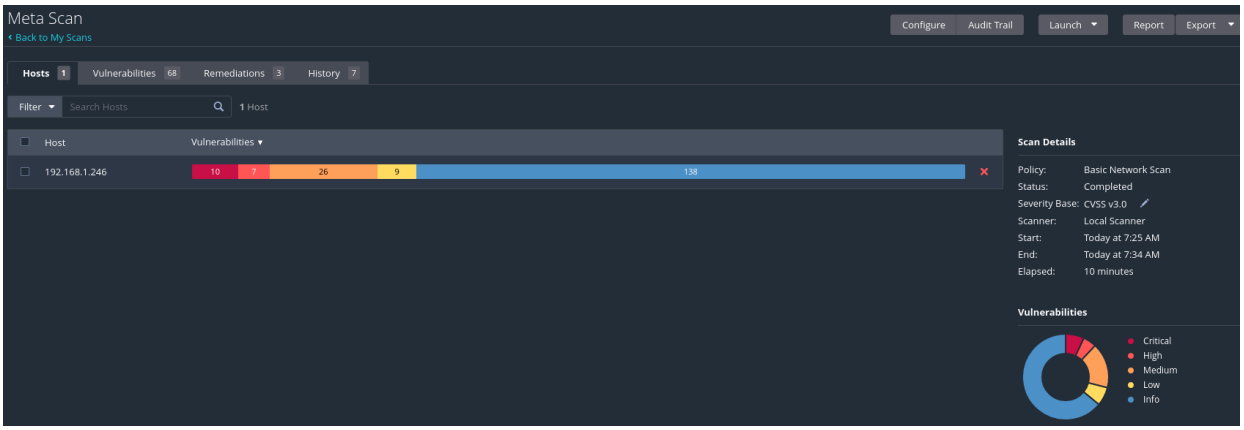
NESSUS

Traccia: Lo studente effettuerà un Vulnerability Scanning sulla macchina Metasploitable utilizzando Nessus, concentrandosi sulle porte comuni. Questo esercizio ha lo scopo di fare pratica con lo strumento Nessus, la configurazione delle scansioni, e di familiarizzare con alcune delle vulnerabilità note.
Fasi dell'Esercizio:

1. Configurazione della Scansione:
    - ○ Target: Metasploitable
    - ○ Porte: Solo le porte comuni (es. 21, 22, 23, 25, 80, 110, 139, 443, 445, 3389
    - ○ Tipo di Scansione, puoi scegliere tra:
        - ■ Basic Network Scan: Configurazione predefinita per una scansione di rete.
        - ■ Advanced Scan: Configurabile in base alle tue esigenze specifiche.
2. Esecuzione della Scansione:
    - ○ Avvia la scansione configurata su Nessus.
    - ○ Attendi il completamento della scansione e assicurati che tutte le porte specificate siano state analizzate.
3. Analisi del Report: Esercizio Traccia
    - ○ Una volta completata la scansione, scarica e analizza il report generato da Nessus.
    - ○ Per ogni vulnerabilità riportata:
        - ■ Leggi attentamente la descrizione fornita nel report.
        - ■ Approfondisci ulteriormente utilizzando i link e le risorse suggerite nel report.
        - ■ Cerca ulteriori informazioni sul Web, se necessario.

Oggi siamo andati a vedere come funziona il software Nessus, ovvero una applicazione atta alla scansione delle vulnerabilità. Le vulnerabilità sono considerate informazioni in quanto, a differenza dei dati (i quali sono oggettivi come porte aperte/chiuse oppure le caratteristiche del sistema operativo), sono considerate soggettive in quanto sottoposte ad una valutazione "variabile".
Ciò che faremo con Nessus sarà la scansione della macchina vulnerabile Metasploitable2 ed andremo ad analizzare 5 delle sue vulnerabilità critiche.

Di seguito andremo a vedere la panoramica generale del risultato ottenuto da questa scansione:



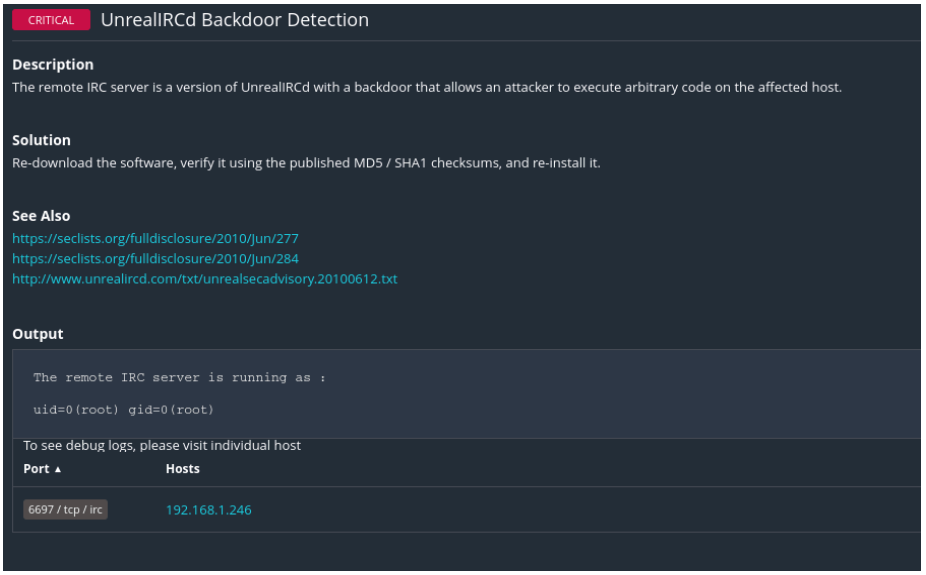
Ciò che emerge dal risultato finale saranno vulnerabilità di vario tipo:

