



EVILGUARD
SOLUTIONS

Chi siamo

Benvenuti in **EvilGuard Solutions**, la vostra difesa impenetrabile contro le minacce cibernetiche.

Sebbene siamo un'azienda nata da poco, il nostro team è composto da esperti di cybersecurity con anni di esperienza nel settore. La nostra missione è semplice: proteggere le vostre informazioni più preziose da ogni tipo di attacco cibernetico.

Cosa facciamo

EvilGuard Solutions offre una gamma completa di servizi di cybersecurity progettati per proteggere aziende di varie dimensioni:

- Monitoraggio e Rilevamento delle Minacce: Utilizziamo tecnologie avanzate per monitorare costantemente le vostre reti e rilevare attività sospette in tempo reale.
- Protezione dei Dati: Implementiamo soluzioni di crittografia e backup per garantire che i vostri dati siano sempre al sicuro.
- Risposta agli Incidenti: Il nostro team è pronto a intervenire rapidamente in caso di violazioni, minimizzando i danni e ripristinando la sicurezza.
- Consulenza e Formazione: Offriamo consulenze personalizzate e programmi di formazione per educare il vostro personale sulle migliori pratiche di sicurezza.

PERCHÉ SIAMO LA SCELTA MIGLIORE

- Esperienza e Competenza: Anche se siamo una nuova realtà, i nostri specialisti di cybersecurity hanno lavorato su progetti complessi e con aziende di rilevanza globale.
- Tecnologia All'Avanguardia: Utilizziamo le tecnologie più recenti e avanzate per offrire soluzioni efficaci e innovative.
- Approccio Personalizzato: Ogni azienda è unica, e noi adattiamo le nostre soluzioni alle specifiche esigenze di ciascun cliente.
- Affidabilità: La vostra sicurezza è la nostra priorità assoluta. Siamo disposti a fornire un servizio su cui potete contare, 24 ore su 24, 7 giorni su 7.

I Vantaggi di SCEGLIERCI

- Protezione Costante: Con **EvilGuard Solutions**, avrete la tranquillità di sapere che le vostre informazioni sono protette da professionisti.
- Risparmio di Tempo e Risorse: Affidandovi a noi, potrete concentrarvi sul vostro business senza preoccuparvi delle minacce cibernetiche.
- Reattività: La nostra capacità di rispondere rapidamente agli incidenti riduce al minimo l'impatto delle violazioni sulla vostra attività.
- Formazione Continua: Mantenere il vostro team aggiornato sulle ultime tendenze e minacce di cybersecurity vi aiuterà a prevenire incidenti futuri.

Contattaci

EvilGuard Solutions è qui per offrirvi la protezione e la tranquillità di cui avete bisogno nel mondo digitale di oggi. Contattateci per scoprire come possiamo aiutare la vostra azienda a rimanere sicura e protetta. Per maggiori informazioni sui nostri servizi, non esitate a contattarci:

- *Telefono: +39 0123 456 789*
- *E-mail: info@evilguard.com*
- *Sito Web: www.evilguard.com*
- *Indirizzo: Via della Sicurezza, 123, 00100 Roma, Italia*

Traccia 1

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.

Requisiti: Configurate l'indirizzo di Windows XP come di seguito: 192.168.240.150

Configurate l'indirizzo della macchina Kali come di seguito: 192.168.240.100

Configurazione indirizzi IP

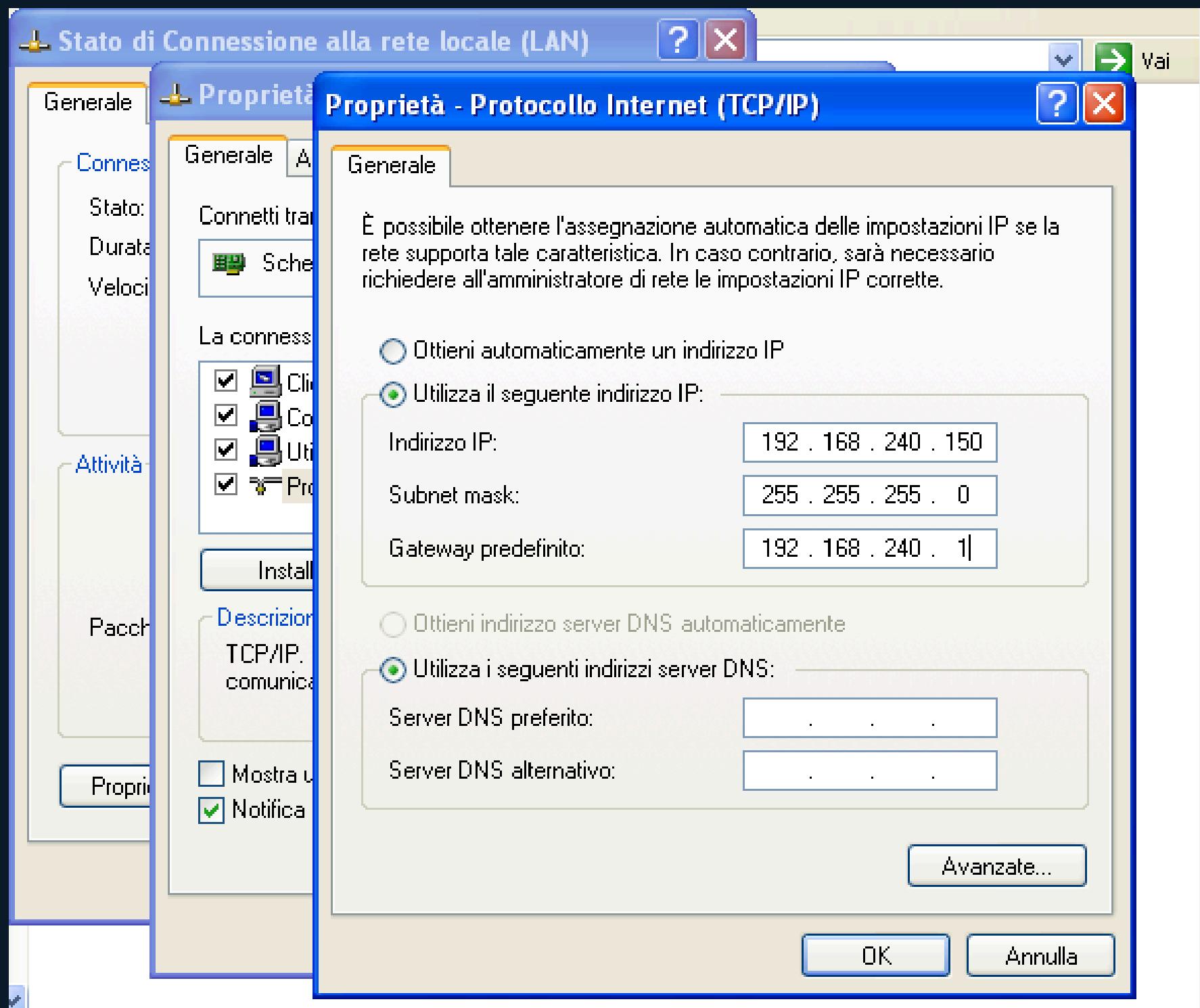
```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

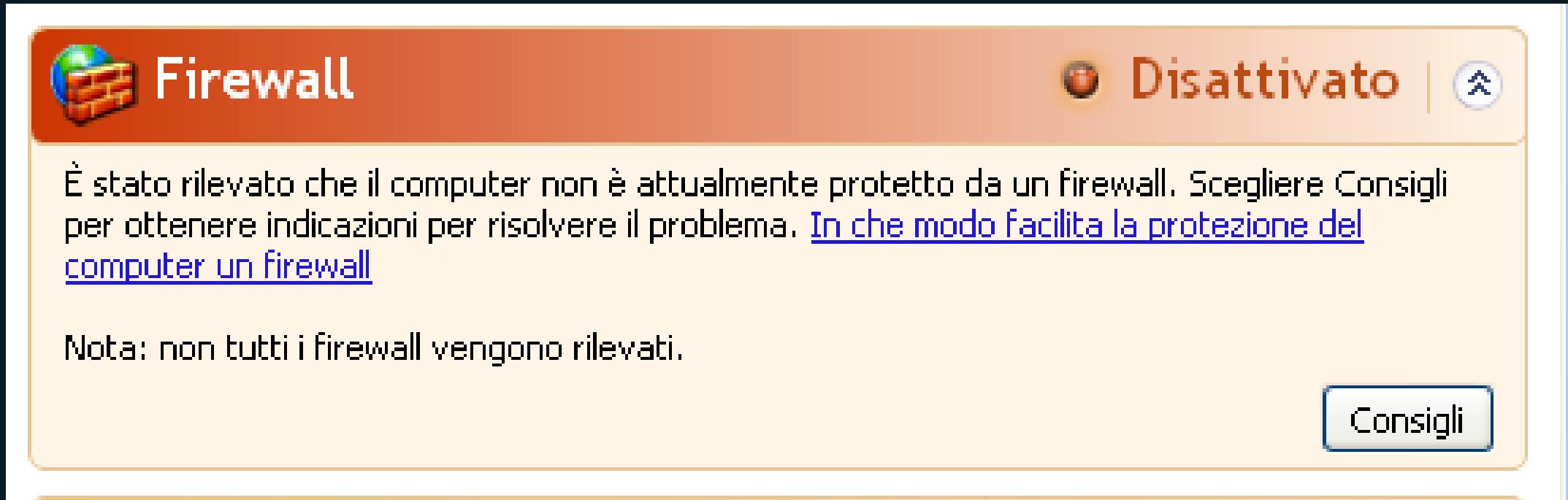
# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.240.100/24
gateway 192.168.240.1
```

Partiamo con la configurazione degli indirizzi IP sia su Kali sia su Windows XP, come richiesto



Scansione con firewall disattivato



Assicuriamoci che il firewall su Windows sia disattivato per andare ad effettuare la prima scansione.

Scansione con firewall disattivato

```
Nmap scan report for 192.168.240.150
Host is up (0.097s 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 7.99 seconds
```

Lanciamo la scansione attraverso il comando '`nmap -sV 192.168.240.150`' che come possiamo vedere va a controllare 1000 porte trovandone 3 aperte. Le porte in questione sono:

Porta 135 (MSRPC): Utilizzata per Microsoft RPC (Remote Procedure Call), un protocollo che permette ai programmi di eseguire procedure su altri computer in rete.

Porta 139 (NetBIOS-SSN): Utilizzata per sessioni di NetBIOS su TCP/IP. Facilita la condivisione di file e stampanti in reti locali.

Porta 445 (Microsoft-DS): Utilizzata per il servizio di condivisione file di Windows (SMB, Server Message Block) su TCP/IP, permette la condivisione di risorse come file e stampanti tra computer in rete.

Scansione con firewall attivo



A questo punto attiviamo il firewall e avviamo una nuova scansione.

Scansione con firewall attivo

```
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 3.27 seconds
```

Effettuando una nuova scansione, sempre utilizzando il comando '*nmap -sV 192.168.240.150*' possiamo notare che il firewall attivo avrà bloccato le richieste ping utilizzate da nmap per determinare se l'host è attivo. La scansione infatti, mostra che nmap non ha ricevuto risposte dai ping inviati, portandolo a concludere che l'host è "down". Come suggerito aggiungiamo il comando *-Pn* che dirà a nmap di evitare il ping e tentare direttamente la scansione delle porte.

Scansione con firewall attivo

```
Nmap scan report for 192.168.240.150
Host is up.
All 1000 scanned ports on 192.168.240.150 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 201.68 seconds
```

Utilizzando dunque il comando '*nmap -sV -Pn 192.168.240.150*', otterremo l'output nell'immagine. Osserviamo che l'host risulta attivo, ma tutte le 1000 porte scansionate sono in stato filtrato. Questo significa che il firewall sull'host sta bloccando le risposte alle richieste di scansione delle porte di nmap. Di conseguenza, nmap non riceve risposta dalle porte, interpretando questo comportamento come "filtered" (filtrato). Da questo risultato, concludiamo perciò che non sarà possibile determinare quali servizi siano attivi sull'host a causa del blocco del firewall.

