IN5290 Ethical Hacking

Lecture 2: Technical Information Gathering

Universitetet i Oslo

Laszlo Erdödi

Lecture Overview

- What are the technical information of the target
- How to collect the technical information
- Typical network layouts
- Identifying the network range of the target

Technical information

- Domain names of the target
- Domain owner(s) of the target
- Domain registrants
- Ip addresses associated with the target websites
- Ip ranges of the target
- Ip range owner(s)
- List of hosted websites
- Hosting companies
- Etc

Domain names

A **domain name** is an identification string that defines a realm of administrative autonomy, authority or control within the Internet.

Example: **aftenposten.no**

second level domain.topleveldomain

Domain names are formed by the rules and procedures of the Domain Name System (DNS). Any name registered in the DNS is a domain name.

Top level domain can be (com, net, info, edu, org and country code) Second and third level domains can be any string. The full length of the domain cannot be longer than 255 characters.

www.mn.uio.no

Domain names

www.mn.uio.no

hostname.thirdlevel.secondlevel.TLD

- A hostname is a domain name that has at least one associated IP address
- The first domain was registered in 1985 (symbolics.com)
- Domains are registered by the domain registrars that are accredited by the Internet Corporation for Assigned Names and Numbers (ICANN)
- each TLD is maintained and serviced technically by an administrative organization operating a registry (*UNINETT Norid AS* for .no)
- All data has to be published and accessible with the *whois* protocol

Domain name registration data – whois (e.g. http://who.is)

The *whois* database must contain the following information:

- Administrative contact
- Technical contact
- Billing contact
- Name servers

Nameservers are computers that provide subdomain information for the particular domain using the *dns* protocol

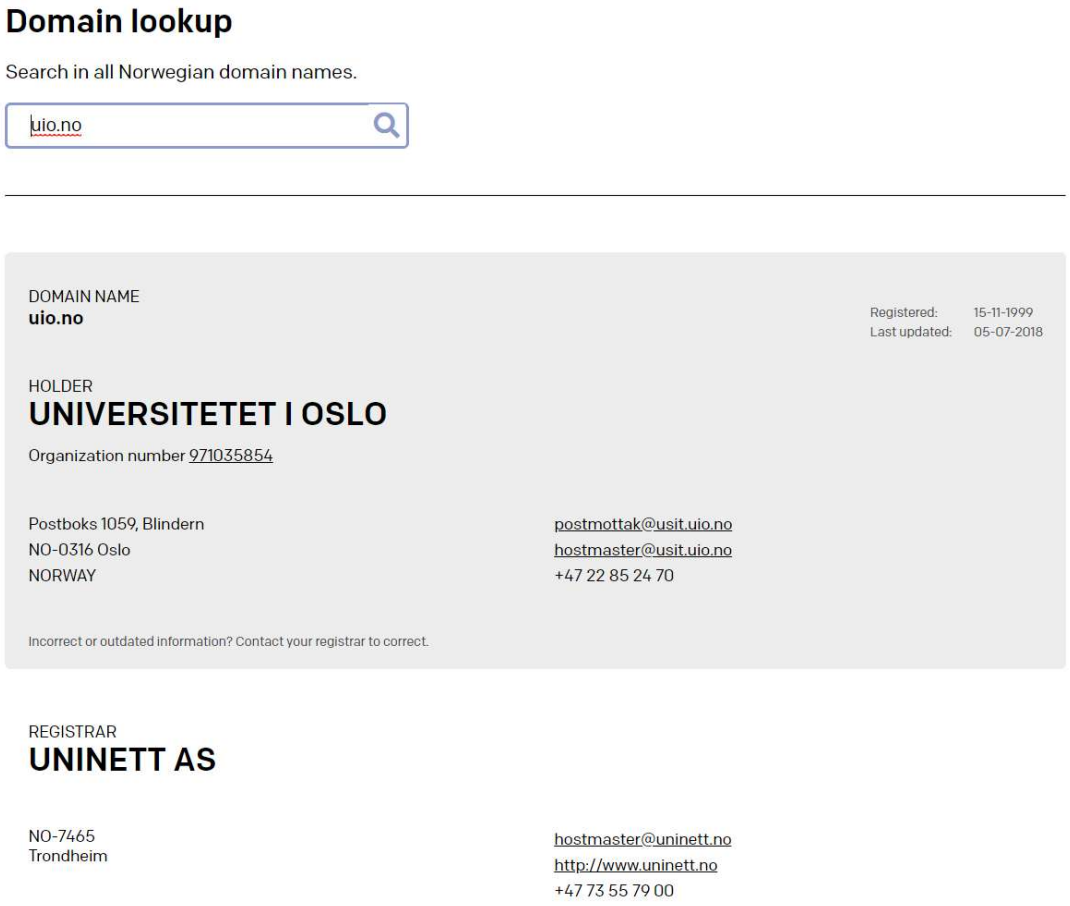
Registrant Contact Information:	
Name	Domain Name Manager
Organization	Turner Broadcasting System, Inc.
Address	One CNN Center
City	Atlanta
State / Province	GA
Postal Code	30303
Country	US
Phone	+1.4048275000
Fax	+1.4048271995
Email	tngroup@turner.com

Administrative Contact Information:	
Name	Domain Name Manager
Organization	Turner Broadcasting System, Inc.
Address	One CNN Center
City	Atlanta
State / Province	GA
Postal Code	30303
Country	US
Phone	+1.4048275000
Fax	+1.4048271995
Email	tngroup@turner.com

Technical Contact Information:	
Name	Domain Name Manager
Organization	Turner Broadcasting System, Inc.
Address	One CNN Center
City	Atlanta
State / Province	GA
Postal Code	30303
Country	US
Phone	+1.4048275000
Fax	+1.4048271995
Email	tngroup@turner.com

Domain names

- Unique name with country code (TLD)
- Domain names belong to private individuals or companies
- Everyone can register a domain (for trademarks there's a priority)
- A domain name is only the right to use a special string, it is not an ip and not a computer!



Domain name owner examples

Find the owner of the following domains:

- nrk.no
- dyreparken.no
- horsepro.no

Find a contact phone number for the following domains:

- footish.se
- termesangiovanni.it

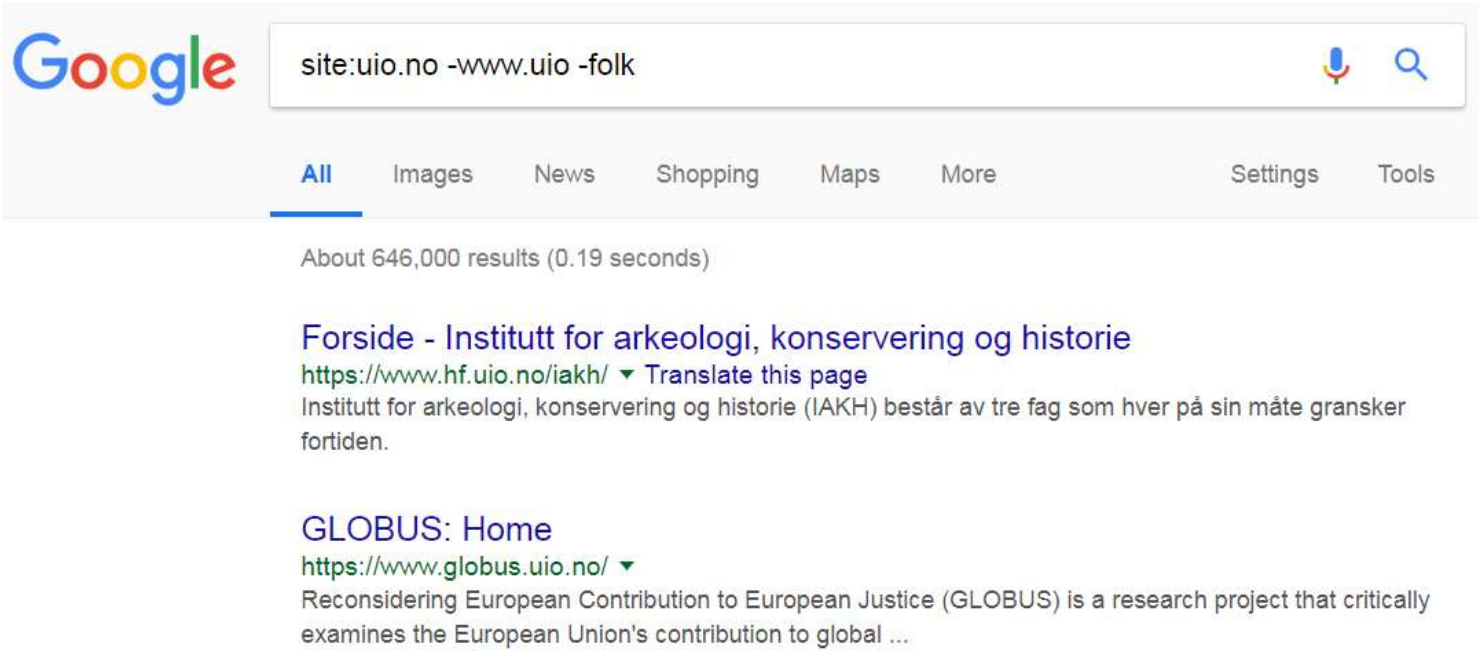
When is the expiration date of the following domains:

- timeanddate.com

Domain name search

- Example1: find third level domains for *uio.no*!

Use the Google with the site: keyword



- Example2: find third level domains for dn.no!

