# NULL SESSION:

NELLA LEZIONE TEORICA ABBIAMO VISTO LA NULL SESSION, VULNERABILITÀ CHE COLPISCE WINDOWS

**TRACCIA:**

- 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.

## #SPIEGARE BREVEMENTE COSA VUOL DIRE NULL SESSION:

ABBIAMO VISTO A LEZIONE CHE LE NULL SESSION SONO UNA DELLE STORICHE VULNERABILITÀ DELLE SHARE DI WINDOWS (CONDIVISIONE DI FILE O DIRECTORY IN RETE TRAMITE NETBIOS - UN PROTOCOLLO DI LIVELLO SESSIONE).
DI NORMA L'UTENTE CHE CONDIVIDE UNA RISORSA PUÒ IMPOSTARE DEI PERMESSI SU UNA SHARE DI RETE, DECIDENDO CHI PUÒ ESEGUIRE QUALI OPERAZIONI (LETTURA, SCRITTURA E MODIFICA DEI PERMESSI). LE NULL SESSION SI BASANO SU UNA VULNERABILITÀ DELL'AUTENTICAZIONE DELLE SHARE AMMINISTRATIVE DI WINDOWS, CHE PERMETTEVANO AD UN ATTACCANTE DI COLLEGARSI DA REMOTO AD UNA SHARE LOCALE O REMOTE SENZA AUTENTICAZIONE (NO LOGIN, NO PASSWORD). QUESTO RENDEVA ACCESSIBILI MOLTI DATI SENSIBILI COME UTENZE E GRUPPI DI SISTEMA/PASSWORD/PROGRAMMI APERTI E PROCESSI IN ESECUZIONE, PERMETTENDO ALL'ATTACCANTE DI DI ESEGUIRE AZIONI SULLA MACCHINA VITTIMA TRAMITE REMOTE PROCEDURE CALL (API O RPC).

## #ELENCARE I SISTEMI CHE SONO VULNERABILI A NULL SESSION:

TUTTI I SISTEMI MICROSOFT WINDOWS SMBV3 PRECEDENTI AL SET DI PATCH DI APRILE 2022 SOFFRIVANO DI QUESTA VULNERABILITÀ DAL 1990 CIRCA. AD ESEMPIO, INVIANDO UNA RICHIESTA FileNormalizedNameInformation SMBV3 NON VALIDA SU UNA DENOMINATA PIPE UN ATTACCANTE POTEVA CAUSARE UN ARRESTO ANOMALO DELLA MACCHINA CON BLUE SCREEN OF DEATH (BSOD) DEL KERNEL DI WINDOWS, CAUSANDO UN RIAVVIO DEL SERVER SMBV3. QUESTO ATTACCO RICHIEDE AUTENTICAZIONE PER LA MAGGIOR PARTE DEI SISTEMI, TRANNE NEL CASO SPECIFICO DOVE UN UTENTE NON AUTENTICATO PUÒ STABILIRE UNA SESSIONE SMB NULL.
DI SEGUITO LE CVE-ID:

- CVE-1999-0519
- CVE-1999-0520
- CVE-2002-1117

## #QUESTI SISTEMI OPERATIVI ESISTONO ANCORA OPPURE SONO ESTINTI DA ANNI E ANNI?

CITANDO LA LEZIONE:
"NEGLI ANNI SCORSI, LA MAGGIOR PARTE DEI SISTEMI WINDOWS ERA VULNERABILE ALLE «NULL SESSION» E GLI ATTACCHI DI QUESTO TIPO HANNO AVUTO UN IMPATTO ENORME SU TUTTO L'ECOSISTEMA WINDOWS.

AD OGGI, SONO ANCORA VERAMENTE POCHI I SISTEMI VULNERABILI, PERLOPIÙ SONO SISTEMI LEGACY."

