

## REPORT S5/L3

---

Effettuare 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.

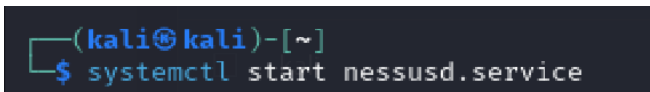
2. Esecuzione della scansione:

- ☐ Avvia la scansione configurata su Nessus.
- ☐ Attendi il completamento della scansione e assicurati che tutte le porte specificate siano state analizzate.

## SVOLGIMENTO

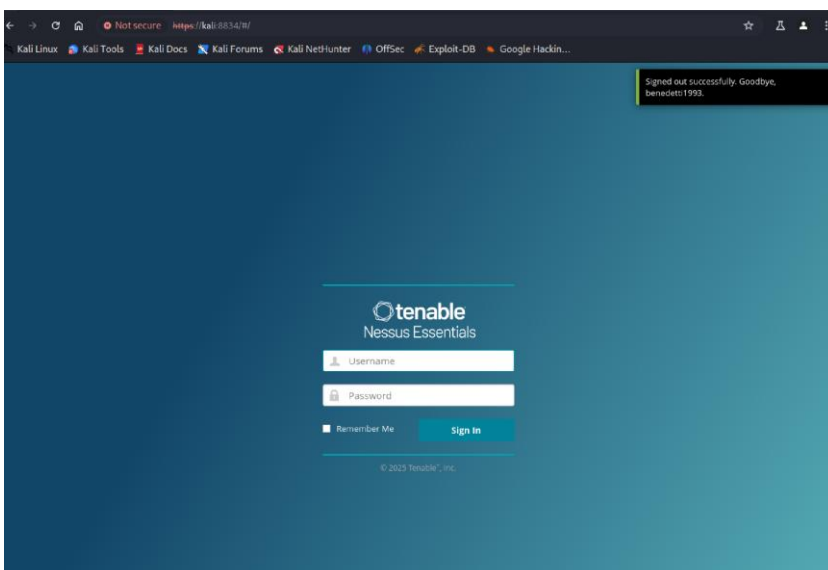
---

Il primo passo dalla macchina Kali è quello di avviare il servizio nessus, mediante comando “**systemctl start nessusd.service**”. **Figura 1**



