



S

TECH

1. PRESENTAZIONE AZIENDA
2. NOZIONI TEORICHE
3. CONFIGURAZIONE VM
4. NMAP & NESSUS SCAN
5. CONCLUSIONI

INDICE



1. Presentazione Azienda

About Us

Info

Azienda leader nel settore della sicurezza informatica, specializzata nella fornitura di soluzioni avanzate per la protezione dei dati e delle infrastrutture aziendali.

Offre servizi di consulenza, implementazione e gestione della sicurezza informatica per clienti in diversi settori, tra cui finanza, sanità, pubblica amministrazione e telecomunicazioni.

Mission statement

Protezione delle informazioni critiche e a mitigare i rischi associati alle minacce informatiche.

Ci impegniamo a fornire soluzioni personalizzate e all'avanguardia che assicurino la continuità operativa e la resilienza delle infrastrutture IT dei nostri clienti.



Vision

Garantire un futuro sicuro e affidabile per aziende e individui attraverso soluzioni di cybersecurity innovative, efficaci e accessibili.

Our values

Innovazione - Affidabilità - Integrità -
Collaborazione - Formazione continua

a



Mara Dello Russo



ZhongShiLiu



Mario Marsicano



André V.

TRACCIA

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. 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.

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

Requisiti: Configurare l'indirizzo di Windows XP come di seguito: 192.168.240.150 Configurare l'indirizzo della macchina Kali come di seguito: 192.168.240.100

2. Nozioni teoriche



FIREWALL

Un firewall è un sistema di sicurezza della rete che monitora e controlla il traffico di rete in base a regole predefinite. Funziona come una barriera tra una rete interna sicura e reti esterne non affidabili, come Internet.

Tipi di Firewall

1. Firewall a filtro di pacchetti: Analizza i pacchetti basandosi su indirizzi IP e numeri di porta.
2. Firewall a ispezione dello stato: Monitora lo stato delle connessioni attive.
3. Firewall di applicazione: Esamina il contenuto dei pacchetti per applicazioni specifiche.
4. Firewall di nuova generazione (NGFW): Combina funzionalità avanzate come ispezione approfondita dei pacchetti e prevenzione delle intrusioni.

Funzionalità Principali

- Filtraggio dei Pacchetti: Blocca o permette il traffico basato su regole.
- NAT (Network Address Translation): Nasconde gli indirizzi IP interni.
- VPN (Virtual Private Network): Crea connessioni sicure tra reti o dispositivi remoti.
- Controllo delle Applicazioni: Regola l'uso delle applicazioni sulla rete.

Vantaggi

- Protezione da accessi non autorizzati
- Monitoraggio del traffico
- Gestione delle minacce
- Implementazione di politiche di sicurezza

Limitazioni

- Non proteggono da minacce interne
- Richiedono configurazione e manutenzione costante
- Non proteggono da tutte le tipologie di attacchi

Conclusione

I firewall sono essenziali per la sicurezza di rete, ma devono essere parte di una strategia di sicurezza più ampia che include altre misure come antivirus e crittografia.



NMAP

Nmap (Network Mapper) è uno strumento di scansione delle reti utilizzato per la sicurezza informatica e l'amministrazione di rete. Permette di scoprire host e servizi su una rete, creando una mappa della rete.

Funzionalità Principali

1. Scansione degli Host: Identifica dispositivi attivi.
2. Rilevamento dei Servizi: Identifica servizi e versioni dei software in esecuzione.
3. Rilevamento del Sistema Operativo: Determina il sistema operativo degli host.
4. Scansione delle Porte: Verifica lo stato delle porte (aperte, chiuse, filtrate).
5. Nmap Scripting Engine (NSE): Esegue script per scansioni avanzate e rilevamento vulnerabilità.

Modalità di Scansione

1. TCP SYN Scan: Scansione stealth che non stabilisce una connessione completa.
2. TCP Connect Scan: Stabilisce una connessione completa, più facile da rilevare.
3. UDP Scan: Scansione delle porte UDP, più lenta.
4. ACK Scan: Determina se le porte sono filtrate o non filtrate.

Vantaggi

- Versatilità: Ampia gamma di funzionalità.
- Facilità d'Uso: Molte opzioni configurabili.
- Supporto Comunitario: Aggiornamenti regolari dalla comunità open source.

Limitazioni

- Rilevabilità: Alcune scansioni possono essere rilevate.
- Tempo di Scansione: Scansioni approfondite possono richiedere molto tempo.
- Autorizzazioni: Alcune scansioni richiedono privilegi elevati.

Conclusione

Nmap è uno strumento essenziale per la mappatura delle reti e la sicurezza informatica, utilizzato per identificare dispositivi, servizi e vulnerabilità. Deve essere utilizzato in modo etico e legale.



LA VULNERABILITA'

Una vulnerabilità è una debolezza o falla in un sistema informatico, software, hardware, o rete che può essere sfruttata da un attaccante per ottenere accesso non autorizzato, compromettere il sistema, o causare danni. Le vulnerabilità possono derivare da errori di progettazione, implementazione, configurazione o aggiornamento del sistema.

Tipi Comuni di Vulnerabilità

1. Vulnerabilità Software:

- Buffer Overflow: Eccesso di dati che supera la capacità di memoria riservata, permettendo l'esecuzione di codice arbitrario.
- SQL Injection: Inserimento di codice SQL malevolo attraverso input utente non validato, che può manipolare il database.

2. Vulnerabilità di Configurazione:

- Configurazioni Predefinite Insecure: Utilizzo di impostazioni di default che non sono sicure.
- Permessi Impropri: Assegnazione inadeguata di permessi di accesso agli utenti.

