W15D1 – Null session & ARP poisoning

Esercizio obbligatorio ed esercizio facoltativo.

Null session

Null session è una vulnerabilità che permette ad utenti non autorizzati di collegarsi ad un sistema Windows senza autenticazione, quindi senza il controllo di username e password. In generale sfrutta una vulnerabilità nell'autenticazione delle share amministrative per permettere ad un attaccante di collegarsi ad una share locale o remota senza autenticazione. Questa connessione avviene spesso tramite la share IPC$, che è una share con privilegi di amministratore e il logon mostrato è NULL SID, il che significa che l'utente non è autenticato. Per stabilire una null session ci si connette alla share IPC$ con il comando net use, con questa sintassi net use \\[Target_IP]\ipc$ "" /user:"" e con questo comando ci si connette al target senza dare delle credenziali. L'attaccante può quindi portare avanti un information gathering per preparare un successivo attacco, magari raccogliendo username e password, trovando gruppi, registri e consultando le share. L'attaccante può anche ottenere un accesso non autorizzato a delle risorse per le quali non avrebbe avuto le credenziali e i permessi per accedere e può anche tentare una privilege escalation. Le null session possono esse sfruttate per attaccare da remoto e tramite API o RPC (remote procedure call) l'attaccante può svolgere qualsiasi tipo di azione malevola.

Tra i sistemi vulnerabili rientrano le versioni più vecchie di Windows, specialmente Windows NT 4.0, Windows 2000, Windows XP (pre SP3) e Windows Server 2003 perché in queste versioni le null session sono abilitate di default e quindi diventa ancora più facile per un attaccante sfruttare questa vulnerabilità. Anche altri sistemi legacy con versioni vecchie e non più supportate di Windows o del protocollo SMB sono vulnerabili. Queste versioni vecchie di Windows non sono più in vendita ed ovviamente non sono in vendita computer o altri device nuovi con queste versioni del sistema operativo. Tuttavia si trovano ancora queste versioni del sistema operativo in dispositivi venduti come usati nel mercato secondario, oppure in sistemi legacy. Si trovano queste versioni vecchie e vulnerabili anche in aziende che per motivi specifici non hanno potuto aggiornare il sistema operativo o non hanno compreso l'importanza dell'aggiornamento e potrebbe presentarsi il caso di aziende che hanno acquistato una licenza software datata per dei motivi specifici interni, anche se questo avviene molto raramente. Le versioni di Windows più moderne come Windows 10 e 11 e le versioni più recenti di Windows Server 2016/2019/2022 non consentono le null session di default e quindi sono più sicure.

Per quanto riguarda le misure per mitigare e risolvere questa vulnerabilità, per prima cosa bisogna disabilitare le null sessions, specialmente quando si ha a che fare con le versioni più vecchie di Windows che le hanno abilitate di default. Si apre il Registry Editor con regedit.exe, si cerca la seguente chiave HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA per i sistemi Windows XP o 2000 oppure si cerca la chiave HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

