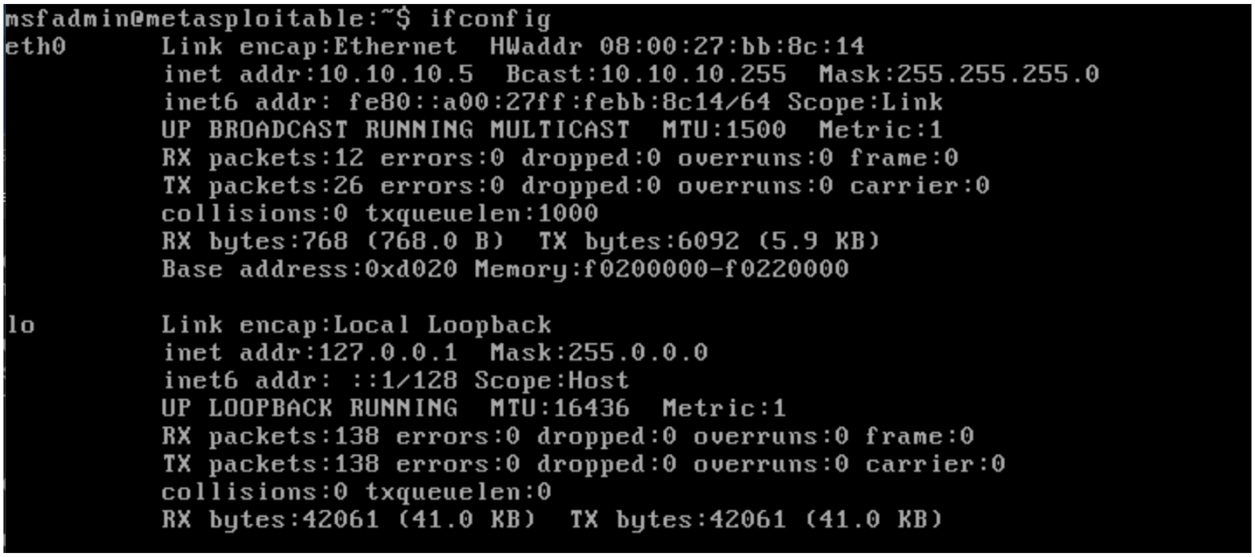
Lab Objective: To deploy a Network Intrusion Detection System (NIDS) and validate its capability to detect active reconnaissance and port scanning activities within a segregated environment (using Kali Linux as the “attacker” and Metasploitable as the “victim”)

System Setup Details: (Oracle VirtualBox v7.2.6)
Analyst: *SecurityOnion* (IP Address: 192.168.1.50)
Network Adapter 1: Bridged, Network Adapter 2: Internal Network (inet)
Attacker: *Kali* (IP Address: 10.10.10.6)
Network Adapter 1: Internal Network (inet, promiscuous mode: Deny)
Victim: *Metasploitable* (IP Address: 10.10.10.5)
Network Adapter 1: Internal Network (inet, promiscuous mode: Allow All)

