W15D1

NULL SESSION

- E’ una sessione di rete Windows stabilita **senza fornire credenziali** (username/password vuoti). Tecnicamente si tratta di una sessione SMB/NetBIOS in cui il client si autentica come *Anonymous* e ottiene un token con privilegi molto limitati, ma sufficiente per interrogare alcuni servizi remoti.

SISTEMI VULNERABILI

- Computer molto vecchi con Windows (es. Windows XP, Server 2003): erano facilmente vulnerabili. Questi sistemi non vengono più venduti o aggiornati da Microsoft, ma possono ancora essere usati in aziende molto vecchie o in apparecchiature non aggiornate.

- Qualsiasi sistema che usa il vecchio protocollo SMBv1 (non specifico a Microsoft): il protocollo è insicuro. Le versioni moderne di Windows non lo installano di default, però apparecchi più vecchi (alcuni NAS, stampanti di rete, dispositivi industriali) potrebbero ancora usarlo.

- Server Linux/Unix che usano Samba: Samba è il software che permette a Linux di parlare SMB; se è configurato per permettere accesso “guest” o anonimo, può offrire informazioni senza autenticazione. Samba è ancora molto usato oggi — il problema è la configurazione, non il fatto che Samba esista.

- NAS, router o appliance datati: molti dispositivi di rete venduti nel passato (o ricondizionati) potrebbero avere firmware vecchi che lasciano aperto l’accesso anonimo.

MITIGAZIONE DELLA VULNERABILITA’

- Disabilitare il vecchio SMBv1 su server e dispositivi se non serve più.

- Bloccare l’accesso anonimo: impedire che utenti “guest” o connessioni senza password possano chiedere informazioni sul sistema.

- Aggiornare firmware e sistem**i**: patchare NAS, router, server e Samba.

- Filtrare le porte di rete usate da SMB (quelle usate per condividere file) sui firewall per evitare accessi dall’esterno.

- Rimuovere o isolare sistemi legacy che non possono essere aggiornati.

- Controllare i log per vedere tentativi di accesso anonimi.

ARP POISONING

- E’ un attacco a livello **link-layer (Layer 2)** in reti IPv4 basate su Ethernet, in cui un attaccante invia **ARP reply falsificati** per associare il proprio **MAC address** a un **IP di un altro host** (tipicamente il gateway o un altro dispositivo critico). Questo provoca l’aggiornamento della **ARP cache** delle vittime con informazioni errate.

SISTEMI VULNERABILI

- Tutte le reti locali tradizionali dove i dispositivi si fidano automaticamente delle informazioni ARP (cioè quasi tutte le LAN IPv4 non protette): PC, smartphone, stampanti, telecamere, IoT.

- Reti con switch non gestiti o hub: più facili da attaccare perché non hanno protezioni.

- Reti Wi-Fi aperte o deboli: se chiunque può connettersi, è facile per un malintenzionato eseguire l’attacco.

- Dispositivi embedded o vecchi che non implementano contromisure.

MITIGAZIONE DELLA VULNERABILITA’

- Usare switch gestiti che supportano funzioni come DHCP Snooping e ARP Inspection: questi impediscono che pacchetti ARP falsi vengano accettati.

- Abilitare sicurezza per porta (legare indirizzi MAC alla porta fisica) o usare 802.1X per l’autenticazione in rete: riducono la possibilità che dispositivi non autorizzati si connettano.

- Mettere solo dispositivi affidabili nella stessa rete e segmentare la rete per separare IoT/guest dall’infrastruttura critica.

- Usare connessioni cifrate (HTTPS, VPN, SSH): anche se i pacchetti vengono intercettati, il contenuto rimane protetto.

RILEVARE

- Strumenti come **arpwatch** o programmi di monitoraggio che segnalano cambi frequenti nelle associazioni IP→MAC.

- Controllare la lista ARP del computer (`arp -a`) per mapping sospetti.

- IDS/IPS che può riconoscere ARP gratuiti o frequenti cambi di mapping.

ANNULLARE / REAGIRE (se l'attacco è in corso)

- Isolare o disconnettere il dispositivo sospetto dalla rete.
- Ripristinare le corrette associazioni ARP (su host critici si possono impostare entry ARP statiche).
- Abilitare le protezioni sullo switch (DAI / port security).
- Raccogliere prove (registrare traffico) e rafforzare la cifratura delle applicazioni.