Laboratory№1 of student Anastasiia Bozhko FB-73

Laboratory number: 1
Laboratory name: Footprinting, Reconnaissance & OSINT
Developers:

- Oleksii Baranovskyi
- Volodymyr Mishyn

Prerequisites: Each student should select company from the world with own infrastructure (AS with network subblock). This company will be used as target during several lab works.

Table of Contents

Exercise 1. Obtain information about domain/IP using whois

Purpose: understand core whois service

After the work the student must

- know: how whois works, how domains and IP-blocks delegated to customers
- be able to: obtain all information from whois service.

Tasks:

- extract information about domain of selected company using whois command
- extract information about domain of selected company using web-based whois service

Material and technical equipping of the workplace

- command console
  - whois command
- web-browser

References

- https://en.wikipedia.org/wiki/WHOIS

TASK 1

Obtain all information about selected domain with using whois command (prove with screenshot). When was domain registered / changed? Who is the owner of domain? What differences between admin, technical and other contacts? Explain.

Answer:

Updated Date: 2020-04-13T08:57:10Z
Creation Date: 2000-04-13T00:29:15Z
Registrant Name: Dronova Natalya Myhailovna

```
nastja@nastja-P5L-MX:~$ whois -h whois.imena.ua roshen.com
Domain Name: ROSHEN.COM
Registry Domain ID: 24809841_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.imena.ua
Registrar URL: http://imena.ua
Updated Date: 2020-04-13T08:57:10Z
Creation Date: 2000-04-13T00:29:15Z
Registrar Registration Expiration Date: 2021-04-13T00:29:15Z
Registrar: Internet Invest, Ltd. dba Imena.ua
Registrar IANA ID: 1112
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Dronova Natalya Myhailovna
Registrant Organization: ROSHEN Confectionery Corporation
Registrant Street: 26 9 Electricov St.
Registrant City: Kiev
Registrant State/Province:
Registrant Postal Code: 04176
Registrant Country: UA
Registrant Phone: +380.443517200
Registrant Phone Ext:
Registrant Fax: +380.443517200
Registrant Fax Ext:
Registrant Email: dronova_n@roshen.com.ua
Registry Admin ID: Not Available From Registry
Admin Name: Dronova Natalya Myhailovna
Admin Organization: ROSHEN Confectionery Corporation
Admin Street: 26 9 Electricov St.
Admin City: Kiev
Admin State/Province:
Admin Postal Code: 04176
Admin Country: UA
Admin Phone: +380.443517200
Admin Phone Ext:
Admin Fax: +380.443517200
Admin Fax Ext:
Admin Email: dronova_n@roshen.com.ua
Registry Tech ID: Not Available From Registry
Tech Name: Dronova Natalya Myhailovna
Tech Organization: ROSHEN Confectionery Corporation
Tech Street: 26 9 Electricov St.
Tech City: Kiev
Tech State/Province:
Tech Postal Code: 04176
Tech Country: UA
Tech Phone: +380.443517200
Tech Phone Ext:
Tech Fax: +380.443517200
Tech Fax Ext:
Tech Email: dronova_n@roshen.com.ua
Name Server: isp.lecos.ua
Name Server: ns16.inhostedns.com
Name Server: ns26.inhostedns.net
Name Server: ns36.inhostedns.org
Name Server: ns.lecos.ua
DNSSEC: Unsigned
Registrar Abuse Contact Email: abuse@imena.ua
Registrar Abuse Contact Phone: +380.442010102
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2020-10-10T12:44:21Z <<<
```

Admin contact - who is responsible for administrative matters regarding domain name.
Tech contact - who technically supports domain name.

TASK 2

Obtain all information about selected domain with using web-based whois service (prove with screenshot).

Answer:

```
Domain Name: ROSHEN.COM
Registry Domain ID: 24809841_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.imena.ua
Registrar URL: http://imena.ua
Updated Date: 2020-04-13T08:57:10Z
Creation Date: 2000-04-13T00:29:15Z
Registrar Registration Expiration Date: 2021-04-13T00:29:15Z
Registrar: Internet Invest, Ltd. dba Imena.ua
Registrar IANA ID: 1112
Domain Status: clientTransferProhibited
https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Dronova Natalya Myhailovna
Registrant Organization: ROSHEN Confectionery Corporation
Registrant Street: 26 9 Electricov St.
Registrant City: Kiev
Registrant State/Province:
Registrant Postal Code: 04176
Registrant Country: UA
Registrant Phone: +380.443517200
Registrant Phone Ext:
Registrant Fax: +380.443517200
Registrant Fax Ext:
Registrant Email: dronova_n@roshen.com.ua
Registry Admin ID: Not Available From Registry
Admin Name: Dronova Natalya Myhailovna
Admin Organization: ROSHEN Confectionery Corporation
Admin Street: 26 9 Electricov St.
Admin City: Kiev
Admin State/Province:
Admin Postal Code: 04176
Admin Country: UA
Admin Phone: +380.443517200
Admin Phone Ext:
Admin Fax: +380.443517200
Admin Fax Ext:
Admin Email: dronova_n@roshen.com.ua
Registry Tech ID: Not Available From Registry
Tech Name: Dronova Natalya Myhailovna
Tech Organization: ROSHEN Confectionery Corporation
Tech Street: 26 9 Electricov St.
Tech City: Kiev
Tech State/Province:
Tech Postal Code: 04176
Tech Country: UA
Tech Phone: +380.443517200
Tech Phone Ext:
Tech Fax: +380.443517200
Tech Fax Ext:
Tech Email: dronova_n@roshen.com.ua
Name Server: isp.lecos.ua
Name Server: ns16.inhostedns.com
Name Server: ns26.inhostedns.net
Name Server: ns36.inhostedns.org
Name Server: ns.lecos.ua
DNSSEC: Unsigned
Registrar Abuse Contact Email: abuse@imena.ua
Registrar Abuse Contact Phone: +380.442010102
URL of the ICANN WHOIS Data Problem Reporting System:
http://wdprs.internic.net/
```

TASK 3

Are any differences between obtained results?

Answer:

I guess that info from terminal and web-site don't differ.

TASK 4

What are network range? Which regional registrar is responsible? (prove with screenshots)

Answer:

185.65.244.0/22

RIPE NNC is responsible in the Europe (RIR).

```
nastja@nastja-P5L-MX:~$ whois  185.65.244.138
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '185.65.244.0 - 185.65.245.255'
nastja@nastja-P5L-MX:~$
nastja@nastja-P5L-MX:~$ whois -h whois.cymru.com -- '-v 185.65.244.138'
AS      | IP               | BGP Prefix          | CC | Registry | Allocated  | AS Name
200000  | 185.65.244.138   | 185.65.244.0/22     | UA | ripencc  | 2014-08-04 | UKRAINE-AS, UA
nastja@nastja-P5L-MX:~$
```

TASK 5

What are NS servers?

Answer:

NS is domain name server, which contains the necessary information about the domain name for its correct work, which indicates where the site and mail, for which this domain name was bought, should be located.

Exercise 2. Obtain general information about selected domain with DNS service

Purpose: understand core DNS service

After the work the student must

- know: how DNS works, how different types of DNS records works
- be able to: obtain all information about target from DNS service.

Tasks:

- extract general DNS records (A,AAAA,NS, MX, SPF, PTR) about domain of selected company using dig command
- general DNS records (A,AAAA,NS, MX, SPF, PTR) about domain of selected company using provided web-based services

Material and technical equipping of the workplace

- command console
  - dig command
- web-browser
  - https://bgp.he.net/
  - https://mxtoolbox.com/

References

- https://en.wikipedia.org/wiki/Domain_Name_System
- https://en.wikipedia.org/wiki/Reverse_DNS_lookup
- https://ru.wikipedia.org/wiki/Dig

TASK 1

Obtain all information about selected domain with using dig command (prove with screenshot). What records are accessible (MX/A/AAAA/NS)? What are goals of these records? Explain

Answer:

```
nastja@nastja-P5L-MX:~$ dig roshen.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> roshen.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49476
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 5, ADDITIONAL: 7

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;roshen.com.                    IN      A

;; ANSWER SECTION:
roshen.com.             3600    IN      A       185.65.244.138

;; AUTHORITY SECTION:
roshen.com.             31892   IN      NS      ns16.inhostedns.com.
roshen.com.             31892   IN      NS      ns36.inhostedns.org.
roshen.com.             31892   IN      NS      isp.lecos.ua.
roshen.com.             31892   IN      NS      ns.lecos.ua.
roshen.com.             31892   IN      NS      ns26.inhostedns.net.

;; ADDITIONAL SECTION:
ns.lecos.ua.            1749    IN      A       195.78.58.1
ns16.inhostedns.com.    148483  IN      A       185.104.44.32
ns16.inhostedns.com.    110127  IN      AAAA    2a06:6440:0:2c20::1
ns26.inhostedns.net.    156830  IN      A       185.104.46.32
ns26.inhostedns.net.    156830  IN      AAAA    2a06:6440:0:2e20::1
ns36.inhostedns.org.    20438   IN      AAAA    2001:bc8:3f3c:105::3

;; Query time: 175 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Sat Oct 10 16:18:41 EEST 2020
;; MSG SIZE  rcvd: 326
```

TASK 2

Obtain PTR-records for obtained IP-addresses from NS/MX/A records (not more 5) (prove with screenshot). Are any differences from direct names? Explain.

Answer:

PTR-records are user for reversed DNS lookup. PTR records provides trust that the given hostname or a domain are connected to the IP address. Ip-address has structure such as from high to low level, and domain name has conversely structure: from low to high level.

(A record)

```
astja@nastja-P5L-MX:~$
astja@nastja-P5L-MX:~$ dig -x 2a06:6440:0:2c20::1

 <<>> DiG 9.10.3-P4-Ubuntu <<>> -x 2a06:6440:0:2c20::1
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64518
; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

; OPT PSEUDOSECTION:
 EDNS: version: 0, flags:; udp: 4096
; QUESTION SECTION:
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.c.2.0.0.0.0.0.4.4.6.6.0.a.2.ip6.arpa. IN PTR

; ANSWER SECTION:
.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.c.2.0.0.0.0.0.4.4.6.6.0.a.2.ip6.arpa. 3600 IN PTR ns16.inhostedns.com.

; AUTHORITY SECTION:
.4.4.6.6.0.a.2.ip6.arpa. 172800 IN      NS      ns2.fastdns.hosting.
.4.4.6.6.0.a.2.ip6.arpa. 172800 IN      NS      ns1.fastdns.hosting.

; ADDITIONAL SECTION:
s1.fastdns.hosting.     185     IN      A       91.222.136.45
s2.fastdns.hosting.     185     IN      A       91.206.200.105

; Query time: 309 msec
; SERVER: 127.0.1.1#53(127.0.1.1)
; WHEN: Sat Oct 10 16:51:43 EEST 2020
; MSG SIZE  rcvd: 217
```

(AAAA)

```
nastja@nastja-P5L-MX:~$
nastja@nastja-P5L-MX:~$
nastja@nastja-P5L-MX:~$
nastja@nastja-P5L-MX:~$ dig -x 195.78.58.1

; <<>> DiG 9.10.3-P4-Ubuntu <<>> -x 195.78.58.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16387
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;1.58.78.195.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
1.58.78.195.in-addr.arpa. 86400 IN      PTR     boa.lecos.ua.
1.58.78.195.in-addr.arpa. 86400 IN      PTR     ns.lecos.ua.

;; AUTHORITY SECTION:
58.78.195.in-addr.arpa. 106019  IN      NS      ns.lecos.ua.
58.78.195.in-addr.arpa. 106019  IN      NS      ns.secondary.net.ua.

;; ADDITIONAL SECTION:
ns.lecos.ua.            5703    IN      A       195.78.58.1

;; Query time: 40 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Sat Oct 10 16:49:19 EEST 2020
;; MSG SIZE  rcvd: 157

nastja@nastja-P5L-MX:~$
nastja@nastja-P5L-MX:~$
```

(NS)

```
nastja@nastja-P5L-MX: ~
nastja@nastja-P5L-MX:~$ dig -x 195.78.58.1

; <<>> DiG 9.10.3-P4-Ubuntu <<>> -x 195.78.58.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3023
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;1.58.78.195.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
1.58.78.195.in-addr.arpa. 86400 IN      PTR     ns.lecos.ua.
1.58.78.195.in-addr.arpa. 86400 IN      PTR     boa.lecos.ua.

;; AUTHORITY SECTION:
58.78.195.in-addr.arpa. 172800  IN      NS      ns.secondary.net.ua.
58.78.195.in-addr.arpa. 172800  IN      NS      ns.lecos.ua.

;; ADDITIONAL SECTION:
ns.lecos.ua.            13072   IN      A       195.78.58.1

;; Query time: 328 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Mon Oct 12 12:11:07 EEST 2020
;; MSG SIZE  rcvd: 157

nastja@nastja-P5L-MX:~$
```

(MX)

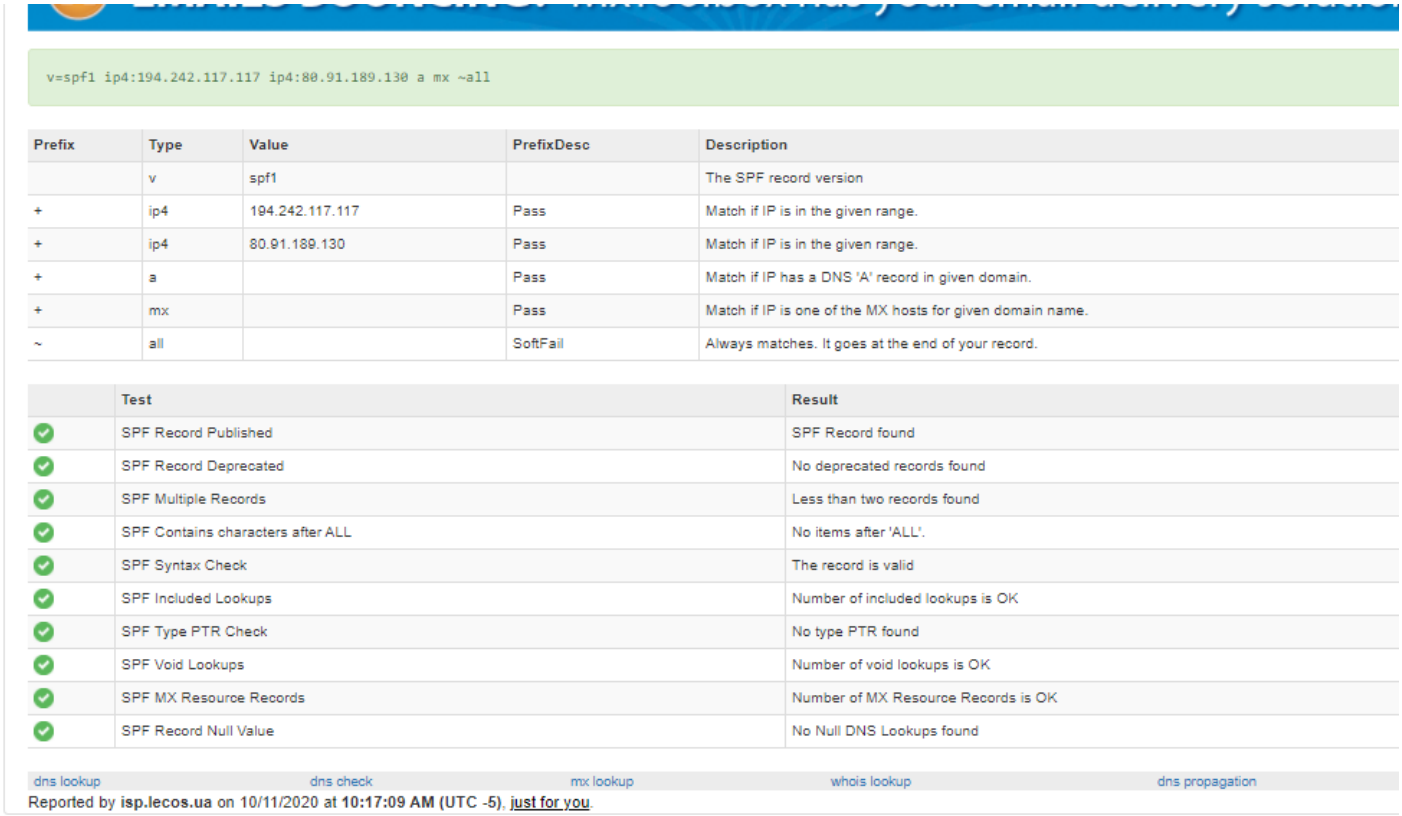
```
nastja@nastja-P5L-MX:~$
nastja@nastja-P5L-MX:~$ dig -x 10 mail2.roshen.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> -x 10 mail2.roshen.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17064
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;10.in-addr.arpa.               IN      PTR

;; AUTHORITY SECTION:
10.in-addr.arpa.        10800   IN      SOA     prisoner.iana.org. hostmaster.root-servers.org. 1 604800 60 604800 604800

;; Query time: 4 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Sat Oct 10 16:52:56 EEST 2020
;; MSG SIZE  rcvd: 121

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52950
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;mail2.roshen.com.              IN      A

;; ANSWER SECTION:
mail2.roshen.com.       3600    IN      A       194.242.117.117

;; AUTHORITY SECTION:
roshen.com.             2924    IN      NS      isp.lecos.ua.
roshen.com.             2924    IN      NS      ns.lecos.ua.

;; ADDITIONAL SECTION:
ns.lecos.ua.            5486    IN      A       195.78.58.1

;; Query time: 47 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Sat Oct 10 16:52:56 EEST 2020
;; MSG SIZE  rcvd: 120
```

```
nastja@nastja-P5L-MX:~$ dig -x 20 mail1.roshen.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> -x 20 mail1.roshen.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12480
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;20.in-addr.arpa.               IN      PTR

;; AUTHORITY SECTION:
20.in-addr.arpa.        10359   IN      SOA     z.arin.net. dns-ops.arin.net. 2017030342 1800 900 691200 10800

;; Query time: 2 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Sat Oct 10 16:54:20 EEST 2020
;; MSG SIZE  rcvd: 98

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39303
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;mail1.roshen.com.              IN      A

;; ANSWER SECTION:
mail1.roshen.com.       3159    IN      A       80.91.189.130

;; AUTHORITY SECTION:
roshen.com.             2840    IN      NS      isp.lecos.ua.
roshen.com.             2840    IN      NS      ns.lecos.ua.

;; ADDITIONAL SECTION:
ns.lecos.ua.            5402    IN      A       195.78.58.1

;; Query time: 2 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Sat Oct 10 16:54:20 EEST 2020
;; MSG SIZE  rcvd: 120
```

TASK 3

Check SPF records of selected domain/subdomain with MxToolbox (prove with screenshot)? Explain results.

Answer:



v=spf1 ip4:194.242.117.117 ip4:80.91.189.130 a mx ~all

Prefix	Type	Value	PrefixDesc	Description
	v	spf1		The SPF record version
+	ip4	194.242.117.117	Pass	Match if IP is in the given range.
+	ip4	80.91.189.130	Pass	Match if IP is in the given range.
+	a		Pass	Match if IP has a DNS 'A' record in given domain.
+	mx		Pass	Match if IP is one of the MX hosts for given domain name.
~	all		SoftFail	Always matches. It goes at the end of your record.

	Test	Result
✓	SPF Record Published	SPF Record found
✓	SPF Record Deprecated	No deprecated records found
✓	SPF Multiple Records	Less than two records found
✓	SPF Contains characters after ALL	No items after 'ALL'.
✓	SPF Syntax Check	The record is valid
✓	SPF Included Lookups	Number of included lookups is OK
✓	SPF Type PTR Check	No type PTR found
✓	SPF Void Lookups	Number of void lookups is OK
✓	SPF MX Resource Records	Number of MX Resource Records is OK
✓	SPF Record Null Value	No Null DNS Lookups found

dns lookup dns check mx lookup whois lookup dns propagation

Reported by **isp.lecos.ua** on 10/11/2020 at **10:17:09 AM (UTC -5)**, just for you.

```
v=spf1 ip4:194.242.117.117 ip4:80.91.189.130 a mx ~all
```

Messages from this domain can be sent from subnets 194.242.117.117 and 80.91.189.130,and from A and MX-records of the current domain, and messages from other servers (all) must be additional verification (~)

TASK 4

Is there any information about AS of the company? (prove with screenshots) What does it mean?

Answer:

Autonomous system (AS) is a large network or group of networks that has a unified routing policy. Every computer or device that connects to the Internet is connected to an AS.

```
nastja@nastja-P5L-MX:~$
nastja@nastja-P5L-MX:~$ whois -h whois.cymru.com -- '-v 185.65.244.138'
AS      | IP               | BGP Prefix          | CC | Registry | Allocated  | AS Name
200000  | 185.65.244.138   | 185.65.244.0/22     | UA | ripencc  | 2014-08-04 | UKRAINE-AS, UA
nastja@nastja-P5L-MX:~$
```

Exercise 3. Obtain general information about target AS

Purpose: understand core BGP protocol

After the work the student must

- know: how what is AS, how AS transfers traffic
- be able to: obtain AS-related information (number, subblocks, connections, routes)

Tasks:

- extract target company AS information with https://bgp.he.net/
- obtain changes in BGP routing to selected AS

Material and technical equipping of the workplace

- command console
  - traceroute command
- web-browser
  - https://bgp.he.net/
  - http://www.routeviews.org/routeviews/
  - https://stat.ripe.net/widget/bgplay

References

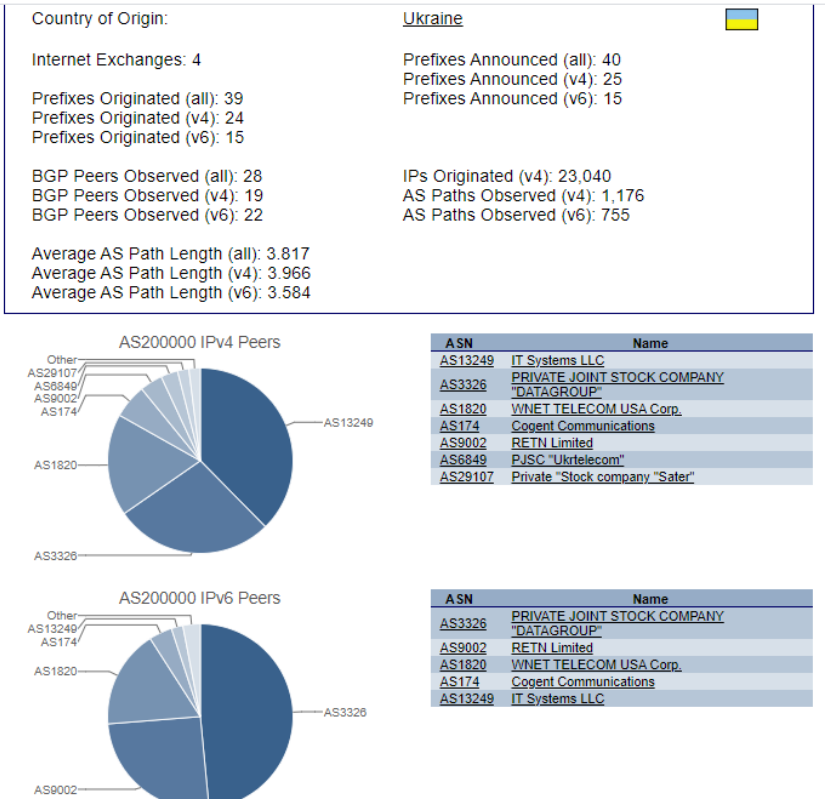
- https://en.wikipedia.org/wiki/Border_Gateway_Protocol

TASK 1

Obtain all AS information with bgp.he.net (prove with screenshot). What is AS number? What subblocks are present?

Answer:

Each AS is assigned autonomous system number (ASN), similar to how every business has a business license with an unique, official number. External parties often refer to ASes by their number alone.AS numbers are unique 16 bit numbers between 1 and 65534 or 32 bit numbers between 131072 and 4294967294.



TASK 2

Are any other AS announce the same subblock? Is it correct?

Answer:

Number of IP prefixes	24 (IPv4) 15 (IPv6)

TASK 3

How many connections current AS has? (prove with screenshot).

Answer:

AS has 23,040 connections

IPs Originated (v4): 23,040
AS Paths Observed (v4): 1,176

TASK 4

What is the main route between target AS and you? Prove it with traceroute command and screenshot of results and IP-AS relation analysis.

Answer:

```
nastja@nastja-P5L-MX:~$ traceroute -A roshen.com
traceroute to roshen.com (185.65.244.138), 30 hops max, 60 byte packets
 1  192.168.1.1 (192.168.1.1) [*]  0.666 ms  0.763 ms  0.917 ms
 2  10.100.126.1 (10.100.126.1) [*]  3.801 ms  3.944 ms  3.913 ms
 3  border-gw.best.net.ua (95.158.0.213) [AS35362]  3.873 ms  4.010 ms  3.967 ms
 4  deltax-10G-gw.ix.net.ua (185.1.50.162) [AS15645]  4.109 ms dtel-ix.delta-x.ua (193.25.180.211) [AS31210]  4.083 ms deltax2-ix.giganet.ua (185.1.63.61) [AS59613]  4.512 ms
 5  * * *
 6  web230.default-host.net (185.65.244.119) [AS200000]  4.425 ms  1.693 ms  1.829 ms
 7  vps-22556.vps-default-host.net (185.65.244.138) [AS200000]  3.139 ms  3.272 ms  3.247 ms
nastja@nastja-P5L-MX:~$
```

Exercise 4. OSINT with Shodan

Purpose: understand Shodan facilities

After the work the student must

- know: how Shodan service works

Tasks:

- confirm, specify and extend information from previous steps with using Shodan service

Material and technical equipping of the workplace

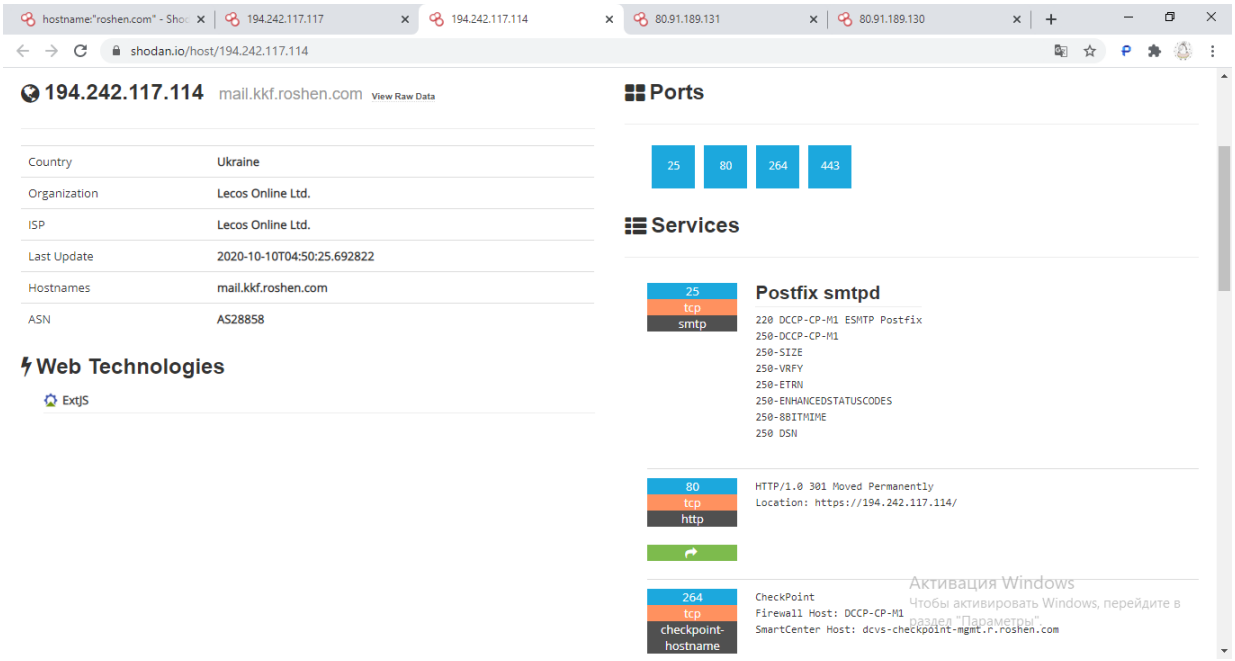
- web-browser
  - https://www.shodan.io/

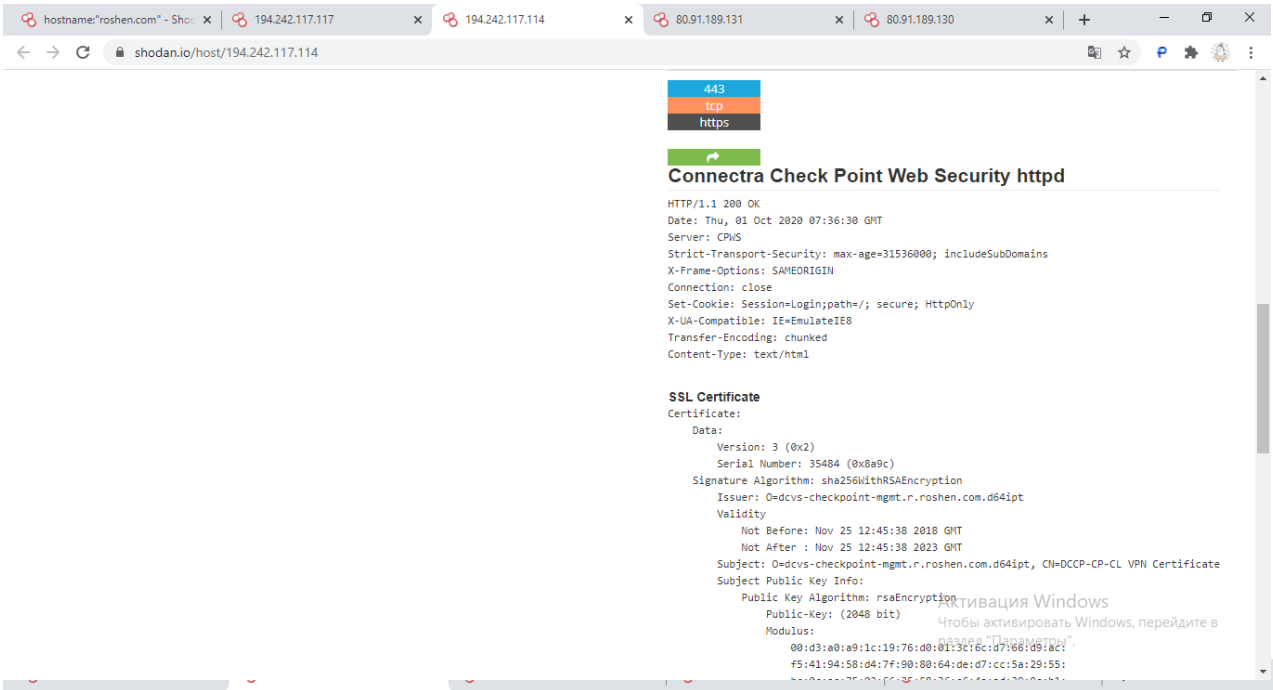
TASK 1

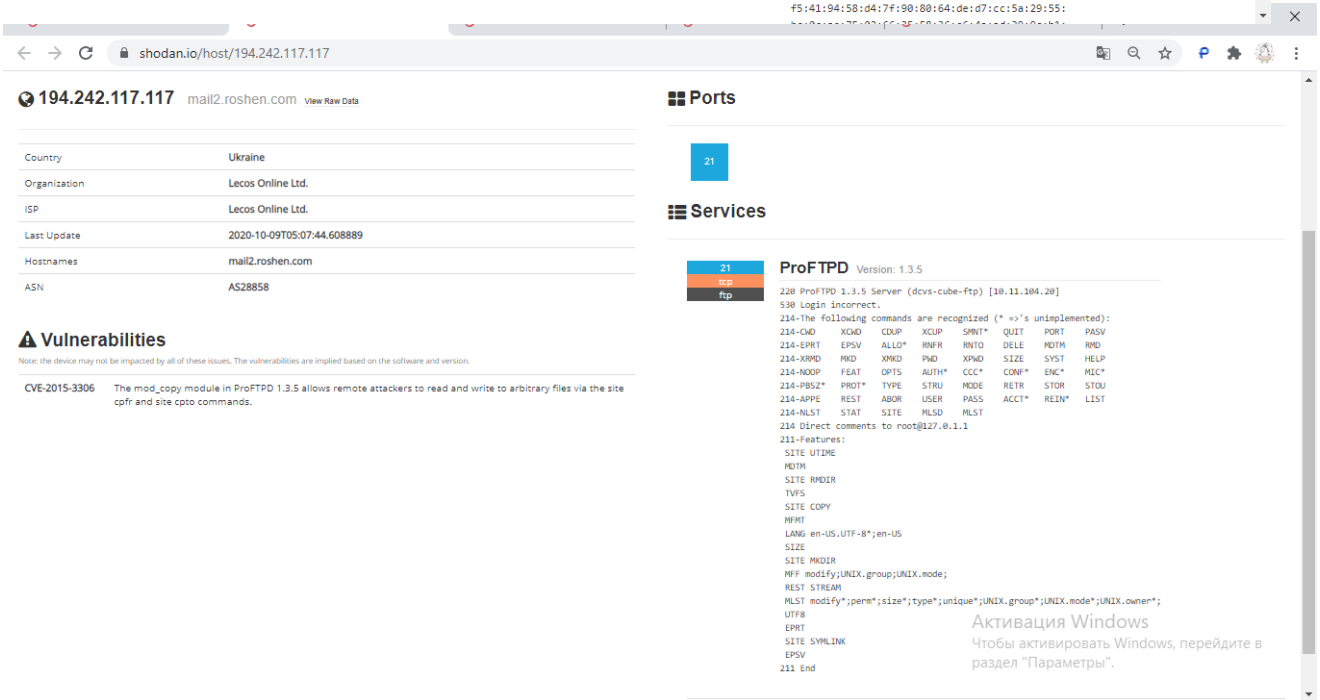
Which information could you obtain with Shodan? (prove with screenshots)

