Report S9-L1

Security Operation: azioni preventive

Il presente report riporta un'esercitazione relativa ad una delle azioni preventive che possono essere poste in essere per tutelare le compagnie da minacce alla sicurezza: la configurazione di un Firewall.

Si parte dall'introduzione teorica, che esplica i concetti alla base dell'esercitazione, per seguire con la preparazione dell'ambiente di lavoro, tramite il settaggio degli indirizzi IP statici, e con lo svolgimento dell'esercitazione relativa all'abilitazione e disabilitazione del Firewall di Windows XP. Le rilevazioni circa l'impatto di una simile misura preventiva di sicurezza sono analizzate mediante la scansione version detection del sistema di Windows XP tramite il tool Nmap.

L'esercitazione si svolge in ambiente di lavoro virtualizzato, utilizzando la macchina Kali Linux, per la scansione delle porte e servizi, e la macchina Windows XP, per la configurazione del Firewall.

Sommario

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).

3. Abilitare il Firewall sulla macchina Windows XP.

4. Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch –sV.

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.

Introduzione

SOC (Security Operations Center)

Un SOC è un'entità organizzativa dedicata alla **gestione della sicurezza informatica**.
Si tratta di un sotto-dipartimento, all'interno del dipartimento di Sicurezza, che eroga **servizi finalizzati alla protezione dei sistemi informatici**, tra i quali sono compresi monitoraggio, analisi e risposta alle minacce alla sicurezza.
Per quanto attiene ai servizi di monitoraggio e risposta, Il SOC si occupa di sorvegliare costantemente l'ambiente infrastrutturale IT per identificare e rispondere alle minacce in tempo reale, utilizzando strumenti come sistemi di rilevamento delle intrusioni, analisi dei log, monitoraggio delle reti e altri strumenti avanzati.
Si possono identificare diverse **categorie di minacce o "incidenti":**

Minacce «avversarie»: da parte di individui, gruppi oppure organizzazioni che tentano di minare la sicurezza di una compagnia. I nemici possono essere gruppi di hacker, impiegati scontenti, competitors e così via. Si tratta quindi di un attacco esterno all'azienda oppure di un'azione volutamente dannosa proveniente dall'interno.
Minacce «strutturali o infrastrutturali»: si verificano quando un device, un asset (come un software o altro), o una componente infrastrutturale non supera determinati test.
Minacce «ambientali»: eventi di natura ambientale e tutti quegli eventi che si possono verificare che non sono sotto il controllo della compagnia.
Minacce «accidentali»: eventi che occorrono quanto un individuo, magari un impiegato della compagnia, svolgendo i suoi compiti giornalieri, esegue per errore delle azioni che possono minare la sicurezza della compagnia, come ad esempio inviare un file con informazioni confidenziali ad un indirizzo email errato.

Incidente

Termine generico in cui sono incluse tutte le casistiche di minacce elencate, comprese quelle ambientali e accidentali.

Incidente di sicurezza

È un evento che ha un impatto negativo sulla riservatezza, integrità o disponibilità di una data risorsa, come **risultato di un attacco esterno oppure di un'azione volutamente dannosa proveniente dall'interno** (ad esempio da un impiegato). Quindi l'incidente di sicurezza viene collegato ad una minaccia avversaria, esterna o interna che sia.

Azioni del SOC rispetto agli incidenti o incidenti di sicurezza

Si possono distinguere 2 tipologie di azioni adottabili dal SOC, secondo una logica temporale, al verificarsi degli incidenti.
Infatti, tali azioni sono distinguibili e classificabili in base al loro posizionamento temporale rispetto ad un incidente/incidente di sicurezza.
Azioni preventive: includono tutte quelle azioni di sicurezza che vengono adottate ed implementate anticipatamente e preventivamente per ridurre i rischi di eventi negativi**.**
Azioni correttive e di risposta agli incidenti: contiene al suo interno tutte le azioni di rimedio a stretto giro per risolvere gli incidenti e ripristinare il corretto funzionamento dei sistemi informativi quanto prima possibile

Firewall

I firewall appartengono alla categoria delle misure di sicurezza preventive rispetto al verificarsi di incidenti di sicurezza. Infatti, l'obiettivo principale dei firewall è quello di controllare e filtrare il traffico di rete, in base a un set di regole predefinite.

Ambiente di lavoro e tool

Preparazione ambiente di lavoro

Impostazione manuale Indirizzi IP statici:

Kali Linux

Si è proceduto dal terminale di Kali Linux, tramite comando **"sudo nano /etc/network/interfaces", ad usare l'editor di testo "nano"**, con privilegio amministrativo ("sudo"), per aprire e modificare il file di configurazione di rete (/etc/network/interfaces) della macchina Kali Linux.

