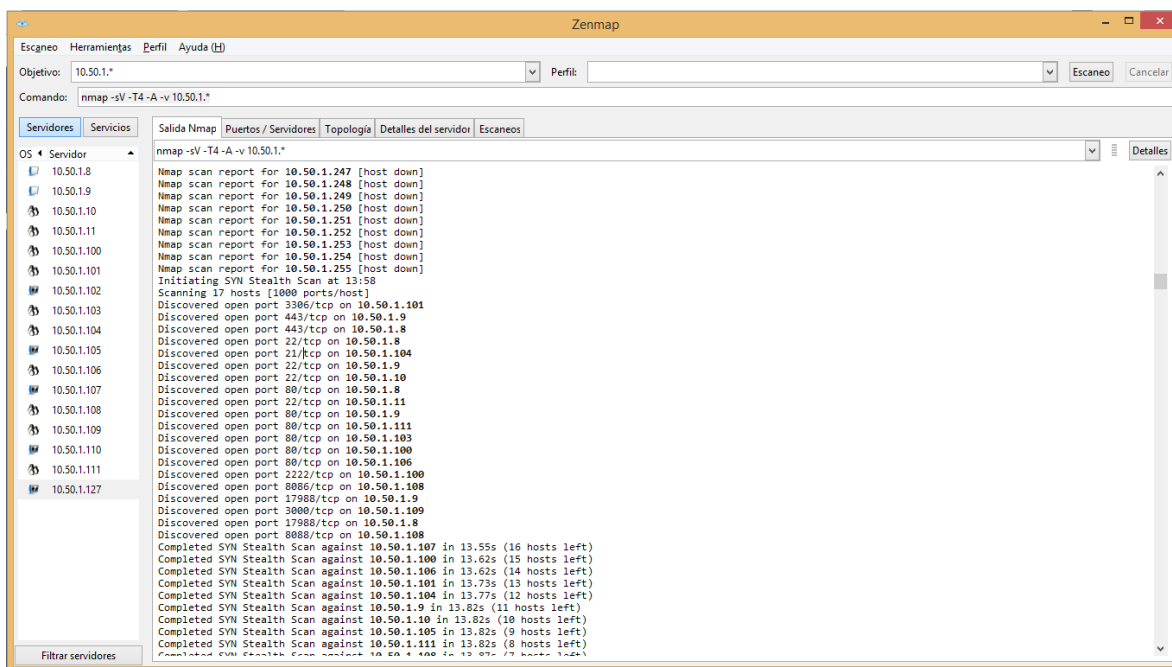


Ilustración 5 Herramienta Zenmap

3.2.1 Red 10.50.1.0

En esta red que incluye los distintos aplicaciones y elementos de servicios para usarse. En esta red se descubrieron los siguientes equipos como activos en la red:

IP	Ping	Nombre del equipo	Puertos	Detectar Web	Direcciones MAC	MAC del fabricante
10.50.1.8	23 ms	[n/a]	22.80.443	HPE-iLO-Server/1.30	00:19:92:B3:5C:A4	Adtran
10.50.1.9	23 ms	[n/a]	22.80.443	HPE-iLO-Server/1.30	00:19:92:B3:5C:A4	Adtran
10.50.1.10	20 ms	[n/a]	22	[n/a]	00:19:92:B3:5C:A4	Adtran
10.50.1.11	18 ms	[n/a]	22	[n/a]	00:19:92:B3:5C:A4	Adtran
10.50.1.100	17 ms	[n/a]	80	Apache/2.4.18 (Ubuntu)	00:19:92:B3:5C:A4	Adtran
10.50.1.101	19 ms	[n/a]	[n/a]	[n/a]	00:19:92:B3:5C:A4	Adtran
10.50.1.102	27 ms	[n/a]	[n/a]	[n/a]	00:19:92:B3:5C:A4	Adtran
10.50.1.103	30 ms	[n/a]	80	nginx/1.10.0 (Ubuntu)	00:19:92:B3:5C:A4	Adtran
10.50.1.104	27 ms	[n/a]	21	[n/a]	00:19:92:B3:5C:A4	Adtran
10.50.1.105	25 ms	[n/a]	[n/a]	[n/a]	00:19:92:B3:5C:A4	Adtran
10.50.1.106	29 ms	[n/a]	[n/a]	[n/a]	00:19:92:B3:5C:A4	Adtran
10.50.1.107	29 ms	[n/a]	[n/a]	[n/a]	00:19:92:B3:5C:A4	Adtran
10.50.1.108	25 ms	[n/a]	[n/a]	[n/a]	00:19:92:B3:5C:A4	Adtran
10.50.1.109	25 ms	[n/a]	[n/a]	[n/a]	00:19:92:B3:5C:A4	Adtran
10.50.1.110	21 ms	[n/a]	[n/a]	[n/a]	00:19:92:B3:5C:A4	Adtran
10.50.1.111	18 ms	[n/a]	[n/a]	[n/a]	00:19:92:B3:5C:A4	Adtran
10.50.1.127	24 ms	[n/a]	[n/a]	[n/a]	00:19:92:B3:5C:A4	Adtran
10.50.1.136	19 ms	[n/a]	23.8	Httpd	00:19:92:B3:5C:A4	Adtran

Ilustración 6 Descubrimiento red 10.50.1.0

Por lo que el análisis y el escaneo de vulnerabilidades se realizará dirigiéndose directo a estos equipos que son los que están conectados y reportaron actividad durante el escaneo. Para el resultado completo del escaneo, favor de dirigirse a la sección de anexos de este documento.

3.2.2 Red 10.50.2.0

Esta red aunque mostro varios equipos conectados, como lo muestra la lista (más detalle en el anexo) estos tienen los equipos filtrados por lo que no se pudo detectar el sistema operativo que se está usando así como tampoco conocer aplicaciones que potencialmente estarían usando.

El resto de las direcciones IP no respondían por lo que no había nadie conectado en esa red. Para el resultado completo del escaneo, favor de dirigirse a la sección de anexos de este documento.

El resultado del escaneo de esta red podría darse con mucha diferencia dado que potencialmente pueden estar haciendo pruebas de conexión de forma remota y existir equipos conectados.

3.2.3 Red 10.50.3.0

Esta red no mostro equipos conectados al momento de descubrirla. Esta es la red en la que estarán las estaciones de captura que se instalarán para capturar las actas validadas. Al momento del escaneo no había aun estaciones que respondieran al escaneo.

El resto de las direcciones IP no respondían por lo que no había nadie conectado en esa red. Para el resultado completo del escaneo, favor de dirigirse a la sección de anexos de este documento.

3.2.4 Red 10.50.4.0 (aun no implementada)

Esta red es en donde se ubicarán los servidores de respaldo con el proveedor de servicios de centro de datos. Al día de la entrega de este reporte esta red no ha sido aún entregada por lo que no hubo manera de escanearla

En esta red, se tendrán los servidores con las aplicaciones de operación y capturarlos cuales están sincronizándose de modo que se tenga un respaldo de trabajo cuando haya alguna situación de caída con los servidores primarios en el centro de operaciones de Saltillo.

4 Anexo I – Descubrimiento del equipo VPNC (189.201.192.30)

```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-07 22:12 Hora de verano central (México)
NSE: Loaded 143 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 22:12
Completed NSE at 22:12, 0.00s elapsed
Initiating NSE at 22:12
Completed NSE at 22:12, 0.00s elapsed
Initiating Ping Scan at 22:12
Scanning 189.201.192.30 [4 ports]
Completed Ping Scan at 22:12, 1.24s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:13
Completed Parallel DNS resolution of 1 host. at 22:13, 7.06s elapsed
Initiating SYN Stealth Scan at 22:13
Scanning slw.spectro.mx (189.201.192.30) [1000 ports]
Discovered open port 443/tcp on 189.201.192.30
Discovered open port 22/tcp on 189.201.192.30
Completed SYN Stealth Scan at 22:13, 4.66s elapsed (1000 total ports)
Initiating Service scan at 22:13
Scanning 2 services on slw.spectro.mx (189.201.192.30)
Completed Service scan at 22:13, 12.48s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against slw.spectro.mx (189.201.192.30)
Initiating Traceroute at 22:13
Completed Traceroute at 22:13, 0.04s elapsed
Initiating Parallel DNS resolution of 9 hosts. at 22:13
Completed Parallel DNS resolution of 9 hosts. at 22:13, 7.54s elapsed
NSE: Script scanning 189.201.192.30.
Initiating NSE at 22:13
Completed NSE at 22:15, 112.66s elapsed
Initiating NSE at 22:15
Completed NSE at 22:15, 0.01s elapsed
Nmap scan report for slw.spectro.mx (189.201.192.30)
Host is up (0.024s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          Cisco SSH 1.25 (protocol 1.99)
|_ ssh-hostkey:
|   2048 eb:44:0d:0b:ef:45:77:6c:70:d4:29:45:64:e8:8e:07 (RSA1)
|   2048 80:47:db:17:22:dc:7a:dd:1d:19:d4:df:43:cd:94:dc (RSA)
|_ sshv1: Server supports SSHv1
443/tcp    open  ssl/http     Cisco Adaptive Security Appliance http config
|_ http-methods:
|_   Supported Methods: GET HEAD POST
|_ http-robots.txt: 1 disallowed entry
|_ /
|_ ssl-cert: Subject: commonName=ASA Temporary Self Signed Certificate
|_ Issuer: commonName=ASA Temporary Self Signed Certificate
|_ Public Key type: rsa
|_ Public Key bits: 2048
|_ Signature Algorithm: sha256WithRSAEncryption
|_ Not valid before: 2017-05-02T17:34:36
|_ Not valid after: 2027-04-30T17:34:36
|_ MD5: e30d a389 e4a0 fc7d edab 286d 8502 f2fd
|_ SHA-1: 4e89 a5ac f40f d118 cc69 f016 6b7e 4225 63d0 eb96
|_ ssl-date: TLS randomness does not represent time
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: firewall
Running: Cisco PIX OS 8.X
OS CPE: cpe:/o:cisco:pix_os:8.4
OS details: Cisco Adaptive Security Appliance (PIX OS 8.4)
Network Distance: 9 hops
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: Randomized
Service Info: OS: IOS; Device: firewall; CPE: cpe:/o:cisco:ios, cpe:/h:cisco:asa

TRACEROUTE (using port 443/tcp)
HOP RTT ADDRESS
1 2.00 ms Router.Home (192.168.1.254)
2 5.00 ms 201.175.71.129
3 12.00 ms mmredes-207-248-44-101.multimedios.net (207.248.44.101)
4 14.00 ms mmredes-207-248-46-37.multimedios.net (207.248.46.37)
5 8.00 ms mmredes-207-248-41-182.multimedios.net (207.248.41.182)
6 28.00 ms 200.53.45.138
7 30.00 ms slw.spectro.mx (189.201.192.38)
```

```
8 37.00 ms slw.spectro.mx (189.201.194.142)
9 39.00 ms slw.spectro.mx (189.201.192.30)
```

```
NSE: Script Post-scanning.
Initiating NSE at 22:15
Completed NSE at 22:15, 0.00s elapsed
Initiating NSE at 22:15
Completed NSE at 22:15, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 162.68 seconds
Raw packets sent: 2057 (92.650KB) | Rcvd: 29 (1.730KB)
```


[illegible]

5.2 Escaneo red

```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-06 13:57 Hora de verano central (México)
NSE: Loaded 143 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 13:58
Completed NSE at 13:58, 0.00s elapsed
Initiating NSE at 13:58
Completed NSE at 13:58, 0.00s elapsed
Initiating Ping Scan at 13:58
Scanning 256 hosts [4 ports/host]
Completed Ping Scan at 13:58, 4.94s elapsed (256 total hosts)
Initiating Parallel DNS resolution of 256 hosts. at 13:58
Completed Parallel DNS resolution of 256 hosts. at 13:58, 11.02s elapsed
Nmap scan report for 10.50.1.0 [host down]
Nmap scan report for 10.50.1.1 [host down]
Nmap scan report for 10.50.1.2 [host down]
Nmap scan report for 10.50.1.3 [host down]
Nmap scan report for 10.50.1.4 [host down]
Nmap scan report for 10.50.1.5 [host down]
Nmap scan report for 10.50.1.6 [host down]
Nmap scan report for 10.50.1.7 [host down]
Nmap scan report for 10.50.1.12 [host down]
Nmap scan report for 10.50.1.13 [host down]
Nmap scan report for 10.50.1.14 [host down]
Nmap scan report for 10.50.1.15 [host down]
Nmap scan report for 10.50.1.16 [host down]
Nmap scan report for 10.50.1.17 [host down]
Nmap scan report for 10.50.1.18 [host down]
Nmap scan report for 10.50.1.19 [host down]
Nmap scan report for 10.50.1.20 [host down]
Nmap scan report for 10.50.1.21 [host down]
Nmap scan report for 10.50.1.22 [host down]
Nmap scan report for 10.50.1.23 [host down]
Nmap scan report for 10.50.1.24 [host down]
Nmap scan report for 10.50.1.25 [host down]
Nmap scan report for 10.50.1.26 [host down]
Nmap scan report for 10.50.1.27 [host down]
Nmap scan report for 10.50.1.28 [host down]
Nmap scan report for 10.50.1.29 [host down]
Nmap scan report for 10.50.1.30 [host down]
Nmap scan report for 10.50.1.31 [host down]
Nmap scan report for 10.50.1.32 [host down]
Nmap scan report for 10.50.1.33 [host down]
Nmap scan report for 10.50.1.34 [host down]
Nmap scan report for 10.50.1.35 [host down]
Nmap scan report for 10.50.1.36 [host down]
Nmap scan report for 10.50.1.37 [host down]
Nmap scan report for 10.50.1.38 [host down]
Nmap scan report for 10.50.1.39 [host down]
Nmap scan report for 10.50.1.40 [host down]
Nmap scan report for 10.50.1.41 [host down]
Nmap scan report for 10.50.1.42 [host down]
Nmap scan report for 10.50.1.43 [host down]
Nmap scan report for 10.50.1.44 [host down]
Nmap scan report for 10.50.1.45 [host down]
Nmap scan report for 10.50.1.46 [host down]
Nmap scan report for 10.50.1.47 [host down]
Nmap scan report for 10.50.1.48 [host down]
Nmap scan report for 10.50.1.49 [host down]
Nmap scan report for 10.50.1.50 [host down]
Nmap scan report for 10.50.1.51 [host down]
Nmap scan report for 10.50.1.52 [host down]
Nmap scan report for 10.50.1.53 [host down]
Nmap scan report for 10.50.1.54 [host down]
Nmap scan report for 10.50.1.55 [host down]
Nmap scan report for 10.50.1.56 [host down]
Nmap scan report for 10.50.1.57 [host down]
Nmap scan report for 10.50.1.58 [host down]
Nmap scan report for 10.50.1.59 [host down]
Nmap scan report for 10.50.1.60 [host down]
Nmap scan report for 10.50.1.61 [host down]
Nmap scan report for 10.50.1.62 [host down]
Nmap scan report for 10.50.1.63 [host down]
Nmap scan report for 10.50.1.64 [host down]
```



```
Nmap scan report for 10.50.1.228 [host down]
Nmap scan report for 10.50.1.229 [host down]
Nmap scan report for 10.50.1.230 [host down]
Nmap scan report for 10.50.1.231 [host down]
Nmap scan report for 10.50.1.232 [host down]
Nmap scan report for 10.50.1.233 [host down]
Nmap scan report for 10.50.1.234 [host down]
Nmap scan report for 10.50.1.235 [host down]
Nmap scan report for 10.50.1.236 [host down]
Nmap scan report for 10.50.1.237 [host down]
Nmap scan report for 10.50.1.238 [host down]
Nmap scan report for 10.50.1.239 [host down]
Nmap scan report for 10.50.1.240 [host down]
Nmap scan report for 10.50.1.241 [host down]
Nmap scan report for 10.50.1.242 [host down]
Nmap scan report for 10.50.1.243 [host down]
Nmap scan report for 10.50.1.244 [host down]
Nmap scan report for 10.50.1.245 [host down]
Nmap scan report for 10.50.1.246 [host down]
Nmap scan report for 10.50.1.247 [host down]
Nmap scan report for 10.50.1.248 [host down]
Nmap scan report for 10.50.1.249 [host down]
Nmap scan report for 10.50.1.250 [host down]
Nmap scan report for 10.50.1.251 [host down]
Nmap scan report for 10.50.1.252 [host down]
Nmap scan report for 10.50.1.253 [host down]
Nmap scan report for 10.50.1.254 [host down]
Nmap scan report for 10.50.1.255 [host down]
Initiating SYN Stealth Scan at 13:58
Scanning 17 hosts [1000 ports/host]
Discovered open port 3306/tcp on 10.50.1.101
Discovered open port 443/tcp on 10.50.1.9
Discovered open port 443/tcp on 10.50.1.8
Discovered open port 22/tcp on 10.50.1.8
Discovered open port 21/tcp on 10.50.1.104
Discovered open port 22/tcp on 10.50.1.9
Discovered open port 22/tcp on 10.50.1.10
Discovered open port 80/tcp on 10.50.1.8
Discovered open port 22/tcp on 10.50.1.11
Discovered open port 80/tcp on 10.50.1.9
Discovered open port 80/tcp on 10.50.1.111
Discovered open port 80/tcp on 10.50.1.103
Discovered open port 80/tcp on 10.50.1.100
Discovered open port 80/tcp on 10.50.1.106
Discovered open port 2222/tcp on 10.50.1.100
Discovered open port 8086/tcp on 10.50.1.108
Discovered open port 17988/tcp on 10.50.1.9
Discovered open port 3000/tcp on 10.50.1.109
Discovered open port 17988/tcp on 10.50.1.8
Discovered open port 8088/tcp on 10.50.1.108
Completed SYN Stealth Scan against 10.50.1.107 in 13.55s (16 hosts left)
Completed SYN Stealth Scan against 10.50.1.100 in 13.62s (15 hosts left)
Completed SYN Stealth Scan against 10.50.1.106 in 13.62s (14 hosts left)
Completed SYN Stealth Scan against 10.50.1.101 in 13.73s (13 hosts left)
Completed SYN Stealth Scan against 10.50.1.104 in 13.77s (12 hosts left)
Completed SYN Stealth Scan against 10.50.1.9 in 13.82s (11 hosts left)
Completed SYN Stealth Scan against 10.50.1.10 in 13.82s (10 hosts left)
Completed SYN Stealth Scan against 10.50.1.105 in 13.82s (9 hosts left)
Completed SYN Stealth Scan against 10.50.1.111 in 13.82s (8 hosts left)
Completed SYN Stealth Scan against 10.50.1.108 in 13.87s (7 hosts left)
Completed SYN Stealth Scan against 10.50.1.102 in 13.89s (6 hosts left)
Completed SYN Stealth Scan against 10.50.1.103 in 13.89s (5 hosts left)
Completed SYN Stealth Scan against 10.50.1.109 in 13.89s (4 hosts left)
Completed SYN Stealth Scan against 10.50.1.110 in 13.93s (3 hosts left)
Completed SYN Stealth Scan against 10.50.1.11 in 14.15s (2 hosts left)
Completed SYN Stealth Scan against 10.50.1.8 in 14.19s (1 host left)
Completed SYN Stealth Scan at 13:58, 14.22s elapsed (17000 total ports)
Initiating Service scan at 13:58
Scanning 20 services on 17 hosts
Completed Service scan at 14:01, 151.35s elapsed (20 services on 17 hosts)
Initiating OS detection (try #1) against 17 hosts
Retrying OS detection (try #2) against 12 hosts
Retrying OS detection (try #3) against 12 hosts
Retrying OS detection (try #4) against 12 hosts
Retrying OS detection (try #5) against 12 hosts
```

```
Initiating Traceroute at 14:01
Completed Traceroute at 14:01, 0.11s elapsed
Initiating Parallel DNS resolution of 17 hosts. at 14:01
Completed Parallel DNS resolution of 17 hosts. at 14:01, 5.53s elapsed
NSE: Script scanning 17 hosts.
Initiating NSE at 14:01
Completed NSE at 14:02, 9.73s elapsed
Initiating NSE at 14:02
Completed NSE at 14:02, 0.49s elapsed
Nmap scan report for 10.50.1.8
NSOCK ERROR [245.8580s] mksock_bind_addr(): Bind to 0.0.0.0:1016 failed (IOD #426): Intento de acceso
a un socket no permitido por sus permisos de acceso. (10013)
Host is up (0.080s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          HP Integrated Lights-Out mpSSH 0.2.1 (protocol 2.0)
| ssh-hostkey:
|   1024 0f:9e:d7:cd:c7:7c:20:be:ce:8d:24:02:40:1b:48:fa (DSA)
|_  2048 e8:45:a7:e2:0b:28:0e:6d:cf:cc:79:42:6e:86:2b:3a (RSA)
80/tcp    open  http         HPE-iLO-Server/1.30
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain
|     Connection: close
|     Date: Sat, 06 May 2017 12:59:37 GMT
|     Server: HPE-iLO-Server/1.30
|     Content-Length: 0
|   GetRequest:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain
|     Connection: close
|     Date: Sat, 06 May 2017 12:59:21 GMT
|     Server: HPE-iLO-Server/1.30
|     Content-Length: 0
|   HTTPOptions:
|     HTTP/1.1 501 Not Implemented
|     Content-Type: text/plain
|     Date: Sat, 06 May 2017 12:59:22 GMT
|     Server: HPE-iLO-Server/1.30
|     X-Frame-Options: sameorigin
|     Content-Length: 0
|   Help:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain
|     Date: Sat, 06 May 2017 12:59:57 GMT
|     Server: HPE-iLO-Server/1.30
|     X-Frame-Options: sameorigin
|     Content-Length: 0
|   LDAPSearchReq:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain
|     Date: Sat, 06 May 2017 13:00:30 GMT
|     Server: HPE-iLO-Server/1.30
|     X-Frame-Options: sameorigin
|     Content-Length: 0
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain
|     Date: Sat, 06 May 2017 13:00:30 GMT
|     Server: HPE-iLO-Server/1.30
|     X-Frame-Options: sameorigin
|     Content-Length: 0
|   LPDString:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain
|     Date: Sat, 06 May 2017 13:00:25 GMT
|     Server: HPE-iLO-Server/1.30
|     X-Frame-Options: sameorigin
|     Content-Length: 0
|   RTSPRequest:
|     HTTP/1.1 501 Not Implemented
|     Content-Type: text/plain
|     Date: Sat, 06 May 2017 12:59:27 GMT
|     Server: HPE-iLO-Server/1.30
|     X-Frame-Options: sameorigin
```

```
| Content-Length: 0
| SSLSessionReq:
| HTTP/1.1 400 Bad Request
| Content-Type: text/plain
| Date: Sat, 06 May 2017 13:00:05 GMT
| Server: HPE-iLO-Server/1.30
| X-Frame-Options: sameorigin
| Content-Length: 0
| TLSSessionReq:
| HTTP/1.1 400 Bad Request
| Content-Type: text/plain
| Date: Sat, 06 May 2017 13:00:10 GMT
| Server: HPE-iLO-Server/1.30
| X-Frame-Options: sameorigin
| Content-Length: 0
|_ http-favicon: Unknown favicon MD5: 92333CE8639E976E70CF8ABFA00CD41E
| http-methods:
|_ Supported Methods: GET HEAD POST
|_ http-server-header: HPE-iLO-Server/1.30
|_ http-title: Did not follow redirect to https://10.50.1.8/
443/tcp open ssl/https HPE-iLO-Server/1.30
| fingerprint-strings:
|_ FourOhFourRequest:
| HTTP/1.1 400 Bad Request
| Content-Type: text/plain
| Connection: close
| Date: Sat, 06 May 2017 12:59:34 GMT
| Server: HPE-iLO-Server/1.30
| Content-Length: 0
|_ GetRequest:
| HTTP/1.1 400 Bad Request
| Content-Type: text/plain
| Connection: close
| Date: Sat, 06 May 2017 12:59:28 GMT
| Server: HPE-iLO-Server/1.30
| Content-Length: 0
|_ HTTPOptions:
| HTTP/1.1 501 Not Implemented
| Content-Type: text/plain
| Date: Sat, 06 May 2017 12:59:29 GMT
| Server: HPE-iLO-Server/1.30
| X-Frame-Options: sameorigin
| Content-Length: 0
|_ Help:
| HTTP/1.1 400 Bad Request
| Content-Type: text/plain
| Date: Sat, 06 May 2017 13:00:10 GMT
| Server: HPE-iLO-Server/1.30
| X-Frame-Options: sameorigin
| Content-Length: 0
|_ LDAPSearchReq:
| HTTP/1.1 400 Bad Request
| Content-Type: text/plain
| Date: Sat, 06 May 2017 13:00:49 GMT
| Server: HPE-iLO-Server/1.30
| X-Frame-Options: sameorigin
| Content-Length: 0
|_ HTTP/1.1 400 Bad Request
| Content-Type: text/plain
| Date: Sat, 06 May 2017 13:00:49 GMT
| Server: HPE-iLO-Server/1.30
| X-Frame-Options: sameorigin
| Content-Length: 0
|_ LPDString:
| HTTP/1.1 400 Bad Request
| Content-Type: text/plain
| Date: Sat, 06 May 2017 13:00:43 GMT
| Server: HPE-iLO-Server/1.30
| X-Frame-Options: sameorigin
| Content-Length: 0
|_ RTSPRequest:
| HTTP/1.1 501 Not Implemented
| Content-Type: text/plain
| Date: Sat, 06 May 2017 12:59:50 GMT
| Server: HPE-iLO-Server/1.30
```

```
| X-Frame-Options: sameorigin
| Content-Length: 0
| SSLSessionReq:
| HTTP/1.1 400 Bad Request
| Content-Type: text/plain
| Date: Sat, 06 May 2017 13:00:18 GMT
| Server: HPE-iLO-Server/1.30
| X-Frame-Options: sameorigin
| Content-Length: 0
| TLSSessionReq:
| HTTP/1.1 400 Bad Request
| Content-Type: text/plain
| Date: Sat, 06 May 2017 13:00:23 GMT
| Server: HPE-iLO-Server/1.30
| X-Frame-Options: sameorigin
| Content-Length: 0
|_ http-favicon: Unknown favicon MD5: 92333CE8639E976E70CF8ABFA00CD41E
|_ http-methods:
|_ Supported Methods: GET
|_ http-server-header: HPE-iLO-Server/1.30
|_ http-title: Site doesn't have a title (text/html).
|_ ssl-cert: Subject: commonName=ILO2M270602M0/organizationName=Hewlett Packard
Enterprise/stateOrProvinceName=Texas/countryName=US
| Subject Alternative Name: DNS:ILO2M270602M0
| Issuer: commonName=Default Issuer (Do not trust)/organizationName=Hewlett Packard
Enterprise/stateOrProvinceName=Texas/countryName=US
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2017-02-11T02:59:49
| Not valid after: 2032-02-11T02:59:49
| MD5: bdda f34a dd29 01d5 3bb9 d66a b496 2629
| SHA-1: 244f 976d 64f6 235a 58d7 033f b09d e5f1 2d12 a2bb
|_ ssl-date: TLS randomness does not represent time
17988/tcp open ilo-vm HP Integrated Lights-Out Virtual Media
2 services unrecognized despite returning data. If you know the service/version, please submit the
following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-

service :
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF-Port80-TCP:V=7.40I=7%D=5/6%Time=590E1CF2%P=i686-pc-windows-windows%r(G
SF:etRequest,9E,"HTTP/1.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20te
SF:xt/plain\r\nConnection:\x20close\r\nDate:\x20Sat,\x2006\x20May\x202017\
SF:x2012:59:21\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30\r\nContent-Length
SF:\x200\r\n\r\n")%r(HTTPOptions,AC,"HTTP/1.1\x20501\x20Not\x20Implement
SF:ed\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat,\x2006\x20May\x202017
SF:\x2012:59:22\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30\r\nX-Frame-Optio
SF:ns:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(RTSPRequest,AC,"H
SF:TTP/1.1\x20501\x20Not\x20Implemented\r\nContent-Type:\x20text/plain\r\n
SF:nDate:\x20Sat,\x2006\x20May\x202017\x2012:59:27\x20GMT\r\nServer:\x20HP
SF:E-iLO-Server/1.30\r\nX-Frame-Options:\x20sameorigin\r\nContent-Length:
SF:\x200\r\n\r\n")%r(FourOhFourRequest,9E,"HTTP/1.1\x20400\x20Bad\x20Requ
SF:est\r\nContent-Type:\x20text/plain\r\nConnection:\x20close\r\nDate:\x20
SF:Sat,\x2006\x20May\x202017\x2012:59:37\x20GMT\r\nServer:\x20HPE-iLO-Serv
SF:er/1.30\r\nContent-Length:\x200\r\n\r\n")%r(Help,A8,"HTTP/1.1\x20400\
SF:x20Bad\x20Request\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat,\x2006
SF:\x20May\x202017\x2012:59:57\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30\r
SF:\nX-Frame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(SS
SF:LSessionReq,A8,"HTTP/1.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20
SF:text/plain\r\nDate:\x20Sat,\x2006\x20May\x202017\x2013:00:05\x20GMT\r\n
SF:Server:\x20HPE-iLO-Server/1.30\r\nX-Frame-Options:\x20sameorigin\r\nCo
SF:ntent-Length:\x200\r\n\r\n")%r(TLSSessionReq,A8,"HTTP/1.1\x20400\x20Ba
SF:d\x20Request\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat,\x2006\x20M
SF:ay\x202017\x2013:00:10\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30\r\nX-F
SF:rame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(LPDStri
SF:ng,A8,"HTTP/1.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plai
SF:n\r\nDate:\x20Sat,\x2006\x20May\x202017\x2013:00:25\x20GMT\r\nServer:\x
SF:20HPE-iLO-Server/1.30\r\nX-Frame-Options:\x20sameorigin\r\nContent-Len
SF:gth:\x200\r\n\r\n")%r(LDAPSearchReq,150,"HTTP/1.1\x20400\x20Bad\x20Req
SF:uest\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat,\x2006\x20May\x2020
SF:17\x2013:00:30\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30\r\nX-Frame-Opt
SF:ions:\x20sameorigin\r\nContent-Length:\x200\r\n\r\nHTTP/1.1\x20400\x20
SF:Bad\x20Request\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat,\x2006\x2
SF:0May\x202017\x2013:00:30\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30\r\nX
SF:-Frame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n");
```



```

=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF-Port443-TCP:V=7.40T=SSL%I=7%D=5/6%Time=590E1CF8%P=i686-pc-windows-wind
SF:ows%r(GetRequest,9E,"HTTP/1.1\x20400\x20Bad\x20Request\r\nContent-Type
SF::\x20text/plain\r\nConnection:\x20close\r\nDate:\x20Sat,\x2006\x20May\x
SF:202017\x2012:59:28\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30\r\nContent
SF:-Length:\x200\r\n\r\n")%r(HTTPOptions,AC,"HTTP/1.1\x20501\x20Not\x20Im
SF:plemented\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat,\x2006\x20May\x
SF:202017\x2012:59:28\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30\r\nX-Fram
SF:e-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(FourOhFour
SF:Request,9E,"HTTP/1.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text
SF:/plain\r\nConnection:\x20close\r\nDate:\x20Sat,\x2006\x20May\x202017\x2
SF:012:59:34\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30\r\nContent-Length:\
SF:x200\r\n\r\n")%r(RTSPRequest,AC,"HTTP/1.1\x20501\x20Not\x20Implemented
SF:\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat,\x2006\x20May\x202017\x
SF:2012:59:50\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30\r\nX-Frame-Options
SF::\x20sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(Help,A8,"HTTP/1.1\
SF:\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat
SF:,\x2006\x20May\x202017\x2013:00:10\x20GMT\r\nServer:\x20HPE-iLO-Server/
SF:1.30\r\nX-Frame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n
SF:")%r(SSLSessionReq,A8,"HTTP/1.1\x20400\x20Bad\x20Request\r\nContent-Ty
SF:pe:\x20text/plain\r\nDate:\x20Sat,\x2006\x20May\x202017\x2013:00:18\x20
SF:GMT\r\nServer:\x20HPE-iLO-Server/1.30\r\nX-Frame-Options:\x20sameorigi
SF:n\r\nContent-Length:\x200\r\n\r\n")%r(TLSSessionReq,A8,"HTTP/1.1\x2040
SF:0\x20Bad\x20Request\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat,\x20
SF:06\x20May\x202017\x2013:00:23\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30
SF:\r\nX-Frame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(
SF:LPDString,A8,"HTTP/1.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20te
SF:xt/plain\r\nDate:\x20Sat,\x2006\x20May\x202017\x2013:00:43\x20GMT\r\nSe
SF:rver:\x20HPE-iLO-Server/1.30\r\nX-Frame-Options:\x20sameorigin\r\nCont
SF:ent-Length:\x200\r\n\r\n")%r(LDAPSearchReq,150,"HTTP/1.1\x20400\x20Bad
SF:\x20Request\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat,\x2006\x20Ma
SF:y\x202017\x2013:00:49\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30\r\nX-Fr
SF:ame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\nHTTP/1.1\x20
SF:400\x20Bad\x20Request\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat,\x
SF:2006\x20May\x202017\x2013:00:49\x20GMT\r\nServer:\x20HPE-iLO-Server/1.
SF:30\r\nX-Frame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n");
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.40%E=4%D=5/6%OT=22%CT=1%CU=40717%PV=Y%DS=1%DC=T%G=Y%TM=590E1DAD
OS:%P=i686-pc-windows-windows)SEQ(SP=106%GCD=1%ISR=108%TI=I%II=I%SS=S%TS=U)
OS:SEQ(II=I)OPS(O1=M564NWONNSNNT11%O2=M564NWONNSNNT11%O3=M280NWONNT11%O4=M5
OS:64NWONNSNNT11%O5=M218NWONNSNNT11%O6=M564)WIN(W1=3018%W2=3018%W3=3110%W4=
OS:32E8%W5=3120%W6=3000)ECN(R=Y%DF=N%T=40%W=3000%O=M564%CC=N%Q=)ECN(R=N)T1(
OS:R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=N%T=4
OS:0%W=0%S=O%A=S+%F=AR%O=%RD=0%Q=)T6(R=N)T7(R=N)U1(R=Y%DF=N%T=FF%IPL=38%UN=
OS:0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=FF%CD=S)

Uptime guess: 17.133 days (since Wed Apr 19 10:50:54 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=264 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: CPE: cpe:/h:hp:integrated_lights-out

TRACEROUTE (using port 110/tcp)

HOP RTT      ADDRESS
1   68.00 ms  10.50.1.8

Nmap scan report for 10.50.1.9
Host is up (0.077s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          HP Integrated Lights-Out mpSSH 0.2.1 (protocol 2.0)
| ssh-hostkey:
|   1024 55:84:5c:31:37:45:34:dd:e9:20:ee:f3:5d:81:da:f7 (DSA)
|   2048 87:47:2f:eb:67:cd:4c:3a:8a:7c:ad:40:ac:65:80:10 (RSA)
80/tcp    open  http         HPE-iLO-Server/1.30
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain
|     Connection: close
|     Date: Sat, 06 May 2017 18:59:39 GMT
|     Server: HPE-iLO-Server/1.30
|     Content-Length: 0

