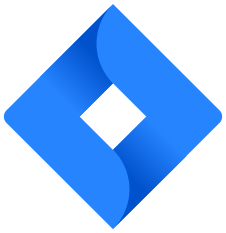


Cyber Safety Solutions

Otman Hmich & Michael Andreoli

Chi siamo?

La nostra azienda è nata dall'unione di un White Hat e un Black Hat, mettiamo a disposizione le nostre conoscenze, maturate grazie alla difesa e all'attacco dei sistemi informatici. Ci dedichiamo a proteggere le informazioni e le risorse digitali delle aziende di tutte le dimensioni. Fondata nel 2024, la nostra missione è fornire soluzioni di sicurezza all'avanguardia per prevenire, rilevare e rispondere alle minacce cibernetiche.

Perchè scegliere Cyber Safety Solutions?

In un mondo in cui le minacce informatiche sono in costante evoluzione, offriamo un approccio proattivo e completo alla sicurezza informatica. I nostri servizi includono:

- **Valutazione della Sicurezza**: Identificazione delle vulnerabilità e delle potenziali minacce con audit di sicurezza completi e penetration testing avanzati.
- **Gestione delle Minacce**: Monitoraggio continuo e risposta immediata agli incidenti per garantire che la vostra azienda sia sempre un passo avanti rispetto agli attaccanti.
- **Consulenza e Formazione**: Assistenza nella creazione di strategie di sicurezza personalizzate e programmi di formazione per sensibilizzare e preparare il personale aziendale.
- **Soluzioni di Sicurezza Personalizzate**: Implementazione di tecnologie di sicurezza su misura, tra cui firewall, sistemi di prevenzione delle intrusioni (IPS), e soluzioni di crittografia avanzate.

In cosa ci distinguiamo?

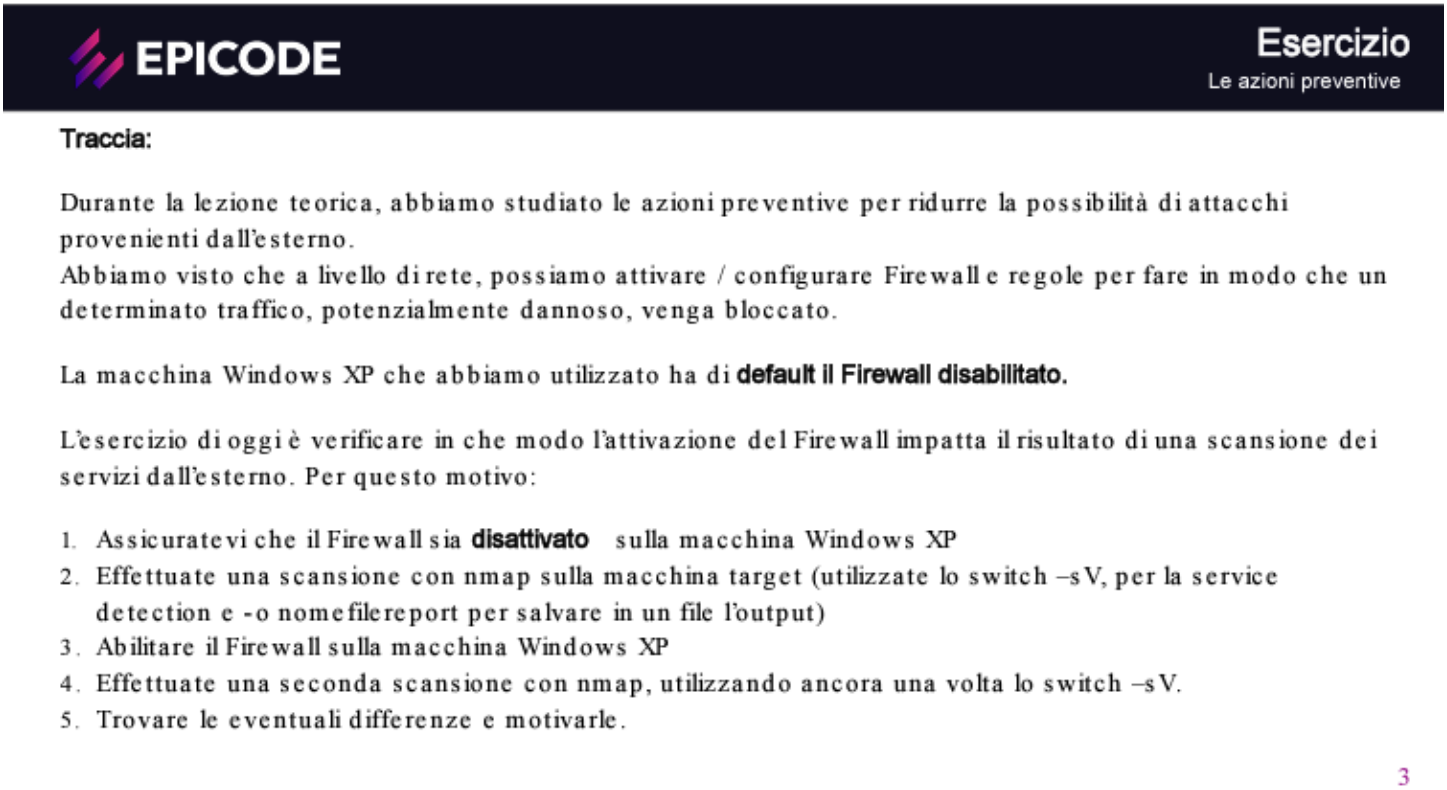
- **Esperienza e Competenza**: Il nostro team è composto da esperti certificati con anni di esperienza nel settore della sicurezza informatica.

- **Tecnologie Avanzate**: Utilizziamo strumenti e tecnologie all'avanguardia per proteggere la vostra azienda dalle minacce più recenti e sofisticate.
- **Approccio Personalizzato**: Siamo dedicati a comprendere le specifiche esigenze della vostra azienda per fornire soluzioni di sicurezza su misura.
- **Affidabilità e Riservatezza**: Garantiamo la massima discrezione e riservatezza nella gestione dei vostri dati e delle vostre informazioni.

La Nostra Visione

Immaginiamo un futuro in cui le aziende possano operare in totale sicurezza nel mondo digitale. Il nostro impegno è quello di costruire soluzioni innovative e affidabili che proteggano il cuore delle vostre operazioni aziendali, permettendovi di concentrarvi sulla crescita e sull'innovazione.

