

# Pentest Toolbox Report

This report is generated by the Toolbox

**Generated on: 2024-05-14 00:37:06**

## Executive Summary

This report contains the results of a comprehensive penetration test conducted to identify and address security vulnerabilities within the target. The findings and recommendations aim to enhance the security posture of the organization.

## Results for 192.168.86.134

### Nmap Results:

Port	Service	Version	CVEs
21	ftp	vsftpd 2.3.4	CVE-2011-2523
22	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)	CVE-2010-4478 CVE-2012-1577 CVE-2010-4478 CVE-2011-1013
23	telnet	Linux telnetd	
25	smtp	Postfix smtpd	
53	domain	ISC BIND 9.4.2	CVE-2008-0122 CVE-2012-1667 CVE-2012-1667 CVE-2014-8500 CVE-2012-5166 CVE-2012-4244 CVE-2012-3817 CVE-2014-8500 CVE-2012-5166 CVE-2012-4244 CVE-2012-3817 CVE-2008-4163 CVE-2010-0382 CVE-2010-0382 CVE-2017-3141 CVE-2015-8461 CVE-2015-8461
80	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)	CVE-2011-3192 CVE-2017-7679 CVE-2017-3167 CVE-2009-1891 CVE-2009-1890
111	rpcbind	2 (RPC #100000)	
139	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)	CVE-2017-7494 CVE-2020-1472 CVE-2020-25719 CVE-2020-17049 CVE-2020-25717 CVE-2020-10745 CVE-2022-45141

445	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)	CVE-2017-7494 CVE-2020-1472 CVE-2020-25719 CVE-2020-17049 CVE-2020-25717 CVE-2020-10745 CVE-2022-45141
512	exec	netkit-rsh rexecd	
1099	java-rmi	GNU Classpath grmiregistry	
1524	bindshell	Metasploitable root shell	
2049	nfs	2-4 (RPC #100003)	
2121	ftp	ProFTPD 1.3.1	CVE-2011-4130 CVE-2011-4130 CVE-2009-0542 CVE-2019-12815 CVE-2010-3867 CVE-2010-3867
3306	mysql	MySQL 5.0.51a-3ubuntu5	CVE-2009-2446 CVE-2009-2446 CVE-2009-4484 CVE-2008-0226 CVE-2008-0226
3632	distccd	distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))	
5432	postgresql	PostgreSQL DB 8.3.0 - 8.3.7	CVE-2013-1903 CVE-2013-1902 CVE-2013-1903 CVE-2013-1902 CVE-2019-10164 CVE-2010-1447 CVE-2010-1169 CVE-2013-1900 CVE-2010-1169 CVE-2010-1447 CVE-2010-1169 CVE-2015-3166 CVE-2015-0244
5900	vnc	VNC (protocol 3.3)	
6000	X11	(access denied)	
6667	irc	UnrealIRCd	
6697	irc	UnrealIRCd	
8009	ajp13	Apache Jserv (Protocol v1.3)	

8180	http	Apache Tomcat/Coyote JSP engine 1.1	
8787	drb	Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)	

### ***Web Scans Results:***

Port	Service	SQLMap	Nikto
80	http	all tested parameters do not appear to be injectable	CVE-1999-0678 CVE-2003-1418

### ***SSH Brute Force Results:***

Port	Username List	Password List	Result
22	top-usernames-shortlist.txt	200_most_used_passwords.txt	SSH connection successful with user/user

## Results for 192.168.1.1

### *SYN Flood Results:*

Port	Result
Port: 53	Test completed
Port: 80	Test completed
Port: 139	Test completed
Port: 443	Test completed
Port: 445	Test completed
Port: 631	Test completed

### *Malformed Packet Results:*

Port	Results
Port: 53	Flag: FPU: No response Flag: U: No response Flag: R: No response Flag: P: No response
Port: 80	Flag: FPU: No response Flag: U: No response Flag: R: No response Flag: P: No response
Port: 139	Flag: FPU: No response Flag: U: No response Flag: R: No response Flag: P: No response
Port: 443	Flag: FPU: No response Flag: U: No response Flag: R: No response Flag: P: No response
Port: 445	Flag: FPU: No response Flag: U: No response Flag: R: No response Flag: P: No response
Port: 631	Flag: FPU: No response Flag: U: No response Flag: R: No response Flag: P: No response