NETWORK SECRUITY AND SCANNING

Lab Topology

- Attacker (Kali): 192.168.56.102
- Target (Metasploitable2): 192.168.56.101
- Management / Scanner (OpenVAS/Nessus): 192.168.56.103

All VMs are NAT/Host-only and isolated from any production network.

Methodology & Tools

Passive & Active Recon: nmap

Vulnerability Scanning: OpenVAS (GVM) and Nessus Essentials

Traffic Capture & Analysis: tcpdump, tshark, Wireshark

DoS Testing (Lab-only): hping3 (SYN flood)

Mitigation & Hardening: iptables, fail2ban

What is Nmap?

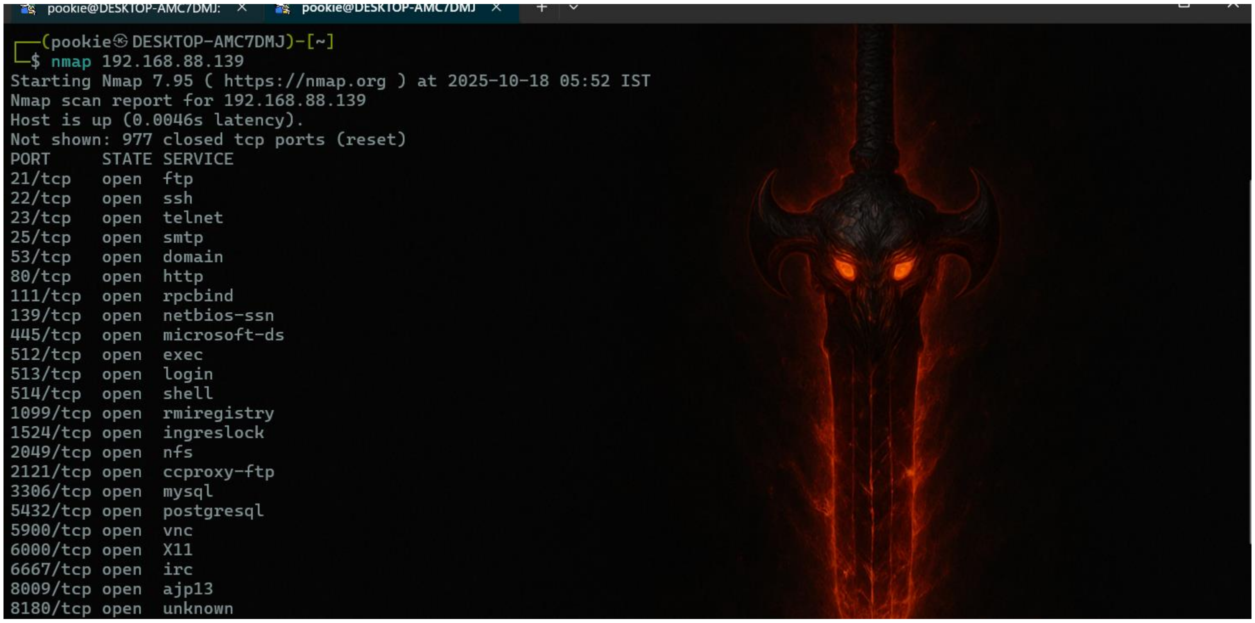
Nmap (Network MAPper) is a powerful open-source tool for discovering hosts, open ports, running services, and OS details on a network. It's used for reconnaissance, security assessments, and troubleshooting.

- **ARP scan (LAN only)** — find live hosts fast.
  ```
  arp-scan –localnet
  Nmap -sn –PA 10.10.10.10
  ```
- **TCP SYN (-sS)** — fast stealthy port discovery.
  ```
  nmap -sS -p1-1000 10.0.0.5
  ```
- **TCP Connect (-sT)** — full handshake if non-root.
  ```
  nmap -sT -p1-1024 target
  ```

- **UDP scan (-sU)** — find UDP services (slow).
  `nmap -sU -p53,161 target`
- **Idle (zombie) scan (-sI)** — stealth using a third host.
  `nmap -sI zombie_ip target`
- **Firewall probes (ACK/FIN/NULL/XMAS)** — test filtering behavior.
  `nmap -sA target` / `nmap -sF -sN -sX target`
- **Decoy / Spoofing** — obfuscate source IPs.
  `nmap -D decoy1,ME,decoy2 target`

  ```
  This actually nmap basic scan you just giving targat ip addres
  only in nmap it will default scan
  ```

  - `Nmap <target>`

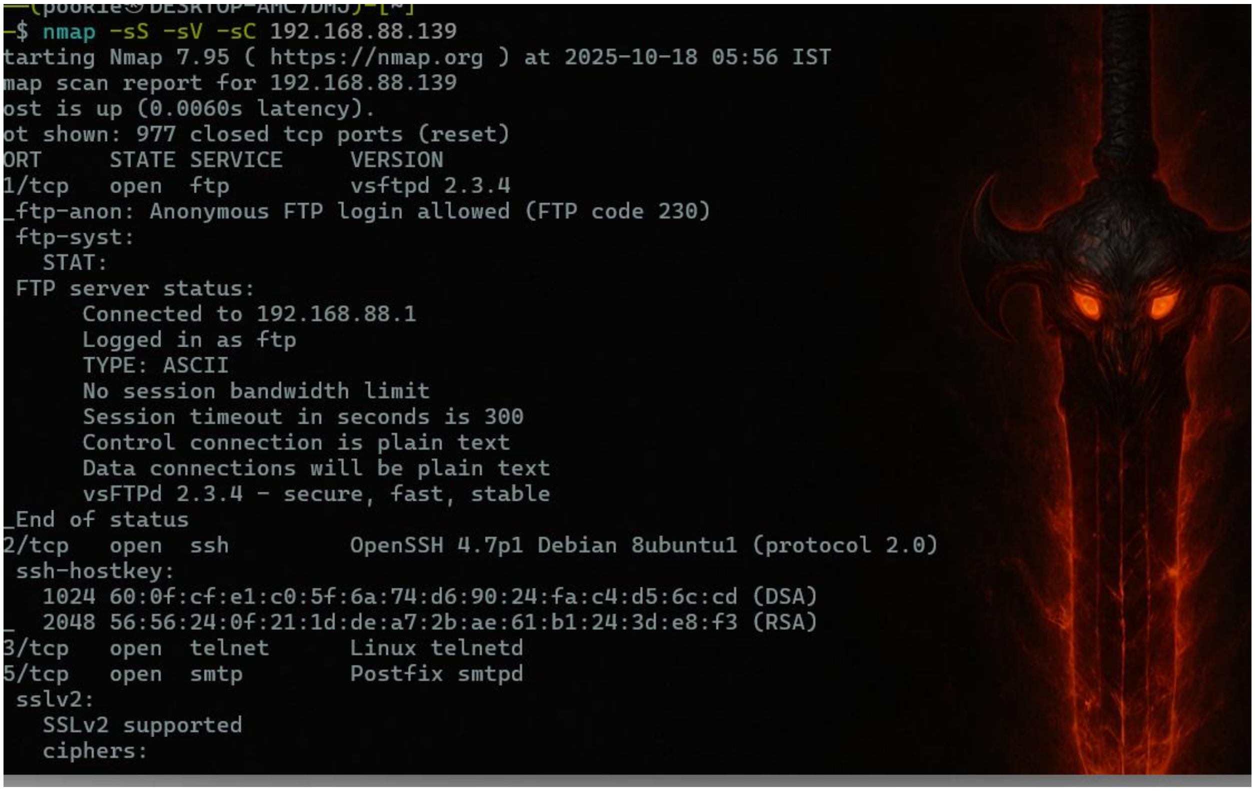


```
┌──(pookie㉿DESKTOP-AMC7DMJ)-[~]
└─$ nmap 192.168.88.139
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-18 05:52 IST
Nmap scan report for 192.168.88.139
Host is up (0.0046s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    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
```

