

ANTONIO FABIO
PERNA NOBILI



INDICE

Parte 1: WHO WE ARE

MISSION

TEAM

REGOLE D'INGAGGIO

PREVENTIVO

Parte 2: INTRODUZIONE

OBBIETTIVO

SVOLGIEMNTO LAVORO RICHIESTO

COCNLUSIONI

Parte 3: INTRODUZIONE

OBBIETTIVO

SVOLGIEMNTO LAVORO RICHIESTO

COCNLUSIONI

Parte 4: INTRODUZIONE

OBBIETTIVO

SVOLGIEMNTO LAVORO RICHIESTO

COCNLUSIONI

Parte 5: INTRODUZIONE

OBBIETTIVO

SVOLGIEMNTO LAVORO RICHIESTO

COCNLUSIONI

Parte 6: INTRODUZIONE

OBBIETTIVO

SVOLGIEMNTO LAVORO RICHIESTO

COCNLUSIONI



WHO WE ARE

CYBER SECURITY
SPECIALIST

Siamo dei professionisti altamente qualificati nel campo della cybersecurity, con una vasta esperienza nella protezione delle infrastrutture digitali. Come liberi professionisti specializzati in sicurezza informatica, ci occupiamo di identificare e mitigare le vulnerabilità.



MISSION

"INSIEME PER PROTEGGERE IL TUO FUTURO DIGITALE"



La nostra missione è rendere il mondo digitale un luogo sicuro e affidabile per tutte le aziende. Ci impegniamo a proteggere i dati sensibili, preservare la reputazione aziendale e garantire la continuità operativa attraverso soluzioni innovative e proattive di sicurezza informatica.

Il nostro obiettivo principale è aiutare le aziende a comprendere l'importanza cruciale di solide misure di sicurezza informatica e implementare soluzioni che proteggano i loro dati e sistemi preziosi da attacchi dannosi.

REGOLE D'INGAGGIO



Le regole d'ingaggio delineano chiaramente i termini, le condizioni e le procedure operative per l'esecuzione dei servizi di sicurezza che forniamo. In seguito abbiamo stipulato un documento che fornisce un quadro dettagliato delle responsabilità, delle aspettative e delle metodologie che verranno utilizzate durante i nostri incarichi.

In modo tale da assicura una comprensione comune tra noi professionisti della sicurezza informatica e il cliente, facilitando un lavoro efficace e sicuro.

REGOLE D'INGAGGIO DOCUMENTO

1. Obiettivo: L'obiettivo principale è migliorare la sicurezza informatica del cliente identificando e mitigando vulnerabilità, configurando adeguatamente firewall, e proteggendo il sistema contro attacchi esterni.

2. Ambito del Lavoro: Il lavoro coprirà i seguenti ambiti, personalizzabili in base alle specifiche esigenze del cliente:

- Valutazione delle vulnerabilità: Analisi iniziale per identificare le debolezze nel sistema.
- Configurazione del firewall: Implementazione e ottimizzazione delle regole del firewall.
- Test di penetrazione: Esecuzione di test controllati per valutare la robustezza delle difese.
- Monitoraggio e manutenzione: Monitoraggio continuo e aggiornamento delle misure di sicurezza.

3. Ambiente di lavoro: L'ambiente in cui si effettueranno i test sarà scelto dal cliente, garantendo la massima aderenza alle necessità specifiche.

Le opzioni includono:

- White Box: Test con conoscenza completa del sistema, inclusi dettagli sull'architettura e sul codice sorgente.
- Gray Box: Test con conoscenza parziale del sistema, limitato a determinate informazioni fornite dal cliente.
- Black Box: Test senza alcuna conoscenza preliminare del sistema, simulando un attacco esterno senza informazioni privilegiate.

4. Strumenti Utilizzati Gli strumenti da utilizzare verranno scelti in anticipo in base alle specifiche esigenze del progetto e del cliente. Se c'è la necessità di un tool specifico per il progetto, il costo dell'abbonamento a questo tool sarà compreso nel preventivo.

5. Pianificazione del Lavoro: Le fasi del lavoro saranno descritte in anticipo in base alle specifiche del progetto. Ecco una sintesi delle possibili fasi:

- Preparazione: Raccolta delle informazioni iniziali, configurazione degli strumenti, impostazione degli ambienti di test.
- Valutazione delle Vulnerabilità: Scansione delle reti, analisi delle vulnerabilità, documentazione dei risultati.
- Configurazione del Firewall: Implementazione delle regole del firewall, test di efficacia, ottimizzazione delle configurazioni.
- Test di Penetrazione: Esecuzione di attacchi simulati, verifica delle difese, suggerimenti per miglioramenti.
- Monitoraggio e Manutenzione: Monitoraggio continuo, aggiornamenti regolari, risposta agli incidenti.

6. Condizioni Operative

- Riservatezza: Tutte le informazioni ottenute durante il progetto saranno trattate con la massima riservatezza.
- Autorizzazioni: Tutte le attività di test di penetrazione richiedono autorizzazioni scritte dal cliente.
- Rapporti di Avanzamento: Rapporti settimanali dettagliati saranno forniti al cliente.

7. Tariffa Oraria e Costi: Tariffa Oraria: €200/ora Stima del Tempo di Lavoro: Da determinare in base alle specifiche del progetto.

8. Conclusione del Progetto: Documentazione Finale: Report conclusivo con tutte le attività svolte, i risultati delle analisi e le raccomandazioni.

- Sessione di Debriefing: Incontro finale per discutere i risultati e i passi successivi.

9. Termini e Condizioni: Pagamenti: Fatturazione mensile basata sulle ore lavorate.

- Modifiche al Contratto: Qualsiasi modifica al contratto deve essere concordata per iscritto.
- Risarcimenti e Garanzie: Dettagli sui risarcimenti in caso di violazioni contrattuali.





PREVENTIVO

- PER I SERVIZI DI SICUREZZA INFORMATICA, LA NOSTRA **TARIFFA ORARIA È DI €200/ORA.**
- QUESTA TARIFFA COMPRENDE TUTTE LE SPESE OPERATIVE E ASSICURA UN SERVIZIO ADEGUATO, PUÒ VARIARE IN CASO DI EMERGENZA (TURNI NOTTURNI, ATTACCHI AL SISTEMA)
- TEST E ATTIVAZIONE FIREWALL 1600€
- BUSINESS CONTINUITY E DEL DISASTER RECOVERY. 1600€
- IOC 1600€
- ISOLAMENTO E RIMOZIONE SISTEMI INFETTI 1600€
- CREARE DELLE SOLUZIONI SULLE RETI ATTACCATE 1600€
- TOTALE ORE DI LAVORO=40
- TOTALE PREVENTIVO= $200 \times 40 = >8000\text{€}$

INTRODUZIONE



VALUTAZIONE DELL'IMPATTO DEL FIREWALL SU WINDOWS XP

L'obiettivo del lavoro assegnato dall'azienda è verificare come l'attivazione del firewall impatti il risultato di una scansione dei servizi dall'esterno. Il processo sarà eseguito seguendo questi passaggi:

- 1. Disattivazione del Firewall:** Assicurarsi che il firewall sia disattivato sulla macchina Windows XP.
- 2. Scansione Iniziale con Nmap:** Effettuare una scansione con Nmap sulla macchina target utilizzando lo switch `-sV` per la rilevazione dei servizi e `-o nomefilereport` per salvare l'output in un file.
- 3. Attivazione del Firewall:** Abilitare il firewall sulla macchina Windows XP.
- 4. Seconda Scansione con Nmap:** Effettuare una seconda scansione con Nmap, utilizzando nuovamente lo switch `-sV`.
- 5. Analisi delle Differenze:** Identificare e motivare le eventuali differenze nei risultati delle due scansioni. Questo processo permetterà di comprendere l'efficacia del firewall nell'oscurare i servizi esposti e di evidenziare l'importanza di una configurazione adeguata per proteggere la rete aziendale da potenziali minacce.

PREVENTIVO **ESERCIZIO 1**



Preventivo Basato su Ore di Lavoro

Dettagli del Lavoro:

- 1.Verifica dello Stato del Firewall: Assicurarsi che il firewall sia disabilitato sulla macchina Windows XP.
- 2.Scansione con Nmap (Firewall disabilitato): Effettuare una scansione con Nmap usando lo switch -sV per la rilevazione dei servizi e salvare l'output in un file.
- 3.Attivazione del Firewall: Abilitare il firewall sulla macchina Windows XP.
- 4.Scansione con Nmap (Firewall abilitato): Effettuare una seconda scansione con Nmap usando lo switch -sV.
- 5.Analisi delle Differenze: Identificare e spiegare le differenze tra le due scansioni.

