REPORT ON THE INTERNAL SERVER SCAN

Student Name

Oluwatimilehin Oluwagbemi

Reg. No

2025/GRC/10712

22nd September, 2025

Course Title

GRC 103 – Risk Assessment and Management Techniques

To: IT Management

From: GRC Audit Team

Date: 22/09/2025

Subject: High-Risk Findings on Development Server ‘metasploitable2’

Executive Summary:

The vulnerability assessment conducted on the internal server ‘metasploitable2’ revealed multiple critical security vulnerabilities that pose an immediate and high risk to the organization’s information assets. The system is non-compliant with several key organizational policies based on the CIS Controls. The vulnerability assessment was conducted on Metasploitable2 VM with IP address 192.168.1.6.

The objectives:

- Discover live hosts and identify open ports/services
- Enumerate software versions and identify known vulnerabilities
- Analyze findings and map them to common compliance frameworks
- Assess the risk level of each finding

Key Findings & Risks:

- Critical Risk – Remote System Compromise: the FTP service version on the internal server is vsftd 2.3.4 which is outdated containing a known backdoor vulnerability with the name CVE-2011-2523. This vulnerability is a backdoor which opens a shell on port 6200/tcp, allowing unauthorized access to affected system. This violates the patch management policy (CIS Control 7.1).
- High Risk – Data Interception: Services (Telnet, FTP) transmit credentials in plaintext, violating data protection standards (NIST CSF PR.DS-2) and risking credential theft.
- High Risk – Weak Authentication: Default and weak passwords are in use, increasing the risk of unauthorised access (CIS 5.2)

Recommended Actions:

- Immediately Isolate the server from the network until remediated
- Apply security patches, especially for vsFTPd
- Unnecessary services such as Telnet, Rlogin should be disabled, also enforce strong password policy.

Phase 1: Discovery and Enumeration

Step 1: Network Discovery

To confirm the target machine is alive and to identify the IP address, I powered it on alongside the attacker machine (Kali Linux), then ran the command ‘ifconfig’ to get the IP address which returned an IP address ‘192.168.1.6’.

The next step is to confirm if its alive and on same network with the attacker machine, I ran the command 'ping -c 4 192.168.1.6' it returned a response which specified the machine is alive and ready to be attacked.

Step 2: Port and Service Enumeration with Nmap

Nmap is a network mapper that's used to get live hosts on a network or open ports/services on a system or server. In this step a comprehensive scan was performed to discover live hosts on the internal server using nmap and also identify open ports, services and versions.

The nmap command used is: nmap -sV -sC -O -p- -oA initial_scan 192.168.1.6

The command probe open ports to determine service/version info, enable OS detection, scan all 65,535-port using default nmap scripts for safe discovery.

Phase 2: Vulnerability Identification

Step 3: Analyzing Nmap Output

The nmap command scanned the entire server and returned all open ports on the server. Below is the list of few open ports/services:

- 21 -FTP running tcp is open which poses a risk of backdoor attack, the version of the FTP running on the internal server is 2.3.4 which is outdated with vulnerability CVE-2011-2523. For this service, there's no session bandwidth limit meaning attackers can push as much traffic as they like which can result into the service being overwhelmed. There's need for setting bandwidth to be consumed by the server as it is a file transfer protocol.
- 22-SSH running tcp is open, and it's running an outdated version 4.7 which makes it vulnerable. From the report generated, the host key is exposed with the type used which is DSA and RSA.
- 23-Telnet is open, doesn't really pose a risk due to the existence of SSH, though if not needed should be disabled.
- 25-SMTP running tcp is open, the mail transfer protocol poses a risk of email spoofing, spamming and MiTm attack, running a postfix smtpd running an outdated cipher.
- 53-DNS running tcp is open, dedicated for Domain Service, banded to an outdated version of 9.4.2
- 139-NetBIOS running tcp is open, a samba server, another means an attacker can break into the server, also running an outdated version.
- 80-HTTP running tcp is open, does not really pose a risk, it shows the web server running on port 80

Step 4: Web Application Assessment:

From the nmap scan, port 80 is open which signifies the web server is open which can be scanned for vulnerabilities. To re-confirm if the web server is open, the IP address was copied and pasted in the browser, it loads up applications such as TWiki, PHP, DWA.

