**Report S9\_L1**

**OSPenTek Solutions - Security Operation: Azioni Preventive**

**Obiettivo dell'Esercizio:**

Come consulente esterno per **OSPenTek Solutions**, il mio obiettivo era verificare l'impatto dell'attivazione del Firewall su una macchina Windows XP sui risultati di una scansione dei servizi effettuata dall'esterno. Ho utilizzato Nmap per questa valutazione, cercando di identificare come le modifiche al Firewall influenzano la visibilità dei servizi offerti dalla macchina.

Immagine che contiene testo, schermata, Carattere, documento

Descrizione generata automaticamente

Immagine che contiene testo, schermata, Carattere, algebra

Descrizione generata automaticamente

**Impostazione delle Macchine:**

- Macchine Virtuali: Per questo esercizio, sono state impostate due macchine virtuali in un ambiente isolato. Una eseguiva Kali Linux, usata per le scansioni di sicurezza, mentre l'altra era basata su Windows XP, fungeva da target.

- Configurazione di Rete: Entrambe le macchine sono state collegate in modalità "Scheda con bridge", permettendo interazioni di rete come in un ambiente di produzione.

Immagine che contiene testo, schermata, Carattere, grafica

Descrizione generata automaticamente

**Configurazione degli Indirizzi IP:**

**- Windows XP:** È stato configurato con un indirizzo IP statico 192.168.240.150 e una subnet mask di 255.255.255.0.

Immagine che contiene testo, elettronica, schermata, software

Descrizione generata automaticamente

**- Kali Linux:** Configurato con un indirizzo IP statico 192.168.240.100, e una subnet mask di 255.255.255.0, impostato attraverso modifiche al file di configurazione di rete.

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

**Scenari di Test:**

**1. Primo Scenario - Firewall Disattivato:**

- Disattivazione del Firewall su Windows XP via Pannello di controllo.

- Esecuzione di una scansione Nmap da Kali Linux verso Windows XP: `nmap -sV -oA scan\_risultato1 192.168.240.150`.

- Risultati: Rilevazione di numerosi servizi aperti, con dettagli ampi sui protocolli e sistemi operativi.

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

**2. Secondo Scenario - Firewall Attivato:**

- Attivazione del Firewall su Windows XP.

- Nuova scansione Nmap eseguita: `nmap -sV -oA scan\_risultato2 192.168.240.150`.

- Risultati: Differenze sostanziali rispetto al primo scenario, con la macchina che appariva offline, indicando che tutte le richieste esterne venivano efficacemente bloccate.

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

**Analisi delle Differenze:**

Le differenze notate tra i risultati delle due scansioni sono significative. Nel primo scenario, con il Firewall disattivato, Nmap è riuscito a rilevare i servizi aperti e a fornire informazioni dettagliate sulla macchina Windows XP, come il sistema operativo e i protocolli utilizzati. Invece, nel secondo scenario, con il Firewall attivato, Nmap non è stato in grado di ottenere gli stessi dettagli e ha indicato che l'host sembrava offline.

La causa di questo risultato diverso è l'attivazione del Firewall sulla macchina Windows XP. Quando il Firewall è attivo, agisce come una barriera di sicurezza, filtrando il traffico in entrata e bloccando le richieste di ping provenienti da Nmap. Di conseguenza, Nmap non riesce a stabilire una connessione diretta con la macchina target e non può raccogliere informazioni dettagliate sui servizi e sul sistema operativo.

**Conclusioni:**

L'analisi condotta dimostra che l'attivazione del Firewall su una macchina Windows XP ha un impatto considerevole sui risultati delle scansioni di sicurezza effettuate dall'esterno. Il Firewall serve come un'importante misura preventiva, non solo nascondendo i dettagli dei servizi aperti ma rendendo anche l'host completamente irraggiungibile da scansioni esterne. Questo sottolinea l'importanza del Firewall come componente essenziale nella protezione dei sistemi informatici contro gli attacchi.