per i Windows Server 2003 e si cerca la riga "RestrictAnonymous", per cui si inserisce il valore 1 solamente per limitare le connessioni anonime e quindi le null session oppure si inserisce il valore 2 che, se disponibile, disabilita stabilmente le null sessions. Si può anche applicare una group policy per i sistemi da Windows 2003 in poi, per cui si entra nell'editor gpedit.msc, si naviga fino a security options seguendo questo path Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options e si abilita la policy "Network access: do not allow anonymous enumeration of SAM accounts and shares", che eviterà appunto le connessioni anonime alla base di null session. Disabilitare le null sessions in questo modo è una soluzione molto efficace per limitare le conseguenze negative di questa vulnerabilità e può quindi mitigare e risolvere in modo efficiente la vulnerabilità null session. Richiede una conoscenza media da parte dell'utente singolo per una corretta configurazione, mentre per un'azienda potrebbe essere laborioso disabilitare null session su tutte le macchine e in tutti i sistemi, anche se non è difficile e si possono studiare delle soluzioni di automazione. È la soluzione più efficace se non si può passare ad una versione di Windows aggiornata. Un'altra soluzione utile consiste nel disabilitare l'accesso ad IPC$ share, una share particolare utilizzata per sfruttare la vulnerabilità null session. Per limitare l'accesso a questa share, si entra nel registry editor regedit.exe, si segue il path HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters e sotto DWORD si aggiunge una nuova voce chiamata "NullSessionShares" da lasciare vuota per non permettere nessuna connessione a questa share o inserendo solo con chi e quali share possono essere condivise. È preferibile disabilitare completamente null session e lasciare questa voce vuota. Questa soluzione è mediamente efficace, perché riduce la superficie di attacco, ma non elimina completamente la vulnerabilità, dato che si viene protetti solo da exploit legati a questa specifica share. Questa soluzione non è difficile da implementare, anche se bisogna evitare di bloccare anche operazioni legittime che coinvolgono questa share. Naturalmente per risolvere questa vulnerabilità è possibile anche passare a versioni di Windows non vulnerabili a null session, come Windows 10 e Windows 11 ed eseguire gli aggiornamenti regolarmente, qualora non vi fossero dei motivi specifici per i quali non è possibile passare a versioni del sistema operativo più sicure ed aggiornate. Passare ad un sistema operativo aggiornato e più sicuro è una soluzione estremamente efficace, perché si utilizzano delle versioni che non abilitano null session di default e quindi si va ad eliminare la vulnerabilità alla radice, ma potrebbe richiede da parte del singolo un sforzo in termini di tempo e di acquisto di nuove licenze e per un'azienda potrebbe essere impegnativo passare ad un sistema operativo aggiornato in tutte le macchine e in tutti i sistemi, rendendo necessaria un'accurata programmazione dell'intervento. Qualora fosse necessario tenere queste versioni vulnerabili a null session, una buona misura di mitigazione potrebbe consistere nell'isolare le macchine vulnerabili segmentando la rete, isolandole anche con delle regole del firewall che limitino le interazioni tra queste macchine ed altre macchine della rete non vulnerabili. Questa soluzione è molto efficace nel mitigare il rischio per tutta la rete, perché con una giusta configurazione si evitano movimenti laterali che possono portare l'attaccante ad arrivare ad altri sistemi, ma richiede delle conoscenze specifiche per essere implementata. Come altra misura si può disabilitare SMBv1, un

protocollo con una versione vecchia e spesso associato alla vulnerabilità null session con il comando Set-SmbServerConfiguration -EnableSMB1Protocol $false dalla Power Shell di Windows. Questa soluzione è molto efficace contro null session e protegge anche da molte altre vulnerabilità, dato che viene disattivata una versione vecchia di un protocollo associato anche ad altri problemi, come il malware WannaCry ed è anche facile da implementare tramite la Power Shell. Si possono anche applicare dei network access control (NAC) che evitano che macchine con configurazioni non sicure dall'esterno, che ad esempio consentono le null session, possano collegarsi alla nostra rete. Questa soluzione è molto efficace, perché aggiunge un ulteriore livello di protezione per la rete, ma è anche complessa da implementare e richiede conoscenze specifiche. Come sempre, è utile applicare dei controlli sugli accessi e sui tentativi di accesso tramite dei tool per il network monitoring e verificare sempre i permessi per i file e per le share per evitare che siano consentiti accessi non voluti o non autorizzati, anche se non è consigliabile puntare solo su questa strategia, dato che non previene l'attacco. Infine serve sempre sensibilizzare gli amministratori e gli utenti di una rete circa i pericoli di questa vulnerabilità, perché degli utenti consapevoli possono agire tempestivamente per prevenire o evitare danni. Riassumendo, la soluzione più efficace anche nel lungo periodo consiste nel passare ad una versione più aggiornata e quindi più sicura del sistema operativo, invece per avere dei benefici più rapidi ed immediati serve disabilitare le null session e limitare l'accesso alla share IPC$, e sul lungo periodo si può pensare ad una segmentazione della rete per proteggersi ulteriormente.

