



THREAT INTELLIGENCE & IOC

TRAFFICO DI RETE E IDENTIFICAZIONE DEGLI INDICATORI DI COMPROMISSIONE (IOC)

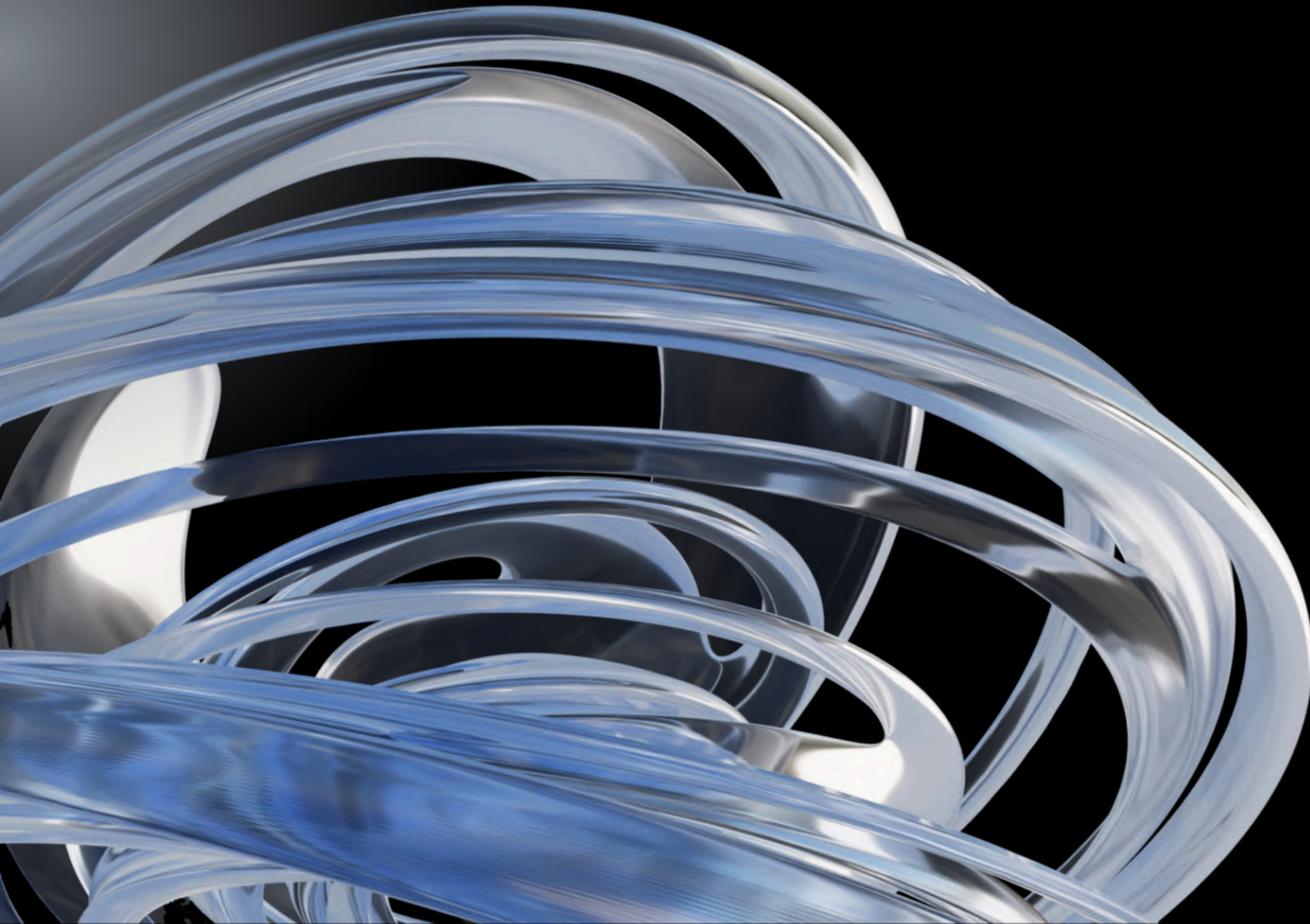
INDICE

- Introduzione
- Threat Intelligence e Indicatori di Compromissione (IOC)
- Analisi del Traffico di Rete
- Ipotesi sui Potenziali Vettori di Attacco
- Approfondimenti Tecnici
- Azioni di Mitigazione e Prevenzione
- Conclusioni

INTRODUZIONE ALLA THREAT INTELLIGENCE

La Threat Intelligence è l'insieme di informazioni che ci aiutano a comprendere, prevenire e rispondere a potenziali minacce alla sicurezza informatica. È come avere un sistema di allarme che monitora costantemente la rete per individuare segnali di pericolo. L'obiettivo è raccogliere dati su:

- Minacce note: Attacchi già identificati in passato.
- Modelli sospetti: Attività inusuali che potrebbero nascondere minacce.
- Indicatori di Compromissione (IOC): Prove che un attacco è in corso o è già avvenuto.