S9-L1



EPICODE

Esercizio
Le azioni preventive

Traccia:

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

La macchina Windows XP che abbiamo utilizzato ha di **default il Firewall disabilitato.**

L'esercizio di oggi è verificare in che modo l'attivazione del Firewall impatta il risultato di una scansione dei servizi dall'esterno. Per questo motivo:

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

3

Step by Step

Scansione della rete

Ci preoccupiamo di effettuare un'approfondita scansione della rete in modo da avere una precisa idea di cosa succede su quali porte.

Remediation

Andiamo ad attivare il firewall su Windows XP in modo da filtrare il traffico in entrata e bloccare potenziali minacce.

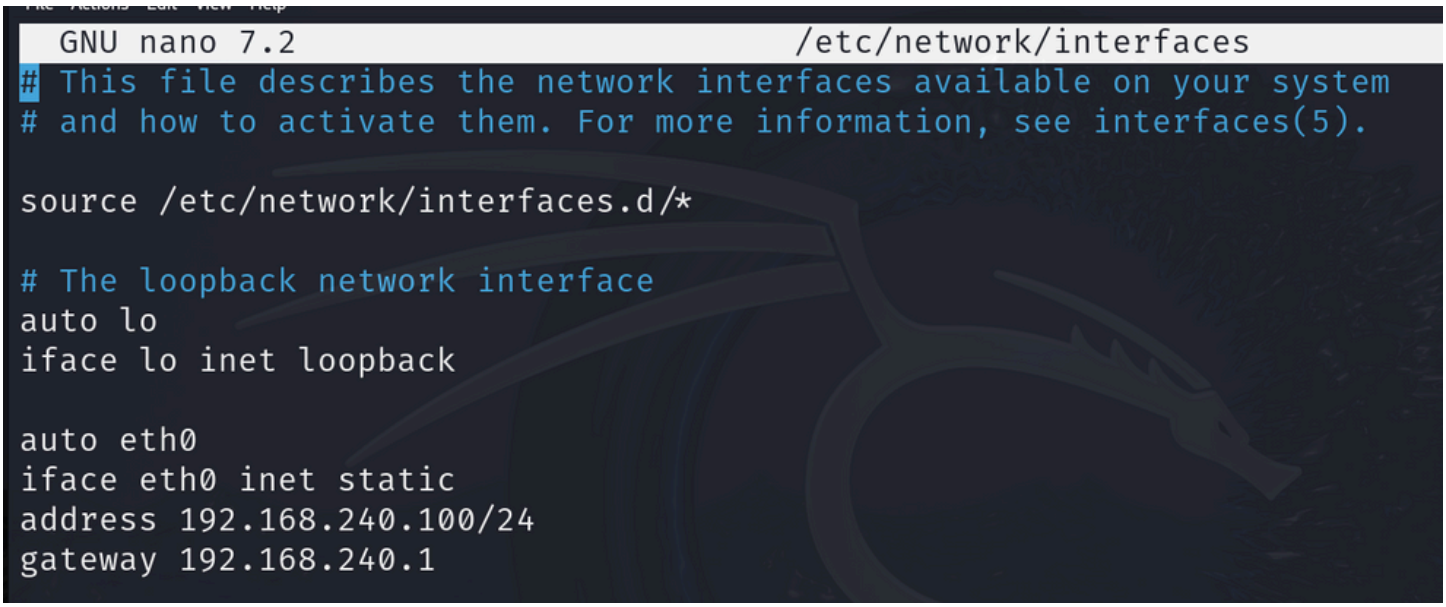
Check

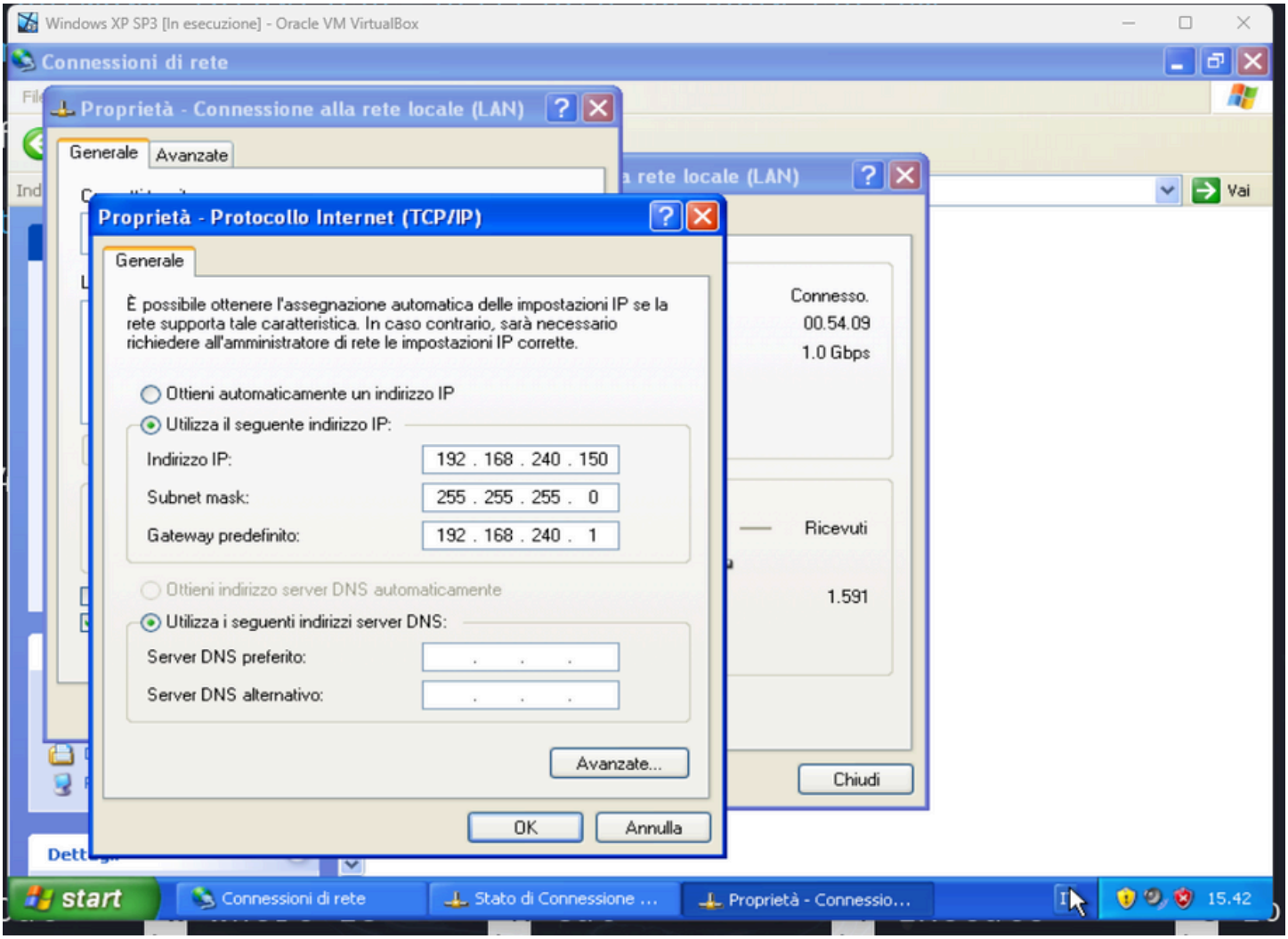
Effettuiamo una nuova scansione e prendiamo nota delle differenze per assicurarci che le nostre azioni abbiano avuto effetto.