3. Vulnerabilità di Rete:

- Man-in-the-Middle (MitM): Intercettazione e alterazione del traffico tra due parti comunicanti.
- Denial of Service (DoS): Sovraccarico di un sistema con traffico eccessivo, rendendolo inaccessibile agli utenti legittimi.
-

Impatto delle Vulnerabilità

- Accesso Non Autorizzato: Gli attaccanti possono ottenere accesso a dati sensibili o sistemi interni.
- Compromissione del Sistema: Esecuzione di codice malevolo, installazione di malware.
- Perdita di Dati: Furto, alterazione o cancellazione di dati importanti.
- Interruzione dei Servizi: Rendere i servizi indisponibili o degradare le loro prestazioni.

Gestione delle Vulnerabilità

- Scansione e Monitoraggio: Utilizzo di strumenti per rilevare vulnerabilità note.
- Patch e Aggiornamenti: Applicazione regolare di patch e aggiornamenti di sicurezza.
- Configurazione Sicura: Implementazione di best practice per configurazioni sicure.
- Formazione: Educazione degli utenti e degli amministratori sulla sicurezza informatica.

Conclusione

Le vulnerabilità sono punti deboli che possono essere sfruttati per attaccare sistemi informatici. La gestione proattiva delle vulnerabilità è essenziale per mantenere la sicurezza e l'integrità dei sistemi.

