

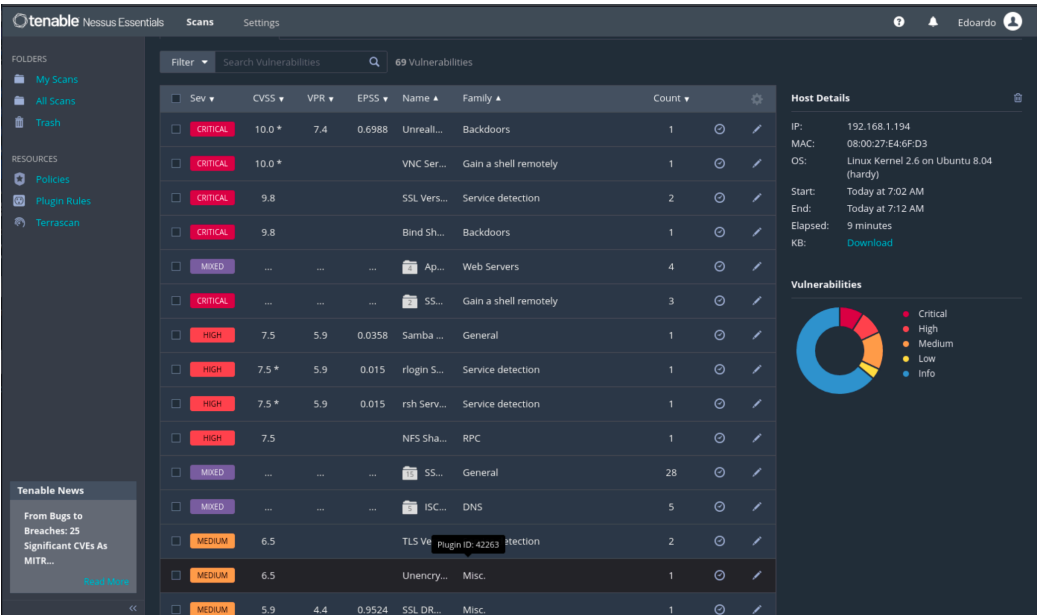
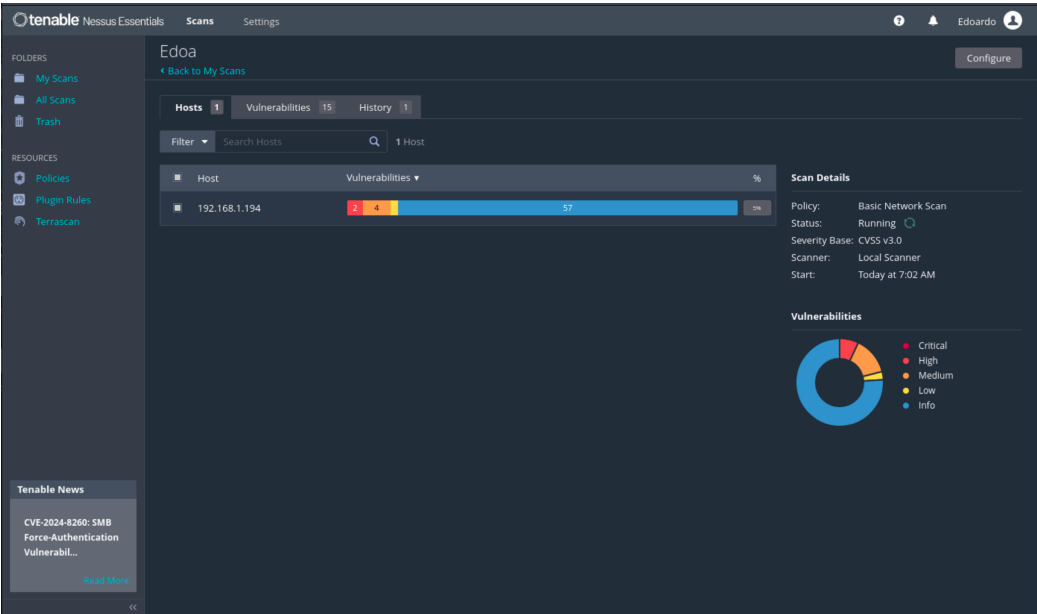
Introduzione

L’obbiettivo di questo esercizio è stato effettuare un vulnerability Scanning sulla macchina Metasploitable utilizzando lo strumento Nessus. Durante l'esecuzione, ho monitorato il progresso e ho atteso il completamento della scansione, assicurandomi che tutte le porte specificate fossero analizzate. La scansione ha impiegato un tempo ragionevole, fornendo risultati dettagliati.

Una volta raggiunta l’interfaccia web per la configurazione della scansione ho selezionato una delle scansioni predefinite, in questo caso “Basic Network Scan”, in alternativa, si potrebbe pensare di scegliere «Advanced Scan» e configurare manualmente tutte le «policy» della nostra scansione.

Nella sezione “Basic” sono stati inserite le informazioni generali come il nome e il target, nello specifico l’indirizzo IP della macchina di Metasploitable: 192.168.1.194.