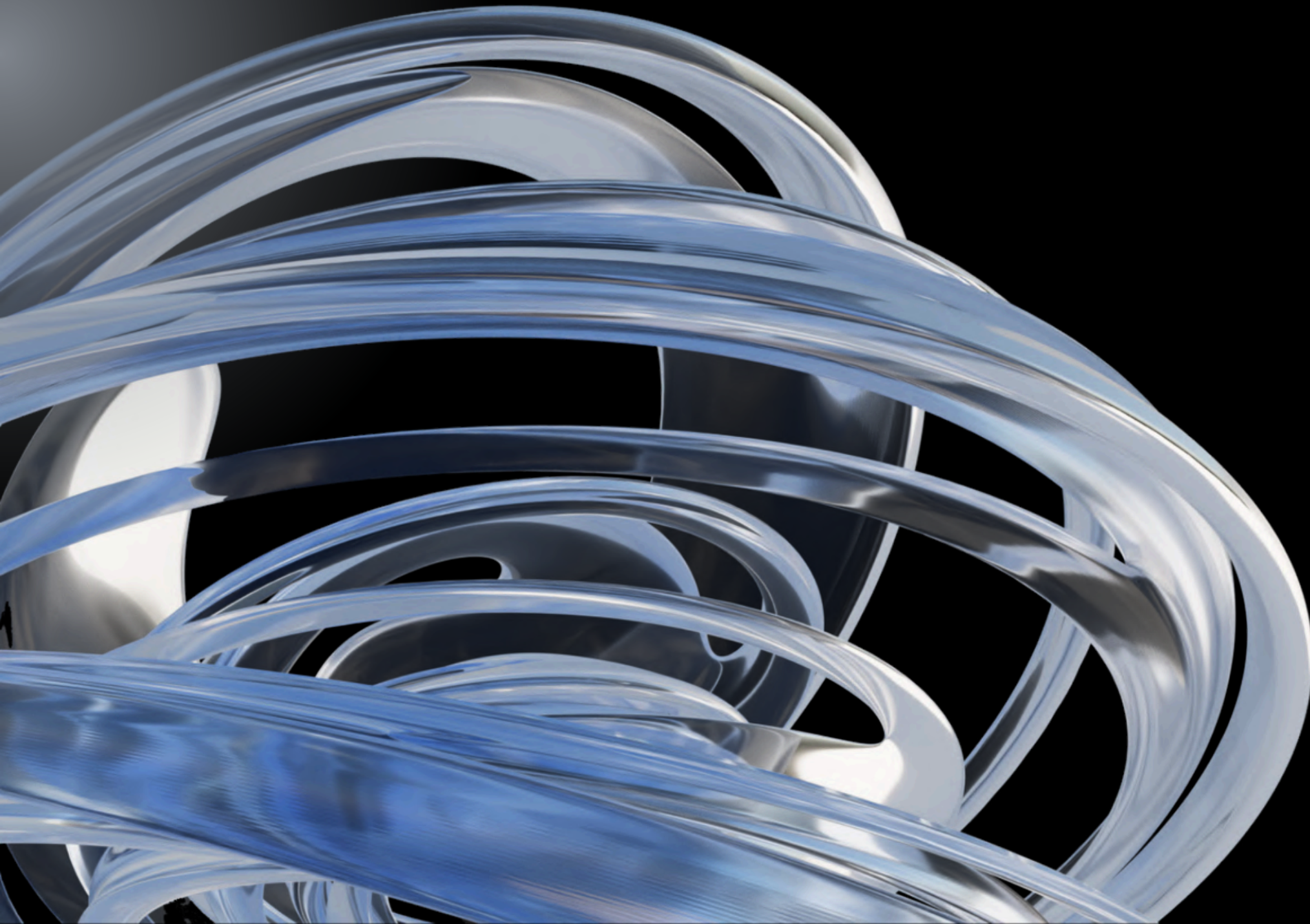


COSA SONO GLI IOC?

