- 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.

1. Una Null Session si basa su una vulnerabilità dell'autenticazione delle share di Windows e può essere utilizzata per il recupero di informazioni dalla macchina target come ad esempio: password, utenti di sun sistema, gruppi, processi e programmi aperti. Le Null Session possono essere sfruttate anche da remoto, senza autenticazione ed è quindi possibile usare il proprio PC per attaccare una macchina Windows vulnerabile.
2. Ad oggi i sistemi vulnerabili risultano essere molto pochi e la maggior parte sono sistemi legacy.
3. I sistemi legacy non sono "estinti", ma sono obsoleti e sono in uso ancora oggi, magari in aziende più vecchie, che non hanno aggiornato o non hanno necessità di aggiornare le macchine.
4. Disattivare l'account Guest: l'account guest consente l'accesso alle risorse della rete senza richiedere nessuna credenziale. Questa azione può ridurre gli accessi di utenti non autorizzati. Questa azione è da tenere sempre in considerazione. Un'altra soluzione efficacie è quella di tenere aggiornato il sistema operativo. Microsoft rilascia regolarmente aggiornamenti del SO Windows per migliorarne la sicurezza. Per mitigare i rischi di vulnerabilità è bene aver installato l'ultimo aggiornamento di sicurezza. Limitare l'accesso alle risorse a utenti specifici, utilizzando i permessi appropriati. Questo riduce gli accessi non autorizzati. Utilizzo di un software di sicurezza per Windows che possa monitorare e prevenire l'accesso non autorizzato.

- 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.

1. L'attacco ARP Poisoning è una tecnica malevola utilizzata per intercettare, analizzare o manipolare il traffico di rete all'interno di una LAN. Questo attacco invia informazioni ARP false sulla rete usando l'omonimo protocollo, facendo risultare il suo indirizzo MAC

come il MAC del router o di un’altra macchina. Ciò consente di intercettare il traffico di rete tra macchine e router oppure può deviare il traffico dati ogni volta che una macchina invia un pacchetto al gateway o al router.

2. L'ARP Poisoning colpisce i sistemi all'interno di una LAN, in particolare tutte le macchine che usano stesso gateway stesso IP di rete. In altre parole, gli utenti all'interno della stessa LAN sono vulnerabili all'attacco ARP Poisoning.

Per mitigare/rilevare/annullare l’ARP poisoning:

3. Utilizzare i vari protocolli come HTTPS, SSL, TLS o VPN, che crittografano i dati in transito impendendogli di essere letti o manipolati. L’uso di switch di livello 3: in questo modo si divide la rete in sottoreti, ma gli switch layer 3 presentano un costo elevato e richiedono configurazione ad hoc. Un costante monitoraggio e un regolare controllo di rete per individuare eventuali intrusioni, accessi non autorizzati o attacchi di ARP poisoning.
4. L’utilizzo di adeguati software per la sicurezza: alcuni software antivirus e anti-malware possono individuare e prevenire attacchi ARP poisoning. L’educazione del personale aziendale: informare gli utenti su eventuali rischi di attacco, misure di cybersecurity da adottare e che non tutto il traffico può essere “pulito” può aiutare a prevenire danni.