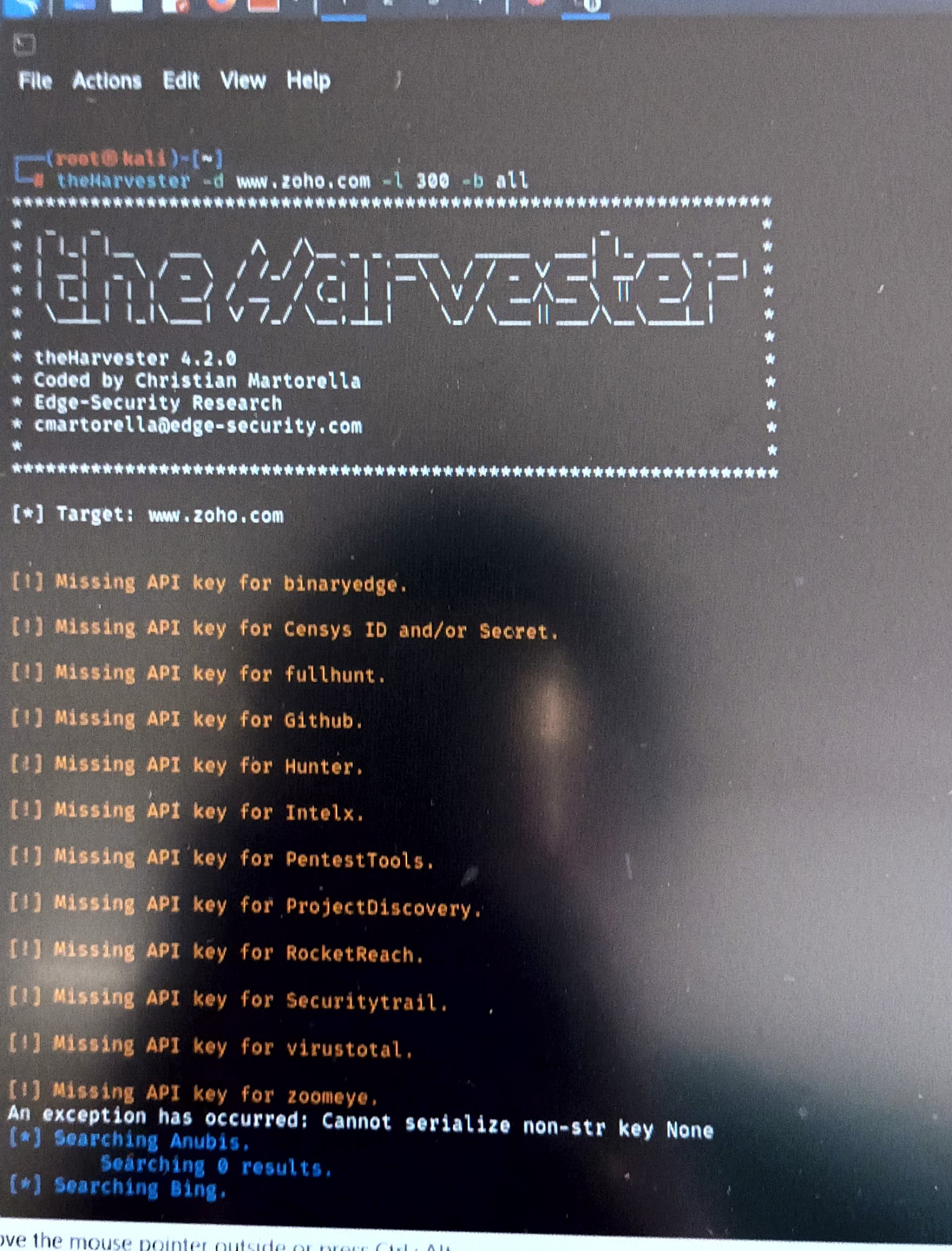
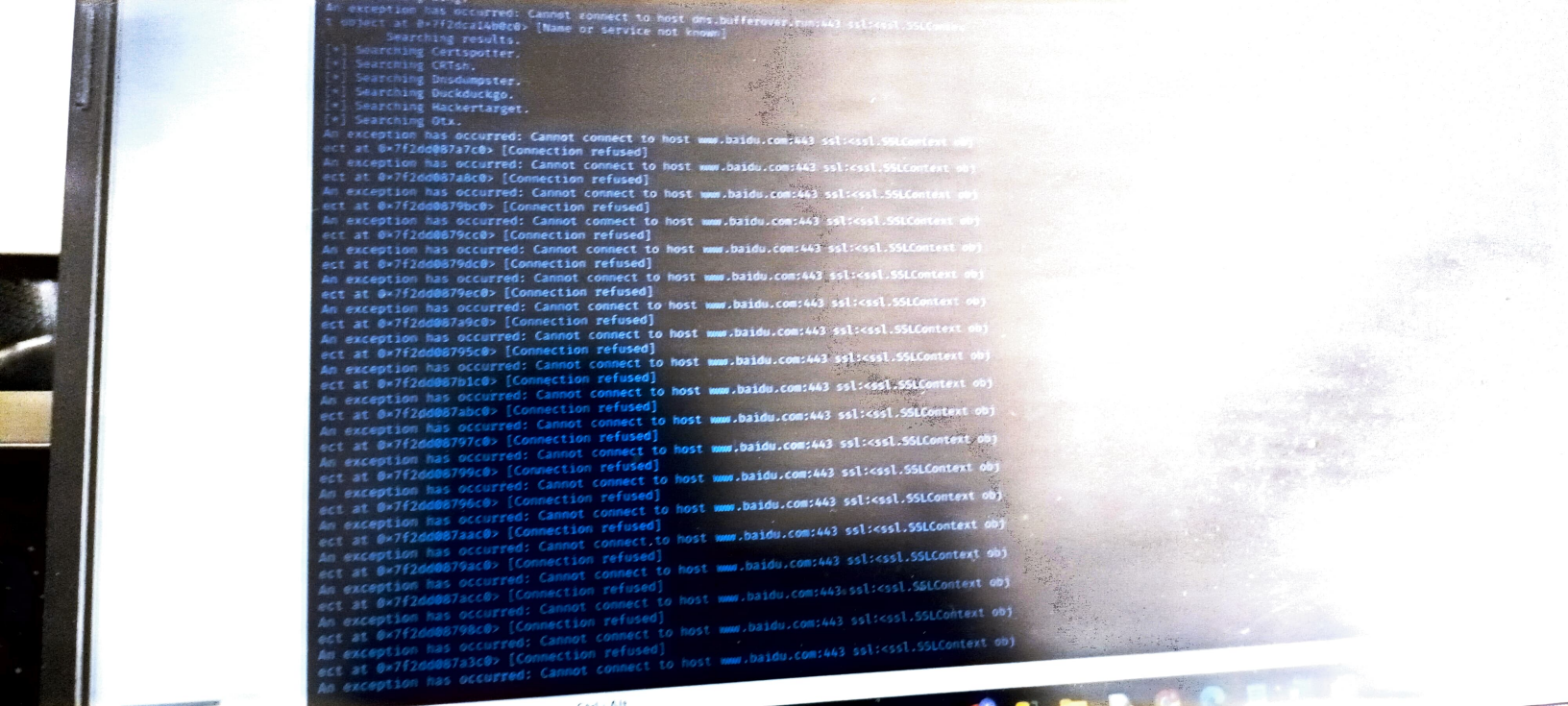
```
┌──(root㉿kali)-[~]
└─# nmap -sT 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-11 00:25 EST
Nmap scan report for 192.168.1.1
Host is up (0.022s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 24.83 seconds

┌──(root㉿kali)-[~]
└─# nmap -sU 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-11 00:26 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.38 seconds

┌──(root㉿kali)-[~]
└─# nmap -sA 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-11 00:26 EST
Nmap scan report for 192.168.1.1
Host is up (0.0050s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds

┌──(root㉿kali)-[~]
└─# nmap -Pn 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-11 00:27 EST
Stats: 0:01:50 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 54.50% done; ETC: 00:31 (0:01:32 remaining)
Nmap scan report for 192.168.1.1
Host is up.
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 201.46 seconds

┌──(root㉿kali)-[~]
└─# nmap -sn 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-11 00:34 EST
Nmap scan report for 192.168.1.1
```

