S9/L1

REPORT

Security Operation: azioni preventive

Presented By :
Noemi de Martino

TRACCIA

Durante questa esercitazione, abbiamo esaminato l'impatto dell'attivazione del firewall su una macchina Windows XP sui risultati di una scansione dei servizi eseguita con nmap. La macchina target aveva l'indirizzo IP 192.168.240.150, mentre la macchina Kali, utilizzata per effettuare le scansioni, aveva l'indirizzo IP 192.168.240.100.

Obiettivi dell'Esperimento

- Verificare l'effetto del firewall disattivato sulla visibilità dei servizi aperti sulla macchina Windows XP.
- Verificare l'effetto del firewall attivato sulla visibilità dei servizi aperti sulla macchina Windows XP.
- Comparare i risultati delle due scansioni per comprendere come il firewall modifichi l'accessibilità dei servizi.

SETTING DELL'AMBIENTE

- Si inizia configurando l'indirizzo ip di Kali Linux

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.240.100  netmask 255.255.255.0  broadcast 192.168.240.255
        inet6 fe80::a00:27ff:fe1e:364a  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:1e:36:4a  txqueuelen 1000  (Ethernet)
        RX packets 2  bytes 650 (650.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 57  bytes 5762 (5.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- Poi si configura l'indirizzo di WindowsXP

```
Microsoft Windows XP [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig

Configurazione IP di Windows


Scheda Ethernet Connessione alla rete locale (LAN):

        Suffisso DNS specifico per connessione:
        Indirizzo IP. . . . . . . . . . . . : 192.168.240.150
        Subnet mask . . . . . . . . . . . . : 255.255.255.0
        Gateway predefinito . . . . . . . . : 192.168.240.1
```

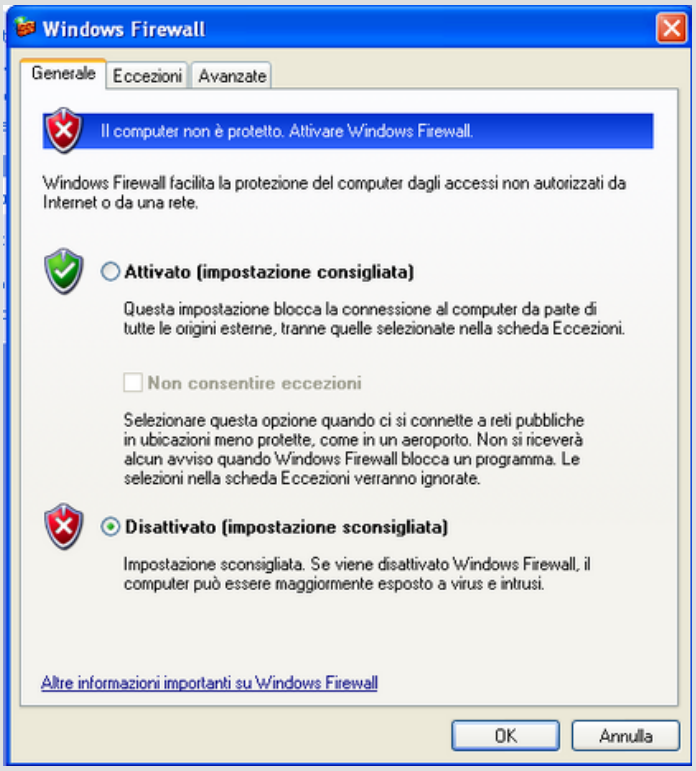
- Si verifica la comunicazione delle due macchine tramite il comando **ping**

```
┌──(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=2.16 ms
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=2.91 ms
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=2.80 ms
64 bytes from 192.168.240.150: icmp_seq=4 ttl=128 time=2.98 ms
```

SCANSIONE NMAP

CON FIREWALL DISATTIVATO

Prima di iniziare la scansione si disattiva il firewall di Windows XP tramite il Pannello di Controllo.



