

**PROJECT:**

Web Application and Penetration Testing

**Task-3**: Exploitation of Open Ports.

**Team – 2.4:**

**GOKUL R** – 20MIS0332 – VIT Vellore

**KAMALESH D** – 20MIS0342 – VIT Vellore

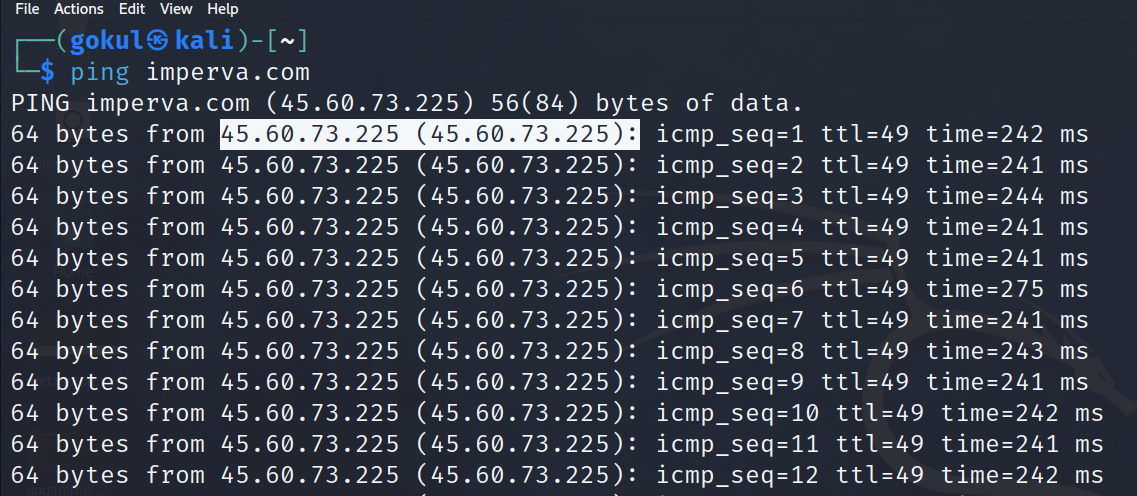
**PRASANNA KUMAR N** – 20BCE2121 – VIT Vellore

