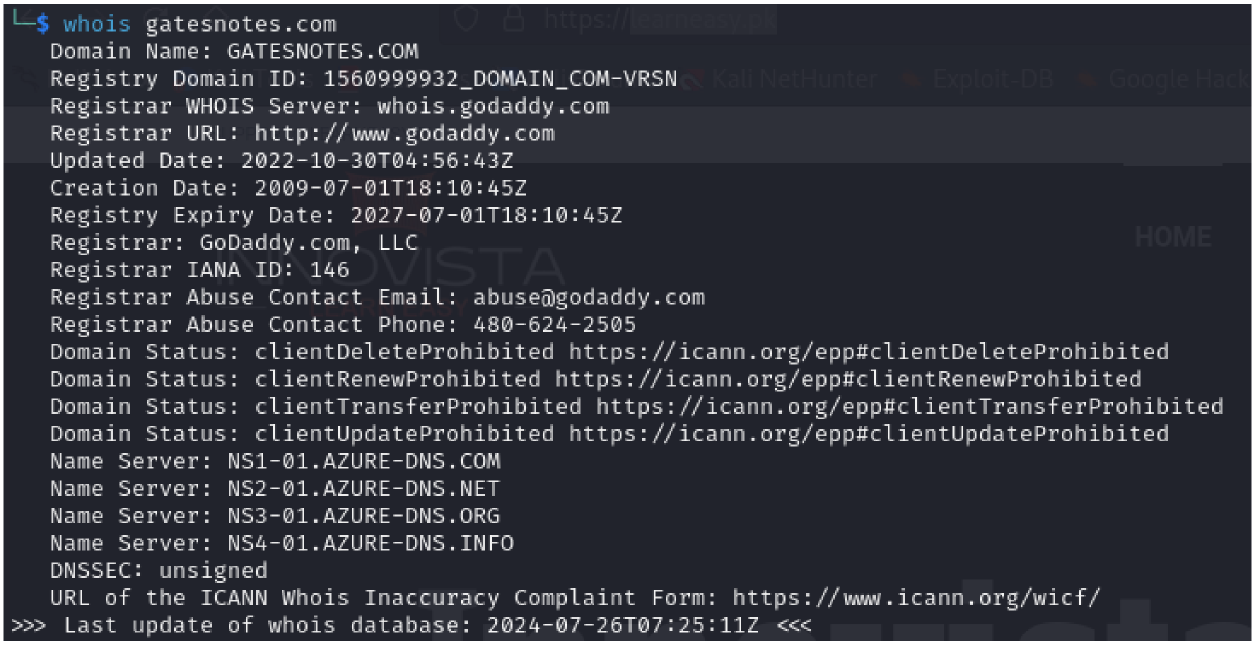
Email and Domain Information Gathering Tools

Tool 1: Whois



```
└─$ whois gatesnotes.com
   Domain Name: GATESNOTES.COM
   Registry Domain ID: 1560999932_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.godaddy.com
   Registrar URL: http://www.godaddy.com
   Updated Date: 2022-10-30T04:56:43Z
   Creation Date: 2009-07-01T18:10:45Z
   Registry Expiry Date: 2027-07-01T18:10:45Z
   Registrar: GoDaddy.com, LLC
   Registrar IANA ID: 146
   Registrar Abuse Contact Email: abuse@godaddy.com
   Registrar Abuse Contact Phone: 480-624-2505
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Name Server: NS1-01.AZURE-DNS.COM
   Name Server: NS2-01.AZURE-DNS.NET
   Name Server: NS3-01.AZURE-DNS.ORG
   Name Server: NS4-01.AZURE-DNS.INFO
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-07-26T07:25:11Z <<<
```

Other info Retrieved

The Registry database contains ONLY .COM, .NET, .EDU domains and

Registrars.

Domain Name: gatesnotes.com

Registry Domain ID: 1560999932_DOMAIN_COM-VRSN

Registrar WHOIS Server: whois.godaddy.com

Registrar URL: https://www.godaddy.com

Updated Date: 2019-09-11T15:42:20Z

Creation Date: 2009-07-01T13:10:45Z

Registrar Registration Expiration Date: 2027-07-01T13:10:45Z

Registrar: GoDaddy.com, LLC

Registrar IANA ID: 146

Registrar Abuse Contact Email: abuse@godaddy.com

Registrar Abuse Contact Phone: +1.4806242505

Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited

Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited

Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited

Registry Registrant ID: Not Available From Registry

Registrant Name: Registration Private

Registrant Organization: Domains By Proxy, LLC

Registrant Street: DomainsByProxy.com

Registrant Street: 100 S. Mill Ave, Suite 1600

Registrant City: Tempe

Registrant State/Province: Arizona

Registrant Postal Code: 85281

Registrant Country: US

Registrant Phone: +1.4806242599

Registrant Phone Ext:

Registrant Fax:

Registrant Fax Ext:

Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=gatesnotes.com

Registry Admin ID: Not Available From Registry

Admin Name: Registration Private

Admin Organization: Domains By Proxy, LLC

Admin Street: DomainsByProxy.com

Admin Street: 100 S. Mill Ave, Suite 1600

Admin City: Tempe

Admin State/Province: Arizona

Admin Postal Code: 85281

Admin Country: US

Admin Phone: +1.4806242599

Admin Phone Ext:

Admin Fax:

Admin Fax Ext:

Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=gatesnotes.com

Registry Tech ID: Not Available From Registry

Tech Name: Registration Private

Tech Organization: Domains By Proxy, LLC

Tech Street: DomainsByProxy.com

Tech Street: 100 S. Mill Ave, Suite 1600

Tech City: Tempe

Tech State/Province: Arizona

Tech Postal Code: 85281

Tech Country: US

Tech Phone: +1.4806242599

Tech Phone Ext:

Tech Fax:

Tech Fax Ext:

Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=gatesnotes.com

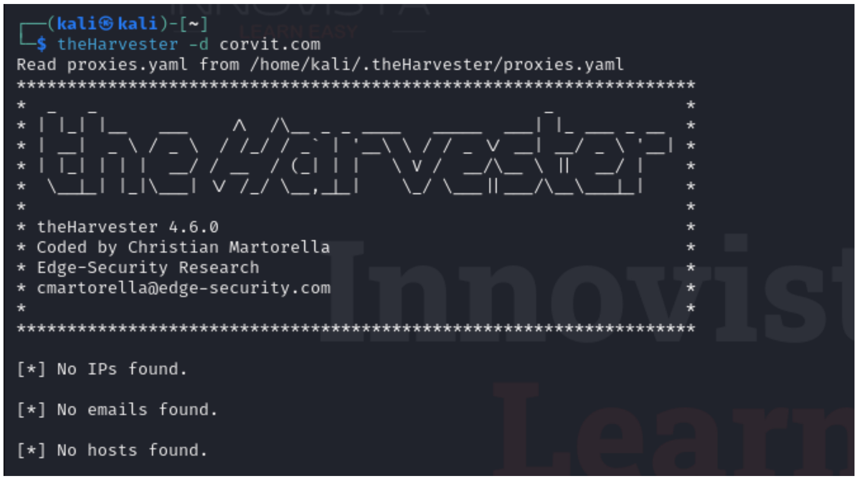
Name Server: NS1-01.AZURE-DNS.COM

Name Server: NS2-01.AZURE-DNS.NET

Name Server: NS3-01.AZURE-DNS.ORG

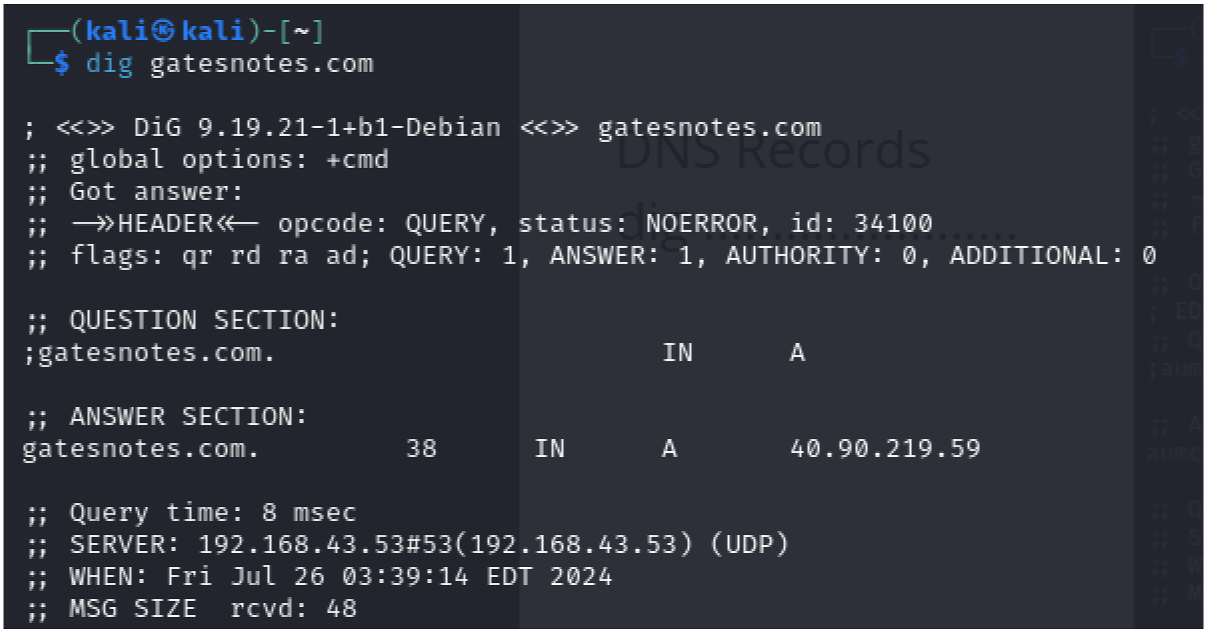
Name Server: NS4-01.AZURE-DNS.INFO

Tool 2: theHarvester



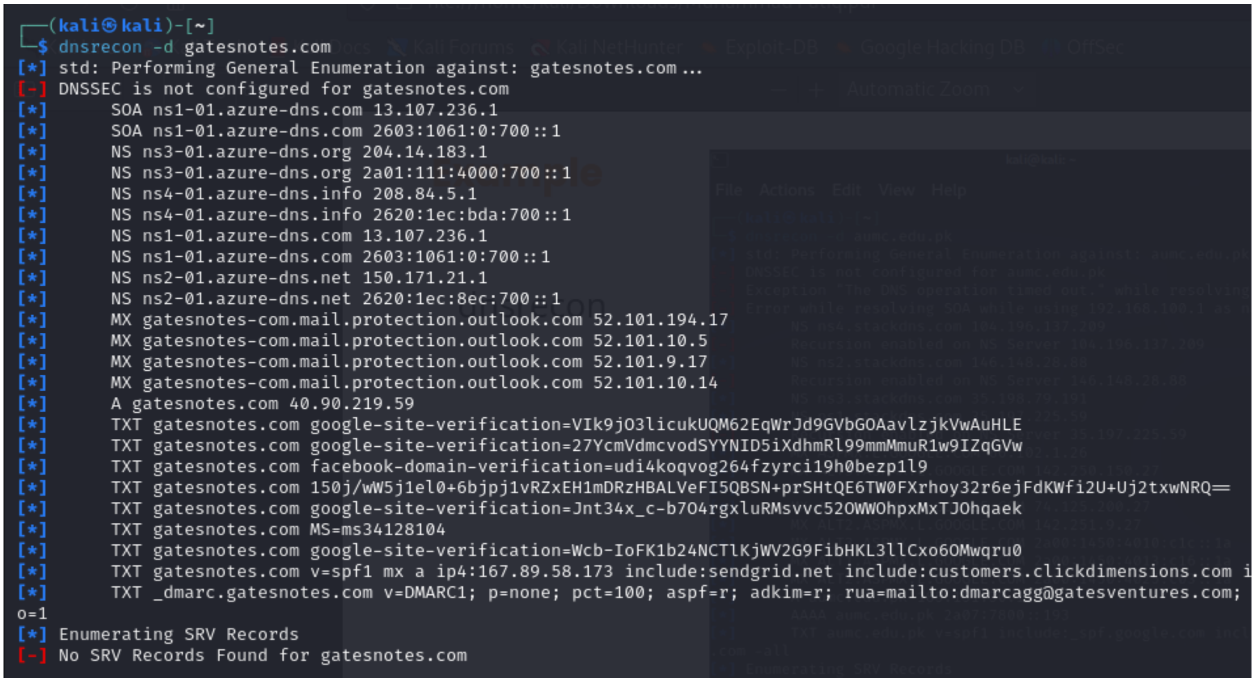
```
┌──(kali㉿kali)-[~]
└─$ theHarvester -d corvit.com
Read proxies.yaml from /home/kali/.theHarvester/proxies.yaml
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.6.0                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] No IPs found.

[*] No emails found.

[*] No hosts found.
```

