

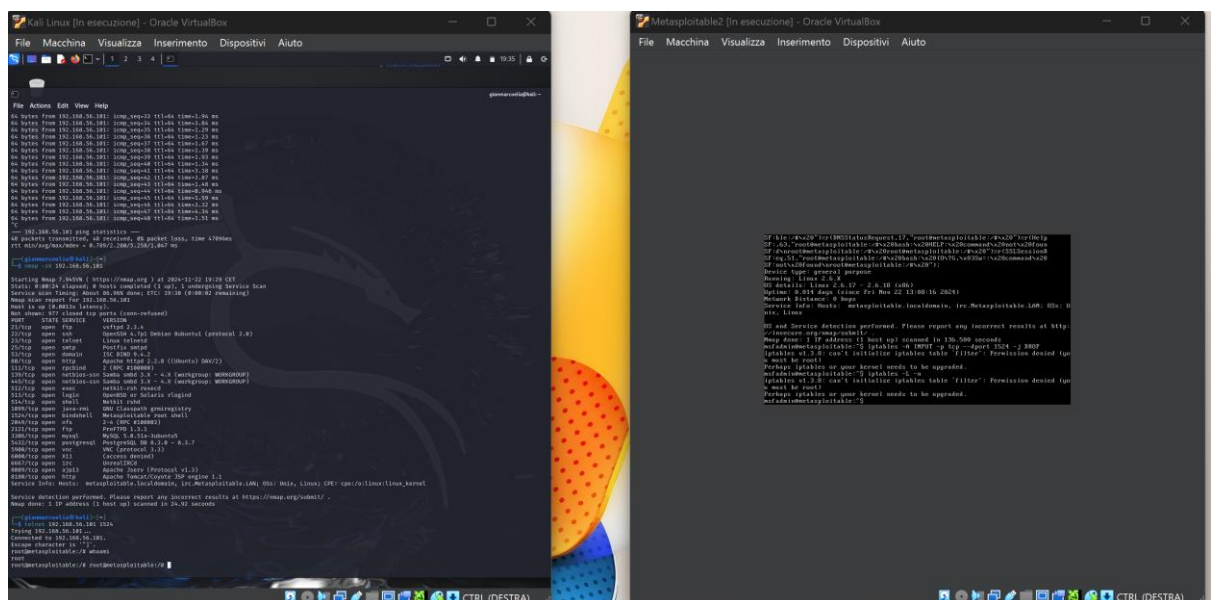
MODULO 3 – GIANMARCO ELIA

VULNERABILITA' NUMERO 1:

Servizio Telnet esposto sulla porta 1524

La vulnerabilità riguarda **il servizio Telnet esposto sulla porta 1524** su Metasploitable2. Questa vulnerabilità può essere utilizzata da un utente malintenzionato per ottenere l'accesso remoto come root senza autenticazione, sfruttando il fatto che la porta 1524 viene spesso utilizzata come "backdoor" preconfigurata.

1. Scansione iniziale con Nmap:



Durante una scansione, è stato individuato il servizio Telnet in ascolto sulla porta 1524 e Nmap ha segnalato che la porta era aperta e ha indicato il servizio.

2. Verifica della vulnerabilità:

```

OS and Service detection performed. Please report any incorrect results at http://insecure.org/nmap/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 136.500 seconds
msfadmin@metasploitable:~$ iptables -A INPUT -p tcp --dport 1524 -j DROP
iptables v1.3.8: can't initialize iptables table 'filter': Permission denied (you must be root)
Perhaps iptables or your kernel needs to be upgraded.
msfadmin@metasploitable:~$ iptables -L -n
iptables v1.3.8: can't initialize iptables table 'filter': Permission denied (you must be root)
Perhaps iptables or your kernel needs to be upgraded.
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$ sudo iptables -L
[sudo] password for msfadmin:
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

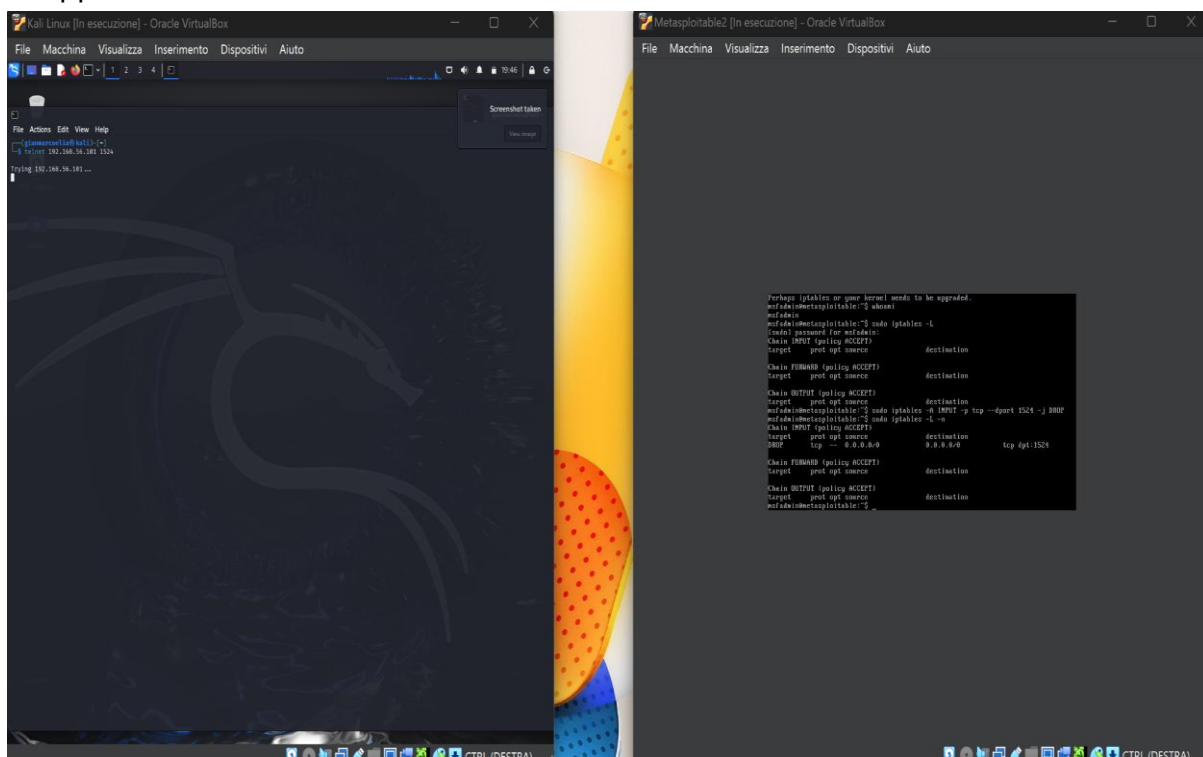
Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
msfadmin@metasploitable:~$ _

```

Ho tentato di connettermi tramite Telnet sulla porta 1524 e sono riuscito ad accedere direttamente come utente root senza password. Questo dimostra come un gray o black hacker potrebbe ottenere il controllo completo del sistema.

3. Applicazione della soluzione:



4. Verifica finale:

A screenshot of a Kali Linux terminal window running inside an Oracle VM VirtualBox. The terminal shows a user named gianmarcoelia performing a telnet connection attempt to 192.168.56.101 on port 1524, which fails with a 'Connection timed out' message. Following this, an nmap scan is executed on the same host and port. The nmap output indicates that the port is 'filtered' and the service is 'ingreslock'. The terminal window has a dark theme with a dragon watermark in the background. The VirtualBox window title is 'Kali Linux [In esecuzione] - Oracle VirtualBox' and the menu bar includes 'File', 'Macchina', 'Visualizza', 'Inserimento', 'Dispositivi', and 'Aiuto'. The system tray at the bottom shows various icons and the text 'CTRL (DESTRA)'.

Dopo aver applicato le regole del firewall, ho tentato nuovamente di connettermi a Telnet sulla porta 1524 ma la connessione è stata rifiutata, confermando che la vulnerabilità era stata mitigata con successo.

VULNERABILITA' NUMERO 2:

NFS Exported Share Information Disclosure

Questa vulnerabilità permette a un attaccante di accedere a condivisioni NFS esportate dal server, se non adeguatamente protette. Può consentire l'accesso non autorizzato a file sensibili, compromettendo l'integrità e la riservatezza del sistema.

