OSINT & Network Scanning Fundamentals

WHOIS Lookup

Finding who owns the domain, when it was registered, and registrar details.

Tool: whois

Command: whois vulnweb.com

Field	Value
Registrar	Gandi SAS
Creation Date	2010-06-14T07:50:29Z
Expiry Date	2027-06-14T07:50:29Z
Name Servers	NS-105-A.GANDI.NET

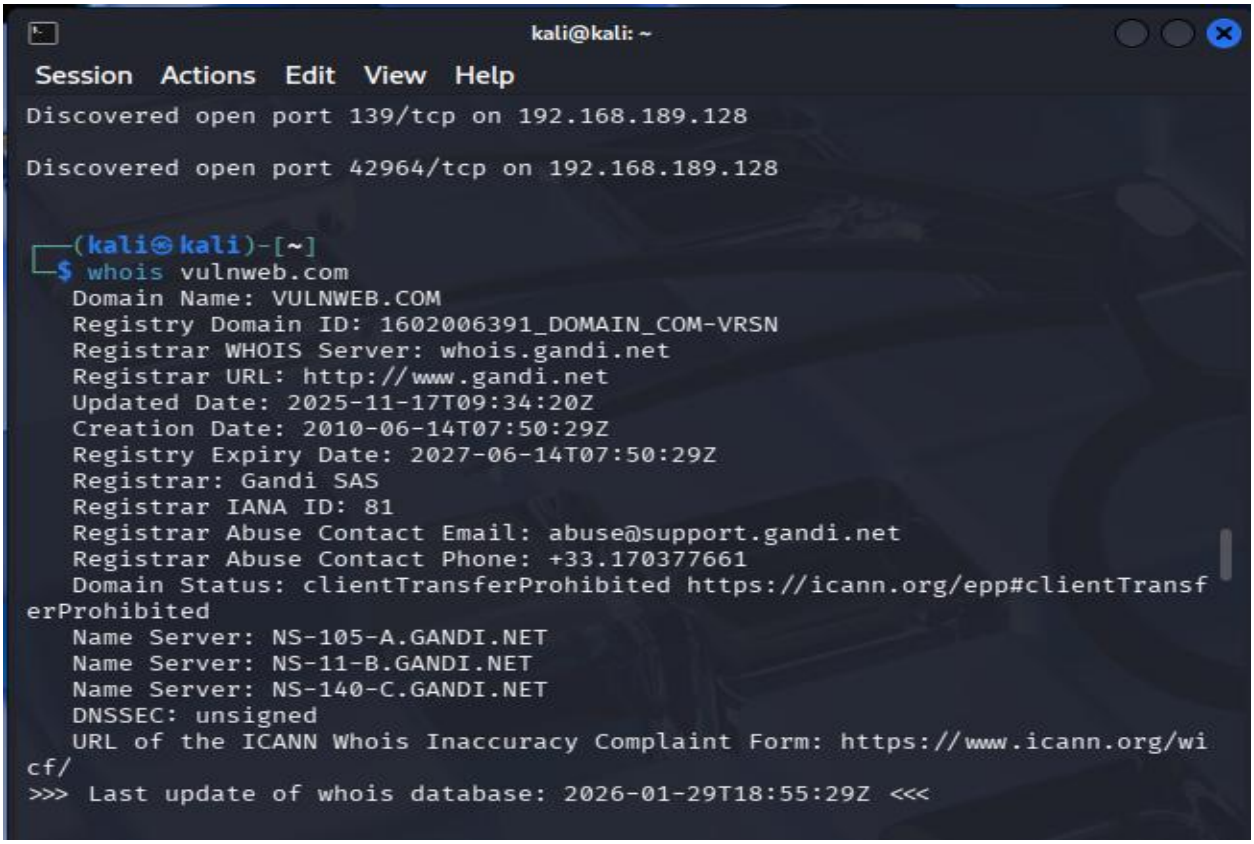


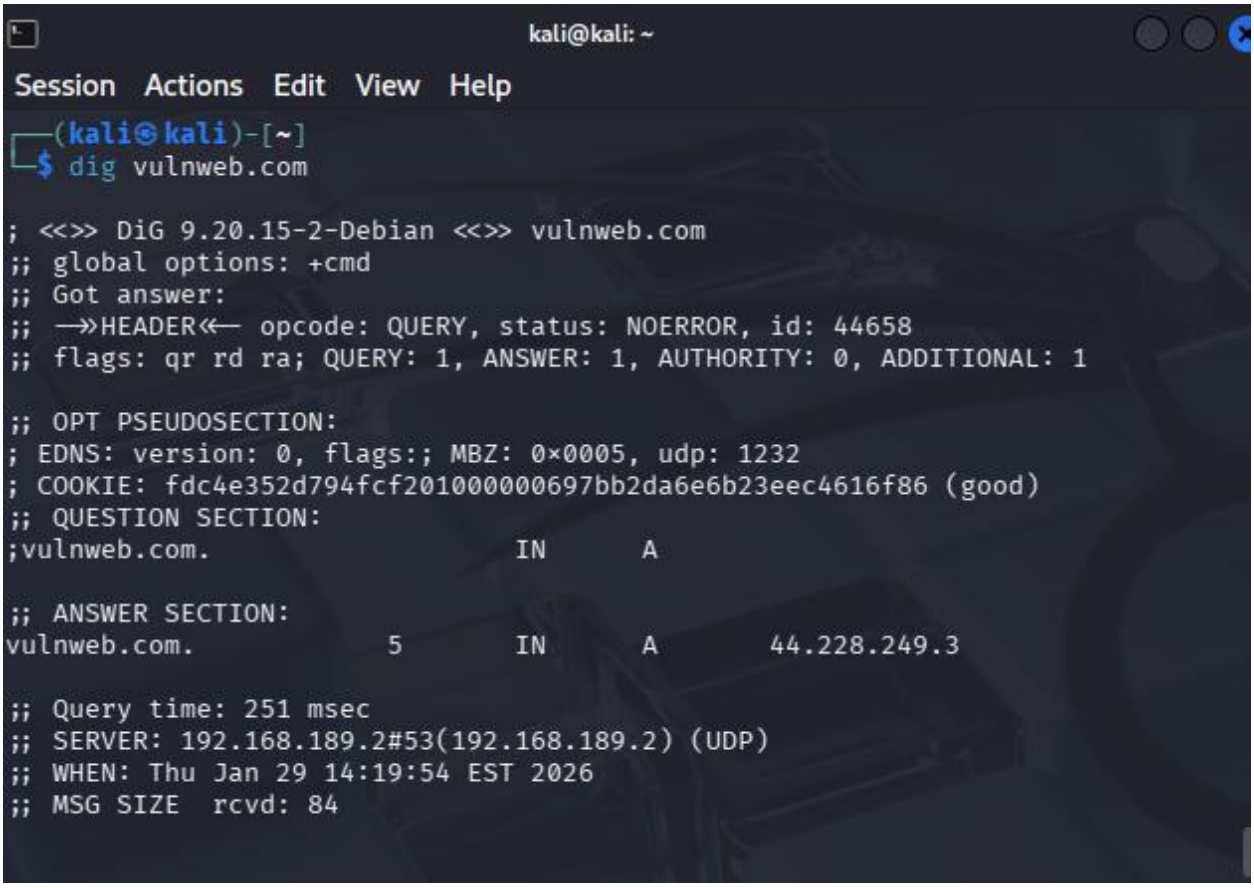
Figure 1 WHOIS output

DNS Enumeration

Finding **DNS records** that map the domain to servers.

