MINI PROJECT - II

ACMEGRADE

Cyber Security (April'24)

NETWORK SCANNING

Submitted by: R.Yogeshram

Email: yogeshramr@gmail.com

NETWORK SCANNING

Network scanning in cybersecurity refers to the process of identifying active devices, hosts, and services on a network. This is typically done to assess the security posture of the network, identify potential vulnerabilities, and discover network resources. Network scanning can be performed using various tools and techniques, and it often includes:

1. IP Address Identification: Discovering active IP addresses on the network to determine what devices are present.
2. Port Scanning: Identifying open ports on devices to understand what services or applications are running. This can reveal potential entry points for attackers.
3. Service Detection: Determining what services (like HTTP, FTP, or SSH) are running on the identified ports. This helps in understanding the software and versions in use, which can be crucial for vulnerability assessment.
4. OS Fingerprinting: Inferring the operating system of a host based on the characteristics of the network traffic it generates. This information can help in tailoring security measures or identifying outdated systems.
5. Vulnerability Scanning: Identifying known vulnerabilities in systems and services that can be exploited by attackers. This involves using databases of known vulnerabilities, like CVE (Common Vulnerabilities and Exposures), and matching them against the software versions detected during scanning.

Network scanning is a fundamental step in both offensive and defensive cybersecurity operations. While it is a critical part of penetration testing and ethical hacking to identify and fix vulnerabilities, it can also be used by malicious actors to map out a network and look for weak points to exploit. Therefore, organizations often monitor for unauthorized scanning activities as a part of their security strategy.

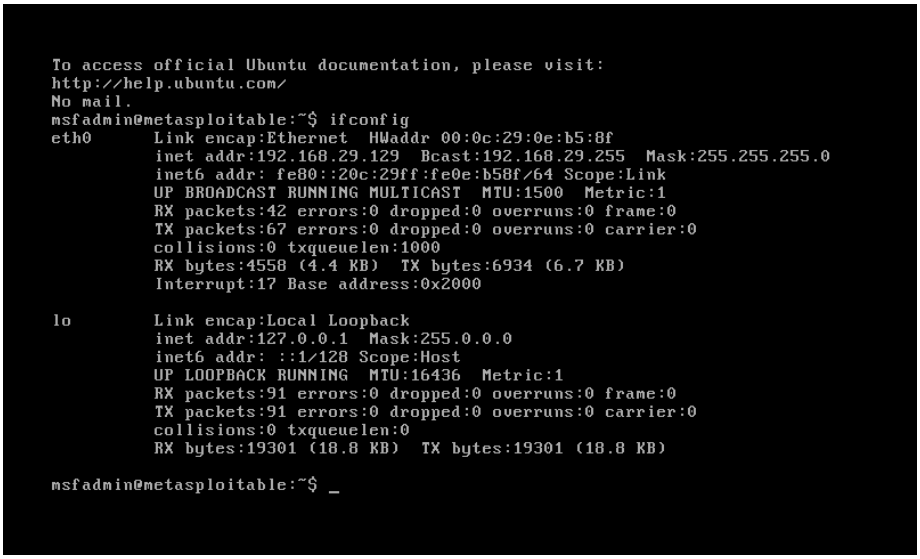
Objectives:

1. To discover live hosts/computer, IP address, and open ports of the victim.
2. To discover services that are running on a host computer.
3. To discover the Operating System and system architecture of the target.
4. To discover and deal with vulnerabilities in Live hosts.

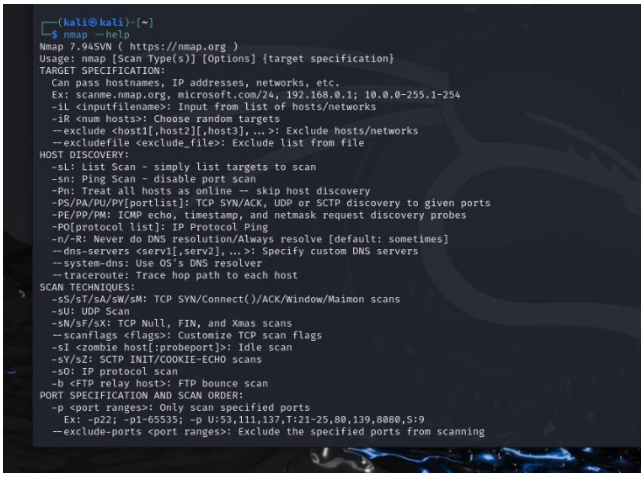
Scanning Methodologies:

1. Select your target – For practice here I used Metasploit
2. Scanning for active devices
3. Scan for open ports
4. Check services on open-ports
5. Grab the versions running on open services
6. Check the OS running on target
7. Bypass security solutions/devices (select right type of scan)

Target Machine :- Metasploit

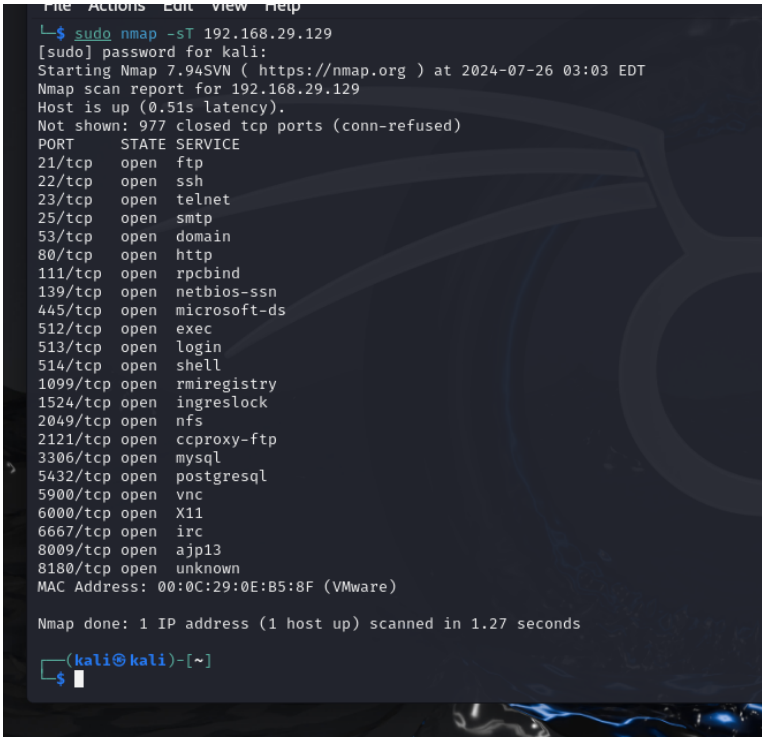


Tool used for network scanning is nmap



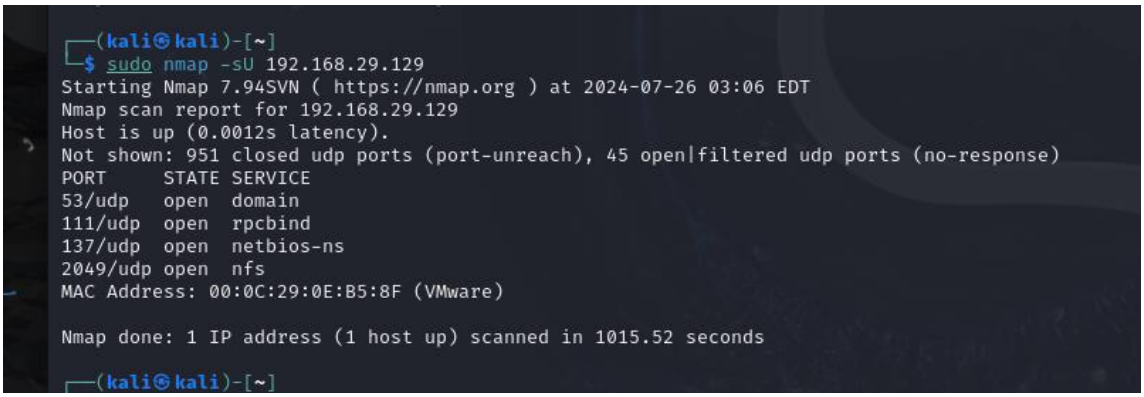
❖ **TCP scan**

A TCP scan, or TCP port scan, is a type of network scanning method used to identify open TCP ports on a host or a network of hosts. TCP ports are associated with specific services and applications, and scanning these ports can provide valuable information about the devices and services available on the network



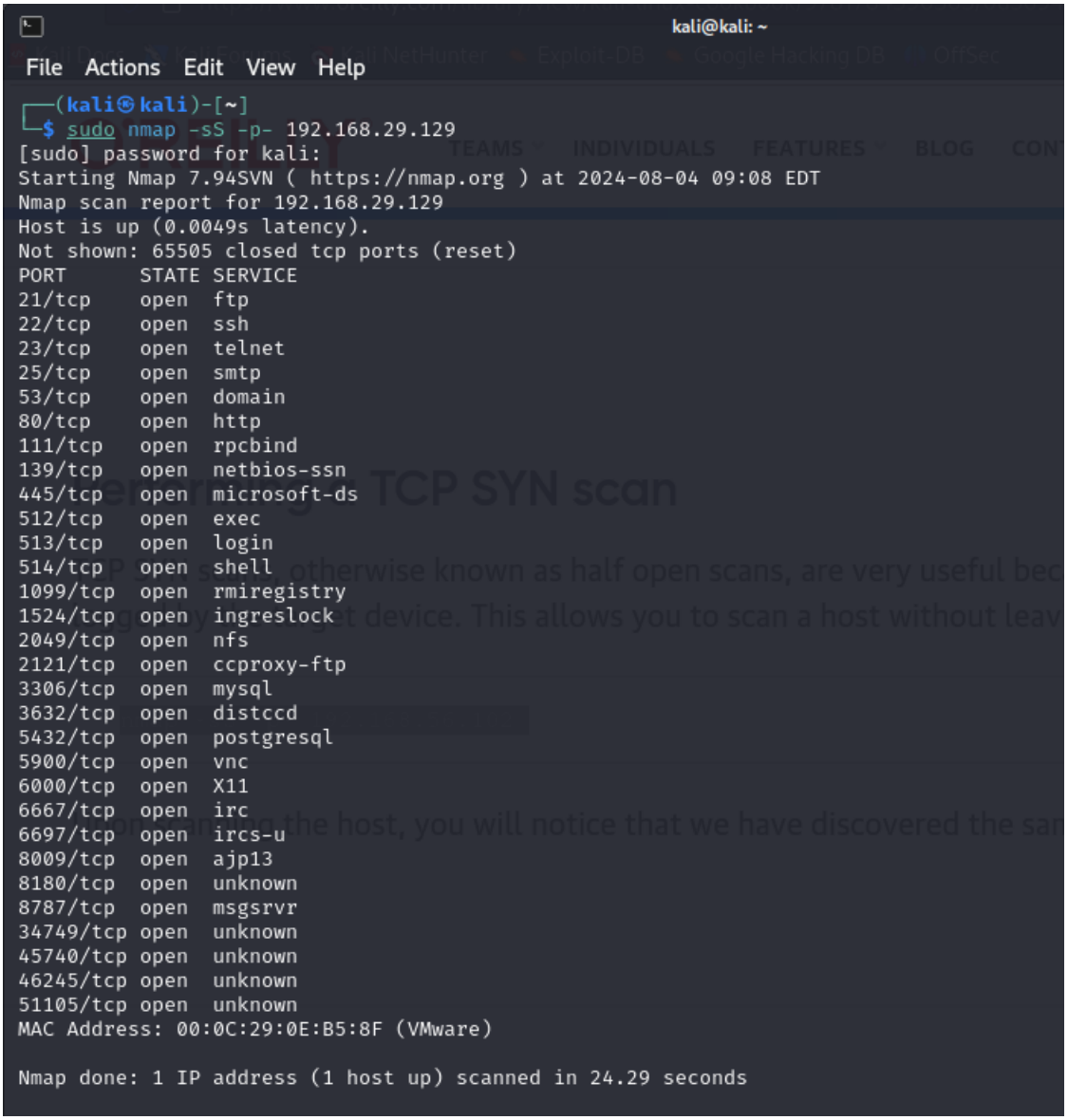
❖ **UDP scan**

A UDP scan is a network scanning technique used to identify open UDP (User Datagram Protocol) ports on a target system. Unlike TCP, UDP is a connectionless protocol, meaning it doesn't establish a connection before data is sent. This characteristic makes UDP scanning fundamentally different and, in some cases, more challenging than TCP scanning.



❖ **SYN scan**

SYN scan or stealth doesn't complete the TCP three-way handshake technique. A hacker sends an SYN packet to the victim, and if an SYN/ACK frame is received back, then the target would complete the connection, and the port is in a position to listen. If an RST is retrieved from the target, it is assumed that the port is closed or not activated. SYN stealth scan is advantageous because a few IDS systems log this as an attack or connection attempt



❖ **Null scan**

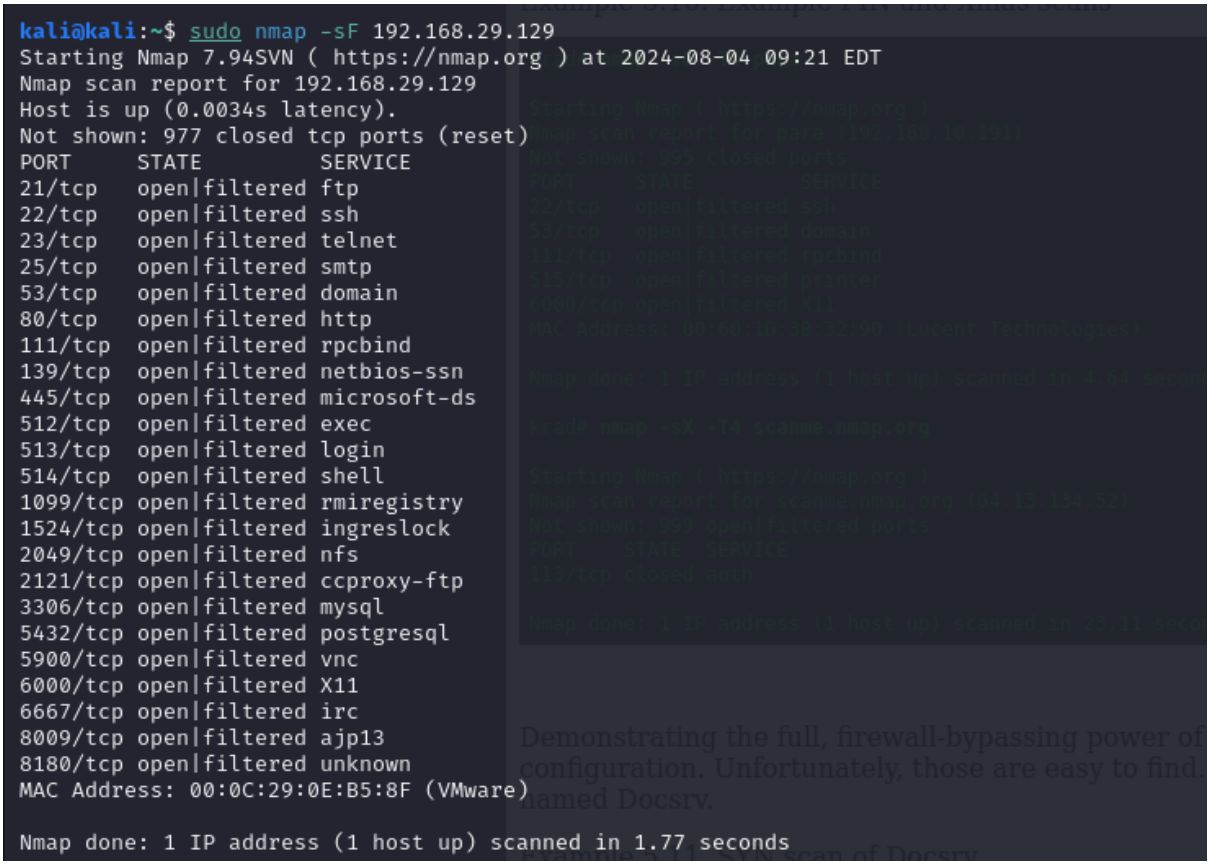
In a null scan, the attacker sends a packet to the target without any flags set within it. Once again, the target will be confused and will not respond. This will indicate the port is open on the target. However, if the target responds with an RST packet, this means the port is closed on the device.

```
kali@kali:~$ sudo nmap -sN 192.168.29.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-04 09:15 EDT
Nmap scan report for 192.168.29.129
Host is up (0.0021s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
23/tcp   open|filtered telnet
25/tcp   open|filtered smtp
53/tcp   open|filtered domain
80/tcp   open|filtered http
111/tcp  open|filtered rpcbind
139/tcp  open|filtered netbios-ssn
445/tcp  open|filtered microsoft-ds
512/tcp  open|filtered exec
513/tcp  open|filtered login
514/tcp  open|filtered shell
1099/tcp open|filtered rmiregistry
1524/tcp open|filtered ingreslock
2049/tcp open|filtered nfs
2121/tcp open|filtered ccproxy-ftp
3306/tcp open|filtered mysql
5432/tcp open|filtered postgresql
5900/tcp open|filtered vnc
6000/tcp open|filtered X11
6667/tcp open|filtered irc
8009/tcp open|filtered ajp13
8180/tcp open|filtered unknown
MAC Address: 00:0C:29:0E:B5:8F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 3.08 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p 1-100 192.168.29.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-04 09:12 EDT
Nmap scan report for 192.168.29.129
Host is up (0.011s latency).
Not shown: 94 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
23/tcp open  telnet
25/tcp open  smtp
53/tcp open  domain
80/tcp open  http
MAC Address: 00:0C:29:0E:B5:8F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
```

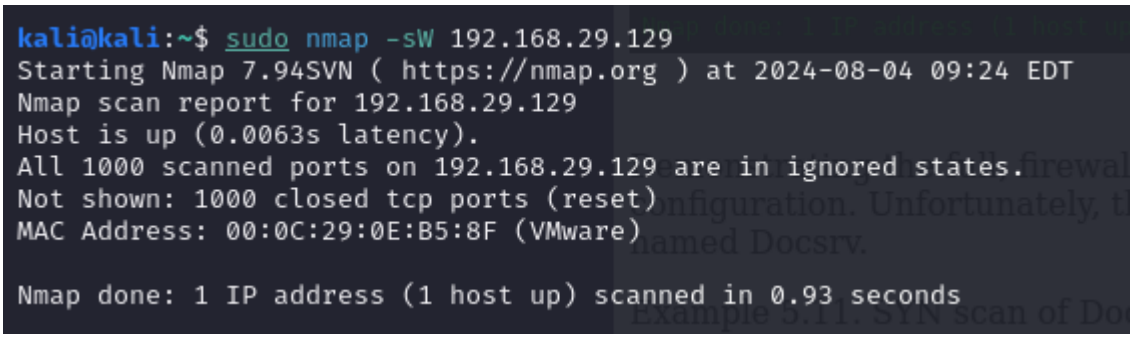
❖ **FIN scan**

The FIN Scan will send a TCP segment with the FIN flag set. When we send this packet to destination that doesn't already have establish session will drop it (means we will not get any response from destination) if we get RST flag from destination then we know that port is closed.



❖ **Wind scan**

Window scan is exactly the same as ACK scan except that it exploits an implementation detail of certain systems to differentiate open ports from closed ones, rather than always printing unfiltered when a RST is returned.



❖ **Maimon scan**

This scan method is used to detect open or filtered ports on a target system.

Functionality: The Maimon scan sends a TCP packet with the FIN/ACK flags set to the target port.
Detection:

- If the port is closed, the target machine will respond with an RST (Reset) packet.
- If the port is open or filtered, there will be no response.

Use Case: This scan type can bypass certain firewalls and packet filters that might block standard SYN or ACK scans, making it useful for stealthier port scanning.

```
kali@kali:~$ sudo nmap -sM 192.168.29.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-04 09:33 EDT
Nmap scan report for 192.168.29.129
Host is up (0.0030s latency).
All 1000 scanned ports on 192.168.29.129 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 00:0C:29:0E:B5:8F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.85 seconds
```

❖ **Xmas scan**

Xmas scan is a type of port scan used to identify open ports on a system. It is also known as a Christmas tree scan because it sets several TCP flags high to resemble a lit-up Christmas tree. It is often used by attackers to identify potential vulnerabilities in a system.

This scan uses a loophole with the TCP RFC to differentiate between open and closed ports. So in other words, the Xmas scan in order to identify listening ports on a targeted system will send a specific packet. If the port is open on the target system then the packets will be ignored.

```
kali@kali:~$ sudo nmap -sX 192.168.29.129
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-04 10:03 EDT
Nmap scan report for 192.168.29.129
Host is up (0.036s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
23/tcp   open|filtered telnet
25/tcp   open|filtered smtp
53/tcp   open|filtered domain
80/tcp   open|filtered http
111/tcp  open|filtered rpcbind
139/tcp  open|filtered netbios-ssn
445/tcp  open|filtered microsoft-ds
512/tcp  open|filtered exec
513/tcp  open|filtered login
514/tcp  open|filtered shell
1099/tcp open|filtered rmiregistry
1524/tcp open|filtered ingreslock
2049/tcp open|filtered nfs
2121/tcp open|filtered ccproxy-ftp
3306/tcp open|filtered mysql
5432/tcp open|filtered postgresql
5900/tcp open|filtered vnc
6000/tcp open|filtered X11
6667/tcp open|filtered irc
8009/tcp open|filtered ajp13
8180/tcp open|filtered unknown
MAC Address: 00:0C:29:0E:B5:8F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.95 seconds
```

- **IDLE scan**

  An idle scan is a TCP port scan method for determining what services are open on a target computer without leaving traces pointing back at oneself. This is accomplished by using packet spoofing to impersonate another computer so that the target believes it's being accessed by the zombie.

  An Idle scan in Nmap is a stealthy scan method that allows you to scan a target without sending packets from your own IP address. Instead, it uses a "zombie" host to probe the target. The zombie host must be idle and have a predictable IP ID sequence number

  Syntax: nmap -sI [zombie_ip] [target_ip]

  Before performing an Idle scan, ensure that you have permission to scan both the zombie and the target hosts. Unauthorized scanning can be illegal and unethical.

```
kali@kali:~$ sudo nmap -p- -sI adobe.com www.riaa.com
WARNING: Many people use -Pn w/Idlescan to prevent pings from their true IP.  On the other hand, timing info Nmap gain
s from pings can allow for faster, more reliable scans.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-04 10:09 EDT
Idle scan using zombie adobe.com (184.84.233.25:443); Class: Incremental
Idle scan is unable to obtain meaningful results from proxy adobe.com (184.84.233.25).  I'm sorry it didn't work out.
QUITTING!
```

❖ Verbosity

verbosity refers to the level of detail included in the output generated by the scan. When you increase the verbosity, Nmap provides more detailed information about its progress and findings during the scan process.

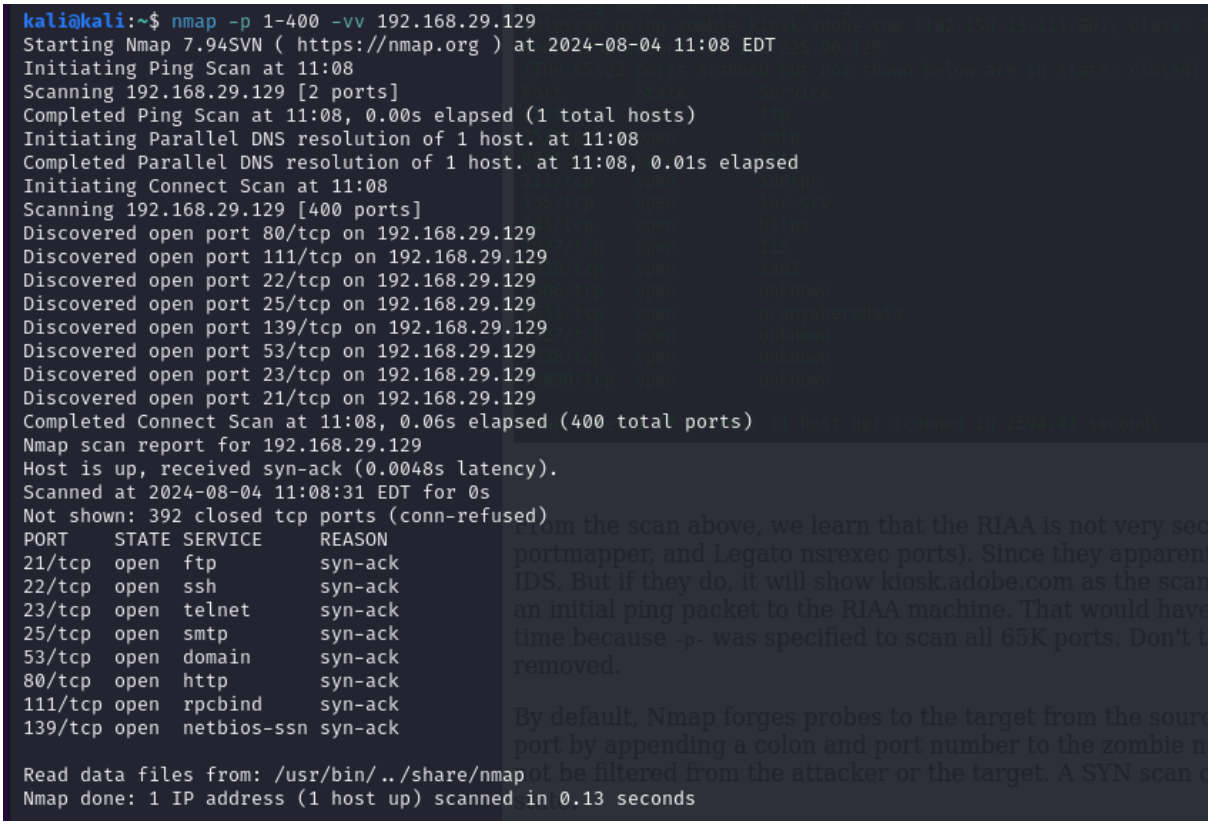
Nmap uses the -v flag to control verbosity. You can increase verbosity by adding more v characters.

Basic Verbosity (-v): This provides a moderate amount of additional information, such as the stages of the scan and the ports being scanned.

Increased Verbosity (-vv): This gives even more detailed information, including timing details and responses from the target.

Maximum Verbosity (-vvv): This provides the maximum amount of detail possible.

Increasing verbosity is particularly useful for troubleshooting and understanding the behavior of the scan, especially during complex or long-running operations.



❖ To find the OS

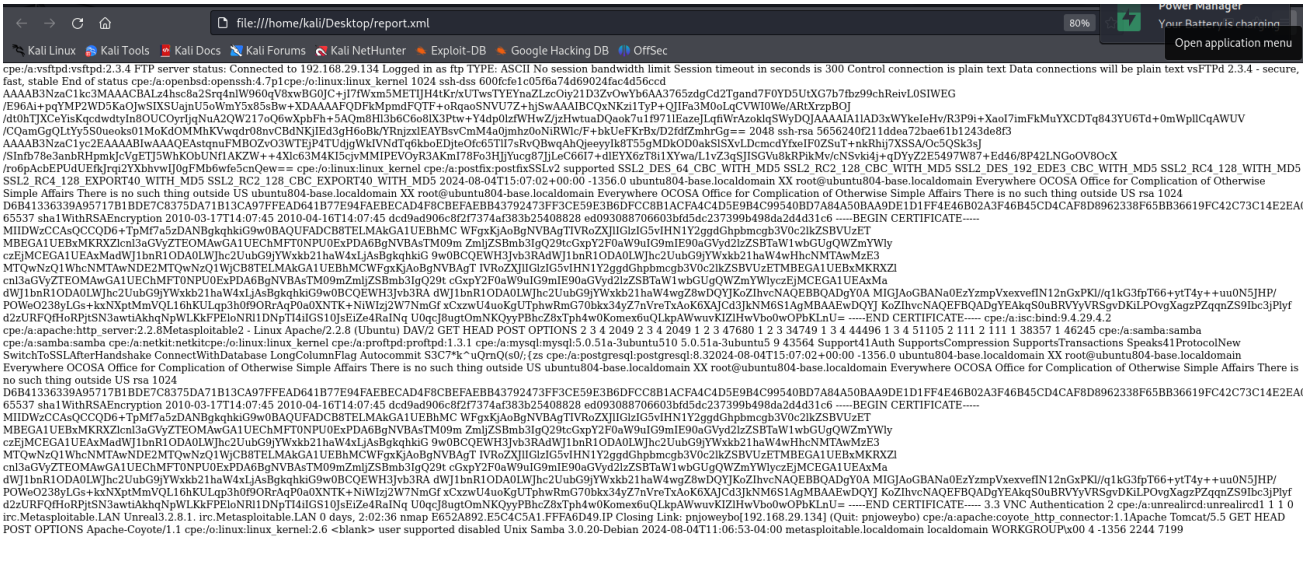
```
kali@kali:~$ sudo nmap -sS -p 1-65535 -vv 192.168.29.129 -sV -O
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-04 11:13 EDT
NSE: Loaded 46 scripts for scanning.
Initiating ARP Ping Scan at 11:13
Scanning 192.168.29.129 [1 port]
Completed ARP Ping Scan at 11:13, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:13
Completed Parallel DNS resolution of 1 host. at 11:13, 0.01s elapsed
Initiating SYN Stealth Scan at 11:13
Scanning 192.168.29.129 [65535 ports]
Discovered open port 111/tcp on 192.168.29.129
Discovered open port 53/tcp on 192.168.29.129
Discovered open port 139/tcp on 192.168.29.129
Discovered open port 25/tcp on 192.168.29.129
Discovered open port 445/tcp on 192.168.29.129
Discovered open port 3306/tcp on 192.168.29.129
Discovered open port 23/tcp on 192.168.29.129
Discovered open port 80/tcp on 192.168.29.129
Discovered open port 22/tcp on 192.168.29.129
Discovered open port 21/tcp on 192.168.29.129
Discovered open port 5900/tcp on 192.168.29.129
Discovered open port 6000/tcp on 192.168.29.129
Discovered open port 8787/tcp on 192.168.29.129
Discovered open port 46245/tcp on 192.168.29.129
Discovered open port 34749/tcp on 192.168.29.129
Discovered open port 51105/tcp on 192.168.29.129
Discovered open port 514/tcp on 192.168.29.129
Discovered open port 8180/tcp on 192.168.29.129
Discovered open port 6667/tcp on 192.168.29.129
Discovered open port 45740/tcp on 192.168.29.129
Discovered open port 512/tcp on 192.168.29.129
Discovered open port 6697/tcp on 192.168.29.129
Discovered open port 1524/tcp on 192.168.29.129
Discovered open port 513/tcp on 192.168.29.129
Discovered open port 2049/tcp on 192.168.29.129
Discovered open port 3632/tcp on 192.168.29.129
Discovered open port 5432/tcp on 192.168.29.129
Discovered open port 8009/tcp on 192.168.29.129
Discovered open port 1099/tcp on 192.168.29.129
```

```
Scanning 30 services on 192.168.29.129
Completed Service scan at 11:16, 126.23s elapsed (30 services on 1 host)
Initiating OS detection (try #1) against 192.168.29.129
NSE: Script scanning 192.168.29.129.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 11:16
Completed NSE at 11:16, 0.19s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 11:16
Completed NSE at 11:16, 0.09s elapsed
Nmap scan report for 192.168.29.129
Host is up, received arp-response (0.0011s latency).
Scanned at 2024-08-04 11:13:55 EDT for 139s
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE     REASON         VERSION
21/tcp    open  ftp         syn-ack ttl 64 vsftpd 2.3.4
22/tcp    open  ssh         syn-ack ttl 64 OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      syn-ack ttl 64 Linux telnetd
25/tcp    open  smtp        syn-ack ttl 64 Postfix smtpd
53/tcp    open  domain      syn-ack ttl 64 ISC BIND 9.4.2
80/tcp    open  http        syn-ack ttl 64 Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     syn-ack ttl 64 2 (RPC #100000)
139/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        syn-ack ttl 64 netkit-rsh rexecd
513/tcp   open  login       syn-ack ttl 64 OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped  syn-ack ttl 64
1099/tcp  open  java-rmi    syn-ack ttl 64 GNU Classpath grmiregistry
1524/tcp  open  bindshell   syn-ack ttl 64 Metasploitable root shell
2049/tcp  open  nfs         syn-ack ttl 64 2-4 (RPC #100003)
2121/tcp  open  ftp         syn-ack ttl 64 ProFTPD 1.3.1
3306/tcp  open  mysql       syn-ack ttl 64 MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     syn-ack ttl 64 distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql  syn-ack ttl 64 PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         syn-ack ttl 64 VNC (protocol 3.3)
6000/tcp  open  X11         syn-ack ttl 64 (access denied)
6667/tcp  open  irc         syn-ack ttl 64 UnrealIRCd
6697/tcp  open  irc         syn-ack ttl 64 UnrealIRCd
8009/tcp  open  ajp13       syn-ack ttl 64 Apache Jserv (Protocol v1.3)
8180/tcp  open  http        syn-ack ttl 64 Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         syn-ack ttl 64 Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
34749/tcp open  mountd      syn-ack ttl 64 1-3 (RPC #100005)
45740/tcp open  java-rmi    syn-ack ttl 64 GNU Classpath grmiregistry
46245/tcp open  status      syn-ack ttl 64 1 (RPC #100024)
51105/tcp open  nlockmgr    syn-ack ttl 64 1-4 (RPC #100021)
MAC Address: 00:0C:29:0E:B5:8F (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
```

```
34749/tcp open  mountd      syn-ack ttl 64 1-3 (RPC #100005)
45740/tcp open  java-rmi    syn-ack ttl 64 GNU Classpath grmiregistry
46245/tcp open  status      syn-ack ttl 64 1 (RPC #100024)
51105/tcp open  nlockmgr    syn-ack ttl 64 1-4 (RPC #100021)
MAC Address: 00:0C:29:0E:B5:8F (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=8/4%OT=21%CT=1%CU=43216%PV=Y%DS=1%DC=D%G=Y%M=000C29
OS:%TM=66AF9B3E%P=x86_64-pc-linux-gnu)SEQ(SP=CB%GCD=1%ISR=CD%TI=Z%CI=Z%II=I
OS:%TS=7)OPS(O1=M5B4ST11NW5%O2=M5B4ST11NW5%O3=M5B4NNT11NW5%O4=M5B4ST11NW5%O
OS:5=M5B4ST11NW5%O6=M5B4ST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6
OS:=16A0)ECN(R=Y%DF=Y%T=40%W=16D0%O=M5B4NNSNW5%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O
OS:%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=16A0%S=O%A=S+%F=AS%O=M5B4ST
OS:11NW5%RD=0%Q=)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=
OS:40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0
OS:%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=1
OS:64%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Uptime guess: 0.073 days (since Sun Aug  4 09:31:02 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=203 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_ker
nel

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 139.74 seconds
           Raw packets sent: 65977 (2.904MB) | Rcvd: 65552 (2.623MB)
```

❖ To save all results displayed

```
kali@kali:~/Desktop$ sudo nmap -vv -A 192.168.29.129 -oX report.xml
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-04 11:29 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 11:29
Completed NSE at 11:29, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 11:29
Completed NSE at 11:29, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 11:29
Completed NSE at 11:29, 0.00s elapsed
Initiating ARP Ping Scan at 11:29
Scanning 192.168.29.129 [1 port]
Completed ARP Ping Scan at 11:29, 0.10s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:29
Completed Parallel DNS resolution of 1 host. at 11:29, 0.00s elapsed
Initiating SYN Stealth Scan at 11:29
Scanning 192.168.29.129 [1000 ports]
Discovered open port 53/tcp on 192.168.29.129
Discovered open port 25/tcp on 192.168.29.129
Discovered open port 3306/tcp on 192.168.29.129
Discovered open port 139/tcp on 192.168.29.129
Discovered open port 111/tcp on 192.168.29.129
Discovered open port 445/tcp on 192.168.29.129
Discovered open port 23/tcp on 192.168.29.129
```

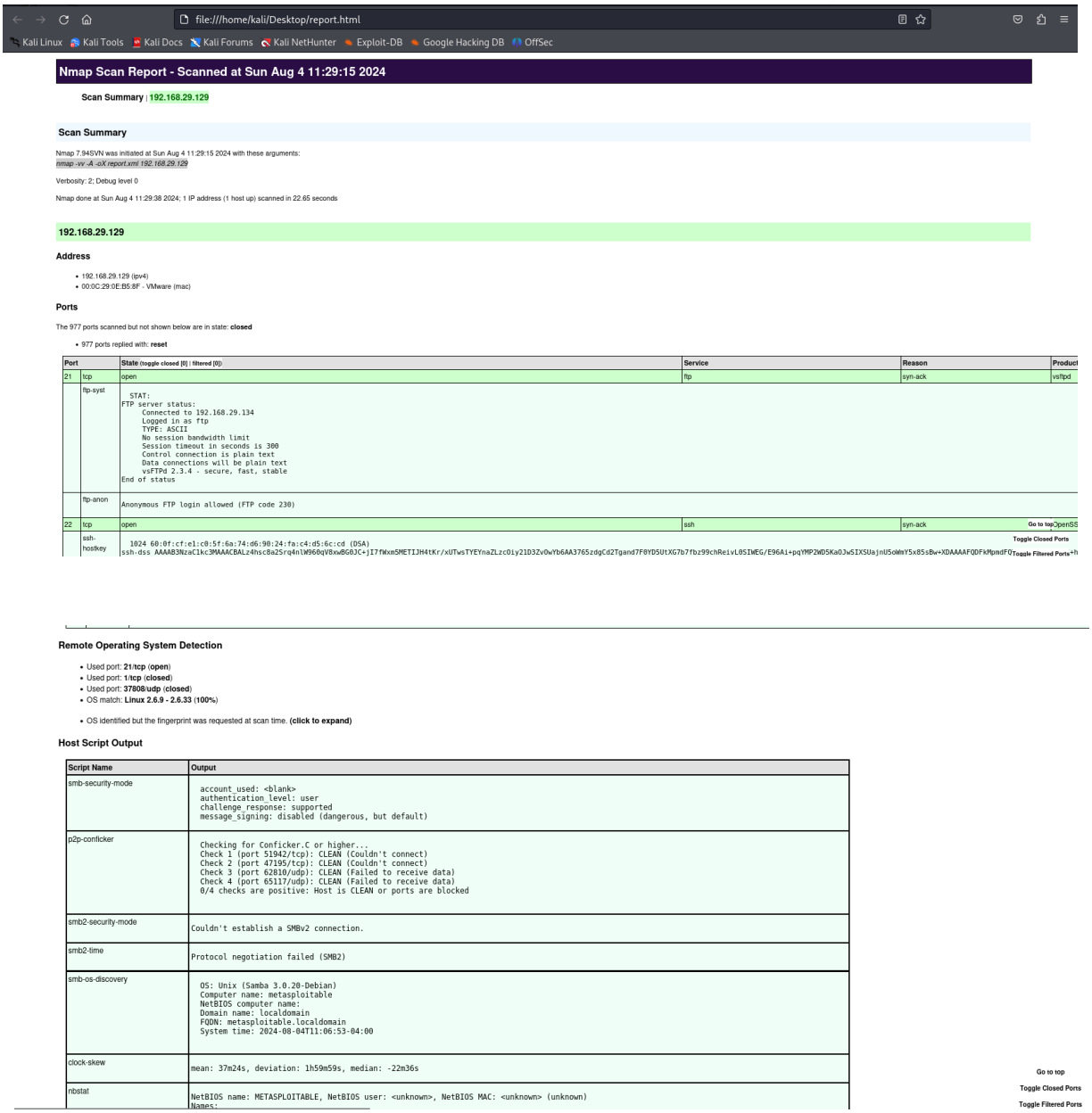


cpe:/a:vsftpd:vsftpd:2.3.4 FTP server status: Connected to 192.168.29.134 Logged in as ftp TYPE: ASCII No session bandwidth limit Session timeout in seconds is 300 Control connection is plain text Data connections will be plain text vsFTPd 2.3.4 - secure, fast, stable End of status cpe:/a:openbsd:openssh:4.7p1 cpe:/o:linux:linux_kernel 1024 ssh-dss 600fcfe1c05f6a74d69024fac4d56ccd
AAAAB3NzaC1kc3MAAACBALz4hsc8a2Srq4nlW960qV8xwBGOJC+jJl7fWxm5METIJH4tKr/xUTwsTYEYnaZLzcOiy21D3ZvOwYb6AA3765zdgCd2Tgand7F0YD5UtXG7b7fbz99chReivL0SIWEG
/E96Ai+pqYMP2WD5KaOJwSIXSUajnU5oWmY5x85sBw+XDAAAAFQDFkMpmdFQTF+oRqaoSNVU7Z+hjSwAAAIBCQxNKzi1TyP+QJIFa3M0oLqCVWI0We/ARtXrzpBOJ
/dt0hTJXCeYisKqcdwdtyIn8OUCOyrIjqNuA2QW217oQ6wXpbFh+5AQm8Hl3b6C6o8IX3Ptw+Y4dp0lzfWHwZ/jzHwtuaDQaok7u1f971IEazeJLqfiWrAzokIqSWyDQJAAAAIA1IAD3xWYkeIeHv/R3P9i+XaoI7imFkMuYXCDTq843YU6Td+0mWpllCqAWUV
/CQamGgQLtYy5S0ueoks01MoKdOMMhKVwqdr08nvCBdNKjIEd3gH6oBk/YRnjzxIEAYBsvCmM4aOjmhzOoNiRWIc/F+bkUeFKrBx/D2fdfZmhrGg== 2048 ssh-rsa 5656240f211ddea72bae61b1243de8f3
AAAAB3NzaC1yc2EAAAABIwAAAQEAstqnuFMBOZvO3WTEjP4TUdjgWkIVNdTq6kboEDjteOfc65TII7sRvQBwqAhQjeeyyIk8T55gMDkOD0akSISXvLDcmcdYIxeIF0ZSuT+nkRhj7XSSA/Oc5QSk3sJ
/SInfb78e3anbRHpmkjcVgETJ5WhKObUNfIAKZW++4Xlc63M4Kl5cjvMMIPEVOyR3AKmI78Fo3HjjYucg87JjLeC66I7+dIEYX6zT8i1XYwa/L1vZJqSJISGVu8kRPikMv/cNSvkj4j+qDYyZ2E5497W87+Ed46/8P42LNGoOV8OcX
/ro6pAcbEPUdUEfkJrqi2YXbvwIJ0qFMb6wfe5cnQew== cpe:/o:linux:linux_kernel cpe:/a:postfix:postfixSSLv2 supported SSL2_DES_64_CBC_WITH_MD5 SSL2_RC2_128_CBC_WITH_MD5 SSL2_DES_192_EDE3_CBC_WITH_MD5 SSL2_RC4_128_WITH_MD5
SSL2_RC4_128_EXPORT40_WITH_MD5 SSL2_RC2_128_CBC_EXPORT40_WITH_MD5 2024-08-04T15:07:02+00:00 -1356.0 ubuntu804-base.localdomain XX root@ubuntu804-base.localdomain Everywhere OCOSA Office for Complication of Otherwise
Simple Affairs There is no such thing outside US ubuntu804-base.localdomain XX root@ubuntu804-base.localdomain Everywhere OCOSA Office for Complication of Otherwise Simple Affairs There is no such thing outside US rsa 1024
D6B41336339A95717B1BDE7C8375DA71B13CA97FFEAD641B77E94FAEBECAD4F8CBEFAEBB43792473FF3CE59E3B6DFCC8B1ACFA4C4D5E9B4C99540BD7A84A50BAA9DE1D1FF4E46B02A3F46B45CD4CAF8D8962338F65BB36619FC42C73C14E2EA(
65537 sha1WithRSAEncryption 2010-03-17T14:07:45 2010-04-16T14:07:45 dcd9ad906c8f2f7374af383b25408828 ed093088706603bfd5dc237399b498da2d4d31c6 -----BEGIN CERTIFICATE-----
MIIDWzCCAsQCCQD6+TpMf7a5zDANBgkqhkiG9w0BAQUFADCB8TELMAkGA1UEBhMC WFgxKjAoBgNVBAgTIVRoZXJlIGlzIG5vIHN1Y2ggdGhpbmcgb3V0c2lkZSBVUzET
MBEGA1UEBxMKRXZlcnl3aGVyZTEOMAwGA1UEChMFT0NPU0ExPDA6BgNVBAsTM09m ZmljZSBmb3IgQ29tcGxpY2F0aW9uIG9mIE90aGVyd2lzZSBTaW1wbGUgQWZmYWly
czEjMCEGA1UEAxMadWJ1bnR1ODA0LWJhc2UubG9jYWxkb21haW4xLjAsBgkqhkiG 9w0BCQEWH3Jvb3RAdWJ1bnR1ODA0LWJhc2UubG9jYWxkb21haW4wHhcNMTAwMzE3
MTQwNzQ1WhcNMTAwNDE2MTQwNzQ1WjCB8TELMAkGA1UEBhMCWFgxKjAoBgNVBAgT IVRoZXJlIGlzIG5vIHN1Y2ggdGhpbmcgb3V0c2lkZSBVUzETMBEGA1UEBxMKRXZl
cnl3aGVyZTEOMAwGA1UEChMFT0NPU0ExPDA6BgNVBAsTM09mZmljZSBmb3IgQ29t cGxpY2F0aW9uIG9mIE90aGVyd2lzZSBTaW1wbGUgQWZmYWlyczEjMCEGA1UEAxMa
dWJ1bnR1ODA0LWJhc2UubG9jYWxkb21haW4xLjAsBgkqhkiG9w0BCQEWH3Jvb3RA dWJ1bnR1ODA0LWJhc2UubG9jYWxkb21haW4wgZ8wDQYJKoZIhvcNAQEBBQADgY0A MIGJAoGBANa0EzYzmpVxexvefIN12nGxPKl//q1kG3fpT66+ytT4y++uu0N5JHP/
POWeO238yLGs+kxNXptMmVQL16hKULqp3h0f9ORrAqP0a0XNTK+NiWIzj2W7NmGf xCxzwU4uoKgUTphwRmG70bkx34yZ7nVreTxAoK6XAJCd3JkNM6S1AgMBAAEwDQYJ KoZIhvcNAQEFBQADgYEAkqS0uBRVYyVRSgvDKiLPOvgXagzPZqqnZS9Ibc3jPlyf
d2zURFQffHoRPjtSN3awtiAkhqNpWLKkFPEloNRI1DNpTI4iIGS10JsEiZe4RaINq U0qcJ8ugtOmNKQyyPBhcZ8xTph4w0Komex6uQLkpAWwuvKlZlHwVbo0wOPbKLnU= -----END CERTIFICATE----- 3,3 VNC Authentication 2 cpe:/a:unrealircd:unrealircd1 1 1 0
irc.Metasploitable.LAN Unreal3.2.8.1. irc.Metasploitable.LAN 0 days, 2:02:36 nmap E652A892.E5C4C5A1.FFFA6D49.IP Closing Link: pnjoweybo[192.168.29.134] (Quit: pnjoweybo) cpe:/a:apache:coyote_http_connector:1.1Apache Tomcat/5.5 GET HEAD
POST OPTIONS Apache-Coyote/1.1 cpe:/o:linux:linux_kernel:2.6 <blank> user supported disabled Unix Samba 3.0.20-Debian 2024-08-04T11:06:53-04:00 metasploitable.localdomain localdomain WORKGROUP\x00 4 -1356 2244 7199

❖ From xml file to HTML file
sudo apt-get install xsltproc
open filename(report.xml)
Sudo xsltproc filename(report.xml) -O report.html
Open report.html

```
kali@kali:~/Desktop$ sudo xsltproc report.xml -o report.html
Warning: program compiled against libxml 212 using older 209

kali@kali:~/Desktop$ open report.html
```

Opens the report.html file in web browser.



file:///home/kali/Desktop/report.html

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec

Nmap Scan Report - Scanned at Sun Aug 4 11:29:15 2024

Scan Summary | 192.168.29.129

Scan Summary

Nmap 7.94SVN was initiated at Sun Aug 4 11:29:15 2024 with these arguments:
nmap -vv -A -oX report.xml 192.168.29.129

Verbosity: 2; Debug level 0

Nmap done at Sun Aug 4 11:29:38 2024; 1 IP address (1 host up) scanned in 22.65 seconds

192.168.29.129

Address

- 192.168.29.129 (ipv4)
- 00:0C:29:0E:B5:8F - VMware (mac)

Ports

The 977 ports scanned but not shown below are in state: **closed**

- 977 ports replied with: **reset**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product
21	tcp	open	ftp	syn-ack	vsftpd
	ftp-syst	STAT: FTP server status: Connected to 192.168.29.134 Logged in as ftp TYPE: ASCII No session bandwidth limit Session timeout in seconds is 300 Control connection is plain text Data connections will be plain text vsFTPd 2.3.4 - secure, fast, stable End of status			
	ftp-anon	Anonymous FTP login allowed (FTP code 230)			
22	tcp	open	ssh	syn-ack	OpenSS
	ssh-hostkey	1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA) ssh-dss AAAAB3NzaC1kc3MAAACBALz4hsc8a2Srq4nlW960qV8xwBGBJC+jI7fWxm5METIJH4tKr/xUTwsTYEYnaZLzcOiy21D3ZvOwYb6AA3765zdgCd2Tgand7F8YD5UtXG7b7fbz99chReivL0SIWEG/E96Ai+pqYMP2WD5KaOJwSIXSUajnU5oWmY5x85sBw+XDAAAAFQDFkMpmdFQ			

Go to top Toggle Closed Ports Toggle Filtered Ports

Remote Operating System Detection

- Used port: **21/tcp** (**open**)
- Used port: **1/tcp** (**closed**)
- Used port: **37808/udp** (**closed**)
- OS match: **Linux 2.6.9 - 2.6.33** (**100%**)

- OS identified but the fingerprint was requested at scan time. **(click to expand)**

Host Script Output

Script Name	Output
smb-security-mode	account_used: <blank> authentication_level: user challenge_response: supported message_signing: disabled (dangerous, but default)
p2p-conficker	Checking for Conficker.C or higher... Check 1 (port 51942/tcp): CLEAN (Couldn't connect) Check 2 (port 47195/tcp): CLEAN (Couldn't connect) Check 3 (port 62810/udp): CLEAN (Failed to receive data) Check 4 (port 65117/udp): CLEAN (Failed to receive data) 0/4 checks are positive: Host is CLEAN or ports are blocked
smb2-security-mode	Couldn't establish a SMBv2 connection.
smb2-time	Protocol negotiation failed (SMB2)
smb-os-discovery	OS: Unix (Samba 3.0.20-Debian) Computer name: metasploitable NetBIOS computer name: Domain name: localdomain FQDN: metasploitable.localdomain System time: 2024-08-04T11:06:53-04:00
clock-skew	mean: 37m24s, deviation: 1h59m59s, median: -22m36s
nbstat	NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown) Names:

Go to top
Toggle Closed Ports
Toggle Filtered Ports