Esercizio W12D1

Svolgiamo l'esercizio tenendo conto della seguente traccia:

Effettuare un Vulnerability Assessment con Nessus sulla macchina Metasploitable, indicando come target solo le porte comuni (potete scegliere come scansione il «basic network scan», o l'advanced e poi configurarlo).

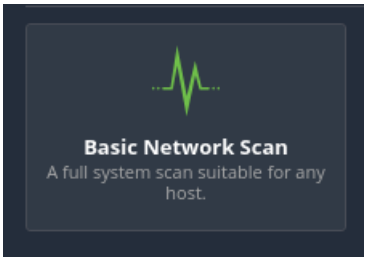
A valle del completamento della scansione, analizzate attentamente il report per ognuna delle vulnerabilità riportate, approfondendo qualora necessario con i link all'interno dei report e/o con contenuto da Web.

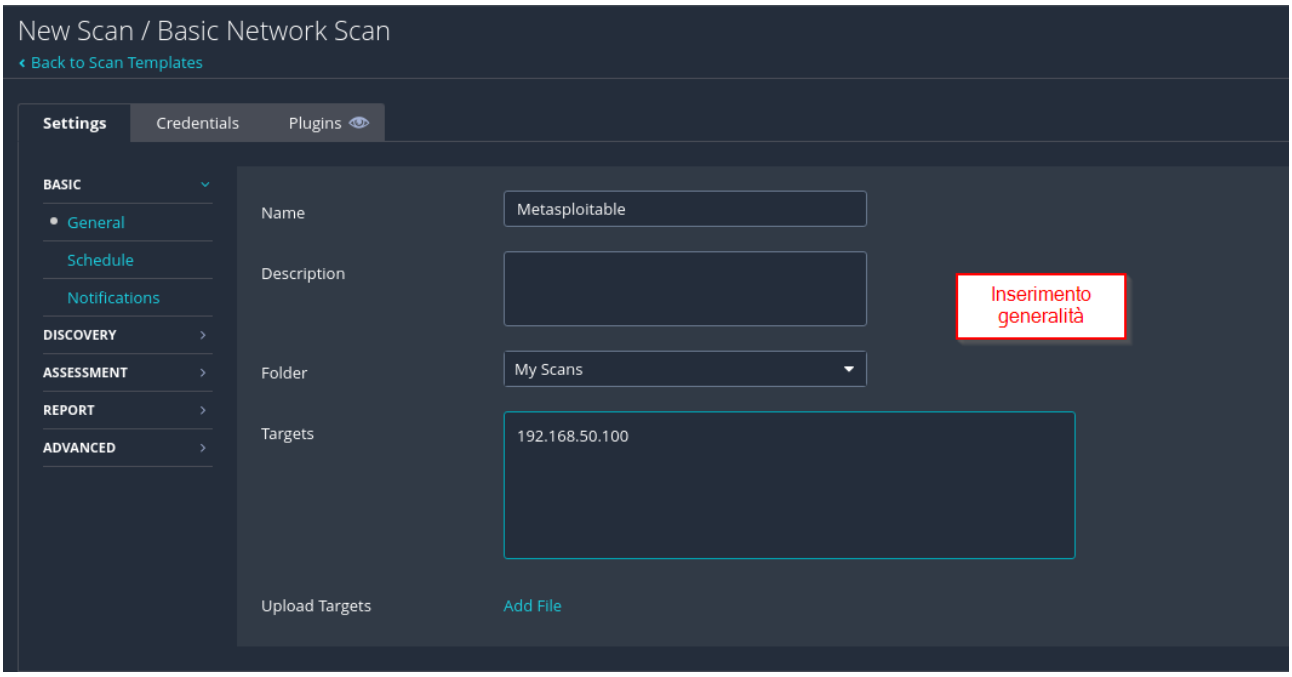
Gli obiettivi dell'esercizio sono:

