



SecureWave



# 2024 REPORT DENIM SOLUTION



**Giugno  
2024**

Scritto da  
**Luca Gaspari**

Per  
**Denim  
Solution**

# SecureWave



SecureWave S.r.l. è un'azienda leader nel settore della sicurezza informatica, specializzata nella protezione dei sistemi informatici e dei dati aziendali da minacce cyber. Con sede a Milano, Italia, SecureWave è stata fondata nel 2015 con l'obiettivo di fornire soluzioni di sicurezza informatica all'avanguardia a clienti di ogni settore.

La missione di SecureWave è proteggere le aziende dalle minacce informatiche, garantendo la sicurezza e l'integrità dei loro dati e sistemi. La visione dell'azienda è diventare il partner di fiducia per la sicurezza informatica a livello globale, offrendo soluzioni innovative e personalizzate per affrontare le sfide più complesse del settore.



# Servizi Offerti



**Vulnerability Assessment:** SecureWave offre servizi di vulnerability assessment per identificare e valutare le vulnerabilità presenti nei sistemi informatici dei clienti. Questo servizio include una dettagliata analisi delle potenziali minacce e raccomandazioni per migliorare la sicurezza.

**Penetration Testing:** L'azienda esegue test di penetrazione simulando attacchi reali per scoprire punti deboli nei sistemi e fornire soluzioni per mitigare i rischi.

**Managed Security Services:** SecureWave fornisce servizi di gestione della sicurezza, monitorando continuamente le reti e i sistemi dei clienti per rilevare e rispondere a minacce in tempo reale.

**Consulting e Compliance:** L'azienda offre consulenza per la conformità normativa e l'implementazione di politiche di sicurezza, aiutando i clienti a rispettare le leggi e le normative vigenti in materia di protezione dei dati.

**Formazione e Sensibilizzazione:** SecureWave organizza corsi di formazione e programmi di sensibilizzazione per educare il personale aziendale sulle best practice di sicurezza informatica.

# Contratto

## Contratto di Servizio per Vulnerability Assessment e Penetration Test

**Tra:** Denim Solutions S.r.l.

Sede legale: Via Esempio, 123, 00100 Roma, Italia

P. IVA: 12345678901

**E:** SecureWave S.r.l.

Sede legale: Via Sicurezza, 45, 20100 Milano, Italia

P. IVA: 98765432109

### Premesso che:

- Il Cliente desidera migliorare la sicurezza dei propri sistemi informatici.
- Il Fornitore è specializzato in servizi di sicurezza informatica, tra cui vulnerability assessment e penetration testing.
- Le parti hanno convenuto di eseguire i servizi con modalità white box, ovvero con piena conoscenza dei sistemi informatici da parte del Fornitore.

Si conviene e si stipula quanto segue:

### Articolo 1: Oggetto del Contratto

Il Fornitore si impegna a fornire i seguenti servizi al Cliente:

- Vulnerability Assessment: Analisi e valutazione delle vulnerabilità presenti nei sistemi informatici del Cliente.
- Penetration Test: Simulazione di attacchi informatici per identificare e sfruttare potenziali vulnerabilità.

### Articolo 2: Modalità di Esecuzione

- White Box Testing: I test saranno eseguiti con piena conoscenza delle infrastrutture, delle architetture di rete, del codice sorgente e dei sistemi informatici del Cliente. Questo approccio consente un'analisi approfondita e accurata delle vulnerabilità.
- Durata: I servizi saranno eseguiti nell'arco di 2 settimane, con un totale di 160 ore lavorative.

### Articolo 3: Preventivo e Costi

Dettagli del Lavoro:

- Tariffa oraria: € 100/ora
- Durata stimata: 2 settimane (80 ore a settimana)
- Totale ore: 160 ore

| Servizio                  | Ore | Tariffa Oraria (€) | Totale (€)    |
|---------------------------|-----|--------------------|---------------|
| Vulnerability Assessment  | 80  | 100                | 8,000         |
| Penetration Test          | 80  | 100                | 8,000         |
| <b>Totale Complessivo</b> | 160 |                    | <b>16,000</b> |

### Pagamenti:

- 50% all'inizio del progetto (€ 8,000)
- 50% alla consegna del rapporto finale (€ 8,000)

### Articolo 4: Riservatezza

- 1. Obblighi di Riservatezza:** Il Fornitore si impegna a mantenere riservate tutte le informazioni relative ai sistemi e ai dati del Cliente. Le informazioni ottenute durante l'esecuzione dei servizi saranno utilizzate esclusivamente per lo scopo del contratto.
- 2. Durata della Riservatezza:** Gli obblighi di riservatezza rimarranno in vigore anche dopo la conclusione del contratto, per un periodo di 5 anni.

### Articolo 5: Permessi e Accessi

- 1. Accesso ai Sistemi:** Il Cliente fornirà al Fornitore tutti gli accessi necessari ai sistemi, alle reti e alle applicazioni per eseguire i test.
- 2. Cooperazione:** Il Cliente coopererà pienamente con il Fornitore, fornendo tutte le informazioni e i documenti necessari per l'esecuzione dei servizi.

### Articolo 6: Rapporti di Lavoro

Alla fine di ogni attività, il Fornitore consegnerà un rapporto dettagliato al Cliente contenente:

- Risultati del vulnerability assessment.
- Analisi dettagliata delle vulnerabilità trovate.
- Raccomandazioni e misure correttive.

### Articolo 7: Responsabilità

Il Fornitore non sarà responsabile per eventuali danni diretti o indiretti derivanti dall'uso delle informazioni fornite. Il Cliente riconosce che l'esecuzione di penetration test può causare interruzioni o danni ai sistemi testati, e accetta tali rischi.

### Articolo 8: Risoluzione del Contratto

Il contratto può essere risolto da entrambe le parti con un preavviso di 30 giorni. In caso di risoluzione anticipata, il Cliente sarà tenuto a pagare per i servizi effettivamente forniti fino alla data di risoluzione.

**Articolo 9: Legge Applicabile e Foro Competente**

Il presente contratto è regolato dalla legge italiana. Per qualsiasi controversia sarà competente il Foro di Milano.

**Firmato:**

Denim Solutions S.r.l.

Mario Rossi

SecureWave S.r.l.

Luca Gaspari

**Contatti:**

SecureWave S.r.l.

Via Sicurezza, 45, 20100 Milano, Italia

Telefono: +39 02 1234567

Email: [info@securewave.it](mailto:info@securewave.it)

Sito web: [www.securewave.it](http://www.securewave.it)

# Introduzione

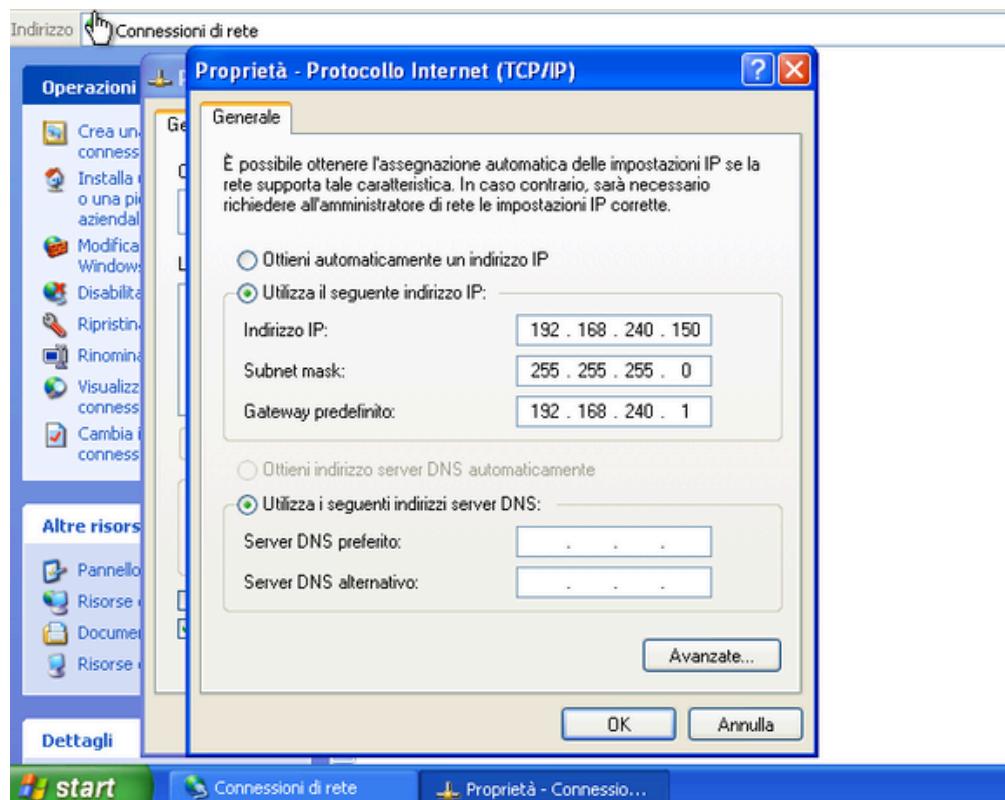
L'assessment è stato condotto su una macchina Windows XP (IP: 192.168.240.150) dalla nostra macchina Kali Linux (IP: 192.168.240.100). Sono stati effettuati vari test con il firewall della macchina Windows XP attivato e disattivato per analizzare le differenze nei risultati.

