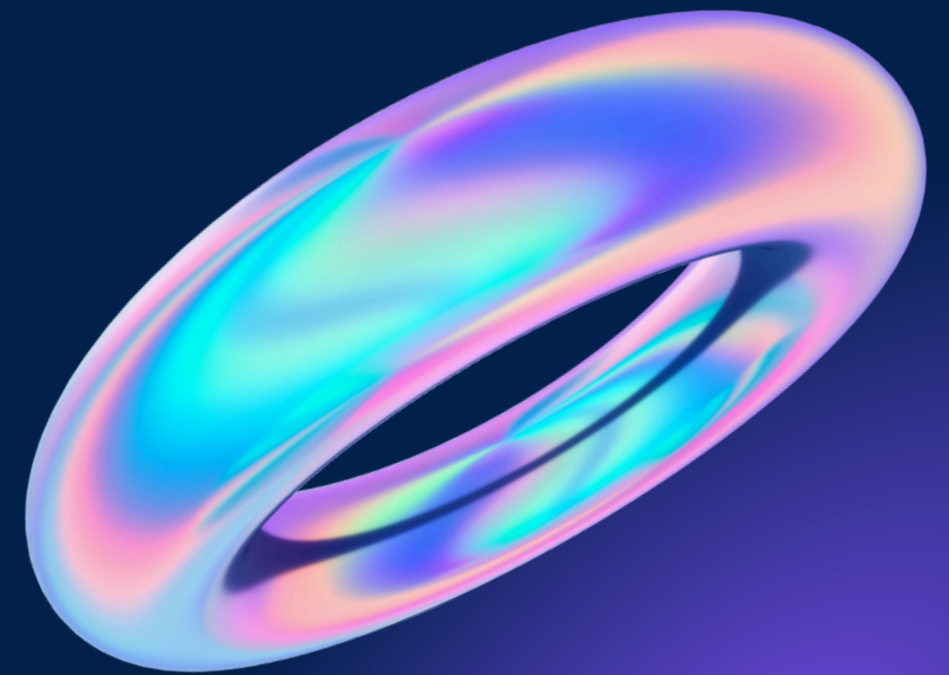




# **VULNERABILITY ASSESSMENT CON NESSUS**

REPORT MORGAN PETRELLI

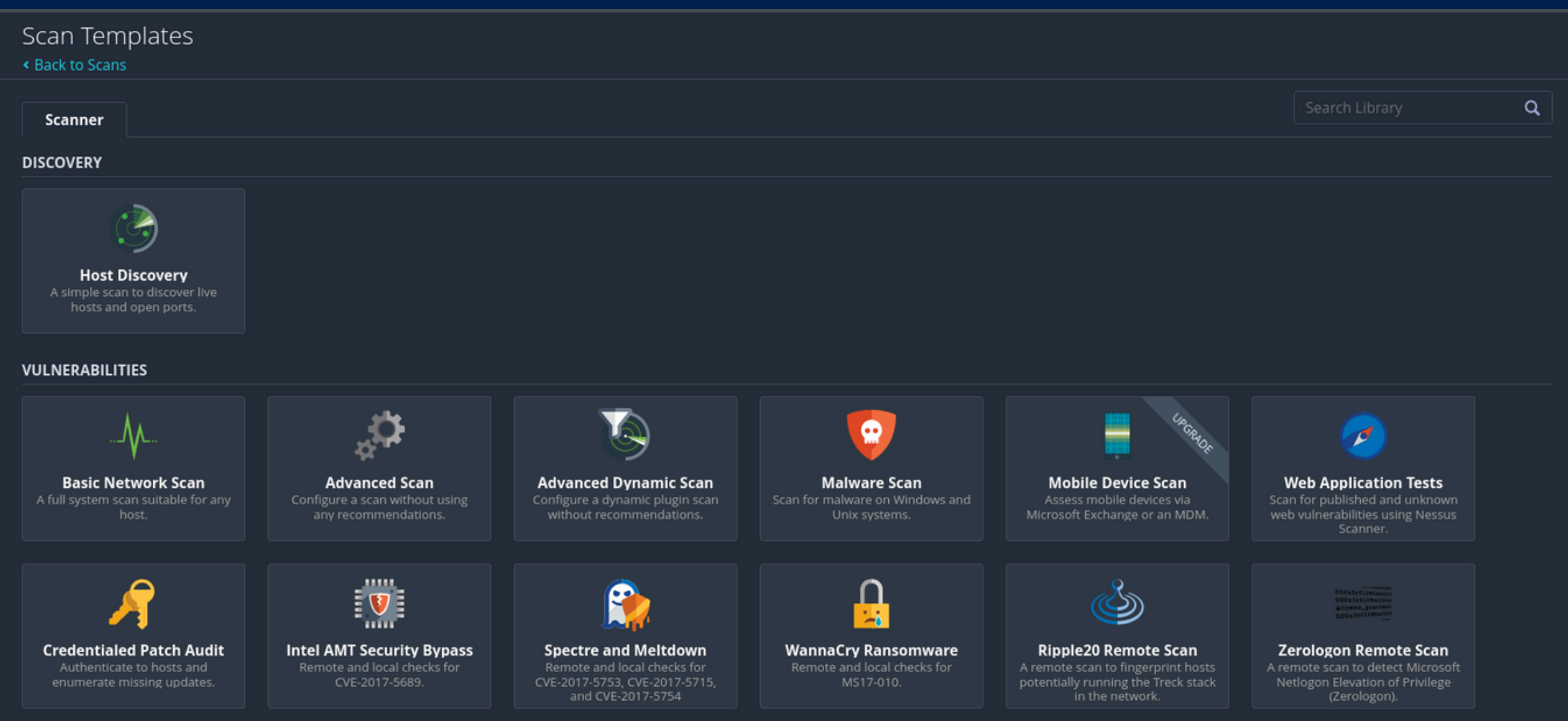
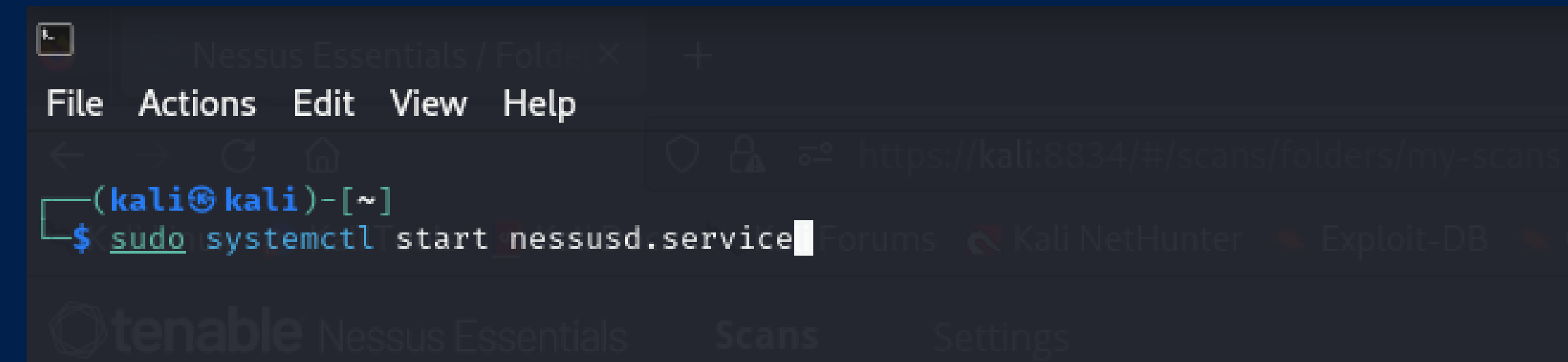


