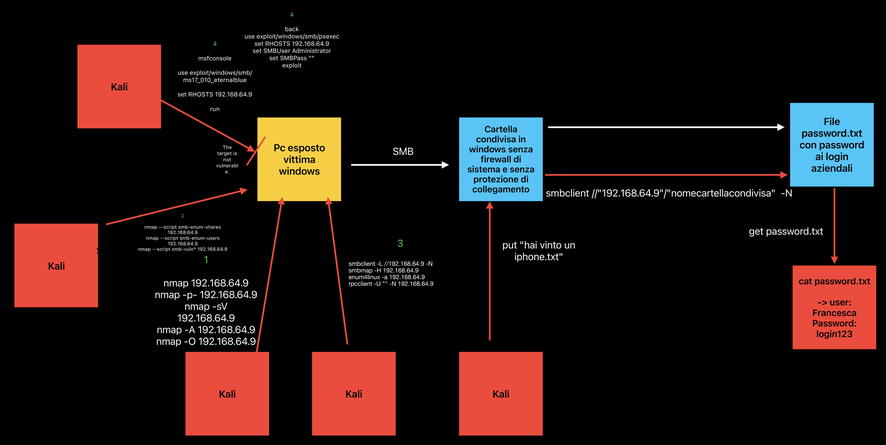

Report di sicurezza – Test su macchina Windows 7 (ambiente virtualizzato)

1. Fase di Ricognizione (Nmap)

È stata eseguita una scansione iniziale delle porte con Nmap.

Le porte TCP risultate aperte sono state 135 (MSRPC), 139 (NetBIOS), 445 (SMB), 5357 (WSDAPI) e l'intervallo 49152–49158 (porte dinamiche RPC).

Questi risultati indicano chiaramente la presenza di un sistema Windows con servizi di rete attivi, in particolare i servizi SMB e RPC.

---

2. Analisi avanzata dei servizi

Sono state eseguite scansioni aggiuntive con Nmap per individuare servizi nascosti, rilevare le versioni dei servizi tramite l'opzione -sV, eseguire il rilevamento del sistema operativo con -O ed effettuare una scansione avanzata con -A.

Dalle analisi non sono emersi servizi aggiuntivi rispetto alla scansione iniziale. Tuttavia, la tipologia dei servizi rilevati conferma la natura Windows del sistema target.

---

3. Individuazione vulnerabilità SMB

Attraverso l'utilizzo degli script NSE di Nmap dedicati al protocollo SMB (smb-vuln*), è stata individuata una vulnerabilità critica nota, MS17-010 (EternalBlue), e una configurazione insicura relativa a una condivisione SMB accessibile senza autenticazione completa.

Dal punto di vista pratico, la vulnerabilità MS17-010 è risultata segnalata come presente ma non sfruttabile con successo, probabilmente a causa dell'architettura del sistema e delle protezioni interne presenti. La condivisione SMB, invece, ha permesso l'accesso ai contenuti della cartella condivisa, la lettura dei file presenti e il caricamento di un file di test, dimostrando un reale problema di esposizione dei dati.

Questo evidenzia un rischio concreto legato alle condivisioni SMB mal configurate, anche in assenza di exploit avanzati funzionanti

---

4. Conclusione tecnica

Il test ha evidenziato che la superficie di attacco principale del sistema era legata al servizio SMB. Anche senza riuscire a ottenere accesso remoto completo al sistema, è stato possibile enumerare i servizi, individuare vulnerabilità note e accedere a risorse condivise non adeguatamente protette.

Questo dimostra come una cattiva configurazione rappresenti già di per sé una vulnerabilità critica, indipendentemente dalla presenza o meno di exploit avanzati.