IPS/IDS Evasion Techniques

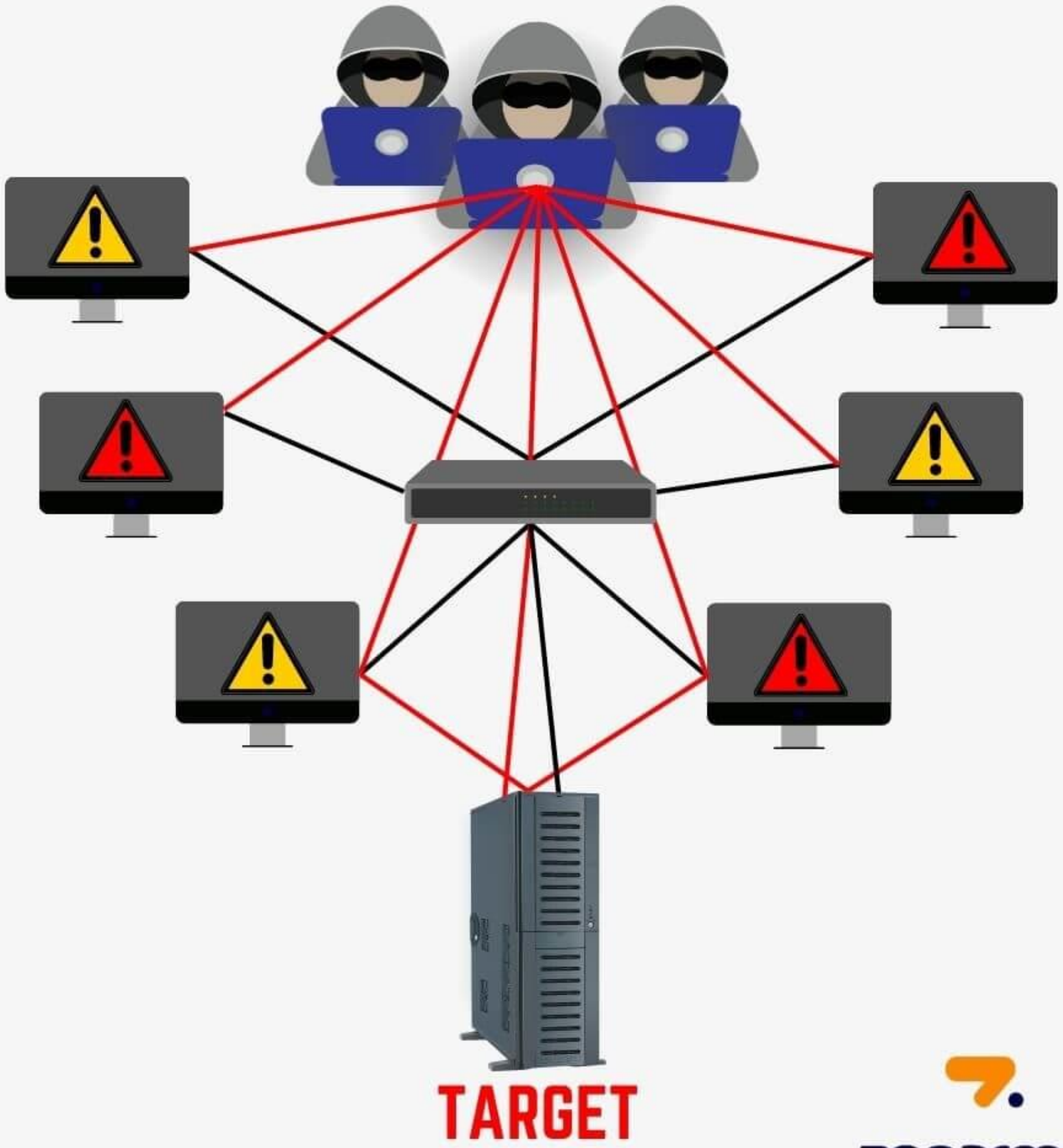
Miroslav Todorović

Agenda

- Network Intrusion
- IDS/IPS
- Network Attacks
- IDS/IPS Evasion Techniques
- Prototype
- Testing