Dettagli tecnici:

- **Servizio coinvolto:** NFS (Network File System)
- **Porta associata:** 2049
- **Strumenti utilizzati:** Nmap, comando showmount

1. Scansione della porta 2049:

```
# /srv/homes      hostname1(rw, sync) hostname2(ro, sync)
#
# Example for NFSv4:
# /srv/nfs4       gss/krb5i(rw, sync, fsid=0, crossmnt)
# /srv/nfs4/homes gss/krb5i(rw, sync)
#
#
# *(rw, sync, no_root_squash, no_subtree_check)
/home/user/shared *(rw, sync, no_root_squash, no_subtree_check)

[ Wrote 13 lines ]

msfadmin@metasploitable:~$ sudo exportfs -a
msfadmin@metasploitable:~$ sudo /etc/init.d/nfs-kernel-server restart
 * Stopping NFS kernel daemon                                [ OK ]
 * Unexporting directories for NFS kernel daemon...          [ OK ]
 * Exporting directories for NFS kernel daemon...             [ OK ]
 * Starting NFS kernel daemon                                  [ OK ]
msfadmin@metasploitable:~$
```

2. Elenco delle directory esportate

```
Kali Linux [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
gianmarcoelia@kali ~
File Actions Edit View Help
(gianmarcoelia@kali)~$ showmount -e 192.168.56.101
clnt_create: RPC: Unknown host
(gianmarcoelia@kali)~$ ping 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data:
64 bytes from 192.168.56.101: icmp_seq=1 ttl=64 time=1.58 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=64 time=0.665 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=64 time=0.655 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=64 time=0.838 ms
64 bytes from 192.168.56.101: icmp_seq=5 ttl=64 time=0.478 ms
64 bytes from 192.168.56.101: icmp_seq=6 ttl=64 time=0.687 ms
64 bytes from 192.168.56.101: icmp_seq=7 ttl=64 time=1.13 ms
64 bytes from 192.168.56.101: icmp_seq=8 ttl=64 time=0.723 ms
64 bytes from 192.168.56.101: icmp_seq=9 ttl=64 time=1.33 ms
64 bytes from 192.168.56.101: icmp_seq=10 ttl=64 time=0.780 ms
64 bytes from 192.168.56.101: icmp_seq=11 ttl=64 time=0.745 ms
64 bytes from 192.168.56.101: icmp_seq=12 ttl=64 time=0.648 ms
64 bytes from 192.168.56.101: icmp_seq=13 ttl=64 time=0.559 ms
64 bytes from 192.168.56.101: icmp_seq=14 ttl=64 time=1.59 ms
64 bytes from 192.168.56.101: icmp_seq=15 ttl=64 time=0.515 ms
64 bytes from 192.168.56.101: icmp_seq=16 ttl=64 time=0.535 ms
64 bytes from 192.168.56.101: icmp_seq=17 ttl=64 time=1.36 ms
64 bytes from 192.168.56.101: icmp_seq=18 ttl=64 time=2.74 ms
64 bytes from 192.168.56.101: icmp_seq=19 ttl=64 time=0.737 ms
64 bytes from 192.168.56.101: icmp_seq=20 ttl=64 time=0.465 ms
64 bytes from 192.168.56.101: icmp_seq=21 ttl=64 time=0.565 ms
64 bytes from 192.168.56.101: icmp_seq=22 ttl=64 time=0.630 ms
64 bytes from 192.168.56.101: icmp_seq=23 ttl=64 time=0.507 ms
64 bytes from 192.168.56.101: icmp_seq=24 ttl=64 time=0.450 ms
64 bytes from 192.168.56.101: icmp_seq=25 ttl=64 time=0.723 ms
64 bytes from 192.168.56.101: icmp_seq=26 ttl=64 time=0.470 ms
64 bytes from 192.168.56.101: icmp_seq=27 ttl=64 time=0.641 ms
64 bytes from 192.168.56.101: icmp_seq=28 ttl=64 time=0.459 ms
64 bytes from 192.168.56.101: icmp_seq=29 ttl=64 time=0.728 ms
64 bytes from 192.168.56.101: icmp_seq=30 ttl=64 time=0.519 ms
64 bytes from 192.168.56.101: icmp_seq=31 ttl=64 time=0.451 ms
^C
--- 192.168.56.101 ping statistics ---
31 packets transmitted, 31 received, 0% packet loss, time 30869ms
rtt min/avg/max/mdev = 0.450/0.803/2.742/0.474 ms
(gianmarcoelia@kali)~$ showmount -e 192.168.56.101
Export list for 192.168.56.101:
/
/home/user/shared
(gianmarcoelia@kali)~$
```

