



REPORT METASPOITABLE VULNERABILITIES

Ernesto Robles

DISPOSITIVI COINVOLTI



Macchina Kali ip: 192.168.1.60

Macchina Metasploitable ip: 192.168.1.67



STRUMENTI UTILIZZATI

Lo strumento utilizzato per la scansione delle vulnerabilità è Nessus sviluppato da Tenable Network Security.

Nessus effettua una serie di test automatici su servizi e porte aperte, cercando di individuare vulnerabilità e potenziali problemi di sicurezza come (vulnerabilità del software, configurazioni errate, password deboli, ecc..). Può essere utilizzato sia in ambito aziendale che personale ed è molto utile per amministratori di sistema, professionisti della sicurezza informatica e pen tester.

Vulnerabilities 70

Filter ▾

Search Vulnerabilities



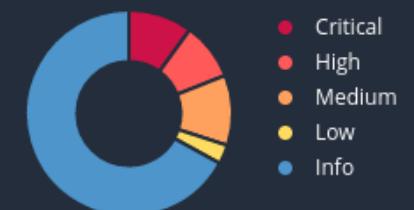
70 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count	⋮
CRITICAL	10.0 *	5.9	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		Bind Shell Backdoor Detection	Backdoors	1	
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3	
MIXED	SSL (Multiple Issues)	Service detection	3	
MIXED	Apache Tomcat (Multiple Issues)	Web Servers	3	
HIGH	7.5		NFS Shares World Readable	RPC	1	
HIGH	7.5 *	6.7	rlogin Service Detection	Service detection	1	
HIGH	7.5 *	6.7	rsh Service Detection	Service detection	1	
HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1	
MIXED	SSL (Multiple Issues)	General	28	
MIXED	ISC Bind (Multiple Issues)	DNS	5	

Host Details

IP: 192.168.1.67
MAC: 08:00:27:4A:E1:25
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start: Today at 3:26 PM
End: Today at 3:44 PM
Elapsed: 19 minutes
KB: [Download](#)

Vulnerabilities



Con la scansione basic network scan scegliendo come target solo le porte comuni si ha come risultato 70 vulnerabilità totali

Nel grafico qua accanto possiamo vedere evidenziate le vulnerabilità in base alla loro criticità.

