

# AGENZIA TURATI

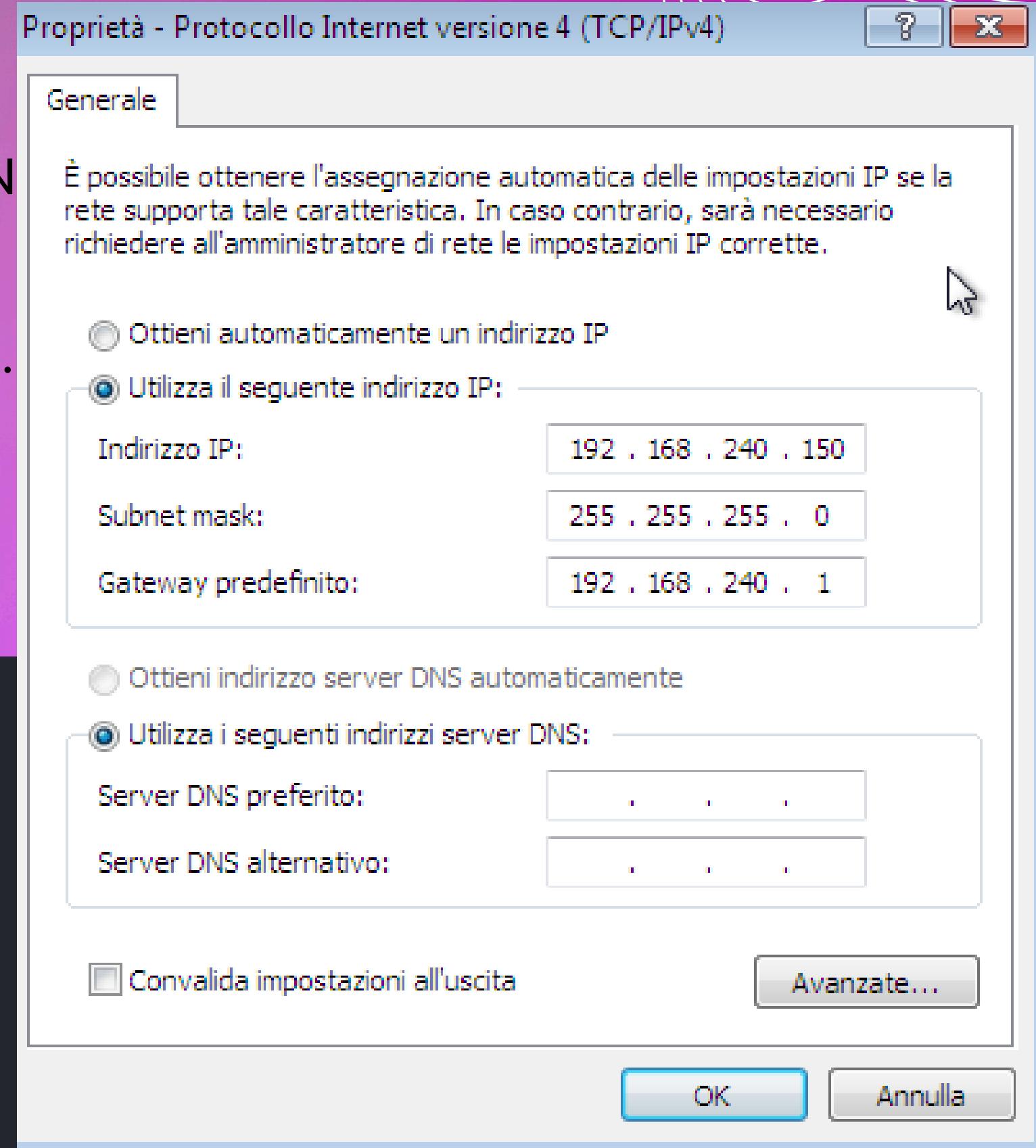


LA MIA AZIENDA TURATI È STATA CONTATTATA DAL SG.  
ROSSI

PER METTERE AL SICURO LA SUA AZIENDA ATTRAVERSO UN  
VULNERABILITY ASSESSMENT.

