Esercizi Teoria Null Session

- **1) Cosa vuol dire Null Session**:

- Una Null Session è una connessione di rete anonima o senza autenticazione a un sistema, spesso utilizzata per accedere alle risorse condivise su una rete. In pratica, significa che un utente o un attaccante può stabilire una connessione a una macchina remota senza fornire alcuna credenziale di accesso, ottenendo un accesso limitato alle informazioni condivise sulla rete.

- **2) Sistemi vulnerabili a Null Session**:

- I sistemi operativi Windows NT, 2000, XP, 2003, e versioni precedenti sono vulnerabili alle Null Session. Tuttavia, nelle versioni più recenti di Windows, Microsoft ha implementato contromisure per mitigare questa vulnerabilità.

- **3) Esistenza dei sistemi operativ**i:

- Le versioni di Windows vulnerabili alle Null Session sono state in gran parte sostituite da versioni più recenti o sono diventate obsolete. Pertanto, è improbabile che vengano utilizzate in ambienti aziendali moderni.

- **4) Modalità per mitigare o risolvere la vulnerabilità**:

- Disabilitare le Null Session: Questa è la soluzione principale. Si può fare attraverso la configurazione delle impostazioni di sicurezza su Windows.
- Aggiornare a versioni più recenti di Windows: Migliorare la sicurezza migrando a sistemi operativi più recenti e supportati.
- Utilizzo di firewall: Configurare un firewall per bloccare le connessioni Null Session dall'esterno.

- **5) Commento sulle azioni di mitigazione**:

- Disabilitare le Null Session richiede uno sforzo relativamente basso, ma può avere un impatto significativo sulla sicurezza. Tuttavia, potrebbe essere necessario assicurarsi che la disabilitazione non interferisca con le operazioni legittime di condivisione di risorse.
- L’aggiornamento a versioni più recenti di Windows è un passo importante per garantire la sicurezza, ma potrebbe richiedere un notevole sforzo di pianificazione e migrazione.
- L’uso di firewall è efficace ma richiede la configurazione e la manutenzione continua per garantire che le regole siano aggiornate e appropriate.

Esercizi teoria Arp Poisoning

- **1) Come funziona l'ARP Poisoning**:

- ARP (Address Resolution Protocol) Poisoning, noto anche come ARP Spoofing, è un tipo di attacco di rete in cui un attaccante invia pacchetti ARP falsificati nella rete locale. L'ARP è utilizzato per mappare gli indirizzi IP agli indirizzi MAC all'interno di una rete. Nell'ARP Poisoning, l'attaccante invia pacchetti ARP contraffatti in modo che le vittime siano indirizzate a un indirizzo MAC controllato dall'attaccante anziché al dispositivo legittimo. Questo consente all'attaccante di intercettare o manipolare il traffico tra le vittime o di eseguire altri attacchi, come il Man-in-the-Middle (MITM).

- **2) Sistemi vulnerabili all'ARP Poisoning**:

- Tutti i dispositivi collegati a una rete locale sono potenzialmente vulnerabili all'ARP Poisoning. Questo attacco sfrutta una debolezza nel protocollo ARP stesso e non è specifico di un sistema operativo particolare.

- **3) Modalità per mitigare, rilevare o annullare l'attacco ARP Poisoning**:

- Utilizzo di ARP Inspection: Molti switch di rete supportano la funzionalità di ARP Inspection, che rileva e previene pacchetti ARP contraffatti. Questa è un'azione preventiva efficace.
- Utilizzo di VLAN: La segmentazione di una rete in VLAN separate può limitare l'ampiezza dell'attacco ARP Poisoning, riducendo la superficie di attacco.
- Utilizzo di ARP Cache Monitoring: Monitorare l'ARP cache sui dispositivi di rete e le workstation per rilevare modifiche sospette.
- Implementazione di protocolli di sicurezza: L'utilizzo di protocolli di sicurezza, come IPsec o VPN, può proteggere il traffico di rete da essere compromesso da attacchi ARP Poisoning.

- **4) Commento sulle azioni di mitigazione**:

- L’utilizzo di ARP Inspection è una soluzione efficace per prevenire l'ARP Poisoning e richiede uno sforzo relativamente basso per essere implementata. Tuttavia, potrebbe essere necessario configurare accuratamente i dispositivi di rete per abilitare questa funzionalità.
- L’uso di VLAN può essere efficace per isolare le reti, ma richiede una pianificazione approfondita della topologia di rete e potrebbe comportare un costo aggiuntivo per l'hardware.
- Il monitoraggio dell'ARP cache è utile per rilevare gli attacchi in corso, ma richiede una supervisione costante e può essere reattivo anziché preventivo.
- L’implementazione di protocolli di sicurezza come IPsec o VPN è una soluzione robusta, ma può richiedere un impegno significativo per la configurazione e la gestione.