Lanciamo poi il comando

nmap -sV 192.168.240.150 -o nmap_scan_firewalldisattivato.txt

- **-sV:** Effettua la rilevazione dei servizi e delle versioni.
- **-o nmap_scan_firewalldisattivato.txt:** Salva l'output della scansione nel file specificato.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150 -o nmap_scan_firewalldisattivato.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-23 11:14 CEST
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 192.168.240.150
Host is up (0.0019s 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 7.40 seconds
```

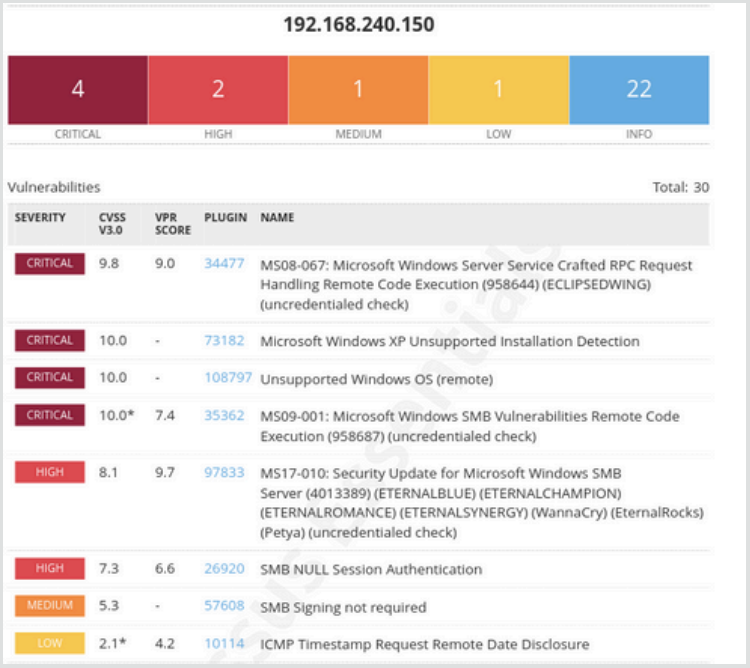
SCANSIONE NMAP

CON FIREWALL DISATTIVATO

Il risultato della scansione ci mostra che ci sono 3 porte aperte:

- **Porta 135/tcp - MSRPC (Microsoft Remote Procedure Call)**
- **Porta 139/tcp - NetBIOS Session Service**
- **Porta 445/tcp - Microsoft-DS (Directory Services)**

Per verificare la gravità delle porte aperte si è utilizzata anche il **Basic Network Scan** di Nessus.
I servizi attivi sulla porta **135** e **139** che sono rispettivamente **Microsoft RPC** e **NetBios**, sono stati segnalati come **CRITICAL.**



192.168.240.150

4	2	1	1	22
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 30

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	34477	MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING) (uncredentialed check)
CRITICAL	10.0	-	73182	Microsoft Windows XP Unsupported Installation Detection
CRITICAL	10.0	-	108797	Unsupported Windows OS (remote)
CRITICAL	10.0*	7.4	35362	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)
HIGH	8.1	9.7	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
HIGH	7.3	6.6	26920	SMB NULL Session Authentication
MEDIUM	5.3	-	57608	SMB Signing not required
LOW	2.1*	4.2	10114	ICMP Timestamp Request Remote Date Disclosure

Mentre il servizio **Microsoft DS** attivo sulla porta **445** è stato catalogato come **HIGH.**

CONSIGLI SULLA SICUREZZA

PORTA 135/TCP - MSRPC (MICROSOFT REMOTE PROCEDURE CALL)

La porta **135/tcp** è utilizzata dal servizio **RPC (Remote Procedure Call) Endpoint Mapper**. Questo servizio è fondamentale per la comunicazione tra applicazioni client e server Windows e permette di localizzare i servizi RPC su una rete.

PER METTERLA IN SICUREZZA POSSIAMO:

1. **Bloccare la Porta sul Firewall:**
   - Configurare il firewall per bloccare il traffico in entrata sulla porta **135/tcp** se non è necessario per le operazioni della rete interna.
2. **Disabilitare Servizi Non Necessari**:
   - Se i servizi **RPC** non sono necessari, disabilitarli tramite i servizi di Windows.
   - Comando: **services.msc** e disabilitare **"Remote Procedure Call (RPC) Locator"** se non richiesto.
3. **Aggiornamenti di Sicurezza**:
   - Assicurarsi che il sistema operativo e le applicazioni siano aggiornati con le ultime patch di sicurezza per prevenire vulnerabilità note.

CONSIGLI SULLA SICUREZZA

PORTA 139/TCP - NETBIOS SESSION SERVICE

La porta **139/tcp** è utilizzata dal **NetBIOS Session** Service per la condivisione di file e stampanti in reti locali Windows. Questo servizio è parte del protocollo **NetBIOS su TCP/IP** (**NetBT**).

PER METTERLA IN SICUREZZA POSSIAMO:

1. **Bloccare la Porta sul Firewall:**
   - Configurare il firewall per bloccare il traffico in entrata sulla porta **139/tcp**, specialmente per connessioni esterne. Lasciarla aperta solo per reti fidate.
2. **Disabilitare NetBIOS su TCP/IP**:
   - Disabilitare **NetBIOS** su **TCP/IP** se non necessario.
   - Passaggi: Aprire le proprietà della connessione di rete; Selezionare "**Internet Protocol** (**TCP/IP**)" e cliccare su "**Proprietà**"; Cliccare su "**Avanzate**" e selezionare la scheda "**WINS**"; Selezionare "**Disabilita NetBIOS su TCP/IP**".
3. **Utilizzare Alternative Moderne**:
   - Utilizzare protocolli più moderni e sicuri per la condivisione di file, come **SMB** su **TCP/IP** diretto tramite la porta **445/tcp**.

CONSIGLI SULLA SICUREZZA

PORTA 445/TCP - MICROSOFT-DS (DIRECTORY SERVICES)

La porta **445/tcp** è utilizzata per il servizio **SMB** (**Server Message Block**) su **TCP/IP** senza bisogno di **NetBIOS**. Questo servizio permette la condivisione di file e stampanti tra computer Windows.

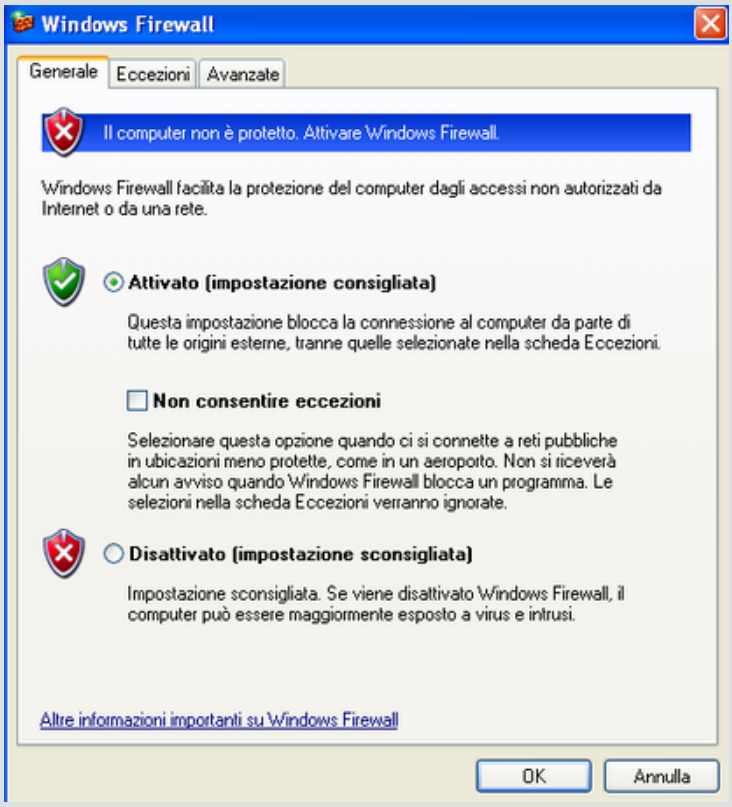
PER METTERLA IN SICUREZZA POSSIAMO:

1. **Bloccare la Porta sul Firewall:**
   - Configurare il firewall per bloccare il traffico in entrata sulla porta **445/tcp** da reti non fidate. Lasciarla aperta solo per reti interne o connessioni VPN sicure.
2. **Configurare SMB Signing e Crittografia:**
   - Abilitare **SMB signing** per autenticare le comunicazioni SMB.
   - Abilitare la **crittografia SMB** per proteggere i dati trasmessi.
3. **Aggiornamenti di Sicurezza**:
   - Assicurarsi che il sistema operativo e le applicazioni siano aggiornati con le ultime patch di sicurezza, specialmente quelle relative a **SMB** (ad esempio, patch per vulnerabilità come **EternalBlue**).
   - Disabilitare il protocollo **SMBv1**, che è obsoleto e presenta diverse vulnerabilità

SCANSIONE NMAP

CON FIREWALL ATTIVATO

Prima di eseguire nuovamente la scansione, riattiviamo il firewall di WindowsXP



Il risultato della scansione con nmap è che non è stato rilevato alcun servizio attivo o che addirittura la macchina potrebbe essere spenta.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150 -o nmap_scan_firewall.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-23 11:56 CEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify v
alid 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 3.12 seconds
```

SCANSIONE NMAP

CON FIREWALL ATTIVATO

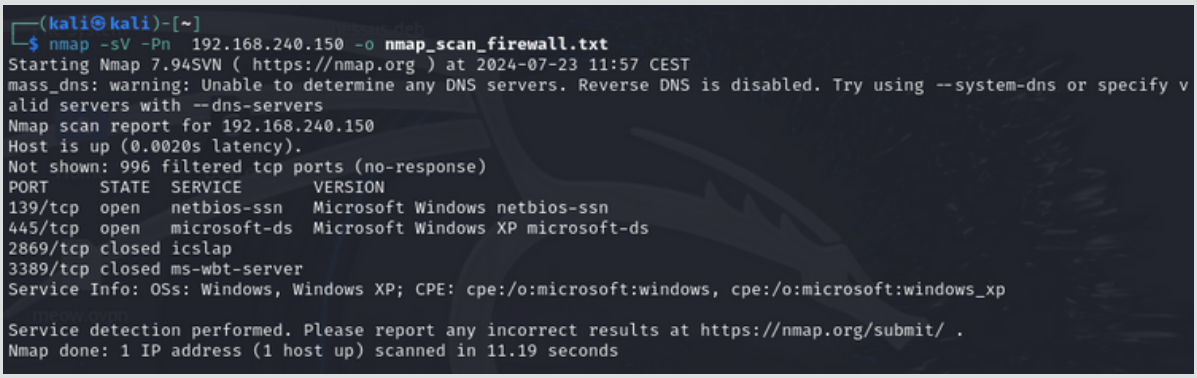
Si riprova nuovamente la scansione con il comando:

nmap -sV -Pn 192.168.240.150 -o nmap_scan_firewall.txt

Aggiungendo**:**

- **-Pn:** Questo switch disabilita la fase di ping di Nmap. Normalmente, Nmap invia un ping ICMP (come il comando ping) per vedere se l'host è attivo prima di eseguire la scansione delle porte. Con -Pn, Nmap assume che l'host sia attivo e procede direttamente alla scansione delle porte. Questo è utile quando l'host potrebbe bloccare i ping ICMP, come nel caso di un firewall attivo.

Ottiamo:



CONFRONTO

DELLE SCANSIONI

L'attivazione del firewall su Windows XP ha un impatto significativo sulla visibilità dei servizi aperti.
Con il firewall disattivato, tutti i servizi esposti sono rilevabili da nmap. Con il firewall attivato, solo alcuni servizi rimangono visibili, e solo se si bypassa la fase di ping con l'opzione -**Pn**. Questo esperimento dimostra l'importanza del firewall nella protezione della rete, limitando l'esposizione dei servizi e riducendo la superficie di attacco.

Le differenze nei risultati delle scansioni sono principalmente dovute al comportamento del firewall:

- **Blocca il traffico ICMP:**
  - Con il firewall attivato, **nmap** non riesce a determinare se l'host è attivo utilizzando ICMP, risultando in una mancata rilevazione iniziale.

- **Comportamento del comando -Pn:**
  - Ignorando la fase di ping, nmap assume che l'host sia attivo e procede con la scansione delle porte, rilevando servizi che rispondono anche con il firewall attivo.