Here different method to scan target to send -sS sealth scan send packet as sync and another is –sV is version scan is used to find open port sowftware running version

And –sC is default vuln script scannig it show is there any vulnerability related to available open ports

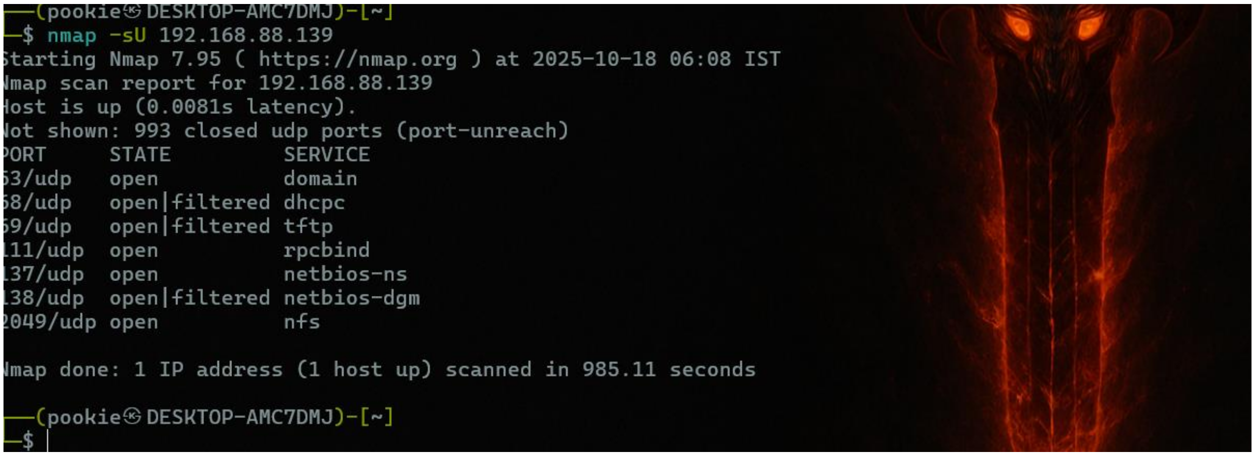
- **-sS**



```
──(pookie㉿DESKTOP-AMC7DMJ)-[~]
─$ nmap -sS -sV -sC 192.168.88.139
tarting Nmap 7.95 ( https://nmap.org ) at 2025-10-18 05:56 IST
map scan report for 192.168.88.139
ost is up (0.0060s latency).
ot shown: 977 closed tcp ports (reset)
ORT     STATE SERVICE     VERSION
1/tcp   open  ftp         vsftpd 2.3.4
_ftp-anon: Anonymous FTP login allowed (FTP code 230)
 ftp-syst:
   STAT:
 FTP server status:
      Connected to 192.168.88.1
      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
2/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
 ssh-hostkey:
   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
3/tcp   open  telnet      Linux telnetd
5/tcp   open  smtp        Postfix smtpd
 sslv2:
   SSLv2 supported
   ciphers:
```

Nmap –sU <target>

UDP scans are **slower** and less reliable than TCP (ICMP rate-limits, firewalls).



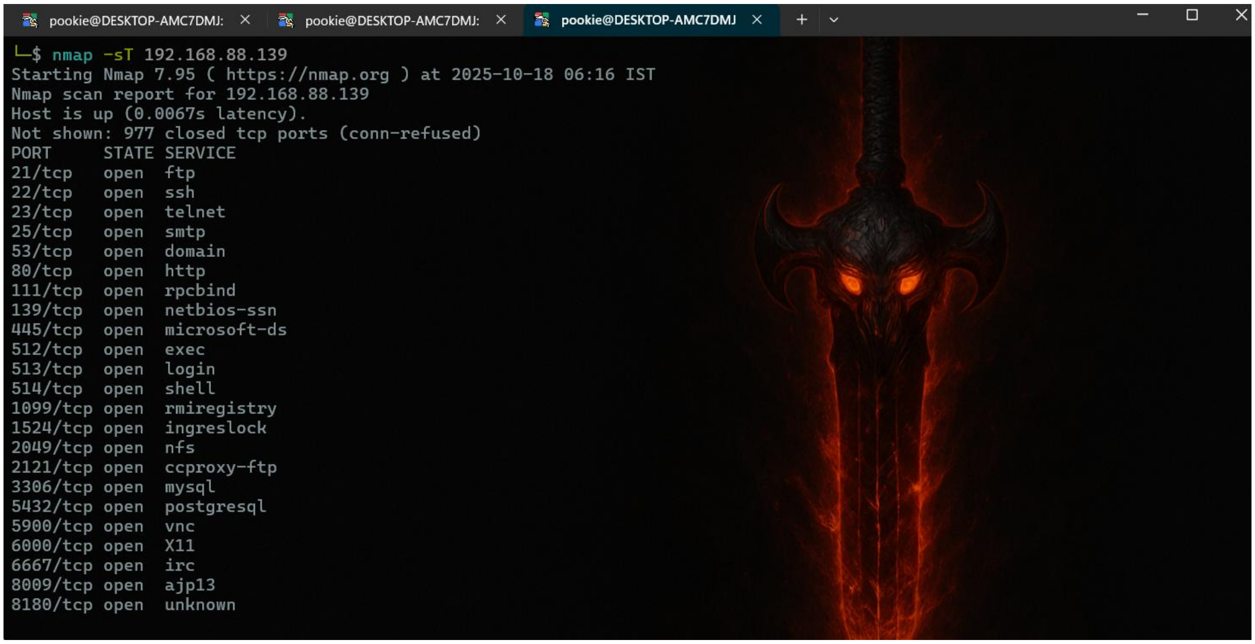
```
──(pookie㉿DESKTOP-AMC7DMJ)-[~]
─$ nmap -sU 192.168.88.139
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-18 06:08 IST
Nmap scan report for 192.168.88.139
Host is up (0.0081s latency).
Not shown: 993 closed udp ports (port-unreach)
PORT     STATE         SERVICE
53/udp   open          domain
68/udp   open|filtered dhcpc
69/udp   open|filtered tftp
111/udp  open          rpcbind
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
2049/udp open          nfs

Nmap done: 1 IP address (1 host up) scanned in 985.11 seconds

──(pookie㉿DESKTOP-AMC7DMJ)-[~]
─$ |
```