```



```
| GetRequest:
|   HTTP/1.1 400 Bad Request
|   Content-Type: text/plain
|   Connection: close
|   Date: Sat, 06 May 2017 18:59:24 GMT
|   Server: HPE-iLO-Server/1.30
|   Content-Length: 0
| HTTPOptions:
|   HTTP/1.1 501 Not Implemented
|   Content-Type: text/plain
|   Date: Sat, 06 May 2017 18:59:24 GMT
|   Server: HPE-iLO-Server/1.30
|   X-Frame-Options: sameorigin
|   Content-Length: 0
| Help:
|   HTTP/1.1 400 Bad Request
|   Content-Type: text/plain
|   Date: Sat, 06 May 2017 19:00:00 GMT
|   Server: HPE-iLO-Server/1.30
|   X-Frame-Options: sameorigin
|   Content-Length: 0
| LDAPSearchReq:
|   HTTP/1.1 400 Bad Request
|   Content-Type: text/plain
|   Date: Sat, 06 May 2017 19:00:33 GMT
|   Server: HPE-iLO-Server/1.30
|   X-Frame-Options: sameorigin
|   Content-Length: 0
|   HTTP/1.1 400 Bad Request
|   Content-Type: text/plain
|   Date: Sat, 06 May 2017 19:00:33 GMT
|   Server: HPE-iLO-Server/1.30
|   X-Frame-Options: sameorigin
|   Content-Length: 0
| LPDString:
|   HTTP/1.1 400 Bad Request
|   Content-Type: text/plain
|   Date: Sat, 06 May 2017 19:00:28 GMT
|   Server: HPE-iLO-Server/1.30
|   X-Frame-Options: sameorigin
|   Content-Length: 0
| RTSPRequest:
|   HTTP/1.1 501 Not Implemented
|   Content-Type: text/plain
|   Date: Sat, 06 May 2017 18:59:29 GMT
|   Server: HPE-iLO-Server/1.30
|   X-Frame-Options: sameorigin
|   Content-Length: 0
| SSLSessionReq:
|   HTTP/1.1 400 Bad Request
|   Content-Type: text/plain
|   Date: Sat, 06 May 2017 19:00:07 GMT
|   Server: HPE-iLO-Server/1.30
|   X-Frame-Options: sameorigin
|   Content-Length: 0
| TLSSessionReq:
|   HTTP/1.1 400 Bad Request
|   Content-Type: text/plain
|   Date: Sat, 06 May 2017 19:00:12 GMT
|   Server: HPE-iLO-Server/1.30
|   X-Frame-Options: sameorigin
|   Content-Length: 0
|_ http-favicon: Unknown favicon MD5: 92333CE8639E976E70CF8ABFA00CD41E
| http-methods:
|_ Supported Methods: GET HEAD POST
|_ http-server-header: HPE-iLO-Server/1.30
|_ http-title: Did not follow redirect to https://10.50.1.9/
443/tcp open ssl/https HPE-iLO-Server/1.30
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain
|     Connection: close
|     Date: Sat, 06 May 2017 18:59:36 GMT
|     Server: HPE-iLO-Server/1.30
```

```
| Content-Length: 0
| GetRequest:
| HTTP/1.1 400 Bad Request
| Content-Type: text/plain
| Connection: close
| Date: Sat, 06 May 2017 18:59:30 GMT
| Server: HPE-iLO-Server/1.30
| Content-Length: 0
| HTTPOptions:
| HTTP/1.1 501 Not Implemented
| Content-Type: text/plain
| Date: Sat, 06 May 2017 18:59:31 GMT
| Server: HPE-iLO-Server/1.30
| X-Frame-Options: sameorigin
| Content-Length: 0
| Help:
| HTTP/1.1 400 Bad Request
| Content-Type: text/plain
| Date: Sat, 06 May 2017 19:00:13 GMT
| Server: HPE-iLO-Server/1.30
| X-Frame-Options: sameorigin
| Content-Length: 0
| LDAPSearchReq:
| HTTP/1.1 400 Bad Request
| Content-Type: text/plain
| Date: Sat, 06 May 2017 19:00:51 GMT
| Server: HPE-iLO-Server/1.30
| X-Frame-Options: sameorigin
| Content-Length: 0
| HTTP/1.1 400 Bad Request
| Content-Type: text/plain
| Date: Sat, 06 May 2017 19:00:51 GMT
| Server: HPE-iLO-Server/1.30
| X-Frame-Options: sameorigin
| Content-Length: 0
| LPDString:
| HTTP/1.1 400 Bad Request
| Content-Type: text/plain
| Date: Sat, 06 May 2017 19:00:46 GMT
| Server: HPE-iLO-Server/1.30
| X-Frame-Options: sameorigin
| Content-Length: 0
| RTSPRequest:
| HTTP/1.1 501 Not Implemented
| Content-Type: text/plain
| Date: Sat, 06 May 2017 18:59:52 GMT
| Server: HPE-iLO-Server/1.30
| X-Frame-Options: sameorigin
| Content-Length: 0
| SSLSessionReq:
| HTTP/1.1 400 Bad Request
| Content-Type: text/plain
| Date: Sat, 06 May 2017 19:00:20 GMT
| Server: HPE-iLO-Server/1.30
| X-Frame-Options: sameorigin
| Content-Length: 0
| TLSSessionReq:
| HTTP/1.1 400 Bad Request
| Content-Type: text/plain
| Date: Sat, 06 May 2017 19:00:25 GMT
| Server: HPE-iLO-Server/1.30
| X-Frame-Options: sameorigin
| Content-Length: 0
|_http-favicon: Unknown favicon MD5: 92333CE8639E976E70CF8ABFA00CD41E
|_http-methods:
|_ Supported Methods: GET
|_http-server-header: HPE-iLO-Server/1.30
|_http-title: Site doesn't have a title (text/html).
|_ssl-cert: Subject: commonName=ILO2M270602LS/organizationName=Hewlett Packard
Enterprise/stateOrProvinceName=Texas/countryName=US
| Subject Alternative Name: DNS:ILO2M270602LS
| Issuer: commonName=Default Issuer (Do not trust)/organizationName=Hewlett Packard
Enterprise/stateOrProvinceName=Texas/countryName=US
| Public Key type: rsa
| Public Key bits: 1024
```

```
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2017-02-11T05:05:22
| Not valid after: 2032-02-11T05:05:22
| MD5: 494f f34f 6dbb 6aa9 7c37 b6aa c442 4094
|_SHA-1: 2800 64cf 0f63 22e9 3267 95f0 110c 29ff 4603 6ce5
|_ssl-date: TLS randomness does not represent time
17988/tcp open ilo-vm HP Integrated Lights-Out Virtual Media
2 services unrecognized despite returning data. If you know the service/version, please submit the
following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-
```

```
service :
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF-Port80-TCP:V=7.40%I=7%D=5/6%Time=590E1CF2%P=i686-pc-windows-windows%r(G
SF:etRequest,9E,"HTTP/1.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20te
SF:xt/plain\r\nConnection:\x20close\r\nDate:\x20Sat,\x2006\x20May\x202017\
SF:\x2018:59:24\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30\r\nContent-Length
SF::\x200\r\n\r\n")%r(HTTPOptions,AC,"HTTP/1.1\x20501\x20Not\x20Implemen
SF:ed\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat,\x2006\x20May\x202017
SF:\x2018:59:24\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30\r\nX-Frame-Optio
SF:ns:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(RTSPRequest,AC,"H
SF:TTP/1.1\x20501\x20Not\x20Implemented\r\nContent-Type:\x20text/plain\r\
SF:nDate:\x20Sat,\x2006\x20May\x202017\x2018:59:29\x20GMT\r\nServer:\x20HP
SF:E-iLO-Server/1.30\r\nX-Frame-Options:\x20sameorigin\r\nContent-Length:
SF:\x200\r\n\r\n")%r(FourOhFourRequest,9E,"HTTP/1.1\x20400\x20Bad\x20Requ
SF:est\r\nContent-Type:\x20text/plain\r\nConnection:\x20close\r\nDate:\x20
SF:Sat,\x2006\x20May\x202017\x2018:59:39\x20GMT\r\nServer:\x20HPE-iLO-Serv
SF:er/1.30\r\nContent-Length:\x200\r\n\r\n")%r(Help,A8,"HTTP/1.1\x20400\
SF:\x20Bad\x20Request\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat,\x2006
SF:\x20May\x202017\x2019:00:00\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30\r
SF:\r\nX-Frame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(SS
SF:LSessionReq,A8,"HTTP/1.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20
SF:text/plain\r\nDate:\x20Sat,\x2006\x20May\x202017\x2019:00:07\x20GMT\r\n
SF:Server:\x20HPE-iLO-Server/1.30\r\nX-Frame-Options:\x20sameorigin\r\nCo
SF:ntent-Length:\x200\r\n\r\n")%r(TLSSessionReq,A8,"HTTP/1.1\x20400\x20Ba
SF:d\x20Request\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat,\x2006\x20M
SF:ay\x202017\x2019:00:12\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30\r\nX-F
SF:rame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(LPDStri
SF:ng,A8,"HTTP/1.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plai
SF:n\r\nDate:\x20Sat,\x2006\x20May\x202017\x2019:00:28\x20GMT\r\nServer:\x
SF:20HPE-iLO-Server/1.30\r\nX-Frame-Options:\x20sameorigin\r\nContent-Len
SF:gth:\x200\r\n\r\n")%r(LDAPSearchReq,150,"HTTP/1.1\x20400\x20Bad\x20Req
SF:uest\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat,\x2006\x20May\x2020
SF:17\x2019:00:33\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30\r\nX-Frame-Opt
SF:ions:\x20sameorigin\r\nContent-Length:\x200\r\n\r\nHTTP/1.1\x20400\x20
SF:Bad\x20Request\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat,\x2006\x2
SF:0May\x202017\x2019:00:33\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30\r\nX
SF:-Frame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n");
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF-Port443-TCP:V=7.40%T=SSL%I=7%D=5/6%Time=590E1CF8%P=i686-pc-windows-wind
SF:ows%r(GetRequest,9E,"HTTP/1.1\x20400\x20Bad\x20Request\r\nContent-Type
SF::\x20text/plain\r\nConnection:\x20close\r\nDate:\x20Sat,\x2006\x20May\x
SF:202017\x2018:59:30\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30\r\nContent
SF:-Length:\x200\r\n\r\n")%r(HTTPOptions,AC,"HTTP/1.1\x20501\x20Not\x20Im
SF:plemented\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat,\x2006\x20May\
SF:SF:\x202017\x2018:59:31\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30\r\nX-Fram
SF:e-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(FourOhFour
SF:Request,9E,"HTTP/1.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text
SF:/plain\r\nConnection:\x20close\r\nDate:\x20Sat,\x2006\x20May\x202017\x2
SF:018:59:36\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30\r\nContent-Length:\
SF:\x200\r\n\r\n")%r(RTSPRequest,AC,"HTTP/1.1\x20501\x20Not\x20Implemented
SF:/r\nContent-Type:\x20text/plain\r\nDate:\x20Sat,\x2006\x20May\x202017\x
SF:2018:59:52\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30\r\nX-Frame-Options
SF::\x20sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(Help,A8,"HTTP/1.1\
SF:\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat
SF:,\x2006\x20May\x202017\x2019:00:13\x20GMT\r\nServer:\x20HPE-iLO-Server/
SF:1.30\r\nX-Frame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n
SF:")%r(TLSSessionReq,A8,"HTTP/1.1\x20400\x20Bad\x20Request\r\nContent-Ty
SF:pe:\x20text/plain\r\nDate:\x20Sat,\x2006\x20May\x202017\x2019:00:20\x20
SF:GMT\r\nServer:\x20HPE-iLO-Server/1.30\r\nX-Frame-Options:\x20sameorigi
SF:n\r\nContent-Length:\x200\r\n\r\n")%r(TLSSessionReq,A8,"HTTP/1.1\x2040
SF:0\x20Bad\x20Request\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat,\x20
SF:06\x20May\x202017\x2019:00:25\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30
SF:/r\nX-Frame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(
SF:LPDString,A8,"HTTP/1.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20te
SF:xt/plain\r\nDate:\x20Sat,\x2006\x20May\x202017\x2019:00:46\x20GMT\r\nSe
```

```
SF: rver:\x20HPE-iLO-Server/1\ .30\r\nX-Frame-Options:\x20sameorigin\r\nCont
SF: ent-Length:\x200\r\n\r\n") %r (LDAPSearchReq,150,"HTTP/1\ .1\x20400\x20Bad
SF: \x20Request\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat,\x2006\x20Ma
SF: y\x202017\x2019:00:51\x20GMT\r\nServer:\x20HPE-iLO-Server/1\ .30\r\nX-Fr
SF: ame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\nHTTP/1\ .1\x20
SF: 400\x20Bad\x20Request\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat,\x
SF: 2006\x20May\x202017\x2019:00:51\x20GMT\r\nServer:\x20HPE-iLO-Server/1\ .
SF: 30\r\nX-Frame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n");
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS: SCAN (V=7.40%E=4%D=5/6%OT=22%CT=1%CU=40319%PV=Y%DS=1%DC=T%G=Y%TM=590E1DAD
OS: %P=i686-pc-windows-windows) SEQ (SP=105%GCD=1%ISR=108%TI=I%II=I%SS=S%TS=U)
OS: SEQ (II=I) OPS (O1=M564NWNNSNNT11%O2=M564NWNNSNNT11%O3=M280NWNNT11%O4=M5
OS: 64NWNNSNNT11%O5=M218NWNNSNNT11%O6=M564) WIN (W1=3018%W2=3018%W3=3110%W4=
OS: 32E8%W5=3120%W6=3000) ECN (R=Y%DF=N%T=40%W=3000%O=M564%CC=N%Q=) ECN (R=N) T1 (
OS: R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=) T2 (R=N) T3 (R=N) T4 (R=N) T5 (R=Y%DF=N%T=4
OS: 0%W=0%S=O%A=S+%F=AR%O=RD=0%Q=) T6 (R=N) T7 (R=N) U1 (R=Y%DF=N%T=FF%IPL=38%UN=
OS: 0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G) IE (R=Y%DFI=N%T=FF%CD=S)

Uptime guess: 16.816 days (since Wed Apr 19 18:27:17 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: CPE: cpe:/h:hp:integrated_lights-out

TRACEROUTE (using port 110/tcp)
HOP RTT ADDRESS
1 55.00 ms 10.50.1.9

Nmap scan report for 10.50.1.10
Host is up (0.12s latency).
Not shown: 999 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 7f:39:aa:4c:91:8c:13:cc:11:44:ad:d0:44:26:45:9c (RSA)
|_ 256 7e:d3:1e:99:39:13:cb:1b:5e:1c:07:46:a8:50:dc:e8 (ECDSA)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS: SCAN (V=7.40%E=4%D=5/6%OT=22%CT=1%CU=40360%PV=Y%DS=1%DC=T%G=Y%TM=590E1DAD
OS: %P=i686-pc-windows-windows) SEQ (SP=107%GCD=1%ISR=10C%TI=Z%II=I%TS=8) SEQ (I
OS: I=I) OPS (O1=M564ST11NW7%O2=M564ST11NW7%O3=M564NNT11NW7%O4=M564ST11NW7%O5=
OS: M564ST11NW7%O6=M564ST11) WIN (W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7
OS: 120) ECN (R=Y%DF=Y%T=40%W=7210%O=M564NNSNW7%CC=Y%Q=) ECN (R=N) T1 (R=Y%DF=Y%T=
OS: 40%S=O%A=S+%F=AS%RD=0%Q=) T2 (R=N) T3 (R=N) T4 (R=N) T5 (R=Y%DF=Y%T=40%W=0%S=O%A
OS: S+S%F=AR%O=RD=0%Q=) T6 (R=N) T7 (R=N) U1 (R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%R
OS: ID=G%RIPCK=G%RUCK=G%RUD=G) IE (R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 110/tcp)
HOP RTT ADDRESS
1 65.00 ms 10.50.1.10

Nmap scan report for 10.50.1.11
Host is up (0.12s latency).
Not shown: 999 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 77:e6:7d:63:90:8e:79:da:08:b6:23:cb:2c:93:b0:6a (RSA)
|_ 256 8b:65:a5:a8:17:85:ef:8f:3c:9c:92:1e:bd:27:67:dc (ECDSA)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS: SCAN (V=7.40%E=4%D=5/6%OT=22%CT=1%CU=33489%PV=Y%DS=1%DC=T%G=Y%TM=590E1DAD
OS: %P=i686-pc-windows-windows) SEQ (SP=102%GCD=1%ISR=10A%TI=Z%II=I%TS=8) SEQ (S
OS: P=103%GCD=1%ISR=10A%TI=Z%TS=8) SEQ (II=I) OPS (O1=M564ST11NW7%O2=M564ST11NW7
OS: %O3=M564NNT11NW7%O4=M564ST11NW7%O5=M564ST11NW7%O6=M564ST11) WIN (W1=7120%W
OS: 2=7120%W3=7120%W4=7120%W5=7120%W6=7120) ECN (R=Y%DF=Y%T=40%W=7210%O=M564NN
OS: SNW7%CC=Y%Q=) ECN (R=N) T1 (R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=) T2 (R=N) T3 (R=
OS: N) T4 (R=N) T5 (R=Y%DF=Y%T=40%W=0%S=O%A=S+%F=AR%O=RD=0%Q=) T6 (R=N) T7 (R=N) U1 (
OS: R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G) IE (R=Y%DFI=
OS: N%T=40%CD=S)
```

```
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 110/tcp)
HOP RTT      ADDRESS
1   71.00 ms 10.50.1.11

Nmap scan report for 10.50.1.100
Host is up (0.12s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.18
|_ http-ls: Volume /
|_ maxfiles limit reached (10)
|_ SIZE  TIME      FILENAME
|_ 0     2017-05-05 01:30  datos.txt
|_ 19    2017-05-04 22:35  echo.php
|_ 20    2017-05-04 22:35  echo1.php
|_ -     2017-05-05 01:51  fotos/
|_ -     2017-05-05 00:23  includes/
|_ 339   2017-05-05 01:04  includes/conecta.php
|_ 220   2017-05-04 23:07  includes/conecta_panoramicos.php
|_ 1.2K  2017-05-05 00:49  includes/demo.php
|_ 17K   2017-05-05 00:55  includes/ez_sql_core.php
|_ 7.1K  2017-05-04 23:25  includes/ez_sql_mysql.php
|_
|_ http-methods:
|_ Supported Methods: POST OPTIONS GET HEAD
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Index of /
2222/tcp  open  ssh       OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 2048 32:31:d3:75:d3:4a:cb:55:09:94:c4:37:c5:b0:b2:db (RSA)
|_ 256  90:8a:22:78:4e:ae:67:55:0c:ee:79:e0:e0:2e:36:15 (ECDSA)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.40%E=4%D=5/6%OT=80%CT=1%CU=35995%PV=Y%DS=1%DC=T%G=Y%TM=590E1DAD
OS:%P=i686-pc-windows-windows) SEQ(SP=100%GCD=1%ISR=10A%TI=Z%II=I%TS=8) SEQ(I
OS:I=I) OPS(O1=M564ST11NW7%O2=M564ST11NW7%O3=M564NNT11NW7%O4=M564ST11NW7%O5=
OS:M564ST11NW7%O6=M564ST11) WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7
OS:120) ECN(R=Y%DF=Y%T=40%W=7210%O=M564NNSNW7%CC=Y%Q=) ECN(R=N) T1(R=Y%DF=Y%T=
OS:40%S=O%A=S+%F=AS%RD=0%Q=) T2(R=N) T3(R=N) T4(R=N) T5(R=Y%DF=Y%T=40%W=0%S=O%A
OS:=S+%F=AR%O=%RD=0%Q=) T6(R=N) T7(R=N) U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%R
OS:ID=G%RIPCK=G%RUCK=G%RUD=G) IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop
Service Info: Host: 127.0.1.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 110/tcp)
HOP RTT      ADDRESS
1   49.00 ms 10.50.1.100

Nmap scan report for 10.50.1.101
Host is up (0.12s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
3306/tcp  open  mysql     MySQL 5.7.17-0ubuntu0.16.04.2
|_ mysql-info:
|_ Protocol: 10
|_ Version: 5.7.17-0ubuntu0.16.04.2
|_ Thread ID: 67327
|_ Capabilities flags: 63487
|_ Some Capabilities: Speaks41ProtocolOld, SupportsCompression, LongPassword, SupportsTransactions,
Support41Auth, ConnectWithDatabase, InteractiveClient,
gnoreSpaceBeforeParenthesis, Speaks41ProtocolNew, FoundRows, SupportsLoadDataLocal,
DontAllowDatabaseTableName, LongColumnFlag, ODBCClient, IgnoreSigpipes

SupportsMultipleResults, SupportsMultipleStatements, SupportsAuthPlugins
|_ Status: Autocommit
|_ Salt: \x14,\x01\x7Fh\x06i+v\x0ERh"*h4Hr!9
|_ Auth Plugin Name: 96
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.40%E=4%D=5/6%OT=3306%CT=1%CU=31376%PV=Y%DS=1%DC=T%G=Y%TM=590E1D
```

```
OS:AD%P=i686-pc-windows-windows) SEQ (SP=107%GCD=1%ISR=10A%TI=Z%II=I%TS=8) SEQ
OS: (II=I) OPS (O1=M564ST11NW7%O2=M564ST11NW7%O3=M564NNT11NW7%O4=M564ST11NW7%O
OS:5=M564ST11NW7%O6=M564ST11) WIN (W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6
OS:=7120) ECN (R=Y%DF=Y%T=40%W=7210%O=M564NNSNW7%CC=Y%Q=) ECN (R=N) T1 (R=Y%DF=Y%
OS:T=40%S=O%A=S+%F=AS%RD=0%Q=) T2 (R=N) T3 (R=N) T4 (R=N) T5 (R=Y%DF=Y%T=40%W=0%S=O
OS:%A=S+%F=AR%O=RD=0%Q=) T6 (R=N) T7 (R=N) U1 (R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G
OS:%RID=G%RIPCK=G%RUCK=G%RUD=G) IE (R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop

TRACEROUTE (using port 110/tcp)
HOP RTT ADDRESS
1 66.00 ms 10.50.1.101

Nmap scan report for 10.50.1.102
Host is up (0.061s latency).
All 1000 scanned ports on 10.50.1.102 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE (using port 110/tcp)
HOP RTT ADDRESS
1 44.00 ms 10.50.1.102

Nmap scan report for 10.50.1.103
Host is up (0.12s latency).
Not shown: 999 closed ports
PORT STATE SERVICE VERSION
80/tcp open http nginx 1.10.0 (Ubuntu)
|_ http-favicon: Unknown favicon MD5: 2958DC82E3B3052BABAC794A2BB97EB2
|_ http-methods:
|_ Supported Methods: GET HEAD POST
|_ http-server-header: nginx/1.10.0 (Ubuntu)
|_ http-title: IEC
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN (V=7.40%E=4%D=5/6%OT=80%CT=1%CU=39358%PV=Y%DS=1%DC=T%G=Y%TM=590E1DAD
OS:%P=i686-pc-windows-windows) SEQ (SP=100%GCD=1%ISR=107%TI=Z%II=I%TS=8) SEQ (S
OS:P=100%GCD=1%ISR=107%TI=Z%TS=8) SEQ (II=I) OPS (O1=M564ST11NW7%O2=M564ST11NW7
OS:%O3=M564NNT11NW7%O4=M564ST11NW7%O5=M564ST11NW7%O6=M564ST11) WIN (W1=7120%W
OS:2=7120%W3=7120%W4=7120%W5=7120%W6=7120) ECN (R=Y%DF=Y%T=40%W=7210%O=M564NN
OS:SNW7%CC=Y%Q=) ECN (R=N) T1 (R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=) T2 (R=N) T3 (R=
OS:N) T4 (R=N) T5 (R=Y%DF=Y%T=40%W=0%S=O%A=S+%F=AR%O=RD=0%Q=) T6 (R=N) T7 (R=N) U1 (
OS:R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G) IE (R=Y%DFI=
OS:N%T=40%CD=S)

Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 110/tcp)
HOP RTT ADDRESS
1 61.00 ms 10.50.1.103

Nmap scan report for 10.50.1.104
Host is up (0.12s latency).
Not shown: 999 closed ports
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.0.8 or later
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN (V=7.40%E=4%D=5/6%OT=21%CT=1%CU=30864%PV=Y%DS=1%DC=T%G=Y%TM=590E1DAD
OS:%P=i686-pc-windows-windows) SEQ (SP=105%GCD=1%ISR=10C%TI=Z%II=I%TS=8) SEQ (I
OS:I=I) OPS (O1=M564ST11NW7%O2=M564ST11NW7%O3=M564NNT11NW7%O4=M564ST11NW7%O5=
OS:M564ST11NW7%O6=M564ST11) WIN (W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7
OS:120) ECN (R=Y%DF=Y%T=40%W=7210%O=M564NNSNW7%CC=Y%Q=) ECN (R=N) T1 (R=Y%DF=Y%T=
OS:40%S=O%A=S+%F=AS%RD=0%Q=) T2 (R=N) T3 (R=N) T4 (R=N) T5 (R=Y%DF=Y%T=40%W=0%S=O%A
OS:=S+%F=AR%O=RD=0%Q=) T6 (R=N) T7 (R=N) U1 (R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%R
OS:ID=G%RIPCK=G%RUCK=G%RUD=G) IE (R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop

TRACEROUTE (using port 110/tcp)
HOP RTT ADDRESS
1 47.00 ms 10.50.1.104
```

```
Nmap scan report for 10.50.1.105
Host is up (0.062s latency).
All 1000 scanned ports on 10.50.1.105 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE (using port 110/tcp)
HOP RTT      ADDRESS
1    44.00 ms  10.50.1.105

Nmap scan report for 10.50.1.106
Host is up (0.12s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.18 ((Ubuntu))
|_ http-methods:
|_   Supported Methods: POST OPTIONS GET HEAD
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Apache2 Ubuntu Default Page: It works
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.40%E=4%D=5/6%OT=80%CT=1%CU=44634%PV=Y%DS=1%DC=T%G=Y%TM=590E1DAD
OS:%P=i686-pc-windows-windows) SEQ(SP=106%GCD=1%ISR=10D%TI=Z%II=I%TS=8) SEQ(I
OS:I=I) OPS(O1=M564ST11NW7%O2=M564ST11NW7%O3=M564NNT11NW7%O4=M564ST11NW7%O5=
OS:M564ST11NW7%O6=M564ST11) WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7
OS:120) ECN(R=Y%DF=Y%T=40%W=7210%O=M564NNSNW7%CC=Y%Q=) ECN(R=N) T1(R=Y%DF=Y%T=
OS:40%S=O%A=S+%F=AS%RD=0%Q=) T2(R=N) T3(R=N) T4(R=N) T5(R=Y%DF=Y%T=40%W=0%S=O%A
OS:=S+%F=AR%O=RD=0%Q=) T6(R=N) T7(R=N) U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%R
OS:ID=G%RIPCK=G%RUCK=G%RUD=G) IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop

TRACEROUTE (using port 110/tcp)
HOP RTT      ADDRESS
1    28.00 ms  10.50.1.106

Nmap scan report for 10.50.1.107
Host is up (0.052s latency).
All 1000 scanned ports on 10.50.1.107 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE (using port 110/tcp)
HOP RTT      ADDRESS
1    30.00 ms  10.50.1.107

Nmap scan report for 10.50.1.108
Host is up (0.073s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
8086/tcp  open  http    InfluxDB http admin 1.2.2
|_ http-title: Site doesn't have a title (text/plain; charset=utf-8).
8088/tcp  open  radan-http?
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.40%E=4%D=5/6%OT=8086%CT=1%CU=44130%PV=Y%DS=1%DC=T%G=Y%TM=590E1D
OS:AD%P=i686-pc-windows-windows) SEQ(SP=106%GCD=1%ISR=10A%TI=Z%II=I%TS=8) SEQ
OS:(I=I) OPS(O1=M564ST11NW7%O2=M564ST11NW7%O3=M564NNT11NW7%O4=M564ST11NW7%O
OS:5=M564ST11NW7%O6=M564ST11) WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6
OS:=7120) ECN(R=Y%DF=Y%T=40%W=7210%O=M564NNSNW7%CC=Y%Q=) ECN(R=N) T1(R=Y%DF=Y%
OS:T=40%S=O%A=S+%F=AS%RD=0%Q=) T2(R=N) T3(R=N) T4(R=N) T5(R=Y%DF=Y%T=40%W=0%S=O
OS:%A=S+%F=AR%O=RD=0%Q=) T6(R=N) T7(R=N) U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G
OS:%RID=G%RIPCK=G%RUCK=G%RUD=G) IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop

TRACEROUTE (using port 110/tcp)
HOP RTT      ADDRESS
1    28.00 ms  10.50.1.108

Nmap scan report for 10.50.1.109
Host is up (0.10s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
3000/tcp  open  http    Grafana
```



```
| http-methods:
|_ Supported Methods: GET HEAD
| http-robots.txt: 1 disallowed entry
|_/
| http-title: Grafana
|_ Requested resource was /login
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.40%E=4%D=5/6%OT=3000%CT=1%CU=43580%PV=Y%DS=1%DC=T%G=Y%TM=590E1D
OS:AD%P=i686-pc-windows-windows) SEQ(SP=103%GCD=1%ISR=10B%TI=Z%II=I%TS=8) SEQ
OS:(II=I) OPS(Ol=M564ST11NW7%O2=M564ST11NW7%O3=M564NNT11NW7%O4=M564ST11NW7%O
OS:5=M564ST11NW7%O6=M564ST11) WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6
OS:=7120) ECN(R=Y%DF=Y%T=40%W=7210%O=M564NNSNW7%CC=Y%Q=) ECN(R=N) T1(R=Y%DF=Y%
OS:T=40%S=O%A=S+%F=AS%RD=0%Q=) T2(R=N) T3(R=N) T4(R=N) T5(R=Y%DF=Y%T=40%W=0%S=O
OS:%A=S+%F=AR%O=RD=0%Q=) T6(R=N) T7(R=N) U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G
OS:%RID=G%RIPCK=G%RUCK=G%RUD=G) IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop

TRACEROUTE (using port 110/tcp)
HOP RTT ADDRESS
1 30.00 ms 10.50.1.109

Nmap scan report for 10.50.1.110
Host is up (0.052s latency).
All 1000 scanned ports on 10.50.1.110 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE (using port 110/tcp)
HOP RTT ADDRESS
1 28.00 ms 10.50.1.110

Nmap scan report for 10.50.1.111
Host is up (0.072s latency).
Not shown: 999 closed ports
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.4.18
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Index of /
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.40%E=4%D=5/6%OT=80%CT=1%CU=32236%PV=Y%DS=1%DC=T%G=Y%TM=590E1DAD
OS:%P=i686-pc-windows-windows) SEQ(SP=FB%GCD=1%ISR=110%TI=Z%II=I%TS=8) SEQ(II
OS:=I) OPS(Ol=M564ST11NW7%O2=M564ST11NW7%O3=M564NNT11NW7%O4=M564ST11NW7%O5=M
OS:564ST11NW7%O6=M564ST11) WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=71
OS:20) ECN(R=Y%DF=Y%T=40%W=7210%O=M564NNSNW7%CC=Y%Q=) ECN(R=N) T1(R=Y%DF=Y%T=4
OS:0%S=O%A=S+%F=AS%RD=0%Q=) T2(R=N) T3(R=N) T4(R=N) T5(R=Y%DF=Y%T=40%W=0%S=O%A=
OS:S+%F=AR%O=RD=0%Q=) T6(R=N) T7(R=N) U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RI
OS:D=G%RIPCK=G%RUCK=G%RUD=G) IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop
Service Info: Host: 127.0.1.1

TRACEROUTE (using port 110/tcp)
HOP RTT ADDRESS
1 33.00 ms 10.50.1.111

Nmap scan report for 10.50.1.127
Host is up (0.051s latency).
All 1000 scanned ports on 10.50.1.127 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE (using port 110/tcp)
HOP RTT ADDRESS
1 34.00 ms 10.50.1.127

Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-06 13:57 Hora de verano central (México)
NSE: Loaded 143 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 13:58
Completed NSE at 13:58, 0.00s elapsed
```



```
Initiating NSE at 13:58
