NULL SESSION

Una Null Session si verifica quando si accede a un sistema senza nome utente o password. Le null session NetBIOS sono una vulnerabilità riscontrata nel Common Internet File System (CIFS) o SMB, a seconda del sistema operativo.

I sistemi afflitti sono: Windows Server 2008 R2, Windows 7 e successive, che utilizza SMB e i sistemi Unix/Linux utilizzano CIFS.

Una volta che un utente malintenzionato ha effettuato una connessione NetBIOS utilizzando una sessione nulla a un sistema, può facilmente ottenere un elenco completo di tutti i nomi utente, gruppi, condivisioni, autorizzazioni, policy, servizi e altro utilizzando l'account utente Null. Gli standard SMB e NetBIOS in Windows includono API che restituiscono informazioni su un sistema tramite la porta TCP 139.

Un metodo per connettere una sessione Null NetBIOS a un sistema Windows consiste nell'utilizzare la condivisione nascosta Inter-Process Communication (IPC$). Questa condivisione nascosta è accessibile utilizzando il comando net use.

Il comando "net use" è un comando integrato di Windows che si connette a una condivisione su un altro computer. Le virgolette vuote (“”) indicano che desideri connetterti senza nome utente e senza password. Per creare una sessione NetBIOS nulla su un sistema con l'indirizzo IP 192.21.7.1 con l'account utente anonimo integrato e una password nulla utilizzando il comando net use, la sintassi è la seguente:

net use \\192.21.7.1 \IPC$ "" /u: ""

Una volta completato con successo il comando net use, l'aggressore dispone di un canale su cui utilizzare altri strumenti e tecniche di hacking.

Disabilitare le sessioni nulle è un modo fondamentale per aiutare a rafforzare la sicurezza e ridurre la superficie di attacco.

È possibile configurare il computer in modo che usi l'identità del computer per il sistema locale con i criteri Sicurezza di rete: Consenti al sistema locale di usare l'identità del computer per NTLM. Se ciò non è possibile, questo criterio può essere usato per impedire che i dati vengano esposti in transito se sono stati protetti con una chiave nota.

Se si abilita questo criterio, i servizi che usano una sessione NULL con sistema locale potrebbero non riuscire a eseguire l'autenticazione perché non potranno usare la firma e la crittografia.

ARP POISONING

Un elemento debole nella catena di sicurezza è la Local Area Network (LAN): se un hacker si trova già nella rete interna, riuscirà ad intrufolarsi nel traffico dati, sfruttando la vulnerabilità del protocollo ARP.

Questo protocollo viene utilizzato nelle reti Ethernet basate su IPv4 per risolvere gli indirizzi IP in quelli MAC.

Questa vulnerabilità è presente in ogni sistema operativo lato server in quanto sfrutta una vulnerabilità della reta.

inviare un pacchetto di risposta con informazioni false e manipolare così la tabella ARP del computer richiedente si chiama ARP poisoning, un “avvelenamento” della cache ARP.

Di solito il pacchetto comprende anche l'indirizzo MAC di un dispositivo di rete, controllato dall'hacker. Il sistema della vittima collega così l'IP di uscita con un indirizzo dell'hardware falso e in seguito invia tutti i pacchetti al sistema controllato dall'hacker.

Per rimanere nascosto, il traffico dati ascoltato viene solitamente inoltrato ad un sistema di destinazione reale. Un hacker ottiene così con l'inganno lo status di man in the middle**.**

Se i pacchetti intercettati non vengono inoltrati, bensì rifiutati, l'ARP poisoning può comportare un Denial of Service (DoS).

Anche la crittografia tramite Wi-Fi Protected Access (WPA) non offre un'adeguata protezione contro questa tecnica. Infatti per poter comunicare nelle reti locali IPv4, devono essere risolti tutti gli indirizzi MAC collegati e ciò avviene solo attraverso il protocollo ARP.

I programmi che vengono utilizzati per l'ARP poisoning come software di attacco vengono trattati solitamente come strumenti di sicurezza e sono disponibili in rete liberamente:

- **ARP0c/WCI:** secondo la pagina del servizio, ARP0c/WCI è un tool che utilizza l'ARP spoofing per intercettare le connessioni in una rete privata. Così il software invia pacchetti di risposta ARP falsi, che devia il traffico dati sul sistema, funzionante su ARP0c/WCI. Un reindirizzamento al sistema di destinazione vero e proprio avviene tramite il bridging engine integrato. Un attacco man in the middle avviene così indisturbato
- **Arpoison:** il tool da riga di comando che genera dei pacchetti ARP personalizzati, in cui l'utente può stabilire a piacere l'indirizzo del mittente e del destinatario. Lo strumento è disponibile liberamente e con licenza GNU.

