

REPORT S9/L5

Threat Intelligence & IOC

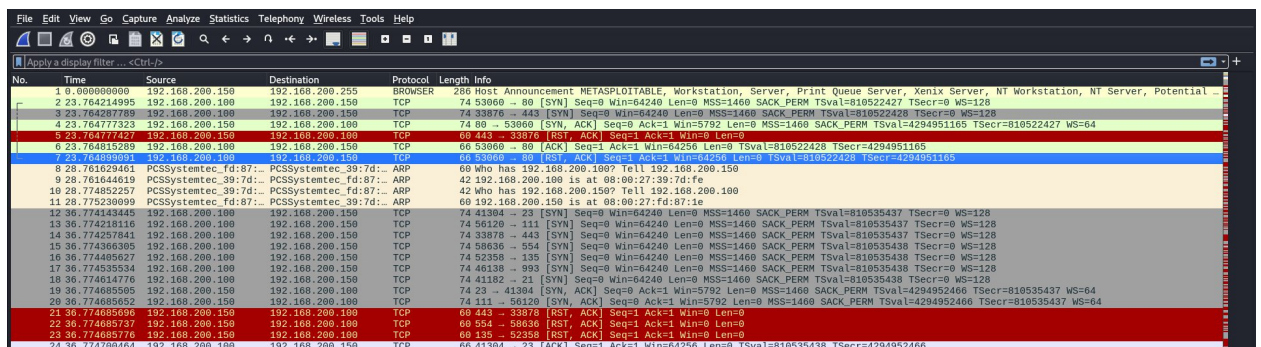
Traccia

Trovate in allegato una cattura di rete effettuata con Wireshark. Analizzate la cattura attentamente e rispondere ai seguenti quesiti:

- Identificare ed analizzare 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 attuale ed eventualmente un simile attacco futuro

Svolgimento

Scarichiamo il file che contiene la cattura dei pacchetti ed apriamolo con Wireshark sulla macchina Kali:



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.200.150	192.168.200.255	BROWSER	286	Host Announcement: METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Potential ...
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53060 -> 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522427 TSecr=0 WS=128
3	23.764267789	192.168.200.100	192.168.200.150	TCP	74	33876 -> 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522428 TSecr=0 WS=128
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	80 -> 53060 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294951165 TSecr=810522427 WS=64
5	23.764777427	192.168.200.150	192.168.200.100	TCP	60	413 -> 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66	53060 -> 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
7	23.764899991	192.168.200.100	192.168.200.150	TCP	60	53060 -> 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
8	28.761629461	PCSSystemtec_fd:87...	PCSSystemtec_39:7d...	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	PCSSystemtec_39:7d...	PCSSystemtec_fd:87...	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	PCSSystemtec_39:7d...	PCSSystemtec_fd:87...	ARP	60	Who has 192.168.200.150? Tell 192.168.200.100
11	28.775230999	PCSSystemtec_fd:87...	PCSSystemtec_39:7d...	ARP	60	192.168.200.150 is at 08:00:27:39:7d:fe
12	36.774434445	192.168.200.100	192.168.200.150	TCP	74	41384 -> 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
13	36.774218116	192.168.200.100	192.168.200.150	TCP	74	56120 -> 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
14	36.774257841	192.168.200.100	192.168.200.150	TCP	74	33878 -> 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
15	36.774365305	192.168.200.100	192.168.200.150	TCP	74	58636 -> 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
16	36.774405627	192.168.200.100	192.168.200.150	TCP	74	52358 -> 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
17	36.774535534	192.168.200.100	192.168.200.150	TCP	74	46138 -> 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
18	36.774614776	192.168.200.100	192.168.200.150	TCP	74	41182 -> 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
19	36.774685505	192.168.200.150	192.168.200.100	TCP	74	23 -> 41384 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
20	36.774685052	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	36.774685050	192.168.200.150	192.168.200.100	TCP	60	443 -> 23 [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	36.774685776	192.168.200.150	192.168.200.100	TCP	60	135 -> 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Dalla schermata principale vediamo quali sono le informazioni principali che ci vengono restituite:

- No: numero dei pacchetti, sono ordinati in base al tempo di arrivo;
- Time: tempo di arrivo del pacchetto;
- Source: l'indirizzo da cui il pacchetto arriva;
- Destination: l'indirizzo a cui è andato il pacchetto;
- Protocol: il tipo di protocollo che sta utilizzando, in questo caso è una richiesta HTTP;
- Length: lunghezza del pacchetto;
- Info: informazioni aggiuntive, in questo caso mostra che è una richiesta GET.

