

# REPORT DIRIGENZIALE VULNERABILITA'

## 192.168.49.101



### Scan Information

Start time: Thu Feb 23 02:22:45 2023  
End time: Thu Feb 23 02:34:04 2023

### Host Information

Netbios Name: METASPLOITABLE  
IP: 192.168.49.101  
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

## Considerazioni generali

Dai risultati delle nostre operazioni ci risultano svariate vulnerabilità, molte anche particolarmente gravi, che comportano quindi seri rischi per i sistemi aziendali.

Alcune di esse permettono a potenziali malintenzionati di assumere il completo controllo dei sistemi aziendali, quindi avendo accesso a file e cartelle riservate, oppure il totale spegnimento ed eliminazione di qualsiasi servizio presente sul server analizzato.

## Priorità di risoluzione

Si consiglia di risolvere prima le vulnerabilità critiche, in quanto sono sia quelle più comuni, e quindi più facili da trovare per un malintenzionato, che le più gravi, che comprometterebbero quindi la completa funzionalità dei sistemi aziendali.

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	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	10.0	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	61708	VNC Server 'password' Password

Alcune di esse sono molto semplici da risolvere, come per esempio l'ultima, cambiando la password di default del servizio.

Altre invece richiedono un intervento strutturale atto ad aggiornare il sistema operativo installato sulla macchina, in quanto così vecchio da non essere più supportato dalle patch di sicurezza.

Successivamente si andranno a risolvere le vulnerabilità di grado alto, che possono comportare una falla nella riservatezza dei dati, oppure un accesso non autorizzato ai dati aziendali.

HIGH	8.6	<a href="#">136769</a>	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	<a href="#">42256</a>	NFS Shares World Readable
HIGH	7.5	<a href="#">42873</a>	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	<a href="#">90509</a>	Samba Badlock Vulnerability
HIGH	7.5*	<a href="#">10205</a>	rlogin Service Detection
HIGH	7.5*	<a href="#">10245</a>	rsh Service Detection

In questo caso la risoluzione è meno strutturale e richiede l'utilizzo di servizi più appropriati per la condivisione di file e cartelle al interno del azienda. E l'aggiornamento di alcuni di quelli già presenti.

Procedendo poi con la risoluzione delle vulnerabilità, passiamo quindi a quelle di rischio medio:

Esse sono simili a quelle di grado alto come rischi, ma tuttavia presuppongono una conoscenza più avanzata dei sistemi informatici da parte di un potenziale attaccante.

MEDIUM	6.8	<a href="#">78479</a>	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	6.5	<a href="#">139915</a>	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	<a href="#">51192</a>	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	<a href="#">57582</a>	SSL Self-Signed Certificate
MEDIUM	6.5	<a href="#">104743</a>	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	<a href="#">42263</a>	Unencrypted Telnet Server
MEDIUM	5.9	<a href="#">136808</a>	ISC BIND Denial of Service
MEDIUM	5.9	<a href="#">31705</a>	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	<a href="#">89058</a>	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	5.9	<a href="#">65821</a>	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	<a href="#">12085</a>	Apache Tomcat Default Files
MEDIUM	5.3	<a href="#">57608</a>	SMB Signing not required
MEDIUM	5.3	<a href="#">15901</a>	SSL Certificate Expiry
MEDIUM	5.3	<a href="#">45411</a>	SSL Certificate with Wrong Hostname
MEDIUM	5.3	<a href="#">26928</a>	SSL Weak Cipher Suites Supported
MEDIUM	4.0*	<a href="#">52611</a>	SMTP Service STARTTLS Plaintext Command Injection
MEDIUM	4.3*	<a href="#">90317</a>	SSH Weak Algorithms Supported
MEDIUM	4.3*	<a href="#">81606</a>	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)

Per risolverle, alcune verranno risolte a cascata dal aggiornamento di alcuni servizi, per altre invece è necessaria la modifica di alcune configurazioni di alcuni servizi presenti. Poi vediamo che alcuni certificati presenti non sono validi, e vanno quindi aggiornati con fonti sicure, ciò è un rischio per la riservatezza delle informazioni che passano al interno dei canali cifrati.

Per ultimo verranno poi risolte le vulnerabilità di grado basso

LOW	3.7	<a href="#">153953</a>	SSH Weak Key Exchange Algorithms Enabled
LOW	3.7	<a href="#">83738</a>	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
LOW	2.6*	<a href="#">70658</a>	SSH Server CBC Mode Ciphers Enabled
LOW	2.6*	<a href="#">71049</a>	SSH Weak MAC Algorithms Enabled
LOW	2.6*	<a href="#">10407</a>	X Server Detection

Esse sono vulnerabilità principalmente di crittografia e algoritmi deboli di cifratura, essi vanno disabilitati e/o aggiornati ove possibile.

Le vulnerabilità di tipo INFO sono semplici possibilità che si hanno per ottenere informazioni riguardo ai servizi e al sistema in uso, non sono di per sé un rischio per la sicurezza se si mantengono tutti i servizi aggiornati, eventualmente con semplici regole di firewall o tramite particolari configurazioni dei servizi possono essere ridotte o eliminate.

Per sintesi ne elencheremo solo alcune:

INFO	N/A	39520	Backported Security Patch Detection (SSH)
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10028	DNS Server BIND version Directive Remote Version Detection
INFO	N/A	11002	DNS Server Detection
INFO	N/A	72779	DNS Server Version Detection
INFO	N/A	35371	DNS Server hostname.bind Map Hostname Disclosure
INFO	N/A	54615	Device Type
INFO	N/A	10092	FTP Server Detection
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure