ARP POISONING

ATTACCHI ALLE RETI(2)

TRACCIA:

- Spiegare brevemente come funziona l'ARP Poisoning
- Elencare i sistemi che sono vulnerabili a ARP Poisoning
- Elencare le modalità per mitigare, rilevare o annullare questo attacco

---

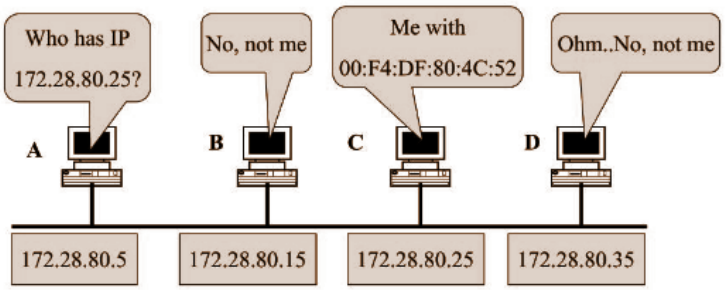
COSA FA L'ARP?

ADDRESS RESOLUTION PROTOCOL

Accetta le richieste: quando un nuovo dispositivo chiede di collegarsi alla rete locale (LAN), fornendo un indirizzo IP.

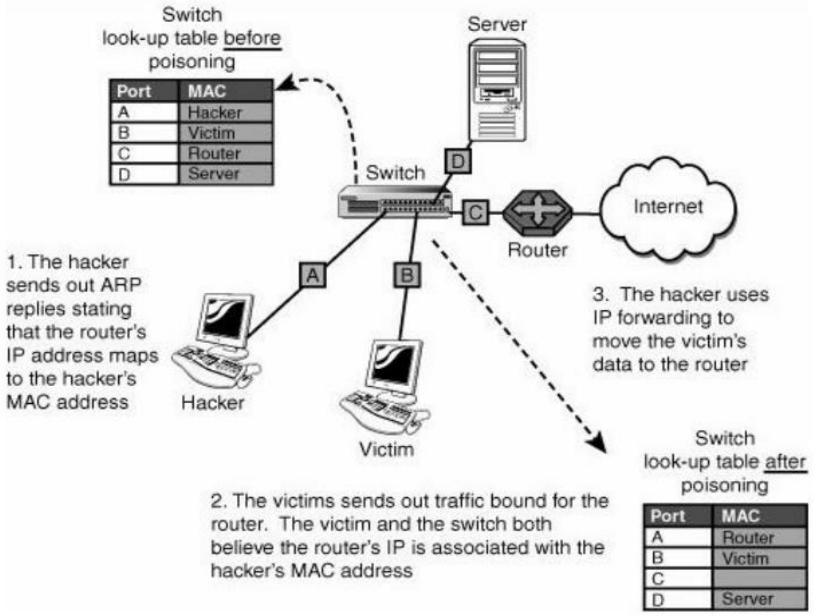
Tradurre: cioè quando i dispositivi sulla LAN non comunicano tramite indirizzo IP, l'ARP converte l'indirizzo IP in un indirizzo MAC.

Invia richieste: se l'ARP non conosce l'indirizzo MAC da utilizzare per un indirizzo IP, invia una richiesta di pacchetto ARP, che interroga altre macchine sulla rete per ottenere ciò che manca.



COME FUNZIONA L'ARP POISONING

Gli hacker utilizzano una serie prevedibile di passaggi per assumere il controllo di una LAN. Inviano un pacchetto ARP falsificato, inviano una richiesta che si connette allo spoofing e prendono il sopravvento. La richiesta viene trasmessa a tutti i computer della LAN e il controllo è completo.



SISTEMI VULNERABILI A ARP POISONING

Un dispositivo connesso a rete locale (LAN) e che utilizza il protocollo ARP può essere assoggettato a questo tipo di attacco. Quindi possono essere vulnerabili sistemi come:

- PC e Laptop
- Smartphone
- Tablet
- Switch
- Router

COSA FARE PER MITIGARE RILEVARE E/O ANNULLARE QUESTI ATTACCHI

- *Iniettare pacchetti ARP falsificati nella rete.* Un attacco di spoofing come questo ti aiuta gestire l'accesso alla rete monitorando i pacchetti IP in entrata e in uscita. I pacchetti sono consentiti o arrestati in base agli indirizzi IP, alle porte e ai protocolli di origine e destinazione.
- *Utilizzare una rete privata VPN* I dispositivi si connettono attraverso un tunnel crittografato e tutte le comunicazioni vengono immediatamente crittografate.
- *La crittografia può essere utile:* se un hacker scava nel tuo sistema e ottiene solo testo confuso senza chiave di decodifica, il danno è limitato. Ma è necessario applicare la crittografia in modo coerente per una protezione completa. Sebbene la crittografia non impedisca effettivamente il verificarsi di un attacco ARP, può mitigare il potenziale danno. Un uso popolare degli attacchi MiTM era quello di acquisire le credenziali di accesso che una volta venivano comunemente trasmesse in testo normale. Con l'uso diffuso della crittografia SSL / TLS sul web, questo tipo di attacco è diventato più difficile.
- *Impostare un ARP statico:* Questi ARP vengono aggiunti alla cache e conservati su base permanente. Questi serviranno come mappature permanenti tra indirizzi MAC e indirizzi IP.
- *Monitora il traffico ARP* e cerca le incoerenze di mappatura

Molte aziende forniscono dei programmi di monitoraggio per supervisionare la rete che per individuare problemi di ARP:

- Arpwatch: Monitora l'attività ethernet, inclusa la modifica degli indirizzi IP e MAC, tramite questo strumento Linux. Controlla il registro ogni giorno e accedi ai timestamp per capire quando è avvenuto l'attacco.
- ARP-GUARD: Accedi a una panoramica grafica della tua rete esistente, incluse illustrazioni di switch e router. Consenti al programma di sviluppare una comprensione di quali dispositivi sono sulla tua rete e crea regole per controllare le connessioni future.
- XArp: utilizzare questo strumento per rilevare gli attacchi che si verificano al di sotto del firewall. Ricevi una notifica non appena inizia un attacco e utilizza lo strumento per determinare cosa fare dopo.
- Wireshark: utilizza questo strumento per sviluppare una comprensione grafica di tutti i dispositivi sulla tua rete. Questo strumento è potente, ma potresti aver bisogno di competenze avanzate per implementarlo correttamente.