Process

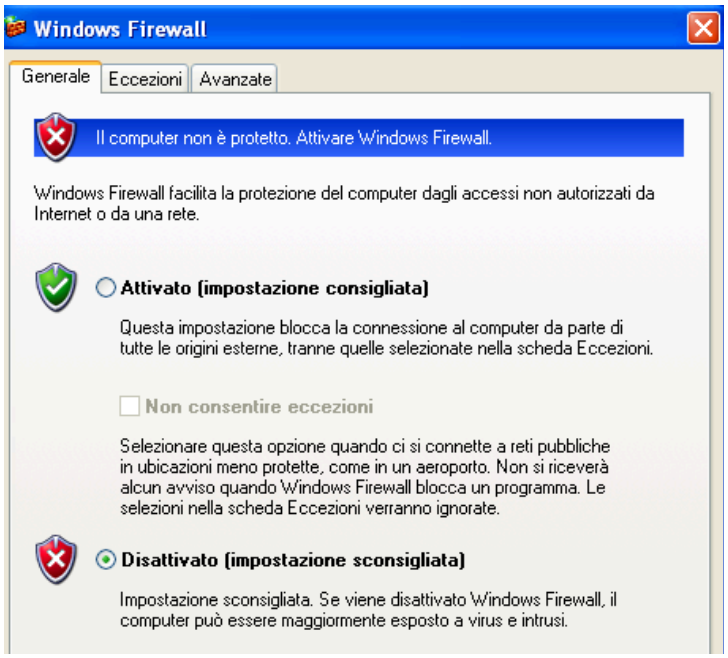
IP Configuration

Andiamo a impostare gli indirizzi IP delle nostre macchine virtuali come richiesto dalla traccia.



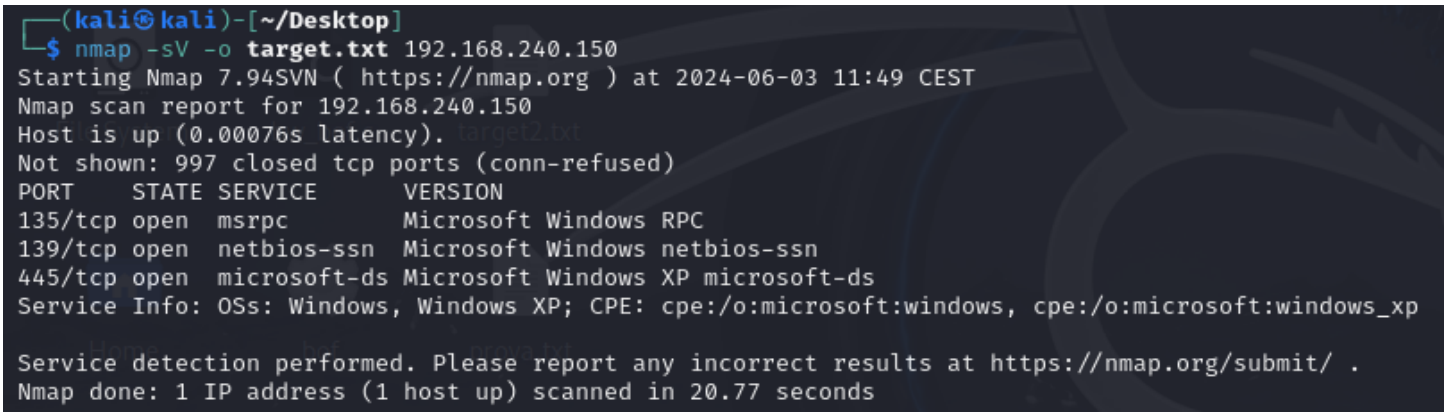


NMAP con firewall disattivo



Andiamo ad effettuare una scansione con nmap sulla nostra macchina windows utilizzando l'opzione -sV per stabilire le porte aperte, le

informazioni e la versione dei servizi attivi, per poi salvare l'output su un file di testo.



Da questa scansione possiamo notare che abbiamo controllato 1000 porte, 997 hanno rifiutato la connessione, perché sono chiuse o perché filtrate. Le 3 porte restanti, risultano aperte con i servizi e le versioni, mostrate nell'immagine.

Porte e servizi associati

- **Porta 135 (msrpc):**
  - Utilizzata pe rle chiamate di procedura remota di Microsoft (RPC).
  - È una porta critica per le funzionalità di rete di Windows e può essere un vettore di attacco se non adeguatamente protetta.

- **Porta 139 (netbios-ssn):**
  - Utilizzata dal servizio NetBIOS per sessioni di rete su TCP/IP.
  - Tipicamente usata per condivisioni di file o stampanti.

- **Porta 445 (microsoft-ds):**
  - Utilizzata per la condivisione di file e stampanti tramite SMB (Server Message Block) su TCP/IP.
  - Sostituisce la funzionalità del NetBIOS sulle reti più moderne.

