Facoltativo:W15D1

Per NULL Session e ARP Poisoning: • Commentare queste azioni di mitigazione, spiegando l’efficacia e l’effort per l’utente/azienda.

1. NULL Session Mitigation

Azione di mitigazione: Disabilitare le NULL Sessions

- **Efficacia**: Disabilitare le NULL Sessions è altamente efficace nel prevenire attacchi legati all'abuso di queste sessioni. Le NULL Sessions sono spesso utilizzate dagli attaccanti per ottenere informazioni di rete o di sistema, come la lista degli utenti, gruppi e condivisioni, senza autenticazione. Bloccandole, si riduce la superficie d’attacco e si protegge l'integrità delle risorse di rete.
- **Effort per l’utente/azienda**: L'effort richiesto è moderato. Disabilitare le NULL Sessions richiede configurazioni specifiche del sistema, solitamente a livello di registry (per Windows) o attraverso policy di sicurezza. L'azienda deve verificare che nessuna applicazione o servizio legittimo utilizzi queste sessioni, poiché potrebbe interrompere la funzionalità di alcuni software legacy. Inoltre, è necessario testare attentamente l'impatto sui sistemi prima di implementare il cambiamento in produzione.

2. ARP Poisoning Mitigation

Azione di mitigazione: Implementare ARP Spoofing Detection e Dynamic ARP Inspection (DAI)

- **Efficacia**: L'implementazione di strumenti per la rilevazione dell'ARP Spoofing e il Dynamic ARP Inspection (DAI) è altamente efficace per prevenire attacchi di ARP Poisoning. Queste tecniche permettono di monitorare e filtrare le richieste ARP, bloccando quelle sospette o non autorizzate. DAI, in particolare, verifica le richieste ARP contro una lista di indirizzi MAC/IP conosciuti e autorizzati, rendendo molto più difficile per un attaccante avvelenare la cache ARP di un dispositivo sulla rete.
- **Effort per l’utente/azienda**: L'effort è elevato, soprattutto in ambienti complessi. La configurazione di DAI richiede una gestione accurata delle liste di indirizzi IP e MAC, oltre alla necessità di strumenti e tecnologie specifiche che supportino queste funzionalità (ad esempio, switch che supportano DAI). Inoltre, le aziende devono formare il personale IT per gestire e mantenere correttamente queste configurazioni. La rilevazione di ARP Spoofing potrebbe richiedere l’implementazione di sistemi IDS/IPS o altri strumenti di sicurezza, aumentando la complessità della gestione della rete.