3. Configurazione VM



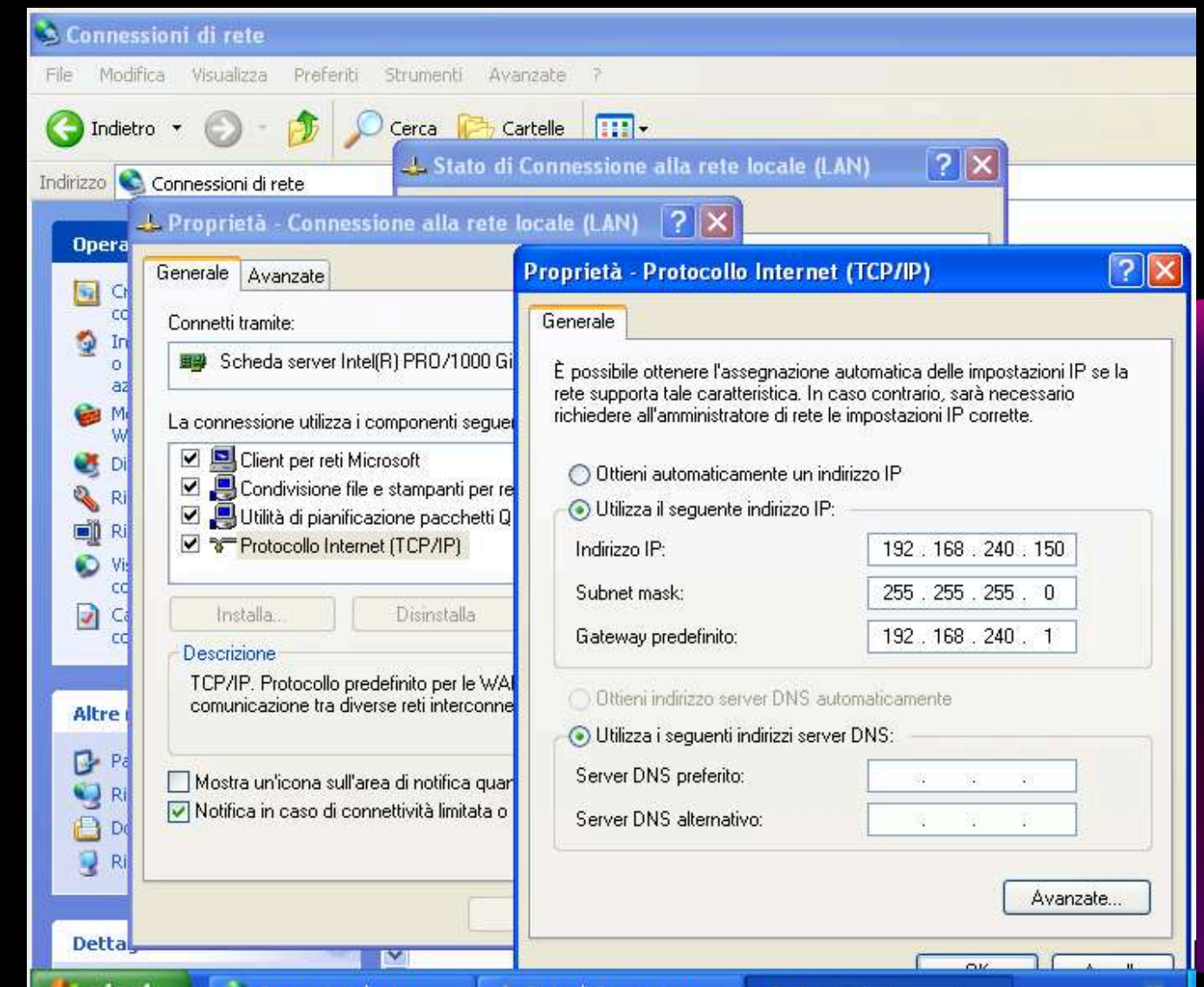
CONFIGURAZIONE IP-KALI LINUX

- **Aprire un terminale di comando:** Avviamo Kali Linux e apriamo un terminale di comando.
- **Accedere al file di configurazione di rete:** Digitiamo `sudo nano /etc/network/interfaces` e premiamo Invio. Questo comando ci permetterà di accedere al file che contiene la configurazione di rete della nostra macchina.
- **Modificare l'indirizzo IP:** Nel file che si aprirà, cerchiamo la riga che contiene l'indirizzo IP attuale. Modifichiamolo con l'indirizzo IP richiesto.
- **Salvare le modifiche:** Per salvare le modifiche, premiamo i tasti Control + O, poi premiamo Invio e per chiudere l'editor nano, premiamo i tasti Control + X.
- **Riavviare la macchina:** Digitiamo `reboot` nel terminale e premiamo Invio per riavviare la macchina.
- **Verificare la modifica dell'indirizzo IP:** Dopo il riavvio, riapriamo un terminale di comando e digitiamo `ifconfig`. Questo comando ci mostrerà la configurazione della rete attuale. Verifichiamo che l'indirizzo IP sia stato modificato correttamente.

```
kali@kali: ~  
File Actions Edit View Help  
  
(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 98 bytes 18882 (18.4 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 32 bytes 3576 (3.4 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    ether 08:00:27:63:22:35 txqueuelen 1000 (Ethernet)  
    RX packets 81 bytes 11458 (11.1 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 65 bytes 11695 (11.4 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 12 bytes 928 (928.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 12 bytes 928 (928.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

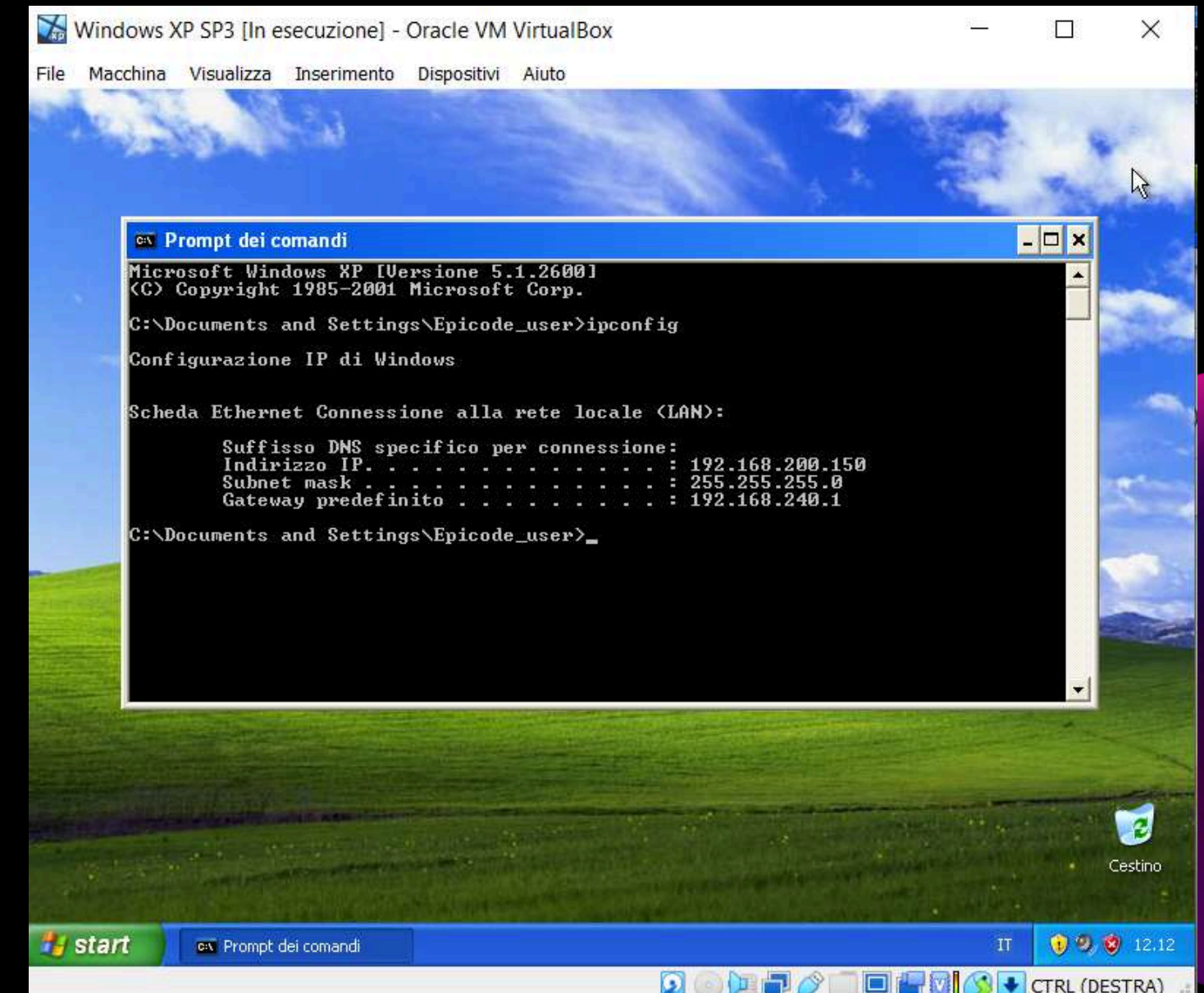

CONFIGURAZIONE IP-WINDOWS XP

- **Aprire il Pannello di Controllo:** Clicchiamo su "Start" nell'angolo in basso a sinistra del desktop e selezioniamo "Pannello di Controllo".
- **Accedere alle Connessioni di Rete:** Nel Pannello di Controllo, doppio clic su "Connessioni di rete e Internet" e quindi su "Connessioni di rete".
- **Selezionare la Connessione di Rete:** clicchiamo su "Connessione alla rete locale (LAN)" e con il tasto destro selezioniamo "Proprietà" dal menu contestuale.
- **Accedere alle Proprietà del Protocollo Internet (TCP/IP):** Nella scheda "Generale" della finestra Proprietà della connessione, scorriamo l'elenco e troviamo "Protocollo Internet (TCP/IP)", lo selezioniamo e clicchiamo su "Proprietà".
- **Modificare l'Indirizzo IP:** Nella finestra Proprietà del Protocollo Internet (TCP/IP), selezioniamo "Utilizza il seguente indirizzo IP". Questa opzione consente di inserire manualmente un indirizzo IP, una Subnet mask e un Gateway predefinito.
- **Inserire i seguenti dettagli:**
