

CS0424IT — ESERCITAZIONE S9L1
SOC: AZIONI PREVENTIVE

Simone La Porta



1 TRACCIA

Durante la lezione teorica, abbiamo studiato le azioni preventive per ridurre la possibilità di attacchi provenienti dall'esterno. Abbiamo visto che a livello di rete, possiamo attivare/configurare Firewall e regole per fare in modo che un determinato traffico, potenzialmente dannoso, venga bloccato. La macchina Windows XP che abbiamo utilizzato ha di default il Firewall disabilitato. L'esercizio di oggi è verificare in che modo l'attivazione del Firewall impatta il risultato di una scansione dei servizi dall'esterno.

Obiettivi

Verificare l'impatto dell'attivazione del Firewall su una macchina Windows XP eseguendo delle scansioni dei servizi dall'esterno.

Istruzioni

1. Assicuratevi che il Firewall sia disattivato sulla macchina Windows XP.
2. Effettuate una scansione con nmap sulla macchina target (utilizzate lo switch -sV per la service detection e -o *nomefilereport* per salvare in un file l'output).
3. Abilitare il Firewall sulla macchina Windows XP.
4. Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch -sV.
5. Trovare le eventuali differenze e motivarle.

Configurazione di rete


- Configurate l'indirizzo di Windows XP come di seguito: 192 . 168 . 240 . 150
- Configurate l'indirizzo della macchina Kali come di seguito: 192 . 168 . 240 . 100

2 SVOLGIMENTO

Configurazione di rete e verifica connettività

Windows XP

- Configurare l'indirizzo IP a 192.168.240.150 tramite il Pannello di Controllo.

A screenshot of a Windows XP Command Prompt window. The title bar is blue and says "C:\ Prompt dei comandi". The window has a black background with white text. It shows the output of the 'ipconfig' command for the Ethernet adapter. The IP address is 192.168.240.150, the subnet mask is 255.255.255.0, and the default gateway is 192.168.240.1.

```
C:\ Prompt dei comandi
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

C:\Documents and Settings\Administrator>_
```

Figura 1: Configurazione di rete Windows XP

Kali Linux

- Impostare l'indirizzo IP a 192.168.240.100.
- Riavviare l'interfaccia di rete e verificare la configurazione con `ifconfig`.

Verifica della comunicazione

- Assicurarsi che entrambe le macchine siano avviate.
- Eseguire il comando `ping` da Kali Linux verso l'indirizzo IP di Windows XP e verificare che ci sia risposta.

```
(kali㉿kali)-[~]  
$ ifconfig eth1  
eth1: 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:feea:d605 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:ea:d6:05 txqueuelen 1000 (Ethernet)  
    RX packets 87 bytes 11457 (11.1 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 42 bytes 4220 (4.1 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(kali㉿kali)-[~]  
$ ping -c 3 192.168.240.150  
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=2.25 ms  
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=1.07 ms  
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=0.533 ms  
  
— 192.168.240.150 ping statistics —  
3 packets transmitted, 3 received, 0% packet loss, time 2002ms  
rtt min/avg/max/mdev = 0.533/1.285/2.249/0.716 ms
```

Figura 2: Configurazione di rete Kali Linux e verifica connettività

Scansione Nmap con Firewall disattivato

Prima di eseguire la scansione, disattiviamo il firewall su Windows XP tramite Pannello di Controllo.

Successivamente, sulla macchina Kali, utilizziamo il comando:

```
nmap -sV 192.168.240.150 -o nome_file_output
```

Questo comando permette di verificare lo stato e la versione delle porte, salvando i risultati in un file di testo. Dopo la scansione, osserviamo che le porte 135, 139 e 445 sono aperte. Il servizio MSRPC (Microsoft Remote Procedure Call) è un protocollo di comunicazione utilizzato per permettere ai programmi di eseguire procedure su macchine remote come se fossero locali. È un'implementazione dei protocolli RPC (Remote Procedure Call) di Microsoft, che consente la comunicazione tra diverse applicazioni su una rete.