- 10 vulnerabilità critiche;
- 7 vulnerabilità alte;
- 26 vulnerabilità medie;
- 9 vulnerabilità basse;
- 138 vulnerabilità info (ovvero rischio quasi irrilevante.

Ora ci concentreremo su 5 vulnerabilità critiche e sulla loro risoluzione.

Unreal|RCd Backdoor Detection

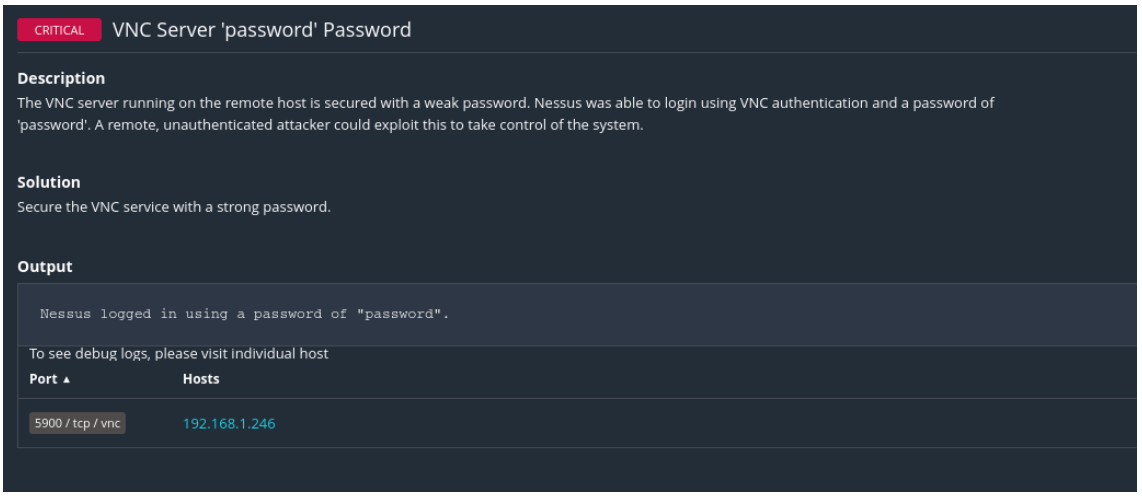
Questa è una delle vulnerabilità più gravi che si possono incontrare durante una scansione, in quanto le Backdoors sono una sorta di porta perennemente aperta ad eventuali attacchi esterni, significa che una parte del codice sorgente è stata malevolmente modificata proprio allo scopo di aver garantito un costante accesso al dispositivo in qualsivoglia momento ed avere completo controllo di esso, letteralmente una “porta sul retro” sempre aperta, se il dispositivo è in funzione.



L’azione che viene consigliata per la sua risoluzione è di riscaricare il software, verificare che sia aggiornato correttamente ed, infine, reinstallarlo.

VNC Server ‘password’ Password

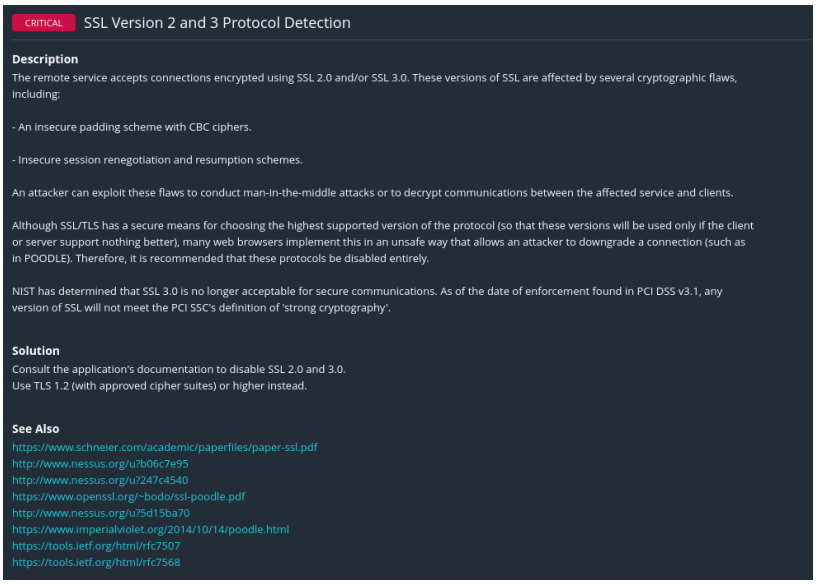
Questa vulnerabilità invece ci comunica che è stata utilizzata una password debole, facile da trovare quindi, per un malintenzionato, è semplice accedere al servizio.