Ore di Lavoro e Tool Utilizzati:

- Preparazione e Configurazione: 1 ora
 - Verifica dello stato del firewall
 - Configurazione degli strumenti necessari (Nmap, firewall settings)
- Scansione Iniziale con Nmap: 1 ora
 - Esecuzione della scansione
 - Salvataggio e verifica dell'output
- Attivazione del Firewall: 0.5 ore
 - Configurazione e verifica del firewall su Windows XP
- Scansione Secondaria con Nmap: 1 ora
 - Esecuzione della seconda scansione
 - Salvataggio e verifica dell'output
- Analisi delle Differenze: 2 ore
 - Confronto tra i risultati delle due scansioni
 - Documentazione e spiegazione delle differenze
- Report Finale e Presentazione: 1.5 ore
 - Redazione di un report completo con le osservazioni
 - Preparazione della presentazione dei risultati

Totale Ore di Lavoro: 8 ore

TOTALE PREVENTIVO: 1600,00 €

COSA FARE

L'obiettivo del lavoro è mostrare all'azienda come l'attivazione del firewall influisca sui risultati di una scansione dei servizi dall'esterno.

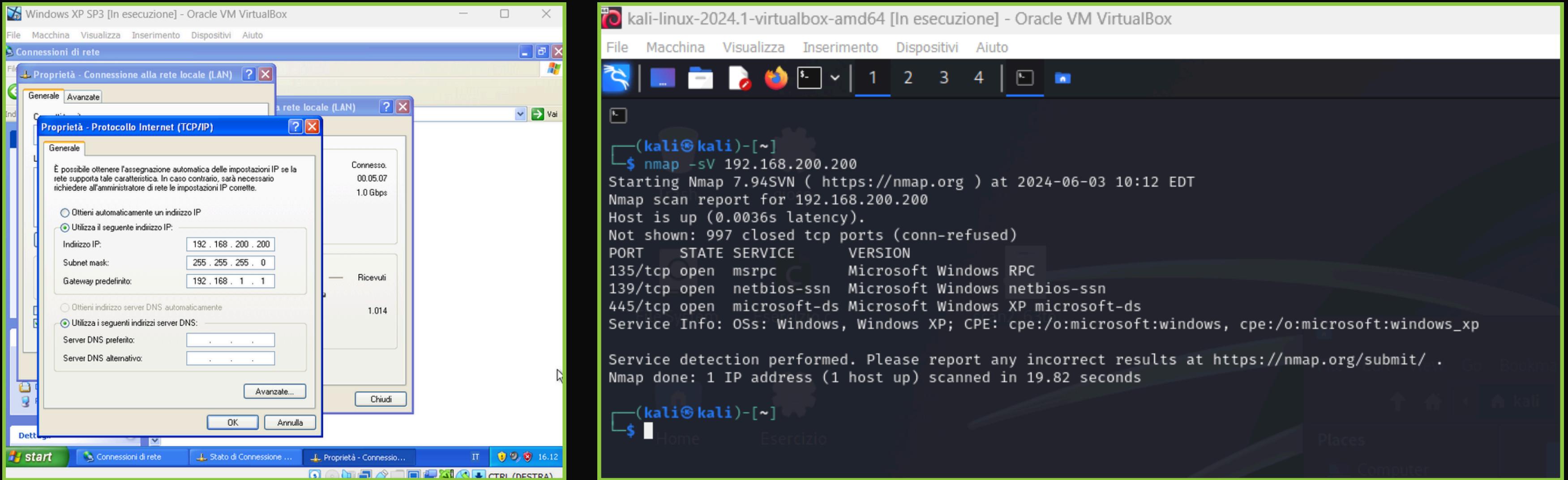
Per raggiungere questo obiettivo, il processo sarà eseguito seguendo questi passaggi:

1. Disattivazione del Firewall: Assicurarsi che il firewall sia disattivato sulla macchina Windows XP.
2. Scansione Iniziale con Nmap: Effettuare una scansione con Nmap sulla macchina target, utilizzando lo switch `-sV` per la rilevazione dei servizi e `-o nomefilereport` per salvare l'output in un file.
3. Attivazione del Firewall: Abilitare il firewall sulla macchina Windows XP.
4. Seconda Scansione con Nmap: Effettuare una seconda scansione con Nmap, utilizzando nuovamente lo switch `-sV`.
5. Analisi delle Differenze: Identificare e spiegare le eventuali differenze nei risultati delle due scansioni.

Mostreremo all'azienda come l'attivazione del firewall può nascondere i servizi esposti, evidenziando l'importanza di una configurazione adeguata per proteggere la rete aziendale da potenziali minacce.



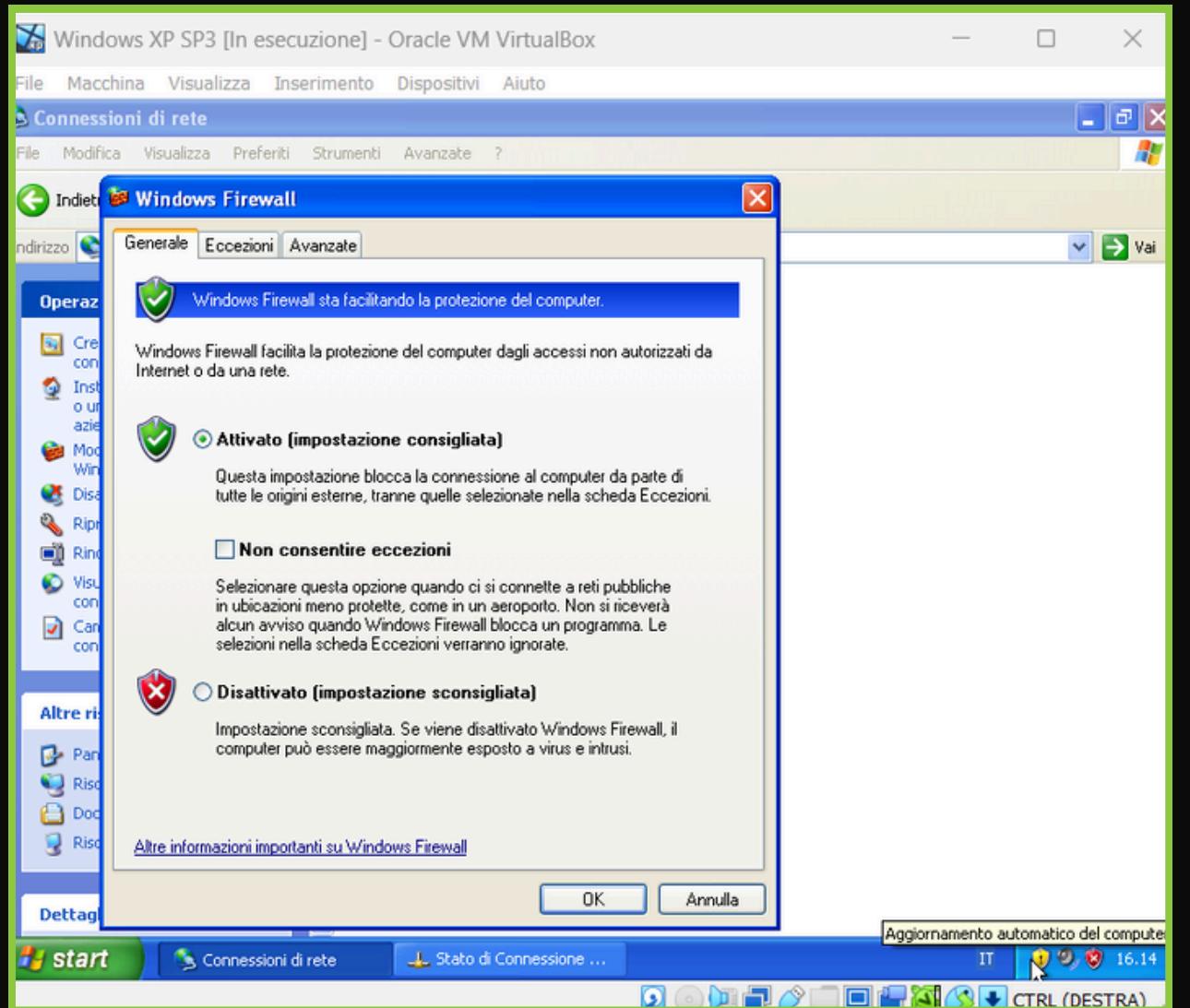
PROVA CON FIREWALL DISATTIVO



Dopo aver configurato l'indirizzo IP della macchina target, procederemo con una scansione utilizzando il comando nmap -sV. Questa operazione ci permetterà di identificare tutte le porte aperte e i servizi attivi sulla macchina, fornendo una visione dettagliata della superficie di attacco esposta.