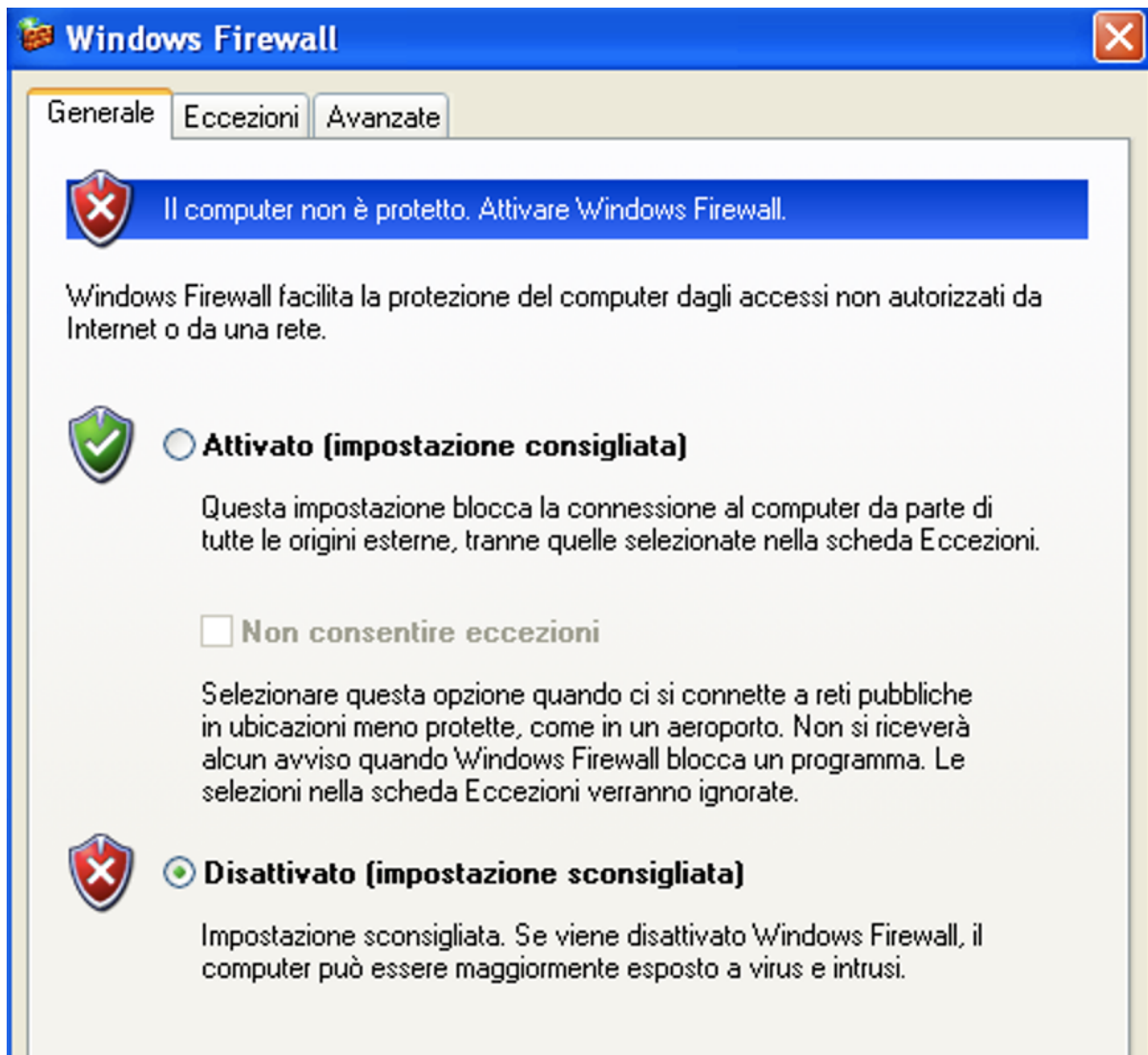


Figura 3: Disattivazione firewall Windows XP

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.240.150 -o nmap_scan_nofirewall.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 11:25 CEST
Nmap scan report for 192.168.240.150
Host is up (0.0010s 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 13.96 seconds
```

Figura 4: Scansione porte con Nmap su Windows XP con firewall disabilitato

Scansione Nessus

Abbiamo effettuato una scansione base con il tool di Vulnerability Scanning Nessus per avere una panoramica generale. Abbiamo riscontrato che i servizi attivi sulla porta 135 e 139, rispettivamente Microsoft RPC e NetBIOS, sono stati catalogati come **CRITICAL**, mentre sulla porta 445 il servizio Microsoft DS è stato catalogato come **HIGH**.

Porta 135 - MSRPC

Il servizio MSRPC (Microsoft Remote Procedure Call) è un protocollo di comunicazione utilizzato per permettere ai programmi di eseguire procedure su macchine remote come se fossero locali. È un'implementazione dei protocolli RPC (Remote Procedure Call) di Microsoft, che consente la comunicazione tra diverse applicazioni su una rete.

- **Vulnerabilità e Sicurezza**

- Exploits di Buffer Overflow: Vulnerabilità che consentono a un attaccante di eseguire codice arbitrario.
- Attacchi DoS (Denial of Service): Attacchi che possono rendere il servizio non disponibile.
- Rilevamento delle Porte: Gli attaccanti possono rilevare le porte aperte e tentare di sfruttare i servizi esposti.

- **Protezione del Servizio MSRPC**

- Firewall: Configurare correttamente i firewall per bloccare l'accesso non autorizzato.