Command

dig vulnweb.com



Command

dig NS vulnweb.com

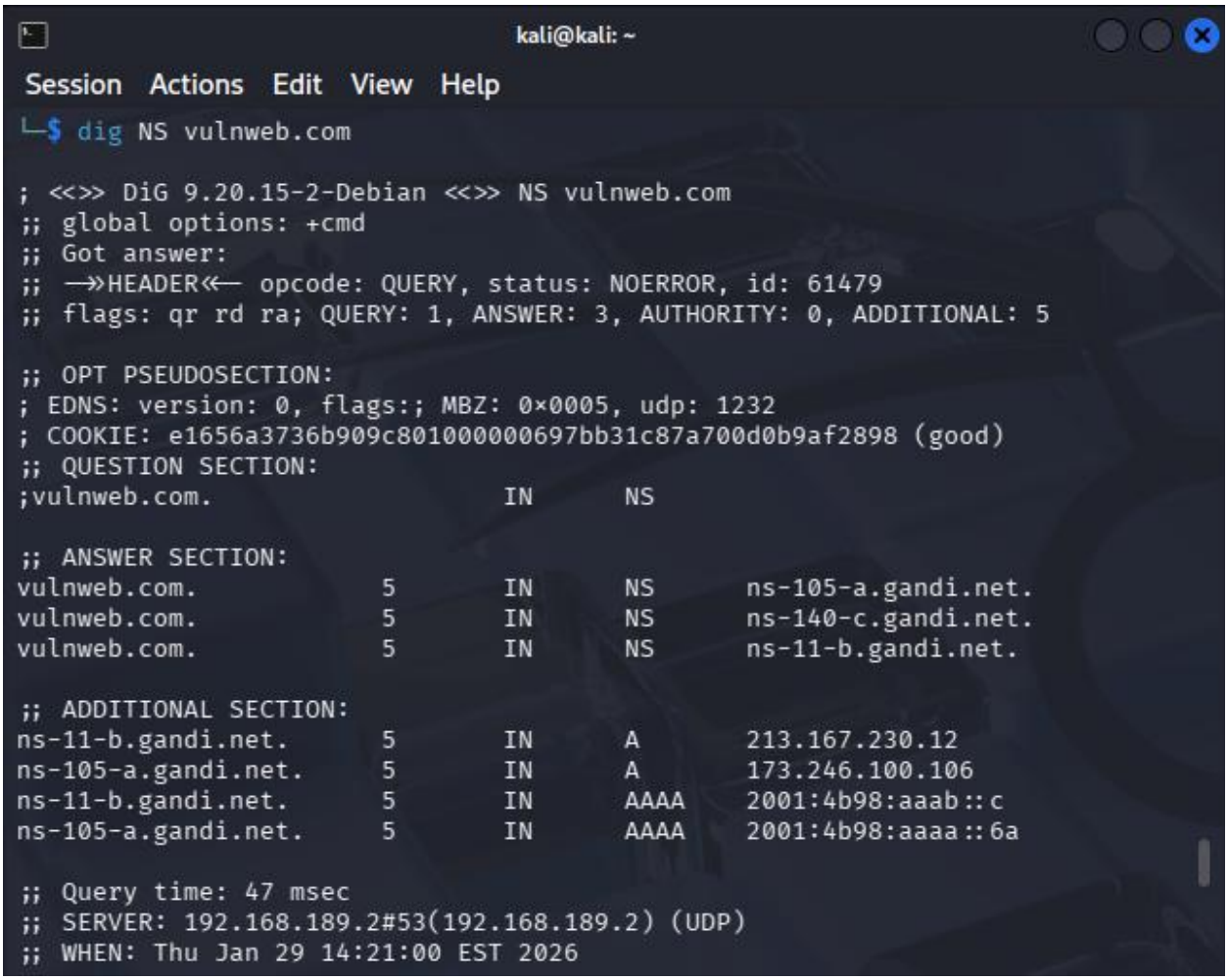


Figure 2 ns

Command

dig MX vulnweb.com

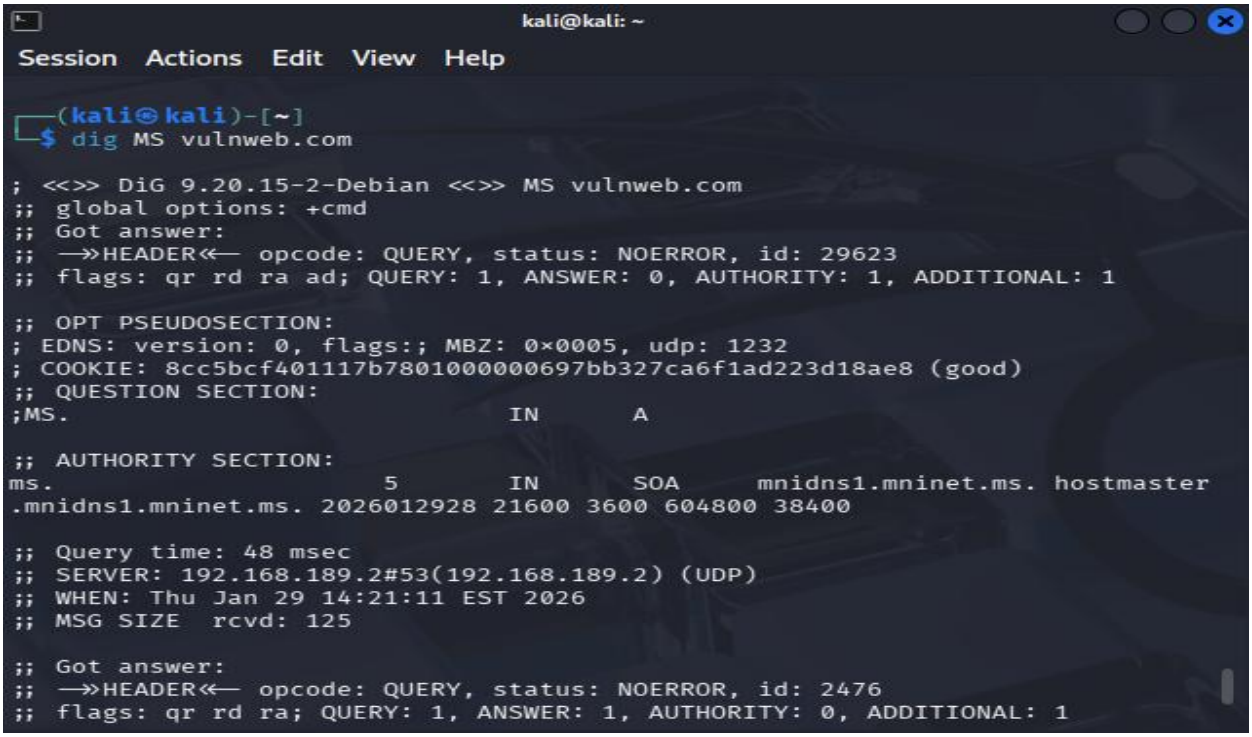


Figure 3 ms record

Table: DNS Records

Record Type	Value	Explanation
A	44.228.249.3	Web server hosted on AWS (Amazon Web Services) in US-East region. Short TTL (5s) suggests dynamic load balancing or DDoS mitigation.
NS	ns-105-a.gandi.net ns-140-c.gandi.net ns-11-b.gandi.net	Domain DNS managed by Gandi.net (French registrar). Three nameservers provide redundancy and high availability.
