TECNOLÓGICO DE MONTERREY®

Dictámen final sobre
Auditoría de Seguridad Información

Reporte de Reconocimiento

Descripción breve

El reporte de escaneo de vulnerabilidades detalla el resultado del análisis de los activos encontrados en el reporte de reconocimiento.

Jesús R. González / Juan Arturo Nolazco

jrgonza@gmail.com jnolazco@itesm.mx

Índice

Versión	Fecha	Descripción
1	18 – Mayo – 2017	Documento de escaneo y análisis de vulnerabilidades correspondiente a la infraestructura del conteo rápido del IEC Documento de escaneo y análisis

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

1 Resumen Ejecutivo

Este documento presenta el resultado del análisis de vulnerabilidades que se realizo sobre los activos del Instituto Electoral de Coahuila así como los mecanismos y herramientas utilizadas para tal propósito.

El análisis presenta las vulnerabilidades con su clasificación basada en la base de datos de vulnerabilidades NVD con su impacto potencial así como la facilidad de explotación.

Este documento no presenta recomendaciones al respecto, solamente lo encontrado y documentado respecto a las clasificaciones de la NVD.

1.1 Alcances

El análisis solicitado por parte del IEC fue sobre activos de información primordiales para la operación del conteo rápido (PREP) el día de la elección estatal. Estos activos son:

- Infraestructura (Redes y servidores)
- Aplicaciones WEB (5 desarrollos)
- Problemas de configuración en infraestructura y servicios (Web servers, DB Servers)

2 Proceso de escaneo

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 os desarrollos en cuestión.

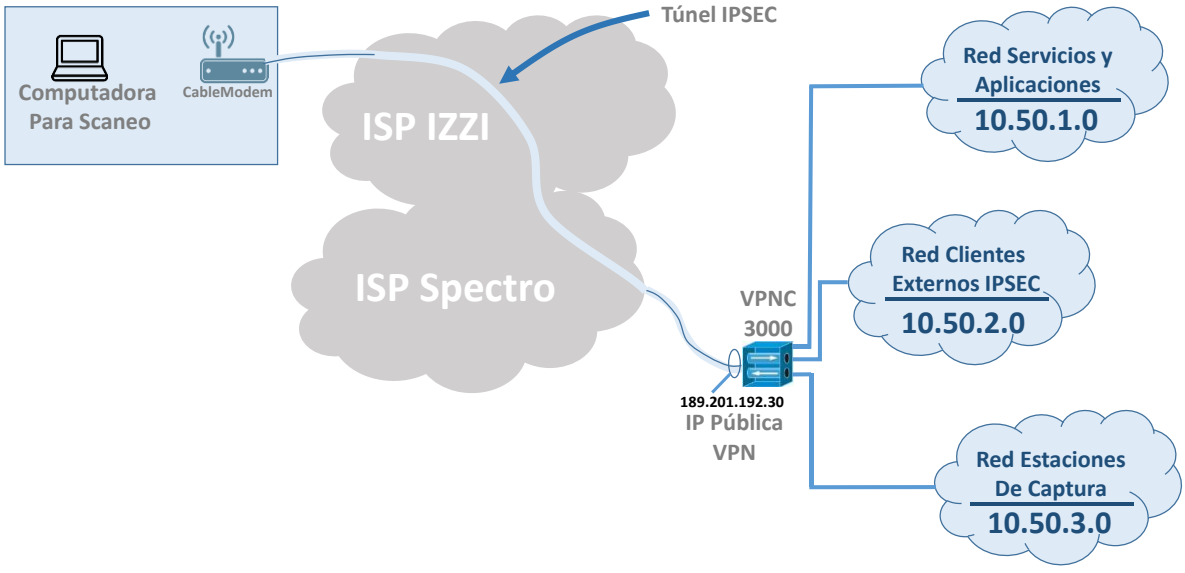

Ilustración 1 Ambiente para descubrimiento de vulnerabilidades

Hoy en día existe SPECTRO como proveedor de servicios, pero previo a las elecciones, habrá un proveedor adicional que aun no entra en producción. Todas las sesiones y pruebas de descubrimiento se hicieron mediante un túnel de IPSEC. Se determino utilizar la red de IZZI ya que de las que se tenía disponible era la que tenía mejor conteo de sitios para alcanzarla.

3 Identificación de vulnerabilidades en los sistemas

Las vulnerabilidades se revisaron contra la base de datos abierta de vulnerabilidades (OSVDB) sobre la cual se encontraron los siguientes activos con las siguientes vulnerabilidades durante los escaneos que se dieron sobre la infraestructura.

10.50.1.100		
ID OSVDB	**ID CVE**	**Descripción**
OSVDB:576	CVE-2015-1476	Requerir un drectorio con %00/, %2e/, %2f/ or %5c/ al final causa que el servidor muestre contenidos del directorio.
OSVDB:119	CVE-1999-0269	remote server may allow directory listings through Web Publisher by forcing the server to show all files via 'open directory browsing'. Web Publisher should be disabled
OSVDB:3092		**/webdav/index.html: WebDAV support is enabled.**
OSVDB:3288		directory listing when /'s are requested

10.50.1.103		
ID		**Descripción**
OSVDB-3092		**/webdav/index.html: WebDAV support is enabled.**

10.50.1.106		
ID		**Descripción**
OSVDB-3233		/jsp-examples/: Apache Java Server Pages documentation

10.50.1.109		
ID		**Descripción**
OSVDB-35878		PHP-Nuke module allows user names and passwords to be viewed
OSVDB-3092		**/webdav/index.html: WebDAV support is enabled.**

10.50.1.111		
ID	**Descripción**	**Descripción**
OSVDB-3268		Directory indexing is enabled
OSVDB-576	CVE-2015-1476	Requerir un drectorio con %00/, %2e/, %2f/ or %5c/ al final causa que el servidor muestre contenidos del directorio.
OSVDB-119	CVE-1999-0269	Remote server may allow directory listings through Web Publisher by forcing the server to show all files via 'open directory browsing'. Web Publisher should be disabled
OSVDB-3288		Abyss 1.03 reveals directory listing when /'s are requested
OSVDB-3233		Apache default file found

Las aplicaciones escaneadas se encuentran sobre la red 10.50.1.0. Para las redes 10.50.2.0 y 10.50.3.0 no encontraron activos que escanear ya que estaban bloqueados o bien apagados. De acuerdo a las entrevistas estas redes están en proceso de configurar los elementos para ser instalados ahí, por lo que al momento del reconocimiento no se encontró nada que verificar.

IP	Puerto	Aplicación	CVE Id	Nivel de Severidad (1-10)
10.50.1.8	TCP/22	HP Integrated Lights-Out mpSSH 0.2.1	-	-
	TCP/80	HPE-iLO-Server/1.30 (SSH)	CVE-2016-4375	Crítico (9.8)
			CVE-2015-5435	Medio (4.0)
	TCP/443	ssl/https HPE-iLO-Server/1.30		
10.50.1.9	TCP/22	OpenSSH 7.2p2 Ubuntu 4ubuntu2.1	CVE-2015-8325	Alto (7.8)
			CVE-2016-3115	Medio (6.4)
	TCP/80	HPE-iLO-Server/1.30	-	-
	TCP/443	ssl/https HPE-iLO-Server/1.30	-	-
10.50.1.10	TCP/22	OpenSSH 7.2p2 Ubuntu 4ubuntu2.1	CVE-2015-8325	Alto (7.8)
			CVE-2016-3115	Medio (6.4)
	TCP/80	Apache httpd 2.4.18	CVE-2016-4979	Alto (7.5)
			CVE-2016-1546	Medio (5.9)
10.50.1.11	TCP/22	OpenSSH 7.2p2 Ubuntu 4ubuntu2.1	CVE-2015-8325	Alto (7.8)
			CVE-2016-3115	Medio (6.4)
10.50.1.100	TCP/80	Apache/2.4.18 (Ubuntu)	CVE-2016-4979	Alto (7.5)
			CVE-2016-1546	Medio (5.9)
	TCP/22	OpenSSH 7.2p2 Ubuntu 4ubuntu2.1	CVE-2015-8325	Alto (7.8)
			CVE-2016-3115	Medio (6.4)
10.50.1.101	TCP3306	MySQL 5.7.17-0ubuntu0.16.04.2	CVE-2017-3600	Medio (6.6)
			CVE-2017-3599	Alto (7.5)
			CVE-2017-3455	Medio (5.5)
			CVE-2017-3454	Medio (5.4)
			CVE-2017-3453	Medio (6.5)
			CVE-2017-3450	Alto (7.5)
			CVE-2017-3331	Medio (6.5)
			CVE-2017-3329	Alto (7.5
			CVE-2017-3309	Alto (7.7)
			CVE-2017-3308	Alto (7.7)
10.50.1.102	-	Detectado pero no reporto puertos	-	-
10.50.1.103	TCP/80	nginx/1.10.0 (Ubuntu)	CVE-2012-1180	Medio (5.0)
10.50.1.104	TCP/21	vsftpd 2.0.8 or later	-	-
10.50.1.105	-	Detectado pero no reporto puertos	-	-
10.50.1.106	TCP/80	Apache httpd 2.4.18 ((Ubuntu))	CVE-2016-4979	Alto (7.5)
			CVE-2016-1546	Medio (5.9)
10.50.1.107	-	Detectado pero no reporto puertos	-	-
10.50.1.108	TCP/8086	InfluxDB http admin 1.2.2	-	-
10.50.1.109	TCP/3000	Grafana	-	-
10.50.1.110		Detectado pero no reporto puertos	-	-
10.50.1.111	TCP/80	Apache httpd 2.4.18	CVE-2016-4979	Alto (7.5)
			CVE-2016-1546	Medio (5.9)

No hay evidencia que estas vulnerabilidades estén presente en los sistemas. El listado se tomo de las versiones de software instaladas y comparada con la lista de National Vulnerability Database (NVD - https://nvd.nist.gov/vuln/search)

Revisando las aplicaciones y versiones que se tienen instaladas, se detallan estas vulnerabilidades (solo están documentadas las que están por encima de la calificación 5.0).

Tabla de Vulnerabilidades y descripción		
Id Vulnerabilidad	**Descripción**	**Fecha de Alta**
CVE-2016-4979	The Apache HTTP Server 2.4.18 through 2.4.20, when mod_http2 and mod_ssl are enabled, does not properly recognize the "SSLVerifyClient require" directive for HTTP/2 request authorization, which allows remote attackers to bypass intended access restrictions by leveraging the ability to send multiple requests over a single connection and aborting a renegotiation	06/Jul/2016
CVE-2016-4375	Multiple unspecified vulnerabilities in HPE Integrated Lights-Out 3 (aka iLO 3) firmware before 1.88, Integrated Lights-Out 4 (aka iLO 4) firmware before 2.44, and Integrated Lights-Out 4 (aka iLO 4) mRCA firmware before 2.32 allow remote attackers to obtain sensitive information, modify data, or cause a denial of service via unknown vectors	08/Sep/2016
CVE-2015-5435	Unspecified vulnerability in HP Integrated Lights-Out (iLO) firmware 3 before 1.85 and 4 before 2.22 allows remote authenticated users to cause a denial of service via unknown vectors.	29/sep/2015
CVE-2015-8325	The do_setup_env function in session.c in sshd in OpenSSH through 7.2p2, when the UseLogin feature is enabled and PAM is configured to read .pam_environment files in user home directories, allows local users to gain privileges by triggering a crafted environment for the /bin/login program, as demonstrated by an LD_PRELOAD environment variable.	30/Abr/2016
CVE-2016-3115	Multiple CRLF injection vulnerabilities in session.c in sshd in OpenSSH before 7.2p2 allow remote authenticated users to bypass intended shell-command restrictions via crafted X11 forwarding data, related to the (1) do_authenticated1 and (2) session_x11_req functions.	22/Mar/2016
CVE-2016-1546	The Apache HTTP Server 2.4.17 and 2.4.18, when mod_http2 is enabled, does not limit the number of simultaneous stream workers for a single HTTP/2 connection, which allows remote attackers to cause a denial of service (stream-processing outage) via modified flow-control windows.	06/Jul/2016
CVE-2012-1180	Use-after-free vulnerability in nginx before 1.0.14 and 1.1.x before 1.1.17 allows remote HTTP servers to obtain sensitive information from process memory via a crafted backend response, in conjunction with a client request.	17/Abr/2015
CVE-2017-3600	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client mysqldump). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in takeover of MySQL Server. Note: CVE-2017-3600 is equivalent to CVE-2016-5483. CVSS 3.0 Base Score 6.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H).	24/Abr/2017
CVE-2017-3599	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Pluggable Auth). Supported versions that are affected are 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). NOTE: the previous information is from the April 2017 CPU. Oracle has not commented on third-party claims that this issue is an integer overflow in sql/auth/sql_authentication.cc which allows remote attackers to cause a denial of service via a crafted authentication packet	24/Abr/2017
CVE-2017-3455	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.7.17 and earlier. Easily "exploitable" vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data as well as unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).	24/Abr/2017
CVE-2017-3454	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: InnoDB). Supported versions that are affected are 5.7.17 and earlier. Easily "exploitable" vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).Abr/24/201	24/Abr/2017
CVE-2017-3453	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	24/Abr/2017

Tabla de Vulnerabilidades y descripción		
Id Vulnerabilidad	**Descripción**	**Fecha de Alta**
CVE-2017-3450	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Memcached). Supported versions that are affected are 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)	24/Abr/2017
CVE-2017-3331	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: InnoDB). Supported versions that are affected are 5.7.17 and earlier. Easily "exploitable" vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	24/Abr/2017
CVE-2017-3329	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Thread Pooling). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	24/Abr/2017
CVE-2017-3309	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. While the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 7.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H).	24/Abr/2017
CVE-2017-3308	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. While the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 7.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H).	24/Abr/2017

Estas vulnerabilidades son asociadas a la versión de la aplicación o sistema operativo que se tienen identificadas, pero en el escaneo no se encontró evidencia que estuvieran presentes en los sistemas, puede haber varias razones:

- Los sistemas estan correctamente parchados pero se encuentran en la misma versión
- El sistema por alguna razón que nos esta bloqueando no permite cuestionar a la aplicación sobre su estado o situación mas alla del nombre, versión y pocos datos adicionales que nos ofrece la tarea de escaneo que hicimos.

Las vulnarabilidades que no se les encontró evidencia, no se les practico análisis de riesgo ya que no se tiene evidencia que existan en los sistemas y tampoco contra que evaluarlo en dado caso. Las medidas a tomar contra estas serían recomendaciones.

4 Vulnerabilidades en el Proceso

En base a los procesos descritos por el personal del IEC, se pudo constatar las siguientes situaciones de vulnerabilidad.

Vulnerabilidad Captura	Descripción
No hay registro de personal de captura en el centro	No hay registro de visitantes y/o personas que están laborando en el centro de acopio central
No se valida la entrada de personal	No se valida la entrada de personal a la entrada del centro de captura
No ha hay manuales que describan los procesos en sitio de operación	No se tienen manuales de procesos en los sitios de operación
Solo hay una persona que lo sabe operar	Solo hay una persona que sabe operar los equipos en sitio
No tener registro de pertenencias	No hay revisión de lo que cada persona trae a las instalaciones
No tener punto de control de entrada en el sitio de captura	No hay un punto de control para registrar pertenencias al entrar al centro de captura
No ha hay manuales que describan los procesos en sitio de operación	No hay manuales para describir procesos en sitios de operación
Falla en los proveedores de Internet para conectar al sitio central	Caídad de enlace de alguno de los proveedores de Internet
Smartphone de captura controlado	Responsable y dueño del Smartphone para captura
Aplicación de captura teléfono	Control de lo que se puede instalar al telefono
Aplicación de captura en host sitio central	No haya validación de dígitos al momento de entrar la captura en el campo de captura
No hay login en las terminales	No se requiere un usuario/clave para entrar en la aplicación de captura en el sitio central de acopio del IEC.

Vulnerabilidad Operación	Descripción
Sin respuesta por parte del equipo de soporte en el centro de datos	No se tiene respuesta del equipo de soporte por parte del centro de datos como plan de respuesta a incidentes
Falla de servicio en la nube	Servicio del proveedor de la nube valla
Enlaces de sitios de centros de acopio remotos.	Enlaces de los sitios remotos de captura reportan incidente de conectividad
Enlace de comunicación del centro acopio central	Enlaces del centro de acopio central reportan incomunicación
Por alguna razón los sistemas de captura fallan	Los sistemas usados en la captura fallan
Caída eléctrica	Falla en los sistemas eléctricos que alimentan a las estaciones de captura centrales
Falla HW	Los servidores tienen falla (en cualquiera de los componentes)
Falla de Disco	El disco de almacenamiento falla o se llena con imágenes.
Plan de contingencia	Se tiene definido, pero aun no se tiene el proveedor para ejecutar dicho plan
Matriz de responsables x aplicación	Localizar a los ingenieros asignados para las aplicaciones
Monitoreo de la infraestructura	Que haya un proceso regular de monitoreo de infraestructura