PROVA CON FIREWALL ATTIVO



Dopo aver attivato il firewall sulla macchina target, ripetiamo la scansione con Nmap utilizzando lo stesso comando nmap -sV. Notiamo che la scansione non riesce a fornire i risultati attesi. La scansione non va a buon fine e ci consiglia di provare con il comando -Pn

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.200.200
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 10:15 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 3.24 seconds
```



PROVA CON FIREWALL ATTIVO

A questo punto, eseguiremo una nuova scansione utilizzando lo switch -Pn con il comando nmap -sV <indirizzo IP> -Pn. Questo switch dice a Nmap di ignorare il ping e di procedere come se il target fosse attivo.

Risultati e Spiegazione:

- Comando: nmap -sV -Pn <indirizzo IP>
- Osservazioni: Con il firewall attivo, Nmap rileva le porte ma non può determinare se sono aperte o chiuse, poiché il firewall limita la comunicazione con la macchina.

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.200.200 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 10:16 EDT
Nmap scan report for 192.168.200.200
Host is up.
All 1000 scanned ports on 192.168.200.200 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 216.37 seconds
```



CONCLUSIONI

- L'attivazione del firewall limita efficacemente la capacità di Nmap di ottenere informazioni dettagliate sulle porte e sui servizi attivi. Questo dimostra l'importanza del firewall nella protezione della rete, in quanto impedisce agli attaccanti di raccogliere informazioni critiche che potrebbero essere utilizzate per attacchi futuri. In questo modo, il firewall contribuisce a mantenere la sicurezza e l'integrità del sistema.



INTRODUZIONE ESERCIZIO 2

Siamo stati incaricati di valutare quantitativamente l'impatto di vari disastri su specifici asset aziendali, nell'ambito della business continuity e del disaster recovery.

Il nostro compito è analizzare i dati disponibili e calcolare la perdita annuale stimata che la compagnia subirebbe in caso di differenti eventi catastrofici.

Questo processo aiuterà l'azienda a comprendere meglio i rischi associati ai loro asset critici e a sviluppare strategie efficaci di mitigazione.



PREVENTIVO ESERCIZIO 2



PREVENTIVO BASATO SU ORE DI LAVORO

Dettagli del Lavoro:

1. Stipulazione disaster recovery planning
2. Stima perdite annue in base al fenomeno che avviene e allo stabilimento che colpisce
 - Inondazione sull'asset «edificio secondario»
 - Terremoto sull'asset «datacenter»
 - Incendio sull'asset «edificio primario»
 - Incendio sull'asset «edificio secondario»
 - Inondazione sull'asset «edificio primario»
 - Terremoto sull'asset «edificio primario»

Totale Ore di Lavoro: 8 ore

TOTALE PREVENTIVO: 1600,00 €

COSA FARE

Il nostro compito è analizzare e calcolare la perdita annuale stimata per la compagnia in caso di differenti eventi disastrosi. Gli scenari da considerare includono:

- Inondazione sull'asset "edificio secondario"
- Terremoto sull'asset "datacenter"
- Incendio sull'asset "edificio primario"
- Incendio sull'asset "edificio secondario"
- Inondazione sull'asset "edificio primario"
- Terremoto sull'asset "edificio primario"



METODOLOGIA

- Raccolta dei Dati: Analisi dei dati forniti dall'azienda relativi ai costi di riparazione, tempo di inattività, e altri fattori economici associati a ciascun asset.
- Valutazione delle Perdite: Calcolo della perdita annuale per ogni scenario disastroso, considerando la frequenza stimata degli eventi e l'impatto economico specifico su ogni asset.
- Presentazione dei Risultati: Redazione di un report dettagliato che includa le stime delle perdite annuali e le raccomandazioni per mitigare tali rischi.



TABELLE DI RIFERIMENTO

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%



INONDAZIONE SULL'ASSET «EDIFICIO SECONDARIO»

Per calcolare il danno subito, dobbiamo calcolare prima a calcolare il danno economico ogni qualvolta si verifica questo tipo di fenomeno.

Prendendo in considerazione le tabelle in precedenza, notiamo che:

- Il valore dell'edificio secondario è di 150.000€ (**AV**)
- l'inondazione fa un danno del 40% (**EF**)

Avendo questi dati alla mano, possiamo andare a calcolare il valore economico del danno che si calcola moltiplicando il valore dell'asset per la percentuale di inondazione;
quindi otterremo questo risultato:

$$150.000 * 0,4 = 60.000\text{€} \text{ (**SLE**)}$$

Fatto ciò, andiamo a spalmare il danno economico per l'occorenza annua e andiamo a calcolare le perdite annue.

Siccome il fenomeno avviene 1 volta ogni 50 anni (**ARO**), andiamo a moltiplicare
 $60.000 * 0,02 = 1200\text{€}$.

Di conseguenza, la perdita annua è di 1200€ (**ALE**)



TERREMOTO SULL'ASSET «DATACENTER»

Procediamo come fatto in precedenza e quindi:

$$SLE = AV * EF \rightarrow 100.000 * 0,95 = 95.000 \text{€}$$

$$ALE = SLE * ARO \rightarrow 95.000 * 0,03 = 2850 \text{€/anno}$$

INCENDIO SULL'ASSET «EDIFICIO PRIMARIO»

$$SLE = AV * EF \rightarrow 350.000 * 0,6 = 210.000 \text{€}$$

$$ALE = SLE * ARO \rightarrow 210.000 * 0,05 = 10.500 \text{€/anno}$$

INCENDIO SULL'ASSET «EDIFICIO SECONDARIO»

$$SLE = AV * EF \rightarrow 150.000 * 0,5 = 75.000 \text{€}$$

$$ALE = SLE * ARO \rightarrow 75.000 * 0,05 = 3.750 \text{€/anno}$$



INONDAZIONE SULL'ASSET «EDIFICIO PRIMARIO»

Procediamo come fatto in precedenza e quindi:

$$SLE = AV * EF \rightarrow 350.000 * 0,55 = 192.000 \text{€}$$

$$ALE = SLE * ARO \rightarrow 192.000 * 0,02 = 3840 \text{€/anno}$$

TERREMOTO SULL'ASSET «EDIFICIO PRIMARIO»

$$SLE = AV * EF \rightarrow 350.000 * 0,8 = 280.000 \text{€}$$

$$ALE = SLE * ARO \rightarrow 280.000 * 0,03 = 8.400 \text{€/anno}$$



INTRODUZIONE ESERCIZIO 3



Ci è stato richiesto di analizzare una cattura di rete effettuata con Wireshark al fine di individuare possibili minacce informatiche e proporre strategie di difesa.

Questo esercizio pratico ci consentirà di mettere in pratica le nostre conoscenze sulla Threat Intelligence e sugli Indicatori di Compromissione (IOC), fornendoci un'opportunità unica per identificare e mitigare potenziali attacchi informatici.



PREVENTIVO BASATO SU ORE DI LAVORO

Dettagli del Lavoro:

1. Identificare attacchi in corso
2. Capire il potenziale vettore di attacco
3. Azioni per ridurre gli impatti dell'attacco

Totale Ore di Lavoro: 8 ore

TOTALE PREVENTIVO: 1600,00 €

COSA FARE

Analizzare attentamente la cattura di rete fornita e identificare eventuali IOC, che sono segnali di attività sospette o comportamenti anomali che potrebbero indicare la presenza di un attacco in corso. Utilizzando queste informazioni, formuleremo ipotesi sui potenziali vettori di attacco utilizzati dagli aggressori. Infine, consiglieremo azioni specifiche per ridurre gli impatti dell'attacco e migliorare la sicurezza complessiva del sistema.



FILE WIRESHARK

1 0.000000000	192.168.200.150	192.168.200.255	BROWSER	286 Host Announcement METASPOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Potential B
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 TSval=810522427 TSecr=0 WS=128
3 23.764287789	192.168.200.100	192.168.200.150	TCP	74 33876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522428 TSecr=0 WS=128
4 23.764777323	192.168.200.150	192.168.200.100	TCP	74 80 → 53060 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294951165 TSecr=810522427 WS=64
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 TSval=810522428 TSecr=4294951165
7 23.764899091	192.168.200.100	192.168.200.150	TCP	66 53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=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
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 TSecr=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 TSecr=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 TSecr=0 WS=128
15 36.774366305	192.168.200.100	192.168.200.150	TCP	74 58636 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=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 TSecr=0 WS=128
17 36.774535534	192.168.200.100	192.168.200.150	TCP	74 46138 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=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 TSecr=0 WS=128
19 36.774685505	192.168.200.150	192.168.200.100	TCP	74 23 → 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
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 TSecr=810535437 WS=64
21 36.774685696	192.168.200.150	192.168.200.100	TCP	60 443 → 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22 36.774685737	192.168.200.150	192.168.200.100	TCP	60 554 → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23 36.774685776	192.168.200.150	192.168.200.100	TCP	60 135 → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24 36.774700464	192.168.200.100	192.168.200.150	TCP	66 41304 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
25 36.774711072	192.168.200.100	192.168.200.150	TCP	66 56120 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
26 36.775141104	192.168.200.150	192.168.200.100	TCP	60 993 → 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27 36.775141273	192.168.200.150	192.168.200.100	TCP	74 21 → 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535438 WS=64
28 36.775174048	192.168.200.100	192.168.200.150	TCP	66 41182 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
29 36.775337800	192.168.200.100	192.168.200.150	TCP	74 59174 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
30 36.775386694	192.168.200.100	192.168.200.150	TCP	74 55656 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
31 36.775524204	192.168.200.100	192.168.200.150	TCP	74 53062 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
32 36.775589806	192.168.200.150	192.168.200.100	TCP	60 113 → 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33 36.775619454	192.168.200.100	192.168.200.150	TCP	66 41304 → 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
34 36.775652497	192.168.200.100	192.168.200.150	TCP	66 56120 → 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
35 36.775796938	192.168.200.150	192.168.200.100	TCP	74 22 → 55656 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
36 36.775797004	192.168.200.150	192.168.200.100	TCP	74 80 → 53062 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
37 36.775803786	192.168.200.100	192.168.200.150	TCP	66 55656 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
38 36.775813232	192.168.200.100	192.168.200.150	TCP	66 53062 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
39 36.775861964	192.168.200.100	192.168.200.150	TCP	66 41182 → 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
40 36.775975876	192.168.200.100	192.168.200.150	TCP	66 55656 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
41 36.776005853	192.168.200.100	192.168.200.150	TCP	66 53062 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466

IN GRIGIO CI SONO TUTTE LE RICHIESTE DA PARTE DELL'ATTACCANTE
 IN VERDE VEDIAMO LE RICHIESTE APPROVATE AD INDICARE PORTE APERTE
 IN ROSSO, TUTTE LE RICHIESTE RIFIUTATE E QUINDI TUTTE LE PORTE CHIUSE



IDENTIFICARE EVENTUALI IOC

Dalla tabella di wireshark caricata in precedenza, possiamo notare che ci sono molteplici richieste **TCP** in corso su porte sempre diverse

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 TSecr=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 TSecr=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 TSecr=0 WS=128
15 36.774366305	192.168.200.100	192.168.200.150	TCP	74 58636 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=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 TSecr=0 WS=128
17 36.774535534	192.168.200.100	192.168.200.150	TCP	74 46138 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=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 TSecr=0 WS=128
19 36.774685505	192.168.200.150	192.168.200.100	TCP	74 23 → 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
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 TSecr=810535437 WS=64



IPOTESI SUI POTENZIALI VETTORI DI ATTACCO

Da quello che possiamo vedere e dalle molteplici richieste, possiamo dire che probabilmente, l'attaccante sta facendo uno scanner sul target e sulle porte perché in alcuni casi vediamo che il target tisponde con (SYN,ACK) ovvero che la porta è aperta mentre, in altri casi, risponde con (RST,ACK) che sta ad indicare la porta chiusa.

Time	Source	Destination	Protocol	Length	Info
0.000000000	192.168.200.150	192.168.200.255	BROWSER	286	Host Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Pote
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 TSval=810522427 TSecr=0 WS=128
23.764287789	192.168.200.100	192.168.200.150	TCP	74	33876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522428 TSecr=0 WS=128
23.764777323	192.168.200.150	192.168.200.100	TCP	74	80 → 53060 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294951165 TSecr=810522427 WS=64
23.764777427	192.168.200.150	192.168.200.100	TCP	60	443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23.764815289	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
23.764899091	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165

AZIONE PER RIDURRE GLI IMPATTI DELL'ATTACCO

Il target Potrebbe utilizzare un firewall per bloccare le richieste in entrata da parte dell'indirizzo 192.168.200.100



COSA FARE

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



PREVENTIVO ESERCIZIO 3



PREVENTIVO BASATO SU ORE DI LAVORO

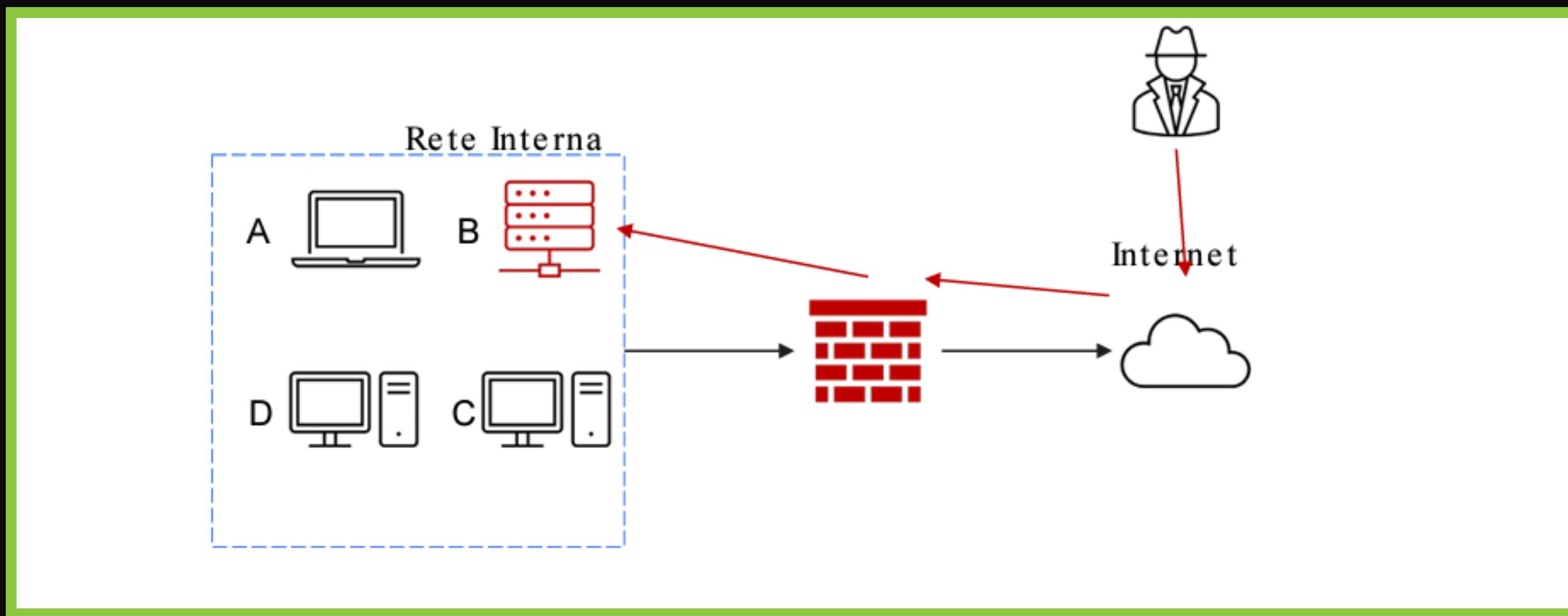
Dettagli del Lavoro:

1. Isolare sistema infetto
2. Rimuovere sistema infetto
3. Spiegare la differenza tra Purge e Destroy per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi.
4. Spiegare il clear