Gli IOC (Indicatori di Compromissione) sono segnali che indicano la presenza di attività sospette o malevole nella rete. Possono essere di vari tipi:

- Indirizzi IP sospetti: Collegamenti da o verso indirizzi IP non riconosciuti o noti per essere associati a minacce.
- Schemi di traffico anomali: Un volume insolitamente alto di dati o connessioni a porte non standard.
- Eventi di sistema sospetti: File modificati o processi inattesi.

Individuare e analizzare gli IOC è fondamentale per proteggere una rete aziendale da attacchi in corso o futuri.



OBIETTIVO DELL'ESERCIZIO

Abbiamo analizzato un file di cattura del traffico di rete utilizzando Wireshark, un potente strumento per il monitoraggio della rete. L'obiettivo è stato:

- Identificare eventuali IOC nel traffico di rete.
- Formulare ipotesi sui possibili vettori di attacco utilizzati.
- Proporre azioni concrete per mitigare l'attacco attuale e prevenire futuri attacchi simili.

ESEMPIO 1

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=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 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	60	443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
7	23.764899091	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
8	28.761629461	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	36.774685505	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=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	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	36.774708464	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=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 TS

ANALISI GENERALE DEL TRAFFICO TCP

Sulla base di questo screenshot, possiamo fare alcune osservazioni e analisi preliminari per comprendere meglio il traffico di rete catturato.

Osservazioni Generali:

1. Traffico TCP

- La maggior parte dei pacchetti nello screenshot è costituita da pacchetti TCP, suggerendo che la comunicazione applicativa tra dispositivi è prevalente nella rete.
- I pacchetti TCP possono includere vari flag, come SYN (inizio connessione), ACK (riconoscimento), e RST (reset), che rappresentano le diverse fasi del processo di comunicazione TCP.

2. Destinazioni Simili

- La maggior parte dei pacchetti è diretta allo stesso indirizzo IP: 192.168.100.100. Questo suggerisce che tale indirizzo possa appartenere a un server centrale o a un dispositivo critico nella rete, che riceve traffico significativo.

3. Flags TCP

- La presenza di pacchetti con flag SYN, ACK, e RST indica che nello screenshot sono rappresentate le fasi iniziali di nuove connessioni TCP, riconoscimenti delle stesse, e potenziali chiusure anomale (RST). Questo è utile per identificare attività sospette o problemi di connessione.

4. Lunghezza dei Pacchetti

- La lunghezza dei pacchetti varia, come ci si aspetta in una comunicazione di rete normale. Pacchetti più piccoli (tipicamente richieste) e pacchetti più grandi (contenenti dati) indicano un mix di scambio di informazioni.

5. Colori dei Pacchetti

- Wireshark utilizza colori differenti per distinguere i protocolli e lo stato delle connessioni. I colori nello screenshot possono indicare, ad esempio, pacchetti TCP con flag specifici, pacchetti ICMP o ARP, o traffico con errori.

POSSIBILI SCENARI

Basandoci sui dati osservati, possiamo ipotizzare alcune situazioni che potrebbero spiegare il traffico:

1. Scansione di Porte

- La presenza di numerosi pacchetti SYN potrebbe indicare una scansione di porte in corso. Un attaccante invia pacchetti SYN a un intervallo di porte per identificare quali sono aperte e quali servizi sono attivi sulla macchina 192.168.100.100. Questo è un passo comune nella fase di ricognizione di un attacco.

2. Attacco DoS

- Se il volume di traffico verso l'indirizzo IP 192.168.100.100 è insolitamente alto, potrebbe trattarsi di un tentativo di attacco Denial-of-Service (DoS).

3. Comunicazione Normale

- Potrebbe trattarsi di una comunicazione legittima tra dispositivi. Ad esempio, un client potrebbe accedere a un server per richiedere dati o servizi. Senza un volume sospetto o pattern anomali, il traffico TCP visto nello screenshot potrebbe essere del tutto normale.