Domain name search - Netcraft

- Finding domains with its owner
- OS version detection

Results for uio.no

Found 12 sites

	Site	Site Report	First seen	Netblock	OS
1.	www.uio.no		august 1995	university of oslo, norway	cisco
2.	folk.uio.no		october 2001	university of oslo, norway	linux
3.	www.mn.uio.no		may 1996	university of oslo, norway	cisco
4.	heim.ifi.uio.no		april 2003	university of oslo, norway	linux - redhat
5.	www.sv.uio.no		october 1995	university of oslo, norway	cisco
6.	www.khm.uio.no		november 2004	university of oslo, norway	cisco
7.	foni.uio.no		august 2011	university of oslo, norway	linux - redhat
8.	www.med.uio.no		may 1996	university of oslo, norway	cisco
9.	app.uio.no		febuary 2017	university of oslo, norway	unknown
10.	passwords12.at.ifi.uio.no		febuary 2013	university of oslo, norway	linux - redhat
11.	home.ifi.uio.no		november 2003	university of oslo, norway	linux - redhat
12.	munin.ping.uio.no		october 2004	university of oslo	linux - debian

Domain name search – Pentest tools

✔ uio.no

Found 79 subdomains

Subdomain	IP address	OS	Server	Technology	Web Platform
localhost.uio.no	127.0.0.1				
vpn1.uio.no	129.240.0.82				
vpn.uio.no	129.240.0.86				
ns2.uio.no	129.240.2.6				
ntp.uio.no	129.240.2.6				
bart.uio.no	129.240.2.42				
storm.uio.no	129.240.2.42				
dummy.uio.no	129.240.2.42				
random.uio.no	129.240.2.42				
data.uio.no	129.240.2.42				
transport.uio.no	129.240.2.42				
scan.uio.no	129.240.2.42				
snmp.uio.no	129.240.2.42				
cvs.uio.no	129.240.2.42				

Domain name search – Dns dumpster

dnsdumpster.com

bimi.ab.ntnu.no	129.241.37.16	UNINETT UNINETT, The Norwegian University & Research Network Norway
brua.ab.ntnu.no	129.241.20.76	UNINETT UNINETT, The Norwegian University & Research Network Norway
gata.ab.ntnu.no	129.241.20.70	UNINETT UNINETT, The Norwegian University & Research Network Norway
havna.ab.ntnu.no	129.241.20.74	UNINETT UNINETT, The Norwegian University & Research Network Norway
parken.ab.ntnu.no	129.241.20.72	UNINETT UNINETT, The Norwegian University & Research Network Norway
stien.ab.ntnu.no	129.241.20.77	UNINETT UNINETT, The Norwegian University & Research Network Norway
torget.ab.ntnu.no	129.241.20.75	UNINETT UNINETT, The Norwegian University & Research Network Norway
adfs.ntnu.no	129.241.34.154	UNINETT UNINETT, The Norwegian University & Research Network Norway
adm.ntnu.no	129.241.161.62	UNINETT UNINETT, The Norwegian University & Research Network Norway

Domain name search – Certificate transparency logs

crt.sh Identity Search

Group by Issuer

Criteria	Type: Identity Match: ILIKE Search: 'uio.no'

crt.sh ID	Logged At ⇧	Not Before	Not After	Common Name	Matching Identities	
2387358455	2020-01-29	2006-01-16	2007-02-09	www.jus.uio.no	www.jus.uio.no	C=ZA, O=Thawte Con
2379225639	2020-01-26	2007-07-03	2010-07-03	warning.uio.no	nagios.uio.no warning.uio.no	C=BE, O=Cybertrust, (
2379225493	2020-01-26	2008-04-25	2010-04-25	datapakken.uio.no	datapakken.uio.no	C=BE, O=Cybertrust, (
2379225582	2020-01-26	2008-10-31	2011-10-31	vortex-pr-2.uio.no	vortex-pr-2.uio.no	C=BE, O=Cybertrust, (
2379225666	2020-01-26	2008-10-31	2011-10-31	vortex-pr-1.uio.no	vortex-pr-1.uio.no	C=BE, O=Cybertrust, (
2379225099	2020-01-26	2007-08-14	2010-08-14	nav.uio.no	nav.uio.no	C=BE, O=Cybertrust, (
2379224048	2020-01-26	2008-04-25	2011-04-25	www.okonomi.uio.no	okonomi.uio.no www.okonomi.uio.no	C=BE, O=Cybertrust, (
2379220837	2020-01-26	2008-12-17	2011-12-17	vpn2.uio.no	vpn2.uio.no vpn.uio.no	C=BE, O=Cybertrust, (
2379220856	2020-01-26	2007-11-15	2010-11-15	wwws.ifi.uio.no	wwws.ifi.uio.no	C=BE, O=Cybertrust, (
2379220685	2020-01-26	2007-08-27	2010-08-27	valg.uio.no	valg.uio.no	C=BE, O=Cybertrust, (
2379220699	2020-01-26	2007-09-19	2010-09-19	hjelp.uio.no	hjelp.uio.no	C=BE, O=Cybertrust, (
2379218006	2020-01-26	2008-08-05	2011-08-05	sympa.uio.no	sympa.uio.no	C=BE, O=Cybertrust, (
2379216542	2020-01-26	2007-08-30	2010-08-30	dav.uio.no	dav.uio.no	C=BE, O=Cybertrust, (
2379217463	2020-01-26	2008-01-16	2011-01-16	dora.uio.no	dora.uio.no	C=BE, O=Cybertrust, (
2379213242	2020-01-26	2007-11-23	2010-11-23	webmail.uio.no	webmail.uio.no	C=BE, O=Cybertrust, (
2379212454	2020-01-26	2007-06-13	2010-06-13	nettskjema.uio.no	nettskjema.uio.no	C=BE, O=Cybertrust, (
2379210935	2020-01-26	2008-03-13	2011-03-13	www.bioportal.uio.no	www.bioportal.uio.no	C=BE, O=Cybertrust, (
2379212411	2020-01-26	2008-10-23	2011-10-23	www.personvern.uio.no	personvern.uio.no www.personvern.uio.no	C=BE, O=Cybertrust, (
2379210522	2020-01-26	2009-04-14	2012-04-14	wiki.uio.no	wiki.uio.no	C=BE, O=Cybertrust, (
2379207042	2020-01-26	2008-03-28	2011-03-28	vortex.uio.no	vortex.uio.no	C=BE, O=Cybertrust, (
2379207081	2020-01-26	2008-12-15	2011-12-15	www.journals.uio.no	www.journals.uio.no	C=BE, O=Cybertrust, (
2379206779	2020-01-26	2007-09-04	2010-09-04	blyant.uio.no	blyant.uio.no	C=BE, O=Cybertrust, (
2379206696	2020-01-26	2008-11-12	2011-11-12	husmann.uio.no	husmann.uio.no www2.hf.uio.no	C=BE, O=Cybertrust, (
2379205851	2020-01-26	2007-08-27	2010-08-27	minestudier.uio.no	minestudier.uio.no	C=BE, O=Cybertrust, (
2379203525	2020-01-26	2008-12-17	2011-12-17	vpn1.uio.no	vpn1.uio.no	C=BE, O=Cybertrust, (

IP addresses

- IPv4: 32bit (2^{32}=4 294 967 296 combinations)
- IPv6: 128bit (2^{128}=3.4*10^{38} combinations)

- IP addresses are for the identification of computers during the communication (OSI 3rd layer, see later).
- In order to be easy to memorize it, 8bit (byte) blocks are used for ipv4 e.g. **129.240.171.52**
- For ipv6 addresses are represented as eight groups of four hexadecimal digits e.g. **2001:0db8:0000:0042:0000:8a2e:0370:7334**

IP ranges – classful networking

IP ranges contain more ip addresses. e.g. 129.240.171.56—129.240.171.63 (8 addresses)

In 1981 the **classfull networking** was created. It consisted of the A, B, and C class of network ranges.

The idea was to divide the ip into the network and subnet part: **129.240.** **171.58**

identifies the network identifies the host within the network

Class A: 0.0.0.0	-127.255.255.255	128 ranges 256^3 in 1 range
Class B: 128.0.0.0	- 191.255.255.255	16384 ranges 256^2 in 1 range
Class C: 192.0.0.0	– 223.255.255.255	2097152 ranges 256 in 1 range

IP Ranges: Classless InterDomain Routing (CIDR)

- CIDR was created in 1993
- Network address length is arbitrary (not only 8,16,24 bits)

Examples:

129.240.171.56 (**10000001.11110000.10101011.00111**000) –
129.240.171.63 (**10000001.11110000.10101011.00111**111)

