

EVILCORP
IF IT WORKS DONT TOUCH IT

REPORT

BY EVILCORP

Scritto da: Andrea Di Benedetto

Graphic Designer: Lorenzo Franchi

Direttore Tecnico: Samuele Aversa

Approvato da: Mario Reitano

Giugno 2024

INDICE S9

L0	
Chi siamo	1
Missione e Visione Aziendale.....	2
Regole di Ingaggio	3
Team Group.....	4
Nostri Prezzi	5
L1	
Obiettivo	6
Configurazione VM	7
V.A. con Firewall Disattivato	8
V.A. con Firewall Attivato.....	10
Conclusioni	12
L2	
Obiettivo	13
Glossario	14
Analisi Formula.....	15
Casistica Incendio	16
Casistica Terremoto	17
Casistica Inondazione.....	18
Conclusioni	19
L3	
Obiettivo	27
IOC & Wireshark	28
Identificazione IOC	29
Potenziali vettori d'attacco.....	31
Confronto Purge & Destroy	32
Prevenzione	33
Conclusioni	33
L4	
Obiettivo	27
lIncident Response	28
Identificazione IOC	29
Potenziali vettori d'attacco.....	31
Confronto Purge & Destroy	32
Prevenzione	33
Conclusioni	33
L5	
Obiettivo	34
Azione Preventive per SQLi e XSS.....	36
Impatti sul Buisness	38
Response	40
Soluzione completa	42
Modifica Aggressiva.....	43
Analisi Anyrun	45
Conclusioni	61



Chi siamo

Nome Azienda: EvilCorp
Settore: Amministrazione

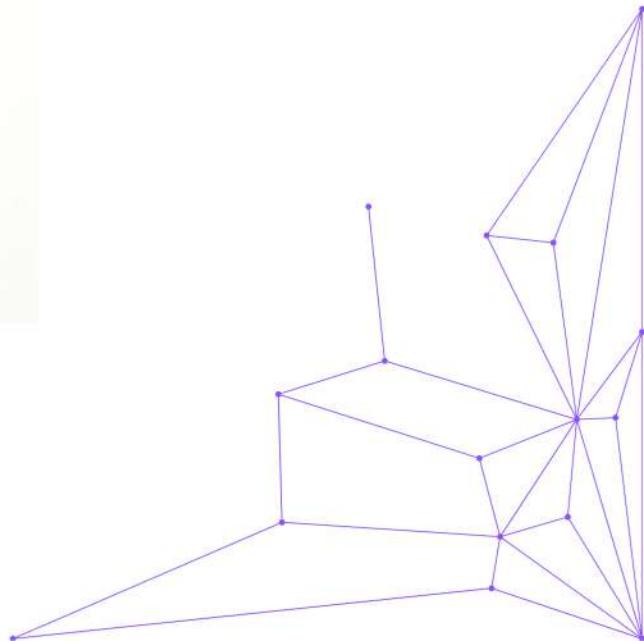
Descrizione dell'Azienda

EvilCorp è un'azienda immaginaria che si occupa di amministrazione. EvilCorp fornisce servizi di amministrazione per altre aziende, gestendo dati sensibili e informazioni riservate. La sicurezza delle loro reti e dei loro dati è cruciale per mantenere la fiducia dei loro clienti e rispettare le normative.



Missione e visione aziendale

Come parte del nostro impegno per garantire la sicurezza informatica, EvilCorp ha incaricato un team di pentester di eseguire un Vulnerability Assessment e un Penetration Testing della rete aziendale. Questo report descrive il processo e le regole di ingaggio, nonché una bozza dei costi operativi.



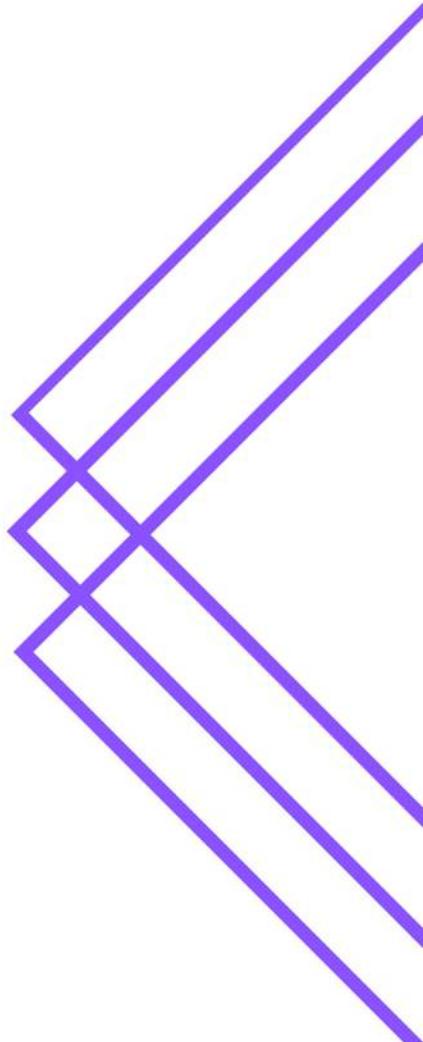
Regole di ingaggio

Le regole di ingaggio definiscono i limiti e le aspettative del nostro lavoro di pentesting. Di seguito sono riportate le regole stabilite per questo incarico:

- 1. Autorizzazione:** EvilCorp ha fornito l'autorizzazione scritta per eseguire la scansione e i test di penetrazione sulla loro rete.
- 2. Scopo del Test:** Le scansioni verranno effettuate solo sugli indirizzi IP forniti dall'azienda.
- 3. Preventivo:** Viene stilato un preventivo del lavoro completo.
- 4. Perimetro d'azione:** Si determina l'area della rete aziendale su cui effettuare i test.
- 5. Ore di Lavoro:** Il team lavorerà dalle 9:00 alle 17:00, dal lunedì al venerdì.
- 6. Impatto sul Sistema:** I test saranno condotti in modo da minimizzare qualsiasi impatto sui sistemi di produzione.
- 7. Riservatezza:** Tutte le informazioni raccolte durante il test saranno mantenute riservate e utilizzate solo ai fini del test.
- 8. Strumenti:** Si presentano gli strumenti utilizzati dai pentester per effettuare l'analisi di rete.

Team Group

Siamo un piccolo team di quattro professionisti, ognuno con una solida esperienza nel campo della cybersecurity. La nostra combinazione di competenze specifiche ci permette di affrontare efficacemente le sfide del settore, assicurando soluzioni innovative e sicure per proteggere al meglio i nostri sistemi e dati.



REFERENCE LINKEDIN

Cliccando sui nostri nomi sarete reindirizzati sulle nostre pagine linkedin



[Andrea
Di Benedetto](#)



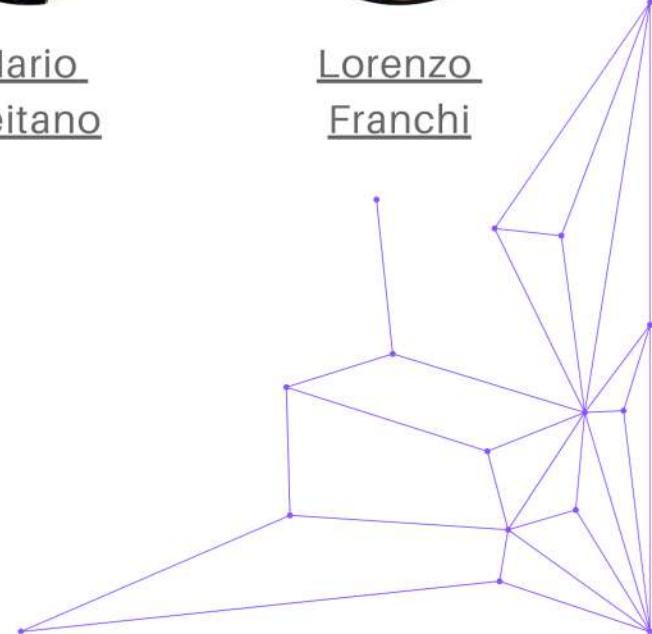
[Samuele
Aversa](#)



[Mario
Reitano](#)



[Lorenzo
Franchi](#)



Budget per il progetto

Nome lavoratore	Responsabilità	Costo Stimato per Settimana
Andrea Di Benedetto	Capo Team, Responsabile della Sicurezza Informatica	\$1,400
Samuele Aversa	Assistenza nella gestione degli incidenti, conduzione delle indagini preliminari	\$1,000 - \$1,200
Lorenzo Franchi	Supporto nelle valutazioni delle vulnerabilità, test di penetrazione di base	\$1,000 - \$1,200
Mario Reitano	Assistenza nella progettazione di soluzioni di rete sicure, gestione di base del firewall	\$1,000 - \$1,200

Costo Stimato Totale per Una Settimana per Quattro Agenti Junior:

Ruolo	Costo Minimo per Settimana	Costo Massimo per Settimana
Andrea Di Benedetto	\$1,400	\$1,600
Samuele Aversa	\$1,000	\$1,200
Lorenzo Franchi	\$1,000	\$1,200
Mario Reitano	\$1,000	\$1,200

Andrea Di Benedetto (Capo Team, Responsabile della Sicurezza Informatica):

Salario Settimanale: \$1,400 - \$1,600

Andrea ricopre un ruolo chiave come capo team, guidando le operazioni del nostro team di sicurezza informatica. Le sue responsabilità di leadership e le competenze specializzate giustificano un salario competitivo in questo range.

Altri Junior Agenti Cybersecurity (Samuele Aversa, Lorenzo Franchi, Mario Reitano):

Salario Settimanale: \$1,000 - \$1,200 ciascuno

Questi membri del team forniscono un supporto essenziale con le loro responsabilità specifiche, che includono la gestione degli incidenti, le valutazioni delle vulnerabilità e la progettazione di soluzioni di rete sicure. I loro salari riflettono le competenze richieste per i rispettivi ruoli e la competitività del mercato.

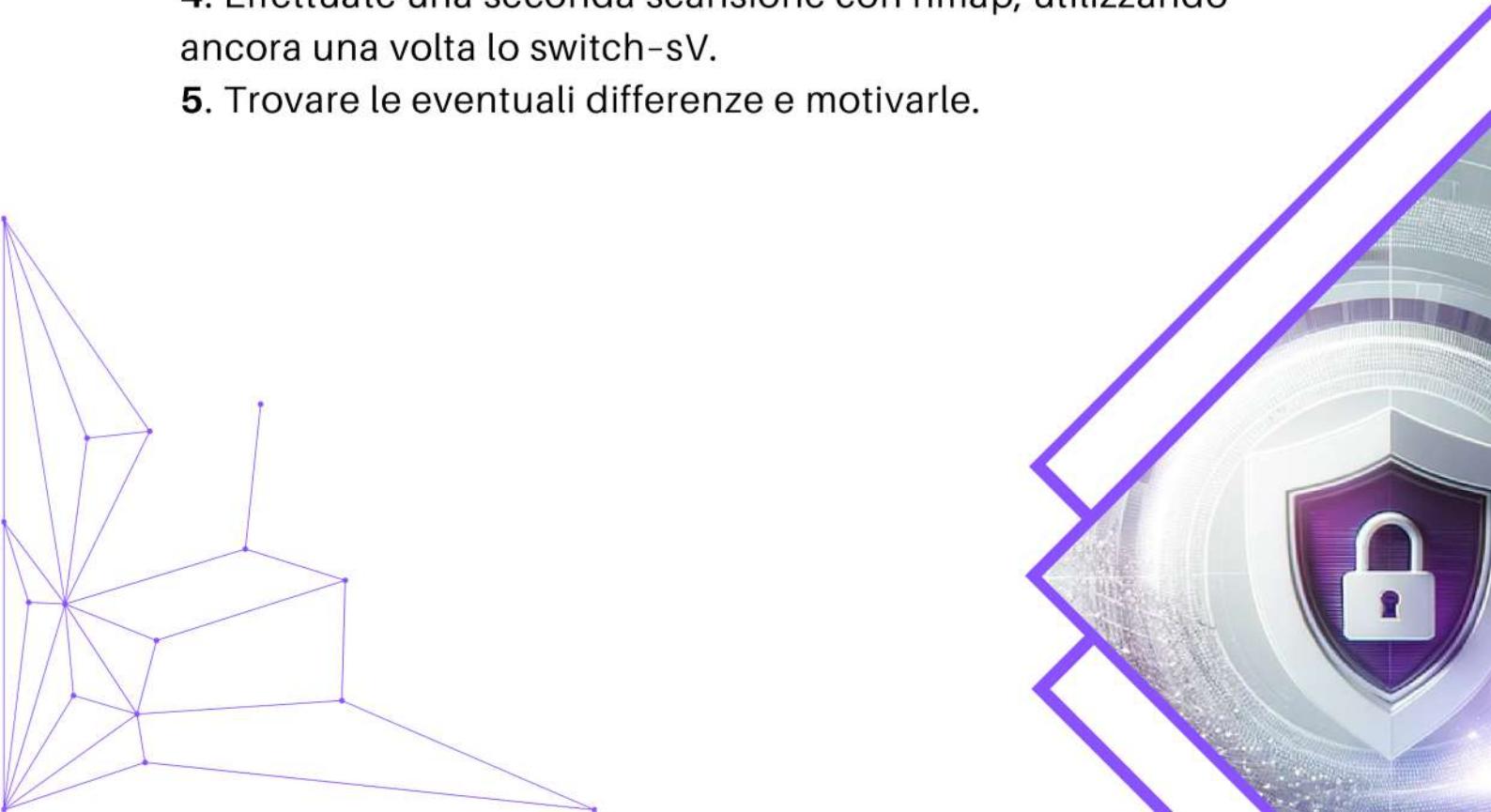
Ruolo	Costo Totale per Settimana (Minimo)	Costo Totale per Settimana (Massimo)
Andrea Di Benedetto	\$1,400	\$1,600
Altri Junior Agenti	\$3,000	\$3,600
Totale	\$4,400	\$5,200

L1

Durante la lezione teorica, abbiamo studiato le azioni preventive per ridurre la possibilità di attacchi provenienti dall'esterno. Abbiamo visto che a livello di rete, possiamo attivare / configurare Firewall e regole per fare in modo che un determinato traffico, potenzialmente dannoso, venga bloccato. La macchina Windows XP 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:

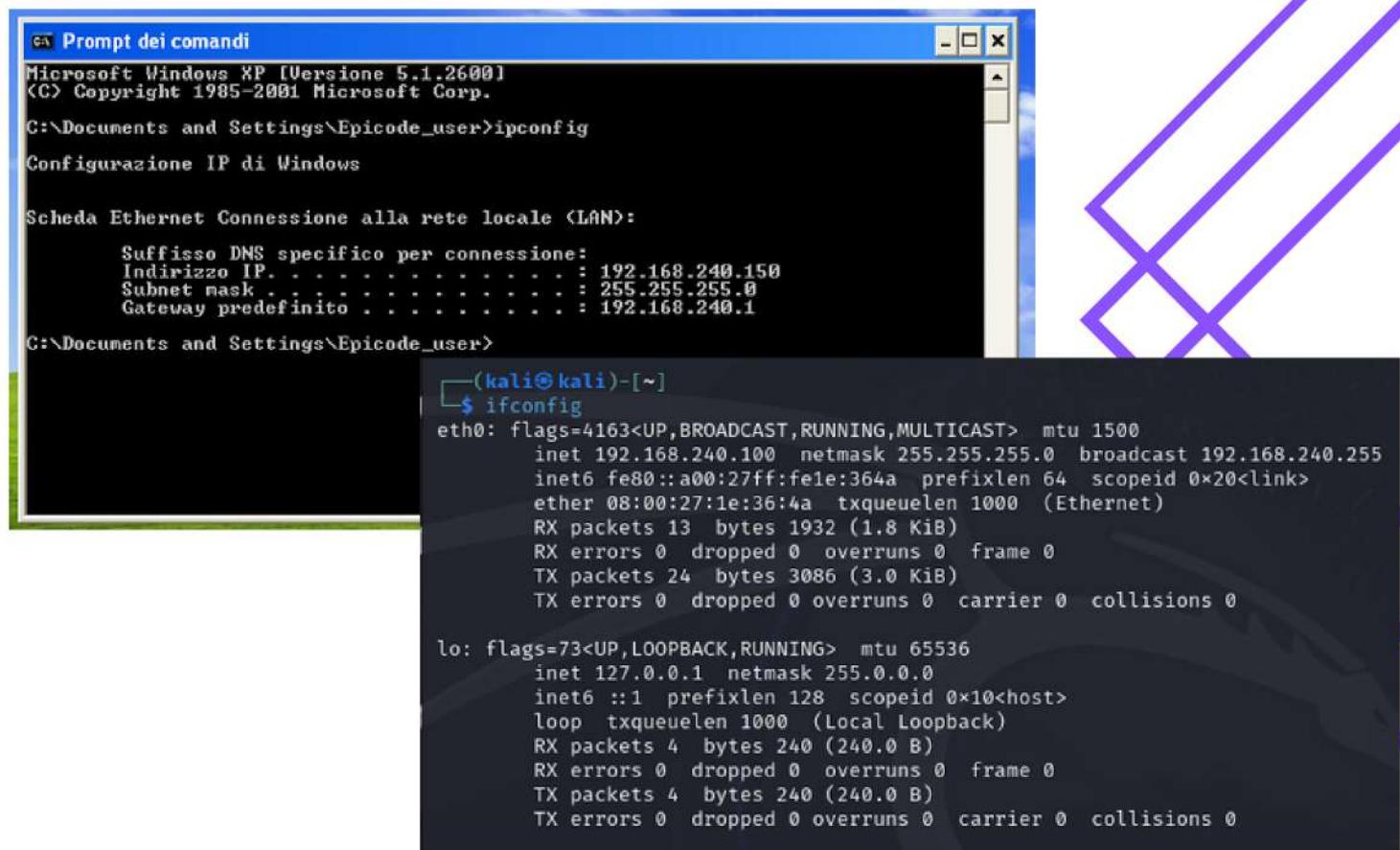
- 1.** Assicuratevi che il Firewall sia disattivato sulla macchina Windows XP
- 2.** Effettuate una scansione con nmap sulla macchina target (utilizzate lo switch-sV, per la service detection e -o nomefilereport per salvare in un file l'output)
- 3.** Abilitare il Firewall sulla macchina Windows XP
- 4.** Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch-sV.
- 5.** Trovare le eventuali differenze e motivarle.



Configurazione VM

Inizialmente si impostano gli indirizzi IP della macchina Kali e Windows XP rispettivamente a 192.168.240.100 e 192.168.240.150, così come richiesto dalla traccia. Per fare ciò si è andato a modificare il file interfaces al PATH /etc/network/ con il comando **<sudo nano /etc/network/interfaces>**.

