TRACCIA

Nella lezione teorica abbiamo visto la Null Session, vulnerabilità che colpisce Windows

• Spiegare brevemente cosa vuol dire Null Session

• Elencare i sistemi che sono vulnerabili a Null Session

• Questi sistemi operativi esistono ancora oppure sono estinti da anni e anni?

• Elencare le modalità per mitigare o risolvere questa vulnerabilità

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

NULL SESSION

La Null Session è una vulnerabilità che colpisce i sistemi Windows, consentendo un accesso non autorizzato quando un utente si connette a una risorsa utilizzando credenziali nulle o vuote. Questa vulnerabilità è predominante nelle versioni più vecchie di Windows come Windows NT, 2000, XP professional e 2003.

Per affrontare la vulnerabilità Null Session e proteggere i sistemi da possibili attacchi, sono disponibili diverse azioni di mitigazione:

1. **Disabilitazione delle Null Session**: Modificare la configurazione del registro di Windows per disabilitare le connessioni Null Session tramite l'Editor del Registro di sistema.
2. **Implementazione di restrizioni di accesso**: Utilizzare le impostazioni di sicurezza avanzate per limitare l'accesso alle risorse solo a utenti autorizzati.
3. **Aggiornamenti del sistema operativo**: Mantenere aggiornato il sistema operativo con le ultime patch di sicurezza rilasciate da Microsoft, poiché le versioni più recenti di Windows contengono correzioni per la vulnerabilità Null Session.
4. **Formazione degli utenti**: Educare gli utenti sull'importanza delle pratiche di sicurezza informatica, inclusa la protezione delle credenziali di accesso e la consapevolezza dei rischi associati alle connessioni non sicure.
5. **Utilizzo di VPN:** Implementare una VPN per creare una connessione crittografata e sicura tra i dispositivi remoti e la rete aziendale, proteggendo i dati da potenziali attacchi di intercettazione durante il trasferimento attraverso reti pubbliche.
6. **Crittografia dei dati**: Utilizzare la crittografia per proteggere i dati sensibili durante la memorizzazione e la trasmissione, impedendo agli attaccanti di accedere o interpretare le informazioni anche se riescono ad ottenere l'accesso ai sistemi.

Queste azioni di mitigazione lavorano sinergicamente per rafforzare la sicurezza complessiva dei sistemi e delle reti aziendali, non solo mitigando la vulnerabilità Null Session, ma offrendo anche un livello più elevato di protezione contro una vasta gamma di minacce informatiche. Tuttavia, è essenziale notare che queste soluzioni richiedono un impegno continuo per l'implementazione, la manutenzione e il monitoraggio per garantire la loro efficacia nel tempo.

TRACCIA 2

Nella lezione teorica abbiamo visto l'attacco ARP Poisoning

• Spiegare brevemente come funziona l'APR Poisoning

• Elencare i sistemi che sono vulnerabili a APR Poisoning

• Elencare le modalità per mitigare, rilevare o annullare questo attacco

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

ARP POISONING

L'ARP Poisoning, o ARP Spoofing, è un attacco di rete in cui un aggressore invia falsi pacchetti ARP alla rete locale al fine di associare il proprio indirizzo MAC a un indirizzo IP legittimo di un'altra macchina sulla rete. Questo trucco fa sì che il traffico di rete destinato alla macchina legittima venga indirizzato all'aggressore, che può quindi intercettare, manipolare o rifiutare il traffico a suo piacimento.

Sistemi vulnerabili all'ARP Poisoning includono praticamente tutte le reti locali che utilizzano il protocollo ARP per risolvere gli indirizzi IP in indirizzi MAC. Questo include sia reti cablate che wireless e non è legato a un sistema operativo specifico, ma piuttosto alla presenza del protocollo ARP nella rete.

Per mitigare, rilevare o annullare l'ARP Poisoning, sono disponibili diverse modalità:

1. **Utilizzo di ARP Spoofing Detection Tools**: Esistono strumenti software che possono rilevare anomalie nel traffico ARP e avvisare gli amministratori di rete in tempo reale. Questi strumenti possono aiutare a identificare gli attacchi ARP Poisoning prima che causino danni significativi.
2. **Configurazione Statica delle Tabelle ARP**: Impostare manualmente le voci nelle tabelle ARP di dispositivi di rete critici può prevenire gli attacchi ARP Poisoning, in quanto elimina la necessità di risoluzione ARP dinamica.
3. **Utilizzo di VLAN e subnetting**: La segmentazione della rete attraverso VLAN e subnetting può limitare l'impatto degli attacchi ARP Poisoning, poiché riduce la visibilità del traffico ARP agli aggressori.
4. **Monitoraggio del traffico di rete**: Mantenere un monitoraggio costante del traffico di rete può aiutare a individuare modelli sospetti o anomalie che potrebbero indicare un attacco ARP Poisoning in corso.

Queste azioni di mitigazione offrono un'efficace difesa contro gli attacchi ARP Poisoning, tuttavia, ogni approccio ha i suoi pro e contro in termini di efficacia e sforzo richiesto:

- **ARP Spoofing Detection Tools**: Questi strumenti offrono un'ottima capacità di individuare gli attacchi ARP Poisoning in tempo reale, ma richiedono un investimento in termini di costi e di configurazione per implementare e mantenere il monitoraggio continuo della rete.

- **Configurazione Statica delle Tabelle ARP**: Questo approccio è altamente efficace nel prevenire gli attacchi ARP Poisoning, ma richiede un lavoro manuale significativo per mantenere e aggiornare le tabelle ARP statiche, soprattutto in reti di grandi dimensioni.
- **Utilizzo di VLAN e subnetting**: La segmentazione della rete tramite VLAN e subnetting può ridurre l'impatto degli attacchi ARP Poisoning, ma richiede una pianificazione e una configurazione iniziali complesse, oltre a potenziali costi aggiuntivi per l'hardware di rete.
- **Monitoraggio del traffico di rete**: Il monitoraggio costante del traffico di rete può aiutare a individuare gli attacchi ARP Poisoning, ma richiede un'attenta analisi e comprensione del traffico di rete normale per riconoscere le anomalie.

In conclusione, la mitigazione dell'ARP Poisoning richiede un approccio olistico che combini diverse strategie di sicurezza, con un equilibrio tra efficacia e sforzo richiesto per l'implementazione e la manutenzione.