giovedì 17 ottobre 2024 14:04

Scansione delle vulnerabilità con Nmap

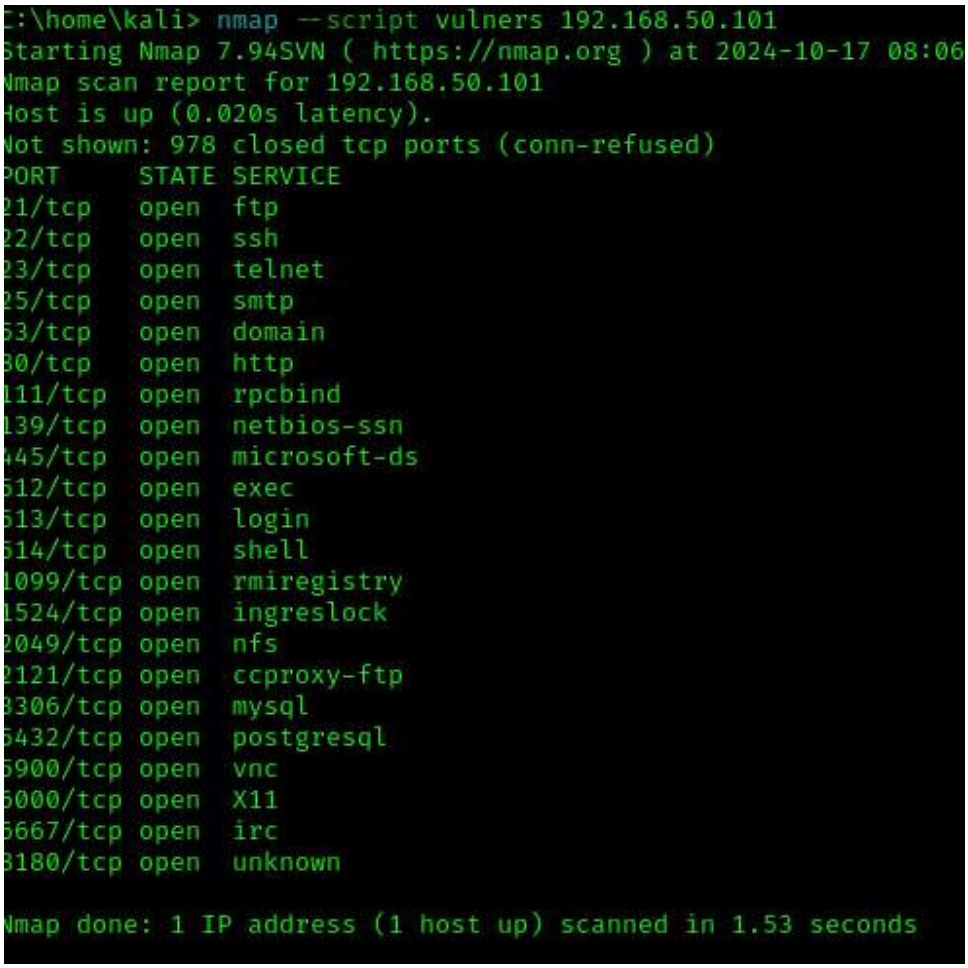
Si richiede allo studente di effettuare delle scansioni di vulnerabilità sul target Metasploitable (target e attaccante su stessa rete o su reti diverse), tramite gli script:

● Vulners

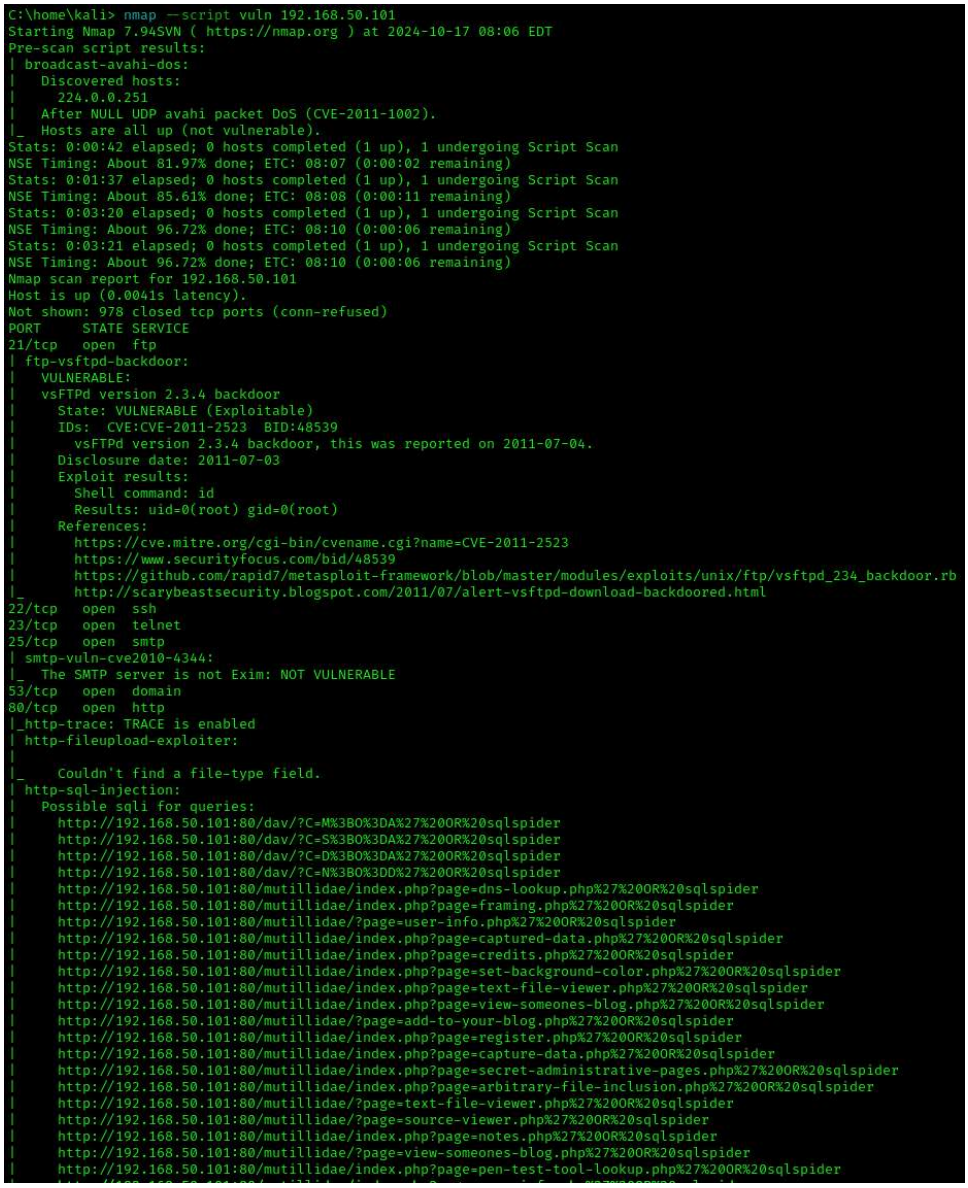
● Vuln

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

Vulners:



Vuln:



3 vulnerabilità che si possono identioficare da quest'ultimo screen sono:

VSFTPD version 2.3.4 backdoor (CVE-2011-2523):

Presente nel servizio FTP in esecuzione sulla porta 21/tcp, questa versione contiene una backdoor che consente a un utente malintenzionato di ottenere accesso root al sistema dopo aver stabilito una connessione FTP. Sono evidenziati anche vari link che indicano exploit pubblici per sfruttare questa vulnerabilità

HTTP - SQL Injection (porta 80/tcp):

Viene rilevata una potenziale vulnerabilità di **SQL Injection** in vari URL, un attaccante potrebbe eseguire query non autorizzate sul database, potenzialmente estraendo, modificando o cancellando dati.

Sono elencate molteplici pagine vulnerabili, inclusi script PHP presenti nel contesto di **Mutillidae**, una web app deliberatamente vulnerabile.

HTTP TRACE Abilitato (porta 80/tcp):

La scansione segnala che la funzione TRACE è abilitata sul server HTTP.

Potrebbe esporre il server a vulnerabilità di tipo Cross-Site Tracing (XST), che può essere utilizzato in combinazione con altre vulnerabilità per rubare dati dell'utente o sessioni di autenticazione.

Differenza tra i due script:

La scansione **Vulners** è più veloce e non comporta traffico extra per il target, mostra solo le porte aperte potenzialmente vulnerabili e non tenta di verificare o sfruttare alcuna vulnerabilità, mentre la scansione **Vuln** invece tenta di scoprire la presenza di vulnerabilità particolari testando direttamente il servizio scoperto, ha un alto grado di fiducia e nessun falso positivo