- Aggiornamenti di Sicurezza: Applicare regolarmente patch e aggiornamenti di sicurezza.
- Autenticazione e Autorizzazione: Utilizzare meccanismi di autenticazione robusti e controllare l'accesso ai servizi.

Porta 139 - NetBIOS-SSN

NetBIOS-SSN (NetBIOS Session Service) è una delle tre componenti del protocollo NetBIOS (Network Basic Input/Output System), utilizzato per la comunicazione tra applicazioni su

diverse macchine in una rete locale (LAN). NetBIOS-SSN è specificamente responsabile della gestione delle sessioni di comunicazione tra computer.

- **Vulnerabilità e Sicurezza**

- Enumerazione di Rete: Gli attaccanti possono utilizzare strumenti per enumerare (scoprire) le risorse di rete, gli utenti e i gruppi su una rete locale.
- Accesso Non Autorizzato: Configurazioni deboli o mancanti possono permettere l'accesso non autorizzato a risorse condivise.
- Attacchi DoS (Denial of Service): Gli attaccanti possono tentare di interrompere il servizio saturando la rete con richieste.

- **Misure di Protezione**

- Firewall: Configurare il firewall per limitare l'accesso alla porta 139, consentendo solo il traffico necessario.
- Disabilitare NetBIOS su TCP/IP: Su reti moderne, può essere utile disabilitare NetBIOS su TCP/IP se non è necessario.
- Aggiornamenti di Sicurezza: Assicurarsi che tutti i sistemi siano aggiornati con le ultime patch di sicurezza.
- Configurazioni di Sicurezza: Implementare politiche di sicurezza robuste, come l'utilizzo di password complesse e l'accesso limitato alle risorse condivise.

Porta 445 - Microsoft DS