ARP poisoning

ARP poisoning, chiamato anche ARP spoofing, è un tipo di attacco che intercetta del traffico su una rete basata su uno switch, un attacco basato quindi sulla manipolazione della tabella ARP in una rete locale, per cui un attaccante riesce ad associare il proprio indirizzo MAC all'IP di un dispositivo, di un gateway o di uno switch. In questo modo è in grado di intercettare le comunicazioni dirette all'IP a cui è associato ed eventualmente bloccare o modificare le comunicazioni che passano per il nodo con l'IP a cui l'attaccante si è associato. In preparazione all'attacco, l'attaccante mappa la rete per associare indirizzi IP ed indirizzi MAC e poi invia dei "gratuitous ARP replies", che sono dei messaggi ARP con informazioni false che comunicano ai dispositivi della rete che l'indirizzo MAC dell'attaccante è associato all'indirizzo IP di un nodo legittimo della rete, come un altro computer oppure uno switch o un altro device. L'attaccante invia quindi delle risposte ARP senza aspettare che un host invii una richiesta ARP e modifica così le tabelle ARP. Di conseguenza la cache ARP dei nodi della rete viene aggiornata, associando il MAC dell'attaccante all'IP legittimo ed ora l'attaccante può intercettare il traffico che passa per il suo nodo nella rete, modificare il contenuto dei dati che passano per il suo nodo, ad esempio iniettando del codice malevolo e può copiare il contenuto dei dati ed inviarlo dove preferisce. È possibile lanciare attacchi man in the middle, portare avanti un session hijacking dopo aver intercettato i token di sessione di un utente, lanciare un attacco DoS o comunque compromettere il corretto funzionamento della rete e rubare dati di qualsiasi tipo.

Per quanto riguarda i sistemi che sono vulnerabili, tutti i sistemi e le reti che utilizzano il protocollo ARP per la mappatura degli indirizzi IP e MAC sono vulnerabili, in particolar modo gli indirizzi IPv4 utilizzano quasi sempre il protocollo ARP e quindi un indirizzo IP versione 4 potrebbe essere vulnerabile. I sistemi più vulnerabili sono le reti LAN, sia che si tratti di LAN con connessioni tramite cavo Ethernet, sia che si tratti di WLAN. I sistemi operativi Windows, Linux e MacOS implementano il protocollo ARP e quindi sono vulnerabili, mentre i dispositivi più a rischio di ARP poisoning sono i router e gli switch, che spesso diventano il bersaglio di questi attacchi per poter intercettare le comunicazioni su una rete. Anche i dispositivi IoT sono a rischio, specie se sono connessi ad una rete senza protezioni per questo tipo di attacco ed anche tutti gli altri tipi di dispositivi che usano il protocollo ARP possono essere vulnerabili. Sono a rischio anche le VPN non configurate bene, così come i sistemi legacy, che essendo vecchi presentano molte vulnerabilità e non implementano misure di sicurezza aggiuntive contro ARP poisoning, come quelle implementare da Windows Defender nelle versioni più recenti di Windows.

Vi sono varie strategie e strumenti per poter individuare un attacco di tipo ARP poisoning: con tool come ARPwatch o XArp si possono notare delle anomalie, come la duplicazione di indirizzi IP o cambiamenti sospetti nelle ARP cache e l'utilizzo di ARP monitoring tools è altamente efficace nella rilevazione in tempo reale di anomalie e richiede uno sforzo moderato in termini di installazione e configurazione. Con il comando arp -a da terminale si può controllare la cache manualmente per cercare eventuali azioni e cambiamenti sospetti. Tool come Wireshark riescono a sniffare il traffico per verificare se ci sono dei movimenti sospetti, come dei passaggi aggiuntivi e non previsti dei pacchetti di dati e i network intrusion detection system NIDS come Snort e Suricata riescono a intercettare delle gratuitous ARP replies sospette e che possono essere alla base di un ARP poisoning. I NIDS sono altamente efficaci nel proteggere da varie minacce, comprese quelle legate ad ARP poisoning, ma richiedono uno sforzo elevato non solo per la configurazione, ma anche per il mantenimento e per vagliare eventuali falsi positivi. Per mitigare il rischio derivante da attacchi basati su ARP poisoning, si possono configurare delle static ARP entries, per evitare che le tabelle ARP vengano modificate manualmente e in modo arbitrario da un attaccante e questa strategia può essere utile soprattutto nei sistemi critici, importanti o particolarmente vulnerabili o sensibili. In questi casi, l'efficacia di questa misura è molto alta e non richiede sforzi eccessivi in termini di configurazione e mantenimento, riuscendo a proteggere velocemente sistemi critici anche in reti molto grandi. In dispositivi come gli switch è possibile anche applicare DAI, ovvero Dynamic ARP Inspection, che verifica le ARP requests e replies per far passare solo le comunicazioni valide sulla base di una tabella ARP validata. Questa soluzione è veramente molto efficace, probabilmente una delle più efficaci contro questa vulnerabilità perché valida i pacchetti ARP in base ad un database già verificato, anche se è complessa da implementare. In generale, il filtraggio dei pacchetti è sempre una buona idea. Negli switch è possibile anche abilitare la feature di port security, che limita il numero di indirizzi MAC associati ad una porta, evitando quindi che la cache ARP venga inondata con troppe ARP responses. È un'idea valida ed efficace e meno complessa rispetto ad altri tool e strumenti indicati precedentemente. Per ridurre la

superficie di attacco si può pensare a delle VLAN, ovvero delle virtual LAN che segmentano la rete creando dei piccoli domini di broadcast e rendendo molto difficile per un attaccante colpire tutta la LAN. Si può pensare anche all'utilizzo di VPN. È una buona idea per proteggere dei segmenti critici di una rete, magari aziendale e non richiede particolari sforzi per essere implementata, se non una pianificazione attenta della rete. Per rendere più sicure le comunicazioni anche in caso di ARP poisoning si può ricorrere alla crittografia end-to-end, usando i protocolli SSL/TLS oppure SSH; è un'ottima soluzione che protegge i dati anche in caso di intercettazione, non troppo difficile da implementare e che protegge anche contro altri tipi di minacce e vulnerabilità. In questo modo, le comunicazioni in transito possono essere intercettate ma saranno comunque criptate. Infine si può implementare anche S ARP o Secure ARP, che usa metodi di crittografia per verificare l'autenticità dei messaggi ARP in una rete; è una soluzione altamente efficace ma anche molto complessa da realizzare, tanto che questo potente strumento non è ancora molto diffuso. Per fermare un attacco basato su ARP poisoning, è necessario per prima cosa isolare l'attaccante, bloccando il suo indirizzo MAC, chiudendo la porta dello switch a cui è collegato il suo dispositivo o prendendo altre misure per isolarlo. Bisogna poi intervenire sulla cache ARP dei dispositivi attaccati, modificando la cache con il comando arp -d su Windows o con il comando ip -s -s neigh flush all su Linux e verificando che poi la tabella ARP venga ricompilata correttamente, associando gli indirizzi MAC ed IP legittimi. Nei casi più gravi, può essere necessario resettare i router e gli switch della rete. Alcune azioni per mitigare il rischio di attacchi basati su ARP poisoning sul lungo termine consistono nel verificare periodicamente, anche con dei tool, che la rete funzioni correttamente e non ci siano comportamenti anomali, aggiornare gli utenti della rete riguardo ai rischi dell'ARP poisoning e fornire strumenti e conoscenze per riconoscere un possibile attacco e utilizzare un next-generation firewall in grado di individuare le azioni alla base di un attacco con ARP poisoning. Utilizzare un next-generation firewall è un'ottima idea, molto efficace contro questo tipo di attacchi e contro altri, anche se richiede un certo sforzo in termini di configurazione e mantenimento. In generale, un singolo utente o una piccola azienda possono proteggersi con la crittografia oppure con le static ARP entries, mentre un'azienda più grande potrebbe optare per opzioni più complesse come VLAN, NIDS, ARP monitoring tools, DAI oppure anche next-generation firewall.