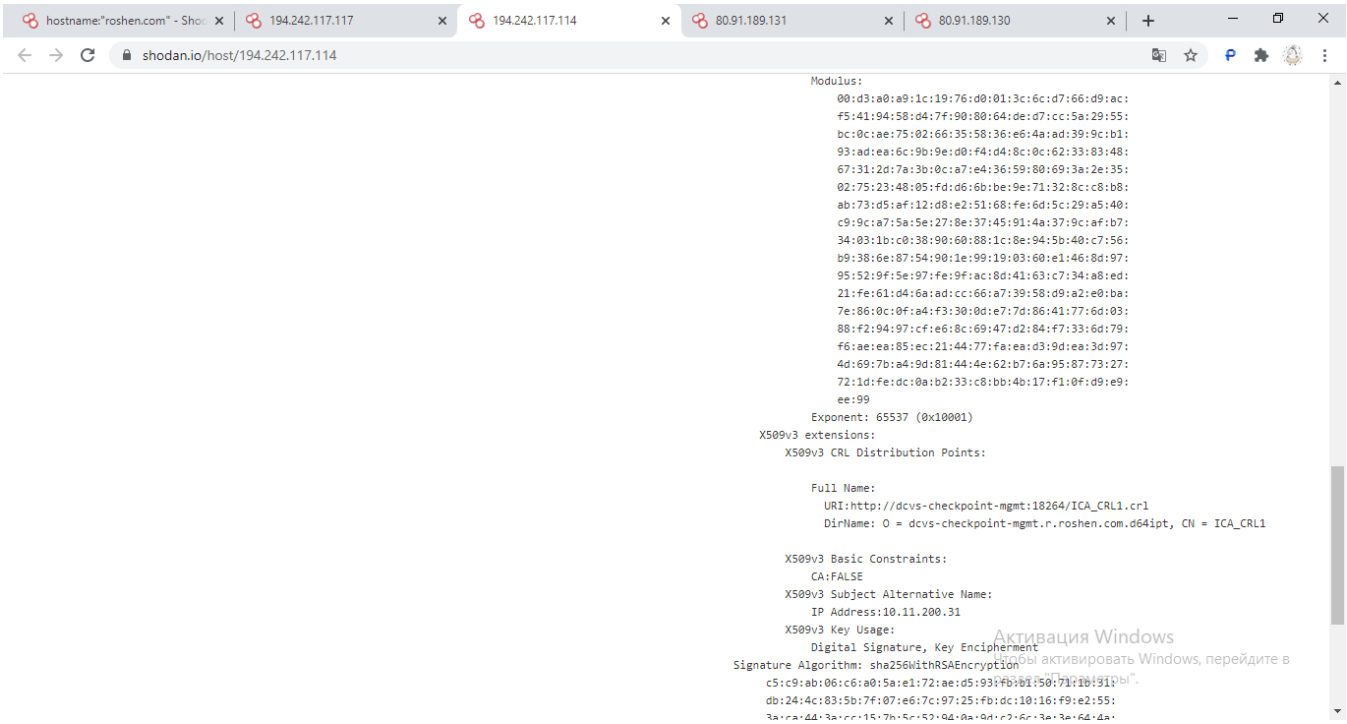
Answer:

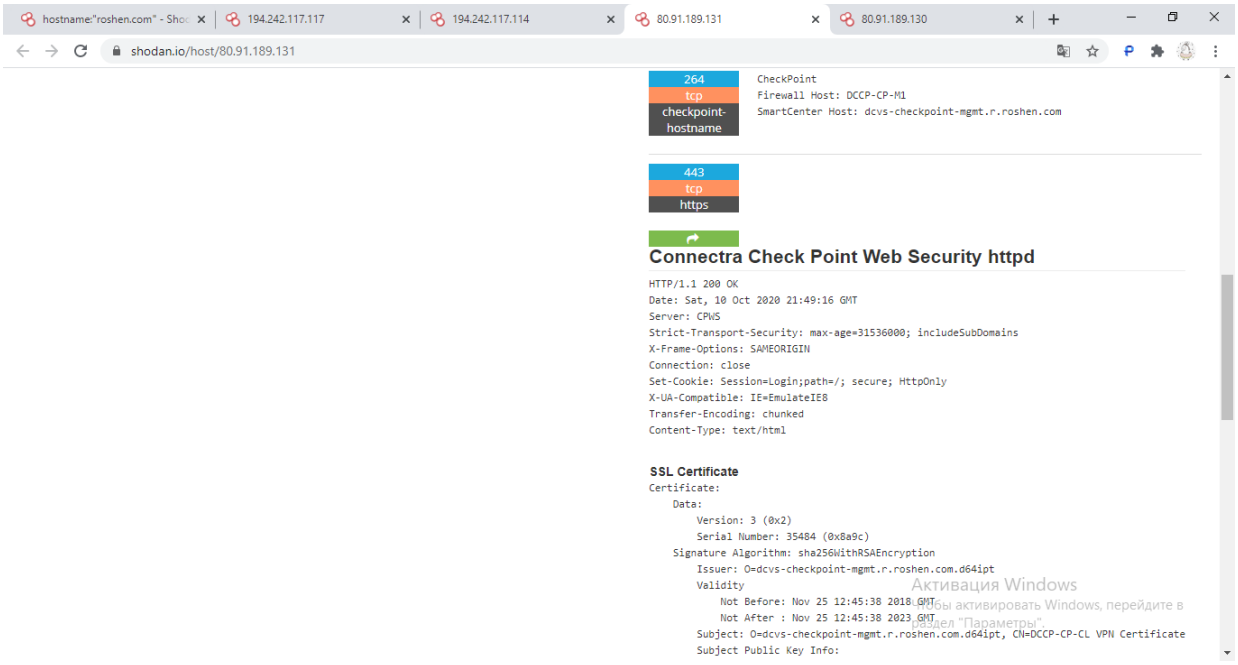
Shodan can give information of objects such as location, organization, http-response, opened ports, donaims, operation system.

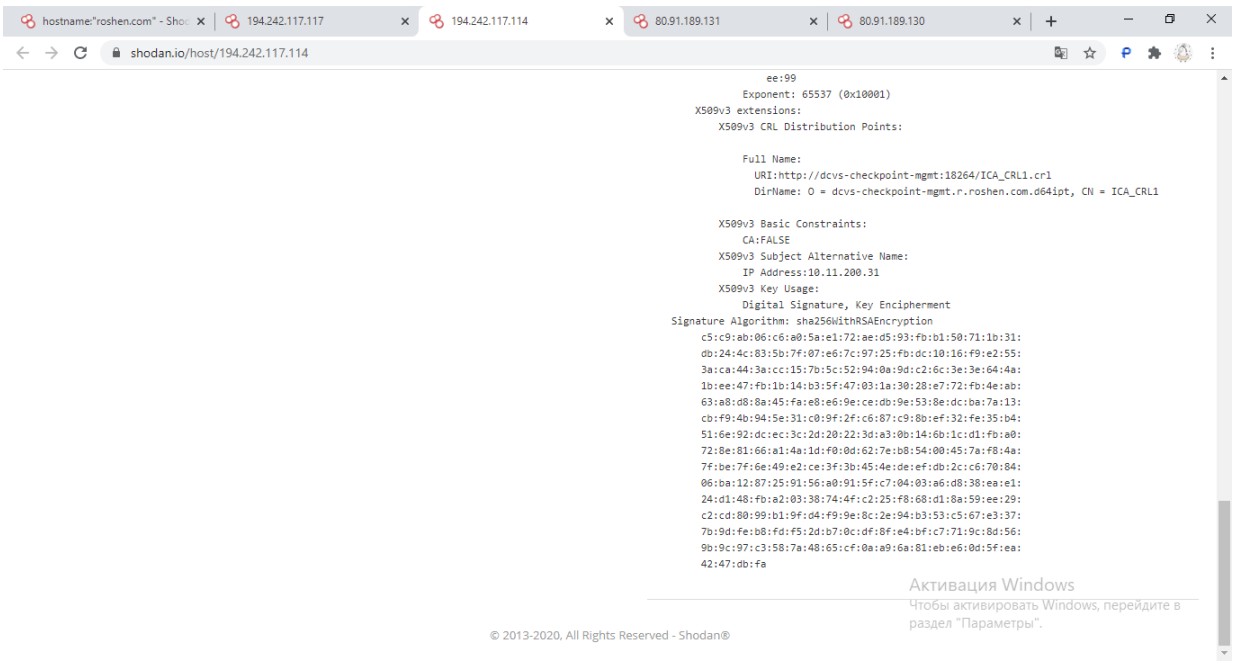

hostname:"roshen.com" - Sho
194.242.117.117
194.242.117.114
80.91.189.131
80.91.189.130
shodan.io/host/194.242.117.114
194.242.117.114 mail.kkf.roshen.com View Raw Data
Country Ukraine
Organization Lecos Online Ltd.
ISP Lecos Online Ltd.
Last Update 2020-10-10T04:50:25.692822
Hostnames mail.kkf.roshen.com
ASN AS28858
Web Technologies
ExtJS
Ports
25 80 264 443
Services
25 tcp smtp
Postfix smtpd
220 DCCP-CP-M1 ESMTP Postfix
250-DCCP-CP-M1
250-SIZE
250-VRFY
250-ETRN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
80 tcp http
HTTP/1.0 301 Moved Permanently
Location: https://194.242.117.114/
264 tcp checkpoint-hostname
CheckPoint
Firewall Host: DCCP-CP-M1
SmartCenter Host: dcvs-checkpoint-mgmt.r.roshen.com
Активация Windows
Чтобы активировать Windows, перейдите в раздел "Параметры".

