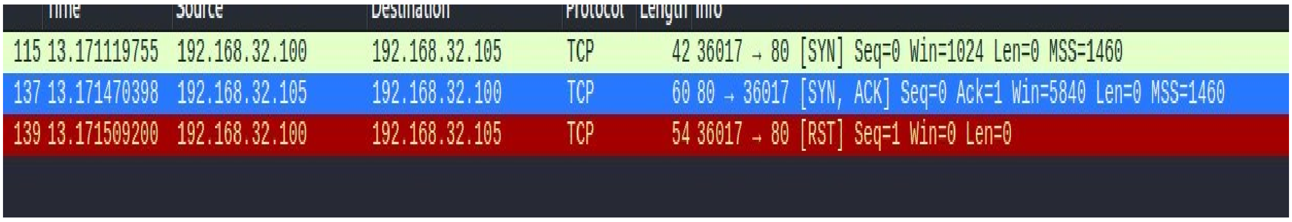
Report 18/05

SYN SCAN

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	PORTGRESQL
5900/TCP	OPEN	VNC
6000/TCP	OPEN	X11
6667/TCP	OPEN	IRC
8009/TCP	OPEN	AJP13
8180/TCP	OPEN	UKNOWN

il Syn scan come abbiamo visto ,è un metodo meno invasivo nella scansione delle porte degli IP infatti avremo comunicazione che si chiuderà inviando un pacchetto RST,non completando il 3 way-hand shake.Qua sotto con il programma Wireshark abbiamo intercettato i pacchetti sulla porta 80 che evidenziano appunto i pacchetti relativi al SYN e SYN/ACK con il successivo RST che evita l'overload del canale.

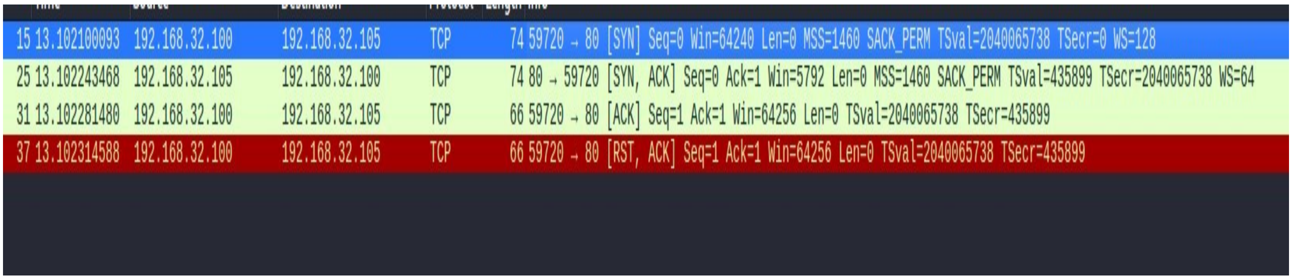


	Time	Source	Destination	Protocol	Length	Info
115	13.171119755	192.168.32.100	192.168.32.105	TCP	42	36017 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
137	13.171470398	192.168.32.105	192.168.32.100	TCP	60	80 → 36017 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
139	13.171509200	192.168.32.100	192.168.32.105	TCP	54	36017 → 80 [RST] Seq=1 Win=0 Len=0