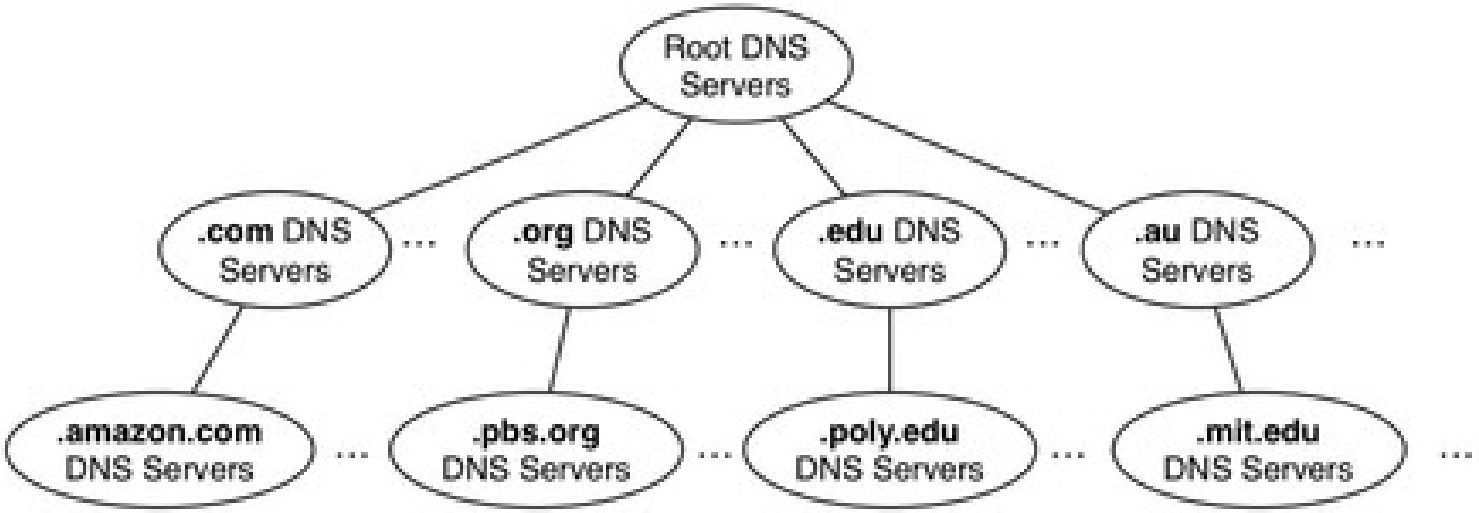
The first 29 bits are fixed in the range, the last three can be anything within the network: **CIDR: 129.240.171.56/29**

130.18.0.0 (**10000010.00010010**.00000000.00000000) –
130.19.255.255 (**10000010.00010011**.11111111.11111111)
130.18.0.0/15

IP Ranges CIDR - examples

- What is the first and last address of the /23 network range that contains: 194.172.10.10?
- What is the first and last address of the /18 network range that contains: 164.44.20.52?
- How many addresses does a /25 network range have?

Domain to ip conversion (DNS service)



- DNS servers are all around the world
- Organized in tree structure (13 root servers)
- The top level domains (.com, .net, .edu, .no, .de, etc.) are directly under the root servers
- DNS data are stored redundantly (master and slave server)

Domain to ip conversion (DNS service)

- Address Mapping **records** (A) ...
- IP Version 6 Address **records** (AAAA) ...
- Canonical Name **records** (CNAME) ...
- Host Information **records** (HINFO) ...
- Mail exchanger **record** (MX) ...
- Name Server **records** (NS) ...
- Reverse-lookup Pointer **records** (PTR)

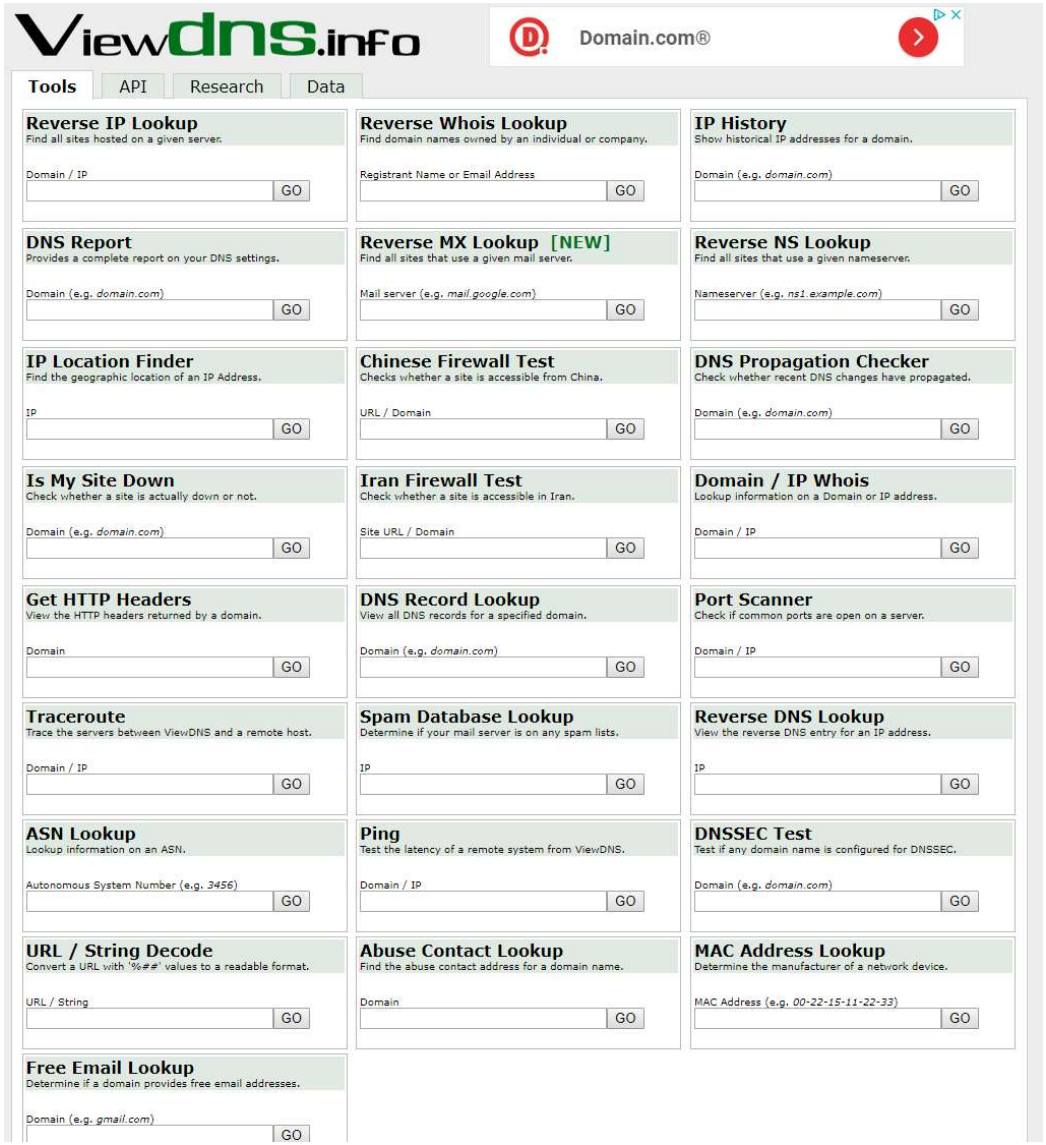
www.uio.no quick info	
General	
FQDN	www.uio.no
Host Name	www
Domain Name	uio.no
Registry	no
TLD	no
DNS	
IP numbers	*129.240.171.52*
Mail servers	*smtp.**uio**.no*
Domain DNS	
Name servers	*server.**nordu**.net* *ns1.**uio**.no* *ns2.**uio**.no* *nn.**uninett**.no*
Mail servers	*smtp.**uio**.no*
IP Numbers	*129.240.171.52*

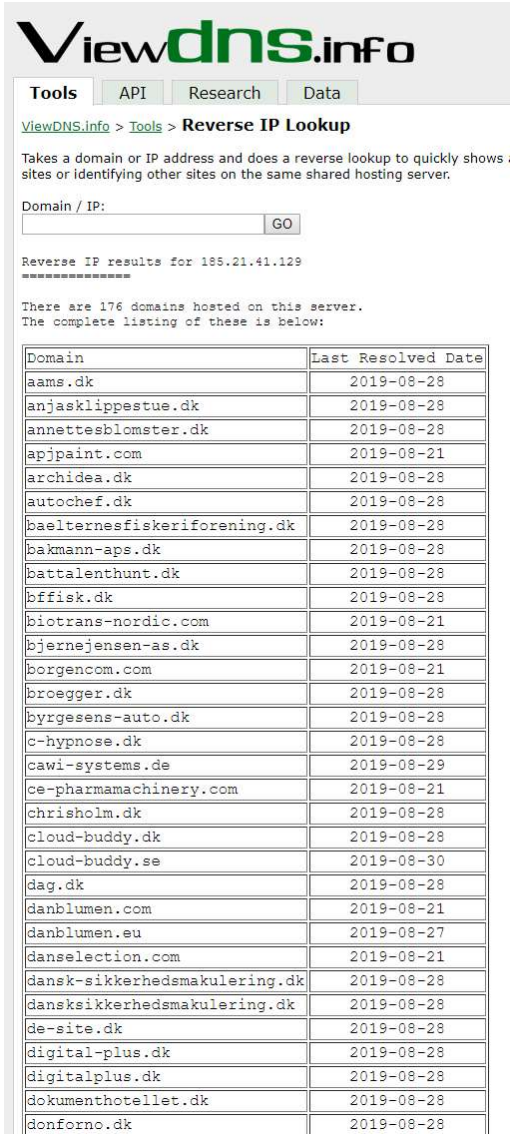
```
root@kali:~# nslookup www.uio.no
Server:         192.168.110.2
Address:        192.168.110.2#53

Non-authoritative answer:
Name:   www.uio.no
Address: 129.240.171.52

root@kali:~#
```

Ip lookup with dns – reverse ip lookup





Ip range owners

The *whois* protocol is also used to get the owner of a particular ip range.

The records are stored in different databases according to the continents.

The Norwegian entries are stored in the European database (RIPE NCC)
If we don't know which database to use the general *whois* protocol helps us.