Traccia 2

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 a pag.18, 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»
 - Terremoto sull'asset «edificio primario»

BUSINESS CONTINUITY & DISASTER RECOVERY

Il BCP (Business Continuity Plan) descrive le politiche e le procedure per minimizzare gli impatti negativi sugli affari di una compagnia a seguito di eventi catastrofici, garantendo la continuità operativa. Le fasi principali del BCP includono:

1) Pianificazione e Scopo

- Analisi Strutturata: Mappatura dei dipartimenti e dei servizi critici.
- Creazione del Team BCP: Include rappresentanti di dipartimenti critici, esperti IT, sicurezza fisica, legale, risorse umane e un dirigente con potere decisionale.
- Valutazione delle Risorse: Definizione delle risorse necessarie per lo sviluppo, test, manutenzione e implementazione del BCP.
- Un'analisi delle leggi e regolamentazioni che la compagnia deve rispettare.

BUSINESS CONTINUITY & DISASTER RECOVERY

2) Business Impact Analysis (BIA)

- Identificazione delle Priorità: Valutazione qualitativa e quantitativa degli asset critici.
- Valutazione dei Rischi: Identificazione dei rischi naturali e causati dall'uomo.
- Valutazione delle Probabilità e Impatti: Utilizzo di ARO (Annualized Rate of Occurrence) e SLE (Single Loss Expectancy) per quantificare le perdite attese.

3) Business Continuity Planning

- Sviluppo della Strategia: Decisione sui rischi da gestire e mitigare.
- Stesura dei Processi: Dettaglio delle procedure per la salvaguardia degli asset critici e del personale.

BUSINESS CONTINUITY & DISASTER RECOVERY

4) Approvazione e Implementazione

- Revisione e Approvazione: Revisione del piano da parte della dirigenza.
- Implementazione del Piano: Training e test per assicurare l'efficacia del BCP.

Il BCP ha quindi come obiettivo quello di ridurre gli impatti negativi sui servizi principali della compagnia e garantire la continuità delle operazioni anche in situazioni di emergenza, mantenendo l'operatività e minimizzando le perdite.

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% |

BUSINESS Continuity & Disaster RECOVERY

Utilizzando i dati delle tabelle, esaminiamo gli eventi e gli impatti sulla compagnia in ordine partendo dal primo e procedendo allo stesso modo per tutti gli altri.

Inondazione sull'Asset «Edificio Secondario»

Per calcolare il danno monetario ogni volta che si verifica l'evento, utilizziamo la formula SLE:

$$SLE = AV \times EF$$

AV: Asset Value (150.000 € per l'edificio secondario)

EF: Exposure Factor (40% per inondazione sull'edificio secondario)

$$SLE = 150.000 \times 0,40 = 60.000 \text{ €}$$

Ogni volta che si verifica un'inondazione, l'impatto è di 60.000 €.

Per la perdita annuale, moltiplichiamo SLE per ARO (1 volta ogni 50 anni = 0,02):

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

L'impatto annuale sarà di 1.200 €.

BUSINESS CONTINUITY & DISASTER RECOVERY

Terremoto sull'Asset «Datacenter»

AV: 100.000 €

EF: 95%

ARO: 1/30 = 0,03

SLE = $100.000 \times 0,95 = 95.000 \text{ €}$

ALE = $95.000 \times 0,0333 = 2.850 \text{ €/anno}$

Incendio sull'Asset «Edificio Primario»

AV: 350.000 €

EF: 60%

ARO: 1/20 = 0,05

SLE = $350.000 \times 0,60 = 210.000 \text{ €}$

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

Incendio sull'Asset «Edificio Secondario»

AV: 150.000 €

EF: 50%

ARO: 1/20 = 0,05

SLE = $150.000 \times 0,50 = 75.000 \text{ €}$

ALE = $75.000 \times 0,05 = 3.750 \text{ €/anno}$

BUSINESS CONTINUITY & DISASTER RECOVERY

Inondazione sull'Asset «Edificio Primario»

AV: 350.000 €

EF: 55%

ARO: $1/50 = 0.02$

SLE = $350.000 \times 0,55 = 192.500 \text{ €}$

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

Terremoto sull'Asset «Edificio Primario»

AV: 350.000 €

EF: 80%

ARO: $1/30 = 0.03$

SLE = $350.000 \times 0,80 = 280.000 \text{ €}$

ALE = $280.000 \times 0,03 = 8400 \text{ €/anno}$

BUSINESS CONTINUITY & DISASTER RECOVERY

Il DRP (Disaster Recovery Plan) è il complemento tecnico al BCP e si concentra sui controlli tecnici per ridurre i rischi e recuperare i servizi dopo un evento catastrofico, fornendo una guida completa per le emergenze. Il DRP include vari documenti e strategie per garantire la resilienza e la continuità operativa.

Documenti Essenziali:

Executive Summary: Documento di sintesi per il management.

Documento Tecnico: Dettagli tecnici per il personale IT.

Piano d'Azione: Istruzioni per tutti i partecipanti al DRP.

Copia Completa del DRP: Per i responsabili principali.

BUSINESS CONTINUITY & DISASTER RECOVERY

Tecniche e Controlli:

Resilienza dei Sistemi: Miglioramento della disponibilità eliminando i single points of failure (SPOF).

Tolleranza agli Errori: Utilizzo di componenti ridondanti per garantire operatività nonostante guasti.

Protezione dei Dischi: Configurazioni RAID per ridondanza e continuità di servizio.

RAID-1: Mirroring dei dati su due dischi.

RAID-5: Utilizzo di almeno tre dischi con parità per recupero dati in caso di guasto.

Failover Cluster: Gruppi di server sincronizzati per garantire continuità operativa anche in caso di guasti.

Disponibilità Elettrica: Generatorie UPS per garantire continuità elettrica.

BUSINESS CONTINUITY & DISASTER RECOVERY

Strategie di Backup:

Full Backup: Copia completa di dati e configurazioni.

Incremental Backup: Copia solo dei dati modificati dall'ultimo backup incrementale.

Differential Backup: Copia dei dati modificati dall'ultimo full backup.

Migrazione al Cloud:

Cold Site: Sito secondario con attrezzature di base, attivato solo in caso di disastro.

Hot Site: Sito secondario sempre attivo con dati aggiornati, costi elevati ma nessuna discontinuità.

Warm Site: Via di mezzo con hardware preconfigurato ma necessità di installazione software e sincronizzazione dati.

Virtualizzazione: Utilizzo di ambienti virtuali per replicare l'infrastruttura.

Disaster Recovery as a Service (DRaaS): Infrastruttura cloud attivata in caso di disastro, ottimizzazione dei costi.

Traccia 3

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.

| Io. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|-------------------|-------------------|----------|--------|--|
| 1 | 0.000000000 | 192.168.200.150 | 192.168.200.255 | BROWSER | 286 | Host Announcement METASPLITTABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Potential... |
| 2 | 23.764214995 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 53060 → 89 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 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=1 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=1 TSval=4294951165 TSecr=810522427 WS=64 |
| 5 | 23.764777427 | 192.168.200.150 | 192.168.200.100 | TCP | 68 | 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 → 89 [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 → 89 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165 |
| 8 | 28.761629461 | PcsCompu_fd:87:1e | PcsCompu_39:7d:fe | ARP | 60 | Who has 192.168.200.100? Tell 192.168.200.150 |
| 9 | 28.761644619 | PcsCompu_39:7d:fe | PcsCompu_fd:87:1e | ARP | 42 | 192.168.200.100 is at 08:00:27:39:7d:fe |
| 10 | 28.774852257 | PcsCompu_39:7d:fe | PcsCompu_fd:87:1e | ARP | 42 | Who has 192.168.200.150? Tell 192.168.200.100 |
| 11 | 28.775230099 | PcsCompu_fd:87:1e | PcsCompu_39:7d:fe | 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=1 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=1 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=1 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=1 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=1 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=1 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=1 TSval=810535438 TSecr=0 WS=128 |
| 19 | 36.774685595 | 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=1 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=1 TSval=4294952466 TSecr=810535437 WS=64 |
| 21 | 36.774685696 | 192.168.200.150 | 192.168.200.100 | TCP | 68 | 443 → 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 22 | 36.774685737 | 192.168.200.150 | 192.168.200.100 | TCP | 68 | 554 → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 23 | 36.774685776 | 192.168.200.150 | 192.168.200.100 | TCP | 68 | 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 | 36.775141184 | 192.168.200.150 | 192.168.200.100 | TCP | 68 | 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=1 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 | 36.775337890 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 59174 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 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=1 TSval=810535439 TSecr=0 WS=128 |
| 31 | 36.775524204 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 53062 → 89 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535439 TSecr=0 WS=128 |
| 32 | 36.775589806 | 192.168.200.150 | 192.168.200.100 | TCP | 68 | 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=1 TSval=4294952466 TSecr=810535439 WS=64 |
| 36 | 36.775797084 | 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=1 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 → 89 [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=810525439 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=810525439 TSecr=4294952466 |

Frame 1: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface eth1, id 0

```
0000  ff ff ff ff ff ff 08 00  27 fd 87 1e 08 00 45 00  ....E.
0010  81 10 00 00 48 00 40 11  26 f6 c0 a8 c8 96 c0 a8  ..@. &....
```

| Apply a display filter ... <Ctrl-/> | | | | | | |
|-------------------------------------|--------------|-----------------|-----------------|----------|--------|---|
| No. | Time | Source | Destination | Protocol | Length | Info |
| 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 |
| 42 | 36.776179338 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 50684 → 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535439 TSecr=0 WS=128 |
| 43 | 36.776233880 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 54220 → 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535439 TSecr=0 WS=128 |
| 44 | 36.776330610 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 34648 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128 |
| 45 | 36.776385694 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 33042 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128 |
| 46 | 36.776402500 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 49814 → 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128 |
| 47 | 36.776451284 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 199 → 50684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 48 | 36.776451357 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 995 → 54220 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 49 | 36.776478201 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 46990 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128 |
| 50 | 36.776496366 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 33206 → 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128 |
| 51 | 36.776512221 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 60632 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128 |
| 52 | 36.776568606 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 49654 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128 |
| 53 | 36.776671271 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128 |
| 54 | 36.776720715 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 54898 → 500 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128 |
| 55 | 36.776813123 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 587 → 34648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 56 | 36.776843423 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 51534 → 487 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128 |
| 57 | 36.776904828 | 192.168.200.150 | 192.168.200.100 | TCP | 74 | 445 → 33042 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535440 WS=64 |
| 58 | 36.776904922 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 256 → 49814 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 59 | 36.776904961 | 192.168.200.150 | 192.168.200.100 | TCP | 74 | 139 → 46990 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535440 WS=64 |
| 60 | 36.776905004 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 143 → 33206 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 61 | 36.776905043 | 192.168.200.150 | 192.168.200.100 | TCP | 74 | 25 → 60632 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535440 WS=64 |
| 62 | 36.776905082 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 110 → 49654 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 63 | 36.776905123 | 192.168.200.150 | 192.168.200.100 | TCP | 74 | 53 → 37282 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535440 WS=64 |
| 64 | 36.776905162 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 500 → 54898 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 65 | 36.776914772 | 192.168.200.100 | 192.168.200.150 | TCP | 66 | 33042 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466 |
| 66 | 36.776941020 | 192.168.200.100 | 192.168.200.150 | TCP | 66 | 46990 → 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466 |
| 67 | 36.776962320 | 192.168.200.100 | 192.168.200.150 | TCP | 66 | 60632 → 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466 |
| 68 | 36.776983878 | 192.168.200.100 | 192.168.200.150 | TCP | 66 | 37282 → 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466 |
| 69 | 36.777118481 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 487 → 51534 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 70 | 36.777143014 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 56990 → 707 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128 |
| 71 | 36.777186821 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 35638 → 436 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128 |
| 72 | 36.777302991 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 34120 → 98 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128 |
| 73 | 36.777337934 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 49780 → 78 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128 |
| 74 | 36.777430632 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 707 → 56990 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 75 | 36.777430741 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 436 → 35638 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 76 | 36.777473018 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 36138 → 580 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128 |
| 77 | 36.777522494 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 52428 → 962 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128 |
| 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 |