Completed NSE at 13:58, 0.00s elapsed
Initiating Ping Scan at 13:58
Scanning 256 hosts [4 ports/host]
Completed Ping Scan at 13:58, 4.94s elapsed (256 total hosts)
Initiating Parallel DNS resolution of 256 hosts. at 13:58
Completed Parallel DNS resolution of 256 hosts. at 13:58, 11.02s elapsed
Nmap scan report for 10.50.1.0 [host down]
Nmap scan report for 10.50.1.1 [host down]
Nmap scan report for 10.50.1.2 [host down]
Nmap scan report for 10.50.1.3 [host down]
Nmap scan report for 10.50.1.4 [host down]
Nmap scan report for 10.50.1.5 [host down]
Nmap scan report for 10.50.1.6 [host down]
Nmap scan report for 10.50.1.7 [host down]
Nmap scan report for 10.50.1.12 [host down]
Nmap scan report for 10.50.1.13 [host down]
Nmap scan report for 10.50.1.14 [host down]
Nmap scan report for 10.50.1.15 [host down]
Nmap scan report for 10.50.1.16 [host down]
Nmap scan report for 10.50.1.17 [host down]
Nmap scan report for 10.50.1.18 [host down]
Nmap scan report for 10.50.1.19 [host down]
Nmap scan report for 10.50.1.20 [host down]
Nmap scan report for 10.50.1.21 [host down]
Nmap scan report for 10.50.1.22 [host down]
Nmap scan report for 10.50.1.23 [host down]
Nmap scan report for 10.50.1.24 [host down]
Nmap scan report for 10.50.1.25 [host down]
Nmap scan report for 10.50.1.26 [host down]
Nmap scan report for 10.50.1.27 [host down]
Nmap scan report for 10.50.1.28 [host down]
Nmap scan report for 10.50.1.29 [host down]
Nmap scan report for 10.50.1.30 [host down]
Nmap scan report for 10.50.1.31 [host down]
Nmap scan report for 10.50.1.32 [host down]
Nmap scan report for 10.50.1.33 [host down]
Nmap scan report for 10.50.1.34 [host down]
Nmap scan report for 10.50.1.35 [host down]
Nmap scan report for 10.50.1.36 [host down]
Nmap scan report for 10.50.1.37 [host down]
Nmap scan report for 10.50.1.38 [host down]
Nmap scan report for 10.50.1.39 [host down]
Nmap scan report for 10.50.1.40 [host down]
Nmap scan report for 10.50.1.41 [host down]
Nmap scan report for 10.50.1.42 [host down]
Nmap scan report for 10.50.1.43 [host down]
Nmap scan report for 10.50.1.44 [host down]
Nmap scan report for 10.50.1.45 [host down]
Nmap scan report for 10.50.1.46 [host down]
Nmap scan report for 10.50.1.47 [host down]
Nmap scan report for 10.50.1.48 [host down]
Nmap scan report for 10.50.1.49 [host down]
Nmap scan report for 10.50.1.50 [host down]
Nmap scan report for 10.50.1.51 [host down]
Nmap scan report for 10.50.1.52 [host down]
Nmap scan report for 10.50.1.53 [host down]
Nmap scan report for 10.50.1.54 [host down]
Nmap scan report for 10.50.1.55 [host down]
Nmap scan report for 10.50.1.56 [host down]
Nmap scan report for 10.50.1.57 [host down]
Nmap scan report for 10.50.1.58 [host down]
Nmap scan report for 10.50.1.59 [host down]
Nmap scan report for 10.50.1.60 [host down]
Nmap scan report for 10.50.1.61 [host down]
Nmap scan report for 10.50.1.62 [host down]
Nmap scan report for 10.50.1.63 [host down]
Nmap scan report for 10.50.1.64 [host down]
Nmap scan report for 10.50.1.65 [host down]
Nmap scan report for 10.50.1.66 [host down]
Nmap scan report for 10.50.1.67 [host down]
Nmap scan report for 10.50.1.68 [host down]
Nmap scan report for 10.50.1.69 [host down]
Nmap scan report for 10.50.1.70 [host down]
Nmap scan report for 10.50.1.71 [host down]
```



```
Nmap scan report for 10.50.1.235 [host down]
Nmap scan report for 10.50.1.236 [host down]
Nmap scan report for 10.50.1.237 [host down]
Nmap scan report for 10.50.1.238 [host down]
Nmap scan report for 10.50.1.239 [host down]
Nmap scan report for 10.50.1.240 [host down]
Nmap scan report for 10.50.1.241 [host down]
Nmap scan report for 10.50.1.242 [host down]
Nmap scan report for 10.50.1.243 [host down]
Nmap scan report for 10.50.1.244 [host down]
Nmap scan report for 10.50.1.245 [host down]
Nmap scan report for 10.50.1.246 [host down]
Nmap scan report for 10.50.1.247 [host down]
Nmap scan report for 10.50.1.248 [host down]
Nmap scan report for 10.50.1.249 [host down]
Nmap scan report for 10.50.1.250 [host down]
Nmap scan report for 10.50.1.251 [host down]
Nmap scan report for 10.50.1.252 [host down]
Nmap scan report for 10.50.1.253 [host down]
Nmap scan report for 10.50.1.254 [host down]
Nmap scan report for 10.50.1.255 [host down]
Initiating SYN Stealth Scan at 13:58
Scanning 17 hosts (1000 ports/host)
Discovered open port 3306/tcp on 10.50.1.101
Discovered open port 443/tcp on 10.50.1.9
Discovered open port 443/tcp on 10.50.1.8
Discovered open port 22/tcp on 10.50.1.8
Discovered open port 21/tcp on 10.50.1.104
Discovered open port 22/tcp on 10.50.1.9
Discovered open port 22/tcp on 10.50.1.10
Discovered open port 80/tcp on 10.50.1.8
Discovered open port 22/tcp on 10.50.1.11
Discovered open port 80/tcp on 10.50.1.9
Discovered open port 80/tcp on 10.50.1.111
Discovered open port 80/tcp on 10.50.1.103
Discovered open port 80/tcp on 10.50.1.100
Discovered open port 80/tcp on 10.50.1.106
Discovered open port 2222/tcp on 10.50.1.100
Discovered open port 8086/tcp on 10.50.1.108
Discovered open port 17988/tcp on 10.50.1.9
Discovered open port 3000/tcp on 10.50.1.109
Discovered open port 17988/tcp on 10.50.1.8
Discovered open port 8088/tcp on 10.50.1.108
Completed SYN Stealth Scan against 10.50.1.107 in 13.55s (16 hosts left)
Completed SYN Stealth Scan against 10.50.1.100 in 13.62s (15 hosts left)
Completed SYN Stealth Scan against 10.50.1.106 in 13.62s (14 hosts left)
Completed SYN Stealth Scan against 10.50.1.101 in 13.73s (13 hosts left)
Completed SYN Stealth Scan against 10.50.1.104 in 13.77s (12 hosts left)
Completed SYN Stealth Scan against 10.50.1.9 in 13.82s (11 hosts left)
Completed SYN Stealth Scan against 10.50.1.10 in 13.82s (10 hosts left)
Completed SYN Stealth Scan against 10.50.1.105 in 13.82s (9 hosts left)
Completed SYN Stealth Scan against 10.50.1.111 in 13.82s (8 hosts left)
Completed SYN Stealth Scan against 10.50.1.108 in 13.87s (7 hosts left)
Completed SYN Stealth Scan against 10.50.1.102 in 13.89s (6 hosts left)
Completed SYN Stealth Scan against 10.50.1.103 in 13.89s (5 hosts left)
Completed SYN Stealth Scan against 10.50.1.109 in 13.89s (4 hosts left)
Completed SYN Stealth Scan against 10.50.1.110 in 13.93s (3 hosts left)
Completed SYN Stealth Scan against 10.50.1.11 in 14.15s (2 hosts left)
Completed SYN Stealth Scan against 10.50.1.8 in 14.19s (1 host left)
Completed SYN Stealth Scan at 13:58, 14.22s elapsed (17000 total ports)
Initiating Service scan at 13:58
Scanning 20 services on 17 hosts
Completed Service scan at 14:01, 151.35s elapsed (20 services on 17 hosts)
Initiating OS detection (try #1) against 17 hosts
Retrying OS detection (try #2) against 12 hosts
Retrying OS detection (try #3) against 12 hosts
Retrying OS detection (try #4) against 12 hosts
Retrying OS detection (try #5) against 12 hosts
Initiating Traceroute at 14:01
Completed Traceroute at 14:01, 0.11s elapsed
Initiating Parallel DNS resolution of 17 hosts. at 14:01
Completed Parallel DNS resolution of 17 hosts. at 14:01, 5.53s elapsed
NSE: Script scanning 17 hosts.
Initiating NSE at 14:01
Completed NSE at 14:02, 9.73s elapsed
```

```
Initiating NSE at 14:02
Completed NSE at 14:02, 0.49s elapsed
Nmap scan report for 10.50.1.8
NSOCK ERROR [245.8580s] mksock_bind_addr(): Bind to 0.0.0.0:1016 failed (IOD #426): Intento de acceso
a un socket no permitido por sus permisos de acceso. (10013)
Host is up (0.080s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          HP Integrated Lights-Out mpSSH 0.2.1 (protocol 2.0)
| ssh-hostkey:
|   1024 0f:9e:d7:cd:c7:7c:20:be:ce:8d:24:02:40:1b:48:fa (DSA)
|_  2048 e8:45:a7:e2:0b:28:0e:6d:cf:cc:79:42:6e:86:2b:3a (RSA)
80/tcp    open  http         HPE-iLO-Server/1.30
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain
|     Connection: close
|     Date: Sat, 06 May 2017 12:59:37 GMT
|     Server: HPE-iLO-Server/1.30
|     Content-Length: 0
|   GetRequest:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain
|     Connection: close
|     Date: Sat, 06 May 2017 12:59:21 GMT
|     Server: HPE-iLO-Server/1.30
|     Content-Length: 0
|   HTTPOptions:
|     HTTP/1.1 501 Not Implemented
|     Content-Type: text/plain
|     Date: Sat, 06 May 2017 12:59:22 GMT
|     Server: HPE-iLO-Server/1.30
|     X-Frame-Options: sameorigin
|     Content-Length: 0
|   Help:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain
|     Date: Sat, 06 May 2017 12:59:57 GMT
|     Server: HPE-iLO-Server/1.30
|     X-Frame-Options: sameorigin
|     Content-Length: 0
|   LDAPSearchReq:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain
|     Date: Sat, 06 May 2017 13:00:30 GMT
|     Server: HPE-iLO-Server/1.30
|     X-Frame-Options: sameorigin
|     Content-Length: 0
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain
|     Date: Sat, 06 May 2017 13:00:30 GMT
|     Server: HPE-iLO-Server/1.30
|     X-Frame-Options: sameorigin
|     Content-Length: 0
|   LPDString:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain
|     Date: Sat, 06 May 2017 13:00:25 GMT
|     Server: HPE-iLO-Server/1.30
|     X-Frame-Options: sameorigin
|     Content-Length: 0
|   RTSPRequest:
|     HTTP/1.1 501 Not Implemented
|     Content-Type: text/plain
|     Date: Sat, 06 May 2017 12:59:27 GMT
|     Server: HPE-iLO-Server/1.30
|     X-Frame-Options: sameorigin
|     Content-Length: 0
|   SSLSessionReq:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain
|     Date: Sat, 06 May 2017 13:00:05 GMT
|     Server: HPE-iLO-Server/1.30
|     X-Frame-Options: sameorigin
```

```
| Content-Length: 0
| TLSSessionReq:
| HTTP/1.1 400 Bad Request
| Content-Type: text/plain
| Date: Sat, 06 May 2017 13:00:10 GMT
| Server: HPE-iLO-Server/1.30
| X-Frame-Options: sameorigin
| Content-Length: 0
|_ http-favicon: Unknown favicon MD5: 92333CE8639E976E70CF8ABFA00CD41E
|_ http-methods:
|_ Supported Methods: GET HEAD POST
|_ http-server-header: HPE-iLO-Server/1.30
|_ http-title: Did not follow redirect to https://10.50.1.8/
443/tcp open ssl/https HPE-iLO-Server/1.30
| fingerprint-strings:
| FourOhFourRequest:
| HTTP/1.1 400 Bad Request
| Content-Type: text/plain
| Connection: close
| Date: Sat, 06 May 2017 12:59:34 GMT
| Server: HPE-iLO-Server/1.30
| Content-Length: 0
| GetRequest:
| HTTP/1.1 400 Bad Request
| Content-Type: text/plain
| Connection: close
| Date: Sat, 06 May 2017 12:59:28 GMT
| Server: HPE-iLO-Server/1.30
| Content-Length: 0
| HTTPOptions:
| HTTP/1.1 501 Not Implemented
| Content-Type: text/plain
| Date: Sat, 06 May 2017 12:59:29 GMT
| Server: HPE-iLO-Server/1.30
| X-Frame-Options: sameorigin
| Content-Length: 0
| Help:
| HTTP/1.1 400 Bad Request
| Content-Type: text/plain
| Date: Sat, 06 May 2017 13:00:10 GMT
| Server: HPE-iLO-Server/1.30
| X-Frame-Options: sameorigin
| Content-Length: 0
| LDAPSearchReq:
| HTTP/1.1 400 Bad Request
| Content-Type: text/plain
| Date: Sat, 06 May 2017 13:00:49 GMT
| Server: HPE-iLO-Server/1.30
| X-Frame-Options: sameorigin
| Content-Length: 0
| HTTP/1.1 400 Bad Request
| Content-Type: text/plain
| Date: Sat, 06 May 2017 13:00:49 GMT
| Server: HPE-iLO-Server/1.30
| X-Frame-Options: sameorigin
| Content-Length: 0
| LPDString:
| HTTP/1.1 400 Bad Request
| Content-Type: text/plain
| Date: Sat, 06 May 2017 13:00:43 GMT
| Server: HPE-iLO-Server/1.30
| X-Frame-Options: sameorigin
| Content-Length: 0
| RTSPRequest:
| HTTP/1.1 501 Not Implemented
| Content-Type: text/plain
| Date: Sat, 06 May 2017 12:59:50 GMT
| Server: HPE-iLO-Server/1.30
| X-Frame-Options: sameorigin
| Content-Length: 0
| SSLSessionReq:
| HTTP/1.1 400 Bad Request
| Content-Type: text/plain
| Date: Sat, 06 May 2017 13:00:18 GMT
| Server: HPE-iLO-Server/1.30
```

```
| X-Frame-Options: sameorigin
| Content-Length: 0
| TLSSessionReq:
| HTTP/1.1 400 Bad Request
| Content-Type: text/plain
| Date: Sat, 06 May 2017 13:00:23 GMT
| Server: HPE-iLO-Server/1.30
| X-Frame-Options: sameorigin
| Content-Length: 0
|_ http-favicon: Unknown favicon MD5: 92333CE8639E976E70CF8ABFA00CD41E
| http-methods:
|_ Supported Methods: GET
|_ http-server-header: HPE-iLO-Server/1.30
|_ http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=ILO2M270602M0/organizationName=Hewlett Packard
Enterprise/stateOrProvinceName=Texas/countryName=US
| Subject Alternative Name: DNS:ILO2M270602M0
| Issuer: commonName=Default Issuer (Do not trust)/organizationName=Hewlett Packard
Enterprise/stateOrProvinceName=Texas/countryName=US
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2017-02-11T02:59:49
| Not valid after: 2032-02-11T02:59:49
| MD5: bbda f34a dd29 01d5 3bb9 d66a b496 2629
| SHA-1: 244f 976d 64f6 235a 58d7 033f b09d e5f1 2d12 a2bb
|_ ssl-date: TLS randomness does not represent time
17988/tcp open ilo-vm HP Integrated Lights-Out Virtual Media
2 services unrecognized despite returning data. If you know the service/version, please submit the
following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-
```

```
service :
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
```

```
SF-Port80-TCP:V=7.40%I=7%D=5/6%Time=590E1CF2%P=i686-pc-windows-windows%r(G
SF:etRequest,9E,"HTTP/1.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20te
SF:xt/plain\r\nConnection:\x20close\r\nDate:\x20Sat,\x2006\x20May\x202017\
SF:x2012:59:21\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30\r\nContent-Length
SF::\x200\r\n\r\n")%r(HTTPOptions,AC,"HTTP/1.1\x20501\x20Not\x20Implement
SF:ed\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat,\x2006\x20May\x202017
SF:x2012:59:22\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30\r\nX-Frame-Optio
SF:ns:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(RTSPRequest,AC,"H
SF:TTTP/1.1\x20501\x20Not\x20Implemented\r\nContent-Type:\x20text/plain\r\
SF:nDate:\x20Sat,\x2006\x20May\x202017\x2012:59:27\x20GMT\r\nServer:\x20HP
SF:E-iLO-Server/1.30\r\nX-Frame-Options:\x20sameorigin\r\nContent-Length:
SF:\x200\r\n\r\n")%r(FourOhFourRequest,9E,"HTTP/1.1\x20400\x20Bad\x20Requ
SF:est\r\nContent-Type:\x20text/plain\r\nConnection:\x20close\r\nDate:\x20
SF:Sat,\x2006\x20May\x202017\x2012:59:37\x20GMT\r\nServer:\x20HPE-iLO-Serv
SF:er/1.30\r\nContent-Length:\x200\r\n\r\n")%r(Help,A8,"HTTP/1.1\x20400\
SF:x20Bad\x20Request\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat,\x2006
SF:\x20May\x202017\x2012:59:57\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30\r
SF:\nX-Frame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(SS
SF:LSessionReq,A8,"HTTP/1.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20
SF:text/plain\r\nDate:\x20Sat,\x2006\x20May\x202017\x2013:00:05\x20GMT\r\n
SF:Server:\x20HPE-iLO-Server/1.30\r\nX-Frame-Options:\x20sameorigin\r\nCo
SF:ntent-Length:\x200\r\n\r\n")%r(TLSSessionReq,A8,"HTTP/1.1\x20400\x20Ba
SF:d\x20Request\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat,\x2006\x20M
SF:ay\x202017\x2013:00:10\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30\r\nX-F
SF:rame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(LPDStri
SF:ng,A8,"HTTP/1.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plai
SF:n\r\nDate:\x20Sat,\x2006\x20May\x202017\x2013:00:25\x20GMT\r\nServer:\x
SF:20HPE-iLO-Server/1.30\r\nX-Frame-Options:\x20sameorigin\r\nContent-Len
SF:gth:\x200\r\n\r\n")%r(LDAPSearchReq,150,"HTTP/1.1\x20400\x20Bad\x20Req
SF:uest\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat,\x2006\x20May\x2020
SF:17\x2013:00:30\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30\r\nX-Frame-Opt
SF:ions:\x20sameorigin\r\nContent-Length:\x200\r\n\r\nHTTP/1.1\x20400\x20
SF:Bad\x20Request\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat,\x2006\x2
SF:0May\x202017\x2013:00:30\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30\r\nX
SF:-Frame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n");
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF-Port443-TCP:V=7.40%T=SSL%I=7%D=5/6%Time=590E1CF8%P=i686-pc-windows-wind
SF:ows%r(GetRequest,9E,"HTTP/1.1\x20400\x20Bad\x20Request\r\nContent-Type
SF::\x20text/plain\r\nConnection:\x20close\r\nDate:\x20Sat,\x2006\x20May\x
SF:202017\x2012:59:28\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30\r\nContent
SF:-Length:\x200\r\n\r\n")%r(HTTPOptions,AC,"HTTP/1.1\x20501\x20Not\x20Im
SF:plemented\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat,\x2006\x20May\
```



```
SF:x202017\x2012:59:29\x20GMT\r\nServer:\x20HPE-iLO-Server/1\1.30\r\nX-Fram
SF:e-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(FourOhFour
SF:Request,9E,"HTTP/1\1.\x20400\x20Bad\x20Request\r\nContent-Type:\x20text
SF:/plain\r\nConnection:\x20close\r\nDate:\x20Sat,\x2006\x20May\x202017\x2
SF:012:59:34\x20GMT\r\nServer:\x20HPE-iLO-Server/1\1.30\r\nContent-Length:\
SF:x200\r\n\r\n")%r(RTSPRequest,AC,"HTTP/1\1.\x20501\x20Not\x20Implemented
SF:\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat,\x2006\x20May\x202017\x
SF:2012:59:50\x20GMT\r\nServer:\x20HPE-iLO-Server/1\1.30\r\nX-Frame-Options
SF::\x20sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(Help,A8,"HTTP/1\1.\
SF:x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat
SF:,\x2006\x20May\x202017\x2013:00:10\x20GMT\r\nServer:\x20HPE-iLO-Server/
SF:1\1.30\r\nX-Frame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n
SF:")%r(SSLSessionReq,A8,"HTTP/1\1.\x20400\x20Bad\x20Request\r\nContent-Ty
SF:pe:\x20text/plain\r\nDate:\x20Sat,\x2006\x20May\x202017\x2013:00:18\x20
SF:GMT\r\nServer:\x20HPE-iLO-Server/1\1.30\r\nX-Frame-Options:\x20sameorigi
SF:n\r\nContent-Length:\x200\r\n\r\n")%r(TLSSessionReq,A8,"HTTP/1\1.\x2040
SF:0\x20Bad\x20Request\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat,\x20
SF:06\x20May\x202017\x2013:00:23\x20GMT\r\nServer:\x20HPE-iLO-Server/1\1.30
SF:\r\nX-Frame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(
SF:LPDString,A8,"HTTP/1\1.\x20400\x20Bad\x20Request\r\nContent-Type:\x20te
SF:xt/plain\r\nDate:\x20Sat,\x2006\x20May\x202017\x2013:00:43\x20GMT\r\nSe
SF:rver:\x20HPE-iLO-Server/1\1.30\r\nX-Frame-Options:\x20sameorigin\r\nCont
SF:ent-Length:\x200\r\n\r\n")%r(LDAPSearchReq,150,"HTTP/1\1.\x20400\x20Bad
SF:\x20Request\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat,\x2006\x20Ma
SF:y\x202017\x2013:00:49\x20GMT\r\nServer:\x20HPE-iLO-Server/1\1.30\r\nX-Fr
SF:ame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\nHTTP/1\1.\x20
SF:400\x20Bad\x20Request\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat,\x
SF:2006\x20May\x202017\x2013:00:49\x20GMT\r\nServer:\x20HPE-iLO-Server/1\
SF:30\r\nX-Frame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n");
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7,40%E=4%D=5/6%OT=22%CT=1%CU=40717%PV=Y%DS=1%DC=T%G=Y%TM=590E1DAD
OS:%P=i686-pc-windows-windows) SEQ(SP=106%GCD=1%ISR=108%TI=I%II=I%SS=S%TS=U)
OS:SEQ(IT=I) OPS(O1=M564NW0NNSNNT11%O2=M564NW0NNSNNT11%O3=M280NW0NNT11%O4=M5
OS:64NW0NNSNNT11%O5=M218NW0NNSNNT11%O6=M564) WIN(W1=3018%W2=3018%W3=3110%W4=
OS:32E8%W5=3120%W6=3000) ECN(R=Y%DF=N%T=40%W=3000%O=M564%CC=N%Q=) ECN(R=N) T1(
OS:R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=) T2(R=N) T3(R=N) T4(R=N) T5(R=Y%DF=N%T=4
OS:0%W=0%S=O%A=S+%F=AR%O=RD=0%Q=) T6(R=N) T7(R=N) U1(R=Y%DF=N%T=FF%IPL=38%UN=
OS:0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G) IE(R=Y%DFI=N%T=FF%CD=S)

Uptime guess: 17.133 days (since Wed Apr 19 10:50:54 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=264 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: CPE: cpe:/h:hp:integrated_lights-out

TRACEROUTE (using port 110/tcp)
HOP RTT ADDRESS
1 68.00 ms 10.50.1.8

Nmap scan report for 10.50.1.9
Host is up (0.077s latency).
Not shown: 996 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh HP Integrated Lights-Out mpSSH 0.2.1 (protocol 2.0)
| ssh-hostkey:
| 1024 55:84:5c:31:37:45:34:dd:e9:20:ee:f3:5d:81:da:f7 (DSA)
| 2048 87:47:2f:eb:67:cd:4c:3a:8a:7c:ad:40:ac:65:80:10 (RSA)
80/tcp open http HPE-iLO-Server/1.30
| fingerprint-strings:
| FourOhFourRequest:
| HTTP/1.1 400 Bad Request
| Content-Type: text/plain
| Connection: close
| Date: Sat, 06 May 2017 18:59:39 GMT
| Server: HPE-iLO-Server/1.30
| Content-Length: 0
| GetRequest:
| HTTP/1.1 400 Bad Request
| Content-Type: text/plain
| Connection: close
| Date: Sat, 06 May 2017 18:59:24 GMT
| Server: HPE-iLO-Server/1.30
| Content-Length: 0
| HTTPOptions:
```



```
| HTTP/1.1 501 Not Implemented
| Content-Type: text/plain
| Date: Sat, 06 May 2017 18:59:24 GMT
| Server: HPE-iLO-Server/1.30
| X-Frame-Options: sameorigin
| Content-Length: 0
| Help:
| HTTP/1.1 400 Bad Request
| Content-Type: text/plain
| Date: Sat, 06 May 2017 19:00:00 GMT
| Server: HPE-iLO-Server/1.30
| X-Frame-Options: sameorigin
| Content-Length: 0
| LDAPSearchReq:
| HTTP/1.1 400 Bad Request
| Content-Type: text/plain
| Date: Sat, 06 May 2017 19:00:33 GMT
| Server: HPE-iLO-Server/1.30
| X-Frame-Options: sameorigin
| Content-Length: 0
| HTTP/1.1 400 Bad Request
| Content-Type: text/plain
| Date: Sat, 06 May 2017 19:00:33 GMT
| Server: HPE-iLO-Server/1.30
| X-Frame-Options: sameorigin
| Content-Length: 0
| LPDString:
| HTTP/1.1 400 Bad Request
| Content-Type: text/plain
| Date: Sat, 06 May 2017 19:00:28 GMT
| Server: HPE-iLO-Server/1.30
| X-Frame-Options: sameorigin
| Content-Length: 0
| RTSPRequest:
| HTTP/1.1 501 Not Implemented
| Content-Type: text/plain
| Date: Sat, 06 May 2017 18:59:29 GMT
| Server: HPE-iLO-Server/1.30
| X-Frame-Options: sameorigin
| Content-Length: 0
| SSLSessionReq:
| HTTP/1.1 400 Bad Request
| Content-Type: text/plain
| Date: Sat, 06 May 2017 19:00:07 GMT
| Server: HPE-iLO-Server/1.30
| X-Frame-Options: sameorigin
| Content-Length: 0
| TLSSessionReq:
| HTTP/1.1 400 Bad Request
| Content-Type: text/plain
| Date: Sat, 06 May 2017 19:00:12 GMT
| Server: HPE-iLO-Server/1.30
| X-Frame-Options: sameorigin
| Content-Length: 0
|_http-favicon: Unknown favicon MD5: 92333CE8639E976E70CF8ABFA00CD41E
|_http-methods:
| Supported Methods: GET HEAD POST
|_http-server-header: HPE-iLO-Server/1.30
|_http-title: Did not follow redirect to https://10.50.1.9/
443/tcp open ssl/https HPE-iLO-Server/1.30
| fingerprint-strings:
| FourOhFourRequest:
| HTTP/1.1 400 Bad Request
| Content-Type: text/plain
| Connection: close
| Date: Sat, 06 May 2017 18:59:36 GMT
| Server: HPE-iLO-Server/1.30
| Content-Length: 0
| GetRequest:
| HTTP/1.1 400 Bad Request
| Content-Type: text/plain
| Connection: close
| Date: Sat, 06 May 2017 18:59:30 GMT
| Server: HPE-iLO-Server/1.30
| Content-Length: 0
```

```
| HTTPOptions:
|   HTTP/1.1 501 Not Implemented
|   Content-Type: text/plain
|   Date: Sat, 06 May 2017 18:59:31 GMT
|   Server: HPE-iLO-Server/1.30
|   X-Frame-Options: sameorigin
|   Content-Length: 0
| Help:
|   HTTP/1.1 400 Bad Request
|   Content-Type: text/plain
|   Date: Sat, 06 May 2017 19:00:13 GMT
|   Server: HPE-iLO-Server/1.30
|   X-Frame-Options: sameorigin
|   Content-Length: 0
| LDAPSearchReq:
|   HTTP/1.1 400 Bad Request
|   Content-Type: text/plain
|   Date: Sat, 06 May 2017 19:00:51 GMT
|   Server: HPE-iLO-Server/1.30
|   X-Frame-Options: sameorigin
|   Content-Length: 0
|   HTTP/1.1 400 Bad Request
|   Content-Type: text/plain
|   Date: Sat, 06 May 2017 19:00:51 GMT
|   Server: HPE-iLO-Server/1.30
|   X-Frame-Options: sameorigin
|   Content-Length: 0
| LPDString:
|   HTTP/1.1 400 Bad Request
|   Content-Type: text/plain
|   Date: Sat, 06 May 2017 19:00:46 GMT
|   Server: HPE-iLO-Server/1.30
|   X-Frame-Options: sameorigin
|   Content-Length: 0
| RTSPRequest:
|   HTTP/1.1 501 Not Implemented
|   Content-Type: text/plain
|   Date: Sat, 06 May 2017 18:59:52 GMT
|   Server: HPE-iLO-Server/1.30
|   X-Frame-Options: sameorigin
|   Content-Length: 0
| SSLSessionReq:
|   HTTP/1.1 400 Bad Request
|   Content-Type: text/plain
|   Date: Sat, 06 May 2017 19:00:20 GMT
|   Server: HPE-iLO-Server/1.30
|   X-Frame-Options: sameorigin
|   Content-Length: 0
| TLSSessionReq:
|   HTTP/1.1 400 Bad Request
|   Content-Type: text/plain
|   Date: Sat, 06 May 2017 19:00:25 GMT
|   Server: HPE-iLO-Server/1.30
|   X-Frame-Options: sameorigin
|   Content-Length: 0
|_ http-favicon: Unknown favicon MD5: 92333CE8639E976E70CF8ABFA00CD41E
| http-methods:
|_ Supported Methods: GET
|_ http-server-header: HPE-iLO-Server/1.30
|_ http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=ILO2M270602LS/organizationName=Hewlett Packard
Enterprise/stateOrProvinceName=Texas/countryName=US
| Subject Alternative Name: DNS:ILO2M270602LS
| Issuer: commonName=Default Issuer (Do not trust)/organizationName=Hewlett Packard
Enterprise/stateOrProvinceName=Texas/countryName=US
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2017-02-11T05:05:22
| Not valid after: 2032-02-11T05:05:22
| MD5: 494f f34f 6dbb 6aa9 7c37 b6aa c442 4094
|_ SHA-1: 2800 64cf 0f63 22e9 3267 95f0 110c 29ff 4603 6ce5
|_ ssl-date: TLS randomness does not represent time
17988/tcp open ilo-vm HP Integrated Lights-Out Virtual Media
```