Ip range owners

Who.is says the network region that contains 129.240.171.52 belongs to the RIPE database

IP Whois

```
NetRange:       129.240.0.0 - 129.242.255.255
CIDR:           129.240.0.0/15, 129.242.0.0/16
NetName:        RN-ERX-129-240-0-0
NetHandle:      NET-129-240-0-0-1
Parent:         NET129 (NET-129-0-0-0-0)
NetType:        Early Registrations, Transferred to RIPE NCC
OriginAS:
Organization:   RIPE Network Coordination Centre (RIPE)
RegDate:        2003-01-10
Updated:        2003-06-18
Comment:        These addresses have been further assigned to users in
Comment:        the RIPE NCC region.  Contact information can be found in
Comment:        the RIPE database at http://www.ripe.net/whois
Ref:            https://rdap.arin.net/registry/ip/129.240.0.0
```

```
inetnum:        129.240.0.0 - 129.240.255.255
netname:        UIONET
descr:          University of Oslo, Norway
country:        NO
```

```
person:         Knut Borge
address:        USIT/UiO
address:        Gaustadalleen 23, Blindern
address:        Postboks 1059 Blindern
address:        N-0316 Oslo
address:        NORWAY
phone:          +47 22 85 25 19
fax-no:         +47 22 85 27 30
e-mail:         unix-drift@usit.uio.no
nic-hdl:        KB100-RIPE
mnt-by:         UNINETT-MNT
created:        1970-01-01T00:00:00Z
last-modified:  2014-11-05T14:11:18Z
```

Login to update

Network range examples

Who is the owner of the following ips and how big is the related network range?

- 5.44.65.150
- 195.88.55.16
- 188.44.50.103
- 198.62.101.225
- 104.18.8.132

Hosted websites – Cloud services

- In several cases a website is hosted. That means it is stored on a webserver
  - that does not belong to the target organization
  - which can contain several other websites

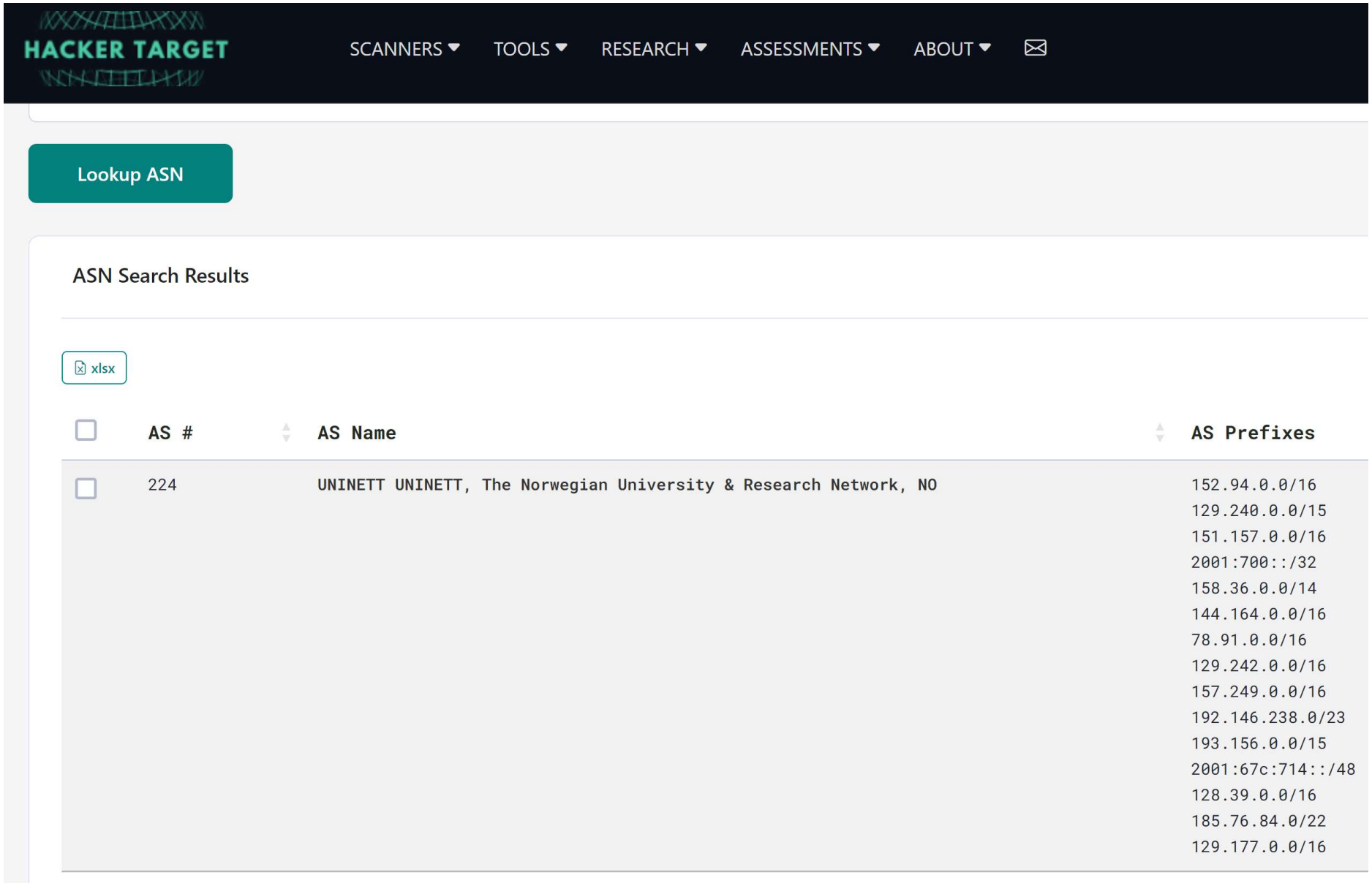
In those cases the webpage cannot be attacked or separate permission is needed from the owner of the server computer

Example: elektronikmesse.dk

Finding network ranges

- Search for all domains including second and third level
- Look for the corresponding ips
- Check which database contains the ip owner (*whois*)
- Check the ip ranges (*ripe, arin*, etc…)
- Check by AS number

ASN lookup


HACKER TARGET
SCANNERS
TOOLS
RESEARCH
ASSESSMENTS
ABOUT
Lookup ASN
ASN Search Results
xlsx
AS #
AS Name
AS Prefixes
224
UNINETT UNINETT, The Norwegian University & Research Network, NO
152.94.0.0/16
129.240.0.0/15
151.157.0.0/16
2001:700::/32
158.36.0.0/14
144.164.0.0/16
78.91.0.0/16
129.242.0.0/16
157.249.0.0/16
192.146.238.0/23
193.156.0.0/15
2001:67c:714::/48
128.39.0.0/16
185.76.84.0/22
129.177.0.0/16

Finding network ranges example

- Practice: Find the network ranges of the owner of dn.no
- Solution (demo)
  - dn.no belongs to the **DAGENS NÆRINGSLIV AS**
  - www.dn.no has the ip 87.238.54.132
  - ripe ncc says it is a part of the network range: 87.238.54.128-143
  - the owner of the range is the NHST media group
  - dn.no has the following second level domains: s1,s2,s3,s4, arkiv, multimedia, investor, hotell, idn, ww5, sjakk, pad
  - All the domains are associated with the same ip (87.238.54.132), except the pad.dn.no which is: 87.238.53.121, and the hosted websites (sjakk,)
  - The pad.dn.no is in the range of 87.238.53.0-143

