ARP Poisoning: Report

Introduzione

Nella lezione teorica abbiamo visto l'attacco ARP Poisoning. In questo report, spiegherò come funziona l'ARP Poisoning, elencherò i sistemi vulnerabili, descriverò le modalità per mitigare, rilevare o annullare questo attacco, e commenterò queste azioni di mitigazione spiegando l'efficacia e l'effort per l'utente/azienda.

1. Spiegare brevemente come funziona l'ARP Poisoning

L'attacco ARP Poisoning è una tecnica malevola utilizzata per intercettare, analizzare o manipolare il traffico di rete all'interno di una LAN (rete locale). Questo attacco sfrutta il protocollo ARP (Address Resolution Protocol) per inviare informazioni ARP false sulla rete, promuovendo il proprio indirizzo MAC come il legittimo indirizzo MAC del router o di un'altra macchina. Ciò consente all'attaccante di intercettare il traffico di rete tra le macchine e il router o di dirottare questo traffico ogni volta che una macchina invia un pacchetto al gateway o al router.

2. Elencare i sistemi che sono vulnerabili a ARP Poisoning

L'attacco ARP Poisoning colpisce esclusivamente i sistemi all'interno di una LAN, in particolare tutte le macchine che utilizzano lo stesso gateway e lo stesso indirizzo IP di rete. In altre parole, gli utenti all'interno della stessa rete locale saranno vulnerabili all'attacco ARP Poisoning.

3. Elencare le modalità per mitigare, rilevare o annullare questo attacco

Tecnica	Descrizione	Efficacia	Effort
Utilizzo di protocolli di sicurezza	I protocolli come HTTPS, SSL, TLS o VPN crittografano i dati in transito e impediscono agli attaccanti di leggerli o manipolarli.	Alta	Medio
Utilizzare Switch livello 3	Si divide la rete in sottoreti, ma gli switch layer 3 hanno un costo maggiore e richiedono configurazione.	Alta	Alto
Monitoraggio costante	Controllare regolarmente la rete per individuare eventuali intrusioni, come accessi non autorizzati o attacchi di ARP poisoning.	Alta	Medio
Utilizzo di software per la sicurezza	Alcuni software antivirus e anti-malware possono individuare e prevenire attacchi ARP poisoning.	Media	Basso
Educazione del personale	Informare gli utenti sulla sicurezza informatica e sui rischi di attacchi come l'ARP poisoning può aiutare a prevenire incidenti.	Alta	Medio

Diversi produttori di software offrono anche dei programmi di monitoring con i quali si possono controllare le reti e rilevare i procedimenti ARP insoliti. Ad esempio:

- **Arpwatch**
- **XArp**
- **Snort**: Un IDS (Intrusion Detection System) che può essere utilizzato per effettuare il monitoraggio.

4. Commentare queste azioni di mitigazione, spiegando l'efficacia e l'effort per l'utente/azienda

Utilizzo di protocolli di sicurezza

- **Efficacia**: Alta. I protocolli di crittografia proteggono i dati in transito, rendendo difficile per gli attaccanti intercettare e manipolare i dati.
- **Effort**: Medio. Implementare HTTPS, SSL, TLS o VPN richiede configurazione iniziale e manutenzione continua.

Utilizzare Switch livello 3

- **Efficacia**: Alta. La suddivisione della rete in sottoreti riduce la superficie di attacco.
- **Effort**: Alto. Gli switch layer 3 sono più costosi e richiedono configurazione avanzata.

Monitoraggio costante

- **Efficacia**: Alta. Rileva rapidamente attività sospette e consente risposte rapide agli attacchi.
- **Effort**: Medio. Richiede strumenti di monitoraggio e personale qualificato per l'analisi.

Utilizzo di software per la sicurezza

- **Efficacia**: Media. Gli antivirus e anti-malware possono rilevare alcuni tipi di attacchi ARP poisoning.
- **Effort**: Basso. Facile da implementare, ma non sempre sufficiente da solo.

Educazione del personale

- **Efficacia**: Alta. Utenti consapevoli possono ridurre il rischio di successo degli attacchi.
- **Effort**: Medio. Richiede formazione continua e aggiornamenti regolari.

Conclusione

L'attacco ARP Poisoning rappresenta una minaccia significativa per le reti locali, ma può essere mitigato efficacemente attraverso una combinazione di tecniche di configurazione di rete, strumenti di monitoraggio e misure di sicurezza avanzate. Ogni metodo di mitigazione ha i suoi vantaggi e svantaggi in termini di efficacia e sforzo richiesto, e la scelta delle tecniche più appropriate dipenderà dalle specifiche esigenze e risorse dell'utente o dell'azienda.