2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at <https://nmap.org/cgi-bin/submit.cgi?new->

```
Service :
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF:Port80-TCP:V=7.40%I=7%D=5/6%Time=590E1CF2%P=i686-pc-windows-windows%r(G
SF:etRequest,9E,"HTTP/1.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20te
SF:xt/plain\r\nConnection:\x20close\r\nDate:\x20Sat,\x2006\x20May\x202017\
SF:x2018:59:24\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30\r\nContent-Length
SF::\x200\r\n\r\n")%r(HTTPOptions,AC,"HTTP/1.1\x20501\x20Not\x20Implement
SF:ed\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat,\x2006\x20May\x202017
SF:\x2018:59:24\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30\r\nX-Frame-Optio
SF:ns:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(RTSPRequest,AC,"H
SF:TP/1.1\x20501\x20Not\x20Implemented\r\nContent-Type:\x20text/plain\r\n
SF:nDate:\x20Sat,\x2006\x20May\x202017\x2018:59:29\x20GMT\r\nServer:\x20HP
SF:E-iLO-Server/1.30\r\nX-Frame-Options:\x20sameorigin\r\nContent-Length:
SF:\x200\r\n\r\n")%r(FourOhFourRequest,9E,"HTTP/1.1\x20400\x20Bad\x20Requ
SF:est\r\nContent-Type:\x20text/plain\r\nConnection:\x20close\r\nDate:\x20
SF:Sat,\x2006\x20May\x202017\x2018:59:39\x20GMT\r\nServer:\x20HPE-iLO-Serv
SF:er/1.30\r\nContent-Length:\x200\r\n\r\n")%r(Help,A8,"HTTP/1.1\x20400\
SF:x20Bad\x20Request\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat,\x2006
SF:\x20May\x202017\x2019:00:00\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30\r
SF:nX-Frame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(SS
SF:LSessionReq,A8,"HTTP/1.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20
SF:text/plain\r\nDate:\x20Sat,\x2006\x20May\x202017\x2019:00:07\x20GMT\r\n
SF:Server:\x20HPE-iLO-Server/1.30\r\nX-Frame-Options:\x20sameorigin\r\nCo
SF:ntent-Length:\x200\r\n\r\n")%r(TLSSessionReq,A8,"HTTP/1.1\x20400\x20Ba
SF:d\x20Request\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat,\x2006\x20M
SF:ay\x202017\x2019:00:12\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30\r\nX-F
SF:rame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(LPDStri
SF:ng,A8,"HTTP/1.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plai
SF:n\r\nDate:\x20Sat,\x2006\x20May\x202017\x2019:00:28\x20GMT\r\nServer:\x
SF:20HPE-iLO-Server/1.30\r\nX-Frame-Options:\x20sameorigin\r\nContent-Len
SF:gth:\x200\r\n\r\n")%r(LDAPSearchReq,150,"HTTP/1.1\x20400\x20Bad\x20Req
SF:uest\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat,\x2006\x20May\x2020
SF:17\x2019:00:33\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30\r\nX-Frame-Opt
SF:ions:\x20sameorigin\r\nContent-Length:\x200\r\n\r\nHTTP/1.1\x20400\x20
SF:Bad\x20Request\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat,\x2006\x2
SF:0May\x202017\x2019:00:33\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30\r\nX
SF:-Frame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n");
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF:Port443-TCP:V=7.40%T=SSL%I=7%D=5/6%Time=590E1CF8%P=i686-pc-windows-wind
SF:ows%r(GetRequest,9E,"HTTP/1.1\x20400\x20Bad\x20Request\r\nContent-Type
SF::\x20text/plain\r\nConnection:\x20close\r\nDate:\x20Sat,\x2006\x20May\x
SF:202017\x2018:59:30\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30\r\nContent
SF:-Length:\x200\r\n\r\n")%r(HTTPOptions,AC,"HTTP/1.1\x20501\x20Not\x20Im
SF:plemented\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat,\x2006\x20May\
SF:x202017\x2018:59:31\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30\r\nX-Fram
SF:e-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(FourOhFour
SF:Request,9E,"HTTP/1.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text
SF:/plain\r\nConnection:\x20close\r\nDate:\x20Sat,\x2006\x20May\x202017\x2
SF:018:59:36\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30\r\nContent-Length:\
SF:x200\r\n\r\n")%r(RTSPRequest,AC,"HTTP/1.1\x20501\x20Not\x20Implemented
SF:\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat,\x2006\x20May\x202017\x
SF:2018:59:52\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30\r\nX-Frame-Options
SF::\x20sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(Help,A8,"HTTP/1.1\
SF:x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat
SF:\x2006\x20May\x202017\x2019:00:13\x20GMT\r\nServer:\x20HPE-iLO-Server/
SF:1.30\r\nX-Frame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n
SF:")%r(SSLSessionReq,A8,"HTTP/1.1\x20400\x20Bad\x20Request\r\nContent-Ty
SF:pe:\x20text/plain\r\nDate:\x20Sat,\x2006\x20May\x202017\x2019:00:20\x20
SF:GMT\r\nServer:\x20HPE-iLO-Server/1.30\r\nX-Frame-Options:\x20sameorigi
SF:n\r\nContent-Length:\x200\r\n\r\n")%r(TLSSessionReq,A8,"HTTP/1.1\x2040
SF:0\x20Bad\x20Request\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat,\x20
SF:06\x20May\x202017\x2019:00:25\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30
SF:\r\nX-Frame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(
SF:LPDString,A8,"HTTP/1.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20te
SF:xt/plain\r\nDate:\x20Sat,\x2006\x20May\x202017\x2019:00:46\x20GMT\r\nSe
SF:rver:\x20HPE-iLO-Server/1.30\r\nX-Frame-Options:\x20sameorigin\r\nCont
SF:ent-Length:\x200\r\n\r\n")%r(LDAPSearchReq,150,"HTTP/1.1\x20400\x20Bad
SF:\x20Request\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat,\x2006\x20Ma
SF:y\x202017\x2019:00:51\x20GMT\r\nServer:\x20HPE-iLO-Server/1.30\r\nX-Fr
SF:ame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\nHTTP/1.1\x20
SF:400\x20Bad\x20Request\r\nContent-Type:\x20text/plain\r\nDate:\x20Sat,\x
SF:2006\x20May\x202017\x2019:00:51\x20GMT\r\nServer:\x20HPE-iLO-Server/1.
```

```
SF:30\r\nX-Frame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n");
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.40%E=4%D=5/6%OT=22%CT=1%CU=40319%PV=Y%DS=1%DC=T%G=Y%TM=590E1DAD
OS:%P=i686-pc-windows-windows) SEQ(SP=105%GCD=1%ISR=108%TI=I%II=I%SS=S%TS=U)
OS:SEQ(II=I) OPS(O1=M564NW0NNSNNT11%O2=M564NW0NNSNNT11%O3=M280NW0NNT11%O4=M5
OS:64NW0NNSNNT11%O5=M218NW0NNSNNT11%O6=M564) WIN(W1=3018%W2=3018%W3=3110%W4=
OS:32E8%W5=3120%W6=3000) ECN(R=Y%DF=N%T=40%W=3000%O=M564%CC=N%Q=) ECN(R=N) T1(
OS:R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=) T2(R=N) T3(R=N) T4(R=N) T5(R=Y%DF=N%T=4
OS:0%W=0%S=O%A=S+%F=AR%O=%RD=0%Q=) T6(R=N) T7(R=N) U1(R=Y%DF=N%T=FF%IPL=38%UN=
OS:0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G) IE(R=Y%DFI=N%T=FF%CD=S)

Uptime guess: 16.816 days (since Wed Apr 19 18:27:17 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: CPE: cpe:/h:hp:integrated_lights-out

TRACEROUTE (using port 110/tcp)
HOP RTT ADDRESS
1 55.00 ms 10.50.1.9

Nmap scan report for 10.50.1.10
Host is up (0.12s latency).
Not shown: 999 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 7f:39:aa:4c:91:8c:13:cc:11:44:ad:d0:44:26:45:9c (RSA)
|_ 256 7e:d3:1e:99:39:13:cb:1b:5e:1c:07:46:a8:50:dc:e8 (ECDSA)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.40%E=4%D=5/6%OT=22%CT=1%CU=40360%PV=Y%DS=1%DC=T%G=Y%TM=590E1DAD
OS:%P=i686-pc-windows-windows) SEQ(SP=107%GCD=1%ISR=10C%TI=Z%II=I%TS=8) SEQ(I
OS:I=I) OPS(O1=M564ST11NW7%O2=M564ST11NW7%O3=M564NNT11NW7%O4=M564ST11NW7%O5=
OS:M564ST11NW7%O6=M564ST11) WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7
OS:120) ECN(R=Y%DF=Y%T=40%W=7210%O=M564NNSNW7%CC=Y%Q=) ECN(R=N) T1(R=Y%DF=Y%T=
OS:40%S=O%A=S+%F=AS%RD=0%Q=) T2(R=N) T3(R=N) T4(R=N) T5(R=Y%DF=Y%T=40%W=0%S=O%A
OS:=S+%F=AR%O=%RD=0%Q=) T6(R=N) T7(R=N) U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%R
OS:ID=G%RIPCK=G%RUCK=G%RUD=G) IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 110/tcp)
HOP RTT ADDRESS
1 65.00 ms 10.50.1.10

Nmap scan report for 10.50.1.11
Host is up (0.12s latency).
Not shown: 999 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 77:e6:7d:63:90:8e:79:da:08:b6:23:cb:2c:93:b0:6a (RSA)
|_ 256 8b:65:a5:a8:17:85:ef:8f:3c:9c:92:1e:bd:27:67:dc (ECDSA)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.40%E=4%D=5/6%OT=22%CT=1%CU=33489%PV=Y%DS=1%DC=T%G=Y%TM=590E1DAD
OS:%P=i686-pc-windows-windows) SEQ(SP=102%GCD=1%ISR=10A%TI=Z%II=I%TS=8) SEQ(S
OS:P=103%GCD=1%ISR=10A%TI=Z%TS=8) SEQ(II=I) OPS(O1=M564ST11NW7%O2=M564ST11NW7
OS:%O3=M564NNT11NW7%O4=M564ST11NW7%O5=M564ST11NW7%O6=M564ST11) WIN(W1=7120%W
OS:2=7120%W3=7120%W4=7120%W5=7120%W6=7120) ECN(R=Y%DF=Y%T=40%W=7210%O=M564NN
OS:SNW7%CC=Y%Q=) ECN(R=N) T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=) T2(R=N) T3(R=
OS:N) T4(R=N) T5(R=Y%DF=Y%T=40%W=0%S=O%A=S+%F=AR%O=%RD=0%Q=) T6(R=N) T7(R=N) U1(
OS:R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G) IE(R=Y%DFI=
OS:N%T=40%CD=S)

Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 110/tcp)
HOP RTT ADDRESS
1 71.00 ms 10.50.1.11
```

```
Nmap scan report for 10.50.1.100
Host is up (0.12s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.18
| http-ls: Volume /
|   maxfiles limit reached (10)
|   SIZE  TIME      FILENAME
|   0      2017-05-05 01:30  datos.txt
|   19     2017-05-04 22:35  echo.php
|   20     2017-05-04 22:35  echo1.php
|   -      2017-05-05 01:51  fotos/
|   -      2017-05-05 00:23  includes/
|   339    2017-05-05 01:04  includes/conecta.php
|   220    2017-05-04 23:07  includes/conecta_panoramicos.php
|   1.2K   2017-05-05 00:49  includes/demo.php
|   17K    2017-05-05 00:55  includes/ez_sql_core.php
|   7.1K   2017-05-04 23:25  includes/ez_sql_mysql.php
|_
|_ http-methods:
|_   Supported Methods: POST OPTIONS GET HEAD
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Index of /
2222/tcp  open  ssh       OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 32:31:d3:75:d3:4a:cb:55:09:94:c4:37:c5:b0:b2:db (RSA)
|   256  90:8a:22:78:4e:ae:67:55:0c:ee:79:e0:e0:2e:36:15 (ECDSA)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.40%E=4%D=5/6%OT=80%CT=1%CU=35995%PV=Y%DS=1%DC=T%G=Y%TM=590E1DAD
OS:%P=i686-pc-windows-windows) SEQ(SP=100%GCD=1%ISR=10A%TI=Z%II=I%TS=8) SEQ(I
OS:I=I) OPS(Ol=M564ST11NW7%O2=M564ST11NW7%O3=M564NNT11NW7%O4=M564ST11NW7%O5=
OS:M564ST11NW7%O6=M564ST11) WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7
OS:120) ECN(R=Y%DF=Y%T=40%W=7210%O=M564NNSNW7%CC=Y%Q=) ECN(R=N) T1(R=Y%DF=Y%T=
OS:40%S=O%A=S+%F=AS%RD=0%Q=) T2(R=N) T3(R=N) T4(R=N) T5(R=Y%DF=Y%T=40%W=0%S=O
OS:=S+%F=AR%O=RD=0%Q=) T6(R=N) T7(R=N) U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%R
OS:ID=G%RIPCK=G%RUCK=G%RUD=G) IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop
Service Info: Host: 127.0.1.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 110/tcp)
HOP RTT      ADDRESS
1   49.00 ms  10.50.1.100

Nmap scan report for 10.50.1.101
Host is up (0.12s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
3306/tcp  open  mysql     MySQL 5.7.17-0ubuntu0.16.04.2
| mysql-info:
|   Protocol: 10
|   Version: 5.7.17-0ubuntu0.16.04.2
|   Thread ID: 67327
|   Capabilities flags: 63487
|   Some Capabilities: Speaks41ProtocolOld, SupportsCompression, LongPassword, SupportsTransactions,
Support41Auth, ConnectWithDatabase, InteractiveClient,
|_
|_ ignoreSpaceBeforeParenthesis, Speaks41ProtocolNew, FoundRows, SupportsLoadDataLocal,
DontAllowDatabaseTableColumn, LongColumnFlag, ODBCClient, IgnoreSigpipes
|_
|_ SupportsMultipleResults, SupportsMultipleStatements, SupportsAuthPlugins
|_   Status: Autocommit
|_   Salt: \x14,\x01\x7Fh\x06i+v\x0ERh"*h4Hr!9
|_   Auth Plugin Name: 96
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.40%E=4%D=5/6%OT=3306%CT=1%CU=31376%PV=Y%DS=1%DC=T%G=Y%TM=590E1D
OS:AD%P=i686-pc-windows-windows) SEQ(SP=107%GCD=1%ISR=10A%TI=Z%II=I%TS=8) SEQ
OS:(I=I) OPS(Ol=M564ST11NW7%O2=M564ST11NW7%O3=M564NNT11NW7%O4=M564ST11NW7%O
OS:5=M564ST11NW7%O6=M564ST11) WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6
OS:=7120) ECN(R=Y%DF=Y%T=40%W=7210%O=M564NNSNW7%CC=Y%Q=) ECN(R=N) T1(R=Y%DF=Y
OS:T=40%S=O%A=S+%F=AS%RD=0%Q=) T2(R=N) T3(R=N) T4(R=N) T5(R=Y%DF=Y%T=40%W=0
OS:%A=S+%F=AR%O=RD=0%Q=) T6(R=N) T7(R=N) U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G
OS:%RID=G%RIPCK=G%RUCK=G%RUD=G) IE(R=Y%DFI=N%T=40%CD=S)
```

```
Network Distance: 1 hop

TRACEROUTE (using port 110/tcp)
HOP RTT      ADDRESS
1   66.00 ms 10.50.1.101

Nmap scan report for 10.50.1.102
Host is up (0.061s latency).
All 1000 scanned ports on 10.50.1.102 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE (using port 110/tcp)
HOP RTT      ADDRESS
1   44.00 ms 10.50.1.102

Nmap scan report for 10.50.1.103
Host is up (0.12s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http      nginx 1.10.0 (Ubuntu)
|_ http-favicon: Unknown favicon MD5: 2958DC82E3B3052BABAC794A2BB97EB2
|_ http-methods:
|_ Supported Methods: GET HEAD POST
|_ http-server-header: nginx/1.10.0 (Ubuntu)
|_ http-title: IEC
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.40%E=4%D=5/6%OT=80%CT=1%CU=39358%PV=Y%DS=1%DC=T%G=Y%TM=590E1DAD
OS:%P=i686-pc-windows-windows) SEQ(SP=100%GCD=1%ISR=107%TI=Z%II=I%TS=8) SEQ(S
OS:P=100%GCD=1%ISR=107%TI=Z%TS=8) SEQ(II=I) OPS(O1=M564ST11NW7%O2=M564ST11NW7
OS:%O3=M564NNT11NW7%O4=M564ST11NW7%O5=M564ST11NW7%O6=M564ST11) WIN(W1=7120%W
OS:2=7120%W3=7120%W4=7120%W5=7120%W6=7120) ECN(R=Y%DF=Y%T=40%W=7210%O=M564NN
OS:SNW7%CC=Y%Q=) ECN(R=N) T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=) T2(R=N) T3(R=
OS:N) T4(R=N) T5(R=Y%DF=Y%T=40%W=0%S=O%A=S+%F=AR%O=%RD=0%Q=) T6(R=N) T7(R=N) U1(
OS:R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G) IE(R=Y%DFI=
OS:N%T=40%CD=S)

Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 110/tcp)
HOP RTT      ADDRESS
1   61.00 ms 10.50.1.103

Nmap scan report for 10.50.1.104
Host is up (0.12s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp       vsftpd 2.0.8 or later
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.40%E=4%D=5/6%OT=21%CT=1%CU=30864%PV=Y%DS=1%DC=T%G=Y%TM=590E1DAD
OS:%P=i686-pc-windows-windows) SEQ(SP=105%GCD=1%ISR=10C%TI=Z%II=I%TS=8) SEQ(I
OS:I=I) OPS(O1=M564ST11NW7%O2=M564ST11NW7%O3=M564NNT11NW7%O4=M564ST11NW7%O5=
OS:M564ST11NW7%O6=M564ST11) WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7
OS:120) ECN(R=Y%DF=Y%T=40%W=7210%O=M564NNSNW7%CC=Y%Q=) ECN(R=N) T1(R=Y%DF=Y%T=
OS:40%S=O%A=S+%F=AS%RD=0%Q=) T2(R=N) T3(R=N) T4(R=N) T5(R=Y%DF=Y%T=40%W=0%S=O%A
OS:=S+%F=AR%O=%RD=0%Q=) T6(R=N) T7(R=N) U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%R
OS:ID=G%RIPCK=G%RUCK=G%RUD=G) IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop

TRACEROUTE (using port 110/tcp)
HOP RTT      ADDRESS
1   47.00 ms 10.50.1.104

Nmap scan report for 10.50.1.105
Host is up (0.062s latency).
All 1000 scanned ports on 10.50.1.105 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE (using port 110/tcp)
```

```
HOP RTT      ADDRESS
1    44.00 ms 10.50.1.105

Nmap scan report for 10.50.1.106
Host is up (0.12s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.18 ((Ubuntu))
|_ http-methods:
|_   Supported Methods: POST OPTIONS GET HEAD
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Apache2 Ubuntu Default Page: It works
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.40%E=4%D=5/6%OT=80%CT=1%CU=44634%PV=Y%DS=1%DC=T%G=Y%TM=590E1DAD
OS:%P=i686-pc-windows-windows) SEQ(SP=106%GCD=1%ISR=10D%TI=Z%II=I%TS=8) SEQ(I
OS:I=I) OPS(O1=M564ST11NW7%O2=M564ST11NW7%O3=M564NNT11NW7%O4=M564ST11NW7%O5=
OS:M564ST11NW7%O6=M564ST11) WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7
OS:120) ECN(R=Y%DF=Y%T=40%W=7210%O=M564NNSNW7%CC=Y%Q=) ECN(R=N) T1(R=Y%DF=Y%T=
OS:40%S=O%A=S+%F=AS%RD=0%Q=) T2(R=N) T3(R=N) T4(R=N) T5(R=Y%DF=Y%T=40%W=0%S=O%A
OS:=S+%F=AR%O=RD=0%Q=) T6(R=N) T7(R=N) U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%R
OS:ID=G%RIPCK=G%RUCK=G%RUD=G) IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop

TRACEROUTE (using port 110/tcp)
HOP RTT      ADDRESS
1    28.00 ms 10.50.1.106

Nmap scan report for 10.50.1.107
Host is up (0.052s latency).
All 1000 scanned ports on 10.50.1.107 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE (using port 110/tcp)
HOP RTT      ADDRESS
1    30.00 ms 10.50.1.107

Nmap scan report for 10.50.1.108
Host is up (0.073s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
8086/tcp  open  http    InfluxDB http admin 1.2.2
|_ http-title: Site doesn't have a title (text/plain; charset=utf-8).
8088/tcp  open  radan-http?
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.40%E=4%D=5/6%OT=8086%CT=1%CU=44130%PV=Y%DS=1%DC=T%G=Y%TM=590E1D
OS:AD%P=i686-pc-windows-windows) SEQ(SP=106%GCD=1%ISR=10A%TI=Z%II=I%TS=8) SEQ
OS:(II=I) OPS(O1=M564ST11NW7%O2=M564ST11NW7%O3=M564NNT11NW7%O4=M564ST11NW7%O
OS:5=M564ST11NW7%O6=M564ST11) WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6
OS:=7120) ECN(R=Y%DF=Y%T=40%W=7210%O=M564NNSNW7%CC=Y%Q=) ECN(R=N) T1(R=Y%DF=Y%
OS:T=40%S=O%A=S+%F=AS%RD=0%Q=) T2(R=N) T3(R=N) T4(R=N) T5(R=Y%DF=Y%T=40%W=0%S=O
OS:%A=S+%F=AR%O=RD=0%Q=) T6(R=N) T7(R=N) U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G
OS:%RID=G%RIPCK=G%RUCK=G%RUD=G) IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop

TRACEROUTE (using port 110/tcp)
HOP RTT      ADDRESS
1    28.00 ms 10.50.1.108

Nmap scan report for 10.50.1.109
Host is up (0.10s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
3000/tcp  open  http    Grafana
|_ http-methods:
|_   Supported Methods: GET HEAD
|_ http-robots.txt: 1 disallowed entry
|_ /
|_ http-title: Grafana
|_ Requested resource was /login
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```