- Indirizzo IP: Inserisci l'indirizzo IP desiderato. Assicurati che l'indirizzo sia univoco e non sia già in uso nella rete.
- Subnet mask: Di solito è "255.255.255.0" per le reti locali standard, ma potrebbe variare in base alla configurazione della rete.
- Gateway predefinito: Inserisci l'indirizzo IP del router o del gateway della rete.
- **Salva le Modifiche:** Dopo aver inserito le informazioni necessarie, fai clic su "OK" per chiudere la finestra Proprietà del Protocollo Internet (TCP/IP). Fai clic su "Chiudi" nella finestra delle Proprietà della connessione di rete.



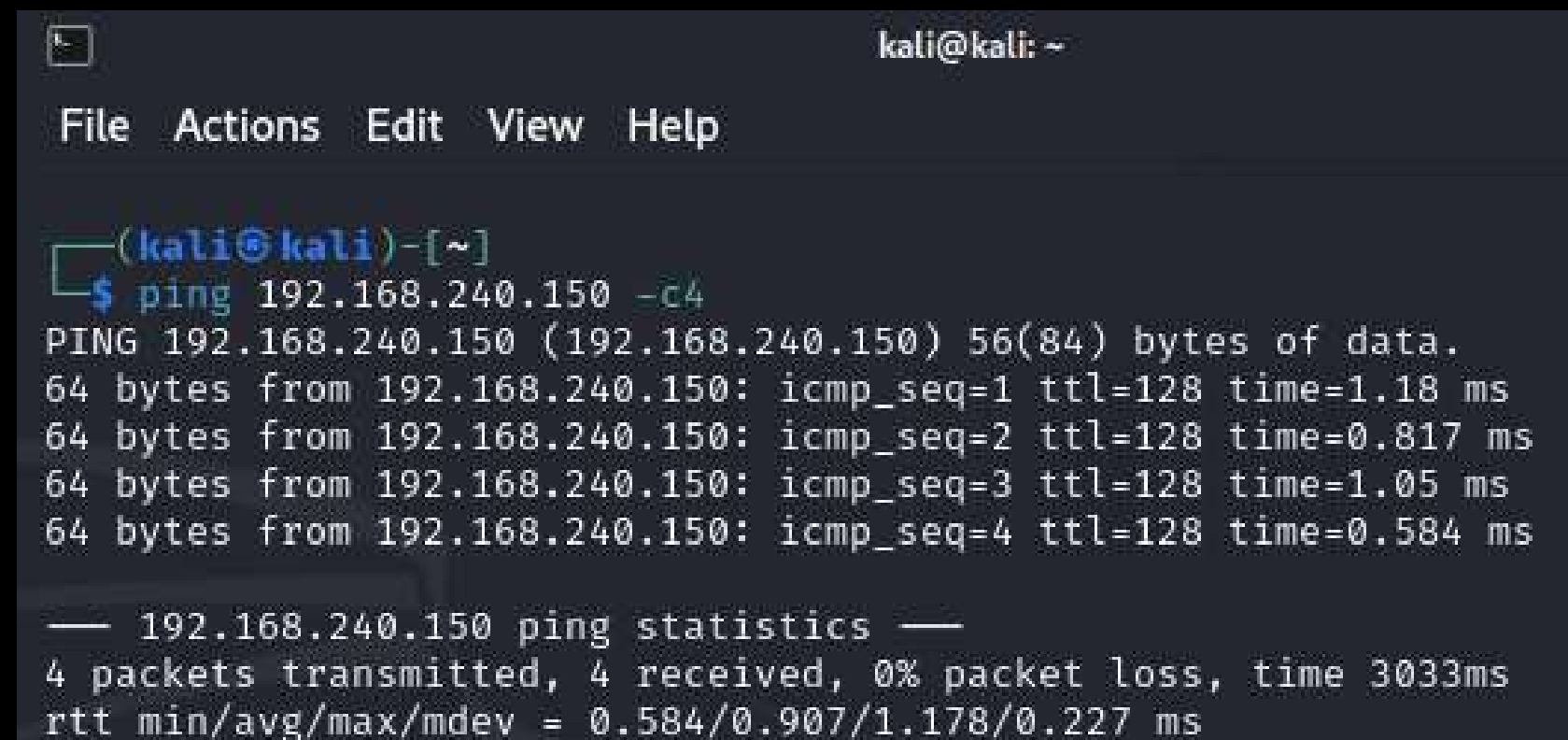
VERIFICA IP-WINDOWS XP

- **Riavviare:** Riavvia la connessione di rete o il computer per applicare le modifiche.
- **Verificare la modifica dell'indirizzo IP:** Puoi verificare l'indirizzo IP configurato aprendo il Prompt dei comandi (Start > Esegui > digita "cmd" e premi Invio) e digitando "ipconfig" seguito da Invio.



VERIFICA COMUNICAZIONE

- **Assicurarsi che entrambe le macchine siano avviate:**
Avviamo sia la macchina virtuale Kali Linux che Windows XP.
- **Eseguire il comando ping:** Apriamo un terminale su Kali Linux e digitiamo il comando ping seguito dall'indirizzo IP della macchina Metasploitable e lo switch -c4 per specificare il numero di pacchetti da inviare e premiamo invio.
- **Interpretare i risultati del ping:** Se la configurazione è corretta, vedremo una serie di righe che indicano il tempo impiegato per l'invio di ogni pacchetto, il numero di pacchetti inviati, ricevuti e persi. Se vediamo una risposta simile alla figura a destra, con il 100% dei pacchetti inviati e 0 pacchetti persi, significa che le due macchine possono comunicare correttamente tra loro.



The screenshot shows a terminal window titled 'kali@kali: ~'. The menu bar includes 'File', 'Actions', 'Edit', 'View', and 'Help'. The prompt is '(kali@kali)-[~]'. The user has entered the command '\$ ping 192.168.240.150 -c4'. The output shows four successful ping responses with varying times. Below the responses, a summary line reads: '— 192.168.240.150 ping statistics —'. The final line of output states: '4 packets transmitted, 4 received, 0% packet loss, time 3033ms' and 'rtt min/avg/max/mdev = 0.584/0.907/1.178/0.227 ms'.

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ ping 192.168.240.150 -c4  
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=1.18 ms  
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=0.817 ms  
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=1.05 ms  
64 bytes from 192.168.240.150: icmp_seq=4 ttl=128 time=0.584 ms  
  
— 192.168.240.150 ping statistics —  
4 packets transmitted, 4 received, 0% packet loss, time 3033ms  
rtt min/avg/max/mdev = 0.584/0.907/1.178/0.227 ms
```