Nikto is the tool used to perform the web application assessment with the command: nikto -h http://192.168.1.6 -o nikto_scan.txt.

The result of the scan is briefly explained below:

- From this scan, nikto discovered the server is running on apache 2.2.8 which is an outdated version and the header PHP/5.2.4 is outdated vulnerable to the cgi-bin Remote Code Execution exploit which an attacker can use to remotely gain access by injecting a malicious code also refer to as backdoor to the server.
- The X-Content-Type-Options header is not set which could allow the user agent to render the content of the site in a different fashion to the MIME type.
- Uncommon header 'tcn' found with contents
- Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names.
- Web Server returns a valid response with junk HTTP methods which may cause false positives.
- HTTP TRACE method is active which suggests the host is vulnerable to XST.
- #wp-config.php# file found. This file contains the credentials, this indicates that the web server is a WordPress application.

Step 5: Focused Vulnerability Scanning

For a more focused scanning based on identified services, nuclei is the tool used. The scanning is done in two phases; for web applications and for all services. For the web applications, the command used is: nuclei -u http://192.168.1.6 -o nuclei_web_scan.txt

The result of the web scan is briefly explained below:

- Nuclei reported the vulnerability based on inherent risks, with informational, high, medium and low risks.
- From the result, there are 40 informational inherent risks, 10 high inherent risks, 2 medium inherent risks, and 6 low risks.

The result of the full scan is briefly explained below:

- The vulnerabilities were reported based on inherent risks which are informational, high, medium and low risks.
- From the result, there are 39 informational risks, 10 high risks, 2 medium risks, 6 low risks.

Phase 3

Step 6: Triage and Risk Assessment
Triage and Risk Assessment:

Finding	Affected Service	CVE/Reference	Inherent Risk (L/M/H)	Compliance Violation	Business Impact
Weak Default	SSH, FTP	N/A	H	CIS 5.1, NIST CSF PR.AC-1	Unauthorized access, data theft.
vsFTPd 2.3.4 Backdoor	FTP	CVE-2011-2523	H	CIS 7.1, CIS 4.1 (Patch Mgmt)	Full system compromise
Unencrypted Telnet Service	Telnet	N/A	H	CIS 9.1, CIS 4.1 NIST CSF PR.DS-2	Credential sniffing, espionage
Unauthorized Email Relaying	SMTP	N/A	M	CIS 13.1, CIS 7.1	Email Spoofing, Spamming, MitM attack
Sensitive Data Exposure/Interception/Unauthorized Access	Domain Name System (DNS)	N/A	M	CIS 8.1, CIS 9.2	DDoS Attacks, DNS Spoofing, Data Exfiltration
Unencrypted HTTP Service	HTTP	N/A	M	CIS 4.1, CIS 6.1	Cross-site scripting, SQL injections, DDoS attacks.
Sensitive Network Information Exposure	NetBIOS	N/A	H	CIS 3.5, CIS 4.1	Ransomware, Unauthorized access

Deliverables:

1. Nmap output files: https://drive.google.com/file/d/1iybhZntgWBwkc2m8YPaTQsBFqJo_aUnz/view?usp=sharing https://drive.google.com/file/d/1FIhEpxWNseiHIwDlJdugTKDXJ-UpjufH/view?usp=sharing
2. Screenshot of the Nmap HTML report: https://drive.google.com/file/d/194UmG-N6rsNlUvi3Yda5s-uZ0iz_sSCN/view?usp=sharing

Nmap Scan Report - Scanned at Tue Sep 16 11:27:09 2025

Scan Summary | **192.168.1.6**

Scan Summary

Nmap 7.95 was initiated at Tue Sep 16 11:27:09 2025 with these arguments:
/usr/lib/nmap/nmap --privileged -sV -sC -O -p- -oA initial_scan 192.168.1.6

Verbosity: 0; Debug level 0

Nmap done at Tue Sep 16 11:29:27 2025; 1 IP address (1 host up) scanned in 138.43 seconds

192.168.1.6

Address

- 192.168.1.6 (ipv4)
- 08:00:27:19:D6:8C - PCS Systemtechnik/Oracle VirtualBox virtual NIC (mac)