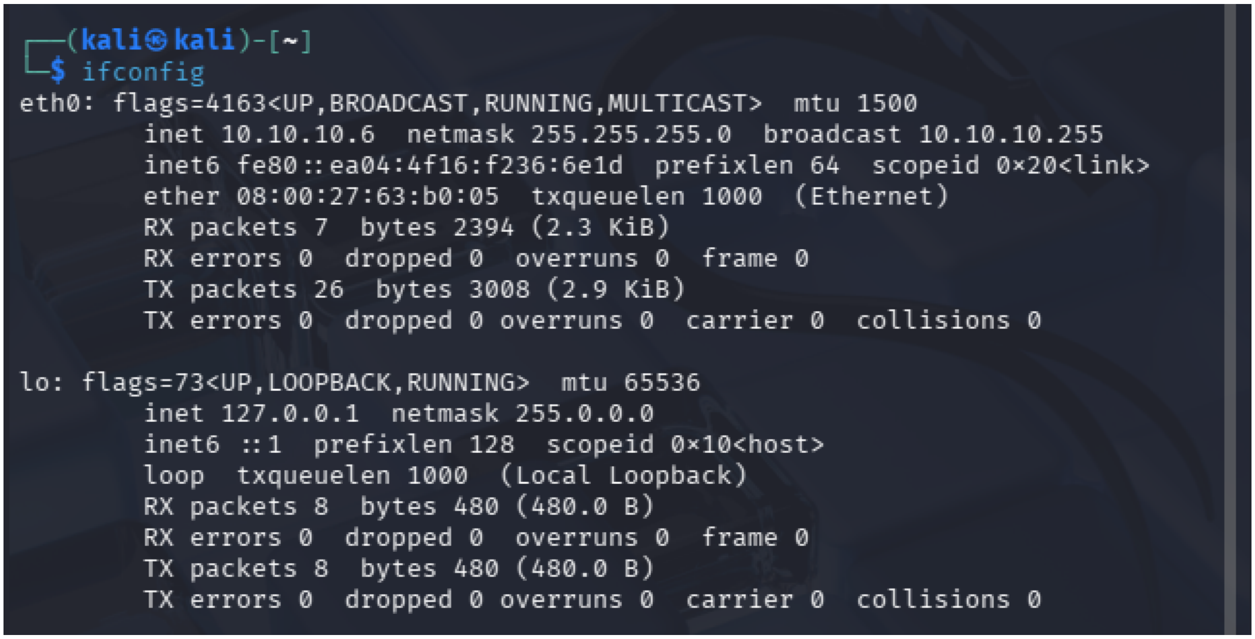


```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:bb:8c:14
          inet addr:10.10.10.5  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:febb:8c14/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:12 errors:0 dropped:0 overruns:0 frame:0
          TX packets:26 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:768 (768.0 B)  TX bytes:6092 (5.9 KB)
          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:138 errors:0 dropped:0 overruns:0 frame:0
          TX packets:138 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:42061 (41.0 KB)  TX bytes:42061 (41.0 KB)
```

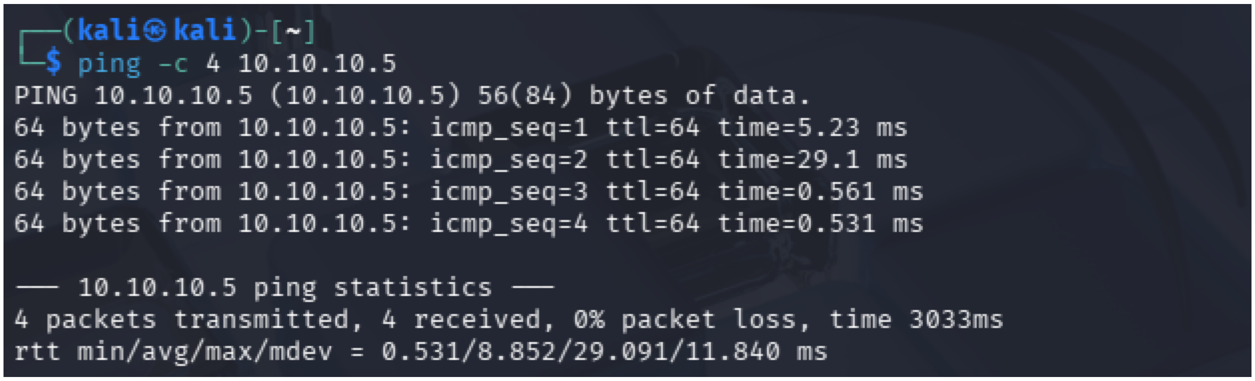
Target System Configuration (Metasploitable):