NMAP con firewall attivo


```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sV -o target2.txt 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 12:01 CEST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.36 seconds
```

Dopo aver effettuato la scansione notiamo che il dispositivo sembra essere offline, questo perchè il firewall ci impedisce di pingare la macchina.

```
  -Pn: Treat all hosts as online -- skip host discovery
```

Utilizziamo lo switch ***-Pn*** in modo da evitare il ping e occuparsi subito della service discovery.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sV -Pn -o target2.txt 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 12:01 CEST
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 218.11 seconds
```

Conclusione

Scansione con firewall disattivo

Eseguendo la scansione con ***nmap*** siamo riusciti ad avere accesso alle porte aperte e a scoprire i servizi atttivi per riuscire a sfruttarle a

nostro piacimento per effettuare accessi da remoto, installare backdoor oppure inserire del codice malevolo.

Scansione con firewall attivo

Attivando il firewall abbiamo riscontrato l'impossibilitàà di eseguire il test di ping e utilizzando l'opzione ***-Pn*** abbiamo cercato di bypassare il test per procedere direttamente alla service discovery, non avendo peerò certezza dello stato delle porte, in quanto il firewall ci blocca l'accesso.

Preventivo

Preventivo n°: 1

Cliente:

Nome del Cliente

Indirizzo azienda Cliente

P.IVA/C.F.

Data: 03/06/2024

Valido fino a: 13/06/2024

Voci/Servizi	Quantità	Prezzo	Iva	Totale
Network Scan	16 ore (8hx2)	1600€	352€ (22%)	1952€
Penetration Test	32 ore (16hx2)	3200€	704€ (22%)	3904€
Remediation Actions	32 ore (16hx2)	3200€	704€ (22%)	3904€
Spese di Viaggio	300€ x 2	600€	132€	732€

Subtotale 8600€

Iva 1892€

Totale 10.492€

S9-L2

Traccia:

Durante la lezione teorica, abbiamo affrontato gli argomenti riguardanti la business continuity e disaster recovery.

Nell'esempio pratico di oggi, ipotizziamo di essere stati assunti per valutare **quantitativamente** l'impatto di un determinato disastro su un asset di una compagnia.

Con il supporto dei dati presenti nelle tabelle che seguono, calcolare la **perdita annuale** che subirebbe la compagnia nel caso di:

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

Dati:

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

EVENTO	ARO
Terremoto	1 volta ogni 30 anni
Incendio	1 volta ogni 20 anni
Inondazione	1 volta ogni 50 anni

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

4

La **business continuity** (continuità operativa) è un concetto aziendale che si riferisce alla capacità di un'organizzazione di mantenere le proprie operazioni essenziali e di continuare a fornire prodotti e servizi durante e dopo un evento di crisi o di emergenza. Questo concetto comprende un insieme di strategie, piani e azioni che un'azienda mette in

atto per affrontare e superare potenziali interruzioni, riducendo al minimo l'impatto sulle operazioni aziendali.

Componenti chiave della business continuity

1. **Analisi dell'Impatto Aziendale (Business Impact Analysis - BIA):** Valuta gli effetti potenziali delle interruzioni sulle diverse funzioni aziendali, identificando le attività critiche e i tempi di ripristino accettabili.
2. **Valutazione dei Rischi:** Identifica e valuta i rischi che potrebbero causare interruzioni, come disastri naturali, cyber-attacchi, guasti tecnologici, pandemie, etc.
3. **Piani di Continuità Operativa (BCP - Business Continuity Plan):** Documenti che descrivono le strategie e le azioni da intraprendere per garantire la continuità delle operazioni essenziali. Includono procedure per la gestione delle crisi, la comunicazione interna ed esterna, e le soluzioni di recupero.
4. **Disaster Recovery Plan (DRP):** Un sottoinsieme del BCP, focalizzato specificamente sul ripristino dei sistemi IT e delle infrastrutture tecnologiche dopo un disastro.
5. **Formazione e Sensibilizzazione:** Programmi di formazione per il personale affinché sia preparato a rispondere correttamente in caso di emergenza.
6. **Test e Manutenzione:** Test periodici e aggiornamenti dei piani di continuità operativa per assicurare che siano efficaci e che riflettano i cambiamenti nell'ambiente aziendale e tecnologico.

Importanza della business continuity

- **Mitigazione** dei Rischi: Riduce i rischi associati alle interruzioni operative, proteggendo l'integrità e la reputazione dell'azienda.
- **Resilienza Aziendale:** Aumenta la capacità dell'organizzazione di adattarsi e rispondere rapidamente alle situazioni di crisi.
- **Compliance:** Aiuta a soddisfare i requisiti normativi e contrattuali relativi alla gestione della continuità operativa.
- **Vantaggio Competitivo:** Migliora la fiducia dei clienti e degli stakeholder, dimostrando un impegno verso la gestione dei rischi e la continuità dei servizi.

Il **disaster recovery** (ripristino in caso di disastro) è un insieme di politiche, strumenti e procedure progettati per proteggere un'organizzazione e garantire il ripristino rapido e completo delle sue infrastrutture tecnologiche e dei sistemi IT in seguito a un evento disastroso. Si tratta di un componente cruciale della business

continuity, focalizzato specificamente sulla continuità dei servizi IT e sulla minimizzazione delle perdite di dati.

Componenti chiave del disaster recovery

1. **Piano di Disaster Recovery (DRP):** Un documento dettagliato che descrive le azioni specifiche da intraprendere per ripristinare i sistemi IT e le infrastrutture tecnologiche dopo un disastro. Include i ruoli e le responsabilità del personale coinvolto, le procedure di emergenza e le risorse necessarie.
2. **Backup dei Dati:** Copie di sicurezza dei dati aziendali, eseguite regolarmente e conservate in luoghi sicuri (spesso off-site) per garantire che possano essere recuperate in caso di perdita o corruzione dei dati originali.
3. **Ripristino del Sistema:** Procedure per reinstallare e riconfigurare hardware e software, compresi server, reti e applicazioni, per riportare l'operatività a uno stato funzionale.
4. **Replicazione dei Dati:** Tecniche di duplicazione dei dati in tempo reale o quasi reale verso un sito di ripristino secondario, in modo da garantire che i dati più recenti siano disponibili in caso di disastro.
5. **Siti di Ripristino (Hot, Warm, Cold):**
   - **Hot Site:** Un sito di ripristino completamente operativo, con hardware, software e dati aggiornati, pronto per essere utilizzato immediatamente.
   - **Warm Site:** Un sito con infrastrutture di base e alcune applicazioni pronte all'uso, ma che richiede un certo tempo di configurazione e aggiornamento.
   - **Cold Site:** Uno spazio fisico predisposto con alcune infrastrutture, ma senza hardware e software pronti, richiedendo un tempo maggiore per essere reso operativo.
6. **Test del Piano di Disaster Recovery:** Test periodici del DRP per verificarne l'efficacia e apportare eventuali correzioni o aggiornamenti. Questi test aiutano a identificare eventuali lacune e garantiscono che il personale sia ben preparato.

Importanza del disaster recovery

- **Minimizzazione del Downtime:** Riduce il

tempo di inattività dei sistemi IT, permettendo all'organizzazione di riprendere rapidamente le operazioni dopo un disastro.

- **Protezione dei Dati:** Garantisce la salvaguardia dei dati critici, riducendo il rischio di perdita di dati che potrebbero essere vitali per l'azienda.

- **Continuità Operativa:** Supporta la continuità delle operazioni aziendali, assicurando che le funzioni essenziali possano continuare anche in situazioni di emergenza.
- **Conformità Normativa:** Aiuta a soddisfare requisiti legali e regolamentari riguardanti la protezione dei dati e la continuità dei servizi.
- **Riduzione dei Costi:** Anche se la pianificazione e l'implementazione di un DRP comportano dei costi, questi sono spesso inferiori ai costi potenziali derivanti da una grave interruzione dei servizi IT.

Esempi di scenari di disaster recovery

- **Disastri Naturali:** Eventi come terremoti, uragani, alluvioni o incendi che possono danneggiare fisicamente le infrastrutture IT.
- **Cyber-attacchi:** Incidenti come attacchi ransomware, malware, hacking o altre forme di compromissione della sicurezza informatica.