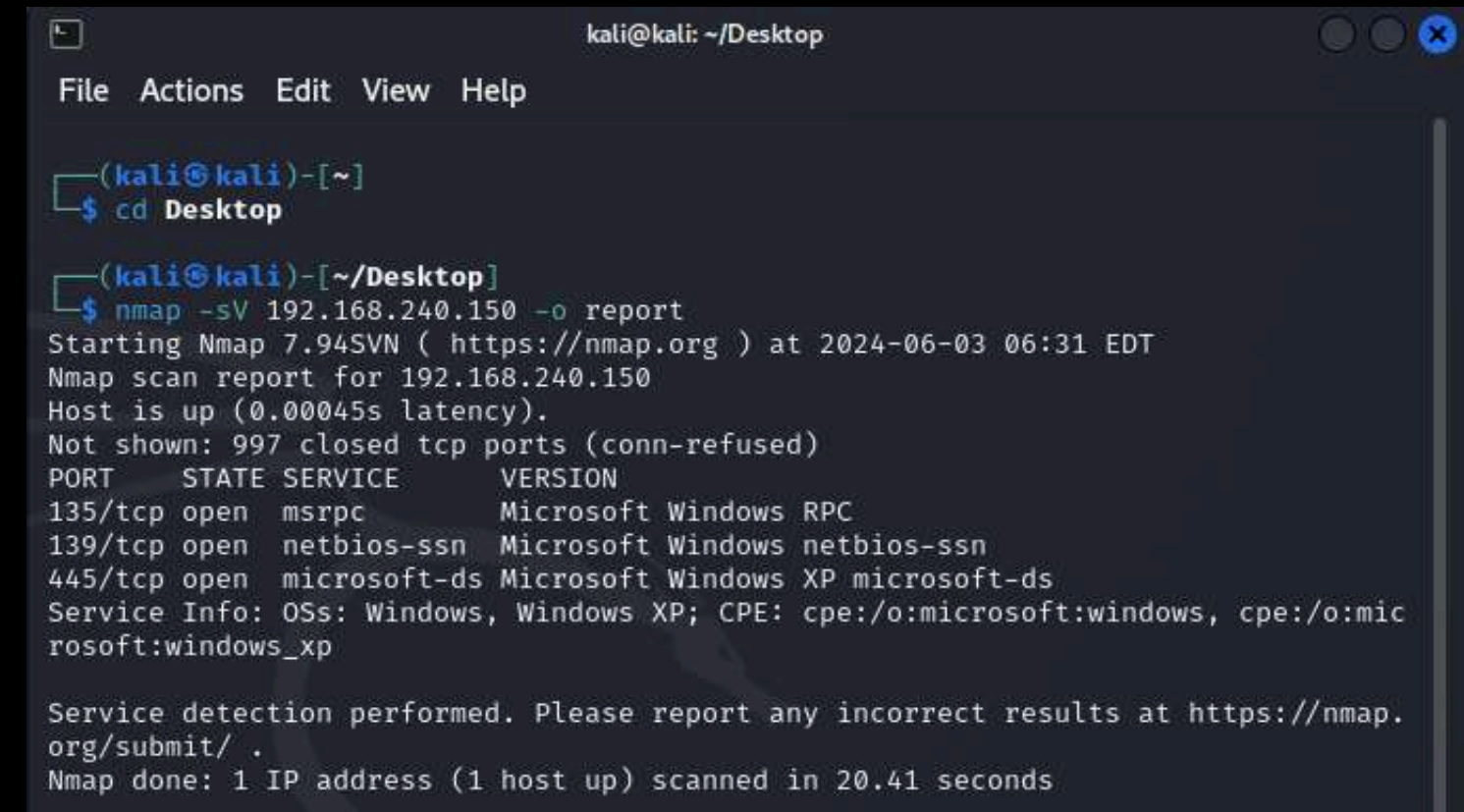
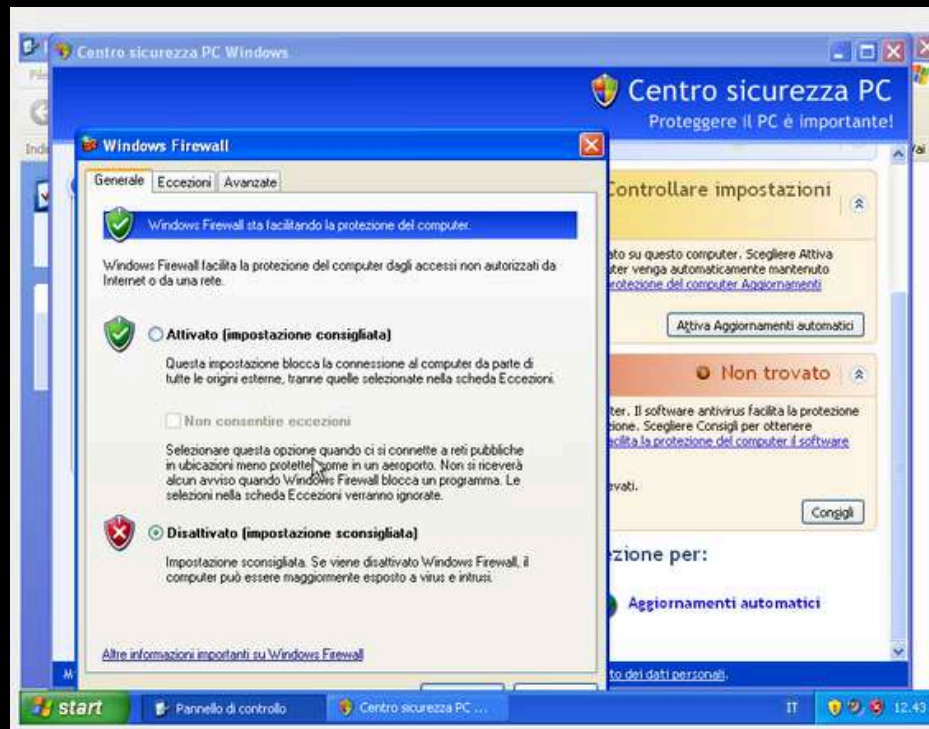
4. Nmap & Nessus scan