Infatti, l'editor ha consentito di impostare il seguente indirizzo IP (address):
IP Kali: 192.168.240.100

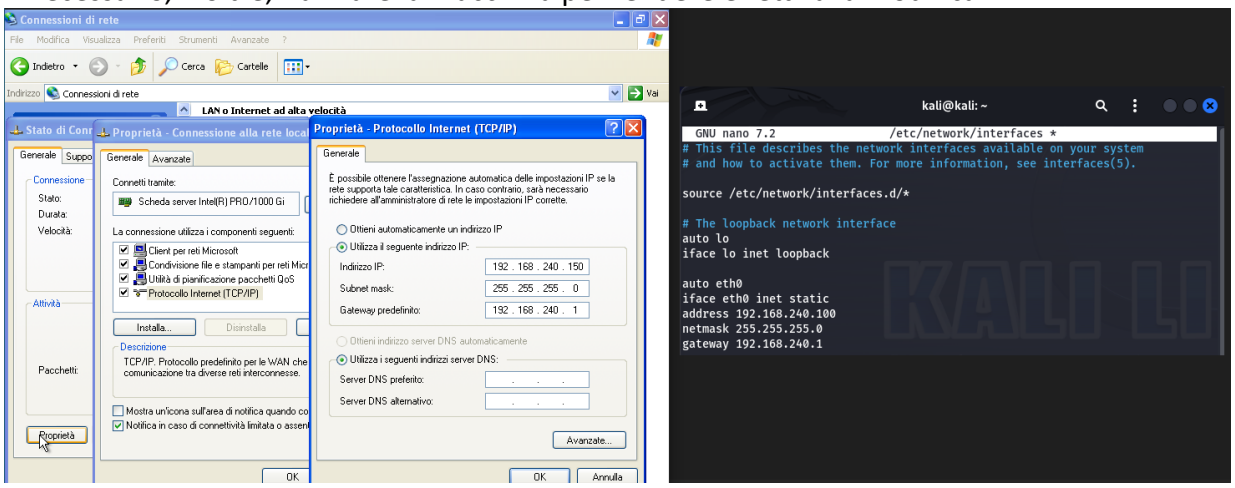
N.B. Per salvare la modifica si utilizzano le seguenti combinazioni di tasti: "**ctrl**" e "**x**" e poi "**invio**" per chiudere il file di configurazione.
È necessario, inoltre, riavviare la macchina per rendere effettiva la modifica.

Windows XP

Si è proceduto a modificare l'IP macchina, seguendo il seguente Percorso: nel menù "start", si è selezionato pannello di controllo, rete e connessione internet, connessioni di rete, dove si è cliccata l'icona della "Connessione alla rete locale (Lan)". Si è aperta, così, la finestra "stato di connessione" e si è cliccato su "Proprietà".
In "generale", cliccando su "Protocollo Internet TCP IP" si è impostato il seguente IP:

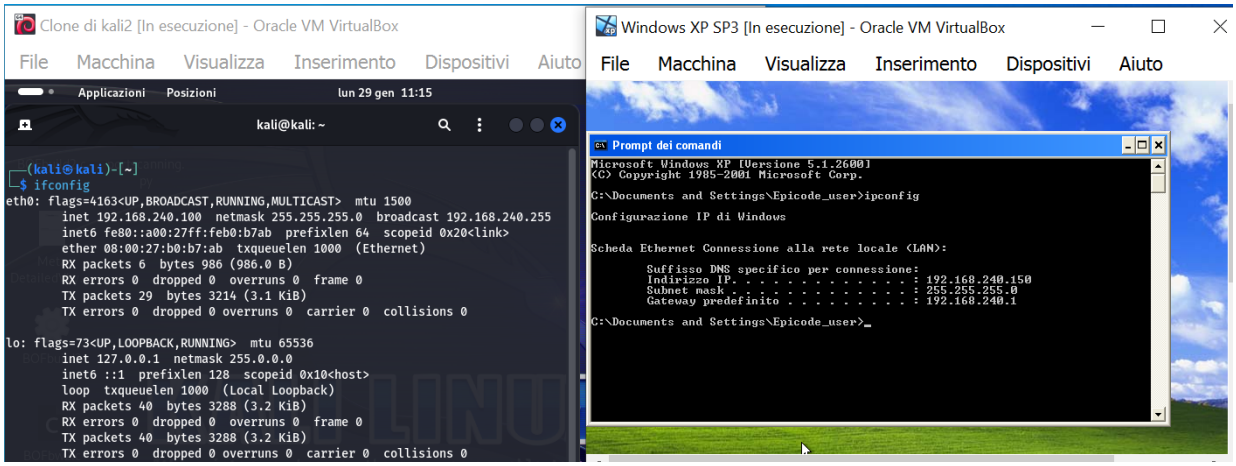
IP Windows XP: 192.168.240.150

N.B. Per salvare la modifica si preme "ok" nella pagina "Proprietà-Protocollo Internet (TCP/IP)" e nella pagina precedente "Proprietà".
È necessario, inoltre, riavviare la macchina per rendere effettiva la modifica.



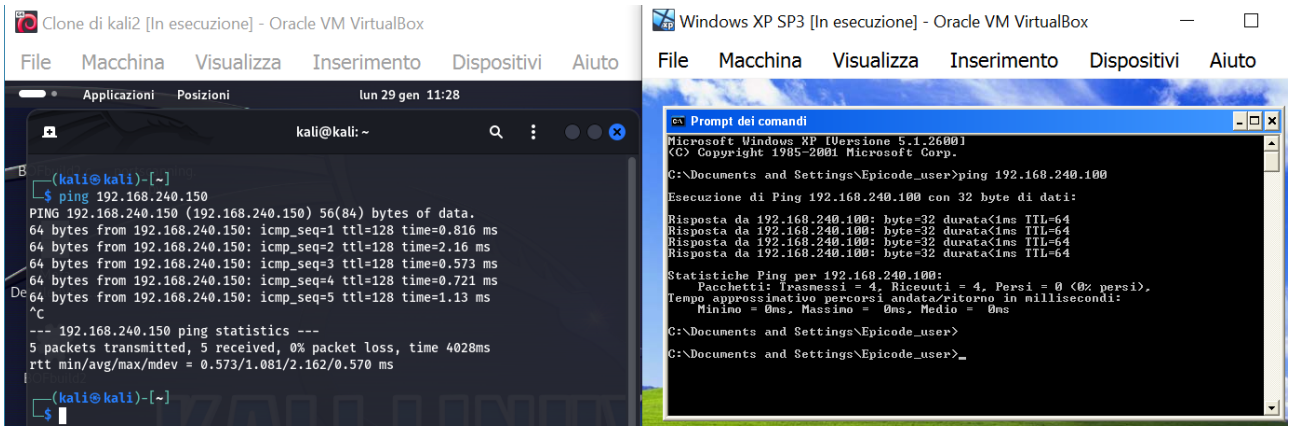
Conferma modifica IP con ifconfig e ipconfig

Successivamente, si è proceduto a confermare la modifica degli indirizzi IP lanciando, dal terminale di Kali Linux, il comando ifconfig, e dal terminale di Windows XP, il comando ipconfig.
I due comandi hanno restituito le configurazioni di rete impostate.



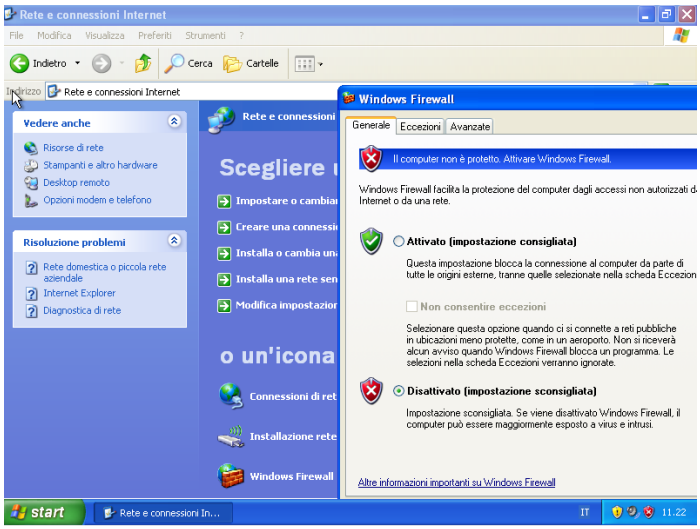
Ping

Ai fini dell'esercitazione è necessario che le due macchine, presenti nella stessa rete locale interna, comunichino fra loro.
Per testare, quindi, **la connettività di rete tra le due macchine**, si è lanciato l'utility ping, seguito dall'indirizzo IP dell'altra macchina, a seconda del terminale dal quale si faccia partire l'utility.
Le due macchine, avendo scambiato pacchetti di dati "icmp" (packets transmitted), hanno comunicato fra loro, dimostrando che le configurazioni erano state impostate correttamente.



Conferma Firewall disattivato

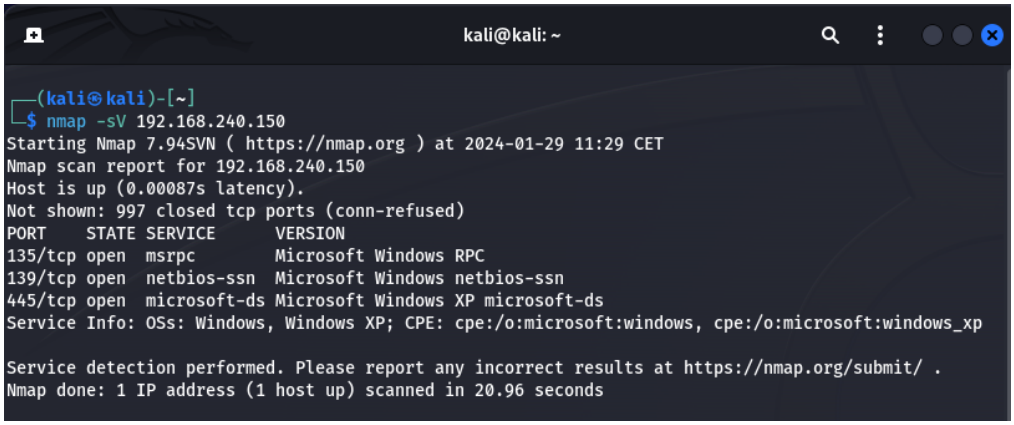
Prima di procedere allo svolgimento dell'esercizio, si è confermato che il Firewall di Windows XP fosse disattivato. Il percorso che si è seguito è stato il seguente: Dal menù "start", "pannello di controllo", "rete e connessioni Internet", "Windows Firewall". Nella finestra "generale" è stato possibile verificare che il firewall era disattivato.



1° scansione di Nmap con Firewall disattivato

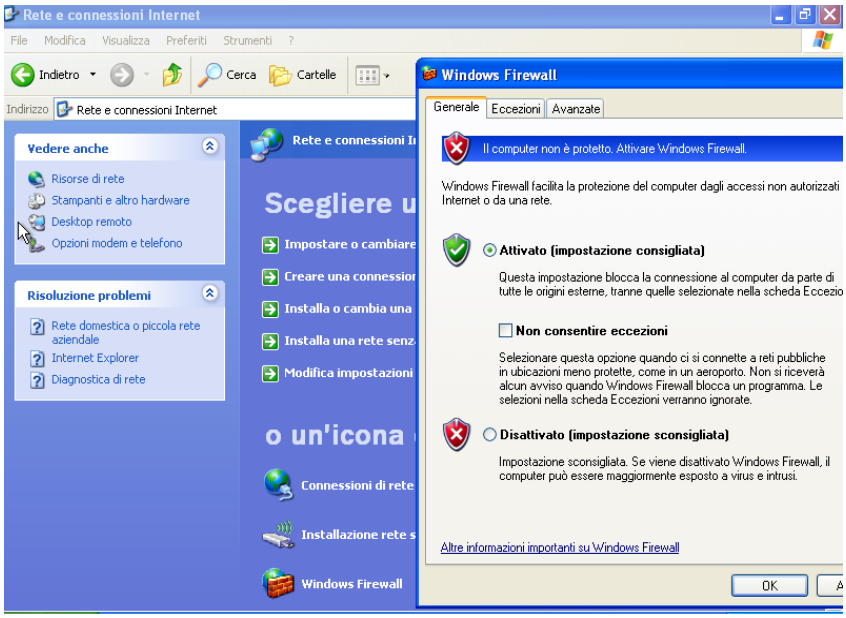
Da terminale di Kali Linux si è lanciato il tool Nmap tramite il comando **"nmap -sV 192.168.240.150".**
In questo modo, il tool ha effettuato una **scansione delle porte** sul dispositivo **Windows XP,** all'indirizzo IP 192.168.240.150, **con individuazione dei servizi completi di versione (-sV), in esecuzione sulle porte.**

L'output della scansione ha confermato che le **porte 135/tcp, 139/tcp e 445/tcp** sono **aperte e che su di esse sono in ascolto, rispettivamente, i servizi Microsoft Windows RPC, NetBIOS-SSN e Microsoft-DS** (Directory Service), suggerendo la presenza di un sistema operativo Windows o Windows XP.



