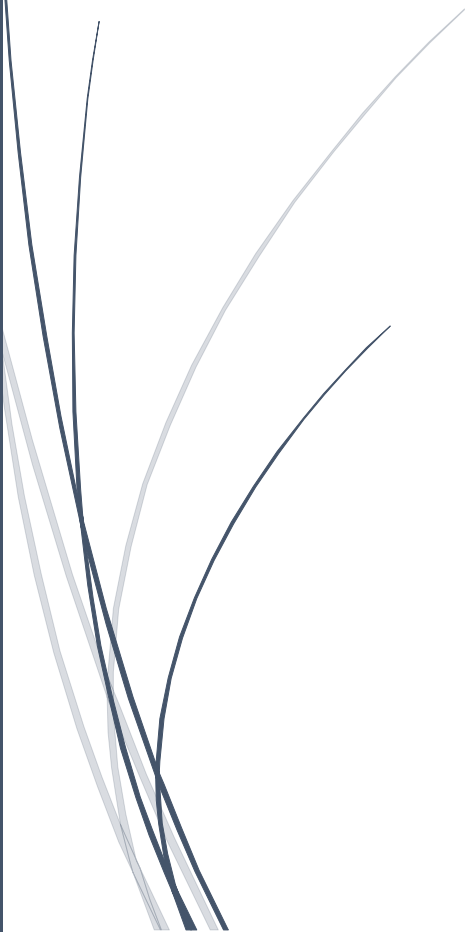


A dark blue vertical bar runs down the left side of the slide. A blue arrow points to the right from this bar, containing the date.

30/05/2024

Vulnerability Assessment ARP Poisoning

Esercizio Modulo 4 - Week 15 – D2
[Orazio Ciccozzi](#)

Several thin, curved lines in dark blue and light grey originate from the bottom left corner and sweep upwards and to the right, creating a sense of movement or a stylized wave.

Sommario

Introduzione 2

Cosa vuol dire Null Session..... 2

Sistemi che sono vulnerabili a Null Session..... 2

Modalità per mitigare o risolvere questa vulnerabilità..... 2

Introduzione

Nella lezione teorica abbiamo visto la Null Session, vulnerabilità che colpisce Windows

- 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
- Commentare queste azioni di mitigazione, spiegando l'efficacia e l'effort per l'utente/azienda.

Cosa è l'ARP Poisoning

L'attacco ARP Poisoning è una tecnica malevola utilizzata per intercettare, analizzare o manipolare il traffico di rete all'interno di una LAN (rete locale). Questo attacco sfrutta il protocollo ARP (Address Resolution Protocol) per inviare informazioni ARP false sulla rete, promuovendo il proprio indirizzo MAC come il legittimo indirizzo MAC del router o di un'altra macchina. Ciò consente all'attaccante di intercettare il traffico di rete tra le macchine e il router o di dirottare questo traffico ogni volta che una macchina invia un pacchetto al gateway o al router.

Sistemi che sono vulnerabili all'ARP Poisoning

L'attacco ARP Poisoning colpisce esclusivamente i sistemi all'interno di una LAN, in particolare tutte le macchine che utilizzano lo stesso gateway e lo stesso indirizzo IP di rete. In altre parole, gli utenti all'interno della stessa rete locale saranno vulnerabili all'attacco ARP Poisoning.

Modalità per mitigare o risolvere questa vulnerabilità

Esistono diverse tecniche per mitigare questo tipo di attacco:

1. Utilizzo di protocolli di sicurezza: i protocolli come HTTPS, SSL, TLS o VPN crittografano i dati in transito e impediscono agli attaccanti di leggerli o manipolarli.
2. Utilizzare Switch livello 3: in questo modo si divide la rete in sottoreti, ma gli switch layer 3 hanno un costo maggiore e richiedono configurazione.
3. Monitoraggio costante: controllare regolarmente la rete per individuare eventuali intrusioni, come accessi non autorizzati o attacchi di ARP poisoning.