## Configurazione della Rete

- Macchina Kali Linux: ip 192.168.240.100
- Macchina Windows XP: ip 192.168.240.150

```
(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 1  bytes 243 (243.0 B)
              RX errors 0  dropped 0  overruns 0  frame 0
              TX packets 16  bytes 2404 (2.3 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 4  bytes 240 (240.0 B)
              RX errors 0  dropped 0  overruns 0  frame 0
              TX packets 4  bytes 240 (240.0 B)
              TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```



# Ping tra le macchine

```
(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=1.25 ms
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=1.59 ms
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=1.41 ms
64 bytes from 192.168.240.150: icmp_seq=4 ttl=128 time=0.349 ms
^C
--- 192.168.240.150 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 0.349/1.148/1.587/0.476 ms

(kali㉿kali)-[~]
$
```

```
Prompt dei comandi
Microsoft Windows XP [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Epicode_user>ping 192.168.240.100
Esecuzione di Ping 192.168.240.100 con 32 byte di dati:

Risposta da 192.168.240.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.240.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.240.100: byte=32 durata=1ms TTL=64

Statistiche Ping per 192.168.240.100:
    Pacchetti: Trasmessi = 3, Ricevuti = 3, Persi = 0 (0% persi),
    Tempo approssimativo percorsi andata/ritorno in millisecondi:
        Minimo = 0ms, Massimo = 1ms, Medio = 0ms
Control-C
^C
C:\Documents and Settings\Epicode_user>
```

# Scansione Nmap

## Scansione senza firewall

Comando utilizzato: nmap -sV 192.168.240.150 -o esercizio1.txt

```
(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150 -o esercizio1.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 15:13 EDT
Nmap scan report for 192.168.240.150
Host is up (0.00043s 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 20.55 seconds
```

Questo comando esegue una scansione di versioni dei servizi (-sV) sull'host con IP 192.168.240.150 e salva i risultati in un file chiamato esercizio1.txt. Con il firewall disattivato, Nmap è in grado di rilevare correttamente le porte aperte e i servizi in esecuzione sull'host.

### Analisi:

Con il firewall disattivato, Nmap è stato in grado di rilevare correttamente l'host come attivo. Sono state trovate tre porte aperte con i rispettivi servizi:

- Porta 135/tcp: Servizio msrpc (Microsoft Windows RPC)
- Porta 139/tcp: Servizio netbios-ssn (Microsoft Windows netbios-ssn)
- Porta 445/tcp: Servizio microsoft-ds (Microsoft Windows XP microsoft-ds)

Questi risultati indicano che con il firewall disattivato, le porte aperte e i servizi esposti possono essere rilevati facilmente, evidenziando le potenziali vulnerabilità

## Scansione con firewall attivo

Comando Utilizzato: nmap -sV 192.168.240.150 -o esercizio2.txt

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.240.150 -o esercizio2.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 15:16 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
```

Analisi:

Quando il firewall era attivo sulla macchina Windows XP, Nmap non è riuscito a rilevare l'host come attivo. Questo è dovuto al fatto che il firewall blocca le sonde di ping, facendo sembrare che l'host non risponda. Nmap suggerisce di utilizzare l'opzione -Pn per ignorare il ping e procedere comunque con la scansione delle porte.

Comando Utilizzato: nmap -Pn -sV 192.168.240.150 -o esercizio3.txt

```
(kali㉿kali)-[~]
$ nmap -Pn -sV 192.168.240.150 -o esercizio3.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 15:18 EDT
Nmap scan report for 192.168.240.150
Host is up.
All 1000 scanned ports on 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 214.64 seconds
```

Analisi:

Utilizzando l'opzione -Pn, Nmap presume che l'host sia attivo anche se non risponde alle sonde di ping. Tuttavia, tutte le porte risultano filtrate, il che significa che il firewall sta bloccando l'accesso a tutte le porte TCP. Nmap non riesce a determinare quali servizi siano in esecuzione a causa delle restrizioni imposte dal firewall.

## Differenze Riscontrate

- Con Firewall Attivo: Nmap non è stato in grado di rilevare l'host come attivo utilizzando le sonde di ping. Anche con l'opzione -Pn, tutte le porte risultavano filtrate, impedendo la rilevazione dei servizi.
- Con Firewall Disattivato: Nmap ha rilevato correttamente l'host e ha identificato tre porte aperte con i rispettivi servizi, indicando che l'host è molto più esposto senza le protezioni del firewall.

## Conclusioni

- Firewall Attivo: Mantiene l'host nascosto dalle sonde di ping e blocca l'accesso a tutte le porte, aumentando significativamente la sicurezza.
- Firewall Disattivato: Espone l'host e i suoi servizi alle scansioni Nmap, rivelando potenziali punti di attacco.

## Raccomandazioni

1. Mantenere il Firewall Attivo: È essenziale per proteggere l'host da accessi non autorizzati e scansioni potenzialmente dannose.
2. Aggiornamento e Patch: Applicare tutte le patch di sicurezza e aggiornamenti per mitigare le vulnerabilità note.
3. Limitare i Servizi Esposi: Rivedere e limitare i servizi in esecuzione sulla macchina per ridurre ulteriormente la superficie di attacco.
4. Monitoraggio Continuo: Implementare soluzioni di monitoraggio e logging per rilevare e rispondere tempestivamente a eventuali tentativi di intrusione.

# Valutazione quantitativa dell'impatto di possibili disastri sugli asset di Denim Solution

Dati:

| ASSET               | VALORE   | EVENTO      | ARO                  |
|---------------------|----------|-------------|----------------------|
| Edificio primario   | 350.000€ | Terremoto   | 1 volta ogni 30 anni |
| Edificio secondario | 150.000€ | Incendio    | 1 volta ogni 20 anni |
| Datacenter          | 100.000€ | Inondazione | 1 volta ogni 50 anni |

| EXPOSURE FACTOR     | Terremoto | Incendio | Inondazione |
|---------------------|-----------|----------|-------------|
| Edificio primario   | 80%       | 60%      | 55%         |
| Edificio secondario | 80%       | 50%      | 40%         |
| Datacenter          | 95%       | 60%      | 35%         |

Prendendo in considerazione i dati forniti in tabella, calcoliamo l'impatto a livello economico dei possibili disastri naturali che potrebbero verificarsi sugli asset di Denim Solution.