Tool 3: dig



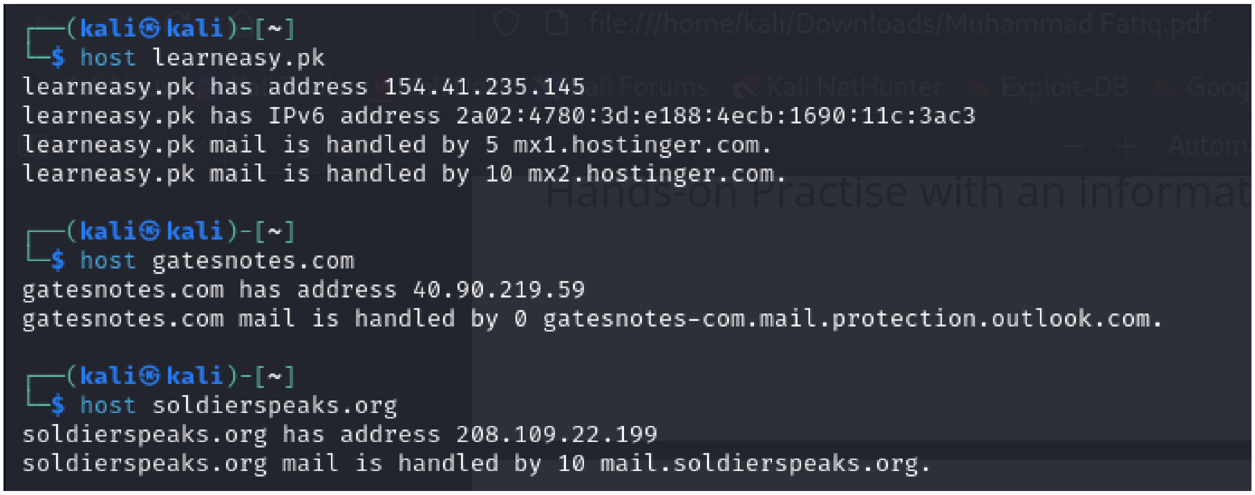
```
┌──(kali㉿kali)-[~]
└─$ dig gatesnotes.com

; <<>> DiG 9.19.21-1+b1-Debian <<>> gatesnotes.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34100
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;gatesnotes.com.                        IN      A

;; ANSWER SECTION:
gatesnotes.com.         38      IN      A       40.90.219.59

;; Query time: 8 msec
;; SERVER: 192.168.43.53#53(192.168.43.53) (UDP)
;; WHEN: Fri Jul 26 03:39:14 EDT 2024
;; MSG SIZE  rcvd: 48
```

Tool 4: dnsrecon



```
┌──(kali㉿kali)-[~]
└─$ dnsrecon -d gatesnotes.com
[*] std: Performing General Enumeration against: gatesnotes.com...
[-] DNSSEC is not configured for gatesnotes.com
[*]      SOA ns1-01.azure-dns.com 13.107.236.1
[*]      SOA ns1-01.azure-dns.com 2603:1061:0:700::1
[*]      NS ns3-01.azure-dns.org 204.14.183.1
[*]      NS ns3-01.azure-dns.org 2a01:111:4000:700::1
[*]      NS ns4-01.azure-dns.info 208.84.5.1
[*]      NS ns4-01.azure-dns.info 2620:1ec:bda:700::1
[*]      NS ns1-01.azure-dns.com 13.107.236.1
[*]      NS ns1-01.azure-dns.com 2603:1061:0:700::1
[*]      NS ns2-01.azure-dns.net 150.171.21.1
[*]      NS ns2-01.azure-dns.net 2620:1ec:8ec:700::1
[*]      MX gatesnotes-com.mail.protection.outlook.com 52.101.194.17
[*]      MX gatesnotes-com.mail.protection.outlook.com 52.101.10.5
[*]      MX gatesnotes-com.mail.protection.outlook.com 52.101.9.17
[*]      MX gatesnotes-com.mail.protection.outlook.com 52.101.10.14
[*]      A gatesnotes.com 40.90.219.59
[*]      TXT gatesnotes.com google-site-verification=VIk9jO3licukUQM62EqWrJd9GVbGOAavlzjkVwAuHLE
[*]      TXT gatesnotes.com google-site-verification=27YcmVdmcvodSYYNID5iXdhmRl99mmMmuR1w9IZqGVw
[*]      TXT gatesnotes.com facebook-domain-verification=udi4koqvog264fzyrci19h0bezp1l9
[*]      TXT gatesnotes.com 150j/wW5j1el0+6bjpj1vRZxEH1mDRzHBALVeFI5QBSN+prSHtQE6TW0FXrhoy32r6ejFdKWfi2U+Uj2txwNRQ==
[*]      TXT gatesnotes.com google-site-verification=Jnt34x_c-b7O4rgxluRMsvvc52OWWOhpxMxTJOhqaek
[*]      TXT gatesnotes.com MS=ms34128104
[*]      TXT gatesnotes.com google-site-verification=Wcb-IoFK1b24NCTlKjWV2G9FibHKL3llCxo6OMwqru0
[*]      TXT gatesnotes.com v=spf1 mx a ip4:167.89.58.173 include:sendgrid.net include:customers.clickdimensions.com i
[*]      TXT _dmarc.gatesnotes.com v=DMARC1; p=none; pct=100; aspf=r; adkim=r; rua=mailto:dmarcagg@gatesventures.com;
o=1
[*] Enumerating SRV Records
[-] No SRV Records Found for gatesnotes.com
```

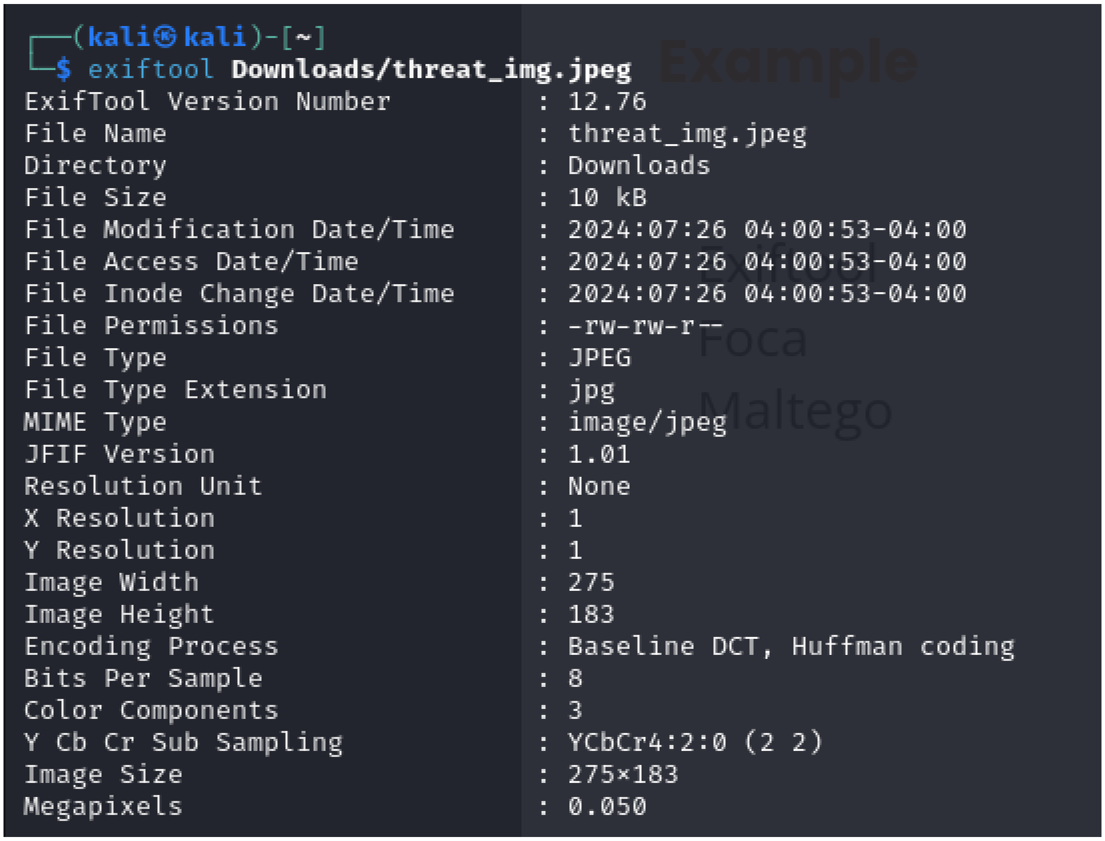
Tool 5: host



```
┌──(kali㉿kali)-[~]
└─$ host learneasy.pk
learneasy.pk has address 154.41.235.145
learneasy.pk has IPv6 address 2a02:4780:3d:e188:4ecb:1690:11c:3ac3
learneasy.pk mail is handled by 5 mx1.hostinger.com.
learneasy.pk mail is handled by 10 mx2.hostinger.com.

┌──(kali㉿kali)-[~]
└─$ host gatesnotes.com
gatesnotes.com has address 40.90.219.59
gatesnotes.com mail is handled by 0 gatesnotes-com.mail.protection.outlook.com.

┌──(kali㉿kali)-[~]
└─$ host soldierspeaks.org
soldierspeaks.org has address 208.109.22.199
soldierspeaks.org mail is handled by 10 mail.soldierspeaks.org.
```

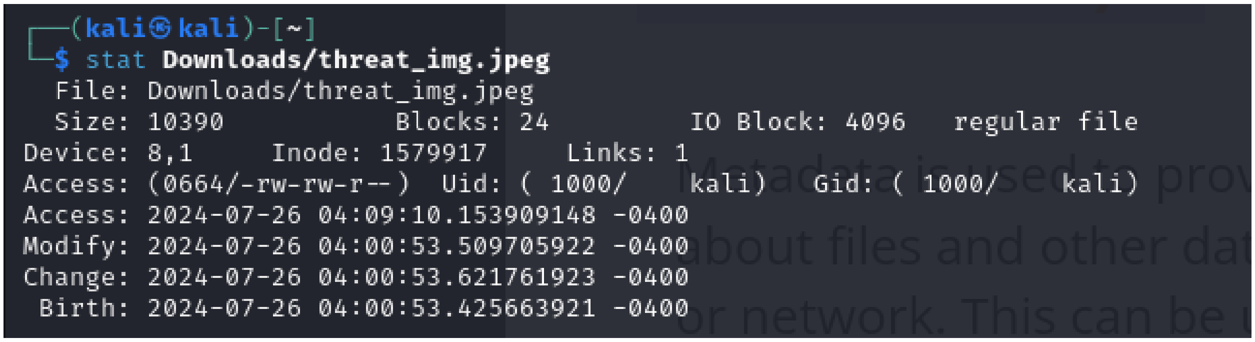
Metadata Analysis Tools

Tool 1: exiftool



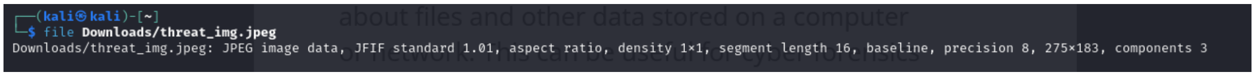
```
┌──(kali㉿kali)-[~]
└─$ exiftool Downloads/threat_img.jpeg
ExifTool Version Number         : 12.76
File Name                       : threat_img.jpeg
Directory                       : Downloads
File Size                       : 10 kB
File Modification Date/Time     : 2024:07:26 04:00:53-04:00
File Access Date/Time           : 2024:07:26 04:00:53-04:00
File Inode Change Date/Time     : 2024:07:26 04:00:53-04:00
File Permissions                : -rw-rw-r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
Image Width                     : 275
Image Height                    : 183
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 275x183
Megapixels                      : 0.050
```

Tool 2: stat



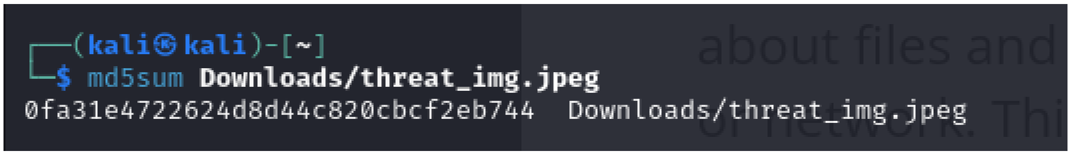
```
┌──(kali㉿kali)-[~]
└─$ stat Downloads/threat_img.jpeg
  File: Downloads/threat_img.jpeg
  Size: 10390           Blocks: 24         IO Block: 4096   regular file
Device: 8,1     Inode: 1579917     Links: 1
Access: (0664/-rw-rw-r--)  Uid: ( 1000/    kali)   Gid: ( 1000/    kali)
Access: 2024-07-26 04:09:10.153909148 -0400
Modify: 2024-07-26 04:00:53.509705922 -0400
Change: 2024-07-26 04:00:53.621761923 -0400
 Birth: 2024-07-26 04:00:53.425663921 -0400
```

Tool 3: file



```
┌──(kali㉿kali)-[~]
└─$ file Downloads/threat_img.jpeg
Downloads/threat_img.jpeg: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 275x183, components 3
```