Anexo 1 – Evidencia Vulnerabilidades 10.50.1.8

```
scann.mc1 10.50.1.8
Starting Scann Report ....
Start Time : 20170512.06031494587013 ..
-------------------------------------------

20170512.06031494587013
Ping Reachable Host 10.50.1.8 ::
PING 10.50.1.8 (10.50.1.8) 56(84) bytes of data.
64 bytes from 10.50.1.8: icmp_req=1 ttl=255 time=3.55 ms
64 bytes from 10.50.1.8: icmp_req=2 ttl=255 time=3.12 ms

--- 10.50.1.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 3.122/3.339/3.557/0.225 ms

20170512.06031494587015

-------------------------------------------
-------------------------------------------
-------------------------------------------
starting NMAP Scann Report ....
20170512.06031494587015

Starting Nmap 5.21 ( http://nmap.org ) at 2017-05-12 06:03 CDT
Nmap scan report for 10.50.1.8
Host is up (0.0036s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
17988/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 2.76 seconds

20170512.06031494587018

-------------------------------------------
-------------------------------------------
-------------------------------------------
 Starting Nmap ScannForce Report
20170512.06031494587018

Starting Nmap 5.21 ( http://nmap.org ) at 2017-05-12 06:03 CDT
NSE: Loaded 36 scripts for scanning.
Initiating SYN Stealth Scan at 06:03
Scanning 10.50.1.8 [1000 ports]
Discovered open port 443/tcp on 10.50.1.8
Discovered open port 80/tcp on 10.50.1.8
Discovered open port 22/tcp on 10.50.1.8
Discovered open port 17988/tcp on 10.50.1.8
Completed SYN Stealth Scan at 06:03, 2.56s elapsed (1000 total ports)
Initiating Service scan at 06:03
Scanning 4 services on 10.50.1.8
Service scan Timing: About 75.00% done; ETC: 06:06 (0:00:35 remaining)
Completed Service scan at 06:05, 112.83s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against 10.50.1.8
Retrying OS detection (try #2) against 10.50.1.8
Initiating Traceroute at 06:05
Completed Traceroute at 06:05, 0.01s elapsed
NSE: Script scanning 10.50.1.8.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 06:05
Completed NSE at 06:05, 1.75s elapsed
NSE: Script Scanning completed.
Nmap scan report for 10.50.1.8
Host is up (0.0033s 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?
```

```
443/tcp   open  ssl/https?
17988/tcp open  unknown
3 services unrecognized despite returning data. If you know the service/version, please submit the
following fingerprints at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=5.21%I=7%D=5/12%Time=59159693%P=x86_64-unknown-linux-gnu%r
SF:(GetRequest,9E,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20
SF:text/plain\r\nConnection:\x20close\r\nDate:\x20Fri,\x2012\x20May\x20201
SF:7\x2005:03:47\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30\r\nContent-Leng
SF:th:\x200\r\n\r\n")%r(HTTPOptions,AC,"HTTP/1\.1\x20501\x20Not\x20Impleme
SF:nted\r\nContent-Type:\x20text/plain\r\nDate:\x20Fri,\x2012\x20May\x2020
SF:17\x2005:03:47\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30\r\nX-Frame-Opt
SF:ions:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(RTSPRequest,AC,
SF:"HTTP/1\.1\x20501\x20Not\x20Implemented\r\nContent-Type:\x20text/plain\
SF:r\nDate:\x20Fri,\x2012\x20May\x202017\x2005:03:52\x20GMT\r\nServer:\x20
SF:HPE-iLO-Server/1\.30\r\nX-Frame-Options:\x20sameorigin\r\nContent-Lengt
SF:h:\x200\r\n\r\n")%r(FourOhFourRequest,9E,"HTTP/1\.1\x20400\x20Bad\x20Re
SF:quest\r\nContent-Type:\x20text/plain\r\nConnection:\x20close\r\nDate:\x
SF:20Fri,\x2012\x20May\x202017\x2005:04:02\x20GMT\r\nServer:\x20HPE-iLO-Se
SF:rver/1\.30\r\nContent-Length:\x200\r\n\r\n")%r(Help,A8,"HTTP/1\.1\x2040
SF:0\x20Bad\x20Request\r\nContent-Type:\x20text/plain\r\nDate:\x20Fri,\x20
SF:12\x20May\x202017\x2005:04:22\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30
SF:\r\nX-Frame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(
SF:SSLSessionReq,A8,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x
SF:20text/plain\r\nDate:\x20Fri,\x2012\x20May\x202017\x2005:04:29\x20GMT\r
SF:\nServer:\x20HPE-iLO-Server/1\.30\r\nX-Frame-Options:\x20sameorigin\r\n
SF:Content-Length:\x200\r\n\r\n")%r(LPDString,A8,"HTTP/1\.1\x20400\x20Bad\
SF:x20Request\r\nContent-Type:\x20text/plain\r\nDate:\x20Fri,\x2012\x20May
SF:\x202017\x2005:04:40\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30\r\nX-Fra
SF:me-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(SIPOption
SF:s,6B8,"HTTP/1\.1\x20501\x20Not\x20Implemented\r\nContent-Type:\x20text/
SF:plain\r\nDate:\x20Fri,\x2012\x20May\x202017\x2005:04:50\x20GMT\r\nServe
SF:r:\x20HPE-iLO-Server/1\.30\r\nX-Frame-Options:\x20sameorigin\r\nContent
SF:-Length:\x200\r\n\r\nHTTP/1\.1\x20501\x20Not\x20Implemented\r\nContent-
SF:Type:\x20text/plain\r\nDate:\x20Fri,\x2012\x20May\x202017\x2005:04:50\x
SF:20GMT\r\nServer:\x20HPE-iLO-Server/1\.30\r\nX-Frame-Options:\x20sameori
SF:gin\r\nContent-Length:\x200\r\n\r\nHTTP/1\.1\x20501\x20Not\x20Implement
SF:ed\r\nContent-Type:\x20text/plain\r\nDate:\x20Fri,\x2012\x20May\x202017
SF:\x2005:04:50\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30\r\nX-Frame-Optio
SF:ns:\x20sameorigin\r\nContent-Length:\x200\r\n\r\nHTTP/1\.1\x20501\x20No
SF:t\x20Implemented\r\nContent-Type:\x20text/plain\r\nDate:\x20Fri,\x2012\
SF:x20May\x202017\x2005:04:50\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30\r\
SF:nX-Frame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\nHTTP/1\.
SF:1\x20501\x20Not\x20Implemented\r\nContent-Type:\x20text/plain\r\nDate:\
SF:x20Fri,\x2012\x20May\x202017\x2005:04:50\x20GMT\r\nServer:\x20HPE-iLO-S
SF:erver/1\.30\r\nX-Frame-Options:\x20sameorigin\r\nContent-Length:\x200\r
SF:\n\r\nHTTP/1\.1\x20501\x20Not\x20Implemented\r\nContent-Ty");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port443-TCP:V=5.21%T=SSL%I=7%D=5/12%Time=59159699%P=x86_64-unknown-linux-
gnu%r(GetRequest,9E,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\
SF:x20text/plain\r\nConnection:\x20close\r\nDate:\x20Fri,\x2012\x20May\x20
SF:2017\x2005:03:53\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30\r\nContent-L
SF:ength:\x200\r\n\r\n")%r(HTTPOptions,AC,"HTTP/1\.1\x20501\x20Not\x20Impl
SF:emented\r\nContent-Type:\x20text/plain\r\nDate:\x20Fri,\x2012\x20May\x2
SF:02017\x2005:03:58\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30\r\nX-Frame-
SF:Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(RTSPRequest,
SF:AC,"HTTP/1\.1\x20501\x20Not\x20Implemented\r\nContent-Type:\x20text/pla
SF:in\r\nDate:\x20Fri,\x2012\x20May\x202017\x2005:04:03\x20GMT\r\nServer:\
SF:x20HPE-iLO-Server/1\.30\r\nX-Frame-Options:\x20sameorigin\r\nContent-Le
SF:ngth:\x200\r\n\r\n")%r(Help,A8,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nC
SF:ontent-Type:\x20text/plain\r\nDate:\x20Fri,\x2012\x20May\x202017\x2005:
SF:04:23\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30\r\nX-Frame-Options:\x20
SF:sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(SSLSessionReq,A8,"HTTP/1
SF:\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain\r\nDate:\x2
SF:0Fri,\x2012\x20May\x202017\x2005:04:31\x20GMT\r\nServer:\x20HPE-iLO-Ser
SF:ver/1\.30\r\nX-Frame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n
SF:\r\n")%r(FourOhFourRequest,9E,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nCo
SF:ntent-Type:\x20text/plain\r\nConnection:\x20close\r\nDate:\x20Fri,\x201
SF:2\x20May\x202017\x2005:04:46\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30\
SF:r\nContent-Length:\x200\r\n\r\n")%r(LPDString,A8,"HTTP/1\.1\x20400\x20B
SF:ad\x20Request\r\nContent-Type:\x20text/plain\r\nDate:\x20Fri,\x2012\x20
SF:May\x202017\x2005:04:46\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30\r\nX-
SF:Frame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(SIPOpt
SF:ions,6B8,"HTTP/1\.1\x20501\x20Not\x20Implemented\r\nContent-Type:\x20te
SF:xt/plain\r\nDate:\x20Fri,\x2012\x20May\x202017\x2005:04:56\x20GMT\r\nSe
```

```
SF:rver:\x20HPE-iLO-Server/1\.30\r\nX-Frame-Options:\x20sameorigin\r\nCont
SF:ent-Length:\x200\r\n\r\nHTTP/1\.1\x20501\x20Not\x20Implemented\r\nConte
SF:nt-Type:\x20text/plain\r\nDate:\x20Fri,\x2012\x20May\x202017\x2005:04:5
SF:6\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30\r\nX-Frame-Options:\x20same
SF:origin\r\nContent-Length:\x200\r\n\r\nHTTP/1\.1\x20501\x20Not\x20Implem
SF:ented\r\nContent-Type:\x20text/plain\r\nDate:\x20Fri,\x2012\x20May\x202
SF:017\x2005:04:57\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30\r\nX-Frame-Op
SF:tions:\x20sameorigin\r\nContent-Length:\x200\r\n\r\nHTTP/1\.1\x20501\x2
SF:0Not\x20Implemented\r\nContent-Type:\x20text/plain\r\nDate:\x20Fri,\x20
SF:12\x20May\x202017\x2005:04:57\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30
SF:\r\nX-Frame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\nHTTP/
SF:1\.1\x20501\x20Not\x20Implemented\r\nContent-Type:\x20text/plain\r\nDat
SF:e:\x20Fri,\x2012\x20May\x202017\x2005:04:57\x20GMT\r\nServer:\x20HPE-iL
SF:O-Server/1\.30\r\nX-Frame-Options:\x20sameorigin\r\nContent-Length:\x20
SF:0\r\n\r\nHTTP/1\.1\x20501\x20Not\x20Implemented\r\nContent-Ty");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port17988-TCP:V=5.21%I=7%D=5/12%Time=59159693%P=x86_64-unknown-linux-
gnu%r(SSLSessionReq,4,"\"\0\x03\0");
Device type: general purpose|media device|printer|WAP|firewall|phone|router
Running (JUST GUESSING) : FreeBSD 6.X (91%), Apple iPhone OS 2.X (89%), HP embedded (88%), Apple
embedded (87%), m0n0wall FreeBSD (87%), Nokia Symbian OS (87%), Juniper JUNOS 9.X (86%)
Aggressive OS guesses: FreeBSD 6.2-RELEASE (91%), Apple iPod touch audio player (iPhone OS 2.1) (89%),
HP LaserJet M1522nf printer (88%), Apple AirPort Extreme WAP v7.3.2 (87%), m0n0wall 1.3b11 - 1.3b15
FreeBSD-based firewall (87%), Nokia N81 mobile phone (Symbian OS) (87%), Juniper Networks JUNOS
9.0R2.10 (86%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.723 days (since Thu May 11 12:44:48 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=265 (Good luck!)
IP ID Sequence Generation: Incremental

TRACEROUTE (using port 8080/tcp)
HOP RTT     ADDRESS
1   3.56 ms 10.50.1.8

Read data files from: /usr/share/nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 121.21 seconds
           Raw packets sent: 1174 (53.564KB) | Rcvd: 1032 (42.116KB)
20170512.06051494587139


-------------------------------------------
-------------------------------------------
.........................................
20170512.06051494587139

NCat check ports Version ProcServer ::
nc 10.50.1.8 22
SSH-2.0-mpSSH_0.2.1

111111$111111
111111Protocol error11111111111111111111111nc 10.50.1.8 80
nc 10.50.1.8 443
nc 10.50.1.8 17988
Nikto Report for 10.50.1.8 ....
20170512.06051494587142

+++++++++++++++++++++++++++++++++++++++++++
20170512.06051494587142

nikto -C all -h 10.50.1.8 -p 22
- Nikto v2.1.4
---------------------------------------------------------------------------
+ No web server found on 10.50.1.8:22
---------------------------------------------------------------------------
+ 0 host(s) tested
nikto -C all -h 10.50.1.8 -p 80
- Nikto v2.1.4
---------------------------------------------------------------------------
^C
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
```

```
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report# cat
IP.block.10.50.1.xServers.ReportAvailPing..SIBLOCKS | xargs -
-i -t scann.mc1 {}
scann.mc1 10.50.1.8
Starting Scann Report ....
Start Time : 20170512.06061494587195 ..
--------------------------------------------

20170512.06061494587195
Ping Reachable Host 10.50.1.8 ::
PING 10.50.1.8 (10.50.1.8) 56(84) bytes of data.
64 bytes from 10.50.1.8: icmp_req=1 ttl=255 time=3.43 ms
64 bytes from 10.50.1.8: icmp_req=2 ttl=255 time=3.18 ms

--- 10.50.1.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 3.185/3.309/3.433/0.124 ms

20170512.06061494587197

--------------------------------------------
--------------------------------------------
--------------------------------------------
starting NMAP Scann Report ....
20170512.06061494587197

Starting Nmap 5.21 ( http://nmap.org ) at 2017-05-12 06:06 CDT
Nmap scan report for 10.50.1.8
Host is up (0.0034s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
17988/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 2.69 seconds

20170512.06061494587199
```

```
---------------------------------------------
---------------------------------------------
---------------------------------------------
 Starting Nmap ScannForce Report
20170512.06061494587199

Starting Nmap 5.21 ( http://nmap.org ) at 2017-05-12 06:06 CDT
NSE: Loaded 36 scripts for scanning.
Initiating SYN Stealth Scan at 06:06
Scanning 10.50.1.8 [1000 ports]
Discovered open port 80/tcp on 10.50.1.8
Discovered open port 22/tcp on 10.50.1.8
Discovered open port 443/tcp on 10.50.1.8
Discovered open port 17988/tcp on 10.50.1.8
Completed SYN Stealth Scan at 06:06, 2.60s elapsed (1000 total ports)
Initiating Service scan at 06:06
Scanning 4 services on 10.50.1.8
Service scan Timing: About 75.00% done; ETC: 06:09 (0:00:36 remaining)
Completed Service scan at 06:08, 112.80s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against 10.50.1.8
Retrying OS detection (try #2) against 10.50.1.8
Initiating Traceroute at 06:08
Completed Traceroute at 06:08, 0.01s elapsed
NSE: Script scanning 10.50.1.8.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 06:08
Completed NSE at 06:08, 1.74s elapsed
NSE: Script Scanning completed.
Nmap scan report for 10.50.1.8
Host is up (0.0034s 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?
443/tcp   open  ssl/https?
17988/tcp open  unknown
3 services unrecognized despite returning data. If you know the service/version, please submit the
following fingerprints at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=5.21%I=7%D=5/12%Time=59159749%P=x86_64-unknown-linux-gnu%r
SF:(GetRequest,9E,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20
SF:text/plain\r\nConnection:\x20close\r\nDate:\x20Fri,\x2012\x20May\x20201
SF:7\x2005:06:49\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30\r\nContent-Leng
SF:th:\x200\r\n\r\n")%r(HTTPOptions,AC,"HTTP/1\.1\x20501\x20Not\x20Impleme
SF:nted\r\nContent-Type:\x20text/plain\r\nDate:\x20Fri,\x2012\x20May\x2020
SF:17\x2005:06:49\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30\r\nX-Frame-Opt
SF:ions:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(RTSPRequest,AC,
SF:"HTTP/1\.1\x20501\x20Not\x20Implemented\r\nContent-Type:\x20text/plain\
SF:r\nDate:\x20Fri,\x2012\x20May\x202017\x2005:06:54\x20GMT\r\nServer:\x20
SF:HPE-iLO-Server/1\.30\r\nX-Frame-Options:\x20sameorigin\r\nContent-Lengt
SF:h:\x200\r\n\r\n")%r(FourOhFourRequest,9E,"HTTP/1\.1\x20400\x20Bad\x20Re
SF:quest\r\nContent-Type:\x20text/plain\r\nConnection:\x20close\r\nDate:\x
SF:20Fri,\x2012\x20May\x202017\x2005:07:04\x20GMT\r\nServer:\x20HPE-iLO-Se
SF:rver/1\.30\r\nContent-Length:\x200\r\n\r\n")%r(Help,A8,"HTTP/1\.1\x2040
SF:0\x20Bad\x20Request\r\nContent-Type:\x20text/plain\r\nDate:\x20Fri,\x20
SF:12\x20May\x202017\x2005:07:24\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30
SF:\r\nX-Frame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(
SF:SSLSessionReq,A8,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x
SF:20text/plain\r\nDate:\x20Fri,\x2012\x20May\x202017\x2005:07:31\x20GMT\r
SF:\nServer:\x20HPE-iLO-Server/1\.30\r\nX-Frame-Options:\x20sameorigin\r\n
SF:Content-Length:\x200\r\n\r\n")%r(LPDString,A8,"HTTP/1\.1\x20400\x20Bad\
SF:x20Request\r\nContent-Type:\x20text/plain\r\nDate:\x20Fri,\x2012\x20May
SF:\x202017\x2005:07:41\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30\r\nX-Fra
SF:me-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(SIPOption
SF:s,6B8,"HTTP/1\.1\x20501\x20Not\x20Implemented\r\nContent-Type:\x20text/
SF:plain\r\nDate:\x20Fri,\x2012\x20May\x202017\x2005:07:51\x20GMT\r\nServe
SF:r:\x20HPE-iLO-Server/1\.30\r\nX-Frame-Options:\x20sameorigin\r\nContent
SF:-Length:\x200\r\n\r\nHTTP/1\.1\x20501\x20Not\x20Implemented\r\nContent-
SF:Type:\x20text/plain\r\nDate:\x20Fri,\x2012\x20May\x202017\x2005:07:51\x
SF:20GMT\r\nServer:\x20HPE-iLO-Server/1\.30\r\nX-Frame-Options:\x20sameori
SF:gin\r\nContent-Length:\x200\r\n\r\nHTTP/1\.1\x20501\x20Not\x20Implement
SF:ed\r\nContent-Type:\x20text/plain\r\nDate:\x20Fri,\x2012\x20May\x202017
SF:\x2005:07:51\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30\r\nX-Frame-Optio
```

```
SF:ns:\x20sameorigin\r\nContent-Length:\x200\r\n\r\nHTTP/1\.1\x20501\x20No
SF:t\x20Implemented\r\nContent-Type:\x20text/plain\r\nDate:\x20Fri,\x2012\
SF:x20May\x202017\x2005:07:51\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30\r\
SF:nX-Frame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\nHTTP/1\.
SF:1\x20501\x20Not\x20Implemented\r\nContent-Type:\x20text/plain\r\nDate:\
SF:x20Fri,\x2012\x20May\x202017\x2005:07:51\x20GMT\r\nServer:\x20HPE-iLO-S
SF:erver/1\.30\r\nX-Frame-Options:\x20sameorigin\r\nContent-Length:\x200\r
SF:\n\r\nHTTP/1\.1\x20501\x20Not\x20Implemented\r\nContent-Ty");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port443-TCP:V=5.21%T=SSL%I=7%D=5/12%Time=5915974F%P=x86_64-unknown-linux-
gnu%r(GetRequest,9E,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\
SF:x20text/plain\r\nConnection:\x20close\r\nDate:\x20Fri,\x2012\x20May\x20
SF:2017\x2005:06:55\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30\r\nContent-L
SF:ength:\x200\r\n\r\n")%r(HTTPOptions,AC,"HTTP/1\.1\x20501\x20Not\x20Impl
SF:emented\r\nContent-Type:\x20text/plain\r\nDate:\x20Fri,\x2012\x20May\x2
SF:02017\x2005:07:00\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30\r\nX-Frame-
SF:Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(RTSPRequest,
SF:AC,"HTTP/1\.1\x20501\x20Not\x20Implemented\r\nContent-Type:\x20text/pla
SF:in\r\nDate:\x20Fri,\x2012\x20May\x202017\x2005:07:05\x20GMT\r\nServer:\
SF:x20HPE-iLO-Server/1\.30\r\nX-Frame-Options:\x20sameorigin\r\nContent-Le
SF:ngth:\x200\r\n\r\n")%r(Help,A8,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nC
SF:ontent-Type:\x20text/plain\r\nDate:\x20Fri,\x2012\x20May\x202017\x2005:
SF:07:25\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30\r\nX-Frame-Options:\x20
SF:sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(SSLSessionReq,A8,"HTTP/1
SF:\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain\r\nDate:\x2
SF:0Fri,\x2012\x20May\x202017\x2005:07:33\x20GMT\r\nServer:\x20HPE-iLO-Ser
SF:ver/1\.30\r\nX-Frame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n
SF:\r\n")%r(FourOhFourRequest,9E,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nCo
SF:ntent-Type:\x20text/plain\r\nConnection:\x20close\r\nDate:\x20Fri,\x201
SF:2\x20May\x202017\x2005:07:48\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30\
SF:r\nContent-Length:\x200\r\n\r\n")%r(LPDString,A8,"HTTP/1\.1\x20400\x20B
SF:ad\x20Request\r\nContent-Type:\x20text/plain\r\nDate:\x20Fri,\x2012\x20
SF:May\x202017\x2005:07:48\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30\r\nX-
SF:Frame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(SIPOpt
SF:ions,6B8,"HTTP/1\.1\x20501\x20Not\x20Implemented\r\nContent-Type:\x20te
SF:xt/plain\r\nDate:\x20Fri,\x2012\x20May\x202017\x2005:07:58\x20GMT\r\nSe
SF:rver:\x20HPE-iLO-Server/1\.30\r\nX-Frame-Options:\x20sameorigin\r\nCont
SF:ent-Length:\x200\r\n\r\nHTTP/1\.1\x20501\x20Not\x20Implemented\r\nConte
SF:nt-Type:\x20text/plain\r\nDate:\x20Fri,\x2012\x20May\x202017\x2005:07:5
SF:8\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30\r\nX-Frame-Options:\x20same
SF:origin\r\nContent-Length:\x200\r\n\r\nHTTP/1\.1\x20501\x20Not\x20Implem
SF:ented\r\nContent-Type:\x20text/plain\r\nDate:\x20Fri,\x2012\x20May\x202
SF:017\x2005:07:58\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30\r\nX-Frame-Op
SF:tions:\x20sameorigin\r\nContent-Length:\x200\r\n\r\nHTTP/1\.1\x20501\x2
SF:0Not\x20Implemented\r\nContent-Type:\x20text/plain\r\nDate:\x20Fri,\x20
SF:12\x20May\x202017\x2005:07:59\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30
SF:\r\nX-Frame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\nHTTP/
SF:1\.1\x20501\x20Not\x20Implemented\r\nContent-Type:\x20text/plain\r\nDat
SF:e:\x20Fri,\x2012\x20May\x202017\x2005:07:59\x20GMT\r\nServer:\x20HPE-iL
SF:O-Server/1\.30\r\nX-Frame-Options:\x20sameorigin\r\nContent-Length:\x20
SF:0\r\n\r\nHTTP/1\.1\x20501\x20Not\x20Implemented\r\nContent-Ty");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port17988-TCP:V=5.21%I=7%D=5/12%Time=59159749%P=x86_64-unknown-linux-
gnu%r(SSLSessionReq,4,"\"\0\x03\0");
Device type: general purpose|media device|printer|WAP|firewall|phone|router
Running (JUST GUESSING) : FreeBSD 6.X (91%), Apple iPhone OS 2.X (89%), HP embedded (88%), Apple
embedded (87%), m0n0wall FreeBSD (87%), Nokia Symbian OS (87%), Juniper JUNOS 9.X (86%)
Aggressive OS guesses: FreeBSD 6.2-RELEASE (91%), Apple iPod touch audio player (iPhone OS 2.1) (89%),
HP LaserJet M1522nf printer (88%), Apple AirPort Extreme WAP v7.3.2 (87%), m0n0wall 1.3b11 - 1.3b15
FreeBSD-based firewall (87%), Nokia N81 mobile phone (Symbian OS) (87%), Juniper Networks JUNOS
9.0R2.10 (86%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.725 days (since Thu May 11 12:44:49 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: Incremental

TRACEROUTE (using port 993/tcp)
HOP RTT     ADDRESS
1   3.76 ms 10.50.1.8

Read data files from: /usr/share/nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 121.20 seconds
           Raw packets sent: 1175 (53.608KB) | Rcvd: 1032 (42.116KB)
```

```
20170512.06081494587321

-------------------------------------------
-------------------------------------------
.........................................
20170512.06081494587321

NCat check ports Version ProcServer ::
nc 10.50.1.8 22
SSH-2.0-mpSSH_0.2.1

151515$151515
151515Protocol error151515151515151515151515nc 10.50.1.8 80
nc 10.50.1.8 443
nc 10.50.1.8 17988
Nikto Report for 10.50.1.8 ....
20170512.06081494587323

++++++++++++++++++++++++++++++++++++++++++++
20170512.06081494587323

nikto -C all -h 10.50.1.8 -p 22
- Nikto v2.1.4
---------------------------------------------------------------------------
+ No web server found on 10.50.1.8:22
---------------------------------------------------------------------------
+ 0 host(s) tested
nikto -C all -h 10.50.1.8 -p 80
- Nikto v2.1.4
---------------------------------------------------------------------------
+ Target IP:          10.50.1.8
+ Target Hostname:    10.50.1.8
+ Target Port:        80
+ Start Time:         2017-05-13 06:09:29
---------------------------------------------------------------------------
+ Server: HPE-iLO-Server/1.30
+ Root page / redirects to: https://10.50.1.8/
+ 6456 items checked: 21359 error(s) and 0 item(s) reported on remote host
+ End Time:           2017-05-13 06:12:07 (158 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
nikto -C all -h 10.50.1.8 -p 17988
- Nikto v2.1.4
---------------------------------------------------------------------------
+ No web server found on 10.50.1.8:17988
---------------------------------------------------------------------------
+ 0 host(s) tested
EOF Nikto Report for 10.50.1.8 ...
20170512.06121494587549

-------------------------------------------
-------------------------------------------
End Completed for 10.50.1.8  Scann Report ....
END Time : 20170512.06121494587549 ..
EoFScann 10.50.1.8
```