```
TCP/IP fingerprint:
OS:SCAN(V=7.40%E=4%D=5/6%OT=3000%CT=1%CU=43580%PV=Y%DS=1%DC=T%G=Y%TM=590E1D
OS:AD%P=i686-pc-windows-windows) SEQ(SP=103%GCD=1%ISR=10B%TI=Z%II=I%TS=8) SEQ
OS:(II=I) OPS(Ol=M564ST11NW7%O2=M564ST11NW7%O3=M564NNT11NW7%O4=M564ST11NW7%O
OS:5=M564ST11NW7%O6=M564ST11) WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6
OS:=7120) ECN(R=Y%DF=Y%T=40%W=7210%O=M564NNSNW7%CC=Y%Q=) ECN(R=N) T1(R=Y%DF=Y%
OS:T=40%S=O%A=S+%F=AS%RD=0%Q=) T2(R=N) T3(R=N) T4(R=N) T5(R=Y%DF=Y%T=40%W=0%S=O
OS:%A=S+%F=AR%O=%RD=0%Q=) T6(R=N) T7(R=N) U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G
OS:%RID=G%RIPCK=G%RUCK=G%RUD=G) IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop

TRACEROUTE (using port 110/tcp)
HOP RTT ADDRESS
1 30.00 ms 10.50.1.109

Nmap scan report for 10.50.1.110
Host is up (0.052s latency).
All 1000 scanned ports on 10.50.1.110 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE (using port 110/tcp)
HOP RTT ADDRESS
1 28.00 ms 10.50.1.110

Nmap scan report for 10.50.1.111
Host is up (0.072s latency).
Not shown: 999 closed ports
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.4.18
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Index of /
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.40%E=4%D=5/6%OT=80%CT=1%CU=32236%PV=Y%DS=1%DC=T%G=Y%TM=590E1DAD
OS:%P=i686-pc-windows-windows) SEQ(SP=FB%GCD=1%ISR=110%TI=Z%II=I%TS=8) SEQ(II
OS:=I) OPS(Ol=M564ST11NW7%O2=M564ST11NW7%O3=M564NNT11NW7%O4=M564ST11NW7%O5=M
OS:564ST11NW7%O6=M564ST11) WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=71
OS:20) ECN(R=Y%DF=Y%T=40%W=7210%O=M564NNSNW7%CC=Y%Q=) ECN(R=N) T1(R=Y%DF=Y%T=4
OS:0%S=O%A=S+%F=AS%RD=0%Q=) T2(R=N) T3(R=N) T4(R=N) T5(R=Y%DF=Y%T=40%W=0%S=O%A=
OS:S+%F=AR%O=%RD=0%Q=) T6(R=N) T7(R=N) U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RI
OS:D=G%RIPCK=G%RUCK=G%RUD=G) IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop
Service Info: Host: 127.0.1.1

TRACEROUTE (using port 110/tcp)
HOP RTT ADDRESS
1 33.00 ms 10.50.1.111

Nmap scan report for 10.50.1.127
Host is up (0.051s latency).
All 1000 scanned ports on 10.50.1.127 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE (using port 110/tcp)
HOP RTT ADDRESS
1 34.00 ms 10.50.1.127

NSE: Script Post-scanning.
Initiating NSE at 14:02
Completed NSE at 14:02, 0.00s elapsed
Initiating NSE at 14:02
Completed NSE at 14:02, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (17 hosts up) scanned in 245.97 seconds
Raw packets sent: 21389 (994.838KB) | Rcvd: 23614 (1.027MB)

SE: Script Post-scanning.
Initiating NSE at 14:02
```



```
Completed NSE at 14:02, 0.00s elapsed
Initiating NSE at 14:02
Completed NSE at 14:02, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (17 hosts up) scanned in 245.97 seconds
      Raw packets sent: 21389 (994.838KB) | Rcvd: 23614 (1.027MB)
```


6.2 Escaneo red