Nella sezione “discovery” invece è stato inserita la modalità del Port scanner, dove si può scegliere uno di default “port scan common ports o all ports” oppure optare per una configurazione custom, in questo caso è stato scelto “all ports”



La prima informazione contenuta nel report è una vista sulle vulnerabilità trovate divise per colore / priorità: Critical, High, Medium, Low, Info.

## 5 VULNERABILITA'

La versione di Samba, un server CIFS/SMB per Linux e Unix, in esecuzione sull'host remoto ha un difetto, noto come Badlock. Un utente malintenzionato man-in-the-middle in grado di intercettare il traffico tra un client e un server che ospita un database SAM può sfruttare questa falla per forzare un downgrade del livello di autenticazione, che consente l'esecuzione di chiamate di rete.

The screenshot shows the Nessus Essentials interface for a scan named 'Edoia / Plugin #90509'. The left sidebar contains navigation options like 'My Scans', 'All Scans', 'Trash', 'Policies', 'Plugin Rules', and 'Terrascan'. The main content area displays the 'Samba Badlock Vulnerability' with a 'HIGH' severity rating. The description explains that the vulnerability affects Samba versions 4.2.11 through 4.4.2, allowing a man-in-the-middle attacker to force a downgrade of the authentication level. The solution is to upgrade to Samba version 4.2.11 or later. The output section shows a message: 'Nessus detected that the Samba Badlock patch has not been applied.' The right sidebar provides 'Plugin Details' including severity, ID, version, type, family, published date, and modified date. It also includes 'VPR Key Drivers' and 'Risk Information'.

Port	Hosts
445 / tcp / cifs	192.168.1.194

il server IRC remoto è una versione di unrealIRCd con una backdoor che consente a un utente malintenzionato di eseguire codice arbitrario sull'host interessato

The screenshot shows the Nessus Essentials interface for a scan named 'Edoia / Plugin #51988'. The left sidebar is the same as the previous screenshot. The main content area displays the 'Bind Shell Backdoor Detection' with a 'CRITICAL' severity rating. The description states that a shell is listening on the remote port without any authentication being required. The solution is to verify if the remote host has been compromised and reinstall the system if necessary. The output section shows a message: 'Nessus was able to execute the command "id" using the following request:'. This produced the following truncated output (limited to 10 lines):  
root@metasploitable:/# uid=0 (root) gid=0 (root) groups=0 (root)  
root@metasploitable:/#  
To see debug logs, please visit individual host  
The right sidebar provides 'Plugin Details' including severity, ID, version, type, family, published date, and modified date. It also includes 'Risk Information'.

Port	Hosts
1524 / tcp / wild_shell	192.168.1.194

Il servizio SMTP remoto contiene un difetto software che potrebbe consentire a un utente malintenzionato da remoto e senza autenticazione di inserire comandi durante la fase del protocollo di testo in chiaro che verranno poi eseguiti durante nella fase del protocollo di testo cifrato.

Uno sfruttamento riuscito potrebbe consentire a un utente malintenzionato di rubare l'e-mail di una vittima o il SAL associato (Simple Authentication and Security Layer)

The image displays three screenshots of the Tenable Nessus Essentials interface, showing details for different vulnerabilities.

**Screenshot 1: SMTP Service STARTTLS Plaintext Command Injection (Plugin #52611)**

- Severity:** Medium
- ID:** 52611
- Version:** 1.21
- Type:** remote
- Family:** SMTP problems
- Published:** March 10, 2011
- Modified:** March 6, 2019
- VPR Key Drivers:** Threat Recency: No recorded events, Threat Intensity: Very Low, Exploit Code Maturity: PoC, Age of Vuln: 730 days +, Product Coverage: Low, CVSSv3 Impact Score: 6.0, Threat Sources: No recorded events
- Risk Information:** Vulnerability Priority Rating (VPR): 7.3, Exploit Prediction Scoring System (EPSS): 0.0114, Risk Factor: Medium, CVSS v2.0 Base Score: 4.0, CVSS v2.0 Temporal Score: 3.1

**Screenshot 2: SSL Version 2 and 3 Protocol Detection (Plugin #20007)**

- Severity:** Critical
- ID:** 20007
- Version:** 1.34
- Type:** remote
- Family:** Service detection
- Published:** October 12, 2005
- Modified:** April 4, 2022
- Risk Information:** Risk Factor: Critical, CVSS v3.0 Base Score: 9.8, CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H, CVSS v2.0 Base Score: 10.0, CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
- Vulnerability Information:** In the news: true

**Screenshot 3: Bind Shell Backdoor Detection (Plugin #51988)**

- Severity:** Critical
- ID:** 51988
- Version:** 1.10
- Type:** remote
- Family:** Backdoors
- Published:** February 15, 2011
- Modified:** April 11, 2022
- Risk Information:** Risk Factor: Critical, CVSS v3.0 Base Score: 9.8, CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H, CVSS v2.0 Base Score: 10.0, CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C