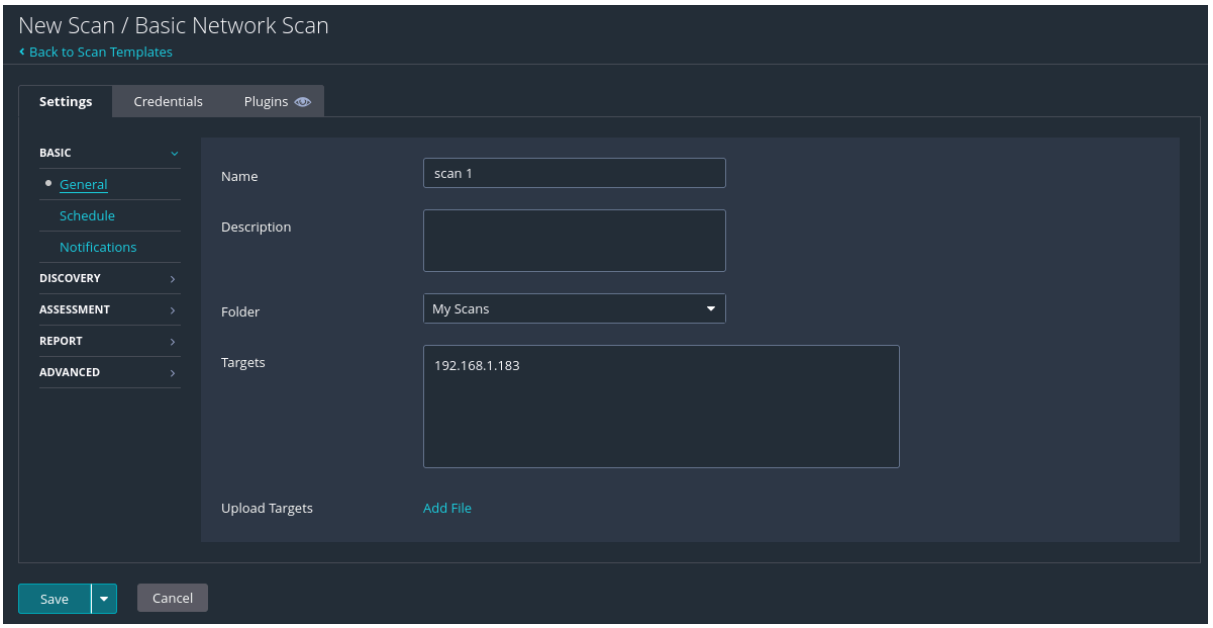
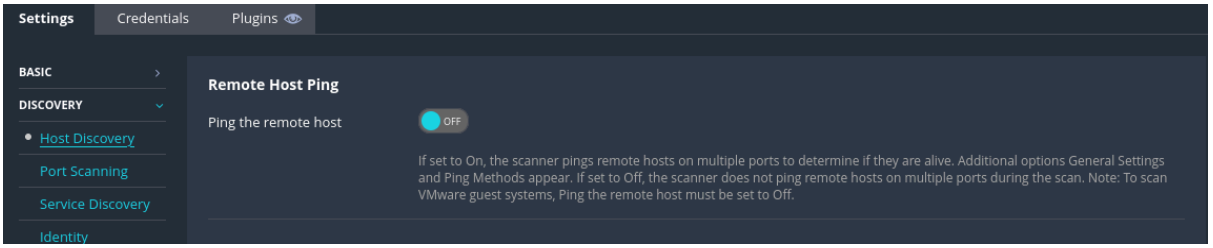
REPORT S5/L3

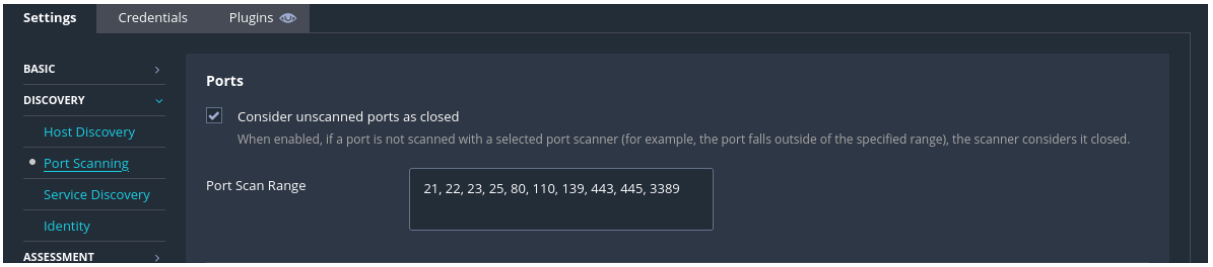
Obiettivo: Esercizio Traccia Lo studente effettuerà un Vulnerability Scanning sulla macchina Metasploitable utilizzando Nessus, concentrandosi sulle porte comuni. Questo esercizio ha lo scopo di fare pratica con lo strumento Nessus, la configurazione delle scansioni, e di familiarizzare con alcune delle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

Dopo Aver attivato il servizio Nessus ed aver eseguito l'accesso su browser ho avviato una nuova scansione di tipo Basic Network Scan.
Nella sezione general ho inserito il target della scan