TCP SCAN

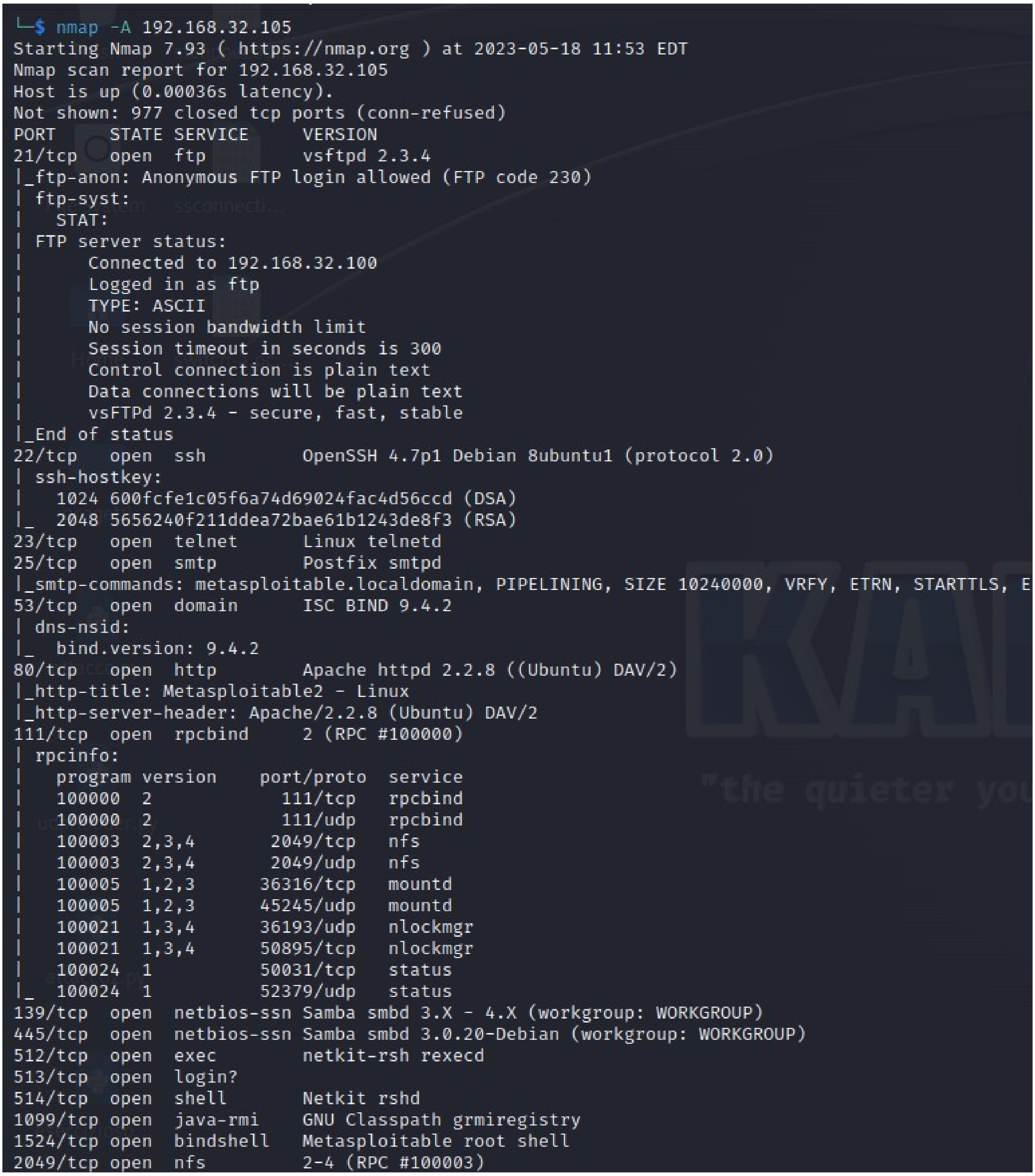
PORT	STATE	SERVICE
21/TCP	OPEN	FTP
22/TCP	OPEN	SSH
23/TCP	OPEN	TELNET
25/TCP	OPEN	SMTP
53/TCP	OPEN	DOMAIN
80/TCP	OPEN	HTTP
111/TCP	OPEN	RPCBIND
139/TCP	OPEN	NETBIOS-SSN
445/TCP	OPEN	MICROSOFT-DS
512/TCP	OPEN	EXEC
513/TCP	OPEN	LOGIN
514/TCP	OPEN	SHELL
1099/TCP	OPEN	RMIREGISTRY
1524/TCP	OPEN	INGRESLOCK
2049/TCP	OPEN	NFS
2121/TCP	OPEN	CCPROXY-FTP
3306/TCP	OPEN	MYSQL
5432/TCP	OPEN	PORTGRESQL
5900/TCP	OPEN	VNC
6000/TCP	OPEN	X11
6667/TCP	OPEN	IRC
8009/TCP	OPEN	AJP13
8180/TCP	OPEN	UKNOWN

Utilizzando il TCP scan, sempre applicando il filtro sulla porta 80,i pacchetti che vediamo vanno ad evidenziare il completamento della procedura 3 way-handshake avviando creando così un canale che in reti molto grandi potrebbe creare una cosiddetta "congestione di rete".



