1. Null Session:

Cosa vuol dire Null Session?

- Una Null Session è una connessione a un sistema Windows senza fornire un nome utente o una password. Sfrutta una configurazione predefinita nei vecchi sistemi operativi Windows, dove era possibile stabilire una connessione anonima con il server tramite il protocollo SMB (Server Message Block). Questo permetteva a un utente non autenticato di accedere a determinate informazioni di rete, come condivisioni di file, liste di utenti e gruppi.

- Sistemi vulnerabili a Null Session:

- I sistemi operativi più vulnerabili sono Windows NT, Windows 2000, Windows XP e alcune versioni di Windows Server 2003. Nei sistemi più moderni, come Windows Vista e versioni successive, questa vulnerabilità è stata mitigata, ma può ancora essere presente se le impostazioni di sicurezza non sono adeguatamente configurate.

- Modalità per mitigare o risolvere questa vulnerabilità:

- Disabilitare le Null Session sul server modificando le impostazioni del registro di sistema.
- Impostare restrizioni su SMB e NetBIOS.
- Applicare patch e aggiornamenti di sicurezza che risolvono queste vulnerabilità.
- Configurare correttamente le policy di sicurezza per limitare l'accesso anonimo.

2. ARP Poisoning:

Come funziona l'ARP Poisoning?

- L'ARP (Address Resolution Protocol) Poisoning è un tipo di attacco di rete in cui un aggressore invia falsi messaggi ARP in una rete locale. Lo scopo è quello di associare l'indirizzo MAC dell'attaccante con l'indirizzo IP di un altro dispositivo sulla rete (ad esempio, il gateway di rete). In questo modo, l'attaccante può intercettare, modificare o interrompere il traffico destinato a quel dispositivo.

- Sistemi vulnerabili a ARP Poisoning:

- Tutti i dispositivi connessi a una rete locale Ethernet sono potenzialmente vulnerabili a questo tipo di attacco, in particolare se non sono implementate misure di sicurezza come la verifica dell'ARP.

- Modalità per mitigare, rilevare o annullare questo attacco:

- Utilizzare switch di rete con funzionalità di "Dynamic ARP Inspection" (DAI), che possono bloccare i pacchetti ARP falsi.
- Implementare l'uso di protocolli sicuri, come l'IPsec, per crittografare il traffico di rete.
- Configurare staticamente le tabelle ARP sui dispositivi critici, limitando così l'uso di ARP dinamico.
- Monitorare la rete con strumenti di rilevamento di intrusioni (IDS) che possano identificare attività sospette legate all'ARP.

Queste spiegazioni ti aiuteranno a completare il tuo compito in modo accurato e dettagliato. Se hai bisogno di ulteriori chiarimenti o di approfondire qualche punto, fammi sapere!