- **IP Address:** *10.10.10.5* confirmed via *ifconfig*.
- **Status:** Interface *eth0* is UP and reachable on the internal *10.10.10.0/24* subnet.
- **Role:** This asset hosts intentionally vulnerable services (FTP, HTTP, MySQL) to serve as the target for Red Team operations.



```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.10.6  netmask 255.255.255.0  broadcast 10.10.10.255
        inet6 fe80::ea04:4f16:f236:6e1d  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:63:b0:05  txqueuelen 1000  (Ethernet)
        RX packets 7  bytes 2394 (2.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 26  bytes 3008 (2.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

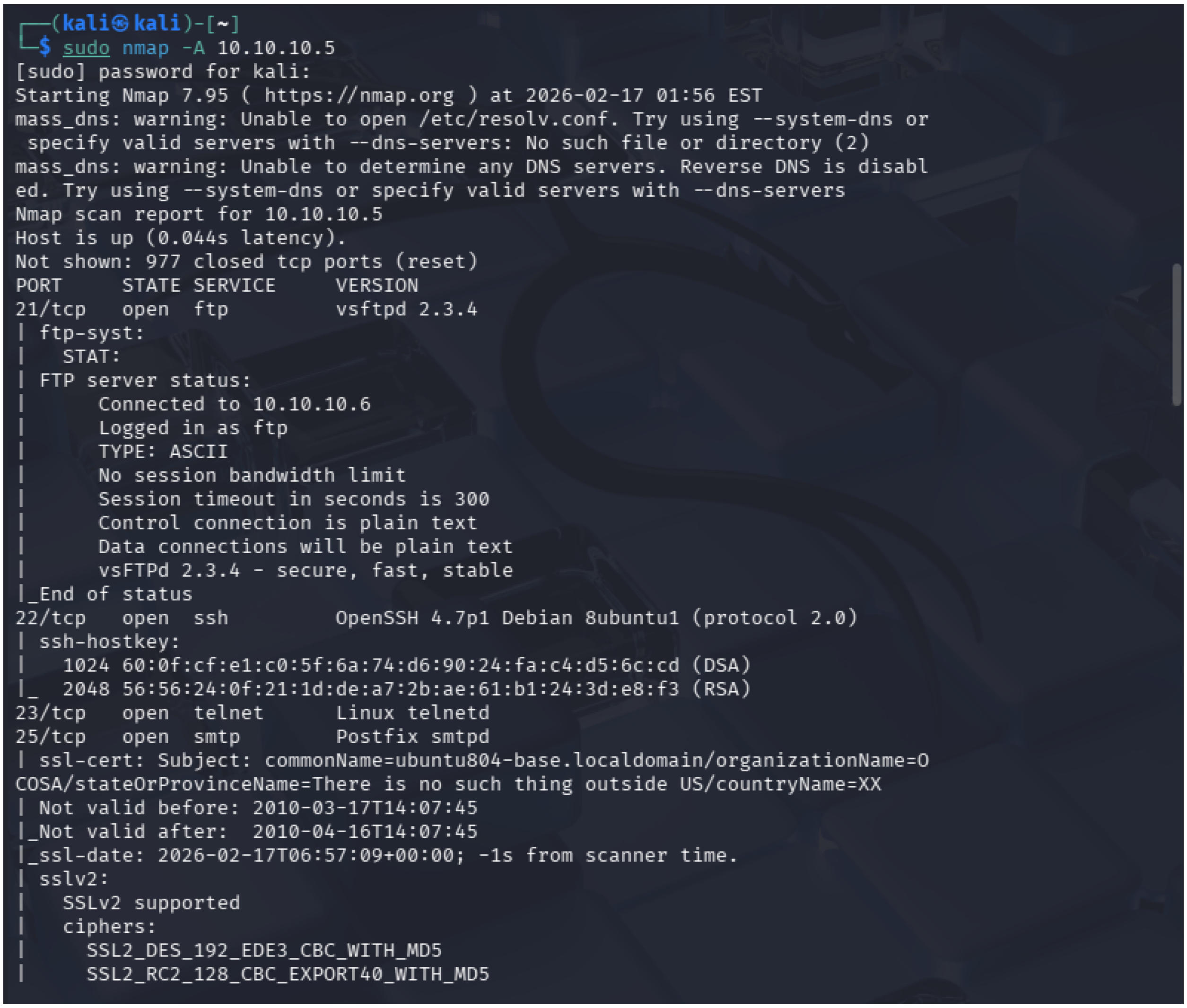


```
┌──(kali㉿kali)-[~]
└─$ ping -c 4 10.10.10.5
PING 10.10.10.5 (10.10.10.5) 56(84) bytes of data.
64 bytes from 10.10.10.5: icmp_seq=1 ttl=64 time=5.23 ms
64 bytes from 10.10.10.5: icmp_seq=2 ttl=64 time=29.1 ms
64 bytes from 10.10.10.5: icmp_seq=3 ttl=64 time=0.561 ms
64 bytes from 10.10.10.5: icmp_seq=4 ttl=64 time=0.531 ms