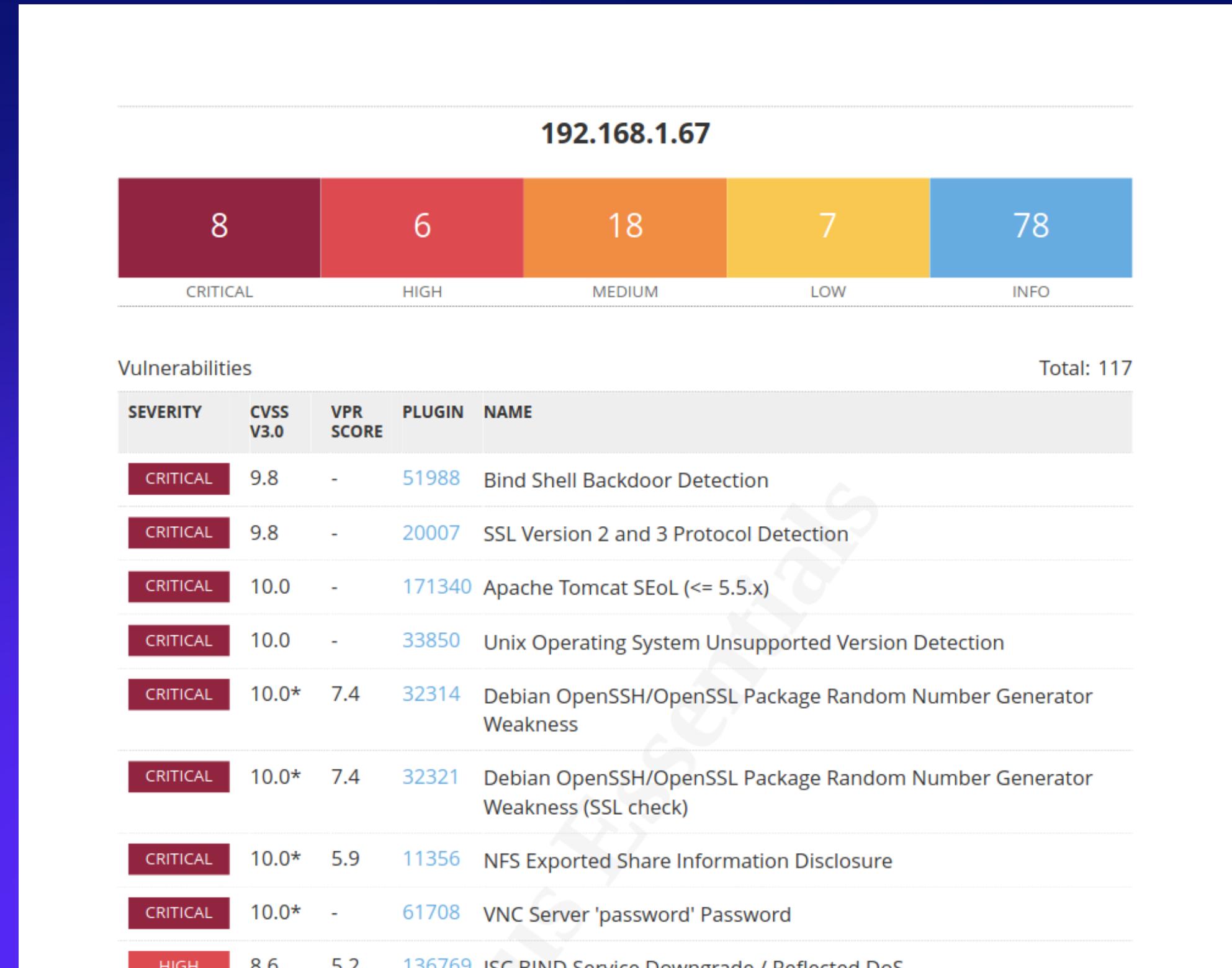
Verranno analizzate ora le prima 4 critical.

La vulnerabilità: "SSL Version 2 and 3 Protocol Detection" fa riferimento al fatto che queste due versioni sono affette da vulnerabilità crittografiche un attaccante potrebbe condurre un man-in-the-middle sfruttandole

Soluzione:

Va consultata la documentazione per disabilitarle e usato al loro posto TLS 1.2 o superiore