SCANSIONE DI WINDOWS FIREWALL DISATTIVATO

Prima di eseguire la scansione, disattiviamo il firewall su Windows XP. Successivamente, sulla macchina Kali, utilizziamo il comando:

`nmap -sV "indirizzo IP target" -oN "nome del file output"`

Questo comando permette di verificare lo stato e la versione delle porte, salvando i risultati in un file di testo.

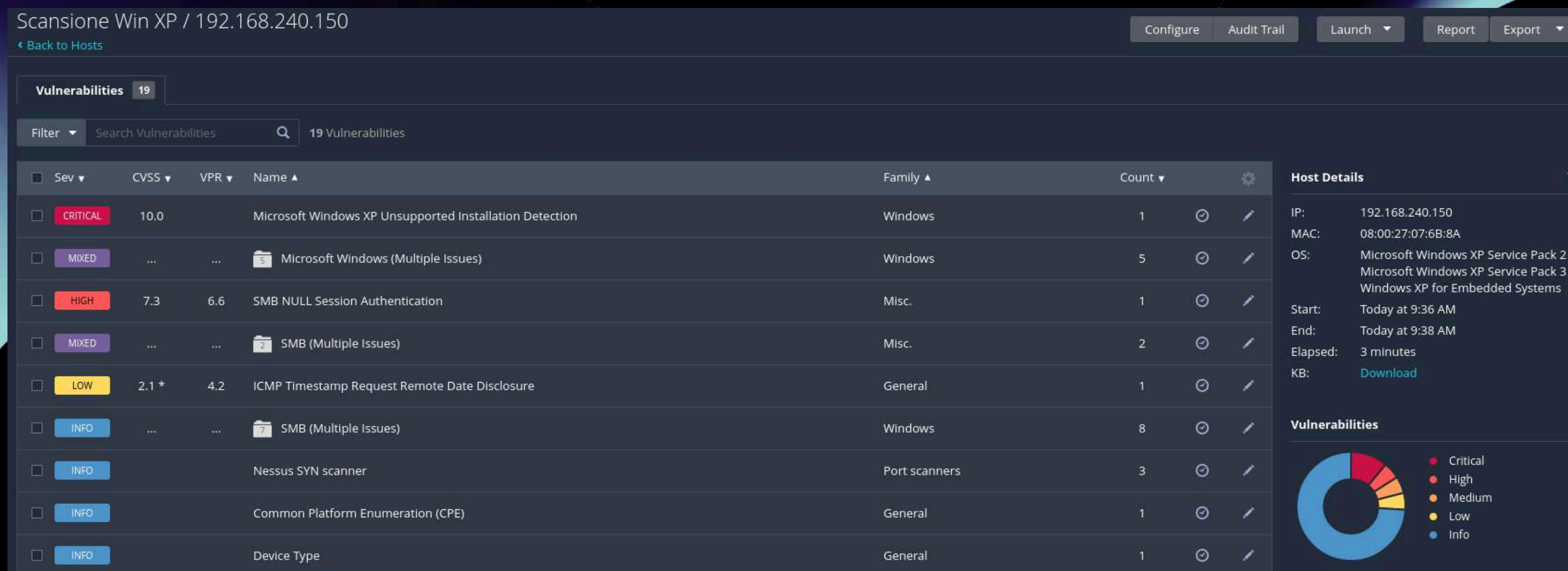


Dopo la scansione, osserviamo che le porte **135**, **139** e **445** sono **aperte**.

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 una implementazione dei protocolli RPC (Remote Procedure Call) di Microsoft, che consente la comunicazione tra diverse applicazioni su una rete.

SCANSIONE NESSUS

Abbiamo effettuato una scansione basic con il tool di Vulnerability Scanning Nessus, in modo da avere una panoramica generale ed abbiamo riscontrato che i servizi attivi sulla porta 135 e 139 , quindi rispettivamente quello di Microsoft RPC e NetBios sono stati catalogati come CRITICAL; mentre sulla porta 445 il servizio Microsoft DS è 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 una implementazione dei protocolli RPC (Remote Procedure Call) di Microsoft, che consente la comunicazione tra diverse applicazioni su una rete.

Vulnerabilità e Sicurezza

MSRPC **può essere un vettore di attacco** se non è adeguatamente protetto.

Alcuni attacchi noti includono:

- 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

NetBIOS-SSN, come altri servizi di rete, **può essere soggetto a vari tipi di attacchi** se non adeguatamente protetto:

- 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, che è stato 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.