Namp –sT <target>

TCP connect scan that sends packet non root full handshake



```
└─$ nmap -sT 192.168.88.139
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-18 06:16 IST
Nmap scan report for 192.168.88.139
Host is up (0.0067s latency).
Not shown: 977 closed tcp ports (conn-refused)
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
```

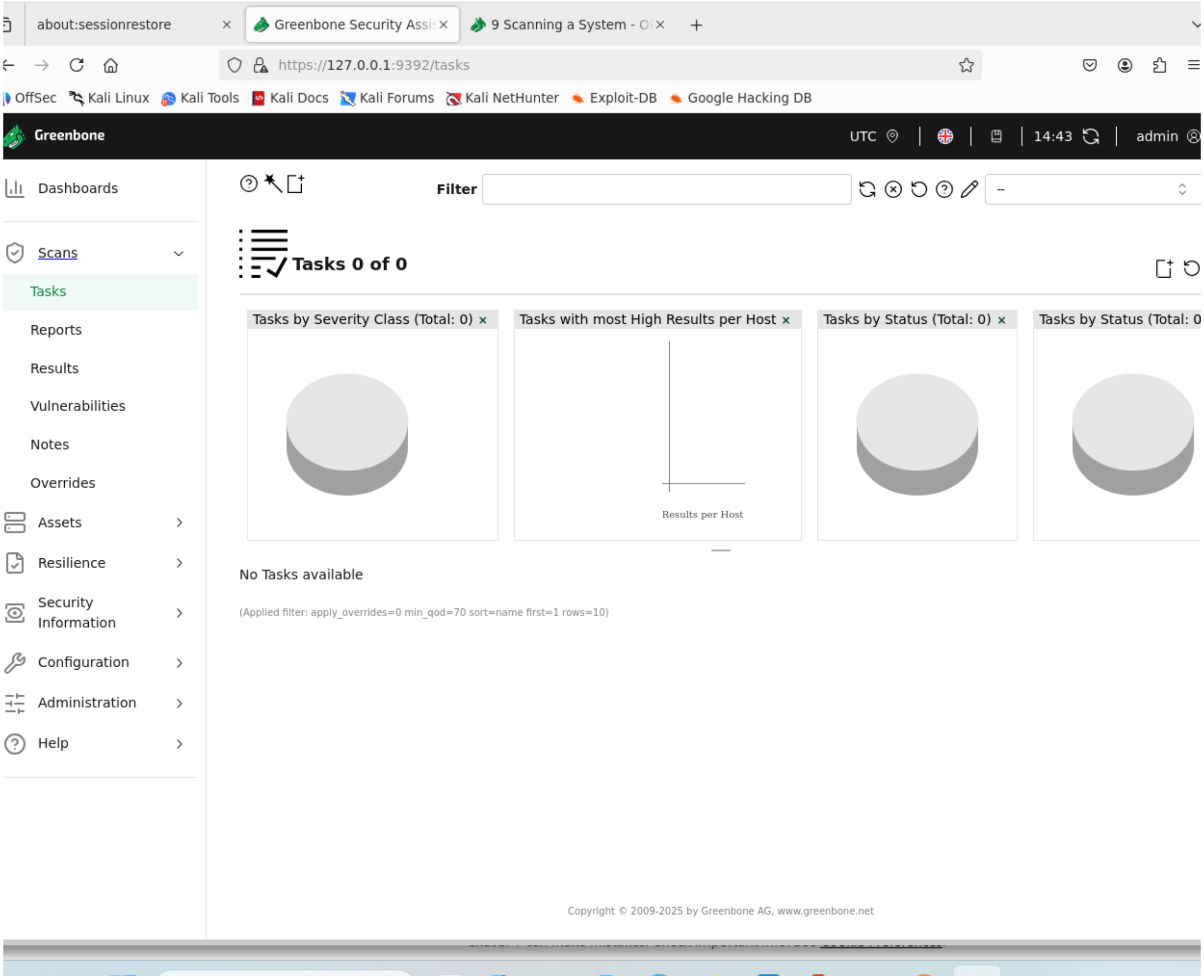
OpenVAS (now part of Greenbone Vulnerability Management / GVM is an open-source vulnerability scanner that discovers, checks and reports vulnerabilities on networked systems.

Key features (short)

- Network vulnerability checks thousands of NVT plugins
- Authenticated (credentialed) and unauthenticated scans.
- Scheduling, report export (PDF/HTML/CSV), and risk/CVSS scoring.
- Web UI API for automation.

Quick setup (very short)

- On Kali: `sudo gvm-setup` (initializes feeds and DB)
- Start: `sudo gvm-start`
- Web UI: open `https://<scanner-ip>:9392` and log in.