Totale Ore di Lavoro: 8 ore

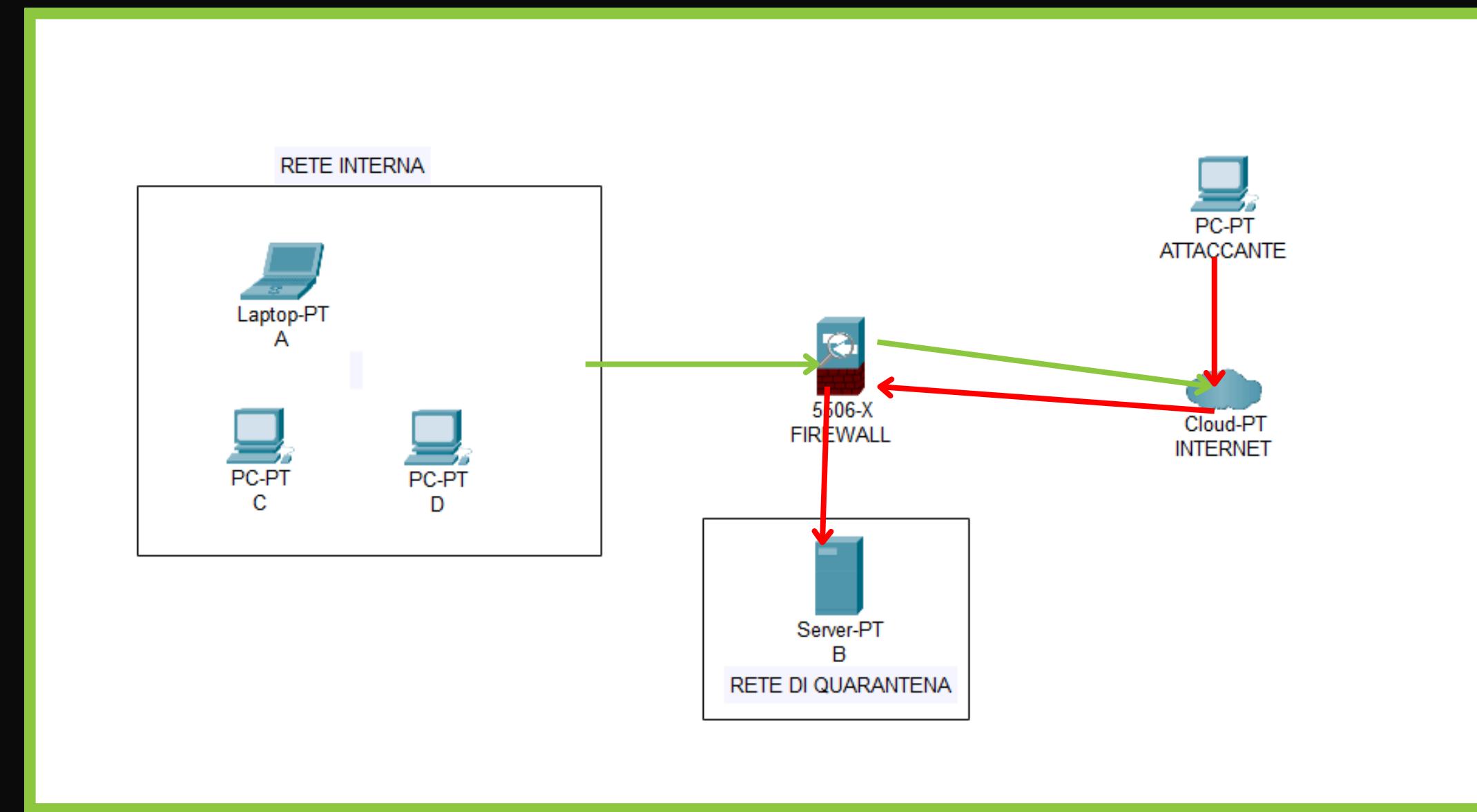
TOTALE PREVENTIVO: 1600,00 €

LA NOSTRA RETE



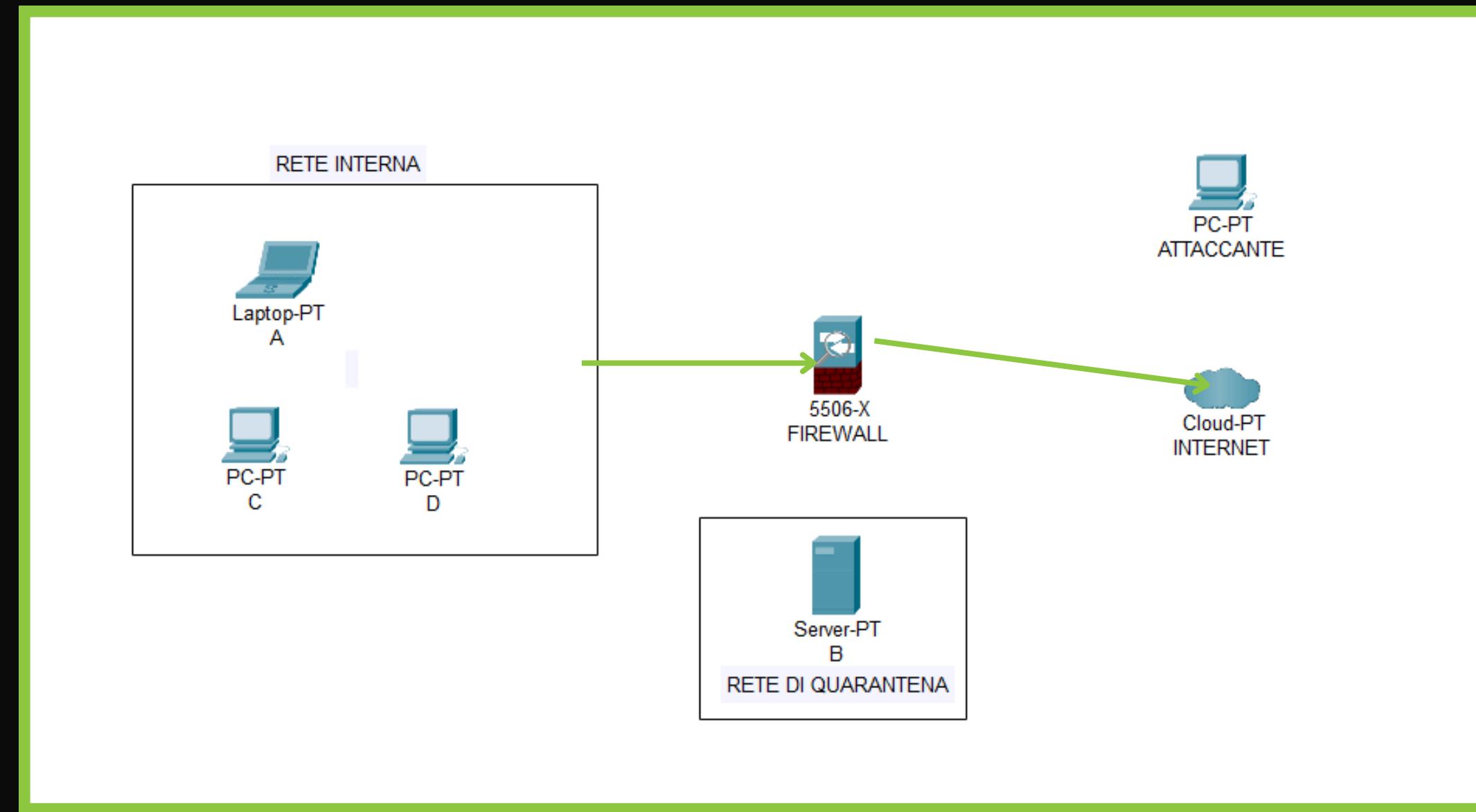
Come possiamo notare, il nostro database è stato attaccato e quindi dobbiamo andare ad isolarlo e poi rimuoverlo dalla rete.

ISOLAMENTO SISTEMA INFETTO



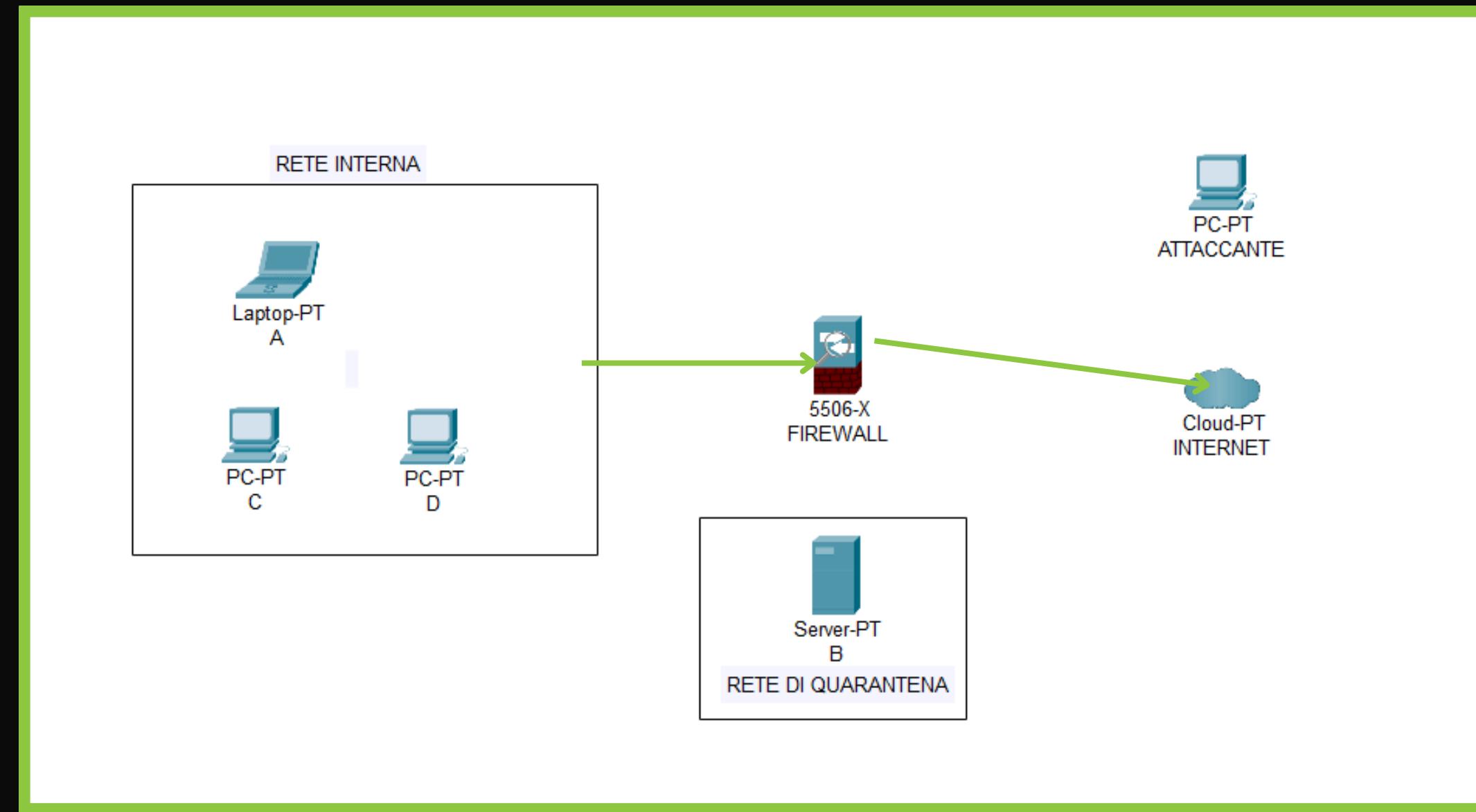
L'isolamento, è una tecnica che toglie il sistema infetto dalla rete interna quindi non gli ha più accesso; tuttavia l'attaccante tramite internet, può accedere al sistema infetto.