INIZIALMENTE HO ESEGUITO UN CONTROLLO SIA CON IL  
FIREWALL DISABILITATO E SIA CON IL FIREWALL ABILITATO.  
COME PRIMO PASSAGGIO HO FATTO PINGARE LE DUE  
MACCHINE IN MODO TALE CHE COMUNICASSERO TRA DI  
LORO

```
(kali㉿kali)-[~]
$ 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=0.736 ms
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=0.677 ms
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=0.395 ms
64 bytes from 192.168.240.150: icmp_seq=4 ttl=128 time=0.457 ms
^C
— 192.168.240.150 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3063ms
rtt min/avg/max/mdev = 0.395/0.566/0.736/0.143 ms
```



Successivamente da kali grazie al comando  
NMAP -sV 192.168.240.150 sono riuscito a vedere  
che nmap ha trovato 3 porte aperte .

La porta 135:msrpc è una tecnologia utilizzata da Microsoft per consentire la comunicazione tra processi in rete.

La porta 139:NetBIOS,è un insieme di protocolli di rete utilizzati principalmente nelle reti locali.

La porta 445: microsoft-ds, utilizzato per memorizzare, organizzare e recuperare informazioni sulla rete

**Salviamo tutto all'interno del nostro file di testo  
possiamo ora effettuare un nuovo ping con il firewall attivo e  
proviamo con il comando:**

**nmap -Pn 192.168.240.150**

```
[root@kali] [/home/kali/Desktop]
# nmap -Pn 192.168.240.150

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 14:00 CEST
Nmap scan report for 192.168.240.150
Host is up (0.00042s latency).
All 1000 scanned ports on 192.168.240.150 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:55:F3:27 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 37.83 seconds
```

**QUESTO COMANDO PERO NON CI DA MOLTE INFORMAZIONI , CI VIENE SOLO  
RESTIUITO IL MC ADDRESS DI WINDOWS XP E SAPPIAMO CHE IL SISTEMA OPERATIVO  
STA OPERANDO NELLA MACCHINA VIRTUALE**

# Con il comando nmap-A è possibile scansionare OS fingerprint, Script scanning e traceroute

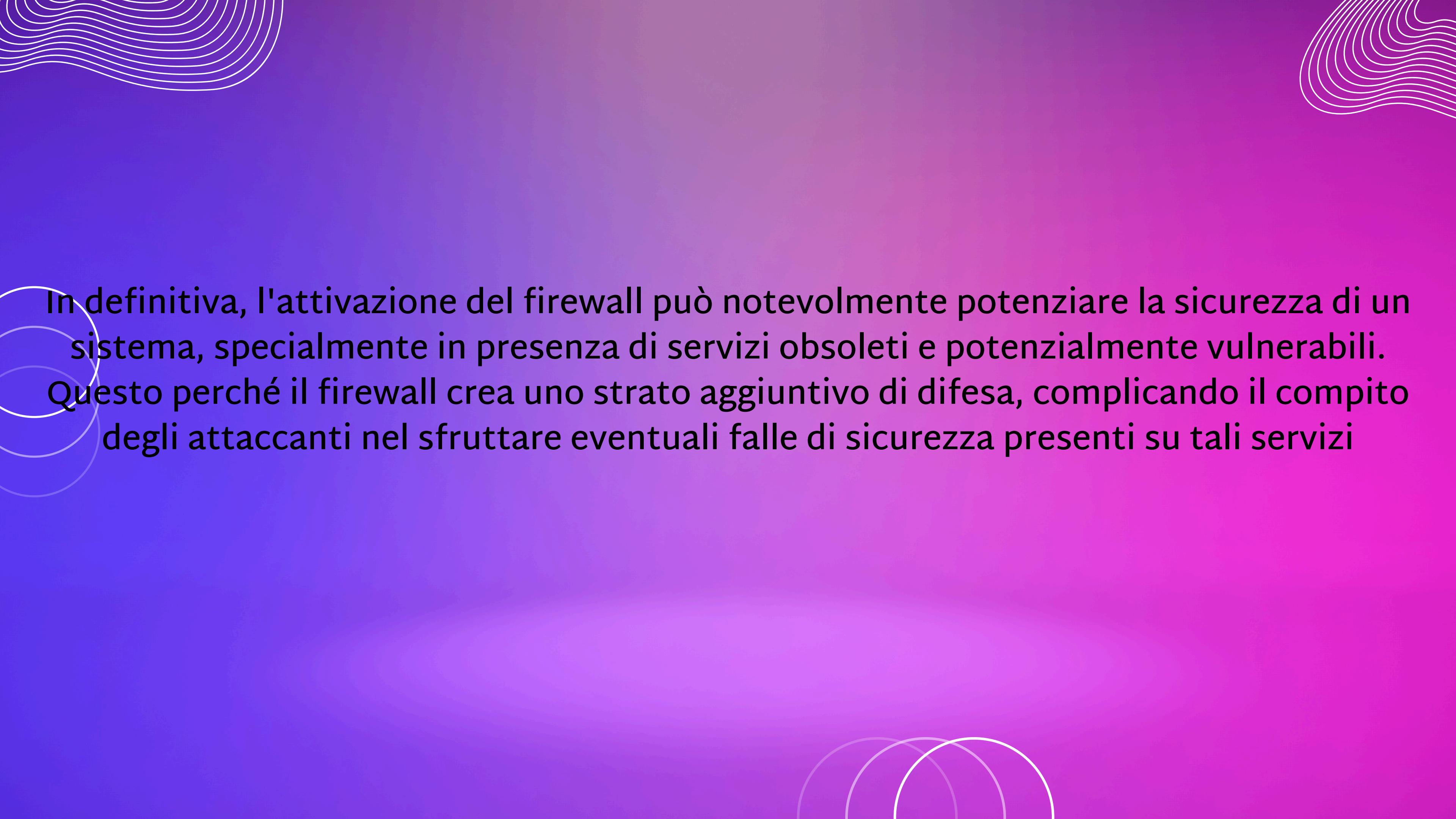
```
[root@kali]-[~/home/kali/Desktop]
# nmap -A 192.168.240.150

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 13:58 CEST
Nmap scan report for 192.168.240.150
Host is up (0.00037s latency).
All 1000 scanned ports on 192.168.240.150 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:55:F3:27 (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1  0.37 ms  192.168.240.150

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 46.42 seconds
```