Analisi di un pacchetto

È possibile avere maggiori informazioni sui pacchetti scambiati aprendo la finestra dei dettagli. Ad esempio, del pacchetto numero 7 vediamo che:

Il frame contiene 66 bytes e, se espandiamo, vediamo le informazioni che possono esserci utili, ad esempio, i protocolli presenti nel frame analizzato e la stringa da utilizzare nel filtro per visualizzare pacchetti simili.

```
Wireshark - Packet 7 - progetto.pcapng
▼ Frame 7: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth1, id 0
  Section number: 1
  ▶ Interface id: 0 (eth1)
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug  9, 2022 05:59:23.658716582 EDT
    UTC Arrival Time: Aug  9, 2022 09:59:23.658716582 UTC
    Epoch Arrival Time: 1660039163.658716582
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000083802 seconds]
    [Time delta from previous displayed frame: 0.000083802 seconds]
    [Time since reference or first frame: 23.764899091 seconds]
    Frame Number: 7
    Frame Length: 66 bytes (528 bits)
    Capture Length: 66 bytes (528 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
```

L'indirizzo di destinazione e la sorgente, con modello e mac address:

```
▼ Ethernet II, Src: PCSSystemtec_39:7d:fe (08:00:27:39:7d:fe), Dst: PCSSystemtec_fd:87:1e (08:00:27:fd:87:1e)
  ▶ Destination: PCSSystemtec_fd:87:1e (08:00:27:fd:87:1e)
  ▶ Source: PCSSystemtec_39:7d:fe (08:00:27:39:7d:fe)
  Type: IPv4 (0x0800)
```

Tipo di protocollo utilizzato, flags, Time to live e altre informazioni del **Livello di rete**.

```
▼ Internet Protocol Version 4, Src: 192.168.200.100, Dst: 192.168.200.150
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0xd8f0 (55536)
  ▶ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x4f87 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.200.100
    Destination Address: 192.168.200.150
```

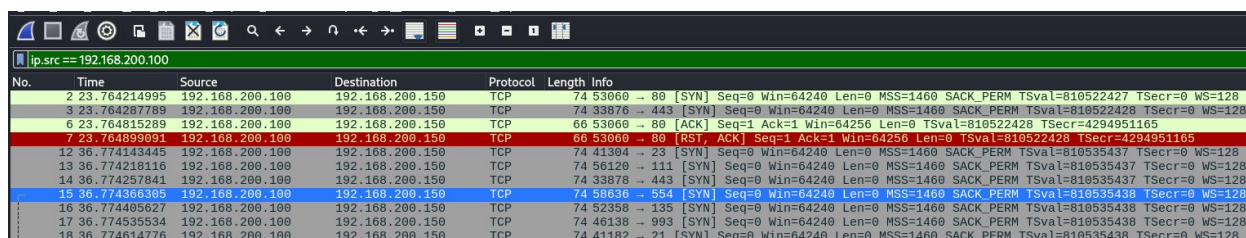
Livello di Trasporto: in questo caso utilizzo TCP, la porta di destinazione è la 80.

```
▼ Transmission Control Protocol, Src Port: 53060, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
  Source Port: 53060
  Destination Port: 80 ←
  [Stream index: 0]
  ▶ [Conversation completeness: Complete, NO_DATA (39)]
  [TCP Segment Len: 0]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 802623072
  [Next Sequence Number: 1 (relative sequence number)]
```

Filtraggio dei pacchetti

Per poter analizzare approfonditamente il traffico e selezionare un'obiettivo bisogna necessariamente utilizzare il sistema di filtraggio. Le stringhe di ricerca sono molte, e ne esistono di ogni tipo.