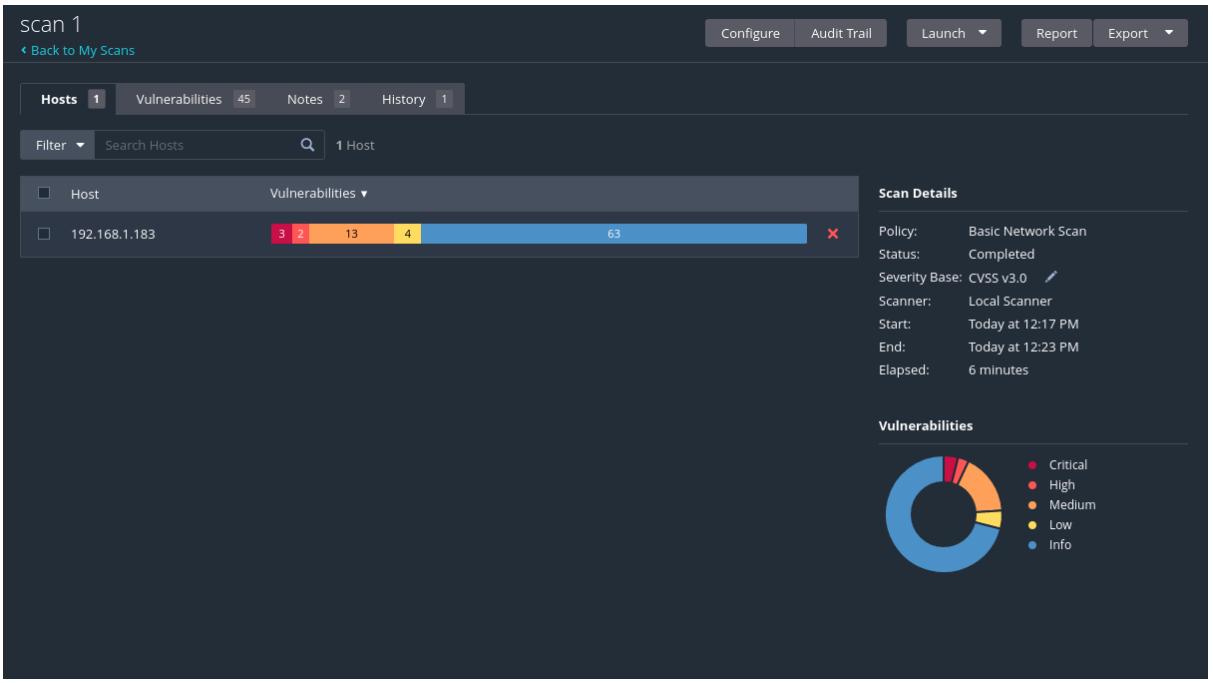


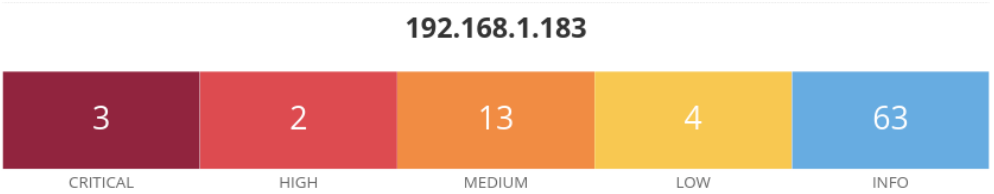
mentre nella sezione discovery ho cambiato lo scan type in custom, ho disattivato il remote host ping e ho inserito il range di porte da scansionare.



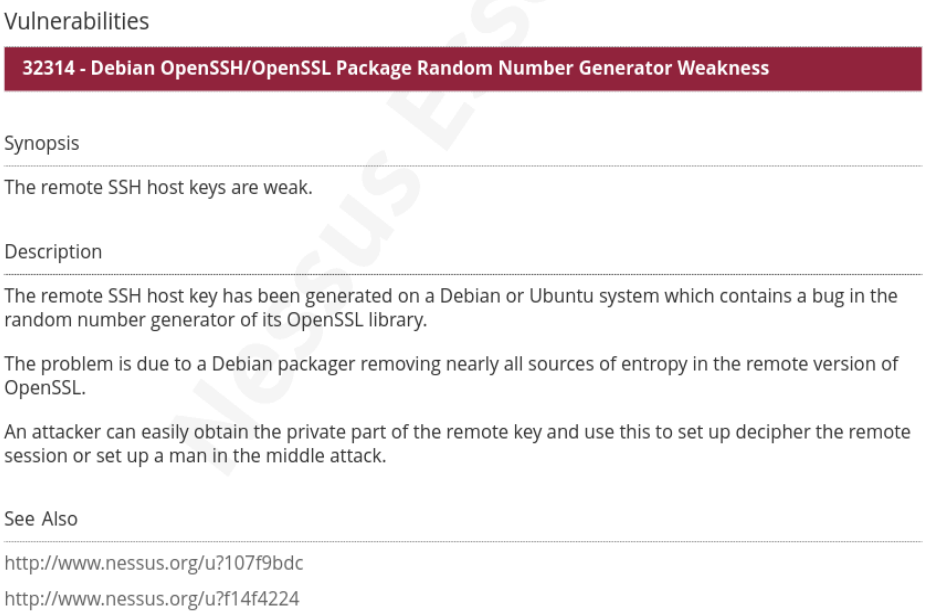


Successivamente ho avviato la scansione e ho estratto il report.





Prendo in esame il prima vulnerabilità critica fornita dal report nella quale vengono forniti una descrizione della vulnerabilità e dei link che riconducono ad una pagina nella quale vengono specificati il tipo di vulnerabilità, servizio e porta sui quali si trova, possibili soluzioni, livello di CVSS e fattori di rischio.



CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:C)

References

BID	29179
CVE	CVE-2008-0166
XREF	CWE:310

Exploitable With

Core Impact (true)

Plugin Information

Published: 2008/05/14, Modified: 2024/07/24

Plugin Output

tcp/22/ssh