

High-Risk Findings on Development Server *Metasploitable'*

To: IT Management

From: GRC Audit Team

Date: 9/22/2020

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- **High Risk:** Outdated and Unpatched Services
Core services (Apache, Samba, MySQL) are running on outdated versions with publicly known exploits.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=0C05A/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, 8BITIME, 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 | <pre> 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 </pre> | | | | | |
| 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 | <pre> Protocol: 10 Version: 5.0.51a-3ubuntu5 Thread ID: 9 </pre> | | | | | |

| | | | | | | | |
|------|------------|---|------------|---------|---------------|---------------|-------------------------------------|
| | mysql-info | <pre> 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_1 </pre> | | | | | |
| 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 | <pre> Subject: commonName=ubuntu804-base.localdomain/organizationName=OC0SA/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 </pre> | | | | | |
| 5900 | tcp | open | vnc | syn-ack | VNC | | protocol 3.3 |
| | vnc-info | <pre> Protocol version: 3.3 Security types: VNC Authentication (2) </pre> | | | | | |
| 6000 | tcp | open | X11 | syn-ack | | | access denied |
| 6667 | tcp | open | irc | syn-ack | UnrealIRCd | | |
| | irc-info | <pre> 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: ltzmijymb[192.168.15.132] (Quit: ltzmijymb) </pre> | | | | | |
| 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/drbb |
| 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.

```

[ic012@ic012 ~]$ nikto -h http://192.168.15.133 -o nikto_scan.txt
- Nikto v2.5.0

+ Target IP: 192.168.15.133
+ Target Hostname: 192.168.15.133
+ Target Port: 80
+ Start Time: 2025-09-21 20:59:23 (GMT1)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: 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/
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /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
+ 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.
+ /: 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. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?PHPBB85F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?PHPPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?PHPPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?PHPPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/Changelog: Server may leak inodes via ETags, header found with file /phpMyAdmin/Changelog, inode: 92462, size: 40540, mtime: Tue Dec 9 18:24:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /phpMyAdmin/Changelog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552
+ /icons/: Directory indexing found.

```

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.

```
[WRN] Found 1 templates with syntax error (use -validate flag for further examination)
[INF] Current nuclei version: v3.4.10 (latest)
[INF] Current nuclei-templates version: v10.2.9 (latest)
[INF] New templates added in latest release: 182
[INF] Templates loaded for current scan: 8497
[WRN] Loading 202 unsigned templates for scan. Use with caution.
[INF] Executing 8295 signed templates from projectdiscovery/nuclei-templates
[INF] Targets loaded for current scan: 1
[INF] Running httpx on input host
[INF] Found 1 URL from httpx
[INF] Templates clustered: 1796 (Reduced 1685 Requests)
[WE-2012-1823] [http] [high] http://192.168.15.133/index.php?-d+allow_url_include%3don+-d+auto_prepend_file%3dphp%3a//input
[INF] Using Interactsh Server: oast.online
[phpmyadmin-panel] [http] [info] http://192.168.15.133/phpMyAdmin/index.php [paths="/phpMyAdmin/index.php"]
[phpinfo-files] [http] [low] http://192.168.15.133/phpinfo.php [paths="/phpinfo.php"]
[http-trace-request] [http] [info] http://192.168.15.133
[external-service-interaction] [http] [info] http://192.168.15.133
[waf-detect-apachegeneric] [http] [info] http://192.168.15.133
[postgres-default-logins] [javascript] [high] 192.168.15.133:5432 [passwords="postgres", usernames="postgres"]
[rlogin-detect] [javascript] [info] 192.168.15.133:513
[ssh-auth-methods] [javascript] [info] 192.168.15.133:22 [{"publickey", "password"}]
[samba-detect] [javascript] [info] 192.168.15.133:445 [{"Samba 3.0.20-Debian"}]
[mysql-info] [javascript] [info] 192.168.15.133:3306 [{"Version: 5.0.51a-3ubuntu5", "Transport: tcp"}]
[pgsql-default-db] [javascript] [high] 192.168.15.133:5432 [database="postgres", password="postgres", usernames="postgres"]
[pgsql-default-db] [javascript] [high] 192.168.15.133:5432 [database="template1", password="postgres", usernames="postgres"]
[ntlm-info] [javascript] [info] 192.168.15.133:445 [{"NTLM: Samba 3.0.20-Debian"}]
[smb-v1-supported] [javascript] [info] 192.168.15.133:445
[smb-version-detect] [javascript] [info] 192.168.15.133:445 [{"SMB 1.0"}]
[ssh-diffie-hellman-logjam] [javascript] [low] 192.168.15.133:22
[ssh-password-auth] [javascript] [info] 192.168.15.133:22
[ssh-server-enumeration] [javascript] [info] 192.168.15.133:22 [{"SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1"}]
[ssh-sha1-mac-algo] [javascript] [info] 192.168.15.133:22
[ssh-cbc-mode-ciphers] [javascript] [low] 192.168.15.133:22
[pgsql-list-database] [javascript] [high] 192.168.15.133:5432 [{"template1", "template0", "postgres"}] [database="postgres", password="postgres", usernames="postgres"]
[ssh-weakkey-exchange-algo] [javascript] [low] 192.168.15.133:22

[pgsql-list-password-hashes] [javascript] [high] 192.168.15.133:5432 [{"postgres : md53175bce1d3201d16594cebf9d7eb3f9d"}] [database="postgres", password="postgres", usernames="postgres"]
[ssh-weak-algo-supported] [javascript] [medium] 192.168.15.133:22
[pgsql-list-users] [javascript] [high] 192.168.15.133:5432 [{"postgres"}] [database="postgres", password="postgres", usernames="postgres"]
[ssh-weak-mac-algo] [javascript] [low] 192.168.15.133:22
[pgsql-file-read] [javascript] [high] 192.168.15.133:5432 [{"global", "pg_clog", "pg_subtrans", "base", "pg_tblspc", "PG_VERSION", "server.key", "postmaster.opts", "server.crt", "pg_xlog", "root.crt", "pg_twophase", "postmaster.pid", "pg_multixact"}] [database="postgres", password="postgres", usernames="postgres"]
[pgsql-version-detect] [javascript] [high] 192.168.15.133:5432 [{"PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)"}] [database="postgres", password="postgres", usernames="postgres"]
[esmtplib-detect] [tcp] [info] 192.168.15.133:25
[CVE-2011-2523] [tcp] [critical] 192.168.15.133:6200
[CVE-2004-2687] [tcp] [high] 192.168.15.133:3632
[ftp-detect] [tcp] [info] 192.168.15.133:21
[nfs-v3-exposed] [tcp] [info] 192.168.15.133:2049
[vsftpd-detect-version] [tcp] [info] 192.168.15.133:21 [{"2.3.4"}]
[smtp-detect] [tcp] [info] 192.168.15.133:25
[openssh-detect] [tcp] [info] 192.168.15.133:22 [{"SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1"}]
[vnc-service-detect] [tcp] [info] 192.168.15.133:5900 [{"RFB 003.003"}]
[smtp-commands-enumerate] [tcp] [info] 192.168.15.133:25 [{"SIZE 10240000", "VRFY", "ETRN", "STARTTLS", "ENHANCEDSTATUSCODES", "8BITMIME", "DSN", "PIPELINING"}]
[tech-detect-php] [http] [info] http://192.168.15.133
[ajp-protocol-detect] [javascript] [info] 192.168.15.133:8009 [{"AJP Detected"}]
[CVE-2020-1938] [tcp] [critical] 192.168.15.133:8009
[ftp-anonymous-login] [tcp] [medium] 192.168.15.133:21
[apache-detect] [http] [info] http://192.168.15.133 [{"Apache/2.2.8 (Ubuntu) DAV/2"}]
[php-detect] [http] [info] http://192.168.15.133 [{"5.2.4"}]
[http-missing-security-headers:clear-site-data] [http] [info] http://192.168.15.133
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://192.168.15.133
[http-missing-security-headers:strict-transport-security] [http] [info] http://192.168.15.133
[http-missing-security-headers:referrer-policy] [http] [info] http://192.168.15.133
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://192.168.15.133
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://192.168.15.133
[http-missing-security-headers:content-security-policy] [http] [info] http://192.168.15.133
[http-missing-security-headers:permissions-policy] [http] [info] http://192.168.15.133
[http-missing-security-headers:x-frame-options] [http] [info] http://192.168.15.133
[http-missing-security-headers:x-content-type-options] [http] [info] http://192.168.15.133
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://192.168.15.133
```

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).