ESEMPIO 2

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

ANALISI GENERALE DEL TRAFFICO TCP

1. Traffico TCP Predominante

- La maggior parte del traffico nello screenshot è costituita da pacchetti TCP, che indicano una comunicazione applicativa attiva tra dispositivi nella rete.
- Il protocollo TCP è utilizzato per garantire una trasmissione affidabile di dati, gestendo errori e sequenze.

2. Destinazione Comune

- Tutti i pacchetti sono indirizzati a un unico IP, 192.168.200.100, suggerendo che tale indirizzo appartenga a un dispositivo critico, come un server, che gestisce richieste centralizzate da altri dispositivi.

3. Flags TCP

- I pacchetti contengono diversi flag TCP, tra cui SYN (richiesta di connessione), ACK (riconoscimento della connessione), e RST (reset della connessione). Questi flag rappresentano:
 - SYN: Tentativo di iniziare una nuova connessione TCP.
 - ACK: Conferma di ricezione o di avvenuta connessione.
 - RST: Interruzione o reset di una connessione esistente.

4. Lunghezza dei Pacchetti

- I pacchetti hanno lunghezze variabili, un comportamento normale che riflette la trasmissione di dati applicativi (di lunghezza maggiore) alternati a pacchetti di controllo.

5. Numeri di Sequenza e di Riconoscimento

- I numeri di sequenza e di riconoscimento aumentano progressivamente, indicando che la comunicazione TCP è attiva e si evolve. Questo è un segnale di una conversazione in corso tra il mittente e il destinatario.

POSSIBILI SCENARI

Le seguenti ipotesi possono essere formulate in base al traffico osservato:

1. Continuazione di una Connessione Precedente

- Potrebbe trattarsi della continuazione di una connessione TCP già stabilita. I numeri di sequenza progressivi confermano uno scambio regolare di dati.

2. Inizio di una Nuova Connessione

- I pacchetti con flag SYN potrebbero rappresentare nuovi tentativi di connessione TCP. Se ci sono molte richieste SYN senza risposte SYN/ACK, potrebbe essere un sintomo di un attacco SYN flood.

3. Scansione di Porte

- Se nello screenshot sono presenti tentativi di connessione a numerose porte, potrebbe essere in corso una scansione di porte. Un attaccante utilizza questa tecnica per scoprire quali servizi sono in esecuzione sull'indirizzo 192.168.200.100.

4. Attacco Mirato

- Qualora i pacchetti contenessero dati anomali, come exploit noti o payload specifici, potrebbe trattarsi di un attacco mirato. Questi attacchi tentano di sfruttare vulnerabilità sul server di destinazione.

IPOTESI SUI VETTORI DI ATTACCO

Scansione di Porte (Port Scanning)

Una scansione di porte è un'operazione in cui un attaccante esamina il sistema di destinazione per individuare porte aperte che potrebbero essere vulnerabili. I pacchetti SYN analizzati nel traffico di rete sono un chiaro indicatore di una scansione di porte. Questi pacchetti vengono inviati a diverse porte di destinazione in modo da testare quali sono aperte, e successivamente l'attaccante utilizza quelle porte per tentare di accedere ai servizi vulnerabili.

Potenziale Impatto:

- La scansione di porte in sé potrebbe non compromettere direttamente il sistema, ma espone i servizi disponibili al rischio di exploit.
- Se l'attaccante riesce a identificare una porta aperta su un servizio vulnerabile, può poi eseguire exploit specifici per prendere il controllo del sistema.

Attacco Denial of Service (DoS):

Nel traffico di rete, abbiamo osservato numerosi pacchetti SYN che, se inviati ripetutamente in un breve lasso di tempo, possono esaurire le risorse del server o dei dispositivi di rete, causando un SYN Flood, che è un tipo di attacco DoS.

Potenziale Impatto:

- La vittima potrebbe subire interruzioni nei servizi, con un'impossibilità di accedere alle risorse online.
- In alcuni casi, se l'attacco è prolungato, potrebbe anche danneggiare fisicamente l'infrastruttura di rete, rallentando l'intero sistema.

IPOTESI SUI VETTORI DI ATTACCO

ARP Spoofing (ARP Cache Poisoning)

L'analisi dei pacchetti ARP suggerisce che potrebbe esserci un tentativo di ARP Spoofing. In questo tipo di attacco, l'aggressore invia messaggi ARP falsificati sulla rete, associando l'indirizzo MAC del suo dispositivo all'indirizzo IP di un altro dispositivo. Questo permette all'attaccante di intercettare il traffico destinato ad altri dispositivi sulla rete, con conseguenti rischi di man-in-the-middle (MITM) o perdita di riservatezza.