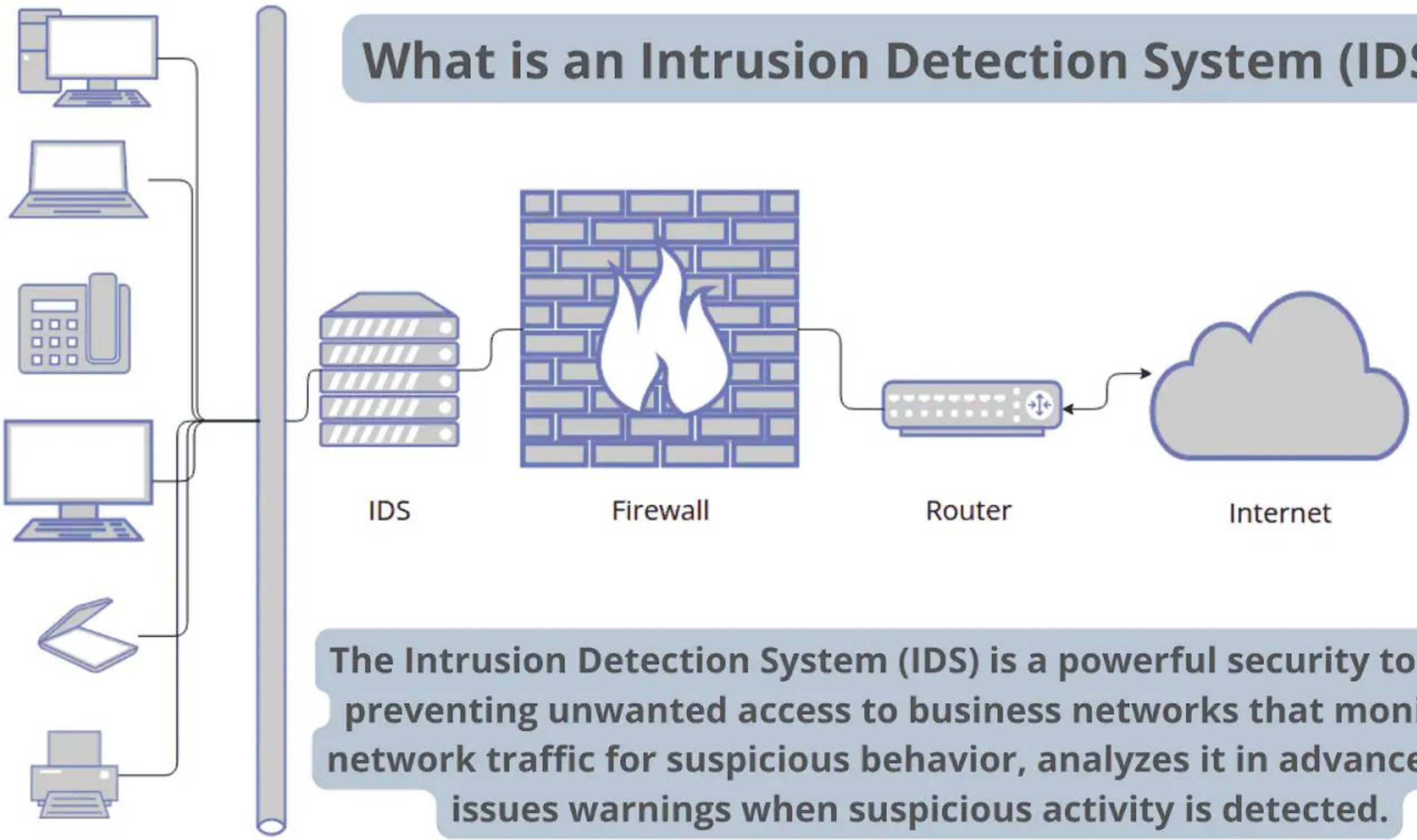
What is Network Intrusion?

A network intrusion is any illegal activity carried out on a digital network. Network incursions frequently entail the theft of valuable network resources and virtually always compromise a network security and/or data security.