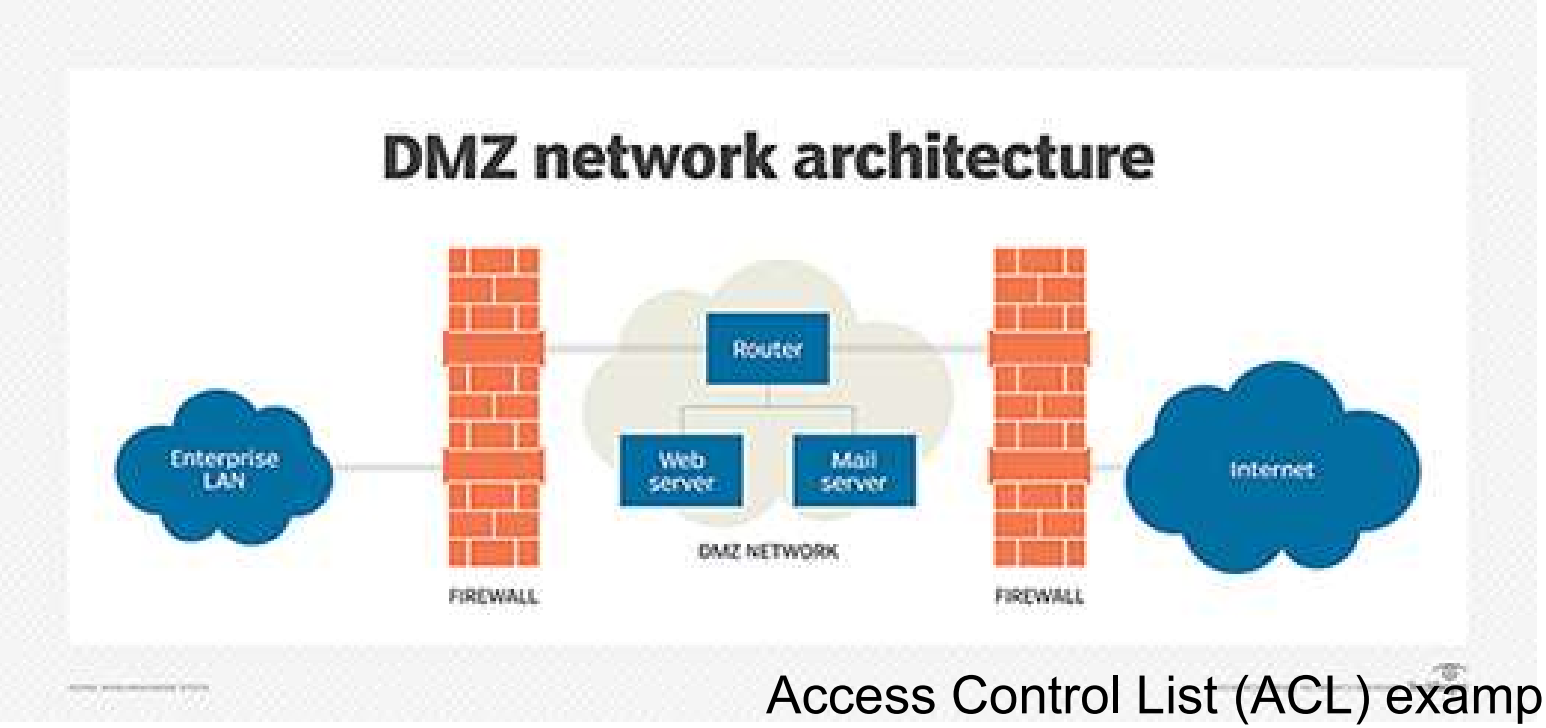
Finding network ranges –reverse whois

With the reverse *whois* service, we can search for domains by providing an email or name.
For example more than 100 domains are associated with the email nhst.no

Finding the range:
dnavis.no -> 87.238.54.132

Domain Name	Creation Date	Registrar
2thefuture.com	2015-04-03	DOMENESHOP AS
2thefuture.no	2013-08-27	
admdir.no	2012-01-25	
aksjespillet.no	2013-08-27	
aquaculturebusiness.com	2006-04-15	DOMENESHOP AS
b2bdagen.no	2013-08-27	
bisbuzz.no	2012-01-25	
businessinfo.no	2017-03-28	
businessnews.no	2012-01-25	
contentshop.no	2012-01-25	
d2.no	2012-01-25	
dagens-naeringsliv.no	2012-01-25	
dagens-naringsliv.no	2012-01-25	
dagensit.no	2013-08-27	
dagensnaeringsliv.no	2012-01-25	
dagensnaringsliv.no	2012-01-25	
dn-dialog.no	2012-01-25	
dn.no	2012-01-25	
dnaktiv.no	2012-01-25	
dnaktivklubb.no	2012-01-25	
dnavis.no	2012-01-25	
dnbo.com	2005-04-14	DOMENESHOP AS
dnbo.no	2012-01-25	
dneiendom.com	2005-11-04	DOMENESHOP AS
dneiendom.no	2012-01-25	
dnenergi.no	2012-01-25	
dngaselle.com	2006-01-26	DOMENESHOP AS
dngaselle.no	2012-01-25	
dngolf.no	2012-01-25	
dngolfen.com	2006-01-26	DOMENESHOP AS
dngolfen.no	2012-01-25	
dnjobb.no	2012-01-25	
dnmarkedspuls.no	2012-01-25	
dnplay.no	2012-01-25	
dnseilcup.com	2006-01-26	DOMENESHOP AS
dnseilcup.no	2012-01-25	
dnservice.no	2012-01-25	
dnspareklubben.com	2006-01-26	DOMENESHOP AS
dnspareklubben.no	2012-01-25	
dntv.no	2012-01-25	
dnvinklubb.no	2012-01-25	

Internal network ip address ranges



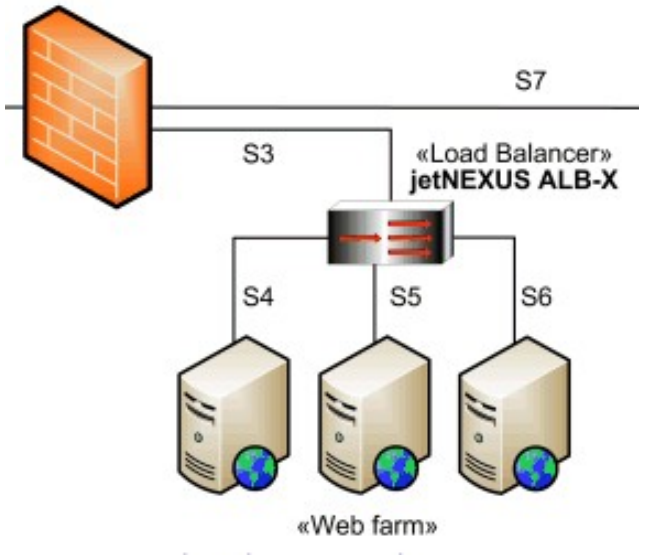
Internal network ips
10.0.0.0/8
192.168.0.0/16
172.16.0.0/12

Access Control List (ACL) example

Priority/ID	Protocol	Source IP	Src Port	Destination IP	Dst Port	Action
R0	tcp	192.168.1.5	any	*.*.*.*	80	deny
R1	tcp	192.168.1.*	any	*.*.*.*	80	allow
R2	tcp	*.*.*.*	any	172.0.1.10	80	allow
R3	tcp	192.168.1.*	any	172.0.1.10	80	deny
R4	tcp	192.168.1.60	any	*.*.*.*	21	deny
R5	tcp	192.168.1.*	any	*.*.*.*	21	allow
R6	tcp	192.168.1.*	any	172.0.1.10	21	allow
R7	tcp	*.*.*.*	any	*.*.*.*	any	deny
R8	udp	192.168.1.*	any	172.0.1.10	53	allow
R9	udp	*.*.*.*	any	172.0.1.10	53	allow
R10	udp	192.168.2.*	any	172.0.2.*	any	allow
R11	udp	*.*.*.*	any	*.*.*.*	any	deny

Domain to ip options

- One domain to one ip
  - A webserver with one website
- Multiple domain to one ip
  - A web server hosts multiple websites
- One domain to multiple ip
  - Load balancer, cloud service



Robtex

- *Robtex* is used for various kinds of research of IP numbers, Domain names, etc.

Example: dn.no

It belongs to NHST Media Group AS

The network range is:

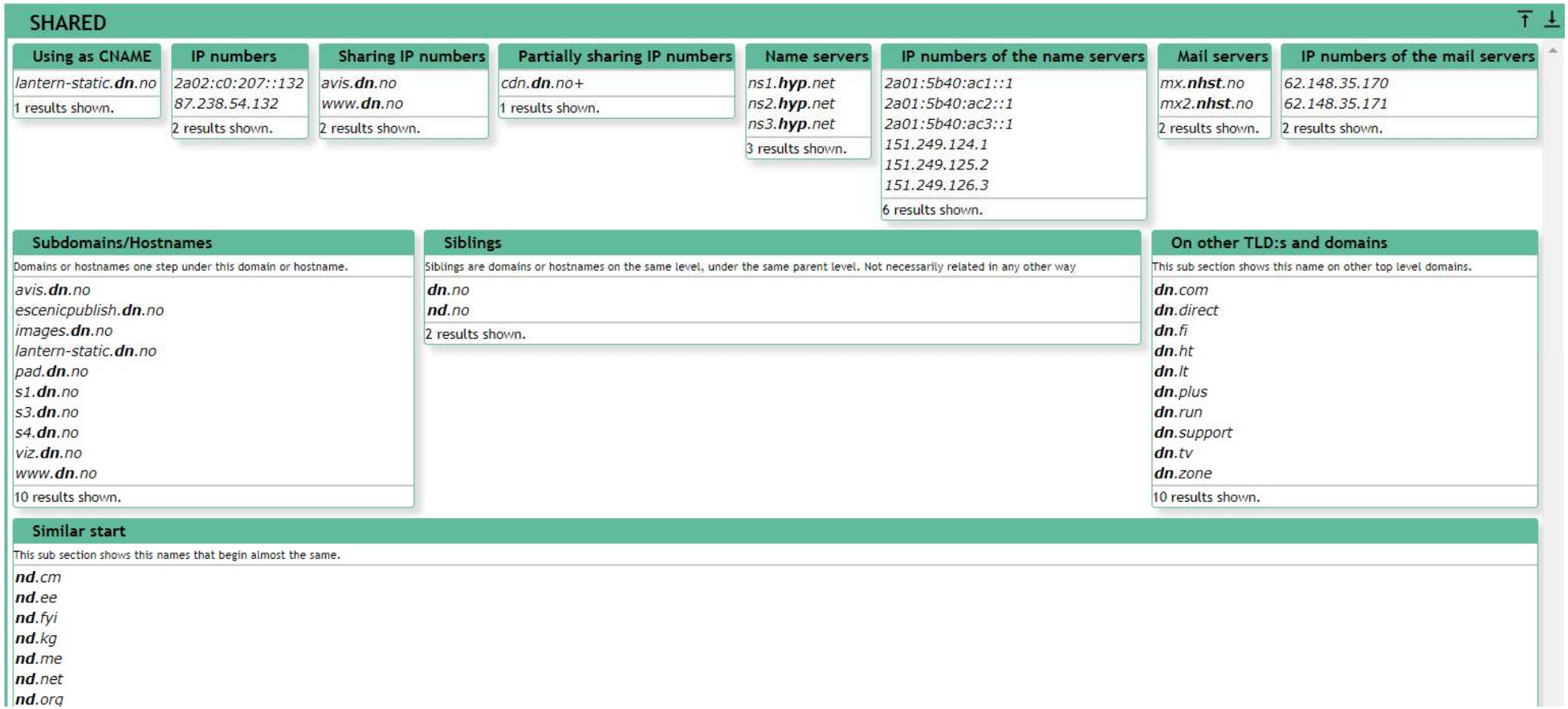
87.238.32.0/19

87.238.32.0-87.238.63.255

Who is Redpill Linpro?