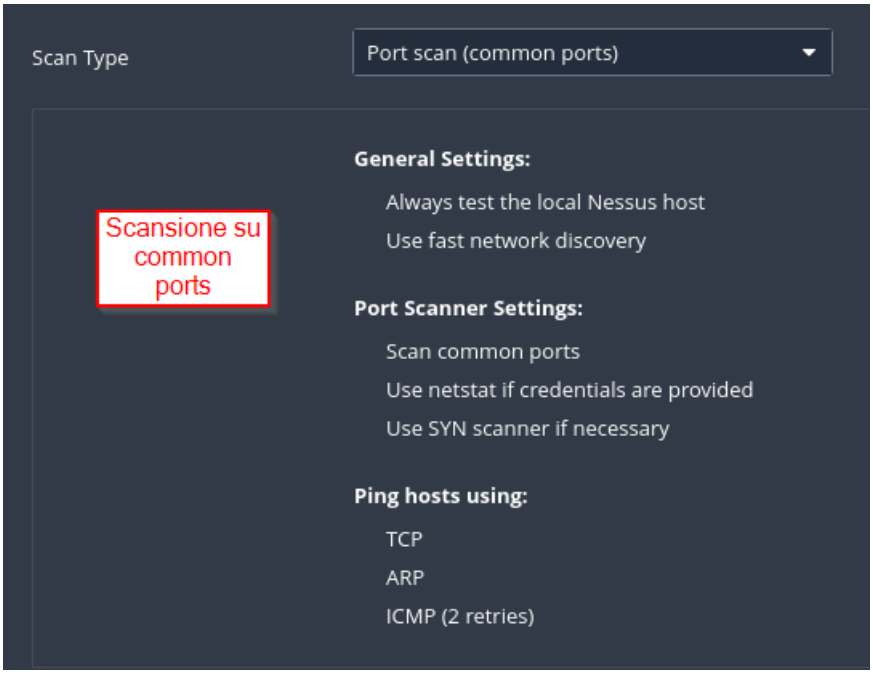
- Fare pratica con lo strumento, con la configurazione e l'avvio delle scansioni.
- Familiarizzare con alcune delle vulnerabilità note che troverete spesso sul vostro percorso da penetration tester.

Preparazione scansione

Visto che andiamo per una basic network scan, non c'è molto da aggiungere se non i dati fondamentali. Le generalità e l'obiettivo della scansione, le common ports.