SLE, acronimo di “Single Loss Expectancy” fornisce una misura monetaria della perdita che si subirebbe al verificarsi dell'evento, calcolato come il prodotto tra il valore dell'asset (AV) e la percentuale impattata in caso di evento (EF)

Primo caso: Inondazione sull'asset edificio secondario

$$\text{SLE} = 150.000\text{€ (AV)} \times 40\% (\text{EF}) = 60.000\text{€}$$

Dopo aver calcolato lo SLE cioè una stima dei danni basata sul valore dell'asset andiamo a calcolare l'ALE (annualized loss expectancy) cioè il valore della perdita subita in un arco temporale di un anno. Questo valore si trova moltiplicando il valore del SLE per il numero di volte stimato dell'evento in un anno (ARO).

$$\text{ALE} = 60.000\text{€ (SLE)} \times 0,02 (\text{ARO}) = 1.200\text{€}$$

Secondo caso: Terremoto sull'asset del Data Center

$$\text{SLE} = 100.000\text{€} \times 95\% = 95.000\text{€}$$

$$\text{ALE} = 95.000\text{€} \times 0,03 = 2.850\text{€}$$

Terzo caso: Incendio sull'asset edificio primario

$$\text{SLE} = 350.000\text{€} \times 60\% = 210.000\text{€}$$

$$\text{ALE} = 210.000\text{€} \times 0,05 = 10.500\text{€}$$

Quarto caso: Incendio sull'asset edificio secondario

$$\text{SLE} = 150.000\text{€} \times 60\% = 90.000\text{€}$$

$$\text{ALE} = 90.000\text{€} \times 0,05 = 4.500\text{€}$$

Quinto caso: Inondazione sull'asset edificio primario

$$\text{SLE} = 350.000\text{€} \times 55\% = 192.500\text{€}$$

$$\text{ALE} = 192.500\text{€} \times 0,02 = 3.850\text{€}$$

Sesto caso: Terremoto sull'asset edificio primario

$$\text{SLE} = 350.000\text{€} \times 80\% = 280.000\text{€}$$

$$\text{ALE} = 280.000\text{€} \times 0,03 = 8.400\text{€}$$

# Analisi e report del traffico di rete

## Cattura effettuata con Wireshark

### Introduzione

Gli Indicatori di Compromissione (IOC) sono evidenze che suggeriscono la presenza di un'attività malevola o di un attacco informatico in corso. Analizzando i pacchetti catturati con Wireshark, possiamo identificare vari IOC che possono indicare tentativi di attacco o comportamenti sospetti.

### Analisi dei pacchetti

Durante l'analisi del traffico di rete con Wireshark, sono stati osservati numerosi pacchetti TCP con flag SYN inviati da un IP (192.168.200.100) verso un altro IP (192.168.200.150), seguiti da risposte con flag RST. Tuttavia, su alcune porte specifiche, la risposta ai pacchetti SYN è positiva, con pacchetti SYN-ACK seguiti da pacchetti ACK, completando così l'handshake TCP a tre vie.

Per prima cosa andando ad analizzare i primi pacchetti della cattura

| Cattura_U3_W1_L3.pcapng |              |                        |                        |          |        |  |
|-------------------------|--------------|------------------------|------------------------|----------|--------|--|
| No.                     | Time         | Source                 | Destination            | Protocol | Length | Info   |
| 1                       | 0.000000000  | 192.168.200.150        | 192.168.200.255        | BROWSER  | 286    | Host Announcement METASPOITABLE, Workstation, Server, Print Queue Server, Xenix Server, ...            |
| 2                       | 23.764214995 | 192.168.200.100        | 192.168.200.150        | TCP      | 74     | 53060 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=810522427 TSecr=0 WS=128              |
| 3                       | 23.764287781 | 192.168.200.100        | 192.168.200.150        | TCP      | 74     | 33876 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=810522428 TSecr=0 WS=128             |
| 4                       | 23.764777323 | 192.168.200.150        | 192.168.200.100        | TCP      | 74     | 89 - 1 [SYN] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TStamp=4294951165 TSecr=0 WS=128            |
| 5                       | 23.764777427 | 192.168.200.150        | 192.168.200.100        | TCP      | 60     | 443 - 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0   |
| 6                       | 23.764815289 | 192.168.200.100        | 192.168.200.150        | TCP      | 66     | 53060 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1460 SACK_PERM TStamp=810522428 TSecr=4294951165      |
| 7                       | 23.764899891 | 192.168.200.100        | 192.168.200.150        | TCP      | 66     | 53060 - 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1460 SACK_PERM TStamp=810522428 TSecr=4294951165 |
| 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  |

Possiamo notare dei pacchetti ARP seguiti da dei messaggi, "who has 192.168.200.100 tell 192.168.200.150" e "who has 192.168.200.150 tell 192.168.200.100" questi messaggi indicano che i dispositivi stanno cercando di risolvere gli indirizzi IP in indirizzi MAC per stabilire la comunicazione. Questo è un comportamento normale nelle reti locali e rappresenta il funzionamento di base di ARP per la risoluzione degli indirizzi.

Successivamente analizzando gli indirizzi ip 192.168.200.100 e 192.168.200.150 si può dedurre che appartengono alla stessa rete. La subnet mask utilizzata è /24 (255.255.255.0), che significa che i primi 24 bit degli indirizzi IP sono utilizzati per identificare la rete e gli ultimi 8 bit sono utilizzati per identificare gli host.

Siccome gli indirizzi rientrano nel range degli IP validi (da 192.168.200.1 a 192.168.200.254) significa che si trovano nella stessa rete.

Analizzando i successivi pacchetti si può osservare il seguente comportamento:

|                  |                 |                 |     |  |
|------------------|-----------------|-----------------|-----|--|
| 12 36. 774143445 | 192.168.200.100 | 192.168.200.150 | TCP | 74 41304 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TsvaL=810535437 Tscr=0 WS=128             |
| 13 36. 774218116 | 192.168.200.100 | 192.168.200.150 | TCP | 74 56120 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TsvaL=810535437 Tscr=0 WS=128            |
| 14 36. 774257841 | 192.168.200.100 | 192.168.200.150 | TCP | 74 33878 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TsvaL=810535437 Tscr=0 WS=128            |
| 15 36. 774366385 | 192.168.200.100 | 192.168.200.150 | TCP | 74 58636 → 654 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TsvaL=810535438 Tscr=0 WS=128            |
| 16 36. 774405627 | 192.168.200.100 | 192.168.200.150 | TCP | 74 52358 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TsvaL=810535438 Tscr=0 WS=128            |
| 17 36. 774535534 | 192.168.200.100 | 192.168.200.150 | TCP | 74 46138 → 99 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TsvaL=810535438 Tscr=0 WS=128             |
| 18 36. 774614776 | 192.168.200.100 | 192.168.200.150 | TCP | 74 41182 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TsvaL=810535438 Tscr=0 WS=128             |
| 19 36. 774685505 | 192.168.200.150 | 192.168.200.100 | TCP | 74 23 → 41304 [SYN, ACK] Seq=1 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TsvaL=4294952466 Tscr=0 WS=128  |
| 20 36. 774685652 | 192.168.200.150 | 192.168.200.100 | TCP | 74 111 → 56120 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TsvaL=4294952466 Tscr=0 WS=128 |
| 21 36. 774685696 | 192.168.200.150 | 192.168.200.100 | TCP | 60 443 → 33607 [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. 774708464 | 192.168.200.100 | 192.168.200.150 | TCP | 66 41304 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TsvaL=810535438 Tscr=4294952466                        |
| 25 36. 774711872 | 192.168.200.100 | 192.168.200.150 | TCP | 66 56120 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TsvaL=810535438 Tscr=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. 775141275 | 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 Tscr=0 WS=128  |
| 28 36. 775174848 | 192.168.200.100 | 192.168.200.150 | TCP | 66 41182 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TsvaL=810535438 Tscr=4294952466                        |

|                   |                 |                 |     |   |
|-------------------|-----------------|-----------------|-----|---|
| 133 36. 780325837 | 192.168.200.100 | 192.168.200.150 | TCP | 74 37252 → 11 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TsvaL=810535444 Tscr=0 WS=128  |
| 134 36. 780346429 | 192.168.200.100 | 192.168.200.150 | TCP | 74 40864 → 11 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TsvaL=810535444 Tscr=0 WS=128  |
| 135 36. 780409818 | 192.168.200.100 | 192.168.200.150 | TCP | 74 36548 → 739 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TsvaL=810535444 Tscr=0 WS=128 |
| 136 36. 780427899 | 192.168.200.100 | 192.168.200.150 | TCP | 74 38866 → 55 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TsvaL=810535444 Tscr=0 WS=128  |
| 137 36. 780427839 | 192.168.200.100 | 192.168.200.150 | TCP | 74 52136 → 999 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TsvaL=810535444 Tscr=0 WS=128 |
| 138 36. 780499997 | 192.168.200.100 | 192.168.200.150 | TCP | 74 38022 → 317 [SYN] Seq=0 Win=0 MSS=1460 SACK_PERM TsvaL=810535444 Tscr=0 WS=128           |
| 139 36. 780577880 | 192.168.200.150 | 192.168.200.100 | TCP | 60 266 → 40822 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0   |
| 140 36. 780577981 | 192.168.200.150 | 192.168.200.100 | TCP | 60 11 → 37252 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0  |
| 141 36. 780578026 | 192.168.200.150 | 192.168.200.100 | TCP | 60 235 → 40648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0   |
| 142 36. 780578074 | 192.168.200.150 | 192.168.200.100 | TCP | 60 739 → 36548 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0   |
| 143 36. 780578119 | 192.168.200.150 | 192.168.200.100 | TCP | 60 38866 → 11 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0  |
| 144 36. 780578158 | 192.168.200.150 | 192.168.200.100 | TCP | 60 999 → 46138 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0   |
| 145 36. 780578198 | 192.168.200.150 | 192.168.200.100 | TCP | 60 317 → 38022 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0   |

### Numerosi Pacchetti SYN:

- Pacchetti con flag SYN inviati da 192.168.200.100 verso 192.168.200.150 su diverse porte.
- Questo potrebbe indicare una scansione delle porte, dove un attaccante tenta di trovare porte aperte e servizi attivi.

