Descrizione sintetica

1. **Spiegazione del funzionamento dell'ARP Poisoning:** L'ARP Poisoning è un attacco che colpisce i dispositivi all'interno della stessa rete LAN, permettendo a un aggressore di intercettare il traffico non criptato degli utenti e di utilizzarlo per scopi dannosi. Questo tipo di attacco è un esempio di Man in the Middle Attack (MITM).

Fasi dell'attacco:

- **Prima fase:** L'aggressore invia risposte ARP non richieste al dispositivo vittima, facendogli credere che il suo indirizzo MAC sia quello del router. In questo modo, il dispositivo vittima invia tutto il traffico destinato al router verso l'aggressore.
- **Seconda fase:** L'aggressore esegue un'operazione simile sul router, facendogli credere che l'IP dell'aggressore corrisponda al MAC della vittima. Di conseguenza, il traffico dal router verso la vittima passa prima attraverso l'aggressore, che può analizzarlo.

Procedura pratica dell'attacco:

- Abilitare l'IP Forwarding sulla macchina vittima: echo 1 > /proc/sys/net/ipv4/ip_forward
- Generare risposte ARP false con i comandi:

  arpspoof -i eth0 -t <IP_VITTIMA> <IP_ROUTER>

  arpspoof -i eth0 -t <IP_ROUTER> <IP_VITTIMA>
- Intercettare e analizzare il traffico usando strumenti come Wireshark.

2. **Sistemi vulnerabili all'ARP Poisoning:** Qualsiasi dispositivo all'interno di una rete LAN che non adotti misure di sicurezza adeguate può essere vulnerabile all'ARP Poisoning. In particolare, i sistemi che trasmettono dati non criptati sono i più a rischio.
3. **Modalità di mitigazione, rilevamento e prevenzione dell'attacco:**
   - **Uso di protocolli di sicurezza:** Implementare protocolli di comunicazione sicura come HTTPS, SSL/TLS, per cifrare il traffico di rete. Questa è una pratica essenziale per proteggere le informazioni sensibili.

- **Monitoraggio del traffico di rete:** Utilizzare software di sicurezza come IDS (Intrusion Detection System) per monitorare costantemente il traffico e rilevare attività sospette. Questo richiede investimenti in strumenti di sicurezza.
- **Educazione del personale:** Formare il personale sulle buone pratiche di sicurezza informatica. Questa strategia include sessioni di formazione e aggiornamenti periodici, comportando un impegno di tempo e risorse da parte dell'azienda.