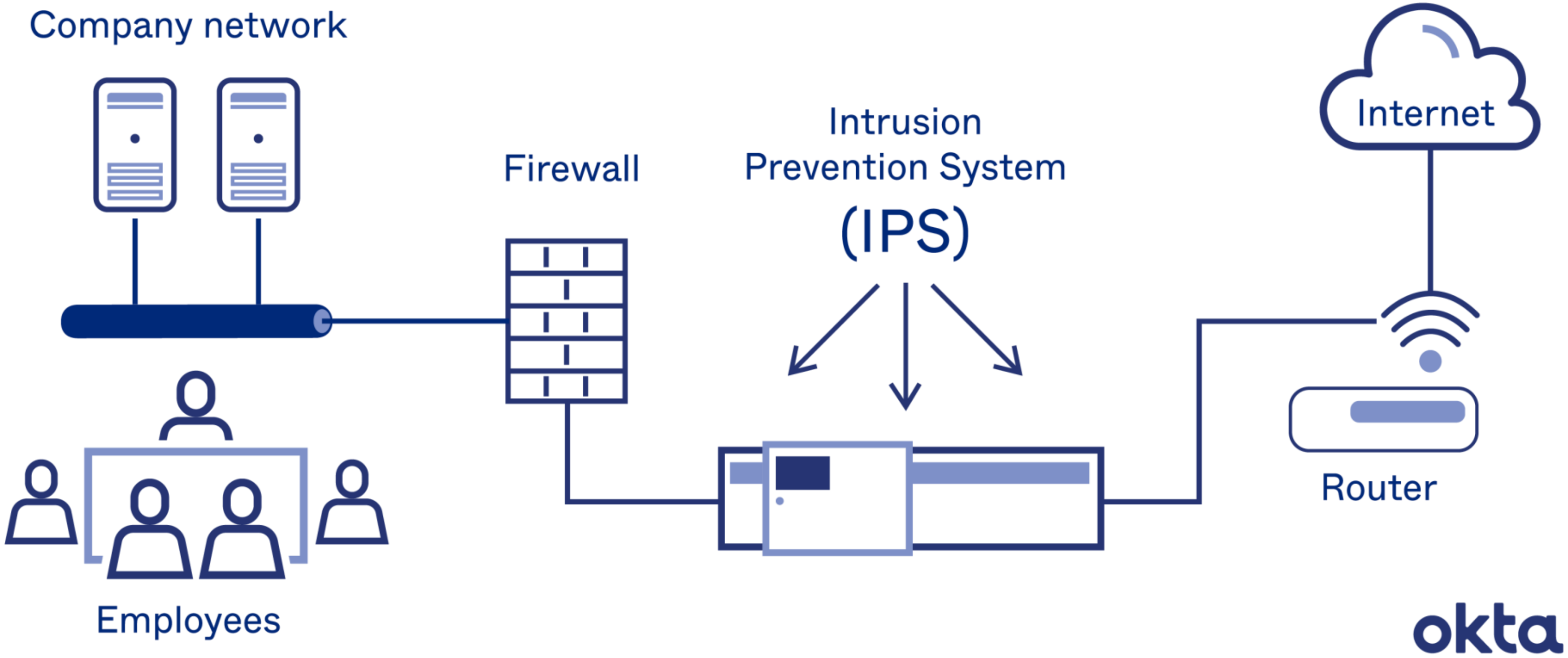
zenarmor

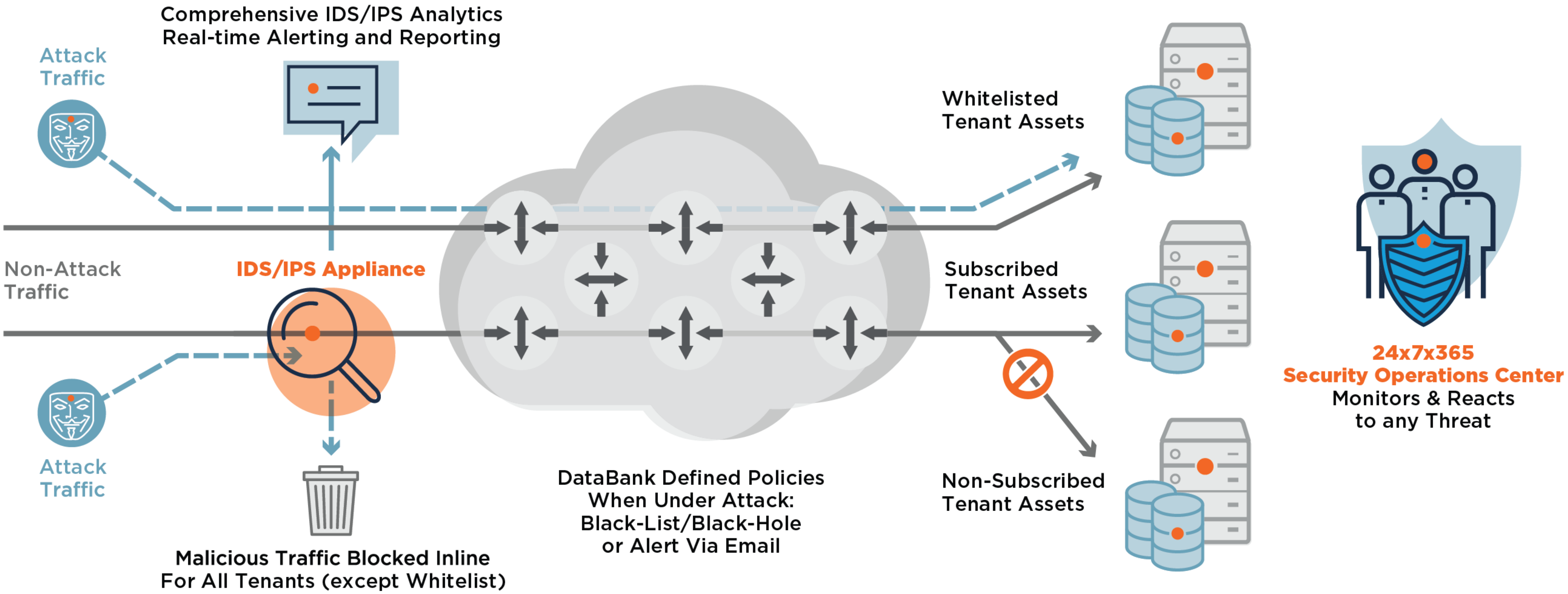
What is an Intrusion Detection System (IDS)?



The Intrusion Detection System (IDS) is a powerful security tool for preventing unwanted access to business networks that monitors network traffic for suspicious behavior, analyzes it in advance, and issues warnings when suspicious activity is detected.

Intrusion Prevention Systems



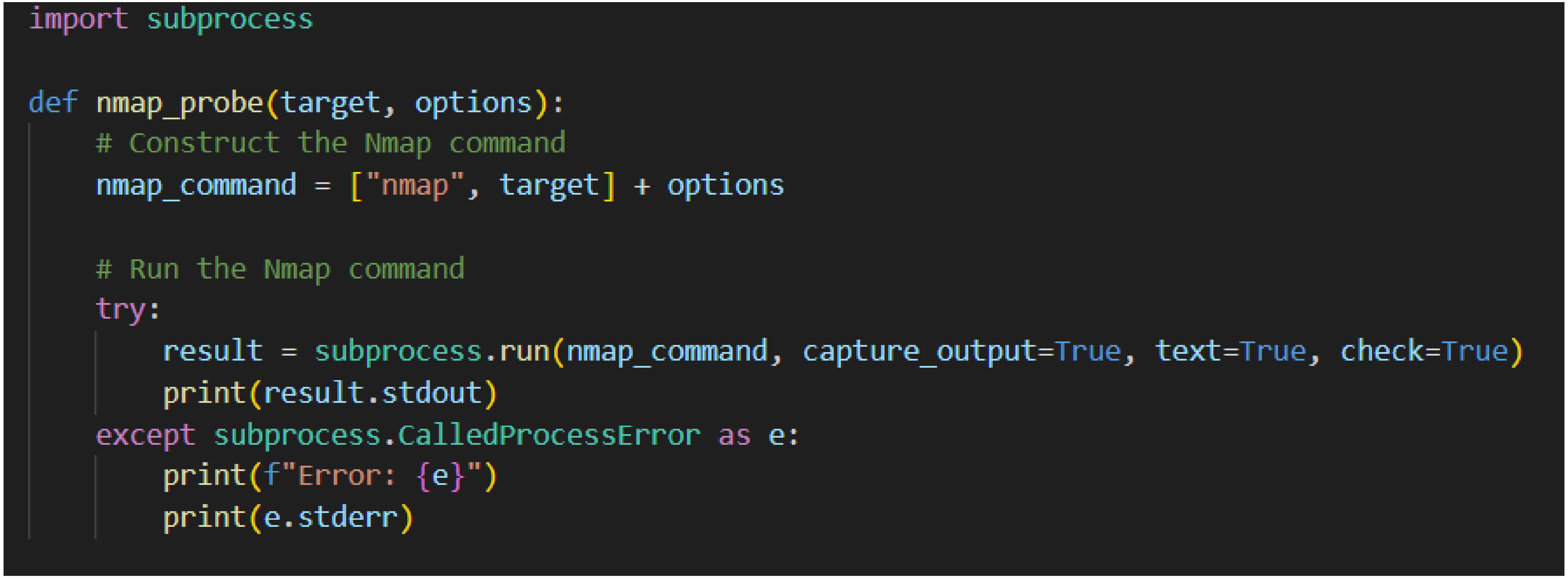
Comprehensive IDS/IPS Analytics
Real-time Alerting and Reporting
Attack Traffic
Non-Attack Traffic
IDS/IPS Appliance
Attack Traffic
Malicious Traffic Blocked Inline
For All Tenants (except Whitelist)
DataBank Defined Policies
When Under Attack:
Black-List/Black-Hole
or Alert Via Email
Whitelisted Tenant Assets
Subscribed Tenant Assets
Non-Subscribed Tenant Assets
24x7x365
Security Operations Center
Monitors & Reacts
to any Threat

IDS/IPS Evasion Techniques

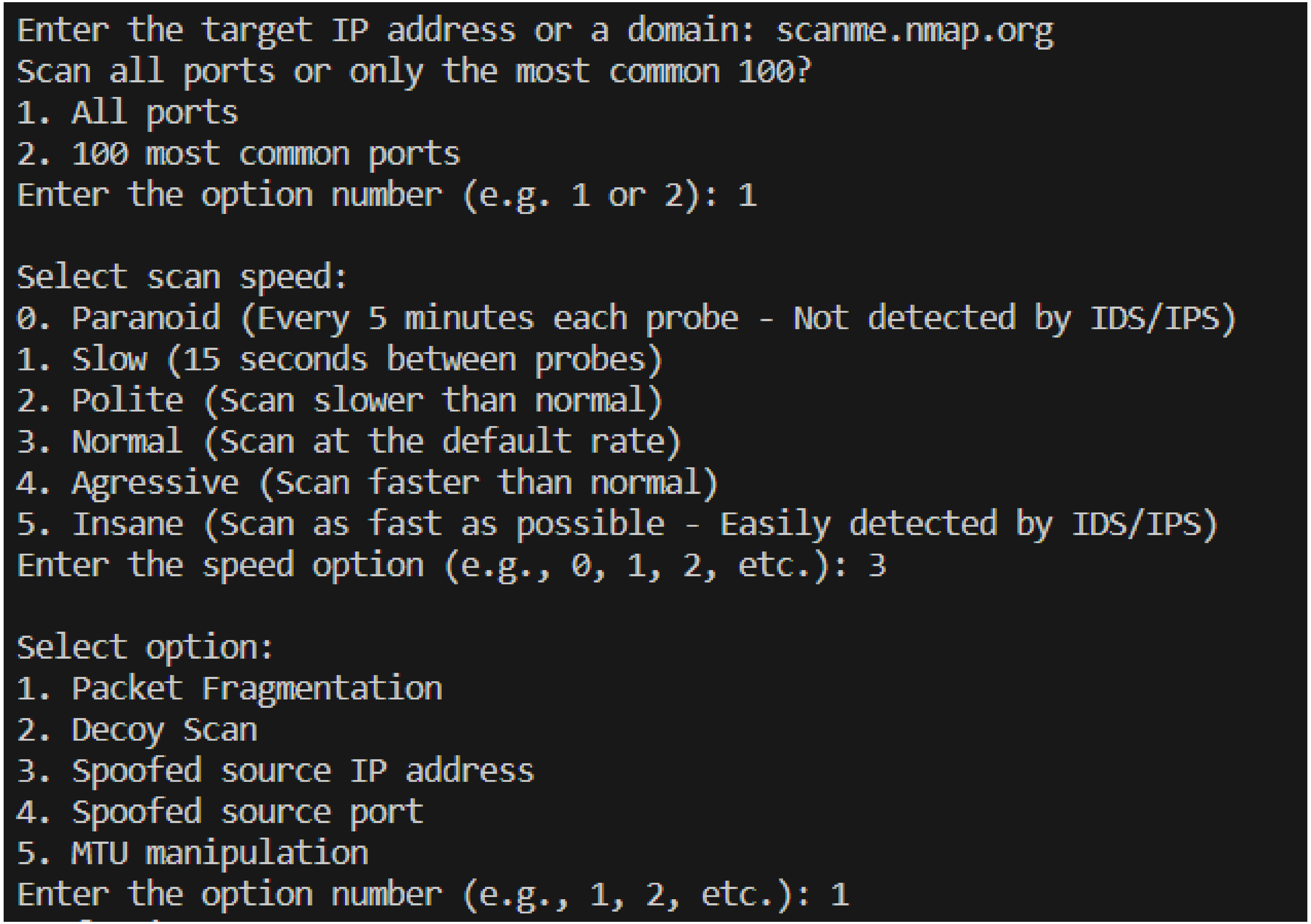
- **Packet Fragmentation**
- **SYN/FIN Scanning using IP Fragments**
- **Source Port Manipulation**
- **IP Address Decoy**
- **Spoofing the IP Address**
- **Sending the Bad Checksums**

Prototype

- Nmap 7.94 + Python

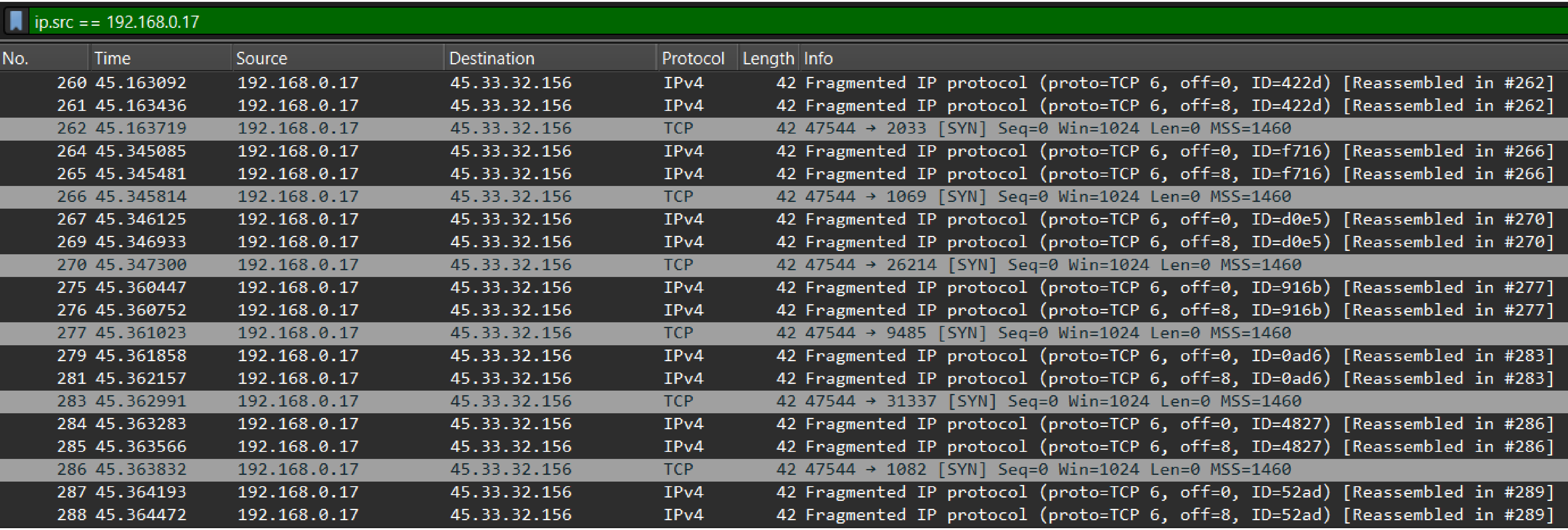


```python
import subprocess

def nmap_probe(target, options):
    # Construct the Nmap command
    nmap_command = ["nmap", target] + options

    # Run the Nmap command
    try:
        result = subprocess.run(nmap_command, capture_output=True, text=True, check=True)
        print(result.stdout)
    except subprocess.CalledProcessError as e:
        print(f"Error: {e}")
        print(e.stderr)
```



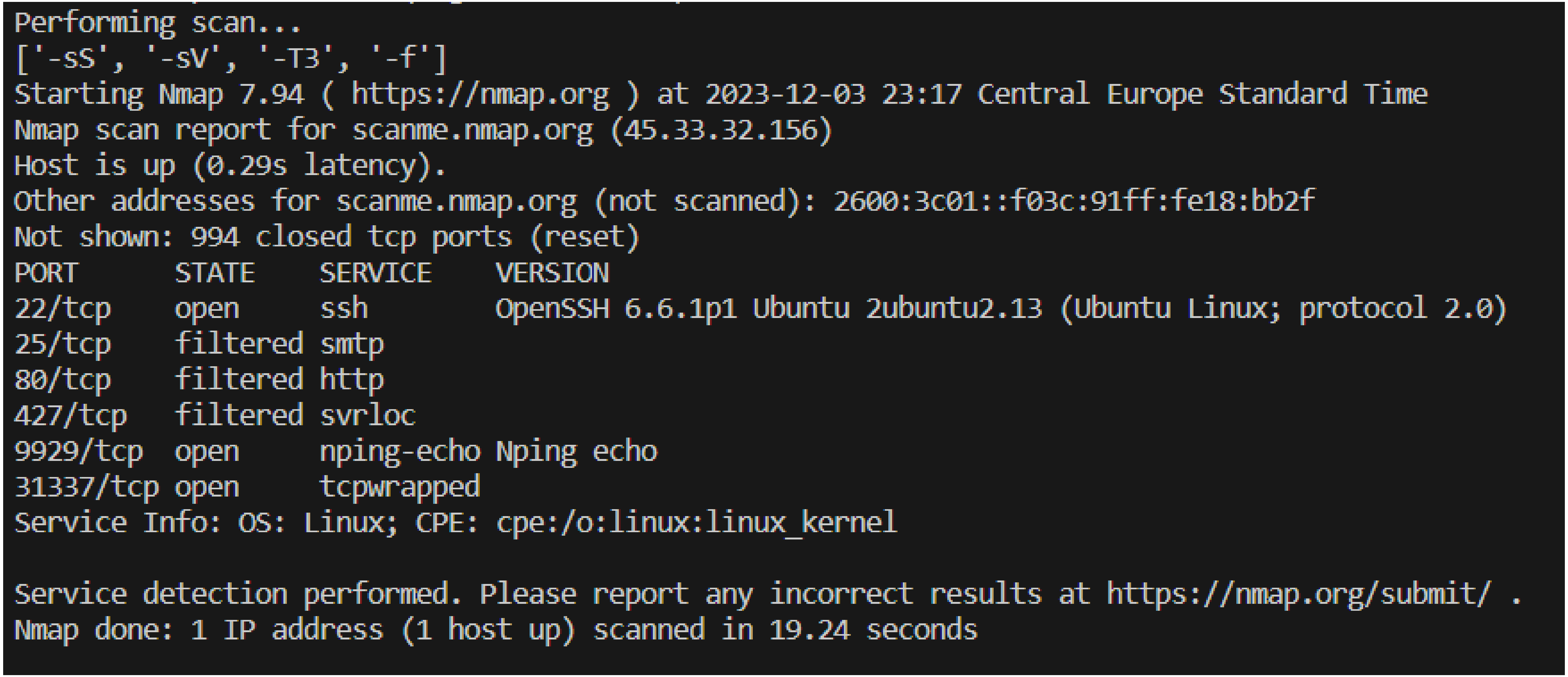
```
Enter the target IP address or a domain: scanme.nmap.org
Scan all ports or only the most common 100?
1. All ports
2. 100 most common ports
Enter the option number (e.g. 1 or 2): 1

Select scan speed:
0. Paranoid (Every 5 minutes each probe - Not detected by IDS/IPS)
1. Slow (15 seconds between probes)
2. Polite (Scan slower than normal)
3. Normal (Scan at the default rate)
4. Agressive (Scan faster than normal)
5. Insane (Scan as fast as possible - Easily detected by IDS/IPS)
Enter the speed option (e.g., 0, 1, 2, etc.): 3

Select option:
1. Packet Fragmentation
2. Decoy Scan
3. Spoofed source IP address
4. Spoofed source port
5. MTU manipulation
Enter the option number (e.g., 1, 2, etc.): 1
```

Fragmentation



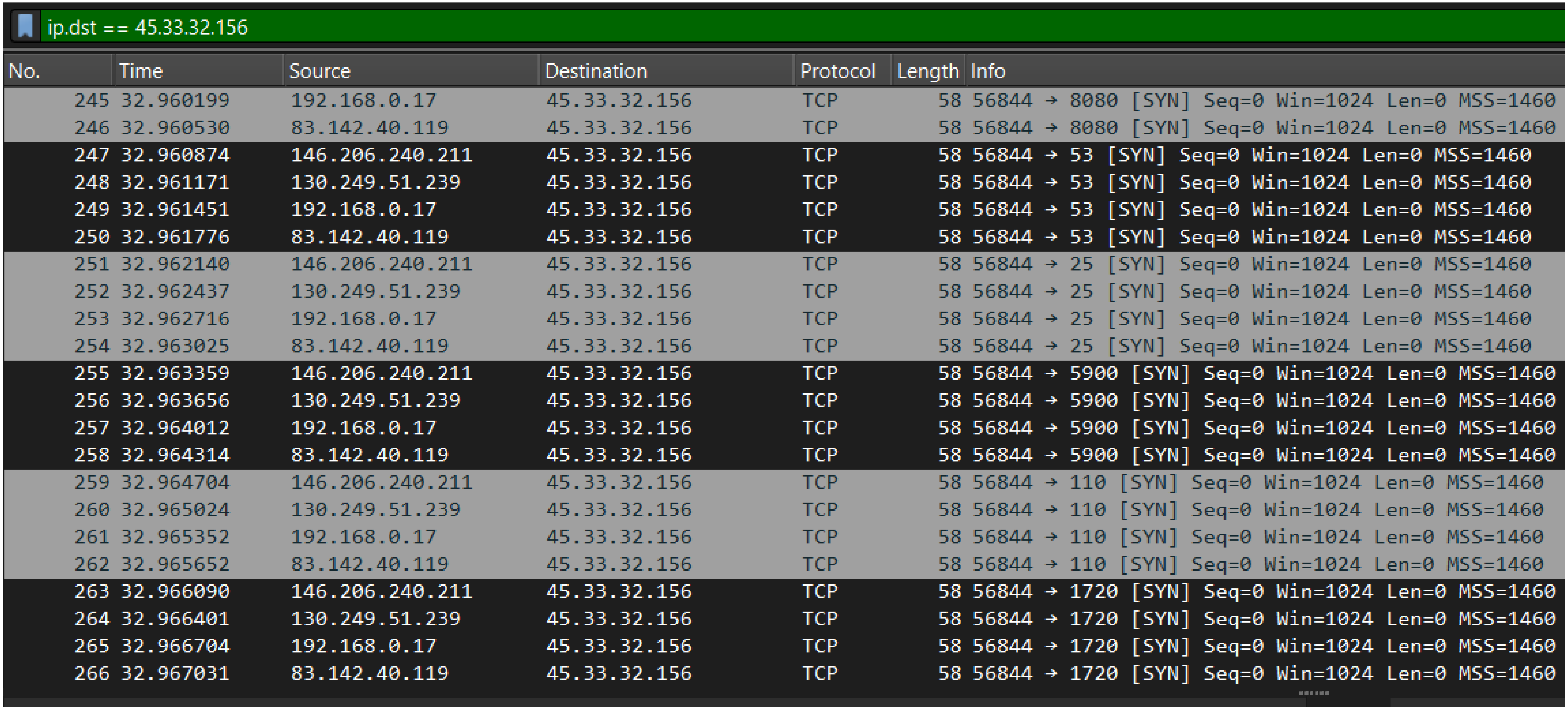
ip.src == 192.168.0.17

No.	Time	Source	Destination	Protocol	Length	Info
260	45.163092	192.168.0.17	45.33.32.156	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=0, ID=422d) [Reassembled in #262]
261	45.163436	192.168.0.17	45.33.32.156	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=8, ID=422d) [Reassembled in #262]
262	45.163719	192.168.0.17	45.33.32.156	TCP	42	47544 → 2033 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
264	45.345085	192.168.0.17	45.33.32.156	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=0, ID=f716) [Reassembled in #266]
265	45.345481	192.168.0.17	45.33.32.156	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=8, ID=f716) [Reassembled in #266]
266	45.345814	192.168.0.17	45.33.32.156	TCP	42	47544 → 1069 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
267	45.346125	192.168.0.17	45.33.32.156	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=0, ID=d0e5) [Reassembled in #270]
269	45.346933	192.168.0.17	45.33.32.156	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=8, ID=d0e5) [Reassembled in #270]
270	45.347300	192.168.0.17	45.33.32.156	TCP	42	47544 → 26214 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
275	45.360447	192.168.0.17	45.33.32.156	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=0, ID=916b) [Reassembled in #277]
276	45.360752	192.168.0.17	45.33.32.156	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=8, ID=916b) [Reassembled in #277]
277	45.361023	192.168.0.17	45.33.32.156	TCP	42	47544 → 9485 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
279	45.361858	192.168.0.17	45.33.32.156	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=0, ID=0ad6) [Reassembled in #283]
281	45.362157	192.168.0.17	45.33.32.156	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=8, ID=0ad6) [Reassembled in #283]
283	45.362991	192.168.0.17	45.33.32.156	TCP	42	47544 → 31337 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
284	45.363283	192.168.0.17	45.33.32.156	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=0, ID=4827) [Reassembled in #286]
285	45.363566	192.168.0.17	45.33.32.156	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=8, ID=4827) [Reassembled in #286]
286	45.363832	192.168.0.17	45.33.32.156	TCP	42	47544 → 1082 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
287	45.364193	192.168.0.17	45.33.32.156	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=0, ID=52ad) [Reassembled in #289]
288	45.364472	192.168.0.17	45.33.32.156	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=8, ID=52ad) [Reassembled in #289]



```
Performing scan...
['-sS', '-sV', '-T3', '-f']
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-03 23:17 Central Europe Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.29s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 994 closed tcp ports (reset)
PORT      STATE    SERVICE    VERSION
22/tcp    open     ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
25/tcp    filtered smtp
80/tcp    filtered http
427/tcp   filtered svrloc
9929/tcp  open     nping-echo Nping echo
31337/tcp open     tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.24 seconds
```

IP Decoy



ip.dst == 45.33.32.156

No.	Time	Source	Destination	Protocol	Length	Info
245	32.960199	192.168.0.17	45.33.32.156	TCP	58	56844 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
246	32.960530	83.142.40.119	45.33.32.156	TCP	58	56844 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
247	32.960874	146.206.240.211	45.33.32.156	TCP	58	56844 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
248	32.961171	130.249.51.239	45.33.32.156	TCP	58	56844 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
249	32.961451	192.168.0.17	45.33.32.156	TCP	58	56844 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
250	32.961776	83.142.40.119	45.33.32.156	TCP	58	56844 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
251	32.962140	146.206.240.211	45.33.32.156	TCP	58	56844 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
252	32.962437	130.249.51.239	45.33.32.156	TCP	58	56844 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
253	32.962716	192.168.0.17	45.33.32.156	TCP	58	56844 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
254	32.963025	83.142.40.119	45.33.32.156	TCP	58	56844 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
255	32.963359	146.206.240.211	45.33.32.156	TCP	58	56844 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
256	32.963656	130.249.51.239	45.33.32.156	TCP	58	56844 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
257	32.964012	192.168.0.17	45.33.32.156	TCP	58	56844 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
258	32.964314	83.142.40.119	45.33.32.156	TCP	58	56844 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
259	32.964704	146.206.240.211	45.33.32.156	TCP	58	56844 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
260	32.965024	130.249.51.239	45.33.32.156	TCP	58	56844 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
261	32.965352	192.168.0.17	45.33.32.156	TCP	58	56844 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
262	32.965652	83.142.40.119	45.33.32.156	TCP	58	56844 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
263	32.966090	146.206.240.211	45.33.32.156	TCP	58	56844 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
264	32.966401	130.249.51.239	45.33.32.156	TCP	58	56844 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
265	32.966704	192.168.0.17	45.33.32.156	TCP	58	56844 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
266	32.967031	83.142.40.119	45.33.32.156	TCP	58	56844 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Conclusion

- Intrusion Detection System (IDS)
- Intrusion Prevention System (IPS)
- IPS/IDS Evasion Techniques
- Prototype