### Risposte con flag RST, ACK:

- L'IP 192.168.200.150 risponde con pacchetti RST, ACK su alcune porte, indicando che queste porte sono chiuse.

### Completamento di Handshake TCP su alcune porte:

- Su alcune porte specifiche, l'IP 192.168.200.150 risponde con pacchetti **SYN-ACK** e successivamente 192.168.200.100 completa l'handshake TCP con un pacchetto **ACK**.
- Questo indica che le connessioni su queste porte sono state stabilite correttamente, suggerendo che i servizi su queste porte sono attivi e accettano connessioni.

## Identificazione degli IOC

Scansione delle Porte:

- La presenza di numerosi pacchetti SYN su diverse porte, con risposte miste di SYN-ACK e RST, è un chiaro indicatore di una scansione delle porte. Questo tipo di attività viene utilizzato per identificare quali servizi sono attivi su un host e quali porte sono aperte.

Connessioni Stabilite su Porte Specifiche:

- L'handshake TCP completato su alcune porte specifiche indica che i servizi su queste porte sono attivi e possono essere potenziali vettori di attacco se vulnerabili.

## Ipotesi sui potenziali vettori d'attacco

Scansione delle Porte:

- Strumenti come Nmap potrebbero essere utilizzati per eseguire la scansione delle porte. L'attaccante invia pacchetti SYN a varie porte per determinare quali sono aperte e quali servizi sono in esecuzione.

Sfruttamento di Vulnerabilità dei Servizi Attivi:

- Una volta identificate le porte aperte e i servizi attivi, l'attaccante potrebbe tentare di sfruttare vulnerabilità note in quei servizi. Ad esempio, potrebbe utilizzare exploit specifici per il software in esecuzione su quelle porte.

## Azioni consigliate

### Monitoraggio delle scansioni delle porte

- Implementare sistemi di rilevamento delle intrusioni (IDS) per monitorare e rilevare attività di scansione delle porte, configurare avvisi per notificare gli amministratori di rete quando viene rilevata una scansione.

### Aggiornamento e Patch dei Servizi

- Assicurarsi che tutti i servizi in esecuzione sui dispositivi di rete siano aggiornati con le ultime patch di sicurezza. Questo riduce la probabilità che gli attaccanti possano sfruttare vulnerabilità note.

### Configurazione del Firewall

- Configurare il firewall per limitare l'accesso alle porte e ai servizi non necessari. Chiudere le porte non utilizzate e applicare regole di accesso restrittive per le porte aperte.

### Segmentazione della Rete

- Implementare la segmentazione della rete per limitare il movimento laterale degli attaccanti, utilizzare VLAN e subnet per isolare segmenti di rete sensibili.

### Analisi dei log

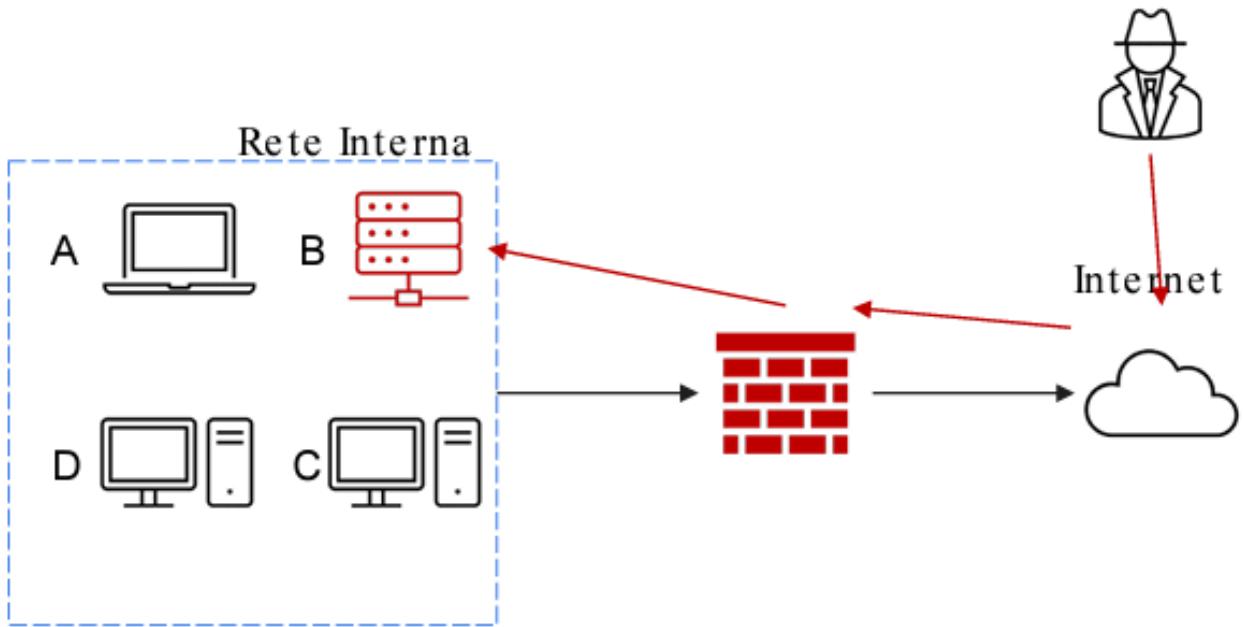
- Controllare regolarmente i log di sistema per rilevare attività sospette. Analizzare i log di connessione per identificare tentativi di accesso non autorizzati o comportamenti anomali.

L'implementazione delle azioni consigliate aiuterà a migliorare la sicurezza della rete e a mitigare i potenziali impatti degli attacchi, monitorare regolarmente il traffico di rete e mantenere aggiornati i sistemi sono pratiche essenziali per proteggere la rete da minacce e vulnerabilità.

# Report di incident response

## Sistema B compromesso

## Schema di rete attuale



## Introduzione

Il giorno 6/06/2024, il nostro team ha ricevuto una segnalazione riguardante una compromissione del sistema B, un database con diversi dischi per lo storage, da parte di un attaccante esterno che è riuscito a infiltrarsi tramite Internet, l'attacco era in corso e necessitava di una risposta immediata per contenere e mitigare l'incidente.

**Per contenere e mitigare l'incidente sono state eseguite le seguenti azioni:**

1

Isolamento del sistema infetto, isolare il sistema è stato il primo passo cruciale per impedire la propagazione dell'attacco ad altri sistemi all'interno della rete interna e per contenere l'incidente.

Utilizzando strumenti di monitoraggio della rete, tra cui IDS (Intrusion Detection Systems) e SIEM (Security Information and Event Management), abbiamo identificato il sistema B compromesso. Questi strumenti ci hanno aiutato a rilevare traffico anomalo e attività sospette.

2

Abbiamo scollegato fisicamente il sistema B dalla rete interna staccando il cavo di rete, la disconnessione fisica è un metodo diretto per interrompere immediatamente qualsiasi comunicazione tra il sistema infetto e il resto della rete.

3

Dopo la disconnessione fisica, abbiamo configurato il firewall hardware per bloccare tutto il traffico in entrata e in uscita dal sistema B. Questo passaggio ha garantito che, anche se il sistema venisse riconnesso accidentalmente, non potesse comunicare con altri sistemi o con l'esterno.