Anexo 2 – Evidencia Vulnerabilidades 10.50.1.9

```
scann.mc1 10.50.1.9
Starting Scann Report ....
Start Time : 20170512.06121494587549 ..
-------------------------------------------

20170512.06121494587549
Ping Reachable Host 10.50.1.9 ::
PING 10.50.1.9 (10.50.1.9) 56(84) bytes of data.
64 bytes from 10.50.1.9: icmp_req=1 ttl=255 time=3.54 ms
64 bytes from 10.50.1.9: icmp_req=2 ttl=255 time=3.21 ms

--- 10.50.1.9 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 3.212/3.380/3.548/0.168 ms

20170512.06121494587551

-------------------------------------------
-------------------------------------------
-------------------------------------------
starting NMAP Scann Report ....
20170512.06121494587551

Starting Nmap 5.21 ( http://nmap.org ) at 2017-05-12 06:12 CDT
Nmap scan report for 10.50.1.9
Host is up (0.0035s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
17988/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 2.71 seconds

20170512.06121494587554

-------------------------------------------
-------------------------------------------
-------------------------------------------
 Starting Nmap ScannForce Report
20170512.06121494587554

Starting Nmap 5.21 ( http://nmap.org ) at 2017-05-12 06:12 CDT
NSE: Loaded 36 scripts for scanning.
Initiating SYN Stealth Scan at 06:12
Scanning 10.50.1.9 [1000 ports]
Discovered open port 443/tcp on 10.50.1.9
Discovered open port 22/tcp on 10.50.1.9
Discovered open port 80/tcp on 10.50.1.9
Discovered open port 17988/tcp on 10.50.1.9
Completed SYN Stealth Scan at 06:12, 2.54s elapsed (1000 total ports)
Initiating Service scan at 06:12
Scanning 4 services on 10.50.1.9
Service scan Timing: About 75.00% done; ETC: 06:14 (0:00:35 remaining)
Completed Service scan at 06:14, 112.79s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against 10.50.1.9
Retrying OS detection (try #2) against 10.50.1.9
Initiating Traceroute at 06:14
Completed Traceroute at 06:14, 0.01s elapsed
NSE: Script scanning 10.50.1.9.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 06:14
Completed NSE at 06:14, 2.09s elapsed
NSE: Script Scanning completed.
Nmap scan report for 10.50.1.9
Host is up (0.0034s 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?
```

```
443/tcp   open  ssl/https?
17988/tcp open  unknown
3 services unrecognized despite returning data. If you know the service/version, please submit the
following fingerprints at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=5.21%I=7%D=5/12%Time=591598AB%P=x86_64-unknown-linux-gnu%r
SF:(GetRequest,9E,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20
SF:text/plain\r\nConnection:\x20close\r\nDate:\x20Fri,\x2012\x20May\x20201
SF:7\x2011:12:44\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30\r\nContent-Leng
SF:th:\x200\r\n\r\n")%r(HTTPOptions,AC,"HTTP/1\.1\x20501\x20Not\x20Impleme
SF:nted\r\nContent-Type:\x20text/plain\r\nDate:\x20Fri,\x2012\x20May\x2020
SF:17\x2011:12:44\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30\r\nX-Frame-Opt
SF:ions:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(RTSPRequest,AC,
SF:"HTTP/1\.1\x20501\x20Not\x20Implemented\r\nContent-Type:\x20text/plain\
SF:r\nDate:\x20Fri,\x2012\x20May\x202017\x2011:12:49\x20GMT\r\nServer:\x20
SF:HPE-iLO-Server/1\.30\r\nX-Frame-Options:\x20sameorigin\r\nContent-Lengt
SF:h:\x200\r\n\r\n")%r(FourOhFourRequest,9E,"HTTP/1\.1\x20400\x20Bad\x20Re
SF:quest\r\nContent-Type:\x20text/plain\r\nConnection:\x20close\r\nDate:\x
SF:20Fri,\x2012\x20May\x202017\x2011:12:59\x20GMT\r\nServer:\x20HPE-iLO-Se
SF:rver/1\.30\r\nContent-Length:\x200\r\n\r\n")%r(Help,A8,"HTTP/1\.1\x2040
SF:0\x20Bad\x20Request\r\nContent-Type:\x20text/plain\r\nDate:\x20Fri,\x20
SF:12\x20May\x202017\x2011:13:19\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30
SF:\r\nX-Frame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(
SF:SSLSessionReq,A8,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x
SF:20text/plain\r\nDate:\x20Fri,\x2012\x20May\x202017\x2011:13:26\x20GMT\r
SF:\nServer:\x20HPE-iLO-Server/1\.30\r\nX-Frame-Options:\x20sameorigin\r\n
SF:Content-Length:\x200\r\n\r\n")%r(LPDString,A8,"HTTP/1\.1\x20400\x20Bad\
SF:x20Request\r\nContent-Type:\x20text/plain\r\nDate:\x20Fri,\x2012\x20May
SF:\x202017\x2011:13:36\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30\r\nX-Fra
SF:me-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(SIPOption
SF:s,6B8,"HTTP/1\.1\x20501\x20Not\x20Implemented\r\nContent-Type:\x20text/
SF:plain\r\nDate:\x20Fri,\x2012\x20May\x202017\x2011:13:46\x20GMT\r\nServe
SF:r:\x20HPE-iLO-Server/1\.30\r\nX-Frame-Options:\x20sameorigin\r\nContent
SF:-Length:\x200\r\n\r\nHTTP/1\.1\x20501\x20Not\x20Implemented\r\nContent-
SF:Type:\x20text/plain\r\nDate:\x20Fri,\x2012\x20May\x202017\x2011:13:46\x
SF:20GMT\r\nServer:\x20HPE-iLO-Server/1\.30\r\nX-Frame-Options:\x20sameori
SF:gin\r\nContent-Length:\x200\r\n\r\nHTTP/1\.1\x20501\x20Not\x20Implement
SF:ed\r\nContent-Type:\x20text/plain\r\nDate:\x20Fri,\x2012\x20May\x202017
SF:\x2011:13:46\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30\r\nX-Frame-Optio
SF:ns:\x20sameorigin\r\nContent-Length:\x200\r\n\r\nHTTP/1\.1\x20501\x20No
SF:t\x20Implemented\r\nContent-Type:\x20text/plain\r\nDate:\x20Fri,\x2012\
SF:x20May\x202017\x2011:13:46\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30\r\
SF:nX-Frame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\nHTTP/1\.
SF:1\x20501\x20Not\x20Implemented\r\nContent-Type:\x20text/plain\r\nDate:\
SF:x20Fri,\x2012\x20May\x202017\x2011:13:46\x20GMT\r\nServer:\x20HPE-iLO-S
SF:erver/1\.30\r\nX-Frame-Options:\x20sameorigin\r\nContent-Length:\x200\r
SF:\n\r\nHTTP/1\.1\x20501\x20Not\x20Implemented\r\nContent-Ty");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port443-TCP:V=5.21%T=SSL%I=7%D=5/12%Time=591598B1%P=x86_64-unknown-linux-
gnu%r(GetRequest,9E,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\
SF:x20text/plain\r\nConnection:\x20close\r\nDate:\x20Fri,\x2012\x20May\x20
SF:2017\x2011:12:50\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30\r\nContent-L
SF:ength:\x200\r\n\r\n")%r(HTTPOptions,AC,"HTTP/1\.1\x20501\x20Not\x20Impl
SF:emented\r\nContent-Type:\x20text/plain\r\nDate:\x20Fri,\x2012\x20May\x2
SF:02017\x2011:12:55\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30\r\nX-Frame-
SF:Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(RTSPRequest,
SF:AC,"HTTP/1\.1\x20501\x20Not\x20Implemented\r\nContent-Type:\x20text/pla
SF:in\r\nDate:\x20Fri,\x2012\x20May\x202017\x2011:13:00\x20GMT\r\nServer:\
SF:x20HPE-iLO-Server/1\.30\r\nX-Frame-Options:\x20sameorigin\r\nContent-Le
SF:ngth:\x200\r\n\r\n")%r(Help,A8,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nC
SF:ontent-Type:\x20text/plain\r\nDate:\x20Fri,\x2012\x20May\x202017\x2011:
SF:13:20\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30\r\nX-Frame-Options:\x20
SF:sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(SSLSessionReq,A8,"HTTP/1
SF:\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain\r\nDate:\x2
SF:0Fri,\x2012\x20May\x202017\x2011:13:28\x20GMT\r\nServer:\x20HPE-iLO-Ser
SF:ver/1\.30\r\nX-Frame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n
SF:\r\n")%r(FourOhFourRequest,9E,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nCo
SF:ntent-Type:\x20text/plain\r\nConnection:\x20close\r\nDate:\x20Fri,\x201
SF:2\x20May\x202017\x2011:13:43\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30\
SF:r\nContent-Length:\x200\r\n\r\n")%r(LPDString,A8,"HTTP/1\.1\x20400\x20B
SF:ad\x20Request\r\nContent-Type:\x20text/plain\r\nDate:\x20Fri,\x2012\x20
SF:May\x202017\x2011:13:43\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30\r\nX-
SF:Frame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\n")%r(SIPOpt
SF:ions,6B8,"HTTP/1\.1\x20501\x20Not\x20Implemented\r\nContent-Type:\x20te
SF:xt/plain\r\nDate:\x20Fri,\x2012\x20May\x202017\x2011:13:53\x20GMT\r\nSe
```

```
SF:rver:\x20HPE-iLO-Server/1\.30\r\nX-Frame-Options:\x20sameorigin\r\nCont
SF:ent-Length:\x200\r\n\r\nHTTP/1\.1\x20501\x20Not\x20Implemented\r\nConte
SF:nt-Type:\x20text/plain\r\nDate:\x20Fri,\x2012\x20May\x202017\x2011:13:5
SF:3\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30\r\nX-Frame-Options:\x20same
SF:origin\r\nContent-Length:\x200\r\n\r\nHTTP/1\.1\x20501\x20Not\x20Implem
SF:ented\r\nContent-Type:\x20text/plain\r\nDate:\x20Fri,\x2012\x20May\x202
SF:017\x2011:13:53\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30\r\nX-Frame-Op
SF:tions:\x20sameorigin\r\nContent-Length:\x200\r\n\r\nHTTP/1\.1\x20501\x2
SF:0Not\x20Implemented\r\nContent-Type:\x20text/plain\r\nDate:\x20Fri,\x20
SF:12\x20May\x202017\x2011:13:53\x20GMT\r\nServer:\x20HPE-iLO-Server/1\.30
SF:\r\nX-Frame-Options:\x20sameorigin\r\nContent-Length:\x200\r\n\r\nHTTP/
SF:1\.1\x20501\x20Not\x20Implemented\r\nContent-Type:\x20text/plain\r\nDat
SF:e:\x20Fri,\x2012\x20May\x202017\x2011:13:54\x20GMT\r\nServer:\x20HPE-iL
SF:O-Server/1\.30\r\nX-Frame-Options:\x20sameorigin\r\nContent-Length:\x20
SF:0\r\n\r\nHTTP/1\.1\x20501\x20Not\x20Implemented\r\nContent-Ty");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port17988-TCP:V=5.21%I=7%D=5/12%Time=591598AB%P=x86_64-unknown-linux-
gnu%r(SSLSessionReq,4,"\"\0\x03\0");
Device type: general purpose|media device|printer|WAP|firewall|phone|router
Running (JUST GUESSING) : FreeBSD 6.X (91%), Apple iPhone OS 2.X (89%), HP embedded (88%), Apple
embedded (87%), m0n0wall FreeBSD (87%), Nokia Symbian OS (87%), Juniper JUNOS 9.X (86%)
Aggressive OS guesses: FreeBSD 6.2-RELEASE (91%), Apple iPod touch audio player (iPhone OS 2.1) (89%),
HP LaserJet M1522nf printer (88%), Apple AirPort Extreme WAP v7.3.2 (87%), m0n0wall 1.3b11 - 1.3b15
FreeBSD-based firewall (87%), Nokia N81 mobile phone (Symbian OS) (87%), Juniper Networks JUNOS
9.0R2.10 (86%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.756 days (since Thu May 11 12:06:16 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: Incremental

TRACEROUTE (using port 3389/tcp)
HOP RTT     ADDRESS
1   3.77 ms 10.50.1.9

Read data files from: /usr/share/nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 121.47 seconds
           Raw packets sent: 1175 (53.608KB) | Rcvd: 1034 (42.257KB)
20170512.06141494587675

-------------------------------------------
-------------------------------------------
.........................................
20170512.06141494587675

NCat check ports Version ProcServer ::
nc 10.50.1.9 22
SSH-2.0-mpSSH_0.2.1

181818$181818
181818Protocol error181818181818181818181818nc 10.50.1.9 80
nc 10.50.1.9 443
nc 10.50.1.9 17988
Nikto Report for 10.50.1.9 ....
20170512.06141494587678

+++++++++++++++++++++++++++++++++++++++++++
20170512.06141494587678

nikto -C all -h 10.50.1.9 -p 22
- Nikto v2.1.4
---------------------------------------------------------------------------
+ No web server found on 10.50.1.9:22
---------------------------------------------------------------------------
+ 0 host(s) tested
nikto -C all -h 10.50.1.9 -p 80
- Nikto v2.1.4
---------------------------------------------------------------------------
+ Target IP:          10.50.1.9
+ Target Hostname:    10.50.1.9
+ Target Port:        80
+ Start Time:         2017-05-13 06:15:24
---------------------------------------------------------------------------
+ Server: HPE-iLO-Server/1.30
```

```
+ Root page / redirects to: https://10.50.1.9/
+ 6456 items checked: 21355 error(s) and 0 item(s) reported on remote host
+ End Time:           2017-05-13 06:18:01 (157 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
nikto -C all -h 10.50.1.9 -p 17988
- Nikto v2.1.4
---------------------------------------------------------------------------
+ No web server found on 10.50.1.9:17988
---------------------------------------------------------------------------
+ 0 host(s) tested
EOF Nikto Report for 10.50.1.9 ...
20170512.06181494587903

-------------------------------------------
-------------------------------------------
End Completed for 10.50.1.9  Scann Report ....
END Time : 20170512.06181494587903 ..
EoFScann 10.50.1.9
```