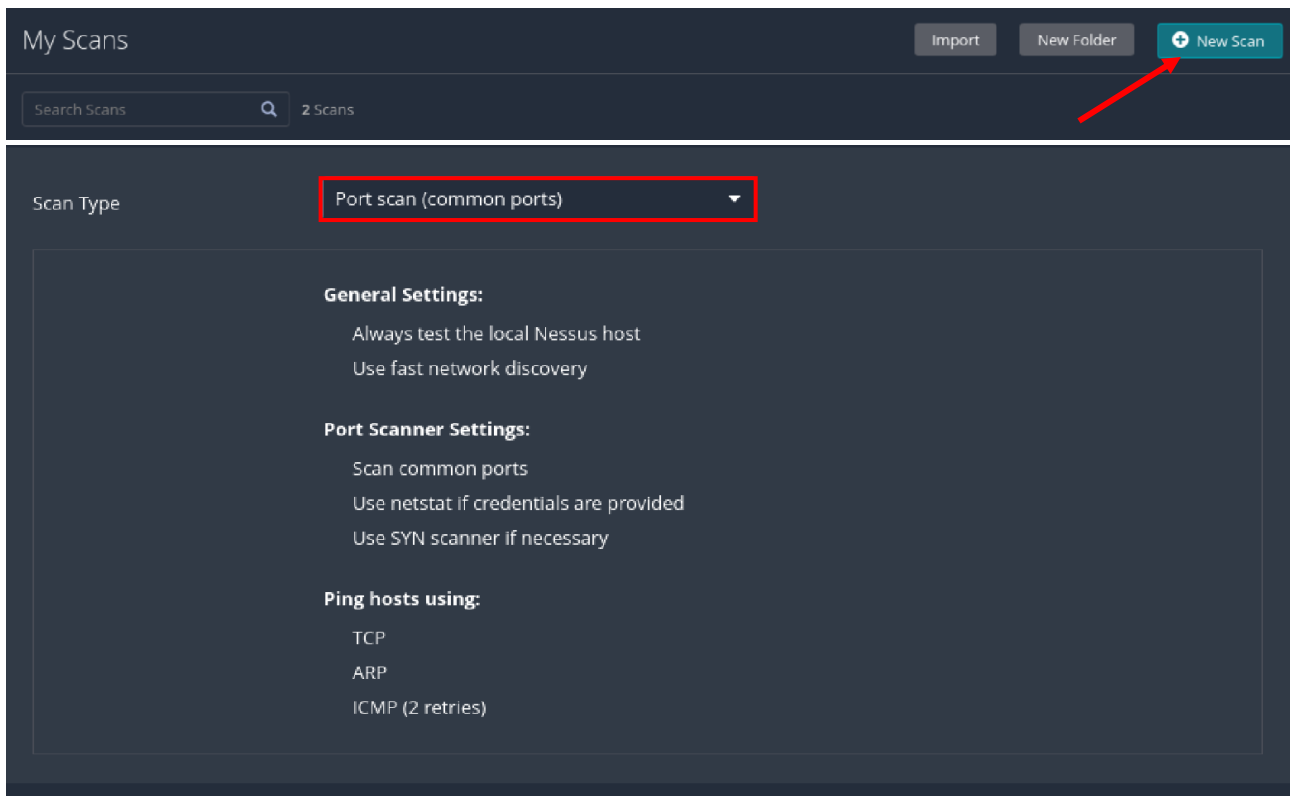
**Figura 1.**

Il servizio sarà sulla porta 8834 alla quale accederemo direttamente dal browser avendo accesso alla pagina di login per avviare la sessione di Nessus. **Figura 2**



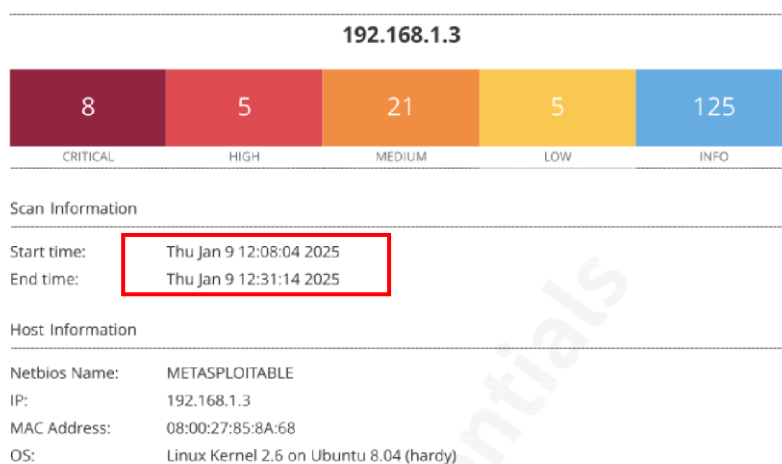
**Figura 2, pagina di login sulla porta 8834.**

Una volta effettuato il login si procede andando a configurare la scansione sul target Metasploitable in particolare solo sulle porte comuni, come da richiesta. Si procede quindi cliccando su “New Scan”, riempiendo i campi e selezionando la scheda “porte comuni” e si lancia la scansione attendendo il risultato. **Figura 3**



**Figura 3**, in alto a destra il pulsante “New Scan” per avviare la scansione, in basso la configurazione delle porte da analizzare.

Successivamente si produrrà un report in formato PDF, e si analizzeranno i risultati prendendo in esame alcune delle vulnerabilità emerse. **Figura 4**



**Figura 4**

Andando ad analizzare la prima pagina del report, si nota come da subito nella parte alta siano messe in evidenza le vulnerabilità rilevate sulla host target con IP: 192.168.1.3 (Metasploitable), ordinate secondo il relativo CVSS (Common vulnerability scoring system), nello specifico sono presenti:

- 8 vulnerabilità con rischio **critico**
- 5 vulnerabilità alto **rischio**
- 21 vulnerabilità rischio **medio**
- 5 vulnerabilità rischio **basso**

Altro elemento importante da tenere in considerazione immediatamente sotto al grafico delle vulnerabilità è quello del tempo di inizio e tempo di fine scansione, in questo caso la scansione è iniziata alle ore 12.08 ed è terminata alle ore 12.31. Nel report per ciascuna delle vulnerabilità rilevata oltre ad esserne presente la descrizione vi è anche la relativa soluzione che può poi essere proposta o meno al cliente, andiamo a prendere in esame per esempio la prima. **Figura 5**

## Vulnerabilities

### 134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)

#### Synopsis

There is a vulnerable AJP connector listening on the remote host.

#### Description

A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).

#### See Also

**Figura 5**

Questa è una vulnerabilità di tipo “**File inclusion**” rilevata su un componente di **Apache Tomcat** anche nota come **GHOSTCAT**, che permette ad un utente remoto di leggere e caricare file su un server vulnerabile. La soluzione proposta dal report è quella di aggiornare la configurazione del componente in questione, visto il rischio critico della vulnerabilità sicuramente questa avrà una priorità elevata.

Andiamo a considerarne un'altra. **Figura 6**

### 32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

#### Synopsis

The remote SSL certificate uses a weak key.

#### Description

The remote x509 certificate on the remote SSL server 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 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>

#### 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.

**Figura 6.**

Nello specifico questa è una vulnerabilità tipica di Debian dovuta ad un bug nella generazione di numeri casuali nelle librerie SSL che a causa di un bug rende predicibili le chiavi crittografiche, la soluzione proposta in questo caso è che tutte le chiavi SSH, SSL e OPeNVPN debbano essere rigenerate. Anche in questo caso il livello di rischio della vulnerabilità in questione è **critico**.

Un'altra minaccia rilevata sempre con rischio **critico** è la “**Bind shell backdoor detection**”, in questo caso è presente una porta aperta sull'host che potrebbe essere sfruttata da un eventuale attaccante per connettersi ed inviare comandi in maniera diretta.