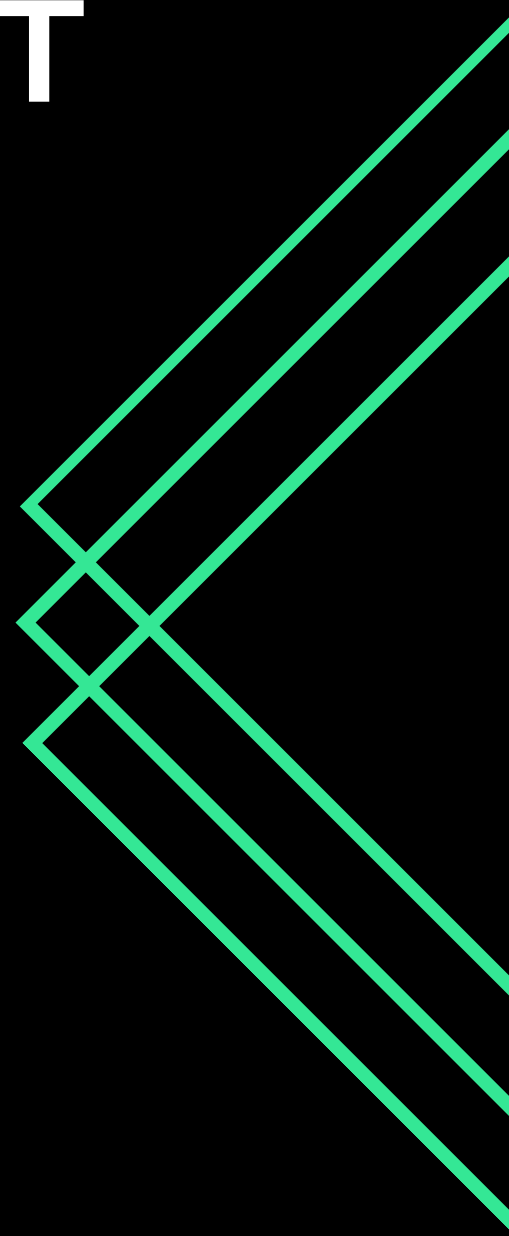



Febbraio 2024

# CYBER SECURITY SPECIALIST

S5L4



Jacopo Trovato

# Vulnerability Assessment

Tramite il software "Tenable" è stata eseguita una scansione Nessus sul target Metaspolitable (192.168.49.101). Sono stati rivelati 133 vulnerabilità di cui:

- 10 Critical;
- 7 High;
- 24 Medium;
- 8 Low;
- 84 Info

Verranno analizzate 2 vulnerabilità tra tutti i vari livelli di criticità.

## Critical

CRITICAL	9.8	8.9	70728	Apache PHP-CGI Remote Code Execution
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.8	5.9	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerability (PMASA-2019-3)
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	5.1	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	5.1	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password

- La prima vulnerabilità significa che sul web remoto l'installazione PHP ha una falla che permette ad un ipotetico attaccante di entrare;
- La vulnerabilità numero 5 indica che il server host è affetto da una vulnerabilità SQLi ovvero una tecnica di hacking che sfrutta alcuni errori nella programmazione di pagine HTML.

# High

HIGH	8.8	7.4	19704	TWiki 'rev' Parameter Arbitrary Command Execution
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	6.7	90509	Samba Badlock Vulnerability
HIGH	7.5*	8.9	59088	PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution
HIGH	7.5*	6.7	36171	phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injection (PMASA-2009-4)

Le criticità di livello High sono meno pericolose delle precedenti ma comunque devono essere motivo di preoccupazione.

- La criticità più alta sta ad indicare che il server web remoto ospita un'applicazione CGI che è affetta da una vulnerabilità di esecuzione.
- La seconda vulnerabilità sta a significare che è affettuata da un Service Downgrade/Reflected DoS che rende vulnerabile il server.