

PROGETTO THREAT INTELLIGENCE:

Nel progetto di oggi dovevamo analizzare un file contenente un'analisi fatta con wireshark, individuando gli IOC e i potenziali vettori di infezione.

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
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 → 53060 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM 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	PCSSystemtec_fd:87:...	PCSSystemtec_39:7d:...	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_fd:87:...	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: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 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 58636 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
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 TSval=810535440 TSecr=0 WS=128
57 36.776904828	192.168.200.150	192.168.200.100	TCP	74 445 → 33842 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM 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 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 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 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 33842 → 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 TSval=810535440 TSecr=0 WS=128

> Frame 31: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth1, id 0

Ethernet II, Src: PCSSystemtec_39:7d:fe (08:00:27:39:7d:fe), Dst: PCSSystemtec_fd:87:1e (08:00:27:fd:87:1e)

Internet Protocol Version 4, Src: 192.168.200.100, Dst: 192.168.200.150

Transmission Control Protocol, Src Port: 53062, Dst Port: 80, Seq: 0, Len: 0

0000 08 00 27 fd 87 1e 08 00 27 39 7d fe 08 00 45 00 ...E:

0010 00 3c 7a 00 40 00 40 06 ae 6f c0 a8 c8 64 c0 a8 ...z:@:o:d

0020 c8 96 cf 46 00 50 a3 d5 1a bf 00 00 00 00 02 ...F:P:.....

0030 fa f0 12 7b 00 00 02 04 05 b4 04 02 08 0a 30 4f ...{.....00

0040 ca 0f 00 00 00 00 01 03 03 07

Analisi Dettagliata degli Indicatori di Compromissione (IOC)

Richiedi ARP sospette

Evento rilevato:

"Chi ha 192.168.200.100? Dillo a 192.168.200.150"

"192.168.200.150 è alle 08:00:27 :fd "

Interpretazione:

Questi pacchetti suggeriscono un possibile tentativo di ARP spoofing , in cui un attore malevolo cerca di legare il proprio indirizzo MAC a un indirizzo IP appropriato. Se non monitorato, potrebbe intercettare, alterare o reindirizzare il traffico di rete.

Raccomandazioni:

Utilizzare tabelle statiche ARP per dispositivi chiave.

Implementare il protocollo Dynamic ARP Inspection (DAI) , se supportato dagli switch.

Utilizzare un sistema di rilevamento intrusi (IDS) come Snort per monitorare richieste ARP anomale.

Connessioni SYN multiple

Evento rilevato:

Numerosi pacchetti SYN verso porte diverse:

Porta 80, 443: HTTP/HTTPS.

Porta 135: chiamata di procedura remota (RPC).

Porta 993: IMAP su SSL/TLS.

Porta 21: FTP.

Interpretazione:

Questa attività potrebbe indicare una scansione delle porte , spesso utilizzata da attaccanti per identificare servizi in ascolto e vulnerabilità. L'uso di porte critiche (443, 80) e non comuni (135, 993) potrebbe essere mirato a sfruttare la vulnerabilità.

Dettagli aggiuntivi:

La scansione sembra provenire da un IP specifico, che potrebbe essere identificato e bloccato immediatamente.

Raccomandazioni:

Configurare un firewall per bloccare connessioni multiple non autorizzate da un singolo IP.

Usa uno strumento di rilevamento anomalie come Zeek o Suricata per registrare questa attività.

Analizzare il log di rete per verificare se l'IP è malevolo o interno.

[09:44]

Risposte ARP non richieste

Evento rilevato:

"192.168.200.150 è alle 08:00:27 :fd "

Interpretazione:

Una risposta ARP non richiesta può indicare che un attore malintenzionato sta annunciando il proprio indirizzo MAC per intercettare il traffico destinato a un dispositivo valido. Questo è un sintomo classico di attacchi Man-In-The-Middle (MITM) .

Raccomandazioni:

Convalidare manualmente la mappatura IP-MAC su dispositivi sospetti.

Impiegare strumenti come ARPwatch per monitorare e registrare attività ARP nella rete.

Implementare il protocollo 802.1X per autenticare i dispositivi collegati alla rete.

Comunicazioni inusuali

Evento rilevato:

Comunicazioni verso porte sensibili (135, 993, 21).

Interpretazione:

Queste porte sono spesso utilizzate per:

135: Scansione RPC per attacchi basati su vulnerabilità Microsoft (es. EternalBlue).

993: Accesso a un server email crittografati tramite IMAP.

21: Tentativi di accesso a un server FTP non protetto.

L'accesso potrebbe essere una fase di riconoscimento o utilizzo attivo.

Raccomandazioni:

Disabilitare i servizi non necessari sulla rete interna.

Utilizzare software di sicurezza come Nessus per eseguire scansioni di vulnerabilità.

IP con comportamento sospetto

IP interessati:

192.168.200.150 come possibile sorgente esterna.

Interpretazione:

La rete dovrebbe essere configurata per isolare sottoreti diverse. La presenza di traffico tra 192.168.200.xe

192.168.200.x potrebbe indicare una configurazione errata o la presenza di un dispositivo compromesso.

Raccomandazioni:

Verificare la configurazione VLAN o le regole di routing.

Effettuare una scansione approfondita 192.168.208.150 per individuare software sospetti o vulnerabili.

Sintesi e azioni raccomandate

Implementare un IDS/IPS:

[09:44]

Per rilevare e bloccare attività sospette, come scansioni delle porte e spoofing ARP.

Rafforzare il dipendente di rete:

Limitare il traffico tra subnet con regole ACL (Access Control List).

Disabilitare servizi non utilizzati sui dispositivi interni.

Monitorare regolarmente:

Utilizzare strumenti come Wireshark, ARPwatch e Suricata per eseguire controlli periodici e registrare anomalie