

PROGETTO S9/L5

Introduzione

L'obiettivo di questa relazione è analizzare un file di cattura di rete (pcapng) effettuato con Wireshark per identificare eventuali Indicatori di Compromissione (IOC) e comprendere la natura dell'attacco in corso. Dall'analisi preliminare, si è ipotizzato che si tratti di un port scanning, una tecnica comunemente utilizzata per esplorare le porte di un dispositivo alla ricerca di vulnerabilità. L'esercizio mira a identificare le evidenze di un possibile attacco e suggerire contromisure adeguate.

Identificazione degli IOC

Dall'analisi dei dati, emergono segnali che suggeriscono un'attività di port scanning. Si può riconoscere osservando i pacchetti TCP e le loro caratteristiche.

Il primo indicatore evidente è l'alto numero di pacchetti **TCP** con flag SYN inviati in rapida successione verso diverse porte su uno stesso host. Questo comportamento è tipico del port scanning, poiché l'attaccante cerca di individuare porte aperte e servizi in ascolto. Inoltre, molti di questi pacchetti sono seguiti da una risposta RST (Reset), il che indica che le porte non erano disponibili o che la connessione è stata rifiutata dal sistema target.

Un altro elemento che conferma la natura dell'attacco è il traffico sulle porte note, molte delle quali corrispondono a servizi critici come HTTP (porta 80), SMB (porta 445) e RDP (porta 3389). Questo suggerisce che l'attività non sia casuale, ma mirata a individuare vulnerabilità nei servizi più frequentemente utilizzati.

Infine, si osservano pacchetti **ARP** sospetti, che potrebbero indicare un tentativo di rilevare host attivi sulla rete locale prima di procedere con la scansione delle porte. Questo è un passaggio comune nelle fasi iniziali di un attacco, noto come "reconnaissance" (ricognizione).

No.	Time	Source	Destination	Protocol	Length	Info
18	7.61644619	192.168.200.150	192.168.200.255	Broadcast	288	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	53960 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810522427 TSecr=0 WS=128
3	23.764207789	192.168.200.100	192.168.200.150	TCP	74	53976 → 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	88 → 53960 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294951165 TSecr=810522427 WS=64
5	23.764777472	192.168.200.150	192.168.200.150	TCP	0	0 → 53976 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66	53960 → 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	66	53960 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
8	28.761629461	PcsCompu_39:7d:fe	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_39:7d:fe	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	PcsCompu_39:7d:fe	PcsCompu_39:7d:fe	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	28.775230099	PcsCompu_39:7d:fe	PcsCompu_39:7d:fe	ARP	60	192.168.200.150 is at 08:00:27:39:7d:fe
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	59126 → 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	53878 → 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	36.774485627	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	36.774685595	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	36.774685996	192.168.200.150	192.168.200.100	TCP	60	413 → 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	36.774687397	192.168.200.150	192.168.200.100	TCP	60	554 → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	36.774687776	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	36.774711872	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	36.775141113	192.168.200.150	192.168.200.150	TCP	0	0 → 41304 [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	36.775174448	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	36.775378800	192.168.200.100	192.168.200.150	TCP	74	59174 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535438 TSecr=0 WS=128
30	36.775386694	192.168.200.100	192.168.200.150	TCP	74	55056 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535439 TSecr=0 WS=128
31	36.775524204	192.168.200.100	192.168.200.150	TCP	74	53862 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535439 TSecr=0 WS=128
32	36.775598806	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	60	41304 → 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
34	36.775652407	192.168.200.100	192.168.200.150	TCP	60	56120 → 113 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
35	36.775799538	192.168.200.150	192.168.200.100	TCP	74	22 → 55056 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535439 WS=64
36	36.775979084	192.168.200.150	192.168.200.100	TCP	74	88 → 53862 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535439 WS=64
37	36.775983780	192.168.200.100	192.168.200.150	TCP	66	55056 → 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	53862 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
39	36.776013124	192.168.200.100	192.168.200.150	TCP	60	41182 → 21 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
40	36.775975876	192.168.200.100	192.168.200.150	TCP	66	55056 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466

Ipotesi sui vettori di attacco utilizzati

L'attacco rilevato sembra essere un tipico esempio di port scanning, un'attività preliminare utilizzata per raccogliere informazioni sulla configurazione della rete e identificare eventuali vulnerabilità. Gli strumenti più comuni per eseguire port scanning includono software come **Nmap**, che consente di identificare porte aperte e servizi attivi su un host. Inoltre, è possibile che l'attaccante abbia utilizzato script personalizzati per evitare di essere rilevato dai sistemi di monitoraggio.

Il port scanning è spesso un preludio a fasi successive di attacco. Una volta identificate le porte aperte, gli attaccanti possono sfruttare vulnerabilità specifiche associate ai servizi in esecuzione su tali porte. Ad esempio, una porta SMB aperta (445) potrebbe essere un punto d'ingresso per exploit noti come EternalBlue, mentre un servizio RDP non protetto (3389) potrebbe essere soggetto a tentativi di brute-force sulle credenziali.

Azioni consigliate per ridurre gli impatti dell'attacco attuale e futuri

Ridurre l'impatto dell'attacco attuale

- Configurare il firewall per rilevare e bloccare i tentativi di port scanning. Molti firewall moderni offrono funzionalità specifiche per rilevare pattern tipici di port scanning e per bloccare automaticamente questi tentativi.
- In alcuni casi si potrebbe bloccare l'IP sospetto, però in questo caso gli indirizzi sembrano essere nella stessa LAN, quindi bloccandolo, non conoscendo la natura di questa scansione, potremmo compromettere l'operabilità nell'azienda. Nel caso fosse stato un IP esterno poteva essere bloccato tramite il firewall, che può filtrare il traffico in ingresso da questi indirizzi IP sospetti.

Ridurre i rischi di attacchi futuri

- Un approccio efficace è limitare l'accesso alle porte critiche, permettendo solo a IP autorizzati di comunicare con tali servizi. Ad esempio, le porte SMB e RDP possono essere configurate per essere accessibili solo da specifici segmenti di rete o tramite VPN. È consigliabile configurare anche il rate limiting per limitare il numero di richieste di connessione provenienti da un singolo indirizzo IP.
- Implementare un sistema di rilevamento e risposta alle intrusioni (IDS/IPS) per monitorare continuamente la rete e rilevare tentativi di port scanning. L'IPS può anche bloccare automaticamente i pacchetti sospetti prima che raggiungano il sistema target.
- L'uso di honeypots può aiutare a identificare gli attaccanti. Questi sistemi sono configurati per sembrare porte vulnerabili e raccogliere informazioni sugli attacchi in corso, riducendo al minimo il rischio per il sistema reale.
- Assicurarsi che tutti i sistemi e le applicazioni siano regolarmente aggiornati per correggere eventuali vulnerabilità conosciute.

Conclusioni

L'analisi del file pcapng ha rivelato la presenza di un attacco di tipo port scanning, confermato dalla rilevazione di numerosi tentativi di connessione TCP a un ampio numero di porte. Sulla base di questi indicatori, è stato ipotizzato l'uso di tecniche come il SYN scan e l'utilizzo di strumenti automatizzati per esplorare le porte vulnerabili come Nmap.

Per mitigare gli effetti dell'attacco attuale e prevenire futuri tentativi, è fondamentale adottare misure di difesa come il rafforzamento dei firewall, l'implementazione di sistemi IDS/IPS, e l'adozione di politiche di sicurezza attive.