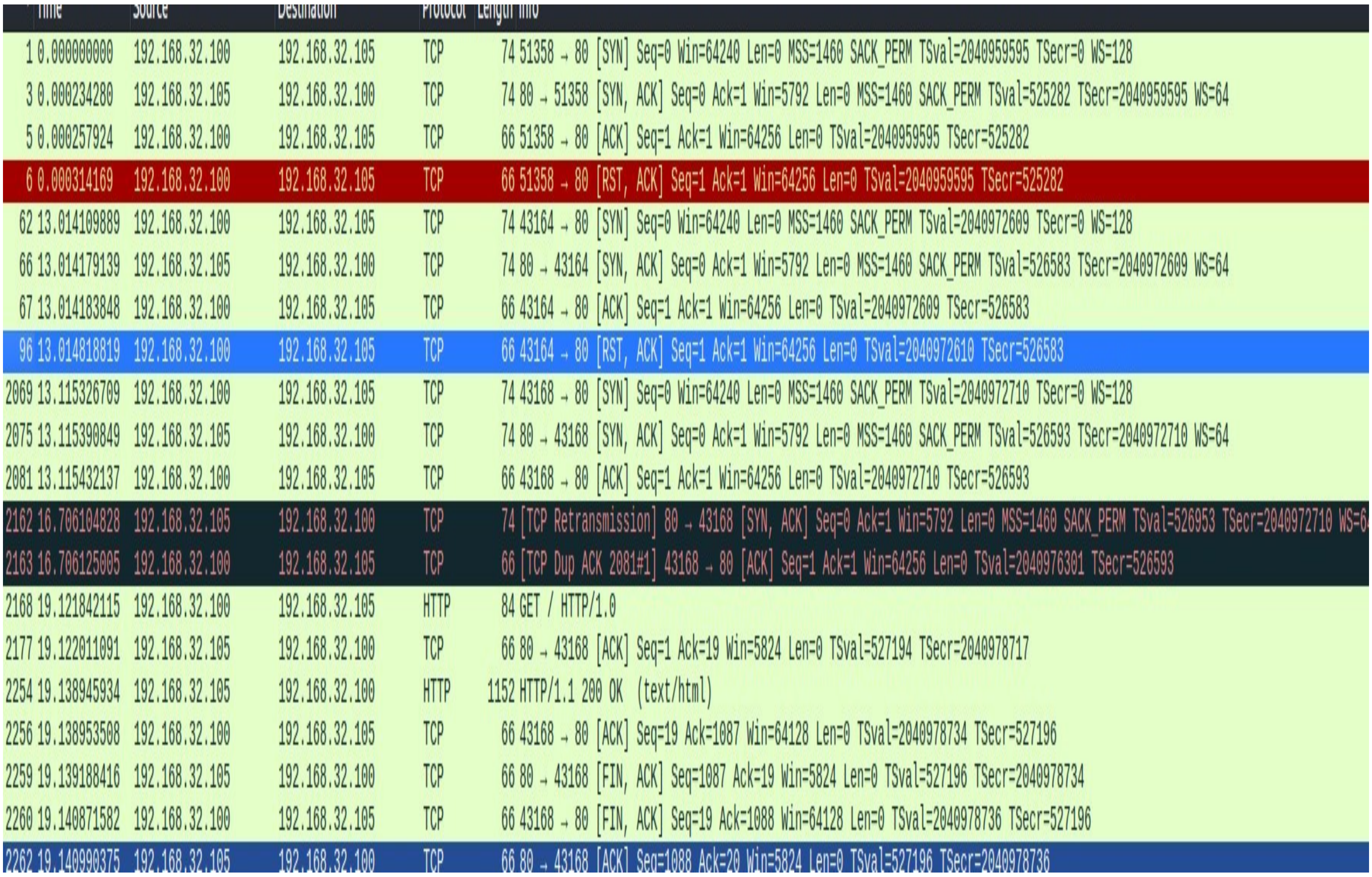
```
15 13.102100093  192.168.32.100  192.168.32.105  TCP  74 59720 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2040065738 TSecr=0 WS=128
25 13.102243468  192.168.32.105  192.168.32.100  TCP  74 80 → 59720 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=435899 TSecr=2040065738 WS=64
31 13.102281480  192.168.32.100  192.168.32.105  TCP  66 59720 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2040065738 TSecr=435899
37 13.102314588  192.168.32.100  192.168.32.105  TCP  66 59720 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2040065738 TSecr=435899
```

