

## PRATICA S5/L3

Obiettivo: 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:

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.

Esecuzione della Scansione: Avvia la scansione configurata su Nessus.

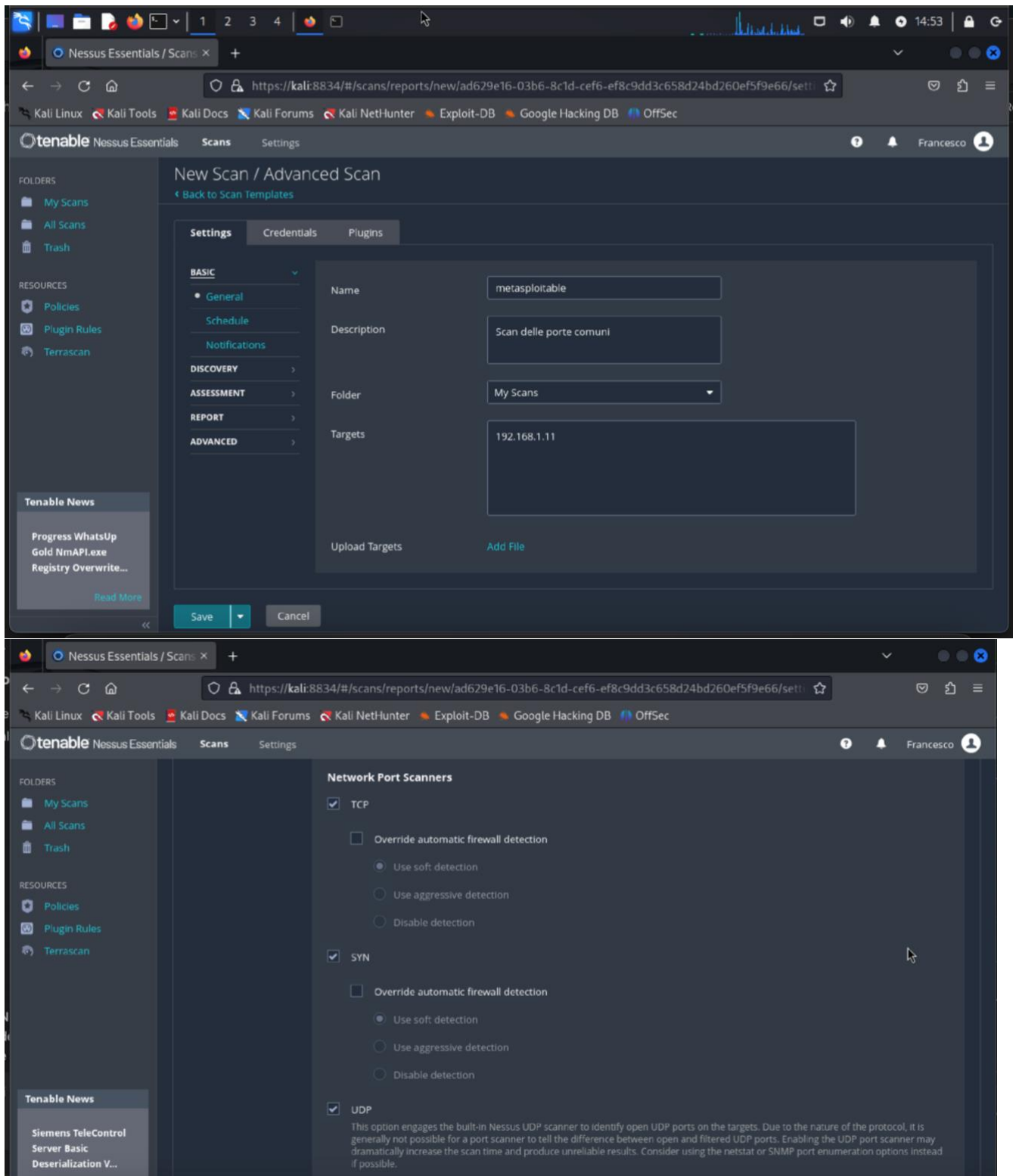
Attendi il completamento della scansione e assicurati che tutte le porte specificate siano state analizzate.

