W15D1

Traccia

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

NULL SESSION :

1 – Spiega brevemente cosa vuol dire Null Session.

La condivisione IPC$ è nota anche come connessione di sessione Null. Usando questa sessione, Windows consente agli utenti anonimi di eseguire determinate attività, ad esempio enumerare i nomi degli account di dominio e delle condivisioni di rete

2 – Elencare i sistemi che sono vulnerabili alla Null Session e se sono ancora in commercio.

Ad oggi, sono ancora veramente pochi i sistemi vulnerabili, perlopiù sono sistemi legacy.

3 – Elencare le modalità per mitigare o risolvere questa vulnerabilità.

Una volta connessi alle condivisioni tramite una Null Session, gli aggressori possono potenzialmente enumerare informazioni sul sistema e sull'ambiente, come utenti e gruppi, sistemi operativi, policy password, privilegi, ecc. Con queste informazioni, un utente malintenzionato può conoscere eventuali vulnerabilità o modi per attaccare al meglio i tuoi sistemi.

Per rafforzare la sicurezza e ridurre la “superficie” di attacco, è necessario :

- Aggiorna alla versione più recente di Windows

- Scarica gli ultimi aggiornamenti di sicurezza di Windows

- Disabilitare le null sessions nelle impostazioni di controllo di Windows

- Disabilita la condivisione di file e stampanti per le reti Microsoft(se non è necessaria)

- Blocca NetBIOS sul tuo server Windows

ARP POISONING

1 – Spiegare brevemente come funziona l’ARP POISONING

Nell'ambito della sicurezza informatica, l'ARP poisoning è una tecnica di hacking che consente ad un attacker, in una switched lan, di concretizzare un attacco di tipo man in the middle verso tutte le macchine che si trovano nello stesso segmento di rete

2 – Elencare i sistemi che sono vulnerabili all’ ARP POISONING

Un attaccante può connettersi direttamente o indirettamente a qualsiasi dispositivo layer 2 come uno switch, hub o bridge. Se le impostazioni di sicurezza non sono ottimali.

3 – Elencare le modalità per mitigare,rilevare o annullare questo attacco.

Esistono diversi metodi per prevenire gli attacchi di ARP Poisoning.

Tabelle ARP statiche

È possibile mappare staticamente tutti gli indirizzi MAC in una rete ai loro legittimi indirizzi IP.

Questo metodo è altamente efficace nel prevenire gli attacchi di ARP Poisoning ma aggiunge un enorme impegno amministrativo.

Qualsiasi modifica alla rete richiederà aggiornamenti manuali delle tabelle ARP in tutti gli host, rendendola impossibile per le organizzazioni più grandi.

In ogni caso, nelle situazioni in cui la sicurezza è cruciale, ritagliare un segmento di rete separato in cui vengono utilizzate le tabelle ARP statiche può aiutare a proteggere le informazioni più preziose.

Sicurezza degli switch

La maggior parte delle funzionalità di switch Ethernet sono progettate per ridurre gli attacchi di ARP Poisoning.
Tipicamente note come Dynamic ARP Ispection (DAI), queste

funzionalità valutano la validità di ciascun messaggio ARP e scartano i pacchetti che sembrano sospetti o dannosi.

Il DAI può anche essere configurato per limitare la velocità con cui i messaggi ARP possono passare attraverso lo switch, impedendo efficacemente gli attacchi DOS.

È generalmente considerata la cosa migliore da fare quella di abilitare il DAI su tutte le porte tranne quelle collegate ad altri switch. La funzione non introduce un impatto significativo sulle prestazioni, ma potrebbe essere necessario abilitarla insieme ad altre funzionalità come il DHCP Snooping.

Abilitare la port security su uno switch può anche aiutare a limitare gli attacchi di ARP Poisoning della cache ARP: essa può essere configurata per consentire l'accesso di un solo indirizzo MAC su una porta di switch, impedendo ad un malintenzionato di assumere più identità di rete.

Sicurezza fisica

Anche il controllo dell'accesso fisico alla tua azienda può aiutare a limitare gli attacchi di ARP Poisoning. I messaggi ARP non vengono inviati oltre i confini della rete locale, quindi, gli aggressori devono essere in prossimità della rete target o avere già il controllo di un dispositivo collegato alla rete.

Nel caso delle reti wireless, la vicinanza non significa necessariamente che il cyber criminale ha bisogno di un accesso fisico diretto; un segnale che si estende ad una strada o un parcheggio nelle vicinanze può essere sufficiente.

Isolamento della rete

Come affermato in precedenza, i messaggi ARP non viaggiano oltre la sottorete locale.

Ciò significa che una rete ben suddivisa può essere meno suscettibile all'ARP Poisoning, poiché un attacco in una sottorete non può avere un impatto sui dispositivi collegati ad un'altra. Concentrare le risorse più importanti in un segmento di rete dedicato e più protetto può ridurre notevolmente il potenziale impatto di un attacco di ARP Poisoning.

Crittografia

Nonostante la crittografia non impedirà un attacco ARP, può diminuirne il potenziale danno. Ad esempio, gli attacchi Man in the middle di solito rubavano le credenziali di accesso comunemente trasmesse in testo chiaro.

Con l'uso diffuso della crittografia SSL/TLS sul web, questo tipo di attacco invece è diventato più difficile. Il malintenzionato può ancora intercettare il traffico, ma non può farne nulla nella sua forma crittografata.