M4-Consegna week 15 day 1 – Daniele Rufo

NULL SESSION

Cosa sono: il termine fa riferimento ad una vulnerabilità delle share di windows tramite cui un attaccante può eseguire un accesso non autorizzato e recuperare informazioni preziose come password, utenti e gruppi di sistema ecc. Questo perché la vulnerabilità, appunto, permette di collegarsi senza autenticazione.
I sistemi vulnerabili sono: Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003 e nessuno di essi è più in commercio. Nonostante questo credo non sia raro trovarli sia in ambito privato che aziendale per motvi diversi, e quindi è una vulnerabilità da tenere in considerazione su tali sistemi.
Mitigazione:

- migrare a versioni OS più recenti
- modifica le configurazioni di windows per non consentire connessioni anonime (va modificato il file HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA)
- disabilitare Smbv1 che è la versione di samba vulnerabile

ARP SPOOFING

Cosa sono: è un attacco usato per intercettare traffico su una rete basata su switch sfruttando una vulnerabilità del protocollo ARP (Address Resolution Protocol). L'Arp completa le associazioni IP/MAC e le salva in una ARP cache ossia una tabella dove conserva le informazioni per utilizzi futuri. Ora l'attaccante va a modificare questa tabella inviando delle Arp response non richieste associando il suo MAC all'IP del router...impersonificando il router sarà in grado di intercettare il traffico. La vulnerabilità non fa riferimento ad un OS specifico in quanto un attaccante potrebbe metterla in atto su sistemi differenti senza problemi.
Mitigazione:

- una soluzione semplice è usare un'estensione per il browser come *https everywhere* che garantisce che tutto il traffico web attraversi una connessione https. In questo modo il traffico è oscurato e un ipotetico man in the middle non potrà leggerlo
- penso che un'idea alteernativa sia scrivere un programma in python che una volta lanciato controlla se il traffico in entrata modifica le voci nella tabella arp. Non saprei scriverlo, è solo un'idea.