Dopo aver fatto un reboot delle macchine, il comando **<ifconfig>** su Kali e il comando **<ipconfig>** su Windows XP dimostra l'effettivo cambio di indirizzi IP.



```

Windows XP Command Prompt (ipconfig output):
Microsoft Windows XP [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Epicode_user>ipconfig

Configurazione IP di Windows

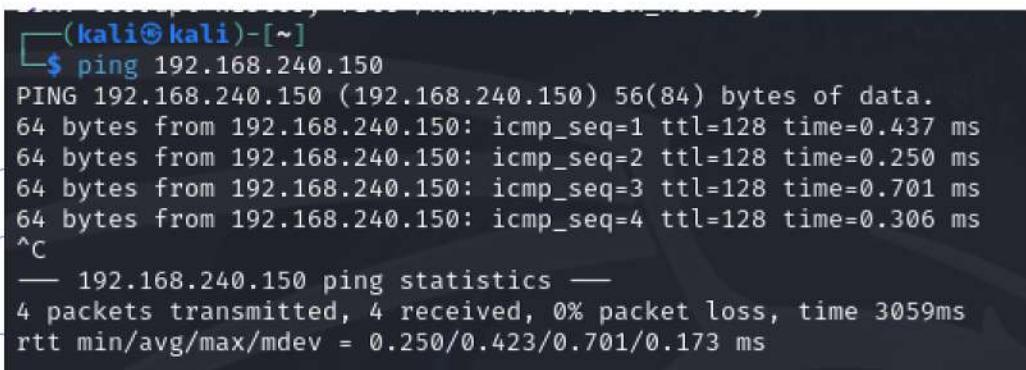
Scheda Ethernet Connessione alla rete locale (LAN):
  Suffisso DNS specifico per connessione:
    Indirizzo IP. . . . . : 192.168.240.150
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.240.1

Kali Linux Terminal (ifconfig output):
(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 13 bytes 1932 (1.8 KiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 24 bytes 3086 (3.0 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

```

Per verificare che le due macchine sono connesse tra loro si effettua un ping con il comando **<ping indirizzo_ip_WinXP>**



```

(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=0.437 ms
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=0.250 ms
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=0.701 ms
64 bytes from 192.168.240.150: icmp_seq=4 ttl=128 time=0.306 ms
^C
--- 192.168.240.150 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3059ms
rtt min/avg/max/mdev = 0.250/0.423/0.701/0.173 ms

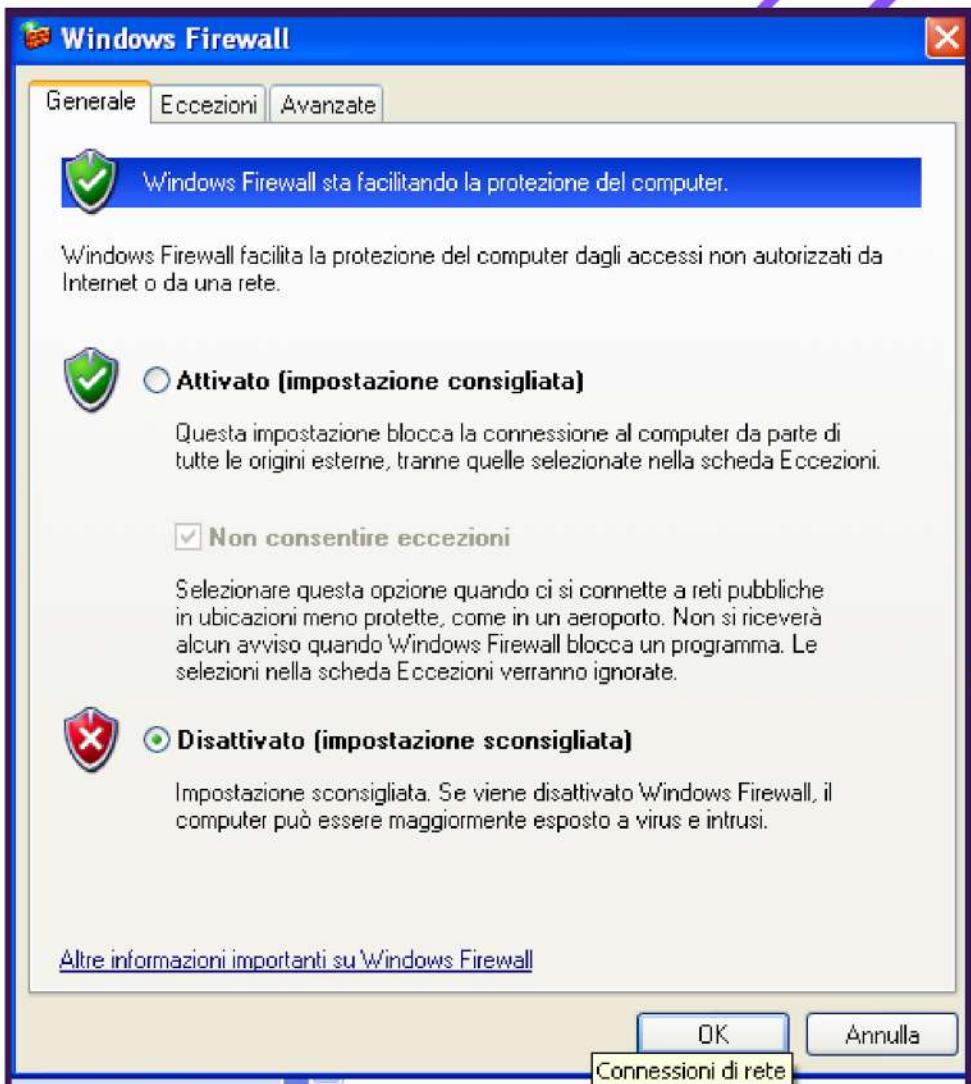
```

V.A. con Firewall

Disattivato

In questa fase viene disattivato il firewall di Windows XP per verificare la sua efficacia in caso di possibili attacchi provenienti dall'estero.

Il firewall di Windows XP è una funzionalità di sicurezza integrata nel sistema operativo progettata per monitorare e controllare il traffico di rete in entrata e in uscita. Funziona bloccando le connessioni non autorizzate e permettendo solo quelle che sono esplicitamente consentite dall'utente o dai programmi installati, contribuendo a proteggere il computer da accessi non autorizzati e attacchi esterni.



V.A. con Firewall Disattivato

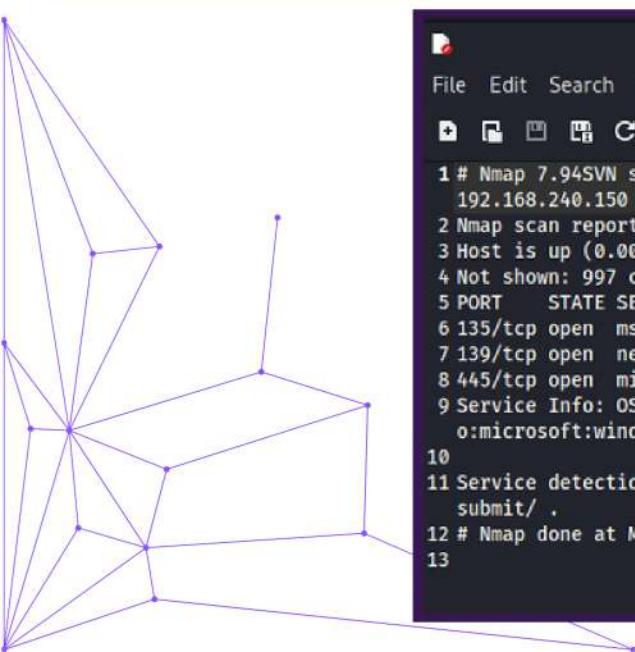
In questa fase viene disattivato il firewall di Windows XP per verificare l'efficacia in caso di possibili attacchi provenienti dall'esterno.

Questo permette di fare una scansione della rete dalla nostra macchina Kali utilizzando lo strumento nmap: con il comando **<nmap -sV indirizzo_ip_WinXP -o report_WinXP>** infatti si è potuta fare una scansione di tutte le porte e servizi attivi sulla macchina target WinXP.

-sV questa opzione permette di rilevare i servizi in esecuzione su ciascun host e di determinare le versioni specifiche di questi servizi.

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.240.150 -o report_winXP
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 10:55 CEST
Nmap scan report for 192.168.240.150
Host is up (0.00027s 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

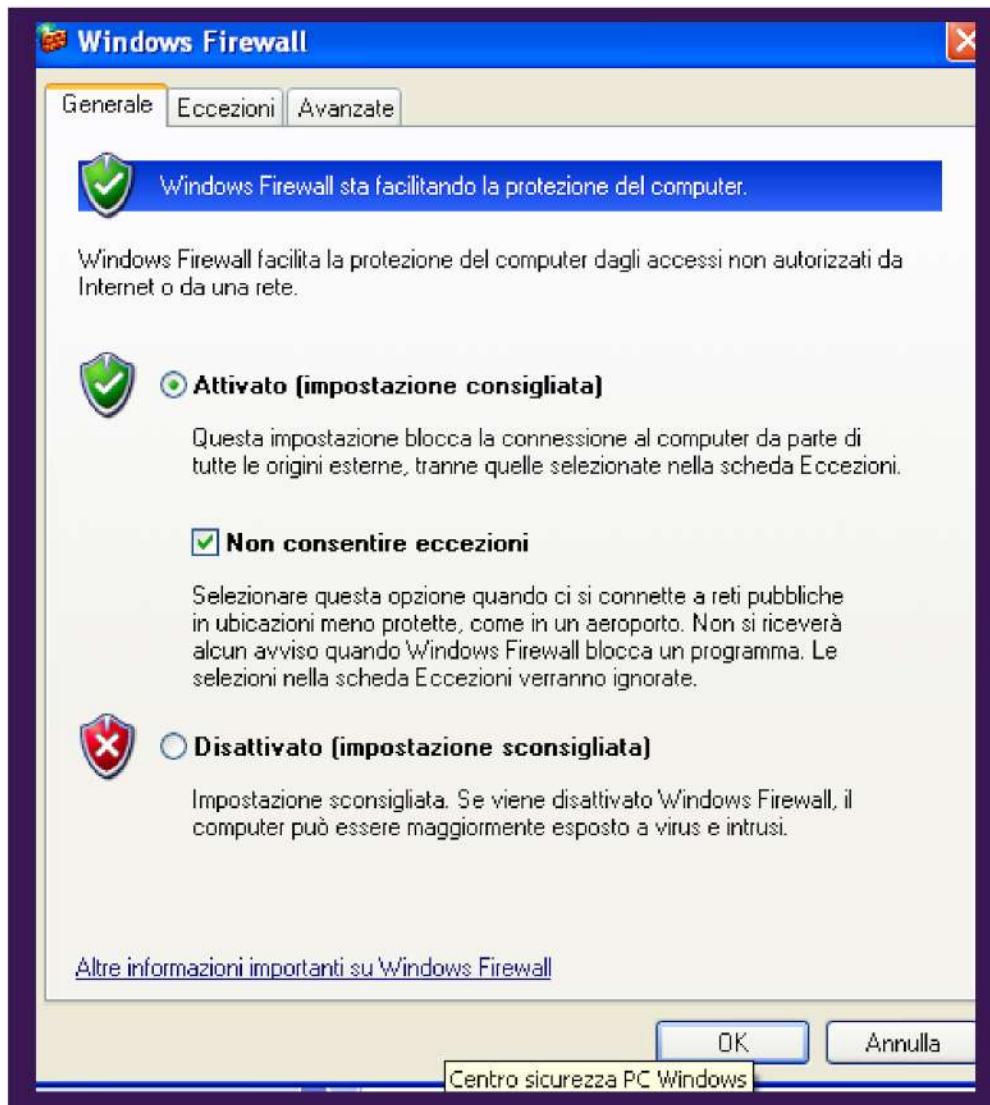
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.39 seconds
```



```
~/report_winXP - Mousepad
File Edit Search View Document Help
File Edit View Insert Document Help
1 # Nmap 7.94SVN scan initiated Mon Jun  3 10:55:45 2024 as: nmap -sV -o report_winXP
192.168.240.150
2 Nmap scan report for 192.168.240.150
3 Host is up (0.00027s latency).
4 Not shown: 997 closed tcp ports (conn-refused)
5 PORT      STATE SERVICE      VERSION
6 135/tcp    open  msrpc        Microsoft Windows RPC
7 139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
8 445/tcp    open  microsoft-ds Microsoft Windows XP microsoft-ds
9 Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp
10
11 Service detection performed. Please report any incorrect results at https://nmap.org/
12 submit/ .
13 # Nmap done at Mon Jun  3 10:56:06 2024 -- 1 IP address (1 host up) scanned in 20.39 seconds
```

V.A. con Firewall Attivo

Successivamente, per verificare l'efficacia del firewall si è rifatta una scansione della rete aziendale con quest'ultimo attivo. A livello di rete, possiamo attivare / configurare Firewall e regole per fare in modo che un determinato traffico, potenzialmente dannoso, venga bloccato.



V.A. con Firewall Attivo

Quando si utilizza Nmap per scansionare un sistema Windows con il firewall attivo, i risultati mostrano in genere meno dettagli sulle porte a causa del blocco operato dal firewall. Durante queste scansioni, è comune trovare:

1. Porte chiuse o filtrate: La maggior parte delle porte viene bloccata dal firewall, risultando inaccessibili o mostrate come chiuse da Nmap.
2. Ritardi nella scansione: Il firewall può causare ritardi o ignorare completamente i pacchetti di scansione, influenzando la velocità e l'efficacia di Nmap.
3. Errori e avvisi: Nmap potrebbe segnalare errori indicando che le porte sono filtrate, suggerendo che il firewall sta impedendo l'accesso.
4. Informazioni limitate sui servizi: Le informazioni raccolte dalle porte aperte sono spesso ridotte, limitando la visibilità dei servizi in esecuzione.
5. False Positivi: Il firewall può causare falsi positivi, facendo apparire alcune porte come chiuse o filtrate anche quando non lo sono.

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.240.150 -o report_winXP_firewall
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 11:05 CEST
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 3.11 seconds
```

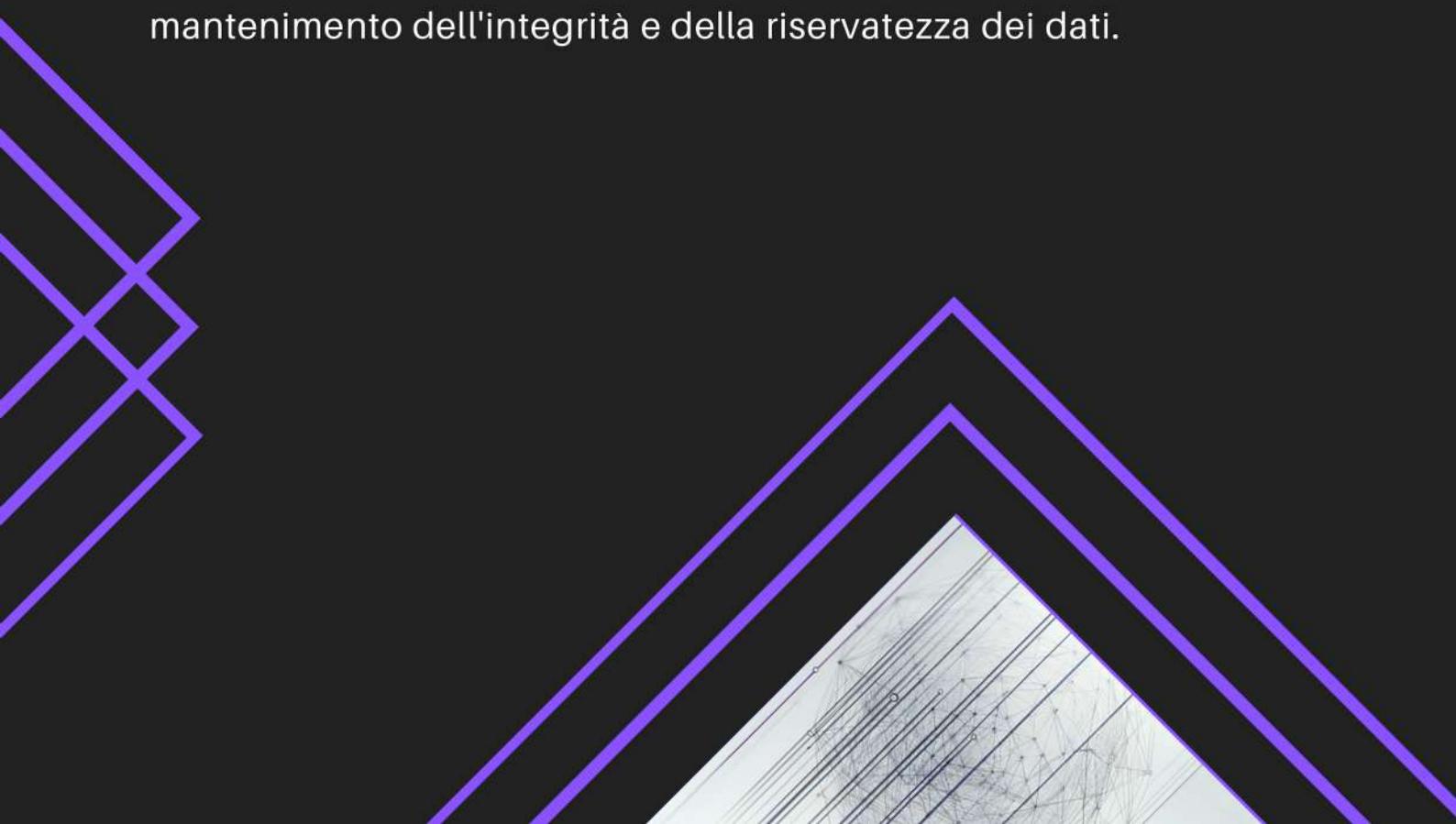


Conclusioni

In conclusione, la scansione Nmap eseguita su un sistema Windows ha rivelato differenze significative nei risultati a seconda dello stato del firewall. Con il firewall disattivato, la scansione ha identificato un numero maggiore di porte aperte e servizi attivi, suggerendo una superficie di attacco più ampia e potenziali vulnerabilità accessibili.

Al contrario, con il firewall attivato, la scansione ha mostrato un numero significativamente ridotto di porte aperte, indicando una protezione più robusta contro accessi non autorizzati. La presenza del firewall ha dimostrato la sua efficacia nel filtrare il traffico di rete e nel proteggere il sistema da potenziali attacchi.

Questi risultati sottolineano l'importanza di mantenere attivo il firewall come componente essenziale della sicurezza di rete. Il confronto tra le due scansioni evidenzia chiaramente il ruolo critico del firewall nella protezione delle risorse del sistema e nel mantenimento dell'integrità e della riservatezza dei dati.



L2

Durante la lezione teorica, abbiamo affrontato gli argomenti riguardanti la business continuity e disaster recovery. Nell'esempio pratico di oggi, ipotizziamo di essere stati assunti per valutare quantitativamente l'impatto di un determinato disastro su un asset di una compagnia. Con il supporto dei dati presenti nelle tabelle che seguono, calcolare la perdita annuale che subirebbe la compagnia nel caso di:

- Inondazione sull'asset «edificio secondario»
- Terremoto sull'asset «datacenter»
- Incendio sull'asset «edificio primario»
- Incendio sull'asset «edificio secondario»
- Inondazione sull'asset «edificio primario»

Dati:

ASSET	VALORE
Edificio primario	350.000€
Edificio secondario	150.000€
Datacenter	100.000€

EVENTO	ARO
Terremoto	1 volta ogni 30 anni
Incendio	1 volta ogni 20 anni
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%

Prima di iniziare

Un **asset** è una risorsa, un bene o un diritto di proprietà che ha un valore economico. Può essere tangibile (immobili, macchinari, merci) o intangibile (marchi, brevetti, competenze). Gli asset sono importanti perché generano valore e sono fondamentali per il successo di un'azienda o individuo.

Le compagnie resilienti predispongono piani e procedure per ridurre gli effetti di un evento catastrofico naturale o di un attacco ed assicurare la continuità operativa, queste pratiche prendono il nome di «business continuity plan» e «disaster recovery».

BUSINESS CONTINUITY PLAN

Il business continuity plan (BCP), piano per la continuità del business, ha lo scopo principale di dettagliare le policy e le procedure per minimizzare gli impatti negativi sull'operatività di una compagnia a valle di un evento catastrofico / attacco, e ad assicurare la continuità delle operazioni svolte dalla compagnia anche in situazioni di emergenza.

Il business continuity plan si compone di quattro step principali:

- Pianificazione e scopo;
- Business impact assessment (BIA), ovvero valutazione degli impatti sul business (può essere qualitativo o quantitativo);
- Business planning, ovvero piano di continuità operativa;
- Approvazione ed implementazione.

