

Analisi e report del traffico di rete

Cattura effettuata con Wireshark

Introduzione

Gli Indicatori di Compromissione (IOC) sono evidenze che suggeriscono la presenza di un'attività malevola o di un attacco informatico in corso. Analizzando i pacchetti catturati con Wireshark, possiamo identificare vari IOC che possono indicare tentativi di attacco o comportamenti sospetti

Analisi dei pacchetti

Durante l'analisi del traffico di rete con Wireshark, sono stati osservati numerosi pacchetti TCP con flag SYN inviati da un IP (192.168.200.100) verso un altro IP (192.168.200.150), seguiti da risposte con flag RST. Tuttavia, su alcune porte specifiche, la risposta ai pacchetti SYN è positiva, con pacchetti SYN-ACK seguiti da pacchetti ACK, completando così l'handshake TCP a tre vie.

Per prima cosa andando ad analizzare i primi pacchetti della cattura

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, ...
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
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	80 → 33876 [ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294951165 TSecr=...
5	23.764777427	192.168.200.150	192.168.200.100	TCP	60	443 → 33876 [RST, ACK] Seq=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	PCSSystemtec_fd:87:...	PCSSystemtec_89:7d:...	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_89:7d:...	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 08:00:27:39:7d:fe

Possiamo notare dei pacchetti **ARP** seguiti da dei messaggi, "who has 192.168.200.100 tell 192.168.200.150" e "who has 192.168.200.150 tell 192.168.200.100" questi messaggi indicano che i dispositivi stanno cercando di risolvere gli indirizzi **IP** in indirizzi **MAC** per stabilire la comunicazione. Questo è un comportamento normale nelle reti locali e rappresenta il funzionamento di base di ARP per la risoluzione degli indirizzi.

Successivamente analizzando gli indirizzi ip 192.168.200.100 e 192.168.200.150 si può dedurre che appartengono alla stessa rete. La subnet mask utilizzata è /24 (255.255.255.0), che significa che i primi 24 bit degli indirizzi IP sono utilizzati per identificare la rete e gli ultimi 8 bit sono utilizzati per identificare gli host.

Siccome gli indirizzi rientrano nel range degli IP validi (da 192.168.200.1 a 192.168.200.254) significa che si trovano nella stessa rete.

Analizzando i successivi pacchetti si può osservare il seguente comportamento:

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	36.774366305	192.168.200.100	192.168.200.150	TCP	74 58630 → 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 → 992 [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	192.168.200.100	192.168.200.150	TCP	74 23 → 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=0
20	36.774685652	192.168.200.100	192.168.200.150	TCP	74 111 → 56120 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=0
21	36.774685696	192.168.200.150	192.168.200.100	TCP	60 443 → 55070 [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	36.774709464	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	36.774711872	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=0
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	36.775337000	192.168.200.100	192.168.200.150	TCP	74 38174 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
133	36.780325837	192.168.200.100	192.168.200.150	TCP	74 37252 → 11 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
134	36.780346429	192.168.200.100	192.168.200.150	TCP	74 36548 → 739 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
135	36.780409818	192.168.200.100	192.168.200.150	TCP	74 38866 → 55 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
136	36.780427899	192.168.200.100	192.168.200.150	TCP	74 52136 → 999 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
137	36.780472830	192.168.200.100	192.168.200.150	TCP	74 38022 → 317 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
138	36.780490897	192.168.200.100	192.168.200.150	TCP	60 266 → 40822 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
139	36.780577880	192.168.200.150	192.168.200.100	TCP	60 11 → 37252 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
140	36.780577981	192.168.200.150	192.168.200.100	TCP	60 235 → 40648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
141	36.780578026	192.168.200.150	192.168.200.100	TCP	60 739 → 36548 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
142	36.780578074	192.168.200.150	192.168.200.100	TCP	60 999 → 52136 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
143	36.780578119	192.168.200.150	192.168.200.100	TCP	60 317 → 38022 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
144	36.780578158	192.168.200.150	192.168.200.100	TCP	
145	36.780578198	192.168.200.150	192.168.200.100	TCP	

Numerosi Pacchetti **SYN**:

- Pacchetti con flag SYN inviati da 192.168.200.100 verso 192.168.200.150 su diverse porte.
- Questo potrebbe indicare una scansione delle porte, dove un attaccante tenta di trovare porte aperte e servizi attivi.

Risposte con flag **RST, ACK**:

- L'IP 192.168.200.150 risponde con pacchetti RST, ACK su alcune porte, indicando che queste porte sono chiuse.

Completamento di **Handshake TCP** su alcune porte:

- Su alcune porte specifiche, l'IP 192.168.200.150 risponde con pacchetti **SYN-ACK** e successivamente 192.168.200.100 completa l'handshake TCP con un pacchetto **ACK**.
- Questo indica che le connessioni su queste porte sono state stabilite correttamente, suggerendo che i servizi su queste porte sono attivi e accettano connessioni.

Identificazione degli IOC

Scansione delle Porte:

- La presenza di numerosi pacchetti SYN su diverse porte, con risposte miste di SYN-ACK e RST, è un chiaro indicatore di una scansione delle porte. Questo tipo di attività viene utilizzato per identificare quali servizi sono attivi su un host e quali porte sono aperte.

Connessioni Stabilite su Porte Specifiche:

- L'handshake TCP completato su alcune porte specifiche indica che i servizi su queste porte sono attivi e possono essere potenziali vettori di attacco se vulnerabili.

Ipotesi sui potenziali vettori d'attacco

Scansione delle Porte:

- Strumenti come Nmap potrebbero essere utilizzati per eseguire la scansione delle porte. L'attaccante invia pacchetti SYN a varie porte per determinare quali sono aperte e quali servizi sono in esecuzione.

Sfruttamento di Vulnerabilità dei Servizi Attivi:

- Una volta identificate le porte aperte e i servizi attivi, l'attaccante potrebbe tentare di sfruttare vulnerabilità note in quei servizi. Ad esempio, potrebbe utilizzare exploit specifici per il software in esecuzione su quelle porte.

Azioni consigliate

Monitoraggio delle scansioni delle porte

- Implementare sistemi di rilevamento delle intrusioni (IDS) per monitorare e rilevare attività di scansione delle porte, configurare avvisi per notificare gli amministratori di rete quando viene rilevata una scansione.

Aggiornamento e Patch dei Servizi

- Assicurarsi che tutti i servizi in esecuzione sui dispositivi di rete siano aggiornati con le ultime patch di sicurezza. Questo riduce la probabilità che gli attaccanti possano sfruttare vulnerabilità note.

Configurazione del Firewall

- Configurare il firewall per limitare l'accesso alle porte e ai servizi non necessari. Chiudere le porte non utilizzate e applicare regole di accesso restrittive per le porte aperte.

Segmentazione della Rete

- Implementare la segmentazione della rete per limitare il movimento laterale degli attaccanti, utilizzare VLAN e subnet per isolare segmenti di rete sensibili.

Analisi dei log

- Controllare regolarmente i log di sistema per rilevare attività sospette. Analizzare i log di connessione per identificare tentativi di accesso non autorizzati o comportamenti anomali.

L'implementazione delle azioni consigliate aiuterà a migliorare la sicurezza della rete e a mitigare i potenziali impatti degli attacchi, monitorare regolarmente il traffico di rete e mantenere aggiornati i sistemi sono pratiche essenziali per proteggere la rete da minacce e vulnerabilità.