La soluzione suggerita è quella di cambiare la password con una più sicura.

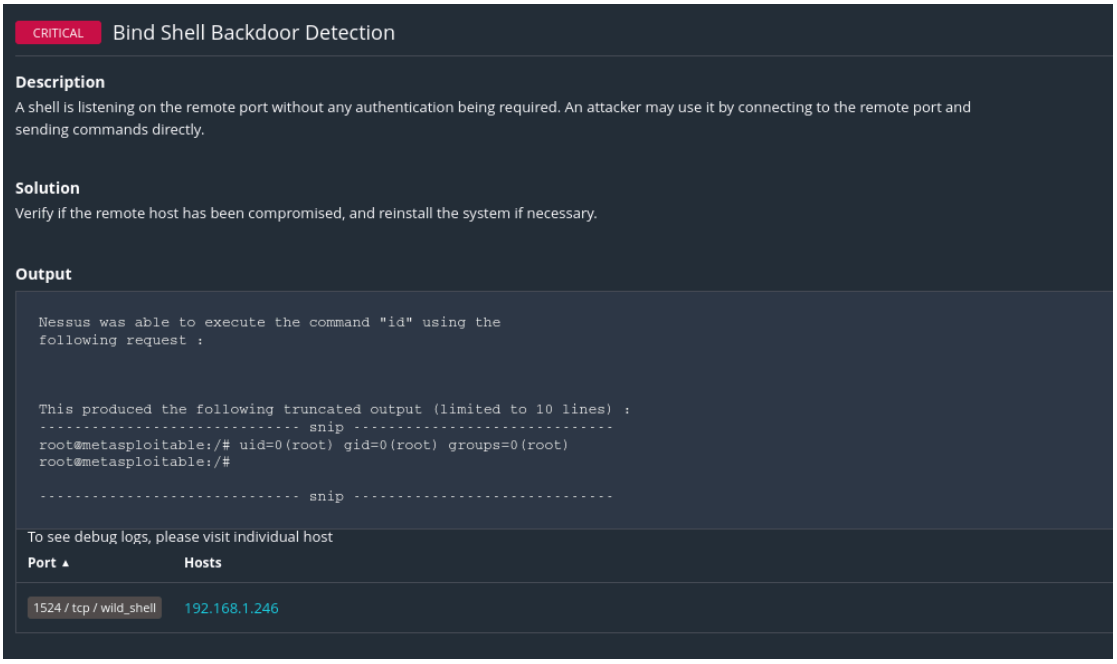
SSL Version 2 and 3 Protocol Detection

Questo tipo di vulnerabilità ci comunica l’utilizzo dei protocolli SSLv2 e SSLv3 considerati obsoleti ed insicuri nella protezione delle comunicazioni tramite HTTPS. Provoca delle gravi falle a livello di crittografia in quanto facilmente soggetta ad attacchi man-in-the-middle, decrittazione del traffico e compromissione dell’integrità dei dati. Il protocollo SSL di base è considerato sicuro, ma le versioni 2 e 3 sono considerate obsolete per l’utilizzo moderno poichè superate dal protocollo TSL, versione più sicura ed aggiornata.



La soluzione suggerita è: disabilitare SSLv2 e SSLv3 e sostituirla con la versione TSL 1.2 o versioni più aggiornate.

Bind Shell Backdoor Detection
Troviamo un'altra vulnerabilità di tipo backdoor, in questo caso di tipo bind shell. Consente all'attaccante di collegarsi al dispositivo tramite shell collegata ad una determinata porta rimanendo in ascolto di connessioni esterne, consentendogli completo controllo sulla macchina compromessa. E' una backdoor difficile da rilevare, spesso viene piazzata tramite malware su porte non comuni o mascherate da servizi legittimi.



La soluzione è di verificare se l'host remoto è stato compromesso e reinstallare il sistema, se necessario.

Apache Tomcat SEoL(<=5.5.x)
L'ultima vulnerabilità che andremo ad analizzare ha a che fare con una specifica versione di Apache Tomcat 5.5.x, sul quale sono state rilevate delle falle a livello di sicurezza che espongono i web server a vari attacchi. La sigla SEoL sta ad indicare un software arrivato a "fine vita", quindi non riceve più aggiornamenti di sicurezza, esponendo il dispositivo che lo usa a maggior rischio di attacchi.

La soluzione in questo caso suggerita è l'aggiornamento di Apache Tomcat alla versione più recente supportata dal dispositivo.