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|-----------------|-----------------|----------|--------|--|
| 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 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128 |
| 81 | 36.777680898 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 51506 → 435 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128 |
| 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 TSval=810535441 TSecr=4294952466 |
| 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 TSval=810535441 TSecr=4294952466 |
| 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 TSval=810535441 TSecr=4294952466 |
| 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 TSval=810535441 TSecr=4294952466 |
| 90 | 36.778179978 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 51450 → 148 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128 |
| 91 | 36.778200161 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 48448 → 806 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128 |
| 92 | 36.778307830 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 54566 → 221 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128 |
| 93 | 36.778385846 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 148 → 51450 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 94 | 36.778385948 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 806 → 48448 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 95 | 36.778449494 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 221 → 54566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 96 | 36.778482791 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 42420 → 1007 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128 |
| 97 | 36.778591226 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 34646 → 206 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128 |
| 98 | 36.778614095 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 54202 → 131 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128 |
| 99 | 36.778663064 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 1007 → 42420 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 100 | 36.778721080 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 206 → 34646 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 101 | 36.778759636 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 40318 → 392 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128 |
| 102 | 36.778781327 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 51276 → 677 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128 |
| 103 | 36.778826294 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 131 → 54202 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 104 | 36.778864493 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 39566 → 856 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128 |
| 105 | 36.778939327 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 392 → 40318 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 106 | 36.778939427 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 677 → 51276 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 107 | 36.778983153 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 47238 → 84 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128 |
| 108 | 36.779029210 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 856 → 39566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 109 | 36.779055243 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 56542 → 807 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128 |
| 110 | 36.779122299 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 84 → 47238 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 111 | 36.779145004 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 40138 → 948 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128 |
| 112 | 36.779252884 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 807 → 56542 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 113 | 36.779273781 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 43140 → 214 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128 |
| 114 | 36.779309462 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 46886 → 106 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128 |
| 115 | 36.779354564 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 948 → 40138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 116 | 36.779378630 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 50204 → 138 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128 |
| 117 | 36.779397023 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 51262 → 884 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128 |
| 118 | 36.779605648 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 214 → 43140 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |

| Apply a display filter ... <Ctrl-/> | | | | | | |
|-------------------------------------|--------------|-----------------|-----------------|----------|--------|--|
| No. | Time | Source | Destination | Protocol | Length | Info |
| 118 | 36.779605648 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 214 → 43140 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 119 | 36.779605750 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 106 → 46886 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 120 | 36.779605798 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 138 → 50204 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 121 | 36.779605843 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 884 → 51262 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 122 | 36.779637573 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 44244 → 699 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128 |
| 123 | 36.779776288 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 43630 → 703 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128 |
| 124 | 36.779856041 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 699 → 44244 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 125 | 36.779911109 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 55136 → 274 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128 |
| 126 | 36.779946174 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 40522 → 42 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128 |
| 127 | 36.780035851 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 703 → 43630 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 128 | 36.780121127 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 274 → 55136 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 129 | 36.780149473 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 57552 → 58 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128 |
| 130 | 36.780170333 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 40822 → 266 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128 |
| 131 | 36.780215176 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 42 → 40522 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 132 | 36.780301750 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 58 → 57552 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 133 | 36.780325837 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 37252 → 11 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128 |
| 134 | 36.780346429 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 40648 → 235 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128 |
| 135 | 36.780409818 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 36548 → 739 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128 |
| 136 | 36.780427899 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 38866 → 55 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128 |
| 137 | 36.780472830 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 52136 → 999 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128 |
| 138 | 36.780490897 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 38022 → 317 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128 |
| 139 | 36.780577880 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 266 → 40822 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 140 | 36.780577981 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 11 → 37252 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 141 | 36.780578026 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 235 → 40648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 142 | 36.780578074 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 739 → 36548 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 143 | 36.780578119 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 55 → 38866 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 144 | 36.780578158 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 999 → 52136 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 145 | 36.780578198 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 317 → 38022 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 146 | 36.780617671 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 49446 → 961 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128 |
| 147 | 36.780701625 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 51192 → 241 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128 |
| 148 | 36.780805705 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 961 → 49446 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 149 | 36.780824718 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 42642 → 293 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128 |
| 150 | 36.780889399 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 241 → 51192 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 151 | 36.780906540 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 41828 → 974 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128 |
| 152 | 36.780958307 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 49014 → 137 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128 |
| 153 | 36.781007559 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 293 → 42642 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 154 | 36.781116869 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 974 → 41828 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 155 | 36.781116971 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 137 → 49014 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 156 | 36.781138769 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 45464 → 223 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128 |
| 157 | 36.781159927 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 42700 → 1014 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128 |

| No. | Time | Source | Destination | Protocol | Length Info |
|-----|--------------|-----------------|-----------------|----------|--|
| 157 | 36.781159927 | 192.168.200.100 | 192.168.200.150 | TCP | 74 42700 → 1014 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128 |
| 158 | 36.781255484 | 192.168.200.150 | 192.168.200.100 | TCP | 60 223 → 45464 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 159 | 36.781255593 | 192.168.200.150 | 192.168.200.100 | TCP | 60 1014 → 42700 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 160 | 36.781321950 | 192.168.200.100 | 192.168.200.150 | TCP | 74 55360 → 918 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128 |
| 161 | 36.781356928 | 192.168.200.100 | 192.168.200.150 | TCP | 74 45648 → 512 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128 |
| 162 | 36.781420319 | 192.168.200.100 | 192.168.200.150 | TCP | 74 53246 → 354 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128 |
| 163 | 36.781487105 | 192.168.200.150 | 192.168.200.100 | TCP | 60 918 → 55360 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 164 | 36.781487210 | 192.168.200.150 | 192.168.200.100 | TCP | 74 512 → 45648 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535445 WS=64 |
| 165 | 36.781512468 | 192.168.200.100 | 192.168.200.150 | TCP | 66 45648 → 512 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535445 TSecr=4294952466 |
| 166 | 36.781621871 | 192.168.200.150 | 192.168.200.100 | TCP | 60 354 → 53246 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 167 | 36.781640161 | 192.168.200.100 | 192.168.200.150 | TCP | 74 55186 → 858 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128 |
| 168 | 36.781734418 | 192.168.200.100 | 192.168.200.150 | TCP | 74 35806 → 663 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128 |
| 169 | 36.781812691 | 192.168.200.150 | 192.168.200.100 | TCP | 60 858 → 55186 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 170 | 36.781989537 | 192.168.200.100 | 192.168.200.150 | TCP | 66 45648 → 512 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535445 TSecr=4294952466 |
| 171 | 36.782069902 | 192.168.200.150 | 192.168.200.100 | TCP | 60 663 → 35806 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 172 | 36.782120740 | 192.168.200.100 | 192.168.200.150 | TCP | 74 38210 → 681 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128 |
| 173 | 36.782140866 | 192.168.200.100 | 192.168.200.150 | TCP | 74 47098 → 561 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128 |
| 174 | 36.782215091 | 192.168.200.100 | 192.168.200.150 | TCP | 74 32950 → 570 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128 |
| 175 | 36.782248180 | 192.168.200.100 | 192.168.200.150 | TCP | 74 38396 → 371 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128 |
| 176 | 36.782390780 | 192.168.200.150 | 192.168.200.100 | TCP | 60 681 → 38210 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 177 | 36.782390884 | 192.168.200.150 | 192.168.200.100 | TCP | 60 561 → 47098 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 178 | 36.782390930 | 192.168.200.150 | 192.168.200.100 | TCP | 60 570 → 32950 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 179 | 36.782390978 | 192.168.200.150 | 192.168.200.100 | TCP | 60 371 → 38396 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 180 | 36.782422713 | 192.168.200.100 | 192.168.200.150 | TCP | 74 43862 → 966 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535446 TSecr=0 WS=128 |
| 181 | 36.782459407 | 192.168.200.100 | 192.168.200.150 | TCP | 74 42162 → 595 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535446 TSecr=0 WS=128 |
| 182 | 36.782534412 | 192.168.200.100 | 192.168.200.150 | TCP | 74 55234 → 838 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535446 TSecr=0 WS=128 |
| 183 | 36.782582077 | 192.168.200.100 | 192.168.200.150 | TCP | 74 33102 → 51 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535446 TSecr=0 WS=128 |
| 184 | 36.782690536 | 192.168.200.150 | 192.168.200.100 | TCP | 60 966 → 43862 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 185 | 36.782690655 | 192.168.200.150 | 192.168.200.100 | TCP | 60 595 → 42162 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 186 | 36.782690713 | 192.168.200.150 | 192.168.200.100 | TCP | 60 838 → 55234 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 187 | 36.782780538 | 192.168.200.100 | 192.168.200.150 | TCP | 74 59404 → 56 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535446 TSecr=0 WS=128 |
| 188 | 36.782854473 | 192.168.200.150 | 192.168.200.100 | TCP | 60 51 → 33102 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 189 | 36.782887993 | 192.168.200.100 | 192.168.200.150 | TCP | 74 41104 → 144 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535446 TSecr=0 WS=128 |
| 190 | 36.783020182 | 192.168.200.150 | 192.168.200.100 | TCP | 60 56 → 59404 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 191 | 36.783042408 | 192.168.200.100 | 192.168.200.150 | TCP | 74 42620 → 874 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535446 TSecr=0 WS=128 |
| 192 | 36.783084243 | 192.168.200.100 | 192.168.200.150 | TCP | 74 58110 → 920 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535446 TSecr=0 WS=128 |
| 193 | 36.783329650 | 192.168.200.150 | 192.168.200.100 | TCP | 60 144 → 41104 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 194 | 36.783329795 | 192.168.200.150 | 192.168.200.100 | TCP | 60 874 → 42620 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 195 | 36.783329836 | 192.168.200.150 | 192.168.200.100 | TCP | 60 920 → 58110 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 196 | 36.783391839 | 192.168.200.100 | 192.168.200.150 | TCP | 74 42696 → 964 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535447 TSecr=0 WS=128 |

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|-----------------|-----------------|----------|--------|---|
| 193 | 36.783329650 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 144 → 41104 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 194 | 36.783329795 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 874 → 42620 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 195 | 36.783329836 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 920 → 58110 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 196 | 36.783391839 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 42696 → 964 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535447 TSecr=0 WS=128 |
| 197 | 36.783426736 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 57372 → 333 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535447 TSecr=0 WS=128 |
| 198 | 36.783557923 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 964 → 42696 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 199 | 36.783557992 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 333 → 57372 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 200 | 36.785397588 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 52872 → 203 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535449 TSecr=0 WS=128 |
| 201 | 36.785443154 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 37880 → 880 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535449 TSecr=0 WS=128 |
| 202 | 36.785551331 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 50932 → 939 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535449 TSecr=0 WS=128 |
| 203 | 36.785624918 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 47472 → 743 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535449 TSecr=0 WS=128 |
| 204 | 36.785675017 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 203 → 52872 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 205 | 36.785675093 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 880 → 37880 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 206 | 36.785721042 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 41984 → 831 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535449 TSecr=0 WS=128 |
| 207 | 36.785738953 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 57854 → 122 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535449 TSecr=0 WS=128 |
| 208 | 36.785824656 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 939 → 50932 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 209 | 36.785824723 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 743 → 47472 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 210 | 36.785880968 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 57402 → 237 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535449 TSecr=0 WS=128 |
| 211 | 36.785943368 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 33718 → 359 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535449 TSecr=0 WS=128 |
| 212 | 36.786209855 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 831 → 41984 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 213 | 36.786209978 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 122 → 57854 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 214 | 36.786210019 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 237 → 57402 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 215 | 36.786210059 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 359 → 33718 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 216 | 36.786254145 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 35164 → 586 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535449 TSecr=0 WS=128 |
| 217 | 36.786292426 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 59734 → 129 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535450 TSecr=0 WS=128 |
| 218 | 36.786455822 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 586 → 35164 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 219 | 36.786455938 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 129 → 59734 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 220 | 36.786788804 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 45416 → 545 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535450 TSecr=0 WS=128 |
| 221 | 36.786815129 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 45154 → 400 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535450 TSecr=0 WS=128 |
| 222 | 36.786864504 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 38180 → 239 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535450 TSecr=0 WS=128 |
| 223 | 36.786899954 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 37952 → 520 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535450 TSecr=0 WS=128 |
| 224 | 36.787023089 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 545 → 45416 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 225 | 36.787023195 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 400 → 45154 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 226 | 36.787069390 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 43106 → 769 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535450 TSecr=0 WS=128 |
| 227 | 36.787191686 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 239 → 38180 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 228 | 36.787191781 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 520 → 37952 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 229 | 36.787229817 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 42460 → 489 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535450 TSecr=0 WS=128 |
| 230 | 36.787306501 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 769 → 43106 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 231 | 36.787346317 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 49988 → 19 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535451 TSecr=0 WS=128 |
| 232 | 36.787470054 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 44644 → 846 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535451 TSecr=0 WS=128 |

Frame 1: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface eth1, id 0

Cos'È il protocollo TCP?