**KRISHNA RAJESH** – 20BCY10080 – VIT Bhopal

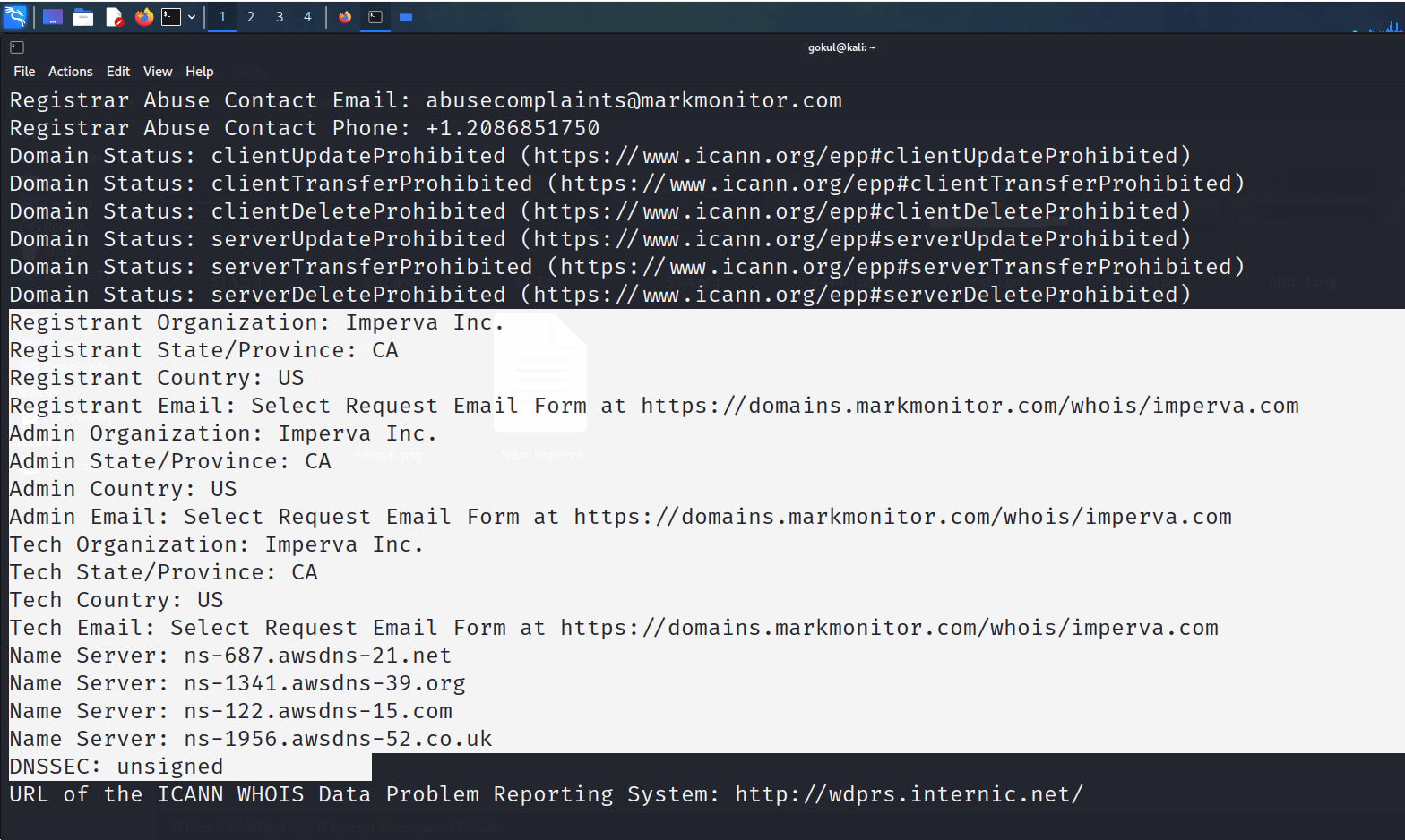
**Website:**<https://www.imperva.com/>

1. Foot printing and Reconnaissance

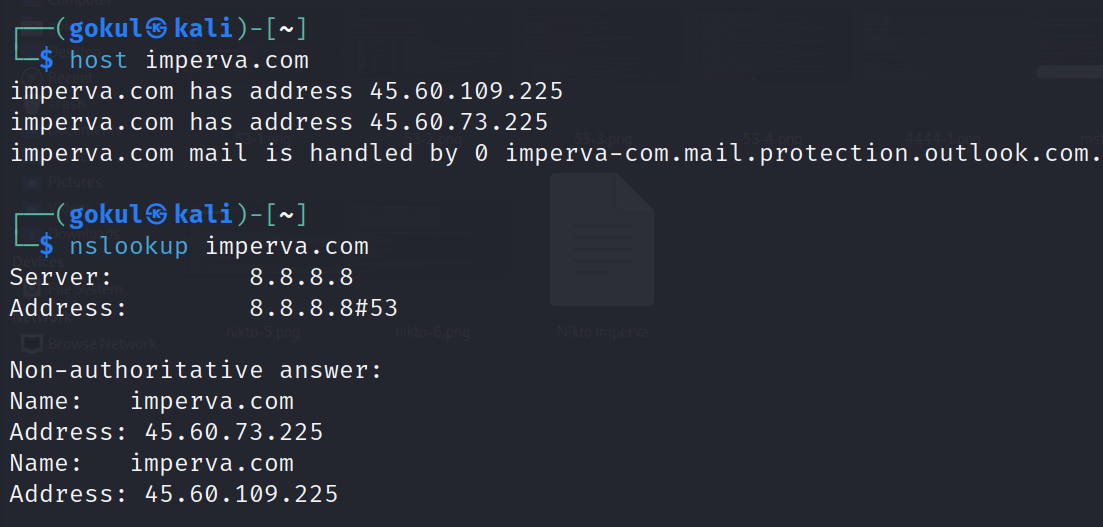
Step 1: Finding IP address:



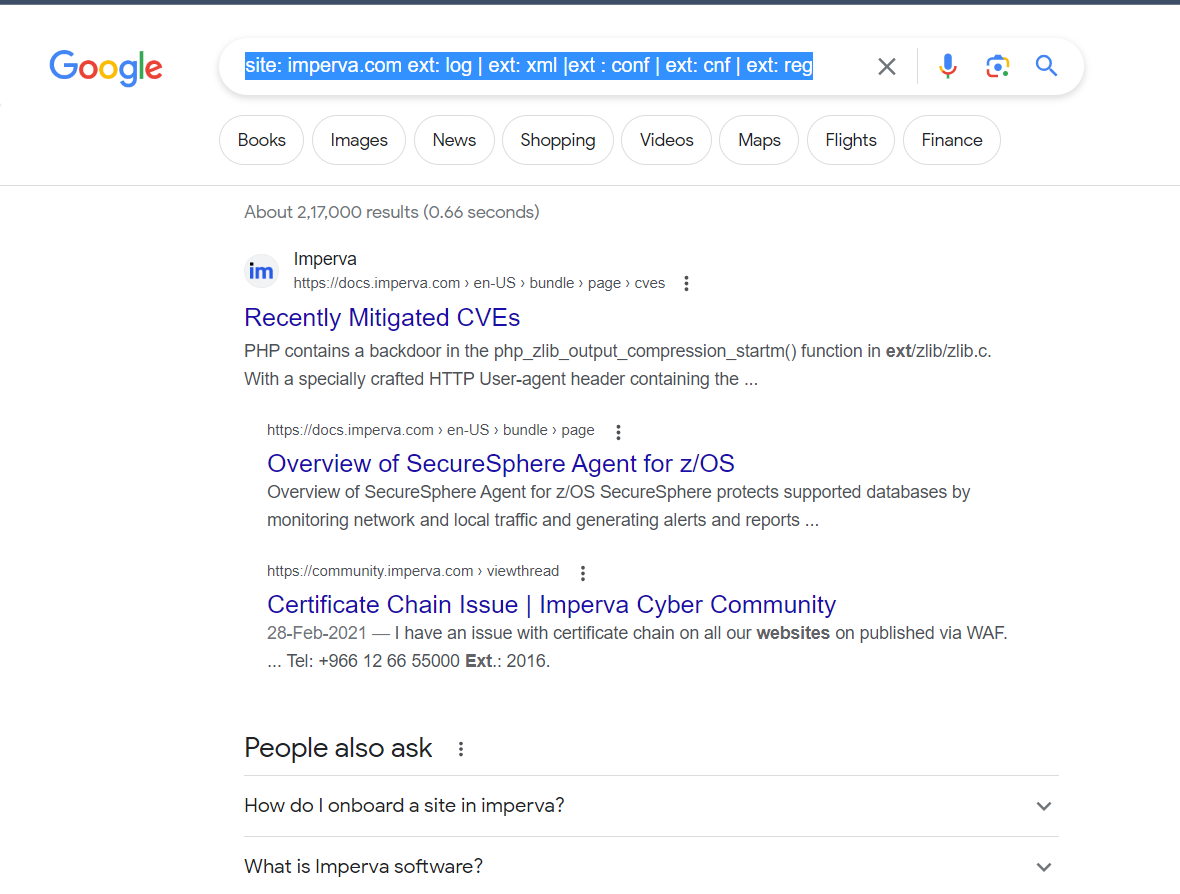
Step 2: Finding all known information from Whois:



Step 3: Finding server and its address:

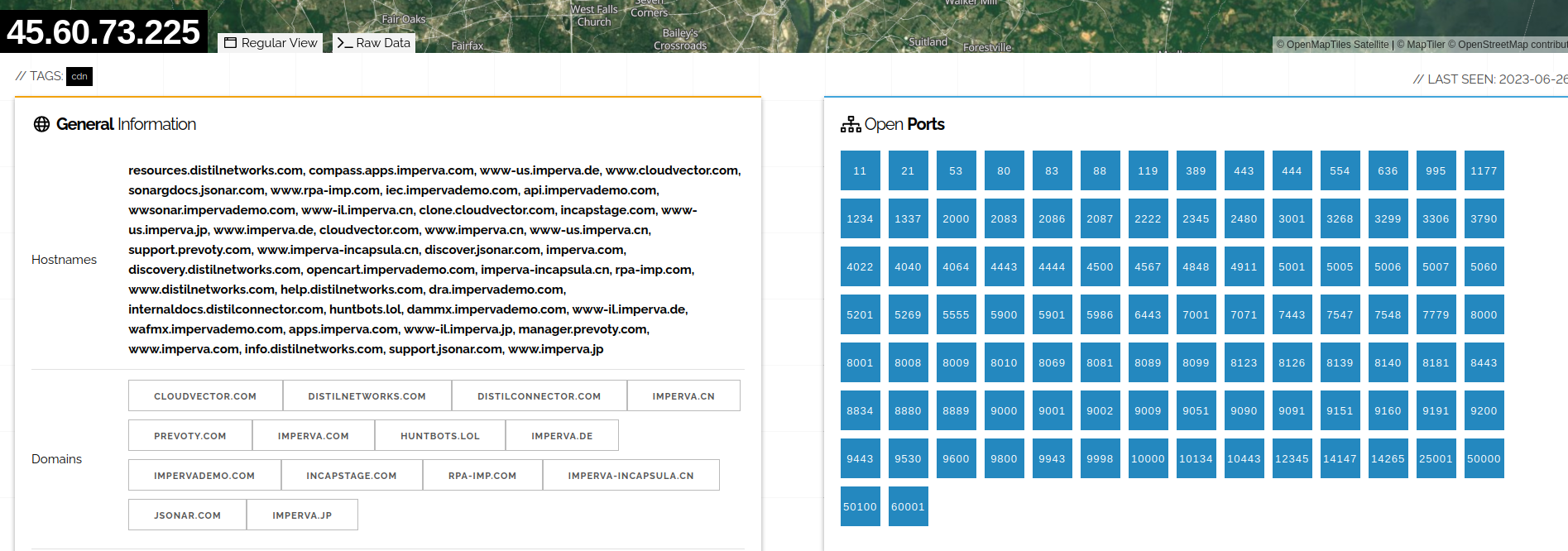


Step 5: Google advance search



2. Open Ports

Step 1: find the open ports



Step 2: Some open ports details

**Port – 21/tcp**

**Protocol name:** File Transfer Protocol (FTP)

**Used for:** Transferring files between a client and a server over a network.

**Vulnerabilities:**

* Anonymous Access: Allowing unauthorized users to access and download files without authentication.
* Weak Authentication: Allowing weak or easily guessable passwords, making it susceptible to brute-force attacks.
* FTP Bounce Attack: Using the FTP server to perform port scanning or connect to other hosts indirectly.
* Command Injection: Exploiting vulnerabilities in FTP client software to execute arbitrary commands on the server.
* FTP Brute-Force Attack: Attempting various username and password combinations to gain unauthorized access.

**Reason to use this port**: Default port for FTP service, widely used for file transfer operations.

**How to exploit FTP vulnerabilities:**

* Anonymous Access: Connect to the FTP server without providing any credentials to access files or directories.
* Weak Authentication: Perform brute-force attacks to guess weak passwords and gain unauthorized access.
* FTP Bounce Attack: Utilize the FTP server to scan other hosts or perform indirect connections to bypass firewalls.
* Command Injection: Exploit vulnerabilities in FTP client software to execute arbitrary commands on the server.
* FTP Brute-Force Attack: Use automated tools to attempt multiple username and password combinations.

**Exploitation script:**

<https://github.com/danielmiessler/SecLists/blob/master/Passwords/Default-Credentials/ftp-betterdefaultpasslist.txt>

**Port – 53/tcp**

**Protocol name:** Domain Service (DNS)   
**Used for:** Translating domain names into IP addresses and vice versa, DNS resolution.

**Vulnerabilities:**

* DNS Zone Transfer: Misconfigured DNS servers allowing unauthorized zone transfers.
* DNS Cache Poisoning: Injecting malicious DNS data into the server's cache.
* DNS Amplification: Misconfigured DNS servers used in DDoS attacks.
* DNS Server Misconfiguration: Open recursive resolvers, open zone transfers, incorrect access control.
* DNS Spoofing: Manipulating DNS responses to redirect users to malicious servers.

**Reason to use this port:** Default port for DNS service, necessary for proper functioning of domain name resolution.

**How to exploit DNS vulnerabilities:**

* DNS Zone Transfer: Exploit misconfigured zone transfer settings to gain unauthorized access to DNS data.
* DNS Cache Poisoning: Inject malicious DNS data into the server's cache to redirect traffic.
* DNS Amplification: Exploit misconfigured DNS servers to generate DDoS traffic.
* DNS Server Misconfiguration: Exploit open recursive resolvers, open zone transfers, or weak access controls.
* DNS Spoofing: Manipulate DNS responses through cache poisoning or man-in-the-middle attacks.

**Exploitation script:** No specific script provided. Exploitation techniques depend on the specific vulnerability being targeted.

**Port – 4444/tcp**

**Protocol name:** krb524,nv-video,eggdrop

**Used for:** default listener port for Metasploit. Also, to eavesdrop on traffic and communications, for its communications, and to receive data from the compromised computer.

**Vulnerabilities:** Trojan, backdoor, rootkits.

**Reason to use this port:** Prior to native Kerberos v5 support, the krb524 service converted Kerberos v5 tickets to v4 for AFS tokens. OpenAFS added support for direct use of v5 tickets, improving security and avoiding blocked ports. Transition away from krb524 service is advised, and alternative authentication methods are available within OpenAFS 1.4.x servers. [Note: That v4 port is used to spread a worm that attacked Microsoft Windows in 2003]

**How to exploit krb524:** Trojan and backdoor software

**Exploitation script:** <https://www.exploit-db.com/exploits/39152>

**Port – 8010/tcp**

**Protocol name:** XMPP

**Vulnerability:** brute force

**Reason to use this port**: The 8010 port lets a dfsclient (located on the same machine as the particular block) access that file directly after making the request on the 8010 ports of DataNode to release any holds on the block. Additionally, this port is also used for DataNodes to communicate with each other when needed.

**How to exploit:** Aircrack-ng, John the Ripper,

**Exploitation script:**

<https://github.com/nmap/nmap/blob/master/scripts/xmpp-brute.nse>

**Port Number: 88/tcp**

**Protocol:** Kerberos

**Purpose:** Kerberos authentication offers several advantages over other access control methods, such as mutual authentication, which allows both the client and the server to verify each other's identity. It also reduces the risk of password theft, as passwords are never sent over the network in plain text.

**Purpose of *88/tcp:***

It’s used only for outbound connections from your storage system.

TCP Port 88 may use a defined protocol to communicate depending on the application. A protocol is a set of formalized rules that explain how data is communicated over a network.

**Vulnerabilities:**

* Trojan & BackDoor-AXC - Pwsteal.likmet.a,   
  BroadWave Streaming Audio Server also uses this port
* Threat - PWSteal.Likmet

**Exploitation:**<https://www.exploit-db.com/exploits/39152>

**Port Number**: 995/tcp

**Protocol:** POP3S protocol

**Purpose:** Post Office Protocol 3, or POP3, is the most commonly used protocol for receiving email over the internet. This standard protocol, which most email servers and their clients support, is used to receive emails from a remote server and send to a local client.

**Vulnerabilities:**

* Email cannot be accessed from another computer (unless configured to do so).
* It can be difficult for a user to export a local mail folder.
* Entire folders of emails can be corrupted, possibly causing you to lose an entire mailbox at once.
* Email attachments can contain viruses that can cause great harm to your PC if they are opened and sometimes virus scanners are unable to detect them.