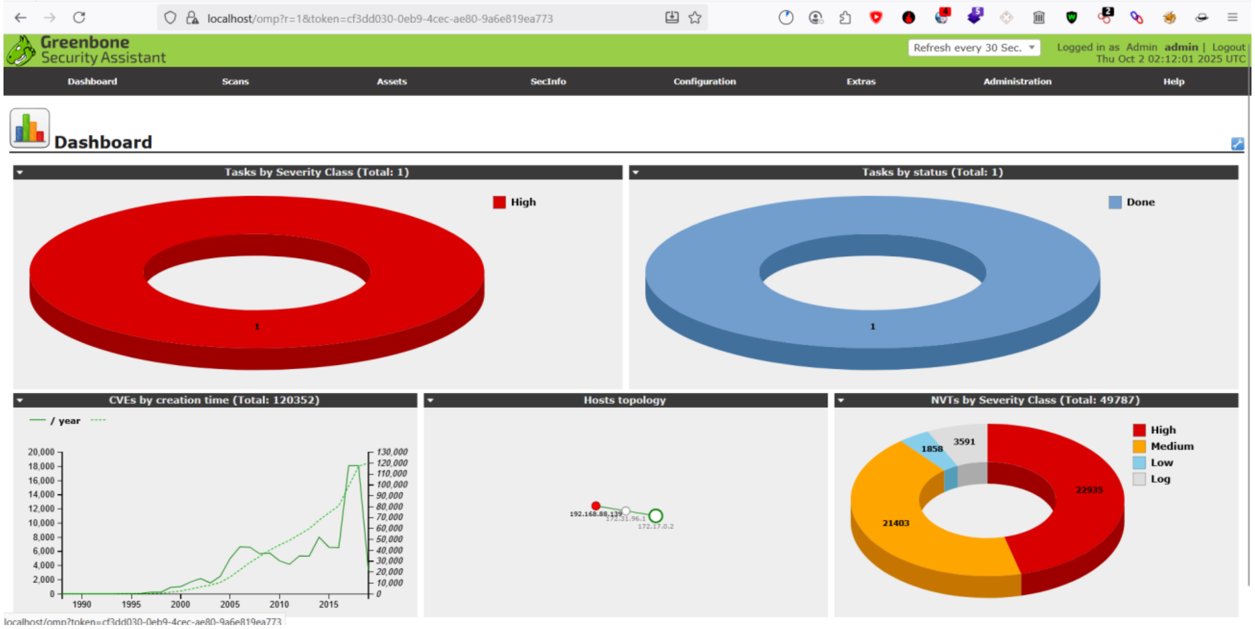
https://127.0.0.1:9392/tasks

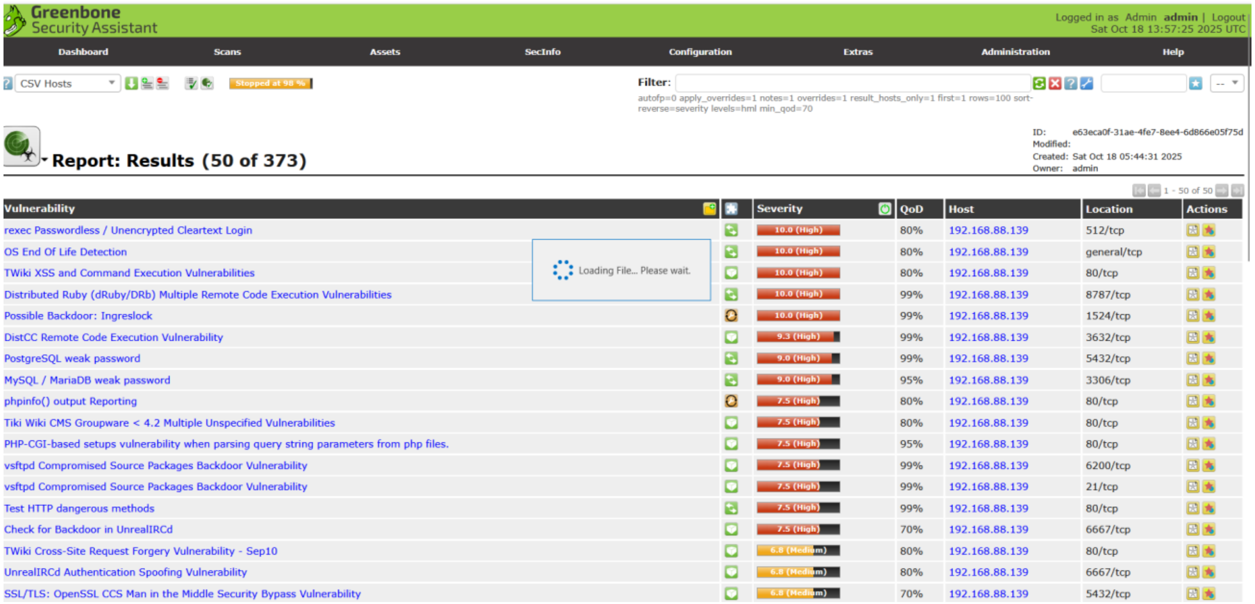
Tasks 0 of 0

No Tasks available

(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

Copyright © 2009-2025 by Greenbone AG, www.greenbone.net





Logged in as Admin admin | Logout
Sat Oct 18 13:57:25 2025 UTC

autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70

ID: e63eca0f-31ae-4fe7-8ee4-6d866e05f75d
Modified:
Created: Sat Oct 18 05:44:31 2025
Owner: admin

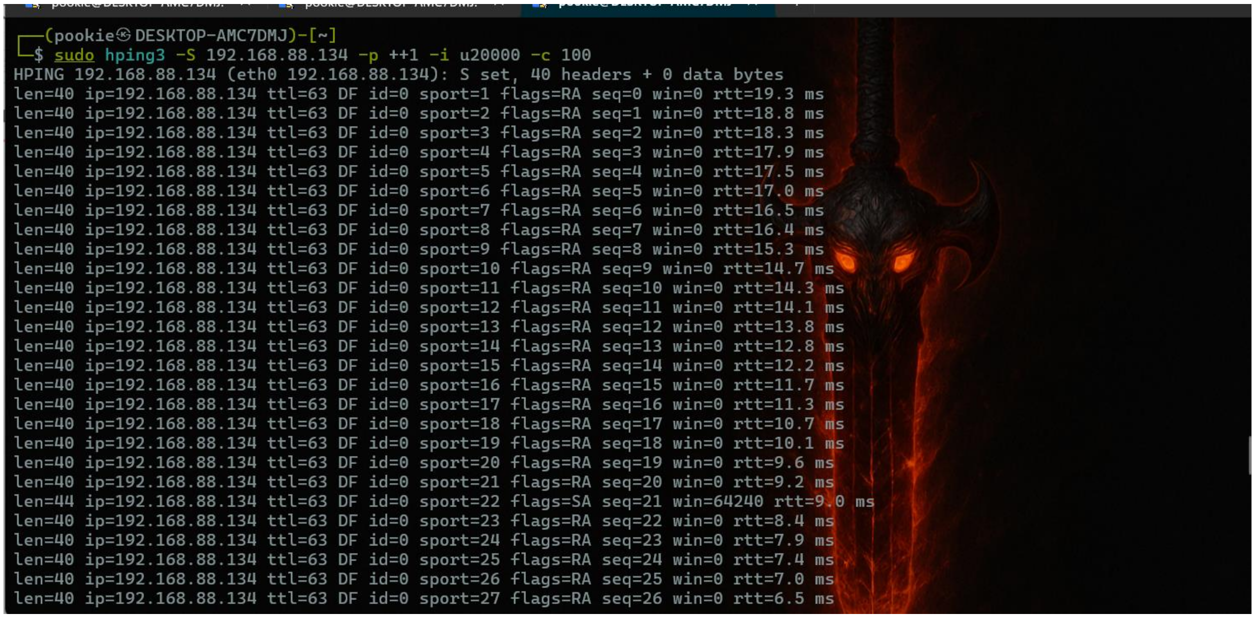
Report: Results (50 of 373)