DISASTER RECOVERY

Il Disaster recovery planning (DRP) può essere visto come il complemento tecnico al BCP, mentre da un lato il BCP copre le tematiche di governance (pianificazione e gestione), il disaster recovery planning include i controlli tecnici da implementare per la riduzione del rischio e per il recupero dei servizi a valle di un evento catastrofico.



Analisi Formula

Nel business continuity plan, la fase di Business Impact Assessment (BIA) ha lo scopo principale di identificare le risorse critiche di una compagnia e le potenziali minacce alle quali esse sono esposte. Durante questa fase avviene l'identificazione delle priorità e dei rischi, la valutazione delle probabilità e degli impatti.

In questo esercizio ci si è concentrati su una valutazione quantitativa degli impatti di un determinato disastro su un asset della compagnia. A tal fine sono stati usati le seguenti definizioni:

- **Annualized Rate of Occurrence (ARO)**: indica il tasso annuale di occorrenza di un evento e la sua probabilità è espressa in numero di volte che l'evento si è verificato nel corso di un anno.
- **Exposure Factor (EF)**: indica la percentuale di asset che verrebbe impattato a seguito del verificarsi di un determinato evento.
- **Single Loss Expectancy (SLE)**: dà 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):

$$\text{SLE} = \text{AV} * \text{EF}$$

- **Annualized Loss Expectancy (ALE)**: il valore della perdita subita in un arco temporale di un anno, che si calcola come:

$$\text{ALE} = \text{SLE} * \text{ARO}$$

«tabella di riferimento»

INCENDIO

Danni agli asset in caso di incendio:

1. Strutturali:

- Crolli parziali o totali di pareti, solai e tetti.
- Compromissione della stabilità strutturale a causa del calore.

2. Non strutturali:

- Distruzione di mobili, attrezzature e arredi.
- Danni agli impianti elettrici, idraulici e di condizionamento.

3. Infrastrutturali:

- Rottura di tubazioni e condutture, causando perdite di acqua o gas.
- Danni a strade, ponti e altre infrastrutture adiacenti.

Prevenzione dei danni agli asset in caso di incendio:

1. Strutturali:

- Utilizzo di materiali ignifughi.
- Installazione di barriere antincendio.
- Manutenzione regolare delle strutture.

2. Non strutturali:

- Installazione di sistemi di rilevazione e allarme antincendio.
- Utilizzo di arredamenti e attrezzature ignifughi.
- Implementazione di piani di evacuazione e sicurezza.

3. Infrastrutturali:

- Ispezione e manutenzione regolare delle tubazioni.
- Installazione di sistemi di spegnimento automatico (sprinkler).
- Creazione di vie di fuga e accessi per i mezzi di soccorso.

Incendio

Asset	Valore dell'asset	Fattore di esposizione	Frequenza ARO	Perdita annuale
Edificio Primario	€350.000	60%	1/20 anni (0,05)	€10.500
Edificio Secondario	€150.000	50%	1/20 anni (0,05)	€3.750
Datacenter	€100.000	60%	1/20 anni (0,05)	€3.000

FORMULE UTILIZZATE:

$$SLE = AV * EF$$

$$ALE = SLE * ARO$$

«tabella di riferimento»

TERREMOTO

Danni agli asset in caso di terremoto:

1. Strutturali:

- Crolli parziali o totali delle fondamenta, pareti, solai e tetti.
- Crepe e fratture in muri, travi e colonne.
- Deformazioni delle strutture portanti.

2. Non strutturali:

- Caduta di mobili, scaffali e apparecchiature.
- Danni agli impianti elettrici, idraulici e di condizionamento.

3. Infrastrutturali:

- Rottura delle tubazioni, causando perdite d'acqua o gas.
- Danni a strade, ponti e ferrovie, ostacolando soccorsi ed evacuazioni.

Prevenzione dei danni agli asset in caso di terremoto:

1. Strutturali:

- Progettazione antisismica.
- Utilizzo di materiali resistenti.
- Retrofit sismico per edifici esistenti.

2. Non strutturali:

- Ancoraggio di mobili e apparecchiature.
- Barriere antisismiche per finestre e porte.

3. Infrastrutturali:

- Rafforzamento delle tubazioni.
- Manutenzione e rinforzo di strade e ponti.

Terremoto

Asset	Valore dell'asset	Fattore di esposizione	Frequenza ARO	Perdita annuale
Edificio Primario	€350.000	80%	1/30 anni (~0,03)	€8.400
Edificio Secondario	€150.000	80%	1/30 anni (~0,03)	€3.600
Datacenter	€100.000	95%	1/30 anni (~0,03)	€2.850

FORMULE UTILIZZATE:

$$SLE = AV * EF$$

$$ALE = SLE * ARO$$

«tabella di riferimento»

INONDAZIONE

Danni agli asset in caso di inondazione:

1. Strutturali:

- Danni alle fondamenta, pareti e pavimenti.
- Erosione e indebolimento delle strutture portanti.

2. Non strutturali:

- Distruzione di mobili, attrezzature e arredi.
- Danni agli impianti elettrici, idraulici e di condizionamento.

3. Infrastrutturali:

- Rottura di tubazioni e condutture, causando perdite di acqua o gas.
- Danni a strade, ponti e altre infrastrutture adiacenti.

Prevenzione dei danni agli asset in caso di inondazione:

1. Strutturali:

- Costruzione sopra il livello di piena.
- Utilizzo di materiali resistenti all'acqua.
- Installazione di barriere contro l'acqua e sistemi di drenaggio.

2. Non strutturali:

- Sollevamento di mobili e attrezzature da terra.
- Utilizzo di materiali impermeabili per arredi e finiture.
- Implementazione di sistemi di rilevazione e allarme per inondazioni.

3. Infrastrutturali:

- Manutenzione e miglioramento dei sistemi di drenaggio e delle condutture.
- Creazione di argini e bacini di contenimento.
- Pianificazione di vie di fuga e accessi per i mezzi di soccorso.

Inondazione

Asset	Valore dell'asset	Fattore di esposizione	Frequenza ARO	Perdita annuale
Edificio Primario	€350.000	55%	1/50 anni (0,02)	€3.850
Edificio Secondario	€150.000	40%	1/50 anni (0,02)	€1.200
Datacenter	€100.000	35%	1/50 anni (0,02)	€700

FORMULE UTILIZZATE:

$$SLE = AV * EF$$

$$ALE = SLE * ARO$$

CONCLUSIONI

Infine i costi per queste calamità naturali sono purtroppo molto alti. Raccomandiamo di tenere dei fondi in caso di emergenza e invitiamo caldamente a eseguire dei controlli annuali per il mantenimento delle infrastrutture. Avere una buona formazione del personale è essenziale in caso di emergenza e potrebbe salvare molte vite.

Scenario	Asset	Valore dell'asset	Fattore di esposizione	Frequenza ARO	Perdita annuale
Terremoto su "Edificio primario"	Edificio Primario	€350.000	80%	1/30 anni (~0,03)	€8.400
Incendio su "Edificio primario"	Edificio Primario	€350.000	60%	1/20 anni (0,05)	€10.500
Inondazione su "Edificio primario"	Edificio Primario	€350.000	55%	1/50 anni (0,02)	€3.850
Terremoto su "Edificio secondario"	Edificio Secondario	€150.000	80%	1/30 anni (~0,03)	€3.600
Incendio su "Edificio secondario"	Edificio Secondario	€150.000	50%	1/20 anni (0,05)	€3.750
Inondazione su "Edificio secondario"	Edificio Secondario	€150.000	40%	1/50 anni (0,02)	€1.200
Terremoto su "Datacenter"	Datacenter	€100.000	95%	1/30 anni (~0,03)	€2.850
Incendio su "Datacenter"	Datacenter	€100.000	60%	1/20 anni (0,05)	€3.000
Inondazione su "Datacenter"	Datacenter	€100.000	35%	1/50 anni (0,02)	€700

L3

Durante la lezione teorica, abbiamo visto la Threat Intelligence e gli indicatori di compromissione. Abbiamo visto che gli IOC sono evidenze o eventi di un attacco in corso, oppure già avvenuto. Per l'esercizio pratico di oggi, trovate in allegato una cattura di rete effettuata con Wireshark. Analizzate la cattura attentamente e rispondere ai seguenti quesiti:

Identificare eventuali IOC, ovvero evidenze di attacchi in corso

In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati

Consigliate un'azione per ridurre gli impatti dell'attacco

76 36.777473018	192.168.200.100	192.168.200.150	TCP	74 36138 → 580 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
77 36.777522494	192.168.200.100	192.168.200.150	TCP	74 52428 → 962 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
78 36.777623082	192.168.200.150	192.168.200.100	TCP	60 98 → 34120 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
79 36.777623149	192.168.200.150	192.168.200.100	TCP	60 78 → 49780 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
80 36.777645027	192.168.200.100	192.168.200.150	TCP	74 41874 → 764 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
81 36.777680898	192.168.200.100	192.168.200.150	TCP	74 51506 → 435 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
82 36.777758636	192.168.200.150	192.168.200.100	TCP	60 580 → 36138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
83 36.777758696	192.168.200.150	192.168.200.100	TCP	60 962 → 52428 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
84 36.777871245	192.168.200.150	192.168.200.100	TCP	60 764 → 41874 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
85 36.777871293	192.168.200.150	192.168.200.100	TCP	60 435 → 51506 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
86 36.777893298	192.168.200.100	192.168.200.150	TCP	66 33042 → 445 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0
87 36.777912717	192.168.200.100	192.168.200.150	TCP	66 46990 → 139 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0
88 36.777986759	192.168.200.100	192.168.200.150	TCP	66 60632 → 25 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 1
89 36.778031265	192.168.200.100	192.168.200.150	TCP	66 37282 → 53 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 1
90 36.778179978	192.168.200.100	192.168.200.150	TCP	74 51450 → 148 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
91 36.778200161	192.168.200.100	192.168.200.150	TCP	74 48448 → 806 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA



IOC & Wireshark

Gli **IOC (Indicator Of Compromise)** sono degli indicatori, ovvero dei segnali che indicano la possibilità che un sistema informatico o una rete siano stati compromessi da attività malevole. Tali segnali vengono utilizzati per ricostruire uno storico e capire cosa è successo. Gli esperti di sicurezza informatica utilizzano gli ioc per individuare, riconoscere ed eliminare le minacce, tra cui malware, attacchi informatici, fughe di dati e altri tipi di compromissione della sicurezza.

La maggior parte degli incidenti di sicurezza vengono identificati grazie all'analisi del traffico di rete che mostra flussi inaspettati o comunque sospetti. Tra le tecniche di recupero flussi di rete ci sono infine i «network monitoring tools», ovvero i software utilizzati per lo sniffing delle comunicazioni su una rete come ad esempio Wireshark.

Wireshark è uno strumento di analisi del traffico di rete che cattura e visualizza i pacchetti in tempo reale ed è utilizzato da amministratori di rete, esperti di sicurezza, sviluppatori di software e studenti per diagnosticare problemi di rete, analizzare protocolli, rilevare vulnerabilità di sicurezza e comprendere il comportamento delle applicazioni di rete. Wireshark intercetta il traffico da diverse interfacce di rete, esamina dettagli dei pacchetti dai livelli più bassi ai più alti, offre filtri potenti per focalizzarsi su pacchetti specifici, supporta Windows, macOS e Linux, decodifica centinaia di protocolli e include un'interfaccia grafica intuitiva oltre a strumenti avanzati per l'analisi di flussi TCP, VoIP e conversazioni TCP/UDP. Viene comunemente utilizzato per identificare e risolvere problemi di rete, rilevare attività sospette, fare debugging e ottimizzazione delle applicazioni di rete e come strumento educativo per comprendere i protocolli e il traffico di rete.

Analisi con Wireshark

Si nota la presenza di una richiesta ARP: andando a leggere le info l'indirizzo IP 192.168.200.150 chiede chi sia 192.168.200.100, e dato che l'arp funziona al 2 livello iso/osi controlla nella mac table e come output darà l'indirizzo mac. Oltre questo possiamo già capire che l'attaccante è interno alla nostra rete.

```
emtec_39:7d:... ARP      60 Who has 192.168.200.100? Tell 192.168.200.150
emtec_fd:87:... ARP      42 192.168.200.100 is at 08:00:27:39:7d:fe
emtec_fd:87:... ARP      42 Who has 192.168.200.150? Tell 192.168.200.100
emtec_39:7d:... ARP      60 192.168.200.150 is at 08:00:27:fd:87:1e
```

La prima cosa che salta all'occhio è la presenza di due soli indirizzi IP. Inoltre l'analisi della moltitudine di richiesta TCP da parte dello stesso indirizzo IP fa pensare che non si tratti di un classico tentativo di connessione.

192.168.200.100	192.168.200.150	TCP	74 41304 → 23 [SYN]
192.168.200.100	192.168.200.150	TCP	74 56120 → 111 [SYN]
192.168.200.100	192.168.200.150	TCP	74 33878 → 443 [SYN]
192.168.200.100	192.168.200.150	TCP	74 58636 → 554 [SYN]

Le richieste TCP fanno una richiesta SYN: se la porta è aperta ci restituirà un SYN, ACK; se la porta sarà chiusa restituirà RST, ACK:

36. //4685505	192.168.200.150	192.168.200.100	TCP	74 23 → 41304 [SYN, ACK] Seq=1 Win=642
36.774685652	192.168.200.150	192.168.200.100	TCP	74 111 → 56120 [SYN, ACK] Seq=1 Win=642
36.774685696	192.168.200.150	192.168.200.100	TCP	60 443 → 33878 [RST, ACK] Seq=1 Win=642
36.774685737	192.168.200.150	192.168.200.100	TCP	60 554 → 58636 [RST, ACK] Seq=1 Win=642
36.774685776	192.168.200.150	192.168.200.100	TCP	60 135 → 52358 [RST, ACK] Seq=1 Win=642

Analizzando una singola porta tramite filtro di Wireshark si nota come l'attaccante abbia effettuerato il Three Way Handshake (TWH). Si può capire da tale attacco come l'attaccante sia un "hacker della domenica" siccome l'attacco viene fatto concludendo il TWH e quindi stabilendo una connessione, nonostante poi venga chiusa. Questo comportamento rende vulnerabile l'attaccante, che in tal modo lascia sue tracce/informazioni utili per essere arrestato.

.168.200.100	192.168.200.150	TCP	74 56120 → 111 [SYN] Seq=0 Win=642
.168.200.100	192.168.200.100	TCP	74 111 → 56120 [SYN, ACK] Seq=0 Ack=1 Win=642
.168.200.100	192.168.200.150	TCP	66 56120 → 111 [ACK] Seq=1 Ack=1 Win=642
.168.200.100	192.168.200.150	TCP	66 56120 → 111 [RST, ACK] Seq=1 Win=642

Identificazione IOC

Dalla cattura di rete fornita, si possono osservare diverse caratteristiche che indicano potenziali attività malevole. Analizziamo i dettagli per identificare gli Indicatori di Compromissione (IOC), ipotizzare i vettori di attacco e consigliare azioni per mitigare gli impatti.

Identificazione degli IOC

1. Connessioni TCP RST e SYN anomale:

- Numerosi pacchetti **TCP** con flag **RST** (reset) e **SYN** (synchronize), che potrebbero indicare un tentativo di interrompere connessioni legittime o di creare nuove connessioni malevoli.
- Ripetute connessioni con porta sorgente e destinazione diverse ma spesso sulle stesse IP, suggerendo un pattern anomalo di comunicazione.

2. Pattern di comunicazione:

- La comunicazione tra gli indirizzi IP **192.168.200.100** e **192.168.200.150** risulta sospetta, con una sequenza di pacchetti **RST**, **SYN**, **ACK** che non segue il normale comportamento di una connessione **TCP**.



Potenziali vettori d'attacco

Ipotesi sui Potenziali Vettori di Attacco

La presenza di molteplici richieste TCP indicano che l'attaccante potrebbe utilizzare strumenti di scansione delle porte, come Nmap o simili, per mappare la superficie di attacco del target. Questo tipo di scansione è spesso il preludio a tentativi di exploit su servizi vulnerabili identificati durante la fase di cognizione. A questo proposito vengono proposti dei potenziali vettori d'attacco:

- **Attacco SYN Flood:**

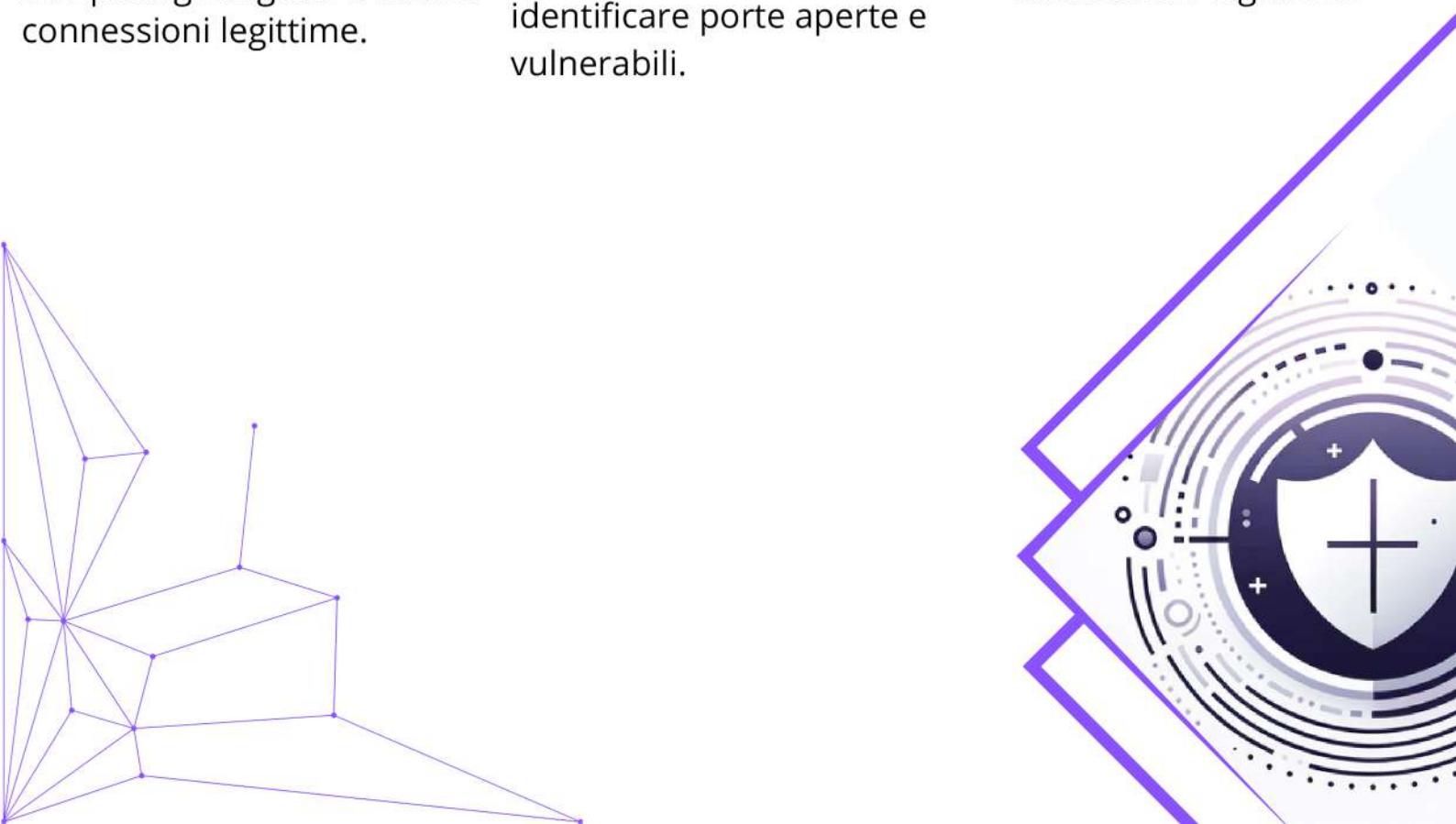
Il continuo invio di pacchetti SYN senza completare il handshake TCP può essere un indicatore di un attacco SYN flood, utilizzato per esaurire le risorse del server e impedirgli di gestire nuove connessioni legittime.