Mentre per quanto riguarda lo Scan switch "-A",si va ad effettuare un cosiddetto "Controllo Aggressivo " verso le porte del nostro IP ,dove oltre a mostrarci il rilevamendo del sistema operativo,la scansione della versione ,la scansione degli script e la traceroute.



```
└─$ nmap -A 192.168.32.105
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 11:53 EDT
Nmap scan report for 192.168.32.105
Host is up (0.00036s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.32.100
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_  2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, E
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      36316/tcp   mountd
|   100005  1,2,3      45245/udp   mountd
|   100021  1,3,4      36193/udp   nlockmgr
|   100021  1,3,4      50895/tcp   nlockmgr
|   100024  1          50031/tcp   status
|_  100024  1          52379/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
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)
```

Infatti analizzando i pacchetti con Wireshark sempre col filtro sulla porta 80 vedremo che i pacchetti arriveranno saranno molti di più dei precedenti scan e soprattutto il tempo di scan sarà molto più lungo per l'ottenimento dei dati.



```
     Time          Source          Destination     Protocol Length Info
   1 0.000000000   192.168.32.100  192.168.32.105  TCP        74 51358 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2040959595 TSecr=0 WS=128
   3 0.000234280   192.168.32.105  192.168.32.100  TCP        74 80 → 51358 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=525282 TSecr=2040959595 WS=64
   5 0.000257924   192.168.32.100  192.168.32.105  TCP        66 51358 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2040959595 TSecr=525282
   6 0.000314169   192.168.32.100  192.168.32.105  TCP        66 51358 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2040959595 TSecr=525282
  62 13.014109889  192.168.32.100  192.168.32.105  TCP        74 43164 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2040972609 TSecr=0 WS=128
  66 13.014179139  192.168.32.105  192.168.32.100  TCP        74 80 → 43164 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=526583 TSecr=2040972609 WS=64
  67 13.014183848  192.168.32.100  192.168.32.105  TCP        66 43164 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2040972609 TSecr=526583
  96 13.014818819  192.168.32.100  192.168.32.105  TCP        66 43164 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2040972610 TSecr=526583
2069 13.115326709  192.168.32.100  192.168.32.105  TCP        74 43168 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2040972710 TSecr=0 WS=128
2075 13.115390849  192.168.32.105  192.168.32.100  TCP        74 80 → 43168 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=526593 TSecr=2040972710 WS=64
2081 13.115432137  192.168.32.100  192.168.32.105  TCP        66 43168 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2040972710 TSecr=526593
2162 16.706104828  192.168.32.105  192.168.32.100  TCP        74 [TCP Retransmission] 80 → 43168 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=526953 TSecr=2040972710 WS=6
2163 16.706125005  192.168.32.100  192.168.32.105  TCP        66 [TCP Dup ACK 2081#1] 43168 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2040976301 TSecr=526593
2168 19.121842115  192.168.32.100  192.168.32.105  HTTP       84 GET / HTTP/1.0
2177 19.122011091  192.168.32.105  192.168.32.100  TCP        66 80 → 43168 [ACK] Seq=1 Ack=19 Win=5824 Len=0 TSval=527194 TSecr=2040978717
2254 19.138945934  192.168.32.105  192.168.32.100  HTTP     1152 HTTP/1.1 200 OK  (text/html)
2256 19.138953508  192.168.32.100  192.168.32.105  TCP        66 43168 → 80 [ACK] Seq=19 Ack=1087 Win=64128 Len=0 TSval=2040978734 TSecr=527196
2259 19.139188416  192.168.32.105  192.168.32.100  TCP        66 80 → 43168 [FIN, ACK] Seq=1087 Ack=19 Win=5824 Len=0 TSval=527196 TSecr=2040978734
2260 19.140871582  192.168.32.100  192.168.32.105  TCP        66 43168 → 80 [FIN, ACK] Seq=19 Ack=1088 Win=64128 Len=0 TSval=2040978736 TSecr=527196
2262 19.140990375  192.168.32.105  192.168.32.100  TCP        66 80 → 43168 [ACK] Seq=1088 Ack=20 Win=5824 Len=0 TSval=527196 TSecr=2040978736
```