Microsoft DS (Directory Services) è un protocollo di rete utilizzato principalmente per la condivisione di file, stampanti e servizi di directory su reti basate su Windows. Si basa sul protocollo SMB (Server Message Block), che è stato sviluppato da Microsoft per facilitare la condivisione di risorse in una rete.

- **Vulnerabilità Comuni**

- Attacchi SMB: Exploit come EternalBlue, utilizzato nel ransomware WannaCry, sfruttano vulnerabilità nel protocollo SMB.

- Accesso Non Autorizzato: Configurazioni errate possono permettere accessi non autorizzati a file e risorse di rete.
- Attacchi di Forza Bruta: Gli attaccanti possono tentare di indovinare le credenziali di accesso utilizzando attacchi di forza bruta.

• Misure di Protezione

- Autenticazione: Utilizzare meccanismi di autenticazione per verificare l'identità degli utenti che accedono alle risorse condivise.
- Crittografia: Utilizzare la crittografia per proteggere i dati durante il transito.
- Firewall: Configurare correttamente i firewall per proteggere i servizi esposti sulle porte 139 e 445.
- Patch e Aggiornamenti: Applicare regolarmente patch di sicurezza e aggiornamenti per correggere vulnerabilità note.

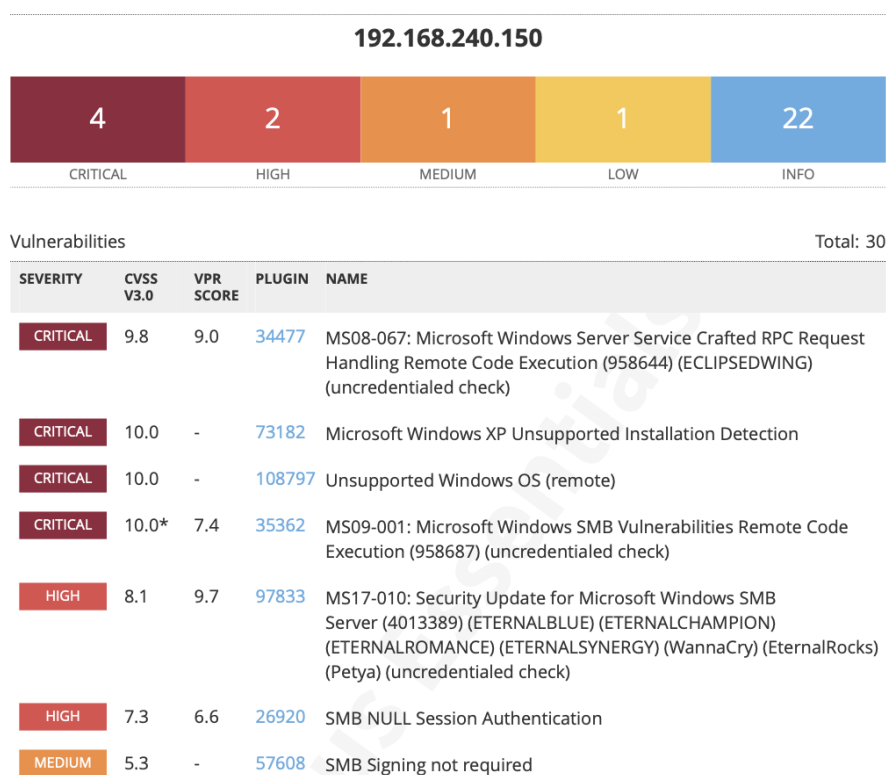


Figura 5: Scansione Nessus su Windows XP

Scansione di Windows con Firewall attivato

Prima di eseguire la scansione, attiviamo il firewall su Windows XP.

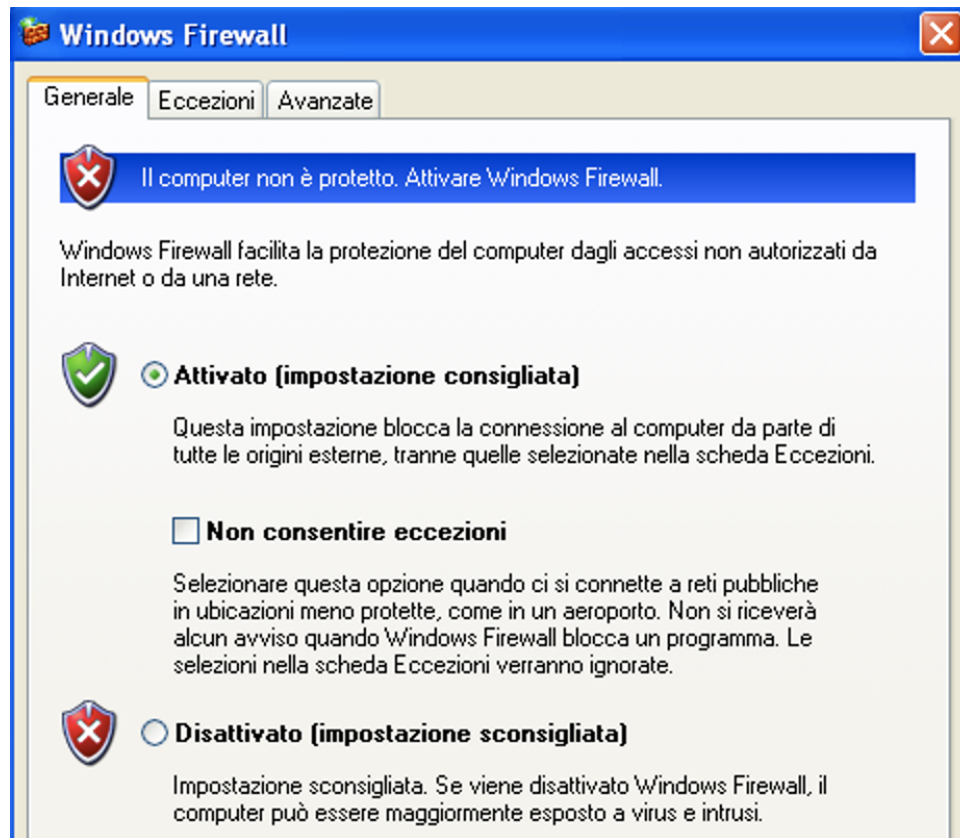


Figura 6: Attivazione Firewall Windows XP

Il risultato della scansione ci riporta che la macchina o non è accesa, oppure se è accesa sta bloccando l'host discovery di nmap. Ci consiglia quindi di provare con il parametro `-Pn`. La situazione è piuttosto chiara: il Firewall sta bloccando il traffico in entrata con protocollo ICMP (il ping).