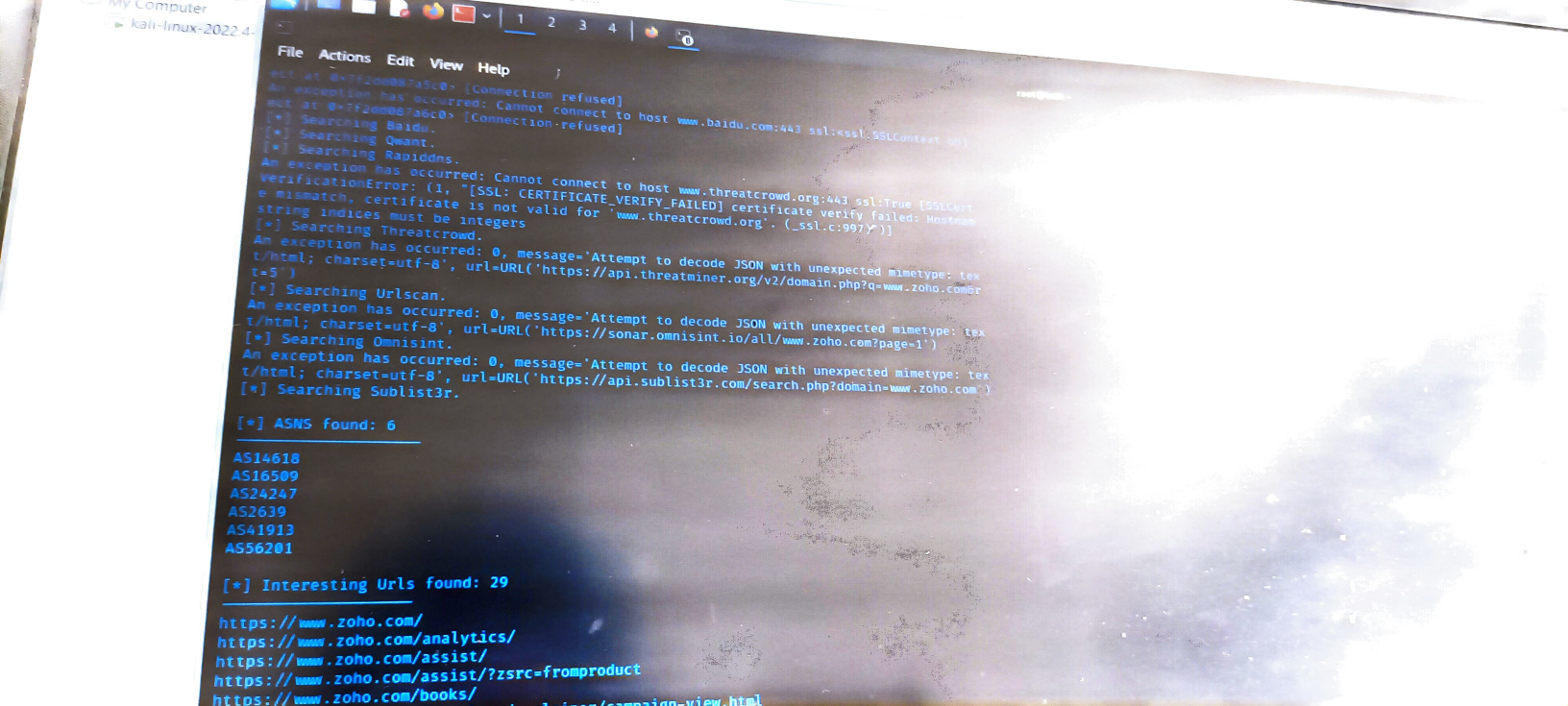


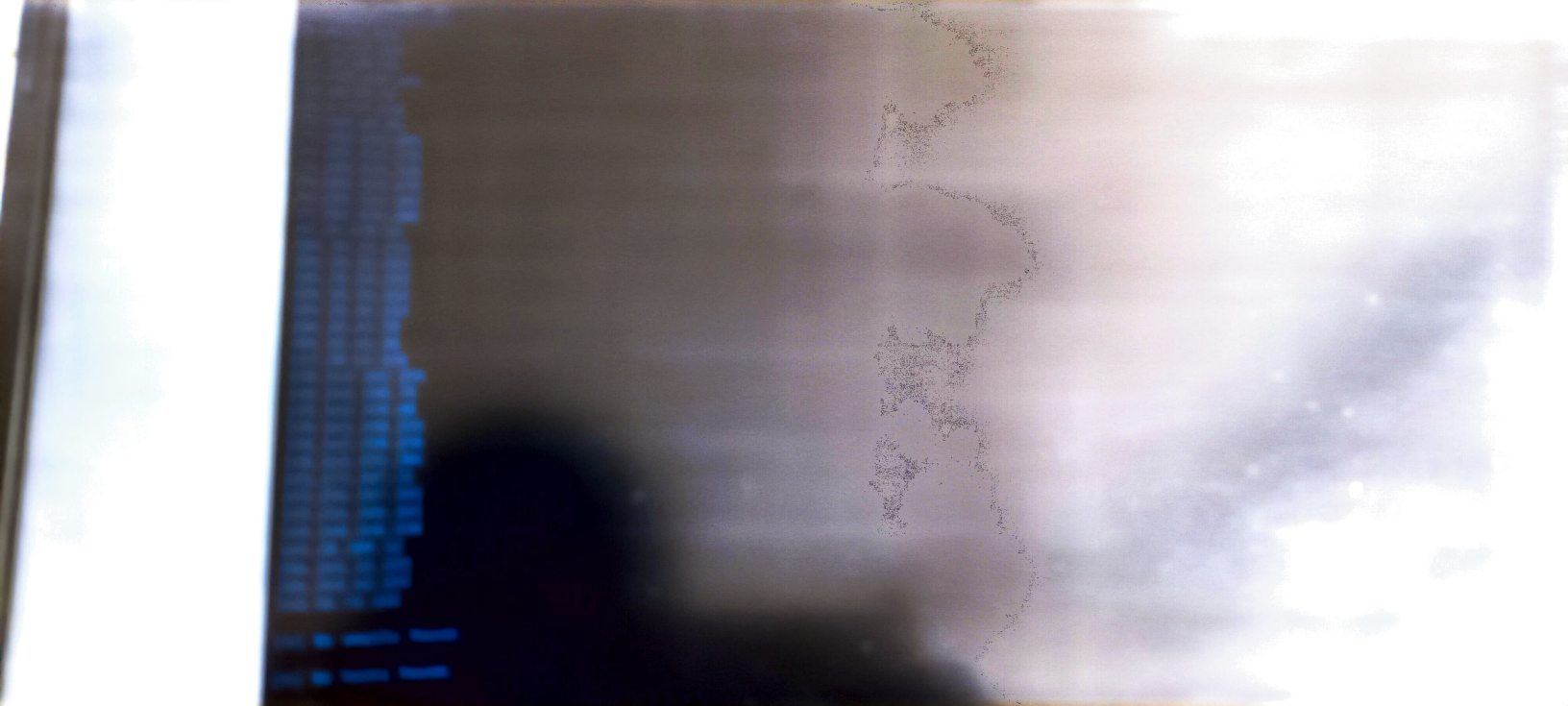
File Actions Edit View Help

```
┌──(root㉿kali)-[~]
└─# theHarvester -d www.zoho.com -l 300 -b all
*******************************************************************
*                                                                 *
*  _   _                                 _                        *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __| '_ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.2.0                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] Target: www.zoho.com

[!] Missing API key for binaryedge.

[!] Missing API key for Censys ID and/or Secret.

[!] Missing API key for fullhunt.

[!] Missing API key for Github.

[!] Missing API key for Hunter.

[!] Missing API key for Intelx.

[!] Missing API key for PentestTools.

[!] Missing API key for ProjectDiscovery.

[!] Missing API key for RocketReach.

[!] Missing API key for Securitytrail.

[!] Missing API key for virustotal.

[!] Missing API key for zoomeye.
An exception has occurred: Cannot serialize non-str key None
[*] Searching Anubis.
        Searching 0 results.
[*] Searching Bing.
```