Anexo 3 – Evidencia Vulnerabilidades 10.50.1.10

```
scann.mc1 10.50.1.10
Starting Scann Report ....
Start Time : 20170512.06181494587903 ..
-------------------------------------------

20170512.06181494587903
Ping Reachable Host 10.50.1.10 ::
PING 10.50.1.10 (10.50.1.10) 56(84) bytes of data.
64 bytes from 10.50.1.10: icmp_req=1 ttl=64 time=3.26 ms
64 bytes from 10.50.1.10: icmp_req=2 ttl=64 time=2.97 ms

--- 10.50.1.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 2.975/3.119/3.264/0.154 ms

20170512.06181494587905
-------------------------------------------
-------------------------------------------
-------------------------------------------
starting NMAP Scann Report ....
20170512.06181494587905

Starting Nmap 5.21 ( http://nmap.org ) at 2017-05-12 06:18 CDT
Nmap scan report for 10.50.1.10
Host is up (0.0062s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
873/tcp open  rsync

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds

20170512.06181494587905
-------------------------------------------
-------------------------------------------
-------------------------------------------
 Starting Nmap ScannForce Report
20170512.06181494587905

Starting Nmap 5.21 ( http://nmap.org ) at 2017-05-12 06:18 CDT
NSE: Loaded 36 scripts for scanning.
Initiating SYN Stealth Scan at 06:18
Scanning 10.50.1.10 [1000 ports]
Discovered open port 22/tcp on 10.50.1.10
Discovered open port 873/tcp on 10.50.1.10
Completed SYN Stealth Scan at 06:18, 0.13s elapsed (1000 total ports)
Initiating Service scan at 06:18
Scanning 2 services on 10.50.1.10
Completed Service scan at 06:18, 6.01s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 10.50.1.10
Retrying OS detection (try #2) against 10.50.1.10
Initiating Traceroute at 06:18
Completed Traceroute at 06:18, 0.01s elapsed
NSE: Script scanning 10.50.1.10.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 06:18
Completed NSE at 06:18, 0.05s elapsed
NSE: Script Scanning completed.
Nmap scan report for 10.50.1.10
Host is up (0.0034s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     (protocol 2.0)
873/tcp open  rsync   (protocol version 31)
1 service unrecognized despite returning data. If you know the service/version, please submit the
following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port22-TCP:V=5.21%I=7%D=5/12%Time=59159A08%P=x86_64-unknown-linux-gnu%r
SF:(NULL,29,"SSH-2\.0-OpenSSH_7\.2p2\x20Ubuntu-4ubuntu2\.1\r\n");
Device type: general purpose|WAP|broadband router
Running (JUST GUESSING) : Linux 2.6.X|2.4.X (89%)
Aggressive OS guesses: Linux 2.6.18 (CentOS 5.1, x86) (89%), Linux 2.6.18 (85%), DD-WRT v23 (Linux
2.4.34) (85%), OpenWrt Kamikaze 8.09 (Linux 2.6.25.20) (85%), Linux 2.6.15 (Ubuntu) (85%), Linux
2.6.15 - 2.6.26 (85%), Linux 2.6.23 (85%), Linux 2.6.27.21-grsec (85%)
```

```
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.717 days (since Thu May 11 13:06:00 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=252 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 443/tcp)
HOP RTT     ADDRESS
1   3.78 ms 10.50.1.10

Read data files from: /usr/share/nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.23 seconds
           Raw packets sent: 1072 (49.076KB) | Rcvd: 1033 (42.720KB)
20170512.06181494587915
-------------------------------------------
-------------------------------------------
.........................................
20170512.06181494587915

NCat check ports Version ProcServer ::
nc 10.50.1.10 22
SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.1

nc 10.50.1.10 873
@RSYNCD: 31.0
Nikto Report for 10.50.1.10 ....
20170512.06181494587915

+++++++++++++++++++++++++++++++++++++++++++
20170512.06181494587915

nikto -C all -h 10.50.1.10 -p 22
- Nikto v2.1.4
---------------------------------------------------------------------------
+ No web server found on 10.50.1.10:22
---------------------------------------------------------------------------
+ 0 host(s) tested
nikto -C all -h 10.50.1.10 -p 873
- Nikto v2.1.4
---------------------------------------------------------------------------
+ No web server found on 10.50.1.10:873
---------------------------------------------------------------------------
+ 0 host(s) tested
EOF Nikto Report for 10.50.1.10 ...
20170512.06191494587959
-------------------------------------------
-------------------------------------------
End Completed for 10.50.1.10  Scann Report ....
END Time : 20170512.06191494587959 ..
EoFScann 10.50.1.10
```

Anexo 4 – Evidencia Vulnerabilidades 10.50.1.11

```
scann.mc1 10.50.1.11
Starting Scann Report ....
Start Time : 20170512.06191494587959 ..
-------------------------------------------

20170512.06191494587959
Ping Reachable Host 10.50.1.11 ::
PING 10.50.1.11 (10.50.1.11) 56(84) bytes of data.
64 bytes from 10.50.1.11: icmp_req=1 ttl=64 time=3.32 ms
64 bytes from 10.50.1.11: icmp_req=2 ttl=64 time=3.03 ms

--- 10.50.1.11 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 3.035/3.178/3.322/0.154 ms

20170512.06191494587961

-------------------------------------------
-------------------------------------------
-------------------------------------------
starting NMAP Scann Report ....
20170512.06191494587961

Starting Nmap 5.21 ( http://nmap.org ) at 2017-05-12 06:19 CDT
Nmap scan report for 10.50.1.11
Host is up (0.0062s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds

20170512.06191494587961

-------------------------------------------
-------------------------------------------
-------------------------------------------
 Starting Nmap ScannForce Report
20170512.06191494587961

Starting Nmap 5.21 ( http://nmap.org ) at 2017-05-12 06:19 CDT
NSE: Loaded 36 scripts for scanning.
Initiating SYN Stealth Scan at 06:19
Scanning 10.50.1.11 [1000 ports]
Discovered open port 22/tcp on 10.50.1.11
Completed SYN Stealth Scan at 06:19, 0.12s elapsed (1000 total ports)
Initiating Service scan at 06:19
Scanning 1 service on 10.50.1.11
Completed Service scan at 06:19, 6.01s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 10.50.1.11
Retrying OS detection (try #2) against 10.50.1.11
Initiating Traceroute at 06:19
Completed Traceroute at 06:19, 0.01s elapsed
NSE: Script scanning 10.50.1.11.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 06:19
Completed NSE at 06:19, 0.06s elapsed
NSE: Script Scanning completed.
Nmap scan report for 10.50.1.11
Host is up (0.0034s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     (protocol 2.0)
1 service unrecognized despite returning data. If you know the service/version, please submit the
following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port22-TCP:V=5.21%I=7%D=5/12%Time=59159A40%P=x86_64-unknown-linux-gnu%r
SF:(NULL,29,"SSH-2\.0-OpenSSH_7\.2p2\x20Ubuntu-4ubuntu2\.1\r\n");
Device type: general purpose|WAP|broadband router
Running (JUST GUESSING) : Linux 2.6.X|2.4.X (89%)
Aggressive OS guesses: Linux 2.6.18 (CentOS 5.1, x86) (89%), Linux 2.6.18 (85%), DD-WRT v23 (Linux
2.4.34) (85%), OpenWrt Kamikaze 8.09 (Linux 2.6.25.20) (85%), Linux 2.6.15 (Ubuntu) (85%), Linux
2.6.15 - 2.6.26 (85%), Linux 2.6.23 (85%), Linux 2.6.27.21-grsec (85%)
No exact OS matches for host (test conditions non-ideal).
```

```
Uptime guess: 0.745 days (since Thu May 11 12:26:12 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 3389/tcp)
HOP RTT     ADDRESS
1   3.74 ms 10.50.1.11

Read data files from: /usr/share/nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.24 seconds
           Raw packets sent: 1072 (49.076KB) | Rcvd: 1034 (42.768KB)
20170512.06191494587972

-------------------------------------------
-------------------------------------------
.........................................
20170512.06191494587972

NCat check ports Version ProcServer ::
nc 10.50.1.11 22
SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.1

Nikto Report for 10.50.1.11 ....
20170512.06191494587972

+++++++++++++++++++++++++++++++++++++++++++
20170512.06191494587972


nikto -C all -h 10.50.1.11 -p 22
- Nikto v2.1.4
---------------------------------------------------------------------------
+ No web server found on 10.50.1.11:22
---------------------------------------------------------------------------
+ 0 host(s) tested
EOF Nikto Report for 10.50.1.11 ...
20170512.06191494587994

-------------------------------------------
-------------------------------------------
End Completed for 10.50.1.11  Scann Report ....
END Time : 20170512.06191494587994 ..
EoFScann 10.50.1.11
```

Anexo 5 – Evidencia Vulnerabilidades 10.50.1.100

```
scann.mc1 10.50.1.100
Starting Scann Report ....
Start Time : 20170512.06191494587994 ..
-------------------------------------------

20170512.06191494587994
Ping Reachable Host 10.50.1.100 ::
PING 10.50.1.100 (10.50.1.100) 56(84) bytes of data.
64 bytes from 10.50.1.100: icmp_req=1 ttl=64 time=3.36 ms
64 bytes from 10.50.1.100: icmp_req=2 ttl=64 time=3.03 ms

--- 10.50.1.100 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 3.035/3.198/3.361/0.163 ms

20170512.06191494587996

-------------------------------------------
-------------------------------------------
-------------------------------------------
starting NMAP Scann Report ....
20170512.06191494587996

Starting Nmap 5.21 ( http://nmap.org ) at 2017-05-12 06:19 CDT
Nmap scan report for 10.50.1.100
Host is up (0.0064s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
80/tcp   open  http
2222/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds

20170512.06191494587996

-------------------------------------------
-------------------------------------------
-------------------------------------------
 Starting Nmap ScannForce Report
20170512.06191494587996

Starting Nmap 5.21 ( http://nmap.org ) at 2017-05-12 06:19 CDT
NSE: Loaded 36 scripts for scanning.
Initiating SYN Stealth Scan at 06:19
Scanning 10.50.1.100 [1000 ports]
Discovered open port 80/tcp on 10.50.1.100
Discovered open port 2222/tcp on 10.50.1.100
Completed SYN Stealth Scan at 06:19, 0.13s elapsed (1000 total ports)
Initiating Service scan at 06:19
Scanning 2 services on 10.50.1.100
Completed Service scan at 06:20, 6.01s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 10.50.1.100
Retrying OS detection (try #2) against 10.50.1.100
Initiating Traceroute at 06:20
Completed Traceroute at 06:20, 0.01s elapsed
NSE: Script scanning 10.50.1.100.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 06:20
Completed NSE at 06:20, 0.05s elapsed
NSE: Script Scanning completed.
Nmap scan report for 10.50.1.100
Host is up (0.0033s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_html-title: Index of /
2222/tcp open  ssh     (protocol 2.0)
1 service unrecognized despite returning data. If you know the service/version, please submit the
following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port2222-TCP:V=5.21%I=7%D=5/12%Time=59159A62%P=x86_64-unknown-linux-gnu
SF:%r(NULL,29,"SSH-2\.0-OpenSSH_7\.2p2\x20Ubuntu-4ubuntu2\.1\r\n");
Device type: general purpose|WAP|broadband router
Running (JUST GUESSING) : Linux 2.6.X|2.4.X (89%)
```

```
Aggressive OS guesses: Linux 2.6.18 (CentOS 5.1, x86) (89%), Linux 2.6.18 (85%), DD-WRT v23 (Linux
2.4.34) (85%), OpenWrt Kamikaze 8.09 (Linux 2.6.25.20) (85%), Linux 2.6.15 (Ubuntu) (85%), Linux
2.6.15 - 2.6.26 (85%), Linux 2.6.23 (85%), Linux 2.6.27.21-grsec (85%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.718 days (since Thu May 11 13:06:00 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 113/tcp)
HOP RTT     ADDRESS
1   3.48 ms 10.50.1.100

Read data files from: /usr/share/nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.23 seconds
           Raw packets sent: 1072 (49.076KB) | Rcvd: 1033 (42.720KB)
20170512.06201494588006

-------------------------------------------
-------------------------------------------
.........................................
20170512.06201494588006

NCat check ports Version ProcServer ::
nc 10.50.1.100 80
nc 10.50.1.100 2222
SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.1

Nikto Report for 10.50.1.100 ....
20170512.06201494588006

+++++++++++++++++++++++++++++++++++++++++++
20170512.06201494588006

nikto -C all -h 10.50.1.100 -p 80
- Nikto v2.1.4
---------------------------------------------------------------------------
+ Target IP:          10.50.1.100
+ Target Hostname:    10.50.1.100
+ Target Port:        80
+ Start Time:         2017-05-13 06:20:28
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ OSVDB-3268: /: Directory indexing found.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3268: /./: Directory indexing found.
+ OSVDB-3268: /?mod=node&nid=some_thing&op=view: Directory indexing found.
+ OSVDB-3268: /?mod=some_thing&op=browse: Directory indexing found.
+ /./: Appending '/./' to a directory allows indexing
+ OSVDB-3268: //: Directory indexing found.
+ //: Apache on Red Hat Linux release 9 reveals the root directory listing by default if there is no
index page.
+ OSVDB-3268: /?Open: Directory indexing found.
+ OSVDB-3268: /?OpenServer: Directory indexing found.
+ OSVDB-3268: /%2e/: Directory indexing found.
+ OSVDB-576: /%2e/: Weblogic allows source code or directory listing, upgrade to v6.0 SP1 or higher.
http://www.securityfocus.com/bid/2513.
+ OSVDB-3268: /?mod=<script>alert(document.cookie)</script>&op=browse: Directory indexing found.
+ OSVDB-3268: /?sql_debug=1: Directory indexing found.
+ OSVDB-3268: ///: Directory indexing found.
+ OSVDB-3268: http://127.0.0.1:2301/ HTTP/1.0: Directory indexing found.
+ OSVDB-3268: /?PageServices: Directory indexing found.
+ OSVDB-119: /?PageServices: The remote server may allow directory listings through Web Publisher by
forcing the server to show all files via 'open directory browsing'. Web Publisher should be disabled.
CVE-1999-0269.
+ OSVDB-3268: /?wp-cs-dump: Directory indexing found.
+ OSVDB-119: /?wp-cs-dump: The remote server may allow directory listings through Web Publisher by
forcing the server to show all files via 'open directory browsing'. Web Publisher should be disabled.
CVE-1999-0269.
+ OSVDB-3268: /fotos/: Directory indexing found.
+ OSVDB-3092: /fotos/: This might be interesting...
+ OSVDB-3268: /includes/: Directory indexing found.
+ OSVDB-3092: /includes/: This might be interesting...
```

```
+ OSVDB-3268:
/////////////////////////////////////////////////////////////////////////////////////////////////////////
/////////////////////////////////////////////////////////////////////////////////////////////////////////
/////////////////////////////////////////////////////: Directory indexing found.
+ OSVDB-3288:
/////////////////////////////////////////////////////////////////////////////////////////////////////////
/////////////////////////////////////////////////////////////////////////////////////////////////////////
/////////////////////////////////////////////////////: Abyss 1.03 reveals directory listing when
/'s are requested.
+ OSVDB-3268: /?pattern=/etc/*&sort=name: Directory indexing found.
+ OSVDB-3268: /?D=A: Directory indexing found.
+ OSVDB-3268: /?N=D: Directory indexing found.
+ OSVDB-3268: /?S=A: Directory indexing found.
+ OSVDB-3268: /?M=A: Directory indexing found.
+ OSVDB-3268: /?\"><script>alert('Vulnerable');</script>: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-3268: /?_CONFIG[files][functions_page]=http://cirt.net/rfiinc.txt?: Directory indexing found.
+ OSVDB-3268: /?npage=-1&content_dir=http://cirt.net/rfiinc.txt?%00&cmd=ls: Directory indexing found.
+ OSVDB-3268: /?npage=1&content_dir=http://cirt.net/rfiinc.txt?%00&cmd=ls: Directory indexing found.
+ OSVDB-3268: /?show=http://cirt.net/rfiinc.txt??: Directory indexing found.
+ 6456 items checked: 0 error(s) and 37 item(s) reported on remote host
+ End Time:           2017-05-13 06:21:53 (85 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
nikto -C all -h 10.50.1.100 -p 2222
- Nikto v2.1.4
---------------------------------------------------------------------------
+ No web server found on 10.50.1.100:2222
---------------------------------------------------------------------------
+ 0 host(s) tested
EOF Nikto Report for 10.50.1.100 ...
20170512.06221494588135

-------------------------------------------
-------------------------------------------
End Completed for 10.50.1.100  Scann Report ....
END Time : 20170512.06221494588135 ..
EoFScann 10.50.1.100
```