Incoming POP3 mail over SSL   
used by Gmail – Cyclops Blink Botnet uses these ports. The malware has targeted governments, WatchGuard firewalls, ASUS routers, etc., it is active as of March 2022, and it is believed to be operated by the Sandworm threat group linked to Russian intelligence. Cyclops Blink botnet malware uses the following TCP ports: 636, 989, 990, 992, 994, 995, 3269, 8443

**Exploitation:**<https://github.com/carlospolop/hacktricks/blob/master/network-services-pentesting/pentesting-pop.md>

Step 3: Exploitation steps for some ports

**Exploiting Port 21:**

Port 21 runs file transfer protocol service.

**Step 1:** Finding whether the port is open or not.

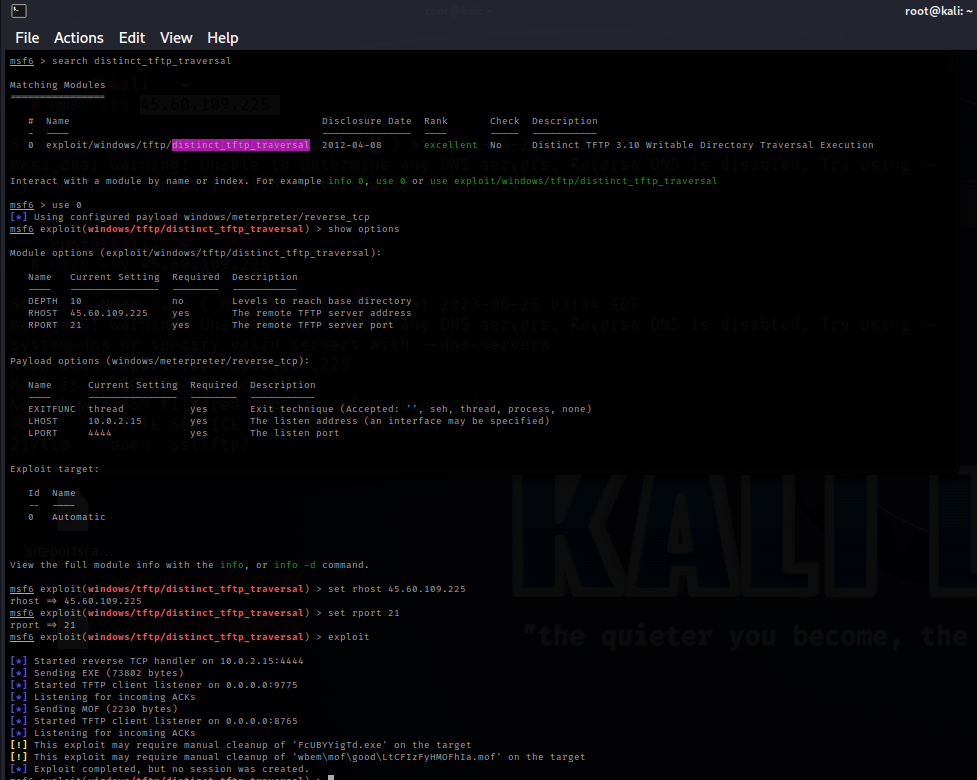
**Step 2:** Login to the ftp of the website using the command “**ftp 45.60.73.225**”

**Step** 3: finding the version of ftp protocol the website is using, using the command “**nmap -sV 45.60.73.225 -p 21**”

**Step 4:** search any exploitation available in Metasploit database using “**searchsploit ftp kerebros**”

**Step 5:** use any auxiliary suitable or which works perfectly to exploit the port. “**use linux/http/hadoop\_unauth\_exec**”