## Rimozione del sistema B infetto

La rimozione del sistema infetto dalla rete aziendale era necessario per prevenire ulteriori compromissioni ed eseguire un'analisi forense accurata in un ambiente controllato.

Come prima azione abbiamo spento il sistema B in modo sicuro per interrompere qualsiasi attività malevola in corso, utilizzando i comandi di spegnimento del sistema operativo.

Successivamente abbiamo creato un'immagine di backup completa del sistema B, questo passaggio è stato cruciale e necessario per l'analisi forense, permettendoci di esaminare il sistema per comprendere come l'attacco è avvenuto e quale tipo di dati sono stati compromessi.

## Smaltimento dei dati compromessi

Dopo l'isolamento e la rimozione del sistema B infetto, è stato fondamentale smaltire correttamente i dischi compromessi per garantire che le informazioni sensibili non possano essere recuperate.

### 1 Clear

Abbiamo eseguito una cancellazione sicura sui dischi compromessi utilizzando i comandi di cancellazione integrati, questo passaggio garantisce che i dati non vengano recuperati tramite mezzi normali.

Questo tipo di cancellazione sicura è stato il primo passo per rendere i dati meno accessibili e pronti per le successive azioni.

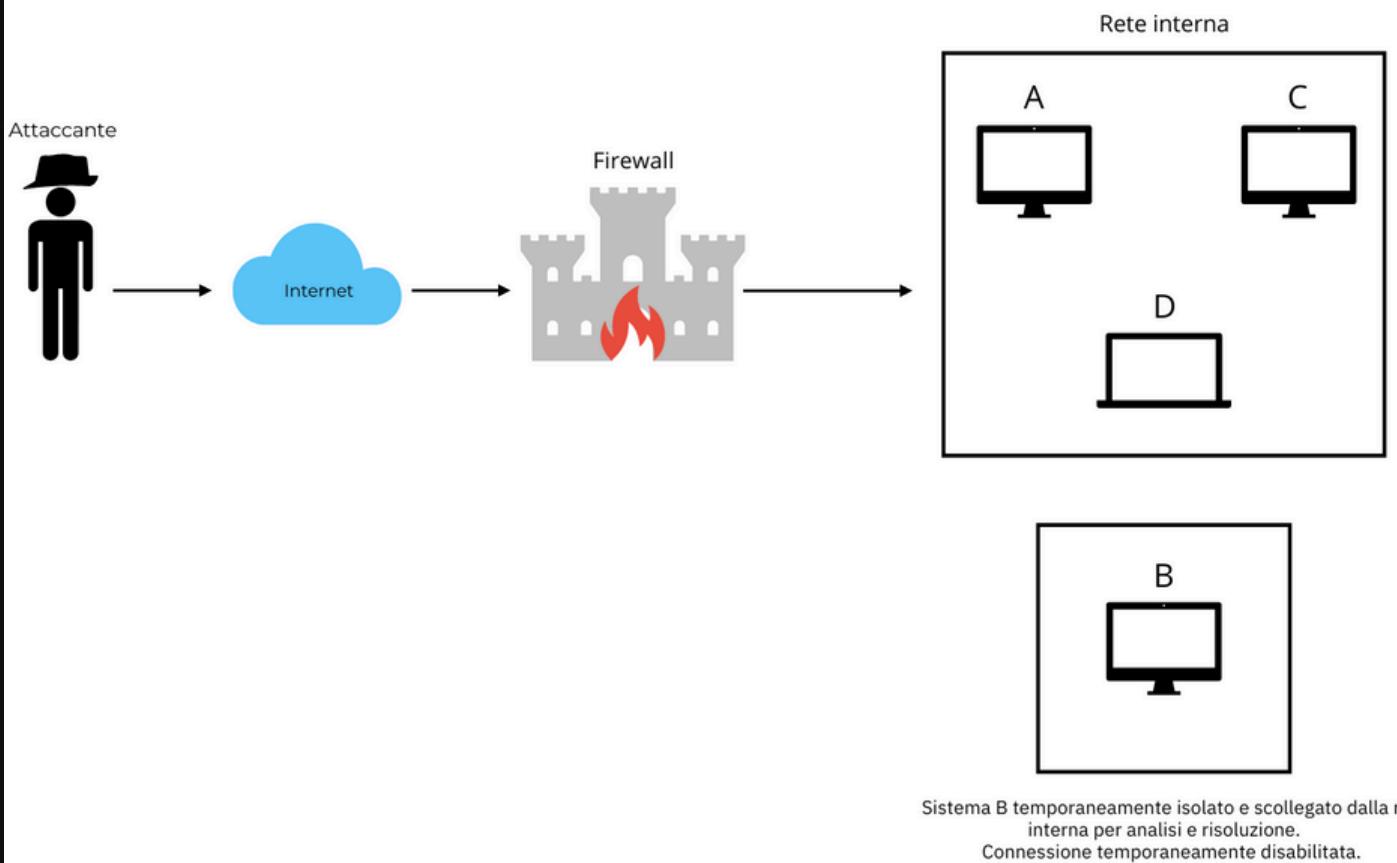
### 2 Purge

Abbiamo utilizzato software specializzati per sovrascrivere i dischi con dati casuali più volte, questo processo rende i dati originali irrecuperabili anche con mezzi più avanzati.

### 3 Destroy

Come ultimo passaggio abbiamo distrutto fisicamente i dischi compromessi. Questa azione garantisce che nessun dato possa essere recuperato in alcun modo.

## Schema di rete attuale dopo le azioni effettuate



## Differenze tra i metodi principali di smaltimento dei dati compromessi

### **Clear:**

Il dispositivo viene completamente ripulito dal suo contenuto con tecniche, si utilizza ad esempio un approccio di tipo read and write dove il contenuto viene sovrascritto più e più volte o si utilizza la funzione di «factory reset» per riportare il dispositivo nello stato iniziale;

### **Purge**

In questo metodo si adottano le metodologie del clear ma anche tecniche di rimozione fisica come l'utilizzo di forti magneti per rendere le informazioni inaccessibili su determinati dispositivi.

### **Destroy**

E' il metodo più netto per lo smaltimento di dispositivi contenenti dati sensibili, oltre ai meccanismi logici e fisici si usano metodi come la disintegrazione, polverizzazione e trapanazione, è il metodo più efficacie ma comporta spese economiche più alte in quanto questi metodo devono essere eseguiti in laboratorio.

## Soluzioni e azioni preventive per i diversi casi

### Azioni preventive per implementare la sicurezza del web server

Per aumentare la sicurezza del web server e proteggerlo da attacchi SQLi e XSS da parte di un utente malintenzionato il nostro team ha ipotizzato le seguenti implementazioni:

#### **Utilizzo di WAF (Web Application Firewall)**

Un WAF può rilevare e bloccare richieste dannose come SQLi e XSS, è in grado anche di analizzare il traffico in tempo reale, bloccando automaticamente le richieste sospette prima che raggiungano il web server. Il WAF lo andremo a posizionare tra gli utenti internet e il web server per andare a filtrare tutte le richieste in entrata.

