M4 D5

ESERCIZIO

GIORNO 3 – ARP POISONING

Spiegazione dell' ARP Poisoning:
ARP Poisoning, o ARP Spoofing, è un tipo di attacco informatico che mira a manipolare la tabella ARP (Address Resolution Protocol) di una rete locale per dirigere il traffico di rete attraverso un dispositivo controllato dall'attaccante. L' ARP Poisoning è un attacco che si può utilizzare per intercettare del traffico su una rete basata su twitch. Per il funzionamento dell' ARP Poisoning: l'attaccante invia pacchetti ARP falsificati nella rete locale, che contengono indirizzi MAC e IP manipolati. Questi pacchetti possono essere inviati ad intervalli regolari per mantenere l'attacco attivo. I dispositivi nella rete locale accettano e memorizzano le informazioni falsificate contenute nei pacchetti ARP. Di conseguenza, la tabella ARP di questi dispositivi viene corrotta, associando indirizzi MAC e IP errati. Quando i dispositivi nella rete devono inviare pacchetti ad un determinato indirizzo IP, si basano sulla tabella ARP per ottenere l'indirizzo MAC corrispondente. Il dispositivo invierà i pacchetti all'indirizzo MAC dell'attaccante invece del dispositivo di destinazione reale.

Sistemi vulnerabili ad ARP Poisoning:

I sistemi che sono vulnerabili all'ARP Poisoning includono praticamente tutti i dispositivi e i sistemi operativi che utilizzano il protocollo ARP. Alcuni esempi sono: Windows (tutte le versioni), Linux, macOS e dispositivi di rete come router, switch e access point.

Elenco modalità di mitigazione, rilevazione o annullamento attacco:

Per mitigare, rilevare o annullare l'attacco di ARP Poisoning, possono essere adottate le seguenti misure: utilizzare meccanismi di sicurezza come ARP Inspection o DHCP Snooping che possono rilevare e prevenire attacchi di ARP Poisoning. Configurare staticamente le tabelle ARP per i dispositivi critici in modo che non rispondano agli aggiornamenti ARP provenienti da fonti non autorizzate. Monitorare regolarmente la tabella ARP della rete e cercare discrepanze o duplicati che potrebbero indicare un attacco. Utilizzare il protocollo ARP Secure, che richiede l'autenticazione tra dispositivi nella rete locale prima di accettare e memorizzare le informazioni ARP. Implementare connessioni crittografate (HTTPS) per proteggere la comunicazione da potenziali attacchi MITM.

Azioni di mitigazione spiegando efficacia ed effort per utente-azienda:

Le azioni di migrazione per mitigare l'ARP Poisoning richiedono un certo sforzo sia per gli utenti che per le aziende. Gli utenti dovranno aggiornare i propri sistemi operativi e dispositivi di rete con versioni che includono soluzioni di sicurezza per prevenire l'ARP Poisoning. Questo potrebbe richiedere l'aggiornamento del firmware del dispositivo o l'installazione di patch di sicurezza. Per le aziende, la migrazione richiederà una pianificazione più ampia. Sarà necessario identificare le vulnerabilità all'ARP Poisoning nella rete, valutare le alternative di mitigazione, pianificare le fasi di migrazione e implementare le misure di sicurezza. L'efficacia dell'azione di migrazione dipenderà dalla corretta pianificazione e implementazione delle contromisure. L'azienda dovrebbe fornire formazione e supporto agli utenti durante il processo di migrazione. L'efficacia delle azioni di migrazione sarà determinata dalla corretta implementazione delle contromisure. Se le misure di sicurezza sono implementate correttamente, l'ARP Poisoning può essere notevolmente ridotto o prevenuto. L'effort richiesto per l'utente e l'azienda dipenderà dalla complessità e dall'estensione della rete e dei dispositivi coinvolti nella migrazione.