Anexo 6 – Evidencia Vulnerabilidades 10.50.1.101

```
scann.mc1 10.50.1.101
Starting Scann Report ....
Start Time : 20170512.06221494588135 ..
-------------------------------------------

20170512.06221494588135
Ping Reachable Host 10.50.1.101 ::
PING 10.50.1.101 (10.50.1.101) 56(84) bytes of data.
64 bytes from 10.50.1.101: icmp_req=1 ttl=64 time=3.25 ms
64 bytes from 10.50.1.101: icmp_req=2 ttl=64 time=3.05 ms

--- 10.50.1.101 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 3.052/3.151/3.250/0.099 ms

20170512.06221494588137


-------------------------------------------
-------------------------------------------
-------------------------------------------
starting NMAP Scann Report ....
20170512.06221494588137


Starting Nmap 5.21 ( http://nmap.org ) at 2017-05-12 06:22 CDT
Nmap scan report for 10.50.1.101
Host is up (0.0065s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds

20170512.06221494588137


-------------------------------------------
-------------------------------------------
-------------------------------------------
 Starting Nmap ScannForce Report
20170512.06221494588137



Starting Nmap 5.21 ( http://nmap.org ) at 2017-05-12 06:22 CDT
NSE: Loaded 36 scripts for scanning.
Initiating SYN Stealth Scan at 06:22
Scanning 10.50.1.101 [1000 ports]
Discovered open port 3306/tcp on 10.50.1.101
Completed SYN Stealth Scan at 06:22, 0.12s elapsed (1000 total ports)
Initiating Service scan at 06:22
Scanning 1 service on 10.50.1.101
Completed Service scan at 06:22, 0.01s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 10.50.1.101
Retrying OS detection (try #2) against 10.50.1.101
Initiating Traceroute at 06:22
Completed Traceroute at 06:22, 0.01s elapsed
NSE: Script scanning 10.50.1.101.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 06:22
Completed NSE at 06:22, 0.01s elapsed
NSE: Script Scanning completed.
Nmap scan report for 10.50.1.101
Host is up (0.0034s 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: 6570
| Some Capabilities: Long Passwords, Connect with DB, Compress, ODBC, Transactions, Secure Connection
| Status: Autocommit
```

```
|_Salt: #Ot1DD)\x03
Device type: general purpose|WAP|broadband router
Running (JUST GUESSING) : Linux 2.6.X|2.4.X (89%)
Aggressive OS guesses: Linux 2.6.18 (CentOS 5.1, x86) (89%), Linux 2.6.18 (85%), DD-WRT v23 (Linux
2.4.34) (85%), OpenWrt Kamikaze 8.09 (Linux 2.6.25.20) (85%), Linux 2.6.15 (Ubuntu) (85%), Linux
2.6.15 - 2.6.26 (85%), Linux 2.6.23 (85%), Linux 2.6.27.21-grsec (85%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.720 days (since Thu May 11 13:06:00 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 995/tcp)
HOP RTT     ADDRESS
1   3.68 ms 10.50.1.101

Read data files from: /usr/share/nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.20 seconds
           Raw packets sent: 1072 (49.076KB) | Rcvd: 1033 (42.716KB)
20170512.06221494588141


-------------------------------------------
-------------------------------------------
.........................................
20170512.06221494588141


NCat check ports Version ProcServer ::
nc 10.50.1.101 3306
[282828
5.7.17-0ubuntu0.16.04.228«2828%
4s%28ÿ÷28ÿ□2828282828282828282828S"_NOD9hXG28mysql_native_password28Nikto Report for 10.50.1.101 ....
20170512.06221494588141


+++++++++++++++++++++++++++++++++++++++++++
20170512.06221494588141


nikto -C all -h 10.50.1.101 -p 3306
- Nikto v2.1.4
---------------------------------------------------------------------------
+ No web server found on 10.50.1.101:3306
---------------------------------------------------------------------------
+ 0 host(s) tested
EOF Nikto Report for 10.50.1.101 ...
20170512.06221494588163



-------------------------------------------
-------------------------------------------
End Completed for 10.50.1.101  Scann Report ....
END Time : 20170512.06221494588163 ..
EoFScann 10.50.1.101
```

Anexo 7 – Evidencia Vulnerabilidades 10.50.1.102

```
scann.mc1 10.50.1.102
Starting Scann Report ....
Start Time : 20170512.06221494588163 ..
-------------------------------------------

20170512.06221494588163
Ping Reachable Host 10.50.1.102 ::
PING 10.50.1.102 (10.50.1.102) 56(84) bytes of data.
64 bytes from 10.50.1.102: icmp_req=1 ttl=64 time=3.20 ms
64 bytes from 10.50.1.102: icmp_req=2 ttl=64 time=3.08 ms

--- 10.50.1.102 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 3.087/3.147/3.207/0.060 ms

20170512.06221494588165

-------------------------------------------
-------------------------------------------
-------------------------------------------

starting NMAP Scann Report ....
20170512.06221494588165

Starting Nmap 5.21 ( http://nmap.org ) at 2017-05-12 06:22 CDT
Nmap scan report for 10.50.1.102
Host is up (0.0064s latency).
All 1000 scanned ports on 10.50.1.102 are closed

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds

20170512.06221494588165
-------------------------------------------
-------------------------------------------
-------------------------------------------
 Starting Nmap ScannForce Report
20170512.06221494588165

Starting Nmap 5.21 ( http://nmap.org ) at 2017-05-12 06:22 CDT
NSE: Loaded 36 scripts for scanning.
Initiating SYN Stealth Scan at 06:22
Scanning 10.50.1.102 [1000 ports]
Completed SYN Stealth Scan at 06:22, 0.12s elapsed (1000 total ports)
Initiating Service scan at 06:22
Initiating OS detection (try #1) against 10.50.1.102
Initiating Traceroute at 06:22
Completed Traceroute at 06:22, 0.01s elapsed
NSE: Script scanning 10.50.1.102.
NSE: Script Scanning completed.
Nmap scan report for 10.50.1.102
Host is up (0.0050s latency).
All 1000 scanned ports on 10.50.1.102 are closed
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: storage-misc|WAP|general purpose
Running: Buffalo embedded, Linksys embedded, Linux 2.6.X
OS details: Buffalo TeraStation NAS device, Linksys WAP54G WAP, Linux 2.6.18 (CentOS 5.1, x86)
Network Distance: 1 hop

TRACEROUTE (using port 110/tcp)
HOP RTT     ADDRESS
1   3.76 ms 10.50.1.102

Read data files from: /usr/share/nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.03 seconds
           Raw packets sent: 1022 (45.634KB) | Rcvd: 1014 (41.122KB)
20170512.06221494588166


-------------------------------------------
-------------------------------------------
.........................................
20170512.06221494588166
```

```
NCat check ports Version ProcServer ::
Nikto Report for 10.50.1.102 ....
20170512.06221494588167

++++++++++++++++++++++++++++++++++++++++++++
20170512.06221494588167


EOF Nikto Report for 10.50.1.102 ...
20170512.06221494588167

------------------------------------------
------------------------------------------
End Completed for 10.50.1.102  Scann Report ....
END Time : 20170512.06221494588167 ..
EoFScann 10.50.1.102
```

Anexo 8 – Evidencia Vulnerabilidades 10.50.1.103

```
scann.mc1 10.50.1.103
Starting Scann Report ....
Start Time : 20170512.06221494588167 ..
-------------------------------------------

20170512.06221494588167
Ping Reachable Host 10.50.1.103 ::
PING 10.50.1.103 (10.50.1.103) 56(84) bytes of data.
64 bytes from 10.50.1.103: icmp_req=1 ttl=64 time=3.19 ms
64 bytes from 10.50.1.103: icmp_req=2 ttl=64 time=3.03 ms

--- 10.50.1.103 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 3.036/3.115/3.194/0.079 ms

20170512.06221494588169

-------------------------------------------
-------------------------------------------
-------------------------------------------
starting NMAP Scann Report ....
20170512.06221494588169

Starting Nmap 5.21 ( http://nmap.org ) at 2017-05-12 06:22 CDT
Nmap scan report for 10.50.1.103
Host is up (0.0060s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds

20170512.06221494588169

-------------------------------------------
-------------------------------------------
-------------------------------------------
 Starting Nmap ScannForce Report
20170512.06221494588169


Starting Nmap 5.21 ( http://nmap.org ) at 2017-05-12 06:22 CDT
NSE: Loaded 36 scripts for scanning.
Initiating SYN Stealth Scan at 06:22
Scanning 10.50.1.103 [1000 ports]
Discovered open port 443/tcp on 10.50.1.103
Discovered open port 80/tcp on 10.50.1.103
Completed SYN Stealth Scan at 06:22, 0.12s elapsed (1000 total ports)
Initiating Service scan at 06:22
Scanning 2 services on 10.50.1.103
Completed Service scan at 06:23, 18.24s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 10.50.1.103
Retrying OS detection (try #2) against 10.50.1.103
Initiating Traceroute at 06:23
Completed Traceroute at 06:23, 0.01s elapsed
NSE: Script scanning 10.50.1.103.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 06:23
Completed NSE at 06:23, 0.02s elapsed
NSE: Script Scanning completed.
Nmap scan report for 10.50.1.103
Host is up (0.0033s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE    VERSION
80/tcp  open  http?
443/tcp open  ssl/https?
2 services unrecognized despite returning data. If you know the service/version, please submit the
following fingerprints at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=5.21%I=7%D=5/12%Time=59159B10%P=x86_64-unknown-linux-gnu%r
SF:(GetRequest,16AC,"HTTP/1\.1\x20200\x20OK\r\nServer:\x20nginx/1\.10\.0\x
SF:20\(Ubuntu\)\r\nDate:\x20Fri,\x2012\x20May\x202017\x2011:22:56\x20GMT\r
```

```
SF:\nContent-Type:\x20text/html;\x20charset=utf-8\r\nConnection:\x20close\
SF:r\nSet-Cookie:\x20PHPSESSID=3hj7tlpng665vnkrd4i9dha986;\x20path=/\r\nEx
SF:pires:\x20Mon,\x2026\x20Jul\x201997\x2005:00:00\x20GMT\r\nCache-Control
SF::\x20no-store,\x20no-cache,\x20must-revalidate\r\nCache-Control:\x20pos
SF:t-check=0,\x20pre-check=0\r\nPragma:\x20no-cache\r\nP3P:\x20CP=\"IDC\x2
SF:0DSP\x20COR\x20ADM\x20DEVi\x20TAIi\x20PSA\x20PSD\x20IVAi\x20IVDi\x20CON
SF:i\x20HIS\x20OUR\x20IND\x20CNT\"\r\n\r\n<!DOCTYPE\x20HTML>\r\n<html\x20x
SF:mlns=\"http://www\.w3\.org/1999/xhtml\"\x20lang=\"es_MX\"\x20xml:lang=\
SF:"es_MX\">\r\n<head>\r\n<meta\x20http-equiv=\"Content-Type\"\x20content=
SF:\"text/html;\x20charset=utf-8\"\x20/>\r\n<meta\x20http-equiv=\"X-UA-Com
SF:patible\"\x20content=\"IE=edge\">\r\n<META\x20NAME=\"google-site-verifi
SF:cation\"\x20content=\"\"\x20/>\r\n<META\x20NAME=\"Title\"\x20CONTENT=\"
SF:IEC\"\x20/>\r\n<META\x20NAME=\"Author\"\x20content=\"JEFR\"\x20/>\r\n<M
SF:ETA\x20NAME=\"Subject\"\x20CONTENT=\"nframework\"\x20/>\r\n<META\x20NAM
SF:E=\"Description\"\x20CONTENT=\"nframework\"\x20/>\r\n<META\x20NAME=\"Ke
SF:ywo")%r(HTTPOptions,157,"HTTP/1\.1\x20405\x20Not\x20Allowed\r\nServer:\
SF:x20nginx/1\.10\.0\x20\(Ubuntu\)\r\nDate:\x20Fri,\x2012\x20May\x202017\x
SF:2011:22:56\x20GMT\r\nContent-Type:\x20text/html\r\nContent-Length:\x201
SF:82\r\nConnection:\x20close\r\n\r\n<html>\r\n<head><title>405\x20Not\x20
SF:Allowed</title></head>\r\n<body\x20bgcolor=\"white\">\r\n<center><h1>40
SF:5\x20Not\x20Allowed</h1></center>\r\n<hr><center>nginx/1\.10\.0\x20\(Ub
SF:untu\)</center>\r\n</body>\r\n</html>\r\n")%r(RTSPRequest,B6,"<html>\r\
SF:n<head><title>400\x20Bad\x20Request</title></head>\r\n<body\x20bgcolor=
SF:\"white\">\r\n<center><h1>400\x20Bad\x20Request</h1></center>\r\n<hr><c
SF:enter>nginx/1\.10\.0\x20\(Ubuntu\)</center>\r\n</body>\r\n</html>\r\n")
SF:%r(X11Probe,157,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nServer:\x20nginx
SF:/1\.10\.0\x20\(Ubuntu\)\r\nDate:\x20Fri,\x2012\x20May\x202017\x2011:22:
SF:56\x20GMT\r\nContent-Type:\x20text/html\r\nContent-Length:\x20182\r\nCo
SF:nnection:\x20close\r\n\r\n<html>\r\n<head><title>400\x20Bad\x20Request<
SF:/title></head>\r\n<body\x20bgcolor=\"white\">\r\n<center><h1>400\x20Bad
SF:\x20Request</h1></center>\r\n<hr><center>nginx/1\.10\.0\x20\(Ubuntu\)</
SF:center>\r\n</body>\r\n</html>\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port443-TCP:V=5.21%T=SSL%I=7%D=5/12%Time=59159B16%P=x86_64-unknown-linux-
gnu%r(GetRequest,16AC,"HTTP/1\.1\x20200\x20OK\r\nServer:\x20nginx/1\.10\.
SF:0\x20\(Ubuntu\)\r\nDate:\x20Fri,\x2012\x20May\x202017\x2011:23:02\x20GM
SF:T\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nConnection:\x20clo
SF:se\r\nSet-Cookie:\x20PHPSESSID=udkh58beblgevshldrkl6lpmh0;\x20path=/\r\
SF:nExpires:\x20Mon,\x2026\x20Jul\x201997\x2005:00:00\x20GMT\r\nCache-Cont
SF:rol:\x20no-store,\x20no-cache,\x20must-revalidate\r\nCache-Control:\x20
SF:post-check=0,\x20pre-check=0\r\nPragma:\x20no-cache\r\nP3P:\x20CP=\"IDC
SF:\x20DSP\x20COR\x20ADM\x20DEVi\x20TAIi\x20PSA\x20PSD\x20IVAi\x20IVDi\x20
SF:CONi\x20HIS\x20OUR\x20IND\x20CNT\"\r\n\r\n<!DOCTYPE\x20HTML>\r\n<html\x
SF:20xmlns=\"http://www\.w3\.org/1999/xhtml\"\x20lang=\"es_MX\"\x20xml:lan
SF:g=\"es_MX\">\r\n<head>\r\n<meta\x20http-equiv=\"Content-Type\"\x20conte
SF:nt=\"text/html;\x20charset=utf-8\"\x20/>\r\n<meta\x20http-equiv=\"X-UA-
SF:Compatible\"\x20content=\"IE=edge\">\r\n<META\x20NAME=\"google-site-ver
SF:ification\"\x20content=\"\"\x20/>\r\n<META\x20NAME=\"Title\"\x20CONTENT
SF:=\"IEC\"\x20/>\r\n<META\x20NAME=\"Author\"\x20content=\"JEFR\"\x20/>\r\
SF:n<META\x20NAME=\"Subject\"\x20CONTENT=\"nframework\"\x20/>\r\n<META\x20
SF:NAME=\"Description\"\x20CONTENT=\"nframework\"\x20/>\r\n<META\x20NAME=\
SF:"Keywo")%r(HTTPOptions,157,"HTTP/1\.1\x20405\x20Not\x20Allowed\r\nServe
SF:r:\x20nginx/1\.10\.0\x20\(Ubuntu\)\r\nDate:\x20Fri,\x2012\x20May\x20201
SF:7\x2011:23:07\x20GMT\r\nContent-Type:\x20text/html\r\nContent-Length:\x
SF:20182\r\nConnection:\x20close\r\n\r\n<html>\r\n<head><title>405\x20Not\
SF:x20Allowed</title></head>\r\n<body\x20bgcolor=\"white\">\r\n<center><h1
SF:>405\x20Not\x20Allowed</h1></center>\r\n<hr><center>nginx/1\.10\.0\x20\
SF:(Ubuntu\)</center>\r\n</body>\r\n</html>\r\n")%r(RTSPRequest,B6,"<html>
SF:\r\n<head><title>400\x20Bad\x20Request</title></head>\r\n<body\x20bgcol
SF:or=\"white\">\r\n<center><h1>400\x20Bad\x20Request</h1></center>\r\n<hr
SF:><center>nginx/1\.10\.0\x20\(Ubuntu\)</center>\r\n</body>\r\n</html>\r\
SF:n")%r(RPCCheck,157,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nServer:\x20ng
SF:inx/1\.10\.0\x20\(Ubuntu\)\r\nDate:\x20Fri,\x2012\x20May\x202017\x2011:
SF:23:07\x20GMT\r\nContent-Type:\x20text/html\r\nContent-Length:\x20182\r\
SF:nConnection:\x20close\r\n\r\n<html>\r\n<head><title>400\x20Bad\x20Reque
SF:st</title></head>\r\n<body\x20bgcolor=\"white\">\r\n<center><h1>400\x20
SF:Bad\x20Request</h1></center>\r\n<hr><center>nginx/1\.10\.0\x20\(Ubuntu\
SF:)</center>\r\n</body>\r\n</html>\r\n");
Device type: general purpose|WAP|broadband router
Running (JUST GUESSING) : Linux 2.6.X|2.4.X (89%)
Aggressive OS guesses: Linux 2.6.18 (CentOS 5.1, x86) (89%), Linux 2.6.18 (85%), DD-WRT v23 (Linux
2.4.34) (85%), OpenWrt Kamikaze 8.09 (Linux 2.6.25.20) (85%), Linux 2.6.15 (Ubuntu) (85%), Linux
2.6.15 - 2.6.26 (85%), Linux 2.6.23 (85%), Linux 2.6.27.21-grsec (85%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.720 days (since Thu May 11 13:06:00 2017)
```

```
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 199/tcp)
HOP RTT     ADDRESS
1   3.54 ms 10.50.1.103

Read data files from: /usr/share/nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.42 seconds
           Raw packets sent: 1072 (49.076KB) | Rcvd: 1033 (42.720KB)
20170512.06231494588191

-------------------------------------------
-------------------------------------------
.........................................
20170512.06231494588191

NCat check ports Version ProcServer ::
nc 10.50.1.103 80
nc 10.50.1.103 443
Nikto Report for 10.50.1.103 ....
20170512.06231494588192

++++++++++++++++++++++++++++++++++++++++++++
20170512.06231494588192


nikto -C all -h 10.50.1.103 -p 80
- Nikto v2.1.4
---------------------------------------------------------------------------
+ Target IP:          10.50.1.103
+ Target Hostname:    10.50.1.103
+ Target Port:        80
+ Start Time:         2017-05-13 06:23:33
---------------------------------------------------------------------------
+ Server: nginx/1.10.0 (Ubuntu)
+ Root page / redirects to: https://10.50.1.103/
+ Number of sections in the version string differ from those in the database, the server reports:
nginx/1.10.0(ubuntu) while the database has: 1.0.4. This may cause false positives.
+ OSVDB-3092: /test.php: This might be interesting...
+ 6456 items checked: 4 error(s) and 2 item(s) reported on remote host
+ End Time:           2017-05-13 06:26:16 (163 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
EOF Nikto Report for 10.50.1.103 ...
20170512.06261494588376

-------------------------------------------
-------------------------------------------
End Completed for 10.50.1.103  Scann Report ....
END Time : 20170512.06261494588376 ..
EoFScann 10.50.1.103
```

