2024

EPICODE

CS0124

REPORT

Week 9 Lesson 4

PREPARED BY : Bruno Falconi

Report sull'Analisi della Cattura di Rete e le Contromisure contro il Tentativo di Attacco

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.

Introduzione:

Durante l'esercizio pratico di oggi, abbiamo analizzato attentamente una cattura di rete effettuata con Wireshark al fine di identificare eventuali indicatori di Compromissione (IOC) e ipotizzare potenziali vettori di attacco. La cattura mostra chiaramente un tentativo di scansione delle porte, presumibilmente eseguito tramite l'uso di un tool come Nmap.

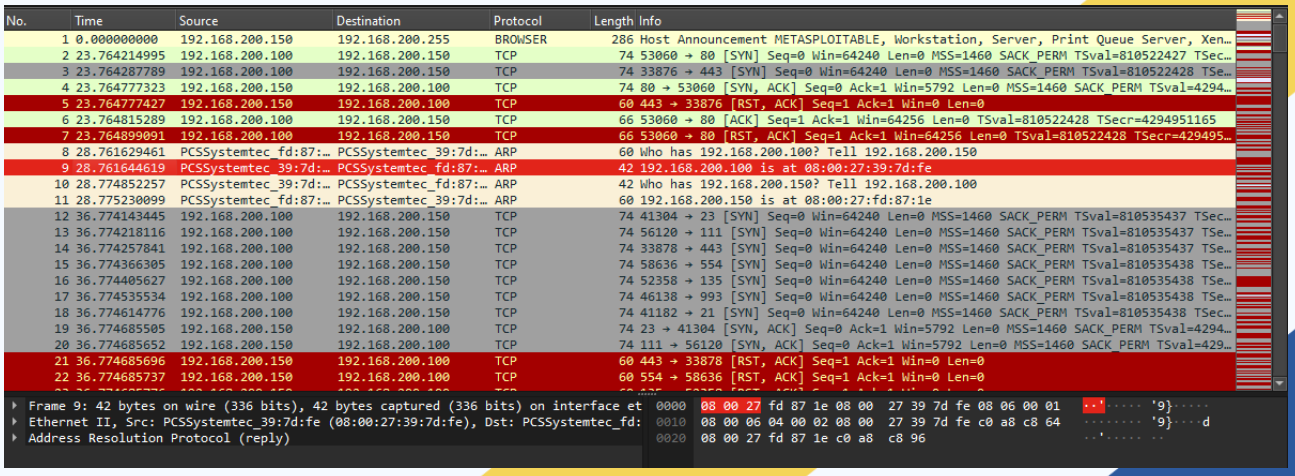
Identificazione degli IOC: Dall'analisi della cattura di rete, sono emersi diversi IOC che suggeriscono un tentativo di scansione delle porte da parte di un potenziale aggressore. Alcuni dei principali IOC identificati includono:

1. **Scansione delle Porte:** La cattura mostra numerosi pacchetti inviati con l'intento di esaminare le porte aperte sul sistema target. Questo comportamento è indicativo di una fase di ricognizione tipica di un attacco informatico.
2. **Indirizzo IP Sorgente:** L'indirizzo IP 192.168.200.100 è stato identificato come l'origine dei pacchetti di scansione delle porte. Questo indirizzo IP potrebbe appartenere all'attaccante che sta conducendo l'operazione.

Ipotesi sui Potenziali Vettori di Attacco:

Basandoci sugli IOC identificati, possiamo ipotizzare diverse modalità attraverso cui l'attaccante potrebbe aver tentato di compromettere il sistema target. Alcune possibili ipotesi includono:

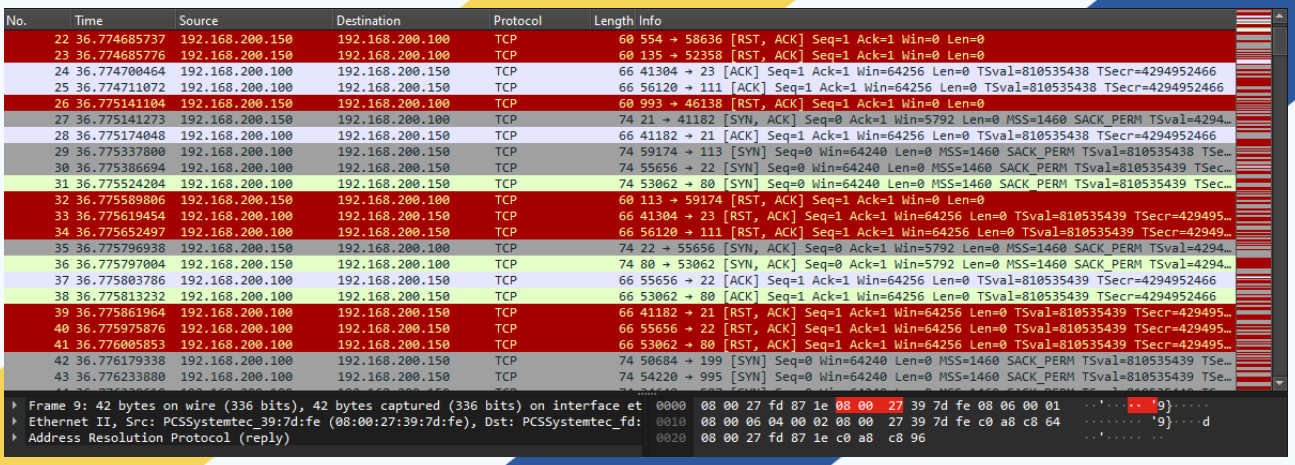
1. **Scansione delle Vulnerabilità:** L'attaccante potrebbe aver utilizzato la scansione delle porte come parte di una strategia più ampia per identificare eventuali vulnerabilità nel sistema target. Una volta individuate, queste vulnerabilità potrebbero essere sfruttate per ottenere accesso non autorizzato al sistema o per lanciare attacchi mirati.
2. **Raccolta di Informazioni:** La scansione delle porte potrebbe essere stata eseguita per raccogliere informazioni sulle risorse di rete disponibili e per mappare la topologia della rete. Queste informazioni potrebbero essere utilizzate per pianificare e eseguire attacchi mirati in futuro.



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, Xen…
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 TSec…
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 TSe…
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=4294…
5	23.764777427	192.168.200.150	192.168.200.100	TCP	60	443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
7	23.764899091	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=429495…
8	28.761629461	PCSSystemtec_fd:87:…	PCSSystemtec_39:7d:…	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	PCSSystemtec_39:7d:…	PCSSystemtec_fd:87:…	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	PCSSystemtec_39:7d:…	PCSSystemtec_fd:87:…	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	28.775230099	PCSSystemtec_fd:87:…	PCSSystemtec_39:7d:…	ARP	60	192.168.200.150 is at 08:00:27:fd:87:1e
12	36.774143445	192.168.200.100	192.168.200.150	TCP	74	41304 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSec…
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 TSe…
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 TSe…
15	36.774366305	192.168.200.100	192.168.200.150	TCP	74	58636 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSe…
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 TSe…
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 TSe…
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 TSec…
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=4294…
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=429…
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

```
▸ Frame 9: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface et
▸ Ethernet II, Src: PCSSystemtec_39:7d:fe (08:00:27:39:7d:fe), Dst: PCSSystemtec_fd:
▸ Address Resolution Protocol (reply)
```

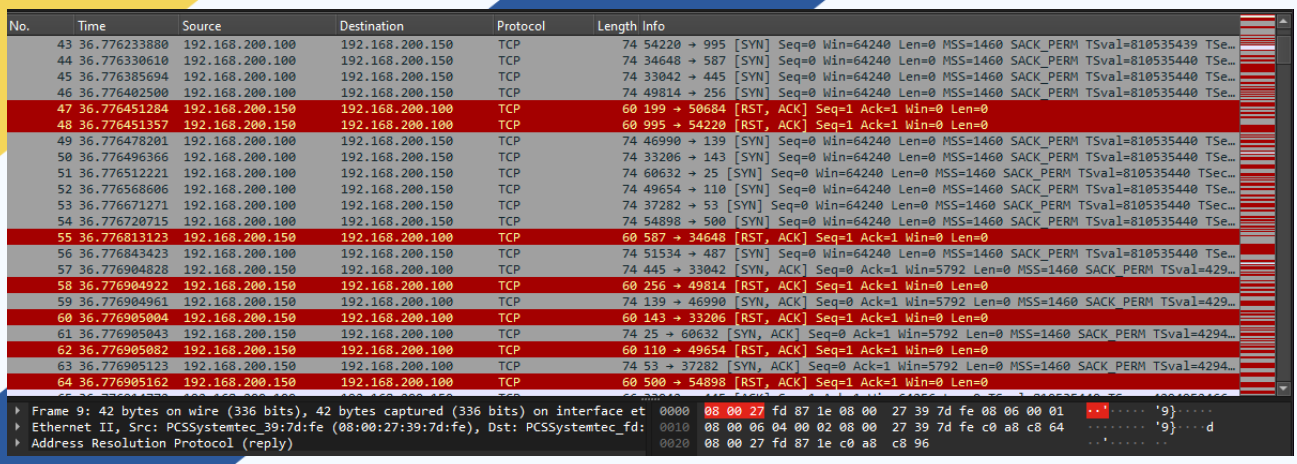
```
0000  08 00 27 fd 87 1e 08 00  27 39 7d fe 08 06 00 01   ··'····· '9}·····
0010  08 00 06 04 00 02 08 00  27 39 7d fe c0 a8 c8 64   ········ '9}····d
0020  08 00 27 fd 87 1e c0 a8  c8 96                     ··'····· ··
```