Il Transmission Control Protocol (TCP) è un protocollo che viene utilizzato per trasmettere dati in modo affidabile tra due nodi in una rete, come un client e un server. Esso garantisce che i dati inviati vengano ricevuti correttamente e nell'ordine corretto. Il TCP è un protocollo orientato alla connessione. Prima di trasmettere i dati, stabilisce una connessione tra il mittente e il destinatario attraverso un processo noto come "three-way handshake".

Per comprendere meglio la situazione, è utile spiegare il processo noto come "three-way handshake":

SYN (Synchronize)

Il client invia un pacchetto SYN al server per iniziare una connessione.

SYN-ACK (Synchronize-Acknowledge)

Il server riceve il pacchetto SYN e risponde con un pacchetto SYN-ACK, indicando che ha ricevuto il pacchetto e che è pronto per iniziare la connessione.

ACK (Acknowledge)

Il client riceve il pacchetto SYN-ACK e risponde con un pacchetto ACK, completando la connessione.

RST (Reset)

Questi pacchetti vengono inviati dal server per interrompere una connessione quando il server non riconosce o non può gestire la richiesta del client. Un elevato numero di pacchetti RST indica che le porte richieste non sono disponibili o il server non è in grado di gestire le connessioni richieste.

Dalla cattura notiamo subito che c'è un numero elevato di richieste TCP su porte sempre diverse.

Questo indica una scansione in corso da parte dell'host 192.168.200.100 verso l'host target 192.168.200.150. La scansione delle porte, come quella rilevata nella cattura di rete, è una pratica comunemente utilizzata dagli attaccanti per identificare i punti deboli in una rete. Una volta identificati, possono sfruttare le vulnerabilità nei servizi per ottenere accesso non autorizzato o causare danni. La presenza di numerose richieste TCP (SYN) su porte diverse indica che l'attaccante sta tentando di mappare quali porte sono aperte sul target. Le risposte SYN+ACK dal target indicano che il three-way handshake è stato completato, confermando che la porta è aperta e pronta a stabilire una connessione. Questo fornisce all'attaccante una lista di porte aperte e potenziali servizi da sfruttare. Le risposte RST+ACK invece, indicano che la porta è chiusa e non disponibile per la connessione. Sebbene queste ultime risposte non forniscano un punto di ingresso, confermano all'attaccante che la scansione sta funzionando e quali porte non sono disponibili.

Riduzione dell'impatto

Implementando alcune misure di sicurezza, è possibile mitigare significativamente il rischio associato a queste attività:

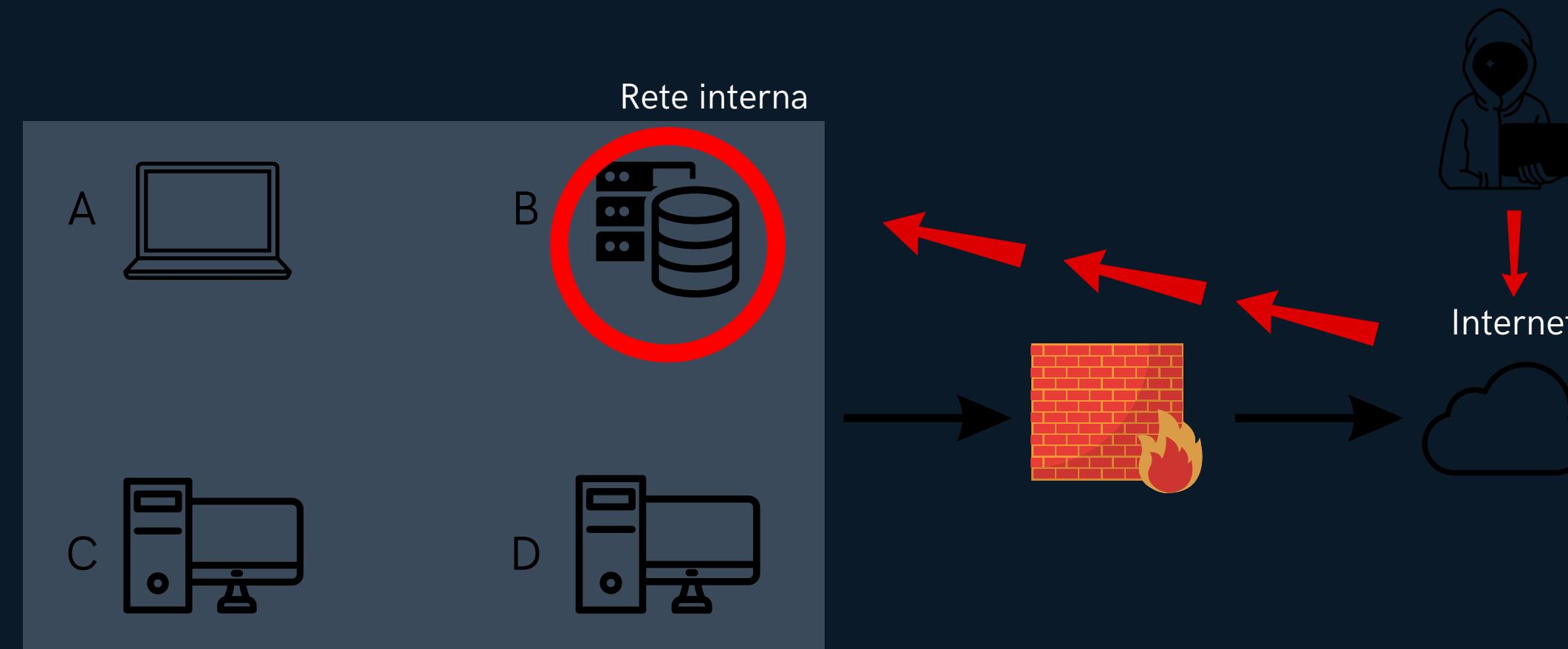
- 1) Chiudere Porte Non Necessarie: ogni servizio esposto su una porta aperta rappresenta un potenziale punto di ingresso per un attaccante. Chiudere le porte non necessarie riduce il numero di vie che un attaccante può utilizzare per tentare di compromettere il sistema. Es. Telnet e FTP.
- 2) Configurare il Firewall: possiamo bloccare l'accesso da indirizzi IP sospetti, come l'IP 192.168.200.100 identificato nella scansione.
- 3) Aggiornare Servizi e Patch: assicurandoci che tutti i servizi esposti siano aggiornati con le ultime patch di sicurezza andremo a ridurre la possibilità che vengano sfruttati.
- 4) Monitorare il Traffico di Rete: implementazione di un Sistema di Rilevamento delle Intrusioni (IDS), ovvero un dispositivo o software che monitora il traffico di rete o le attività di sistema per attività sospette e avvisa gli amministratori quando tali attività vengono rilevate.
- 5) Effettuare Valutazioni di Sicurezza Regolarmente: questo ci aiuterà a individuare le vulnerabilità prima che vengano sfruttate.

Traccia 4

Con riferimento alla figura in basso, 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.



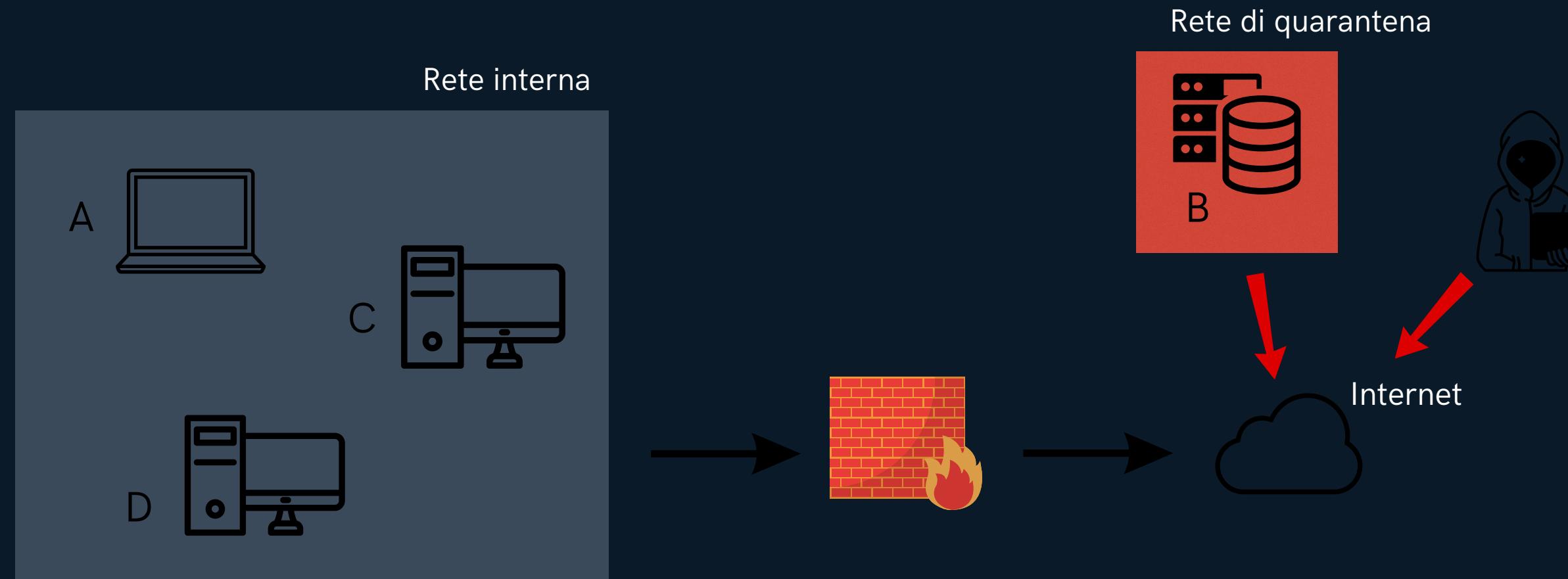
INCIDENT RESPONSE

Siamo nella fase di riduzione dell'impatto sull'incidente. Come abbiamo visto, il database B è stato interamente compromesso da un attaccante. Avremo bisogno quindi di applicare un piano di risposta all'incidente che varierà in base alla sua gravità. La prima strategia per contenere l'impatto consiste nell'***isolamento*** del sistema infetto (B) in modo che l'attaccante non possa accedere anche ai sistemi A, C e D. Possiamo farlo inserendolo in una rete isolata di quarantena in modo da restringere l'accesso alla rete interna da parte dell'attaccante, ma continuando a mantenere l'accesso a internet. Un altro piano di risposta all'incidente consiste nella ***rimozione*** del sistema dalla rete sia interna sia internet in modo che l'attaccante non possa mantenere neppure l'accesso al sistema infettato. Infine per lo smaltimento o il riutilizzo di un sistema compromesso possiamo sfruttare le tecniche '***Purge***', '***Destroy***' e '***Clear***'.

ISOLAMENTO

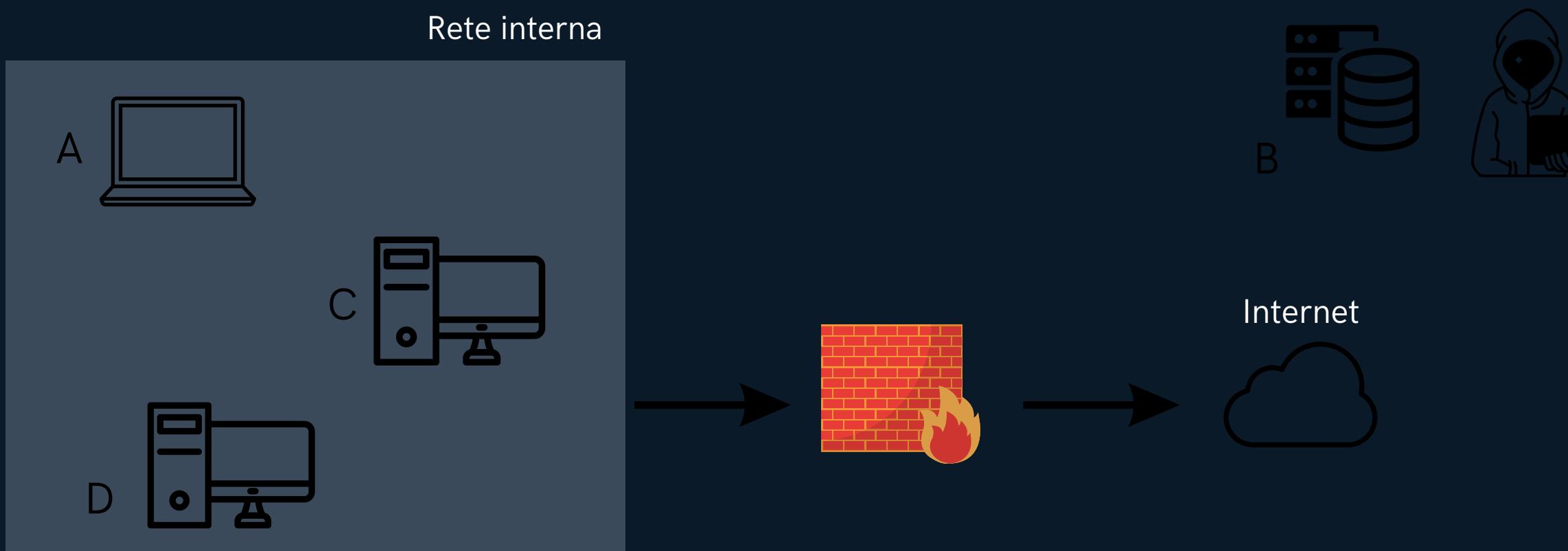
Come possiamo notare nell'immagine, siamo andati a isolare il sistema infetto B creando una rete di quarantena.