Riusciamo a vedere quanti dispositivi di rete sono stati attraversati dai pacchetti e il tempo di risposta della macchina .



In definitiva, l'attivazione del firewall può notevolmente potenziare la sicurezza di un sistema, specialmente in presenza di servizi obsoleti e potenzialmente vulnerabili. Questo perché il firewall crea uno strato aggiuntivo di difesa, complicando il compito degli attaccanti nel sfruttare eventuali falle di sicurezza presenti su tali servizi

# IMPATTI DANNOSI PER L'AZIENDA

Un incendio nell'edificio principale rappresenta il rischio più grave, seguito da un'eventuale inondazione nell'edificio secondario e da un terremoto nel data center. Tuttavia, ciascuno di questi eventi potrebbe avere conseguenze serie per l'azienda, richiedendo piani di continuità aziendale e di ripristino dei disastri ben strutturati per mitigare gli impatti.

Incendio nell'edificio principale:

- Impatto: Danneggiamento esteso di infrastrutture, documenti, attrezzature e potenziale rischio per la sicurezza delle persone.
- Conseguenze: Interruzione operativa, perdita di dati critici, danni reputazionali e significative perdite finanziarie.

Inondazione nell'edificio secondario:

- Impatto: Danneggiamento di attrezzature, archivi e infrastrutture, seppur in misura inferiore rispetto all'edificio principale.
- Conseguenze: Interruzione operativa nella sede, perdita di risorse locali, possibili rallentamenti delle attività e costi di riparazione.

Terremoto nel data center:

- Impatto: Potenziali danni strutturali agli apparati informatici, interruzioni di rete e perdita di dati critici.
- Conseguenze: Interruzione operativa dell'IT, perdita di dati, danni permanenti all'infrastruttura e costi significativi per il ripristino.