3. Montaggio delle condivisioni

```
File Macchina Visualizza Inserimento Dispositivi Aiuto
gianmarcoelia@kali: ~
File Actions Edit View Help
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.
64 bytes from 192.168.56.101: icmp_seq=1 ttl=64 time=1.58 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=64 time=0.665 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=64 time=0.655 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=64 time=0.838 ms
64 bytes from 192.168.56.101: icmp_seq=5 ttl=64 time=0.478 ms
64 bytes from 192.168.56.101: icmp_seq=6 ttl=64 time=0.687 ms
64 bytes from 192.168.56.101: icmp_seq=7 ttl=64 time=1.13 ms
64 bytes from 192.168.56.101: icmp_seq=8 ttl=64 time=0.723 ms
64 bytes from 192.168.56.101: icmp_seq=9 ttl=64 time=1.33 ms
64 bytes from 192.168.56.101: icmp_seq=10 ttl=64 time=0.780 ms
64 bytes from 192.168.56.101: icmp_seq=11 ttl=64 time=0.745 ms
64 bytes from 192.168.56.101: icmp_seq=12 ttl=64 time=0.648 ms
64 bytes from 192.168.56.101: icmp_seq=13 ttl=64 time=0.559 ms
64 bytes from 192.168.56.101: icmp_seq=14 ttl=64 time=1.59 ms
64 bytes from 192.168.56.101: icmp_seq=15 ttl=64 time=0.515 ms
64 bytes from 192.168.56.101: icmp_seq=16 ttl=64 time=0.535 ms
64 bytes from 192.168.56.101: icmp_seq=17 ttl=64 time=1.36 ms
64 bytes from 192.168.56.101: icmp_seq=18 ttl=64 time=2.74 ms
64 bytes from 192.168.56.101: icmp_seq=19 ttl=64 time=0.737 ms
64 bytes from 192.168.56.101: icmp_seq=20 ttl=64 time=0.465 ms
64 bytes from 192.168.56.101: icmp_seq=21 ttl=64 time=0.565 ms
64 bytes from 192.168.56.101: icmp_seq=22 ttl=64 time=0.630 ms
64 bytes from 192.168.56.101: icmp_seq=23 ttl=64 time=0.507 ms
64 bytes from 192.168.56.101: icmp_seq=24 ttl=64 time=0.450 ms
64 bytes from 192.168.56.101: icmp_seq=25 ttl=64 time=0.723 ms
64 bytes from 192.168.56.101: icmp_seq=26 ttl=64 time=0.470 ms
64 bytes from 192.168.56.101: icmp_seq=27 ttl=64 time=0.641 ms
64 bytes from 192.168.56.101: icmp_seq=28 ttl=64 time=0.459 ms
64 bytes from 192.168.56.101: icmp_seq=29 ttl=64 time=0.728 ms
64 bytes from 192.168.56.101: icmp_seq=30 ttl=64 time=0.519 ms
64 bytes from 192.168.56.101: icmp_seq=31 ttl=64 time=0.451 ms
^C
--- 192.168.56.101 ping statistics ---
31 packets transmitted, 31 received, 0% packet loss, time 30869ms
rtt min/avg/max/mdev = 0.450/0.803/2.742/0.474 ms

(gianmarcoelia@kali)~$ showmount -e 192.168.56.101
Export list for 192.168.56.101:
*
/home/user/shared *

(gianmarcoelia@kali)~$ sudo mkdir -p /mnt/nfs_mount
[sudo] password for gianmarcoelia:

(gianmarcoelia@kali)~$ sudo mount -t nfs 192.168.56.101:/home/user/shared /mnt/nfs_mount
Created symlink '/run/systemd/system/remote-fs.target.wants/rpc-statd.service' → '/usr/lib/systemd/system/rpc-statd.service'.

(gianmarcoelia@kali)~$ ls -la /mnt/nfs_mount
total 8
drwxr-xr-x 2 root root 4096 Nov 25 19:38 .
drwxr-xr-x 3 root root 4096 Nov 25 19:51 ..

(gianmarcoelia@kali)~$ sudo touch /mnt/nfs_mount/test_file

(gianmarcoelia@kali)~$
```

Accesso ai file nella directory esportata.

Risoluzione: Configurazione di autorizzazioni specifiche per limitare l'accesso alle condivisioni NFS a IP o sottoreti affidabili. Disattivazione delle esportazioni NFS non necessarie.