Seleziono l'indirizzo ip sorgente che mi interessa, tramite la query: **ip.src == 192.168.200.100**



No.	Time	Source	Destination	Protocol	Length	Info
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522427 TSecr=0 WS=128
3	23.764287789	192.168.200.100	192.168.200.150	TCP	74	33876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522428 TSecr=0 WS=128
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
7	23.764899091	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
12	36.774143445	192.168.200.100	192.168.200.150	TCP	74	41304 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
13	36.774218116	192.168.200.100	192.168.200.150	TCP	74	56120 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
14	36.774257841	192.168.200.100	192.168.200.150	TCP	74	33878 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
15	36.774305005	192.168.200.100	192.168.200.150	TCP	74	53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
16	36.774405627	192.168.200.100	192.168.200.150	TCP	74	52358 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
17	36.774535534	192.168.200.100	192.168.200.150	TCP	74	46138 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
18	36.774614776	192.168.200.100	192.168.200.150	TCP	74	41182 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128

Analisi degli IOC (Indicatori di Compromissione)

Prima di procedere con l'analisi dei pacchetti catturati, descriviamo in breve gli **Indicatori di Compromissione (IOC)**. Questi sono dei segnali che indicano attività malevola. Analizzando i pacchetti catturati da Wireshark, possiamo identificare gli IOC più comuni, come ad esempio:

1. Presenza elevata di pacchetti RST (reset), ACK (aknowledge)

Se notiamo una grande quantità di questi pacchetti, possiamo ipotizzare un tentativo deliberato di interrompere o destabilizzare la connessione.

Spiegazione: Gli attacchi che utilizzano pacchetti RST possono essere sfruttati per disconnettere client e server, interrompendo i servizi, proprio come durante un attacco DDoS (Distributed Denial of Service).

39	36.775861964	192.168.200.100	192.168.200.150	TCP	66	41182 → 21 [RST, ACK]
40	36.775975876	192.168.200.100	192.168.200.150	TCP	66	55656 → 22 [RST, ACK]
41	36.776005853	192.168.200.100	192.168.200.150	TCP	66	53062 → 80 [RST, ACK]

2. Presenza elevata di pacchetti SYN

I pacchetti SYN sono il primo passo nella creazione di una connessione TCP Three-way Handshake (SYN - SYN/ACK - ACK). Una quantità elevata di questi pacchetti senza ACK in risposta ci fa pensare ad un attacco SYN Flood.

Spiegazione: Questo attacco è pensato per sovraccaricare il server, esaurendo la tabella delle connessioni, impedendo l'accettazione di nuove connessioni.

42	36.776179338	192.168.200.100	192.168.200.150	TCP	74	50684 → 199 [SYN]
43	36.776233880	192.168.200.100	192.168.200.150	TCP	74	54220 → 995 [SYN]
44	36.776330610	192.168.200.100	192.168.200.150	TCP	74	34648 → 587 [SYN]
45	36.776385694	192.168.200.100	192.168.200.150	TCP	74	33042 → 445 [SYN]
46	36.776402500	192.168.200.100	192.168.200.150	TCP	74	49814 → 256 [SYN]
49	36.776478201	192.168.200.100	192.168.200.150	TCP	74	46990 → 139 [SYN]
50	36.776496366	192.168.200.100	192.168.200.150	TCP	74	33206 → 143 [SYN]
51	36.776512221	192.168.200.100	192.168.200.150	TCP	74	60632 → 25 [SYN]
52	36.776568606	192.168.200.100	192.168.200.150	TCP	74	49654 → 110 [SYN]
53	36.776671271	192.168.200.100	192.168.200.150	TCP	74	37282 → 53 [SYN]
54	36.776720715	192.168.200.100	192.168.200.150	TCP	74	54898 → 500 [SYN]
56	36.776843423	192.168.200.100	192.168.200.150	TCP	74	51534 → 487 [SYN]

3. Tempi estremamente ravvicinati

I pacchetti vengono inviati con tempi estremamente ravvicinati (nell'ordine di millisecondi).

Spiegazione: Questo è indicativo di attacchi lanciati da strumenti automatizzati come script malevoli o software di attacco (es. Metasploit, etc.).

