



TechNova  
Solutions

# TECHNOVA SOLUTIONS



# OVERVIEW

01

About Us

02

Obbiettivo

03

Regole di ingaggio

04

Processo Effettuato

05

Rimedi

06

Conclusioni



# ABOUT US

**NOME:**

TechNova Solutions

**SETTORE:**

Tecnologia e sviluppo software

TechNova Solutions è un'azienda di tecnologia e sviluppo software con sede a Milano. Specializzata in soluzioni software personalizzate per clienti di vari settori, TechNova Solutions si impegna a fornire prodotti innovativi e di alta qualità, con un forte focus sulla sicurezza informatica e la protezione dei dati.



# OBIETTIVO

Sono stato incaricato da TechNova Solutions di condurre un penetration testing (pentesting) e un vulnerability assessment per valutare la sicurezza dei loro sistemi informatici e della rete aziendale. Questo incarico ha l'obiettivo di identificare eventuali vulnerabilità e punti deboli che potrebbero essere sfruttati da potenziali aggressori. Nel presente report, fornirò una descrizione dettagliata delle regole di ingaggio che abbiamo stabilito, del processo metodico che ho seguito per eseguire i test, delle soluzioni proposte per mitigare le vulnerabilità riscontrate e dei costi associati a queste misure di sicurezza. L'obiettivo finale è garantire che TechNova Solutions possa rafforzare la propria postura di sicurezza e proteggere efficacemente i propri dati e sistemi critici.

# REGOLE DI INGAGGIO

**01**

Obiettivi

- Identificare le vulnerabilità nei sistemi informatici e nella rete.
- Valutare il livello di sicurezza attuale.
- Proporre soluzioni per mitigare le vulnerabilità identificate.

**02**

Scopo

- Sistemi inclusi: Server, workstation, dispositivi di rete, applicazioni web.
- Tipi di test: Test di intrusione esterni ed interni, test delle applicazioni web, analisi delle configurazioni di rete.

**03**

Limitazioni

- Nessuna interruzione delle operazioni aziendali.
- Accesso limitato agli ambienti di produzione per minimizzare i rischi.
- Riservatezza su tutte le informazioni raccolte durante i test.

**04**

Autorizzazioni

- Accesso autorizzato ai sistemi e alle risorse necessarie per eseguire i test.
- Informazioni di contatto per il team di sicurezza IT interno in caso di emergenze.

# PROCESSO EFFETTUATO

**Identificare le vulnerabilità presenti nei sistemi e nella rete di TechNova Solutions.**

Scansione delle vulnerabilità: Utilizzo di scanner di vulnerabilità per rilevare porte aperte, servizi in esecuzione e vulnerabilità note. Per la scansione ho usato Nmap

Per prima cosa ho eseguito un ping da dentro la rete LAN per verificare se fossi connesso correttamente alla rete e poi ho effettuato una scansione con Nmap usando gli switch -sV per avere più informazioni sui servizi attivi nelle porte e -o per creare un file in cui salvare la scansione.

```
(kali㉿kali)-[~/Desktop/Epicode/S9]
$ 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=3.94 ms
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=3.96 ms
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=4.67 ms
^C
--- 192.168.240.150 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 3.941/4.190/4.669/0.338 ms

(kali㉿kali)-[~/Desktop/Epicode/S9]
$ nmap -sV -o Report.txt 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-04 09:08 EDT
Nmap scan report for 192.168.240.150 (192.168.240.150)
Host is up (0.0023s 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 11.04 seconds
```

Come si può vedere ci sono tre porte aperte:

- Porta 135/tcp (msrpc): Questa è la porta utilizzata per il servizio Microsoft Remote Procedure Call (RPC). RPC è un protocollo che consente a un programma su una macchina di richiedere un servizio da un programma situato su un'altra macchina in una rete. Tuttavia, può essere sfruttato da attaccanti per eseguire codice arbitrario o effettuare attacchi di denial of service (DoS).

- Porta 139/tcp (netbios-ssn): Questa porta è associata al servizio Microsoft NetBIOS Session Service (netbios-ssn). Il servizio NetBIOS gestisce le sessioni di comunicazione tra computer in una rete locale. Tuttavia, è noto che NetBIOS presenta vulnerabilità di sicurezza e può essere utilizzato per condurre attacchi come lo sniffing di dati di rete o l'esecuzione di code arbitrarie.