```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-02 23:26 Hora de verano central (México)
NSE: Loaded 143 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 23:26
Completed NSE at 23:26, 0.00s elapsed
Initiating NSE at 23:26
Completed NSE at 23:26, 0.00s elapsed
Initiating ARP Ping Scan at 23:26
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 23:26, 1.31s elapsed (255 total hosts)
Initiating Parallel DNS resolution of 255 hosts. at 23:26
Completed Parallel DNS resolution of 255 hosts. at 23:26, 19.79s elapsed
Initiating SYN Stealth Scan at 23:26
Scanning 64 hosts [1000 ports/host]
SYN Stealth Scan Timing: About 2.20% done; ETC: 23:50 (0:23:01 remaining)
SYN Stealth Scan Timing: About 6.69% done; ETC: 23:50 (0:21:50 remaining)
SYN Stealth Scan Timing: About 11.62% done; ETC: 23:50 (0:20:39 remaining)
SYN Stealth Scan Timing: About 16.77% done; ETC: 23:50 (0:19:27 remaining)
SYN Stealth Scan Timing: About 21.88% done; ETC: 23:50 (0:18:16 remaining)
SYN Stealth Scan Timing: About 27.17% done; ETC: 23:50 (0:17:04 remaining)
SYN Stealth Scan Timing: About 32.31% done; ETC: 23:50 (0:15:51 remaining)
SYN Stealth Scan Timing: About 37.46% done; ETC: 23:50 (0:14:38 remaining)
SYN Stealth Scan Timing: About 42.60% done; ETC: 23:50 (0:13:26 remaining)
SYN Stealth Scan Timing: About 47.74% done; ETC: 23:50 (0:12:13 remaining)
SYN Stealth Scan Timing: About 52.88% done; ETC: 23:50 (0:11:02 remaining)
SYN Stealth Scan Timing: About 57.94% done; ETC: 23:50 (0:09:50 remaining)
SYN Stealth Scan Timing: About 63.08% done; ETC: 23:50 (0:08:37 remaining)
SYN Stealth Scan Timing: About 68.24% done; ETC: 23:50 (0:07:25 remaining)
SYN Stealth Scan Timing: About 73.40% done; ETC: 23:50 (0:06:12 remaining)
SYN Stealth Scan Timing: About 78.56% done; ETC: 23:50 (0:05:00 remaining)
SYN Stealth Scan Timing: About 83.71% done; ETC: 23:50 (0:03:48 remaining)
SYN Stealth Scan Timing: About 88.86% done; ETC: 23:50 (0:02:36 remaining)
SYN Stealth Scan Timing: About 94.01% done; ETC: 23:50 (0:01:24 remaining)
Completed SYN Stealth Scan against 10.50.2.36 in 1387.09s (63 hosts left)
Completed SYN Stealth Scan against 10.50.2.21 in 1388.84s (62 hosts left)
Completed SYN Stealth Scan against 10.50.2.29 in 1388.95s (61 hosts left)
Completed SYN Stealth Scan against 10.50.2.28 in 1389.93s (60 hosts left)
Completed SYN Stealth Scan against 10.50.2.35 in 1390.04s (59 hosts left)
Completed SYN Stealth Scan against 10.50.2.37 in 1390.04s (58 hosts left)
Completed SYN Stealth Scan against 10.50.2.1 in 1390.48s (57 hosts left)
Completed SYN Stealth Scan against 10.50.2.6 in 1390.59s (56 hosts left)
Completed SYN Stealth Scan against 10.50.2.56 in 1391.24s (55 hosts left)
Completed SYN Stealth Scan against 10.50.2.50 in 1392.01s (54 hosts left)
Completed SYN Stealth Scan against 10.50.2.57 in 1392.12s (53 hosts left)
Completed SYN Stealth Scan against 10.50.2.49 in 1392.89s (52 hosts left)
Completed SYN Stealth Scan against 10.50.2.14 in 1393.21s (51 hosts left)
Completed SYN Stealth Scan against 10.50.2.22 in 1393.32s (50 hosts left)
Completed SYN Stealth Scan against 10.50.2.27 in 1393.43s (49 hosts left)
Completed SYN Stealth Scan against 10.50.2.44 in 1393.65s (48 hosts left)
Completed SYN Stealth Scan against 10.50.2.0 in 1393.87s (47 hosts left)
Completed SYN Stealth Scan against 10.50.2.63 in 1393.87s (46 hosts left)
Completed SYN Stealth Scan against 10.50.2.64 in 1393.87s (45 hosts left)
Completed SYN Stealth Scan against 10.50.2.15 in 1394.09s (44 hosts left)
Completed SYN Stealth Scan against 10.50.2.47 in 1394.42s (43 hosts left)
Completed SYN Stealth Scan against 10.50.2.48 in 1394.42s (42 hosts left)
Completed SYN Stealth Scan against 10.50.2.7 in 1394.64s (41 hosts left)
Completed SYN Stealth Scan against 10.50.2.58 in 1395.84s (40 hosts left)
Completed SYN Stealth Scan against 10.50.2.5 in 1395.95s (39 hosts left)
Completed SYN Stealth Scan against 10.50.2.20 in 1396.06s (38 hosts left)
Completed SYN Stealth Scan against 10.50.2.30 in 1396.17s (37 hosts left)
Completed SYN Stealth Scan against 10.50.2.41 in 1396.28s (36 hosts left)
Completed SYN Stealth Scan against 10.50.2.59 in 1396.49s (35 hosts left)
Completed SYN Stealth Scan against 10.50.2.34 in 1396.82s (34 hosts left)
Completed SYN Stealth Scan against 10.50.2.10 in 1397.15s (33 hosts left)
Completed SYN Stealth Scan against 10.50.2.24 in 1397.26s (32 hosts left)
Completed SYN Stealth Scan against 10.50.2.38 in 1397.37s (31 hosts left)
Completed SYN Stealth Scan against 10.50.2.42 in 1397.37s (30 hosts left)
Completed SYN Stealth Scan against 10.50.2.12 in 1397.69s (29 hosts left)
Completed SYN Stealth Scan against 10.50.2.13 in 1397.69s (28 hosts left)
Completed SYN Stealth Scan against 10.50.2.26 in 1397.80s (27 hosts left)
Completed SYN Stealth Scan against 10.50.2.51 in 1397.91s (26 hosts left)
Completed SYN Stealth Scan against 10.50.2.55 in 1398.02s (25 hosts left)
```

```
Completed SYN Stealth Scan against 10.50.2.16 in 1398.13s (24 hosts left)
Completed SYN Stealth Scan against 10.50.2.46 in 1398.35s (23 hosts left)
Completed SYN Stealth Scan against 10.50.2.2 in 1398.46s (22 hosts left)
Completed SYN Stealth Scan against 10.50.2.3 in 1398.46s (21 hosts left)
Completed SYN Stealth Scan against 10.50.2.62 in 1398.46s (20 hosts left)
Completed SYN Stealth Scan against 10.50.2.25 in 1398.57s (19 hosts left)
Completed SYN Stealth Scan against 10.50.2.43 in 1398.68s (18 hosts left)
Completed SYN Stealth Scan against 10.50.2.8 in 1398.78s (17 hosts left)
Completed SYN Stealth Scan against 10.50.2.23 in 1398.89s (16 hosts left)
Completed SYN Stealth Scan against 10.50.2.45 in 1399.00s (15 hosts left)
Completed SYN Stealth Scan against 10.50.2.53 in 1399.00s (14 hosts left)
Completed SYN Stealth Scan against 10.50.2.4 in 1399.11s (13 hosts left)
Completed SYN Stealth Scan against 10.50.2.17 in 1399.11s (12 hosts left)
Completed SYN Stealth Scan against 10.50.2.52 in 1399.22s (11 hosts left)
Completed SYN Stealth Scan against 10.50.2.9 in 1399.44s (10 hosts left)
Completed SYN Stealth Scan against 10.50.2.54 in 1399.44s (9 hosts left)
Completed SYN Stealth Scan against 10.50.2.33 in 1399.55s (8 hosts left)
Completed SYN Stealth Scan against 10.50.2.19 in 1399.66s (7 hosts left)
Completed SYN Stealth Scan against 10.50.2.18 in 1399.77s (6 hosts left)
Completed SYN Stealth Scan against 10.50.2.40 in 1399.78s (5 hosts left)
Completed SYN Stealth Scan against 10.50.2.61 in 1399.78s (4 hosts left)
Completed SYN Stealth Scan against 10.50.2.31 in 1399.89s (3 hosts left)
Completed SYN Stealth Scan against 10.50.2.39 in 1399.89s (2 hosts left)
Completed SYN Stealth Scan against 10.50.2.60 in 1399.89s (1 host left)
Completed SYN Stealth Scan at 23:50, 1400.00s elapsed (64000 total ports)
Initiating Service scan at 23:50
Initiating OS detection (try #1) against 64 hosts
Retrying OS detection (try #2) against 64 hosts
NSE: Script scanning 64 hosts.
Initiating NSE at 23:50
Completed NSE at 23:50, 0.16s elapsed
Initiating NSE at 23:50
Completed NSE at 23:50, 0.00s elapsed
Nmap scan report for 10.50.2.0
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.0 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.00 ms 10.50.2.0

Nmap scan report for 10.50.2.1
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.1 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.00 ms 10.50.2.1

Nmap scan report for 10.50.2.2
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.2 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.00 ms 10.50.2.2

Nmap scan report for 10.50.2.3
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.3 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
```

```
1 0.00 ms 10.50.2.3

Nmap scan report for 10.50.2.4
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.4 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.00 ms 10.50.2.4

Nmap scan report for 10.50.2.5
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.5 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.00 ms 10.50.2.5

Nmap scan report for 10.50.2.6
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.6 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.00 ms 10.50.2.6

Nmap scan report for 10.50.2.7
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.7 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.00 ms 10.50.2.7

Nmap scan report for 10.50.2.8
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.8 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.00 ms 10.50.2.8

Nmap scan report for 10.50.2.9
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.9 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.00 ms 10.50.2.9

Nmap scan report for 10.50.2.10
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.10 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.10

Nmap scan report for 10.50.2.12
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.12 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.12

Nmap scan report for 10.50.2.13
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.13 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.13

Nmap scan report for 10.50.2.14
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.14 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.14

Nmap scan report for 10.50.2.15
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.15 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.15

Nmap scan report for 10.50.2.16
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.16 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.16

Nmap scan report for 10.50.2.17
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.17 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.17

Nmap scan report for 10.50.2.18
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.18 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
```

```
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.18

Nmap scan report for 10.50.2.19
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.19 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.19

Nmap scan report for 10.50.2.20
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.20 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.20

Nmap scan report for 10.50.2.21
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.21 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.21

Nmap scan report for 10.50.2.22
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.22 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.22

Nmap scan report for 10.50.2.23
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.23 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.23

Nmap scan report for 10.50.2.24
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.24 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.24

Nmap scan report for 10.50.2.25
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.25 are filtered
```



```
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms 10.50.2.25
```

```
Nmap scan report for 10.50.2.26
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.26 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms 10.50.2.26
```

```
Nmap scan report for 10.50.2.27
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.27 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms 10.50.2.27
```

```
Nmap scan report for 10.50.2.28
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.28 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms 10.50.2.28
```

```
Nmap scan report for 10.50.2.29
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.29 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms 10.50.2.29
```

```
Nmap scan report for 10.50.2.30
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.30 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms 10.50.2.30
```

```
Nmap scan report for 10.50.2.31
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.31 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms 10.50.2.31
```

```
Nmap scan report for 10.50.2.32
```

```
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.32 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

TRACEROUTE

HOP	RTT	ADDRESS
1	0.00 ms	10.50.2.32

```
Nmap scan report for 10.50.2.33
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.33 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

TRACEROUTE

HOP	RTT	ADDRESS
1	0.00 ms	10.50.2.33

```
Nmap scan report for 10.50.2.34
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.34 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

TRACEROUTE

HOP	RTT	ADDRESS
1	0.00 ms	10.50.2.34

```
Nmap scan report for 10.50.2.35
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.35 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

TRACEROUTE

HOP	RTT	ADDRESS
1	0.00 ms	10.50.2.35

```
Nmap scan report for 10.50.2.36
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.36 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

TRACEROUTE

HOP	RTT	ADDRESS
1	0.00 ms	10.50.2.36

```
Nmap scan report for 10.50.2.37
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.37 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

TRACEROUTE

HOP	RTT	ADDRESS
1	0.00 ms	10.50.2.37

```
Nmap scan report for 10.50.2.38
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.38 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

TRACEROUTE

HOP	RTT	ADDRESS
1	0.00 ms	10.50.2.38

```
Nmap scan report for 10.50.2.39
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.39 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.39
```

```
Nmap scan report for 10.50.2.40
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.40 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.40
```

```
Nmap scan report for 10.50.2.41
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.41 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.41
```

```
Nmap scan report for 10.50.2.42
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.42 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.42
```

```
Nmap scan report for 10.50.2.43
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.43 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.43
```

```
Nmap scan report for 10.50.2.44
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.44 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.44
```

```
Nmap scan report for 10.50.2.45
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.45 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
```

```
HOP RTT    ADDRESS
1  0.00 ms 10.50.2.45

Nmap scan report for 10.50.2.46
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.46 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT    ADDRESS
1  0.00 ms 10.50.2.46

Nmap scan report for 10.50.2.47
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.47 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT    ADDRESS
1  0.00 ms 10.50.2.47

Nmap scan report for 10.50.2.48
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.48 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT    ADDRESS
1  0.00 ms 10.50.2.48

Nmap scan report for 10.50.2.49
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.49 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT    ADDRESS
1  0.00 ms 10.50.2.49

Nmap scan report for 10.50.2.50
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.50 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT    ADDRESS
1  0.00 ms 10.50.2.50

Nmap scan report for 10.50.2.51
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.51 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT    ADDRESS
1  0.00 ms 10.50.2.51

Nmap scan report for 10.50.2.52
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.52 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms 10.50.2.52

Nmap scan report for 10.50.2.53
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.53 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms 10.50.2.53

Nmap scan report for 10.50.2.54
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.54 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms 10.50.2.54

Nmap scan report for 10.50.2.55
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.55 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms 10.50.2.55

Nmap scan report for 10.50.2.56
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.56 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms 10.50.2.56

Nmap scan report for 10.50.2.57
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.57 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms 10.50.2.57

Nmap scan report for 10.50.2.58
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.58 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms 10.50.2.58

Nmap scan report for 10.50.2.59
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.59 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
```

```
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.59
```

```
Nmap scan report for 10.50.2.60
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.60 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.60
```

```
Nmap scan report for 10.50.2.61
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.61 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.61
```

```
Nmap scan report for 10.50.2.62
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.62 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.62
```

```
Nmap scan report for 10.50.2.63
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.63 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.63
```

```
Nmap scan report for 10.50.2.64
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.64 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.64
```

```
Initiating SYN Stealth Scan at 23:50
Scanning 64 hosts [1000 ports/host]
SYN Stealth Scan Timing: About 2.18% done; ETC: 00:14 (0:23:11 remaining)
SYN Stealth Scan Timing: About 6.05% done; ETC: 00:14 (0:21:59 remaining)
SYN Stealth Scan Timing: About 10.98% done; ETC: 00:14 (0:20:48 remaining)
SYN Stealth Scan Timing: About 15.92% done; ETC: 00:14 (0:19:38 remaining)
SYN Stealth Scan Timing: About 20.86% done; ETC: 00:14 (0:18:28 remaining)
SYN Stealth Scan Timing: About 26.00% done; ETC: 00:14 (0:17:16 remaining)
SYN Stealth Scan Timing: About 31.16% done; ETC: 00:14 (0:16:03 remaining)
SYN Stealth Scan Timing: About 36.31% done; ETC: 00:14 (0:14:51 remaining)
SYN Stealth Scan Timing: About 41.46% done; ETC: 00:14 (0:13:39 remaining)
SYN Stealth Scan Timing: About 46.62% done; ETC: 00:14 (0:12:27 remaining)
SYN Stealth Scan Timing: About 51.77% done; ETC: 00:14 (0:11:14 remaining)
```

```
SYN Stealth Scan Timing: About 56.93% done; ETC: 00:14 (0:10:02 remaining)
SYN Stealth Scan Timing: About 62.08% done; ETC: 00:14 (0:08:50 remaining)
SYN Stealth Scan Timing: About 67.23% done; ETC: 00:14 (0:07:38 remaining)
SYN Stealth Scan Timing: About 72.38% done; ETC: 00:14 (0:06:26 remaining)
SYN Stealth Scan Timing: About 77.53% done; ETC: 00:14 (0:05:14 remaining)
SYN Stealth Scan Timing: About 82.57% done; ETC: 00:14 (0:04:03 remaining)
SYN Stealth Scan Timing: About 87.75% done; ETC: 00:14 (0:02:51 remaining)
SYN Stealth Scan Timing: About 92.89% done; ETC: 00:14 (0:01:39 remaining)
Completed SYN Stealth Scan against 10.50.2.119 in 1389.32s (63 hosts left)
Completed SYN Stealth Scan against 10.50.2.67 in 1390.52s (62 hosts left)
Completed SYN Stealth Scan against 10.50.2.82 in 1390.74s (61 hosts left)
Completed SYN Stealth Scan against 10.50.2.96 in 1390.96s (60 hosts left)
Completed SYN Stealth Scan against 10.50.2.116 in 1391.29s (59 hosts left)
Completed SYN Stealth Scan against 10.50.2.68 in 1391.51s (58 hosts left)
Completed SYN Stealth Scan against 10.50.2.79 in 1391.73s (57 hosts left)
Completed SYN Stealth Scan against 10.50.2.81 in 1391.73s (56 hosts left)
Completed SYN Stealth Scan against 10.50.2.89 in 1391.84s (55 hosts left)
Completed SYN Stealth Scan against 10.50.2.97 in 1391.95s (54 hosts left)
Completed SYN Stealth Scan against 10.50.2.103 in 1392.06s (53 hosts left)
Completed SYN Stealth Scan against 10.50.2.104 in 1392.06s (52 hosts left)
Completed SYN Stealth Scan against 10.50.2.106 in 1392.06s (51 hosts left)
Completed SYN Stealth Scan against 10.50.2.78 in 1392.60s (50 hosts left)
Completed SYN Stealth Scan against 10.50.2.80 in 1392.60s (49 hosts left)
Completed SYN Stealth Scan against 10.50.2.83 in 1392.60s (48 hosts left)
Completed SYN Stealth Scan against 10.50.2.101 in 1392.83s (47 hosts left)
Completed SYN Stealth Scan against 10.50.2.117 in 1393.05s (46 hosts left)
Completed SYN Stealth Scan against 10.50.2.118 in 1393.05s (45 hosts left)
Completed SYN Stealth Scan against 10.50.2.120 in 1393.05s (44 hosts left)
Completed SYN Stealth Scan against 10.50.2.109 in 1393.70s (43 hosts left)
Completed SYN Stealth Scan against 10.50.2.123 in 1393.81s (42 hosts left)
Completed SYN Stealth Scan against 10.50.2.66 in 1393.92s (41 hosts left)
Completed SYN Stealth Scan against 10.50.2.128 in 1393.92s (40 hosts left)
Completed SYN Stealth Scan against 10.50.2.74 in 1394.03s (39 hosts left)
Completed SYN Stealth Scan against 10.50.2.88 in 1394.14s (38 hosts left)
Completed SYN Stealth Scan against 10.50.2.90 in 1394.14s (37 hosts left)
Completed SYN Stealth Scan against 10.50.2.100 in 1394.25s (36 hosts left)
Completed SYN Stealth Scan against 10.50.2.122 in 1394.47s (35 hosts left)
Completed SYN Stealth Scan against 10.50.2.124 in 1394.47s (34 hosts left)
Completed SYN Stealth Scan against 10.50.2.71 in 1394.58s (33 hosts left)
Completed SYN Stealth Scan against 10.50.2.110 in 1394.91s (32 hosts left)
Completed SYN Stealth Scan against 10.50.2.121 in 1395.02s (31 hosts left)
Completed SYN Stealth Scan against 10.50.2.125 in 1395.02s (30 hosts left)
Completed SYN Stealth Scan against 10.50.2.70 in 1395.13s (29 hosts left)
Completed SYN Stealth Scan against 10.50.2.73 in 1395.13s (28 hosts left)
Completed SYN Stealth Scan against 10.50.2.85 in 1395.23s (27 hosts left)
Completed SYN Stealth Scan against 10.50.2.99 in 1395.35s (26 hosts left)
Completed SYN Stealth Scan against 10.50.2.102 in 1395.35s (25 hosts left)
Completed SYN Stealth Scan against 10.50.2.114 in 1395.45s (24 hosts left)
Completed SYN Stealth Scan against 10.50.2.69 in 1395.56s (23 hosts left)
Completed SYN Stealth Scan against 10.50.2.84 in 1395.67s (22 hosts left)
Completed SYN Stealth Scan against 10.50.2.86 in 1395.67s (21 hosts left)
Completed SYN Stealth Scan against 10.50.2.91 in 1395.67s (20 hosts left)
Completed SYN Stealth Scan against 10.50.2.98 in 1395.78s (19 hosts left)
Completed SYN Stealth Scan against 10.50.2.105 in 1395.78s (18 hosts left)
Completed SYN Stealth Scan against 10.50.2.108 in 1395.78s (17 hosts left)
Completed SYN Stealth Scan against 10.50.2.65 in 1395.89s (16 hosts left)
Completed SYN Stealth Scan against 10.50.2.72 in 1395.89s (15 hosts left)
Completed SYN Stealth Scan against 10.50.2.115 in 1395.89s (14 hosts left)
Completed SYN Stealth Scan against 10.50.2.77 in 1396.00s (13 hosts left)
Completed SYN Stealth Scan against 10.50.2.92 in 1396.00s (12 hosts left)
Completed SYN Stealth Scan against 10.50.2.107 in 1396.11s (11 hosts left)
Completed SYN Stealth Scan against 10.50.2.111 in 1396.11s (10 hosts left)
Completed SYN Stealth Scan against 10.50.2.93 in 1396.22s (9 hosts left)
Completed SYN Stealth Scan against 10.50.2.94 in 1396.22s (8 hosts left)
Completed SYN Stealth Scan against 10.50.2.75 in 1396.33s (7 hosts left)
Completed SYN Stealth Scan against 10.50.2.127 in 1396.33s (6 hosts left)
Completed SYN Stealth Scan against 10.50.2.95 in 1396.35s (5 hosts left)
Completed SYN Stealth Scan against 10.50.2.113 in 1396.35s (4 hosts left)
Completed SYN Stealth Scan against 10.50.2.76 in 1396.45s (3 hosts left)
Completed SYN Stealth Scan against 10.50.2.87 in 1396.45s (2 hosts left)
Completed SYN Stealth Scan against 10.50.2.112 in 1396.45s (1 host left)
Completed SYN Stealth Scan at 00:14, 1396.45s elapsed (64000 total ports)
Initiating Service scan at 00:14
Initiating OS detection (try #1) against 64 hosts
Retrying OS detection (try #2) against 64 hosts
```

```
NSE: Script scanning 64 hosts.
Initiating NSE at 00:14
Completed NSE at 00:14, 0.17s elapsed
Initiating NSE at 00:14
Completed NSE at 00:14, 0.02s elapsed
Nmap scan report for 10.50.2.65
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.65 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.65

Nmap scan report for 10.50.2.66
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.66 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.66

Nmap scan report for 10.50.2.67
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.67 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.67

Nmap scan report for 10.50.2.68
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.68 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.68

Nmap scan report for 10.50.2.69
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.69 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.69

Nmap scan report for 10.50.2.70
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.70 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.70

Nmap scan report for 10.50.2.71
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.71 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
```



```
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.71
```

```
Nmap scan report for 10.50.2.72
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.72 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.72
```

```
Nmap scan report for 10.50.2.73
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.73 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.73
```

```
Nmap scan report for 10.50.2.74
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.74 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.74
```

```
Nmap scan report for 10.50.2.75
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.75 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.75
```

```
Nmap scan report for 10.50.2.76
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.76 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.76
```

```
Nmap scan report for 10.50.2.77
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.77 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.77
```

```
Nmap scan report for 10.50.2.78
Host is up (0.00s latency).
```

```
All 1000 scanned ports on 10.50.2.78 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

TRACEROUTE

```
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.78
```

```
Nmap scan report for 10.50.2.79
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.79 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

TRACEROUTE

```
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.79
```

```
Nmap scan report for 10.50.2.80
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.80 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

TRACEROUTE

```
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.80
```

```
Nmap scan report for 10.50.2.81
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.81 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

TRACEROUTE

```
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.81
```

```
Nmap scan report for 10.50.2.82
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.82 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

TRACEROUTE

```
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.82
```

```
Nmap scan report for 10.50.2.83
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.83 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

TRACEROUTE

```
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.83
```

```
Nmap scan report for 10.50.2.84
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.84 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

TRACEROUTE

```
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.84
```

```
Nmap scan report for 10.50.2.85
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.85 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.85
```

```
Nmap scan report for 10.50.2.86
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.86 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.86
```

```
Nmap scan report for 10.50.2.87
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.87 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.87
```

```
Nmap scan report for 10.50.2.88
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.88 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.88
```

```
Nmap scan report for 10.50.2.89
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.89 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.89
```

```
Nmap scan report for 10.50.2.90
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.90 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.90
```

```
Nmap scan report for 10.50.2.91
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.91 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
```

```
HOP RTT    ADDRESS
1      0.00 ms 10.50.2.91

Nmap scan report for 10.50.2.92
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.92 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT    ADDRESS
1      0.00 ms 10.50.2.92

Nmap scan report for 10.50.2.93
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.93 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT    ADDRESS
1      0.00 ms 10.50.2.93

Nmap scan report for 10.50.2.94
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.94 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT    ADDRESS
1      0.00 ms 10.50.2.94

Nmap scan report for 10.50.2.95
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.95 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT    ADDRESS
1      0.00 ms 10.50.2.95

Nmap scan report for 10.50.2.96
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.96 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT    ADDRESS
1      0.00 ms 10.50.2.96

Nmap scan report for 10.50.2.97
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.97 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT    ADDRESS
1      0.00 ms 10.50.2.97

Nmap scan report for 10.50.2.98
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.98 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms 10.50.2.98

Nmap scan report for 10.50.2.99
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.99 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms 10.50.2.99

Nmap scan report for 10.50.2.100
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.100 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms 10.50.2.100

Nmap scan report for 10.50.2.101
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.101 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms 10.50.2.101

Nmap scan report for 10.50.2.102
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.102 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms 10.50.2.102

Nmap scan report for 10.50.2.103
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.103 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms 10.50.2.103

Nmap scan report for 10.50.2.104
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.104 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms 10.50.2.104

Nmap scan report for 10.50.2.105
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.105 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
```

```
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.105
```

```
Nmap scan report for 10.50.2.106
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.106 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.106
```

```
Nmap scan report for 10.50.2.107
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.107 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.107
```

```
Nmap scan report for 10.50.2.108
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.108 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.108
```

```
Nmap scan report for 10.50.2.109
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.109 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.109
```

```
Nmap scan report for 10.50.2.110
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.110 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.110
```