Abilitazione Firewall di Windows XP

Come richiesto dalla traccia, si è proceduto ad abilitare il Firewall di Windows XP, impostando l'opzione "Attivato" nella pagina "generale" di Windows Firewall.
Si è, quindi, seguito il percorso visto in precedenza (menù "start", "pannello di controllo", "rete e connessioni Internet", "Windows Firewall").



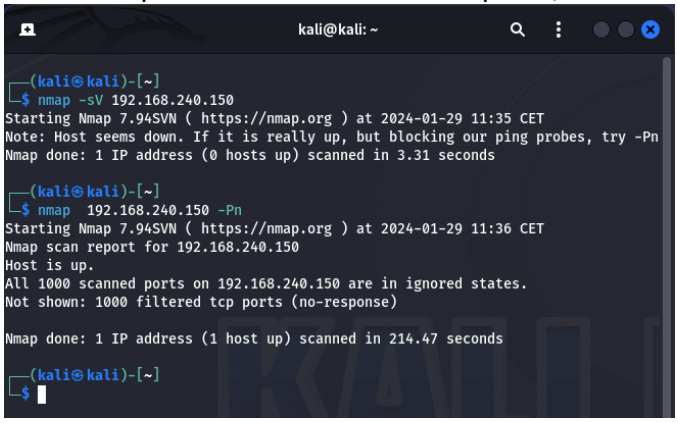
2° scansione con Nmap con Firewall abilitato

- Si è effettuata una **2° scansione** di tipo **Version Detection** del sistema **Windows XP**, lanciando nuovamente il comando **"nmap -sV 192.168.240.150".**

  L'output della scansione di Windows XP, all'indirizzo 192.168.240.150**, non restituisce lo stato delle porte e i servizi ad esse associati in quanto l'host sembra essere "giù", cioè inattivo sulla rete.** Consiglia, quindi, di utilizzare **l'opzione -Pn** per capire se l'host è attivo ma blocca i pacchetti di interrogazioni inviati da Nmap per raccogliere informazioni sulle porte e servizi durante le scansioni.

- Con il comando **"nmap -Pn 192-168.240.150**", si effettua una scansione ipotizzando che Windows XP sia attivo. In particolare, si disabilità l'utility ping, tale per cui si ignorano le evidenze legate alla ricezione e invio dei pacchetti di interrogazione alla macchina per capire se sia raggiungibile, prima di procedere alla scansione.
  In pratica, si scansiona direttamente il target, ipotizzando che sia attivo.

  L'output della scansione indica che l'host è "up", è attivo, ma tutte le 1000 porte scansionate sono in uno stato "ignorato", e vengono indicate come "filtered" con la dicitura "no-response".
  Questo indica che, nonostante l'host risponda ai sondaggi di ping (come indicato da "up"), il firewall impedisce la scansione delle porte, filtrandole**.**



Differenze tra la 1° e la 2° scansione di Nmap

Quindi nel caso della 1° scansione con Nmap, tutte le porte sono state scansionate, restituendo quelle aperte con rilevazione dei servizi ad esse associati.
Nella 2° scansione, Nmap tenta di effettuare l'host discovery, cioè inviare pacchetti con l'utility ping. Stavolta, il tool non effettua la scansione in quanto Windows XP non risponde ai pacchetti inviati.
In altri termini, Nmap conclude che l'host non è accessibile in quel momento, sulla base della mancanza di risposte ai pacchetti di tipo ping.
Quindi, con l'ultima scansione, tramite l'opzione -Pn si ignora il ping e si forza la scansione, presumendo che l'host sia attivo indipendentemente dalla risposta al ping.
In questo modo, Nmap lancia la scansione confermando che l'host di destinazione è attivo ma che le 1000 porte scansionate hanno uno status che non è possibile identificare in quanto filtrate da un dispositivo di sicurezza, ovvero il Firewall.

Conclusioni

In conclusione, nella 1° scansione Version Detection, Nmap è stato in grado di scansionare porte e servizi, restituendoli in output, in quanto Windows XP era completamente accessibile, dato che il Firewall era disattivato.

L'abilitazione del Firewall, senza prevedere nessuna eccezione alla comunicazione, filtra le connessioni alle porte e ai servizi di Windows XP, di fatto impedendo la scansione delle porte e dei servizi. In sostanza, l'host è attivo sulla rete ma è reso irraggiungibile data l'impostazione del Firewall che lo "blinda".