- **Scansione di Porte:**

L'alto numero di pacchetti con flag SYN e la varietà di porte coinvolte possono suggerire un'attività di scansione delle porte, in cui un attaccante cerca di identificare porte aperte e vulnerabili.

- **Attacco DDoS:**

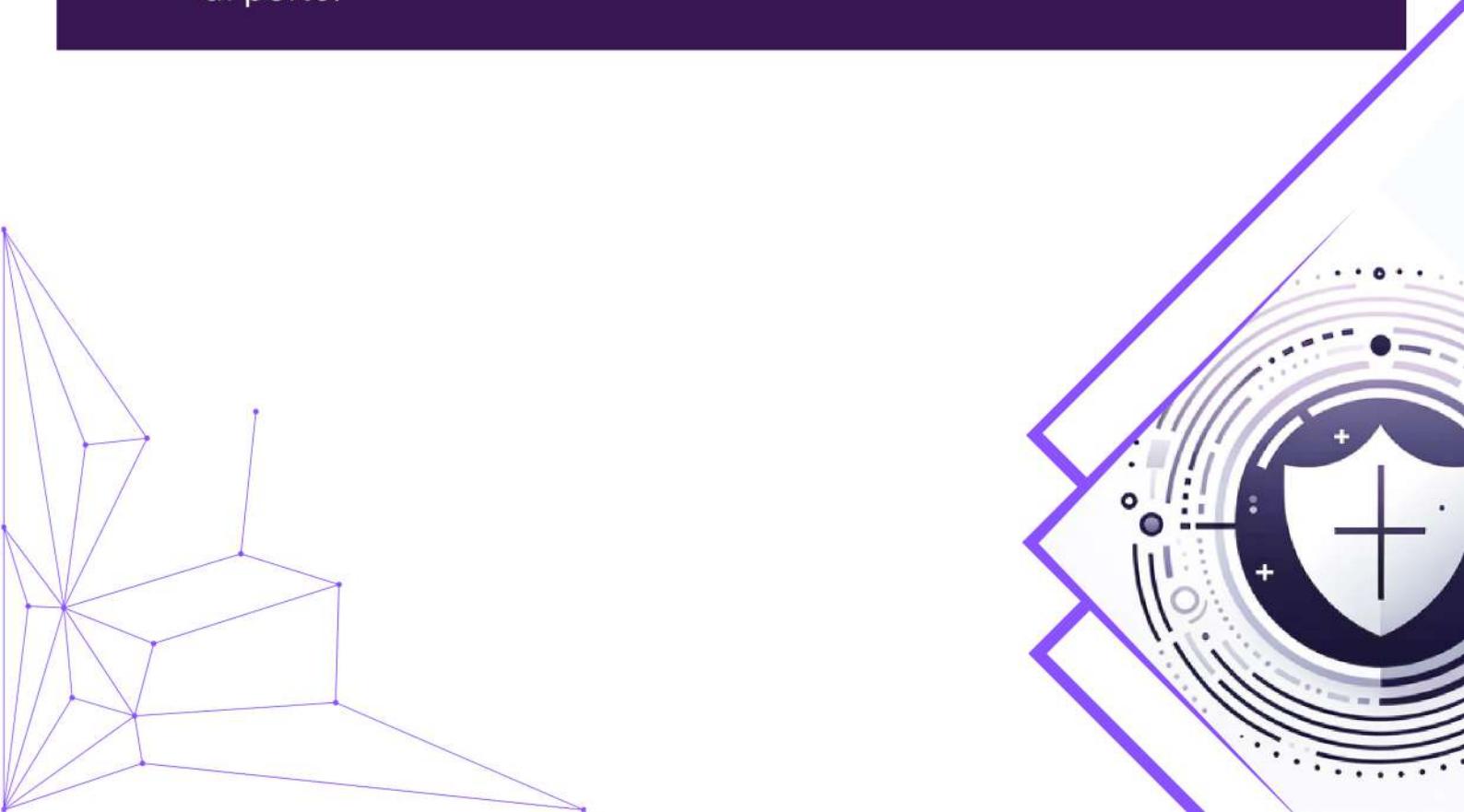
La presenza di numerosi pacchetti RST può indicare un tentativo di sovraccaricare il sistema con richieste eccessive, interrompendo le connessioni legittime.



Prevenzione

Azioni Consigliate per Ridurre gli Impatti dell'Attacco

- Implementare Filtraggio degli Indirizzi IP:
 - Configurare il firewall per bloccare gli indirizzi IP sospetti (192.168.200.100 e 192.168.200.150) se non appartengono a dispositivi autorizzati.
- Abilitare Sistemi di Rilevamento delle Intrusioni (IDS):
 - Utilizzare IDS per monitorare e rilevare pattern anomali di traffico e bloccare automaticamente le connessioni sospette.
- Limitare le Connessioni Incomplete:
 - Configurare il server per limitare il numero di connessioni incomplete (handshake TCP non completati), riducendo l'impatto degli attacchi SYN flood.
- Monitoraggio Costante del Traffico di Rete:
 - Implementare un sistema di monitoraggio del traffico di rete per identificare rapidamente qualsiasi attività sospetta e rispondere tempestivamente.
- Aggiornamento delle Politiche di Sicurezza:
 - Rivedere e aggiornare le politiche di sicurezza per includere misure specifiche contro i tipi di attacco identificati, come DDoS e scansioni di porte.



CONCLUSIONI

Durante il monitoraggio della rete, sono state identificate evidenze di Indicatori di Compromissione (IOC), in particolare richieste TCP ripetute. Questo comportamento anomalo suggerisce la possibilità di un attacco in corso. Un'analisi più dettagliata dei log di rete ha rivelato che l'indirizzo IP 192.168.200.100 sta effettuando una scansione sul target 192.168.200.150. Tale attività è tipica di una fase di ricognizione, in cui l'attaccante cerca di individuare porte e servizi aperti per sfruttare eventuali vulnerabilità. L'evidenza delle richieste TCP ripetute indica che l'attaccante potrebbe utilizzare strumenti di scansione delle porte, come Nmap o simili, per mappare la superficie di attacco del target. Questo tipo di scansione è spesso il preludio a tentativi di exploit su servizi vulnerabili identificati durante la fase di ricognizione. Per ridurre l'impatto dell'attacco e prevenire ulteriori tentativi di compromissione, si consiglia di implementare immediatamente delle policy di firewall che bloccino tutte le richieste provenienti dall'IP dell'attaccante (192.168.200.100). Questo intervento impedirebbe all'attaccante di continuare la scansione e di ottenere ulteriori informazioni sulle porte e sui servizi in ascolto sul target 192.168.200.150. In sintesi, l'adozione di misure di blocco a livello di firewall rappresenta un'azione tempestiva ed efficace per contrastare le attività malevoli in corso, proteggendo così l'integrità e la sicurezza della rete.



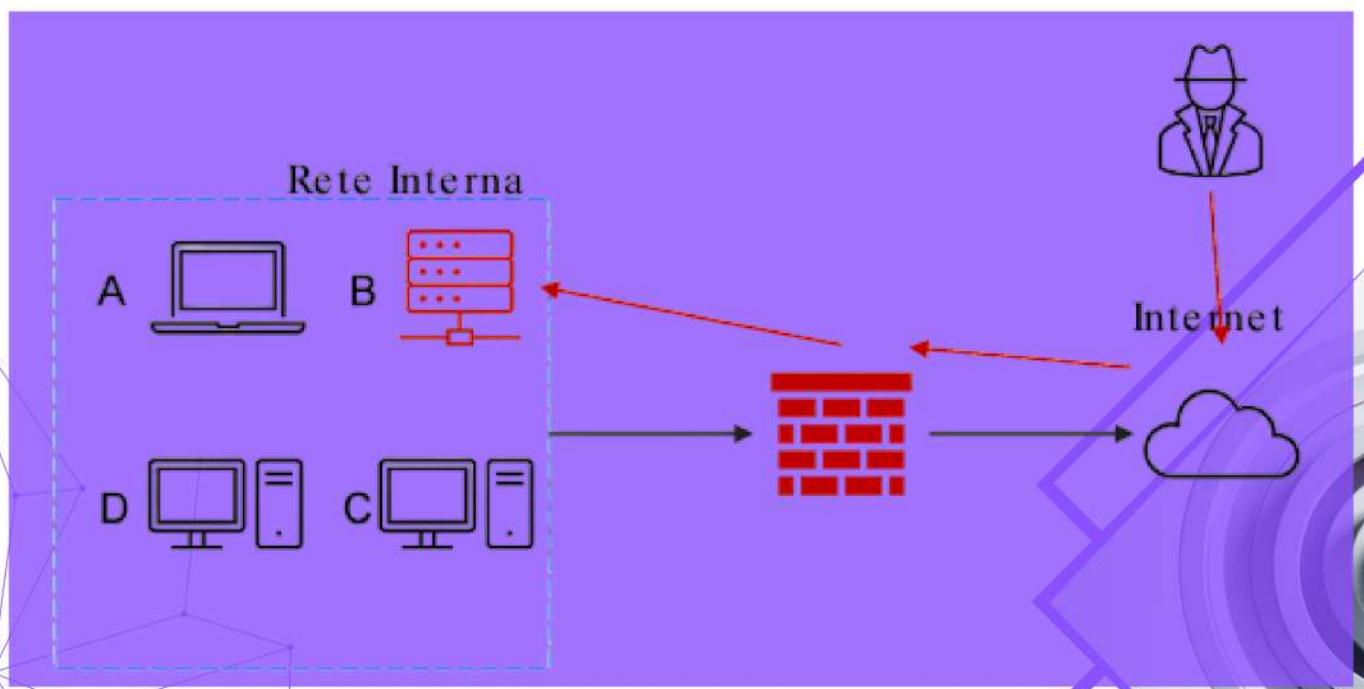
L4

Con riferimento alla figura sotto, il sistema B (un database con diversi dischi per lo storage) è stato compromesso interamente da un attaccante che è riuscito a bucare la rete ed accedere al sistema tramite Internet.

L'attacco è attualmente in corso e siete parte del team di CSIRT.

Rispondere ai seguenti quesiti.

- Mostrate le tecniche di: I) Isolamento II) Rimozione del sistema B infetto
- Spiegate la differenza tra Purge e Destroy per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi. Indicare anche Clear



Incident Response

Sebbene le aziende possano adottare precauzioni e preparare la protezione perimetrale per gli incidenti di sicurezza, la possibilità che si verifichi un incidente non è mai nulla.

Pertanto, le aziende devono prevedere che prima o poi si verificherà un incidente di sicurezza, come un virus o una fuga di dati sensibili, e creare un cosiddetto "**incident response plan**", ovvero un piano di risposta agli incidenti.

Il team responsabile di attuare il piano di risposta agli incidenti è il **CSIRT (Computer Security Incident Response Team)**. Il CSIRT deve essere in grado di rispondere all'incidente di sicurezza in maniera calma e consistente. Il processo di incident response non è un processo lineare, ma include dei cicli per tornare alle fasi precedenti dove necessario, e si articola generalmente come mostrato sotto.



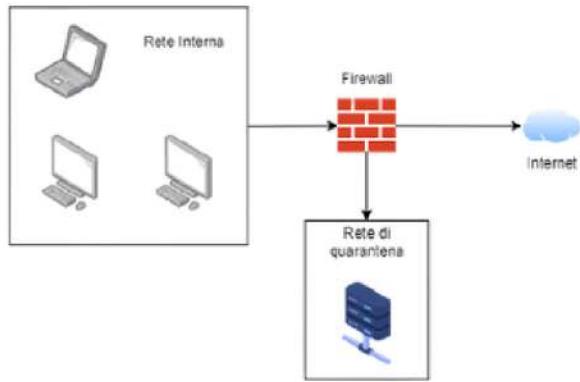
Completate le valutazioni, il CSIRT deve trovare una soluzione per ridurre al minimo gli impatti dell'incidente. Inizia la fase di contenimento, eliminazione e recupero che ha come scopo principale:

- La riduzione degli impatti causati dall'incidente;
- L'eliminazione dell'incidente dalla rete e dai sistemi;
- Il recupero dei servizi e delle operatività standard.

Tecniche di contenimento

Nella seconda fase del piano di risposta agli incidenti, ci si preoccupa del contenimento dei danni, eliminazione dell'incidente e recupero dei servizi standard.

SEGMENTAZIONE:



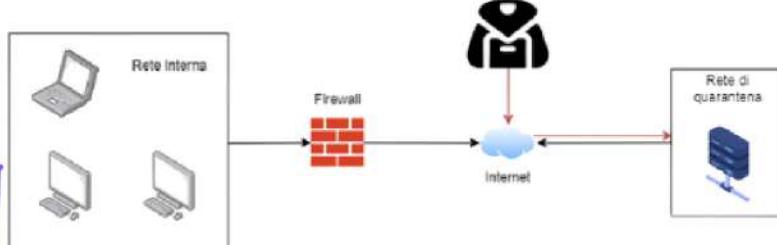
La segmentazione include tutte quelle attività che permettono di dividere una rete in diverse LAN o VLAN. Consiste nel dividere la rete o i sistemi in segmenti più piccoli per limitare la diffusione dell'incidente all'interno dell'organizzazione. In questo modo si riduce l'impatto dell'incidente isolando le parti compromesse del sistema, limitando la possibilità che l'incidente si propaghi ad altre parti della rete.

In questo caso la segmentazione permette di separare il dispositivo infetto, creando una rete ad hoc detta "rete di quarantena".

ISOLAMENTO:

Quando la segmentazione non basta, è necessario un contenimento maggiore: si utilizza la tecnica dell'isolamento.

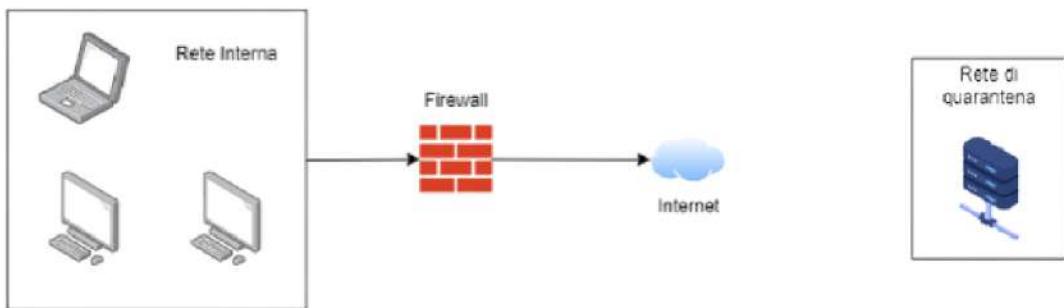
L'isolamento consiste nella completa disconnessione del sistema infetto dalla rete, per restringere ancora maggiormente l'accesso alla rete interna da parte dell'attaccante e impedire che la minaccia possa influenzare altre parti del sistema. In questo caso si nota come l'attaccante abbia ancora accesso al dispositivo isolato tramite internet.



Tecniche di contenimento

RIMOZIONE: Se l'isolamento non è ancora abbastanza, si utilizza la tecnica di contenimento più stringente: la rimozione completa del sistema dalla rete sia interna sia internet. In questo modo l'attaccante non avrà né accesso alla rete interna né tantomeno alla macchina infettata.

Lo scopo di questa tecnica è quello di garantire che i sistemi compromessi siano puliti e sicuri prima di essere rimessi in produzione.



Le tecniche di contenimento sono essenziali nella gestione degli incidenti di sicurezza. La segmentazione aiuta a limitare la diffusione dell'incidente, l'isolamento protegge immediatamente le risorse critiche, e la rimozione garantisce che le minacce siano eliminate e che i sistemi siano sicuri prima di tornare operativi. Queste tecniche lavorano insieme per minimizzare l'impatto di un incidente e proteggere l'integrità e la disponibilità dei sistemi informatici dell'organizzazione.

Rimozione Informazioni Sensibili

Clear

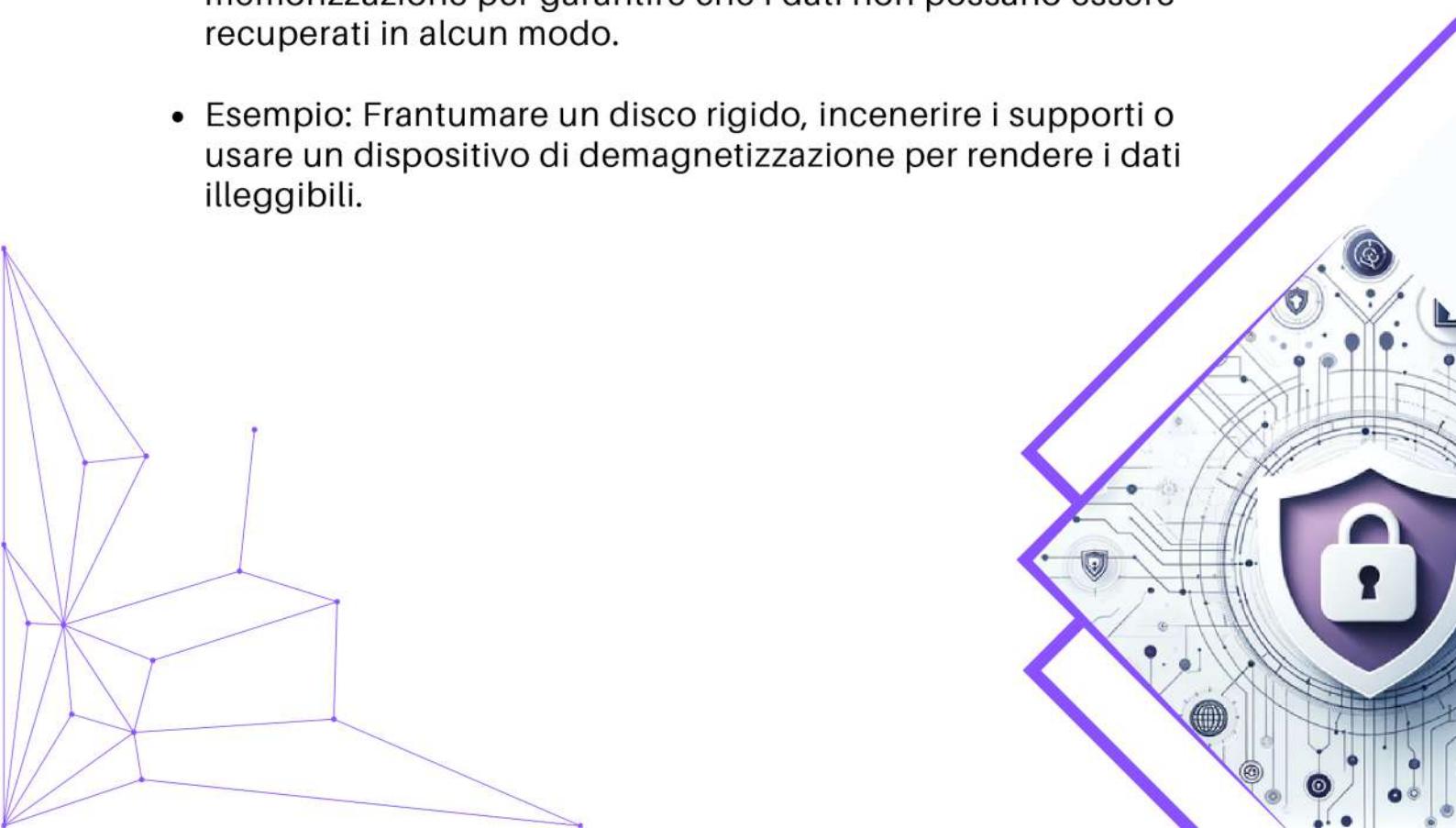
- Definizione: Eliminare i dati in modo che non possano essere recuperati utilizzando strumenti software standard.
- Esempio: Formattare rapidamente un disco rigido o eliminare file utilizzando comandi di cancellazione.

