

## 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

New Scan / Basic Network Scan  
[← Back to Scan Templates](#)

**Settings** | Credentials | Plugins

**BASIC**

- General
- Schedule
- Notifications

**DISCOVERY**

**ASSESSMENT**

**REPORT**

**ADVANCED**

Name: scan 1

Description:

Folder: My Scans

Targets: 192.168.1.183

Upload Targets [Add File](#)

Save Cancel

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.

**Settings** | Credentials | Plugins

**BASIC**

**DISCOVERY**

- Host Discovery
- Port Scanning
- Service Discovery
- Identity

**Remote Host Ping**

Ping the remote host ☐ OFF

If set to On, the scanner pings remote hosts on multiple ports to determine if they are alive. Additional options General Settings and Ping Methods appear. If set to Off, the scanner does not ping remote hosts on multiple ports during the scan. Note: To scan VMware guest systems, Ping the remote host must be set to Off.

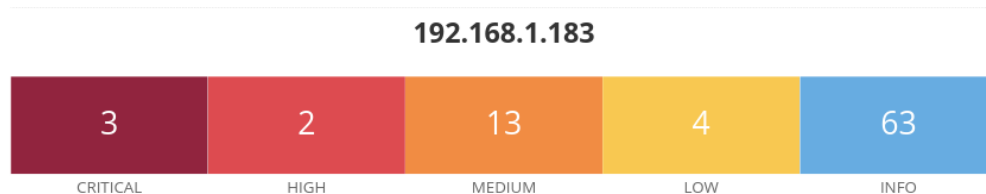
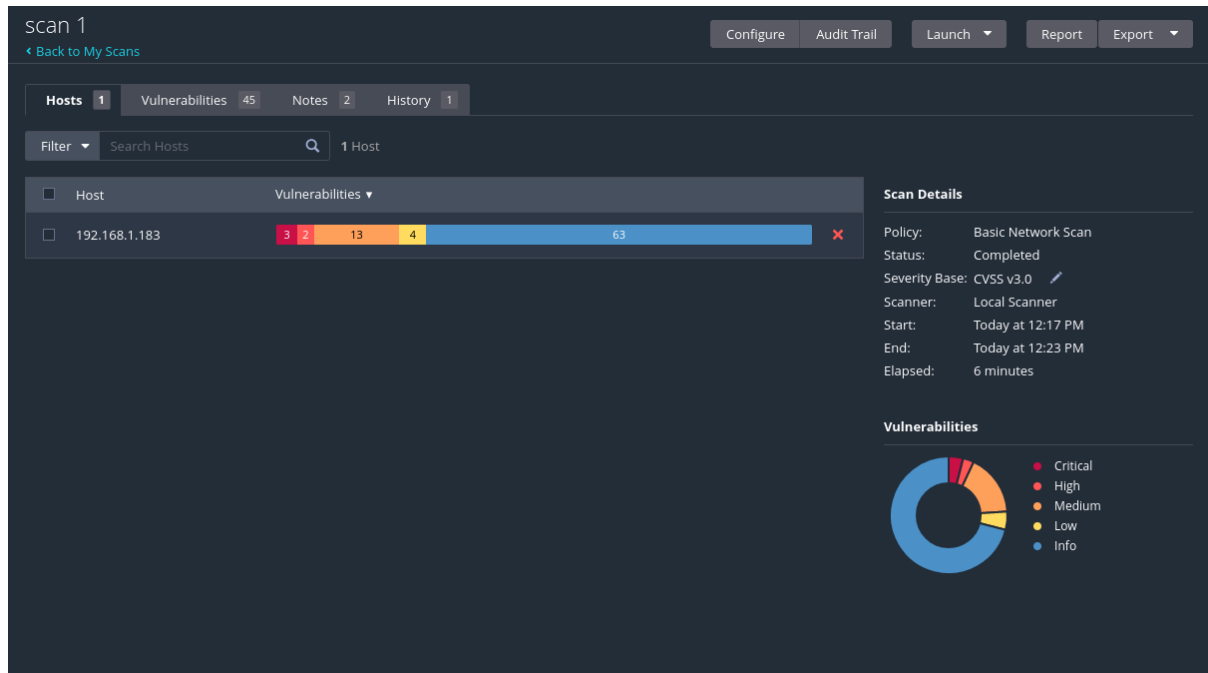
**Ports**

☒ Consider unscanned ports as closed

When enabled, if a port is not scanned with a selected port scanner (for example, the port falls outside of the specified range), the scanner considers it closed.

Port Scan Range: 21, 22, 23, 25, 80, 110, 139, 443, 445, 3389

Successivamente ho avviato la scansione e ho estratto il report.



Prendo in esame la prima vulnerabilità critica fornita dal report nella quale vengono forniti una descrizione della vulnerabilità e dei link che conducono 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.

#### Vulnerabilities

##### 32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

#### Synopsis

The remote SSH host keys are weak.

#### 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.

#### See Also

<http://www.nessus.org/u?107f9bdc>

<http://www.nessus.org/u?f14f4224>

#### 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