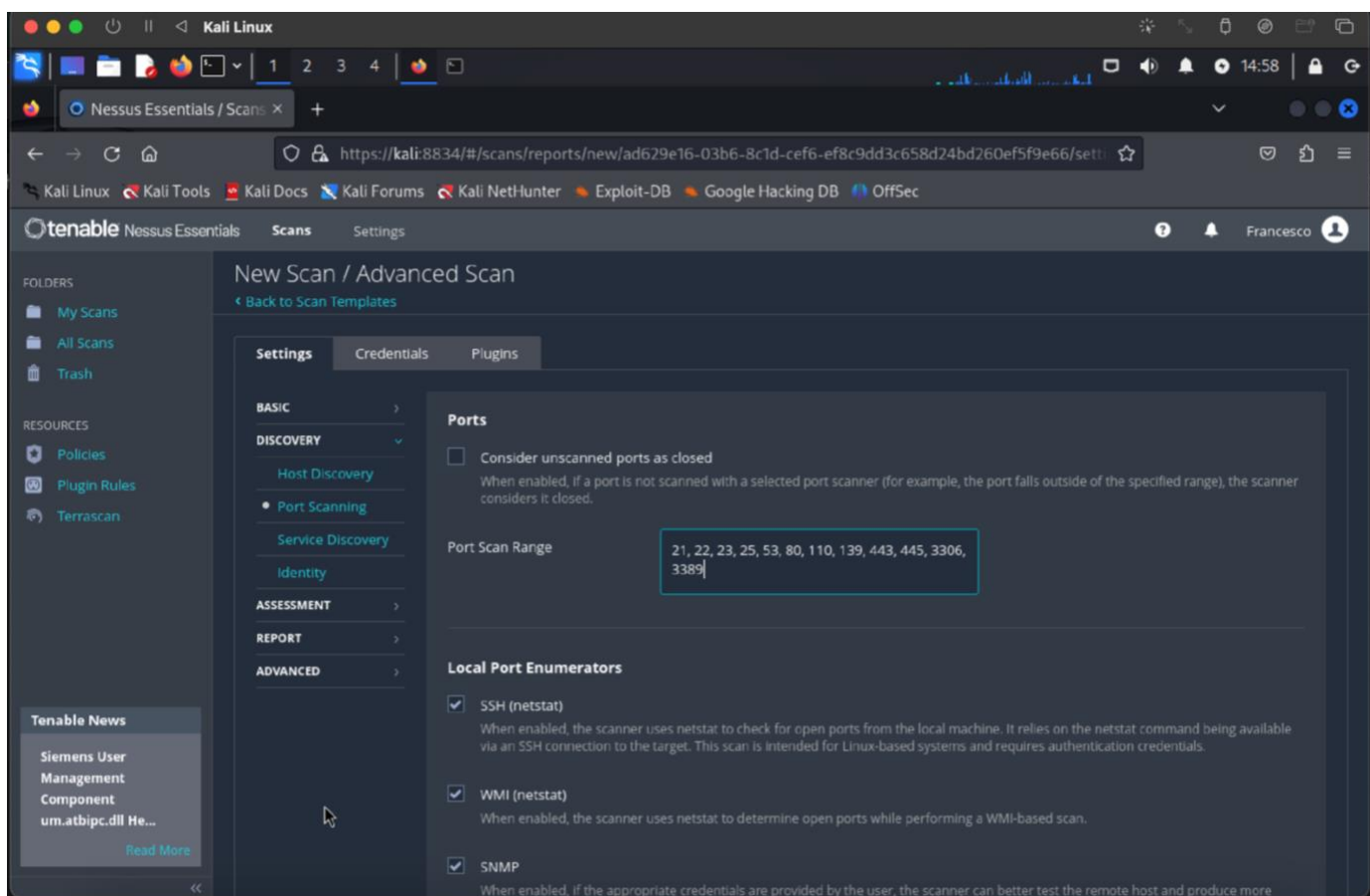
Per svolgere questo esercizio avviamo la VM kali linux ed in contemporanea la VM Metasploitable.

Una volta effettuato l'accesso, dobbiamo creare una nuova scansione, in questo caso io ho scelto advanced scan, in modo da poter personalizzare i parametri della scansione in base a quello che ci serve.