Purge

- Definizione: Eliminare i dati in modo che non possano essere recuperati nemmeno con strumenti avanzati di recupero dati.
- Esempio: Sovrascrivere i dati su un disco rigido con modelli specifici di dati casuali più volte.

Destroy

- Definizione: Distruggere fisicamente i supporti di memorizzazione per garantire che i dati non possano essere recuperati in alcun modo.
- Esempio: Frantumare un disco rigido, incenerire i supporti o usare un dispositivo di demagnetizzazione per rendere i dati illeggibili.



Confronto Purge - Destroy

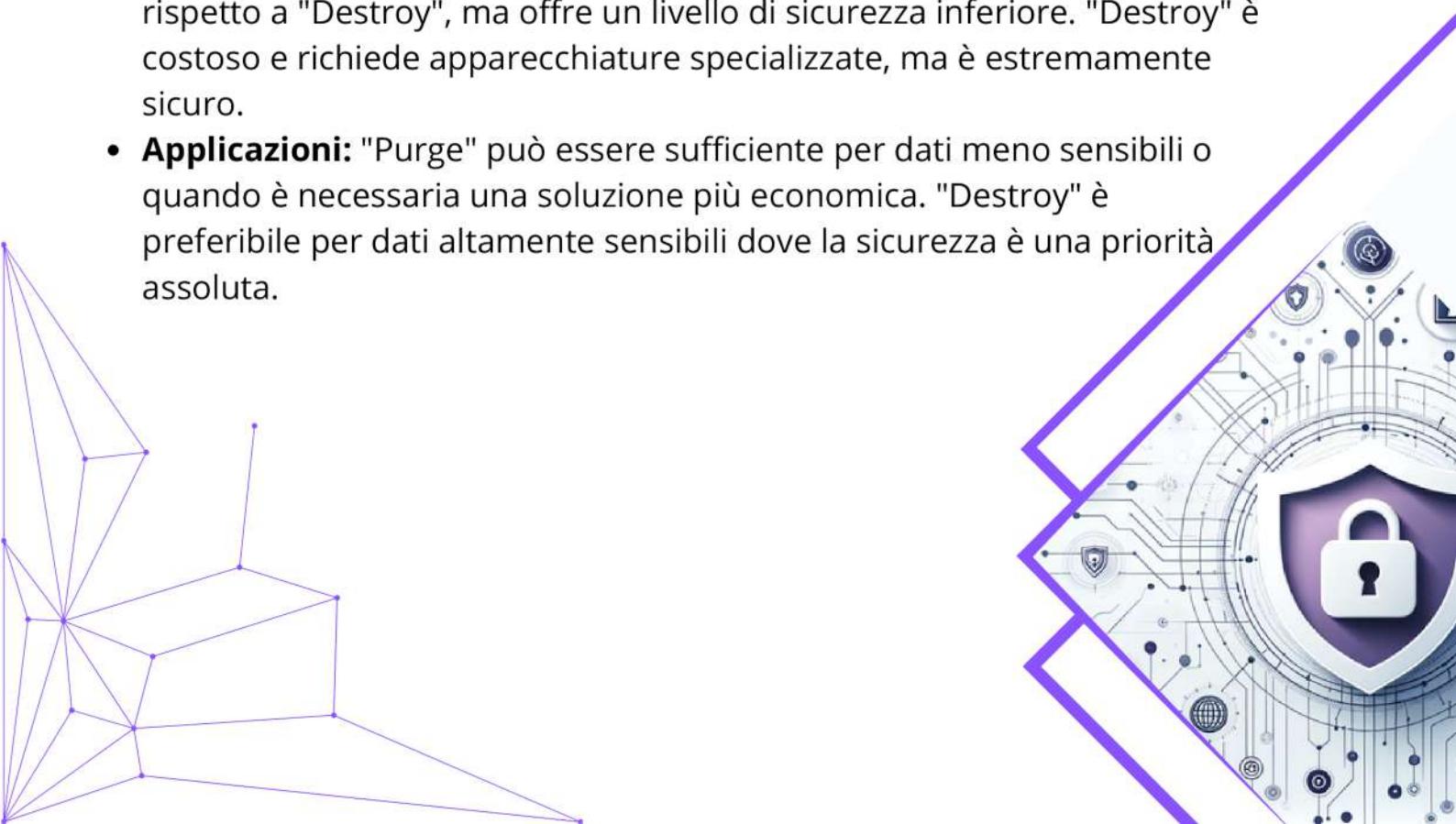
Purge

- **Approccio:** "Purge" adotta sia metodi logici che fisici per rimuovere i contenuti sensibili. Include tecniche come la degaussing, che utilizza forti campi magnetici per alterare i dati memorizzati su dispositivi magnetici, rendendoli inaccessibili.
- **Efficacia:** Sebbene efficace, non garantisce la distruzione fisica del dispositivo, quindi alcune tracce residue di dati potrebbero teoricamente essere recuperate con tecniche molto avanzate.

Destroy

- **Approccio:** "Destroy" è un metodo più radicale e definitivo. Oltre ai metodi logici e fisici, coinvolge tecniche di laboratorio che fisicamente distruggono il supporto di memorizzazione, rendendo impossibile qualsiasi tentativo di recupero dei dati.
- **Efficacia:** Garantisce la completa distruzione dei dati e del dispositivo, eliminando ogni possibilità di recupero. È il metodo più sicuro, ma anche il più costoso e complesso.

- **Effort e Costi:** "Purge" richiede meno risorse economiche e tecnologiche rispetto a "Destroy", ma offre un livello di sicurezza inferiore. "Destroy" è costoso e richiede apparecchiature specializzate, ma è estremamente sicuro.
- **Applicazioni:** "Purge" può essere sufficiente per dati meno sensibili o quando è necessaria una soluzione più economica. "Destroy" è preferibile per dati altamente sensibili dove la sicurezza è una priorità assoluta.



CONCLUSIONI

In questo esercizio, il sistema B della rete aziendale è stato compromesso da un attaccante attraverso l'accesso a Internet. Per mitigare l'incidente, si possono implementare delle tecniche di isolamento scollegando il sistema dalla rete e creando una VLAN quarantena. La rimozione delle minacce può essere effettuata tramite scansioni antimalware, applicazione di patch e, se necessario, ripristino da backup sicuri.

Per eliminare definitivamente le informazioni sensibili, è necessario utilizzare tecniche di purge per sovrascrivere i dati, e successivamente distruggere fisicamente i dischi compromessi per garantire la non recuperabilità delle informazioni.

Queste azioni combinate permettono di contenere l'incidente, rimuovere la minaccia e garantire la sicurezza dei dati sensibili, minimizzando l'impatto sull'infrastruttura aziendale e proteggendo l'integrità delle informazioni.

L5

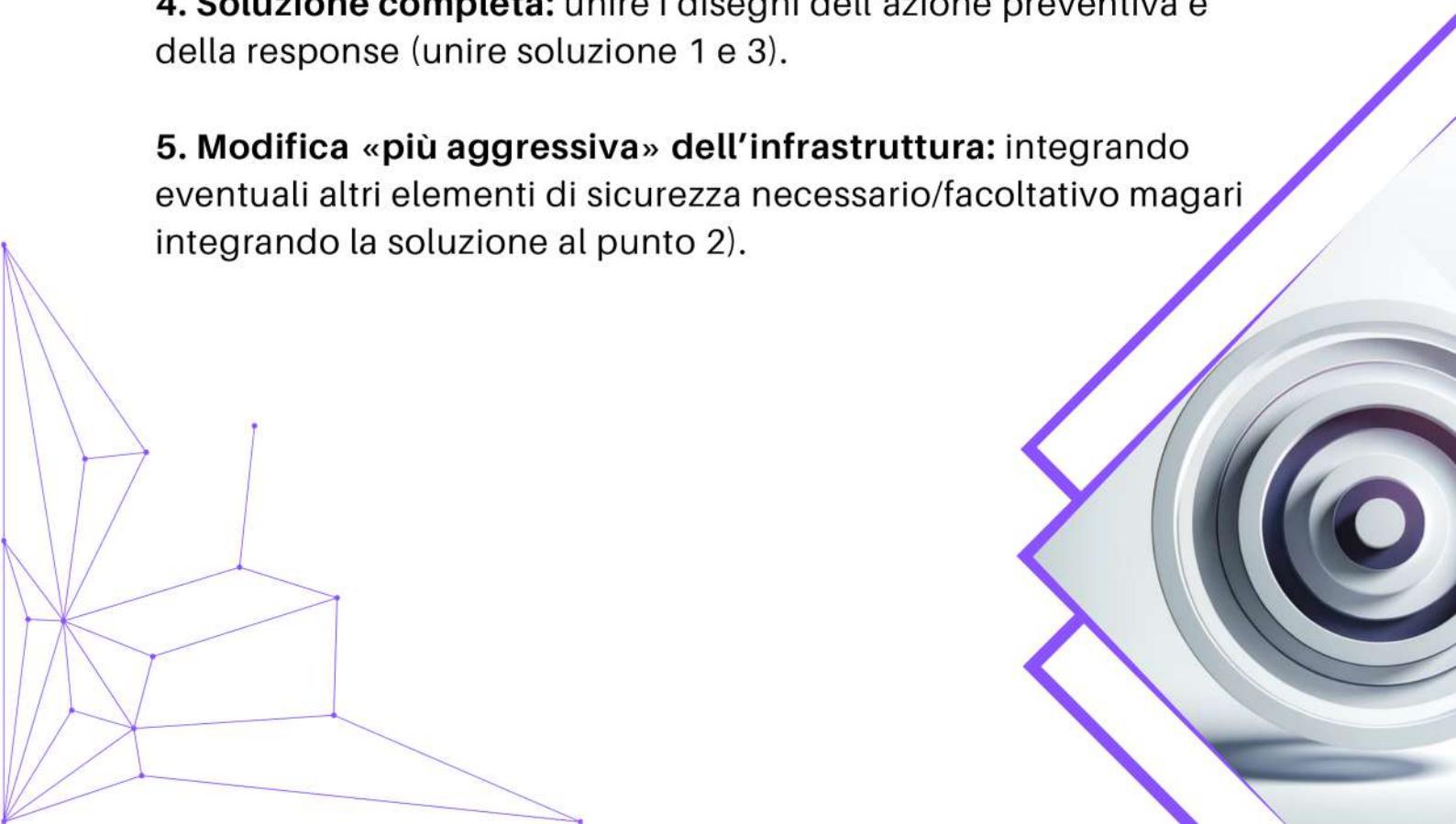
1. Azioni preventive: quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni.

2. Impatti sul business: l'applicazione Web subisce un attacco di tipo DDoS dall'esterno che rende l'applicazione non raggiungibile per 10 minuti . Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media ogni minuto gli utenti spendono 1.500 € sulla piattaforma di e-commerce . Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica.

3. Response: l'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificate la figura in slide 2 con la soluzione proposta.

4. Soluzione completa: unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3).

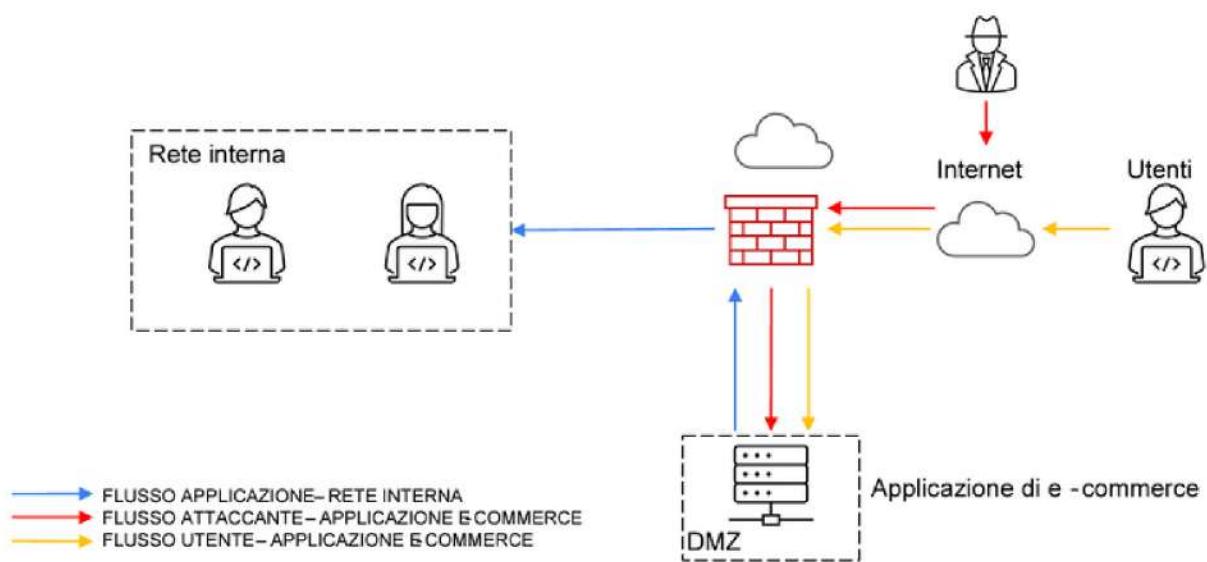
5. Modifica «più aggressiva» dell'infrastruttura: integrando eventuali altri elementi di sicurezza necessario/facoltativo magari integrando la soluzione al punto 2).



Traccia

Architettura di rete:

L'applicazione di e-commerce deve essere disponibile per gli utenti tramite sulla piattaforma. La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna. Rete interna FLUSSO APPLICAZIONE -RETE INTERNA FLUSSO ATTACCANTE - APPLICAZIONE E-COMMERCE FLUSSO UTENTE -APPLICAZIONE E-COMMERCE Esercizio Traccia e requisiti Internet per effettuare acquisti



Bonus:

Esercizio Traccia e requisiti Analizzare le seguenti segnalazioni caricate su anyrun e fare un piccolo report di ciò che si scopre relativo alla segnalazione dell'eventuale attacco spiegando ad utenti e dirigenti la tipologia di attacco e come evitare questi attacchi in futuro:

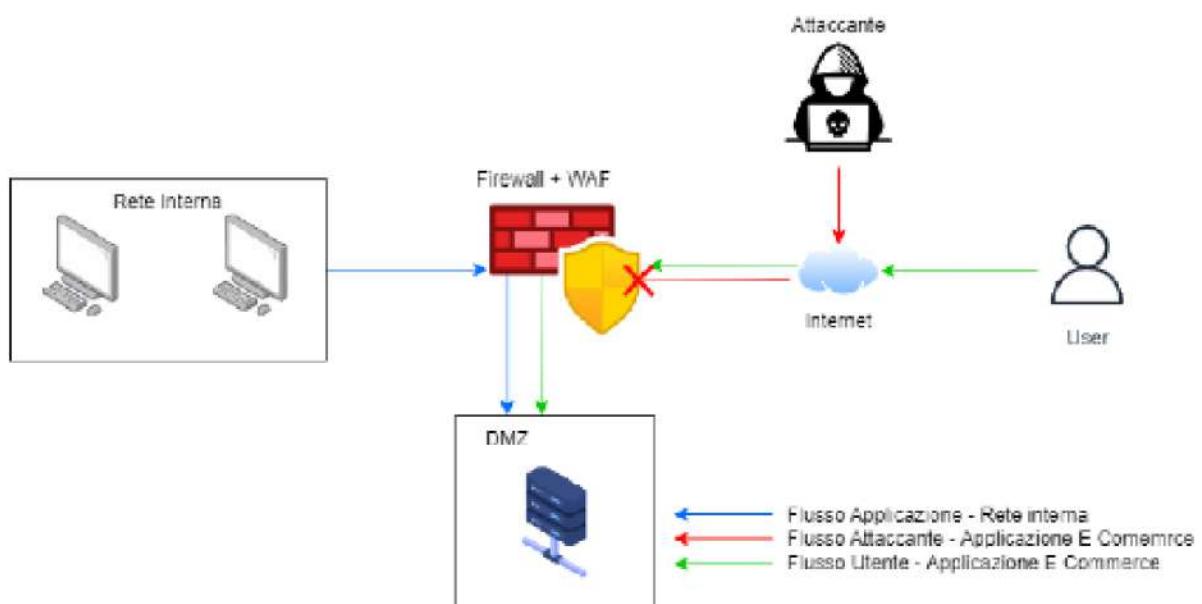
Azione Preventive per SQLi e XSS

- 1. Utilizzare Query Preparati:** Implementare query preparate per evitare l'iniezione di SQL.
- 2. Sanitizzazione degli Input:** Applicare una sanitizzazione e validazione degli input degli utenti per prevenire attacchi XSS. Ciò impedisce l'inclusione di script dannosi o comandi SQL nelle richieste.
- 3. Content Security Policy (CSP):** Implementare una CSP per limitare le risorse che possono essere caricate ed eseguite.
- 4. Firewall Applicativo (WAF):** Aggiungere un WAF per filtrare e monitorare il traffico HTTP verso e dall'applicazione web. Questo dispositivo monitora il traffico di rete e limita le richieste inviate alle applicazioni, consentendo l'accesso solo agli utenti privilegiati. Esistono due tipologie di WAF:
 - WAF basati su rete: vengono installati come appliance hardware o software all'interno della rete e si occupano dell'analisi del traffico di rete a livello di pacchetti.
 - WAF bassati su cloud: sono forniti come servizi in abbonamento da un provider di sicurezza cloud e si occupano dell'analisi del traffico di rete a livello di applicazione.
- 5. Autenticazione e Autorizzazione Robusta:** Migliorare i controlli di accesso con autenticazione multifattoriale (MFA).
- 6. Aggiornamenti e Patch:** Mantenere aggiornato il software e applicare tempestivamente le patch di sicurezza.
- 7. Monitoraggio e Logging:** Implementare un sistema di monitoraggio e logging per rilevare attività sospette.

Azione Preventive per SQLi e XSS

XSS	SQLblind
Meccanismo: Iniezione di codice JavaScript malevolo in pagine web attraverso campi di input non sanificati.	Meccanismo: Manipolazione di query SQL attraverso input non sanificati senza ricevere direttamente i risultati delle query.
Ambito di Esecuzione: Nel contesto del browser dell'utente.	Ambito di Esecuzione: A livello del database del server.
Obiettivo Primario: Rubare cookie di sessione, credenziali di accesso e manipolare il contenuto della pagina web.	Obiettivo Primario: Estrarre dati sensibili dal database deducendo informazioni senza vedere direttamente i risultati delle query.
Tipi Principali: Stored XSS, Reflected XSS, DOM-based XSS.	Tipi Principali: Boolean-based Blind SQL Injection, Time-based Blind SQL Injection.
Risultati Visibili: Immediatamente visibili nel browser della vittima.	Risultati Visibili: Non visibili direttamente, dedotti tramite induzioni logiche o tempi di risposta.
Prevenzione: Validazione e sanificazione degli input, Content Security Policy (CSP).	Prevenzione: Uso di query preparate, sanificazione degli input, controllo rigoroso degli errori.
Impatto: Compromissione dell'interazione utente, furto di dati di sessione, manipolazione dei contenuti.	Impatto: Accesso non autorizzato a dati sensibili nel database, anche senza mostrare direttamente i risultati delle query.

Di seguito è mostrata la figura con le dovute implementazioni richieste dal primo punto dell'esercizio:



Impatti sul business

Per calcolare l'impatto economico della non raggiungibilità del servizio per 10 minuti, consideriamo che in media ogni minuto gli utenti spendono 1.500 €.