Essa impedirà all'attaccante di accedere alla rete interna, ma l'accesso a internet verrà conservato permettendogli quindi di mantenere l'accesso al sistema infetto.



RIMOZIONE

Come possiamo vedere, questa tecnica prevede la rimozione completa del sistema B compromesso per impedirne l'uso da parte dell'attaccante. In questo modo egli non avrà più accesso né alla rete interna né ad internet e quindi al sistema infetto stesso. Rappresenta ovviamente una soluzione più drastica poiché anche gli utenti legittimi perderanno eventualmente l'accesso al database.



FASE di RECUPERO

Dopo aver rimosso l'incidente dalla rete, ci dedichiamo alla fase di recupero dei dati, che ha anche come obiettivo quello di evitare un eventuale attacco identico in futuro. E' importante che i sistemi compromessi dall'attaccante vengano ripuliti prima del riutilizzo o perlomeno smaltiti. A questo scopo utilizziamo tre approcci per gestire i dispositivi che contengono informazioni sensibili: "Clear", "Purge" e "Destroy".

- **CLEAR**

Il metodo "Clear" utilizza tecniche logiche per rimuovere i dati presenti sul dispositivo. Questo approccio è principalmente software-based e mira a rendere i dati inaccessibili tramite strumenti di recupero standard. Queste tecniche sono la sovrascrittura in cui il contenuto del disco viene sovrascritto più volte con dati casuali o con un determinato schema di bit per garantire che i dati originali siano irreversibili, e il factory reset che restituisce il dispositivo allo stato di fabbrica. Questo metodo è rapido e relativamente economico e soprattutto adeguato per quei dispositivi che devono essere riutilizzati o rivenduti. Tuttavia non garantisce la totale irrecuperabilità dei dati contro attacchi avanzati e può non essere sufficiente nel caso in cui dati siano estremamente sensibili.



- PURGE

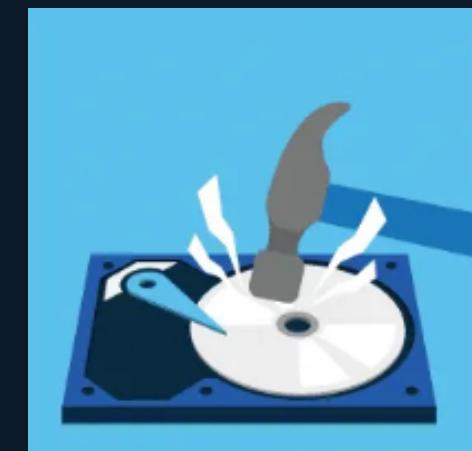
Il metodo "Purge" combina tecniche logiche di rimozione dei dati con tecniche fisiche per aumentare la sicurezza della cancellazione. Questo metodo è più robusto rispetto a "Clear" e mira a rendere i dati irrecuperabili anche con strumenti avanzati. Queste tecniche sono la sovrascrittura avanzata che in questo caso ha schemi di sovrascrittura più complessi e multipli passaggi, e il degaussing in cui si utilizzano forti magneti o campi magnetici per smagnetizzare il disco e cancellare tutte le informazioni registrate su supporti magnetici come hard disk tradizionali e nastri magnetici. Perciò, pur richiedendo attrezzature specializzate, questo metodo offre un livello di sicurezza superiore rispetto al precedente e rende i dati irrecuperabili anche con strumenti avanzati



- DESTROY

Il metodo "Destroy" è l'approccio più definitivo e sicuro per eliminare i dati da un dispositivo. Implica infatti la sua distruzione fisica per garantire che i dati non possano essere recuperati in alcun modo.

Questo metodo è spesso utilizzato per dati altamente sensibili o quando il dispositivo non deve essere riutilizzato. Si ricorre dunque a tecniche di laboratorio come l'incenerimento, la disintegrazione, la trapanazione o la frantumazione. Pur garantendo che i dati non possano essere recuperati in alcun modo, è perciò il metodo più costoso in termini di risorse e attrezzature.



Traccia 5

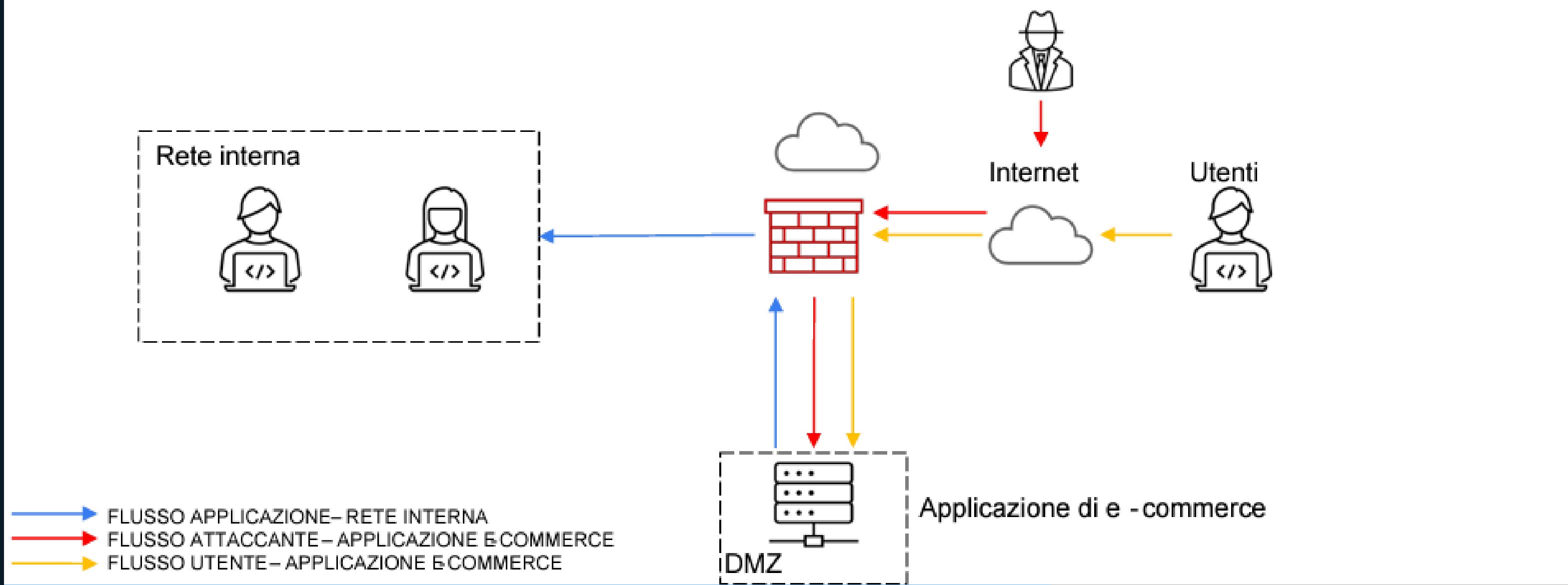
Con riferimento alla figura nella slide successiva, rispondere ai seguenti quesiti.

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 vostra 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 (se necessario/facoltativo magari integrando la soluzione al punto 2).

Architettura di rete:

L'applicazione di e - commerce deve essere disponibile per gli utenti tramite Internet per effettuare acquisti 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.



Azioni preventive

Per affrontare efficacemente gli incidenti di sicurezza, è essenziale adottare alcune misure preventive, ovvero tutte quelle azioni progettate per ridurre la probabilità che si verifichino questi eventi. Attacchi di tipo SQLi o XSS sono molto comuni nell'ambito delle applicazioni web.

- SQL INJECTION

SQL Injection è una tecnica di attacco che sfrutta le vulnerabilità nei campi di input delle applicazioni web per iniettare comandi SQL malevoli all'interno delle query inviate al database. Questo permette agli attaccanti di manipolare le query SQL originali e accedere, modificare o cancellare i dati presenti nel database. Nell' SQL Injection classica, la manipolazione di query SQL è diretta, tramite input non validato. Nell' SQL Injection di tipo Blind, l'attacco è più sofisticato poiché l'attaccante non riceve un feedback diretto dall'applicazione, ma deduce la presenza della vulnerabilità attraverso risposte indirette.

Azioni preventive

- XSS

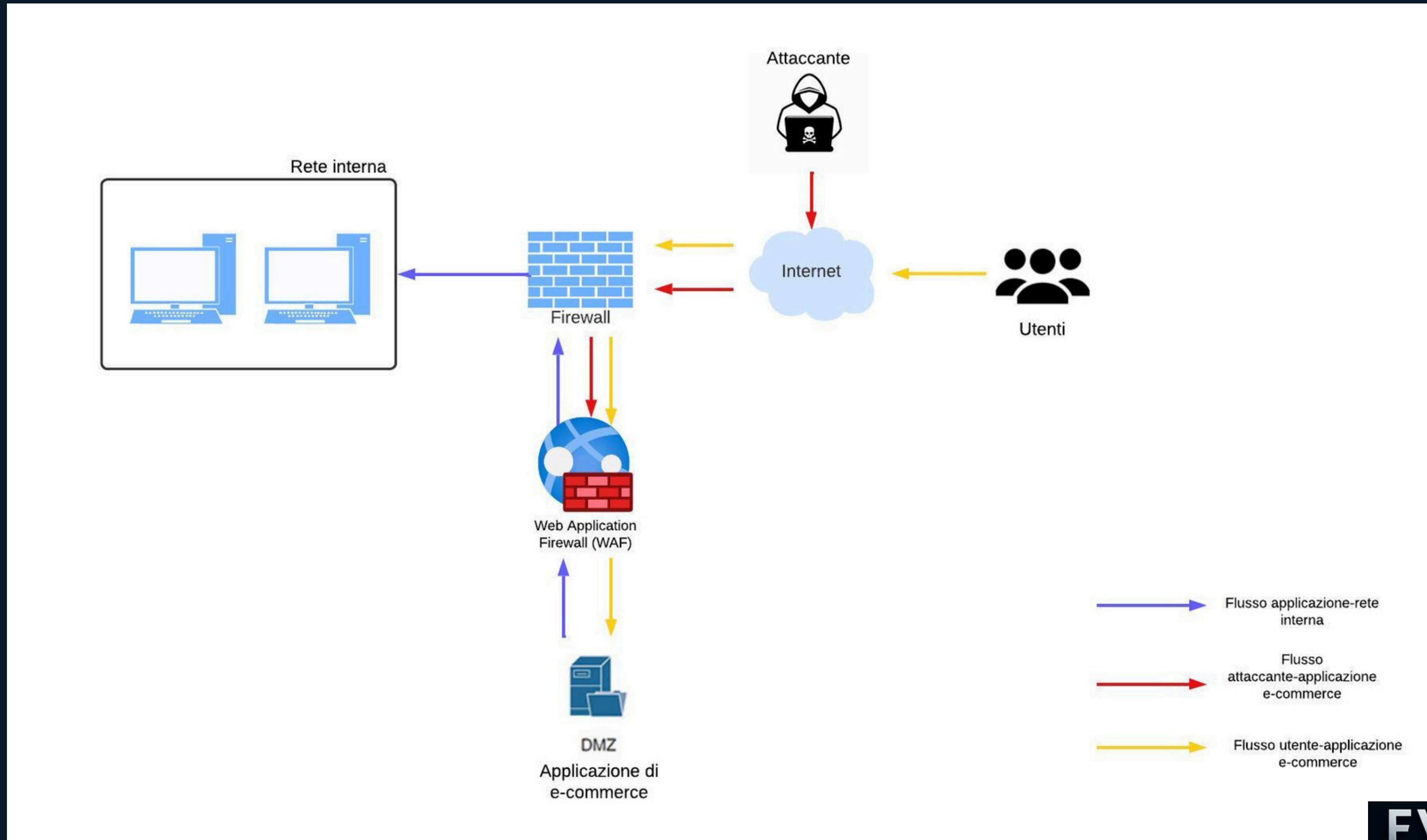
XSS (Cross-Site Scripting) invece, è una tecnica di attacco che consente agli attaccanti di iniettare script maligni in pagine web visualizzate da altri utenti. Questi script possono eseguire operazioni non autorizzate come rubare cookie, sessioni, o eseguire azioni a nome dell'utente vittima. Nel XSS Riflesso, gli script maligni sono inseriti nei parametri delle richieste HTTP e vengono eseguiti immediatamente nel browser dell'utente, senza essere memorizzati sul server. Nel XSS Persistente, gli script maligni vengono memorizzati sul server e vengono eseguiti ogni volta che un utente visualizza la pagina compromessa.