## **TRACCIA:**

**ESERCIZIO TRACCIA EFFETTUARE UN VULNERABILITY ASSESSMENT CON NESSUS SULLA MACCHINA METASPLOITABLE INDICANDO COME TARGET SOLO LE PORTE COMUNI (POTETE SCEGLIERE COME SCANSIONE IL «BASIC NETWORK SCAN», O L'ADVANCED E POI CONFIGURARLO). A VALLE DEL COMPLETAMENTO DELLA SCANSIONE, ANALIZZATE ATTENTAMENTE IL REPORT PER OGNUNA DELLE VULNERABILITÀ RIPORTATE, APPROFONDENDO QUALORA NECESSARIO CON I LINK ALL'INTERNO DEI REPORT E/O CON CONTENUTO DA WEB. GLI OBIETTIVI DELL'ESERCIZIO SONO:**














- FARE PRATICA CON LO STRUMENTO, CON LA CONFIGURAZIONE E L'AVVIO DELLE SCANSIONI.**
- FAMILIARIZZARE CON ALCUNE DELLE VULNERABILITÀ NOTE CHE TROVERETE SPESSO SUL VOSTRO PERCORSO DA PENETRATION TESTER.**

CON QUESTO COMANDO  
SI AVVIA IL SERVIZIO DI  
NESSUS



POI HO PREMUTO SU “BASIC  
NETWORK SCAN” PER  
EFFETTUARE UNA SCANSIONE  
DELLE VULNERABILITÀ DI  
METASPLOITABLE

**HO CONFIGURATO LA SCANSIONE INSERENDO NOME, INDIRIZZO IP, TIPO DI SCAN E COME DEVE ESSERE IL REPORT FINALE.**

 Sev ▼	CVSS ▼	VPR ▼	Name ▲	Family ▲	Count ▼
 CRITICAL	10.0 *		NFS Exported Share Information Disclosure	RPC	1
 CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1
 CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1
 CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2
 CRITICAL	9.8		Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1
 MIXED	...	...	 4 Phpmyadmin (Multiple Issues)	CGI abuses	4
 CRITICAL	...	...	 2 SSL (Multiple Issues)	Gain a shell remotely	3
 MIXED	...	...	 3 PHP (Multiple Issues)	CGI abuses	3
 HIGH	7.5 *		CGI Generic Remote File Inclusion <div>Plugin ID: 42256</div>	CGI abuses	1

HO OTTENUTO LE VARIE VULNERABILITÀ  
PRESENTI SU META

Generate Report

Report Format:

☐ HTML

☒ PDF

☐ CSV

Select a Report Template:

SYSTEM

Complete List of Vulnerabilities by Host

Detailed Vulnerabilities By Host

Detailed Vulnerabilities By Plugin

Vulnerability Operations

Template Description:

This report presents detailed vulnerabilities by host.

Filters Applied:

None

Formatting Options:

☒ Include page breaks between vulnerability results

Generate Report

Cancel

☐ Save as default

IN FINE HO SCARICATO IL  
REPORT COME PDF PER  
VISUALIZZARLO