Vulnerability		Severity	QoD	Host	Location	Actions
rexec Passwordless / Unencrypted Cleartext Login		10.0 (High)	80%	192.168.88.139	512/tcp	
OS End Of Life Detection		10.0 (High)	80%	192.168.88.139	general/tcp	
TWiki XSS and Command Execution Vulnerabilities		10.0 (High)	80%	192.168.88.139	80/tcp	
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities		10.0 (High)	99%	192.168.88.139	8787/tcp	
Possible Backdoor: Ingreslock		10.0 (High)	99%	192.168.88.139	1524/tcp	
DistCC Remote Code Execution Vulnerability		9.3 (High)	99%	192.168.88.139	3632/tcp	
PostgreSQL weak password		9.0 (High)	99%	192.168.88.139	5432/tcp	
MySQL / MariaDB weak password		9.0 (High)	95%	192.168.88.139	3306/tcp	
phpinfo() output Reporting		7.5 (High)	80%	192.168.88.139	80/tcp	
Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities		7.5 (High)	80%	192.168.88.139	80/tcp	
PHP-CGI-based setups vulnerability when parsing query string parameters from php files.		7.5 (High)	95%	192.168.88.139	80/tcp	
vsftpd Compromised Source Packages Backdoor Vulnerability		7.5 (High)	99%	192.168.88.139	6200/tcp	
vsftpd Compromised Source Packages Backdoor Vulnerability		7.5 (High)	99%	192.168.88.139	21/tcp	
Test HTTP dangerous methods		7.5 (High)	99%	192.168.88.139	80/tcp	
Check for Backdoor in UnrealIRCd		7.5 (High)	70%	192.168.88.139	6667/tcp	
TWiki Cross-Site Request Forgery Vulnerability - Sep10		6.8 (Medium)	80%	192.168.88.139	80/tcp	
UnrealIRCd Authentication Spoofing Vulnerability		6.8 (Medium)	80%	192.168.88.139	6667/tcp	
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability		6.8 (Medium)	70%	192.168.88.139	5432/tcp	

SYN Flood Analysis (lab-only)

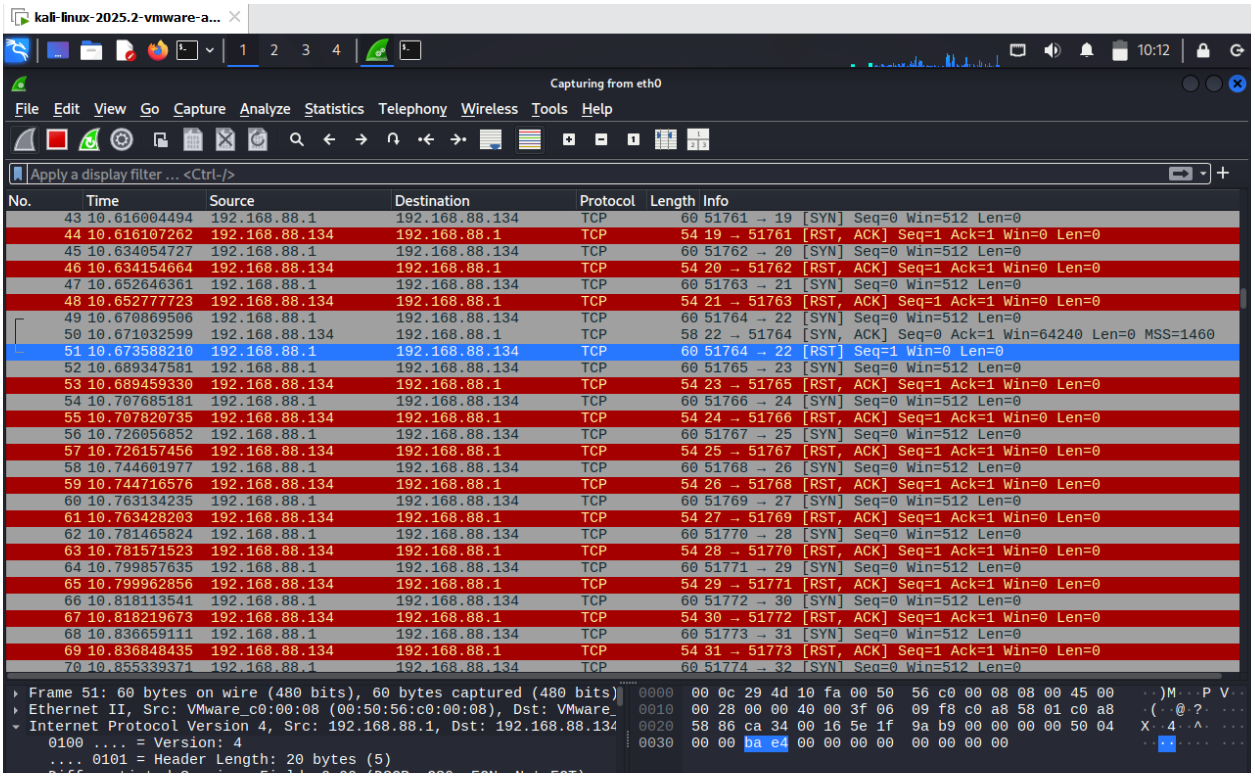
Command used (attacker):

```
sudo hping3 --flood -S -p 80 192.168.56.101
```



