TEAM 2.7

TEAM MEMBERS

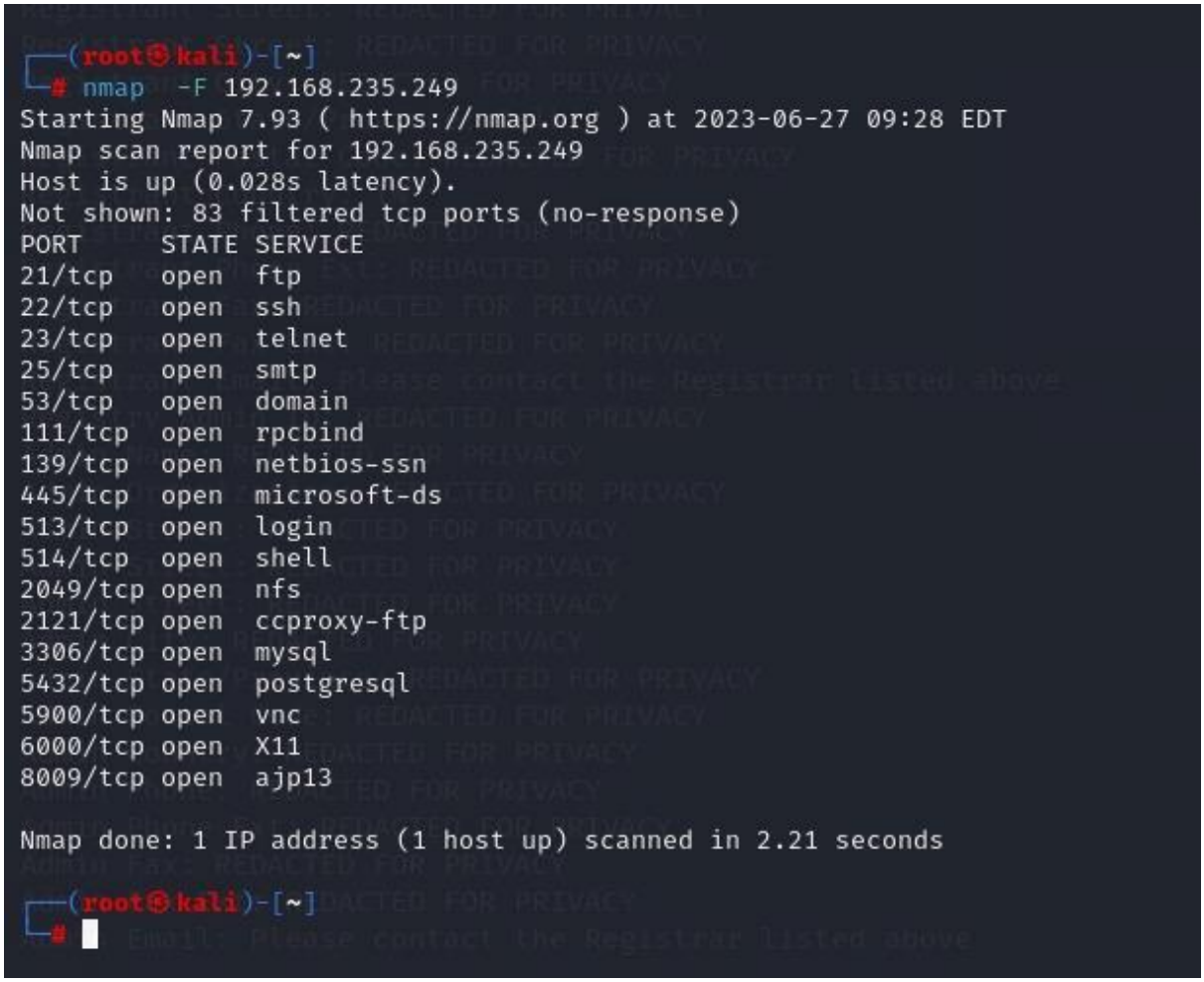
ADITYA DADASAHEB LAWAND

AYUSH SHARMA

VEDANT MUDALAIAR

ADITYA MAHESHWARI

PRACTISE WEBSITE : METASPLOITABLE 2



Open Ports:

● Port 21/tcp: This is the FTP (File Transfer Protocol) port. The version mentioned, vsftpd 2.3.4, has had several vulnerabilities in the past.

● Port 22/tcp: This is the SSH (Secure Shell) port, which provides secure remote login and command execution. The version specified, OpenSSH 4.7p1 Debian 8ubuntu1, has had vulnerabilities in older versions.

● Port 23/tcp: This is the Telnet port, which is an insecure protocol for remote access. The presence of the Linux telnetd service indicates that Telnet is enabled on the system. Telnet is known to transmit data in clear text, making it susceptible to eavesdropping.

● Port 25/tcp: This is the SMTP (Simple Mail Transfer Protocol) port used for email transmission. The presence of Postfix smtpd suggests that the server is running a mail server. Security risks associated with SMTP ports mainly involve email relay and spam issues.

● Port 53/tcp: This is the DNS (Domain Name System) port. The presence of ISC BIND 9.4.2 indicates the system is running a DNS server. DNS servers can be vulnerable to various types of attacks, including DNS spoofing and denial-of-service (DoS) attacks.

● Port 111/tcp: This is the RPC (Remote Procedure Call) port used for network services. The presence of rpcbind indicates that the system has RPC services running. Misconfigured or vulnerable RPC services can be exploited to gain unauthorized access or launch remote attacks.

● Port 445/tcp: Port 445 is a well-known port number used in the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) communications. It is primarily associated with the Microsoft-DS (Directory Services) service, which is used for file and printer sharing in Windows networks.

● Port 513/tcp: This is the login port used for remote login. The presence of OpenBSD or Solaris rlogind indicates that the system allows remote login using the rlogin protocol. Similar to Telnet, rlogin transmits data in clear text, making it vulnerable to eavesdropping.

● Port 514/tcp: This port is tcpwrapped, meaning that the service listening on this port is not identifiable based on the provided information. Further analysis is needed to determine the exact nature and potential vulnerabilities associated with this port.

● Port 2049/tcp: This is the NFS (Network File System) port used for file sharing between computers. The presence of NFS indicates that the system has NFS services running. NFS can have security vulnerabilities, such as unauthorized access or information disclosure if not properly configured and secured.

● Port 2121/tcp: This is the FTP (File Transfer Protocol) port, specifically for ProFTPD version 1.3.1. Similar to port 21, the version specified may have vulnerabilities associated with it.

● Port 3306/tcp: This is the MySQL database port. The presence of MySQL 5.0.51a-3ubuntu5 suggests that a MySQL server is running. It is crucial to secure the MySQL server properly, including setting strong passwords, restricting access, and keeping the server up to date, to prevent unauthorized access or data breaches.

● Port 5432/tcp: This is the PostgreSQL database port. The presence of PostgreSQL DB 8.3.0 - 8.3.7 indicates a running PostgreSQL server. Like MySQL, it is important to secure the PostgreSQL server by applying security patches, using strong authentication, and implementing proper access controls to protect the data stored in the database.

● Port 5900/tcp: This is the VNC (Virtual Network Computing) port. VNC is a remote desktop protocol. The presence of VNC (protocol 3.3) suggests that a VNC server is running on the system. VNC can be a security risk if not properly configured, as it could allow unauthorized access to the system. It is recommended to secure the VNC server by using strong passwords, encryption, and limiting access to trusted networks or users.

● Port 6000/tcp: Port 6000 is a well-known port number used in computer networking. It is associated with the X Window System, a widely used windowing system for Unix-like operating systems. Here are some key points about port 6000:

1. X Window System: The X Window System, often referred to as X11, is a protocol and software suite that provides the foundation for graphical user interfaces (GUIs) in Unix, Linux, and other Unix-like systems. It allows users to run applications with graphical interfaces and display them on remote machines.
2. X11 Display Manager: Port 6000 is used by the X11 display manager to listen for incoming X Window System connections. When an application on one machine wants to display its graphical output on another machine, it connects to port 6000 on the remote machine to establish a communication channel.

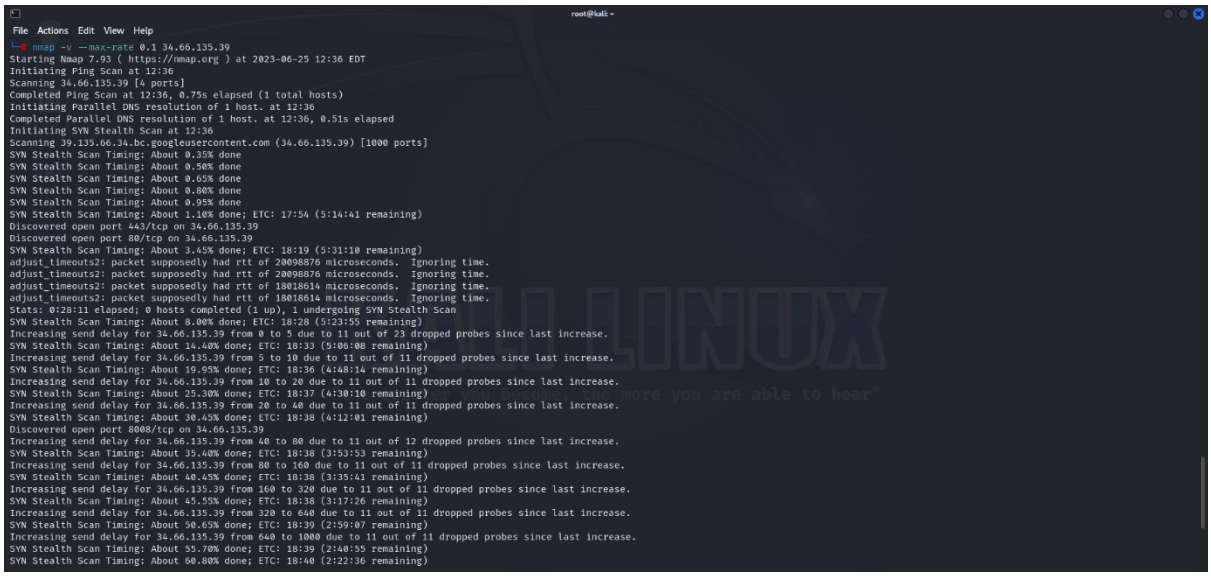
● Port 8009/tcp: Port 8009 is a commonly used port in computer networking. Here are some key points about port 8009:

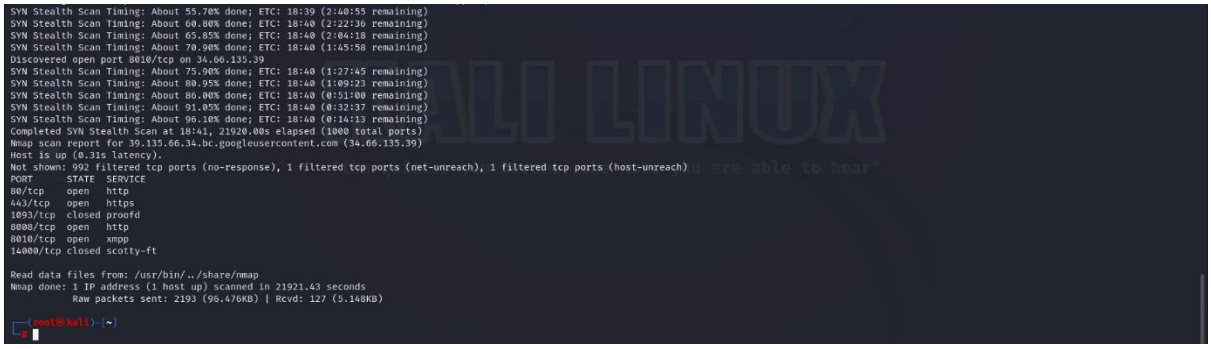
1. AJP Connector: Port 8009 is associated with the Apache JServ Protocol (AJP) connector. AJP is a communication protocol used to proxy requests from a web server to an application server. It allows web servers, such as Apache HTTP Server, to delegate the processing of dynamic content to an application server, such as Apache Tomcat or JBoss.
2. Proxying HTTP Requests: The AJP connector listens on port 8009 and acts as a communication channel between the web server and the application server. When a web server receives an HTTP request for a dynamic resource, it can forward that request to the application server via the AJP connector on port 8009.

Port 8009 and the AJP connector are commonly used in setups where a web server delegates dynamic request processing to an application server. By utilizing port 8009, organizations can optimize performance and scalability for web applications.

TARGET WEBSITE www.5ivebypenta.com

NMAP SLOW SCAN





PORTS

● Port 8008/tcp: Port 8008 is a well-known port number used in computer networking. Here are some key points about port 8008:

1. Alternative HTTP Port: Port 8008 is often used as an alternative port for Hypertext Transfer Protocol (HTTP) communication. HTTP is the underlying protocol for browsing the web and retrieving web content. While the default port for HTTP is 80, port 8008 can be used as an alternate port for HTTP traffic in specific cases.
2. Google Chrome DevTools: Port 8008 is commonly associated with the Google Chrome DevTools Protocol. DevTools is a set of web developer tools integrated into the Google Chrome browser. It allows developers to inspect, debug, and profile web applications. Port 8008 is used for communication between the browser and the DevTools frontend.

● Port 8010/tcp : Port 8010 is not assigned to any specific service or protocol by the Internet Assigned Numbers Authority (IANA) as of my knowledge cutoff in September 2021. This means that port 8010 is not associated with a well-known service or protocol.

In general, unassigned port numbers can be used for various purposes based on specific application or system configurations. It is possible that port 8010 is used by some applications or services in specific environments, but without further context or information, it is difficult to provide specific details about its usage.

NSLOOKUP

```
┌──(root㉿kali)-[~]
└─# nslookup www.5ivebypenta.in
Server:         192.168.235.203
Address:        192.168.235.203#53

Non-authoritative answer:
Name:   www.5ivebypenta.in
Address: 34.66.135.39
```

HOST

```
┌──(root㉿kali)-[~]
└─# host www.5ivebypenta.in
www.5ivebypenta.in has address 34.66.135.39

┌──(root㉿kali)-[~]
└─# host -t ns www.5ivebypenta.in
www.5ivebypenta.in has no NS record

┌──(root㉿kali)-[~]
└─# host -t mx www.5ivebypenta.in
www.5ivebypenta.in has no MX record
```

WHOIS

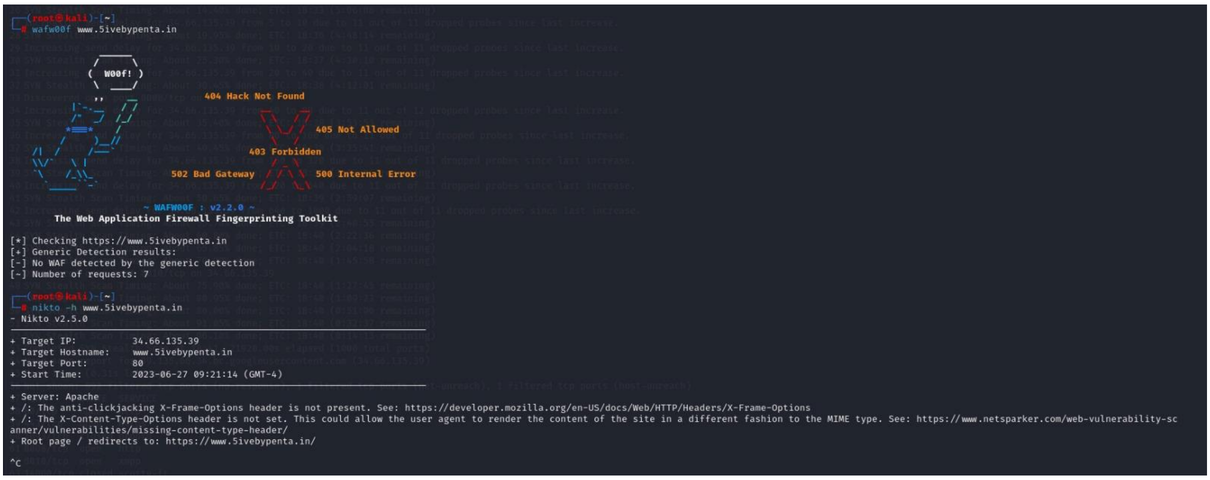
```
┌──(root㉿kali)-[~]
└─# whois 5ivebypenta.in
Domain Name: 5ivebypenta.in
Registry Domain ID: DF732D323759445F4A4D302A5A2395D19-IN
Registrar WHOIS Server:
Registrar URL: https://publicdomainregistry.com/
Updated Date: 2023-02-12T07:42:05Z
Creation Date: 2021-02-19T04:29:23Z
Registry Expiry Date: 2024-02-19T04:29:23Z
Registrar: Endurance Digital Domain Technology LLP
Registrar IANA ID: 801217
Registrar Abuse Contact Email: abuse@publicdomainregistry.com
Registrar Abuse Contact Phone: +1.2013775952
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: 5ive By Penta Sports
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Delhi
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: IN
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please contact the Registrar listed above
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext: REDACTED FOR PRIVACY
Admin Email: Please contact the Registrar listed above
Registry Tech ID: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
```

```
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext: REDACTED FOR PRIVACY
Tech Fax: REDACTED FOR PRIVACY
Tech Fax Ext: REDACTED FOR PRIVACY
Tech Email: Please contact the Registrar listed above
Name Server: ns2.intermesh.net
Name Server: ns1.intermesh.net
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2023-06-27T13:19:28Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

Access to .IN WHOIS information is provided to assist persons in determining the contents of a domain name registration record in the .IN registry database. The data in this record is provided by .IN Registry f
or informational purposes only ,and .IN does not guarantee its accuracy.  This service is intended only for query-based access. You agree that you will use this data only for lawful purposes and that, under no
circumstances will you use this data to (a) allow, enable, or otherwise support the transmission by e-mail, telephone, or facsimile of mass unsolicited, commercial advertising or solicitations to entities other
 than the data recipient's own existing customers; or (b) enable high volume, automated, electronic processes that send queries or data to the systems of Registry Operator or a Registrar, or NIXI except as reas
onably necessary to register domain names or modify existing registrations. All rights reserved. .IN reserves the right to modify these terms at any time. By submitting this query, you agree to abide by this po
licy.
```

WAFWOOF



XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX