



COrtana  
Security

# PROGETTO SETTIMANALE

# S9/L5

*Presented by: Gabriele Arcelli, Giammarco Iorio,  
Stefano Cesaroni & Valerio Zampone*

# GIORNO 1



*Nell'esercizio di oggi vedremo come la presenza di un firewall riesca ad impattare considerevolmente sulla sicurezza di un sistema operativo. In effetti, nonostante Windows XP sia un sistema operativo piuttosto obsoleto in termini di sicurezza, la presenza di un firewall riesce comunque a limitare le azioni che un dispositivo può compiere da remoto sulla macchina e quindi ne aumenta sensibilmente la sicurezza.*



OGGETTO: Ingaggio da parte del Sig. Rossi per la messa in sicurezza rete aziendale

Il Sig. Rossi si è rivolto alla nostra azienda, la "C0rtana Security" per valutare la sicurezza della propria rete aziendale.

Il primo step sarà quello di mettere in evidenza l'importanza di un firewall, pertanto verrà mostrata la risposta del dispositivo del sig. Rossi con e senza firewall.

Il dispositivo utilizza la versione di windows XP, e perciò non risulta essere propriamente aggiornato.





FIREWALL DISATTIVATO

*Abbiamo configurato gli IP delle macchine secondo quanto segue:*

*Kali Linux : 192.168.240.100/24*

*Windows XP: 192.168.240.150/24*

*Effettueremo dei test sulla macchina windows XP con nmap prima con il firewall disattivato e poi con il firewall attivato per mettere in evidenza le implementazioni che in firewall apporta in termini di sicurezza.*



```
└─(kali㉿kali)-[~]
└─$ ping 192.168.240.150
PING 192.168.240.150 (192.168.240.150) 56(84) bytes of data.
64 bytes from 192.168.240.150: icmp_seq=1 ttl=128 time=0.736 ms
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=0.677 ms
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=0.395 ms
64 bytes from 192.168.240.150: icmp_seq=4 ttl=128 time=0.457 ms
^C
--- 192.168.240.150 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3063ms
rtt min/avg/max/mdev = 0.395/0.566/0.736/0.143 ms
```

Dalla macchina di Kali effettuiamo prima un ping per assicurarci che le macchine comunichino tra loro.



Dalla macchina di Kali effettuiamo prima una scansione dei servizi e delle relative versioni con il comando di nmap “-sV”.

```
[root@kali] ~
# nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 12:29 CEST
Nmap scan report for 192.168.240.150
Host is up (0.00027s latency).
Not shown: 997 closed tcp ports (reset)
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
MAC Address: 08:00:27:55:F3:27 (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 20.99 seconds
```

Possiamo notare che nmap ha trovato 3 porte aperte con i rispettivi servizi e versioni.

Porta 135 (msrpc): Utilizzata per le chiamate di procedura remota di Microsoft (RPC). È una porta critica per le funzionalità di rete di Windows e può essere un vettore di attacco se non adeguatamente protetta.

Porta 139 (netbios-ssn): Utilizzata dal servizio NetBIOS per sessioni di rete su TCP/IP. Tipicamente usata per condivisioni di file e stampanti.

Porta 445 (microsoft-ds): Utilizzata per la condivisione di file e stampanti tramite SMB (Server Message Block) su TCP/IP. Sostituisce la funzionalità del NetBIOS sulle reti più moderne.



Possiamo salvare direttamente i risultati ottenuti in un file di testo che chiameremo “windowsreport”; dopodichè ci spostiamo nella directory dove è contenuto il file di testo, apriamo il terminale (come root) e aggiungiamo alla scansione precedente il comando “-o” seguito dal nome del file di testo.

```
[root@kali] [/home/kali/Desktop]
# nmap -sV -o windowsreport 192.168.240.150
```

I risultati verranno inseriti e salvati direttamente all'interno del file di testo.



**FIREWALL ATTIVO**

Proviamo nuovamente ad effettuare un ping tra le due macchine; possiamo già notare delle differenze rispetto a quando il firewall era disattivato.

```
(root㉿kali)-[~/home/kali/Desktop]
# ping 192.168.240.150
PING 192.168.240.150 (192.168.240.150) 56(84) bytes of data.
^C
--- 192.168.240.150 ping statistics ---
54 packets transmitted, 0 received, 100% packet loss, time 54813ms
```

La macchina sembra essere irraggiungibile tramite ping. Possiamo ipotizzare che il firewall stia bloccando le richieste ICMP (quindi anche i pacchetti inviati da noi tramite ping).

Proviamo dunque un comando meno invasivo per provare ad aggirare il firewall e vedere se riceviamo risposta dalla macchina di windows XP: diamo in input il comando “nmap -PN” seguito dall’IP della macchina di windows XP.

```
(root㉿kali)-[~/home/kali/Desktop]
# nmap -Pn 192.168.240.150

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 14:00 CEST
Nmap scan report for 192.168.240.150
Host is up (0.00042s latency).
All 1000 scanned ports on 192.168.240.150 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:55:F3:27 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 37.83 seconds
```

Anche questa volta non siamo riusciti ad ottenere molte informazioni sulla macchina; tuttavia, ci viene restituito il MAC Address della macchina di windows XP e scopriamo anche che il sistema operativo è in esecuzione all’interno di una macchina virtuale.

Proviamo con un metodo più invasivo. Il comando “nmap -A” è il metodo di scansione più completo. Questo comando unisce in un'unica soluzione le seguenti scansioni:

- OS fingerprint: Rilevamento del sistema operativo
- Version detection: analisi delle porte aperte, servizi attivi sulle porte e relative versioni (corrispondente al comando “nmap -sV”).
- Script scanning: Raccolta informazioni aggiuntive per identificare vulnerabilità (corrispondente al comando “nmap --script=default”).
- Traceroute: tenta di identificare il percorso preso dai pacchetti per raggiungere il target (corrispondente al comando “nmap -traceroute”).

```
(root㉿kali)-[~/home/kali/Desktop]
# nmap -A 192.168.240.150

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 13:58 CEST
Nmap scan report for 192.168.240.150
Host is up (0.00037s latency).
All 1000 scanned ports on 192.168.240.150 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:55:F3:27 (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.37 ms  192.168.240.150

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 46.42 seconds
```

Otteniamo qualche informazione aggiuntiva sulla macchina, ovvero il numero di HOP (cioè quanti dispositivi di rete sono statiattraversati dai pacchetti da noi inviati) e il RTT (Tempo di andata e ritorno, cioè il tempo di risposta della macchina al pacchetto inviato).



Effettuiamo nuovamente la scansione con il comando “nmap -sV” delle porte e versione dei servizi presenti su di esse e possiamo osservare come nessuna porta sia raggiungibile.

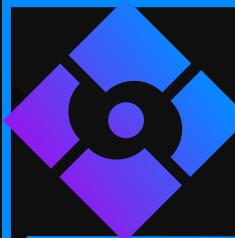
```
[root@kali]~[~/home/kali/Desktop]
# nmap -sV 192.168.240.150

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 15:19 CEST
Nmap scan report for 192.168.240.150
Host is up (0.00038s latency).
All 1000 scanned ports on 192.168.240.150 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:55:F3:27 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 38.30 seconds
```

In conclusione, possiamo affermare che il firewall incrementa sensibilmente la sicurezza di una macchina, anche se questa presenta servizi obsoleti e quindi poco sicuri, rendendo più difficile per un attaccante sfruttarne le vulnerabilità.





Cortana  
Security

## Fattura

- Costo Manodopera = 100\$/h  
 $\times 8h = 800$$
- Sopralluogo = 200 \$

Tot: 1000\$