```
Nmap scan report for 10.50.2.111
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.111 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.111
```

```
Nmap scan report for 10.50.2.112
Host is up (0.00s latency).
```

```
All 1000 scanned ports on 10.50.2.112 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.112
```

```
Nmap scan report for 10.50.2.113
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.113 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.113
```

```
Nmap scan report for 10.50.2.114
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.114 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.114
```

```
Nmap scan report for 10.50.2.115
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.115 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.115
```

```
Nmap scan report for 10.50.2.116
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.116 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.116
```

```
Nmap scan report for 10.50.2.117
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.117 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.117
```

```
Nmap scan report for 10.50.2.118
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.118 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.118
```

```
Nmap scan report for 10.50.2.119
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.119 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.119

Nmap scan report for 10.50.2.120
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.120 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.120

Nmap scan report for 10.50.2.121
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.121 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.121

Nmap scan report for 10.50.2.122
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.122 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.122

Nmap scan report for 10.50.2.123
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.123 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.123

Nmap scan report for 10.50.2.124
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.124 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.124

Nmap scan report for 10.50.2.125
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.125 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
```



```
1 0.00 ms 10.50.2.125

Nmap scan report for 10.50.2.126
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.126 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.00 ms 10.50.2.126

Nmap scan report for 10.50.2.127
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.127 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.00 ms 10.50.2.127

Nmap scan report for 10.50.2.128
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.128 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.00 ms 10.50.2.128

Initiating SYN Stealth Scan at 00:14
Scanning 64 hosts [1000 ports/host]
SYN Stealth Scan Timing: About 2.16% done; ETC: 00:38 (0:23:27 remaining)
SYN Stealth Scan Timing: About 5.59% done; ETC: 00:38 (0:22:13 remaining)
SYN Stealth Scan Timing: About 10.33% done; ETC: 00:38 (0:20:59 remaining)
SYN Stealth Scan Timing: About 15.27% done; ETC: 00:38 (0:19:47 remaining)
SYN Stealth Scan Timing: About 20.22% done; ETC: 00:38 (0:18:37 remaining)
SYN Stealth Scan Timing: About 25.36% done; ETC: 00:38 (0:17:25 remaining)
SYN Stealth Scan Timing: About 30.52% done; ETC: 00:38 (0:16:12 remaining)
SYN Stealth Scan Timing: About 35.67% done; ETC: 00:38 (0:15:00 remaining)
SYN Stealth Scan Timing: About 40.83% done; ETC: 00:38 (0:13:48 remaining)
SYN Stealth Scan Timing: About 45.98% done; ETC: 00:38 (0:12:36 remaining)
SYN Stealth Scan Timing: About 51.13% done; ETC: 00:38 (0:11:24 remaining)
SYN Stealth Scan Timing: About 56.29% done; ETC: 00:38 (0:10:11 remaining)
SYN Stealth Scan Timing: About 61.44% done; ETC: 00:38 (0:08:59 remaining)
SYN Stealth Scan Timing: About 66.59% done; ETC: 00:38 (0:07:47 remaining)
SYN Stealth Scan Timing: About 71.73% done; ETC: 00:38 (0:06:35 remaining)
SYN Stealth Scan Timing: About 76.88% done; ETC: 00:38 (0:05:23 remaining)
SYN Stealth Scan Timing: About 82.03% done; ETC: 00:38 (0:04:11 remaining)
SYN Stealth Scan Timing: About 87.18% done; ETC: 00:38 (0:02:59 remaining)
SYN Stealth Scan Timing: About 92.33% done; ETC: 00:38 (0:01:47 remaining)
SYN Stealth Scan Timing: About 97.50% done; ETC: 00:38 (0:00:35 remaining)
Completed SYN Stealth Scan against 10.50.2.175 in 1385.34s (63 hosts left)
Completed SYN Stealth Scan against 10.50.2.133 in 1386.28s (62 hosts left)
Completed SYN Stealth Scan against 10.50.2.183 in 1386.83s (61 hosts left)
Completed SYN Stealth Scan against 10.50.2.161 in 1388.13s (60 hosts left)
Completed SYN Stealth Scan against 10.50.2.134 in 1389.24s (59 hosts left)
Completed SYN Stealth Scan against 10.50.2.147 in 1390.11s (58 hosts left)
Completed SYN Stealth Scan against 10.50.2.155 in 1390.22s (57 hosts left)
Completed SYN Stealth Scan against 10.50.2.174 in 1390.44s (56 hosts left)
Completed SYN Stealth Scan against 10.50.2.176 in 1391.18s (55 hosts left)
Completed SYN Stealth Scan against 10.50.2.154 in 1391.62s (54 hosts left)
Completed SYN Stealth Scan against 10.50.2.160 in 1391.64s (53 hosts left)
Completed SYN Stealth Scan against 10.50.2.177 in 1391.84s (52 hosts left)
Completed SYN Stealth Scan against 10.50.2.178 in 1391.84s (51 hosts left)
Completed SYN Stealth Scan against 10.50.2.132 in 1392.04s (50 hosts left)
Completed SYN Stealth Scan against 10.50.2.139 in 1392.06s (49 hosts left)
Completed SYN Stealth Scan against 10.50.2.140 in 1392.06s (48 hosts left)
Completed SYN Stealth Scan against 10.50.2.141 in 1392.65s (47 hosts left)
Completed SYN Stealth Scan against 10.50.2.148 in 1392.67s (46 hosts left)
```

```
Completed SYN Stealth Scan against 10.50.2.162 in 1392.86s (45 hosts left)
Completed SYN Stealth Scan against 10.50.2.130 in 1393.09s (44 hosts left)
Completed SYN Stealth Scan against 10.50.2.182 in 1393.53s (43 hosts left)
Completed SYN Stealth Scan against 10.50.2.136 in 1393.73s (42 hosts left)
Completed SYN Stealth Scan against 10.50.2.153 in 1393.86s (41 hosts left)
Completed SYN Stealth Scan against 10.50.2.169 in 1393.97s (40 hosts left)
Completed SYN Stealth Scan against 10.50.2.188 in 1394.17s (39 hosts left)
Completed SYN Stealth Scan against 10.50.2.156 in 1394.39s (38 hosts left)
Completed SYN Stealth Scan against 10.50.2.181 in 1394.61s (37 hosts left)
Completed SYN Stealth Scan against 10.50.2.142 in 1394.73s (36 hosts left)
Completed SYN Stealth Scan against 10.50.2.152 in 1394.83s (35 hosts left)
Completed SYN Stealth Scan against 10.50.2.180 in 1395.05s (34 hosts left)
Completed SYN Stealth Scan against 10.50.2.149 in 1395.27s (33 hosts left)
Completed SYN Stealth Scan against 10.50.2.163 in 1395.28s (32 hosts left)
Completed SYN Stealth Scan against 10.50.2.164 in 1395.28s (31 hosts left)
Completed SYN Stealth Scan against 10.50.2.184 in 1395.48s (30 hosts left)
Completed SYN Stealth Scan against 10.50.2.189 in 1395.48s (29 hosts left)
Completed SYN Stealth Scan against 10.50.2.186 in 1395.83s (28 hosts left)
Completed SYN Stealth Scan against 10.50.2.129 in 1395.92s (27 hosts left)
Completed SYN Stealth Scan against 10.50.2.192 in 1395.92s (26 hosts left)
Completed SYN Stealth Scan against 10.50.2.146 in 1395.94s (25 hosts left)
Completed SYN Stealth Scan against 10.50.2.159 in 1396.05s (24 hosts left)
Completed SYN Stealth Scan against 10.50.2.170 in 1396.14s (23 hosts left)
Completed SYN Stealth Scan against 10.50.2.191 in 1396.15s (22 hosts left)
Completed SYN Stealth Scan against 10.50.2.144 in 1396.26s (21 hosts left)
Completed SYN Stealth Scan against 10.50.2.158 in 1396.36s (20 hosts left)
Completed SYN Stealth Scan against 10.50.2.131 in 1396.47s (19 hosts left)
Completed SYN Stealth Scan against 10.50.2.135 in 1396.47s (18 hosts left)
Completed SYN Stealth Scan against 10.50.2.167 in 1396.59s (17 hosts left)
Completed SYN Stealth Scan against 10.50.2.151 in 1396.78s (16 hosts left)
Completed SYN Stealth Scan against 10.50.2.166 in 1396.81s (15 hosts left)
Completed SYN Stealth Scan against 10.50.2.187 in 1396.92s (14 hosts left)
Completed SYN Stealth Scan against 10.50.2.143 in 1397.00s (13 hosts left)
Completed SYN Stealth Scan against 10.50.2.145 in 1397.00s (12 hosts left)
Completed SYN Stealth Scan against 10.50.2.157 in 1397.00s (11 hosts left)
Completed SYN Stealth Scan against 10.50.2.173 in 1397.03s (10 hosts left)
Completed SYN Stealth Scan against 10.50.2.137 in 1397.14s (9 hosts left)
Completed SYN Stealth Scan against 10.50.2.138 in 1397.14s (8 hosts left)
Completed SYN Stealth Scan against 10.50.2.165 in 1397.21s (7 hosts left)
Completed SYN Stealth Scan against 10.50.2.150 in 1397.25s (6 hosts left)
Completed SYN Stealth Scan against 10.50.2.185 in 1397.25s (5 hosts left)
Completed SYN Stealth Scan against 10.50.2.168 in 1397.37s (4 hosts left)
Completed SYN Stealth Scan against 10.50.2.172 in 1397.37s (3 hosts left)
Completed SYN Stealth Scan against 10.50.2.179 in 1397.37s (2 hosts left)
Completed SYN Stealth Scan against 10.50.2.171 in 1397.45s (1 host left)
Completed SYN Stealth Scan at 00:38, 1397.45s elapsed (64000 total ports)
Initiating Service scan at 00:38
Initiating OS detection (try #1) against 64 hosts
Retrying OS detection (try #2) against 64 hosts
NSE: Script scanning 64 hosts.
Initiating NSE at 00:38
Completed NSE at 00:38, 0.19s elapsed
Initiating NSE at 00:38
Completed NSE at 00:38, 0.02s elapsed
Nmap scan report for 10.50.2.129
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.129 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.00 ms 10.50.2.129

Nmap scan report for 10.50.2.130
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.130 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.00 ms 10.50.2.130
```

```
Nmap scan report for 10.50.2.131
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.131 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.131
```

```
Nmap scan report for 10.50.2.132
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.132 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.132
```

```
Nmap scan report for 10.50.2.133
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.133 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.133
```

```
Nmap scan report for 10.50.2.134
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.134 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.134
```

```
Nmap scan report for 10.50.2.135
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.135 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.135
```

```
Nmap scan report for 10.50.2.136
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.136 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.136
```

```
Nmap scan report for 10.50.2.137
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.137 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.137

Nmap scan report for 10.50.2.138
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.138 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.138

Nmap scan report for 10.50.2.139
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.139 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.139

Nmap scan report for 10.50.2.140
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.140 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.140

Nmap scan report for 10.50.2.141
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.141 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.141

Nmap scan report for 10.50.2.142
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.142 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.142

Nmap scan report for 10.50.2.143
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.143 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.143

Nmap scan report for 10.50.2.144
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.144 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
```

```
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.144

Nmap scan report for 10.50.2.145
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.145 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.145

Nmap scan report for 10.50.2.146
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.146 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.146

Nmap scan report for 10.50.2.147
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.147 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.147

Nmap scan report for 10.50.2.148
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.148 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.148

Nmap scan report for 10.50.2.149
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.149 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.149

Nmap scan report for 10.50.2.150
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.150 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.150

Nmap scan report for 10.50.2.151
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.151 are filtered
```

```
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.151

Nmap scan report for 10.50.2.152
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.152 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.152

Nmap scan report for 10.50.2.153
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.153 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.153

Nmap scan report for 10.50.2.154
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.154 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.154

Nmap scan report for 10.50.2.155
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.155 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.155

Nmap scan report for 10.50.2.156
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.156 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.156

Nmap scan report for 10.50.2.157
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.157 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.157

Nmap scan report for 10.50.2.158
```

```
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.158 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.158
```

```
Nmap scan report for 10.50.2.159
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.159 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.159
```

```
Nmap scan report for 10.50.2.160
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.160 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.160
```

```
Nmap scan report for 10.50.2.161
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.161 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.161
```

```
Nmap scan report for 10.50.2.162
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.162 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.162
```

```
Nmap scan report for 10.50.2.163
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.163 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.163
```

```
Nmap scan report for 10.50.2.164
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.164 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.164
```

```
Nmap scan report for 10.50.2.165
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.165 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.165
```

```
Nmap scan report for 10.50.2.166
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.166 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.166
```

```
Nmap scan report for 10.50.2.167
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.167 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.167
```

```
Nmap scan report for 10.50.2.168
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.168 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.168
```

```
Nmap scan report for 10.50.2.169
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.169 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.169
```

```
Nmap scan report for 10.50.2.170
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.170 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.170
```

```
Nmap scan report for 10.50.2.171
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.171 are filtered
```