- **Guasti Tecnologici:** Malfunzionamenti di hardware, blackout elettrici o problemi di rete che possono causare l'interruzione dei servizi IT.
- **Errori Umani:** Azioni involontarie del personale che possono portare alla cancellazione di dati, configurazioni errate o altri problemi operativi.

Fasi del disaster recovery

1. **Preparazione:** Sviluppo del DRP, identificazione delle risorse critiche e dei rischi, implementazione delle soluzioni di backup e replicazione dei dati.
2. **Risposta all'Incidente:** Attivazione del DRP subito dopo il verificarsi di un disastro, compresa la comunicazione con i team interni ed esterni.
3. **Ripristino:** Esecuzione delle procedure di ripristino per riportare i sistemi IT e le operazioni aziendali a uno stato funzionale.
4. **Ritorno alla Normalità:** Rientro alla normale operatività, valutazione dei danni, aggiornamento del DRP basato sulle lezioni apprese durante l'incidente.
5. **Revisione e Aggiornamento:** Analisi dell'efficacia del DRP, identificazione delle aree di miglioramento e aggiornamento del piano per affrontare future minacce e cambiamenti nell'infrastruttura IT.

ALE: Annualized loss expectancy.

Valore delle perdite stimate nell'arco di un anno.

ALE = SLE * ARO.

SLE: Single loss expectancy.

Valore delle perdite in caso di un determinato evento.

ARO: Annualized Rate of Occurence.

Stima della frequenza con cui un particolare evento di rischio si verifica in un anno.

SLE = AV * EF.

AV: Asset Value.

Valore dell'asset.

EF: Exposure Factor.

La percentuale di danno o perdita che si stima avverrà a causa dell'evento specifico.

Inondazione Asset Edificio Secondario:

SLE = 150.000€ * 40% = 60.000€

ALE = 60.000€ * 0.02 = ***1.200€***

Terremoto Asset Datacenter:

SLE = 100.000€ * 95% = 95.000€

ALE = 95.000€ * 0.03 = ***2.850€***

Incendio Asset Edificio Primario:

SLE = 350.000€ * 60% = 210.000€

ALE = 210.000€ * 0.05 = ***10.500€***

Incendio Asset Edificio Secondario:

SLE = 150.000€ * 50% = 75.000€

ALE = 75.000€ * 0.05 = ***3.750€***

Inondazione Asset Edificio Primario:

SLE = 350.000€ * 55% = 192.500€

ALE = 192.500€ * 0.02 = ***9.650€***

Terremoto Asset Edificio Primario:

SLE = 350.000€ * 80% = 280.000€

ALE = 280.000€ * 0.03 = ***8.400€***

S9-L3

Traccia:

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

La **threat intelligence** (intelligence sulle minacce) è la raccolta, l'analisi e l'utilizzo di informazioni riguardanti minacce attuali o potenziali alla sicurezza informatica di un'organizzazione. L'obiettivo della threat intelligence è quello di comprendere meglio le minacce, gli attori malevoli, le loro motivazioni, le tecniche utilizzate e i potenziali impatti sulle infrastrutture aziendali. Questo permette alle organizzazioni di anticipare, identificare e rispondere efficacemente agli attacchi informatici.

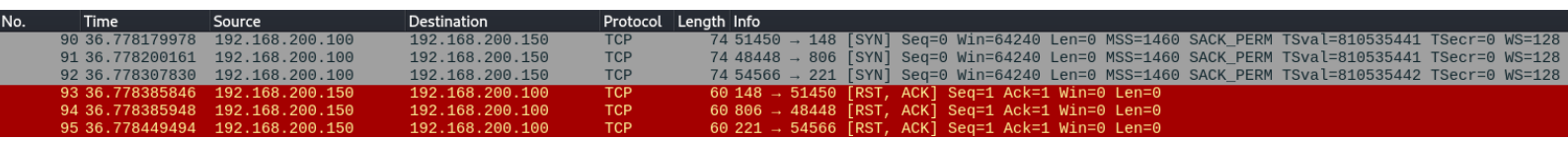
Componenti chiave della threat intelligence

1. **Raccolta delle Informazioni**: Raccogliere dati da diverse fonti, sia interne che esterne, come registri di sistema, reti, fonti open-source, community di sicurezza, e fornitori di intelligence. Questi dati possono includere indicatori di compromissione (IoC), tattiche,

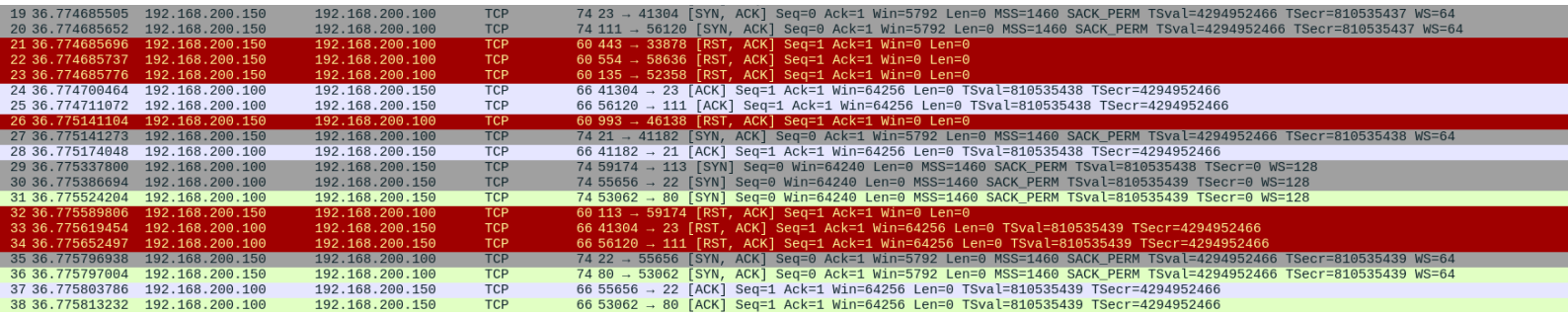
tecniche e procedure (TTP), e informazioni sugli attori delle minacce.
2. **Analisi dei Dati**: Analizzare i dati raccolti per identificare modelli, tendenze e relazioni che possano indicare la presenza di minacce. Questo processo può essere supportato da strumenti di analisi avanzata, algoritmi di machine learning e team di analisti esperti.
3. **Contestualizzazione**: Contestualizzare le informazioni raccolte, fornendo una visione più chiara di come una minaccia specifica potrebbe impattare l'organizzazione. Questo include la valutazione delle vulnerabilità specifiche dell'organizzazione e l'adattamento delle informazioni di intelligence al proprio contesto.
4. **Condivisione delle Informazioni**: Condividere le informazioni rilevanti con i team di sicurezza interni e, in alcuni casi, con partner esterni o consorzi di sicurezza per migliorare la risposta collettiva alle minacce.