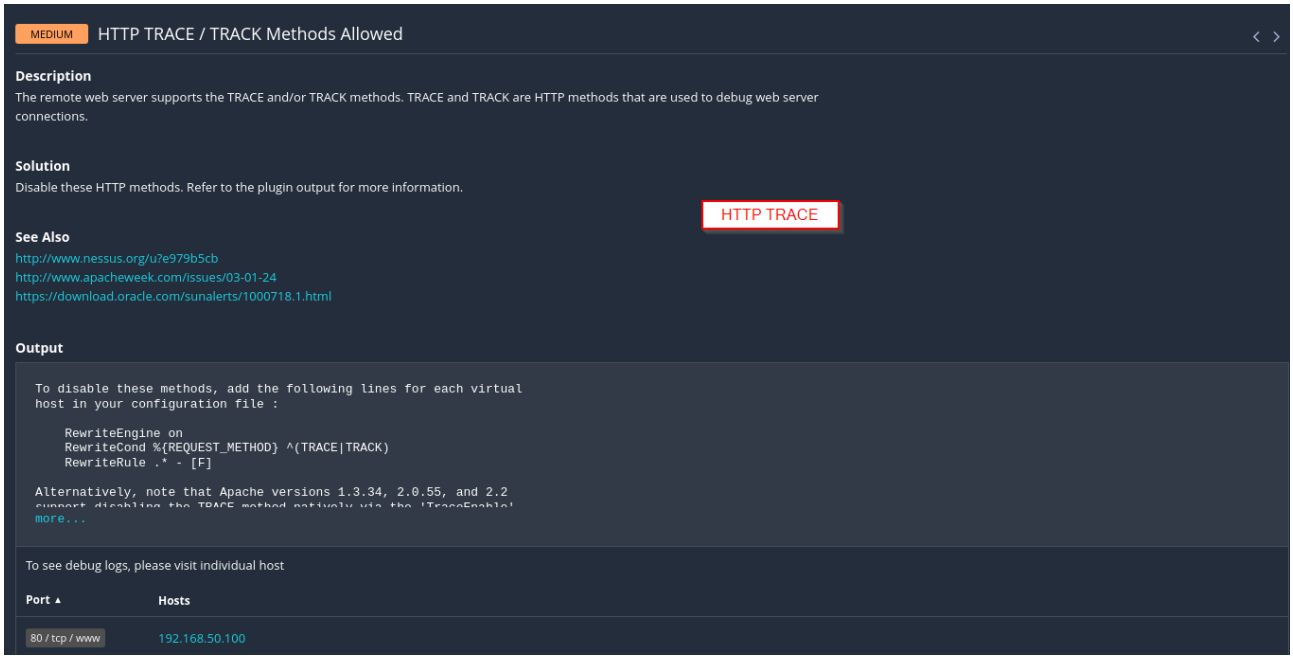




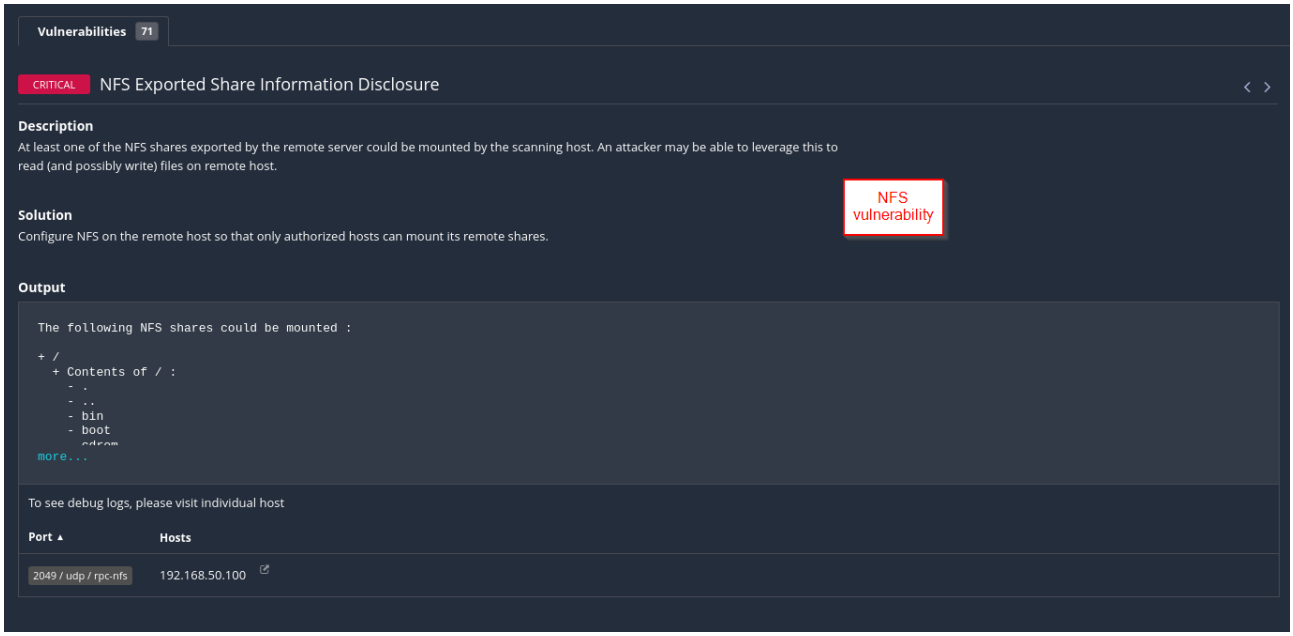


Risultati

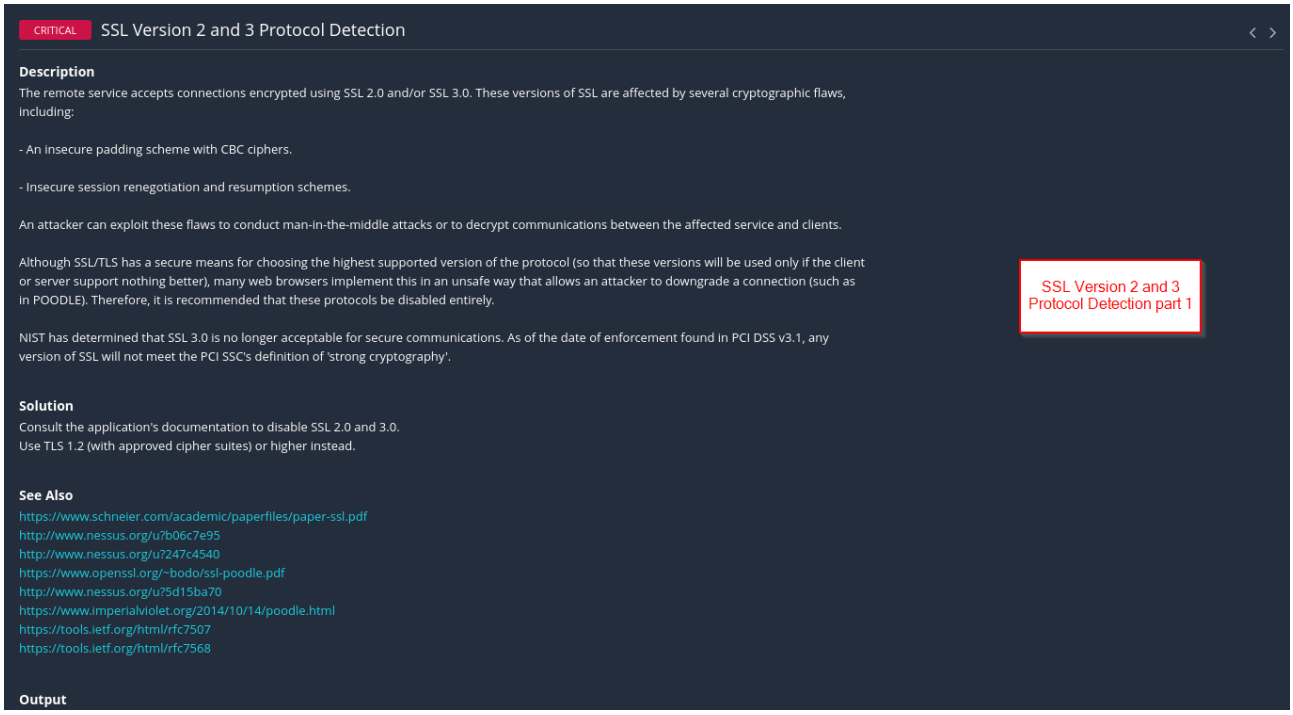
Secondo quanto trovato, andiamo ad analizzare alcune delle vulnerabilità scovate grazie allo scanner.



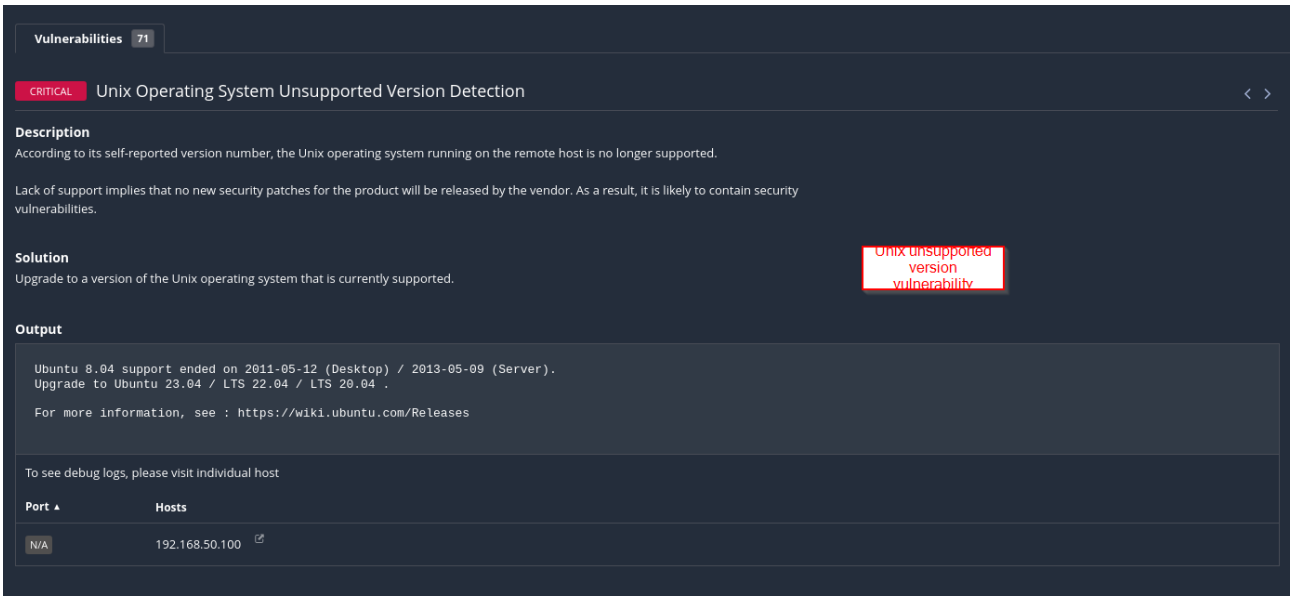
Il metodo HTTP TRACE consente di ottenere una copia di una richiesta HTTP inviata al server. Questo metodo è stato utilizzato in passato per attacchi di tipo Cross-Site Tracing (XST), che consentono a un attaccante di rubare i cookie di autenticazione di un utente. Il metodo HTTP TRACK invece è simile al metodo TRACE, non è supportato da tutti i browser, ma permette di inviare dati al server, rendendolo di fatto più pericoloso. La soluzione migliore è disabilitare i metodi totalmente.



