Cyber Security Analyst

PROJECT REPORT

SCANSIONE DI VULNERABILITA' TRAMITE SCRIPT

In risposta all'esercizio su: (vedi consegna nella pag. seguente)

Prepared by

Fulvio Zalateu

Security Rookies

Consegna:

Si richiede allo studente di effettuare delle scansioni di vulnerabilità sul target Metasploitable (target e attaccante su stessa rete o su reti diverse), tramite gli script:

● Vuln ● Vulners

Analizzare 3 vulnerabilità identificate a scelta. Spiegare le differenze tra i due script.

Svolgimento

Scansione con il modulo vuln

Utilizzare il comando
nmap --script vuln -sV -p-
192.168.50.100
Cosa fa questo comando:
• --script vuln: lancia lo script Nmap vuln, che cerca vulnerabilità nei servizi.
• -sV: effettua una rilevazione delle versioni dei servizi. • -p-: scansiona tutte le porte, dalla 1 alla 65535.
• 192.168.50.100: IP del target Metasploitable.

La scansione ha rivelato molte vulnerabilità possibilmente sfruttabili da un attaccante

Scansione con il modulo vulners

Lo script vulners è simile, ma più specifico. Usa il database Vulners per identificare vulnerabilità note, in base alle versioni dei software rilevati sul target: nmap --script vulners -sV -p- 192.168.50.100

Anche in questo caso la scansione ha restituito molte vulnerabilità sfruttabili.

Differenze tra vuln e vulners

- vuln: è un insieme di script che cerca vulnerabilità comuni nei servizi esposti su un sistema. Fornisce una panoramica generale delle possibili debolezze, coprendo diverse problematiche di sicurezza.
- vulners: è più specifico. Confronta le versioni dei software trovati con un database esterno (Vulners) e restituisce un elenco di vulnerabilità conosciute, con riferimenti ai CVE (Common Vulnerabilities and Exposures). È più preciso nel collegare le vulnerabilità a quelle già documentate.

GRAZIE