RIMOZIONE SISTEMA INFETTO



La rimozione, è una tecnica che elimina completamente il sistema infetto dalla rete rendendolo inaccessibile sia da internet che dalla rete interna; in questo modo, l'attaccante, non ha nemmeno più accesso al sistema infetto.

RIMOZIONE SISTEMA INFETTO



La rimozione, è una tecnica che elimina completamente il sistema infetto dalla rete rendendolo inaccessibile sia da internet che dalla rete interna; in questo modo, l'attaccante, non ha nemmeno più accesso al sistema infetto.

DIFFERENZA TRA PURGE E DESTROY

PURGE: si riferisce alla cancellazione sicura dei dati o all'eliminazione delle minacce da un sistema.

PURGING DEI DATI:

- Cancellazione Sicura: Eliminazione permanente dei dati in modo che non possano essere recuperati.
- Pulizia del Disco: Cancellazione completa di tutti i dati da un disco.
- Distruzione dei File: Suddivisione e sovrascrittura dei file con dati casuali per prevenire il recupero.

PURGING DELLE MINACCE:

- Rimozione del Malware: Rilevamento ed eliminazione del malware con software antivirus o anti-malware.
- Correzione delle Vulnerabilità: Aggiornamento del software per risolvere vulnerabilità sfruttabili dagli hacker.
- Pulizia dei Log: Analisi e rimozione dei log sospetti o malevoli.

MISURE PREVENTIVE:

- Backup Regolari: Mantenere backup regolari dei dati critici prima di effettuare il purging.
- Controlli di Accesso: Garantire che solo il personale autorizzato possa eseguire operazioni di purging.
- Tracciabilità: Conservare registri di tutte le attività di purging per responsabilità e riferimenti futuri.



DESTROY: si riferisce alla distruzione definitiva dei dati o delle minacce da un sistema.

DISTRUZIONE DEI DATI:

- Cancellazione Sicura: Eliminazione permanente dei dati in modo che non possano essere recuperati, utilizzando strumenti che sovrascrivono i dati più volte.
- Formattazione Completa: Cancellazione totale di tutti i dati da un disco utilizzando software specializzato per garantire che anche i frammenti di dati siano irrecuperabili.
- Distruzione Fisica: Distruzione fisica del supporto di memorizzazione, come dischi rigidi o SSD, tramite frantumazione o smagnetizzazione.

DISTRUZIONE DELLE MINACCE:

- Eliminazione del Malware: Rilevamento e rimozione completa del malware dal sistema utilizzando software antivirus o anti-malware.
- Correzione delle Vulnerabilità: Applicazione di patch e aggiornamenti software per risolvere vulnerabilità che potrebbero essere sfruttate dagli attaccanti.
- Pulizia dei Log: Rimozione dei log che contengono tracce di attività sospette o malevoli.

MISURE PREVENTIVE:

- Backup Regolari: Eseguire backup regolari dei dati critici prima della distruzione per prevenire la perdita accidentale di dati importanti.
- Controlli di Accesso: Garantire che solo il personale autorizzato possa eseguire operazioni di distruzione per prevenire usi impropri.
- Tracciabilità: Mantenere registri dettagliati di tutte le attività di distruzione per responsabilità e per futuri riferimenti.



CLEAR: si riferisce alla pulizia o alla cancellazione dei dati da un sistema.

PULIZIA DEI DATI:

- Cancellazione Standard: Eliminazione dei file utilizzando le normali funzioni del sistema operativo, con la possibilità che i dati siano recuperabili con strumenti specializzati.
- Cancellazione Sicura: Uso di strumenti per la cancellazione sicura che sovrascrivono i dati per impedirne il recupero.
- Svuotamento del Cestino: Eliminazione dei file spostati nel cestino del sistema operativo per liberar spazio su disco.

PULIZIA DELLE MINACCE:

- Rimozione del Malware: Scansione e pulizia del sistema per rimuovere malware, spyware e altri software dannosi.
- Aggiornamenti Software: Installazione di patch e aggiornamenti per correggere vulnerabilità e migliorare la sicurezza del sistema.
- Pulizia dei Log: Eliminazione dei log obsoleti o sospetti per mantenere il sistema pulito e monitorato.

MISURE PREVENTIVE:

- Backup Regolari: Mantenere backup regolari dei dati critici prima di effettuare il purging.
- Controlli di Accesso: Garantire che solo il personale autorizzato possa eseguire operazioni di purging.
- Tracciabilità: Conservare registri di tutte le attività di purging per responsabilità e riferimenti futuri.



INTRODUZIONE



Siamo stati incaricati di valutare e migliorare la sicurezza della loro applicazione web.

In risposta a questa richiesta, abbiamo condotto un'analisi dettagliata delle potenziali minacce e delle vulnerabilità dell'applicazione, identificando le azioni preventive e le strategie di risposta più efficaci per proteggere l'applicazione dagli attacchi e garantire la continuità operativa del business.

PREVENTIVO ESERCIZIO 5



PREVENTIVO BASATO SU ORE DI LAVORO

Dettagli del Lavoro:

1. Illustrare azioni preventive per la rete
2. Calcolare le perdite orarie
3. Implementare la rete del punto 1
4. Unire le due reti create

Totale Ore di Lavoro: 8 ore

TOTALE PREVENTIVO: 1600,00 €

SICUREZZA DELL'APPLICAZIONE WEB



PANORAMICA

Andremo a vedere una serie di misure di sicurezza proattive raccomandate per proteggere un'applicazione web da attacchi di tipo SQL Injection (SQLi) e Cross-Site Scripting (XSS) da parte di utenti malintenzionati.

Ogni misura è accompagnata da una spiegazione dettagliata del suo scopo e dell'importanza nella difesa dell'applicazione.

ANALISI DELLE MISURE DI SICUREZZA

Validazione dei dati in ingresso : verificare e validare tutti i dati in ingresso per garantire che siano conformi ai formati attesi e sicuri.

- Scopo : La validazione dei dati in ingresso è essenziale per garantire che solo i dati conformi e sicuri vengano accettati dall'applicazione.
- Importanza : Evitare l'iniezione di dati dannosi o non validi che potrebbero essere utilizzati per compromettere il sistema o accedere a informazioni sensibili.

Parametrizzazione delle Query SQL : Utilizzare parametri nelle query SQL invece di concatenare direttamente valori input utente nelle stringhe di query.

- Scopo : Utilizzare parametri nelle query SQL riduce il rischio di SQL Injection, in quanto impedisce agli attaccanti di inserire comandi SQL dannosi tramite input utente.
- Importanza : protegge l'integrità dei dati nel database e previene potenziali violazioni della sicurezza attraverso query malevoli.

Escape dei Dati : Fare l'escape dei dati prima del rendering sul lato client per prevenire attacchi XSS.

- Scopo : La fuga dei dati previene attacchi XSS convertendo caratteri speciali in entità HTML o JavaScript, impedendo l'esecuzione di codice dannoso sul lato client.
- Importanza : protegge gli utenti dall'esposizione a script dannosi e preserva l'integrità e la sicurezza dei dati visualizzati nell'interfaccia utente.