<https://www.schneier.com/academic/paperfiles/paper-ssl.pdf>



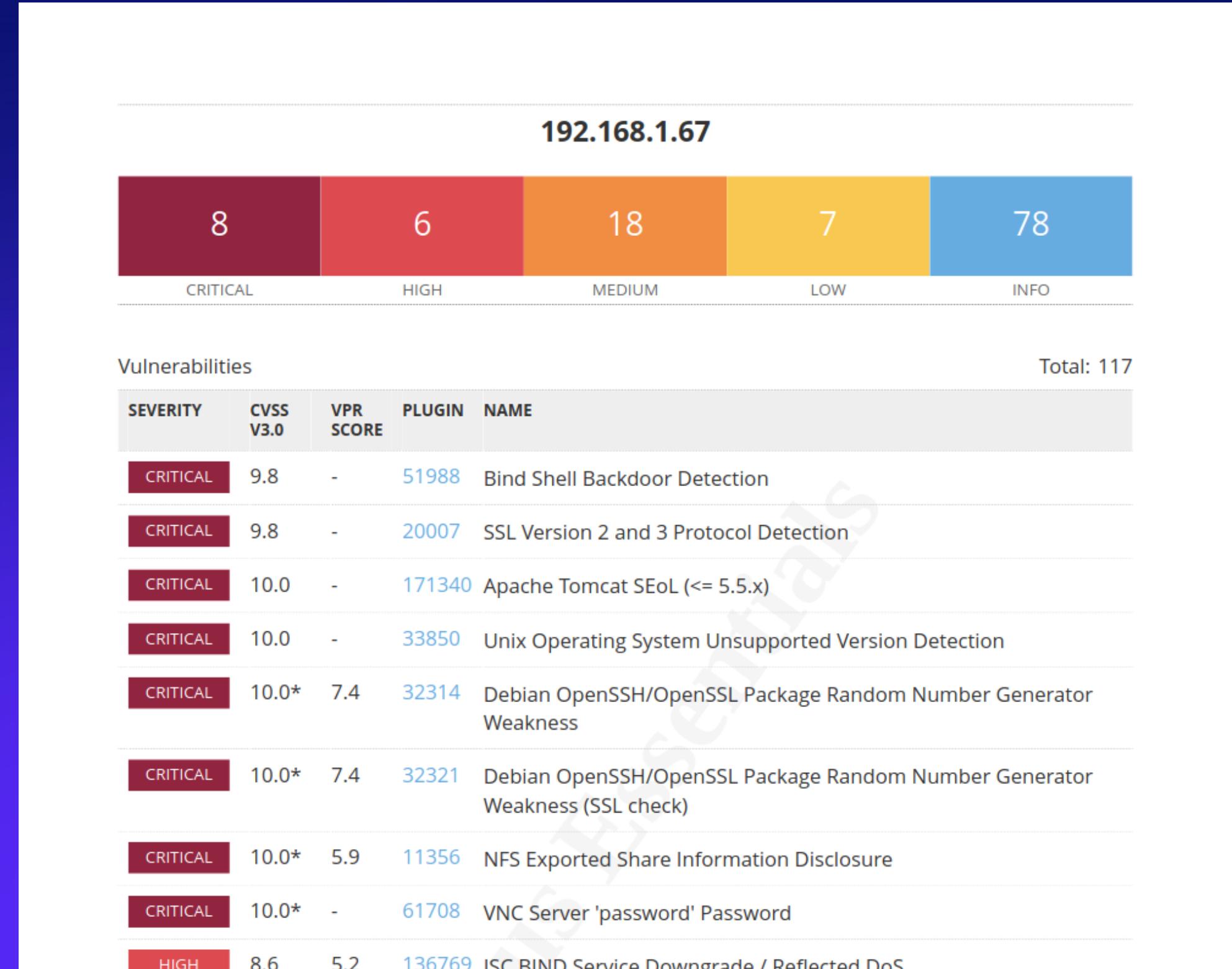
Nel grafico qua accanto possiamo vedere evidenziate le vulnerabilità in base alla loro criticità.

Verranno analizzate ora le prima 4 critical.

La vulnerabilità: "Bind Shell Backdoor Detection" fa riferimento al fatto che la shell è in ascolto sulla porta senza nessuna regola di autenticazione, un attaccante si potrebbe connettere ed inviare comandi direttamente.

Soluzione:

Bisogna verificare che l'host non sia compromesso e reinstallato il suo sistema operativo per sicurezza.