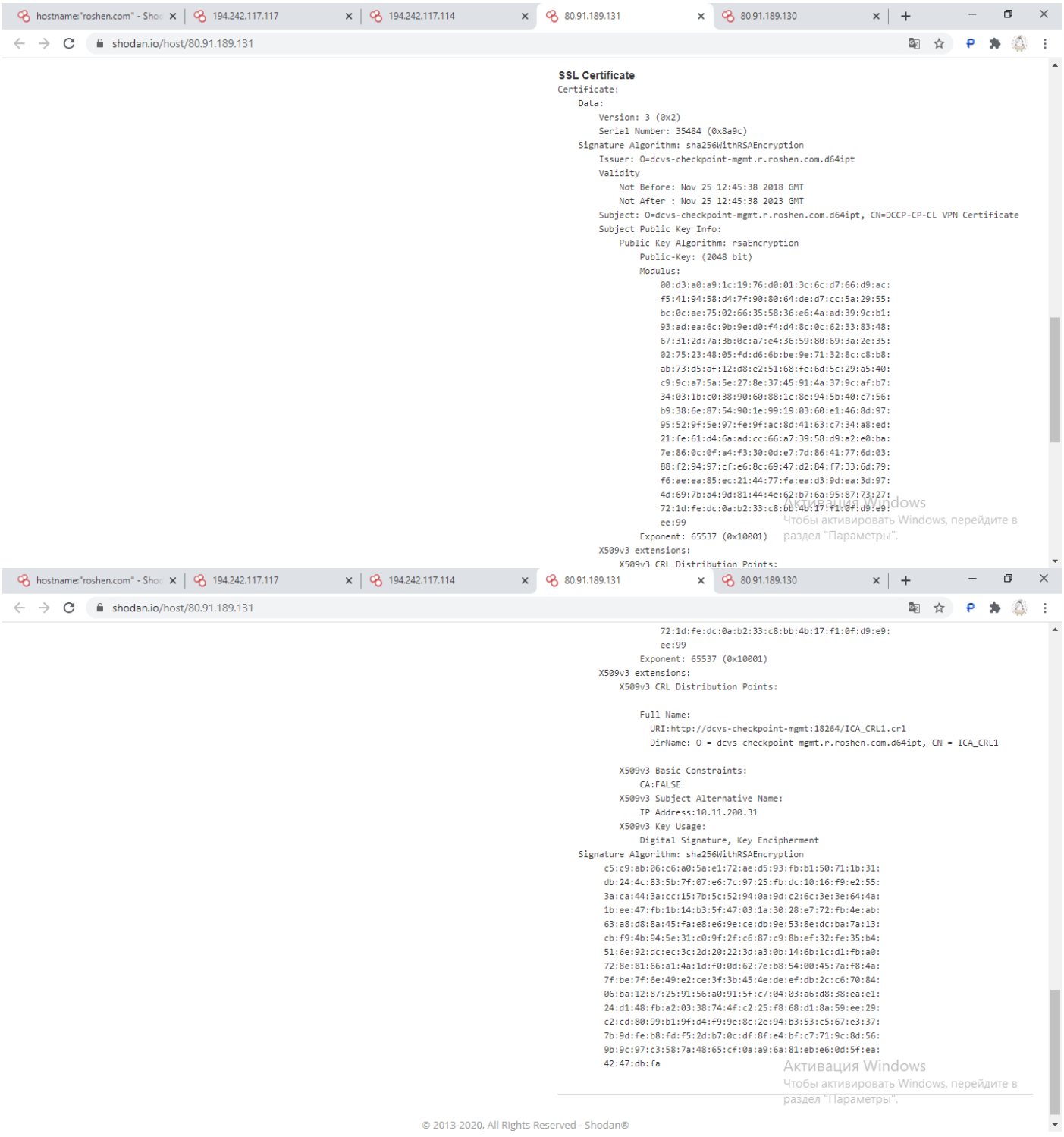

hostname:"roshen.com" - Sho
194.242.117.117
194.242.117.114
80.91.189.131
80.91.189.130
shodan.io/host/194.242.117.114
443 tcp https
Connectra Check Point Web Security httpd
HTTP/1.1 200 OK
Date: Thu, 01 Oct 2020 07:36:30 GMT
Server: CPWS
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Frame-Options: SAMEORIGIN
Connection: close
Set-Cookie: Session=Login;path=/; secure; HttpOnly
X-UA-Compatible: IE=EmulateIE8
Transfer-Encoding: chunked
Content-Type: text/html
SSL Certificate
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 35484 (0x8a9c)
Signature Algorithm: sha256WithRSAEncryption
Issuer: O=dcvs-checkpoint-mgmt.r.roshen.com.d64ipt
Validity
Not Before: Nov 25 12:45:38 2018 GMT
Not After : Nov 25 12:45:38 2023 GMT
Subject: O=dcvs-checkpoint-mgmt.r.roshen.com.d64ipt, CN=DCCP-CP-CL VPN Certificate
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:d3:a0:a9:1c:19:76:d0:01:3c:6c:d7:66:d9:ac:
f5:41:94:58:d4:7f:90:80:64:de:d7:cc:5a:29:55:
Активация Windows
Чтобы активировать Windows, перейдите в раздел "Параметры".


shodan.io/host/194.242.117.117
194.242.117.117 mail2.roshen.com View Raw Data
Country Ukraine
Organization Lecos Online Ltd.
ISP Lecos Online Ltd.
Last Update 2020-10-09T05:07:44.608889
Hostnames mail2.roshen.com
ASN AS28858
Vulnerabilities
Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.
CVE-2015-3306 The mod_copy module in ProFTPD 1.3.5 allows remote attackers to read and write to arbitrary files via the site cpfr and site cpto commands.
Ports
21
Services
21 tcp ftp
ProFTPD Version: 1.3.5
220 ProFTPD 1.3.5 Server (dcvs-cube-ftp) [10.11.104.20]
530 Login incorrect.
214-The following commands are recognized (* =>'s unimplemented):
214-CWD XCWD CDUP XCUP SMNT* QUIT PORT PASV
214-EPRT EPSV ALLO* RNFR RNTO DELE MDTM RMD
214-XRMD MKD XMKD PWD XPWD SIZE SYST HELP
214-NOOP FEAT OPTS AUTH* CCC* CONF* ENC* MIC*
214-PBSZ* PROT* TYPE STRU MODE RETR STOR STOU
214-APPE REST ABOR USER PASS ACCT* REIN* LIST
214-NLST STAT SITE MLSD MLST
214 Direct comments to root@127.0.1.1
211-Features:
SITE UTIME
MDTM
SITE RMDIR
TVFS
SITE COPY
MFMT
LANG en-US.UTF-8*;en-US
SIZE
SITE MKDIR
MFF modify;UNIX.group;UNIX.mode;
REST STREAM
MLST modify*;perm*;size*;type*;unique*;UNIX.group*;UNIX.mode*;UNIX.owner*;
UTF8
EPRT
SITE SYMLINK
EPSV
211 End
Активация Windows
Чтобы активировать Windows, перейдите в раздел "Параметры".


