M4-Consegna week 18 day 1 – Daniele Rufo

Security Operation: azioni preventive

Considerata la traccia ho disattivato il firewall sulla macchina target (windows xp) ed effettuata una scansione con lo switch “service detection” (-sV). Ecco l’output:

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.104
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-17 12:29 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
Nmap scan report for 192.168.50.104
Host is up (0.0016s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.62 seconds

┌──(kali㉿kali)-[~]
└─$
```

La scansione è andata a buon fine e ha riportato l’elenco delle porte aperte. Con il firewall attivo invece il risultato della scansione è differente. Come si vede dallo screenschot sotto nmap non è riuscito a stabilire se le porte siano chiuse o aperte poiché “filtrate”. Questo è generalmente correlato all’azione del firewall che blocca i pacchetti in entrata e quindi non permette di verificare lo stato delle porte.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.104
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-17 12:34 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
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.20 seconds

┌──(kali㉿kali)-[~]
└─$
```

Nmap consiglia di provare una scansione con -Pn come switch per aggirare il problema. Tale opzione ipotizza che l’host sia attivo e non invia ping aspettando risposta dalla macchina target prima di cominciare la scansione….la fa partire subito in ogni caso.
Un’altra metodologia è quella di frammentazione dei pacchetti così che una volta inviati siano così piccoli da eludere la sorveglianza del firewall (switch -f per frammentare e –mtu= per scegliere la maximum transmission unit). Funzionano entrambi i metodi ed il risultato non differisce.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.50.104 -f --mtu=256
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-17 12:42 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
Nmap scan report for 192.168.50.104
Host is up (0.00099s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE      VERSION
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 08:00:27:5C:8D:1C (Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.17 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.50.104 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-17 12:44 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
Nmap scan report for 192.168.50.104
Host is up (0.00083s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE      VERSION
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 08:00:27:5C:8D:1C (Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.48 seconds
```

Diversa è la situazione invece se confrontiamo la scansione effettuata con firewall attivato e non. Queste le principali differenze riscontrate e le considerazioni:

- con firewall attivo una porta, precisamente la 445, che è dedicata ai servizi windows di condivisone SMB non è segnalata come aperta ed invece lo è. SMB può diventare facilmente un vettore di attacco.
- Le porte “not shown” con firewall attivo sono state filtrate il che vuol dire che non conosciamo esattamente lo stato della porta. Potrebbe aver rifiutato la connessione od essere rimasta silente per azione del firewall. Con firewall disattivo invece non abbiamo dubbi poiché dopo il num di port chiuso è chiaramente riportato “conn-refused” il che implica che le porte non sono state filtrate ma sono chiuse e la connessione è stata rifiutata (credo inviino un pacchetto RST per rifiutare, ma di questo non sono sicuro).

Alla fine si può dire che il firewall funziona parzialmente e andrebbe implementato con rules/policy. Se è vero che nasconde il servizio sulla porta 445 (che come detto è una vulnerabilità tra l’altro) ma la scansione ci torna lo stesso informazioni su altre porte sfruttabili per un attacco.