



Vulnerability Scanning Lab

Consolidated Critical Vulnerabilities (Metasploitable2 – 192.168.56.102)

Nmap Scan Report:

```
# Nmap 7.95 scan initiated Sun Aug 31 12:05:14 2025 as: /usr/lib/nmap/nmap --privileged -sV -oN nmap_scan.txt 192.168.56.102
Nmap scan report for 192.168.56.102
Host is up (0.066s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:39:DC:85 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Aug 31 12:05:28 2025 -- 1 IP address (1 host up) scanned in 13.42 seconds
```







Nikto Scan Results:

```
- Nikto v2.5.0/
+ Target Host: 192.168.56.102
+ Target Port: 80
+ GET /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ GET /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options:
+ GET /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See:
https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/:
+ GET /index: Uncommon header 'tcn' found, with contents: list.
+ GET /index: Apache mod negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See:
http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275:
+ HEAD Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ EYFDYFBE /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ TRACE /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing:
+ GET /phpinfo.php: Output from the phpinfo() function was found.
+ GET /doc/: Directory indexing found.
+ GET /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: CVE-1999-0678:
+ GET /?-PHPBB85F2A0-3C92-11D3-A2A0-4C7B0C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184:
+ GET /?-PHPPE9568F36-D428-11D2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184:
+ GET /?-PHPPE9568F36-D428-11D2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184:
+ GET /?-PHPPE9568F36-D428-11D2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184:
+ GET /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ GET /phpMyAdmin/changelog: Server may leak inodes via ETags, header found with file /phpMyAdmin/changelog, inode: 92462, size: 40540, mtime: Tue Dec 9 12:24:00 2008. See: CVE-2003-1418:
+ GET /phpMyAdmin/changelog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ GET /test/: Directory indexing found.
+ GET /test/: This might be interesting.
+ GET /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552:
+ GET /icons/: Directory indexing found.
+ GET /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/:
+ GET /phpMyAdmin/: phpMyAdmin directory found.
+ GET /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ GET /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/:
+ GET /wp-config.php#: #wp-config.php# file found. This file contains the credentials.
```



OpenVAS Scan Results:

66 vulnerabilities were found. Some of the highest rated vulnerabilities:

Information	Results <small>(66 of 618)</small>	Hosts <small>(1 of 1)</small>	Ports <small>(17 of 23)</small>	Applications <small>(19 of 19)</small>	Operating Systems <small>(1 of 1)</small>	CVEs <small>(33 of 33)</small>	Closed CVEs <small>(0 of 0)</small>	TLS Certificates <small>(2 of 2)</small>	Error Messages <small>(0 of 0)</small>	User Tags <small>(0)</small>	
											<div><div></div><div><</div><div>1 - 66 of 66</div><div>></div><div></div></div>
Vulnerability ↑↓		 Severity ↓	QoD ↑↓	Host IP ↑↓	Name ↑↓	Location ↑↓	EPSS Score ↑↓ Percentage ↑↓		Created ↑↓		
TWiki XSS and Command Execution Vulnerabilities		 <div><div></div>10.0 (High)</div>	80 %	192.168.56.102		80/tcp	N/A	N/A	Sun, Aug 31, 2025 5:45 PM Coordinated Universal Time		
Operating System (OS) End of Life (EOL) Detection		 <div><div></div>10.0 (High)</div>	80 %	192.168.56.102		general/tcp	N/A	N/A	Sun, Aug 31, 2025 5:41 PM Coordinated Universal Time		
rlogin Passwordless Login		 <div><div></div>10.0 (High)</div>	80 %	192.168.56.102		513/tcp	N/A	N/A	Sun, Aug 31, 2025 5:33 PM Coordinated Universal Time		
Possible Backdoor: Ingreslock		 <div><div></div>10.0 (High)</div>	99 %	192.168.56.102		1524/tcp	N/A	N/A	Sun, Aug 31, 2025 5:50 PM Coordinated Universal Time		
Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities		 <div><div></div>10.0 (High)</div>	99 %	192.168.56.102		8787/tcp	N/A	N/A	Sun, Aug 31, 2025 5:49 PM		

Combined table for vulnerabilities and remediations:

ID	Service/Port	Vulnerability (Tools)	CVSS	Priority	Remediation
002	Rexec/Rlogin (512/513)	Unencrypted login & root access (OpenVAS)	10.0	Critical	Disable rsh/rexec/rlogin, enforce SSH only.
003	Ingreslock (1524/tcp)	Backdoor shell (OpenVAS)	10.0	Critical	Remove/disable ingress service, block port 1524.
005	dRuby (8787/tcp)	Remote Code Execution (OpenVAS)	10.0	Critical	Disable dRuby service, firewall port 8787, update Ruby.



010	Apache/PHP (80/tcp)	- TWiki Command Exec (CVE-2008-5304/5305) - PHP CGI Argument Injection (CVE-2012-1823) - PHP 5.2.4 multiple RCEs (Nikto, OpenVAS)	9.8–1 0	Critical	Upgrade to supported Apache & PHP, remove TWiki or update, disable CGI.
016	OS (general)	Ubuntu 8.04 EOL (OpenVAS)	10.0	Critical	Migrate host OS to supported Ubuntu LTS or other maintained distribution.
001	FTP (21/tcp)	vsftpd 2.3.4 backdoor (Nmap, OpenVAS)	9.8	Critical	Remove vsftpd 2.3.4, upgrade FTP or disable FTP entirely.
006	MySQL (3306/tcp)	Default root/no password (Nmap, OpenVAS)	9.8	Critical	Enforce strong root password, update MySQL to supported version.
009	Apache Tomcat (8009)	Ghostcat AJP RCE (CVE-2020-1938) (OpenVAS)	9.8	Critical	Update Tomcat \geq 9.0.31 / 8.5.51, disable AJP if unused.
004	DistCC (3632/tcp)	Remote Code Execution (OpenVAS)	9.3	Critical	Disable distccd, patch or remove legacy service.



011	Apache (80/tcp)	Outdated Apache 2.2.8 (Nikto, OpenVAS)	9.1	Critical	Upgrade to supported Apache (≥ 2.4), enable security headers.
008	Samba/SMB (445/tcp)	Vulnerable 3.x series (Nmap, OpenVAS)	8.6	High	Patch Samba or disable SMB, block port 445 externally.
007	PostgreSQL (5432/tcp)	Outdated 8.3, multiple CVEs (Nmap, OpenVAS)	7.5	High	Upgrade PostgreSQL to current LTS, restrict network access.
013	Apache (80/tcp)	phpinfo.php exposed (Nikto)	7.5	High	Remove phpinfo.php from production, restrict access.
014	Apache (80/tcp)	HTTP TRACE enabled (Nikto)	5.0	Medium	Disable TRACE method in Apache (TraceEnable off).
015	Apache (80/tcp)	Directory indexing enabled (Nikto)	4.3	Medium	Disable autoindex module or restrict with .htaccess.



Escalation email to the developers:

Subject: Urgent Remediation Required – Critical Vulnerabilities on 192.168.56.102

Team,

Our latest security assessment identified **critical exploitable issues** on host 192.168.56.102.

Highlights include:

- **vsftpd 2.3.4 backdoor (CVE-2011-2523)** – verified by Nmap and OpenVAS; connects to port 6200 providing shell access.
- **Tomcat Ghostcat (CVE-2020-1938)** – PoC: retrieve /WEB-INF/web.xml via AJP on port 8009.
- **MySQL root with no password** – full DB access confirmed.
- **Ubuntu 8.04 EOL** – no vendor support, unpatchable.

These vulnerabilities allow remote attackers to fully compromise the system. Immediate remediation (patch, disable backdoors, migrate OS) is required. Detailed PoC evidence is attached in the scan report.

— Security Team