## #ELENCARE LE MODALITÀ PER MITIGARE O RISOLVERE QUESTA VULNERABILITÀ:

HO TROVATO QUESTA SOLUZIONE ONLINE:

BISOGNA DISATTIVARE LA REGISTRAZIONE DEGLI EVENTI DI ACCESSO ANONIMO (SU WINDOWS XP E VERSIONI SUCCESSIVE) È POSSIBILE DISATTIVARE COMPLETAMENTE GLI ACCESSI ANONIMI (OVVERO SESSIONI NULL), MA CIÒ POTREBBE INFLUIRE SULL'ACCESSIBILITÀ DA PARTE DEGLI UTENTI NEI DOMINI ATTENDIBILI. PRIMA DI MODIFICARE LE NORME IN TUTTO IL DOMINIO, SI CONSIGLIA DI TESTARLE SU UN NUMERO LIMITATO DI SISTEMI. WINDOWS XP E VERSIONI SUCCESSIVE FORNISCONO 6 CRITERI ELENCATI DI SEGUITO PER CONTROLLARE A QUALI INFORMAZIONI È POSSIBILE ACCEDERE IN MODO ANONIMO. (QUESTI CRITERI SI TROVANO NELLO SNAP-IN CRITERI DI SICUREZZA LOCALI DI MICROSOFT MANAGEMENT CONSOLE-MMC IN CONFIGURAZIONE COMPUTER\IMPOSTAZIONI DI WINDOWS\IMPOSTAZIONI SICUREZZA\CRITERI LOCALI\OPZIONI DI SICUREZZA.)

1. ACCESSO ALLA RETE: CONSENTE LA TRADUZIONE ANONIMA DEL SID/NOME
2. ACCESSO ALLA RETE: NON CONSENTIRE L'ENUMERAZIONE ANONIMA DEGLI ACCOUNT SAM
3. ACCESSO ALLA RETE: NON CONSENTIRE L'ENUMERAZIONE ANONIMA DI ACCOUNT E CONDIVISIONI SAM
4. ACCESSO ALLA RETE: CONSENTI A TUTTI DI APPLICARE LE AUTORIZZAZIONI AGLI UTENTI ANONIMI
5. ACCESSO ALLA RETE: NAMED PIPES A CUI È POSSIBILE ACCEDERE IN MODO ANONIMO
6. ACCESSO ALLA RETE: CONDIVISIONI A CUI È POSSIBILE ACCEDERE IN MODO ANONIMO

I VALORI PREDEFINITI PER QUESTI CRITERI SONO ACCETTABILI PER I SERVER SU UNA TIPICA LAN INTERNA.
PER I SERVER RAFFORZATI, COME I SERVER INTERNET, CONSIGLIAMO DI DISABILITARE I CRITERI 1 E 4, ABILITARE I CRITERI 2 E 3 E SPECIFICARE ELENCHI VUOTI PER I CRITERI 5 E 6.
NON È POSSIBILE DISABILITARE IN MODO SPECIFICO LA REGISTRAZIONE DEGLI EVENTI DI ACCESSO ANONIMO. IN GENERALE, CERCARE DI IMPEDIRE A WINDOWS DI REGISTRARE IL "RUMORE" È INUTILE. L'UNICO APPROCCIO CHE FUNZIONA È IMPLEMENTARE UNA SOLUZIONE DI GESTIONE DEI LOG CHE FILTRI IL RUMORE PER TE.

## #COMMENTARE QUESTE AZIONI DI MITIGAZIONE, SPIEGANDO L'EFFICACIA E L'EFFORT PER L'UTENTE/AZIENDA:

CERTAMENTE NON AVERE PIÙ UNA VULNERABILITÀ CHE PERMETTE A MALINTENZIONATI DI ENTRARE IN POSSESSO DI DATI PRIVATI DI UN'AZIENDA È UN'OTTIMA COSA. DIVERSI PROGETTI E KNOW-HOW POTREBBERO ESSERE RUBATI E RIVENDUTI ALLA CONCORRENZA, COSÌ COME DATI PERSONALI RESTERANNO PROTETTI NON RISCHIANDO DI DIVENTARE FONTE DI RICATTO. AGGIORNARE I PROPRI HARDWARE E SOFTWARE AZIENDALI È SEMPRE IL PRIMO PASSO VERSO LA ROSOLUAZIONE DI MOLTI BUG OBSOLETI RISOLTI CON PATCH E RIMODERNIZZAZIONE DEI SISTEMI. IN ALCUNI CASI DOVE QUESTO NON FOSSE POSSIBILE, MITIGARE ED ARGIBARE NON SIGNIFICA RISOLVERE DEL TUTTO IL PROBLEMA, MA MIGLIORARE PER LO MENO IL SERVIZIO E DIMINUIRE LA POSSIBILITÀ DI INTRUSIONI.