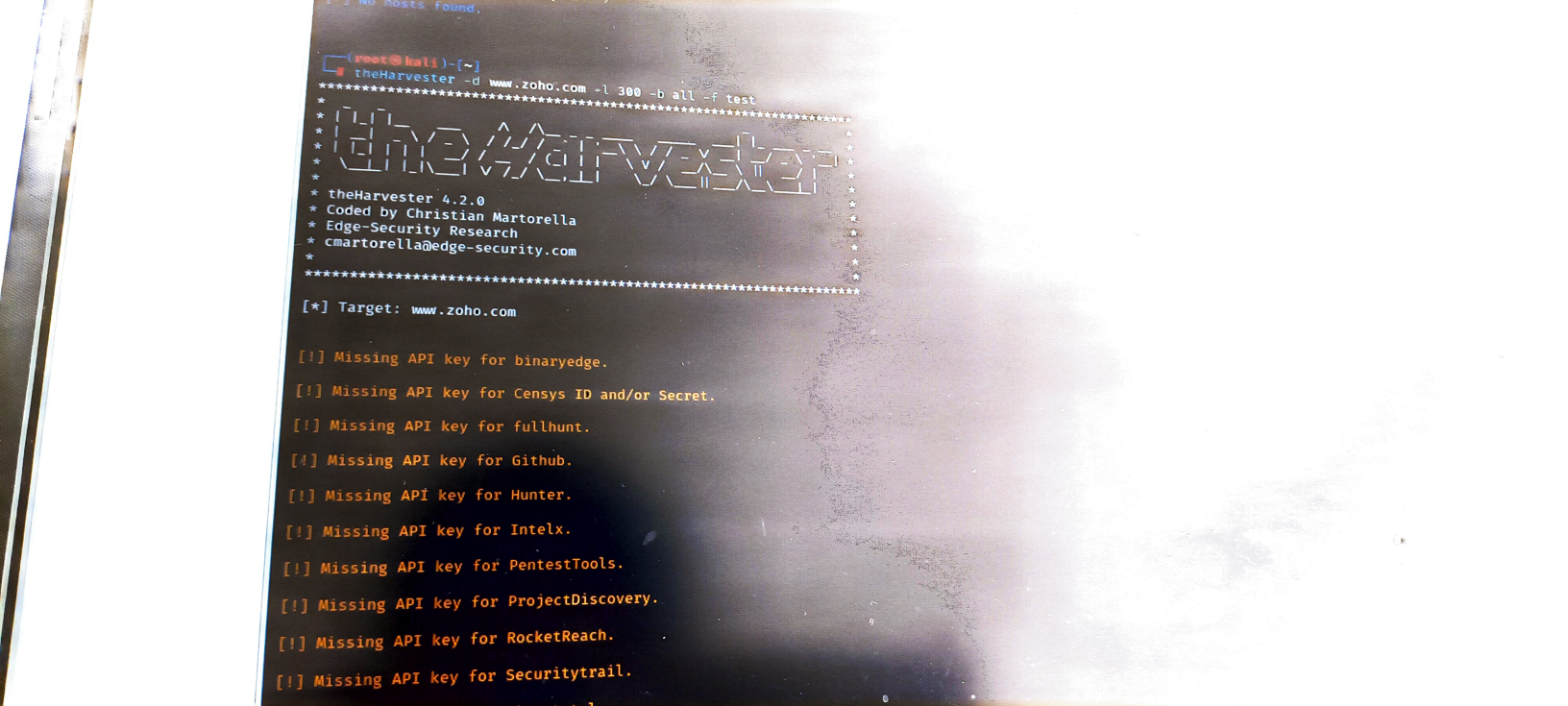
ove the mouse pointer outside or press Ctrl+Alt