Anexo 9 – Evidencia Vulnerabilidades 10.50.1.104

```
scann.mc1 10.50.1.104
Starting Scann Report ....
Start Time : 20170512.06261494588376 ..
-------------------------------------------

20170512.06261494588376
Ping Reachable Host 10.50.1.104 ::
PING 10.50.1.104 (10.50.1.104) 56(84) bytes of data.
64 bytes from 10.50.1.104: icmp_req=1 ttl=64 time=3.23 ms
64 bytes from 10.50.1.104: icmp_req=2 ttl=64 time=3.02 ms

--- 10.50.1.104 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 3.029/3.131/3.234/0.116 ms

20170512.06261494588378

-------------------------------------------
-------------------------------------------
-------------------------------------------
starting NMAP Scann Report ....
20170512.06261494588378


Starting Nmap 5.21 ( http://nmap.org ) at 2017-05-12 06:26 CDT
Nmap scan report for 10.50.1.104
Host is up (0.0059s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
21/tcp open  ftp

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds

20170512.06261494588378

-------------------------------------------
-------------------------------------------
-------------------------------------------
 Starting Nmap ScannForce Report
20170512.06261494588378


Starting Nmap 5.21 ( http://nmap.org ) at 2017-05-12 06:26 CDT
NSE: Loaded 36 scripts for scanning.
Initiating SYN Stealth Scan at 06:26
Scanning 10.50.1.104 [1000 ports]
Discovered open port 21/tcp on 10.50.1.104
Completed SYN Stealth Scan at 06:26, 0.12s elapsed (1000 total ports)
Initiating Service scan at 06:26
Scanning 1 service on 10.50.1.104
Completed Service scan at 06:27, 86.11s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 10.50.1.104
Retrying OS detection (try #2) against 10.50.1.104
Initiating Traceroute at 06:27
Completed Traceroute at 06:27, 0.01s elapsed
NSE: Script scanning 10.50.1.104.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 06:27
Completed NSE at 06:27, 8.05s elapsed
NSE: Script Scanning completed.
Nmap scan report for 10.50.1.104
Host is up (0.0034s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     (Generally vsftp or WU-FTPD)
1 service unrecognized despite returning data. If you know the service/version, please submit the
following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port21-TCP:V=5.21%I=7%D=5/12%Time=59159BE1%P=x86_64-unknown-linux-gnu%r
SF:(NULL,9,"220\x20IEC\r\n")%r(GenericLines,9,"220\x20IEC\r\n")%r(Help,2F,
SF:"220\x20IEC\r\n530\x20Please\x20login\x20with\x20USER\x20and\x20PASS\.\
SF:r\n")%r(GetRequest,2F,"220\x20IEC\r\n530\x20Please\x20login\x20with\x20
SF:USER\x20and\x20PASS\.\r\n")%r(HTTPOptions,2F,"220\x20IEC\r\n530\x20Plea
SF:se\x20login\x20with\x20USER\x20and\x20PASS\.\r\n")%r(RTSPRequest,2F,"22
```

```
SF:0\x20IEC\r\n530\x20Please\x20login\x20with\x20USER\x20and\x20PASS\.\r\n
SF:")%r(RPCCheck,9,"220\x20IEC\r\n")%r(DNSVersionBindReq,9,"220\x20IEC\r\n
SF:")%r(DNSStatusRequest,9,"220\x20IEC\r\n")%r(SSLSessionReq,2F,"220\x20IE
SF:C\r\n530\x20Please\x20login\x20with\x20USER\x20and\x20PASS\.\r\n")%r(SM
SF:BProgNeg,9,"220\x20IEC\r\n")%r(X11Probe,9,"220\x20IEC\r\n")%r(FourOhFou
SF:rRequest,2F,"220\x20IEC\r\n530\x20Please\x20login\x20with\x20USER\x20an
SF:d\x20PASS\.\r\n")%r(LPDString,2F,"220\x20IEC\r\n530\x20Please\x20login\
SF:x20with\x20USER\x20and\x20PASS\.\r\n")%r(LDAPBindReq,9,"220\x20IEC\r\n"
SF:)%r(SIPOptions,185,"220\x20IEC\r\n530\x20Please\x20login\x20with\x20USE
SF:R\x20and\x20PASS\.\r\n530\x20Please\x20login\x20with\x20USER\x20and\x20
SF:PASS\.\r\n530\x20Please\x20login\x20with\x20USER\x20and\x20PASS\.\r\n53
SF:0\x20Please\x20login\x20with\x20USER\x20and\x20PASS\.\r\n530\x20Please\
SF:x20login\x20with\x20USER\x20and\x20PASS\.\r\n530\x20Please\x20login\x20
SF:with\x20USER\x20and\x20PASS\.\r\n530\x20Please\x20login\x20with\x20USER
SF:\x20and\x20PASS\.\r\n530\x20Please\x20login\x20with\x20USER\x20and\x20P
SF:ASS\.\r\n530\x20Please\x20login\x20with\x20USER\x20and\x20PASS\.\r\n530
SF:\x20Please\x20login\x20with\x20USER\x20and\x20PASS\.\r\n");
Device type: general purpose|WAP|broadband router
Running (JUST GUESSING) : Linux 2.6.X|2.4.X (89%)
Aggressive OS guesses: Linux 2.6.18 (CentOS 5.1, x86) (89%), Linux 2.6.18 (85%), DD-WRT v23 (Linux
2.4.34) (85%), OpenWrt Kamikaze 8.09 (Linux 2.6.25.20) (85%), Linux 2.6.15 (Ubuntu) (85%), Linux
2.6.15 - 2.6.26 (85%), Linux 2.6.23 (85%), Linux 2.6.27.21-grsec (85%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.724 days (since Thu May 11 13:06:00 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 445/tcp)
HOP RTT     ADDRESS
1   3.63 ms 10.50.1.104

Read data files from: /usr/share/nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 98.34 seconds
           Raw packets sent: 1072 (49.076KB) | Rcvd: 1033 (42.716KB)
20170512.06271494588477


-------------------------------------------
-------------------------------------------
.........................................
20170512.06271494588477


NCat check ports Version ProcServer ::
nc 10.50.1.104 21
220 IEC

Nikto Report for 10.50.1.104 ....
20170512.06271494588477


+++++++++++++++++++++++++++++++++++++++++++
20170512.06271494588477


nikto -C all -h 10.50.1.104 -p 21
- Nikto v2.1.4
---------------------------------------------------------------------------
+ ERROR: SKIPPORTS (nikto.conf) contains 21 -- not checking
+ 0 host(s) tested
EOF Nikto Report for 10.50.1.104 ...
20170512.06281494588499

-------------------------------------------
-------------------------------------------
End Completed for 10.50.1.104  Scann Report ....
END Time : 20170512.06281494588499 ..
EoFScann 10.50.1.104
```

Anexo 10 – Evidencia Vulnerabilidades 10.50.1.105

```
scann.mc1 10.50.1.105
Starting Scann Report ....
Start Time : 20170512.06281494588499 ..
-------------------------------------------

20170512.06281494588499
Ping Reachable Host 10.50.1.105 ::
PING 10.50.1.105 (10.50.1.105) 56(84) bytes of data.
64 bytes from 10.50.1.105: icmp_req=1 ttl=64 time=3.33 ms
64 bytes from 10.50.1.105: icmp_req=2 ttl=64 time=3.06 ms

--- 10.50.1.105 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 3.062/3.197/3.333/0.146 ms

20170512.06281494588501

-------------------------------------------
-------------------------------------------
-------------------------------------------
starting NMAP Scann Report ....
20170512.06281494588501

Starting Nmap 5.21 ( http://nmap.org ) at 2017-05-12 06:28 CDT
Nmap scan report for 10.50.1.105
Host is up (0.0061s latency).
All 1000 scanned ports on 10.50.1.105 are closed

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds

20170512.06281494588501

-------------------------------------------
-------------------------------------------
-------------------------------------------
 Starting Nmap ScannForce Report
20170512.06281494588501

Starting Nmap 5.21 ( http://nmap.org ) at 2017-05-12 06:28 CDT
NSE: Loaded 36 scripts for scanning.
Initiating SYN Stealth Scan at 06:28
Scanning 10.50.1.105 [1000 ports]
Completed SYN Stealth Scan at 06:28, 0.12s elapsed (1000 total ports)
Initiating Service scan at 06:28
Initiating OS detection (try #1) against 10.50.1.105
Initiating Traceroute at 06:28
Completed Traceroute at 06:28, 0.01s elapsed
NSE: Script scanning 10.50.1.105.
NSE: Script Scanning completed.
Nmap scan report for 10.50.1.105
Host is up (0.0049s latency).
All 1000 scanned ports on 10.50.1.105 are closed
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: storage-misc|WAP|general purpose
Running: Buffalo embedded, Linksys embedded, Linux 2.6.X
OS details: Buffalo TeraStation NAS device, Linksys WAP54G WAP, Linux 2.6.18 (CentOS 5.1, x86)
Network Distance: 1 hop

TRACEROUTE (using port 1025/tcp)
HOP RTT     ADDRESS
1   3.24 ms 10.50.1.105

Read data files from: /usr/share/nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.01 seconds
           Raw packets sent: 1022 (45.634KB) | Rcvd: 1014 (41.122KB)
20170512.06281494588502

-------------------------------------------
-------------------------------------------
.........................................
20170512.06281494588502
```

```
NCat check ports Version ProcServer ::
Nikto Report for 10.50.1.105 ....
20170512.06281494588502

++++++++++++++++++++++++++++++++++++++++++++
20170512.06281494588502

EOF Nikto Report for 10.50.1.105 ...
20170512.06281494588502

------------------------------------------
------------------------------------------
End Completed for 10.50.1.105  Scann Report ....
END Time : 20170512.06281494588502 ..
EoFScann 10.50.1.105
```

Anexo 11 – Evidencia Vulnerabilidades 10.50.1.106

```
scann.mc1 10.50.1.106
Starting Scann Report ....
Start Time : 20170512.06281494588502 ..
-------------------------------------------

20170512.06281494588502
Ping Reachable Host 10.50.1.106 ::
PING 10.50.1.106 (10.50.1.106) 56(84) bytes of data.
64 bytes from 10.50.1.106: icmp_req=1 ttl=64 time=3.35 ms
64 bytes from 10.50.1.106: icmp_req=2 ttl=64 time=3.06 ms

--- 10.50.1.106 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 3.062/3.206/3.350/0.144 ms

20170512.06281494588504


-------------------------------------------
-------------------------------------------
-------------------------------------------
starting NMAP Scann Report ....
20170512.06281494588504


Starting Nmap 5.21 ( http://nmap.org ) at 2017-05-12 06:28 CDT
Nmap scan report for 10.50.1.106
Host is up (0.0065s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds

20170512.06281494588505


-------------------------------------------
-------------------------------------------
-------------------------------------------
 Starting Nmap ScannForce Report
20170512.06281494588505



Starting Nmap 5.21 ( http://nmap.org ) at 2017-05-12 06:28 CDT
NSE: Loaded 36 scripts for scanning.
Initiating SYN Stealth Scan at 06:28
Scanning 10.50.1.106 [1000 ports]
Discovered open port 80/tcp on 10.50.1.106
Completed SYN Stealth Scan at 06:28, 0.12s elapsed (1000 total ports)
Initiating Service scan at 06:28
Scanning 1 service on 10.50.1.106
Completed Service scan at 06:28, 6.01s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 10.50.1.106
Retrying OS detection (try #2) against 10.50.1.106
Initiating Traceroute at 06:28
Completed Traceroute at 06:28, 0.01s elapsed
NSE: Script scanning 10.50.1.106.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 06:28
Completed NSE at 06:28, 0.02s elapsed
NSE: Script Scanning completed.
Nmap scan report for 10.50.1.106
Host is up (0.0033s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_html-title: Apache2 Ubuntu Default Page: It works
Device type: general purpose|WAP|broadband router
Running (JUST GUESSING) : Linux 2.6.X|2.4.X (89%)
```

```
Aggressive OS guesses: Linux 2.6.18 (CentOS 5.1, x86) (89%), Linux 2.6.18 (85%), DD-WRT v23 (Linux
2.4.34) (85%), OpenWrt Kamikaze 8.09 (Linux 2.6.25.20) (85%), Linux 2.6.15 (Ubuntu) (85%), Linux
2.6.15 - 2.6.26 (85%), Linux 2.6.23 (85%), Linux 2.6.27.21-grsec (85%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.724 days (since Thu May 11 13:05:59 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 53/tcp)
HOP RTT     ADDRESS
1   3.72 ms 10.50.1.106

Read data files from: /usr/share/nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.19 seconds
           Raw packets sent: 1072 (49.076KB) | Rcvd: 1032 (42.664KB)
20170512.06281494588515


-------------------------------------------
-------------------------------------------
.........................................
20170512.06281494588515


NCat check ports Version ProcServer ::
nc 10.50.1.106 80
Nikto Report for 10.50.1.106 ....
20170512.06281494588515


+++++++++++++++++++++++++++++++++++++++++++
20170512.06281494588515


nikto -C all -h 10.50.1.106 -p 80
- Nikto v2.1.4
---------------------------------------------------------------------------
+ Target IP:          10.50.1.106
+ Target Hostname:    10.50.1.106
+ Target Port:        80
+ Start Time:         2017-05-13 06:28:57
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ ETag header found on server, fields: 0x2c39 0x54e65bbfe7477
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3233: /icons/README: Apache default file found.
+ 6456 items checked: 0 error(s) and 3 item(s) reported on remote host
+ End Time:           2017-05-13 06:30:24 (87 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
EOF Nikto Report for 10.50.1.106 ...
20170512.06301494588624



-------------------------------------------
-------------------------------------------
End Completed for 10.50.1.106  Scann Report ....
END Time : 20170512.06301494588624 ..
EoFScann 10.50.1.106
```

Anexo 12 – Evidencia Vulnerabilidades 10.50.1.107

```
scann.mc1 10.50.1.107
Starting Scann Report ....
Start Time : 20170512.06301494588624 ..
-------------------------------------------

20170512.06301494588624
Ping Reachable Host 10.50.1.107 ::
PING 10.50.1.107 (10.50.1.107) 56(84) bytes of data.
64 bytes from 10.50.1.107: icmp_req=1 ttl=64 time=3.15 ms
64 bytes from 10.50.1.107: icmp_req=2 ttl=64 time=3.04 ms

--- 10.50.1.107 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 3.045/3.099/3.153/0.054 ms

20170512.06301494588626


-------------------------------------------
-------------------------------------------
-------------------------------------------
starting NMAP Scann Report ....
20170512.06301494588626


Starting Nmap 5.21 ( http://nmap.org ) at 2017-05-12 06:30 CDT
Nmap scan report for 10.50.1.107
Host is up (0.0065s latency).
All 1000 scanned ports on 10.50.1.107 are closed

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds

20170512.06301494588626


-------------------------------------------
-------------------------------------------
-------------------------------------------
 Starting Nmap ScannForce Report
20170512.06301494588626



Starting Nmap 5.21 ( http://nmap.org ) at 2017-05-12 06:30 CDT
NSE: Loaded 36 scripts for scanning.
Initiating SYN Stealth Scan at 06:30
Scanning 10.50.1.107 [1000 ports]
Completed SYN Stealth Scan at 06:30, 0.12s elapsed (1000 total ports)
Initiating Service scan at 06:30
Initiating OS detection (try #1) against 10.50.1.107
Initiating Traceroute at 06:30
Completed Traceroute at 06:30, 0.01s elapsed
NSE: Script scanning 10.50.1.107.
NSE: Script Scanning completed.
Nmap scan report for 10.50.1.107
Host is up (0.0050s latency).
All 1000 scanned ports on 10.50.1.107 are closed
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: storage-misc|WAP|general purpose
Running: Buffalo embedded, Linksys embedded, Linux 2.6.X
OS details: Buffalo TeraStation NAS device, Linksys WAP54G WAP, Linux 2.6.18 (CentOS 5.1, x86)
Network Distance: 1 hop

TRACEROUTE (using port 113/tcp)
HOP RTT     ADDRESS
1   3.54 ms 10.50.1.107

Read data files from: /usr/share/nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.02 seconds
           Raw packets sent: 1022 (45.634KB) | Rcvd: 1014 (41.122KB)
20170512.06301494588627
```

```
-------------------------------------------
-------------------------------------------
.........................................
20170512.06301494588627


NCat check ports Version ProcServer ::
Nikto Report for 10.50.1.107 ....
20170512.06301494588627


+++++++++++++++++++++++++++++++++++++++++++
20170512.06301494588627


EOF Nikto Report for 10.50.1.107 ...
20170512.06301494588627



-------------------------------------------
-------------------------------------------
End Completed for 10.50.1.107  Scann Report ....
END Time : 20170512.06301494588627 ..
EoFScann 10.50.1.107
```