VULNERABILITA' NUMERO 3:

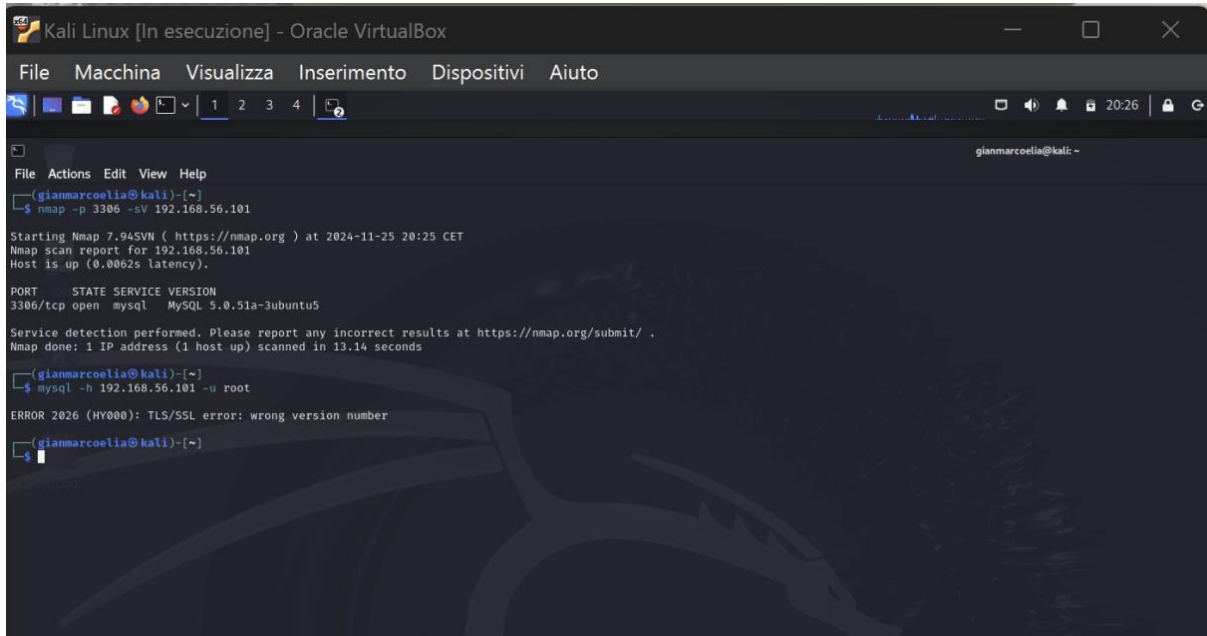
MySQL Remote Access (senza password)

Questa vulnerabilità consente l'accesso remoto al database MySQL senza autenticazione, permettendo a un attaccante di visualizzare o modificare i dati.

Dettagli tecnici:

- **Servizio coinvolto:** MySQL
- **Porta associata:** 3306
- **Strumenti utilizzati:** Nmap, client MySQL

1. Scansione della porta 3306



```
Kali Linux [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
gianmarcoelia@kali: ~
File Actions Edit View Help
(gianmarcoelia@kali)~$ nmap -p 3306 -sV 192.168.56.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-25 20:25 CET
Nmap scan report for 192.168.56.101
Host is up (0.0062s latency).

PORT      STATE SERVICE VERSION
3306/tcp  open  mysql   MySQL 5.0.51a-3ubuntu5

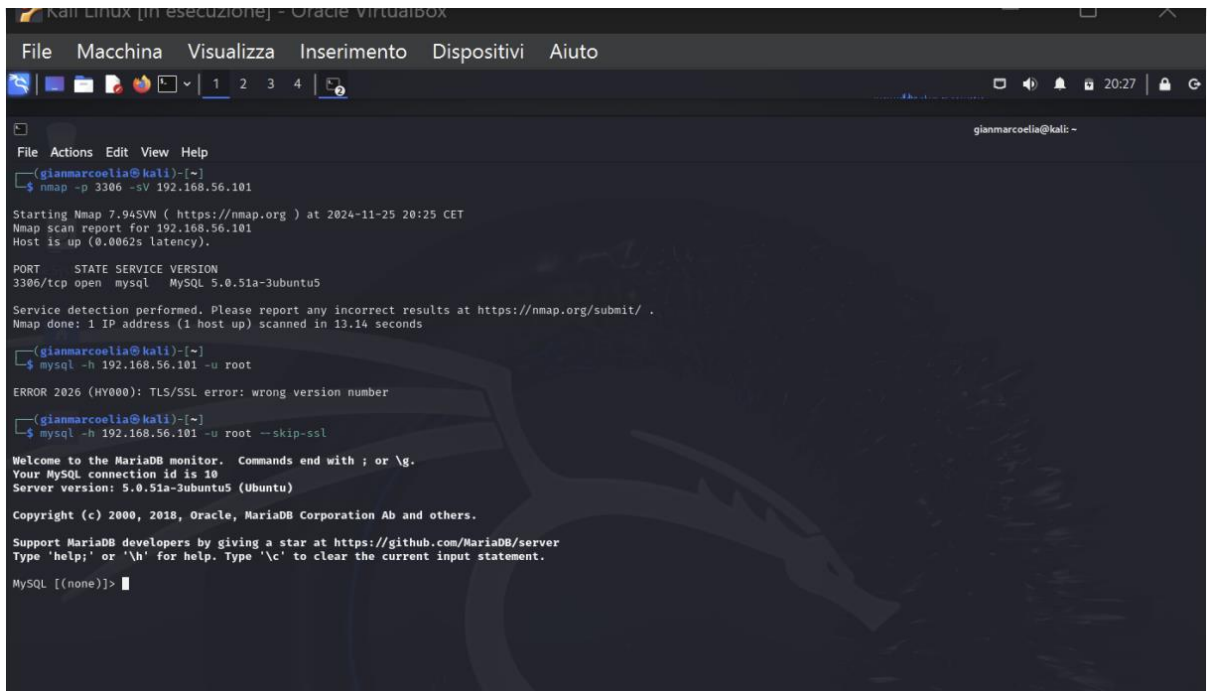
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.14 seconds

(gianmarcoelia@kali)~$ mysql -h 192.168.56.101 -u root
ERROR 2026 (HY000): TLS/SSL error: wrong version number

(gianmarcoelia@kali)~$
```

