

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

```
kali@kali: ~  
Session Actions Edit View Help  
Discovered open port 139/tcp on 192.168.189.128  
Discovered open port 42964/tcp on 192.168.189.128  
  
(kali@kali)-[~]  
$ whois vulnweb.com  
Domain Name: VULNWEB.COM  
Registry Domain ID: 1602006391_DOMAIN_COM-VRSN  
Registrar WHOIS Server: whois.gandi.net  
Registrar URL: http://www.gandi.net  
Updated Date: 2025-11-17T09:34:20Z  
Creation Date: 2010-06-14T07:50:29Z  
Registry Expiry Date: 2027-06-14T07:50:29Z  
Registrar: Gandi SAS  
Registrar IANA ID: 81  
Registrar Abuse Contact Email: abuse@support.gandi.net  
Registrar Abuse Contact Phone: +33.170377661  
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransf  
erProhibited  
Name Server: NS-105-A.GANDI.NET  
Name Server: NS-11-B.GANDI.NET  
Name Server: NS-140-C.GANDI.NET  
DNSSEC: unsigned  
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wi  
cf/  
>>> Last update of whois database: 2026-01-29T18:55:29Z <<<
```

Figure 1 WHOIS output

DNS Enumeration

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

Command

dig vulnweb.com

```
kali@kali: ~  
Session Actions Edit View Help  
(kali@kali)-[~]  
$ dig vulnweb.com  
  
; <<>> DiG 9.20.15-2-Debian <<>> vulnweb.com  
;; global options: +cmd  
;; Got answer:  
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 44658  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 1232  
; COOKIE: fdc4e352d794fcf201000000697bb2da6e6b23eec4616f86 (good)  
;; QUESTION SECTION:  
;vulnweb.com.                IN      A  
  
;; ANSWER SECTION:  
vulnweb.com.                5       IN      A      44.228.249.3  
  
;; Query time: 251 msec  
;; SERVER: 192.168.189.2#53(192.168.189.2) (UDP)  
;; WHEN: Thu Jan 29 14:19:54 EST 2026  
;; MSG SIZE rcvd: 84
```

Command

dig NS vulnweb.com

```
kali@kali: ~  
Session Actions Edit View Help  
└─$ dig NS vulnweb.com  
  
; <<>> DiG 9.20.15-2-Debian <<>> NS vulnweb.com  
;; global options: +cmd  
;; Got answer:  
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 61479  
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 5  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 1232  
; COOKIE: e1656a3736b909c801000000697bb31c87a700d0b9af2898 (good)  
;; QUESTION SECTION:  
;vulnweb.com. IN NS  
  
;; ANSWER SECTION:  
vulnweb.com. 5 IN NS ns-105-a.gandi.net.  
vulnweb.com. 5 IN NS ns-140-c.gandi.net.  
vulnweb.com. 5 IN NS ns-11-b.gandi.net.  
  
;; ADDITIONAL SECTION:  
ns-11-b.gandi.net. 5 IN A 213.167.230.12  
ns-105-a.gandi.net. 5 IN A 173.246.100.106  
ns-11-b.gandi.net. 5 IN AAAA 2001:4b98:aaab::c  
ns-105-a.gandi.net. 5 IN AAAA 2001:4b98:aaaa::6a  
  
;; Query time: 47 msec  
;; SERVER: 192.168.189.2#53(192.168.189.2) (UDP)  
;; WHEN: Thu Jan 29 14:21:00 EST 2026
```

Figure 2 ns

Command

dig MX vulnweb.com

```

kali@kali: ~
Session Actions Edit View Help

(kali@kali)-[~]
$ dig MS vulnweb.com

; <<>> DiG 9.20.15-2-Debian <<>> MS vulnweb.com
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 29623
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 1232
; COOKIE: 8cc5bcf401117b7801000000697bb327ca6f1ad223d18ae8 (good)
;; QUESTION SECTION:
;MS.                                IN      A

;; AUTHORITY SECTION:
ms.                5        IN      SOA     mnidns1.mninet.ms. hostmaster
.mninet.ms. 2026012928 21600 3600 604800 38400

;; Query time: 48 msec
;; SERVER: 192.168.189.2#53(192.168.189.2) (UDP)
;; WHEN: Thu Jan 29 14:21:11 EST 2026
;; MSG SIZE rcvd: 125

;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 2476
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