# INCENDIO

ASSET	VALORE ASSET	FATTORE DI ESPOSIZIONE	FREQUENZA ARO	PERDITA ANNUALE
EDIFICIO PRIMARIO	350.000	60%	1/20 ANNI	10.500
EDIFICIO SECONDARIO	150.000	50%	1/20 ANNI	3.750
DATA CENTER	100.000	60%	1/20 ANNI	3.000

# TERREMOTO

ASSET	VALORE ASSET	FATTORE DI ESPOSIZIONE	FREQUENZA ARO	PERDITA ANNUALE
EDIFICIO PRIMARIO	350.000	80%	1/30 ANNI	9.400
EDIFICIO SECONDARIO	150.000	80%	1/30 ANNI	3.600
DATA CENTER	100.000	95%	1/30 ANNI	2.850

# INONDAZIONE

ASSET	VALORE ASSET	FATTORE DI ESPOSIZIONE	FREQUENZA ARO	PERDITA ANNUALE
EDIFICIO PRIMARIO	350.000	55%	1/50 ANNI	3.850
EDIFICIO SECONDARIO	150.000	40%	1/50 ANNI	1.200
DATA CENTER	100.000	35%	1/50 ANNI	700

# IOC

Verifichiamo se sono presenti indicatori di compromissione ovvero prove, segni o dati che suggeriscono che un sistema potrebbe essere stato compromesso o è sotto attacco.

Gli IOC sono fondamentali per rilevare e rispondere a minacce informatiche.

Utilizzando whreshark rileviamo in queste righe pacchetti ARP collegati al dispositivo PCSSystemtec nel traffico di rete. Questi pacchetti potrebbero segnalare un potenziale attacco Man in the Middle (MITM), in particolare se le richieste ARP risultano anomale. Gli attacchi MITM frequentemente utilizzano l'ARP spoofing per intercettare il traffico di rete.

```
8 28.761629461 PCSSystemtec_fd:87:... PCSSystemtec_39:7d:... ARP      60 Who has 192.168.200.100? Tell 192.168.200.150  
9 28.761644619 PCSSystemtec_39:7d:... PCSSystemtec_fd:87:... ARP      42 192.168.200.100 is at 08:00:27:39:7d:fe  
10 28.774852257 PCSSystemtec_39:7d:... PCSSystemtec_fd:87:... ARP     42 Who has 192.168.200.150? Tell 192.168.200.100  
11 28.775230099 PCSSystemtec_fd:87:... PCSSystemtec_39:7d:... ARP     60 192.168.200.150 is at 08:00:27:fd:87:1e
```

Arriviamo alla conclusione che nel peggio dei casi qualcuno stia per effettuare un ARP Poisoning anche conosciuto come ARP spoofing ovvero una tecnica di attacco informatico che manipola il protocollo ARP (Address Resolution Protocol) per associare l'indirizzo MAC (Media Access Control) dell'attaccante a un indirizzo IP legittimo nella rete locale (LAN). Questo permette all'attaccante di intercettare, modificare o interrompere il traffico di rete.

È importante notare la presenza di numerose richieste provenienti dallo stesso indirizzo IP su porte diverse. Questo comportamento può indicare che qualcuno stia eseguendo una scansione della rete utilizzando strumenti come Nmap. Le porte stanno bloccando queste richieste tramite reset. Tale attività di scansione può essere un segnale di tentativi di rilevare vulnerabilità nei sistemi di rete.

21	36.774685696	192.168.200.150	192.168.200.100	TCP	60 443 → 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	36.774685737	192.168.200.150	192.168.200.100	TCP	60 554 → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	36.774685776	192.168.200.150	192.168.200.100	TCP	60 135 → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	36.774700464	192.168.200.100	192.168.200.150	TCP	66 41304 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
25	36.774711072	192.168.200.100	192.168.200.150	TCP	66 56120 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
26	36.775141104	192.168.200.150	192.168.200.100	TCP	60 993 → 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	36.775141273	192.168.200.150	192.168.200.100	TCP	74 21 → 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535438 WS=64
28	36.775174048	192.168.200.100	192.168.200.150	TCP	66 41182 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
29	36.775337800	192.168.200.100	192.168.200.150	TCP	74 59174 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
30	36.775386694	192.168.200.100	192.168.200.150	TCP	74 55656 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
31	36.775524204	192.168.200.100	192.168.200.150	TCP	74 53062 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
32	36.775589806	192.168.200.150	192.168.200.100	TCP	60 113 → 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	36.775619454	192.168.200.100	192.168.200.150	TCP	66 41304 → 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
34	36.775652497	192.168.200.100	192.168.200.150	TCP	66 56120 → 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466

Nella riga 27 possiamo vedere pacchetti syn ack .