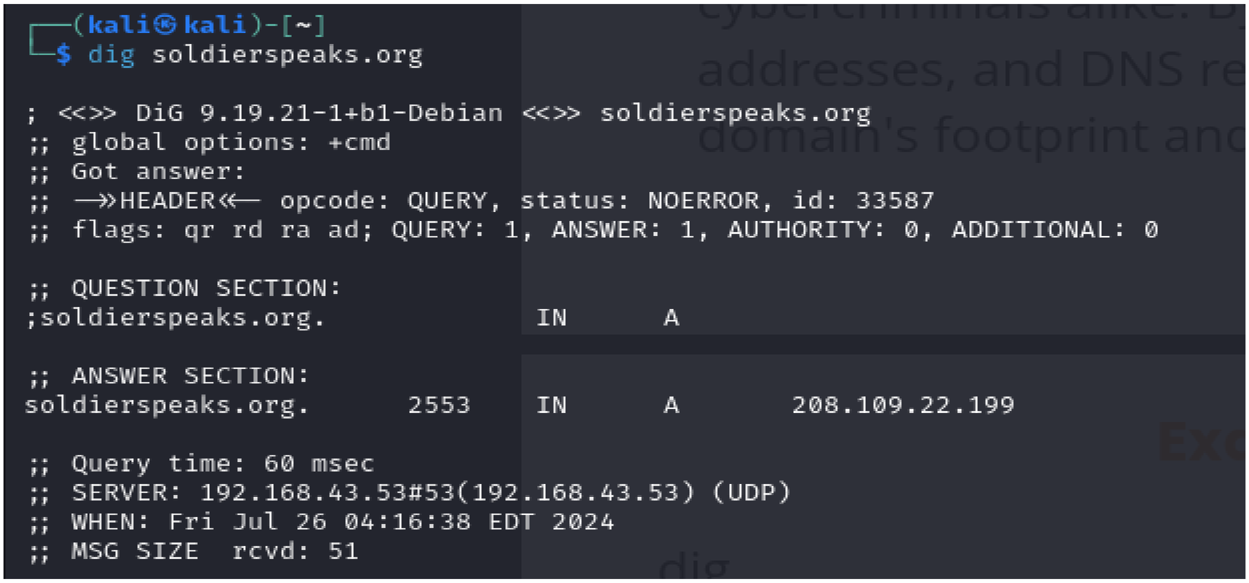
Tool 4: md5sum



```
┌──(kali㉿kali)-[~]
└─$ md5sum Downloads/threat_img.jpeg
0fa31e4722624d8d44c820cbcf2eb744  Downloads/threat_img.jpeg
```

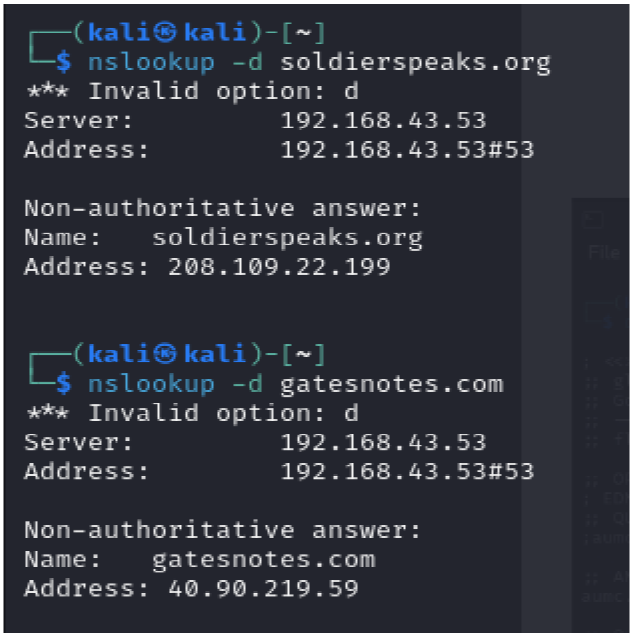
DNS Enumeration Tools

Tool 1: dig



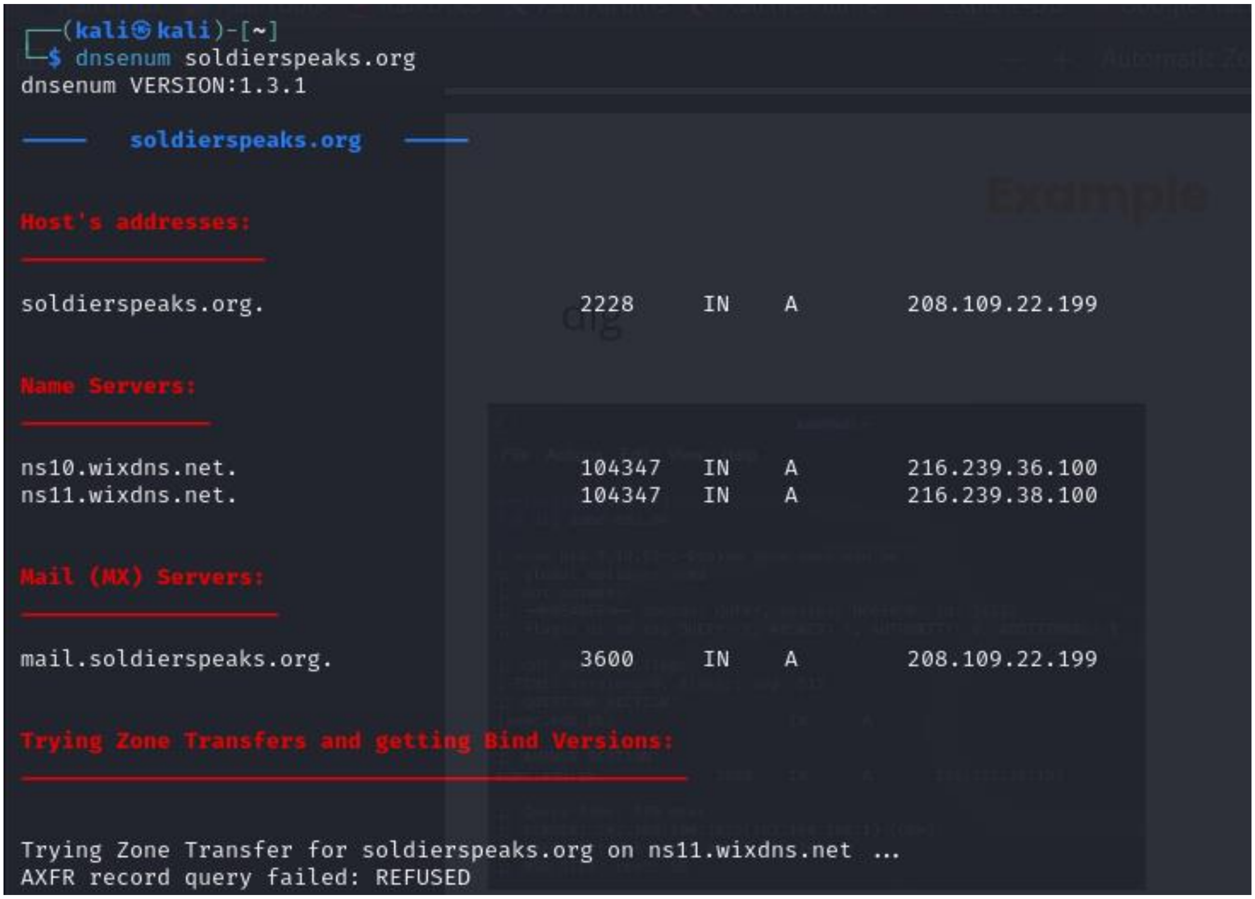
```
┌──(kali㉿kali)-[~]
└─$ dig soldierspeaks.org

; <<>> DiG 9.19.21-1+b1-Debian <<>> soldierspeaks.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33587
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;soldierspeaks.org.             IN      A

;; ANSWER SECTION:
soldierspeaks.org.      2553    IN      A       208.109.22.199

;; Query time: 60 msec
;; SERVER: 192.168.43.53#53(192.168.43.53) (UDP)
;; WHEN: Fri Jul 26 04:16:38 EDT 2024
;; MSG SIZE  rcvd: 51
```