Calcolo:

- Spesa media per minuto: 1.500 €
- Durata dell'interruzione: 10 minuti
- Impatto economico = Spesa media per minuto x Durata dell'interruzione
- Impatto economico = $1.500 \text{ €} \times 10 = 15.000 \text{ €}$

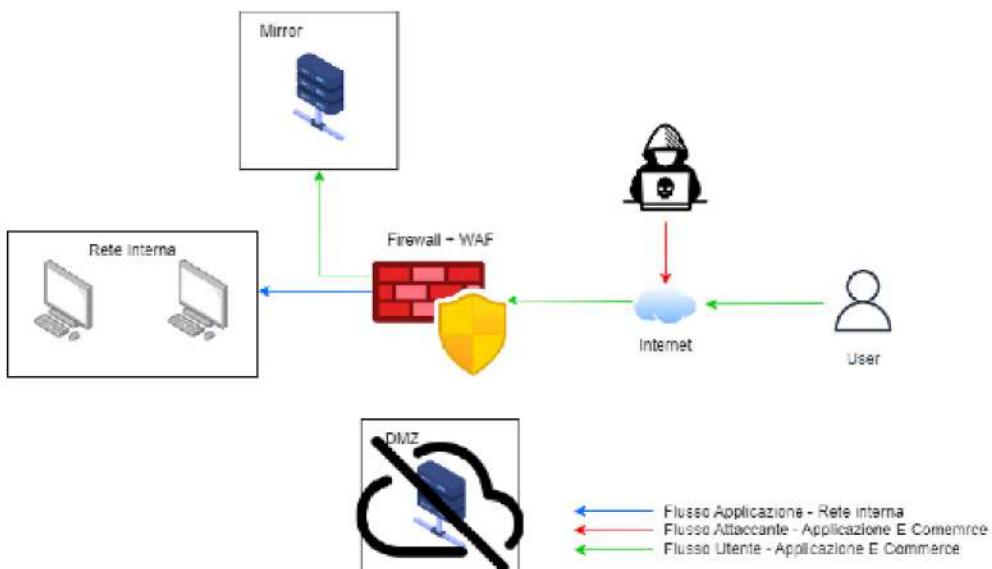
Quindi, l'impatto economico totale dovuto alla non raggiungibilità del servizio per 10 minuti è di 15.000 €.



Impatti sul business

In questi casi la mancata erogazione del servizio rappresenterebbe un danno non indifferente per l'azienda.

- **Utilizzare un Servizio di Mitigazione DDoS:** Implementare servizi specializzati che possono rilevare e mitigare attacchi DDoS in tempo reale.
- **Firewall e WAF**
 - Configurare correttamente il firewall e il Web Application Firewall (WAF) per filtrare il traffico sospetto e prevenire accessi non autorizzati.
 - Implementare regole di firewall che limitino il traffico in ingresso e uscita solo ai servizi necessari.
- **Configurazione di Rate Limiting:** Limitare il numero di richieste che un singolo indirizzo IP può fare in un certo periodo di tempo. Si basa sul monitoraggio degli indirizzi IP da cui provengono le richieste e sul monitoraggio di quanto tempo trascorre tra richieste consecutive.
- **Impiego di CDN (Content Delivery Network):** Utilizzare una CDN per distribuire il contenuto su server globali, riducendo il carico sui server principali e migliorando la resilienza contro gli attacchi.
- **Server Mirror:** per garantire la business continuity, oltre ad incrementare la firewall policy, si può fare uso di un server mirror che sostituisca il server principale, permettendo la continua erogazione del servizio.



Response

In caso di infezione da malware nell'applicazione web, la priorità è impedire la propagazione del malware sulla rete interna, senza rimuovere l'accesso dell'attaccante alla macchina infetta.

In questa fase si fa riferimento al piano di risposta degli incidenti (incident response plan), in cui ci si preoccupa del contenimento dei danni, eliminazione dell'incidente e recupero dei servizi standard.

Per un excursus sulla teoria delle tecniche di contenimento si faccia riferimento alla parte di esercizio S9L4, a pagina 29.

Azioni Preventive:

- 1. Isolamento del Server Infetto:** Isolare immediatamente il server infetto all'interno della DMZ per evitare che il malware si diffonda alla rete interna.
- 2. Monitoraggio e Logging:** Implementare un sistema di monitoraggio e logging avanzato per tracciare tutte le attività sul server infetto.
- 3. Segmentazione della Rete:** Utilizzare VLAN e altre tecniche di segmentazione per limitare la comunicazione tra la macchina infetta e la rete interna.
- 4. Aggiornamenti e Patch di Sicurezza:** Assicurarsi che tutti i sistemi siano aggiornati con le ultime patch di sicurezza per prevenire ulteriori infezioni.

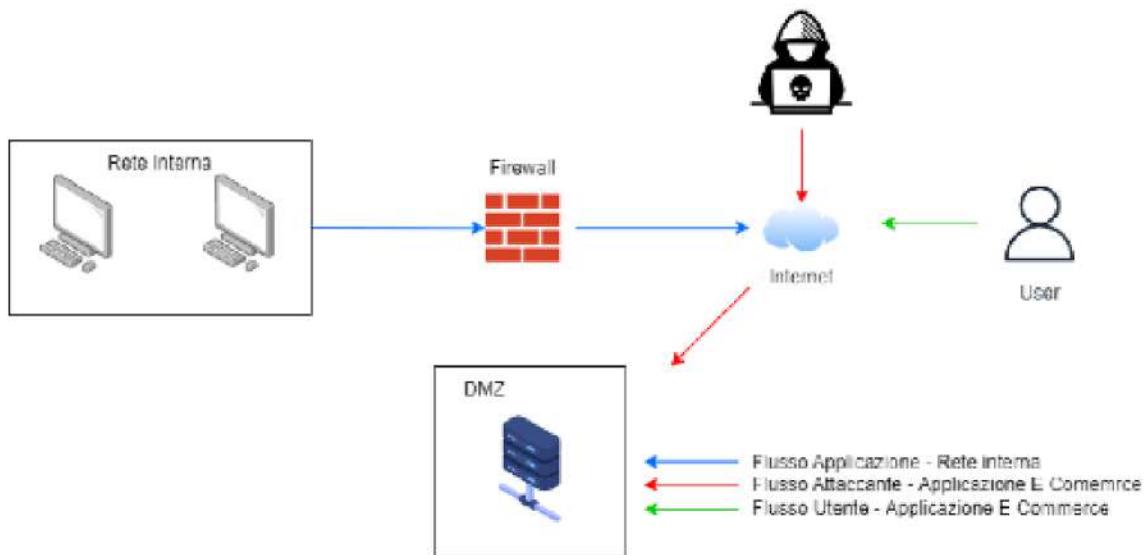
Queste misure permettono di contenere l'infezione senza compromettere il monitoraggio dell'attaccante.

Response

Alla luce delle azioni preventive mostrate, la soluzione più idonea alla richiesta dell'esercizio è l'isolamento del server infetto. In questo modo si impedisce all'attaccante di accedere alla rete interna. Questo richiede la modifica delle policy del firewall per inserire l'IP dell'attaccante nella blacklist, bloccando eventuali tentativi di connessione.

Isolata la rete, l'attaccante avrà ancora accesso alla DMZ tramite internet. Nonostante ciò, l'accesso e le operazioni di acquisto degli utenti leciti vengono bloccati per prevenire il furto di informazioni e la diffusione di virus e/o altre minacce.

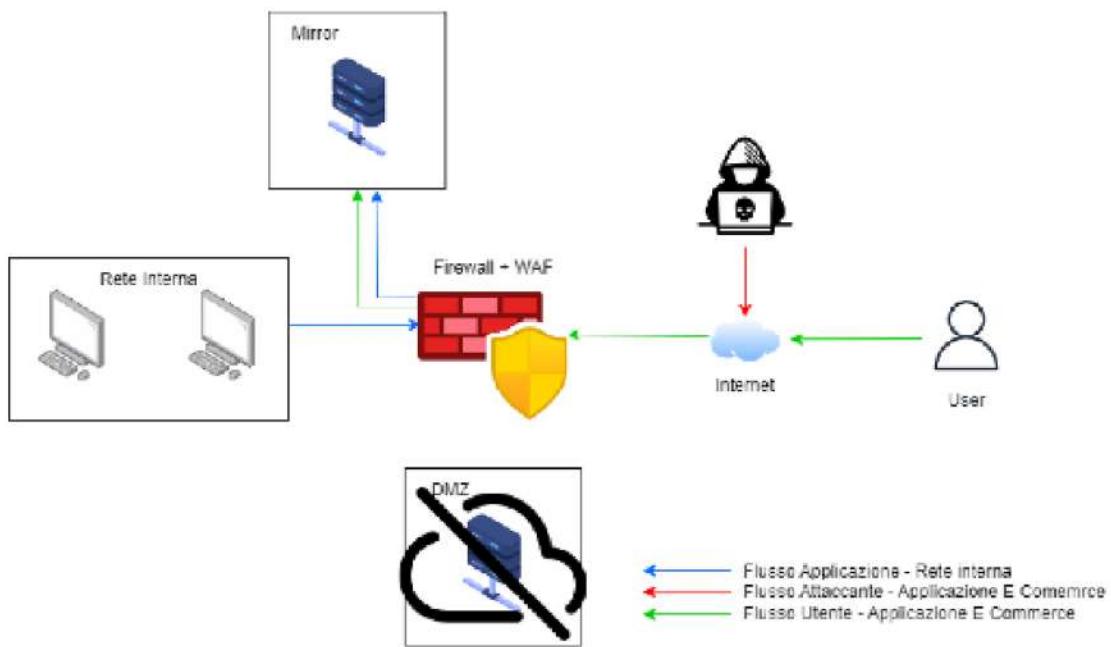
Evitare danni agli utenti e all'immagine dell'azienda è cruciale.



Soluzione completa

Soluzione Proposta per Prevenire la Propagazione del Malware

1. **Isolamento della Web Application:** Separare l'applicazione web infetta dalla rete interna per evitare che il malware si propaghi.
2. **Modifica delle Firewall Policy:** Inserire l'IP dell'attaccante nella blacklist del firewall per bloccare ulteriori tentativi di connessione.
3. **Blocco delle Operazioni Utente:** Sospendere temporaneamente le operazioni di acquisto degli utenti leciti per evitare furti di informazioni, diffusione di virus e altre minacce.
4. **Monitoraggio Continuo:** Continuare a monitorare il server infetto per raccogliere dati utili e impedire ulteriori danni.



Modifiche aggressive

- **Firewall perimetrale:**

- Dispositivo di sicurezza di rete situato al confine tra la rete interna di un'organizzazione e le reti esterne, come Internet. Esso monitora e controlla il traffico di rete in base a regole di sicurezza predefinite, proteggendo le risorse interne da accessi non autorizzati e attacchi informatici. Il firewall perimetrale analizza pacchetti di dati e registra attività di rete, fornendo una difesa fondamentale contro le minacce esterne.

- **Backup e Disaster Recovery**

- Eseguire backup regolari e mantenere un piano di ripristino di emergenza aggiornato per minimizzare il tempo di inattività.
- Integrazione di un server di backup remoto per il disaster recovery.

- **Firewall e WAF**

- Configurare correttamente il firewall e il Web Application Firewall (WAF) per filtrare il traffico sospetto e prevenire accessi non autorizzati.
- Implementare regole di firewall che limitino il traffico in ingresso e uscita solo ai servizi necessari.

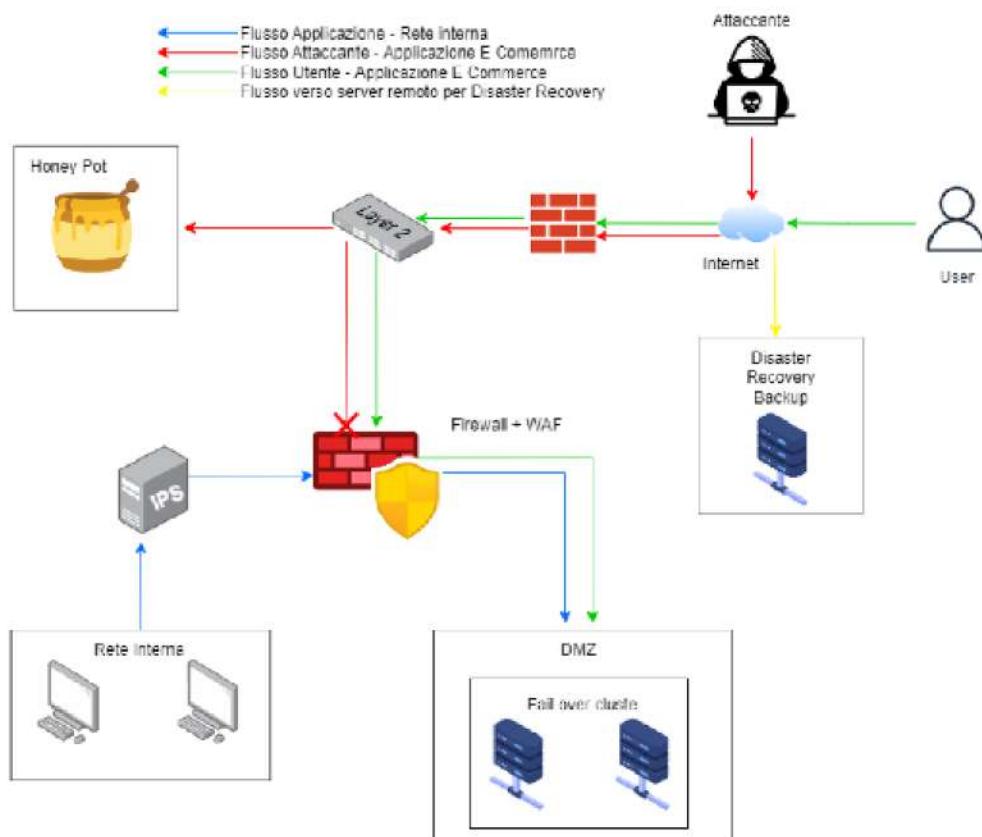
- **Segmentazione della Rete**

- Utilizzare la segmentazione della rete per isolare le parti critiche del sistema e prevenire la propagazione del malware.

- **IPS (Intrusion Prevention System)** è un dispositivo di sicurezza di rete che monitora il traffico per rilevare e prevenire minacce in tempo reale, bloccando automaticamente attività dannose.

- **Honey Pot:** è un sistema di sicurezza informatica deliberatamente vulnerabile e progettato per attirare e monitorare gli attaccanti. Il suo scopo principale è rilevare, analizzare e studiare i tentativi di intrusione, raccogliendo informazioni sulle tecniche utilizzate dagli attaccanti. Queste informazioni aiutano a migliorare le difese di sicurezza dell'organizzazione.

Modifiche aggressive



Best Practices

- **Monitoraggio e Logging**
 - Implementare sistemi di monitoraggio e logging avanzati per rilevare e rispondere rapidamente alle attività sospette.
- **Formazione degli Utenti**
 - Educare gli utenti sui rischi di phishing e altre tecniche di ingegneria sociale per ridurre la probabilità di infezioni da malware.
- **Autenticazione Multifattoriale (MFA)**
 - Implementare l'autenticazione multifattoriale per aggiungere un ulteriore livello di sicurezza agli accessi dei sistemi.

Queste azioni preventive riducono significativamente l'impatto sul business e migliorano la resilienza dell'infrastruttura IT contro attacchi e interruzioni di servizio.

Analisi Anyrun

Any.Run è un servizio online che fornisce un ambiente sicuro e controllato per l'esecuzione e l'analisi dei file eseguibili, dei documenti e delle URL sospette o dannosi. Si tratta di una piattaforma che consente agli utenti di caricare e analizzare file o collegamenti web per identificare potenziali minacce informatiche come malware, virus o altre forme di software dannoso.

Di seguito si mostrano i punti e le funzionalità principali di Any.Run:

Esecuzione sicura: Any.Run offre un ambiente virtualizzato che permette agli utenti di esaminare file e URL in sicurezza, senza rischi di malware per i propri sistemi o reti.

Analisi comportamentale: Any.Run monitora e documenta meticolosamente le attività del software durante l'esecuzione di file e URL. Le azioni osservate includono la creazione e modifica di file, le comunicazioni di rete, e le interazioni con il registro di sistema, tra le altre.

Report dettagliati: Dopo l'analisi, Any.Run genera report approfonditi sulle attività dei file o URL esaminati. I report includono dettagli come gli URL visitati, i file generati, e le modifiche al registro di sistema, fornendo informazioni essenziali per identificare e comprendere le minacce.

Condivisione e collaborazione: Gli utenti di Any.Run possono condividere i risultati delle loro analisi con altri membri della comunità o con esperti di sicurezza informatica, promuovendo la collaborazione e lo scambio di informazioni sulle minacce rilevate.

Strumenti aggiuntivi: Any.Run include funzionalità supplementari come l'analisi statica dei file e la ricerca di indicatori di compromissione (IOC), che sono strumenti cruciali per l'identificazione e l'analisi approfondita delle minacce informatiche.



Analisi Anyrun

PowerShell è una shell di comando e un linguaggio di scripting creato da Microsoft per i sistemi Windows. Progettato per superare le capacità del tradizionale prompt dei comandi (cmd.exe), offre numerose funzionalità avanzate per automatizzare le operazioni di gestione e amministrazione dei sistemi Windows.

Di seguito sono mostrate alcune funzionalità principali di PowerShell:

Object-Based: gestisce gli output dei comandi come oggetti, non solo come semplici stringhe di testo. Questo permette una manipolazione dei dati più flessibile e avanzata, sfruttando proprietà e metodi specifici degli oggetti.

Cmdlets: i cmdlet (pronunciati "command-lets") sono i componenti base utilizzati per eseguire operazioni specifiche. Questi piccoli comandi possono svolgere una varietà di funzioni, dall'estrazione di informazioni di sistema alla gestione dei file o all'implementazione di azioni amministrative.

Pipeline: PowerShell permette l'uso di pipeline, una funzionalità che consente di collegare più cmdlet in sequenza. L'output di un cmdlet può essere direttamente utilizzato come input per il successivo, facilitando la realizzazione di operazioni complesse attraverso la combinazione di cmdlet più semplici.

Scripting Language: PowerShell è un linguaggio di scripting avanzato che supporta variabili, strutture di controllo del flusso come cicli e condizioni, funzioni e molto altro. Questo permette di creare script in PowerShell per automatizzare attività complesse e ripetitive, rendendo la gestione dei sistemi più efficiente.

Integrazione con .NET: PowerShell è profondamente integrato con il framework .NET, permettendo di utilizzare le sue librerie e funzionalità direttamente negli script PowerShell. Questa integrazione estende significativamente le potenzialità di PowerShell.

Interfaccia utente grafica (GUI): PowerShell permette di sviluppare interfacce utente grafiche (GUI) utilizzando Windows Presentation Foundation (WPF) o Windows Forms. Questo consente agli amministratori di creare strumenti personalizzati che facilitano la gestione dei sistemi Windows, rendendo il processo più accessibile e visivamente intuitivo.

Analisi Anyrun

Un file **.bat**, abbreviazione di "batch file", è un tipo di documento utilizzato nei sistemi operativi Windows per eseguire automaticamente una sequenza di comandi DOS (Disk Operating System). Questi comandi sono processati dall'interprete dei comandi del sistema operativo una volta che il file è avviato. In sintesi, i file batch sono uno strumento efficace per automatizzare attività sui sistemi Windows.

Di seguito sono descritte le principali proprietà del file .bat:

Automatizzazione delle attività: I file batch sono ampiamente impiegati per automatizzare attività ripetitive o complesse. Possono, ad esempio, eseguire sequenze di comandi di sistema, copiare file da una posizione all'altra o modificare file di configurazione.

Sintassi dei comandi: I comandi inseriti in un file batch possono essere qualsiasi comando DOS o specifici comandi del prompt di Windows. Questi includono operazioni come navigare tra le directory con cd, copiare file con copy, eliminare file con del, creare directory con mkdir, visualizzare messaggi con echo, tra gli altri.