Robtex

- DNS data is indicated
- Subdomains, similar domains, domains with other TLD



SHARED

Using as CNAME	IP numbers	Sharing IP numbers	Partially sharing IP numbers	Name servers	IP numbers of the name servers	Mail servers	IP numbers of the mail servers
*lantern-static.**dn**.no*	*2a02:c0:207::132*	*avis.**dn**.no*	*cdn.**dn**.no+*	*ns1.**hyp**.net*	*2a01:5b40:ac1::1*	*mx.**nhst**.no*	*62.148.35.170*
1 results shown.	*87.238.54.132*	*www.**dn**.no*	1 results shown.	*ns2.**hyp**.net*	*2a01:5b40:ac2::1*	*mx2.**nhst**.no*	*62.148.35.171*
	2 results shown.	2 results shown.		*ns3.**hyp**.net*	*2a01:5b40:ac3::1*	2 results shown.	2 results shown.
				3 results shown.	*151.249.124.1*		
					151.249.125.2		
					151.249.126.3		
					6 results shown.		

Subdomains/Hostnames

Domains or hostnames one step under this domain or hostname.

*avis.**dn**.no*
*escenicpublish.**dn**.no*
*images.**dn**.no*
*lantern-static.**dn**.no*
*pad.**dn**.no*
*s1.**dn**.no*
*s3.**dn**.no*
*s4.**dn**.no*
*viz.**dn**.no*
*www.**dn**.no*
10 results shown.

Siblings

Siblings are domains or hostnames on the same level, under the same parent level. Not necessarily related in any other way

***dn**.no*
***nd**.no*
2 results shown.

On other TLD:s and domains

This sub section shows this name on other top level domains.

***dn**.com*
***dn**.direct*
***dn**.fi*
***dn**.ht*
***dn**.lt*
***dn**.plus*
***dn**.run*
***dn**.support*
***dn**.tv*
***dn**.zone*
10 results shown.

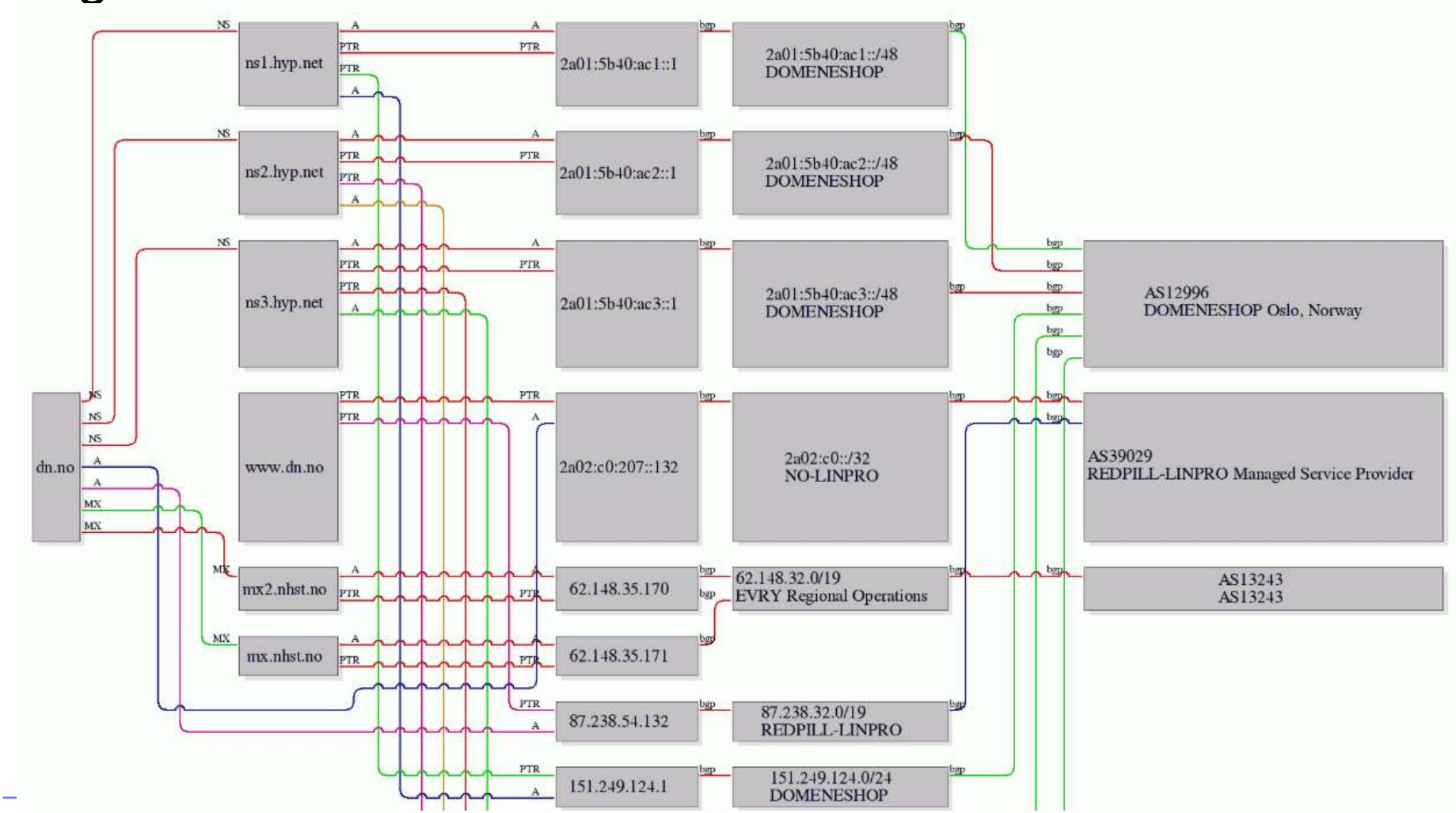
Similar start

This sub section shows this names that begin almost the same.

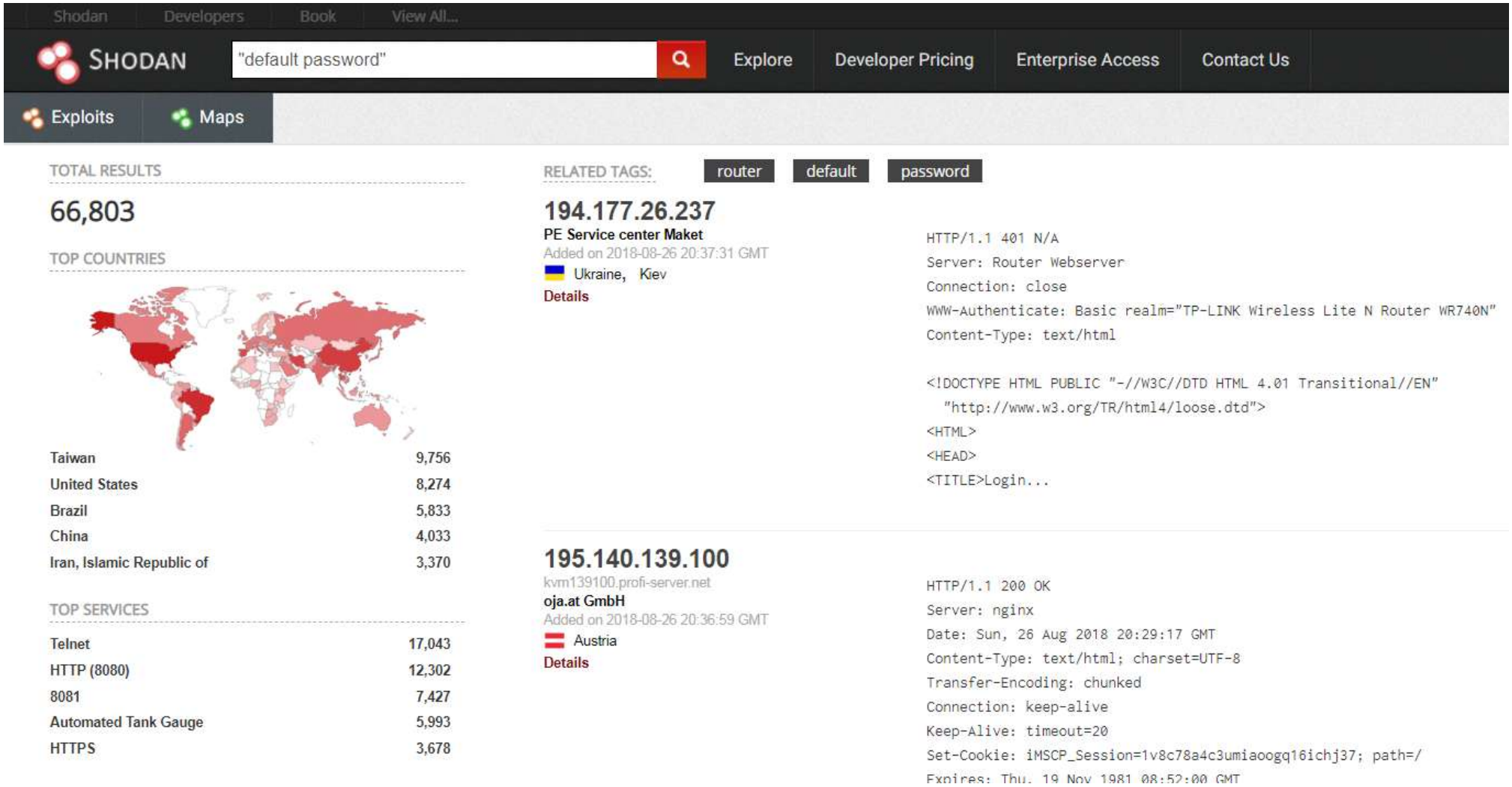
***nd**.cm*
***nd**.ee*
***nd**.fyi*
***nd**.kg*
***nd**.me*
***nd**.net*
***nd**.org*

Robtex – graph view

It also presents a graph view of the target related ips and ranges



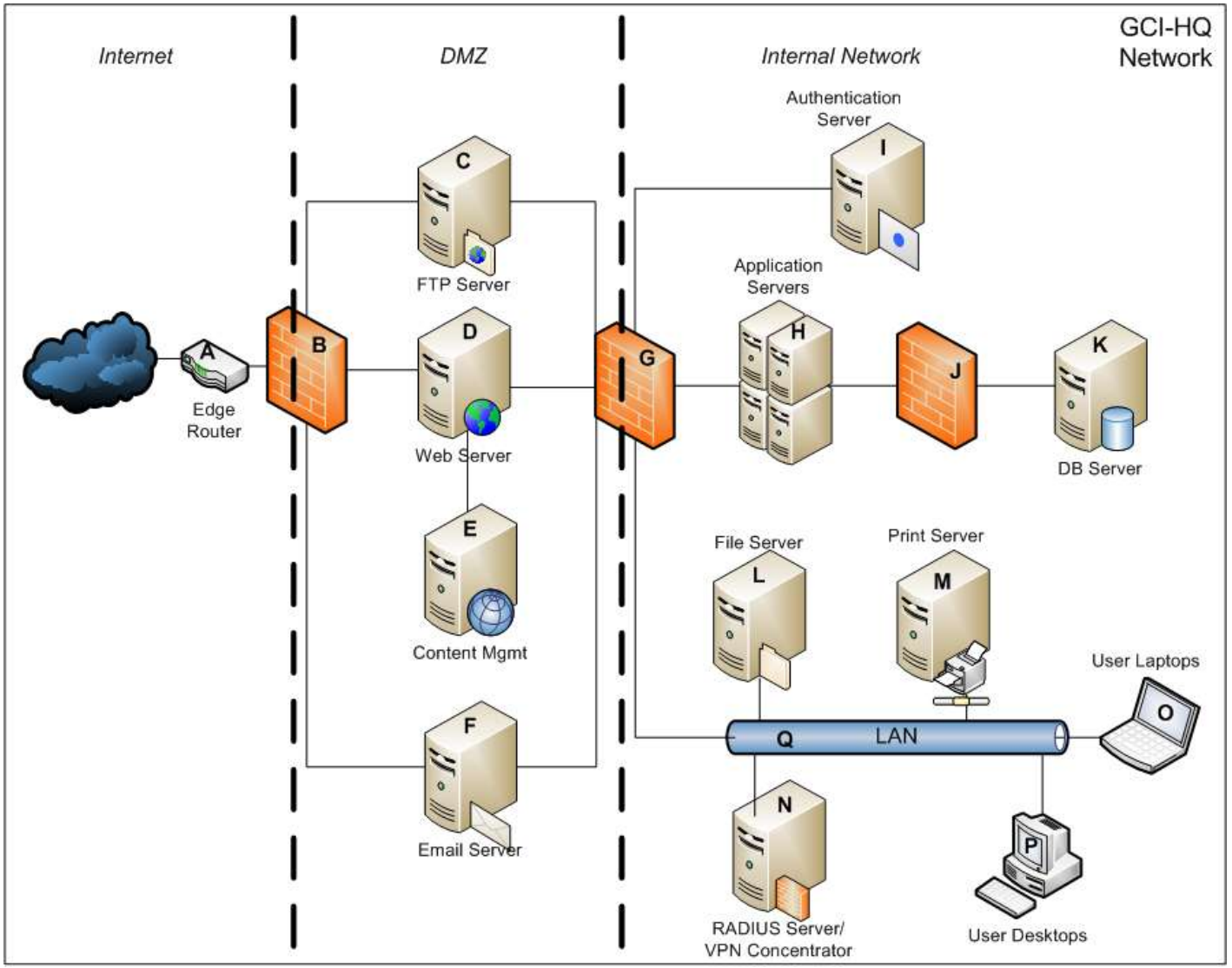
Shodan –IOT device finder



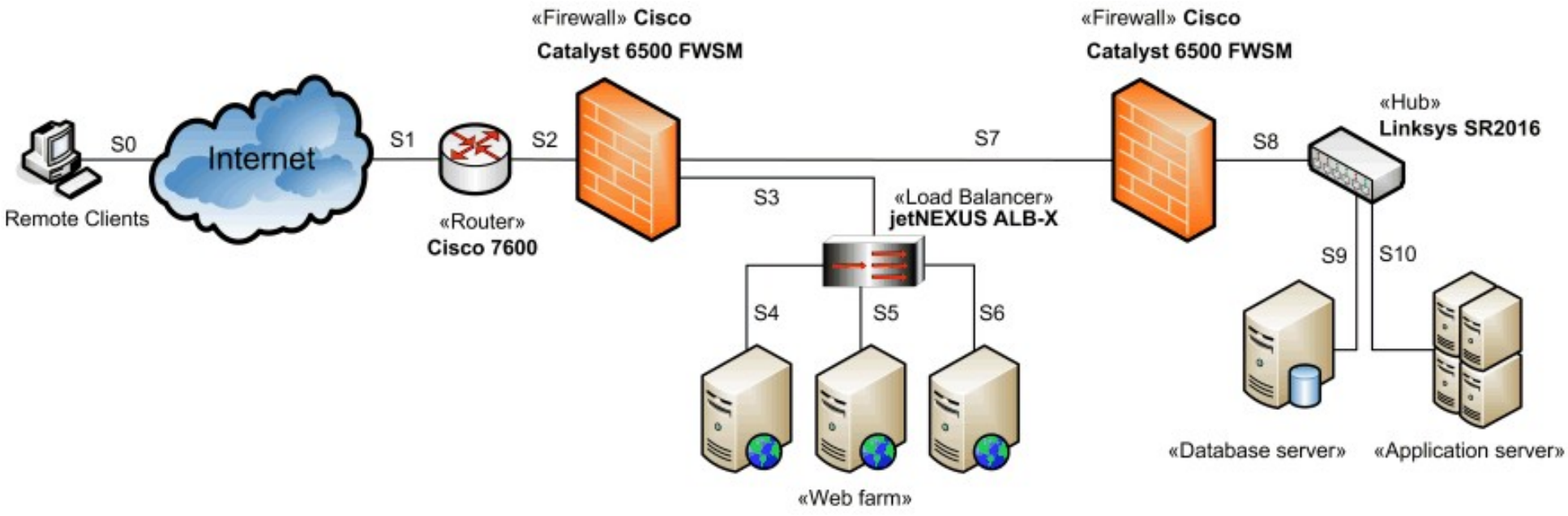
Types of computers in the network

- Server
- Network device (router, switch)
- Firewall (stateless, statefull), Ids, Ips
- Printers
- User desktops
- User laptops
- Mobil devices
- IOTs

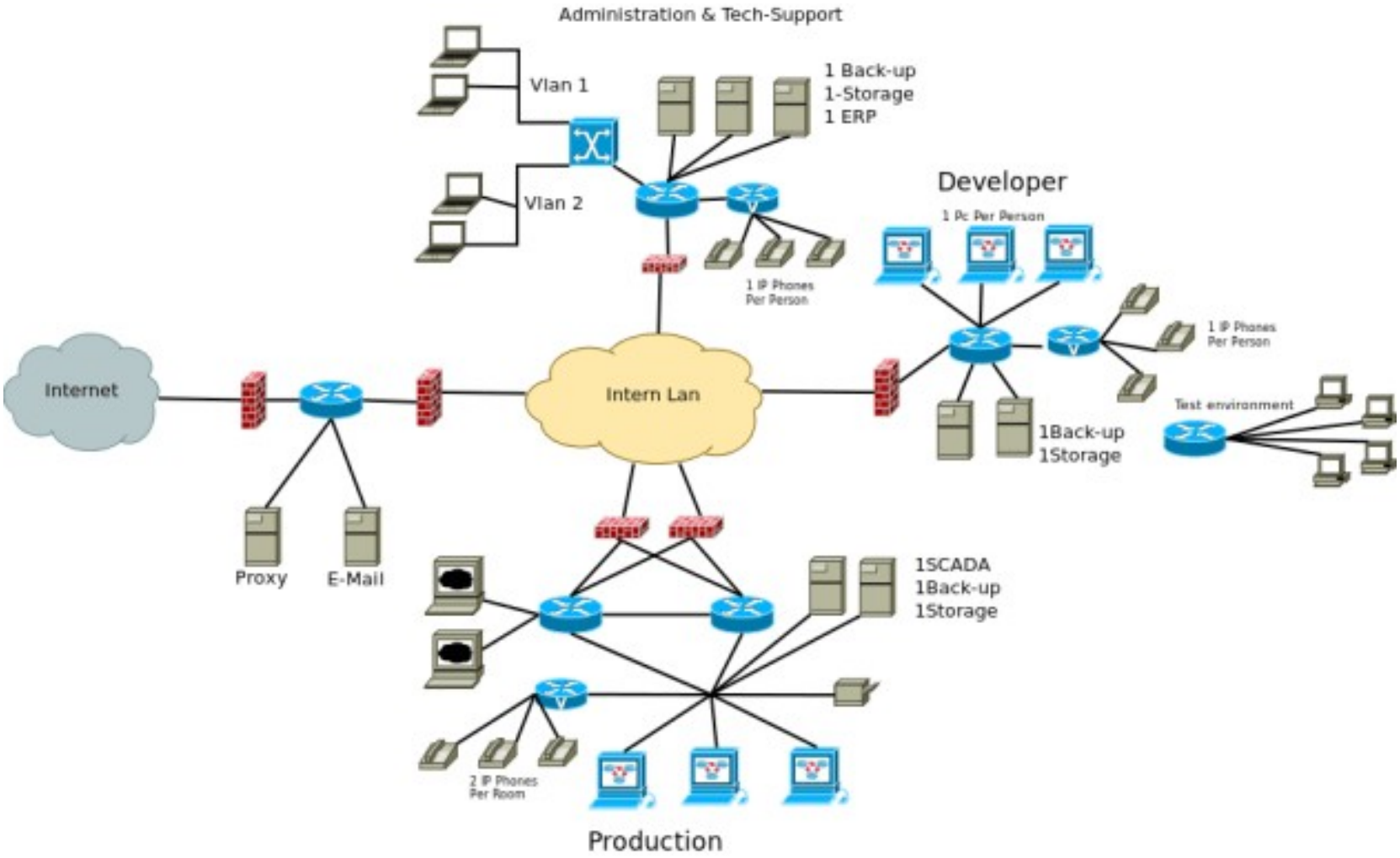
Network layout example 1.



