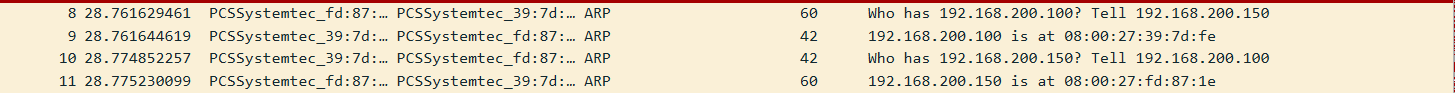
**PROGETTO 11.10**

1. **Identificare ed analizzare eventuali IOC, ovvero evidenze di attacchi in corso:**

La prima cosa che possiamo osservare è che abbiamo un iniziale tentativo di connessione TCP seguito solo successivamente da una chiamata ARP. Questo potrebbe avvenire o per verificare che gli host siano raggiungibili o per cercare di reperire ulteriori informazioni sugli stessi.

**Immagine che contiene testo, schermata, Carattere, numero

Descrizione generata automaticamente**



Dopo la chiamata ARP si tenta nuovamente di dare avvio ad una connessione TCP:

Immagine che contiene testo, schermata, Carattere, numero

Descrizione generata automaticamente

TCP è un protocollo orientato alla connessione, il che significa che stabilisce una connessione affidabile tra due host prima che i dati possano essere scambiati; tale processo è conosciuto come “three-way handshake”:

SYN -->

<-- SYN/ACK

ACK -->

Osserviamo come in questo caso non sia possibile portare a termine la connessione TCP in quanto interviene una risposta RST. Quando una connessione TCP deve essere interrotta bruscamente, il flag RST viene utilizzato per chiudere immediatamente la connessione senza terminare la stessa.

Immagine che contiene testo, schermata, Carattere, numero

Descrizione generata automaticamente

Osservando attentamente possiamo notare che non sono stati traferiti dati in quanto sia Seq che Ack sono pari a 1, oltremodo il Len=0 ci sta ad indicare che nel segmento TCP non ci sono dati da trasmettere. Il pacchetto è utilizzato solo per il controllo della connessione e non porta alcun payload di dati.



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

Quanto sopra individuato potrebbe essere associato ad un comportamento malevolo in quanto un aggressore potrebbe inviare pacchetti RST per identificare quali porte sono aperte o chiuse su un sistema e ricevendo un RST in risposta comprendere che la porta è chiusa o potrebbe oltremodo essere indicativo di un attaccante che sta tentando di interrompere una connessione legittima tra due parti.

Da un ulteriore analisi possiamo osservare un tentativo di connessione su porte diverse, il che potrebbe essere ulteriormente indicativo di un tentativo di scansione delle porte stesse.

Risulta poi evidente dagli screen riportati di seguito come i tentativi di connessione provengano da un solo indirizzo ip (192.168.200.100) e come lo stesso tenti di inviare una grande quantità di pacchetti in un breve periodo di tempo. Ciò potrebbe essere indicativo di un attacco brute-force o di un attacco SYN Flood. In questo caso si tratta di un comune attacco Dos/DDoS in cui un gran numero di pacchetti **SYN** viene inviato senza mai ricevere ACK e quindi senza mai completare la connessione. Un attacco del genere potrebbe saturare le risorse del server rendendolo, quindi, incapace di gestire nuove connessioni legittime.

Non ritengo però di tratti di un SYN flood in quanto continuiamo ad avere flag RST che chiudono la connessione senza terminarla. In un di attacco SYN flood l’aggressore sfrutta il fatto che, dopo aver ricevuto un primo pacchetto SYN, il server attaccato risponderà con uno o più pacchetti SYN/ACK attendendo poi la fase finale dell’handshake. Il server attaccato rimarrà quindi in attesa di una risposta che però non arriverà mai mentre l’aggressore continuerà ad inviare pacchetti SYN costringendo così il server attaccato a mantenere contemporaneamente più connessioni aperte comportando ciò che ad un certo punto il server sarà sovraccaricato e non sarà più in grado di funzionare normalmente.

Immagine che contiene testo, schermata, menu, Carattere

Descrizione generata automaticamente

Immagine che contiene testo, schermata, menu, Carattere

Descrizione generata automaticamente



1. **Consigliate un’azione per ridurre gli impatti dell’attacco attuale ed eventualmente un simile attacco futuro**

Per ridurre l’impatto dei possibili attacchi che sono stati configurati si potrebbero innanzitutto implementare le configurazioni dei firewall al fine di bloccare o limitare il traffico non autorizzato o comunque sospetto. Si potrebbero quindi filtrare i pacchetti provenienti da indirizzi IP non autorizzati o da porte non utilizzate.

È oltretutto consigliabile un monitoraggio continuo del traffico mediante strumenti come Wireshark che possano aiutarci a rilevare attività sospette.

Sarebbe poi consigliabile assicurarsi che i servizi esposti (es. http) siano aggiornati alle ultime patch di sicurezza, oltremodo sarebbe necessario disabilitare o rimuovere quei servizi non necessari che espongono però la rete a dei rischi. È poi necessario assicurarsi che i servizi che utilizzano TLS/SSL abbiano certificati aggiornati e non siano vulnerabili ad eventuali exploit.

Nel caso in cui si trattasse di un attacco SYN Flood sarebbe necessario prevenirlo mediante l’abilitazione di SYN cookies sul server modificando così la gestione delle connessioni TCP al fine di impedire di allocare risorse fino a quando la connessione non sia stata completata.

Infine, è necessario implementare un sistema di backup regolare di tutti i dati e servizi critici così da permetterci un ripristino rapido del servizio nel caso in cui l’attacco avesse successo.

È importante poi assicurarsi di testare regolarmente i piani di disaster recovery così che possano essere rapidamente implementati in caso di necessità.