33	36	775619454	192.168.200.100	192.168.200.150	TCP	66 41304	→ 23	[RST, ACK]	
34	36	775652497	192.168.200.100	192.168.200.150	TCP	66 56120	→ 111	[RST, ACK]	
37	36	775803786	192.168.200.100	192.168.200.150	TCP	66 55656	→ 22	[ACK]	Seq=1
38	36	775813232	192.168.200.100	192.168.200.150	TCP	66 53062	→ 80	[ACK]	Seq=1
39	36	775861964	192.168.200.100	192.168.200.150	TCP	66 41182	→ 21	[RST, ACK]	
40	36	775975876	192.168.200.100	192.168.200.150	TCP	66 55656	→ 22	[RST, ACK]	
41	36	776005853	192.168.200.100	192.168.200.150	TCP	66 53062	→ 80	[RST, ACK]	
42	36	776179338	192.168.200.100	192.168.200.150	TCP	74 50684	→ 199	[SYN]	Seq=0
43	36	776233880	192.168.200.100	192.168.200.150	TCP	74 54220	→ 995	[SYN]	Seq=0
44	36	776330610	192.168.200.100	192.168.200.150	TCP	74 34648	→ 587	[SYN]	Seq=0
45	36	776385694	192.168.200.100	192.168.200.150	TCP	74 33042	→ 445	[SYN]	Seq=0
46	36	776402500	192.168.200.100	192.168.200.150	TCP	74 49814	→ 256	[SYN]	Seq=0
49	36	776478201	192.168.200.100	192.168.200.150	TCP	74 46990	→ 139	[SYN]	Seq=0
50	36	776496366	192.168.200.100	192.168.200.150	TCP	74 33206	→ 143	[SYN]	Seq=0
51	36	776512221	192.168.200.100	192.168.200.150	TCP	74 60632	→ 25	[SYN]	Seq=0
52	36	776568606	192.168.200.100	192.168.200.150	TCP	74 49654	→ 110	[SYN]	Seq=0
53	36	776671271	192.168.200.100	192.168.200.150	TCP	74 37282	→ 53	[SYN]	Seq=0
54	36	776720715	192.168.200.100	192.168.200.150	TCP	74 54898	→ 500	[SYN]	Seq=0
56	36	776843423	192.168.200.100	192.168.200.150	TCP	74 51534	→ 487	[SYN]	Seq=0

Ipotesi sui potenziali vettori di attacco

A questo punto ipotizziamo, in base a quanto visto sopra, quali possono essere i vettori di attacco utilizzati. I vettori di attacco sono le tecniche utilizzate dagli hacker per ottenere l'accesso non autorizzato a un dispositivo o ad una rete, sfruttando le vulnerabilità.

1. Compromissione interna (Host compromesso)

Un dispositivo della rete locale (es. 192.168.200.100) potrebbe essere stato infettato da malware ed essere usato per attaccare altri dispositivi nella rete. Questo tipo di compromissione avviene quando un utente scarica file infetti, clicca su link phishing, o quando il dispositivo non è adeguatamente protetto.

Conseguenze: Un host compromesso può fungere da punto di partenza per attacchi più complessi, inclusi DDoS, spionaggio interno o furto di dati.

2. Utilizzo di strumenti di attacco automatizzati

La regolarità e il volume del traffico anomalo indicano l'uso di strumenti automatizzati come Metasploit. Questi strumenti possono essere configurati per eseguire attacchi DoS, SYN Flood o altri exploit noti.

Conseguenze: L'uso di strumenti automatizzati amplifica l'efficacia e la rapidità di un attacco, rendendolo difficile da rilevare e mitigare.

Azioni per ridurre gli impatti dell'attacco e prevenirne di futuri

Alcune delle tecniche di mitigazione utilizzate contro i vettori di attacco si basano su controlli a più livelli e sulla difesa in profondità. Alcune delle misure includono la classificazione e la marcatura dei pacchetti, i tracker della sorgente IP, il controllo del traffico, l'intercettazione TCP, l'instradamento basato su criteri, i firewall, l'intercettazione TCP, il riconoscimento delle applicazioni basate sulla rete, la velocità di accesso impegnata e gli switch di livello 3.

Possiamo suddividere queste tecniche tra quelle di riduzione dell'impatto, andando così a studiare un piano di azione in caso di attacco, e quelle di prevenzione, così da evitare che gli attacchi possano presentarsi / ripetersi in futuro.