Estensione dei comandi: I file batch supportano l'uso di variabili, cicli, condizioni e altri elementi di programmazione per rendere le operazioni più dinamiche e adattabili. Ad esempio, è possibile impiegare costrutti IF-ELSE per eseguire differenti azioni in base a condizioni specifiche, ampliando così la flessibilità e l'efficacia dello script.

Esecuzione dei file batch: I file batch possono essere avviati semplicemente con un doppio clic sul file stesso o digitando il loro nome nel prompt dei comandi di Windows. Una volta eseguiti, il sistema operativo processa e attua tutti i comandi elencati nel file in sequenza.

Modifica dei file batch: I file batch sono modificabili utilizzando qualsiasi editor di testo, come Notepad o Notepad++. È essenziale essere consapevoli che i comandi contenuti in un file batch possono influire notevolmente sul sistema. Pertanto, è raccomandato prestare particolare attenzione nella modifica e nell'esecuzione di questi file.

Analisi Anyrun

Un file con estensione **.exe** rappresenta un'eseguibile di Windows, cioè un tipo di file che include codice eseguibile progettato per essere lanciato direttamente dal sistema operativo Microsoft Windows. Questi file sono essenziali per l'esecuzione di programmi e applicazioni su piattaforme Windows.

Codice eseguibile: Un file .exe contiene istruzioni in linguaggio macchina, che è il linguaggio a basso livello direttamente comprensibile dalla CPU del computer. Questo tipo di istruzioni è responsabile per l'avvio di programmi, la gestione dell'interazione con l'hardware, l'organizzazione dei file e la facilitazione della comunicazione di rete.

Applicazioni software: I file .exe sono comunemente associati a programmi software quali applicazioni desktop, utility di sistema, giochi, e altri tipi di software. Quando si lancia un file .exe, il sistema operativo carica ed esegue il codice contenuto all'interno del file, avviando così il programma specifico.

Sicurezza: I file .exe possono variare notevolmente in termini di sicurezza; alcuni sono sicuri e provengono da fonti affidabili, mentre altri possono contenere malware o virus che mirano a danneggiare il sistema o rubare informazioni personali. È cruciale scaricare ed eseguire file .exe solo da fonti sicure e riconosciute, e utilizzare software antivirus robusto per difendere il sistema dalle minacce informatiche.

Compatibilità: I file .exe sono progettati specificamente per il sistema operativo Windows e non possono essere eseguiti direttamente su altri sistemi operativi come macOS o Linux. Tuttavia, è possibile eseguire alcuni file .exe su questi sistemi utilizzando emulatori o strumenti di compatibilità come Wine.

Creazione di file .exe: I file .exe vengono generati utilizzando software di sviluppo come Microsoft Visual Studio, Borland Delphi e altri ambienti di sviluppo. Questi strumenti permettono agli sviluppatori di scrivere il codice sorgente del programma e di compilarlo in un file .exe eseguibile.



Analisi Anyrun

cmd.exe è il prompt dei comandi di Windows, noto anche come Command Prompt. È un'applicazione a riga di comando che fornisce un'interfaccia testuale per interagire con il sistema operativo Windows. Di seguito una spiegazione più dettagliata:

Interfaccia testuale: Il Command Prompt offre un'interfaccia testuale dove gli utenti possono inserire comandi specifici per eseguire varie operazioni sul sistema. Tutti gli input e output avvengono tramite testo, senza l'utilizzo di elementi grafici.

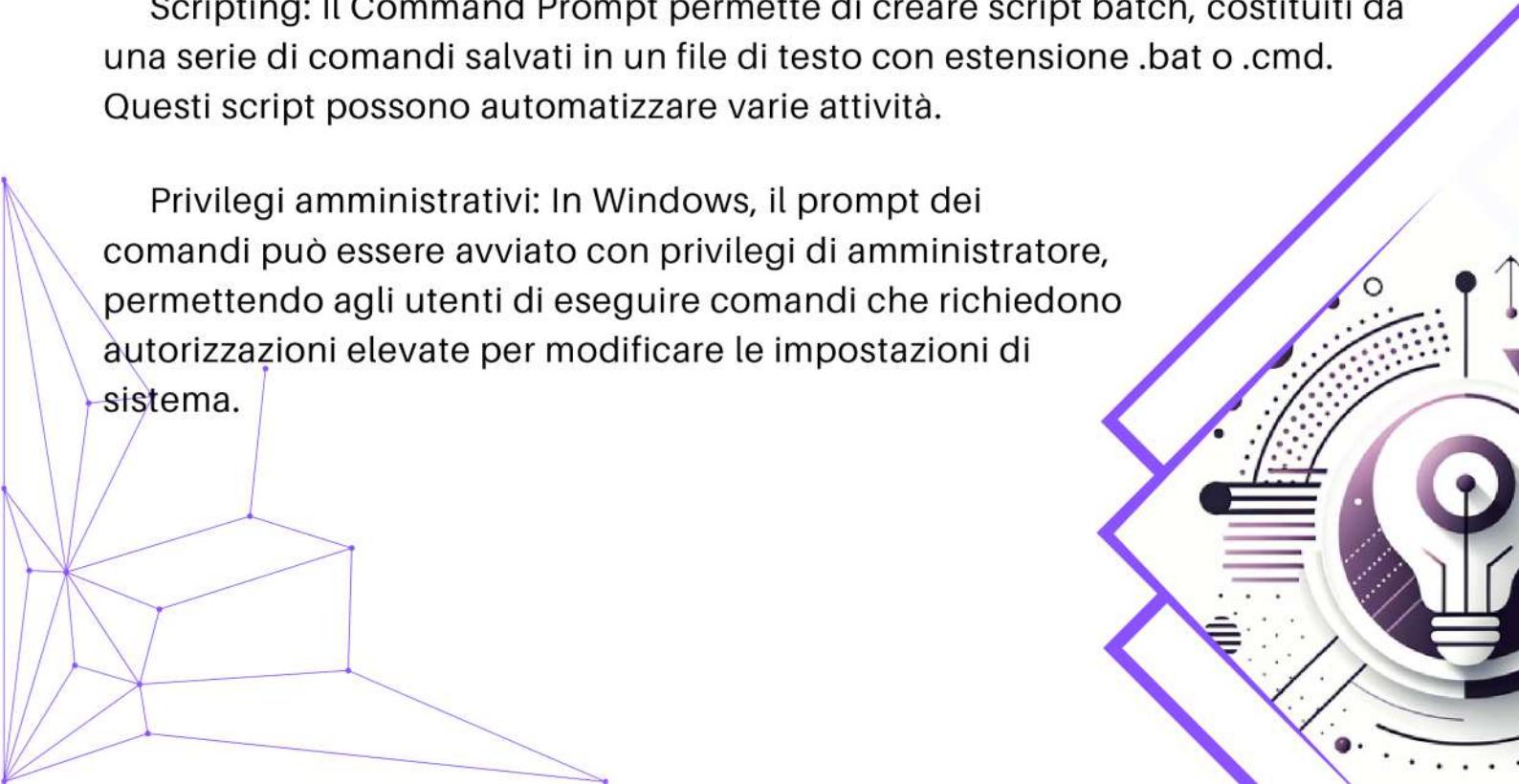
Esecuzione di comandi: Gli utenti possono immettere comandi per eseguire programmi, navigare tra le directory, gestire file e cartelle, eseguire operazioni di rete, visualizzare informazioni di sistema e molto altro.

Sintassi dei comandi: I comandi nel prompt dei comandi di Windows seguono una sintassi specifica. Ad esempio, il comando `dir` elenca i file e le cartelle in una directory, mentre `cd` cambia la directory corrente.

Variabili di ambiente: Il prompt dei comandi consente di visualizzare e modificare le variabili di ambiente del sistema, come le variabili PATH che definiscono i percorsi di ricerca per i file eseguibili.

Scripting: Il Command Prompt permette di creare script batch, costituiti da una serie di comandi salvati in un file di testo con estensione .bat o .cmd. Questi script possono automatizzare varie attività.

Privilegi amministrativi: In Windows, il prompt dei comandi può essere avviato con privilegi di amministratore, permettendo agli utenti di eseguire comandi che richiedono autorizzazioni elevate per modificare le impostazioni di sistema.



Analisi Anyrun

L'.exe PERFORMANCE BOOSTER

Questo script batch sembra essere un tool di ottimizzazione per migliorare le prestazioni dei sistemi Windows, in particolare delle versioni 1709, 1809 e 1903. Ecco una panoramica delle sue funzioni:

1. Configurazione dell'ambiente:

- `@shift /0` : Comando invalido, probabilmente per gestire gli argomenti della riga di comando.
- `@ECHO OFF` : Disattiva l'eco dei comandi.
- `pushd "%~dp0"` : Cambia la directory corrente in quella dello script.

2. Impostazione della modalità di visualizzazione:

- `MODE CON: COLS=78 LINES=54` : Imposta la console su 78x54.

3. Impostazione del titolo della finestra:

- Imposta il titolo della console su "PERFORMANCE BOOSTER_v3.6 by n1kobg".

4. Navigazione alla directory di sistema:

- `cd %systemroot%\system32` : Cambia la directory in quella di sistema.

5. Impostazione della policy di esecuzione di PowerShell:

- `Powershell Set-ExecutionPolicy Unrestricted -Force` : Consente l'esecuzione di tutti gli script PowerShell.

6. Cancellazione dello schermo:

- `CLS` : Cancella la console.

7. Visualizzazione di messaggi di avviso:

- Mostra avvisi sull'uso e i rischi dello strumento.



Analisi Anyrun

8. Creazione di un punto di ripristino e backup del registro:

- Chiede all'utente se desidera fare il backup del registro e crea un punto di ripristino.

9. Patching del file hosts:

- Rimuove l'attributo di sola lettura del file hosts e lo copia nella directory di sistema, quindi lo apre in Notepad.

10. Menu di avvio:

- Mostra un menu con varie opzioni di ottimizzazione: miglioramento delle prestazioni, servizi Windows, stop della telemetria, tweak generali, e uscita.

11. Attende l'input dell'utente:

- Richiede all'utente di scegliere un'opzione e esegue l'azione corrispondente.

12. Esegue l'azione selezionata:

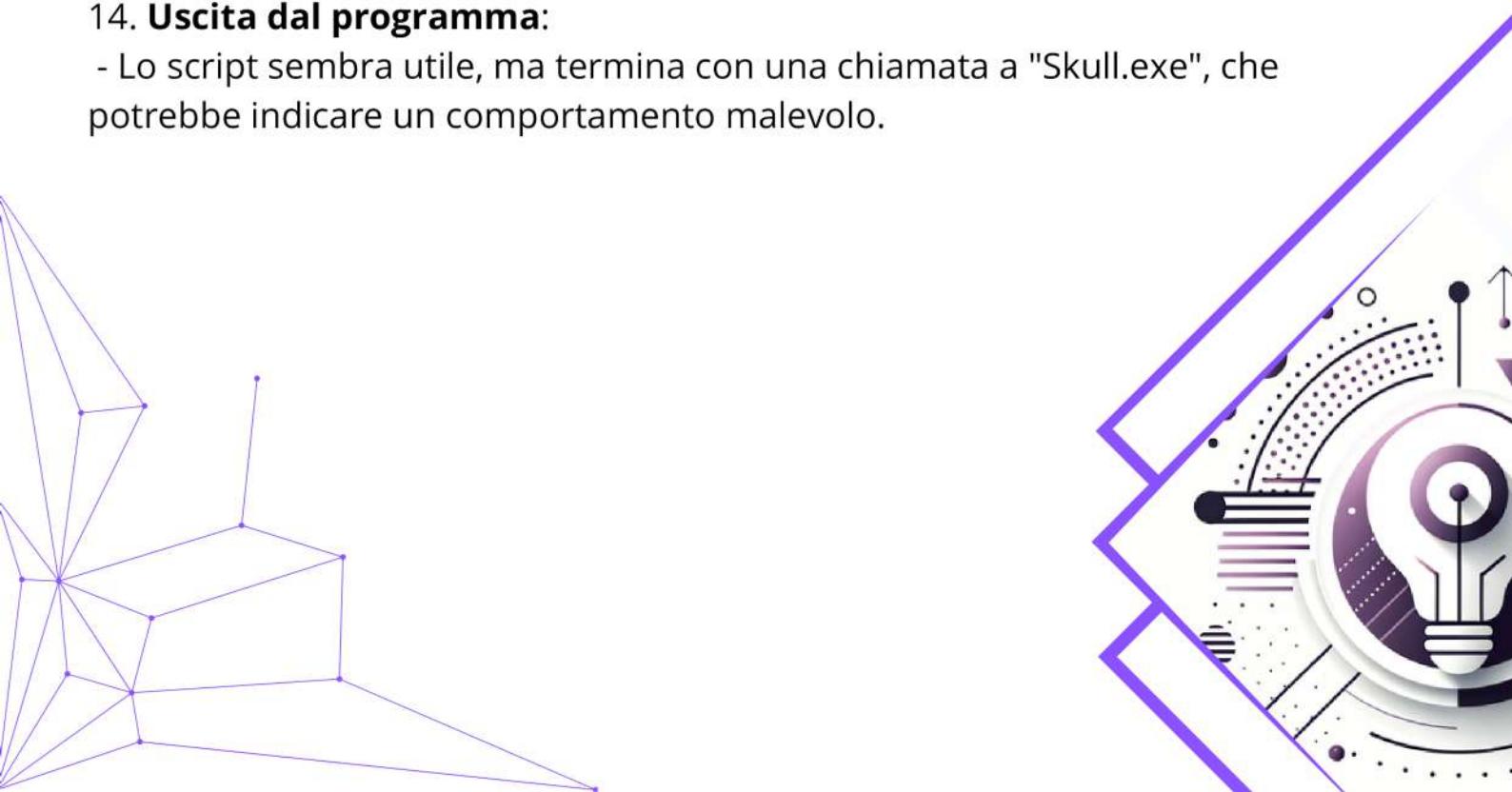
- Ogni opzione del menu esegue una specifica ottimizzazione o modifica.

13. Torna al menu principale:

- Dopo ogni azione, il programma ritorna al menu principale.

14. Uscita dal programma:

- Lo script sembra utile, ma termina con una chiamata a "Skull.exe", che potrebbe indicare un comportamento malevolo.



Analisi Anyrun

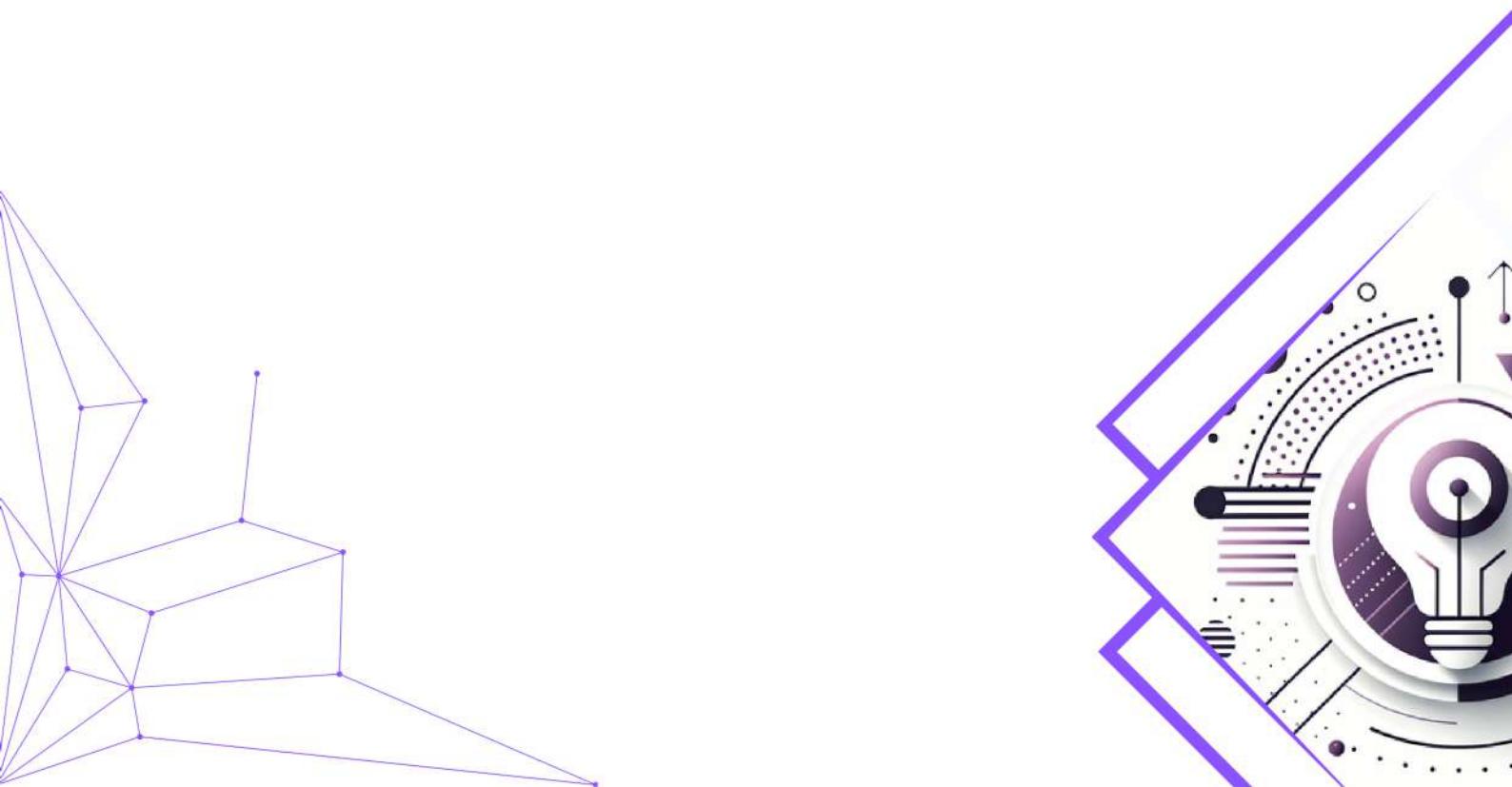
Script in sintesi:

Lo script inizia impostando i parametri della finestra della console, il titolo e cambiando la directory alla cartella system32. Successivamente, imposta la policy di esecuzione di PowerShell su "Unrestricted" (senza restrizioni).

Viene visualizzato un avviso che specifica che lo strumento è progettato per versioni particolari di Windows (v1709, v1809, v1903) e raccomanda cautela per evitare possibili danni al sistema. L'utente deve confermare di aver compreso questi avvisi.

Lo script offre poi la possibilità di eseguire il backup del registro di sistema e creare un punto di ripristino. Modifica il file hosts e lo apre in Notepad per eventuali modifiche.