I pacchetti SYN-ACK (Synchronize-Acknowledge) sono una parte fondamentale del processo di stabilimento di una connessione TCP (Transmission Control Protocol). Il processo di stabilimento della connessione è noto come "Three-Way Handshake" (stretta di mano a tre vie)

27	36.775141273	192.168.200.150	192.168.200.100	TCP	74	21 → 41182 [SYN, ACK]
----	--------------	-----------------	-----------------	-----	----	-----------------------

# CONSIGLI SU COME RIDURRE IMPATTI ATTACCO

Creare subnet distinte per ciascuna area di lavoro in modo che, in caso di intrusione, l'attaccante non possa spostarsi facilmente all'interno della rete aziendale. Questa segmentazione della rete limita il raggio d'azione dell'attaccante, migliorando la sicurezza complessiva.

1.

Installare e configurare un firewall per bloccare richieste sospette. Questa misura rafforza la sicurezza della rete aziendale, prevenendo accessi non autorizzati e proteggendo i dati sensibili.

2.

Controllare attentamente l'host 192.168.200.150 e il dispositivo PCSSystemtec, bloccandoli immediatamente se si rilevano attività sospette

3.

Ho ricevuto una chiamata urgente: un attacco informatico era in corso contro il sistema B, un database essenziale supportato da molteplici dischi di storage. La situazione richiedeva un intervento immediato e coordinato per contenere e neutralizzare la minaccia. Ecco un resoconto dettagliato delle azioni intraprese, che dimostrano la prontezza e l'efficacia delle tecniche utilizzate.

# CRONOLOGIA AZIONI DI MITIGAZIONE

## Fase 1: Valutazione dell'attacco

Appena ricevuta la notifica, ho attivato il protocollo di emergenza e convocato il team di sicurezza informatica. Abbiamo subito condotto una valutazione preliminare per identificare l'origine e la natura dell'attacco. Utilizzando strumenti di monitoraggio avanzati, abbiamo individuato attività sospette su più dischi di storage del sistema B.

## Fase 2: Isolamento del sistema

Per prevenire ulteriori danni e limitare la diffusione dell'attacco, ho deciso di isolare il sistema B dalla rete principale. Questo passaggio cruciale ha permesso di interrompere immediatamente la comunicazione dell'attaccante con il nostro database, impedendo ulteriori compromissioni.

## Fase 3: Analisi forense

Dopo aver isolato il sistema, abbiamo avviato un'analisi forense dettagliata. Ho assegnato ruoli specifici a ciascun membro del team per esaminare i log di sistema, analizzare il traffico di rete e verificare l'integrità dei dati. L'obiettivo era identificare eventuali punti di ingresso utilizzati dall'attaccante e capire la portata dell'intrusione.

#### Fase 4: Eliminazione della minaccia

Identificati i punti di ingresso, abbiamo proceduto con l'eliminazione della minaccia. Abbiamo aggiornato tutte le firme antivirus e antimalware, eseguito scansioni complete su tutti i dischi di storage e rimosso i file dannosi individuati. Inoltre, abbiamo applicato patch di sicurezza per correggere le vulnerabilità sfruttate dall'attaccante.

#### Fase 5: Ripristino e verifica

Completata l'eliminazione della minaccia, abbiamo avviato il processo di ripristino del sistema. Ho supervisionato il ripristino dei dati dai backup sicuri e verificato l'integrità e la completezza delle informazioni ripristinate. Successivamente, abbiamo condotto una serie di test per garantire che il sistema B fosse completamente operativo e privo di ulteriori minacce.

#### Fase 6: Rafforzamento delle difese

Infine, ho coordinato un piano di rafforzamento delle difese per prevenire futuri attacchi. Abbiamo implementato misure di sicurezza aggiuntive, come la segmentazione della rete, l'adozione di sistemi di rilevamento delle intrusioni più avanzati e la formazione continua del personale sulla sicurezza informatica.



**La differenza tra "purge" e "destroy" nel contesto della gestione dei dati e della sicurezza informatica è la seguente:**



**Purge:** Rimuove i dati in modo tale che non siano facilmente recuperabili usando strumenti convenzionali, ma potrebbero essere recuperati con tecniche avanzate. Tipicamente, questo implica la sovrascrittura dei dati una o più volte.

**Destroy:** Elimina i dati in modo permanente e irreversibile, rendendone impossibile il recupero. Questo può includere la distruzione fisica dei dispositivi di storage o l'utilizzo di metodi di cancellazione avanzati che assicurano che i dati non possano essere ricostruiti.