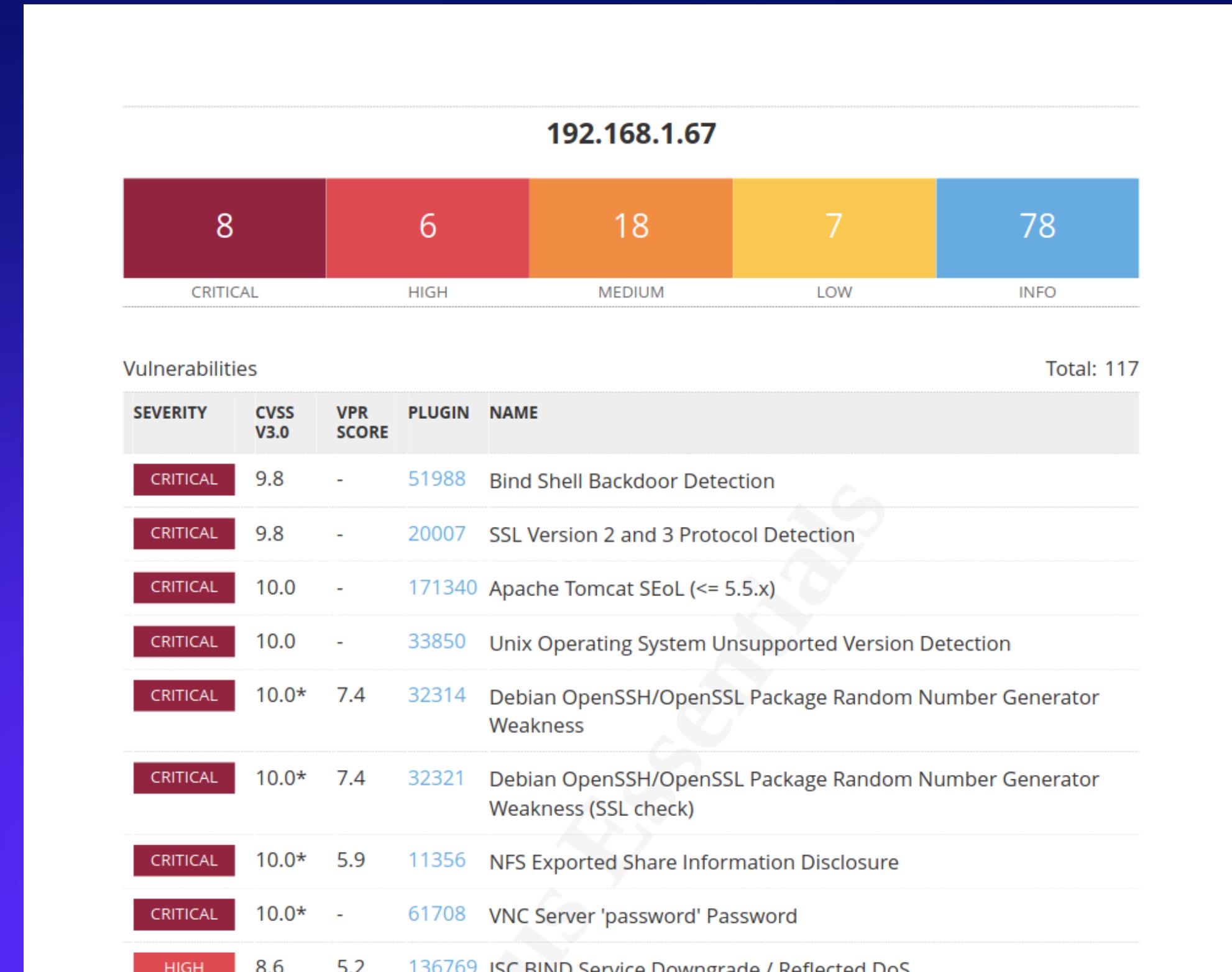
Nel grafico qua accanto possiamo vedere evidenziate le vulnerabilità in base alla loro criticità.

Verranno analizzate ora le prima 4 critical.

La vulnerabilità: "Unix Operating System Unsupported Version Detection" fa riferimento al fatto che la versione del OS è vecchia e senza più supporto di aggiornamenti.

Soluzione:

Bisogna aggiornare ad una versione corrente che dunque dispone degli aggiornamenti di sicurezza



Nel grafico qua accanto possiamo vedere evidenziate le vulnerabilità in base alla loro criticità.

Verranno analizzate ora le prima 4 critical.

La vulnerabilità: "Apache Tomcat SEoL (<= 5.5.x)" fa riferimento al fatto che la versione è datata e il suo vendor ne ha abbandonato il supporto rimanendo così senza aggiornamenti recenti di sicurezza.

Soluzione:

Bisogna aggiornare ad una versione corrente che dunque dispone degli aggiornamenti di sicurezza

<https://tomcat.apache.org/tomcat-55-eol.html>