Ports

The 65505 ports scanned but not shown below are in state: **closed**

- 65505 ports replied with: **reset**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
21	tcp	open	ftp	syn-ack	vsftpd	2.3.4	
	ftp-anon	Anonymous FTP login allowed (FTP code 230)					
	ftp-syst	STAT: FTP server status: Connected to 192.168.1.5 Logged in as ftp TYPE: ASCII No session bandwidth limit Session timeout in seconds is 300 Control connection is plain text Data connections will be plain text vsFTPd 2.3.4 - secure, fast, stable End of status					
22	tcp	open	ssh	syn-ack	OpenSSH	4.7p1 Debian 8ubuntu1	protocol 2.0
	ssh-hostkey	1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA) 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)					
23	tcp	open	telnet	syn-ack	Linux telnetd		
25	tcp	open	smtp	syn-ack	Postfix smtpd		
	sslv2	SSLv2 supported ciphers: SSL2_RC4_128_WITH_MD5 SSL2_RC4_128_EXPORT40_WITH_MD5 SSL2_DES_64_CBC_WITH_MD5 SSL2_DES_192_EDE3_CBC_WITH_MD5 SSL2_RC2_128_CBC_EXPORT40_WITH_MD5 SSL2_RC2_128_CBC_WITH_MD5					
	ssl-cert	Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX Not valid before: 2010-03-17T14:07:45 Not valid after: 2010-04-16T14:07:45					
	ssl-date	2025-09-16T10:29:29+00:00; +2s from scanner time.					
	smtp-commands	metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN					
53	tcp	open	domain	syn-ack	ISC BIND	9.4.2	
	dns-nsid	bind.version: 9.4.2					
80	tcp	open	http	syn-ack	Apache httpd	2.2.8	(Ubuntu) DAV/2
	http-server-header	Apache/2.2.8 (Ubuntu) DAV/2					
	http-title	Metasploitable2 - Linux					
111	tcp	open	rpcbind	syn-ack		2	RPC #100000
	rpcinfo	program version port/proto service 100000 2 111/tcp rpcbind 100000 2 111/udp rpcbind 100003 2,3,4 2049/tcp nfs 100003 2,3,4 2049/udp nfs 100005 1,2,3 39643/udp mountd 100005 1,2,3 50709/tcp mountd 100021 1,3,4 41721/tcp nlockmgr 100021 1,3,4 56057/udp nlockmgr 100024 1 35182/udp status 100024 1 39602/tcp status					
139	tcp	open	netbios-ssn	syn-ack	Samba smbd	3.X - 4.X	workgroup: WORKGROUP
445	tcp	open	netbios-ssn	syn-ack	Samba smbd	3.0.20-Debian	workgroup: WORKGROUP
512	tcp	open	exec	syn-ack	netkit-rsh rexecd		
513	tcp	open	login	syn-ack			
514	tcp	open	tcpwrapped	syn-ack			
1099	tcp	open	java-rmi	syn-ack	GNU Classpath grmiregistry		
1524	tcp	open	bindshell	syn-ack	Metasploitable root shell		
2049	tcp	open	nfs	syn-ack		2-4	RPC #100003
2121	tcp	open	ftp	syn-ack	ProFTPD	1.3.1	
3306	tcp	open	mysql	syn-ack	MySQL	5.0.51a-3ubuntu5	
	mysql-info	Protocol: 10 Version: 5.0.51a-3ubuntu5 Thread ID: 8 Capabilities flags: 43564 Some Capabilities: Support41Auth, SwitchToSSLAfterHandshake, ConnectWithDatabase, Speaks41ProtocolNew, LongColumnFlag, SupportsTransactions, SupportsCompression Status: Autocommit Salt: R[Tq_e`1pd%^BL:z{{va						

Go to top
Toggle Closed Ports
Toggle Filtered Ports

3632	tcp	open	distccd	syn-ack	distccd	v1	(GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4)
5432	tcp	open	postgresql	syn-ack	PostgreSQL DB	8.3.0 - 8.3.7	
	ssl-cert	Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX Not valid before: 2010-03-17T14:07:45 Not valid after: 2010-04-16T14:07:45					
	ssl-date	2025-09-16T10:29:29+00:00; +2s from scanner time.					
5900	tcp	open	vnc	syn-ack	VNC		protocol 3.3
	vnc-info	Protocol version: 3.3 Security types: VNC Authentication (2)					
6000	tcp	open	X11	syn-ack			access denied
6667	tcp	open	irc	syn-ack	UnrealIRCd		
6697	tcp	open	irc	syn-ack	UnrealIRCd		
	irc-info	users: 2 servers: 1 lusers: 2 lservers: 0 server: irc.Metasploitable.LAN version: Unreal3.2.8.1. irc.Metasploitable.LAN uptime: 0 days, 0:09:16 source ident: nmap source host: 7C418B9C.78DED367.FFFA6D49.IP error: Closing Link: ykxjrwfgr[192.168.1.5] (Quit: ykxjrwfgr)					
8009	tcp	open	ajp13	syn-ack	Apache Jserv		Protocol v1.3
	ajp-methods	Failed to get a valid response for the OPTION request					
8180	tcp	open	http	syn-ack	Apache Tomcat/Coyote JSP engine	1.1	
	http-title	Apache Tomcat/5.5					
	http-server-header	Apache-Coyote/1.1					
	http-favicon	Apache Tomcat					
8787	tcp	open	drb	syn-ack	Ruby DRb RMI		Ruby 1.8; path /usr/lib/ruby/1.8/drb
39602	tcp	open	status	syn-ack		1	RPC #100024
41721	tcp	open	nlockmgr	syn-ack		1-4	RPC #100021
44358	tcp	open	java-rmi	syn-ack	GNU Classpath grmiregistry		
50709	tcp	open	mountd	syn-ack		1-3	RPC #100005

Remote Operating System Detection

- Used port: **21/tcp** (**open**)
- Used port: **1/tcp** (**closed**)
- Used port: **34486/udp** (**closed**)
- OS match: **Linux 2.6.9 - 2.6.33** (**100%**)

Host Script Output

Go to top
Toggle Closed Ports
Toggle Filtered Ports

		error: Closing Link: ykxjrwfgr[192.168.1.5] (Quit: ykxjrwfgr)					
8009	tcp	open	ajp13	syn-ack	Apache Jserv		Protocol v1.3
	ajp-methods	Failed to get a valid response for the OPTION request					
8180	tcp	open	http	syn-ack	Apache Tomcat/Coyote JSP engine	1.1	
	http-title	Apache Tomcat/5.5					
	http-server-header	Apache-Coyote/1.1					
	http-favicon	Apache Tomcat					
8787	tcp	open	drb	syn-ack	Ruby DRb RMI		Ruby 1.8; path /usr/lib/ruby/1.8/drb
39602	tcp	open	status	syn-ack		1	RPC #100024
41721	tcp	open	nlockmgr	syn-ack		1-4	RPC #100021
44358	tcp	open	java-rmi	syn-ack	GNU Classpath grmiregistry		
50709	tcp	open	mountd	syn-ack		1-3	RPC #100005

Remote Operating System Detection

- Used port: **21/tcp** (**open**)
- Used port: **1/tcp** (**closed**)
- Used port: **34486/udp** (**closed**)
- OS match: **Linux 2.6.9 - 2.6.33** (**100%**)

Host Script Output

Script Name	Output
nbstat	NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
smb-os-discovery	OS: Unix (Samba 3.0.20-Debian) Computer name: metasploitable NetBIOS computer name: Domain name: localdomain FQDN: metasploitable.localdomain System time: 2025-09-16T06:29:20-04:00
clock-skew	mean: 1h00m01s, deviation: 2h00m00s, median: 1s
smb-security-mode	account_used: guest authentication_level: user challenge_response: supported message_signing: disabled (dangerous, but default)
smb2-time	Protocol negotiation failed (SMB2)

Go to top
Toggle Closed Ports
Toggle Filtered Ports

Misc Metrics (click to expand)

3. Nikto and Nuclei scan results: https://drive.google.com/file/d/1IUKOmCB1ySmQwhMXhVCY1PPUDkrrJNkJ/view?usp=sharing https://drive.google.com/file/d/1YtoeUNy1XM3NVfKOnt9Vfy5Kxg8q86aD/view?usp=sharing https://drive.google.com/file/d/1_NOz-AqmAQTh3m6EMhnZxCQi70SqLr9-/view?usp=sharing