Report Esercizio S9-L5

Identificare ed analizzare eventuali IOC, ovvero evidenze di attacchi in corso

Sicuramente il più sostanziale indicatore di compromissione rilevato nella cattura dei pacchetti con Wireshark è il numero elevato di pacchetti SYN inviati da 192.168.200.100 al target 192.168.200.150. Questo comportamento mi ha subito ricondotto ad una scansione di rete che ha come obbiettivo quello di individuare le porte aperte e i servizi attivi sulla macchina target.

Mi sono quindi apprestato ad individuare il tipo di scansione. Inizialmente ho ipotizzato fosse una scansione SYN (half-open) in quanto tendenzialmente più veloce e discreta, ma osservando bene le connessioni mi sono reso conto che la macchina attaccante 192.168.200.100 non bloccava la connessione una volta stabilito se la porta di riferimento fosse aperta ma al contrario finalizzava il triplo handshake e stabiliva una connessione completa.

Infatti si può osservare come la macchina attaccante completa l'handshake TCP inviando un ACK dopo aver ricevuto il SYN-ACK dalla macchina target. Questo ci conferma che si tratta di una scansione TCP connect (-sT e non -sS come ipotizzavo inizialmente).

Riassumendo: in primis la macchina attaccante invia un pacchetto TCP SYN per avviare una connessione e vedere se la porta è aperta. Se la porta è aperta, la macchina target risponde con un pacchetto SYN-ACK confermando che è possibile stabilire una connessione. Se la porta è chiusa, la macchina target risponde con un pacchetto RST ACK. Di nuovo, se la porta è aperta la macchina attaccante invia un ACK alla macchina target instaurando una connessione completa. Possiamo notare come dopo essere instaurata la connessione viene chiusa.

16	36.774405627	192.168.200.100	192.168.200.150	TCP	74 52358 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=146
17	36.774535534	192.168.200.100	192.168.200.150	TCP	74 46138 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=146
18	36.774614776	192.168.200.100	192.168.200.150	TCP	74 41182 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
19	36.774685505	192.168.200.150	192.168.200.100	TCP	74 23 → 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=
20	36.774685652	192.168.200.150	192.168.200.100	TCP	74 111 → 56120 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len
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	36.774700464	192.168.200.100	192.168.200.150	TCP	66 41304 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TS
25	36.774711072	192.168.200.100	192.168.200.150	TCP	66 56120 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 T
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=
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
29	36.775337800	192.168.200.100	192.168.200.150	TCP	74 59174 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=146
30	36.775386694	192.168.200.100	192.168.200.150	TCP	74 55656 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
31	36.775524204	192.168.200.100	192.168.200.150	TCP	74 53062 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
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
34	36.775652497	192.168.200.100	192.168.200.150	TCP	66 56120 → 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Le
35	36.775796938	192.168.200.150	192.168.200.100	TCP	74 22 → 55656 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=
36	36.775797004	192.168.200.150	192.168.200.100	TCP	74 80 → 53062 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=
37	36.775803786	192.168.200.100	192.168.200.150	TCP	66 55656 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TS
38	36.775813232	192.168.200.100	192.168.200.150	TCP	66 53062 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TS
39	36.775861964	192.168.200.100	192.168.200.150	TCP	66 41182 → 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len
40	36.775975876	192.168.200.100	192.168.200.150	TCP	66 55656 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len
41	36.776005853	192.168.200.100	192.168.200.150	TCP	66 53062 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len
42	36.776179338	192.168.200.100	192.168.200.150	TCP	74 50684 → 199 [SYN] Seq=0 Win=64240 Len=0 MSS=146

In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati

Questa scansione può essere considerata come il primo passo di un attacco. Ci troviamo probabilmente nella fase di ricognizione dove l'attaccante sta cercando di individuare le porte aperte e quali servizi sono attivi e potenzialmente vulnerabili.

Le porte, soprattutto le più note come la 80 (HTTP), 21 (FTP) e 25 (SMTP), potrebbero essere vulnerabili a exploit specifici come SQL injection, cross-site scripting, attacchi di Brute Force, attacchi DoS o phishing. Inoltre, le porte aperte meno comuni potrebbero avere servizi vulnerabili esposti con configurazioni errate o non aggiornate.

Consigliate un'azione per ridurre gli impatti dell'attacco attuale ed eventualmente un simile attacco futuro

Le azioni da intraprendere per una mitigazione dell'attacco potrebbero essere:

- Configurare il firewall per bloccare tutto il traffico in entrata proveniente da 192.168.200.100, interrompendo la scansione.
- Verificare la configurazione dei servizi attivi sulle porte aperte assicurandosi che non ci siano vulnerabilità note e che siano stati applicati tutti gli aggiornamenti più recenti.
- Monitorare il traffico in tempo reale per rilevare attività sospette provenienti da alti IP.
- Disabilitare temporaneamente i servizi non essenziali.
- Implementare regole di accesso mirate.

Invece, per prevenire eventuali attacchi futuri si potrebbero:

- Limitare i servizi esposti, riducendo il numero di porte aperte al minimo necessario e configurando un firewall per consentire il traffico solo verso servizi essenziali.
- Implementare un IDS e utilizzare strumenti appositi per monitorare e segnalare attività anomale sulla rete, come scansioni o connessioni sospette.
- Segmentare la rete separando i sistemi vulnerabili dalla rete principale per ridurre il rischio di propagazioni in caso di compromissione.
- Condurre test di sicurezza periodici per individuare e correggere eventuali vulnerabilità.