Traccia W18D1(1):

EPICODE

Esercizio
Le azioni preventive

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 in formato OVA che abbiamo utilizzato nella Unit 2 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. Per questo motivo:

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.

EPICODE

Esercizio
Le azioni preventive

Traccia:

Che differenze notate? E quale può essere la causa del risultato diverso?

Requisiti:

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

EPICODE

Esercizio
Le azioni preventive

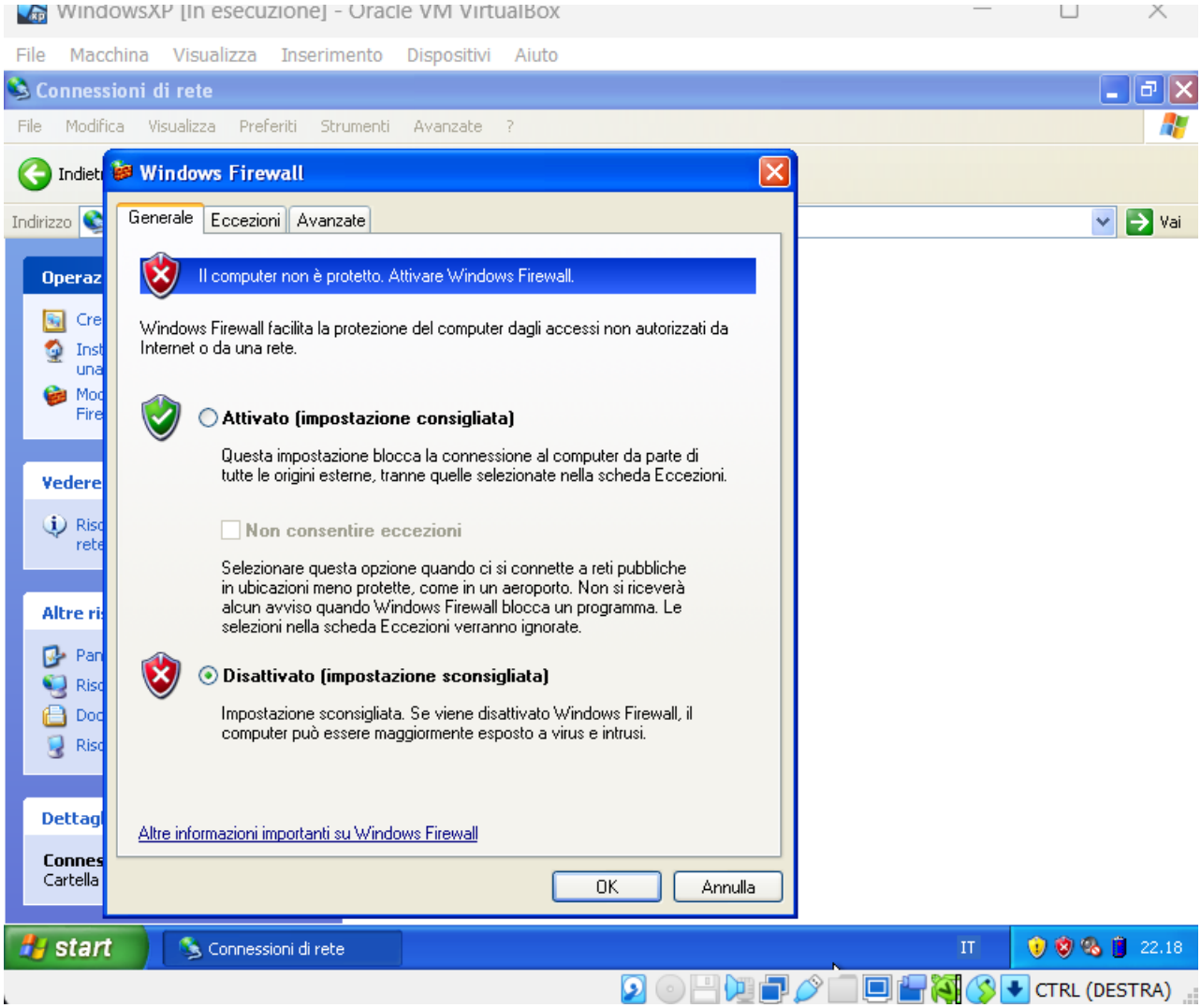
Bonus:

Monitorare i log di Windows durante queste operazioni.

1. Quali log vengono modificati? (se vengono modificati)
2. Cosa si riesce a trovare?

Soluzione:

1) Con attivazione del Firewall:


WindowsXP [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Connessioni di rete
File Modifica Visualizza Preferiti Strumenti Avanzate ?
Indietro
Indirizzo
Vai
Windows Firewall
Generale
Eccezioni
Avanzate
Il computer non è protetto. Attivare Windows Firewall.
Windows Firewall facilita la protezione del computer dagli accessi non autorizzati da Internet o da una rete.
Attivato (impostazione consigliata)
Questa impostazione blocca la connessione al computer da parte di tutte le origini esterne, tranne quelle selezionate nella scheda Eccezioni.
Non consentire eccezioni
Selezionare questa opzione quando ci si connette a reti pubbliche in ubicazioni meno protette, come in un aeroporto. Non si riceverà alcun avviso quando Windows Firewall blocca un programma. Le selezioni nella scheda Eccezioni verranno ignorate.
Disattivato (impostazione sconsigliata)
Impostazione sconsigliata. Se viene disattivato Windows Firewall, il computer può essere maggiormente esposto a virus e intrusi.
Altre informazioni importanti su Windows Firewall
OK
Annulla
Operaz
Vedere
Altre ri
Dettagl
Cartella
start
Connessioni di rete
IT
22.18
CTRL (DESTRA)

```
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ ping 192.168.50.104
PING 192.168.50.104 (192.168.50.104) 56(84) bytes of data.
64 bytes from 192.168.50.104: icmp_seq=1 ttl=128 time=1.21 ms
64 bytes from 192.168.50.104: icmp_seq=2 ttl=128 time=1.68 ms
64 bytes from 192.168.50.104: icmp_seq=3 ttl=128 time=2.05 ms
^C
── 192.168.50.104 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2006ms
rtt min/avg/max/mdev = 1.205/1.644/2.048/0.345 ms

┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.51.104 -o XP.doc
You are using a deprecated option in a dangerous way. Did you mean: -oX P.doc
QUITTING!

┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.51.104 -o WinXP.doc
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-10 17:17 EDT
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 3.58 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.104 -o WinXP.doc
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-10 17:17 EDT
Nmap scan report for 192.168.50.104
Host is up (0.0024s 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 19.54 seconds

┌──(kali㉿kali)-[~]
└─$
```

2) Con attivazione del Firewall:

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.104 -o WinXPF.doc -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-10 17:20 EDT
Nmap scan report for 192.168.50.104
Host is up.
All 1000 scanned ports on 192.168.50.104 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 217.69 seconds

┌──(kali㉿kali)-[~]
└─$
```