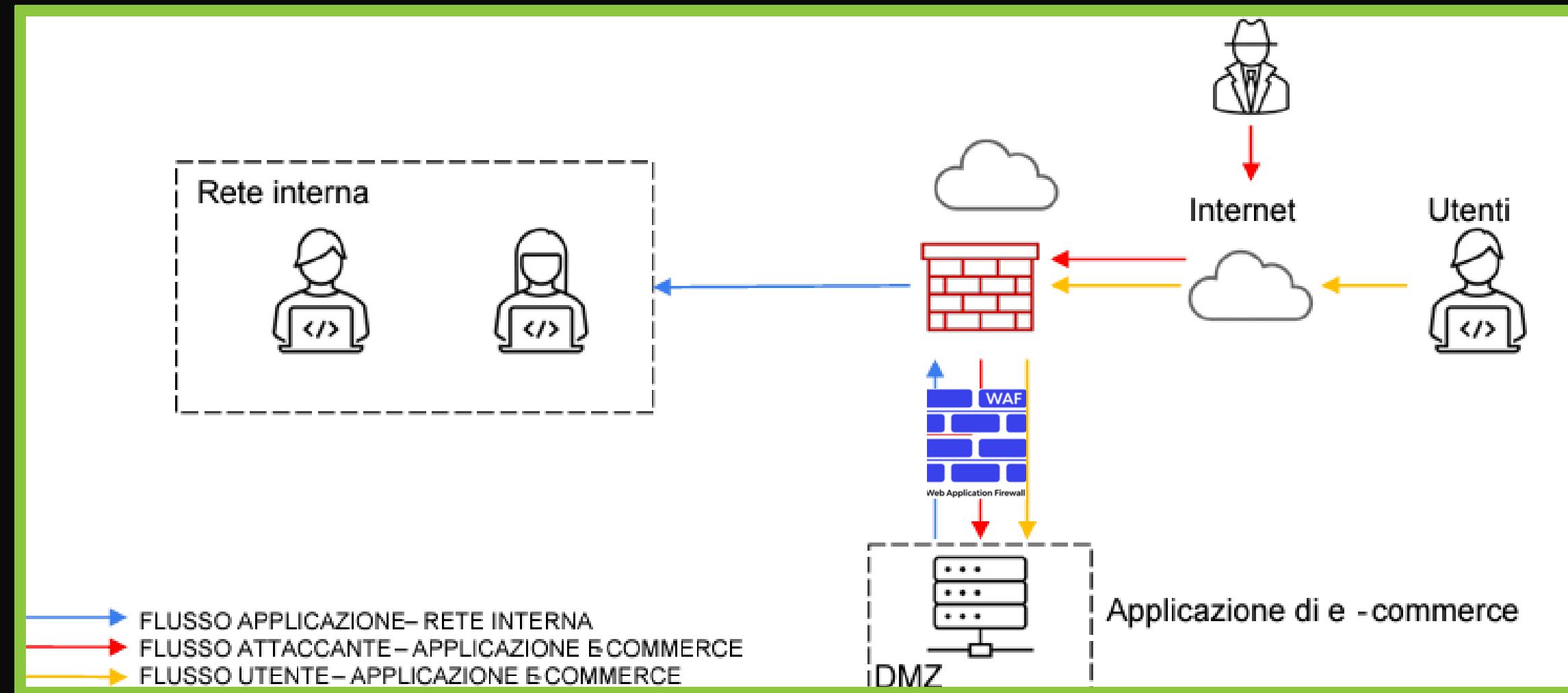
Sistema di gestione degli accessi : implementare un robusto sistema di gestione degli accessi per regolare l'accesso alle risorse dell'applicazione.

- Scopo : Regola l'accesso alle risorse dell'applicazione per garantire che gli utenti possano accedere solo alle risorse per cui hanno il permesso.
- Importanza : Limita il rischio di accessi non autorizzati e protegge i dati sensibili da accessi indesiderati.

Aggiornamento del software

- Scopo : mantenere aggiornati il software dell'applicazione e le librerie di terze parti per ridurre la probabilità di sfruttamento delle minacce note.
- Importanza : Riduce l'esposizione alle minacce della sicurezza e garantisce che l'applicazione rimanga protetta dalle ultime minacce informatiche.

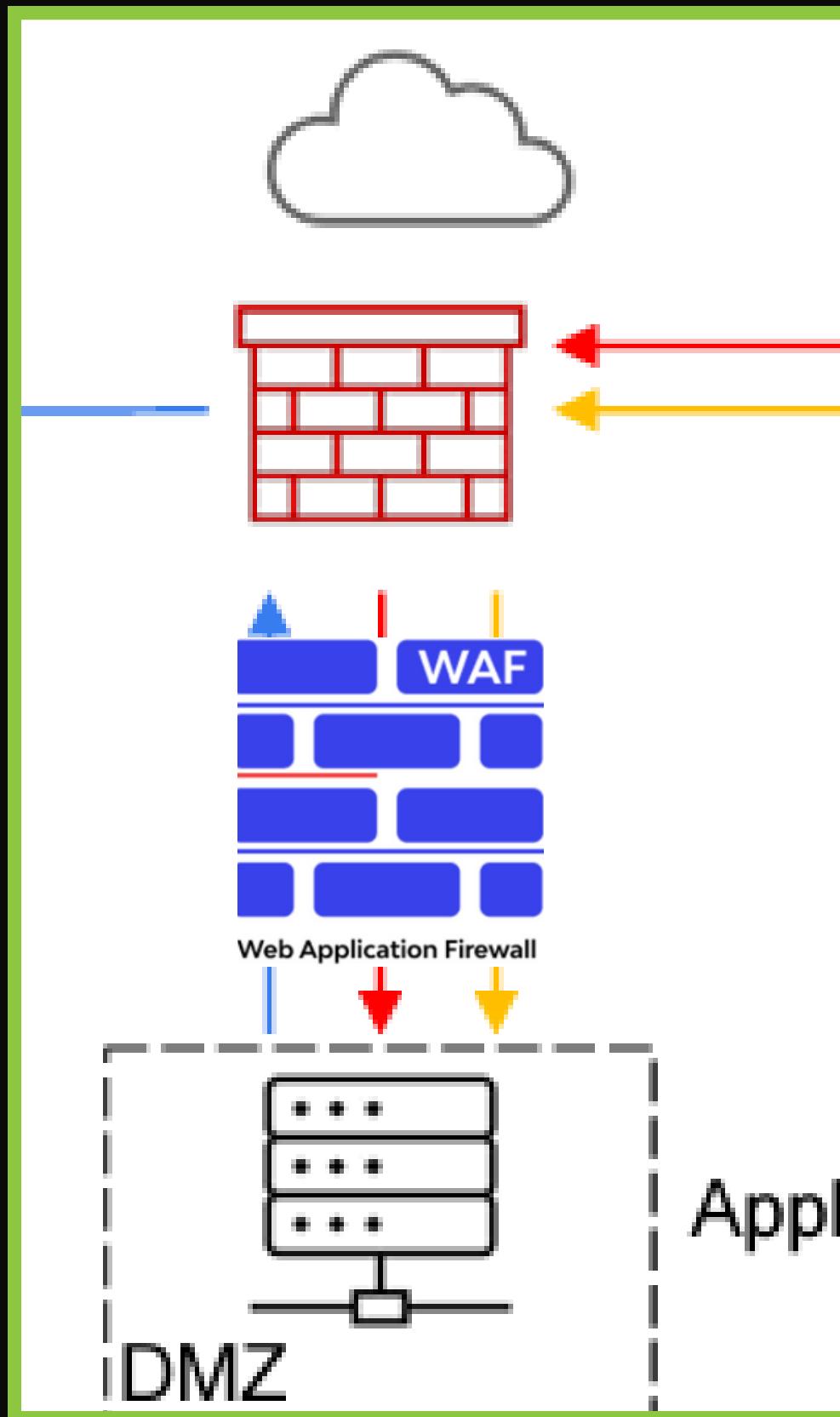
FIREWALL DELLE APPLICAZIONI WEB (WAF)



Implementare un WAF per filtrare e monitorare il traffico HTTP in ingresso e in uscita, rilevando e bloccando potenziali attacchi.

- **Scopo :** Un WAF filtra e monitora il traffico HTTP/HTTPS in ingresso e in uscita, identificando e bloccando attacchi noti e sospetti.
- **Importanza :** Aggiunge uno strato di difesa aggiuntiva all'applicazione, rilevando e bloccando attivamente le minacce prima che raggiungano il server web.

