

Relazione sull'Analisi del Traffico di Rete

Esercizio

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:

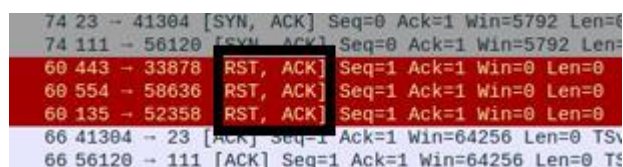
Identificare eventuali IOC, ovvero evidenze di attacchi in corso

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

Consigliate un'azione per ridurre gli impatti dell'attacco

Indicatori di Compromissione (IOC)

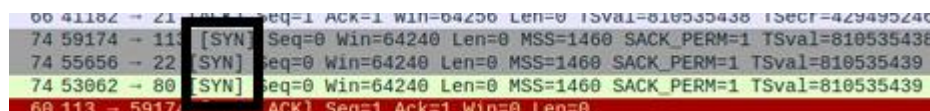
Numerosi pacchetti RST (Reset):



```
74 23 → 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
74 111 → 56120 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
60 443 → 33878 RST, ACK Seq=1 Ack=1 Win=0 Len=0
60 554 → 58636 RST, ACK Seq=1 Ack=1 Win=0 Len=0
60 135 → 52358 RST, ACK Seq=1 Ack=1 Win=0 Len=0
66 41304 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=
66 56120 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=
```

Molti pacchetti TCP presentano i flag RST e ACK, indicando connessioni interrotte o rifiutate. Questo è evidente in numerosi frame.


Sequenze di pacchetti SYN senza risposte adeguate:



```
60 41182 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=429495240
74 59174 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535438 TSecr=
74 55656 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535439 TSecr=
74 53062 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535439 TSecr=
60 113 → 59174 [ACK] Seq=1 Ack=1 Win=0 Len=0
```

Diversi tentativi di connessione SYN sono seguiti da pacchetti RST, suggerendo tentativi di connessione falliti. Questo è particolarmente evidente in tutti gli screenshot.

Richieste ARP broadcast:



```
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 ARP 74 41304 → 23 [ACK] Seq=0 Ack=1 Win=64256 Len=0 MSS=1460 TSval=
```

Ci sono richieste ARP broadcast che potrebbero indicare una scansione della rete. Questo è evidente nei frame 10 e 11 del primo screenshot.

Ipotesi sui Potenziali Vettori di Attacco

Scansioni delle Porte:

I pacchetti SYN seguiti da RST possono indicare una scansione delle porte per rilevare quali servizi sono attivi su 192.168.200.150. Questo tipo di attività è tipica di strumenti come Nmap utilizzati dagli attaccanti per mappare la rete.

Attacchi di Denial of Service (DoS):

I numerosi pacchetti RST potrebbero far parte di un attacco DoS volto a interrompere le connessioni esistenti o impedire nuove connessioni. Questo può sovraccaricare il sistema target e interrompere i servizi legittimi.

Rilevamento della Rete:

Le richieste ARP broadcast possono essere indicative di una scansione della rete per mappare i dispositivi collegati. Questo è spesso il primo passo di un attaccante per ottenere una visione completa della rete target.

Azioni Consigliate per Ridurre gli Impatti dell'Attacco

Configurare il Firewall:

Bloccare gli indirizzi IP sospetti e limitare il traffico alle porte necessarie. Implementare regole di firewall rigorose per prevenire scansioni e connessioni non autorizzate.

Implementare IDS/IPS:

Utilizzare sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS) per monitorare e bloccare il traffico sospetto. Questi sistemi possono rilevare tentativi di scansione delle porte e attacchi DoS.

Monitoraggio Continuo:

Implementare un sistema di monitoraggio continuo della rete per identificare e rispondere rapidamente ad attività anomale. Utilizzare strumenti di logging e analisi per mantenere una visione aggiornata della rete.

Segmentazione della Rete:

Dividere la rete in segmenti separati per limitare la propagazione di eventuali attacchi. Utilizzare VLAN e altre tecniche di segmentazione per isolare i dispositivi critici e limitare l'accesso.

Formazione e Consapevolezza:

Fornire formazione continua al personale sulla sicurezza informatica e le migliori pratiche per rilevare e rispondere agli attacchi. La consapevolezza del personale è cruciale per una risposta rapida ed efficace agli incidenti.