MX	Priority 10: aspmx.l.google.com Priority 10: alt1.aspmx.l.google.com Priority 10: alt2.aspmx.l.google.com Priority 10: alt3.aspmx.l.google.com Priority 10: alt4.aspmx.l.google.com	Email handled by Google Workspace. Five mail servers with equal priority (10) provide load balancing and failover. Professional email infrastructure with enterprise security features.

Figure 4 DNS Records

Subdomain Enumeration

Trying **multiple tools** because each one finds data differently.

Tool 1: Sublist3r

Command

sublist3r -d vulnweb.com

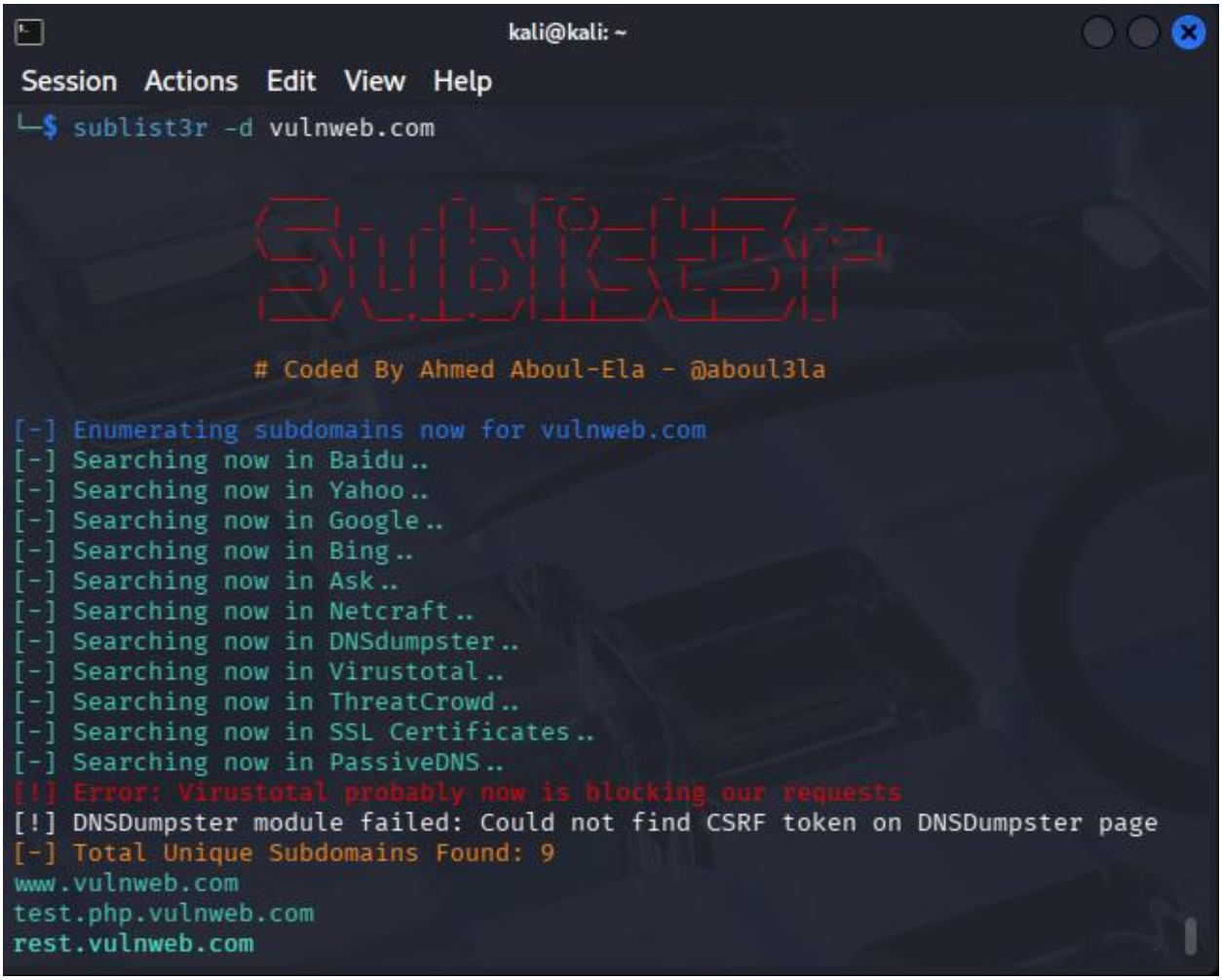


Figure 5 Sublist3r Outputs

SUB DOMAINS for Sublist3r :

b.vulnweb.com

home.vulnweb.com

p.vulnweb.com

sp.vulnweb.com

stasp.vulnweb.com

zzz.vulnweb.com

autoconfig.vulnweb.com

ec2-13-210-145-106.ap-southeast-2.compute.vulnweb.com

ml5.vulnweb.com

testjsp.vulnweb.com

www.tetphp.vulnweb.com

estphp.vulnweb.com

beta.vulnweb.com

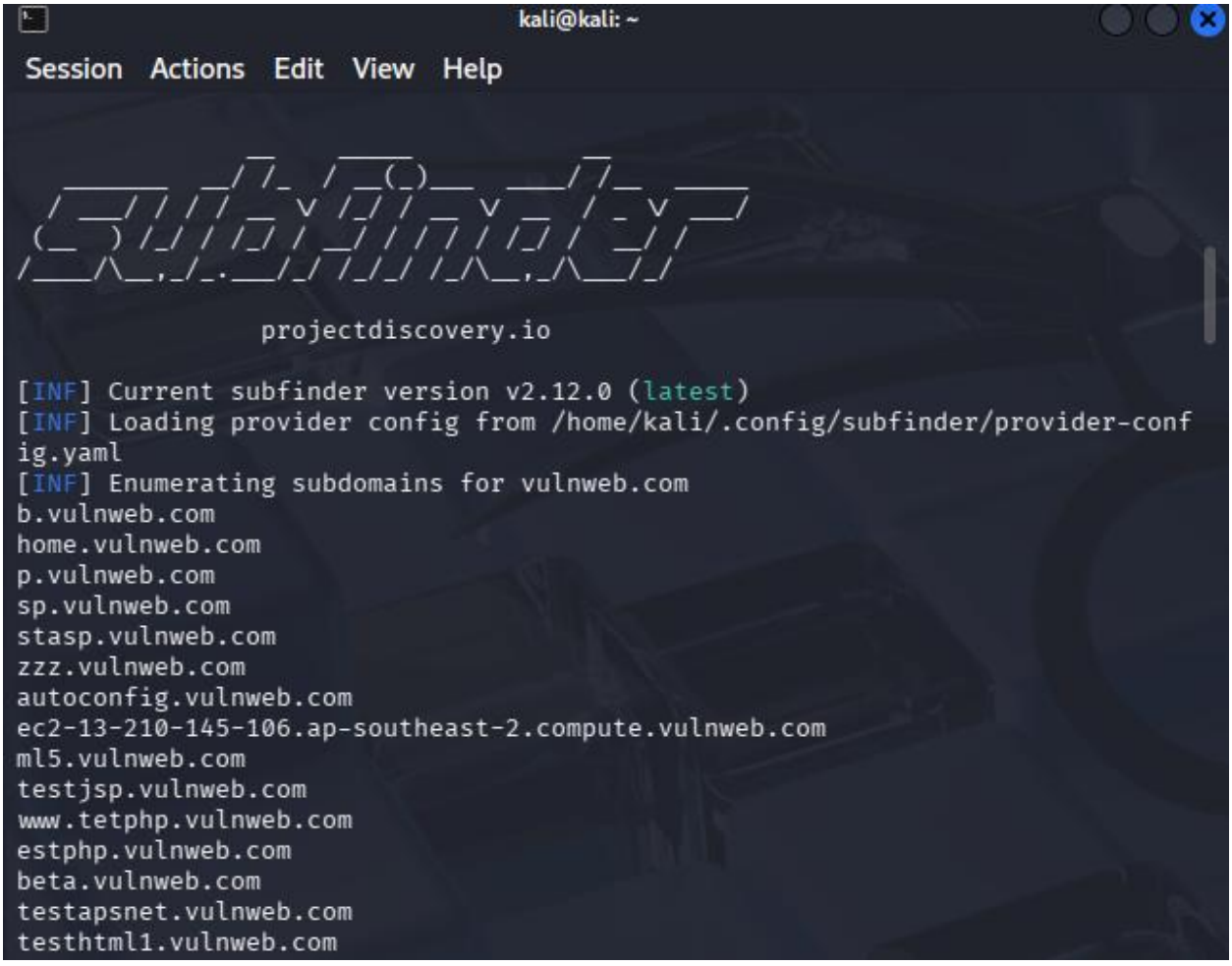
testaspnet.vulnweb.com

testhtml1.vulnweb.com

Tool 2: Amass

Command

amass enum -passive -d vulnweb.com



SUB DOMAINS for Subfinder :

www.vulnweb.com

test.php.vulnweb.com

rest.vulnweb.com

Tool 3: crt.sh

Tool 3: crt.sh (Certificate Transparency)

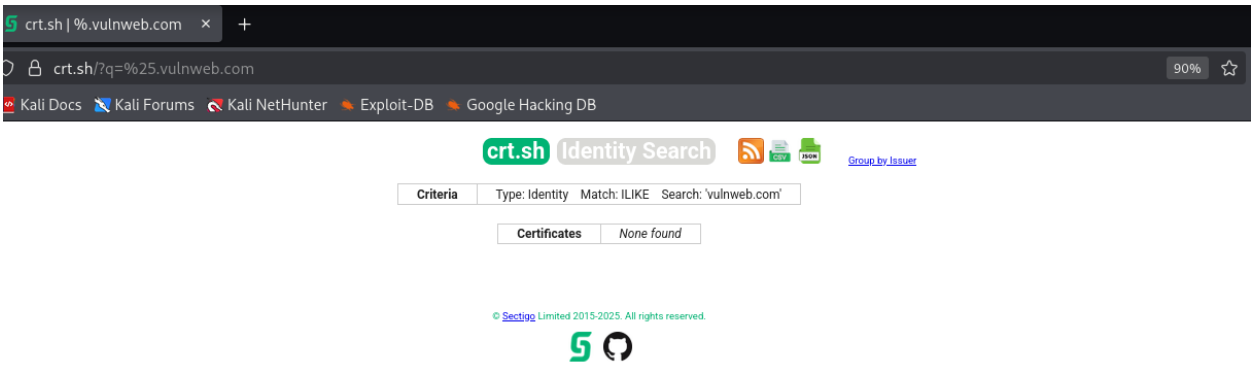
Purpose
To identify subdomains of *vulnweb.com* that appear in publicly issued SSL/TLS certificates.

Method
The crt.sh database was queried using a wildcard search to find any certificates associated with subdomains of the target domain.

Query Used
%25.vulnweb.com

Observations / Results
No subdomains related to *vulnweb.com* were found in the Certificate Transparency logs. This indicates that either no SSL certificates have been issued for subdomains of this domain or such certificates are not publicly logged.

Security Insight
The absence of certificate records reduces the likelihood of discovering hidden or forgotten subdomains through Certificate Transparency, thereby slightly limiting the exposed attack surface via this method.



Tool 4: theHarvester

Purpose

To gather publicly available information such as subdomains and email addresses related **to *vulnweb.com* using search engine data.**

Command Used

theHarvester -d vulnweb.com -b google

Observations / Results

TheHarvester returned a message indicating that the Google search engine is no longer supported. As a result, no subdomains or email addresses were collected using this data source.

Reason

Modern search engines like Google actively block automated scraping tools. TheHarvester has therefore removed or disabled support for these engines in recent versions.

Recorded Data

Data Type	Result
Subdomains	None found
Emails	None found

Security Insight

Since theHarvester was unable to retrieve data from Google, no additional attack surface information was discovered through this method. This highlights how defensive controls and platform restrictions can limit OSINT collection.

OSINT Summary

In this OSINT exercise, multiple passive reconnaissance tools were used to gather publicly available information about the domain *vulnweb.com*. Subdomain enumeration tools such as Sublist3r and Amass successfully identified exposed assets, while other tools like crt.sh and theHarvester returned no results due to limited certificate data and unsupported

search engines. SpiderFoot was also unable to produce results, likely due to tool or data source limitations. This demonstrates that OSINT results vary across tools and that understanding tool limitations is as important as the data collected.

Network Scanning

Network Scanning Lab Setup: A controlled lab environment was created using VirtualBox. Kali Linux was used as the scanning machine, and Metasploitable was used as the vulnerable target.

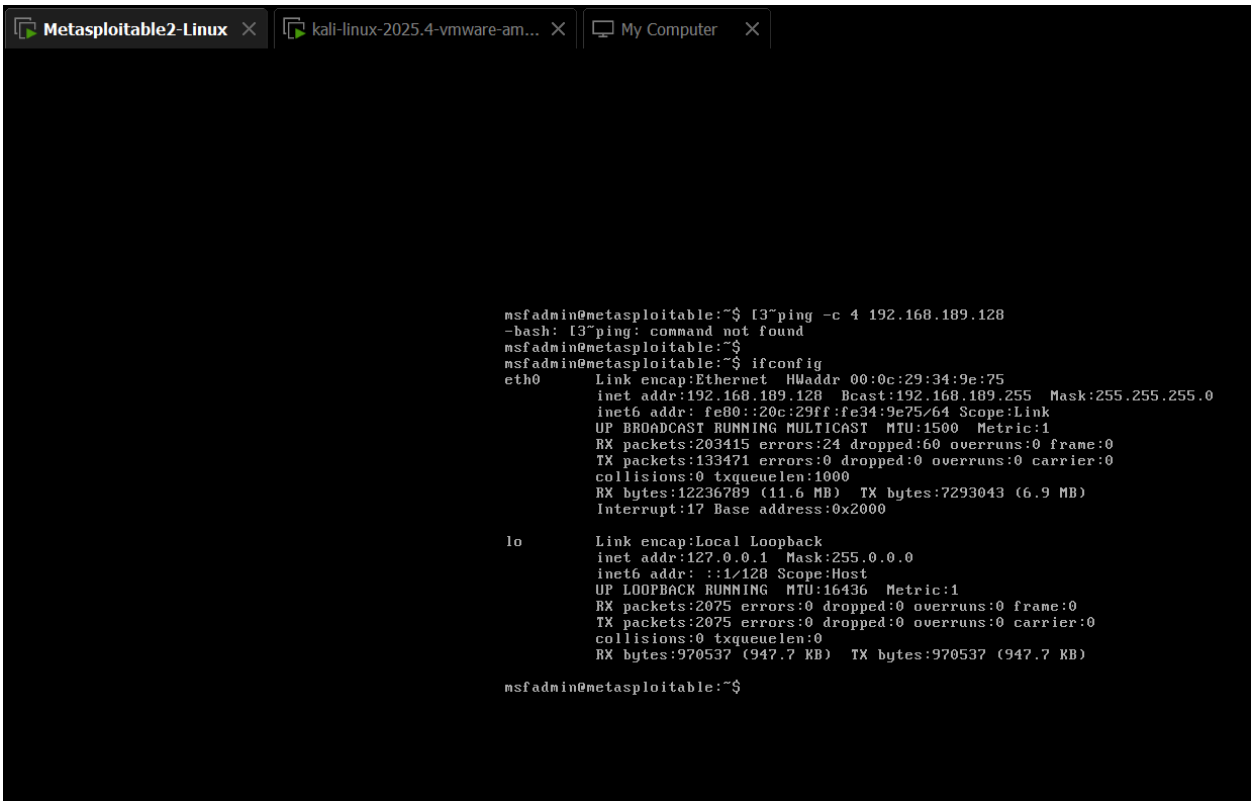


Figure 6 Metasploitable terminal

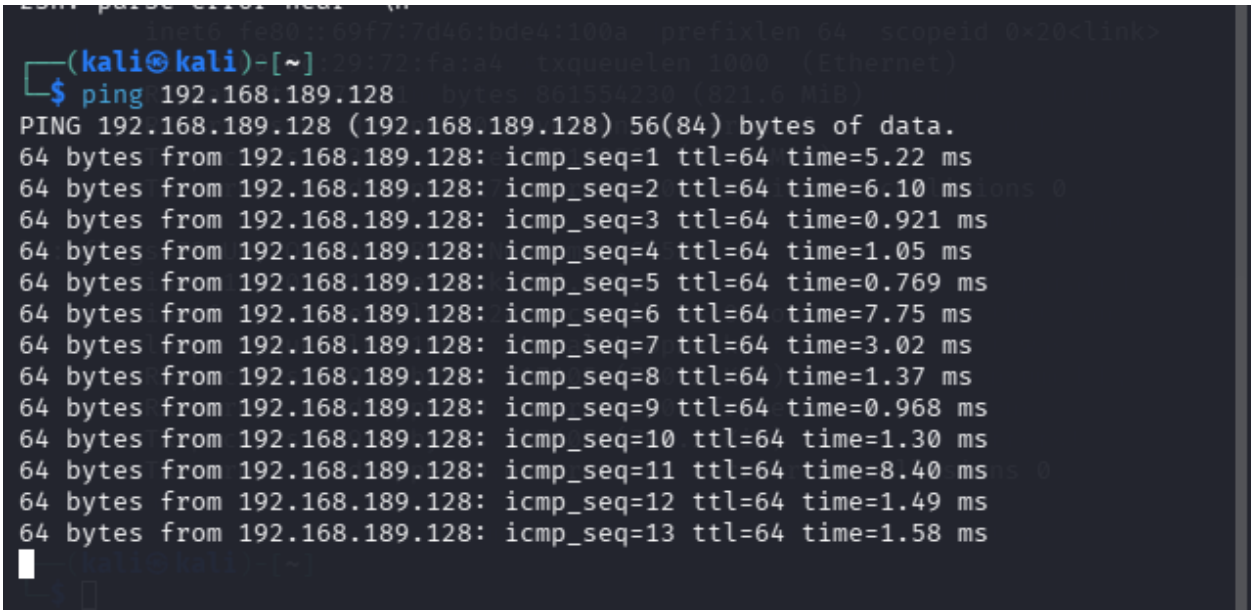


Figure 7 Linux terminal after ping

ICMP echo requests from Kali Linux to the Metasploitable machine were successful. Continuous replies with zero packet loss confirm that both virtual machines are correctly configured on the same network and are reachable

Machine	Operating System	IP Address
Attacker Machine	Kali Linux	192.168.189.129
Target Machine	Metasploitable	192.168.189.128

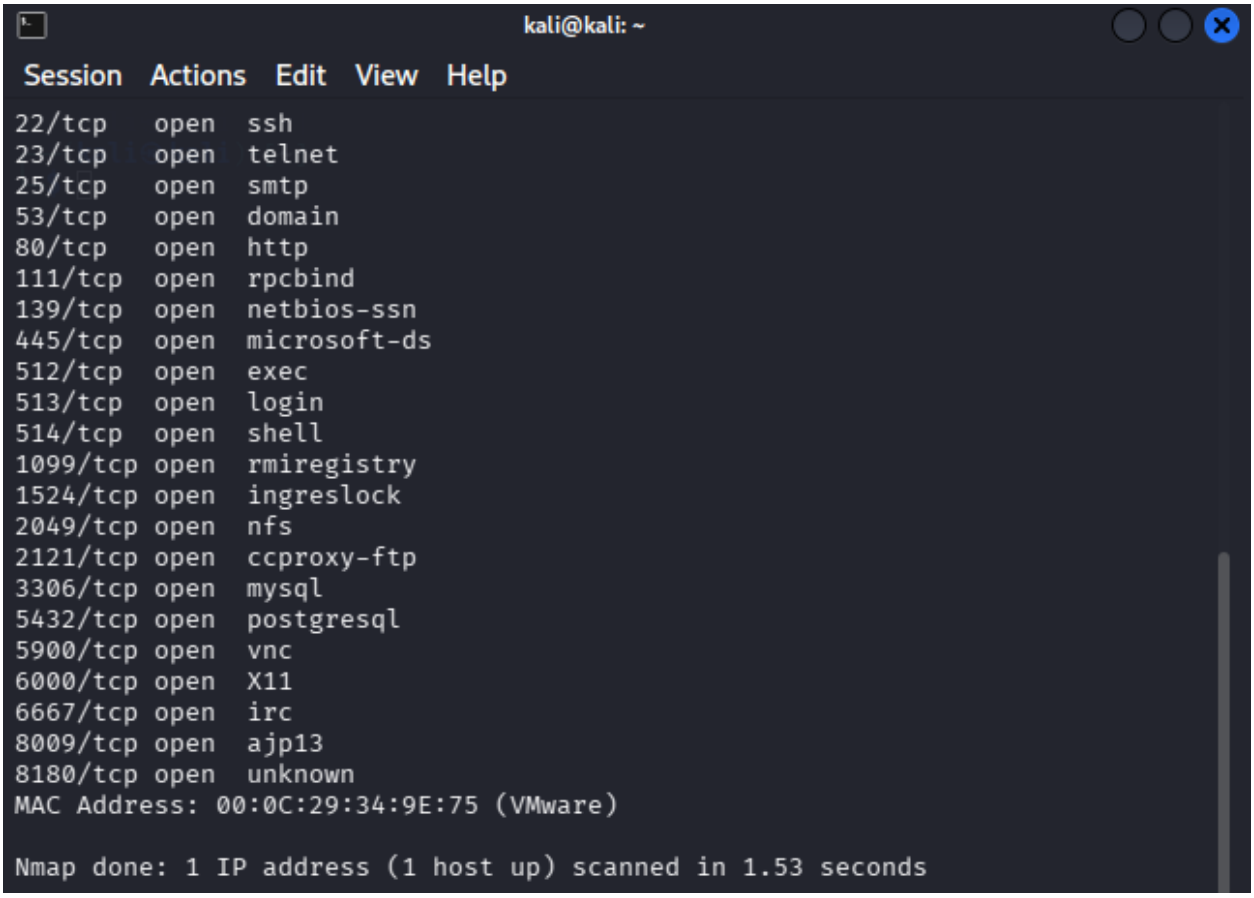
```
┌──(kali㉿kali)-[~]
└─$ ping -c 4 192.168.189.128
PING 192.168.189.128 (192.168.189.128) 56(84) bytes of data.
64 bytes from 192.168.189.128: icmp_seq=1 ttl=64 time=5.62 ms
64 bytes from 192.168.189.128: icmp_seq=2 ttl=64 time=6.29 ms
64 bytes from 192.168.189.128: icmp_seq=3 ttl=64 time=2.30 ms
64 bytes from 192.168.189.128: icmp_seq=4 ttl=64 time=4.82 ms

── 192.168.189.128 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3009ms
rtt min/avg/max/mdev = 2.298/4.757/6.291/1.512 ms
```

The reachability of the Metasploitable virtual machine was verified using ICMP ping.

Nmap Scanning

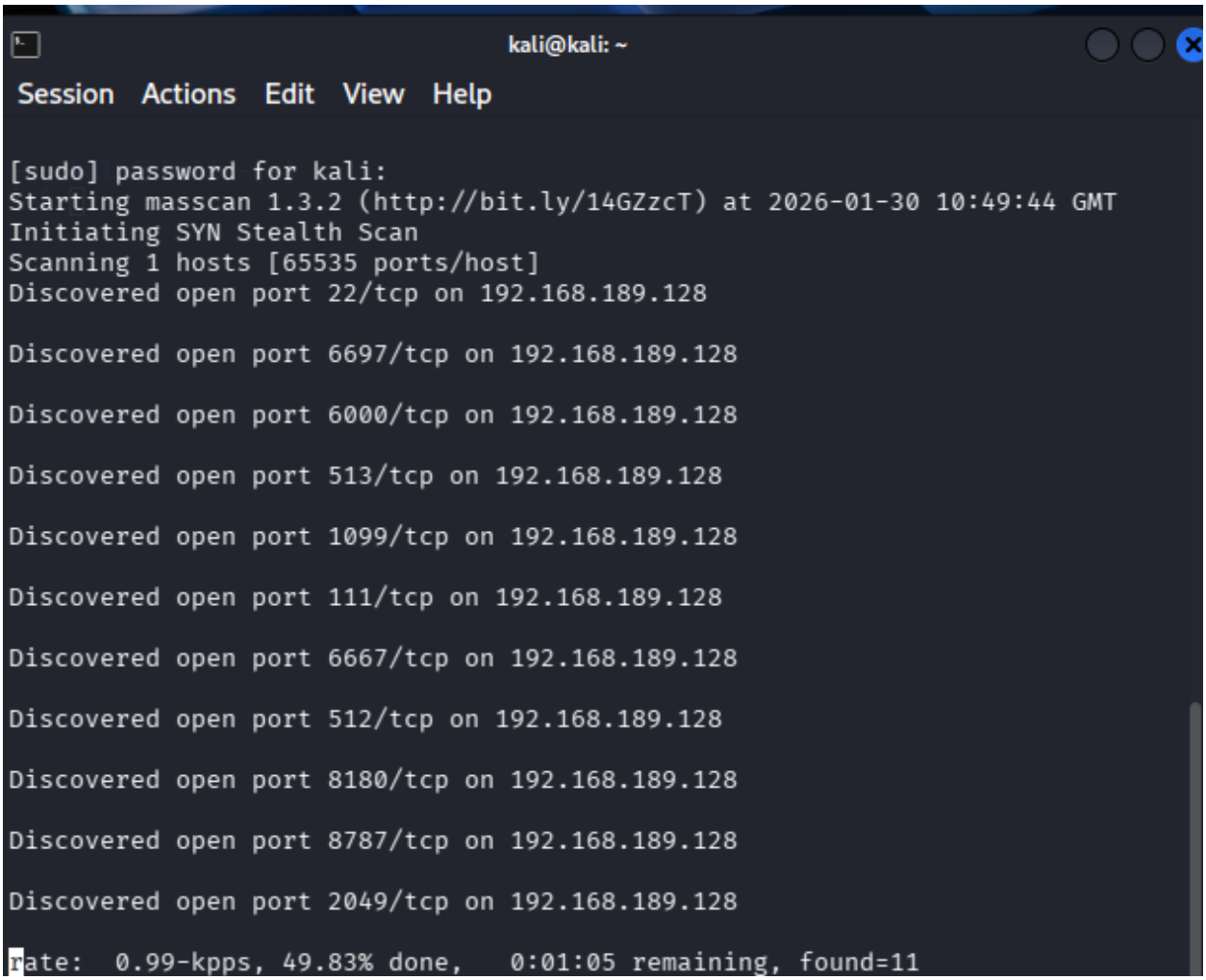
Nmap was used to identify open ports and running services.



Port	Protocol	Service	Description
21	TCP	FTP	File Transfer Service
22	TCP	SSH	Secure Remote Access
23	TCP	Telnet	Unencrypted Remote Login
25	TCP	SMTP	Email Transfer Service
53	TCP	DNS	Domain Name Service
80	TCP	HTTP	Web Server
111	TCP	RPCBind	Remote Procedure Call Service
139	TCP	NetBIOS-SSN	Windows File Sharing

Port	Protocol	Service	Description
445	TCP	Microsoft-DS	SMB File Sharing
512	TCP	Exec	Remote Command Execution
513	TCP	Login	Remote Login Service
514	TCP	Shell	Remote Shell Access
1099	TCP	RMI Registry	Java RMI Service
1524	TCP	Ingreslock	Backdoor / Remote Access
2049	TCP	NFS	Network File System
2121	TCP	FTP (ccproxy)	Alternative FTP Service
3306	TCP	MySQL	Database Service
5432	TCP	PostgreSQL	Database Service
5900	TCP	VNC	Remote Desktop Access
6000	TCP	X11	Graphical Display Service
6667	TCP	IRC	Chat Service
8009	TCP	AJP13	Apache JServ Protocol
8180	TCP	HTTP (Alt)	Alternative Web Service

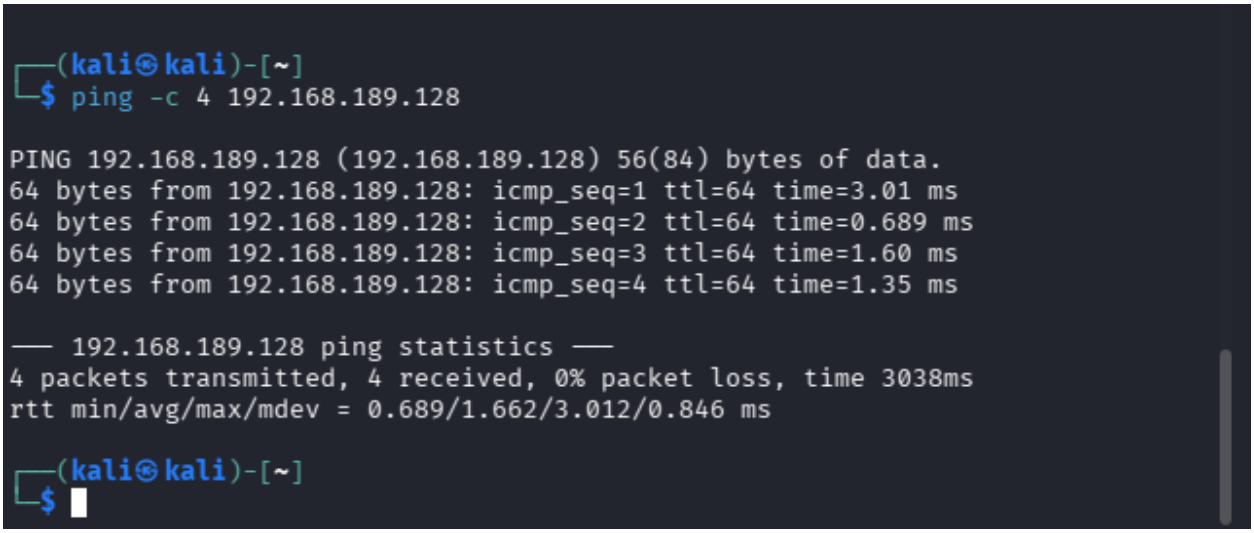
Masscan (from Kali Linux)



Masscan was executed from the Kali Linux machine to quickly identify open TCP ports on the Metasploitable target. The scan completed significantly faster than Nmap; however, it only reported open ports and did not provide service or version information. In contrast, Nmap provided detailed service and version data, demonstrating that Masscan is suitable for rapid port discovery while Nmap is used for in-depth analysis.

Metasploitable VM Lab

Target: Metasploitable VM
Attacker: Kali Linux
Target IP: 192.168.189.128



The reachability of the Metasploitable virtual machine was verified using ICMP ping

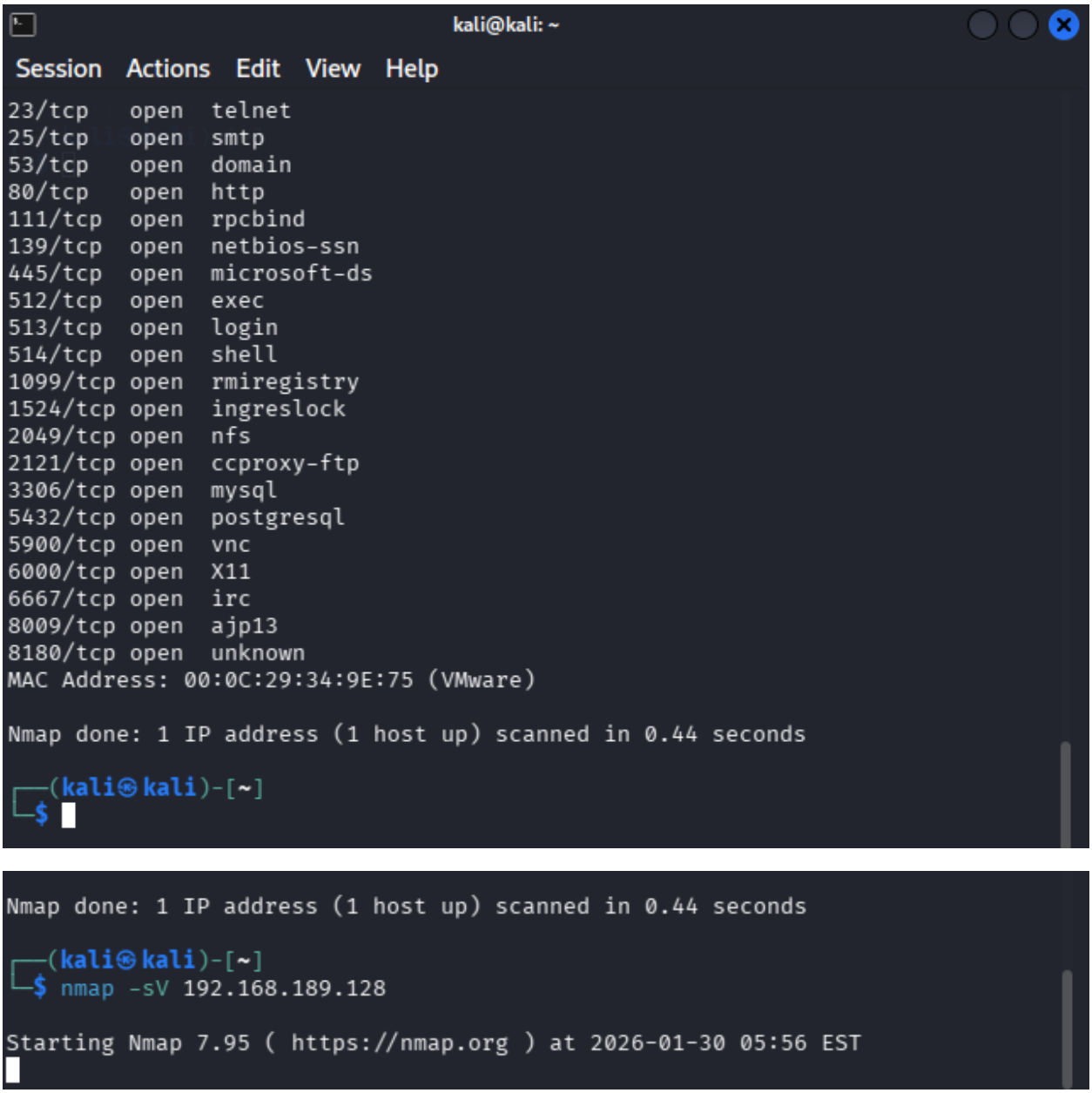


Figure 8 Identifying Services & Versions

SECURITY ANALYSIS

Service	Meaning	Security Risk
FTP (21)	File transfer service	Credentials sent in cleartext
SSH (22)	Remote login	Brute-force / weak passwords
Telnet (23)	Legacy remote access	Completely unencrypted
HTTP (80)	Web server	Vulnerable web apps
MySQL (3306)	Database service	Unauthorized data access

Security Interpretation

The presence of exposed services such as FTP, SSH, Telnet, HTTP, and MySQL significantly increases the attack surface of the system. FTP and Telnet transmit data in cleartext, making them vulnerable to credential interception. SSH, while encrypted, can be targeted through brute-force attacks if weak credentials are used. The exposed MySQL service could allow unauthorized access to sensitive database information. These findings demonstrate how misconfigured or legacy services can lead to serious security vulnerabilities.