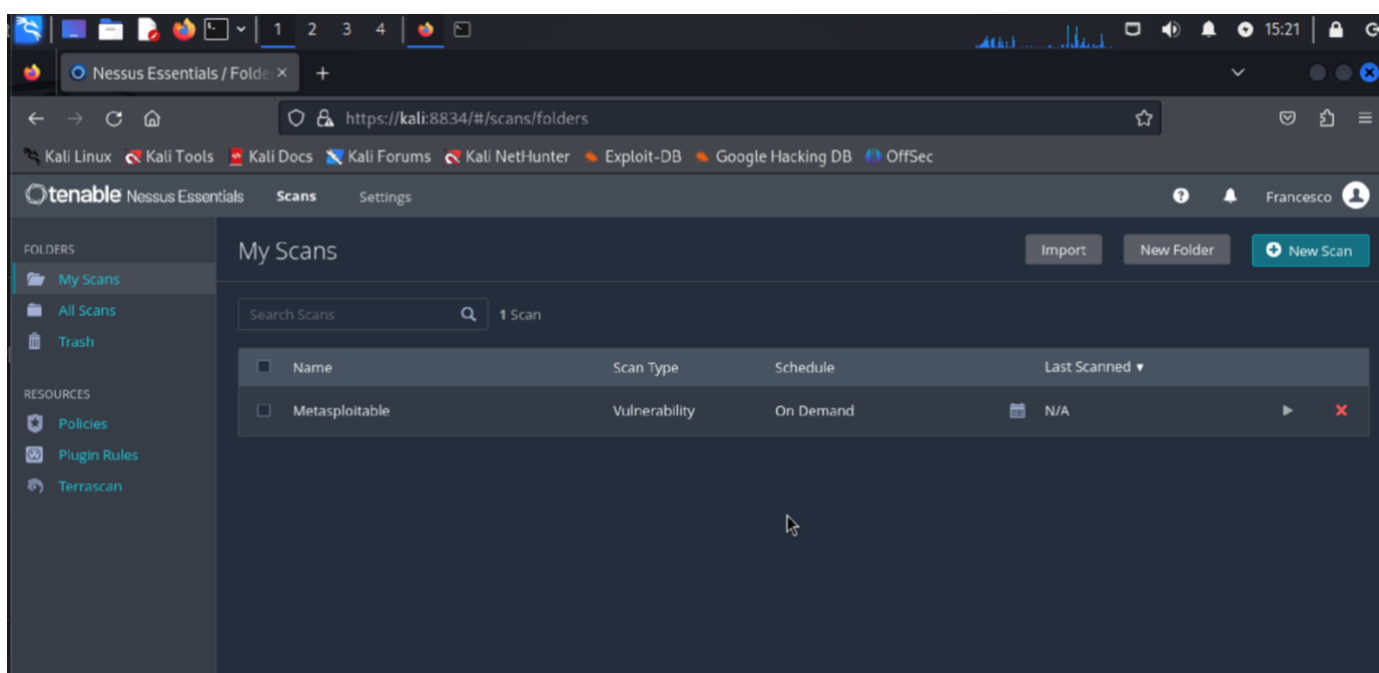
Procediamo dando un nome alla scansione, inseriamo l'indirizzo IP del target, in questo caso 192.168.1.11 (Metasploitable).

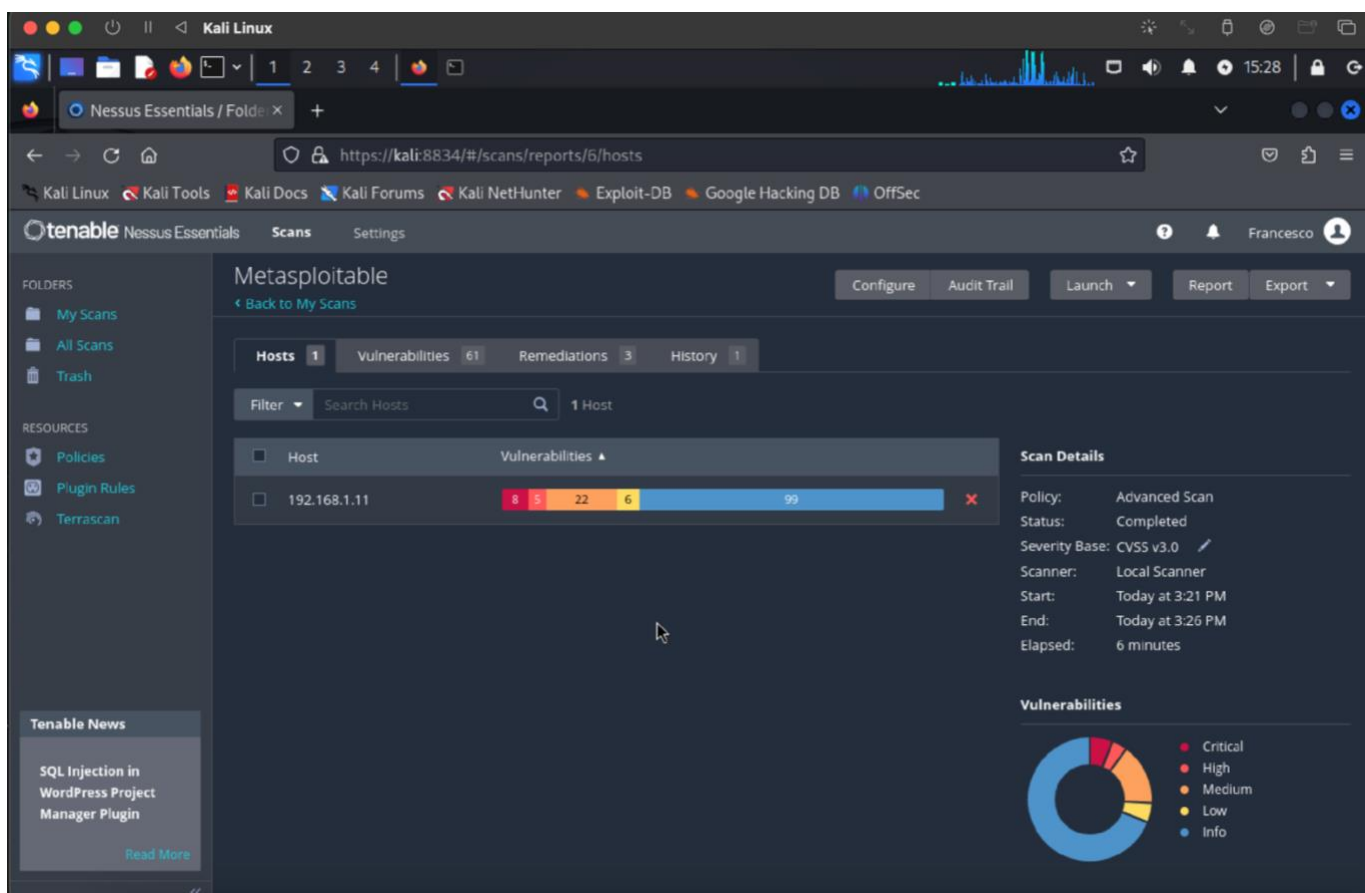
Inoltre, procediamo con la selezione delle porte che ci interessano, quelle comuni, in modo che nessun eviti di perdere tempo scansionando anche le porte che non ci interessano.





Dopo aver effettuato le operazioni precedentemente descritte, salviamo, avviamo lo scan ed attendiamo il risultato.





Nessus ci fornisce un report sulla stessa pagina nella quale abbiamo effettuato lo scan, e cliccandoci possiamo andare a vedere le varie vulnerabilities trovate. In questo caso a noi interessa principalmente lo scan delle porte comuni e di conseguenza vedere se è stato effettuato correttamente lo scan delle porte specificate in precedenza ed eventualmente vedere se sono state segnalate criticità su di esse.