hostname:"roshen.com" - Sho
194.242.117.117
194.242.117.114
80.91.189.131
80.91.189.130
shodan.io/host/194.242.117.114
Modulus:
00:d3:a0:a9:1c:19:76:d0:01:3c:6c:d7:66:d9:ac:
f5:41:94:58:d4:7f:90:80:64:de:d7:cc:5a:29:55:
bc:0c:ae:75:02:66:35:58:36:e6:4a:ad:39:9c:b1:
93:ad:ea:6c:9b:9e:d0:f4:d4:8c:0c:62:33:83:48:
67:31:2d:7a:3b:0c:a7:e4:36:59:80:69:3a:2e:35:
02:75:23:48:05:fd:d6:6b:be:9e:71:32:8c:c8:b8:
ab:73:d5:af:12:d8:e2:51:68:fe:6d:5c:29:a5:40:
c9:9c:a7:5a:5e:27:8e:37:45:91:4a:37:9c:af:b7:
34:03:1b:c0:38:90:60:88:1c:8e:94:5b:40:c7:56:
b9:38:6e:87:54:90:1e:99:19:03:60:e1:46:8d:97:
95:52:9f:5e:97:fe:9f:ac:8d:41:63:c7:34:a8:ed:
21:fe:61:d4:6a:ad:cc:66:a7:39:58:d9:a2:e0:ba:
7e:86:0c:0f:a4:f3:30:0d:e7:7d:86:41:77:6d:03:
88:f2:94:97:cf:e6:8c:69:47:d2:84:f7:33:6d:79:
f6:ae:ea:85:ec:21:44:77:fa:ea:d3:9d:ea:3d:97:
4d:69:7b:a4:9d:81:44:4e:62:b7:6a:95:87:73:27:
72:1d:fe:dc:0a:b2:33:c8:bb:4b:17:f1:0f:d9:e9:
ee:99
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 CRL Distribution Points:
Full Name:
URI:http://dcvs-checkpoint-mgmt:18264/ICA_CRL1.crl
DirName: O = dcvs-checkpoint-mgmt.r.roshen.com.d64ipt, CN = ICA_CRL1
X509v3 Basic Constraints:
CA:FALSE
X509v3 Subject Alternative Name:
IP Address:10.11.200.31
X509v3 Key Usage:
Digital Signature, Key Encipherment
Signature Algorithm: sha256WithRSAEncryption
c5:c9:ab:06:c6:a0:5a:e1:72:ae:d5:93:fb:b1:50:71:1b:31:
db:24:4c:83:5b:7f:07:e6:7c:97:25:fb:dc:10:16:f9:e2:55:
Активация Windows
Чтобы активировать Windows, перейдите в раздел "Параметры".


hostname:"roshen.com" - Sho
194.242.117.117
194.242.117.114
80.91.189.131
80.91.189.130
shodan.io/host/80.91.189.131
264
tcp
checkpoint-hostname
CheckPoint
Firewall Host: DCCP-CP-M1
SmartCenter Host: dcvs-checkpoint-mgmt.r.roshen.com
443
tcp
https
Connectra Check Point Web Security httpd
HTTP/1.1 200 OK
Date: Sat, 10 Oct 2020 21:49:16 GMT
Server: CPWS
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Frame-Options: SAMEORIGIN
Connection: close
Set-Cookie: Session=Login;path=/; secure; HttpOnly
X-UA-Compatible: IE=EmulateIE8
Transfer-Encoding: chunked
Content-Type: text/html
SSL Certificate
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 35484 (0x8a9c)
Signature Algorithm: sha256WithRSAEncryption
Issuer: O=dcvs-checkpoint-mgmt.r.roshen.com.d64ipt
Validity
Not Before: Nov 25 12:45:38 2018 GMT
Not After : Nov 25 12:45:38 2023 GMT
Subject: O=dcvs-checkpoint-mgmt.r.roshen.com.d64ipt, CN=DCCP-CP-CL VPN Certificate
Subject Public Key Info:
Активация Windows
Чтобы активировать Windows, перейдите в раздел "Параметры".


hostname:"roshen.com" - Sho
194.242.117.117
194.242.117.114
80.91.189.131
80.91.189.130
shodan.io/host/194.242.117.114
ee:99
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 CRL Distribution Points:
Full Name:
URI:http://dcvs-checkpoint-mgmt:18264/ICA_CRL1.crl
DirName: O = dcvs-checkpoint-mgmt.r.roshen.com.d64ipt, CN = ICA_CRL1
X509v3 Basic Constraints:
CA:FALSE
X509v3 Subject Alternative Name:
IP Address:10.11.200.31
X509v3 Key Usage:
Digital Signature, Key Encipherment
Signature Algorithm: sha256WithRSAEncryption
c5:c9:ab:06:c6:a0:5a:e1:72:ae:d5:93:fb:b1:50:71:1b:31:
db:24:4c:83:5b:7f:07:e6:7c:97:25:fb:dc:10:16:f9:e2:55:
3a:ca:44:3a:cc:15:7b:5c:52:94:0a:9d:c2:6c:3e:3e:64:4a:
1b:ee:47:fb:1b:14:b3:5f:47:03:1a:30:28:e7:72:fb:4e:ab:
63:a8:d8:8a:45:fa:e8:e6:9e:ce:db:9e:53:8e:dc:ba:7a:13:
cb:f9:4b:94:5e:31:c0:9f:2f:c6:87:c9:8b:ef:32:fe:35:b4:
51:6e:92:dc:ec:3c:2d:20:22:3d:a3:0b:14:6b:1c:d1:fb:a0:
72:8e:81:66:a1:4a:1d:f0:0d:62:7e:b8:54:00:45:7a:f8:4a:
7f:be:7f:6e:49:e2:ce:3f:3b:45:4e:de:ef:db:2c:c6:70:84:
06:ba:12:87:25:91:56:a0:91:5f:c7:04:03:a6:d8:38:ea:e1:
24:d1:48:fb:a2:03:38:74:4f:c2:25:f8:68:d1:8a:59:ee:29:
c2:cd:80:99:b1:9f:d4:f9:9e:8c:2e:94:b3:53:c5:67:e3:37:
7b:9d:fe:b8:fd:f5:2d:b7:0c:df:8f:e4:bf:c7:71:9c:8d:56:
9b:9c:97:c3:58:7a:48:65:cf:0a:a9:6a:81:eb:e6:0d:5f:ea:
42:47:db:fa
Активация Windows
Чтобы активировать Windows, перейдите в раздел "Параметры".
© 2013-2020, All Rights Reserved - Shodan®



TASK 2

Are any additional information about researched target? (prove with screenshots)

Answer:

We have also information about services, web technologies, vulnerabilities and SSL Certificate.

Exercise 5. Automate OSINT with Maltego and FOCA

Purpose: understand Maltego facilities

After the work the student must

- know: how Maltego works

Tasks:

- obtain all information from previous steps with Maltego facilities

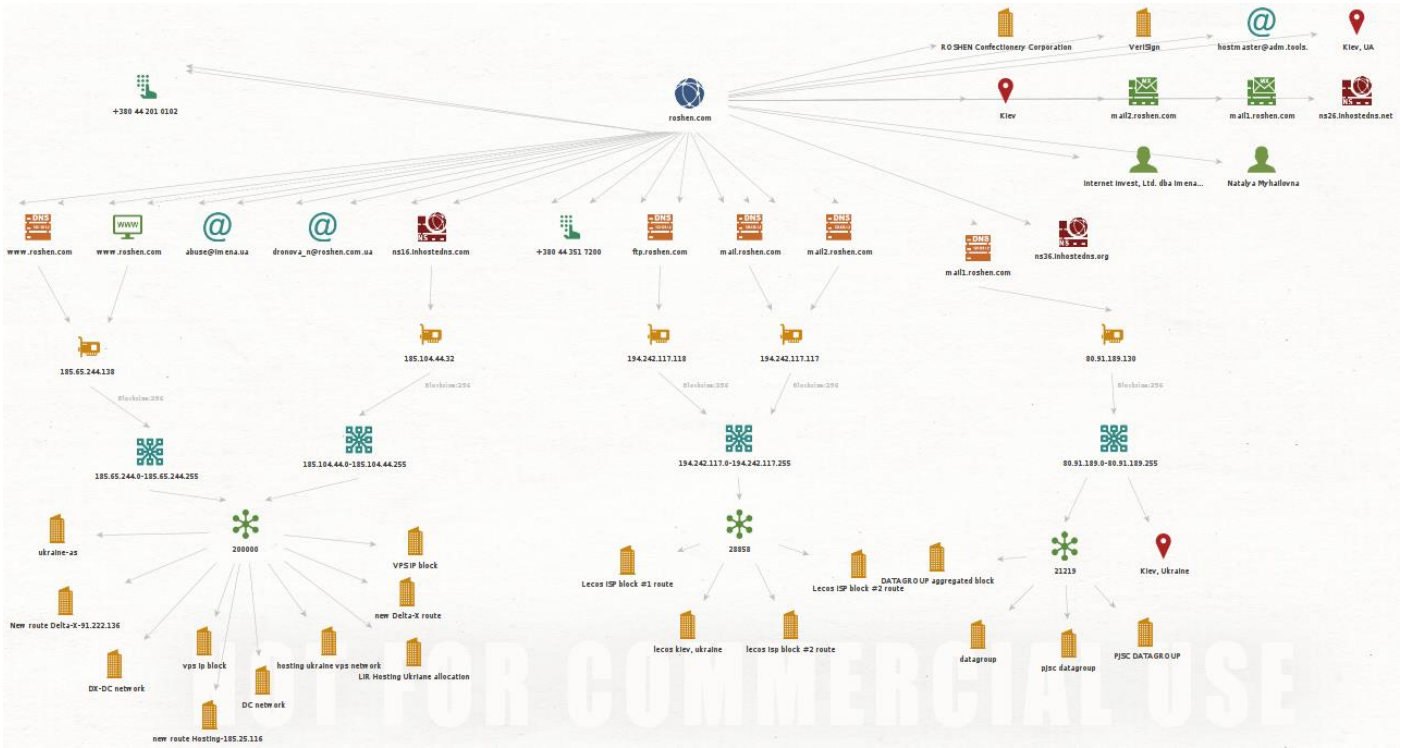
Material and technical equipping of the workplace