Sicurezza

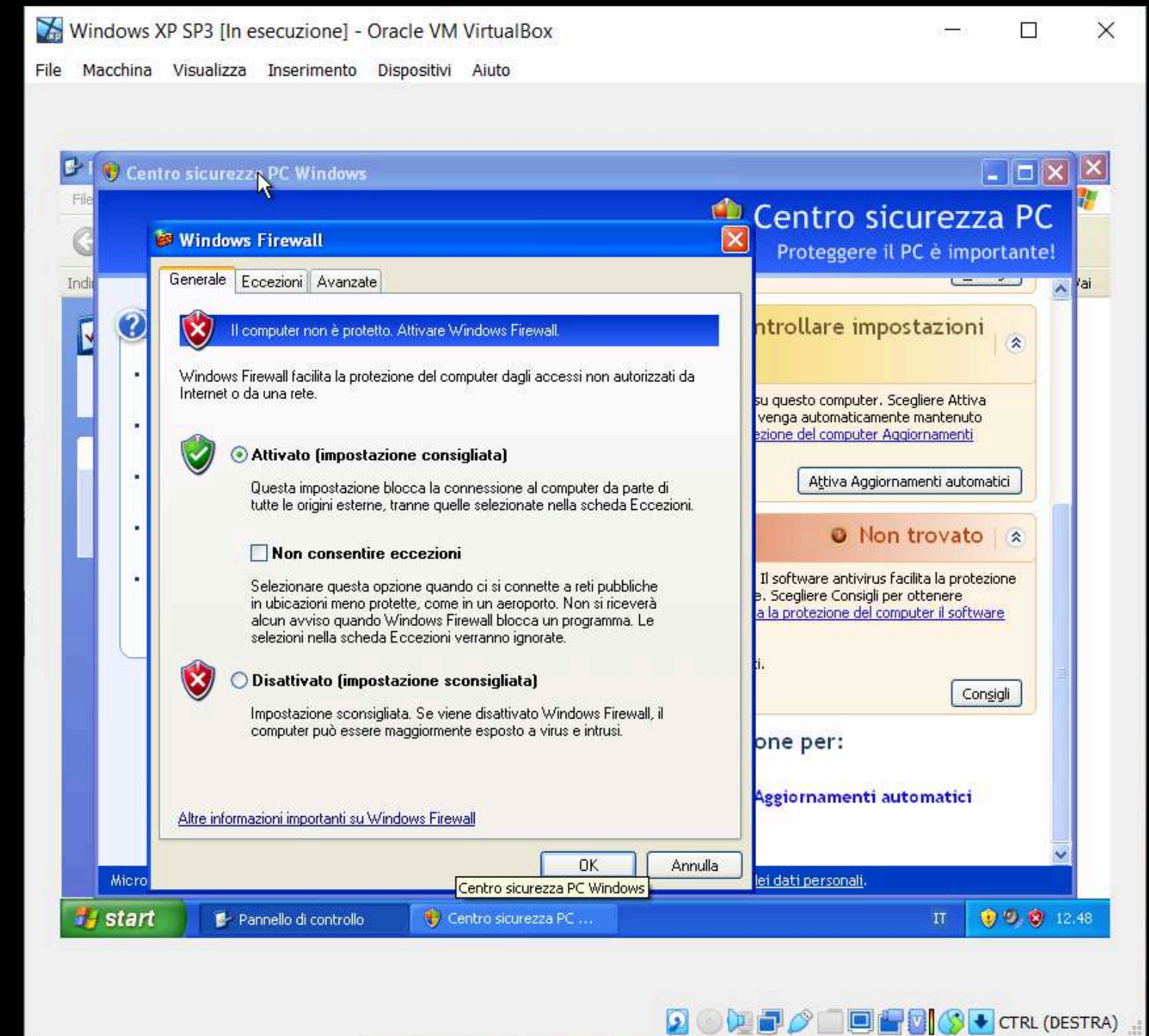
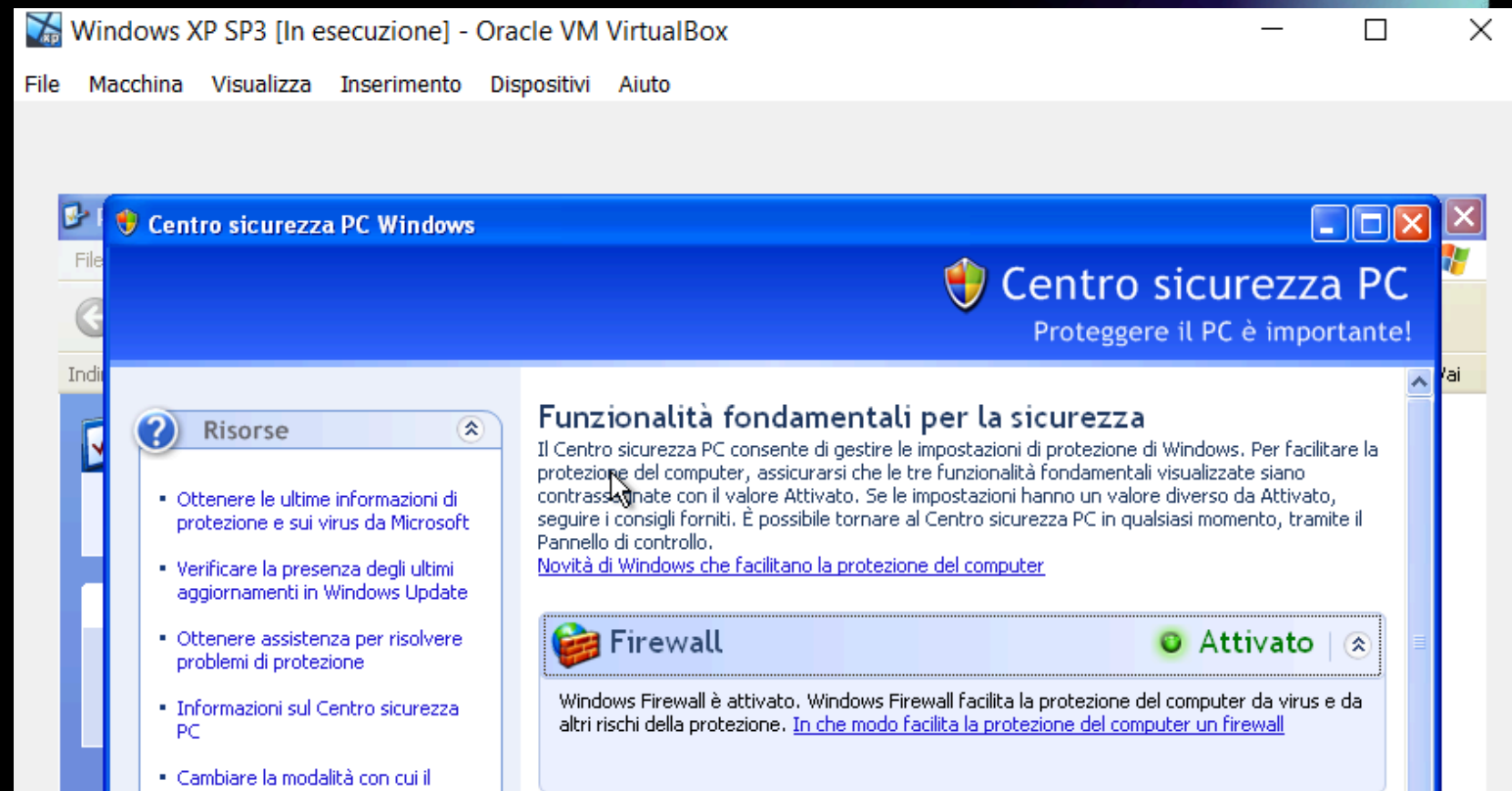
- Autenticazione: Utilizza meccanismi di autenticazione per verificare l'identità degli utenti che accedono alle risorse condivise.
- Crittografia: Può utilizzare la crittografia per proteggere i dati durante il transito.
- Firewall: È importante configurare correttamente i firewall per proteggere i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