5. **Risposta alle Minacce**: Utilizzare le informazioni di threat intelligence per sviluppare e implementare misure di sicurezza proattive e reattive, come il rafforzamento delle difese, l'aggiornamento delle policy di sicurezza, e la conduzione di indagini e attività di mitigazione in caso di incidenti.

Gli **indicatori di compromissione** (IoC, Indicators of Compromise) sono segnali o tracce che suggeriscono che un sistema informatico potrebbe essere stato compromesso o che un attacco informatico potrebbe essere in corso. Questi indicatori possono essere utilizzati dai professionisti della sicurezza informatica per rilevare, analizzare e rispondere alle minacce informatiche in modo efficace.

Per controllare il traffico dei pacchetti, andremo ad utilizzare **Wireshark,** un programma che permette di vedere cosa sta succedendo in una rete informatica. Cattura e mostra i dati che vengono scambiati tra computer e altri dispositivi in tempo reale. È utilizzato per risolvere problemi di rete, migliorare le prestazioni e rilevare attività sospette. In parole semplici, Wireshark è un potente strumento per controllare e analizzare il traffico di rete.



No.	Time	Source	Destination	Protocol	Length	Info
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 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 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 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



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

Possiamo trovare le risposte della macchina attaccata con il flag RST "Reset" nei pacchetti TCP. Quando un pacchetto TCP contiene il flag RST, significa che una delle parti coinvolte nella comunicazione desidera terminare la connessione.

Conclusione

Come possiamo notare, risultano numerose richieste TCP su porte sempre differenti da parte della macchina con indirizzo IP 192.168.200.100 verso la macchina 192.168.200.100 questi potrebbero essere indicatori di compromissione.

Sono presenti sia risposte con il flag [RST, ACK] "Reset" che riposte con il flag [SYN, ACK]. Quando un pacchetto TCP contiene il flag RST, significa che una delle parti coinvolte nella comunicazione desidera terminare la connessione e molto probabilmente la porta è chiusa.

Con il flag [SYN, ACK] invece, andiamo a stabilire che la porta è aperta e la connessione va a buon fine.

Avendo risposte differenti, possiamo dedurre che sia in corso una scansione sulla macchina target.

Consigli

Uno dei principali rimedi per bloccare l'accesso alle porte è quello di configurare una regola Firewall per bloccare l'indirizzo IP dell'attaccante.

Attraverso un Firewall è possibile filtrare il traffico in entrata e/o in uscita su determinate porte, oltre a chiudere porte non essenziali.

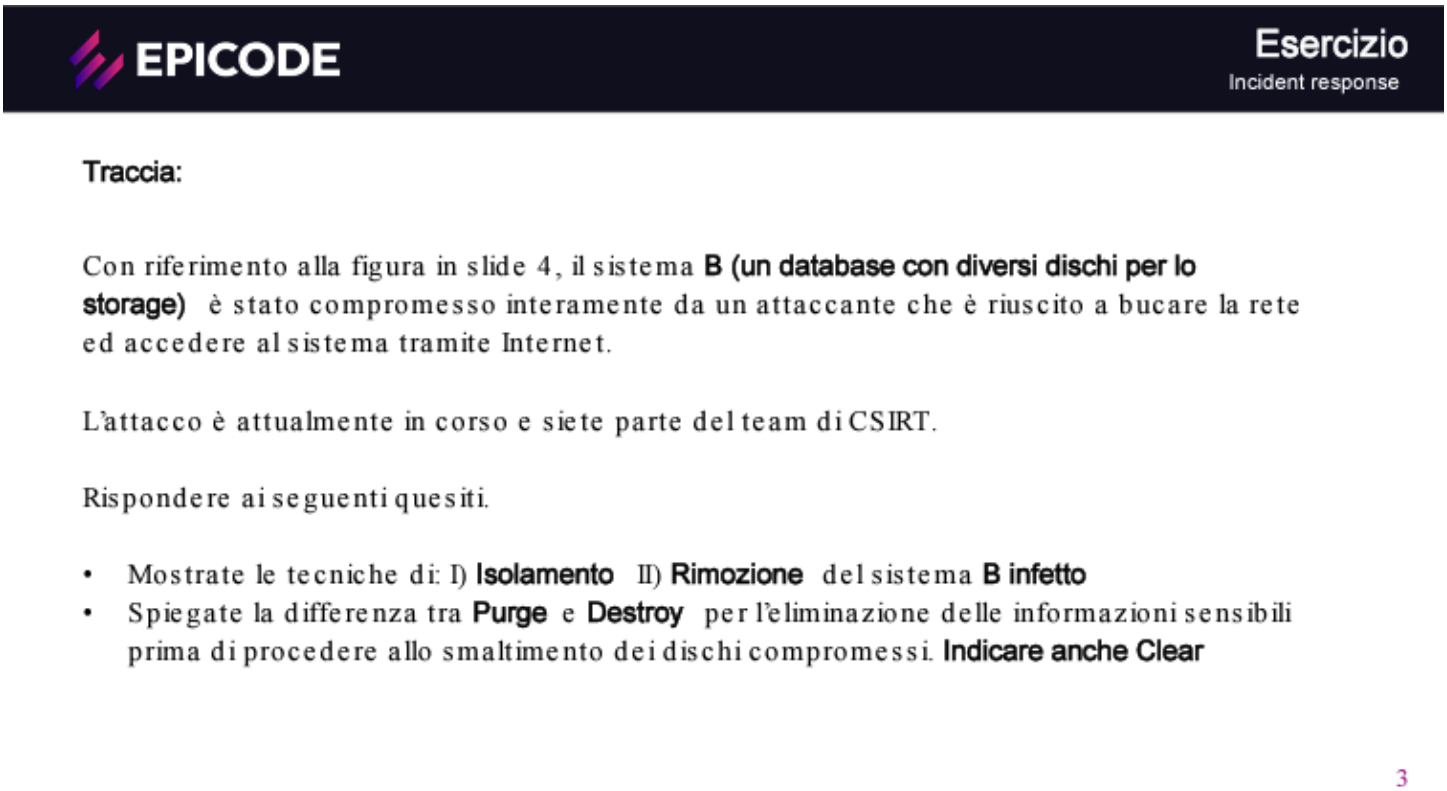
Potremmo utilizzare un IPS per prevenire e bloccare automaticamente azioni non autorizzate.

Potremmo utilizzare una VPN così da limitare l'accesso ai soli utenti autorizzati.

Effettuare regolari valutazioni di sicurezza.

Uno dei possibili rimedi fondamentali è la continua educazione e formazione del personale riguardo le minacce informatiche.

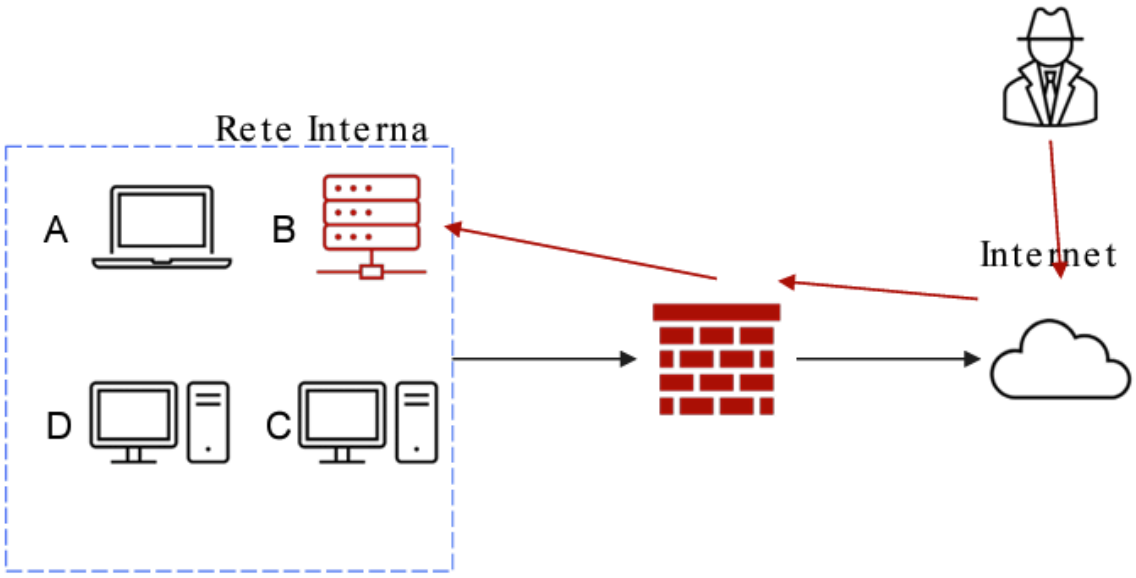
S9-L4



Un **CSIRT** (Computer Security Incident Response Team) è un gruppo di esperti in sicurezza informatica che si occupa di gestire e rispondere agli incidenti di sicurezza, come attacchi informatici, violazioni di dati, malware, e altre minacce.

Cosa fa un CSIRT

1. **Rileva**: Monitora i sistemi informatici per individuare attività sospette o dannose.
2. **Risponde**: Interviene rapidamente per limitare i danni causati dagli incidenti di sicurezza.
3. **Ripristina**: Aiuta a riparare i sistemi compromessi e a ripristinare le operazioni normali.
4. **Previene**: Fornisce consigli e raccomandazioni per migliorare la sicurezza e prevenire futuri incidenti.



RILEVAMENTO:

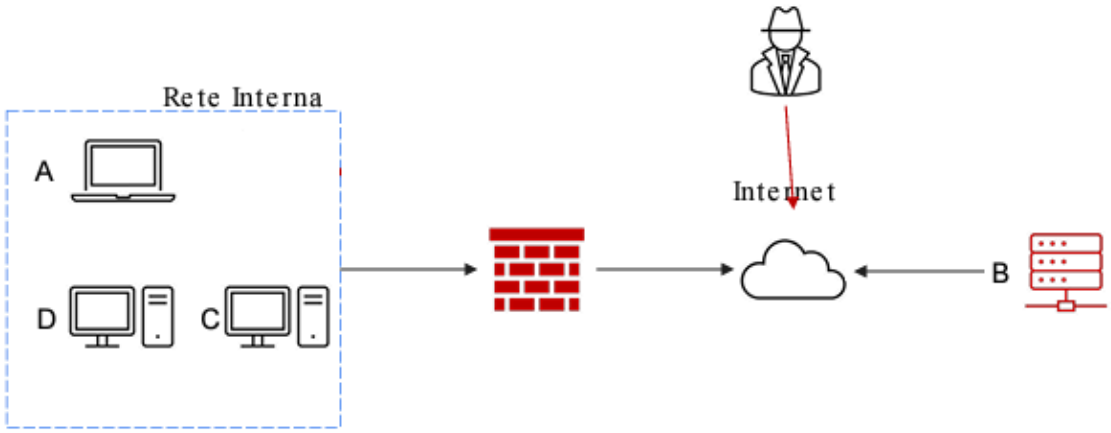
Durante questa fase, il **CSIRT** va a scoprire come è avvenuto l'incidente, quali sistemi ha impattato e quali potrebbero essere i prossimi sistemi a rischio. Una volta completate le valutazioni, il team deve trovare una soluzione per ridurre gli impatti dell'incidente.