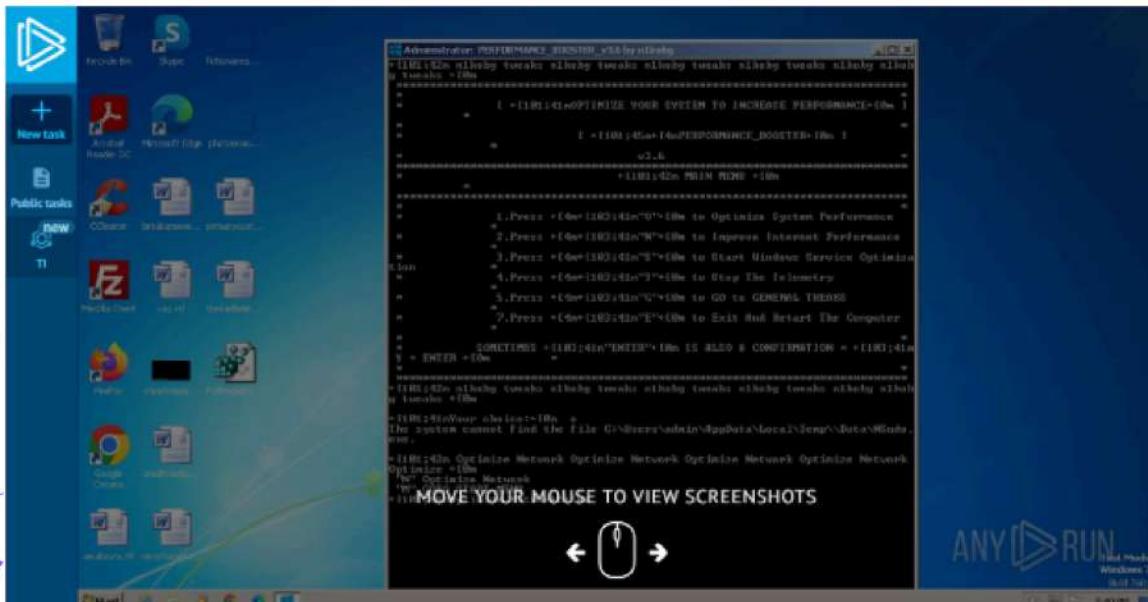
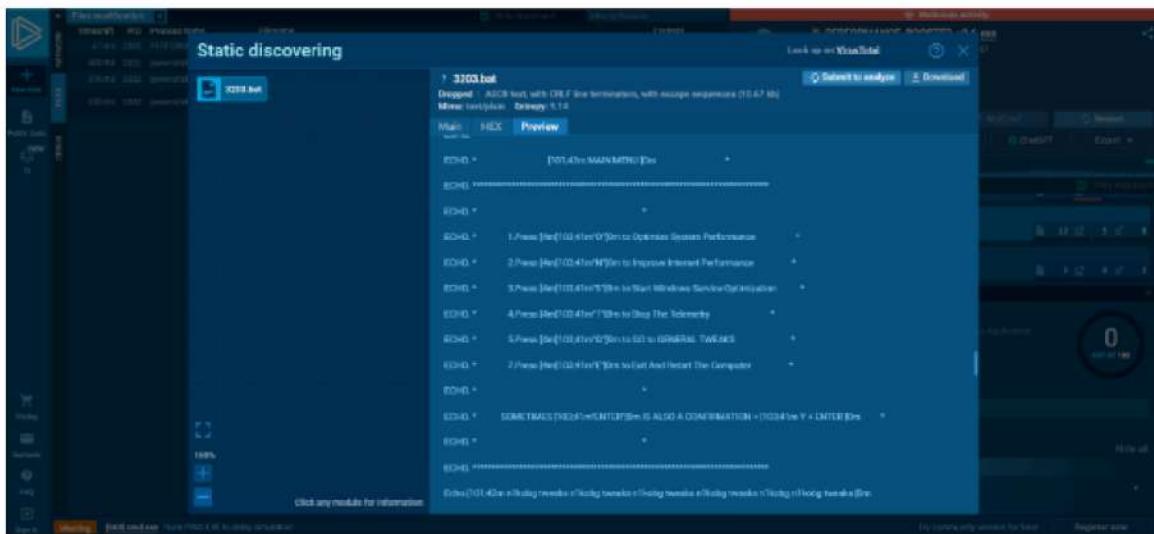
Infine, viene mostrato il menu principale con diverse opzioni di ottimizzazione: migliorare le prestazioni del sistema e di Internet, ottimizzare i servizi, interrompere la telemetria, applicare modifiche generali e uscire dal programma. Ogni opzione esegue un'azione specifica, spesso tramite uno strumento o uno script esterno. Alla chiusura, viene eseguito il file Skull.exe.



Analisi Anyrun

Le criticità

Analizzando le criticità attraverso la pagina di riferimento fornita dalla traccia dell'esercizio utilizzando AnyRun è un servizio online che fornisce un ambiente sicuro e controllato per l'esecuzione e l'analisi dei file eseguibili, dei documenti e delle URL sospette o dannosi. Si tratta di una piattaforma che consente agli utenti di caricare e analizzare file o collegamenti web per identificare potenziali minacce informatiche come malware, virus o altre forme di software dannoso., troviamo la sorgente del file all'interno del tool di analisi. Si nota che il programma è ottimizzato per un PC Windows 10 a 64 bit



Analisi Anyrun

Dove quest'ultimo viene analizzato ed emergono delle criticità:

The screenshot shows the Anyrun analysis interface with several sections of detected behaviors:

- Warning 1**:
 - [T1059.003 Windows Command Shell \(2\)](#)
 - Executing commands from a ".bat" file
 - Starts CMD.EXE for commands execution- Other 3**:
 - Create files in a temporary directory
 - [T1012 Query Registry \(1\)](#)
 - Checks supported languages
 - [T1082 System Information Discovery \(1\)](#)
 - Checks supported languages

Il primo warning T1059 presenta due sotto-punti molto preoccupanti:

Esecuzione automatica del file .bat senza richiesta o autorizzazione da parte dell'utente.

Apertura di cmd.exe in modalità amministratore da parte del programma.

The screenshot shows the Anyrun analysis interface with several sections of detected behaviors:

- Danger 1**:
 - [T1059.001 PowerShell \(1\)](#)
 - Changes powershell execution policy (Unrestricted)
- Warning 4**:
 - Runs PING.EXE to delay simulation
 - [T1222.001 Windows File and Directory Permissions Modification \(1\)](#)
 - Uses ATTRIB.EXE to modify file attributes
 - [T1564.001 Hidden Files and Directories \(1\)](#)
 - Uses ATTRIB.EXE to modify file attributes
 - [T1059.001 PowerShell \(1\)](#)
 - Starts POWERSHELL.EXE for commands execution

Analisi Anyrun

Il **primo pericolo** è la modifica della politica di esecuzione di PowerShell (senza restrizioni): impostare la Execution Policy su Unrestricted è rischioso poiché permette l'esecuzione di qualsiasi script, inclusi quelli scaricati da Internet, senza restrizioni. Questo potrebbe esporre il sistema a rischi di sicurezza. Tuttavia, in alcuni contesti, come durante l'esecuzione di script di automazione su sistemi di sviluppo o test, questa impostazione può risultare utile.

The screenshot shows a dark-themed user interface for an analysis tool. At the top, a yellow bar displays the text "Warning 4". Below this, the main area contains several items listed in a tree-like structure:

- Runs PING.EXE to delay simulation**
- T1222.001 Windows File and Directory Permissions Modification (1)**
 - ↳ **Uses ATTRIB.EXE to modify file attributes**
- T1564.001 Hidden Files and Directories (1)**
 - ↳ **Uses ATTRIB.EXE to modify file attributes**
- T1059.001 PowerShell (1)**
 - ↳ **Starts POWERSHELL.EXE for commands execution**

Gli ultimi 4 warning sono dovuti al fatto che il programma modifica il file ATTRIB.EXE, utilizzato per:

- Visualizzazione degli attributi di un file o una directory: Il comando attrib.exe permette di visualizzare gli attributi di un file o una directory. Ad esempio, eseguendo `attrib.exe nomefile.txt`, verranno mostrati gli attributi del file nomefile.txt.
- Modifica degli attributi di un file o una directory: Il comando attrib.exe può anche modificare gli attributi di un file o una directory. Ad esempio, `attrib.exe +r nomefile.txt` imposterà il file nomefile.txt come "solo lettura", mentre `attrib.exe -r nomefile.txt` rimuoverà l'attributo "solo lettura" dal file.
- Gestione degli attributi nascosti e di sistema: Attrib.exe consente di impostare o rimuovere gli attributi "nascosto" e "di sistema" dai file e dalle directory. Questo può essere utile per nascondere o mostrare determinati file e directory nel sistema operativo.
- Operazioni su più file e directory: attrib.exe supporta operazioni su più file e directory contemporaneamente. Ad esempio, attrib.exe +r *.txt imposta tutti i file con estensione .txt come "solo lettura".

Analisi Anyrun

Installer Microsoft EDGE

Utilizzando Any.Run, viene ricercato e aperto il seguente link:

[<https://1drv.ms/u/s!At7eQ7h8kx6-nQM1RTCuz3aQspOE>]
[\(https://1drv.ms/u/s!At7eQ7h8kx6-nQM1RTCuz3aQspOE\)](https://1drv.ms/u/s!At7eQ7h8kx6-nQM1RTCuz3aQspOE), che ci reindirizza a una pagina di OneDrive.



Automaticamente, Windows richiede di scaricare Microsoft Edge poiché il link è stato aperto con Explorer anziché con Edge. Per impostare Microsoft Edge come browser predefinito al posto di Internet Explorer per aprire determinati tipi di file o per la navigazione web, segui questi passaggi su un sistema operativo Windows:

1. Apri Impostazioni di Windows:
 - Fai clic sull'icona dell'ingranaggio nel menu Start oppure premi il tasto Windows + I sulla tastiera.
2. Seleziona "App":
 - All'interno delle impostazioni di Windows, cerca e fai clic sull'opzione "App".

Analisi Anyrun

Impostazioni predefinite:

1. Apri "App predefinite":

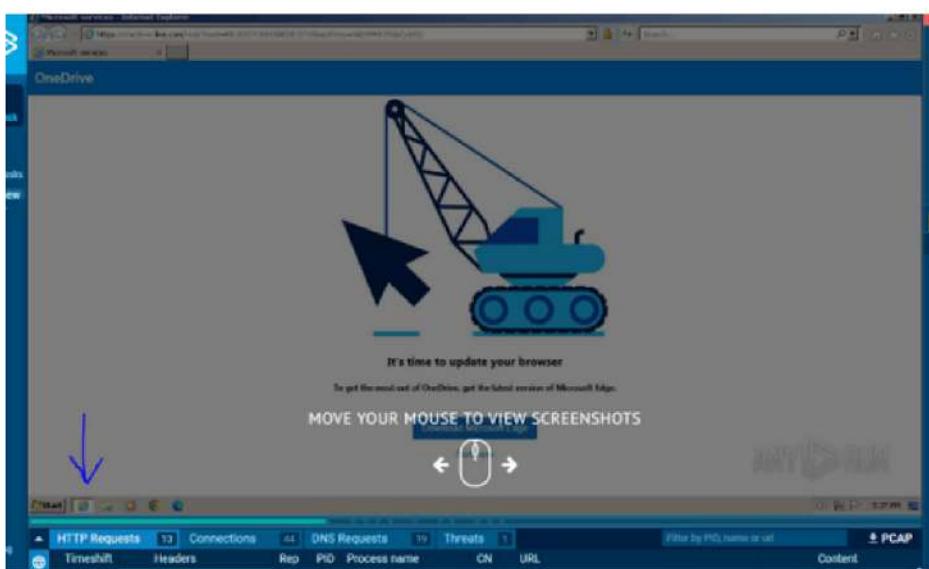
- Nell'elenco di opzioni, trova e fai clic su "App predefinite" nella barra laterale sinistra.

2. Scegli il Browser Web:

- Scorri verso il basso fino a trovare "Browser Web" nell'elenco delle app predefinite. Fai clic su di esso.

3. Seleziona Microsoft Edge:

- Dall'elenco dei browser web disponibili, trova Microsoft Edge e fai clic su di esso per impostarlo come browser predefinito.



Seguendo l'installazione guidata, è possibile tenere traccia automaticamente di tutti gli indirizzi coinvolti nel processo.

Questo permette di monitorare ogni URL e percorso utilizzato durante l'installazione.

Analisi Anyrun



Al termine dell'installazione, Microsoft Edge si aprirà automaticamente, indicando che è stato correttamente installato sul dispositivo.

Una problematica riscontrata dall'analisi è la possibile violazione della privacy, che può derivare dal tracciamento e dalla raccolta di dati durante il processo di installazione e utilizzo del browser.

Analisi Anyrun

Threat details

Here are the details of the threat

Main Stream data HTTP Suri^{new}cata rule

Potential Corporate Privacy Violation

ET POLICY PE EXE or DLL Windows file download HTTP

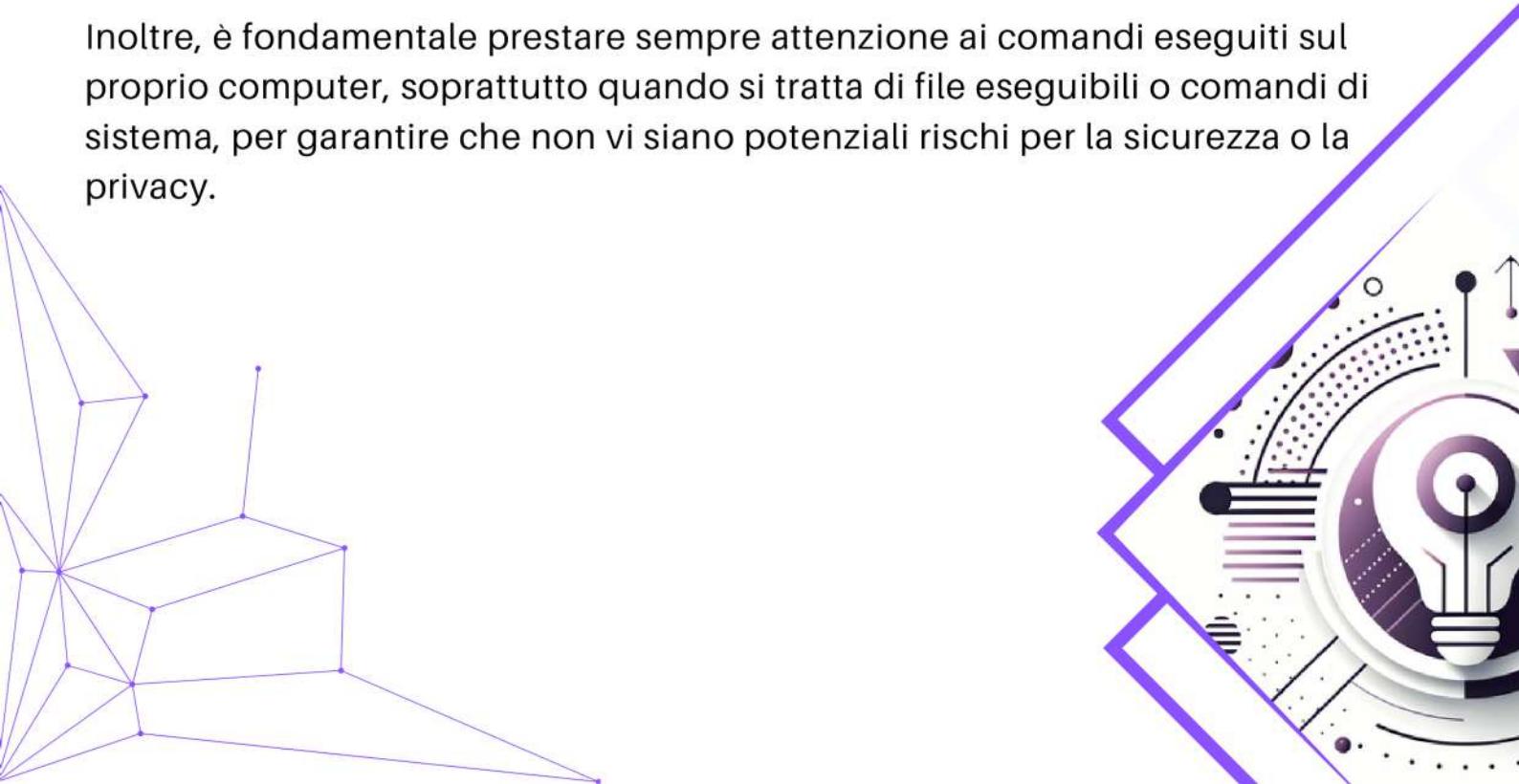
Src / Dst	2.21.20.142 : 80 ↳ 192.168.100.152 : 49245
Timeshift	32509 ms
SID	2018959
Transport	TCP
App Protocol	HTTP
Src IP	2.21.20.142
Dest IP	192.168.100.152
Src Port	80
Dest Port	49245
HTTP TxID	1
To DestIP Packet	78
To SrcIP Packet	20
Total Bytes	104440
Rule metadata	updated_at 2023_04_12; former_category POLICY; created_at 2014_08_19;

Una potenziale violazione della privacy aziendale può verificarsi quando un'azienda gestisce in modo improprio o illegale le informazioni personali dei propri dipendenti, clienti o altre parti interessate. Questo può includere:

- La raccolta non autorizzata di dati personali.
- L'accesso non autorizzato ai dati sensibili.
- La mancanza di sicurezza delle informazioni.
- La divulgazione non autorizzata dei dati personali.

Tali comportamenti possono mettere a rischio la privacy delle persone coinvolte e comportare gravi conseguenze legali, finanziarie e reputazionali per l'azienda. Pertanto, è essenziale che le aziende adottino politiche e pratiche rigorose per proteggere la privacy dei loro dipendenti e clienti.

Inoltre, è fondamentale prestare sempre attenzione ai comandi eseguiti sul proprio computer, soprattutto quando si tratta di file eseguibili o comandi di sistema, per garantire che non vi siano potenziali rischi per la sicurezza o la privacy.



Analisi Anyrun

Invece come unico "Warning" riscontriamo:

Behavior activities
(PID: 3796) MicrosoftEdgeUpdate.exe

Source: process First seen: 29109 ms

?

Warning / Unusual Activities
Executes as Windows Service
T1569.002 Service Execution

Image: C:\Program Files\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe
Cmdline: "C:\Program Files\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe" /svc

"Unusual activities" significa letteralmente "attività insolite" o "attività non comuni". Nel contesto aziendale o della sicurezza informatica, il termine si riferisce a comportamenti o azioni che si discostano dalla norma e che potrebbero indicare una potenziale minaccia o un problema.

Per verificare l'affidabilità della fonte, è importante controllare l'indirizzo e assicurarsi che provenga da una fonte attendibile.

CONCLUSIONI

L'analisi della sicurezza per l'applicazione di e-commerce ha evidenziato la necessità di misure preventive e risposte efficaci agli attacchi. Per proteggere contro SQL Injection (SQLi) e Cross-Site Scripting (XSS), è essenziale implementare un Web Application Firewall (WAF) e adottare pratiche di validazione e sanitizzazione degli input.

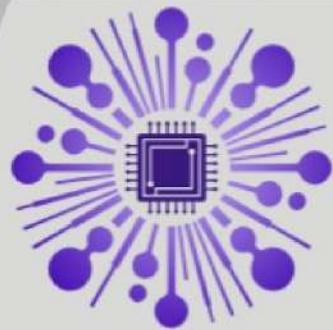
In caso di attacco DDoS, che potrebbe causare una perdita economica significativa, è consigliabile usare soluzioni di mitigazione DDoS per ridurre l'impatto. Se il sistema viene infettato da malware, la priorità è isolare il server compromesso per evitare la propagazione all'interno della rete.

Una protezione completa dovrebbe combinare le misure preventive con le strategie di risposta, includendo WAF, segmentazione della rete, mitigazione DDoS e politiche firewall rafforzate. L'integrazione di sistemi di rilevamento delle intrusioni (IDS/IPS) e l'autenticazione multi-fattore (MFA) possono ulteriormente migliorare la sicurezza.

Analisi delle segnalazioni su AnyRun

L'analisi delle segnalazioni su AnyRun ha permesso di identificare e comprendere diverse tipologie di attacco, come phishing e malware. È importante educare utenti e dirigenti riguardo alla natura di questi attacchi e implementare misure preventive come l'addestramento sulla sicurezza informatica, l'utilizzo di software di sicurezza aggiornati e la creazione di policy di sicurezza efficaci.

In conclusione, proteggere l'infrastruttura di e-commerce richiede un approccio multilivello che combina misure preventive, strategie di risposta e miglioramenti infrastrutturali. Seguendo queste raccomandazioni, si può significativamente ridurre il rischio di attacchi e minimizzare l'impatto sul business.



EVILCORP

IF IT WORKS DONT TOUCH IT



EPICODE

Giugno 2024