- Porta 445/tcp (microsoft-ds): Questa porta è utilizzata per il servizio Microsoft-DS (Directory Services) su sistemi operativi Windows. Questo servizio consente la condivisione di file e stampanti in una rete locale. Tuttavia, la porta 445 è nota per essere vulnerabile a svariate forme di attacco, inclusi attacchi di tipo ransomware come WannaCry, e può essere sfruttata per ottenere l'accesso non autorizzato ai file e alle risorse condivise sul sistema.

# RIMEDI

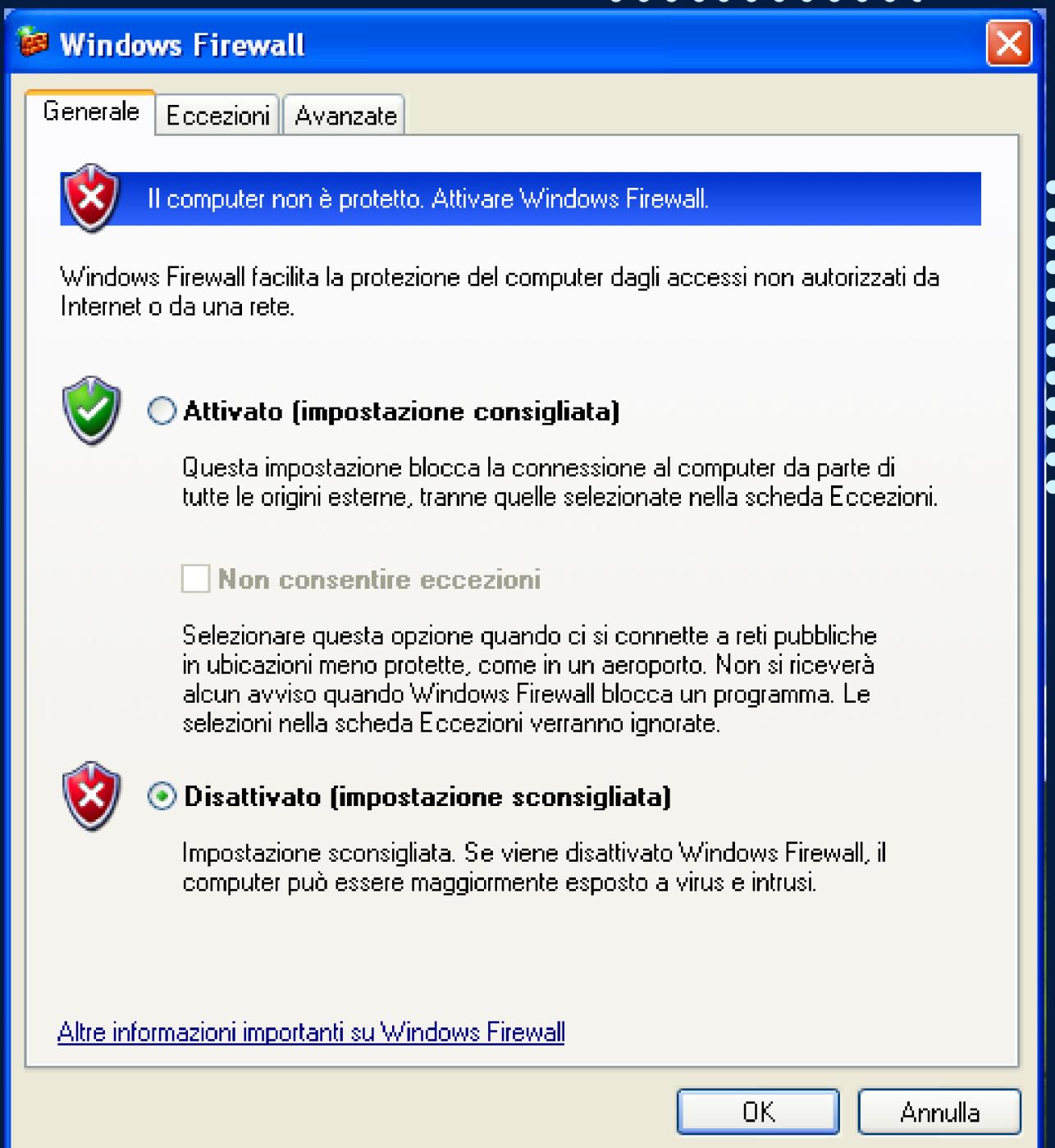
La soluzione più semplice e sicura per affrontare le potenziali vulnerabilità sarebbe quella di migrare verso un sistema operativo più recente e supportato, beneficiando così delle ultime patch di sicurezza e delle funzionalità di protezione avanzate. Tuttavia, comprendendo che l'azienda è completamente strutturata su Windows XP e desidera continuare ad utilizzarlo per motivi di compatibilità o legacy, si è reso necessario esaminare più attentamente le regole del firewall per implementare misure di sicurezza aggiuntive.