Entrambi gli attacchi sfruttano vulnerabilità comuni nelle applicazioni web, ma mentre SQLi mira a compromettere il database, XSS è focalizzato sull'utente finale e sul browser.

Azioni preventive

Cosa possiamo fare per proteggerci da questi attacchi? L'adozione di un Web Application Firewall (WAF) è essenziale per bloccare attacchi come XSS e SQLi, poiché ci permette di filtrare il traffico web malevolo prima che possa raggiungere il server. Per quanto riguarda la sicurezza della rete, un attaccante può sfruttare le vulnerabilità per superare i firewall perimetrali e compromettere la DMZ (Demilitarized Zone), che ospita infrastrutture critiche come i server e-commerce accessibili dall'esterno. Il WAF agirà come una barriera protettiva avanzata, frapponendosi tra internet e le risorse digitali da proteggere. Esaminando e analizzando il traffico http/https in ingresso, applicherà un insieme di regole e politiche di sicurezza per identificare e bloccare le richieste potenzialmente dannose prima che raggiungano il server dell'applicazione. Una caratteristica importante del WAF è la sua alta configurabilità, infatti gli stessi amministratori possono definire queste regole basandosi sulle esigenze uniche della rete e delle applicazioni da proteggere. Questa flessibilità consente di ottimizzare la sicurezza senza compromettere le prestazioni o la funzionalità delle applicazioni. Inoltre, molti WAF moderni offrono funzionalità avanzate come l'apprendimento automatico e l'analisi comportamentale per adattarsi dinamicamente alle nuove minacce, migliorando continuamente la protezione in tempo reale.

Azioni preventive



Impatti sul business

Cos'è un attacco DDoS?

Un attacco DDoS (Distributed Denial of Service) è un tipo di attacco informatico mirato a rendere un servizio, una rete o un sito web inaccessibile agli utenti legittimi. Questo viene realizzato sovraccaricando il sistema bersaglio con un'enorme quantità di traffico malevolo proveniente da molteplici sorgenti, spesso attraverso una botnet (una rete di computer infettati da malware e controllati dall'attaccante). Gli attaccanti coordinano i bot per inviare simultaneamente un gran numero di richieste al server bersaglio o alla rete. Questo sovraccarico di richieste può saturare la larghezza di banda del server, esaurire le risorse di sistema o causare il crash dell'applicazione bersaglio, rendendo il servizio inaccessibile per gli utenti legittimi. Quindi l'obiettivo principale di un attacco DDoS è rendere il servizio inaccessibile, causando interruzioni significative. Le aziende possono subire grosse perdite finanziarie dovute all'inaccessibilità dei servizi online, alla perdita di clienti e alle spese per mitigare l'attacco.

Impatti sul business

Azioni Preventive per Mitigare gli Attacchi DDoS

1. Distribuzione del Carico (Load Balancing): Un load balancer distribuisce il traffico di rete su più server, evitando che un singolo server venga sovraccaricato. Aumenta la capacità di gestione del traffico, migliora la disponibilità del servizio e riduce il rischio di downtime, utilizzando hardware o soluzioni software per il bilanciamento del carico.
2. Content Delivery Network (CDN): Una CDN distribuisce il contenuto statico (come immagini, video, file JavaScript) su più nodi geograficamente dispersi. Riduce il carico sul server principale, migliora le prestazioni e offre una prima linea di difesa contro attacchi DDoS volumetrici.
3. Rate Limiting: Limita il numero di richieste che un singolo IP può fare in un dato periodo di tempo e previene l'abuso delle risorse del server da parte di singoli attaccanti o botnet.

Impatti sul business

4. Web Application Firewall (WAF): Un WAF protegge le applicazioni web filtrando e monitorando il traffico HTTP, bloccando richieste dannose. Protegge contro una vasta gamma di attacchi, inclusi SQLi, XSS e alcuni tipi di attacchi DDoS.
5. Soluzioni Anti-DDoS: Servizi specifici di mitigazione DDoS (come Cloudflare DDoS Protection) che rilevano e filtrano il traffico malevolo. Forniscono una protezione dedicata contro attacchi DDoS, filtrando il traffico a livello di rete prima che raggiunga il server.
6. Monitoraggio Continuo e Allerta: Monitorare costantemente il traffico di rete per identificare comportamenti anomali e attivare allarmi in caso di sospetti attacchi, permette una risposta rapida minimizzando i tempi di inattività.

Impatti sul business

7. Segmentazione della Rete: Isolare diverse parti della rete per limitare i movimenti laterali in caso di compromissione, contiene l'impatto di un attacco, impedendo che si diffonda ad altri segmenti della rete stessa.
8. Autenticazione a Due Fattori (2FA): Implementare 2FA per l'accesso ai sistemi critici e alle applicazioni aumenta la sicurezza, riducendo il rischio di compromissione delle credenziali.
9. Piani di Risposta agli Incidenti: Il CSIRT (Computer Security Incident Response Team) si occupa della gestione degli incidenti di sicurezza informatica, classificando gli incidenti in base a fattori come il livello di criticità dell'incidente, per determinare la risposta più appropriata e mitigare l'impatto negativo sull'azienda.
10. Backup e Ripristino: Implementare strategie di backup regolari per i dati e le configurazioni di sistema, garantisce che i dati possano essere ripristinati rapidamente in caso di perdita o compromissione.

Impatti sul business

Un attacco DDoS (Distributed Denial of Service) che rende l'applicazione inaccessibile per 10 minuti può avere gravi ripercussioni economiche e operative. Per un sito di e-commerce, l'impatto è particolarmente significativo poiché ogni minuto di inattività si traduce in una perdita diretta di entrate. Se gli utenti spendono in media 1.500 € al minuto, l'impatto economico totale per 10 minuti di inattività sarà:

$$\underline{10 \text{ minuti} \times 1.500 \text{ €/minuto} = 15.000 \text{ €}}$$

Oltre alla perdita diretta di ricavi, ci sono altri fattori da considerare, per esempio un'eventuale perdita di vendite poiché gli utenti che non riescono ad accedere al sito potrebbero decidere in futuro di fare acquisti altrove. I clienti infatti, potrebbero considerare l'azienda meno affidabile se il sito non è disponibile generando un danno alla sua reputazione che può anche avere effetti a lungo termine. Infine come abbiamo già visto, la risposta a un attacco DDoS può richiedere l'intervento di esperti di sicurezza informatica, l'acquisto di servizi di mitigazione DDoS e l'implementazione di ulteriori misure di sicurezza.

RESPONSE

Cos'è un Malware?

Il termine "malware" è l'abbreviazione di "malicious software" e si riferisce a qualsiasi software progettato per danneggiare, disturbare, rubare informazioni o causare altri comportamenti indesiderati su dispositivi informatici. Il malware può infettare computer, server, dispositivi mobili e reti, causando una vasta gamma di problemi, dalla perdita di dati alla compromissione della sicurezza.

Tipi di Malware

1. Virus

Un virus è un tipo di malware che si allega a file legittimi e si replica quando quei file vengono eseguiti. Può danneggiare file, rallentare il sistema e diffondersi ad altri dispositivi.

2. Worm

Un worm è simile a un virus ma ha la capacità di autoreplicarsi senza l'intervento dell'utente. Si diffonde attraverso le reti, sfruttando vulnerabilità nei sistemi per infettare più dispositivi.

RESPONSE

3. Trojan Horse (Trojan)

I trojan sono malware che si mascherano da software legittimo per ingannare gli utenti e farli installare. Una volta installati, possono creare backdoor, rubare informazioni o causare altri danni.

4. Spyware

Lo spyware è progettato per spiare l'attività dell'utente senza il suo consenso. Raccoglie informazioni personali, come credenziali di accesso e dati di navigazione, e le invia a terze parti.

5. Adware

L'adware visualizza annunci pubblicitari indesiderati sul dispositivo dell'utente. Anche se non sempre dannoso, può rallentare il sistema e compromettere la privacy dell'utente.

6. Ransomware

Il ransomware critta i dati dell'utente e richiede un riscatto per decriptarli. Questo tipo di malware è particolarmente dannoso perché può rendere inaccessibili dati cruciali.

RESPONSE

7. Rootkit

I rootkit sono progettati per nascondere la presenza di altri malware sul sistema, permettendo loro di operare senza essere rilevati. Possono anche concedere accesso amministrativo agli attaccanti.

8. Keylogger

I keylogger registrano ogni tasto premuto dall'utente, raccogliendo informazioni sensibili come password e dati finanziari. Questa informazione viene poi inviata all'attaccante.

9. Botnet

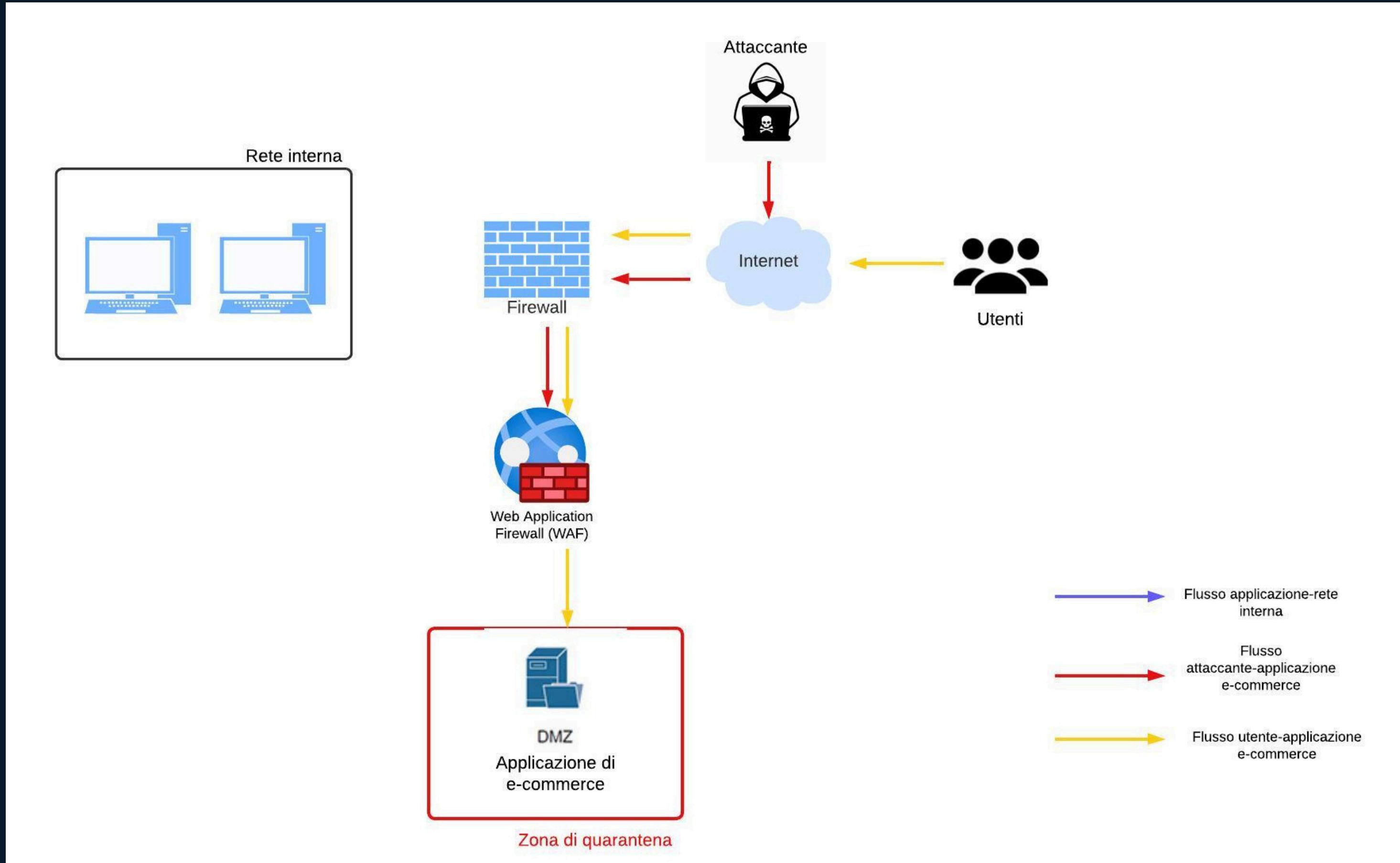
Una botnet è una rete di computer infetti controllati da un attaccante. I computer, chiamati "bot", possono essere utilizzati per lanciare attacchi DDoS, inviare spam e svolgere altre attività dannose.