**Step 6:** Then “**show options > set rhosts > set rport > exploit/run**”



**Exploiting Port 53:**

**DNS Cache Poisoning:**

**Step 1:** Check whether the port is open or not using the command “**nmap 45.60.73.225 -p 53**”.

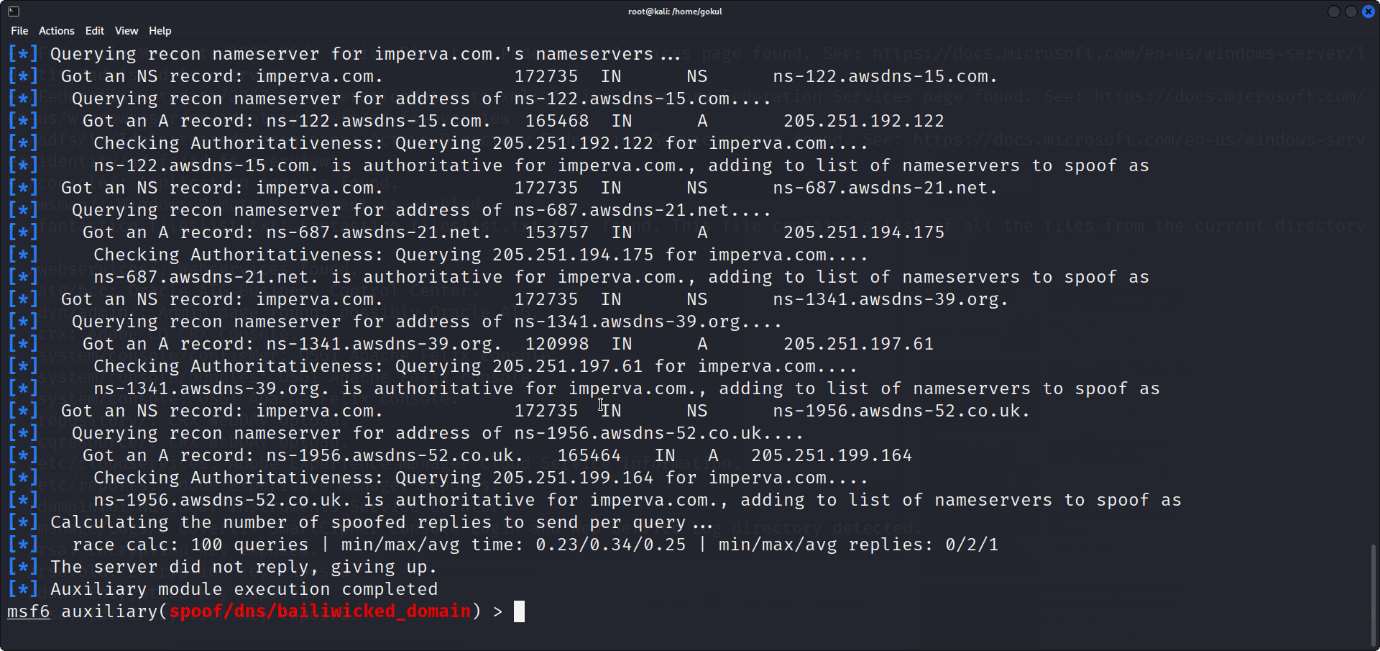
**Step 2:** Find the version of the dns service used by the website using the command “**nmap -sV 45.60.73.225 -p 53**”

**Step 3:** Search for exploits available in Metasploit using “searchsploit dns ”

**Step 4:** Select what type of attack whether spoofing or sniffing.

**Step 5**: Select the auxiliary “**use spoof/dns/baliwicked\_domain**”

**Step 6:** Then use the exploit using the commands “**show options > set rhosts > set domain > set newdns**”



**Exploiting Port 4444:**

**Step 1:** Check whether the port is open or not using the command “**nmap 45.60.73.225 -p 4444**”.

**Step 2:** Know what service and version is being used by the website using the command “**nmap -sV 45.60.73.225 -p 4444**”. It is using krb524

**Step 3:** Search any exploitation available in exploit database “**searchsploit krb524**”

**Step 4:** Select the sockso\_traversal to make an attack that will allow to download files from the directory using the command “**use scanner/http/sockso\_traversal**”

**Step 5:** Then set rhosts and run/exploit

Session Hijacking:

