W15D1 - Null Session e ARP Poisoning

- **Null Session**:

Una Null Session è una connessione fatta a un computer Windows tramite la rete, senza bisogno di inserire nome utente o password. Veniva usata soprattutto per collegarsi ai servizi di condivisione file (come SMB o NetBIOS). In passato, permetteva a chi si collegava di vedere informazioni importanti del sistema, come la lista degli utenti, i gruppi, le cartelle condivise e alcune impostazioni. Per questo poteva essere sfruttata da un attaccante per raccogliere dati utili e preparare un attacco.

- Elencare i sistemi che sono vulnerabili a Null Session e se sono ancora in commercio

I sistemi più vulnerabili alla Null Session sono:

1. Windows NT
2. Windows 2000
3. Windows XP
4. Windows Server 2003

Questi sistemi permettevano connessioni anonime (senza login) ai servizi di rete come SMB/NetBIOS, e quindi erano a rischio.

- Elencare le modalità per mitigare o risolvere la vulnerabilità Null Session

1. Disabilitare l'accesso anonimo nei criteri di sicurezza di Windows.
2. Bloccare le porte SMB/NetBIOS sul firewall.
3. Rimuovere le condivisioni anonime o impostare permessi più restrittivi.
4. Aggiornare sistemi vecchi (es. Windows XP, Server 2003).
5. Disattivare NetBIOS dove non serve.
6. Configurare Samba in modo sicuro, senza accesso guest.
7. Segmentare la rete per isolare i servizi di condivisione file.
8. Monitorare i log per individuare accessi sospetti.

- **ARP Poisoning**

L'ARP Poisoning è un attacco che avviene nelle reti locali (LAN). L’attaccante invia messaggi ARP falsi per ingannare i dispositivi della rete e far credere che il suo indirizzo MAC corrisponde a un IP importante, come quello del gateway. In questo modo, il traffico della rete passa attraverso l’attaccante, che può spiarlo, modificarlo (attacco man-in-the-middle) o bloccarlo (attacco DoS).

- Elencare i sistemi che sono vulnerabili a ARP Poisoning

qualsiasi dispositivo IPv4 sullo stesso dominio di broadcast è potenzialmente vulnerabile.

- Elencare le modalità per mitigare, rilevare o annullare l’ARP Poisoning

Mitigare:

- Attivare Dynamic ARP Inspection (DAI) sui switch gestiti.
- Usare ARP statici per gateway e host importanti.
- Separare la rete in VLAN e usare port security.
- Usare HTTPS, VPN, SSH per proteggere i dati anche se intercettati.
- Aggiornare dispositivi di rete e firmware.

Rilevare:

- Usare strumenti come arpwatch, Wireshark o Snort.
- Controllare se l’indirizzo MAC cambia per lo stesso IP.
- Cercare rallentamenti o errori nei certificati (MITM).

Annullare:

- Scollegare il dispositivo sospetto.
- Cancellare la cache ARP (es. arp -d + ping il gateway).
- Impostare ARP statico (arp -s IP MAC).
- Analizzare i pacchetti con Wireshark per prove.