10. Backdoor

Una backdoor è un metodo nascosto per bypassare le normali autenticazioni e ottenere accesso non autorizzato a un sistema. Spesso installata da altri malware, può essere utilizzata per prendere il controllo del sistema.

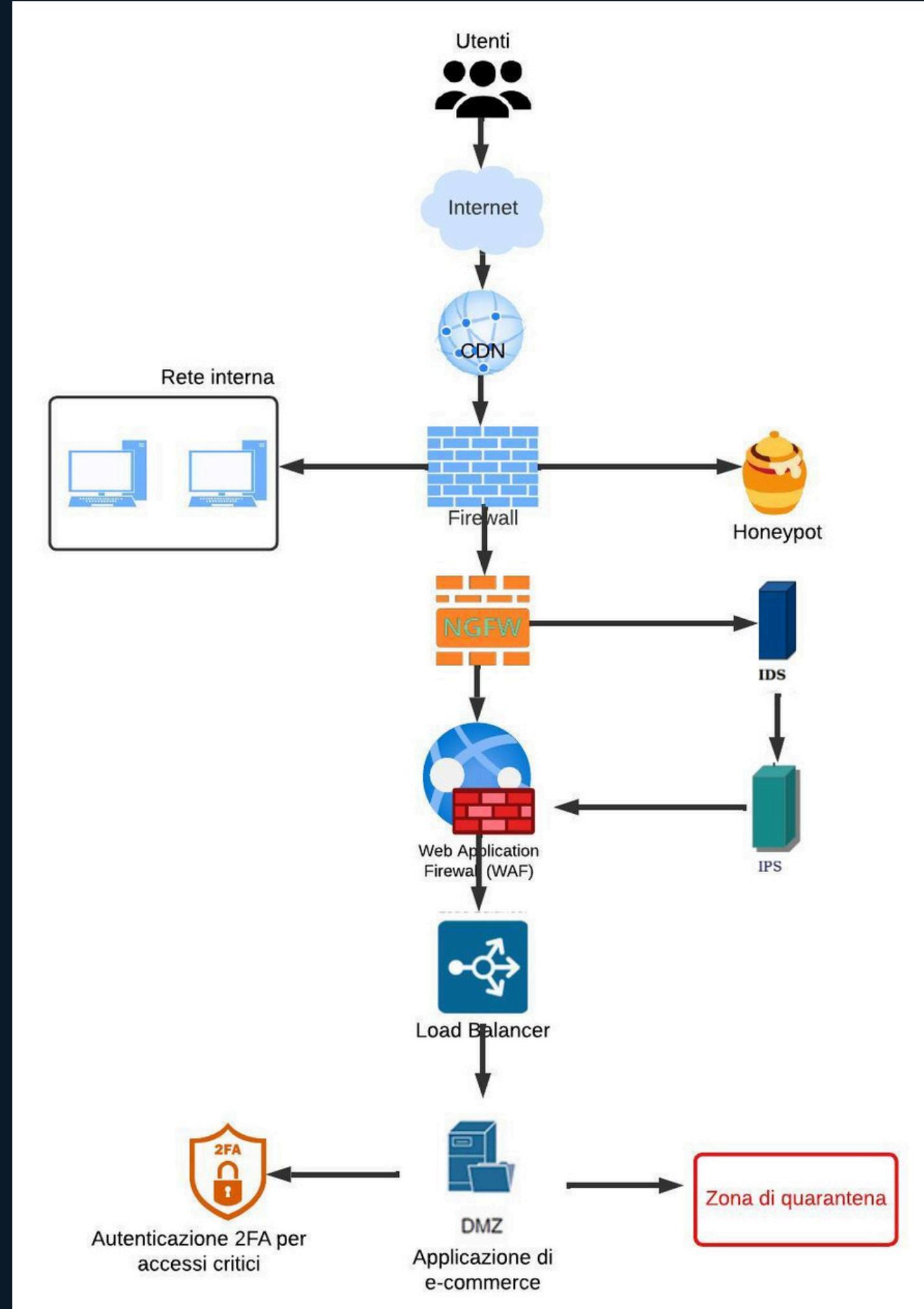
RESPONSE

L'applicazione web è stata infettata da un malware e la nostra priorità è proteggere la rete interna. Per farlo utilizziamo la tecnica dell'isolamento, che come abbiamo visto precedentemente, consiste nel separare la macchina infetta dalla rete interna e dagli utenti legittimi, garantendoci che il malware non possa propagarsi ulteriormente. La prima azione consiste nel rilevare la macchina compromessa all'interno della DMZ che ospita l'applicazione di e-commerce. Una volta identificata la macchina infetta, andiamo a creare una zona di quarantena all'interno della DMZ che verrà isolata dalle altre parti della rete e destinata esclusivamente al contenimento della macchina infetta. Successivamente, configuriamo il firewall per bloccare qualsiasi traffico dalla macchina infetta verso la rete interna e verso gli utenti legittimi. In questo modo, il malware non può propagarsi oltre la zona di quarantena. Possiamo mantenere il traffico tra la macchina infetta e l'attaccante, approfittandone per monitorare e analizzare l'attività malevola senza rischio di propagazione.



Soluzioni per una rete sicura

La sicurezza della rete è una priorità assoluta per qualsiasi organizzazione che voglia proteggere i propri dati e le proprie risorse digitali. L'implementazione di una rete sicura richiede una combinazione di tecnologie avanzate e pratiche di sicurezza rigorose. Ogni componente del nostro schema di rete è stato scelto e posizionato strategicamente per massimizzare la protezione e l'efficienza operativa. Grazie alle implementazioni nella slide successiva, la nostra rete risulterà ben protetta contro una vasta gamma di minacce, garantendo al contempo prestazioni elevate e alta disponibilità.



DESCRIZIONE degli ELEMENTI IMPLEMENTati

1. Content Delivery Network (CDN)

Un CDN è una rete distribuita di server che fornisce contenuti agli utenti in base alla loro posizione geografica. La sua funzione principale è migliorare le prestazioni del sito web, riducendo la latenza e mitigando attacchi DDoS distribuendo il carico del traffico su più server.

2. Next Generation Firewall (NGFW)

Il NGFW offre una protezione avanzata rispetto ai firewall tradizionali, integrando funzioni di ispezione approfondita dei pacchetti, prevenzione delle intrusioni e controllo delle applicazioni. Questa tecnologia permette di identificare e bloccare minacce avanzate, garantendo una sicurezza proattiva.

3. Intrusion Detection System (IDS)

L'IDS monitora il traffico di rete alla ricerca di attività sospette o non autorizzate. Questo sistema è fondamentale per rilevare potenziali attacchi e anomalie, avvisando gli amministratori di rete in tempo reale per permettere una rapida risposta.

DESCRIZIONE degli ELEMENTI IMPLEMENTati

4. Intrusion Prevention System (IPS)

L'IPS non solo rileva attività sospette come l'IDS, ma agisce anche per bloccarle. Questo sistema è posizionato dopo l'IDS per garantire che qualsiasi traffico malevolo identificato venga immediatamente neutralizzato, prevenendo potenziali danni.

5. Web Application Firewall (WAF)

Il WAF protegge le applicazioni web da una vasta gamma di attacchi come SQL Injection, Cross-Site Scripting (XSS) e Cross-Site Request Forgery (CSRF). Filtra e monitora il traffico HTTP/HTTPS tra l'applicazione web e Internet, garantendo che solo il traffico legittimo raggiunga i server dell'applicazione.

6. Load Balancer

Il Load Balancer distribuisce il traffico in entrata tra più server, garantendo alta disponibilità e affidabilità dell'applicazione. Questo strumento è essenziale per evitare sovraccarichi su singoli server e per migliorare le prestazioni complessive del sistema.

DESCRIZIONE degli ELEMENTI IMPLEMENTati

7. Honeypot

Un Honeypot è un sistema progettato per attirare e analizzare il traffico malevolo. Viene utilizzato come trappola per i potenziali attaccanti, permettendo agli amministratori di rete di studiare le tattiche degli hacker e migliorare le difese della rete.

8. Two-Factor Authentication (2FA)

La 2FA aggiunge un ulteriore livello di sicurezza richiedendo agli utenti di fornire due forme di identificazione prima di accedere a risorse critiche. Questo sistema riduce significativamente il rischio di accessi non autorizzati, proteggendo le informazioni sensibili.

BONUS

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-bfb67d47f1d7/>

<https://app.any.run/tasks/60b9570f-175b-4b03-816b-a38cc2b0255e/>

REPORT 1

The screenshot shows a Windows desktop environment. A command prompt window titled "Administrator: PERFORMANCE_BOOSTER_v3.6 by nikobg" is open, displaying a warning message about running the batch file. The message states: "DON'T RUN THE WHOLE BATCH FILE IF YOUR WINDOWS IS NOT v1709.v1809". It also mentions that the tool is for personal use only, has no guarantee, and is optimized for Win10 v1809. The window also contains some binary or hex code.

The desktop background features a watermark for "ANYRUN Test Mode".

Below the desktop, an "AnyRun" analysis interface is displayed. The main table shows network traffic analysis:

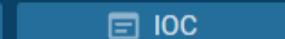
| | HTTP Requests | | 0 | Connections | | 4 | DNS Requests | | 0 | Threats | | 0 | Filter by PID, domain, name or ip | | | PCAP |
|----------|---------------|----------|-----|-------------|--------------|----|-----------------|------|--------|---------|-------------|---|-----------------------------------|--|--|------|
| | Timeshift | Protocol | Rep | PID | Process name | CN | IP | Port | Domain | ASN | Traffic | | | | | |
| Pricing | 378 ms | UDP | ✓ | 4 | System | ? | 192.168.100.255 | 137 | - | - | ↑ 994 b ↓ | | | | | |
| Contacts | 383 ms | UDP | ✓ | 4 | System | ? | 192.168.100.255 | 138 | - | - | ↑ 2.38 Kb ↓ | | | | | |
| FAQ | 2375 ms | UDP | ? | 1080 | svchost.exe | ? | 224.0.0.252 | 5355 | - | - | ↑ 48 b ↓ | | | | | |
| Sign In | 4375 ms | UDP | ? | 1080 | svchost.exe | ? | 224.0.0.252 | 5355 | - | - | ↑ 48 b ↓ | | | | | |

At the bottom of the screen, a status bar displays: "Warning [668] cmd.exe Runs PING.EXE to delay simulation".

 Malicious activity

Win7 32 bit
Complete

Indicators:   

Processes Filter by PID or name Only important

| PID | Process Name | Command Line | File I/O | Network | Memory | Threads | Handles |
|------|--------------------------------|--|----------|---------|--------|---------|---------|
| 2088 | PERFORMANCE BOOSTER_v3.6.exe | | 140 | 6 | 19 | | |
| 668 | cmd.exe | /c "C:\Users\admin\AppData\Local\Temp\3201.tmp\3202.tmp\3203.bat C..." | 7k | 133 | 110 | | |
| 2380 | mode.com | MODE CON: COLS=78 LINES=54 | 39 | 8 | 16 | | |
| 3332 | powershell.exe | Set-ExecutionPolicy Unrestricted -Force | 2k | 639 | 87 | | |
| 2824 | regedit.exe | /e "C:\Users\admin\Desktop\FullRegistryBackup.reg" | 5k | 359k | 30 | | |
| 3612 | SystemPropertiesProtection.exe | | 653 | 103 | 88 | | |
| 3888 | attrib.exe | -r C:\Windows\System32\drivers\etc\hosts | 49 | 9 | 15 | | |
| 3880 | PING.EXE | localhost -n 2 | 77 | 148 | 24 | | |
| 2948 | notepad.exe | C:\Windows\system32\Drivers/etc/hosts | | | | | |

Try community version for free!

