Esercitazione WEEK 15 D1 (2)

ARP Poisoning

Ettore Farris - 05/02/2024

Descrizione sintetica

- 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.

- **Spiegare brevemente come funziona l'APR Poisoning**

Un attacco ARP Poisoning colpisce i sistemi che fanno parte di una stessa rete LAN. Un attaccante potrebbe intercettare il traffico non crittografato degli altri utenti e utilizzarlo per scopi malevoli. L'ARP Poisoning è un esempio di Man in the Middle Attack.

L'attacco è diviso in due fasi: nella prima, la macchina attaccante manda delle risposte ARP non richieste al dispositivo vittima affermando che il suo indirizzo MAC è associato a quello del router. In questo modo si fa credere alla vittima che l'attaccante è il router, costringendola di fatto ad inoltrare il traffico destinato ad altre reti alla macchina attaccante. Nella seconda fase si fa lo stesso col router, ovvero si fa credere a questo che l'IP della macchina attaccante è associato al MAC della macchina vittima: in questo modo il traffico proveniente da internet verso la vittima, viene prima inoltrato alla macchina attaccante che può ispezionarlo.

Dal punto di vista pratico, l'attacco richiede due passaggi:

- Attivazione dell'IP Forwarding sulla macchina vittima mediante il comando *"echo 1 > /proc/sys/net/ipv4/ip_forward"*
- Generare le false risposte ARP lanciando contemporaneamente:
  "arpspoof -i eth0 -t <IP_TARGET> <IP_ROUTER>"
  "arpspoof -i eth0 -t <IP_ROUTER> <IP_TARGET>"

Il traffico può essere poi intercettato e analizzato con Wireshark.

- **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.

- L'attacco è efficace quando viene trasmesso del traffico di rete non cifrato. Pertanto è necessario usare protocolli sicuri come HTTPS, SSL TLS ecc. Questa è sempre una buona pratica di sicurezza da tenere in considerazione.
- Per difendersi da attacchi ARP si può monitorare il traffico di rete, anche mediante l'utilizzo dei software di sicurezza che monitorano costantemente il traffico di rete, come un IDS. Questo richiede un costo da parte dell'azienda.
- Educazione del personale. Investimento in disseminazione di buone pratiche di sicurezza da adottare all'interno dell'azienda. Questo ovviamente richiede tempo e denaro investito in formazione.