── 10.10.10.5 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3033ms
rtt min/avg/max/mdev = 0.531/8.852/29.091/11.840 ms
```

Attacker Connectivity & Reachability Check:

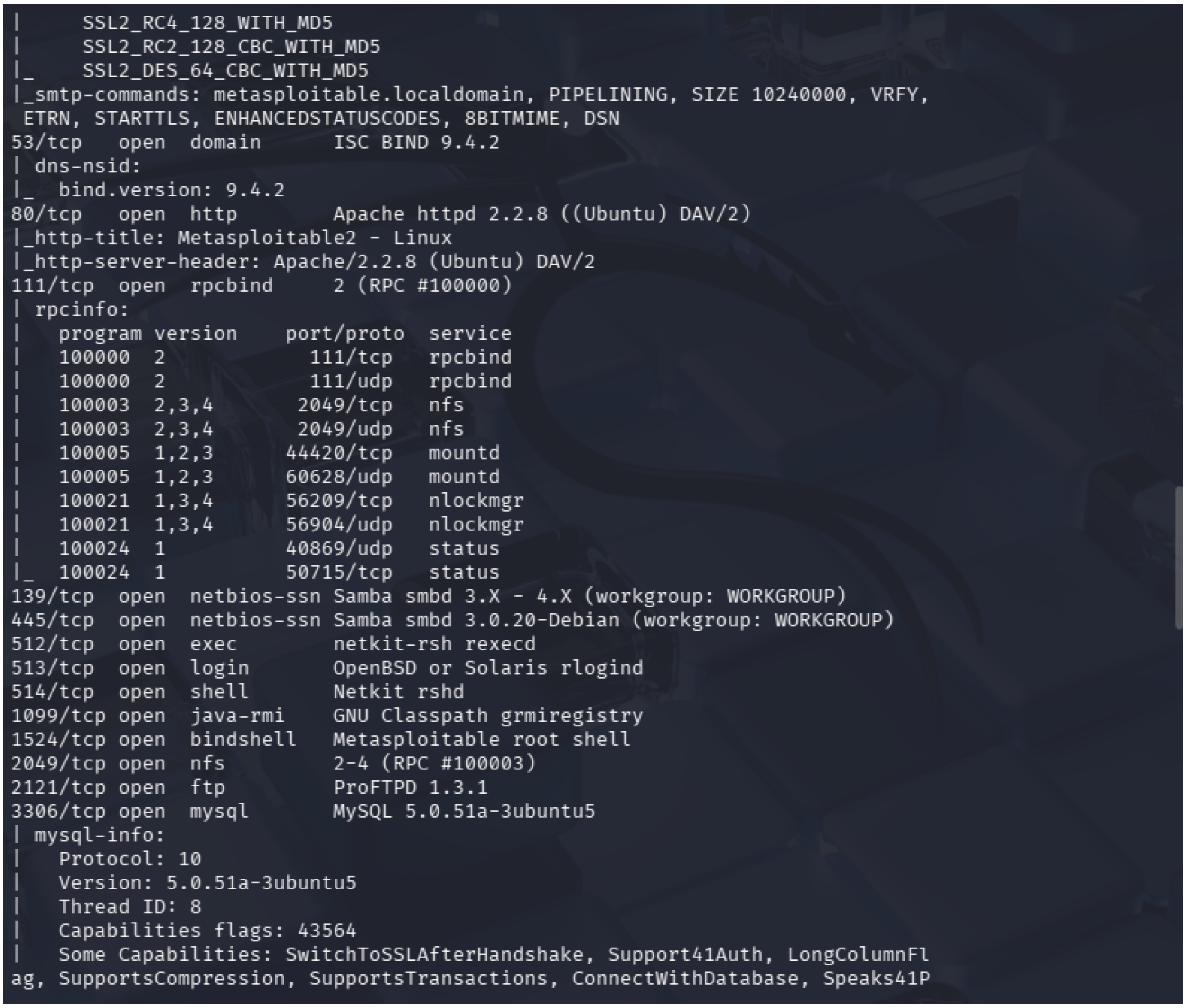
- **IP Address:** *10.10.10.6* (Static Assignment).
- **Connectivity Test:** Successful ICMP Echo (Ping) requests to the target (*10.10.10.5*) confirm network path availability and low latency (<1ms), verifying the virtual switch configuration.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A 10.10.10.5
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-17 01:56 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or
 specify valid servers with --dns-servers: No such file or directory (2)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabl
ed. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.10.10.5
Host is up (0.044s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.10.6
|      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 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)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=O
COSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2026-02-17T06:57:09+00:00; -1s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
```

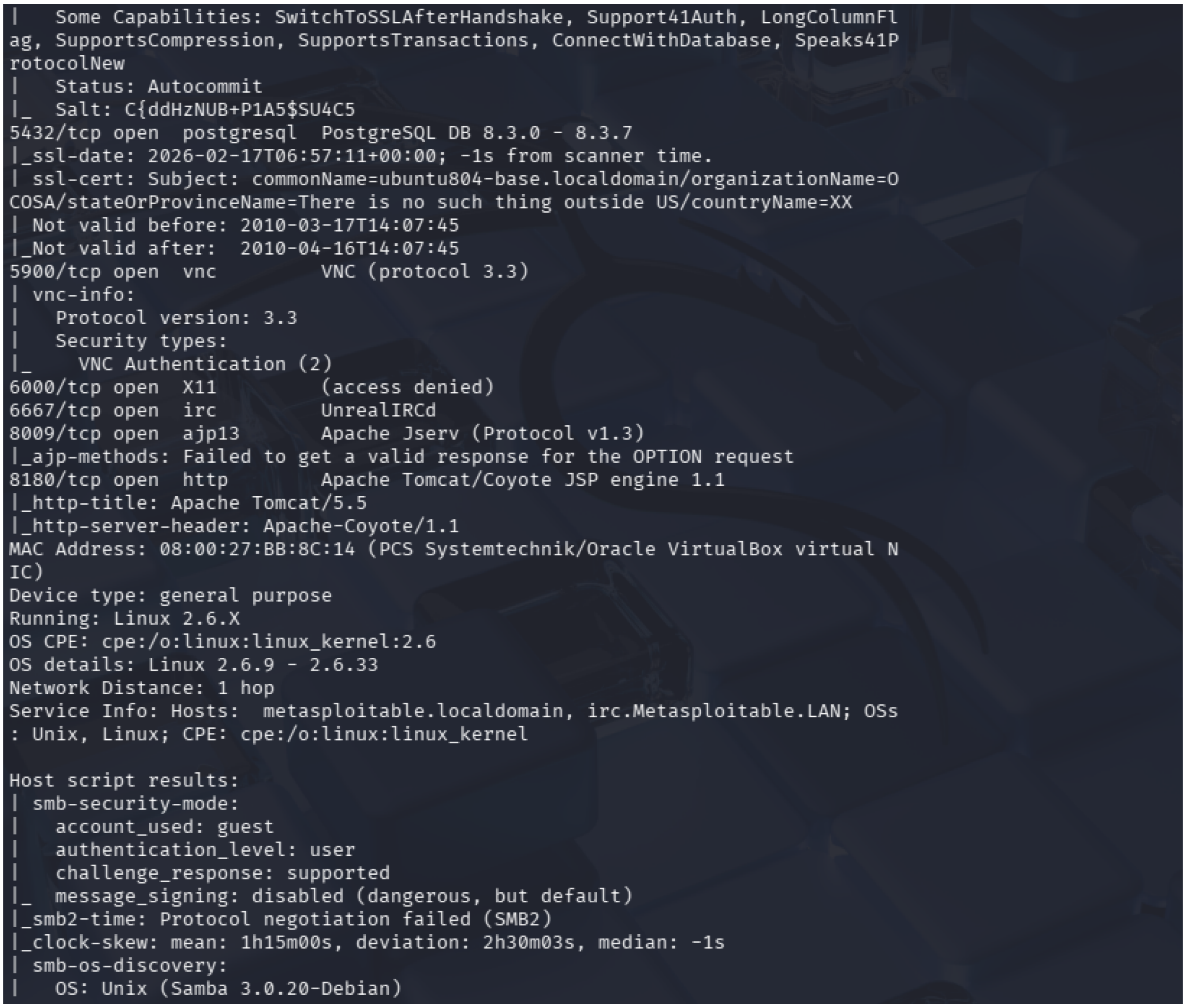
Execution of Aggressive Reconnaissance Scan (1/3):

- **Command**: *sudo nmap -A 10.10.10.5*
- **Objective**: To fingerprint the operating system and enumerate running services/versions.
- **Findings**: The scan revealed multiple high-risk open ports, including **FTP (21)**, **SSH (22)**, **Telnet (23)**, and **HTTP (80)**.
- **Significance**: The *-A* flag utilizes aggressive scripts that generate "noisy" network traffic, intended to test if the NIDS (Security Onion) can detect non-stealthy scanning behavior.



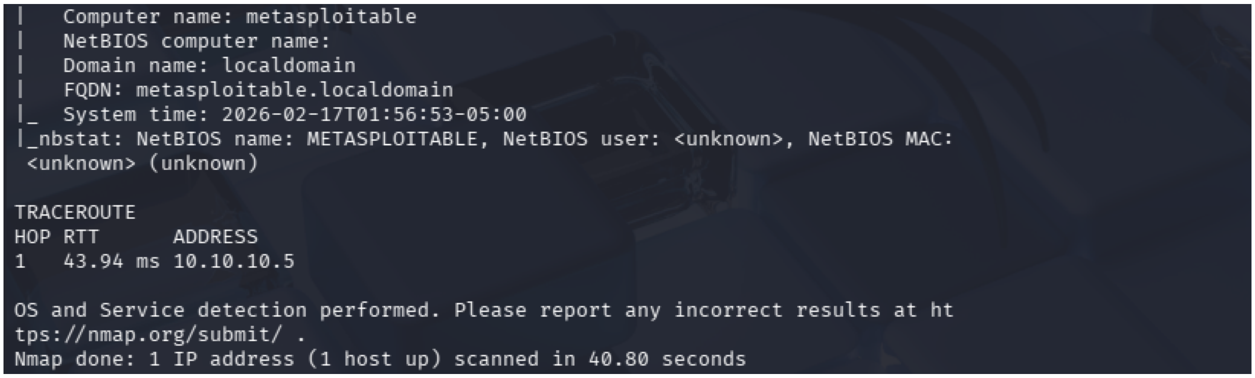
```
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|_    SSL2_DES_64_CBC_WITH_MD5
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY,
 ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
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      44420/tcp   mountd
|   100005  1,2,3      60628/udp   mountd
|   100021  1,3,4      56209/tcp   nlockmgr
|   100021  1,3,4      56904/udp   nlockmgr
|   100024  1          40869/udp   status
|_  100024  1          50715/tcp   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       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
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 8
|   Capabilities flags: 43564
|   Some Capabilities: SwitchToSSLAfterHandshake, Support41Auth, LongColumnFl
ag, SupportsCompression, SupportsTransactions, ConnectWithDatabase, Speaks41P
```

Execution of Aggressive Reconnaissance Scan (Continued 2/3)



```
|   Some Capabilities: SwitchToSSLAfterHandshake, Support41Auth, LongColumnFl
ag, SupportsCompression, SupportsTransactions, ConnectWithDatabase, Speaks41P
rotocolNew
|   Status: Autocommit
|_  Salt: C{ddHzNUB+P1A5$SU4C5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2026-02-17T06:57:11+00:00; -1s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=O
COSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/5.5
|_http-server-header: Apache-Coyote/1.1
MAC Address: 08:00:27:BB:8C:14 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs
: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 1h15m00s, deviation: 2h30m03s, median: -1s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
```

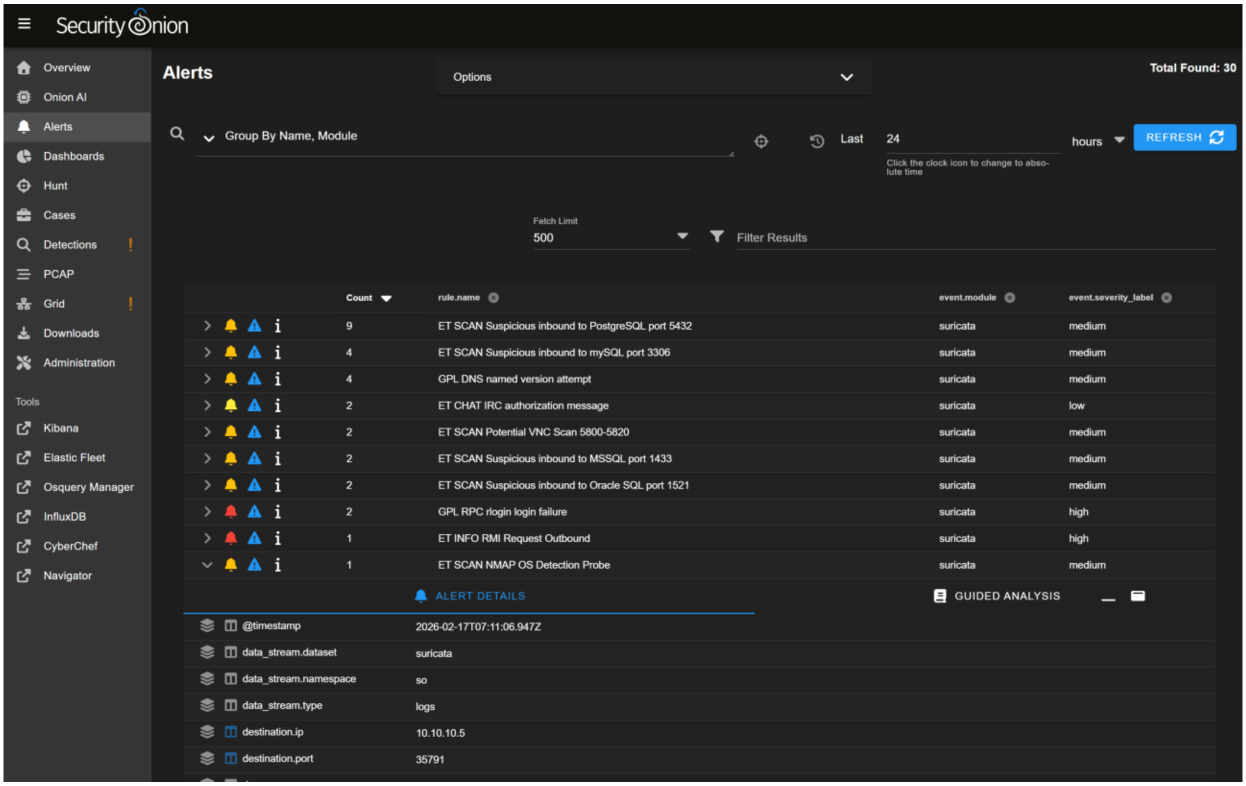


```
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2026-02-17T01:56:53-05:00
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC:
 <unknown> (unknown)

TRACEROUTE
HOP RTT      ADDRESS
1   43.94 ms 10.10.10.5

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 40.80 seconds
```

Execution of Aggressive Reconnaissance Scan (Continued 3/3)



Alerts

Total Found: 30

Group By Name, Module

Last 24 hours

Click the clock icon to change to absolute time

Fetch Limit 500

Count	rule.name	event.module	event.severity_label
9	ET SCAN Suspicious inbound to PostgreSQL port 5432	suricata	medium
4	ET SCAN Suspicious inbound to mySQL port 3306	suricata	medium
4	GPL DNS named version attempt	suricata	medium
2	ET CHAT IRC authorization message	suricata	low
2	ET SCAN Potential VNC Scan 5800-5820	suricata	medium
2	ET SCAN Suspicious inbound to MSSQL port 1433	suricata	medium
2	ET SCAN Suspicious inbound to Oracle SQL port 1521	suricata	medium
2	GPL RPC rlogin login failure	suricata	high
1	ET INFO RMI Request Outbound	suricata	high
1	ET SCAN NMAP OS Detection Probe	suricata	medium

@timestamp	2026-02-17T07:11:06.947Z
data_stream.dataset	suricata
data_stream.namespace	so
data_stream.type	logs
destination.ip	10.10.10.5
destination.port	35791

Network Intrusion Detection System (NIDS) Alert Validation (Suricata):

- **Dashboard View**: The Security Onion "Alerts" console successfully ingested and indexed the attack traffic.
- **Key Alerts Generated**:
  - *ET SCAN Nmap OS Detection Probe* (confirming OS fingerprinting attempts).
  - *ET SCAN Suspicious inbound to PostgreSQL/MySQL* (this is also confirming service enumeration).
- **Analyst Conclusion**: The sensor correctly identified the source IP (*10.10.10.6*) and categorized the activity as a "Network Scan," validating that the IDS ruleset is active and monitoring the internal network tap.