Port 80/tcp was found to be open

To see debug logs, please visit individual host

Port ▲

Hosts

80 / tcp / www

192.168.1.11



Port 139/tcp was found to be open

To see debug logs, please visit individual host

Port ▲

Hosts

139 / tcp / smb

192.168.1.11



Port 445/tcp was found to be open

To see debug logs, please visit individual host

Port ▲

Hosts

445 / tcp / cifs

192.168.1.11



Port 25/tcp was found to be open

To see debug logs, please visit individual host

Port ▼

Hosts

25 / tcp / smtp

192.168.1.11



Port 80/tcp was found to be open

To see debug logs, please visit individual host

Port ▲

Hosts

80 / tcp / www

192.168.1.11



Port 139/tcp was found to be open

To see debug logs, please visit individual host




Port ▲

Hosts

139 / tcp / smb

192.168.1.11



Output	
Port 21/tcp was found to be open	
To see debug logs, please visit individual host	
Port ▲	Hosts
21 / tcp / ftp	192.168.1.11 
Port 22/tcp was found to be open	
To see debug logs, please visit individual host	
Port ▲	Hosts
22 / tcp / ssh	192.168.1.11 
Port 23/tcp was found to be open	
To see debug logs, please visit individual host	
Port ▲	Hosts
23 / tcp / telnet	192.168.1.11 

Una volta verificato se è stato effettuato lo scan delle porte da noi selezionate, andiamo a controllare se ci sono state segnalate criticità su di esse.

Andando a controllare il report ho notato delle criticità su alcune delle porte.

Nello specifico le porte interessate sono: 22, 23, 25, 445.





The image displays two screenshots of the Nessus Essentials web interface, showing vulnerability reports for two different hosts.

**Top Screenshot: Samba Badlock Vulnerability**

- URL:** <https://kali:8834/#/scans/reports/6/hosts/2/vulnerabilities/90509>
- Severity:** HIGH
- Description:** The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.
- Solution:** Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.
- See Also:** <http://badlock.org>, <https://www.samba.org/samba/security/CVE-2016-2118.html>
- Output:** Nessus detected that the Samba Badlock patch has not been applied. To see debug logs, please visit individual host.
- Table:**

Port	Hosts
445 / tcp / cifs	192.168.1.11
- Plugin Details:**
  - Severity: High
  - ID: 90509
  - Version: 1.8
  - Type: remote
  - Family: General
  - Published: April 13, 2016
  - Modified: November 20, 2019
- VPR Key Drivers:**
  - Threat Recency: No recorded events
  - Threat Intensity: Very Low
  - Exploit Code Maturity: Unproven
  - Age of Vuln: 730 days +
  - Product Coverage: Medium
  - CVSSv3 Impact Score: 5.9
  - Threat Sources: No recorded events
- Risk Information:**
  - Vulnerability Priority Rating (VPR): 5.9
  - Exploit Prediction Scoring System (EPSS): 0.0489
  - Risk Factor: Medium
  - CVSS v3.0 Base Score: 7.5

**Bottom Screenshot: Debian OpenSSH/OpenSSL Package Random Number Generator W...**

- URL:** <https://kali:8834/#/scans/reports/6/hosts/2/vulnerabilities/group/32321/32314>
- Severity:** CRITICAL
- Description:** The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library. The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL. An attacker can easily obtain the private part of the remote key and use this to set up decipher the remote session or set up a man in the middle attack.
- Solution:** Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL and OpenVPN key material should be re-generated.
- See Also:** <http://www.nessus.org/u?107f9bdc>, <http://www.nessus.org/u?14f4224>
- Output:** No output recorded. To see debug logs, please visit individual host.
- Table:**

Port	Hosts
22 / tcp / ssh	192.168.1.11
- Plugin Details:**
  - Severity: Critical
  - ID: 32314
  - Version: 1.21
  - Type: remote
  - Family: Gain a shell remotely
  - Published: May 14, 2008
  - Modified: July 24, 2024
- VPR Key Drivers:**
  - Threat Recency: No recorded events
  - Threat Intensity: Very Low
  - Exploit Code Maturity: Functional
  - Age of Vuln: 730 days +
  - Product Coverage: Medium
  - CVSSv3 Impact Score: 3.6
  - Threat Sources: No recorded events
- Risk Information:**
  - Vulnerability Priority Rating (VPR): 5.1
  - Exploit Prediction Scoring System (EPSS): 0.1994
  - Risk Factor: Critical
  - CVSS v2.0 Base Score: 10.0

Nessus ci fornisce spiegazioni dettagliate per quanto riguarda le criticità riscontrate e ci fornisce una soluzione per risolverle.



Inoltre, fornisce dei link utili per poter cercare maggiori informazioni e correggere al meglio le varie vulnerabilità.

Possiamo infine scaricare il report fornito da nessus in PDF ed approfondirlo.