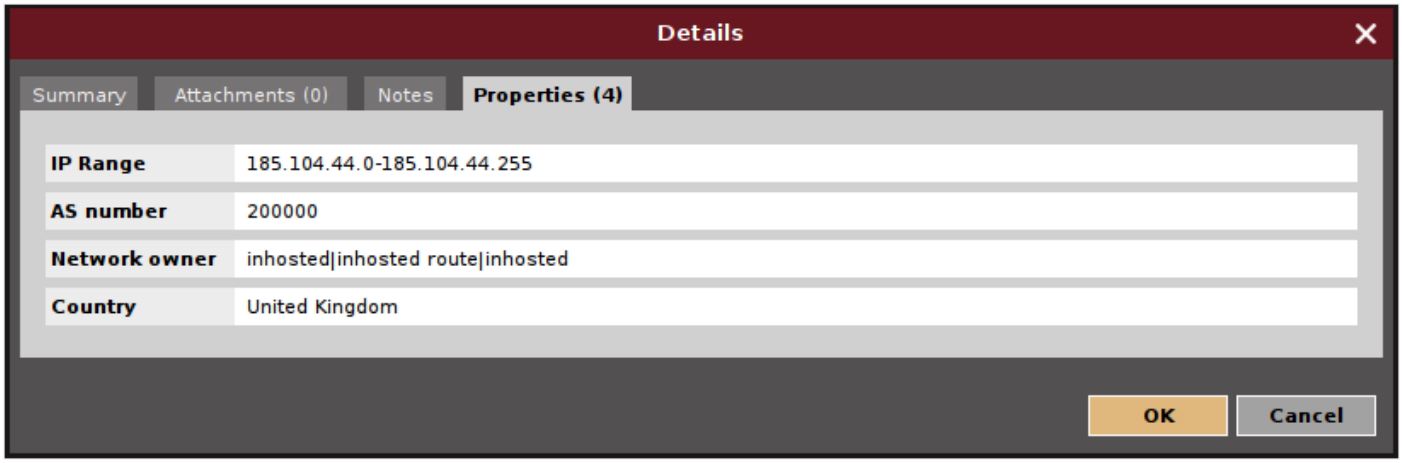
- Maltego
- FOCA

TASK 1

Which information could you obtain with Maltego? (prove with screenshots)

Answer:





TASK 2

Are any differences from automated and manual data gathering? (prove with screenshots) Explain.

Answer:

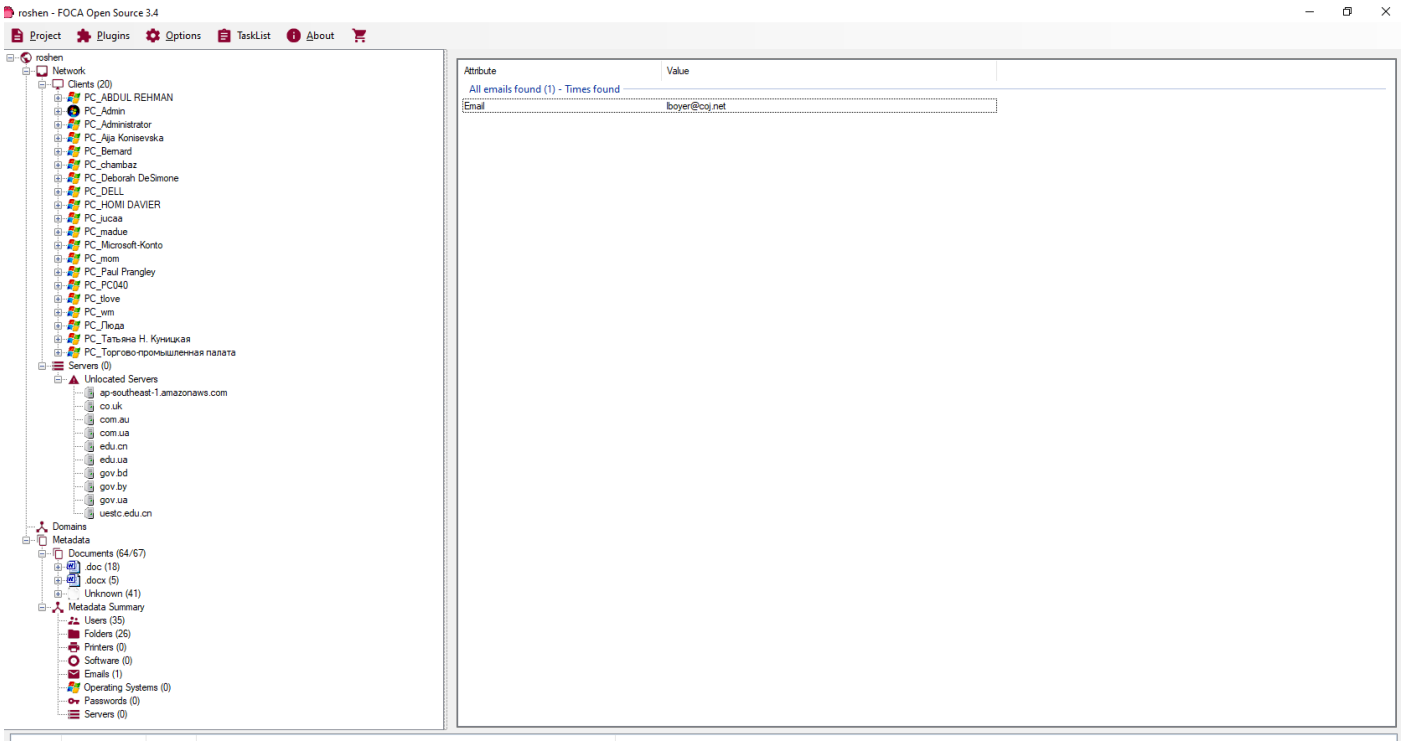
TASK 3 & TASK 4

Download and extract metadata from files obtained from target company domain/subdomains with FOCA? (prove with screenshots) Explain.

Are any usernames / emails? (prove with screenshots)

I found 20 usernames and 1 email. Can obtain a lot of metadata from .docx and .doc

Answer:



Exercise 6. Checking credentials with Pastebin and Haveibeenpwned

Purpose: understand OSIT

After the work the student must

- know: how to check credentials in public available databases

Tasks:

- check all credentials from previous steps with provided resources

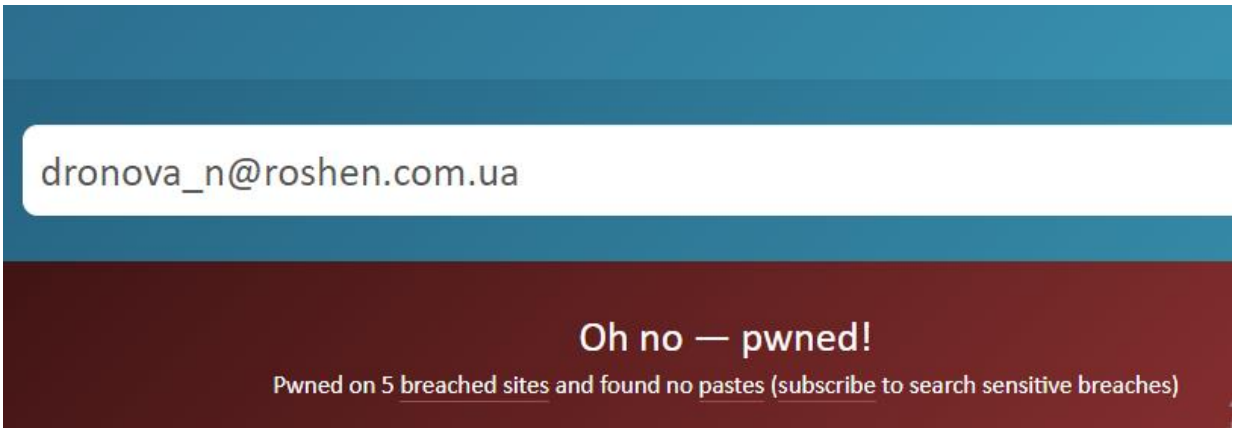
Material and technical equipping of the workplace

- https://haveibeenpwned.com/
- https://pastebin.com/

TASK 1

Check obtained emails with Haveibeenpwned? (prove results with screenshots) Is something interesting?

Answer:



TASK 2

Check obtained emails, domains and IP-addresses with Pastebin? (prove results with screenshots) Is something interesting?

Answer:

I tried to obtain something interesting, however all info was boring.