- **Ettercap:** Ettercap è un tool di ARP poisoning per gli attacchi man in the middle. È possibile automatizzare azioni come quelle di sniffing, degli attacchi ARP e della raccolta di password. Ettercap può manipolare i dati intercettati e attacca anche le connessioni che sono protette tramite SSH o protocollo SSL. Il programma viene ufficialmente offerto come software per la sicurezza e funziona anche per i test di prodotti.

- **NetCut:** con il software per la gestione di rete NetCut gli amministratori si occupano della loro rete basata sul protocollo ARP. Lo strumento individua tutti i dispositivi connessi in rete e restituisce i relativi indirizzi MAC. NetCut è particolarmente indicato per gli attacchi DoS, a patto che l'hacker si trovi nella stessa rete della vittima. Con il software non si possono realizzare gli attacchi man in the middle.

Contromisure

Praticamente tutte le reti IPv4 sono soggette ad attacchi di questo tipo perché l'ARP spoofing utilizza a proprio vantaggio il funzionamento dell'Address Resolution Protocol. Nemmeno l'**introduzione degli indirizzi IPv6** è riuscito a risolvere questo problema.

Il nuovo standard IP rinuncia infatti all'ARP e regola la risoluzione dell'indirizzo nella LAN tramite NDP (Neighbor Discovery Protocol), che è però a sua volta soggetto ad attacchi di spoofing. **Si può risolvere questa falla di sicurezza tramite il protocollo Secure Neighbor Discovery (SEND)**, tuttavia tenendo in conto che è supportato ancora da pochi sistemi operativi per il desktop.

Una protezione possibile per impedire la manipolazione della cache ARP è offerta dalle **tabelle ARP che si possono ad esempio impostare su Windows tramite il programma della riga di comando ARP e l'istruzione *arp –s*.** Visto che non si devono modificare manualmente i record di questo tipo, questa misura preventiva *si limita solitamente ai sistemi più importanti della rete.*

Un'altra misura contro l'uso indebito del protocollo ARP è rappresentata dalla suddivisione della rete tramite gli **switch del livello 3.**

Le risposte broadcast raggiungono così incontrollate solo i sistemi che si trovano nello stesso segmento di rete, mentre le richieste ARP negli altri segmenti vengono verificati dallo switch.

Se questo switch è in funzione sul livello di rete (livello 3), accanto all'indirizzo MAC viene verificato e portato allo stesso stato anche l'indirizzo IP con i record precedenti.

- **Arpwatch**: se lo strumento open source e multipiattaforma Arpwatch viene integrato in una rete locale IPv4, vengono mostrate continuamente tutte le attività ARP che si svolgono nella LAN.

- **ARP-Guard:** anche ARP Guard dell'azienda ISL osserva la rete interna e si basa così su due diversi sensori. Il sensore LAN lavora analogamente come Arpwatch, quindi analizza i pacchetti in entrata e avvisa in presenza di anomalie.

- **XArp**: il software XArp si basa su moduli attivi e passivi per proteggere la rete dall'ARP poisoning. I moduli passivi analizzano i pacchetti ARP, che vengono inviati in rete e aggiornano l'assegnazione dell'indirizzo forniti con i record più vecchi. Se così facendo vengono riscontrate delle anomalie, il programma suona l'allarme.

Anche **l'Intrusion Detection System (IDS)** Snort dispone di un preprocessore integrato contro l'ARP spoofing che consente di controllare il traffico dati nella rete e di creare manualmente delle liste di comparazione. Tale metodo risulta però faticoso rispetto ad altri.

Inoltre i sistemi IDS vengono soprattutto utilizzati nella transizione dalle reti esterne. Se vale la pena di utilizzarli anche in una rete LAN, deve venir stabilito caso per caso. A volte una misura simile può incontrare delle resistenze, perché in un'azienda un amministratore che controlla la rete tramite IDS ha accesso a tutto il traffico di rete e quindi è in grado di sorvegliare tutte le attività dei dipendenti. Per questo motivo si tende a non ricorrere a questa funzione di controllo.