Network layout example 2.



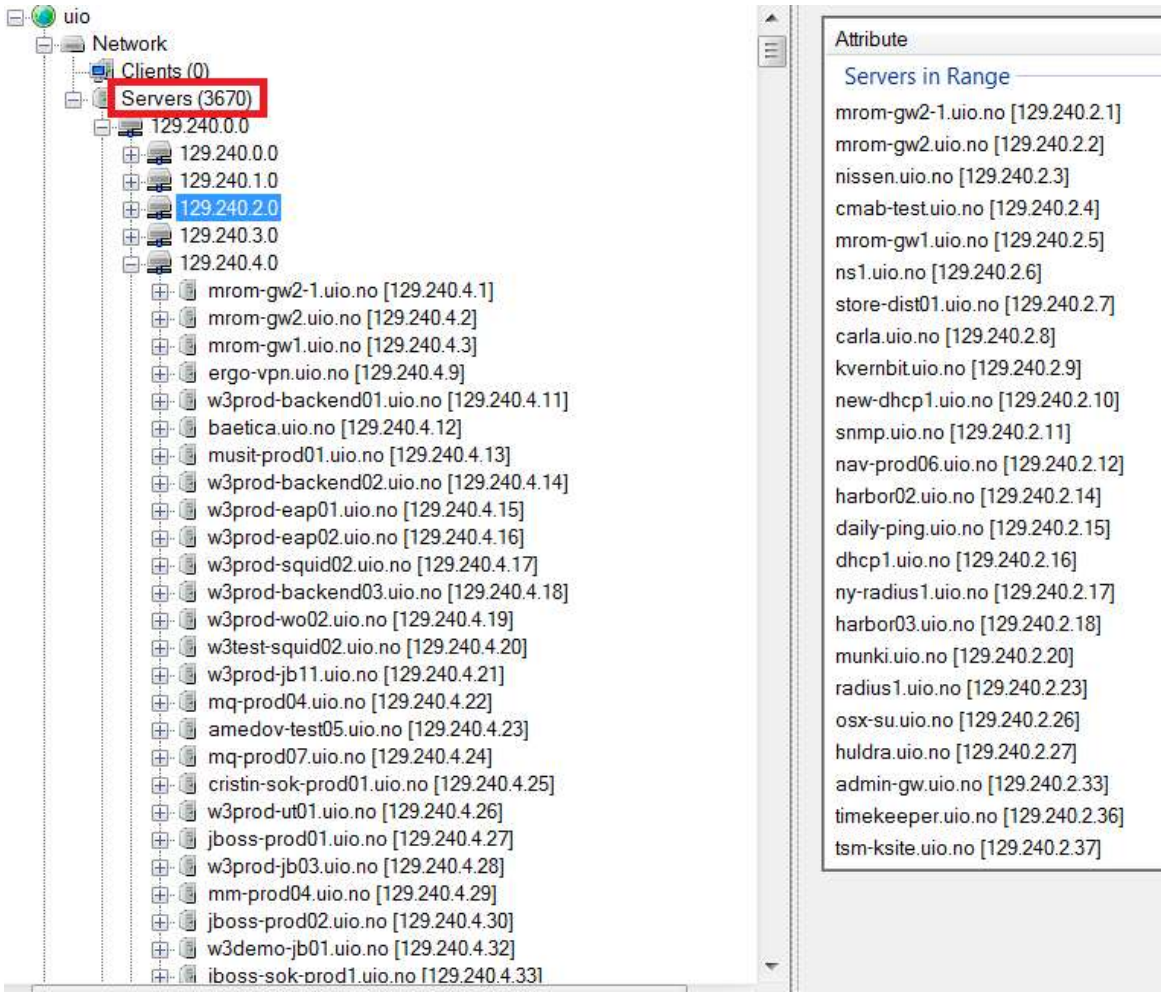
Network layout example 3.



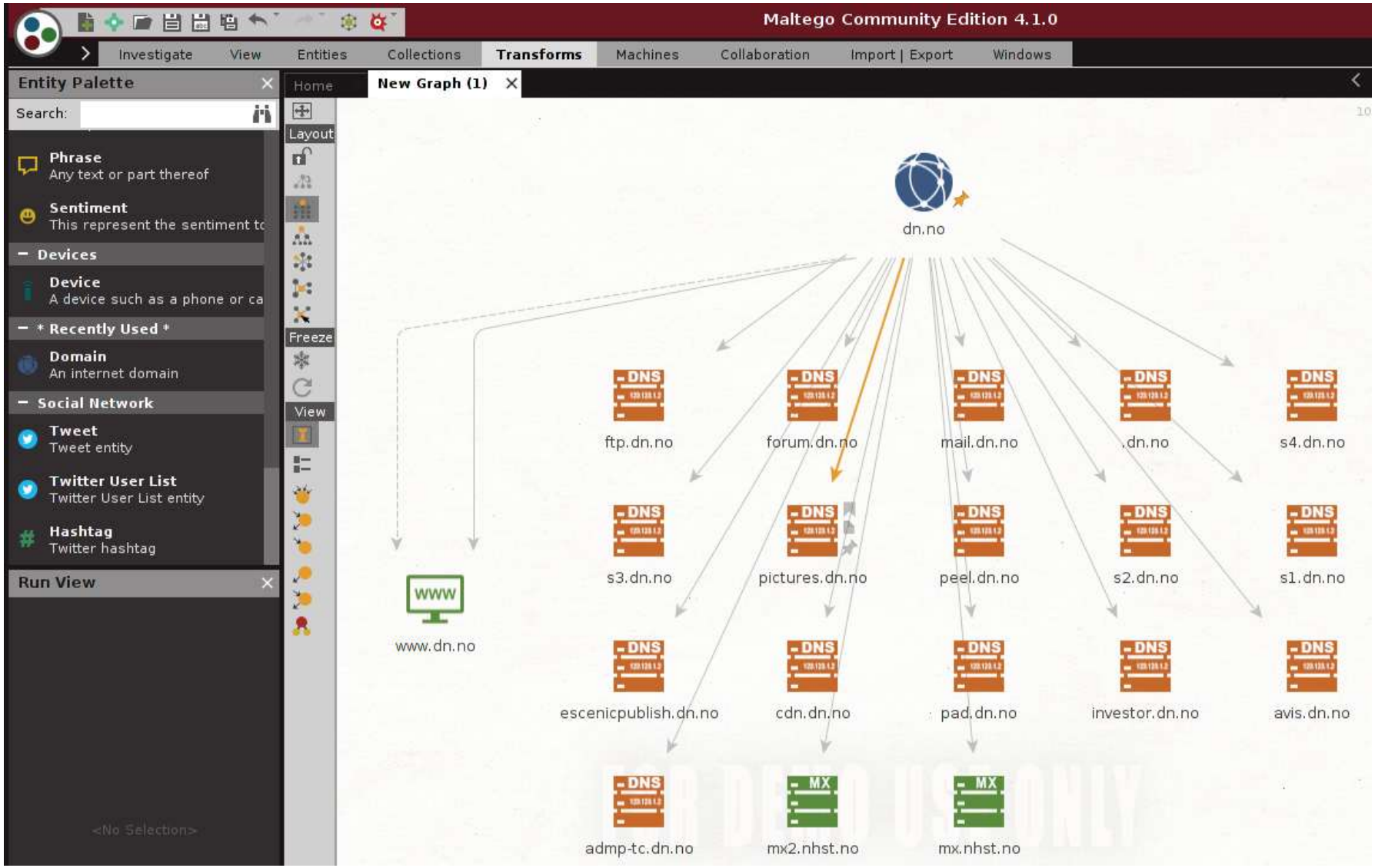
FOCA

Automatically identifies subdomains, servers, ips

- Websearch (google, bing)
- Fingerprinting
- DNS data
- IP Bing
- PTR search
- Shodan & Robtex
- Brute-forcing



Maltego – Information gathering tool



End of lecture