SCANSIONE DI WINDOWS FIREWALL ATTIVATO

Prima di eseguire la scansione, attiviamo il firewall su Windows XP. Successivamente, avviamo un'altra scansione sulla macchina Kali utilizzando lo stesso comando:

`nmap -sV "indirizzo IP target" -oN "nome del file output"`

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.



SCANSIONE DI WINDOWS FIREWALL ATTIVATO

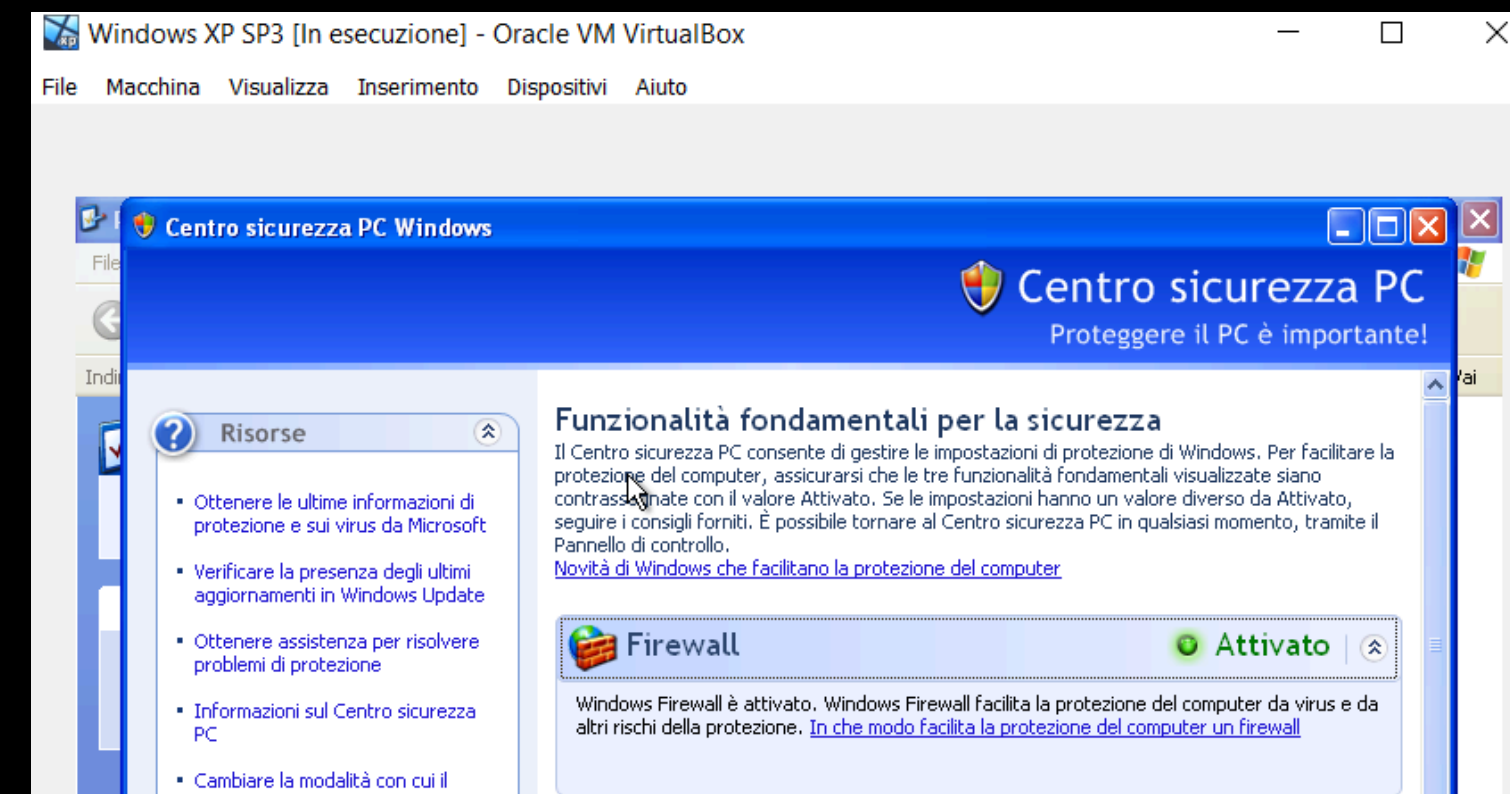
Prima di eseguire la scansione, attiviamo il firewall su Windows XP. Successivamente, avviamo un'altra scansione sulla macchina Kali utilizzando lo stesso comando:

nmap -sV "indirizzo IP target" -oN "nome del file output"

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.

```
(root@kali)-[/home/kali]
# nmap -sV 192.168.240.150 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 09:15 EDT
Nmap scan report for 192.168.240.150
Host is up (0.00053s latency).
All 1000 scanned ports on 192.168.240.150 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:07:6B:8A (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 36.68 seconds
```



- **-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.



5. Conclusioni

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, attivando il firewall, si notano due principali differenze:

1. 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.
2. 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 né identificare i servizi attivi su di esse.

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



S9_L1

Cyber Secure Tech. - Report