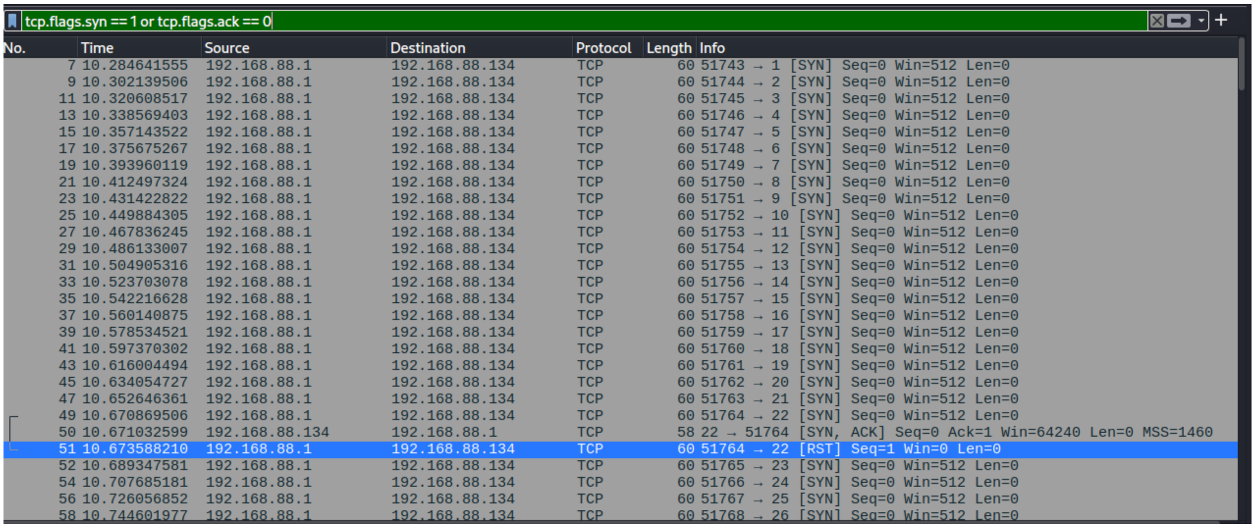
```
┌──(pookie㉿DESKTOP-AMC7DMJ)-[~]
└─$ sudo hping3 -S 192.168.88.134 -p ++1 -i u20000 -c 100
HPING 192.168.88.134 (eth0 192.168.88.134): S set, 40 headers + 0 data bytes
len=40 ip=192.168.88.134 ttl=63 DF id=0 sport=1 flags=RA seq=0 win=0 rtt=19.3 ms
len=40 ip=192.168.88.134 ttl=63 DF id=0 sport=2 flags=RA seq=1 win=0 rtt=18.8 ms
len=40 ip=192.168.88.134 ttl=63 DF id=0 sport=3 flags=RA seq=2 win=0 rtt=18.3 ms
len=40 ip=192.168.88.134 ttl=63 DF id=0 sport=4 flags=RA seq=3 win=0 rtt=17.9 ms
len=40 ip=192.168.88.134 ttl=63 DF id=0 sport=5 flags=RA seq=4 win=0 rtt=17.5 ms
len=40 ip=192.168.88.134 ttl=63 DF id=0 sport=6 flags=RA seq=5 win=0 rtt=17.0 ms
len=40 ip=192.168.88.134 ttl=63 DF id=0 sport=7 flags=RA seq=6 win=0 rtt=16.5 ms
len=40 ip=192.168.88.134 ttl=63 DF id=0 sport=8 flags=RA seq=7 win=0 rtt=16.4 ms
len=40 ip=192.168.88.134 ttl=63 DF id=0 sport=9 flags=RA seq=8 win=0 rtt=15.3 ms
len=40 ip=192.168.88.134 ttl=63 DF id=0 sport=10 flags=RA seq=9 win=0 rtt=14.7 ms
len=40 ip=192.168.88.134 ttl=63 DF id=0 sport=11 flags=RA seq=10 win=0 rtt=14.3 ms
len=40 ip=192.168.88.134 ttl=63 DF id=0 sport=12 flags=RA seq=11 win=0 rtt=14.1 ms
len=40 ip=192.168.88.134 ttl=63 DF id=0 sport=13 flags=RA seq=12 win=0 rtt=13.8 ms
len=40 ip=192.168.88.134 ttl=63 DF id=0 sport=14 flags=RA seq=13 win=0 rtt=12.8 ms
len=40 ip=192.168.88.134 ttl=63 DF id=0 sport=15 flags=RA seq=14 win=0 rtt=12.2 ms
len=40 ip=192.168.88.134 ttl=63 DF id=0 sport=16 flags=RA seq=15 win=0 rtt=11.7 ms
len=40 ip=192.168.88.134 ttl=63 DF id=0 sport=17 flags=RA seq=16 win=0 rtt=11.3 ms
len=40 ip=192.168.88.134 ttl=63 DF id=0 sport=18 flags=RA seq=17 win=0 rtt=10.7 ms
len=40 ip=192.168.88.134 ttl=63 DF id=0 sport=19 flags=RA seq=18 win=0 rtt=10.1 ms
len=40 ip=192.168.88.134 ttl=63 DF id=0 sport=20 flags=RA seq=19 win=0 rtt=9.6 ms
len=40 ip=192.168.88.134 ttl=63 DF id=0 sport=21 flags=RA seq=20 win=0 rtt=9.2 ms
len=44 ip=192.168.88.134 ttl=63 DF id=0 sport=22 flags=SA seq=21 win=64240 rtt=9.0 ms
len=40 ip=192.168.88.134 ttl=63 DF id=0 sport=23 flags=RA seq=22 win=0 rtt=8.4 ms
len=40 ip=192.168.88.134 ttl=63 DF id=0 sport=24 flags=RA seq=23 win=0 rtt=7.9 ms
len=40 ip=192.168.88.134 ttl=63 DF id=0 sport=25 flags=RA seq=24 win=0 rtt=7.4 ms
len=40 ip=192.168.88.134 ttl=63 DF id=0 sport=26 flags=RA seq=25 win=0 rtt=7.0 ms
len=40 ip=192.168.88.134 ttl=63 DF id=0 sport=27 flags=RA seq=26 win=0 rtt=6.5 ms
```

Capture: `pcaps/synflood.pcap` — analyze via Wireshark using filter `tcp.flags.syn == 1 && tcp.flags.ack == 0`.