Andando a controllare il Firewall esso risultava disabilitato, quindi sono andato ad attivarlo e a riprovare la scansione.

```
(kali㉿kali)-[~/Desktop/Epicode/S9]
$ nmap -sV -o Report.txt 192.168.240.150 | Plain text document
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-04 09:30 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 3.17 seconds

(kali㉿kali)-[~/Desktop/Epicode/S9]
$ nmap -Pn -sV -o Report.txt 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-04 09:30 EDT
Nmap scan report for 192.168.240.150 (192.168.240.150)
Host is up.
All 1000 scanned ports on 192.168.240.150 (192.168.240.150) 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 201.79 seconds
```



Andando a rieseguire lo scan ci dice le porte blocano il ping, quindi provo a ad usare lo switch -Pn che non completa la connessione TCP ma le porte sono filtrate quindi non abbiamo nessuna informazione.

# Analisi delle Regole del Firewall:

Quindi per diminuire i rischi bisogna attivare il firewall ed impostare correttamente delle regole in modo da permettere alle persone autorizzate di usare i servizi e bloccare gli estranei.

- Porta 135/tcp (msrpc): È consigliabile limitare l'accesso alla porta 135 solo ai server o ai servizi specifici che ne necessitano, riducendo così l'esposizione a potenziali attacchi. Inoltre, è possibile implementare regole di filtraggio per bloccare il traffico proveniente da fonti non attendibili o non autorizzate.
- Porta 139/tcp (netbios-ssn): Poiché NetBIOS è noto per le sue vulnerabilità, si consiglia di disabilitare il servizio se non è strettamente necessario per le operazioni aziendali. Se la disabilitazione non è un'opzione, è fondamentale implementare regole di firewall rigorose per limitare l'accesso solo ai dispositivi e agli utenti autorizzati.
- Porta 445/tcp (microsoft-ds): Essendo vulnerabile a svariate forme di attacco, è vitale applicare regole di firewall che limitino l'accesso alla porta 445 solo ai servizi essenziali e ai dispositivi di rete fidati. Inoltre, è consigliabile considerare l'implementazione di una VPN per proteggere il traffico di rete sensibile e mitigare i rischi associati alla condivisione di file e stampanti su questa porta.

# CONCLUSIONI

Questo approccio consente di mantenere l'infrastruttura operativa su Windows XP, pur introducendo misure di sicurezza aggiuntive attraverso le regole del firewall, al fine di mitigare i rischi di sicurezza associati alle vulnerabilità identificate durante il processo di scansione dei servizi.

In conclusione, l'esame delle regole del firewall svolge un ruolo fondamentale nel garantire la sicurezza delle infrastrutture IT, specialmente in contesti in cui l'utilizzo di sistemi operativi legacy come Windows XP è inevitabile. Nonostante le potenziali vulnerabilità associate ai servizi identificati durante la scansione, è possibile implementare misure di sicurezza aggiuntive attraverso il firewall per mitigare i rischi e proteggere l'azienda da possibili attacchi esterni. Tuttavia, è importante sottolineare che l'adozione di un sistema operativo più moderno e supportato rimane la soluzione più efficace per garantire un livello ottimale di sicurezza informatica. Pertanto, si consiglia vivamente a TechNova Solutions di pianificare una strategia di migrazione verso sistemi operativi aggiornati, lavorando in collaborazione con i reparti IT e di sicurezza per garantire una transizione fluida e sicura.

Nel frattempo, l'implementazione di regole del firewall rigorose e la costante vigilanza sulle minacce informatiche consentiranno a TechNova Solutions di mantenere un ambiente IT sicuro e resiliente, proteggendo i propri dati e sistemi critici dagli attacchi esterni.