FRANCESCO PERSICHETTI

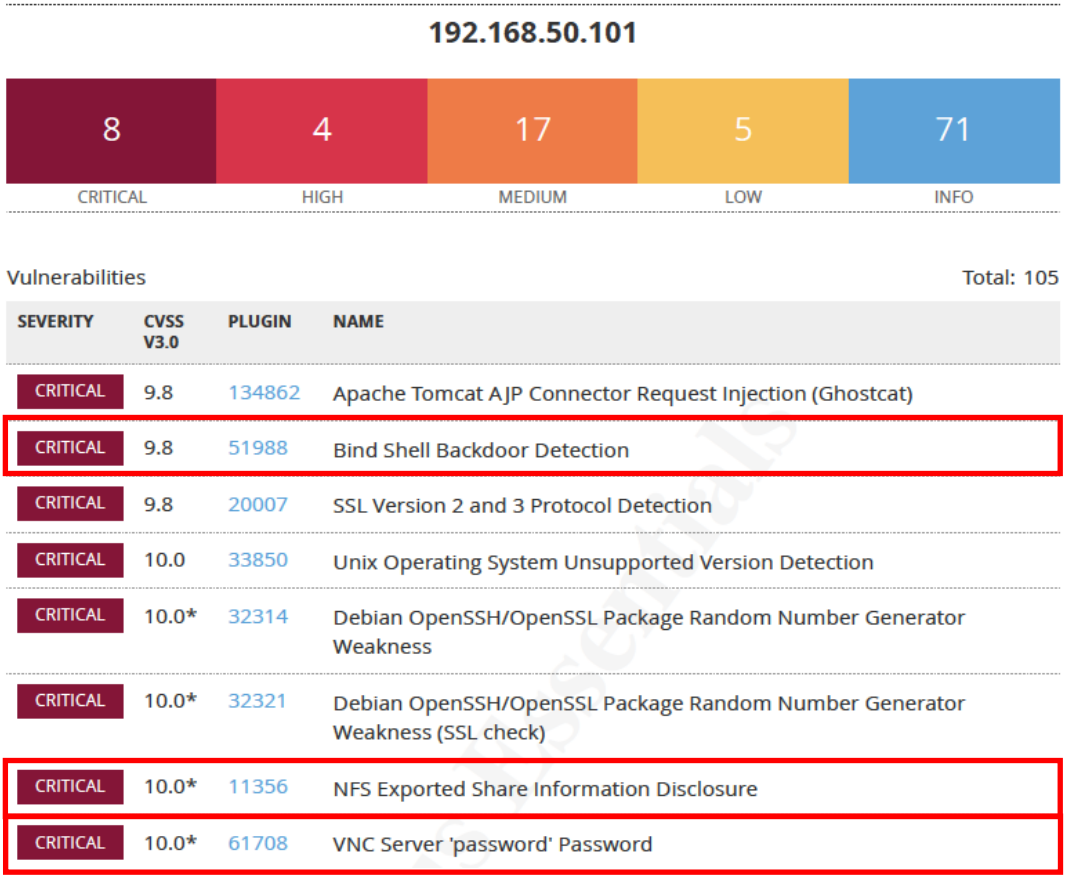
Metasploitable

Scan Information

Start time:	Fri Nov 25 08:59:26 2022
End time:	Fri Nov 25 09:26:10 2022

Host Information

Netbios Name:	METASPLOITABLE
IP:	192.168.50.101
MAC Address:	08:00:27:74:3D:F0
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)



192.168.50.101

8	4	17	5	71
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 105

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

Ai fini dell'esercitazione prendiamo in considerazione solo le vulnerabilità evidenziate in rosso

51988 - Bind Shell Backdoor Detection

DESCRIZIONE:

Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarlo collegandosi alla porta remota e inviando comandi direttamente.

SOLUZIONE:

Verificare se l'host remoto è stato compromesso e, se necessario, reinstallare il sistema.

RISK FACTOR: CRITICAL

Plugin Output: tcp/1524/wild_shell

11356 - NFS Exported Share Information Disclosure

DESCRIZIONE:

Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un utente malintenzionato potrebbe essere in grado di sfruttare questo per leggere (e possibilmente scrivere) file su host remoto.

SOLUZIONE:

Configura NFS sull'host remoto in modo che solo gli host autorizzati possano montare le sue condivisioni remote.

RISK FACTOR: CRITICAL

Plugin Output: udp/2049/rpc-nfs

61708 - VNC Server 'password' Password

DESCRIZIONE:

Il server VNC in esecuzione sull'host remoto è protetto da una password debole. Nessus è stato in grado di accedere utilizzando l'autenticazione VNC e una password di "password". Un utente malintenzionato remoto e non autenticato potrebbe sfruttarlo per assumere il controllo del sistema.

SOLUZIONE:

Proteggi il servizio VNC con una password sicura.

RISK FACTOR: CRITICAL

Plugin Outpu: tcp/5900/vnc