Potenziale Impatto:

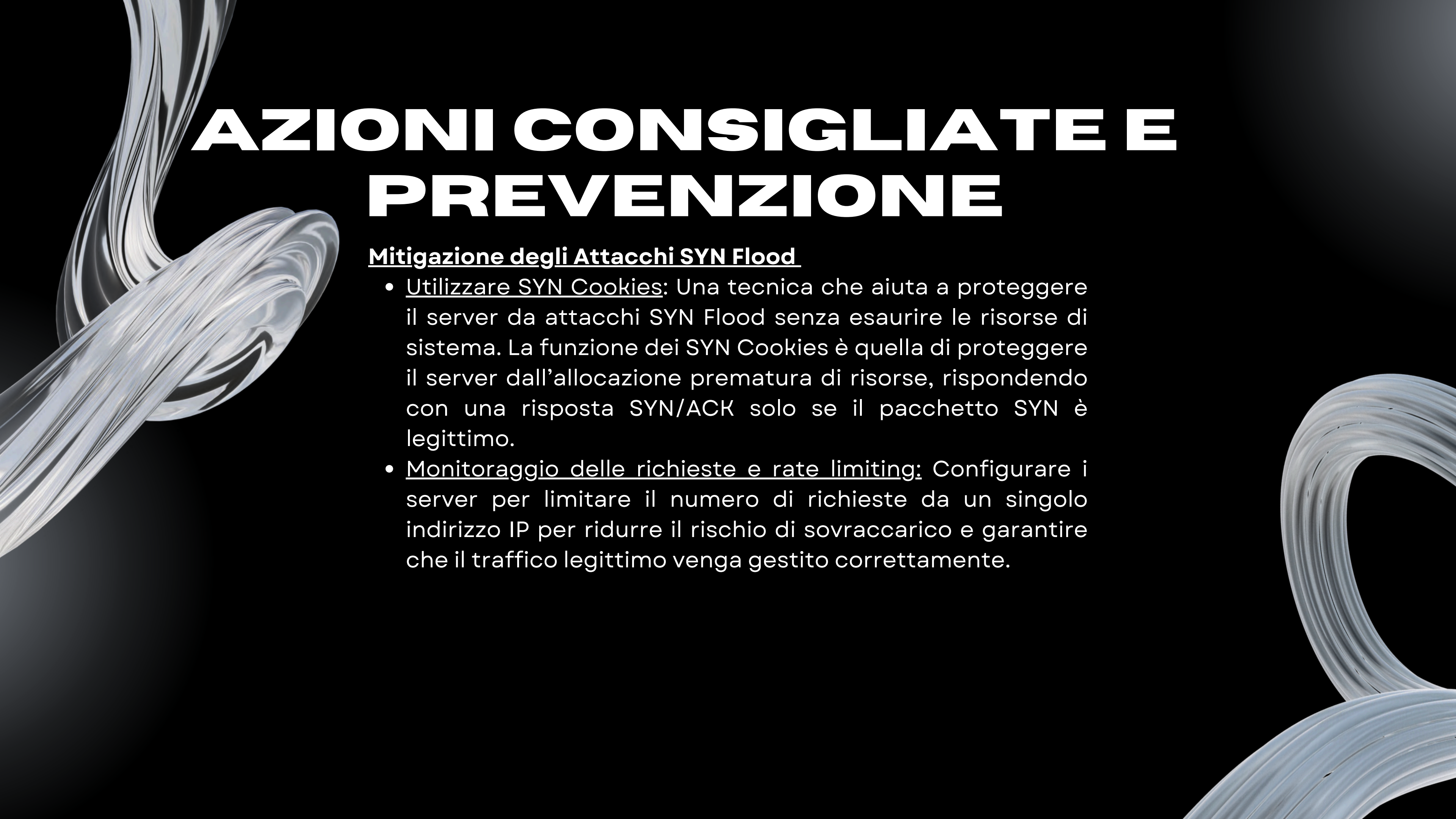
- Intercettazione e manipolazione del traffico di rete.
- Furto di dati sensibili come credenziali di accesso o informazioni private.
- Possibilità di lanciare attacchi ulteriori sfruttando l'accesso alle comunicazioni.

Attacchi Mirati (Exploitation)

Gli attacchi mirati sono quei tipi di attacchi che sfruttano specifiche vulnerabilità nei software o nei dispositivi della rete per ottenere accesso non autorizzato. Se i pacchetti TCP o UDP analizzati contengono exploit di vulnerabilità note, potrebbero essere tentativi di attacchi mirati come l'iniezione di codice o l'esecuzione di comandi remoti.

Potenziale Impatto:

- Accesso non autorizzato a sistemi aziendali e risorse critiche.
- Possibilità di eseguire operazioni dannose, come l'installazione di malware o il furto di dati riservati.
- Compromissione della rete e accesso a più dispositivi interconnessi.



AZIONI CONSIGLIATE E PREVENZIONE

Mitigazione degli Attacchi SYN Flood

- Utilizzare SYN Cookies: Una tecnica che aiuta a proteggere il server da attacchi SYN Flood senza esaurire le risorse di sistema. La funzione dei SYN Cookies è quella di proteggere il server dall'allocazione prematura di risorse, rispondendo con una risposta SYN/ACK solo se il pacchetto SYN è legittimo.
- Monitoraggio delle richieste e rate limiting: Configurare i server per limitare il numero di richieste da un singolo indirizzo IP per ridurre il rischio di sovraccarico e garantire che il traffico legittimo venga gestito correttamente.

DIFESA CONTRO ARP SPOOFING

- Implementazione di Static ARP Entries: Configurare la tabella ARP dei dispositivi di rete per associare staticamente gli indirizzi IP ai rispettivi indirizzi MAC. Questo impedisce ai dispositivi di aggiornare automaticamente la loro cache ARP con informazioni errate.
- Monitoraggio ARP con strumenti di sicurezza: Utilizzare strumenti come arpswatch o Wireshark per rilevare e allertare quando un dispositivo sta cercando di inviare pacchetti ARP falsificati sulla rete.
- Protocollo di autenticazione tramite 802.1X: Implementare il controllo dell'accesso alla rete tramite 802.1X, per garantire che solo i dispositivi legittimi possano accedere alla rete interna e impedire attacchi come ARP Spoofing.