```
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```



```
TRACEROUTE
HOP RTT      ADDRESS
   0.00 ms 10.50.2.171

Nmap scan report for 10.50.2.172
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.172 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms 10.50.2.172

Nmap scan report for 10.50.2.173
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.173 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms 10.50.2.173

Nmap scan report for 10.50.2.174
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.174 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms 10.50.2.174

Nmap scan report for 10.50.2.175
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.175 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms 10.50.2.175

Nmap scan report for 10.50.2.176
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.176 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms 10.50.2.176

Nmap scan report for 10.50.2.177
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.177 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms 10.50.2.177

Nmap scan report for 10.50.2.178
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.178 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
```

```
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.178

Nmap scan report for 10.50.2.179
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.179 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.179

Nmap scan report for 10.50.2.180
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.180 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.180

Nmap scan report for 10.50.2.181
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.181 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.181

Nmap scan report for 10.50.2.182
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.182 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

RACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.182

Nmap scan report for 10.50.2.183
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.183 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.183

Nmap scan report for 10.50.2.184
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.184 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.184

Nmap scan report for 10.50.2.185
Host is up (0.00s latency).
```

```
All 1000 scanned ports on 10.50.2.185 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.185
```

```
Nmap scan report for 10.50.2.186
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.186 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.186
```

```
Nmap scan report for 10.50.2.187
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.187 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.187
```

```
Nmap scan report for 10.50.2.188
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.188 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.188
```

```
Nmap scan report for 10.50.2.189
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.189 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.189
```

```
Nmap scan report for 10.50.2.190
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.190 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.190
```

```
Nmap scan report for 10.50.2.191
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.191 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.191
```

```
Nmap scan report for 10.50.2.192
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.192 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms 10.50.2.192

Initiating Parallel DNS resolution of 1 host. at 00:38
Completed Parallel DNS resolution of 1 host. at 00:38, 5.64s elapsed
Initiating SYN Stealth Scan at 00:38
Scanning 63 hosts [1000 ports/host]
SYN Stealth Scan Timing: About 2.19% done; ETC: 01:02 (0:23:04 remaining)
SYN Stealth Scan Timing: About 5.48% done; ETC: 01:01 (0:21:50 remaining)
SYN Stealth Scan Timing: About 9.48% done; ETC: 01:01 (0:20:41 remaining)
SYN Stealth Scan Timing: About 14.33% done; ETC: 01:01 (0:19:32 remaining)
SYN Stealth Scan Timing: About 19.04% done; ETC: 01:01 (0:18:21 remaining)
SYN Stealth Scan Timing: About 24.48% done; ETC: 01:01 (0:17:10 remaining)
SYN Stealth Scan Timing: About 29.71% done; ETC: 01:01 (0:16:00 remaining)
SYN Stealth Scan Timing: About 34.94% done; ETC: 01:01 (0:14:50 remaining)
SYN Stealth Scan Timing: About 40.17% done; ETC: 01:01 (0:13:39 remaining)
SYN Stealth Scan Timing: About 45.40% done; ETC: 01:01 (0:12:28 remaining)
SYN Stealth Scan Timing: About 50.43% done; ETC: 01:01 (0:11:19 remaining)
SYN Stealth Scan Timing: About 55.47% done; ETC: 01:01 (0:10:10 remaining)
SYN Stealth Scan Timing: About 60.49% done; ETC: 01:01 (0:09:01 remaining)
SYN Stealth Scan Timing: About 65.72% done; ETC: 01:01 (0:07:50 remaining)
Completed SYN Stealth Scan against 10.50.2.245 in 964.69s (62 hosts left)
Completed SYN Stealth Scan against 10.50.2.209 in 966.00s (61 hosts left)
SYN Stealth Scan Timing: About 70.74% done; ETC: 01:01 (0:06:41 remaining)
Completed SYN Stealth Scan against 10.50.2.218 in 979.56s (60 hosts left)
Completed SYN Stealth Scan against 10.50.2.202 in 981.20s (59 hosts left)
Completed SYN Stealth Scan against 10.50.2.237 in 981.75s (58 hosts left)
Completed SYN Stealth Scan against 10.50.2.238 in 982.62s (57 hosts left)
Completed SYN Stealth Scan against 10.50.2.210 in 986.67s (56 hosts left)
Completed SYN Stealth Scan against 10.50.2.246 in 995.08s (55 hosts left)
Completed SYN Stealth Scan against 10.50.2.211 in 1005.80s (54 hosts left)
SYN Stealth Scan Timing: About 75.96% done; ETC: 01:01 (0:05:30 remaining)
Completed SYN Stealth Scan against 10.50.2.217 in 1101.05s (53 hosts left)
Completed SYN Stealth Scan against 10.50.2.244 in 1106.41s (52 hosts left)
SYN Stealth Scan Timing: About 80.98% done; ETC: 01:01 (0:04:21 remaining)
Completed SYN Stealth Scan against 10.50.2.253 in 1127.63s (51 hosts left)
Completed SYN Stealth Scan against 10.50.2.224 in 1133.64s (50 hosts left)
Completed SYN Stealth Scan against 10.50.2.223 in 1135.17s (49 hosts left)
Completed SYN Stealth Scan against 10.50.2.216 in 1138.23s (48 hosts left)
Completed SYN Stealth Scan against 10.50.2.251 in 1140.85s (47 hosts left)
Completed SYN Stealth Scan against 10.50.2.196 in 1140.96s (46 hosts left)
Completed SYN Stealth Scan against 10.50.2.252 in 1141.62s (45 hosts left)
Completed SYN Stealth Scan against 10.50.2.225 in 1151.06s (44 hosts left)
Completed SYN Stealth Scan against 10.50.2.232 in 1151.17s (43 hosts left)
Completed SYN Stealth Scan against 10.50.2.197 in 1152.81s (42 hosts left)
SYN Stealth Scan Timing: About 85.99% done; ETC: 01:01 (0:03:12 remaining)
Completed SYN Stealth Scan against 10.50.2.236 in 1231.97s (41 hosts left)
Completed SYN Stealth Scan against 10.50.2.203 in 1232.30s (40 hosts left)
Completed SYN Stealth Scan against 10.50.2.195 in 1233.50s (39 hosts left)
Completed SYN Stealth Scan against 10.50.2.254 in 1235.25s (38 hosts left)
Completed SYN Stealth Scan against 10.50.2.231 in 1235.69s (37 hosts left)
Completed SYN Stealth Scan against 10.50.2.239 in 1236.89s (36 hosts left)
Completed SYN Stealth Scan against 10.50.2.220 in 1237.87s (35 hosts left)
Completed SYN Stealth Scan against 10.50.2.219 in 1241.15s (34 hosts left)
Completed SYN Stealth Scan against 10.50.2.247 in 1241.37s (33 hosts left)
Completed SYN Stealth Scan against 10.50.2.227 in 1242.24s (32 hosts left)
Completed SYN Stealth Scan against 10.50.2.255 in 1243.44s (31 hosts left)
Completed SYN Stealth Scan against 10.50.2.204 in 1246.94s (30 hosts left)
SYN Stealth Scan Timing: About 91.22% done; ETC: 01:01 (0:02:01 remaining)
Completed SYN Stealth Scan against 10.50.2.193 in 1267.94s (29 hosts left)
Completed SYN Stealth Scan against 10.50.2.228 in 1268.27s (28 hosts left)
Completed SYN Stealth Scan against 10.50.2.199 in 1294.74s (27 hosts left)
Completed SYN Stealth Scan against 10.50.2.230 in 1300.86s (26 hosts left)
Completed SYN Stealth Scan against 10.50.2.229 in 1301.30s (25 hosts left)
Completed SYN Stealth Scan against 10.50.2.201 in 1301.85s (24 hosts left)
Completed SYN Stealth Scan against 10.50.2.226 in 1303.49s (23 hosts left)
```

```
Completed SYN Stealth Scan against 10.50.2.234 in 1310.63s (22 hosts left)
Completed SYN Stealth Scan against 10.50.2.215 in 1311.29s (21 hosts left)
Completed SYN Stealth Scan against 10.50.2.233 in 1311.72s (20 hosts left)
Completed SYN Stealth Scan against 10.50.2.198 in 1312.82s (19 hosts left)
Completed SYN Stealth Scan against 10.50.2.200 in 1313.69s (18 hosts left)
Completed SYN Stealth Scan against 10.50.2.243 in 1316.75s (17 hosts left)
Completed SYN Stealth Scan against 10.50.2.205 in 1317.63s (16 hosts left)
Completed SYN Stealth Scan against 10.50.2.235 in 1320.04s (15 hosts left)
SYN Stealth Scan Timing: About 96.23% done; ETC: 01:01 (0:00:52 remaining)
Completed SYN Stealth Scan against 10.50.2.208 in 1321.79s (14 hosts left)
Completed SYN Stealth Scan against 10.50.2.206 in 1343.00s (13 hosts left)
Completed SYN Stealth Scan against 10.50.2.214 in 1345.08s (12 hosts left)
Completed SYN Stealth Scan against 10.50.2.240 in 1345.18s (11 hosts left)
Completed SYN Stealth Scan against 10.50.2.213 in 1345.62s (10 hosts left)
Completed SYN Stealth Scan against 10.50.2.207 in 1351.42s (9 hosts left)
Completed SYN Stealth Scan against 10.50.2.241 in 1354.82s (8 hosts left)
Completed SYN Stealth Scan against 10.50.2.250 in 1355.26s (7 hosts left)
Completed SYN Stealth Scan against 10.50.2.212 in 1358.76s (6 hosts left)
Completed SYN Stealth Scan against 10.50.2.194 in 1359.63s (5 hosts left)
Completed SYN Stealth Scan against 10.50.2.248 in 1362.91s (4 hosts left)
Completed SYN Stealth Scan against 10.50.2.249 in 1368.38s (3 hosts left)
Completed SYN Stealth Scan against 10.50.2.222 in 1369.04s (2 hosts left)
Completed SYN Stealth Scan against 10.50.2.242 in 1370.02s (1 host left)
Completed SYN Stealth Scan at 01:01, 1372.44s elapsed (63000 total ports)
Initiating Service scan at 01:01
Initiating OS detection (try #1) against 63 hosts
Retrying OS detection (try #2) against 63 hosts
NSE: Script scanning 63 hosts.
Initiating NSE at 01:02
Completed NSE at 01:02, 0.19s elapsed
Initiating NSE at 01:02
Completed NSE at 01:02, 0.02s elapsed
Nmap scan report for 10.50.2.193
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.193 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.00 ms 10.50.2.193

Nmap scan report for 10.50.2.194
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.194 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.00 ms 10.50.2.194

Nmap scan report for 10.50.2.195
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.195 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.00 ms 10.50.2.195

Nmap scan report for 10.50.2.196
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.196 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.00 ms 10.50.2.196
```

```
Nmap scan report for 10.50.2.197
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.197 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.197
```

```
Nmap scan report for 10.50.2.198
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.198 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.198
```

```
Nmap scan report for 10.50.2.199
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.199 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.199
```

```
Nmap scan report for 10.50.2.200
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.200 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.200
```

```
Nmap scan report for 10.50.2.201
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.201 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.201
```

```
Nmap scan report for 10.50.2.202
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.202 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.202
```

```
Nmap scan report for 10.50.2.203
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.203 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.203

Nmap scan report for 10.50.2.204
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.204 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.204

Nmap scan report for 10.50.2.205
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.205 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.205

Nmap scan report for 10.50.2.206
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.206 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.206

Nmap scan report for 10.50.2.207
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.207 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.207

Nmap scan report for 10.50.2.208
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.208 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.208

Nmap scan report for 10.50.2.209
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.209 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.209

Nmap scan report for 10.50.2.210
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.210 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
```

```
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms 10.50.2.210

Nmap scan report for 10.50.2.211
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.211 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms 10.50.2.211

Nmap scan report for 10.50.2.212
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.212 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms 10.50.2.212

Nmap scan report for 10.50.2.213
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.213 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms 10.50.2.213

Nmap scan report for 10.50.2.214
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.214 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms 10.50.2.214

Nmap scan report for 10.50.2.215
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.215 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms 10.50.2.215

Nmap scan report for 10.50.2.216
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.216 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms 10.50.2.216

Nmap scan report for 10.50.2.217
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.217 are filtered
```



```
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.217

Nmap scan report for 10.50.2.218
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.218 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.218

Nmap scan report for 10.50.2.219
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.219 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.219

Nmap scan report for 10.50.2.220
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.220 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.220

Nmap scan report for 10.50.2.221
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.221 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.221

Nmap scan report for 10.50.2.222
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.222 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.222

Nmap scan report for 10.50.2.223
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.223 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.223

Nmap scan report for 10.50.2.224
```

```
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.224 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.224
```

```
Nmap scan report for 10.50.2.225
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.225 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.225
```

```
Nmap scan report for 10.50.2.226
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.226 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.226
```

```
Nmap scan report for 10.50.2.227
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.227 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.227
```

```
Nmap scan report for 10.50.2.228
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.228 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.228
```

```
Nmap scan report for 10.50.2.229
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.229 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.229
```

```
Nmap scan report for 10.50.2.230
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.230 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.230
```

```
Nmap scan report for 10.50.2.231
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.231 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.231
```

```
Nmap scan report for 10.50.2.232
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.232 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.232
```

```
Nmap scan report for 10.50.2.233
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.233 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.233
```

```
Nmap scan report for 10.50.2.234
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.234 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.234
```

```
Nmap scan report for 10.50.2.235
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.235 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.235
```

```
Nmap scan report for 10.50.2.236
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.236 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms  10.50.2.236
```

```
Nmap scan report for 10.50.2.237
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.237 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
```

```
HOP RTT    ADDRESS
1      0.00 ms 10.50.2.237

Nmap scan report for 10.50.2.238
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.238 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT    ADDRESS
1      0.00 ms 10.50.2.238

Nmap scan report for 10.50.2.239
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.239 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT    ADDRESS
1      0.00 ms 10.50.2.239

Nmap scan report for 10.50.2.240
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.240 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT    ADDRESS
1      0.00 ms 10.50.2.240

Nmap scan report for 10.50.2.241
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.241 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT    ADDRESS
1      0.00 ms 10.50.2.241

Nmap scan report for 10.50.2.242
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.242 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT    ADDRESS
1      0.00 ms 10.50.2.242

Nmap scan report for 10.50.2.243
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.243 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT    ADDRESS
1      0.00 ms 10.50.2.243

Nmap scan report for 10.50.2.244
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.244 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms 10.50.2.244

Nmap scan report for 10.50.2.245
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.245 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms 10.50.2.245

Nmap scan report for 10.50.2.246
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.246 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms 10.50.2.246

Nmap scan report for 10.50.2.247
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.247 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms 10.50.2.247

Nmap scan report for 10.50.2.248
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.248 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms 10.50.2.248

Nmap scan report for 10.50.2.249
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.249 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms 10.50.2.249

Nmap scan report for 10.50.2.250
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.250 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1    0.00 ms 10.50.2.250

Nmap scan report for 10.50.2.251
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.251 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
```

```
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.251

Nmap scan report for 10.50.2.252
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.252 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.252

Nmap scan report for 10.50.2.253
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.253 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.253

Nmap scan report for 10.50.2.254
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.254 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.254

Nmap scan report for 10.50.2.255
Host is up (0.00s latency).
All 1000 scanned ports on 10.50.2.255 are filtered
MAC Address: 00:19:92:B3:5C:A4 (Adtran)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.00 ms  10.50.2.255

Initiating SYN Stealth Scan at 01:02
Scanning 10.50.2.11 [1000 ports]
Discovered open port 1025/tcp on 10.50.2.11
Discovered open port 443/tcp on 10.50.2.11
Discovered open port 139/tcp on 10.50.2.11
Discovered open port 445/tcp on 10.50.2.11
Discovered open port 135/tcp on 10.50.2.11
Discovered open port 80/tcp on 10.50.2.11
Discovered open port 554/tcp on 10.50.2.11
Discovered open port 1027/tcp on 10.50.2.11
Discovered open port 902/tcp on 10.50.2.11
Discovered open port 1028/tcp on 10.50.2.11
Discovered open port 912/tcp on 10.50.2.11
Discovered open port 1026/tcp on 10.50.2.11
Discovered open port 6646/tcp on 10.50.2.11
Discovered open port 10243/tcp on 10.50.2.11
Discovered open port 2869/tcp on 10.50.2.11
Discovered open port 1030/tcp on 10.50.2.11
Discovered open port 5357/tcp on 10.50.2.11
Discovered open port 1031/tcp on 10.50.2.11
Completed SYN Stealth Scan at 01:02, 1.11s elapsed (1000 total ports)
Initiating Service scan at 01:02
Scanning 18 services on 10.50.2.11
Completed Service scan at 01:04, 118.70s elapsed (18 services on 1 host)
```

```
Initiating OS detection (try #1) against 10.50.2.11
NSE: Script scanning 10.50.2.11.
Initiating NSE at 01:04
Completed NSE at 01:05, 65.18s elapsed
Initiating NSE at 01:05
Completed NSE at 01:05, 1.02s elapsed
Nmap scan report for 10.50.2.11
Host is up (0.062s latency).
Not shown: 982 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http
|_ fingerprint-strings:
|_   DNSStatusRequest:
|_   Ia`k,
|_   DNSVersionBindReq:
|_   KWSUP
|_   FourOhFourRequest, GetRequest:
|_   HTTP/1.0 404 Not Found
|_   HTTPOptions:
|_   lDIlF
|_   RPCCheck:
|_   J#u5}w
|_   RTSPRequest:
|_   Jm//:
|_   #,Mo4
|_   TLSSessionReq:
|_   |dq"
|_ http-methods:
|_   Supported Methods: GET
|_ http-title: Site doesn't have a title.
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
443/tcp   open  https
|_ fingerprint-strings:
|_   GetRequest:
|_   HTTP/1.0 404 Not Found
|_   RPCCheck:
|_   B,[e
|_   SSLSessionReq:
|_   4{Xsf
|_   Dwf.
|_   dq_L/
|_ http-methods:
|_   Supported Methods: GET
|_ http-title: Site doesn't have a title.
445/tcp   open  microsoft-ds  Windows 8.1 Single Language 9600 microsoft-ds (workgroup: WORKGROUP)
554/tcp   open  rtsp?
902/tcp   open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp   open  vmware-auth   VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
1025/tcp   open  msrpc        Microsoft Windows RPC
1026/tcp   open  msrpc        Microsoft Windows RPC
1027/tcp   open  msrpc        Microsoft Windows RPC
1028/tcp   open  msrpc        Microsoft Windows RPC
1030/tcp   open  msrpc        Microsoft Windows RPC
1031/tcp   open  msrpc        Microsoft Windows RPC
2869/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-server-header: Microsoft-HTTPAPI/2.0
|_ http-title: Service Unavailable
6646/tcp   open  tcpwrapped
10243/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-server-header: Microsoft-HTTPAPI/2.0
|_ http-title: Not Found
2 services unrecognized despite returning data. If you know the service/version, please submit the
following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-Service :
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF-Port80-TCP:V=7.40I=7%D=5/3%Time=59097269%P=i686-pc-windows-windows%r(G
SF:etRequest,1A,"HTTP/1\0\0x20404\0x20Not\0x20Found\r\n\r\n")%r(HTTPOptions,
SF:40,"%xa9\xc3\xfb\x07jL\xcf\xcf:\x96\x95q`\x8aZ\x09\x1a\xb5\xedlDIlF\x9
SF:3\3xa5\xab\xe2R\xd3\ccc\xcfJ\x84\x7f\xal\x00\x04\x0bV\xcf\x03\xba\x20\x9
SF:b\x0b\xef\xff\x14\x9f\xda\xfe\x7\x80\xd8\xdlYh\x00\x08\x02\xcc&")%r(RT
SF:SPRequest,40,"C\xec\xdf\x7a\x7b!\xad\x00\xdf@\x9a\x9d\x08w\x99\xaf\xde\
SF:xdb\*\x05qA#\xf9a\xfd&\xa3Jm//:\x19q\x9d\x04\xaa#,Mo4\x1c\xcb3\x03Q
SF:\x80l\|\x86\x02\x1f\x03~\x03_\x9cH\x09kT")%r(FourOhFourRequest,1A,"HTT
SF:/1\0\0x20404\0x20Not\0x20Found\r\n\r\n")%r(RPCCheck,5E,"%x1d\x1d\x03\
```

```
SF:xa4\x1d\x07\xf0\xe2\xdc=\xf2i\x06\xdc~\xb3]v\x96Y\xfe\x07\xeenpP\x12\x
SF:0c0\xcb)\[\xd5\x11\x16\x0e!\x20\x08\x94gW\x02!i\xfa\xaa\0\x15v\x06\x98
SF:\^x8e\x9bm\x15\xe7\x92\xfe\x0bH\x07\xe2\x03h\xdd\x1bJ#u5}w\x9eH\x0b\x
SF:0eE\x04\x0b\xad\x1f\x0a\x9e\(\xe7\x8dI\xe5\xda")%r(DNSVersionBindRe
SF:q,34,"tKWsUP\x99M)\x1a0\x94A'\xa86\x16G\xbc\xac\xfeR\x0f\x03\x09\xac\
SF:x061\x08\xeb\x04\x7fRW\x03\x0e\np\xbb\x00\x86dL\x80\x05\x11\x9d\xce\|
SF:\x81")%r(DNSStatusRequest,34,"x11\x1c\xea'\x96\xdb\xae\x97\x02\x08\x82
SF:\x8b\x09\xab\x07\x02\xef\x12%\x88m7\xda\.\xad\x06\x93\xcf\x05\x08\x0f\x
SF:a6\x03Ia'k,\x08\x05\x855'\xca88L\x04\x0a\x9e\x0b6u")%r(SSLSessionReq,68,
SF:"\xec3/\x08\x0f\x1d\x0dY)\xad\x0cay\]\x9b\x07\x80\x03f38U\x0b9\x00\x94\x01
SF:\xe5\x08\xeb\x08\xaa;\x04\xad\[\x08*\xe4\xfe\x17\x00\x01\x06\x04\x03
SF:\x05\x08\x0a5z\x0a\x06+\x17\xab<\x09\x92\x0c\x93\xcd\x0e\x08\x17\x1eW\x
SF:81,\x02\x88\x04\x06\x09\x02\x09d&\x07\x94\?\x9b\x00\x07\xff~\x07I\xee\xcb\
SF:\xc0\x0a\x0b\x02\x0f\x04\x88\xefbU\x0a0\x08Uz\x0c")%r(TLSSessionReq,59,"x83KV\
SF:x20\x07\xed\x09\x17<\x02B\xac\xee\x0a1\x0a\xdb<\x9a\x01\x0a\x08dLub\x04P
SF:6C\x058k\x07<\x0a\x03\|dq"\x88\x1f\x0f\x0d\x08\x0d\x09\x0a\x04\x0c7\x11vt
SF:C\x0f\x0a\x0aR\x0e"\x04\x0c\x0b+\x0d\x10\x90\x05\x07v\x0c\x0f\x08\x07\x0b
SF:\xc6\x0d\x09\x01q\x00\x04J\x19B16\x10\x1c")%r(Kerberos,39,"r\]\x09C\x0a
SF:1\x0b\x0c7;\xec\x04\x0bU\xad\x06\x06>\x08\x04\x1b\x0a\x09\x05\x0b0\[\x03
SF:\xf25\x0b3Q\xef\x086f\x0a\x07\x07S\x0d1-A\x12c\x0a'\x84RM\x0eb\x08fwy\x1bK\
SF:\xbfb\x08H")%r(SMBProgNeg,33,"x0b6\x0a7QX\x17\x04d\x0b4h\x0a~\n\x0c\x10\n>C
SF:\xc6\x0d\x02\]\x02\$\x07\x85\x00c\x08\x06\x0b.\t\x0ab\x09rV\x08f\x0a\x0edx@
SF:\xa94g\x15h\x0f2f\x0a\x03\x0c");
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF-Port443-TCP:V=7.40I=7%D=5/3Time=5909726E%P=i686-pc-windows-windos%r(
SF:SSLSessionReq,67,"x00\x05\xee\x1a\x9e(\xb2\x1b\(\x84\x05<\x0e\o\tG\x0f
SF:a\x14\x02\x1a\x0cbv\x19\x984{Xsf\x0aFS\x04\x9c<\x06\x0a\x0a0\x03\x17'\x
SF:af\x0b6s\x04\x08@f7;\xf8Dwf\.\x07\xbb\x1c\x0eb\x03\x07\x1c\x0c\x082dq
SF:_L/\x10\x0aewN\t\x03\x07\x04\x0b4\x0c\xcc\x0a96\x084\x0a)\x0e8\xac\x05b\x1
SF:7\x0cc6\x13\x0c\t)\|\")%r(TLSSessionReq,53,"x02\xec>\x07KN\x0e\x0b2\x06H\
SF:x92m\x0b4'\xb9<\x0f\x1f\x02\x89w\x0d\x08\x0a\x0a\x0a\x0b\x01\x0b\x12GS\x0d\x09
SF:d9m\x0d<\x09\x03c\x08\x0a@x11+\x08\x05\x07f\x0dbu\x09c\x0ebYj\x0df:\xf6\x0b
SF:\x0f\x08e\x1f\x0d\x09"\x08\x0d\x09\x0af\x0fN\x09EV\x0afv\x07\x0c1\x12\x0f
SF:\xe1+\")%r(SSLv23SessionReq,3F,"x06\x04\x09\x0c\x0b7\x089\x0f9ME\x0a+\xc
SF:0B\x08c\x04\x0af\x0cc\x0fd\x08\x0a4z\x0ft0\x05\x0a1\x0d\x0c\x08\x08\]\x0b\x0b
SF:\xed\x06\x11*\x0f\^x05\xef\xfb#\x10'\x1\xecj\x14_\x0e\xff\x10\x0e2s\xec
SF:\x08\x09\x0b\x08\x04\x0e0")%r(OpenVPN,32,"x0b4\x0b0\x0a1\x094\^x080\x08f\x0b
SF:9a\x091\x0bc5\x0b8P\x0e$P\x07frRH\x0fd4\x0b1\|0\$\x081P\x12\x08g#\x08n\x093\x1
SF:87\x0b7)\x08f\x0f0\x09a\x0c2\x02\x1d\?M\x0a")%r(GetRequest,1A,"HTTP/1.0\x20
SF:404\x20Not\x20Found\r\n\r\n")%r(HTTPOptions,33,"~u\x0eb\x0c\x08f\t\x07f\x0a
SF:3\x07fk\x1f\x08cw\x08\x0aR\x1e\x0bX\)\x0b5\x0caue\x02\x0b7\x088\x0d1\x0e\x02u\
SF:\x14t{\x06\x06\x05\x04d\x0b0\x18Qs\x096F\x096\x0d0K#\x0b")%r(RTSPRequest,61
SF:"\x06j\]\x1a\x0cXe\xfb\x0b\x09\x09\x0f\x0d\x09\x0f7\x0aB\x0b3\x0c9pZ\x11\x
SF:d8\x0b\x11\x0a\x06fT\x1az4\x09d\x04Ko\x02\x1a\x0c\x05\x0f0\x0f0MQ\*\x08\x0d4
SF:\x0b2M\x14\xad\x0b3\x08\x0ab\x0e\x05f5n\x02/\x0ef\x0b6c\x09b\x04\x1f\x0e\$\x0a5\
SF:\x0e\x0b1y\x08\x0b\x0d\x07zU\x089-6\x17\x090\x08vVB\x097\x0d1\x091b\x12\x0b\x087\x0e
SF:b{\xf8\x05\x0b\x0a1n")%r(RPCCheck,38,";\x0b'\x09c\x09f\x0fs\x0b2T\x0ab\x16X
SF:st\x09b\x0eds\x0a\x0a2\x0a\x0c\x1aH\x0e95\x0c0\x0dbB,\[e\x09c\x05\x0ac\x09c\x0a2
SF:k:<\x0b8\x0a0\x946\x02\x0c1L\x13\x087\x07\x096\x086Zk\x17\*")%r(DNSVersionBin
SF:dReq,52,"x08\x06\x16\x06fT\x09eh~\(\x06n\x04\x0b6&\x0a\x0e0m\x07;0\x01\x12
SF:\xf9\x0f1\x08\x06\x01\x0e1\x0a\x096\x08f\x0d1X\x0fay\x091&\x09c\x0b6'\xaaamY!\xc
SF:9\x0f\x07\x01\x0a3=J\.\x03n\x06\x0d0z{\x1f\x05\x0d1'\x0b0\x07f\x085\x10Q\x08
SF:1\x06\x07eW\x0e2\]\x0a\x0b\x11M\x0d\x06\?")%r(DNSStatusRequest,6E,"Y\x0a9\
SF:\xec'r\x16f\x0d\x047\x0e\x08fL\x07j\x07\x0f0\x0ef;Y\x04\x0ebd\x0c\x0f6Wz\x0b
SF:0V\x099\x1b_\x02'D3\x0efW\t\x0a\x06_\x0ccnu~\x06\x09b\x0a0\x0c6\x0c2\x04f\x0eb\
SF:\x11\x0a\x0b0\x04J\x0a6s\x0abg\x0b\x0ca0>\xf96~\x090\x0e2\x0d6T\x086\x0a\x0c\x0e
SF:a\x10tdy\x0b9s\tw\x091\x02\x0ab\x0fb\x0f9\x0cf~\x0f\x0b\x0e\n\x0a0=\xa5\x08\x08d\
SF:x15\x0a2\x0a1\x17\x0a\x0d7");
Device type: general purpose
Running: Microsoft Windows Vista|7
OS CPE: cpe:/o:microsoft:windows_vista cpe:/o:microsoft:windows_7::sp1
OS details: Microsoft Windows Vista or Windows 7 SP1
Uptime guess: 2.313 days (since Sun Apr 30 17:34:37 2017)
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: PCGZZ01; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| nbstat: NetBIOS name: PCGZZ01, NetBIOS user: <unknown>, NetBIOS MAC: 00:05:9a:3c:78:00 (Cisco
Systems)
| Names:
| PCGZZ01<20> Flags: <unique><active>
| PCGZZ01<00> Flags: <unique><active>
| WORKGROUP<00> Flags: <group><active>
```



```
| smb-os-discovery:
|   OS: Windows 8.1 Single Language 9600 (Windows 8.1 Single Language 6.3)
|   OS CPE: cpe:/o:microsoft:windows_8.1::-
|   NetBIOS computer name: PCGZZ01\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2017-05-03T01:04:14-05:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_ smbv2-enabled: Server supports SMBv2 protocol
```

```
NSE: Script Post-scanning.
Initiating NSE at 01:05
Completed NSE at 01:05, 0.00s elapsed
Initiating NSE at 01:05
Completed NSE at 01:05, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (256 hosts up) scanned in 5934.61 seconds
Raw packets sent: 523514 (24.195MB) | Rcvd: 4316 (179.252KB)
```


7.2 Escaneo red

```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-04 07:29 Hora de verano central (México)
NSE: Loaded 143 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 07:29
Completed NSE at 07:29, 0.00s elapsed
Initiating NSE at 07:29
Completed NSE at 07:29, 0.00s elapsed
Initiating Ping Scan at 07:29
Scanning 256 hosts [4 ports/host]
Ping Scan Timing: About 27.93% done; ETC: 07:31 (0:01:20 remaining)
Ping Scan Timing: About 56.69% done; ETC: 07:31 (0:00:47 remaining)
Completed Ping Scan at 07:31, 106.93s elapsed (256 total hosts)
Nmap scan report for 10.50.3.0 [host down]
Nmap scan report for 10.50.3.1 [host down]
Nmap scan report for 10.50.3.2 [host down]
Nmap scan report for 10.50.3.3 [host down]
Nmap scan report for 10.50.3.4 [host down]
Nmap scan report for 10.50.3.5 [host down]
Nmap scan report for 10.50.3.6 [host down]
Nmap scan report for 10.50.3.7 [host down]
Nmap scan report for 10.50.3.8 [host down]
Nmap scan report for 10.50.3.9 [host down]
Nmap scan report for 10.50.3.10 [host down]
Nmap scan report for 10.50.3.11 [host down]
Nmap scan report for 10.50.3.12 [host down]
Nmap scan report for 10.50.3.13 [host down]
Nmap scan report for 10.50.3.14 [host down]
Nmap scan report for 10.50.3.15 [host down]
Nmap scan report for 10.50.3.16 [host down]
Nmap scan report for 10.50.3.17 [host down]
Nmap scan report for 10.50.3.18 [host down]
Nmap scan report for 10.50.3.19 [host down]
Nmap scan report for 10.50.3.20 [host down]
Nmap scan report for 10.50.3.21 [host down]
Nmap scan report for 10.50.3.22 [host down]
Nmap scan report for 10.50.3.23 [host down]
Nmap scan report for 10.50.3.24 [host down]
Nmap scan report for 10.50.3.25 [host down]
Nmap scan report for 10.50.3.26 [host down]
Nmap scan report for 10.50.3.27 [host down]
Nmap scan report for 10.50.3.28 [host down]
Nmap scan report for 10.50.3.29 [host down]
Nmap scan report for 10.50.3.30 [host down]
Nmap scan report for 10.50.3.31 [host down]
Nmap scan report for 10.50.3.32 [host down]
Nmap scan report for 10.50.3.33 [host down]
Nmap scan report for 10.50.3.34 [host down]
Nmap scan report for 10.50.3.35 [host down]
Nmap scan report for 10.50.3.36 [host down]
Nmap scan report for 10.50.3.37 [host down]
Nmap scan report for 10.50.3.38 [host down]
Nmap scan report for 10.50.3.39 [host down]
Nmap scan report for 10.50.3.40 [host down]
Nmap scan report for 10.50.3.41 [host down]
Nmap scan report for 10.50.3.42 [host down]
Nmap scan report for 10.50.3.43 [host down]
Nmap scan report for 10.50.3.44 [host down]
Nmap scan report for 10.50.3.45 [host down]
Nmap scan report for 10.50.3.46 [host down]
Nmap scan report for 10.50.3.47 [host down]
Nmap scan report for 10.50.3.48 [host down]
Nmap scan report for 10.50.3.49 [host down]
Nmap scan report for 10.50.3.50 [host down]
Nmap scan report for 10.50.3.51 [host down]
Nmap scan report for 10.50.3.52 [host down]
Nmap scan report for 10.50.3.53 [host down]
Nmap scan report for 10.50.3.54 [host down]
Nmap scan report for 10.50.3.55 [host down]
Nmap scan report for 10.50.3.56 [host down]
Nmap scan report for 10.50.3.57 [host down]
Nmap scan report for 10.50.3.58 [host down]
Nmap scan report for 10.50.3.59 [host down]
Nmap scan report for 10.50.3.60 [host down]
```



```
Nmap scan report for 10.50.3.211 [host down]
Nmap scan report for 10.50.3.212 [host down]
Nmap scan report for 10.50.3.213 [host down]
Nmap scan report for 10.50.3.214 [host down]
Nmap scan report for 10.50.3.215 [host down]
Nmap scan report for 10.50.3.216 [host down]
Nmap scan report for 10.50.3.217 [host down]
Nmap scan report for 10.50.3.218 [host down]
Nmap scan report for 10.50.3.219 [host down]
Nmap scan report for 10.50.3.220 [host down]
Nmap scan report for 10.50.3.221 [host down]
Nmap scan report for 10.50.3.222 [host down]
Nmap scan report for 10.50.3.223 [host down]
Nmap scan report for 10.50.3.224 [host down]
Nmap scan report for 10.50.3.225 [host down]
Nmap scan report for 10.50.3.226 [host down]
Nmap scan report for 10.50.3.227 [host down]
Nmap scan report for 10.50.3.228 [host down]
Nmap scan report for 10.50.3.229 [host down]
Nmap scan report for 10.50.3.230 [host down]
Nmap scan report for 10.50.3.231 [host down]
Nmap scan report for 10.50.3.232 [host down]
Nmap scan report for 10.50.3.233 [host down]
Nmap scan report for 10.50.3.234 [host down]
Nmap scan report for 10.50.3.235 [host down]
Nmap scan report for 10.50.3.236 [host down]
Nmap scan report for 10.50.3.237 [host down]
Nmap scan report for 10.50.3.238 [host down]
Nmap scan report for 10.50.3.239 [host down]
Nmap scan report for 10.50.3.240 [host down]
Nmap scan report for 10.50.3.241 [host down]
Nmap scan report for 10.50.3.242 [host down]
Nmap scan report for 10.50.3.243 [host down]
Nmap scan report for 10.50.3.244 [host down]
Nmap scan report for 10.50.3.245 [host down]
Nmap scan report for 10.50.3.246 [host down]
Nmap scan report for 10.50.3.247 [host down]
Nmap scan report for 10.50.3.248 [host down]
Nmap scan report for 10.50.3.249 [host down]
Nmap scan report for 10.50.3.250 [host down]
Nmap scan report for 10.50.3.251 [host down]
Nmap scan report for 10.50.3.252 [host down]
Nmap scan report for 10.50.3.253 [host down]
Nmap scan report for 10.50.3.254 [host down]
Nmap scan report for 10.50.3.255 [host down]
NSE: Script Post-scanning.
Initiating NSE at 07:31
Completed NSE at 07:31, 0.00s elapsed
Initiating NSE at 07:31
Completed NSE at 07:31, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 256 IP addresses (0 hosts up) scanned in 125.62 seconds
Raw packets sent: 2048 (77.824KB) | Rcvd: 14143 (3.257MB)
```

8 Anexo V Descubrimiento de la red 10.50.4.0

Al momento del escaneo y descubrimiento de las redes, esta no estaba implementada aún.