Null Session

1. Cosa vuol dire Null Session:
Una Null Session è una connessione a una risorsa di rete senza bisogno di autenticarsi, cioè senza inserire nome utente e password. Si sfrutta soprattutto su vecchi sistemi Windows per accedere a file e stampanti condivisi.

2. Sistemi vulnerabili a Null Session:
- Windows NT 4.0
- Windows 2000
- Windows XP
- Windows Server 2003
- Alcuni Windows Server 2008

Questi sistemi non sono più in commercio e non ricevono aggiornamenti, ma potrebbero ancora essere usati in vecchie infrastrutture.

3. Come risolvere o mitigare il problema:
- Disabilitare le Null Session: Bloccare le connessioni anonime su file e stampanti condivisi.
- Aggiornare i sistemi: Passare a versioni di Windows più moderne e sicure.
- Configurare il firewall: Chiudere le porte TCP 139 e 445 per impedire queste connessioni.
- Proteggere le risorse condivise: Richiedere sempre l'autenticazione per accedere alle risorse di rete.

ARP Poisoning

1. Come funziona l'ARP Poisoning:
L'ARP Poisoning è un attacco dove un hacker invia messaggi falsi sulla rete locale, facendo credere ai dispositivi che il suo indirizzo MAC appartenga a un altro dispositivo legittimo. Così, il traffico destinato a quell'indirizzo IP viene reindirizzato all'hacker, che può spiarlo o modificarlo.

2. Sistemi vulnerabili a ARP Poisoning:
- Tutti i dispositivi su una rete locale (LAN) che usano ARP per associare gli indirizzi IP agli indirizzi MAC possono essere vulnerabili, inclusi PC, server, router e switch.
- Le reti non protette o non segmentate sono più a rischio.

3. Come prevenire o rilevare questo attacco:
- Impostare ARP statici: Configurare manualmente le associazioni IP-MAC per i dispositivi importanti.
- Usare switch di sicurezza avanzata: Switch con 'Dynamic ARP Inspection' (DAI) possono bloccare l'ARP Poisoning.
- Segmentare la rete: Dividere la rete in VLAN per limitare la portata degli attacchi.
- Monitorare la rete: Usare sistemi di rilevamento delle intrusioni per scoprire attività sospette.
- Passare a IPv6: Con IPv6, l'ARP non viene più usato, eliminando questo problema.

Commento sulle azioni di mitigazione (Facoltativo)

Efficacia delle azioni:
Le misure proposte sono abbastanza efficaci nel ridurre i rischi di Null Session e ARP Poisoning. Disabilitare le Null Session e aggiornare i sistemi è una protezione solida, mentre configurare ARP statici e usare switch con DAI aiuta a prevenire l'ARP Poisoning.
L'implementazione di queste misure può richiedere risorse e tempo. Ad esempio, gestire manualmente gli ARP statici può essere impegnativo su reti grandi. Aggiornare i sistemi e comprare switch più sicuri potrebbe richiedere investimenti, ma è fondamentale per una buona sicurezza. Segmentare la rete e passare a IPv6 sono soluzioni più a lungo termine, ma molto efficaci.