An exception has occurred: Cannot connect to host dns.bufferover.run:443 ssl:<ssl.SSLContext
t object at 0x7f2dca140c0> [Name or service not known]
Searching results.
[*] Searching Certspotter.
[*] Searching CRTsh.
[*] Searching Dnsdumpster.
[*] Searching Duckduckgo.
[*] Searching Hackertarget.
[*] Searching Otx.
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext obj
ect at 0x7f2dd087a7c0> [Connection refused]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext obj
ect at 0x7f2dd087a8c0> [Connection refused]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext obj
ect at 0x7f2dd08879bc0> [Connection refused]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext obj
ect at 0x7f2dd08879cc0> [Connection refused]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext obj
ect at 0x7f2dd08879dc0> [Connection refused]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext obj
ect at 0x7f2dd08879ec0> [Connection refused]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext obj
ect at 0x7f2dd087a9c0> [Connection refused]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext obj
ect at 0x7f2dd08795c0> [Connection refused]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext obj
ect at 0x7f2dd087b1c0> [Connection refused]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext obj
ect at 0x7f2dd087abc0> [Connection refused]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext obj
ect at 0x7f2dd08797c0> [Connection refused]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext obj
ect at 0x7f2dd08799c0> [Connection refused]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext obj
ect at 0x7f2dd08796c0> [Connection refused]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext obj
ect at 0x7f2dd087aac0> [Connection refused]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext obj
ect at 0x7f2dd08879ac0> [Connection refused]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext obj
ect at 0x7f2dd087acc0> [Connection refused]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext obj
ect at 0x7f2dd08798c0> [Connection refused]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext obj
ect at 0x7f2dd087a3c0> [Connection refused]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext obj


My Computer
kali-linux-2022.4-
1 2 3 4
File Actions Edit View Help
ect at 0x7f2ed0a7a5c0> [Connection refused]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext obj
ect at 0x7f2ed0a7a6c0> [Connection refused]
[*] Searching Baidu.
[*] Searching Qwant.
[*] Searching Rapiddns.
An exception has occurred: Cannot connect to host www.threatcrowd.org:443 ssl:True [SSLCert
VerificationError: (1, "[SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed: Hostnam
e mismatch, certificate is not valid for 'www.threatcrowd.org'. (_ssl.c:997)")]
string indices must be integers
[*] Searching Threatcrowd.
An exception has occurred: 0, message='Attempt to decode JSON with unexpected mimetype: tex
t/html; charset=utf-8', url=URL('https://api.threatminer.org/v2/domain.php?q=www.zoho.com&r
t=5')
[*] Searching Urlscan.
An exception has occurred: 0, message='Attempt to decode JSON with unexpected mimetype: tex
t/html; charset=utf-8', url=URL('https://sonar.omnisint.io/all/www.zoho.com?page=1')
[*] Searching Omnisint.
An exception has occurred: 0, message='Attempt to decode JSON with unexpected mimetype: tex
t/html; charset=utf-8', url=URL('https://api.sublist3r.com/search.php?domain=www.zoho.com')
[*] Searching Sublist3r.
[*] ASNS found: 6
AS14618
AS16509
AS24247
AS2639
AS41913
AS56201
[*] Interesting Urls found: 29
https://www.zoho.com/
https://www.zoho.com/analytics/
https://www.zoho.com/assist/
https://www.zoho.com/assist/?zsrc=fromproduct
https://www.zoho.com/books/



```
[*] IPs found: 28
-------------------
8.39.54.155
8.40.222.155
13.32.99.51
13.227.219.101
18.66.15.12
52.4.217.128
74.201.84.81
74.201.112.101
74.201.112.118
74.201.113.118
74.201.113.176
74.201.113.203
74.201.155.201
89.36.170.52
104.16.11.213
104.16.12.213
104.16.13.213
104.16.14.213
104.16.15.213
104.16.43.59
104.16.44.59
117.20.43.131
136.143.182.155
136.143.190.79
136.143.190.80
136.143.190.155
136.143.190.156
136.143.191.204
165.173.187.32
165.254.167.165
165.254.168.165
169.148.148.139
185.20.209.52
204.141.32.155
204.141.42.155
216.52.72.155

[*] No emails found.

[*] No hosts found.
```