Anexo 13 – Evidencia Vulnerabilidades 10.50.1.108

```
scann.mc1 10.50.1.108
Starting Scann Report ....
Start Time : 20170512.06301494588627 ..
-------------------------------------------

20170512.06301494588627
Ping Reachable Host 10.50.1.108 ::
PING 10.50.1.108 (10.50.1.108) 56(84) bytes of data.
64 bytes from 10.50.1.108: icmp_req=1 ttl=64 time=3.30 ms
64 bytes from 10.50.1.108: icmp_req=2 ttl=64 time=3.03 ms

--- 10.50.1.108 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 3.036/3.168/3.300/0.132 ms

20170512.06301494588629

-------------------------------------------
-------------------------------------------
-------------------------------------------
starting NMAP Scann Report ....
20170512.06301494588629

Starting Nmap 5.21 ( http://nmap.org ) at 2017-05-12 06:30 CDT
Nmap scan report for 10.50.1.108
Host is up (0.0064s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
8086/tcp open  unknown
8088/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds

20170512.06301494588630

-------------------------------------------
-------------------------------------------
-------------------------------------------
 Starting Nmap ScannForce Report
20170512.06301494588630

Starting Nmap 5.21 ( http://nmap.org ) at 2017-05-12 06:30 CDT
NSE: Loaded 36 scripts for scanning.
Initiating SYN Stealth Scan at 06:30
Scanning 10.50.1.108 [1000 ports]
Discovered open port 8088/tcp on 10.50.1.108
Discovered open port 8086/tcp on 10.50.1.108
Completed SYN Stealth Scan at 06:30, 0.12s elapsed (1000 total ports)
Initiating Service scan at 06:30
Scanning 2 services on 10.50.1.108
Completed Service scan at 06:31, 66.19s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 10.50.1.108
Retrying OS detection (try #2) against 10.50.1.108
Initiating Traceroute at 06:31
Completed Traceroute at 06:31, 0.01s elapsed
NSE: Script scanning 10.50.1.108.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 06:31
Completed NSE at 06:31, 0.01s elapsed
NSE: Script Scanning completed.
Nmap scan report for 10.50.1.108
Host is up (0.0033s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
8086/tcp open  unknown
8088/tcp open  unknown
1 service unrecognized despite returning data. If you know the service/version, please submit the
following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port8086-TCP:V=5.21%I=7%D=5/12%Time=59159CDC%P=x86_64-unknown-linux-gnu
SF:%r(GenericLines,58,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:
SF:\x20text/plain\r\nConnection:\x20close\r\n\r\n400\x20Bad\x20Request")%r
SF:(GetRequest,CB,"HTTP/1\.0\x20404\x20Not\x20Found\r\nContent-Type:\x20te
SF:xt/plain;\x20charset=utf-8\r\nX-Content-Type-Options:\x20nosniff\r\nX-I
```

```
SF:nfluxdb-Version:\x201\.2\.2\r\nDate:\x20Fri,\x2012\x20May\x202017\x2011
SF::30:36\x20GMT\r\nContent-Length:\x2019\r\n\r\n404\x20page\x20not\x20fou
SF:nd\n")%r(HTTPOptions,CB,"HTTP/1\.0\x20404\x20Not\x20Found\r\nContent-Ty
SF:pe:\x20text/plain;\x20charset=utf-8\r\nX-Content-Type-Options:\x20nosni
SF:ff\r\nX-Influxdb-Version:\x201\.2\.2\r\nDate:\x20Fri,\x2012\x20May\x202
SF:017\x2011:30:36\x20GMT\r\nContent-Length:\x2019\r\n\r\n404\x20page\x20n
SF:ot\x20found\n")%r(RTSPRequest,58,"HTTP/1\.1\x20400\x20Bad\x20Request\r\
SF:nContent-Type:\x20text/plain\r\nConnection:\x20close\r\n\r\n400\x20Bad\
SF:x20Request")%r(Help,58,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-T
SF:ype:\x20text/plain\r\nConnection:\x20close\r\n\r\n400\x20Bad\x20Request
SF:")%r(SSLSessionReq,58,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Ty
SF:pe:\x20text/plain\r\nConnection:\x20close\r\n\r\n400\x20Bad\x20Request"
SF:)%r(FourOhFourRequest,CB,"HTTP/1\.0\x20404\x20Not\x20Found\r\nContent-T
SF:ype:\x20text/plain;\x20charset=utf-8\r\nX-Content-Type-Options:\x20nosn
SF:iff\r\nX-Influxdb-Version:\x201\.2\.2\r\nDate:\x20Fri,\x2012\x20May\x20
SF:2017\x2011:31:01\x20GMT\r\nContent-Length:\x2019\r\n\r\n404\x20page\x20
SF:not\x20found\n")%r(LPDString,58,"HTTP/1\.1\x20400\x20Bad\x20Request\r\n
SF:Content-Type:\x20text/plain\r\nConnection:\x20close\r\n\r\n400\x20Bad\x
SF:20Request")%r(SIPOptions,58,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nCont
SF:ent-Type:\x20text/plain\r\nConnection:\x20close\r\n\r\n400\x20Bad\x20Re
SF:quest");
Device type: general purpose|WAP|broadband router
Running (JUST GUESSING) : Linux 2.6.X|2.4.X (89%)
Aggressive OS guesses: Linux 2.6.18 (CentOS 5.1, x86) (89%), Linux 2.6.18 (85%), DD-WRT v23 (Linux
2.4.34) (85%), OpenWrt Kamikaze 8.09 (Linux 2.6.25.20) (85%), Linux 2.6.15 (Ubuntu) (85%), Linux
2.6.15 - 2.6.26 (85%), Linux 2.6.23 (85%), Linux 2.6.27.21-grsec (85%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.726 days (since Thu May 11 13:06:00 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 1723/tcp)
HOP RTT     ADDRESS
1   3.61 ms 10.50.1.108

Read data files from: /usr/share/nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 70.38 seconds
           Raw packets sent: 1072 (49.076KB) | Rcvd: 1034 (42.860KB)
20170512.06311494588700

-------------------------------------------
-------------------------------------------
.........................................
20170512.06311494588700

NCat check ports Version ProcServer ::
nc 10.50.1.108 8086
nc 10.50.1.108 8088
Nikto Report for 10.50.1.108 ....
20170512.06311494588700

+++++++++++++++++++++++++++++++++++++++++++
20170512.06311494588700

nikto -C all -h 10.50.1.108 -p 8086
- Nikto v2.1.4
---------------------------------------------------------------------------
+ Target IP:          10.50.1.108
+ Target Hostname:    10.50.1.108
+ Target Port:        8086
+ Start Time:         2017-05-13 06:32:02
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ 6456 items checked: 0 error(s) and 0 item(s) reported on remote host
+ End Time:           2017-05-13 06:33:35 (93 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
nikto -C all -h 10.50.1.108 -p 8088
- Nikto v2.1.4
---------------------------------------------------------------------------
+ No web server found on 10.50.1.108:8088
---------------------------------------------------------------------------
+ 0 host(s) tested
```

```
EOF Nikto Report for 10.50.1.108 ...
20170512.06331494588836

---------------------------------------------
---------------------------------------------
End Completed for 10.50.1.108  Scann Report ....
END Time : 20170512.06331494588836 ..
EoFScann 10.50.1.108
```

Anexo 14 – Evidencia Vulnerabilidades 10.50.1.109

```
scann.mc1 10.50.1.109
Starting Scann Report ....
Start Time : 20170512.06331494588836 ..
-------------------------------------------

20170512.06331494588836
Ping Reachable Host 10.50.1.109 ::
PING 10.50.1.109 (10.50.1.109) 56(84) bytes of data.
64 bytes from 10.50.1.109: icmp_req=1 ttl=64 time=3.35 ms
64 bytes from 10.50.1.109: icmp_req=2 ttl=64 time=3.05 ms

--- 10.50.1.109 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 3.054/3.203/3.353/0.159 ms

20170512.06331494588838

-------------------------------------------
-------------------------------------------
-------------------------------------------
starting NMAP Scann Report ....
20170512.06331494588838

Starting Nmap 5.21 ( http://nmap.org ) at 2017-05-12 06:33 CDT
Nmap scan report for 10.50.1.109
Host is up (0.0063s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE
3000/tcp open  ppp

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds

20170512.06331494588838

-------------------------------------------
-------------------------------------------
-------------------------------------------
 Starting Nmap ScannForce Report
20170512.06331494588838

Starting Nmap 5.21 ( http://nmap.org ) at 2017-05-12 06:33 CDT
NSE: Loaded 36 scripts for scanning.
Initiating SYN Stealth Scan at 06:33
Scanning 10.50.1.109 [1000 ports]
Discovered open port 3000/tcp on 10.50.1.109
Completed SYN Stealth Scan at 06:33, 0.12s elapsed (1000 total ports)
Initiating Service scan at 06:33
Scanning 1 service on 10.50.1.109
Completed Service scan at 06:35, 66.31s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 10.50.1.109
Retrying OS detection (try #2) against 10.50.1.109
Initiating Traceroute at 06:35
Completed Traceroute at 06:35, 0.01s elapsed
NSE: Script scanning 10.50.1.109.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 06:35
Completed NSE at 06:35, 0.01s elapsed
NSE: Script Scanning completed.
Nmap scan report for 10.50.1.109
Host is up (0.0033s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE VERSION
3000/tcp open  ppp?
1 service unrecognized despite returning data. If you know the service/version, please submit the
following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3000-TCP:V=5.21%I=7%D=5/12%Time=59159DAD%P=x86_64-unknown-linux-gnu
SF:%r(GenericLines,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:
SF:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20
SF:Bad\x20Request")%r(GetRequest,10A,"HTTP/1\.0\x20302\x20Found\r\nLocatio
SF:n:\x20/login\r\nSet-Cookie:\x20grafana_sess=6d7baa2e52503995;\x20Path=/
SF:;\x20HttpOnly\r\nSet-Cookie:\x20redirect_to=%252F;\x20Path=/\r\nDate:\x
SF:20Fri,\x2012\x20May\x202017\x2011:34:05\x20GMT\r\nContent-Length:\x2029
SF:\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\n\r\n<a\x20href=\"/l
```

```
SF:ogin\">Found</a>\.\n\n")%r(Help,67,"HTTP/1\.1\x20400\x20Bad\x20Request\
SF:r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20clos
SF:e\r\n\r\n400\x20Bad\x20Request")%r(HTTPOptions,1EAB,"HTTP/1\.0\x20404\x
SF:20Not\x20Found\r\nContent-Type:\x20text/html;\x20charset=UTF-8\r\nSet-C
SF:ookie:\x20grafana_sess=db7c7ed6a657c361;\x20Path=/;\x20HttpOnly\r\nDate
SF::\x20Fri,\x2012\x20May\x202017\x2011:34:10\x20GMT\r\n\r\n<!DOCTYPE\x20h
SF:tml>\n<html\x20lang=\"en\">\n\x20\x20<head>\n\x20\x20\x20\x20<meta\x20c
SF:harset=\"utf-8\">\n\x20\x20\x20\x20<meta\x20http-equiv=\"X-UA-Compatibl
SF:e\"\x20content=\"IE=edge,chrome=1\">\n\x20\x20\x20\x20<meta\x20name=\"v
SF:iewport\"\x20content=\"width=device-width\">\n\x20\x20\x20\x20<meta\x20
SF:name=\"theme-color\"\x20content=\"#000\">\n\n\x20\x20\x20\x20<title>Gra
SF:fana</title>\n\n\t\t<link\x20href='/public/css/fonts\.min\.css'\x20rel=
SF:'stylesheet'\x20type='text/css'>\n\n\t\t\n\t\t\x20\x20<link\x20rel=\"st
SF:ylesheet\"\x20href=\"/public/css/grafana\.dark\.min\.fc104690\.css\">\n
SF:\t\t\n\n\x20\x20\x20\x20<link\x20rel=\"icon\"\x20type=\"image/png\"\x20
SF:href=\"/public/img/fav32\.png\">\n\t\t<base\x20href=\"/\"\x20/>\n\n\t</
SF:head>\n\n\t<body\x20ng-cloak>\n\t\t<grafana-app\x20class=\"grafana-app\
SF:">\n\n\t\t\t<aside\x20class=\"sidemenu-wrapper\">\n\t\t\t\t<sidemenu\x2
SF:0ng-if=\"contextSrv\.sidemenu\"></sidemenu>\n\t\t\t</aside>\n\n\t\t\t<d
SF:iv\x20class=\"page-alert-list\">\n\t\t\t\t<div\x20ng-repeat='a')%r(RTSP
SF:Request,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text
SF:/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x20R
SF:equest");
Device type: general purpose|WAP|broadband router
Running (JUST GUESSING) : Linux 2.6.X|2.4.X (89%)
Aggressive OS guesses: Linux 2.6.18 (CentOS 5.1, x86) (89%), Linux 2.6.18 (85%), DD-WRT v23 (Linux
2.4.34) (85%), OpenWrt Kamikaze 8.09 (Linux 2.6.25.20) (85%), Linux 2.6.15 (Ubuntu) (85%), Linux
2.6.15 - 2.6.26 (85%), Linux 2.6.23 (85%), Linux 2.6.27.21-grsec (85%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.729 days (since Thu May 11 13:06:00 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=256 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 993/tcp)
HOP RTT     ADDRESS
1   3.46 ms 10.50.1.109

Read data files from: /usr/share/nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 70.48 seconds
           Raw packets sent: 1072 (49.076KB) | Rcvd: 1034 (42.871KB)
20170512.06351494588909

-------------------------------------------
-------------------------------------------
.........................................
20170512.06351494588909

NCat check ports Version ProcServer ::
nc 10.50.1.109 3000
Nikto Report for 10.50.1.109 ....
20170512.06351494588909

+++++++++++++++++++++++++++++++++++++++++++
20170512.06351494588909

nikto -C all -h 10.50.1.109 -p 3000
- Nikto v2.1.4
---------------------------------------------------------------------------
+ Target IP:          10.50.1.109
+ Target Hostname:    10.50.1.109
+ Target Port:        3000
+ Start Time:         2017-05-13 06:35:31
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ Root page / redirects to: /login
+ robots.txt contains 1 entry which should be manually viewed.
+ OSVDB-35878: /modules.php?name=Members_List&letter='%20OR%20pass%20LIKE%20'a%25'/*: PHP-Nuke module
allows user names and passwords to be viewed.
+ OSVDB-3092: /login/: This might be interesting...
+ 6456 items checked: 21 error(s) and 3 item(s) reported on remote host
+ End Time:           2017-05-13 06:45:09 (578 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

```
EOF Nikto Report for 10.50.1.109 ...
20170512.06451494589509

---------------------------------------------
---------------------------------------------
End Completed for 10.50.1.109  Scann Report ....
END Time : 20170512.06451494589509 ..
EoFScann 10.50.1.109
```

Anexo 15 – Evidencia Vulnerabilidades 10.50.1.110

```
scann.mc1 10.50.1.110
Starting Scann Report ....
Start Time : 20170512.06451494589509 ..
-------------------------------------------

20170512.06451494589509
Ping Reachable Host 10.50.1.110 ::
PING 10.50.1.110 (10.50.1.110) 56(84) bytes of data.
64 bytes from 10.50.1.110: icmp_req=1 ttl=64 time=3.27 ms
64 bytes from 10.50.1.110: icmp_req=2 ttl=64 time=2.99 ms

--- 10.50.1.110 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 2.991/3.131/3.272/0.151 ms

20170512.06451494589511


-------------------------------------------
-------------------------------------------
-------------------------------------------
starting NMAP Scann Report ....
20170512.06451494589511


Starting Nmap 5.21 ( http://nmap.org ) at 2017-05-12 06:45 CDT
Nmap scan report for 10.50.1.110
Host is up (0.0063s latency).
All 1000 scanned ports on 10.50.1.110 are closed

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds

20170512.06451494589512


-------------------------------------------
-------------------------------------------
-------------------------------------------
 Starting Nmap ScannForce Report
20170512.06451494589512



Starting Nmap 5.21 ( http://nmap.org ) at 2017-05-12 06:45 CDT
NSE: Loaded 36 scripts for scanning.
Initiating SYN Stealth Scan at 06:45
Scanning 10.50.1.110 [1000 ports]
Completed SYN Stealth Scan at 06:45, 0.12s elapsed (1000 total ports)
Initiating Service scan at 06:45
Initiating OS detection (try #1) against 10.50.1.110
Initiating Traceroute at 06:45
Completed Traceroute at 06:45, 0.01s elapsed
NSE: Script scanning 10.50.1.110.
NSE: Script Scanning completed.
Nmap scan report for 10.50.1.110
Host is up (0.0048s latency).
All 1000 scanned ports on 10.50.1.110 are closed
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: storage-misc|WAP|general purpose
Running: Buffalo embedded, Linksys embedded, Linux 2.6.X
OS details: Buffalo TeraStation NAS device, Linksys WAP54G WAP, Linux 2.6.18 (CentOS 5.1, x86)
Network Distance: 1 hop

TRACEROUTE (using port 1025/tcp)
HOP RTT     ADDRESS
1   3.42 ms 10.50.1.110

Read data files from: /usr/share/nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.02 seconds
           Raw packets sent: 1022 (45.634KB) | Rcvd: 1014 (41.122KB)
20170512.06451494589513
```

```
---------------------------------------------
---------------------------------------------
.............................................
20170512.06451494589513


NCat check ports Version ProcServer ::
Nikto Report for 10.50.1.110 ....
20170512.06451494589513


+++++++++++++++++++++++++++++++++++++++++++++
20170512.06451494589513


EOF Nikto Report for 10.50.1.110 ...
20170512.06451494589513



---------------------------------------------
---------------------------------------------
End Completed for 10.50.1.110  Scann Report ....
END Time : 20170512.06451494589513 ..
EoFScann 10.50.1.110
```

Anexo 16 – Evidencia Vulnerabilidades 10.50.1.111

```
scann.mc1 10.50.1.111
Starting Scann Report ....
Start Time : 20170512.06451494589513 ..
-------------------------------------------

20170512.06451494589513
Ping Reachable Host 10.50.1.111 ::
PING 10.50.1.111 (10.50.1.111) 56(84) bytes of data.
64 bytes from 10.50.1.111: icmp_req=1 ttl=64 time=3.21 ms
64 bytes from 10.50.1.111: icmp_req=2 ttl=64 time=3.06 ms

--- 10.50.1.111 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 3.064/3.137/3.210/0.073 ms

20170512.06451494589515


-------------------------------------------
-------------------------------------------
-------------------------------------------
starting NMAP Scann Report ....
20170512.06451494589515


Starting Nmap 5.21 ( http://nmap.org ) at 2017-05-12 06:45 CDT
Nmap scan report for 10.50.1.111
Host is up (0.0063s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds

20170512.06451494589515


-------------------------------------------
-------------------------------------------
-------------------------------------------
 Starting Nmap ScannForce Report
20170512.06451494589515



Starting Nmap 5.21 ( http://nmap.org ) at 2017-05-12 06:45 CDT
NSE: Loaded 36 scripts for scanning.
Initiating SYN Stealth Scan at 06:45
Scanning 10.50.1.111 [1000 ports]
Discovered open port 22/tcp on 10.50.1.111
Discovered open port 80/tcp on 10.50.1.111
Completed SYN Stealth Scan at 06:45, 0.12s elapsed (1000 total ports)
Initiating Service scan at 06:45
Scanning 2 services on 10.50.1.111
Completed Service scan at 06:45, 6.01s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 10.50.1.111
Retrying OS detection (try #2) against 10.50.1.111
Initiating Traceroute at 06:45
Completed Traceroute at 06:45, 0.01s elapsed
NSE: Script scanning 10.50.1.111.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 06:45
Completed NSE at 06:45, 0.05s elapsed
NSE: Script Scanning completed.
Nmap scan report for 10.50.1.111
Host is up (0.0033s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_html-title: Index of /
```

```
1 service unrecognized despite returning data. If you know the service/version, please submit the
following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port22-TCP:V=5.21%I=7%D=5/12%Time=5915A052%P=x86_64-unknown-linux-gnu%r
SF:(NULL,29,"SSH-2\.0-OpenSSH_7\.2p2\x20Ubuntu-4ubuntu2\.1\r\n");
Device type: general purpose|WAP|broadband router
Running (JUST GUESSING) : Linux 2.6.X|2.4.X (89%)
Aggressive OS guesses: Linux 2.6.18 (CentOS 5.1, x86) (89%), Linux 2.6.18 (85%), DD-WRT v23 (Linux
2.4.34) (85%), OpenWrt Kamikaze 8.09 (Linux 2.6.25.20) (85%), Linux 2.6.15 (Ubuntu) (85%), Linux
2.6.15 - 2.6.26 (85%), Linux 2.6.23 (85%), Linux 2.6.27.21-grsec (85%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.736 days (since Thu May 11 13:06:00 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 199/tcp)
HOP RTT     ADDRESS
1   3.48 ms 10.50.1.111