Come ci mostra la figura, abbiamo subito un attacco al sistema B che ormai risulta essere compromesso.

ISOLAMENTO:

Il primo step di un piano di risposta agli incidenti è il contenimento del danno causato dall'incidente di sicurezza. Le attività di contenimento hanno lo scopo primario di isolare l'incidente in modo tale che non possa creare ulteriori danni a reti / sistemi.

Andiamo ad isolare il sistema B dalla nostra rete interna, possiamo segmentare la rete suddividendola in diverse LAN o VLAN per creare una rete di quarantena, con le dovute configurazioni per contenere il sistema infetto. Il modo più efficace è quello di isolarlo completamente dalla nostra rete, in quanto l'attaccante è già riuscito a superare il nostro firewall, e sarebbe in grado quindi di infettare di nuovo il sistema, che potrebbe anche avere all'interno eventuali backdoor o malware che andrebbero ad infettare l'intera rete.

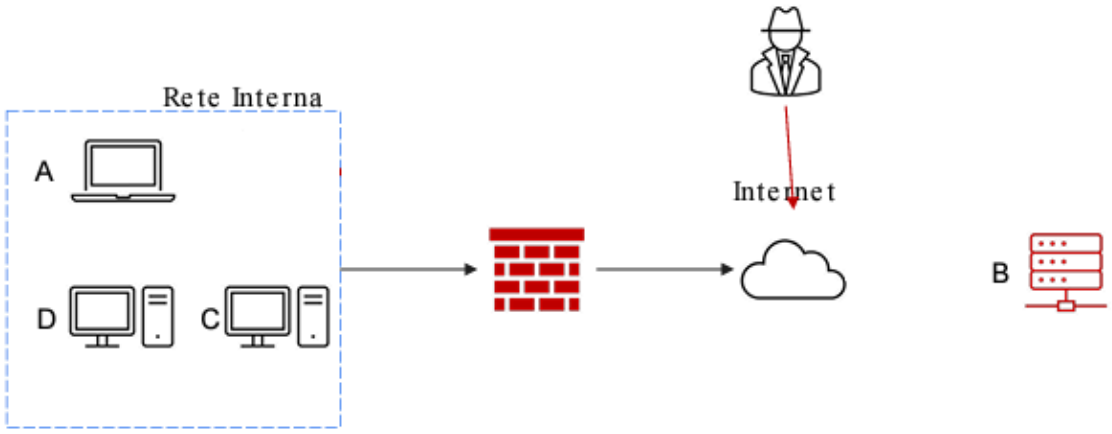


RIMOZIONE:

In questa fase lo scopo è eliminare tutte le attività, le componenti, i processi che restano dell'incidente all'interno della rete o sui sistemi. Questa attività può includere la rimozione di eventuali backdoor installate da un malware, oppure ripulire dischi e chiavette USB compromesse. La fase di rimozione dipende molto da che tipo di incidente di sicurezza è in corso. Una lista dettagliata delle attività da seguire per macro-casistica deve essere elencata nei «playbooks».

Un **playbook** CSIRT (Computer Security Incident Response Team) è un documento dettagliato che contiene le istruzioni e le procedure che un'organizzazione segue per gestire gli incidenti di sicurezza informatica in modo efficiente ed efficace. Il playbook CSIRT fornisce una guida passo dopo passo per identificare, rispondere, mitigare e ripristinare gli incidenti di sicurezza, al fine di limitare i danni e ripristinare la normale operatività il prima possibile. Questi playbook possono essere personalizzati in base alle specifiche esigenze e alle infrastrutture di sicurezza di un'organizzazione.

Se l'isolamento non dovesse essere sufficiente, procederemo con la rimozione del sistema dalla rete sia interna sia internet. In modo che l'attaccante non sia in grado di accedere né alla rete interna né alla macchina infettata.



RIPRISTINO:

La fase di recupero consiste nel tornare alla normale operatività delle applicazioni e servizi. Andiamo a eseguire il recupero dei dati persi, la correzione dei sistemi obsoleti, e la revisione delle politiche di sicurezza per proteggerci meglio in futuro in modo da evitare che lo stesso attacco possa accadere di nuovo.

Dopo un attacco informatico, i sistemi, i server e gli host che sono stati compromessi potrebbero non essere più affidabili. Per renderli nuovamente sicuri ed utilizzabili, ci sono due approcci principali:

1. **Reconstruction (Ricostruzione)**: il recupero delle parti ancora affidabili di un sistema compromesso.
2. **Rebuilding (Ricostruzione totale)**: la ricostruzione completa del sistema compromesso.

Durante la fase di recupero, ci troviamo spesso ad affrontare il problema di cosa fare con un disco o un sistema di memorizzazione compromesso. Prima di decidere se **eliminarlo** o **riutilizzarlo**, dobbiamo essere sicuri che le informazioni siano completamente inaccessibili. In generale, abbiamo tre opzioni:

CLEAR - PURGE - DESTROY:

Clear significa cancellare i dati in modo che non si possano vedere facilmente, ad esempio sovrascrivendoli con altri dati. Si fa quando si vuole riutilizzare il dispositivo nella stessa azienda.

Purge: Significa eliminare i dati in modo sicuro e irreversibile, rendendo molto difficile, se non impossibile, il recupero. È un processo più

approfondito rispetto alla semplice cancellazione.

Destroy: Significa distruggere fisicamente il supporto di memorizzazione (come dischi rigidi o CD) per assicurarsi che i dati non possano essere recuperati in alcun modo.

La differenza è che **clear** è una semplice sovrascrittura dei dati, **purge** è cancellare i dati in modo sicuro rendendo molto difficile recupero e **destroy** è distruggere il supporto fisico che contiene i dati, rendendoli impossibili da recuperare.
