W15D2

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.

Spiegazione:

E’ un tipo di attacco basato su intercettazione di traffico di dati mediante switch, un man in the middle essenzialmente.

Mitigazione:

La protezione offerta da un buon NAC (Network Access Control), ovviamente, non è limitata a una sola tecnologia, ma deve la sua efficacia a un insieme di soluzioni ben integrate tra loro.

Un NAC deve quindi, innanzitutto, rilevare i dispositivi di rete autorizzati e creare così una “baseline” grazie alla quale individuare subito quelli estranei. Solo a questo punto entrano in gioco tecnologie che si occupano specificamente di rilevare attacchi come ARP Poisoning e MAC Spoofing. E per offrire un ulteriore livello di difesa, ecco che un NAC di alto livello include anche sistemi di autenticazione come LDAP, RADIUS e AD o password manager.