

W11D2 - Nicholas Di Angelo -

Relazione sulla Scansione con Nmap

Obiettivo: Effettuare una scansione della rete da un sistema Kali Linux con indirizzo IP 192.168.1.100 verso un sistema Windows 7 con indirizzo IP 192.168.1.5. Utilizzeremo Nmap con diversi comandi per ottenere informazioni dettagliate sulla topologia di rete e sui servizi in esecuzione sul sistema target.

Comandi Utilizzati:

1. `nmap -O ip`: Questo comando esegue una scansione per identificare il sistema operativo del target.
2. `nmap -sS Ip`: Questo comando esegue una scansione SYN per identificare le porte aperte sul target.
3. `nmap -sV ip`: Questo comando esegue una scansione per identificare i servizi in esecuzione sulle porte aperte del target e cerca di determinarne le versioni.
4. `nmap -oN report1 Ip`: Questo comando esegue una scansione generale e salva i risultati in un file di output di testo chiamato "report1".

Risultati:

1. **Scansione del Sistema Operativo (-O):** Il comando ha identificato il sistema operativo del target come Windows 7.
2. **Scansione TCP SYN (-sS):** La scansione ha rivelato diverse porte aperte sul target, tra cui le porte 80 (HTTP) e 443 (HTTPS).
3. **Scansione dei Servizi (-sV):** La scansione ha identificato i servizi in esecuzione sulle porte aperte, incluso un server HTTP sulla porta 80 e un server HTTPS sulla porta 443. È stata anche fornita una stima delle versioni dei servizi.
4. **Salvataggio dei Risultati (-oN):** I risultati della scansione sono stati salvati nel file di output "report1" per ulteriori analisi e referenze future.

Conclusioni: La scansione con Nmap ha fornito informazioni utili sulla configurazione di rete del sistema target, inclusi dettagli sul sistema operativo, le porte aperte e i servizi in esecuzione. Queste informazioni possono essere utilizzate per valutare la sicurezza della rete e identificare eventuali vulnerabilità o punti deboli che potrebbero essere sfruttati dagli attaccanti. È consigliabile eseguire scansioni periodiche per mantenere aggiornata la conoscenza della rete e garantire una maggiore sicurezza.

Il risultato ottenuto durante la scansione potrebbe essere influenzato da diversi fattori, tra cui:

1. **Firewall:** Il firewall sul sistema target potrebbe bloccare alcune richieste di scansione, limitando così la visibilità delle porte aperte e dei servizi in esecuzione.
2. **Configurazione di Rete:** La configurazione della rete potrebbe impedire la corretta comunicazione tra il sistema di scansione e il sistema target, riducendo l'efficacia della scansione.
3. **Protezione degli IDS/IPS:** Sistemi di rilevamento delle intrusioni (IDS) o sistemi di prevenzione delle intrusioni (IPS) potrebbero rilevare e bloccare le scansioni in corso, riducendo la loro efficacia.

Per continuare a effettuare la scansione e ottenere risultati più completi, è possibile adottare diverse soluzioni:

1. **Regole Firewall:** Verificare e aggiornare le regole del firewall sul sistema target per consentire il traffico da e verso il sistema di scansione.
2. **Configurazione di Rete:** Verificare la configurazione di rete su entrambi i sistemi per garantire che non ci siano problemi di connettività che potrebbero influire sulla scansione.
3. **Limitazioni IDS/IPS:** Se possibile, aggiornare le regole degli IDS/IPS per consentire la scansione senza interruzioni.
4. **Utilizzo di Opzioni Nmap:** Esplorare altre opzioni di Nmap che potrebbero essere più adatte al contesto di scansione, come l'uso di tecniche di scansione stealth o l'impostazione di parametri più specifici per la scansione.

Implementando queste soluzioni, si potrebbe aumentare la probabilità di ottenere risultati completi e accurati durante la scansione della rete. Tuttavia, è importante agire sempre in conformità con le politiche e le normative aziendali relative alla sicurezza e alla privacy delle informazioni.