#### **Validazione e sanificazione degli input utenti**

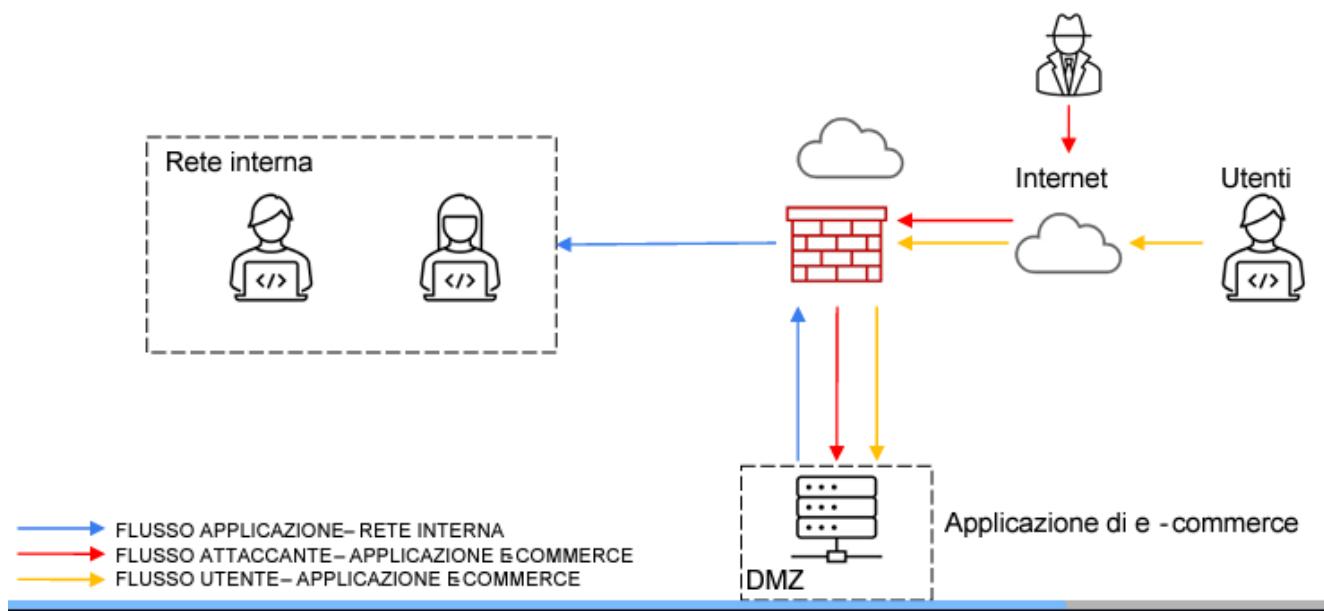
La validazione e la sanificazione degli input degli utenti prevengono l'inserimento di codici malevoli che potrebbe sfruttare vulnerabilità SQLi e XSS, questo processo garantisce che solo i dati sicuri vengano elaborati dall'applicazione oltre a questo si devono aumentare i controlli sui dati in ingresso e su tutti i punti di input del web server.

Quindi si deve modificare il codice dell'applicazione per utilizzare query SQL parametrizzate, eliminando la concatenazione di input dell'utente direttamente nelle query. L'uso di queste query evita l'iniezione di codice SQL malevolo, proteggendo così l'integrità del database.

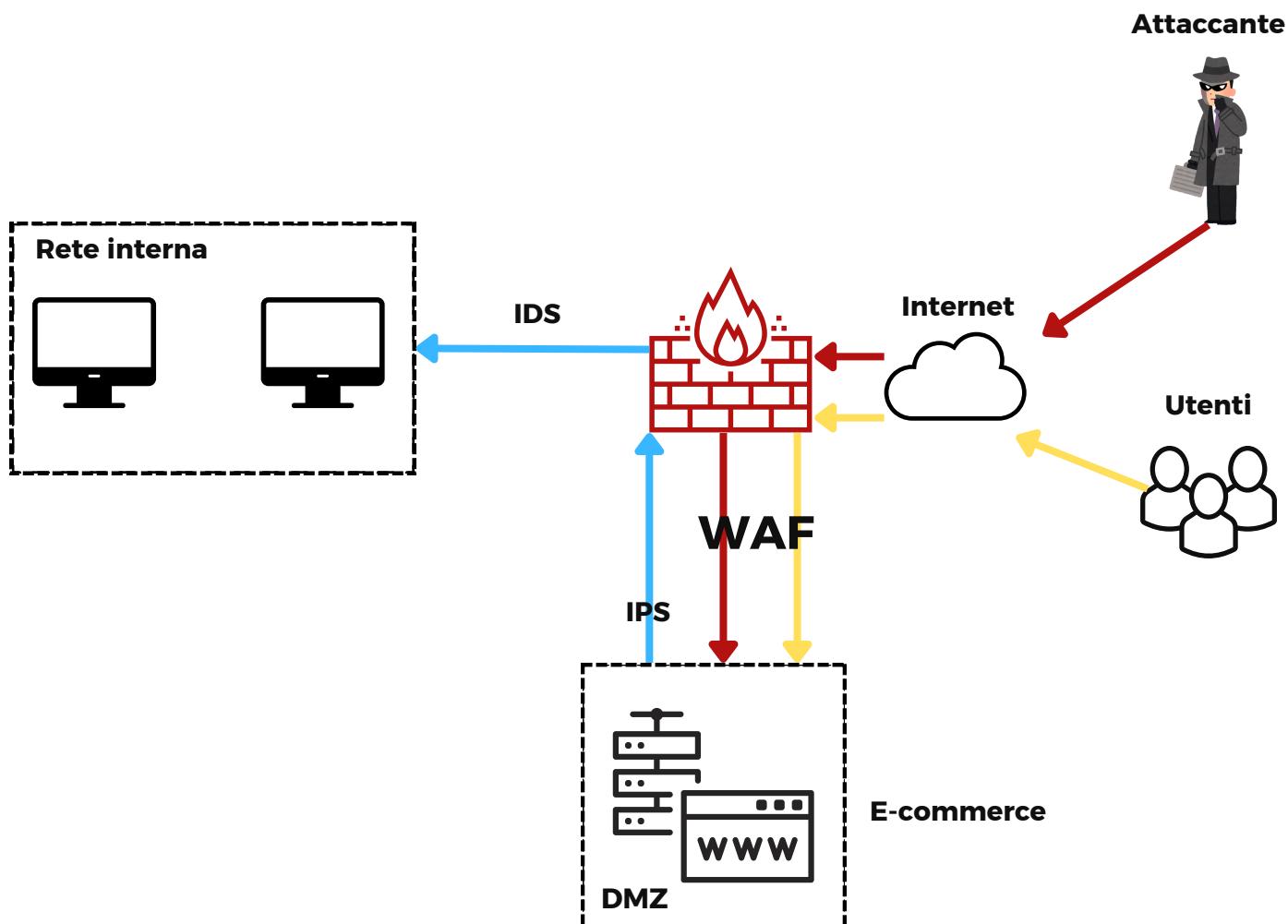
E' altrettanto importante anche implementare un sistema di gestione dei ruoli che assegna permessi specifici a ciascun utente in base alle loro necessità operative riducendo il rischio di esecuzione di comandi pericolosi e accessi non autorizzati.

Aggiunta anche di un IDS (funzione di avvisare con un alert in caso di attacco) e un IPS (agisce attivamente bloccando la minaccia) per rilevare e prevenire intrusioni. Installare anche soluzioni antivirus per ogni dispositivo nella rete.

## Schema di rete iniziale:



## Schema di rete con implementazione di WAF, IDS e IPS:



## Impatti sul business

### Ipotetico attacco DDoS

Ipotizzando che il web server venga attaccato dall'esterno con un **attacco DDoS** che rende **irraggiungibile** il **servizio per 10 minuti**, considerando che in media gli **utenti spendono 1500€ al minuto** andiamo a **calcolare il danno economico** che reca questo tipo di attacco.

Comprendendo l'impatto finanziario di un downtime è stato cruciale per giustificare un ipotetico investimento in soluzioni preventive.

**1500€ per minuto di downtime = 15.000 € per 10 minuti di indisponibilità.**

### Ipotetico investimento per soluzioni preventive in caso di attacco DDoS

#### Implementazione di un servizio di protezione DDoS

Un servizio di protezione DDoS rileva e mitiga attacchi DDoS, assicurando che l'applicazione rimanga accessibile anche durante tentativi di sovraccarico, il servizio deve essere posizionato come strato esterno di difesa.

#### Ridondanza e failover

Avere sistemi di failover e ridondanza assicura che il servizio rimanga disponibile anche se una parte dell'infrastruttura viene compromessa.

Si deve quindi configurare server di backup e percorsi di rete ridondanti che possono essere attivati automaticamente in caso di attacco, garantendo così la continuità del servizio.

## Response

Ipotizzando che la web app venga infettata da un malware e che la nostra priorità è non far propagare il malware nella rete, ma non ci interessa di rimuovere l'accesso da parte dell'attaccante alla macchina infetta seguiranno le seguenti azioni per rimuovere la minaccia:

### **Isolamento della macchina infetta:**

Isolare la macchina infetta impedisce al malware di propagarsi ulteriormente nella rete, proteggendo l'integrità e la confidenzialità dei dati su altre macchine, di conseguenza andremo a disconnettere immediatamente la macchina infetta dalla rete e avvieremo protocolli di isolamento per prevenirne la diffusione.

### **Attivazione del server ridondante:**

Per mantenere la disponibilità del servizio attiveremo un server ridondante, questo garantisce che gli utenti possano continuare a utilizzare l'applicazione senza interruzioni, mantenendo l'accessibilità del servizio.

Questo server ridondante permetterà di ridurre i tempi di inattività essendo pronto a subentrare in caso di emergenza.

Una volta effettuata questa implementazione ci si dovrà assicurare che il server ridondante sia costantemente aggiornato e sincronizzato con il server principale.

Si dovrà configurare il sistema per attivare automaticamente il server ridondante in caso di isolamento del server principale.

si dovrà verificare che il server ridondante sia completamente operativo e accessibile dagli utenti.

## **Analisi forense:**

L'analisi forense ci permetterà di capire come il malware ha infettato il sistema e quali dati potrebbero essere stati compromessi, aiutando a prevenire futuri incidenti e migliorando le difese esistenti.

Andremo a stilare un report documentando le scoperte ed identificando i vettori d'attacco.

## **Ripristino da backup:**

Andremo a ripristinare il sistema utilizzando backup verificati e aggiornati, assicurandoci che il malware sia completamente rimosso prima del ripristino.

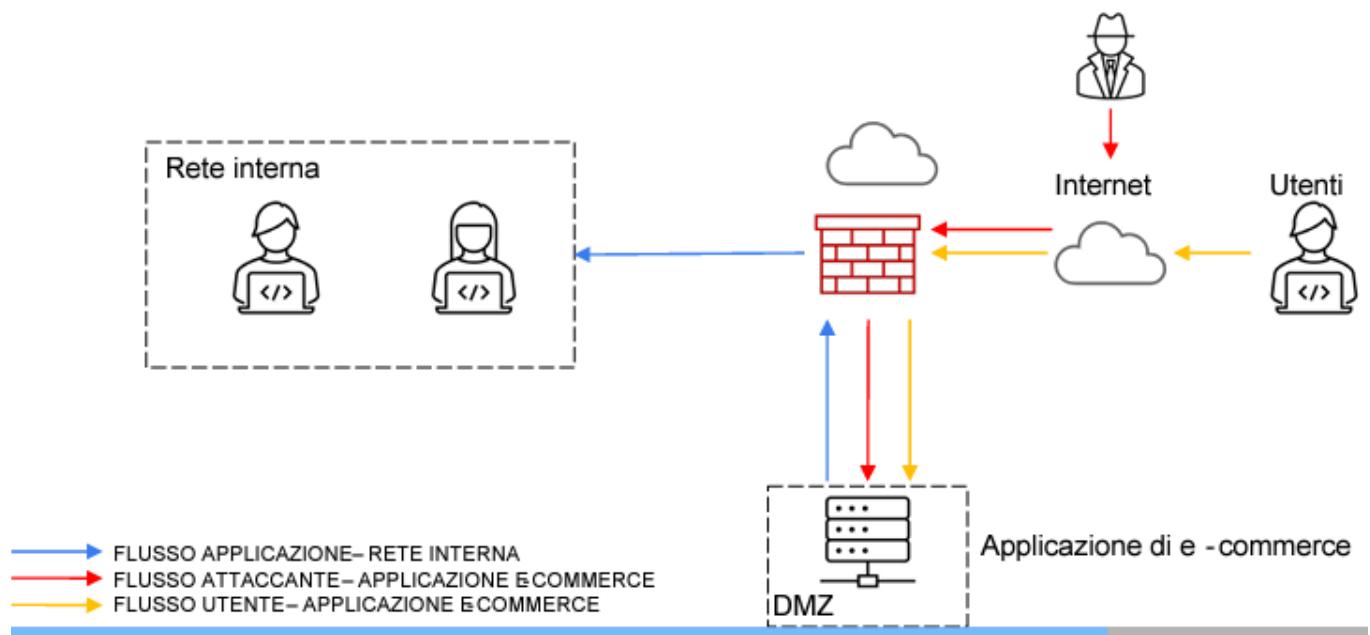
Utilizzare backup puliti assicura che il sistema possa essere ripristinato senza il rischio di reinfezione, mantenendo l'integrità del sistema.

Una volta ripristinata la web app si dovranno utilizzare strumenti di monitoraggio come SIEM (Security Information and Event Management) per raccogliere e analizzare i log di sistema in tempo reale.

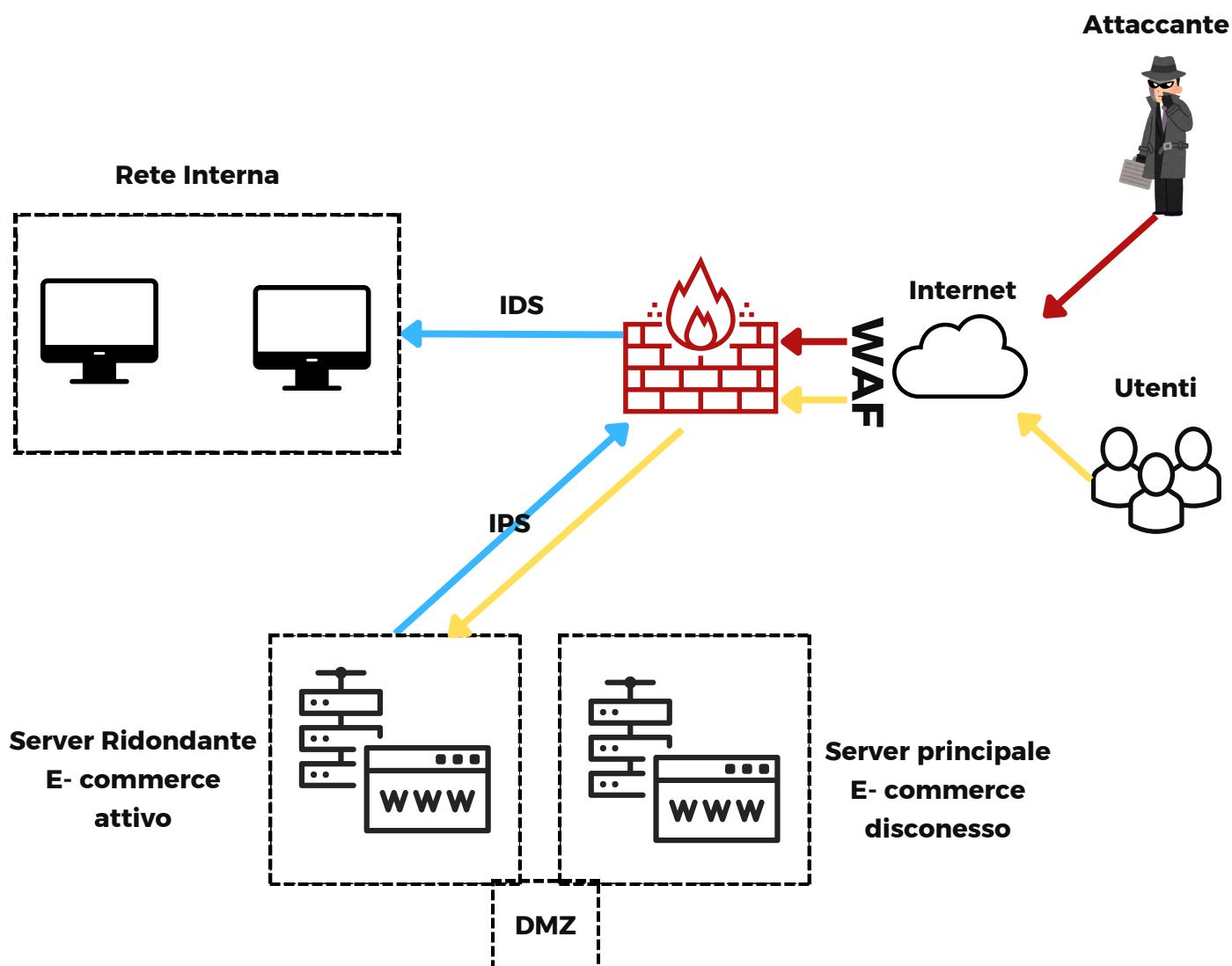
Implementare regole di monitoraggio specifiche per rilevare comportamenti anomali e potenziali tentativi di propagazione di nuovi malware.