Register now

EVILGUARD
SOLUTIONS

REPORT 1

Il file "PERFORMANCE_BOOSTER_v3.6.exe" analizzato tramite any.run è un tipo di malware progettato per scaricare ed eseguire altri malware sul sistema infetto. Durante l'analisi, sono stati osservati diversi comportamenti dannosi che indicano un'infezione significativa e potenzialmente pericolosa.

Il malware esegue comandi da un file batch (.bat) utilizzando CMD.EXE, un comportamento comune tra i malware che automatizzano operazioni dannose. Questo include la modifica del registro di sistema tramite regedit.exe, una tecnica utilizzata per garantirsi la persistenza sul sistema infetto e disabilitare funzioni di sicurezza. Il malware stabilisce anche connessioni UDP verso indirizzi IP locali e multicast, suggerendo attività di scansione della rete o comunicazione con altre macchine infette. Queste connessioni potrebbero essere utilizzate per esfiltrare dati o ricevere comandi da un server di comando e controllo (C2).

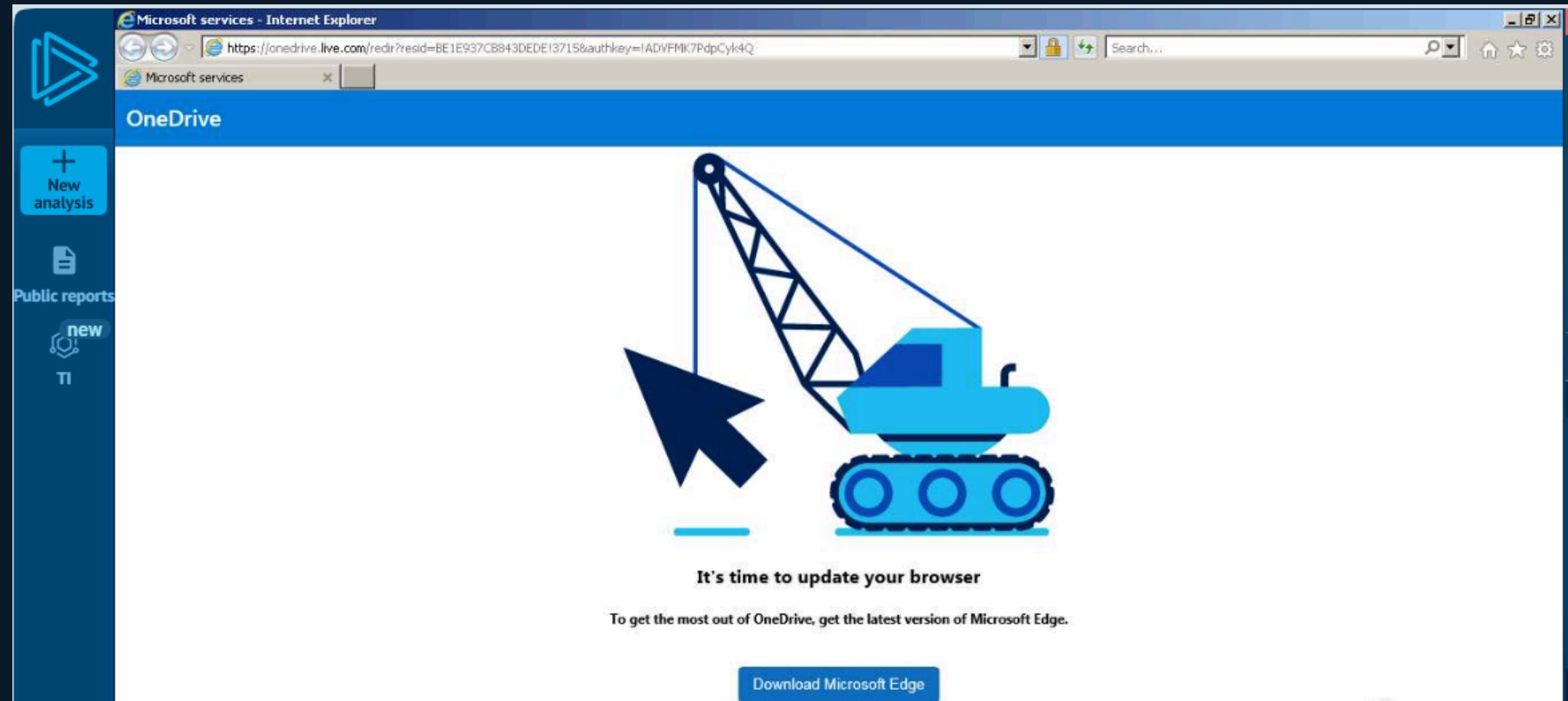
Inoltre, il malware utilizza powershell.exe per eseguire script non firmati, aumentando le capacità di compromissione del sistema. La possibilità di eseguire script PowerShell senza restrizioni permette al malware di eseguire comandi e script dannosi, incrementando il rischio per il sistema infetto. Il malware crea anche file temporanei, che potrebbero contenere payload aggiuntivi o dati esfiltrati, rappresentando ulteriori rischi per la sicurezza.

REPORT 1

Per mitigare l'impatto del malware, è fondamentale intraprendere le seguenti azioni:

- Rimozione del Malware: utilizzare software antivirus e anti-malware aggiornati per rilevare e rimuovere il malware. Effettuare una scansione completa del sistema per assicurarsi che non ci siano altre infezioni.
- Ripristino delle Modifiche al Registro di Sistema: utilizzare strumenti di ripristino del registro di sistema per annullare le modifiche apportate dal malware. Verificare manualmente le chiavi di registro critiche per assicurarsi che non siano state compromesse.
- Monitoraggio del Traffico di Rete: configurare firewall e sistemi di rilevamento delle intrusioni (IDS) per monitorare e bloccare il traffico sospetto. Analizzare i log di rete per identificare eventuali comunicazioni non autorizzate con server esterni.
- Educazione e Formazione degli Utenti: educare gli utenti sui rischi del malware e sulle migliori pratiche per evitare infezioni, come evitare di eseguire file sospetti e mantenere aggiornati i software di sicurezza.
- Backup Regolari dei Dati: assicurarsi che tutti i dati critici siano regolarmente salvati su backup sicuri, in modo da poter ripristinare il sistema in caso di attacchi gravi come il ransomware.

REPORT 2



The screenshot shows a Microsoft Edge browser window. The address bar displays "Microsoft services - Internet Explorer" and the URL "https://onedrive.live.com/redir?resid=BE1E937CB843DEDE13715&authkey=ADVFMK7PdpCyk4Q". The main content area features a blue and white illustration of a construction crane and excavator. Below the illustration, the text "It's time to update your browser" is displayed. A large blue button labeled "Download Microsoft Edge" is present. On the left side of the browser, there is a vertical sidebar with various icons and links, including "New analysis", "Public reports", "TI", "Pricing", "Contacts", "FAQ", and "Sign In".



The screenshot shows the ANYRUN platform interface for analyzing malicious activity. At the top, it displays "Malicious activity" with a link to "https://1drv.ms/u/s!At7eQ7h8kx6-nQM1RTCuz3aQspOE". It indicates "Win7 32 bit" and "Complete" status, with "Start: 08.02.2024, 18:37" and "Total time: 60 s". The interface includes tabs for "IOC", "MalConf", and "Restart", and buttons for "Text report", "Graph", "ATT&CK", "ChatGPT", and "Export". A CPU usage chart is shown above a list of processes. The process list includes:

- 1632 iexplore.exe "https://1drv.ms/u/s!At7eQ7h8kx6-nQM1RTCuz3aQspOE"
- 3564 iexplore.exe SCODEF:1632 CREDAT:267521 /prefetch:2
- 3360 MicrosoftEdgeSetup.exe PE

Process details for ID 3564 show "No verdict". The right side of the interface features a circular rating of "10 OUT OF 100" and a "More Info" section with a warning about T1036.003 Rename System Utilities (1) and Process drops legitimate windows executable.

Try community version for free!

EVILGUARD
SOLUTIONS

REPORT 2

I dati indicano che Internet Explorer (iexplore.exe) è stato avviato utilizzando uno specifico URL come parametro della riga di comando.

I programmi legittimi, come i browser web, spesso vengono eseguiti con URL specifici come parametri della riga di comando per accedere direttamente a pagine web o risorse. Questo comportamento è comune quando gli utenti cliccano su link o segnalibri per navigare su siti web.

I programmi dannosi possono sfruttare questo comportamento avviando programmi legittimi come Internet Explorer con URL malevoli come parametri della riga di comando per scaricare ed eseguire contenuti dannosi. In questo caso, il processo rimuove il contenuto eseguibile e sostituisce i file eseguibili legittimi di Windows, suggerendo azioni potenzialmente pericolose. Questa tecnica può essere usata per eludere il rilevamento ed eseguire payload dannosi sul sistema. Inoltre, la cancellazione dei file eseguibili subito dopo l'avvio può indicare un tentativo di permanere nel sistema e mantenere il controllo per scopi malevoli.

REPORT 2

```
C:\Users\admin\AppData\Local\Temp\EU9F13.tmp\MicrosoftEdgeUpdate.exe /installsource taggedmi  
/install "appguid={56EB18F8-B008-4CBD-B6D2-  
8C97FE7E9062}&appname=Microsoft%20Edge&needsadmin=prefers&usagestats=0"
```

Questa riga di comando è utilizzata per eseguire il file MicrosoftEdgeUpdate.exe situato in una cartella temporanea, con parametri relativi all'origine dell'installazione, GUID dell'app, nome dell'app, privilegi di amministratore e statistiche di utilizzo. I programmi legittimi possono usare righe di comando simili per aggiornare software o installare nuove applicazioni con parametri specifici per l'origine dell'installazione, il nome dell'app e i privilegi.

Gli autori malintenzionati potrebbero sfruttare questa riga di comando per eseguire una versione falsa o dannosa di MicrosoftEdgeUpdate.exe da una cartella temporanea, inducendo gli utenti a installare malware con il pretesto di un aggiornamento software legittimo. I parametri possono anche essere manipolati per ottenere privilegi di amministratore o raccogliere dati sull'uso del sistema per scopi dannosi.

REPORT 2

Per prevenire attacchi che sfruttano l'esecuzione di comandi tramite URL, come nel caso del malware "1drv.ms", è essenziale implementare una serie di misure di sicurezza:

1. Educazione degli Utenti

- Consapevolezza della Sicurezza: Formare gli utenti sui rischi legati all'apertura di file e all'esecuzione di comandi da URL non verificati.
- Formazione Continua: Offrire corsi regolari su tecniche di phishing e ingegneria sociale.

2. Controllo delle Applicazioni

- Restrizioni su URL e Comandi: Limitare l'uso di URL come parametri della riga di comando attraverso policy aziendali.
- Whitelist: Utilizzare whitelist per permettere solo URL e applicazioni approvate.

3. Protezione del Sistema

- Antivirus e Anti-Malware: Mantenere aggiornati i software di sicurezza per rilevare e bloccare malware.
- Patch di Sicurezza: Applicare regolarmente aggiornamenti di sicurezza per chiudere vulnerabilità.

REPORT 2

4. Monitoraggio e Rilevamento

- Sistemi di Rilevamento delle Intrusioni (IDS): Monitorare il traffico di rete per individuare attività sospette.
- Monitoraggio dei Log: Analizzare i log di sistema e di rete per rilevare comportamenti anomali.

5. Isolamento e Contenimento

- Sandboxing: Isolare l'esecuzione di programmi non fidati in ambienti sicuri.
- Segmentazione della Rete: Segmentare la rete per limitare la propagazione del malware.

6. Controllo degli Accessi

- Autenticazione a Due Fattori (2FA): Implementare 2FA per accedere a risorse critiche.
- Gestione dei Privilegi: Assegnare privilegi minimi necessari per ridurre l'impatto di una compromissione.

7. Backup e Ripristino

- Backup Regolari: Eseguire backup regolari dei dati critici e conservarli in posizioni sicure.
- Piani di Risposta agli Incidenti: Stabilire piani di risposta per garantire una reazione rapida ed efficace in caso di compromissione.

Grazie



Per maggiori informazioni visita: www.evilguard.com