Tool 2: nslookup



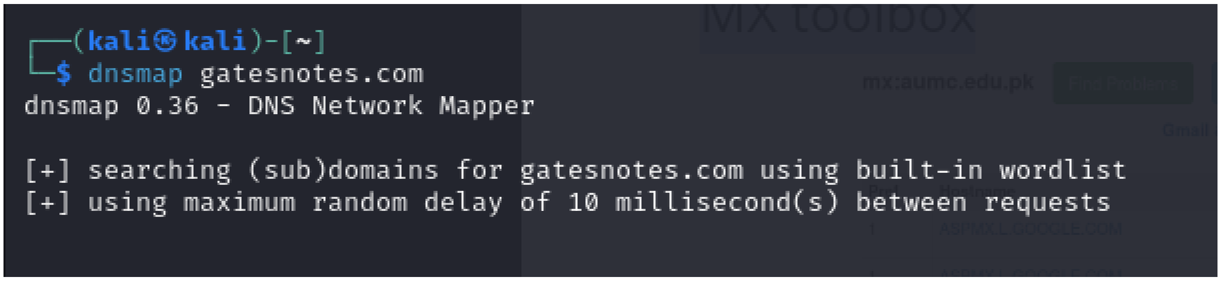
```
┌──(kali㉿kali)-[~]
└─$ nslookup -d soldierspeaks.org
*** Invalid option: d
Server:         192.168.43.53
Address:        192.168.43.53#53

Non-authoritative answer:
Name:   soldierspeaks.org
Address: 208.109.22.199


┌──(kali㉿kali)-[~]
└─$ nslookup -d gatesnotes.com
*** Invalid option: d
Server:         192.168.43.53
Address:        192.168.43.53#53

Non-authoritative answer:
Name:   gatesnotes.com
Address: 40.90.219.59
```

Tool 3: dnsenum



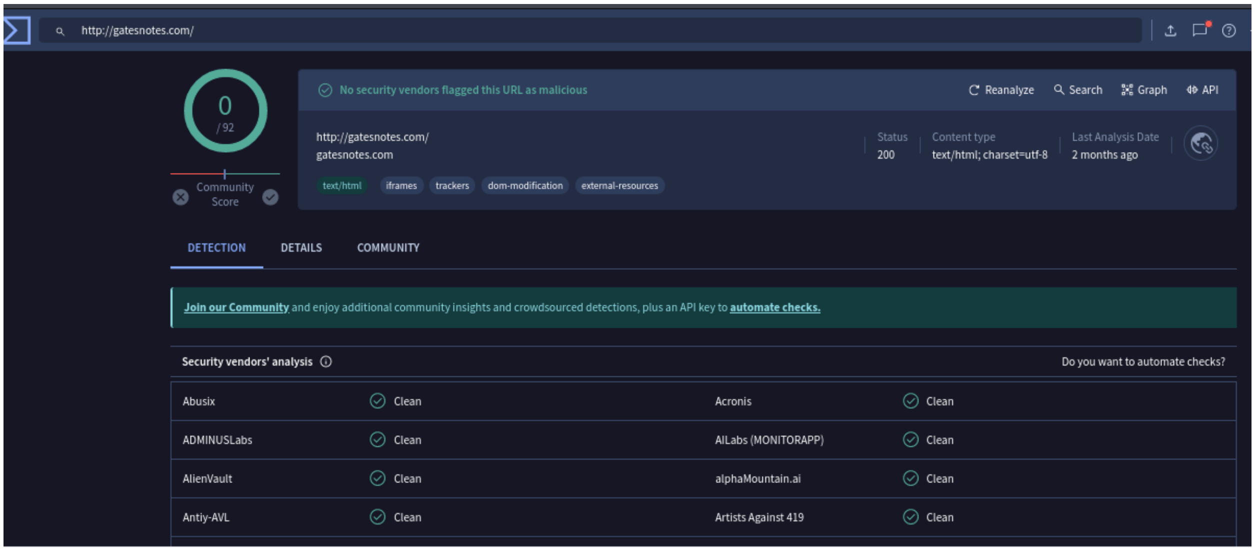
```
┌──(kali㉿kali)-[~]
└─$ dnsenum soldierspeaks.org
dnsenum VERSION:1.3.1

─────   soldierspeaks.org   ─────


Host's addresses:
__________________

soldierspeaks.org.                       2228     IN    A        208.109.22.199


Name Servers:
______________

ns10.wixdns.net.                         104347   IN    A        216.239.36.100
ns11.wixdns.net.                         104347   IN    A        216.239.38.100


Mail (MX) Servers:
___________________

mail.soldierspeaks.org.                  3600     IN    A        208.109.22.199


Trying Zone Transfers and getting Bind Versions:
_________________________________________________


Trying Zone Transfer for soldierspeaks.org on ns11.wixdns.net ...
AXFR record query failed: REFUSED
```

Tool 4: dnsmap



```
┌──(kali㉿kali)-[~]
└─$ dnsmap gatesnotes.com
dnsmap 0.36 - DNS Network Mapper

[+] searching (sub)domains for gatesnotes.com using built-in wordlist
[+] using maximum random delay of 10 millisecond(s) between requests
```

Tool 5: Virus Total



No security vendors flagged this URL as malicious

http://gatesnotes.com/
gatesnotes.com

Status 200

Content type text/html; charset=utf-8

Last Analysis Date 2 months ago

text/html iframes trackers dom-modification external-resources

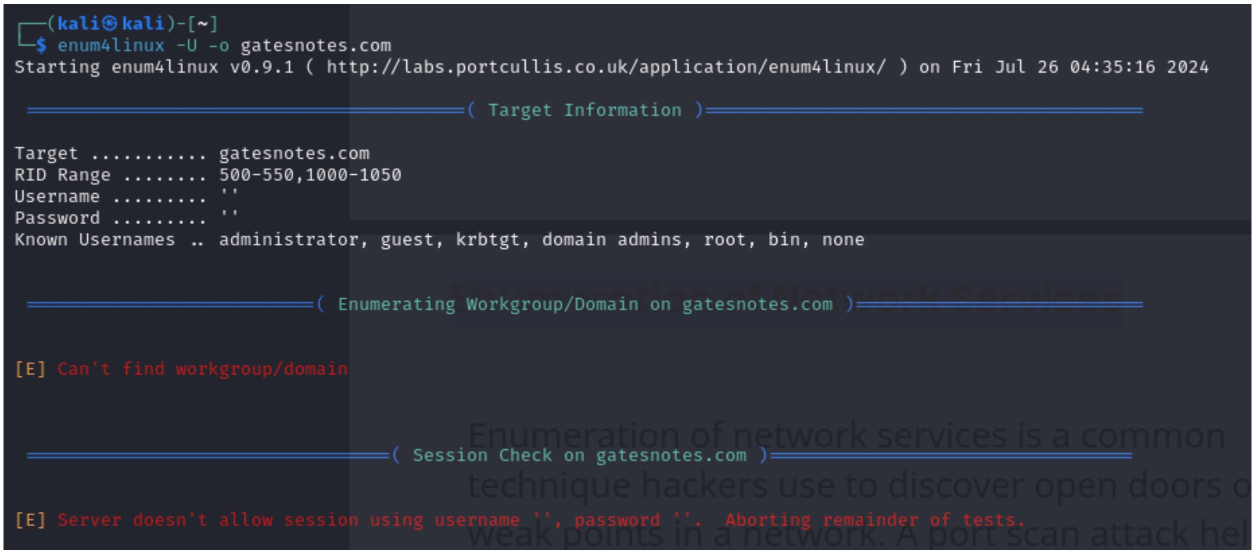
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis — Do you want to automate checks?

Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AILabs (MONITORAPP)	Clean
AlienVault	Clean	alphaMountain.ai	Clean
Antiy-AVL	Clean	Artists Against 419	Clean

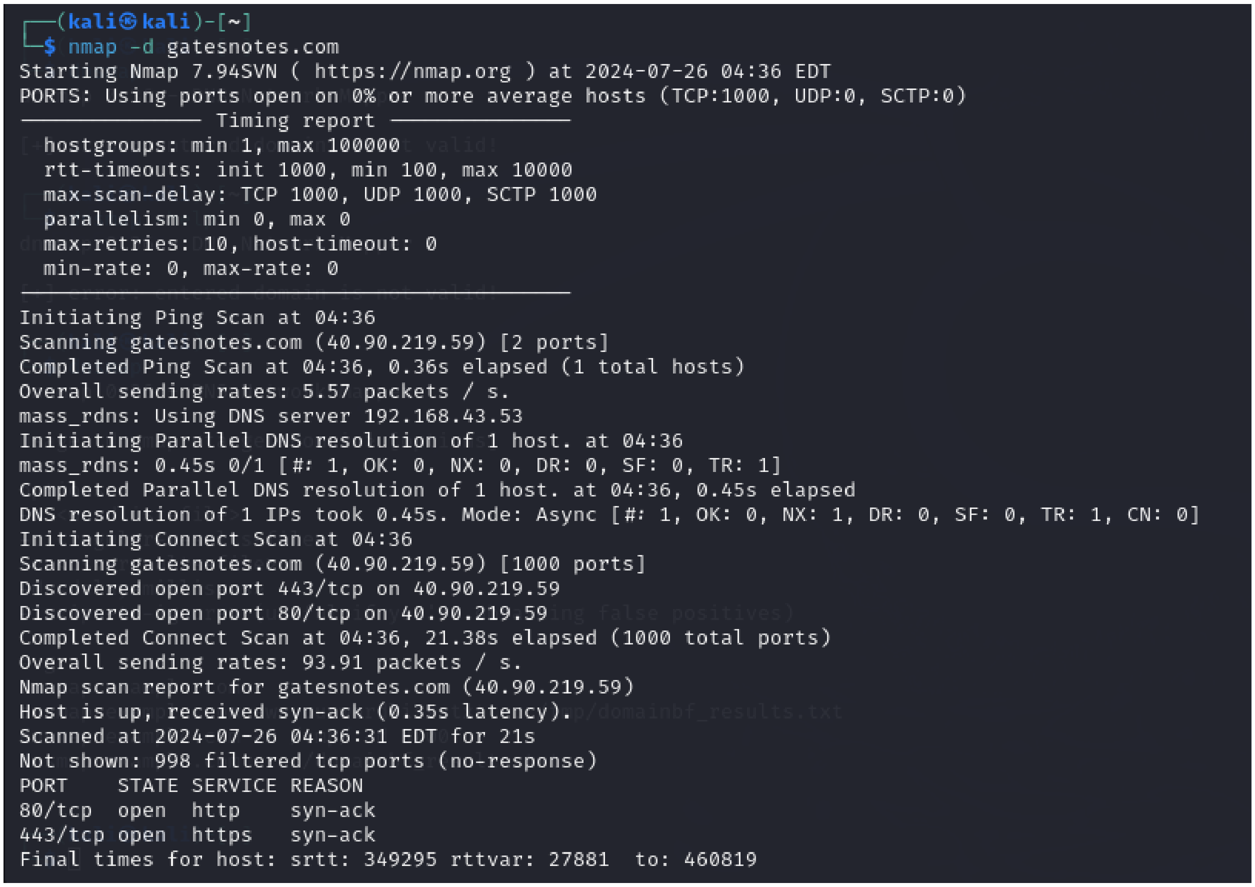
Enumeration of Network Services

Tool 1: enum4linux



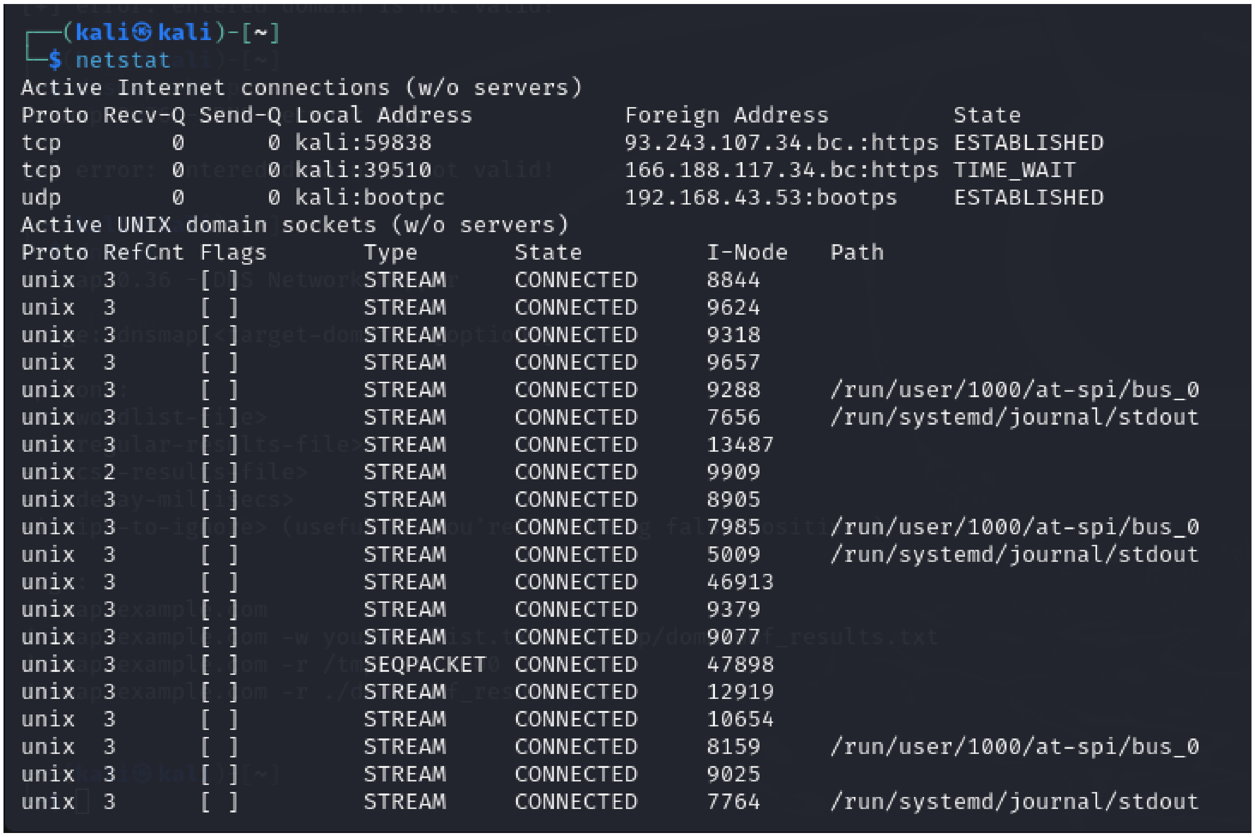
```
┌──(kali㉿kali)-[~]
└─$ enum4linux -U -o gatesnotes.com
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Jul 26 04:35:16 2024

 ==========================================( Target Information )==========================================

Target ........... gatesnotes.com
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ===========================( Enumerating Workgroup/Domain on gatesnotes.com )===========================


[E] Can't find workgroup/domain



 ==================================( Session Check on gatesnotes.com )==================================


[E] Server doesn't allow session using username '', password ''.  Aborting remainder of tests.
```

Tool 2: nmap



```
┌──(kali㉿kali)-[~]
└─$ nmap -d gatesnotes.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-26 04:36 EDT
PORTS: Using ports open on 0% or more average hosts (TCP:1000, UDP:0, SCTP:0)
─────────────── Timing report ───────────────
  hostgroups: min 1, max 100000
  rtt-timeouts: init 1000, min 100, max 10000
  max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
  parallelism: min 0, max 0
  max-retries: 10, host-timeout: 0
  min-rate: 0, max-rate: 0
─────────────────────────────────────────────
Initiating Ping Scan at 04:36
Scanning gatesnotes.com (40.90.219.59) [2 ports]
Completed Ping Scan at 04:36, 0.36s elapsed (1 total hosts)
Overall sending rates: 5.57 packets / s.
mass_rdns: Using DNS server 192.168.43.53
Initiating Parallel DNS resolution of 1 host. at 04:36
mass_rdns: 0.45s 0/1 [#: 1, OK: 0, NX: 0, DR: 0, SF: 0, TR: 1]
Completed Parallel DNS resolution of 1 host. at 04:36, 0.45s elapsed
DNS resolution of 1 IPs took 0.45s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 04:36
Scanning gatesnotes.com (40.90.219.59) [1000 ports]
Discovered open port 443/tcp on 40.90.219.59
Discovered open port 80/tcp on 40.90.219.59
Completed Connect Scan at 04:36, 21.38s elapsed (1000 total ports)
Overall sending rates: 93.91 packets / s.
Nmap scan report for gatesnotes.com (40.90.219.59)
Host is up, received syn-ack (0.35s latency).
Scanned at 2024-07-26 04:36:31 EDT for 21s
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE REASON
80/tcp  open  http    syn-ack
443/tcp open  https   syn-ack
Final times for host: srtt: 349295 rttvar: 27881  to: 460819
```

Tool 3: netstat



```
┌──(kali㉿kali)-[~]
└─$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 kali:59838              93.243.107.34.bc.:https ESTABLISHED
tcp        0      0 kali:39510              166.188.117.34.bc:https TIME_WAIT
udp        0      0 kali:bootpc             192.168.43.53:bootps    ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  3      [ ]         STREAM     CONNECTED     8844
unix  3      [ ]         STREAM     CONNECTED     9624
unix  3      [ ]         STREAM     CONNECTED     9318
unix  3      [ ]         STREAM     CONNECTED     9657
unix  3      [ ]         STREAM     CONNECTED     9288     /run/user/1000/at-spi/bus_0
unix  3      [ ]         STREAM     CONNECTED     7656     /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     13487
unix  2      [ ]         STREAM     CONNECTED     9909
unix  3      [ ]         STREAM     CONNECTED     8905
unix  3      [ ]         STREAM     CONNECTED     7985     /run/user/1000/at-spi/bus_0
unix  3      [ ]         STREAM     CONNECTED     5009     /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     46913
unix  3      [ ]         STREAM     CONNECTED     9379
unix  3      [ ]         STREAM     CONNECTED     9077
unix  3      [ ]         SEQPACKET  CONNECTED     47898
unix  3      [ ]         STREAM     CONNECTED     12919
unix  3      [ ]         STREAM     CONNECTED     10654
unix  3      [ ]         STREAM     CONNECTED     8159     /run/user/1000/at-spi/bus_0
unix  3      [ ]         STREAM     CONNECTED     9025
unix  3      [ ]         STREAM     CONNECTED     7764     /run/systemd/journal/stdout
```