REGOLE DI FILTRAGGIO PER IL WAF



- Filtraggio per SQL Injection (SQLi) : Bloccare le richieste contenenti parole chiave SQL, caratteri speciali SQL e parametri SQL concatenati direttamente nelle stringhe di query.
- Filtraggio per Cross-Site Scripting (XSS) : Bloccare le richieste contenenti script JavaScript, attributi HTML e caratteri speciali HTML.
- Filtraggio Generale : Bloccare le richieste per risorse non autorizzate, tentativi di esecuzione di comandi di sistema e richieste di file locali.
- Validazione dei Formati dei Dati : Bloccare le richieste contenenti dati non validi o in formati non attesi.
- Monitoraggio del traffico anomalo : monitorare e bloccare le richieste con tasso elevato di richieste al secondo e provenienti da IP sospetti.

CONCLUSIONI



L'implementazione di queste misure di sicurezza consente di mitigare in modo significativo i rischi di attacchi di tipo SQL Injection e Cross-Site Scripting contro l'applicazione web.

È fondamentale adottare, controlli tecnici con buone pratiche di sviluppo e gestione dei sistemi per garantire una protezione efficace contro le minacce informatiche.

ATTACCO DDOS

L'attacco Ddos causa il crush della web app per 10 minuti e, se potenzialmente in un minuto si racano 1.500€, in 10 minuti, l'azienda, ha perso 15.000€.

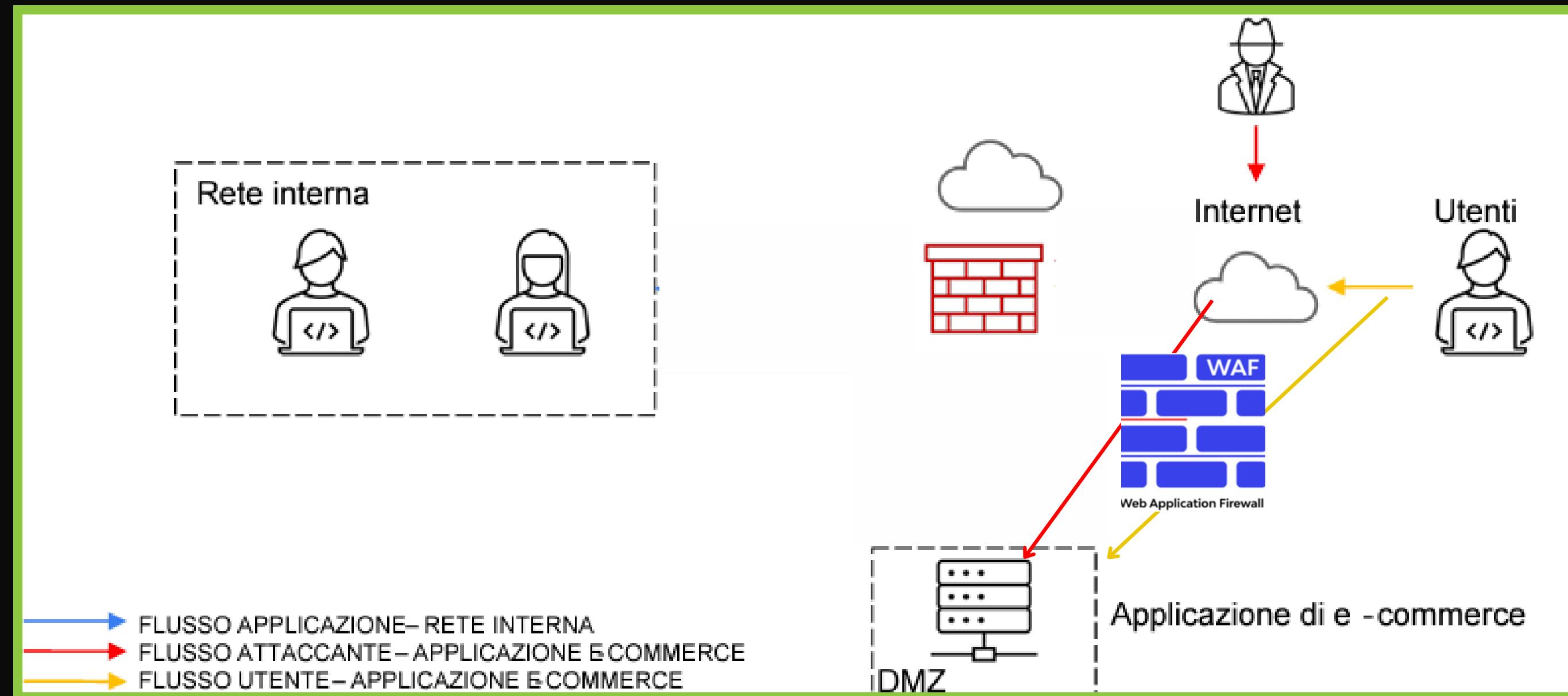
Il risultato si ottiene moltiplicando il tempo per le perdite al minuto; quindi:
Impatto sul business=1500€*10minuti= 15.000€.

Azioni Preventive:

1. Implementare un CDN (Content Delivery Network): Distribuisce il traffico su più server, riducendo l'impatto di un attacco DDoS.
2. Utilizzare un WAF (Web Application Firewall): Filtra il traffico dannoso prima che raggiunga i server.
3. Ridondanza e Bilanciamento del Carico: Distribuire il carico su server multipli per evitare punti singoli di fallimento.
4. Monitoraggio Continuo: Utilizzare strumenti di monitoraggio per rilevare e rispondere rapidamente agli attacchi.



In questo modo, avendo isolato l'applicazione di e-commerce, tutti avranno accesso all'applicazione ma l'attaccante non potrà accedere all'interno della rete aziendale.



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:

<https://app.any.run/tasks/8e6ad6d9-4d54-48e8-ad95-bfb67d47fd7/>

Il file "**PERFORMANCE BOOSTER_v3.6.exe**" è stato identificato come malevolo. L'analisi ha rivelato comportamenti tipici di un attacco Trojan.

Attività Sospette:

1. Modifica della politica di esecuzione di PowerShell: Il file ha modificato la politica di esecuzione di PowerShell senza restrizioni. Questa azione consente l'esecuzione dello script PowerShell senza controllo di sicurezza.
2. Avvio di cmd.exe: Il file ha avviato il prompt dei comandi di Windows (cmd.exe) per eseguire comandi e interagire con il sistema.
3. Utilizzo di PowerShell per operare con account locali: Il file ha utilizzato PowerShell per interagire con gli account utente locali del sistema, potenzialmente per ottenere privilegi elevati o accedere a risorse sensibili.
4. Esecuzione di comandi da un file ".bat": Il file ha eseguito comandi da un file batch (.bat), il che potrebbe indicare attività automatizzate o l'esecuzione di procedure specifiche.
5. Verifica dell'Installazione di .NET: È stata verificata la presenza di .NET Framework sul sistema, il che potrebbe essere utilizzato per determinare la compatibilità o identificare vulnerabilità specifiche.

Prevenzione:

1. Educazione degli Utenti: Formare gli utenti a riconoscere software e link sospetti.
2. Software di Sicurezza: Implementare antivirus e anti-malware aggiornati.
3. Monitoraggio della Rete: Monitorare il traffico di rete per rilevare attività insolite.

[https://app.any.run/tasks/60b9570f-175b-4b03-816b-a38cc2b0255e /](https://app.any.run/tasks/60b9570f-175b-4b03-816b-a38cc2b0255e/)

I file è stato identificato come malevolo. L'analisi evidenzia comportamenti tipici di un Trojan.

Attività Sospette:

- Connessioni di Rete: Il file tenta di connettersi a server remoti, suggerendo esfiltrazione di dati.
- Modifiche al Sistema: Effettua cambiamenti ai file di sistema e al registro di Windows.
- Download di Componenti Aggiuntivi: Scarica ulteriori componenti malevoli.

Azioni Rilevate:

- Scrittura su file di sistema.indica che il software sta modificando o creando nuovi file all'interno del sistema operativo. Le modifiche ai file di sistema possono avere diverse finalità, che vanno dalla registrazione di dati di configurazione o di log, all'infezione del sistema con malware o alla sostituzione di file esistenti con versione
- Modifiche al registro.possono compromettere il funzionamento del sistema e dei programmi installati. Le azioni come l'aggiunta, la modifica o l'eliminazione di chiavi o valori di registrazione possono essere utilizzate per installare o configurare software, ma anche per scopi maligni come l'avvio automatico di programmi dannosi.
- Tentativi di connessione a IP sospetti, indica che il software sta tentando di stabilire una connessione a indirizzi IP che sono considerati sospetti o non attendibili

Prevenzione:

- Educazione e Formazione: Formare gli utenti a riconoscere link e file sospetti.
- Software di Sicurezza: Implementare e mantenere aggiornati antivirus e anti-malware.
- Aggiornamenti di Sistema: Assicurarsi che tutti i sistemi e software siano aggiornati.
- Monitoraggio della Rete: Monitorare attivamente il traffico di rete per rilevare attività sospette.