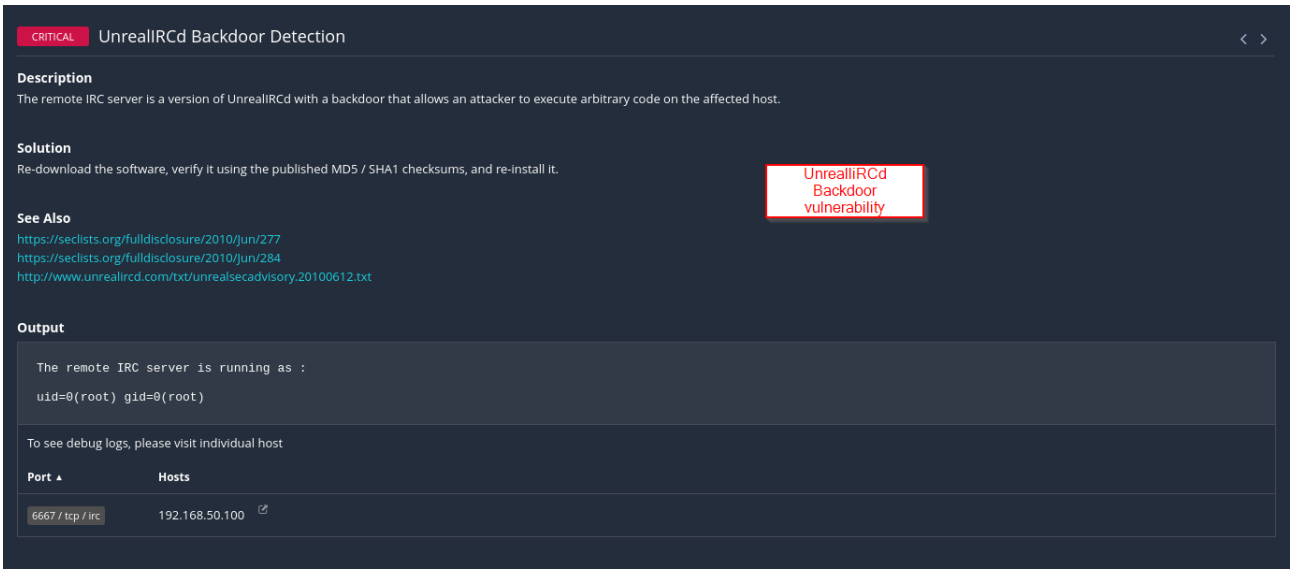
Un protocollo NFS(Network File System) malconfigurato può causare diversi problemi di sicurezza. Questo permette ad un utente malintenzionato di accedere a file o directory a cui non dovrebbe avere accesso. Tale protocollo potrebbe essere usato anche per inviare DoS, andando di fatto a saturare il server con richieste di servizio. Per rimuovere queto rischio occorre delegare la parte remota di NFS solo agli utenti autorizzati.



In questo caso la vulnerabilità sta nel fatto che la porta 5432 monta il protocollo SSL(secure socket layers) 2.0 e 3.0. Essi sono deprecati per via degli attacchi che li hanno scoperchiati in passato. Un esempio di quest'ultimi sono il Padding Oracle, che decifra parte del testo cifrato mediante lo sfruttamento del pattern MAC-than-encrypt, oppure semplicemente il BIAS, che sfrutta la debolezza dei cifrari basati su RC4. Per eliminare un tale problema il modo migliore sarebbe sostituire SSL con il ben noto e moderno protocollo di sicurezza TLS(transport layer security) 1.2.



Dopo lo scan Version Detection del sistema operativo, emerge come la macchina sfoggi una versione non più supportata. Non è solo un fatto di prestazioni, ma anche di carenza di aggiornamenti riguardo la sicurezza del dispositivo. La soluzione a tale vulnerabilità è l'aggiornamento all'ultima versione di Unix.



Lo scanner identifica all’interno di UnrealRCd(un server Internet Relay Chat open source) una backdoor che consente ad un attaccante la possibilità di eseguire comandi arbitrari sul server. Per scongiurare il rischio dobbiamo reinstallare una versione pulita del software.