Riduzione dell'impatto

1. Bloccare il traffico sospetto tramite il firewall

Configurando delle regole per bloccare il traffico tra 192.168.200.100 e 192.168.200.150.

Se il comportamento malevolo continua, possiamo bloccare interamente il traffico proveniente dall'host infetto, quindi lo isoliamo, e analizzare il dispositivo.

2. Rimuovere il dispositivo 192.168.200.100 dalla rete interna per evitare ulteriori compromissioni.

2.1 Effettuare una scansione antivirus.

2.2 **Abilitare SYN Cookies.** I SYN Cookies sono un meccanismo di protezione contro l'attacco SYN Flood che consente al server di gestire richieste senza riservare risorse fino al completamento dell'handshake.

3. Rate Limiting

Configurare il router o il firewall per limitare il numero di connessioni TCP simultanee da ogni indirizzo IP.

4. Monitoraggio continuo

Utilizzare strumenti di monitoraggio in tempo reale per rilevare e bloccare traffico anomalo.

Azioni preventive

1. Segmentazione della rete

Separare i dispositivi critici in segmenti isolati utilizzando VLAN o zone di sicurezza.

2. Patch di sicurezza

Assicurarsi che tutti i dispositivi nella rete siano aggiornati.

3. Implementazione di un IDS/IPS

Implementare un sistema IDS/IPS per rilevare e prevenire automaticamente attività sospette.

4. Formazione del personale

Educare gli utenti finali su pratiche di sicurezza informatica, come evitare link sospetti e riconoscere tentativi di phishing.

5. Backup e ripristino

Mantenere backup regolari di tutti i dati critici per minimizzare gli impatti in caso di compromissione.

Bonus

Traccia

Siete chiamati a progettare le difese di questo scenario:

Azienda Mak produce dei macchinari e il cliente vuole mettere in sicurezza tutto l'ecosistema. Abbiamo da una parte l'azienda Mak, poi c'è il macchinario e dall'altra parte c'è il cliente che lo utilizza.

Il macchinario è basato su Windows 10, ha porta di rete (usata solo per gli aggiornamenti e la diagnostica remota), porta USB (sono disabilitate le pendrive, ovviamente).

La diagnostica remota è fatta attraverso la VPN del cliente.

Il macchinario è sostanzialmente bloccato. La partizione del sistema operativo non è scrivibile mentre c'è una seconda partizione per il software di gestione del macchinario.

Il software di gestione è realizzato con il linguaggio C99.

Il macchinario è installato nelle varie aziende clienti.

1. Valutare le eventuali vulnerabilità e punti di attacco.
2. Proporre al cliente soluzioni di sicurezza
3. Progettare un sistema di monitoraggio del traffico (Windows 10 è bloccato dalla casa madre, non è modificabile).

Proponete al cliente due soluzioni, una economica (massimo 500 euro) e una più costosa (massimo 2500 euro).

Svolgimento

La valutazione dello scenario proposto esaminerà la configurazione hardware e software, la rete, l'accesso remoto e la sicurezza già implementata.

Valutazione delle vulnerabilità e punti di attacco

1) *Windows 10 come sistema operativo*

L'utilizzo di un sistema operativo che attualmente possiamo giudicare come "vecchio" porta con sé diverse criticità, raggruppabili in due gruppi:

- **Aggiornamenti:** Sebbene il sistema sia bloccato e limitato, è essenziale verificare che gli aggiornamenti di sicurezza di Windows 10 siano regolari. Purtroppo siamo a ridosso della data in cui questo sistema operativo non verrà più supportato, quindi non riceverà aggiornamenti di sistema. Pertanto la mancata applicazione di patch di sicurezza potrebbe rappresentare un rischio.
- **Vulnerabilità:** Nel corso degli anni di attività di Windows 10 sono state rilevate tante vulnerabilità, alcune delle quali non risolte. Pertanto anche se la macchina è "bloccata", potrebbero essere sfruttabili da attacchi esterni (via VPN o rete).