```
(kali@kali)-[~]
$ nmap -sV 192.168.240.150 -o nmap_scan_firewall.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 11:25 CEST
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 3.15 seconds
```

Figura 7: Scansione Nmap su Windows XP con Firewall attivato

Nel report, notiamo che la macchina Kali non ha ricevuto nessuna risposta dalle porte scansionate, poiché sono filtrate dal firewall che blocca le richieste esterne.

Successivamente, avviamo un'altra scansione sulla macchina Kali utilizzando il comando:

```
nmap -sV 192.168.240.150 -Pn.
```

Parametri utilizzati:

- -sV: Effettua il rilevamento della versione dei servizi in esecuzione sulle porte aperte.
- 192.168.240.150: Specifica l'indirizzo IP del bersaglio da scansionare.
- -Pn: Disabilita il ping al bersaglio. Questo è utile quando si sospetta che il ping ICMP sia bloccato dal firewall.

```
(kali㉿kali)-[~]  
$ nmap -sV -Pn 192.168.240.150 -o nmap_scan_pn.txt  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 11:24 CEST  
Nmap scan report for 192.168.240.150  
Host is up (0.0013s 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  
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 24.44 seconds
```

Figura 8: Scansione Nmap su Windows XP con Firewall attivato e con il comando -Pn

Differenze tra le due scansioni effettuate

Nella prima scansione effettuata con il firewall disattivato sulla macchina Windows XP, è possibile eseguire liberamente una scansione dei servizi attivi sulle porte dell'IP di destinazione. Tuttavia, nella seconda scansione, attivando il firewall, si notano due principali differenze:

1. **Blocco dei Servizi Disponibili:** Il firewall blocca la scansione esterna verso i servizi disponibili, mostrando principalmente porte filtrate. Di conseguenza, non è possibile determinare quali porte siano effettivamente aperte e quali chiuse né identificare i servizi attivi su di esse.
2. **Necessità dell'Opzione -Pn:** È necessario aggiungere l'opzione -Pn per bypassare il blocco del ping ICMP, probabilmente imposto da una regola del firewall. Questo permette di proseguire con la scansione senza che il ping iniziale venga bloccato e di visualizzare lo stato dell'host attivo.

Questi cambiamenti evidenziano l'efficacia del firewall nel limitare le informazioni accessibili ai tentativi di scansione dall'esterno, migliorando la sicurezza della rete.