Identificazione del servizio MySQL in ascolto

2. Connessione al server MySQL senza autenticazione



```
Kali Linux [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
gianmarcoelia@kali: ~
File Actions Edit View Help
(gianmarcoelia@kali)~$ nmap -p 3306 -sV 192.168.56.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-25 20:25 CET
Nmap scan report for 192.168.56.101
Host is up (0.0062s latency).

PORT      STATE SERVICE VERSION
3306/tcp  open  mysql   MySQL 5.0.51a-3ubuntu5

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.14 seconds

(gianmarcoelia@kali)~$ mysql -h 192.168.56.101 -u root
ERROR 2026 (HY000): TLS/SSL error: wrong version number

(gianmarcoelia@kali)~$ mysql -h 192.168.56.101 -u root --skip-ssl
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 10
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>
```

Il risultato è accesso non autenticato al database MySQL.

3. Esplorazione della tabella User

Kali Linux [In esecuzione] - Oracle VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

Nessus Essentials / Vulnerabilities

My Basic Network Scan

Back to 1

Hosts Vulnerabilities History

Filter Search Vulnerabilities 34 Vulnerabilities

Severity	CVEs	VPE	EPIS	Name	Family	Count
Critical	10.0.1			NFS Exported Share Information Disclosure	RPC	1
Critical	10.0.1			VNC Server password Password	Gain a shell remotely	1
Critical	9.8			Brind Shell Backdoor Detection	Backdoors	1
Critical	7.3			Samba Badlock Vulnerability	General	1
High				ISC Bind Multiple Issues	DNS	5
High				HTTP Multiple Issues	Web Servers	5
High				Apache Tomcat Multiple Issues	Web Servers	2
High				SMB Multiple Issues	Misc	2
High	2.1.1			ICMP Timestamp Request Remote Data Disclosure	General	1
High				SMB Multiple Issues	Windows	7
High				DNS Multiple Issues	DNS	3
High				VNC Multiple Issues	Service detection	3
High				RPC Multiple Issues	RPC	2
High				Web Server Multiple Issues	Web Servers	2
High				Nessus SYN Scanner	Port Scanners	25
High				RPC Services Enumeration	Service detection	10
High				Service Detection	Service detection	8
High				Apache Karrier Linux Distribution Disclosure	Web Servers	1
High				NFS Share Export LNK	RPC	1
High				PHP Version Detection	Web Servers	1
High				PostgreSQL Server Detection	Service detection	1

Scan Details

Policy: Basic Network Scan

Status: Running

Severity Base: CVEs v3.0

Scanner: Local Scanner

Start: Today at 8:21 PM

Vulnerabilities

Legend: Critical (Red), High (Orange), Medium (Yellow), Low (Green), Info (Blue)

Five Cyber Agencies Sound Alarm About Active Dire...

Read More

Page 10 of 10

CTRL (DESTRA)