No hosts found.
root@kali)-[~]
theHarvester -d www.zoho.com -l 300 -b all -f test
theHarvester 4.2.0
Coded by Christian Martorella
Edge-Security Research
cmartorella@edge-security.com
[*] Target: www.zoho.com
[!] Missing API key for binaryedge.
[!] Missing API key for Censys ID and/or Secret.
[!] Missing API key for fullhunt.
[!] Missing API key for Github.
[!] Missing API key for Hunter.
[!] Missing API key for Intelx.
[!] Missing API key for PentestTools.
[!] Missing API key for ProjectDiscovery.
[!] Missing API key for RocketReach.
[!] Missing API key for Securitytrail.

hp.com

Updated 4 days ago

Domain Information

Domain:	hp.com
Registrar:	MarkMonitor Inc.
Registered On:	1986-03-03
Expires On:	2024-03-04
Updated On:	2023-01-31
Status:	clientDeleteProhibited clientTransferProhibited clientUpdateProhibited serverDeleteProhibited serverTransferProhibited serverUpdateProhibited
Name Servers:	ns1.hp.com ns2.hp.com ns3.hp.com ns4.hp.com ns5.hp.com ns6.hp.com

Registrant Contact

Interested in similar domains?

- tradehp.com
- trihp.com
- sheshhp.com
- smarthpcorp.com
- hehp.net
- hpapp.net

Registrant Contact

Name:	Domain Administrator
Organization:	HP Inc.
Street:	1501 Page Mill Road,
City:	Palo Alto
State:	CA
Postal Code:	94304
Country:	US
Phone:	+1.8005247638
Fax:	+1.8005247638
Email:	hp.domains@hp.com

Administrative Contact

Name:	Domain Administrator
Organization:	HP Inc.
Street:	1501 Page Mill Road,
City:	Palo Alto

Phone:	+1.8005247638
Fax:	+1.8005247638
Email:	hp.domains@hp.com

Technical Contact

Name:	Domain Administrator
Organization:	HP Inc.
Street:	1501 Page Mill Road,
City:	Palo Alto
State:	CA
Postal Code:	94304
Country:	US
Phone:	+1.8005247638
Fax:	+1.8005247638
Email:	hp.domains@hp.com

Raw Whois Data

```
Domain Name: hp.com
Registry Domain ID: 5205407_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
```

Raw Whois Data

```
Domain Name: hp.com
Registry Domain ID: 5205407_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2023-01-31T09:47:35+0000
Creation Date: 1986-03-03T05:00:00+0000
Registrar Registration Expiration Date: 2024-03-04T00:00:00+0000
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhib
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferPr
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhib
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhib
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferPr
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhib
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: HP Inc.
Registrant Street: 1501 Page Mill Road,
Registrant City: Palo Alto
Registrant State/Province: CA
Registrant Postal Code: 94304
Registrant Country: US
Registrant Phone: +1.8005247638
Registrant Phone Ext:
Registrant Fax: +1.8005247638
Registrant Fax Ext:
Registrant Email: hp.domains@hp.com
Registry Admin ID:
```

DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2023-02-06T14:56:19+0000 <<<

For more information on WHOIS status codes, please visit:
https://www.icann.org/resources/pages/epp-status-codes

If you wish to contact this domain's Registrant, Administrative, or Technical contact, and such email address is not visible above, you may do so via our web form, pursuant to ICANN's Temporary Specification. To verify that you are not a robot, please enter your email address to receive a link to a page that facilitates email communication with the relevant contact(s).

Web-based WHOIS:
https://domains.markmonitor.com/whois

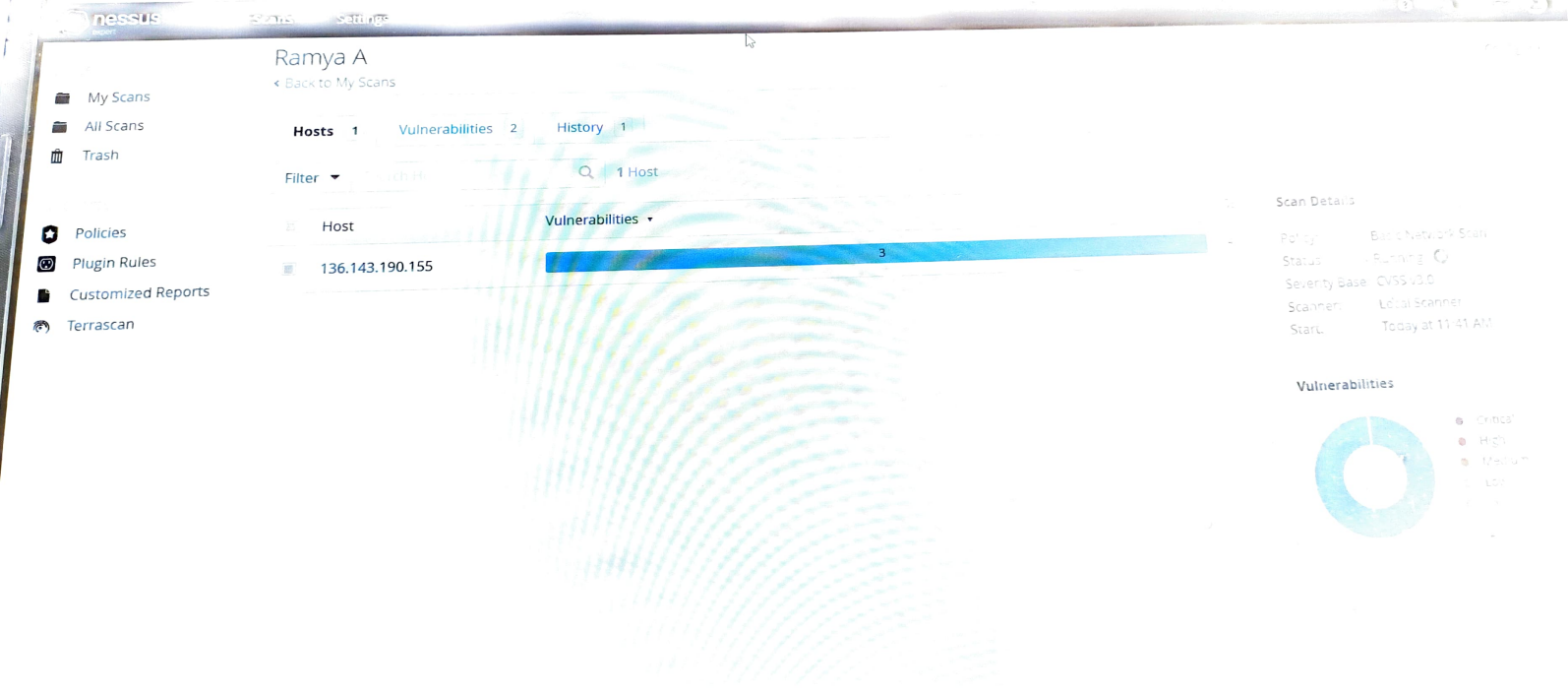
If you have a legitimate interest in viewing the non-public WHOIS details, send your request and the reasons for your request to **whoisrequest**@markmonitor.com and specify the domain name in the subject line. We will review that request and may ask for supporting documentation and explanation.

The data in MarkMonitor's WHOIS database is provided for information purposes, and to assist persons in obtaining information about or related to a domain name's registration record. While MarkMonitor believes the data to be accurate, the data is provided "as is" with no guarantee or warranties regarding its accuracy.

By submitting a WHOIS query, you agree that you will use this data only for lawful purposes and that, under no circumstances will you use this data to:
(1) allow, enable, or otherwise support the transmission by email, telephone, or facsimile of mass, unsolicited, commercial advertising, or spam; or
(2) enable high volume, automated, or electronic processes that send queries, data, or email to MarkMonitor (or its systems) or the domain name contacts (or its systems).

MarkMonitor reserves the right to modify these terms at any time.

By submitting this query, you agree to abide by this policy.


Ramya A
Back to My Scans
My Scans
All Scans
Trash
Policies
Plugin Rules
Customized Reports
Terrascan
Hosts 1
Vulnerabilities 2
History 1
Filter
1 Host
Host
Vulnerabilities
136.143.190.155
3
Scan Details
Vulnerabilities

Hosts 1 | Vulnerabilities 11 | History 1

Filter

11 Vulnerabilities

Sev	Score	Name	Family	
INFO	...	4 SSL (Multiple Issues)	General	
INFO	...	2 HTTP (Multiple Issues)	Web Servers	
INFO	...	3 TLS (Multiple Issues)	General	
INFO	...	2 TLS (Multiple Issues)	Misc.	2
INFO	...	2 TLS (Multiple Issues)	Service detection	2
INFO		Service Detection	Service detection	3
[illegible]		Nessus SYN scanner	Port scanners	2
[illegible]		Additional DNS Hostnames	General	1
[illegible]		SSL Root Certification Authority Certificate Information	General	1
[illegible]		TCP/IP Timestamps Supported	General	1
[illegible]		Traceroute Information	General	1

Vulnerabilities

Ranya A

My Scans
All Scans
Trash

Policies
Plugin Rules
Customized Reports
Terrascan

Hosts 1 | **Vulnerabilities 11** | History 1

Filter | 11 Vulnerabilities

Sev	Score	Name	Family	Count
INFO	...	SSL (Multiple Issues)	General	4
INFO	...	HTTP (Multiple Issues)	Web Servers	3
INFO	...	TLS (Multiple Issues)	General	3
INFO	...	TLS (Multiple Issues)	Misc.	2
INFO	...	TLS (Multiple Issues)	Service detection	2
INFO		Service Detection	Service detection	3
INFO		Nessus SYN scanner	Port scanners	2
INFO		Additional DNS Hostnames	General	1
INFO		SSL Root Certification Authority Certificate Information	General	1
INFO		TCP/IP Timestamps Supported	General	1
INFO		Traceroute Information	General	1

Scan Details

Vulnerabilities

```
(c) Microsoft Corporation. All rights reserved.

C:\Users\ramya>tracert hp.com

Tracing route to hp.com [15.73.192.108]
over a maximum of 30 hops:

  1    95 ms     2 ms     3 ms  192.168.78.198
  2   192 ms   237 ms   319 ms  192.168.29.10
  3    26 ms    19 ms    37 ms  192.168.28.61
  4    35 ms    12 ms    12 ms  192.168.31.25
  5    37 ms    15 ms    13 ms  192.168.31.19
  6     *       46 ms    36 ms  192.168.31.33
  7     *        *        *     Request timed out.
  8    23 ms    18 ms    53 ms  nsg-corporate-173.101.187.122.airtel.in [122.187.101.173]
  9   166 ms   163 ms   158 ms  116.119.106.121
 10    40 ms    12 ms    25 ms  182.79.198.218
 11   165 ms   176 ms   152 ms  182.79.198.129
 12   170 ms   153 ms   153 ms  mei-b5-link.ip.twelve99.net [62.115.34.8]
 13   180 ms   165 ms   170 ms  prs-bb1-link.ip.twelve99.net [62.115.124.54]
 14   412 ms   317 ms   318 ms  ash-bb2-link.ip.twelve99.net [62.115.112.242]
 15   329 ms   270 ms   369 ms  ash-b1-link.ip.twelve99.net [62.115.143.121]
 16   345 ms   327 ms   379 ms  192.205.33.25
 17   269 ms   269 ms   311 ms  cr82.wshdc.ip.att.net [12.122.135.102]
 18   365 ms   326 ms   313 ms  wswdc22crs.ip.att.net [12.122.135.250]
 19   306 ms   279 ms   280 ms  attga21crs.ip.att.net [12.122.2.29]
 20   316 ms   307 ms   281 ms  nwrla22crs.ip.att.net [12.122.2.146]
 21   441 ms   352 ms   357 ms  nwrla21crs.ip.att.net [12.122.30.73]
 22   402 ms   411 ms   386 ms  hs1tx21crs.ip.att.net [12.122.28.161]
 23   298 ms   293 ms   304 ms  santx22crs.ip.att.net [12.122.28.114]
 24   297 ms   280 ms   312 ms  12.123.236.149
 25   426 ms   297 ms   333 ms  206.121.19.114
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
                                 Request timed out.
```

```
C:\>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:5939         LAPTOP-NMG9PJ9R:62083  ESTABLISHED
  TCP    127.0.0.1:53203        LAPTOP-NMG9PJ9R:53204  ESTABLISHED
  TCP    127.0.0.1:53204        LAPTOP-NMG9PJ9R:53203  ESTABLISHED
  TCP    127.0.0.1:56329        LAPTOP-NMG9PJ9R:56330  ESTABLISHED
  TCP    127.0.0.1:56330        LAPTOP-NMG9PJ9R:56329  ESTABLISHED
  TCP    127.0.0.1:62083        LAPTOP-NMG9PJ9R:5939   ESTABLISHED
  TCP    127.0.0.1:62117        LAPTOP-NMG9PJ9R:62118  ESTABLISHED
  TCP    127.0.0.1:62118        LAPTOP-NMG9PJ9R:62117  ESTABLISHED
  TCP    127.0.0.1:63273        LAPTOP-NMG9PJ9R:63274  ESTABLISHED
  TCP    127.0.0.1:63274        LAPTOP-NMG9PJ9R:63273  ESTABLISHED
  TCP    127.0.0.1:63287        LAPTOP-NMG9PJ9R:63288  ESTABLISHED
  TCP    127.0.0.1:63288        LAPTOP-NMG9PJ9R:63287  ESTABLISHED
  TCP    127.0.0.1:63435        LAPTOP-NMG9PJ9R:63436  ESTABLISHED
  TCP    127.0.0.1:63436        LAPTOP-NMG9PJ9R:63435  ESTABLISHED
  TCP    192.168.78.88:49598    20.198.119.84:https    ESTABLISHED
  TCP    192.168.78.88:52665    117.18.237.29:http     CLOSE_WAIT
  TCP    192.168.78.88:52897    ec2-15-207-187-50:https  ESTABLISH
  TCP    192.168.78.88:53497    a-0003:https           TIME_WAIT
  TCP    192.168.78.88:53620    192.168.78.198:domain  TIME_WAIT
  TCP    192.168.78.88:53621    192.168.78.198:domain  TIME_WAIT
  TCP    192.168.78.88:53622    192.168.78.198:domain  TIME_WAIT
  TCP    192.168.78.88:53663    192.168.78.198:domain  TIME_WAIT
  TCP    192.168.78.88:53664    192.168.78.198:domain  TIME_WAIT
  TCP    192.168.78.88:53665    192.168.78.198:domain  TIME_WAIT
```