Nell’esercizio di oggi vado analizzo una cattura di rete tramite Wireshark per determinare potenziali Indicatori di Compromissione (IOC), in questo posso determinare una strategia di azioni per mitigare gli eventuali attacchi in corso e futuri

Dagli screenshot forniti ho notato i seguenti IOC:

Numerosi pacchetti TCP RST (Reset) provenienti dall’host 192.168.200.150 che interrompono le connessioni in modo anomalo. Questo puo indicare un attacco in corso, come un tentativo di nascondere la propria attività malevola.

L’host 192.168.200.100 invia numerosi pacchetti SYN verso 192.168.200.150, utilizzando le porte 80 (HTTP) e 443 (HTTPS). Questo comportamento può indicare un attacco SYN flood, un tipo di attacco DOS.

Traffico ARP sospetto, PcsCompu_39:7d:fe sembra stia avendo un traffico ARP abbastanza sospetto. Questo potrebbe indicare un tentativo di ARP Spoofing o Man-in-the-Middle (MITM)

192.168.200.150 risponde sulla porta 80. Questo potrebbe indicare la presenza di un’applicazione vulnerabile o mal configurata.

In base agli IOC individuati, posso formulare le seguenti ipotesi sui vettori di attacco:

Scansione di rete, l’attacante potrebbe aver utilizzato strumenti di scanning, come Nmap, per identificare le porte aperte e i servizi attivi sull’host 192.168.200.150

La porta 80 aperta potrebbe essere stata sfruttata tramite un attacco mirato con un tentativo di sfruttamento di vulnerabilità su HTTP utilizzando exploit noti per vulnerabilità su web server o applicazioni web

Denial-of-Service (DOS), il volume elevato di pacchetti SYN e RST potrebbe indicare un tentativo di saturare il server, impedendogli di rispondere a richieste legittime.

ARP Spoofing o MITM (man in the middle), l’attività ARP sospetta potrebbe essere stata utilizzata per manipolare il traffico, indirizzando le comunicazioni verso l’attaccante per intercettare o modificare i dati.

Per mitigare possiamo compiere le seguenti azioni:

Host 192.168.200.150 compromesso, blocare l'ip dalla rete per impedire ulteriori compromissioni o danni

Monitoraggio del traffico di rete, continuare ad analizzare il traffico in tempo reale per individuare ulteriori attività sospette

Verifica dei log di sistema, analizzare i log di 192.168.200.150 e del server HTTP per identificare eventuali tentativi di accesso non autorizzato o exploit

Per cercare di prevenire queste vulnerabilità possiamo cercare di effettuare delle azioni preventive:

Aggiornamento software, verificare che tutti i sistemi e le applicazioni, in particolare il web server, siano aggiornati con le ultime patch di sicurezza.

Configurare il firewall per bloccare il traffico non autorizzato e limitare l'accesso alle sole porte e protocolli necessari.

Abilitazione di IDS/IPS, implementare sistemi di rilevamento e prevenzione delle intrusioni per identificare e bloccare automaticamente le attività malevole

Protezione contro attacchi ARP, configurare staticamente le tabelle ARP o abilitare funzionalità come Dynamic ARP Inspection per mitigare i rischi di ARP Spoofing.

Implementazione di rate limiting, limitare il numero di richieste SYN che un singolo host può inviare al server in un determinato intervallo di tempo, limitando la possibilità di attacchi DoS