Null session e ARP Poisoning

Sommario

Traccia esercizio

Null Session:

- Spiegare brevemente cosa vuol dire Null Session
- Elencare i sistemi che sono vulnerabili a Null Session e se sono ancora in commercio
- Elencare le modalità per mitigare o risolvere questa vulnerabilità

ARP Poisoning:

- 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

Esercizio Facoltativo

Per NULL Session e ARP Poisoning:

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

Svolgimento esercizio

Null Session

1. Cosa vuol dire Null Session?

Una Null Session è una connessione non autenticata a un server Windows. Questo significa che un utente (o un attaccante) può connettersi senza inserire nome utente o password e accedere ad alcune informazioni del server. In passato, questa funzionalità era pensata per facilitare la condivisione di risorse in rete, ma rappresenta un rischio di sicurezza perché permette a chiunque di ottenere informazioni come nomi degli utenti, gruppi o condivisioni di rete, che possono essere sfruttate per attacchi più avanzati.

2. Sistemi vulnerabili a Null Session

I seguenti sistemi operativi Windows, ora legacy, erano vulnerabili a Null Session:

- Windows NT 4.0
- Windows 2000
- Windows XP
- Windows Server 2003
- Windows Vista
- Windows 7
- Windows 8

Questi sistemi non sono più supportati da Microsoft e non dovrebbero essere utilizzati. Tuttavia, è possibile che alcune aziende o organizzazioni utilizzino ancora questi sistemi in ambienti specifici, ma ciò li espone a rischi elevati.

3. Modalità per mitigare o risolvere la vulnerabilità

- Aggiornare il sistema operativo: Passare a versioni di Windows moderne (come Windows 10 o Windows Server 2016/2019) elimina il problema, poiché queste versioni hanno rimosso o disabilitato le Null Session.
- Disabilitare SMBv1 e NetBIOS: Se non è possibile aggiornare subito, si possono disattivare i protocolli SMBv1 e NetBIOS, che sono spesso sfruttati nelle Null Session.
- Limitare l'accesso alle condivisioni di rete: Assicurarsi che solo gli utenti autenticati possano accedere alle risorse condivise.
- Configurare il firewall: Bloccare il traffico non necessario sui protocolli SMB e NetBIOS per ridurre la possibilità di exploit da parte di attaccanti.

ARP Poisoning

1. Come funziona l'ARP Poisoning?

L'ARP Poisoning è un attacco che colpisce le reti locali (LAN). ARP (Address Resolution Protocol) è il protocollo che consente ai dispositivi in rete di trovare l'indirizzo fisico (MAC) di un dispositivo dato il suo indirizzo IP. In un attacco ARP Poisoning, l'attaccante invia informazioni false alla rete, facendo credere ai dispositivi di rete che l'attaccante sia un altro dispositivo, come ad esempio il router. In questo modo, l'attaccante può intercettare o modificare il traffico che passa tra i dispositivi nella rete.

2. Sistemi vulnerabili a ARP Poisoning

Tutti i dispositivi che usano ARP sono potenzialmente vulnerabili, quindi:

- Computer connessi a una rete locale
- Switch e router che non hanno protezioni specifiche contro ARP Poisoning
- Dispositivi IoT (come telecamere di sicurezza, sensori, ecc.) che si connettono alla rete

3. Modalità per mitigare, rilevare o annullare l'attacco

- Aggiungere voci ARP statiche: Configurare manualmente le tabelle ARP sui dispositivi critici (come il gateway) impedisce che vengano sostituite da informazioni false.
- Sicurezza delle porte (Port Security): Nei dispositivi di rete come switch, è possibile limitare il numero di indirizzi MAC che possono essere accettati da una singola porta, riducendo il rischio di attacchi.
- Strumenti di rilevamento ARP Poisoning: Utilizzare software come _arpwatch_ o _XArp_ per monitorare la rete e rilevare pacchetti ARP sospetti o falsificati.
- Segmentazione della rete: Suddividere la rete in segmenti più piccoli riduce l'impatto di un possibile attacco.
- Utilizzare VPN o crittografia: Se i dati in transito sono crittografati, anche in caso di avvenuto attacco ARP Poisoning, l'attaccante non potrà leggere le informazioni intercettate.

Svolgimento esercizio facoltativo

Null Session

- **Efficacia**: L'aggiornamento del sistema operativo è la soluzione migliore perché elimina completamente la vulnerabilità. Disabilitare SMBv1 e NetBIOS è una soluzione temporanea ma aiuta a ridurre il rischio.
- **Effort**: Aggiornare il sistema operativo richiede molto lavoro, specialmente in aziende con molte macchine da aggiornare. Tuttavia, è una misura necessaria per garantire la sicurezza a lungo termine. La disabilitazione di SMBv1 e NetBIOS è più semplice, ma richiede comunque la gestione costante per evitare problemi.

ARP Poisoning

- **Efficacia**: L'aggiunta di voci ARP statiche e l'uso di strumenti di rilevamento sono soluzioni efficaci, ma possono essere complicate da implementare in grandi reti. L'uso di VPN e la crittografia dei dati sono altre buone misure perché proteggono i dati anche in caso di attacco.
- **Effort**: Configurare ARP statico richiede tempo e attenzione, soprattutto in reti con molti dispositivi. L'implementazione di misure come la sicurezza delle porte richiede hardware e competenze tecniche. L'uso della crittografia è una buona pratica, ma può introdurre complessità nella gestione della rete.