No.	Time	Source	Destination	Protocol	Length	Info
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=4294…
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 TSe…
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 TSec…
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 TSec…
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=429495…
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=42949…
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=4294…
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=4294…
37	36.775803786	192.168.200.100	192.168.200.150	TCP	66	55656 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
38	36.775813232	192.168.200.100	192.168.200.150	TCP	66	53062 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
39	36.775861964	192.168.200.100	192.168.200.150	TCP	66	41182 → 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=429495…
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=429495…
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=429495…
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 TSval=810535439 TSe…
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 TSval=810535439 TSe…

```
▸ Frame 9: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface et
▸ Ethernet II, Src: PCSSystemtec_39:7d:fe (08:00:27:39:7d:fe), Dst: PCSSystemtec_fd:
▸ Address Resolution Protocol (reply)
```

```
0000  08 00 27 fd 87 1e 08 00  27 39 7d fe 08 06 00 01   ··'····· '9}·····
0010  08 00 06 04 00 02 08 00  27 39 7d fe c0 a8 c8 64   ········ '9}····d
0020  08 00 27 fd 87 1e c0 a8  c8 96                     ··'····· ··
```



No.	Time	Source	Destination	Protocol	Length	Info
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 TSval=810535439 TSe…
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 TSval=810535440 TSe…
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 TSval=810535440 TSe…
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 TSval=810535440 TSe…
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 TSval=810535440 TSe…
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 TSval=810535440 TSe…
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 TSval=810535440 TSec…
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 TSval=810535440 TSe…
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 TSval=810535440 TSec…
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 TSval=810535440 TSe…
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 TSval=810535440 TSe…
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 TSval=429…
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	192.168.200.100	192.168.200.150	TCP	74	139 → 46990 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=429…
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 TSval=4294…
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 TSval=4294…
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

```
▸ Frame 9: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface et
▸ Ethernet II, Src: PCSSystemtec_39:7d:fe (08:00:27:39:7d:fe), Dst: PCSSystemtec_fd:
▸ Address Resolution Protocol (reply)
```

```
0000  08 00 27 fd 87 1e 08 00  27 39 7d fe 08 06 00 01   ··'····· '9}·····
0010  08 00 06 04 00 02 08 00  27 39 7d fe c0 a8 c8 64   ········ '9}····d
0020  08 00 27 fd 87 1e c0 a8  c8 96                     ··'····· ··
```

Contromisure Consigliate:

Per mitigare gli impatti di un potenziale attacco basato sulla scansione delle porte, si consiglia di adottare le seguenti contromisure:

1. **Filtraggio delle Porte tramite Firewall:** Si consiglia di configurare un firewall per filtrare il traffico in ingresso e in uscita, limitando l'accesso solo alle porte necessarie per le operazioni legittime del sistema. Questo impedirà all'attaccante di determinare facilmente lo stato delle porte e renderà più difficile per loro identificare potenziali punti di ingresso nel sistema.

2. **Blocco dell'Indirizzo IP dell'Attaccante:** È consigliabile bloccare l'indirizzo IP sorgente dell'attaccante (192.168.200.100) utilizzando misure di sicurezza come il blocco IP sul firewall o sulla configurazione del router. Questa azione impedirà all'attaccante di continuare i propri tentativi di scansione delle porte e ridurrà il rischio di compromissione del sistema.

Conclusioni:

In conclusione, l'analisi della cattura di rete ha rivelato un tentativo di scansione delle porte da parte di un attaccante. È fondamentale adottare misure di sicurezza adeguate, come il filtraggio delle porte tramite firewall e il blocco degli indirizzi IP sospetti, per proteggere il sistema da potenziali attacchi informatici e ridurre gli impatti delle minacce sulla sicurezza dei dati e delle risorse di rete.