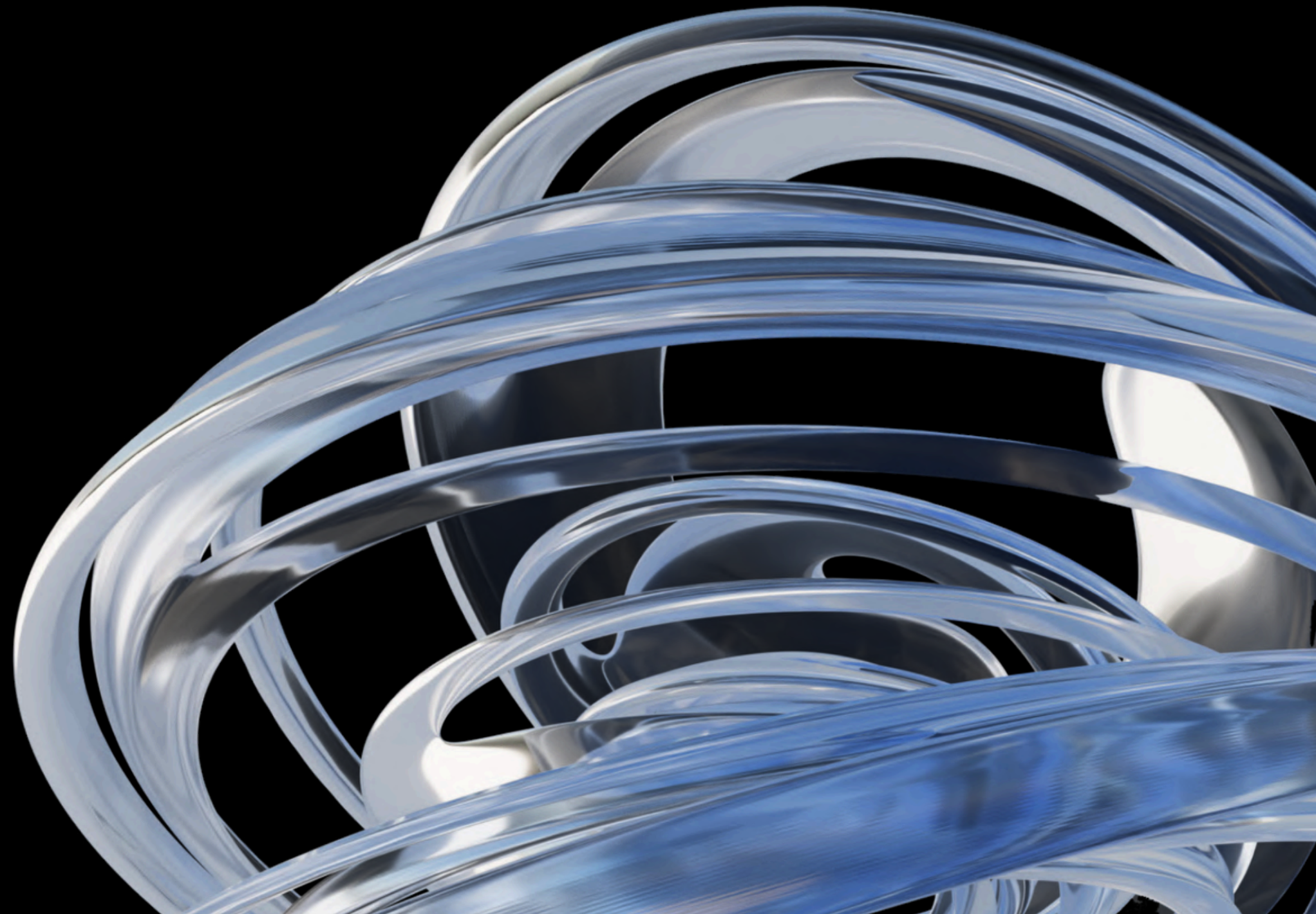


PREVENZIONE DEGLI ATTACCHI MIRATI

- Aggiornamento regolare dei sistemi: Le vulnerabilità nel software sono una delle principali vie di attacco per gli hacker. Assicurarsi che tutti i sistemi e le applicazioni siano costantemente aggiornati per correggere le vulnerabilità conosciute.
- Utilizzo di Firewall e IDS/IPS: Installare e configurare correttamente firewall e sistemi di rilevamento/prevenzione delle intrusioni (IDS/IPS), che possano identificare e bloccare tentativi di exploit basati su vulnerabilità note.
- Formazione continua e simulazioni di attacchi: Sottoporre il personale IT e gli utenti a corsi di formazione periodici sulla sicurezza informatica e condurre esercitazioni di risposta a incidenti per testare la prontezza dell'organizzazione.

CONCLUSIONI

L'analisi del traffico di rete ha portato alla luce possibili indicatori di compromissione (IOC) che suggeriscono attacchi attivi come la scansione di porte, un potenziale SYN Flood e un possibile ARP Spoofing. Ognuno di questi scenari è una minaccia significativa per la sicurezza della rete aziendale e potrebbe portare a gravi conseguenze come la perdita di disponibilità, la compromissione dei dati o l'intercettazione delle comunicazioni.






RACCOMANDAZIONI

- È fondamentale implementare misure di sicurezza proattive, come l'uso di SYN Cookies, monitoraggio ARP e soluzioni anti-DoS per contrastare questi attacchi.
- Gli aggiornamenti regolari, la formazione del personale e la configurazione di sistemi IDS/IPS sono passi cruciali per prevenire gli attacchi mirati e proteggere i dati sensibili.
- Infine, è importante testare regolarmente le difese della rete attraverso simulazioni di attacco per garantire che l'infrastruttura possa resistere a minacce future.

L'adozione di queste tecniche di prevenzione, combinata con un monitoraggio continuo, può ridurre significativamente il rischio di compromissioni e garantire un'infrastruttura di rete sicura e resiliente.

The background is a dark gradient. On the left, there is a dynamic, flowing liquid-like shape in shades of light blue and white, resembling a splash or a ribbon. On the right, there is a stack of several thin, light blue rings or coils, stacked together.

Non aspettare che un attacco
accada per reagire. La
preparazione oggi protegge la tua
rete domani.

A flowing white fabric, possibly a dress or a piece of art, is shown against a black background. The fabric is draped and folded, creating a sense of movement and elegance. It occupies the left side of the frame, with its folds and curves catching the light.

GRAZIE

AMATO SARA
29/11/2024 S9 L5