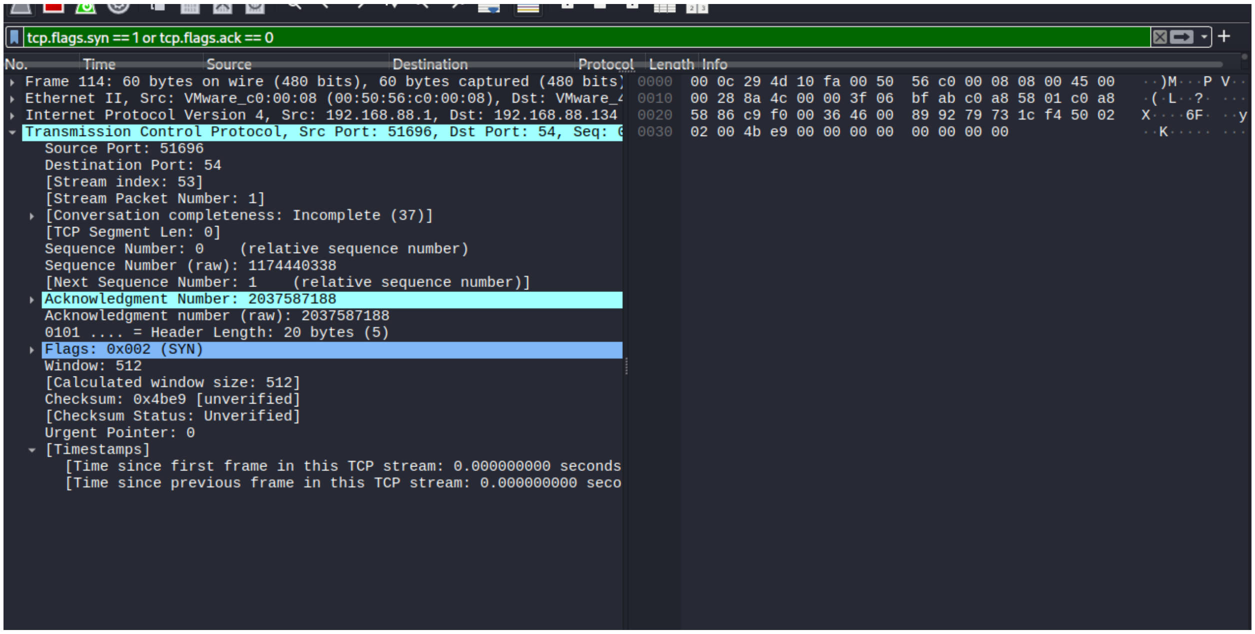


```
No.   Time          Source          Destination     Protocol Length Info
   43 10.616004494  192.168.88.1    192.168.88.134  TCP      60 51761 → 19 [SYN] Seq=0 Win=512 Len=0
   44 10.616107262  192.168.88.134  192.168.88.1    TCP      54 19 → 51761 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   45 10.634054727  192.168.88.1    192.168.88.134  TCP      60 51762 → 20 [SYN] Seq=0 Win=512 Len=0
   46 10.634154664  192.168.88.134  192.168.88.1    TCP      54 20 → 51762 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   47 10.652646361  192.168.88.1    192.168.88.134  TCP      60 51763 → 21 [SYN] Seq=0 Win=512 Len=0
   48 10.652777723  192.168.88.134  192.168.88.1    TCP      54 21 → 51763 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   49 10.670869506  192.168.88.1    192.168.88.134  TCP      60 51764 → 22 [SYN] Seq=0 Win=512 Len=0
   50 10.671032599  192.168.88.134  192.168.88.1    TCP      58 22 → 51764 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
   51 10.673588210  192.168.88.1    192.168.88.134  TCP      60 51764 → 22 [RST] Seq=1 Win=0 Len=0
   52 10.689347581  192.168.88.1    192.168.88.134  TCP      60 51765 → 23 [SYN] Seq=0 Win=512 Len=0
   53 10.689459330  192.168.88.134  192.168.88.1    TCP      54 23 → 51765 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   54 10.707685181  192.168.88.1    192.168.88.134  TCP      60 51766 → 24 [SYN] Seq=0 Win=512 Len=0
   55 10.707820735  192.168.88.134  192.168.88.1    TCP      54 24 → 51766 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   56 10.726056852  192.168.88.1    192.168.88.134  TCP      60 51767 → 25 [SYN] Seq=0 Win=512 Len=0
   57 10.726157456  192.168.88.134  192.168.88.1    TCP      54 25 → 51767 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   58 10.744601977  192.168.88.1    192.168.88.134  TCP      60 51768 → 26 [SYN] Seq=0 Win=512 Len=0
   59 10.744716576  192.168.88.134  192.168.88.1    TCP      54 26 → 51768 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   60 10.763134235  192.168.88.1    192.168.88.134  TCP      60 51769 → 27 [SYN] Seq=0 Win=512 Len=0
   61 10.763428203  192.168.88.134  192.168.88.1    TCP      54 27 → 51769 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   62 10.781465824  192.168.88.1    192.168.88.134  TCP      60 51770 → 28 [SYN] Seq=0 Win=512 Len=0
   63 10.781571523  192.168.88.134  192.168.88.1    TCP      54 28 → 51770 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   64 10.799857635  192.168.88.1    192.168.88.134  TCP      60 51771 → 29 [SYN] Seq=0 Win=512 Len=0
   65 10.799962856  192.168.88.134  192.168.88.1    TCP      54 29 → 51771 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   66 10.818113541  192.168.88.1    192.168.88.134  TCP      60 51772 → 30 [SYN] Seq=0 Win=512 Len=0
   67 10.818219673  192.168.88.134  192.168.88.1    TCP      54 30 → 51772 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   68 10.836659111  192.168.88.1    192.168.88.134  TCP      60 51773 → 31 [SYN] Seq=0 Win=512 Len=0
   69 10.836848435  192.168.88.134  192.168.88.1    TCP      54 31 → 51773 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   70 10.855339371  192.168.88.1    192.168.88.134  TCP      60 51774 → 32 [SYN] Seq=0 Win=512 Len=0
```

```
› Frame 51: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)   0000  00 0c 29 4d 10 fa 00 50  56 c0 00 08 08 00 45 00   ··)M···P V·····E·
› Ethernet II, Src: VMware_c0:00:08 (00:50:56:c0:00:08), Dst: VMware_   0010  00 28 00 00 40 00 3f 06  09 f8 c0 a8 58 01 c0 a8   ·(··@·?· ····X···
⌄ Internet Protocol Version 4, Src: 192.168.88.1, Dst: 192.168.88.134   0020  58 86 ca 34 00 16 5e 1f  9a b9 00 00 00 00 50 04   X··4··^· ······P·
    0100 .... = Version: 4                                                0030  00 00 ba e4 00 00 00 00  00 00 00 00               ········ ····
    .... 0101 = Header Length: 20 bytes (5)
```



```
tcp.flags.syn == 1 or tcp.flags.ack == 0
No.   Time         Source           Destination      Protocol Length Info
    7 10.284641555 192.168.88.1     192.168.88.134   TCP      60 51743 → 1 [SYN] Seq=0 Win=512 Len=0
    9 10.302139506 192.168.88.1     192.168.88.134   TCP      60 51744 → 2 [SYN] Seq=0 Win=512 Len=0
   11 10.320608517 192.168.88.1     192.168.88.134   TCP      60 51745 → 3 [SYN] Seq=0 Win=512 Len=0
   13 10.338569403 192.168.88.1     192.168.88.134   TCP      60 51746 → 4 [SYN] Seq=0 Win=512 Len=0
