Nella lezione teorica abbiamo visto l'attacco **ARP Poisoning**

Traccia

- Spiegare brevemente come funziona l'APR Poisoning
- Elencare i sistemi che sono vulnerabili a APR Poisoning
- Elencare le modalità per mitigare, rilevare o annullare questo attacco
- Commentare queste azioni di mitigazione, spiegando l'efficacia e l'effort per l'utente/azienda.

Introduzione all'ARP Poisoning

L'ARP Poisoning (Address Resolution Protocol Poisoning), noto anche come ARP Spoofing, è un tipo di attacco informatico che sfrutta la vulnerabilità del protocollo ARP, utilizzato per la risoluzione degli indirizzi IP in indirizzi MAC in una rete locale (LAN). Questo attacco permette a un aggressore di intercettare, modificare o bloccare il traffico di rete tra dispositivi sulla stessa LAN.

Sistemi Vulnerabili

1. **Reti Ethernet**: Le reti Ethernet che utilizzano il protocollo ARP sono vulnerabili. Questo include la maggior parte delle reti locali (LAN) tradizionali.
2. **Dispositivi di Rete**: Router, switch, hub, e punti di accesso che non implementano misure di sicurezza contro ARP Poisoning.
3. **Computer e Server**: Tutti i dispositivi collegati a una LAN che utilizzano il protocollo ARP per la risoluzione degli indirizzi.
4. **Sistemi Operativi**: La maggior parte dei sistemi operativi, inclusi Windows, macOS, Linux, e Unix, che non adottano misure preventive contro questo tipo di attacco.

Nota: Nonostante l'ARP Poisoning sia una vulnerabilità nota da tempo, molti di questi sistemi sono ancora in uso ed esistenti in reti non adeguatamente protette.

Mitigazione dell'ARP Poisoning

Ecco una lista di soluzioni tecniche per mitigare la vulnerabilità dell'ARP Poisoning:

Utilizzare Switch con Funzionalità di Sicurezza Avanzata

- **Port Security**: Configurare i switch per limitare il numero di indirizzi MAC per porta e prevenire indirizzi MAC non autorizzati.
- **Dynamic ARP Inspection (DAI)**: Implementare DAI nei switch per controllare le risposte ARP e assicurarsi che corrispondano a indirizzi IP legittimi.

ARP Statico

- **Definizione Manuale degli ARP**: Configurare staticamente le tabelle ARP nei dispositivi di rete per i dispositivi più critici. Questo impedisce che ARP spoofing possa alterare le corrispondenze IP-MAC.

Filtraggio di Pacchetti

- **Firewall e Filtri di Pacchetti**: Configurare firewall o filtri di pacchetti per monitorare e bloccare traffico ARP sospetto o non autorizzato.

VPN (Virtual Private Network)

- **Segregazione del Traffico**: Utilizzare VPN per isolare e proteggere il traffico di rete, rendendo difficile per un attaccante all'interno della LAN intercettare o manipolare il traffico.

Protezione Endpoint

- **Antivirus e Anti-Malware**: Utilizzare soluzioni di sicurezza endpoint che includano funzionalità di rilevamento e prevenzione di attacchi ARP spoofing.

- **Rilevamento di Intrusioni (IDS)**: Implementare sistemi di rilevamento di intrusioni per monitorare la rete alla ricerca di attività sospette correlate a ARP Poisoning.

Segmentazione della Rete

- **VLAN (Virtual Local Area Network)**: Segmentare la rete in VLAN per limitare la portata di eventuali attacchi e ridurre la superficie d'attacco.

- **Network Access Control (NAC)**: Utilizzare NAC per controllare l'accesso alla rete e garantire che solo dispositivi autorizzati possano comunicare.

Protocollo IPv6

- **Migrazione a IPv6**: Considerare la migrazione a IPv6, che utilizza il protocollo Neighbor Discovery Protocol (NDP) invece di ARP, riducendo la vulnerabilità a questo tipo di attacchi.

Monitoraggio e Logging

- **Monitoraggio Continuo**: Implementare soluzioni di monitoraggio continuo della rete per identificare e rispondere rapidamente a tentativi di ARP Poisoning.

- **Logging Dettagliato**: Configurare il logging dettagliato degli eventi di rete per facilitare l'analisi forense in caso di attacchi.

Educazione e Consapevolezza

- **Formazione del Personale**: Educare gli utenti e il personale IT sui rischi e le contromisure relative all'ARP Poisoning.

- **Policy di Sicurezza**: Stabilire e implementare policy di sicurezza rigorose che includano best practice per la protezione contro attacchi di rete.

Conclusione

L'ARP Poisoning rappresenta una minaccia significativa per le reti locali, ma con l'implementazione di misure di sicurezza adeguate, è possibile mitigare efficacemente questo rischio. La combinazione di soluzioni hardware e software, insieme a una robusta policy di sicurezza e formazione del personale, può proteggere le reti da attacchi di ARP spoofing.