2) *Porta di rete (per aggiornamenti e diagnostica remota)*

Nonostante la porta di rete sia configurata solo per determinati compiti, è molto importante porre attenzione su come queste configurazioni siano state fatte. Ovvero:

- **VPN:** Questa è un canale sicuro, ma deve essere configurata correttamente. Inoltre la gestione delle credenziali di accesso deve essere adeguata. Tutto questo per evitare attacchi come il "man-in-the-middle" che potrebbero compromettere l'integrità della comunicazione e della trasmissione dei dati tramite VPN.
- **Firewall:** È necessario assicurarsi che la rete sia protetta da un firewall e che l'accesso remoto venga consentito solo tramite IP autorizzati.

3) *Porta USB disabilitata*

Disabilitare l'utilizzo delle pendrive è una buona pratica, perché evitiamo l'uso di **Rubber Ducky** o che programmi infetti possano essere trasferiti tramite essa (**Stuxnet** ne è stato un esempio). Bisogna però garantire che non possano essere attaccate altre periferiche USB per scopi malevoli.

4) *Partizione di sistema non scrivibile*

La partizione di sistema non scrivibile aiuta a prevenire modifiche non autorizzate. È necessario assicurarsi che non ci siano vulnerabilità del software di gestione che possano essere sfruttate.

5) *Software di gestione del macchinario (C99)*

C99 (conosciuto precedentemente come C9X) è il nome informale dello standard **ISO/IEC 9899:1999**, una versione precedente del linguaggio di programmazione C. Pertanto poniamo l'attenzione su due punti:

- **Vulnerabilità del software:** potrebbe contenere errori di sicurezza dovuti all'utilizzo di un linguaggio di programmazione standardizzato alla fine degli anni '90.
- **Aggiornamenti del software:** Se il software non è aggiornabile facilmente, il rischio di vulnerabilità potrebbe crescere nel tempo.

Proposte di soluzioni di sicurezza

Soluzione Economica (fino a 500€):

1. Sistema di monitoraggio di rete

È consigliato l'utilizzo di un software di monitoraggio della rete come **Wireshark**. Questi strumenti sono open source e gratuiti pertanto non impattano sulla stima finale del preventivo e si può configurare con dei filtri per identificare attività sospette o non autorizzate.

2. Firewall hardware

Può bloccare attacchi o accessi non autorizzati alla rete. Il firewall dovrebbe essere configurato per permettere solo la connessione dalla VPN e limitare ogni altra forma di comunicazione non necessaria. È anche possibile installare il firewall direttamente sul router in modo da limitare la spesa.

3. Gestione delle credenziali

Sarebbe utile implementare una gestione delle credenziali che prevede l'autenticazione a due fattori e l'utilizzo di un sistema di generazione e gestione delle password per garantire che le credenziali non siano vulnerabili.

4. Aggiornamenti software

Il sistema operativo non sarà più aggiornabile, ma è possibile pianificare gli aggiornamenti per il software di gestione del macchinario così da correggere le potenziali vulnerabilità del programma stesso.

Soluzione Economica (fino a 500€):

1. SIEM

Questi sistemi di monitoraggio offrono funzionalità avanzate di analisi dei log, rilevamento delle intrusioni, e allerta in tempo reale su eventi sospetti.

2. Firewall UTM

Questo tipo di firewall fornisce la protezione contro vari tipi di attacchi e le minacce zero-day. Forniscono anche la gestione del traffico VPN, la protezione da intrusioni e il filtraggio avanzato.

3. Vulnerability Scanning e Penetration Testing

Con questo budget è importante considerare l'esecuzione di un **penetration test** e un **vulnerability scanning** sul software di gestione del macchinario e sull'intero ecosistema. Inoltre si potrebbe implementare **Nessus** per monitorare periodicamente le vulnerabilità.

4. Autenticazione multifattoriale

L'adozione dell'autenticazione multifattoriale su tutte le connessioni remote alla VPN contribuirà a prevenire l'accesso non autorizzato.

In conclusione:

- La soluzione economica si concentra su strumenti software open-source e misure di sicurezza base (monitoraggio del traffico, firewall, e gestione delle credenziali).
- La soluzione costosa fornisce una protezione più robusta e avanzata tramite l'uso di un SIEM, firewall di ultima generazione e analisi periodiche del sistema.

Naturalmente è sempre possibile implementare entrambe le soluzioni, perchè complementari, per aumentare ulteriormente la sicurezza dell'intero ecosistema.