Read data files from: /usr/share/nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.25 seconds
           Raw packets sent: 1072 (49.076KB) | Rcvd: 1034 (42.772KB)
20170512.06451494589526


-------------------------------------------
-------------------------------------------
.........................................
20170512.06451494589526


NCat check ports Version ProcServer ::
nc 10.50.1.111 22
SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.1

nc 10.50.1.111 80
Nikto Report for 10.50.1.111 ....
20170512.06451494589526


+++++++++++++++++++++++++++++++++++++++++++
20170512.06451494589526


nikto -C all -h 10.50.1.111 -p 22
- Nikto v2.1.4
---------------------------------------------------------------------------
+ No web server found on 10.50.1.111:22
---------------------------------------------------------------------------
+ 0 host(s) tested
nikto -C all -h 10.50.1.111 -p 80
- Nikto v2.1.4
---------------------------------------------------------------------------
+ Target IP:          10.50.1.111
+ Target Hostname:    10.50.1.111
+ Target Port:        80
+ Start Time:         2017-05-13 06:46:09
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ OSVDB-3268: /: Directory indexing found.
+ Allowed HTTP Methods: OPTIONS, GET, HEAD, POST
+ OSVDB-3268: /./: Directory indexing found.
+ OSVDB-3268: /?mod=node&nid=some_thing&op=view: Directory indexing found.
+ OSVDB-3268: /?mod=some_thing&op=browse: Directory indexing found.
+ /./: Appending '/./' to a directory allows indexing
+ OSVDB-3268: //: Directory indexing found.
+ //: Apache on Red Hat Linux release 9 reveals the root directory listing by default if there is no
index page.
+ OSVDB-3268: /?Open: Directory indexing found.
+ OSVDB-3268: /?OpenServer: Directory indexing found.
+ OSVDB-3268: /%2e/: Directory indexing found.
+ OSVDB-576: /%2e/: Weblogic allows source code or directory listing, upgrade to v6.0 SP1 or higher.
http://www.securityfocus.com/bid/2513.
+ OSVDB-3268: /?mod=<script>alert(document.cookie)</script>&op=browse: Directory indexing found.
```

```
+ OSVDB-3268: /?sql_debug=1: Directory indexing found.
+ OSVDB-3268: ///: Directory indexing found.
+ OSVDB-3268: http://127.0.0.1:2301/ HTTP/1.0: Directory indexing found.
+ OSVDB-3268: /?PageServices: Directory indexing found.
+ OSVDB-119: /?PageServices: The remote server may allow directory listings through Web Publisher by
forcing the server to show all files via 'open directory browsing'. Web Publisher should be disabled.
CVE-1999-0269.
+ OSVDB-3268: /?wp-cs-dump: Directory indexing found.
+ OSVDB-119: /?wp-cs-dump: The remote server may allow directory listings through Web Publisher by
forcing the server to show all files via 'open directory browsing'. Web Publisher should be disabled.
CVE-1999-0269.
+ OSVDB-3268:
//////////////////////////////////////////////////////////////////////////////////////////////////////
//////////////////////////////////////////////////////////////////////////////////////////////////////
//////////////////////////////////////////////////: Directory indexing found.
+ OSVDB-3288:
//////////////////////////////////////////////////////////////////////////////////////////////////////
//////////////////////////////////////////////////////////////////////////////////////////////////////
//////////////////////////////////////////////////: Abyss 1.03 reveals directory listing when
/'s are requested.
+ OSVDB-3268: /?pattern=/etc/*&sort=name: Directory indexing found.
+ OSVDB-3268: /?D=A: Directory indexing found.
+ OSVDB-3268: /?N=D: Directory indexing found.
+ OSVDB-3268: /?S=A: Directory indexing found.
+ OSVDB-3268: /?M=A: Directory indexing found.
+ OSVDB-3268: /?\"><script>alert('Vulnerable');</script>: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-3268: /?_CONFIG[files][functions_page]=http://cirt.net/rfiinc.txt?: Directory indexing found.
+ OSVDB-3268: /?npage=-1&content_dir=http://cirt.net/rfiinc.txt?%00&cmd=ls: Directory indexing found.
+ OSVDB-3268: /?npage=1&content_dir=http://cirt.net/rfiinc.txt?%00&cmd=ls: Directory indexing found.
+ OSVDB-3268: /?show=http://cirt.net/rfiinc.txt??: Directory indexing found.
+ 6456 items checked: 0 error(s) and 33 item(s) reported on remote host
+ End Time:           2017-05-13 06:47:36 (87 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
EOF Nikto Report for 10.50.1.111 ...
20170512.06471494589656



-------------------------------------------
-------------------------------------------
End Completed for 10.50.1.111  Scann Report ....
END Time : 20170512.06471494589656 ..
EoFScann 10.50.1.111
```

Anexo 17 – Evidencia Vulnerabilidades 10.50.1.127

```
scann.mc1 10.50.1.127
Starting Scann Report ....
Start Time : 20170512.06471494589656 ..
-------------------------------------------

20170512.06471494589656
Ping Reachable Host 10.50.1.127 ::
PING 10.50.1.127 (10.50.1.127) 56(84) bytes of data.
64 bytes from 10.50.1.127: icmp_req=1 ttl=64 time=3.24 ms
64 bytes from 10.50.1.127: icmp_req=2 ttl=64 time=3.06 ms

--- 10.50.1.127 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 3.065/3.153/3.241/0.088 ms

20170512.06471494589658


-------------------------------------------
-------------------------------------------
-------------------------------------------
starting NMAP Scann Report ....
20170512.06471494589658


Starting Nmap 5.21 ( http://nmap.org ) at 2017-05-12 06:47 CDT
Nmap scan report for 10.50.1.127
Host is up (0.0062s latency).
All 1000 scanned ports on 10.50.1.127 are closed

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds

20170512.06471494589658


-------------------------------------------
-------------------------------------------
-------------------------------------------
 Starting Nmap ScannForce Report
20170512.06471494589658



Starting Nmap 5.21 ( http://nmap.org ) at 2017-05-12 06:47 CDT
NSE: Loaded 36 scripts for scanning.
Initiating SYN Stealth Scan at 06:47
Scanning 10.50.1.127 [1000 ports]
Completed SYN Stealth Scan at 06:47, 0.12s elapsed (1000 total ports)
Initiating Service scan at 06:47
Initiating OS detection (try #1) against 10.50.1.127
Initiating Traceroute at 06:47
Completed Traceroute at 06:47, 0.01s elapsed
NSE: Script scanning 10.50.1.127.
NSE: Script Scanning completed.
Nmap scan report for 10.50.1.127
Host is up (0.0050s latency).
All 1000 scanned ports on 10.50.1.127 are closed
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: storage-misc|WAP|general purpose
Running: Buffalo embedded, Linksys embedded, Linux 2.6.X
OS details: Buffalo TeraStation NAS device, Linksys WAP54G WAP, Linux 2.6.18 (CentOS 5.1, x86)
Network Distance: 1 hop

TRACEROUTE (using port 22/tcp)
HOP RTT     ADDRESS
1   3.71 ms 10.50.1.127

Read data files from: /usr/share/nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.03 seconds
           Raw packets sent: 1022 (45.634KB) | Rcvd: 1014 (41.122KB)
20170512.06471494589659
```

```
-------------------------------------------
-------------------------------------------
.........................................
20170512.06471494589659


NCat check ports Version ProcServer ::
Nikto Report for 10.50.1.127 ....
20170512.06471494589660


+++++++++++++++++++++++++++++++++++++++++++
20170512.06471494589660


EOF Nikto Report for 10.50.1.127 ...
20170512.06471494589660



-------------------------------------------
-------------------------------------------
End Completed for 10.50.1.127  Scann Report ....
END Time : 20170512.06471494589660 ..
EoFScann 10.50.1.127
```

Anexo 18 Evidencia Vulnerabilidades 10.50.1.128

```
scann.mc1 10.50.1.128
Starting Scann Report ....
Start Time : 20170512.06471494589660 ..
-------------------------------------------

20170512.06471494589660
Ping Reachable Host 10.50.1.128 ::
PING 10.50.1.128 (10.50.1.128) 56(84) bytes of data.
64 bytes from 10.50.1.128: icmp_req=1 ttl=255 time=5.91 ms
64 bytes from 10.50.1.128: icmp_req=2 ttl=255 time=5.08 ms

--- 10.50.1.128 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 5.089/5.500/5.911/0.411 ms

20170512.06471494589662


-------------------------------------------
-------------------------------------------
-------------------------------------------
starting NMAP Scann Report ....
20170512.06471494589662


Starting Nmap 5.21 ( http://nmap.org ) at 2017-05-12 06:47 CDT
Nmap scan report for 10.50.1.128
Host is up (0.0094s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
23/tcp   open  telnet
80/tcp   open  http
443/tcp  open  https
515/tcp  open  printer
631/tcp  open  ipp
9100/tcp open  jetdirect

Nmap done: 1 IP address (1 host up) scanned in 7.47 seconds

20170512.06471494589669


-------------------------------------------
-------------------------------------------
-------------------------------------------
 Starting Nmap ScannForce Report
20170512.06471494589669



Starting Nmap 5.21 ( http://nmap.org ) at 2017-05-12 06:47 CDT
NSE: Loaded 36 scripts for scanning.
Initiating SYN Stealth Scan at 06:47
Scanning 10.50.1.128 [1000 ports]
Discovered open port 21/tcp on 10.50.1.128
Discovered open port 80/tcp on 10.50.1.128
Discovered open port 23/tcp on 10.50.1.128
Discovered open port 443/tcp on 10.50.1.128
Discovered open port 515/tcp on 10.50.1.128
Discovered open port 631/tcp on 10.50.1.128
Warning: 10.50.1.128 giving up on port because retransmission cap hit (2).
Discovered open port 9100/tcp on 10.50.1.128
Completed SYN Stealth Scan at 06:47, 8.73s elapsed (1000 total ports)
Initiating Service scan at 06:47
Scanning 6 services on 10.50.1.128
Completed Service scan at 06:49, 66.75s elapsed (7 services on 1 host)
Initiating OS detection (try #1) against 10.50.1.128
Retrying OS detection (try #2) against 10.50.1.128
Initiating Traceroute at 06:49
Completed Traceroute at 06:49, 0.02s elapsed
NSE: Script scanning 10.50.1.128.
NSE: Starting runlevel 1 (of 1) scan.
```

```
Initiating NSE at 06:49
Completed NSE at 06:49, 30.10s elapsed
NSE: Script Scanning completed.
Nmap scan report for 10.50.1.128
Host is up (0.018s latency).
Not shown: 991 closed ports
PORT     STATE    SERVICE    VERSION
21/tcp   open     ftp        Brother/HP printer ftpd 1.13
|_ftp-anon: Anonymous FTP login allowed
23/tcp   open     telnet     Brother/HP printer telnetd
80/tcp   open     http       Brother/HP printer webadmin (Debut embedded httpd 1.20)
| robots.txt: has 1 disallowed entry
|_/
| html-title: Brother MFC-J6920DW
|_Requested resource was http://10.50.1.128/general/status.html
443/tcp  open     ssl/http   Brother/HP printer webadmin (Debut embedded httpd 1.20)
| robots.txt: has 1 disallowed entry
|_/
| html-title: Brother MFC-J6920DW
|_Requested resource was http://10.50.1.128/general/status.html
515/tcp  open     printer
631/tcp  open     ipp?
3325/tcp filtered unknown
5050/tcp filtered mmcc
9100/tcp open     jetdirect?
Device type: general purpose|printer|media device|WAP|firewall|phone|router
Running (JUST GUESSING) : FreeBSD 6.X (91%), HP embedded (90%), Apple iPhone OS 2.X (88%), OpenBSD 4.X
(87%), Apple embedded (87%), m0n0wall FreeBSD (86%), Nokia Symbian OS (85%), Juniper JUNOS 9.X (85%)
Aggressive OS guesses: FreeBSD 6.2-RELEASE (91%), HP LaserJet M1522nf printer (90%), Apple iPod touch
audio player (iPhone OS 2.1) (88%), OpenBSD 4.3 (87%), Apple AirPort Extreme WAP v7.3.2 (87%),
m0n0wall 1.3b11 - 1.3b15 FreeBSD-based firewall (86%), Nokia N81 mobile phone (Symbian OS) (85%),
Juniper Networks JUNOS 9.0R2.10 (85%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.830 days (since Thu May 11 10:54:35 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: Busy server or unknown class
Service Info: Device: printer

TRACEROUTE (using port 587/tcp)
HOP RTT      ADDRESS
1   10.53 ms 10.50.1.128

Read data files from: /usr/share/nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 110.47 seconds
           Raw packets sent: 1419 (64.344KB) | Rcvd: 1178 (47.996KB)
20170512.06491494589780


-------------------------------------------
-------------------------------------------
.........................................
20170512.06491494589780


NCat check ports Version ProcServer ::
nc 10.50.1.128 21
220 FTP print service:V-1.13/Use the network password for the ID if updating.

nc 10.50.1.128 23
[2J[1;1fÿûÿû————————————————————————ÿý————————————————————————ÿûÿû
————————————————————————ÿý————————————————————————nc 10.50.1.128 80
nc 10.50.1.128 443
nc 10.50.1.128 515
nc 10.50.1.128 631
nc 10.50.1.128 9100
Nikto Report for 10.50.1.128 ....
20170512.06491494589789


+++++++++++++++++++++++++++++++++++++++++++
20170512.06491494589789
```

```
nikto -C all -h 10.50.1.128 -p 21
- Nikto v2.1.4
----------------------------------------------------------------------------
+ ERROR: SKIPPORTS (nikto.conf) contains 21 -- not checking
+ 0 host(s) tested
nikto -C all -h 10.50.1.128 -p 23
- Nikto v2.1.4
----------------------------------------------------------------------------
+ No web server found on 10.50.1.128:23
----------------------------------------------------------------------------
+ 0 host(s) tested
nikto -C all -h 10.50.1.128 -p 80
- Nikto v2.1.4
----------------------------------------------------------------------------
+ Target IP:          10.50.1.128
+ Target Hostname:    10.50.1.128
+ Target Port:        80
+ Start Time:         2017-05-13 06:51:12
----------------------------------------------------------------------------
+ Server: debut/1.20
+ Root page / redirects to: /general/status.html
+ robots.txt contains 1 entry which should be manually viewed.



^C
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report# cat
IP.block.10.50.1.xServers.ReportAvailPing..SIBLOCKS | xargs -
-i -t scann.mc1 {} [K[K[K[C[C[C[C[C[C[C [K{}
[A[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C
[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C
[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C| xargs -i[1P[A
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C
[C[C[C[C| xargs -i [1P[A
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C
[C[C[C| xargs -i -[1P[A
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C
[C[C| xargs -i -t[1P[A
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C
[C| xargs -i -t [1P[A
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C
| xargs -i -t s[1P[A
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C|
xargs -i -t sc[1P[A
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C|
xargs -i -t sca[1P[A
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C|
xargs -i -t scan[C[1P[A
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C| xargs
-i -t scann[1P[A
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C| xargs -i
-t scann.[1P[A
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C| xargs -i -
t scann.m[1P[A
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C| xargs -i -t
scann.mc[1P[A
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C| xargs -i -t
scann.mc1[1P {}[A
```

```
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C| xargs -i -t
scann.mc1 [1P{}[A
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C| xargs -i -t
scann.mc1 {[1P}[A
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C| xargs -i -t
scann.mc1 {}[K[A
]0;root@swiss1: ~/salt.co/reportroot@swiss1:~/salt.co/report#
[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C| xargs -i -t scann.mc1
{}
[K[A[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C
[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[1P

[K[A[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C
[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[C[1P[1P[1P[1P[1P[1P[1P[1P[1P[1P[1P[1P[1P[1P[1P[1P[1P[1P[1P[1P[1P[1P
[1P[1P[1P[1P[1P[1P[1P[1P[1P[1P[1P[1P[1P[1P[1P[1@x[1@a[1@r[1@g[1@s[1@
[1P[1P[1P[1P[1P[1P[1@e[1@c[1@h[1@o[1@ [1@"[1@1[1@0[1@.[1@5[1@0[1@.[1@1[1@.[1@1[1@2[1@8[1@"[1@
scann.mc1 10.50.1.128
Starting Scann Report ....
Start Time : 20170512.11401494607256 ..
--------------------------------------------

20170512.11401494607256
Ping Reachable Host 10.50.1.128 ::
PING 10.50.1.128 (10.50.1.128) 56(84) bytes of data.

--- 10.50.1.128 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1999ms


20170512.11411494607268


--------------------------------------------
--------------------------------------------
--------------------------------------------
starting NMAP Scann Report ....
20170512.11411494607268


Starting Nmap 5.21 ( http://nmap.org ) at 2017-05-12 11:41 CDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -PN
Nmap done: 1 IP address (0 hosts up) scanned in 3.05 seconds

20170512.11411494607271


--------------------------------------------
--------------------------------------------
--------------------------------------------
 Starting Nmap ScannForce Report
20170512.11411494607271



Starting Nmap 5.21 ( http://nmap.org ) at 2017-05-12 11:41 CDT
NSE: Loaded 36 scripts for scanning.
Initiating SYN Stealth Scan at 11:41
Scanning 10.50.1.128 [1000 ports]
Completed SYN Stealth Scan at 11:42, 51.06s elapsed (1000 total ports)
Initiating Service scan at 11:42
Initiating OS detection (try #1) against 10.50.1.128
Retrying OS detection (try #2) against 10.50.1.128
Initiating Traceroute at 11:42
Completed Traceroute at 11:42, 9.06s elapsed
NSE: Script scanning 10.50.1.128.
NSE: Script Scanning completed.
Nmap scan report for 10.50.1.128
Host is up.
All 1000 scanned ports on 10.50.1.128 are filtered
Too many fingerprints match this host to give specific OS details

TRACEROUTE (using proto 1/icmp)
```

```
HOP RTT     ADDRESS
1   ... 30

Read data files from: /usr/share/nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 63.89 seconds
           Raw packets sent: 2138 (97.192KB) | Rcvd: 0 (0B)
20170512.11421494607335


-------------------------------------------
-------------------------------------------
.........................................
20170512.11421494607335


NCat check ports Version ProcServer ::
Nikto Report for 10.50.1.128 ....
20170512.11421494607338


++++++++++++++++++++++++++++++++++++++++++++
20170512.11421494607338


EOF Nikto Report for 10.50.1.128 ...
20170512.11421494607341



-------------------------------------------
-------------------------------------------
End Completed for 10.50.1.128  Scann Report ....
END Time : 20170512.11421494607341 ..
EoFScann 10.50.1.128
```