## Conclusione

Questo attacco ha messo alla prova la nostra capacità di risposta e la solidità delle nostre misure di sicurezza. Grazie alla prontezza del nostro team e all'efficacia delle tecniche impiegate, siamo riusciti a contenere e neutralizzare la minaccia in modo tempestivo. Continueremo a migliorare le nostre difese per proteggere i dati essenziali del sistema B e mantenere la fiducia dei nostri utenti.

# INCIDENT RESPONSE

## Introduzione

Sono stato incaricato di affrontare un attacco informatico in corso contro il sistema B, un database essenziale con multipli dischi di storage. In questo report, descrivo le azioni intraprese per contenere e neutralizzare la minaccia, adottando un approccio passo-passo che evidenzia la nostra reattività e l'efficacia delle tecniche impiegate.

Inoltre, fornirò una valutazione sull'impatto economico di un downtime e delineerò misure preventive e di risposta a vari tipi di attacco.

# Azioni Preventive

Per difendere l'applicazione web da attacchi di tipo SQL Injection (SQLi) e Cross-Site Scripting (XSS), ho implementato le seguenti misure preventive:

Ho verificato e pulito tutti i dati forniti dagli utenti per eliminare caratteri sospetti, utilizzando librerie di sanitizzazione che rimuovono codici pericolosi.

Ho utilizzato prepared statements o query parametrizzate per prevenire l'inserimento di codice SQL malevolo.

Content Security Policy (CSP)

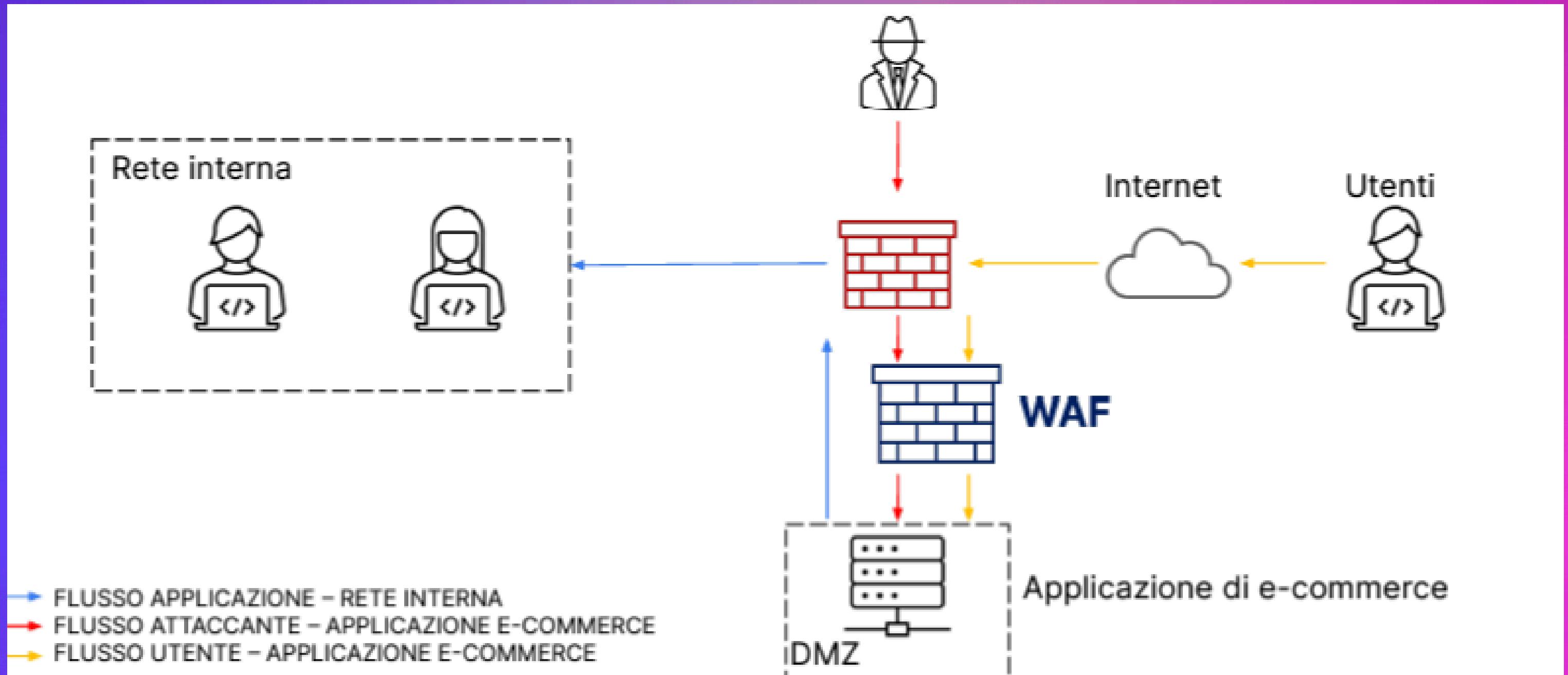
Ho implementato una politica di sicurezza dei contenuti per prevenire l'esecuzione di script non autorizzati.

Ho utilizzato metodi di escaping appropriati per il contesto (HTML, JavaScript, SQL) per impedire l'inserimento di codice voluto.

Web Application Firewall (WAF)

Ho implementato un WAF per filtrare e bloccare attacchi SQLi e XSS.

Ho assicurato che il software, il server web e il database siano aggiornati con le ultime patch di sicurezza.



# Impatto sul Business

## Calcolo dell'Impatto Economico

Ho calcolato l'impatto economico di un downtime di 10 minuti dovuto a un attacco DDoS, considerando che in media ogni minuto gli utenti spendono 1.500 €:

$$\text{Impatto} = 1.500 \text{ €} \times 10 = 15.000 \text{ €}$$
$$\text{Impatto} = 1.500 \text{ €} \times 10 = 15.000 \text{ €}$$

## Azioni Preventive contro DDoS

Per mitigare l'impatto di futuri attacchi DDoS, ho implementato le seguenti misure:

### 1. Content Delivery Network (CDN)

- Utilizzo di una CDN per distribuire il traffico e ridurre l'impatto di un attacco DDoS.

### 2. Rate Limiting

- Implementazione di limiti di frequenza per le richieste provenienti da singoli indirizzi IP.

### 3. Web Application Firewall (WAF)

- Configurazione di un WAF per identificare e bloccare traffico anomalo.

### 4. Scrubbing Services

- Utilizzo di servizi di scrubbing per filtrare il traffico malevolo.

### 5. Ridondanza e Failover

- Configurazione di meccanismi di ridondanza e failover per mantenere la disponibilità del servizio.

# **Response: Contenimento del Malware**

## **Azioni di Contenimento**

Quando l'applicazione web è stata infettata da un malware, la mia priorità era impedire la propagazione del malware sulla rete. Ecco le azioni che ho intrapreso:

### **1. Isolamento della Macchina Infetta**

- Ho disconnesso immediatamente la macchina infetta dalla rete per impedire la propagazione del malware.

### **2. Monitoraggio del Traffico di Rete**

- Ho configurato strumenti di monitoraggio per osservare e analizzare il traffico di rete.

### **3. Segmentazione della Rete**

- Ho implementato segmentazione della rete per limitare l'accesso tra diverse parti della rete.

### **4. Analisi e Contenimento**

- Ho condotto un'analisi dettagliata del malware per capire il vettore di attacco e contenere la minaccia.

# **Architettura di Rete**

## **Descrizione dell'Architettura di Rete**

L'applicazione di e-commerce deve essere disponibile per gli utenti tramite la piattaforma. La rete interna è raggiungibile dalla DMZ (Demilitarized Zone) per via delle policy sul firewall. Questo significa che se il server nella DMZ viene compromesso, un attaccante potrebbe potenzialmente raggiungere la rete interna.



## **Unione di Azioni Preventive e di Risposta**

### **Implementazione Combinata**

Ho combinato tutte le misure preventive e di risposta descritte per creare una soluzione di sicurezza completa:

1. Sanitizzazione e Validazione dell'Input: Implementazione nel form di input.
2. Parametrizzazione delle Query e CSP: Annotazione nell'applicazione.
3. WAF e CDN: Integrazione per la protezione contro DDoS e attacchi comuni.
4. Isolamento e Segmentazione della Rete: Isolamento delle macchine infette e segmentazione della rete per limitare i danni.
5. DMZ e Firewall Policies: Protezione della rete interna attraverso una corretta configurazione delle policy del firewall e segregazione della DMZ.