   15 10.357143522 192.168.88.1     192.168.88.134   TCP      60 51747 → 5 [SYN] Seq=0 Win=512 Len=0
   17 10.375675267 192.168.88.1     192.168.88.134   TCP      60 51748 → 6 [SYN] Seq=0 Win=512 Len=0
   19 10.393960119 192.168.88.1     192.168.88.134   TCP      60 51749 → 7 [SYN] Seq=0 Win=512 Len=0
   21 10.412497324 192.168.88.1     192.168.88.134   TCP      60 51750 → 8 [SYN] Seq=0 Win=512 Len=0
   23 10.431422822 192.168.88.1     192.168.88.134   TCP      60 51751 → 9 [SYN] Seq=0 Win=512 Len=0
   25 10.449884305 192.168.88.1     192.168.88.134   TCP      60 51752 → 10 [SYN] Seq=0 Win=512 Len=0
   27 10.467836245 192.168.88.1     192.168.88.134   TCP      60 51753 → 11 [SYN] Seq=0 Win=512 Len=0
   29 10.486133007 192.168.88.1     192.168.88.134   TCP      60 51754 → 12 [SYN] Seq=0 Win=512 Len=0
   31 10.504905316 192.168.88.1     192.168.88.134   TCP      60 51755 → 13 [SYN] Seq=0 Win=512 Len=0
   33 10.523703078 192.168.88.1     192.168.88.134   TCP      60 51756 → 14 [SYN] Seq=0 Win=512 Len=0
   35 10.542216628 192.168.88.1     192.168.88.134   TCP      60 51757 → 15 [SYN] Seq=0 Win=512 Len=0
   37 10.560140875 192.168.88.1     192.168.88.134   TCP      60 51758 → 16 [SYN] Seq=0 Win=512 Len=0
   39 10.578534521 192.168.88.1     192.168.88.134   TCP      60 51759 → 17 [SYN] Seq=0 Win=512 Len=0
   41 10.597370302 192.168.88.1     192.168.88.134   TCP      60 51760 → 18 [SYN] Seq=0 Win=512 Len=0
   43 10.616004494 192.168.88.1     192.168.88.134   TCP      60 51761 → 19 [SYN] Seq=0 Win=512 Len=0
   45 10.634054727 192.168.88.1     192.168.88.134   TCP      60 51762 → 20 [SYN] Seq=0 Win=512 Len=0
   47 10.652646361 192.168.88.1     192.168.88.134   TCP      60 51763 → 21 [SYN] Seq=0 Win=512 Len=0
   49 10.670869506 192.168.88.1     192.168.88.134   TCP      60 51764 → 22 [SYN] Seq=0 Win=512 Len=0
   50 10.671032599 192.168.88.134   192.168.88.1     TCP      58 22 → 51764 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
   51 10.673588210 192.168.88.1     192.168.88.134   TCP      60 51764 → 22 [RST] Seq=1 Win=0 Len=0
   52 10.689347581 192.168.88.1     192.168.88.134   TCP      60 51765 → 23 [SYN] Seq=0 Win=512 Len=0
   54 10.707685181 192.168.88.1     192.168.88.134   TCP      60 51766 → 24 [SYN] Seq=0 Win=512 Len=0
   56 10.726056852 192.168.88.1     192.168.88.134   TCP      60 51767 → 25 [SYN] Seq=0 Win=512 Len=0
   58 10.744601977 192.168.88.1     192.168.88.134   TCP      60 51768 → 26 [SYN] Seq=0 Win=512 Len=0
```



```
tcp.flags.syn == 1 or tcp.flags.ack == 0
No.   Time   Source   Destination   Protocol   Length   Info
› Frame 114: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)   0000  00 0c 29 4d 10 fa 00 50  56 c0 00 08 08 00 45 00   ··)M···P V···
› Ethernet II, Src: VMware_c0:00:08 (00:50:56:c0:00:08), Dst: VMware_4   0010  00 28 8a 4c 00 00 3f 06  bf ab c0 a8 58 01 c0 a8   ·(·L··?· ····
› Internet Protocol Version 4, Src: 192.168.88.1, Dst: 192.168.88.134    0020  58 86 c9 f0 00 36 46 00  89 92 79 73 1c f4 50 02   X····6F· ···y
⌄ Transmission Control Protocol, Src Port: 51696, Dst Port: 54, Seq: 0  0030  02 00 4b e9 00 00 00 00  00 00 00 00               ··K····· ····
    Source Port: 51696
    Destination Port: 54
    [Stream index: 53]
    [Stream Packet Number: 1]
  › [Conversation completeness: Incomplete (37)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 1174440338
    [Next Sequence Number: 1    (relative sequence number)]
  › Acknowledgment Number: 2037587188
    Acknowledgment number (raw): 2037587188
    0101 .... = Header Length: 20 bytes (5)
  › Flags: 0x002 (SYN)
    Window: 512
    [Calculated window size: 512]
    Checksum: 0x4be9 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ⌄ [Timestamps]
      [Time since first frame in this TCP stream: 0.000000000 seconds
      [Time since previous frame in this TCP stream: 0.000000000 seco
```

Mitigation demo: On the target, add iptables rate limiting and `conntrack` rules; show restored service after applying rules.

Firewall & Hardening (iptables examples)

A safe minimal ruleset (saved as `scripts/iptables_rules.sh`) is provided. Key snippets:

# default-deny inbound, allow established

```
iptables -P INPUT DROP
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -p tcp --dport 22 -m conntrack --ctstate NEW -j ACCEPT
iptables -A INPUT -p tcp --dport 80 -m conntrack --ctstate NEW -j ACCEPT
```

Block a scanner IP:

```
iptables -I INPUT -s <scanner-ip> -j DROP
```

Detect & mitigate portscan attempts using recent module: