High-Risk Findings on Development Server *Metasploitable'*

To: IT Management
From: GRC Audit Team
Date: 9/22/20205

Executive Summary

As part of our internal security assurance program, a vulnerability assessment was conducted on the development server Metasploitable. The review identified multiple critical and high-risk vulnerabilities that create significant exposure to system compromise, data theft, and operational disruption. The server is non-compliant with organizational security baselines and recognized standards (CIS Controls, NIST CSF).

Failure to address these findings could result in regulatory non-compliance, reputational damage, and financial loss if exploited.

Key Risks Identified

- **Critical Risk:** Remote System Compromise
  The FTP service (vsFTPd 2.3.4) contains a known backdoor (CVE-2011-2523), allowing attackers to take full control of the system without authentication.
  Business Impact*:* Full compromise of development systems, potential entry point into wider network.

- **High Risk:** Data Interception
  Services including Telnet and FTP transmit sensitive credentials in plaintext.
  Business Impact*:* impact will include theft of login details, unauthorized access to systems and confidential data.

- **High Risk:** Weak Authentication Practices
  Presence of default and weak passwords across multiple services.
  Business Impact*:* Increased risk of unauthorized access and insider threat.

- **High Risk:** Outdated and Unpatched Services
  Core services (Apache, Samba, MySQL) are running on outdated versions with publicly known exploits.
  Business Impact*:* Exploitation could lead to denial-of-service, privilege escalation, or data breach.

3. Recommended Actions

1. **Isolate the Server**: Remove from network until remediated.
2. **Apply Patches & Updates**: Upgrade or replace vulnerable services (particularly vsFTPd, Apache, Samba).
3. **System Hardening**: Disable unnecessary services (Telnet, Rlogin); enforce strong password policies; enable encrypted protocols.
4. **Strengthen Deployment Processes**: Ensure all systems undergo security baseline checks and patch verification prior to going live.

4. Next Steps

The GRC Audit Team recommends that remediation actions be initiated within 7 days due to the critical severity of the findings. A follow-up verification will be conducted to confirm closure of identified risks.

Appendix A: Tools Used and Output

Nmap

- Purpose: Network discovery and service/version enumeration.
- Usage: Full TCP/UDP port scans, service detection (-sV), NSE vulnerability scripts, and targeted scans to validate open services.
- Output: Identified running services and versions (SSH, HTTP, FTP, PostgreSQL, MySQL, SMB, VNC, AJP, distccd, etc.), which informed further template-based checks.

Nmap Scan Report - Scanned at Sun Sep 21 20:40:27 2025

Scan Summary | **192.168.15.133**

Scan Summary

Nmap 7.95 was initiated at Sun Sep 21 20:40:27 2025 with these arguments:
/usr/lib/nmap/nmap --privileged -sV -sC -O -p- -oA initial_scan 192.168.15.133

Verbosity: 0; Debug level 0

Nmap done at Sun Sep 21 20:42:51 2025; 1 IP address (1 host up) scanned in 144.28 seconds

192.168.15.133

Address

- 192.168.15.133 (ipv4)
- 00:0C:29:F3:AC:04 - VMware (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 192.168.15.132 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		
	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					
	smtp-commands	metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN					
	sslv2	SSLv2 supported ciphers: SSL2_RC2_128_CBC_WITH_MD5 SSL2_DES_192_EDE3_CBC_WITH_MD5 SSL2_RC4_128_EXPORT40_WITH_MD5 SSL2_RC4_128_WITH_MD5 SSL2_RC2_128_CBC_EXPORT40_WITH_MD5 SSL2_DES_64_CBC_WITH_MD5					
	ssl-date	2025-09-21T18:42:51+00:00; -1h00m00s from scanner time.					

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-title	Metasploitable2 - Linux					
	http-server-header	Apache/2.2.8 (Ubuntu) DAV/2					
111	tcp	open	rpcbind	syn-ack		2	RPC #100000
	rpcinfo	program version port/proto service 100003 2,3,4 2049/tcp nfs 100005 1,2,3 57812/tcp mountd 100005 1,2,3 59390/udp mountd 100021 1,3,4 33561/udp nlockmgr 100021 1,3,4 37270/tcp nlockmgr					
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	OpenBSD or Solaris rlogind		
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: 9					

	mysql-info	Protocol: 10 Version: 5.0.51a-3ubuntu5 Thread ID: 9 Capabilities flags: 43564 Some Capabilities: Speaks41ProtocolNew, SupportsCompression, LongColumnFlag, SupportsTransactions, ConnectWithDatabase, SwitchToSSLAfterHandshake, Support41Auth Status: Autocommit Salt: 7ws]TpXF6y"99SuqZP_l					
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-date	2025-09-21T18:42:51+00:00; -1h00m00s from scanner time.					
	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					
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		
	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, 0:17:05 source ident: nmap source host: E5795288.B4DCF864.FFFA6D49.IP error: Closing Link: ltzmiyjmb[192.168.15.132] (Quit: ltzmiyjmb)					
6697	tcp	open	irc	syn-ack	UnrealIRCd		

	http-title	Apache Tomcat/5.5					
	http-server-header	Apache-Coyote/1.1					
8787	tcp	open	drb	syn-ack	Ruby DRb RMI		Ruby 1.8; path /usr/lib/ruby/1.8/drb
37270	tcp	open	nlockmgr	syn-ack		1-4	RPC #100021
52304	tcp	open	status	syn-ack		1	RPC #100024
52988	tcp	open	java-rmi	syn-ack	GNU Classpath grmiregistry		
57812	tcp	open	mountd	syn-ack		1-3	RPC #100005

emote Operating System Detection

- Used port: **21/tcp** (**open**)
- Used port: **1/tcp** (**closed**)
- Used port: **39219/udp** (**closed**)
- OS match: **Linux 2.6.9 - 2.6.33** (**100%**)

ost Script Output

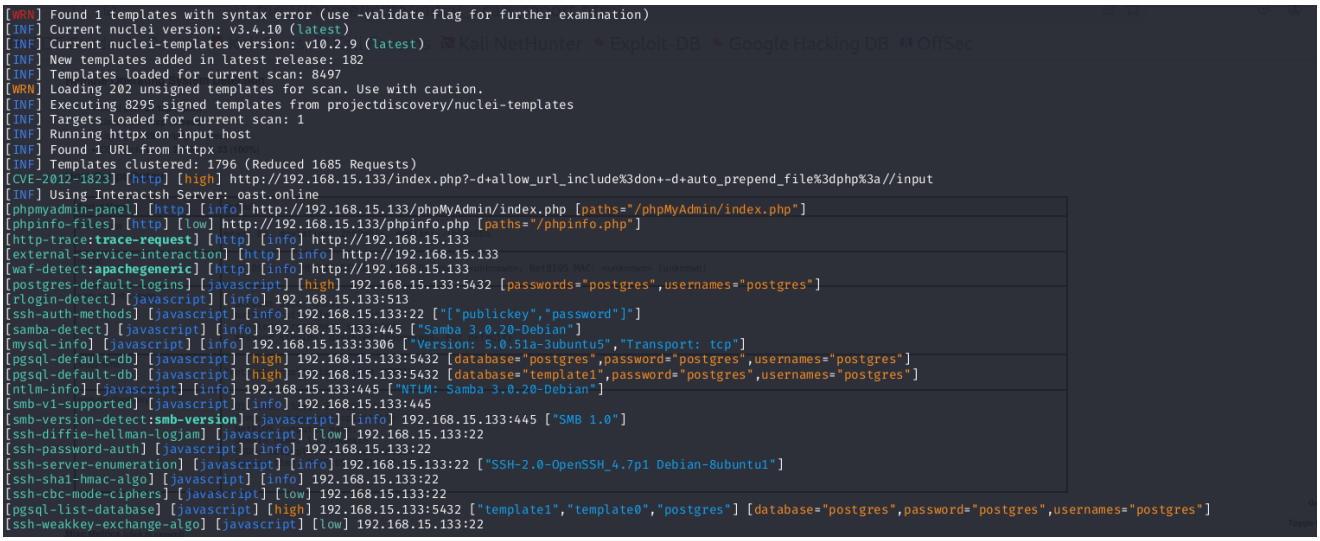
Script Name	Output
clock-skew	mean: 0s, deviation: 2h00m01s, median: -1h00m00s
nbstat	NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
smb-security-mode	account_used: guest authentication_level: user challenge_response: supported message_signing: disabled (dangerous, but default)
smb2-time	Protocol negotiation failed (SMB2)

Nikto

- Purpose: Web application and server misconfiguration scanning.
- Usage: Scanned HTTP service for common misconfigurations, script exposures, directory listings, and test files.
- Output: Findings such as phpinfo.php exposure, directory indexing (/doc/, /test/), missing security headers, and phpMyAdmin exposure — corroborating Nuclei/Nmap results.

Nuclei

- Purpose: Automated template-based vulnerability detection (CVE checks, misconfigurations).
- Usage: Scanned with nuclei using the nuclei-templates repository (v10.2.9), focused CVE and http/tcp templates, and validated matches; debug output used for evidence.
- Output: High/critical CVE detections (e.g., CVE-2020-1938, CVE-2012-1823, CVE-2011-2523) and numerous service-specific findings used in the risk table.



Appendix B – Detailed Risk Assessment Table

Assessment Source: Nuclei + Nikto Scans of Development Server ‘Metasploitable’

Finding	Affected Service	CVE / Reference	Severity	Compliance Violation	Business Impact
vsFTPd 2.3.4 Backdoor	FTP	CVE-2011-2523	Critical	CIS 7.1 (Patch Mgmt)	Full system compromise; remote attacker gains shell access.
Weak / Default Credentials	SSH, FTP, MySQL	N/A	High	CIS 5.2, NIST CSF PR.AC-1	Unauthorized access, insider threat, data theft.
Unencrypted Telnet Service	Telnet	N/A	High	NIST CSF PR.DS-2	Credential sniffing, espionage, MITM attacks.
Outdated Apache (2.2.x)	HTTP	Multiple CVEs (e.g., CVE-2011-3192)	High	CIS 7.1	DoS, remote code execution, website defacement.
Outdated Samba (3.x)	SMB	CVE-2007-2447, others	High	CIS 7.1	Remote code execution, lateral movement within network.
Open MySQL without Encryption	MySQL	N/A	High	NIST CSF PR.DS-2	Credential theft, unauthorized database access.
PHP CGI Vulnerabilities	Web (Nikto)	Multiple CVEs	Medium	CIS 7.1	Information disclosure, RCE on poorly configured servers.
Directory Listing Enabled	Apache	N/A	Medium	CIS 9.2 (Restrict Info Exposure)	Attackers can discover sensitive files, scripts.
Self-Signed / Expired SSL Certificate	HTTPS	N/A	Medium	NIST CSF PR.DS-2	User impersonation, SSL stripping attacks.
Misconfigured HTTP Headers	Apache	Nikto findings (X-Frame-Options, X-XSS-Protection missing)	Low	OWASP ASVS 14.4	Increases exposure to XSS/Clickjacking.
Multiple Open Ports (65535 scanned)	Various	N/A	Low	CIS 9.2	Expands attack surface; reconnaissance exposure.

Appendix C – Severity Classification

- **Critical:** Immediate remediation required (exploit known in the wild, full compromise possible).
- **High:** High likelihood of exploitation; risk to confidentiality, integrity, availability.
- **Medium:** Exploitable but limited impact; mitigations may reduce urgency.
- **Low:** Best practice issues; low business impact but should be addressed.

Appendix D – Mapping to Security Frameworks

- **CIS Controls:** 5.2 (Authentication), 7.1 (Patch Mgmt), 9.2 (Info Exposure).
- **NIST CSF:** PR.AC-1 (Access Control), PR.DS-2 (Data Protection), PR.IP-1 (Baseline Configs).
- **OWASP ASVS:** 14.4 (HTTP Headers).