# Schema di rete aggiornato alle implementazioni e azioni usate per prevenire l'attacco DDoS e l'infezione malware

## Schema di rete iniziale:



## Schema di rete aggiornato:



## Modifica “più aggressiva” dell’infrastruttura di rete

**Si possono applicare le seguenti modifiche:**

### **Monitoraggio continuo:**

Il monitoraggio continuo permette di rilevare attività anomale in tempo reale, migliorando la capacità di rispondere rapidamente agli incidenti e mantenendo la confidenzialità e l'integrità dei dati.

E' importante quindi implementare strumenti di monitoraggio come SIEM (Security Information and Event Management) per raccogliere e analizzare i log di sistema in tempo reale, permettendo una risposta immediata agli incidenti.

### **Sicurezza a più livelli:**

Utilizzare una combinazione di firewall, IDS/IPS e soluzioni antivirus avanzate crea una difesa a più livelli che aumenta la sicurezza complessiva dell'infrastruttura.

Quindi è necessario configurare firewall per controllare il traffico in entrata e in uscita, utilizzare IDS/IPS per rilevare e prevenire intrusioni, e installare soluzioni antivirus su tutti i sistemi per rilevare e rimuovere malware.

### **Formazione del personale:**

Il personale addestrato può riconoscere e rispondere rapidamente agli incidenti di sicurezza, riducendo il rischio di errore umano e migliorando la confidenzialità e l'integrità dei dati.

Quindi è essenziale fornire formazione continua e aggiornamenti regolari al personale su best practice di sicurezza e protocolli di risposta agli incidenti.

## Schema di rete completo

Flusso web app - rete interna

Flusso internet/utenti - web app



Server  
ridondante

Server  
Principale

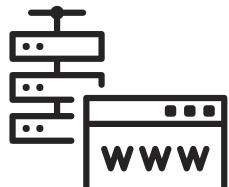
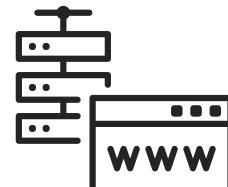
Internet

WAF



IPS

DMZ



IDS

IDS

Rete Interna



# Report e analisi delle segnalazioni “any run”

Analizzando tutti gli screen presenti su any run di questa segnalazione possiamo notare:

The screenshot shows a Windows 7 desktop environment. A central window titled "Administrator: PERFORMANCE BOOSTER\_v3.6.exe" displays a series of numbered steps for system optimization, such as pressing keys like F10, F11, and F12. Below this window, a message says "MOVE YOUR MOUSE TO VIEW SCREENSHOTS". At the bottom of the screen, there is a taskbar with icons for various applications like FileZilla Client, Microsoft Edge, and Google Chrome. On the left side, there is a sidebar with options like "New analysis", "Public reports", and "FAQ". The main part of the screen shows a network traffic analysis interface with tabs for "HTTP Requests", "Connections", "DNS Requests", and "Threats". Under the "Connections" tab, several UDP connections are listed, primarily from the local host (192.168.100.255) to port 137. The "Threats" tab shows no results. At the bottom, a warning message states "[668] cmd.exe Runs PING.EXE to delay simulation". To the right of the desktop, there is a separate window titled "Malicious activity" which provides detailed analysis of the malware sample, including its MD5 hash, start time, and a list of processes running on the system.

Il file "PERFORMANCE BOOSTER\_v3.6.exe" è stato eseguito su un sistema Windows 7, l'analisi tramite Any.Run indica che si tratta di un'attività potenzialmente dannosa.

## Esecuzione comandi:

si possono osservare vari comandi eseguiti tramite **cmd.exe** e **powershell.exe**, questi comandi includono modifiche alle impostazioni di sistema, esecuzione di script PowerShell.

## Attività di Rete:

sono presenti connessioni **UDP** a diversi indirizzi IP esterni, suggerendo che il malware stia comunicando con server remoti.

La finestra del comando mostra messaggi e avvisi minacciosi, probabilmente per intimidire l'utente e prevenire interventi sul sistema infetto.

Il malware "PERFORMANCE BOOSTER\_v3.6.exe" sembra progettato per ottenere accesso remoto data la presenza di connessioni a server remoti e l'esecuzione di comandi di sistema suggeriscono che il malware potrebbe essere utilizzato per controllare il sistema da remoto comportamento tipico di una backdoor.

Di conseguenza molto probabilmente tenterà di:

- Disabilitare punti di ripristino e modificare le impostazioni di sicurezza del sistema per prevenire la sua rimozione e mantenere l'accesso.
- Eseguire comandi e script sul sistema infetto, il che può includere il download di ulteriori malware, esfiltrazione di dati, o altre attività dannose.
- Utilizzare connessioni di rete per comunicare con server remoti, ricevere istruzioni e inviare dati rubati.

## Secondo caso:

Analizzando tutti gli screen presenti su any run di questa segnalazione possiamo notare:

The screenshot shows two windows side-by-side. On the left is a Microsoft Edge browser window with a URL like <https://1drv.ms/u/s!At7eQ7h8kx6-nQM1...>. The page content includes a large blue crane icon, a message 'It's time to update your browser.', and a button 'MOVE YOUR MOUSE TO VIEW SCREENSHOTS'. Below the browser is a taskbar with icons for Start, Task View, File Explorer, and others. On the right is a Malicious activity analysis interface titled 'Win7 32 bit Complete'. It shows a timeline with several processes: iexplore.exe, MicrosoftEdgeSetup.exe, MicrosoftEdgeUpdate.exe, and MicrosoftEdgeUpdateSet... All processes are shown in red, indicating they are malicious. The interface also displays network traffic analysis with tables for HTTP Requests and DNS Requests, and a detailed process list.

Il malware viene eseguito tramite il browser Internet Explorer su un sistema Windows 7, la finestra mostra un sito di OneDrive falso con un messaggio che invita ad aggiornare il browser.

## Esecuzione:

Il malware scarica ed esegue un file chiamato **MicrosoftEdgeSetup.exe**, che finge di essere un installer legittimo di Microsoft Edge successivamente vengono eseguiti anche diversi file **MicrosoftEdgeUpdate.exe**, suggerendo che il malware sta tentando di sembrare legittimo.

Sono presenti connessioni **HTTP** e **DNS** a vari domini, inclusi **ctldl.windowsupdate.com** e **ocsp.digicert.com**, suggerendo che il malware sta cercando di imitare comportamenti legittimi per nascondere le sue attività.

Il file **MicrosoftEdgeUpdate.exe** esegue controlli sulle impostazioni di fiducia di Windows, probabilmente per assicurarsi che il download e l'installazione possano procedere senza essere bloccati da politiche di sicurezza.

### Potenziale Violazione della Privacy:

Questo avviso indica una possibile violazione della privacy aziendale, segnalando che svchost.exe potrebbe essere coinvolto in attività sospette come il download di file PE (Portable Executable).

| HTTP Requests   | 13                                    | Connections | 44 | DNS Requests | 19           | Threats  | 1 | Filter by message | PCAP |
|---|---------------------------------------|-------------|----|--------------|--------------|--|---|-------------------|------|
| Timeshift   | Class                                 |             |    | PID          | Process name | Message  |   |                   |      |
| 32509 ms  | Potential Corporate Privacy Violation |             |    | 856          | svchost.exe  | ET POLICY PE EXE or DLL Windows file download HTTP |   |                   |      |
| <b>Warning</b> [3408] MicrosoftEdgeUpdate.exe Checks Windows Trust Settings |                                       |             |    |              |              |  |   |                   |      |

### Ipotesi di funzionamento

Questo malware è stato creato per imitare un software legittimo, di conseguenza una persona va a scaricare ed eseguire software falso che imita programmi legittimi come Microsoft Edge andando ad ingannare l'utente e camuffare le sue attività dannose.

Sembra riuscire anche a stabilire connessioni a server esterni, includendo l'utilizzo di domini affidabili per ridurre i sospetti e consentire il download di altri componenti malware.

Riesce anche a modificare le impostazioni di sicurezza per assicurarsi che le sue attività non siano bloccate da politiche di sicurezza esistenti nel dispositivo infetto.