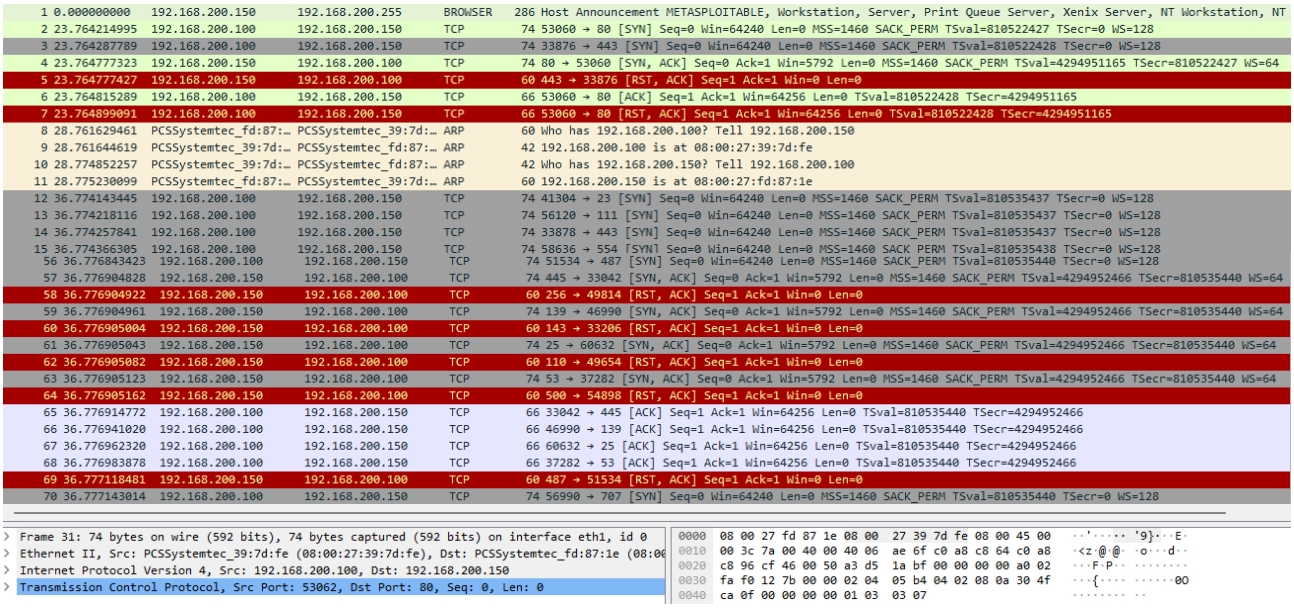
PROGETTO THREAT INTELLIGENCE:

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



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 192.168.208.150per 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