Null Session

Una **Null Session** è una connessione anonima a un server Windows tramite SMB (Server Message Block) o NetBIOS. Questa connessione viene chiamata "null" perché non richiede un nome utente o una password per autenticarsi, permettendo a un attaccante di accedere a risorse di rete condivise o a informazioni sensibili come elenchi di utenti, gruppi, servizi di rete, ecc.

Sistemi vulnerabili

I sistemi vulnerabili alle Null Session includono:

- **Windows NT 4.0**
- **Windows 2000**
- **Windows XP**
- **Windows Server 2003**

Questi sistemi operativi sono obsoleti e non sono più supportati ufficialmente da Microsoft. Tuttavia, possono ancora essere in uso in ambienti legacy.

Mitigazione

Per mitigare o risolvere questa vulnerabilità, si possono adottare le seguenti misure:

1. **Aggiornamento dei Sistemi Operativi:** Passare a versioni più recenti e supportate di Windows, che non permettono più le Null Session.
2. **Configurazione delle policy di sicurezza:** Modificare le impostazioni di sicurezza per limitare o disabilitare l'accesso anonimo tramite SMB e NetBIOS.
3. **Firewall:** Configurare il firewall per bloccare il traffico SMB/NetBIOS da sorgenti non fidate.
4. **Audit e Monitoraggio:** Monitorare i log di rete e di sicurezza per identificare eventuali tentativi di connessione anonima.

ARP Poisoning

L'**ARP Poisoning** (o **ARP Spoofing**) è un attacco di rete in cui un attaccante invia messaggi ARP (Address Resolution Protocol) falsificati sulla rete locale (LAN). L'obiettivo è associare l'indirizzo MAC dell'attaccante con l'indirizzo IP di un altro dispositivo sulla rete, come il gateway. Questo consente all'attaccante di intercettare, modificare o bloccare il traffico di rete tra i dispositivi.

Sistemi vulnerabili

Tutti i dispositivi che utilizzano ARP (Address Resolution Protocol) sono potenzialmente vulnerabili all'ARP Poisoning, inclusi:

- **Sistemi Windows, Linux, macOS**
- **Router**

- **Switch non gestiti**
- **Dispositivi IoT**

Mitigazione

Per mitigare o prevenire l'ARP Poisoning, si possono adottare le seguenti misure:

1. **Static ARP Entries:** Configurare manualmente le tabelle ARP con voci statiche per dispositivi critici (come il gateway).
2. **Use of Secure ARP Protocols:** Implementare protocolli sicuri come **Dynamic ARP Inspection (DAI)** su switch gestiti, che verificano l'integrità delle risposte ARP.
3. **Encryption:** Usare protocolli cifrati come **HTTPS**, **SSH**, **VPN** per proteggere i dati anche se l'attaccante riesce a intercettare il traffico.
4. **Intrusion Detection Systems (IDS):** Utilizzare IDS per rilevare comportamenti anomali legati all'ARP, come l'invio massiccio di pacchetti ARP.
5. **Network Segmentation:** Segmentare la rete in modo da limitare l'accesso ai dispositivi sensibili, riducendo l'impatto di eventuali attacchi.