```

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

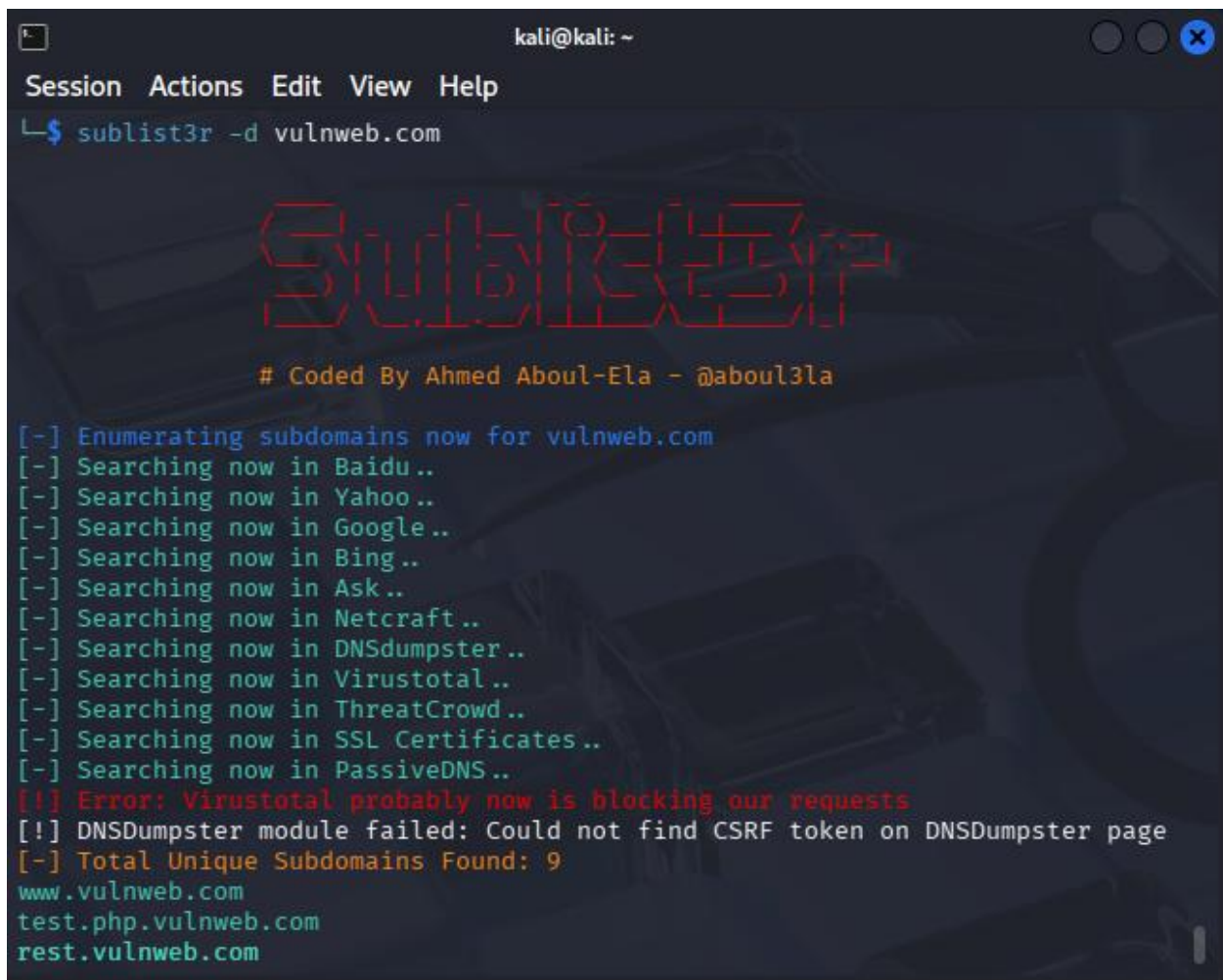
Subdomain Enumeration

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

Tool 1: Sublist3r

Command

```
sublist3r -d vulnweb.com
```



```
kali@kali: ~
Session Actions Edit View Help
└─$ sublist3r -d vulnweb.com

  SUBLIST3R

# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for vulnweb.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSDumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[!] DNSDumpster module failed: Could not find CSRF token on DNSDumpster page
[-] Total Unique Subdomains Found: 9
www.vulnweb.com
test.php.vulnweb.com
rest.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

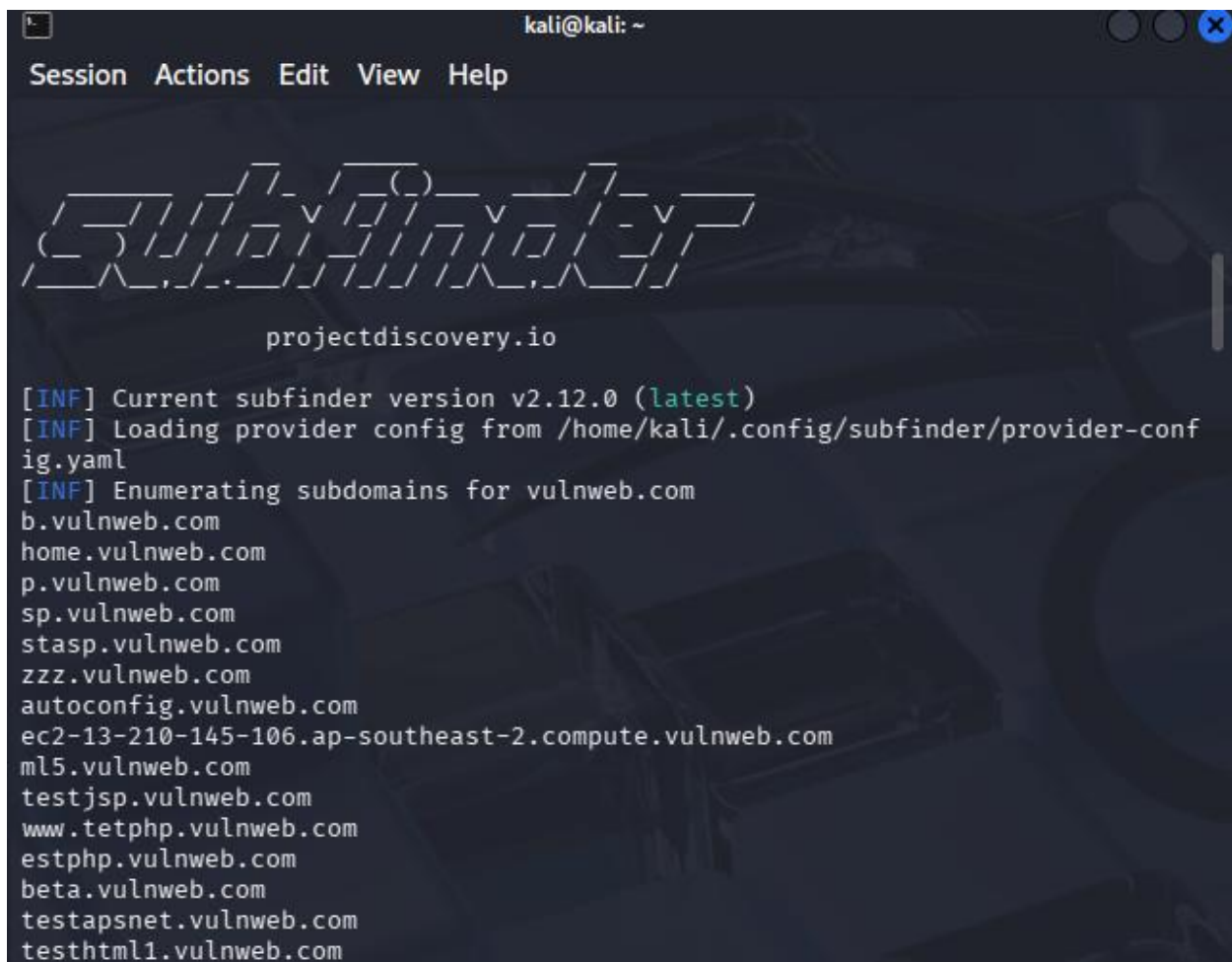
testaspnet.vulnweb.com

testhtml1.vulnweb.com

Tool 2: Amass

Command

amass enum -passive -d vulnweb.com



```
kali@kali: ~  
Session Actions Edit View Help  
  
Subfinder  
projectdiscovery.io  
  
[INF] Current subfinder version v2.12.0 (latest)  
[INF] Loading provider config from /home/kali/.config/subfinder/provider-config.yaml  
[INF] Enumerating subdomains for vulnweb.com  
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  
testapsnet.vulnweb.com  
testhtml1.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

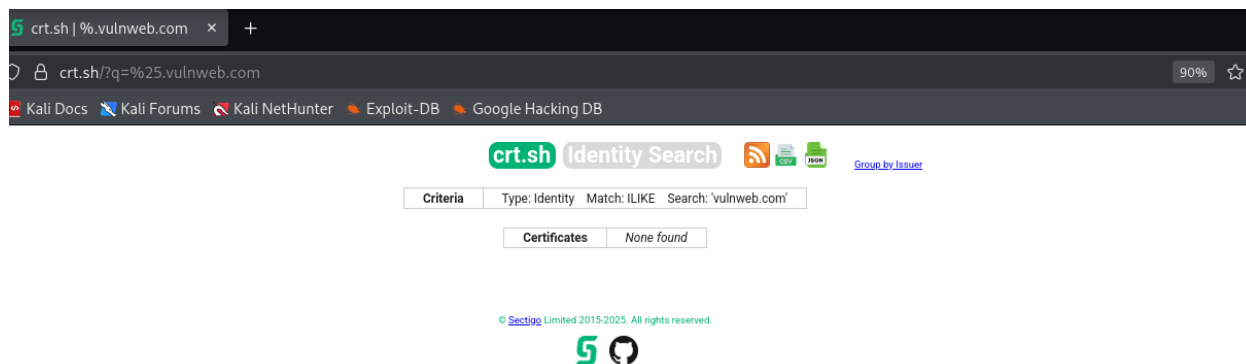
%25.vulnweb.com

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.

```
sudo apt install jq
=== CRT.SH RESULTS ===
zsh: unmatched '
zsh: parse error in command substitution

(kali㉿kali)-[~]
$ theHarvester -d vulnweb.com -b google
Read proxies.yaml from /etc/theHarvester/proxies.yaml
*****
*                               *
* | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | *
* | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | *
* | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | *
* | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | *
* | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | *
*                               *
* theHarvester 4.8.2           *
* Coded by Christian Martorella *
* Edge-Security Research       *
* cmartorella@edge-security.com *
*                               *
*****
The following engines are not supported: {'google'}

[!] Invalid source.

(kali㉿kali)-[~]
$
```

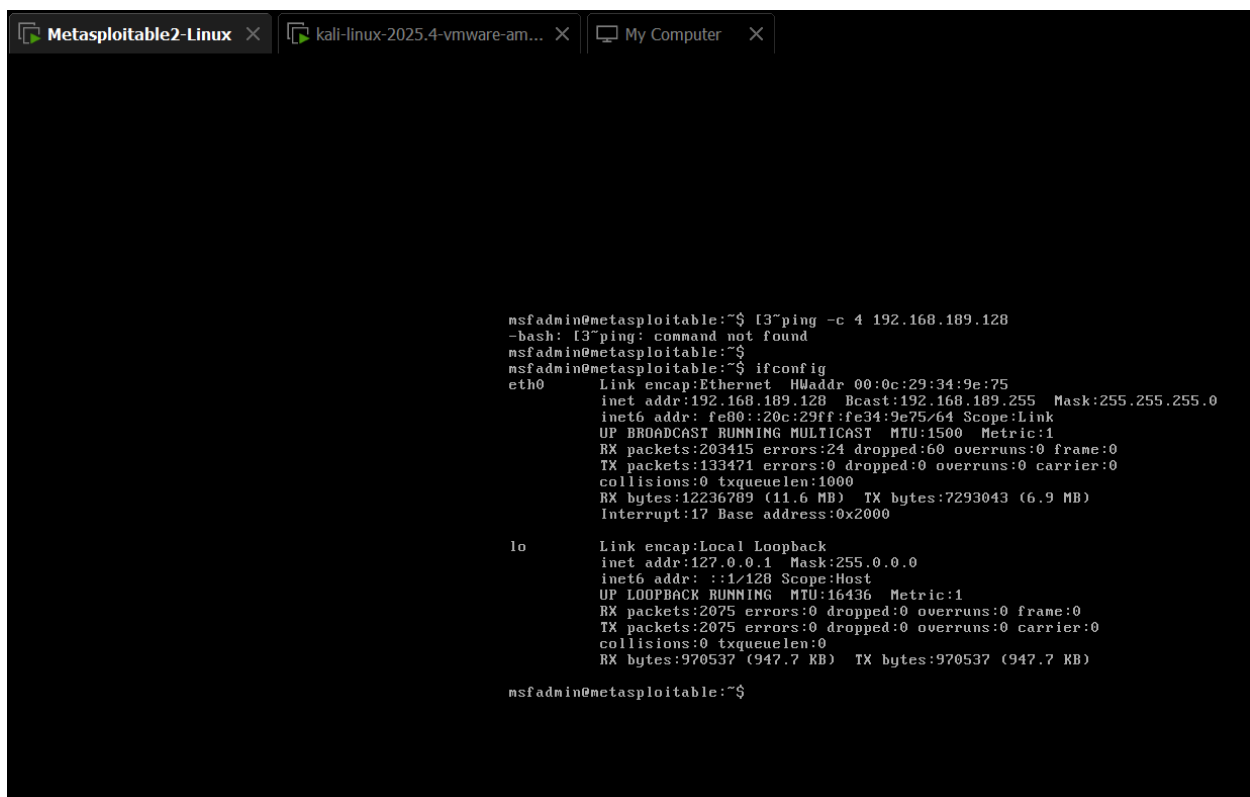
OSINT Summary

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.



```
nsfadmin@metasploitable:~$ [3~ping -c 4 192.168.189.128
-bash: [3~ping: command not found
nsfadmin@metasploitable:~$
nsfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:34:9e:75
          inet addr:192.168.189.128  Bcast:192.168.189.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe34:9e75/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:203415 errors:24 dropped:60 overruns:0 frame:0
          TX packets:133471 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:12236789 (11.6 MB)  TX bytes:7293043 (6.9 MB)
          Interrupt:17 Base address:0x2000

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:2075 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2075 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:970537 (947.7 KB)  TX bytes:970537 (947.7 KB)

nsfadmin@metasploitable:~$
```

Figure 6 Metasploitable terminal

```
(kali㉿kali)-[~]  
$ ping 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=5.22 ms  
64 bytes from 192.168.189.128: icmp_seq=2 ttl=64 time=6.10 ms  
64 bytes from 192.168.189.128: icmp_seq=3 ttl=64 time=0.921 ms  
64 bytes from 192.168.189.128: icmp_seq=4 ttl=64 time=1.05 ms  
64 bytes from 192.168.189.128: icmp_seq=5 ttl=64 time=0.769 ms  
64 bytes from 192.168.189.128: icmp_seq=6 ttl=64 time=7.75 ms  
64 bytes from 192.168.189.128: icmp_seq=7 ttl=64 time=3.02 ms  
64 bytes from 192.168.189.128: icmp_seq=8 ttl=64 time=1.37 ms  
64 bytes from 192.168.189.128: icmp_seq=9 ttl=64 time=0.968 ms  
64 bytes from 192.168.189.128: icmp_seq=10 ttl=64 time=1.30 ms  
64 bytes from 192.168.189.128: icmp_seq=11 ttl=64 time=8.40 ms  
64 bytes from 192.168.189.128: icmp_seq=12 ttl=64 time=1.49 ms  
64 bytes from 192.168.189.128: icmp_seq=13 ttl=64 time=1.58 ms
```

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.

```
kali@kali: ~  
Session Actions Edit View Help  
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  
MAC Address: 00:0C:29:34:9E:75 (VMware)  
  
Nmap done: 1 IP address (1 host up) scanned in 1.53 seconds
```

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)


```
kali@kali: ~  
Session Actions Edit View Help  
[sudo] password for kali:  
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2026-01-30 10:49:44 GMT  
Initiating SYN Stealth Scan  
Scanning 1 hosts [65535 ports/host]  
Discovered open port 22/tcp on 192.168.189.128  
  
Discovered open port 6697/tcp on 192.168.189.128  
  
Discovered open port 6000/tcp on 192.168.189.128  
  
Discovered open port 513/tcp on 192.168.189.128  
  
Discovered open port 1099/tcp on 192.168.189.128  
  
Discovered open port 111/tcp on 192.168.189.128  
  
Discovered open port 6667/tcp on 192.168.189.128  
  
Discovered open port 512/tcp on 192.168.189.128  
  
Discovered open port 8180/tcp on 192.168.189.128  
  
Discovered open port 8787/tcp on 192.168.189.128  
  
Discovered open port 2049/tcp on 192.168.189.128  
  
Rate: 0.99-kpps, 49.83% done, 0:01:05 remaining, found=11
```

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

```
(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=3.01 ms  
64 bytes from 192.168.189.128: icmp_seq=2 ttl=64 time=0.689 ms  
64 bytes from 192.168.189.128: icmp_seq=3 ttl=64 time=1.60 ms  
64 bytes from 192.168.189.128: icmp_seq=4 ttl=64 time=1.35 ms  
  
— 192.168.189.128 ping statistics —  
4 packets transmitted, 4 received, 0% packet loss, time 3038ms  
rtt min/avg/max/mdev = 0.689/1.662/3.012/0.846 ms  
  
(kali㉿kali)-[~]  
$
```

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

```
kali@kali: ~  
Session Actions Edit View Help  
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  
MAC Address: 00:0C:29:34:9E:75 (VMware)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds  
  
(kali@kali)-[~]  
$
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds  
  
(kali@kali)-[~]  
$ nmap -sV 192.168.189.128  
  
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-30 05:56 EST  
$
```

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.