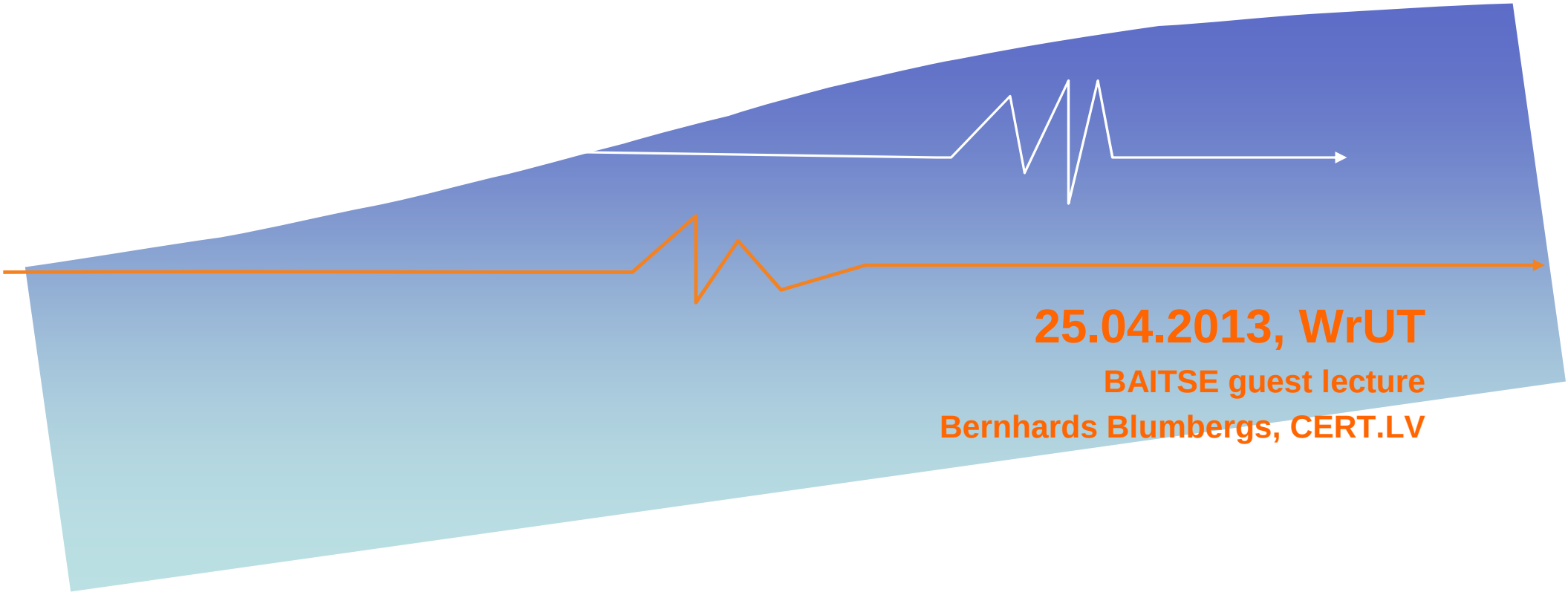
CERT.LV

Basics of executing a penetration test



25.04.2013, WrUT

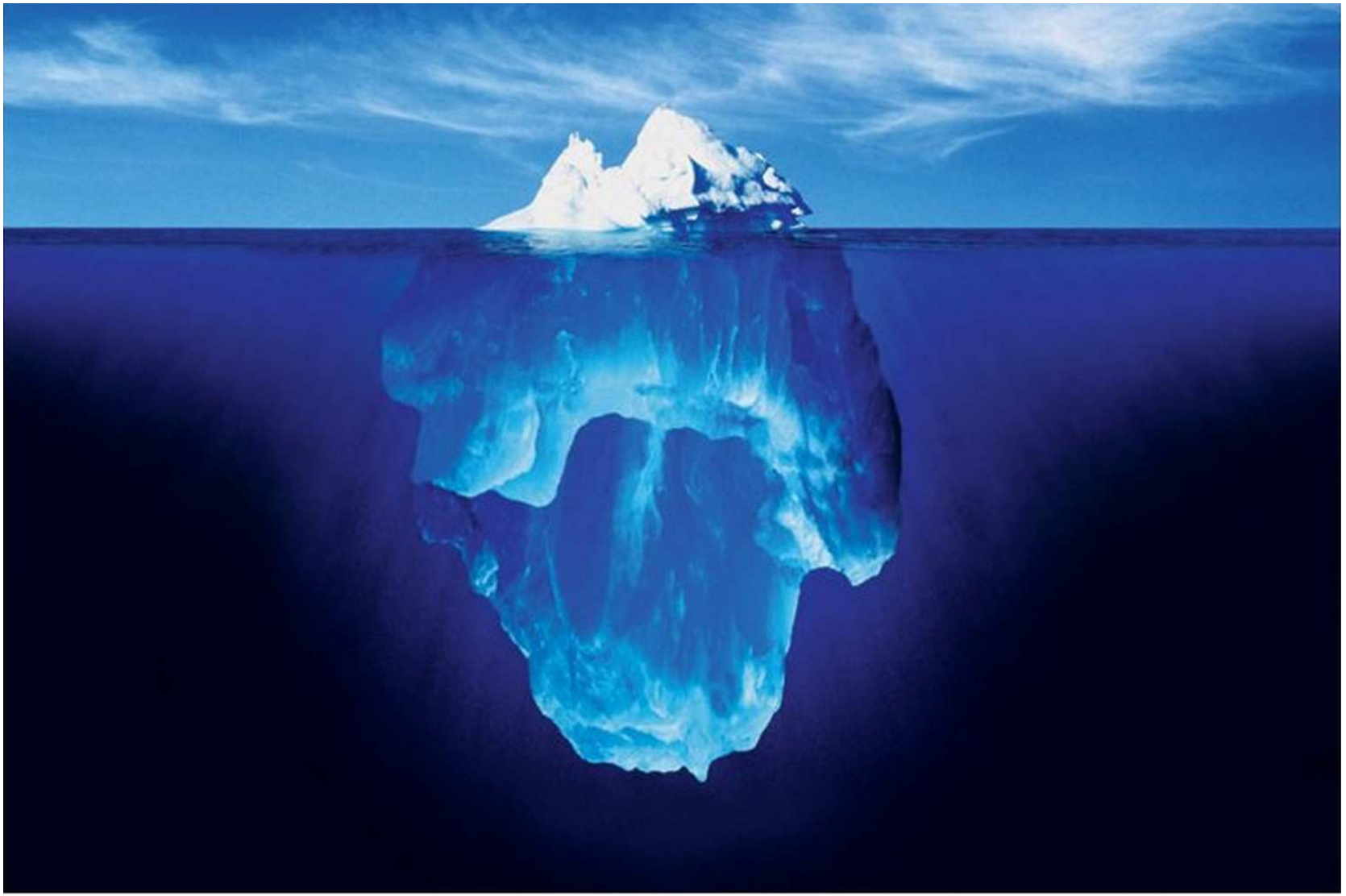
BAITSE guest lecture

Bernhards Blumbergs, CERT.LV

Outline

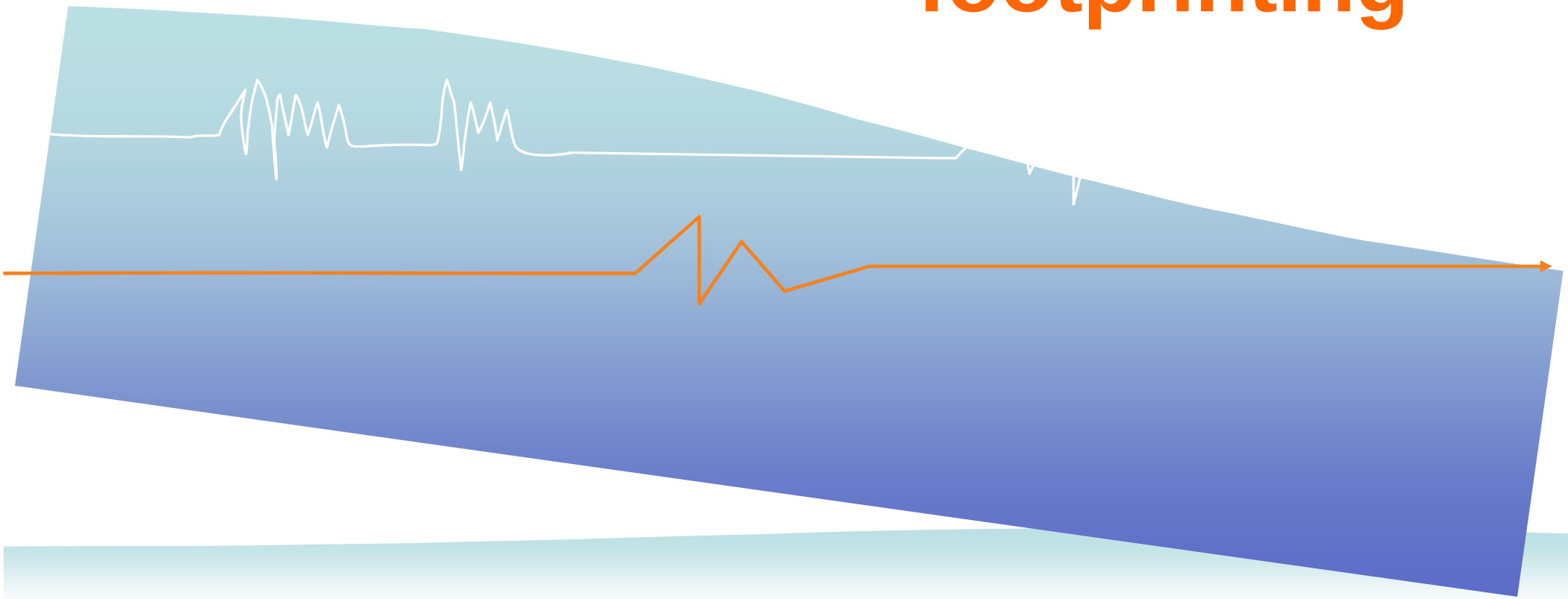
- Reconnaissance and footprinting
- Scanning and enumeration
- System exploitation

Outline



CERT.LV

Reconnaisance and footprinting



What is footprinting?

- Collect and uncover information
- Know your target
- Plan and prepare your attack

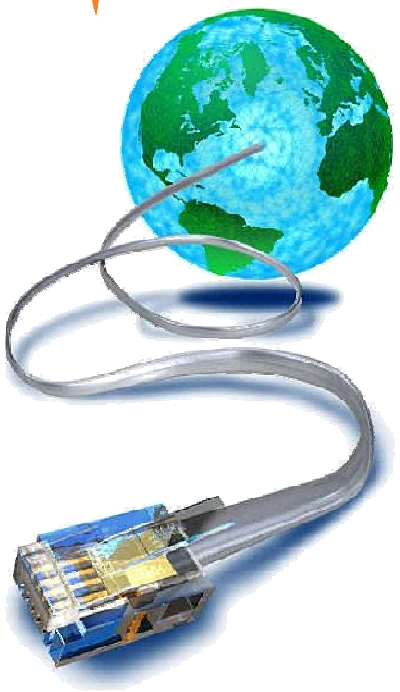
Footprinting types

- Internet footprinting
- Organizational footprinting
- Whois footprinting
- DNS footprinting
- Network footprinting
- Website footprinting
- E-mail footprinting
- Google hacking
- Vulnerability identification

Open Source Intelligence

- Reconnaissance information derived from publicly available sources

Reconnaissance types



- Passive
  - No interaction with the target
- Active
  - Interaction with target directly or indirectly

Passive - Internet search

- Company URLs

cern

Web Images News More Search tools

About 25,700,000 results (0.39 seconds)

CERN - the European Organization for Nuclear Research
www.**cern**.ch/ - Cached
Feb 22, 2013 – European Laboratory for Particle Physics. Includes an introduction of the laboratory, information on experiments being conducted, publication ...
Score: **26** / 30 - 42 Google reviews

Route de Meyrin 385 1217 Meyrin, Switzerland
+41 22 767 84 84

Users' pages - Careers at CERN

CERN - The Large Hadron Collider
public.web.**cern**.ch/public/en/lhc/lhc-en.html - Cached
The Large Hadron Collider (LHC) is a gigantic scientific instrument near ...

CERN

Directions

Passive - Internet search

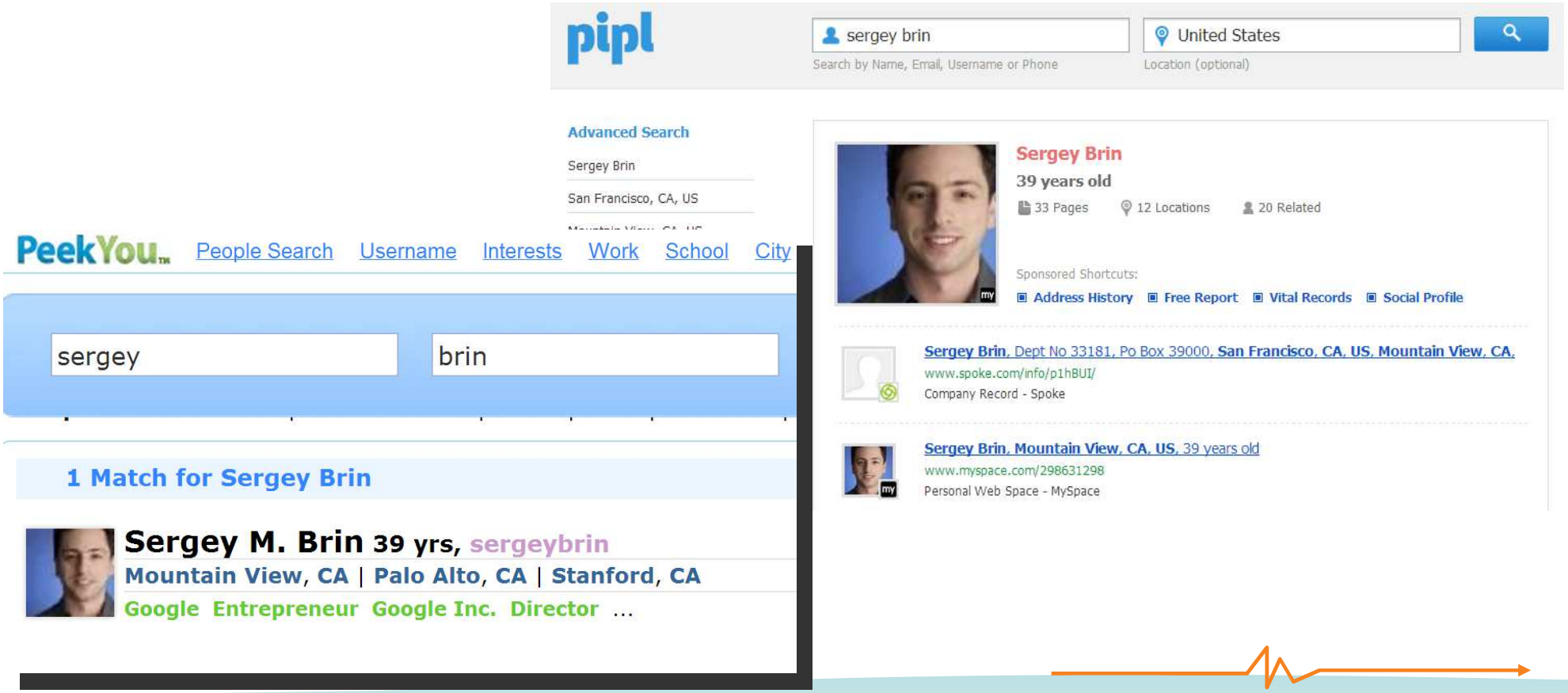
- Public and restricted websites

Passive - Internet search

- Company information:
  - Company registry databases
  - Financial information
  - Personnel
  - Press releases
  - Vacancies, jobs sites
  - Procurements

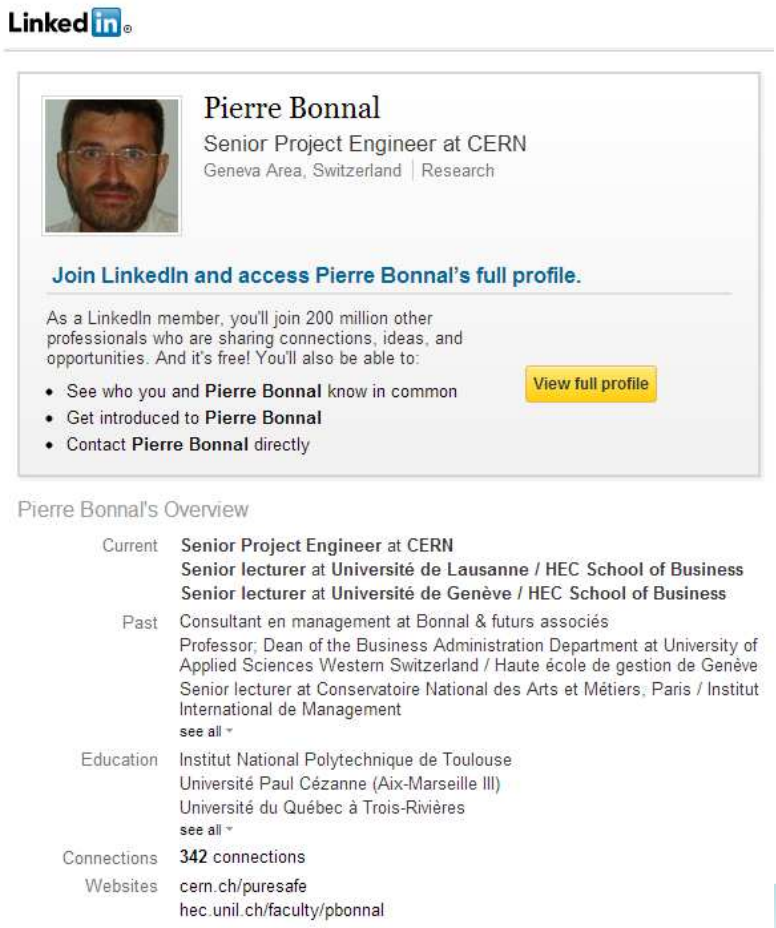
Passive - Internet search

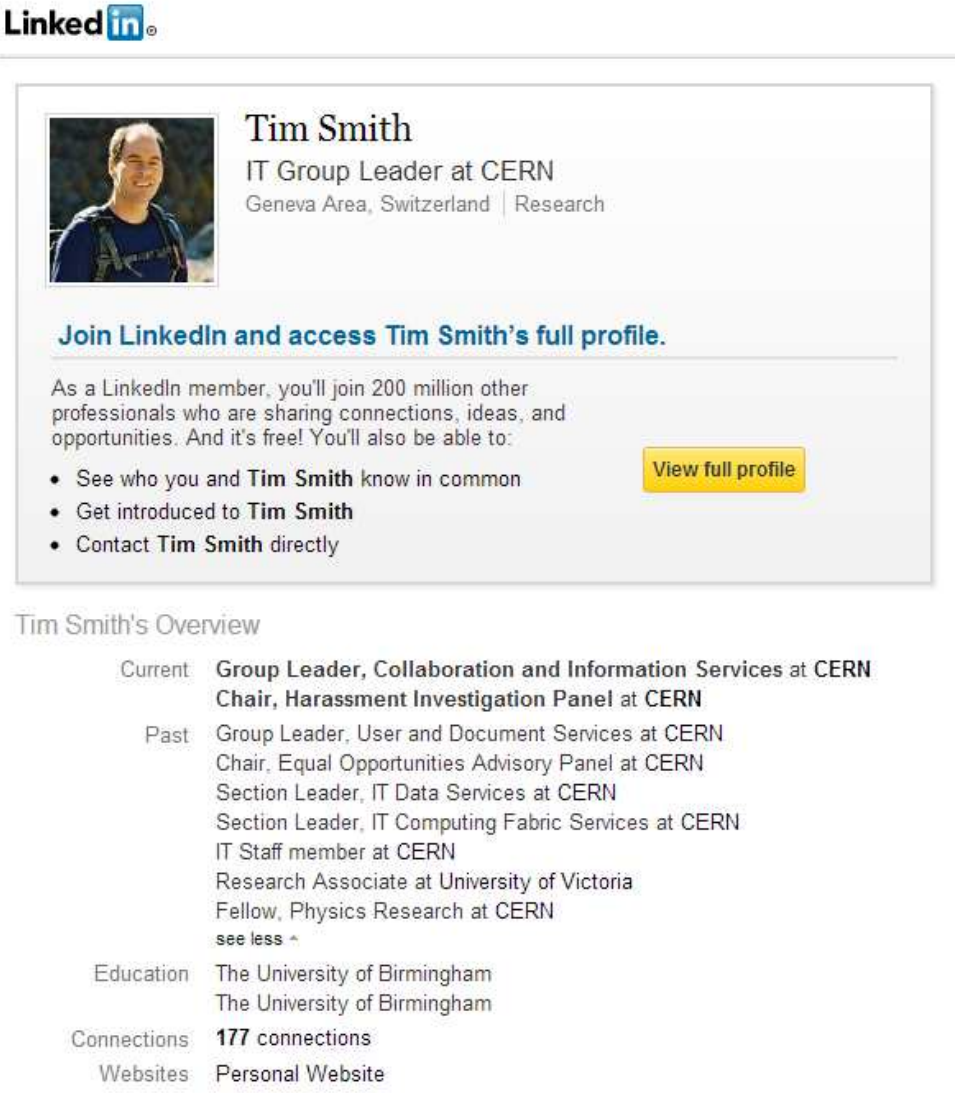
- People search:
- Pipl.com, Peekyou.com



Passive - Internet search

- Social networks:
- Linkedin.com





Passive - Internet search

- Social networks:
- Facebook, Twitter

Tweets

Rita Stiene @zakitis69 now

Big shift tonight! Migrating corporate test environment from VirtualBox to Hyper-V on Win2k8r2 production environment. Four beers packed! :)

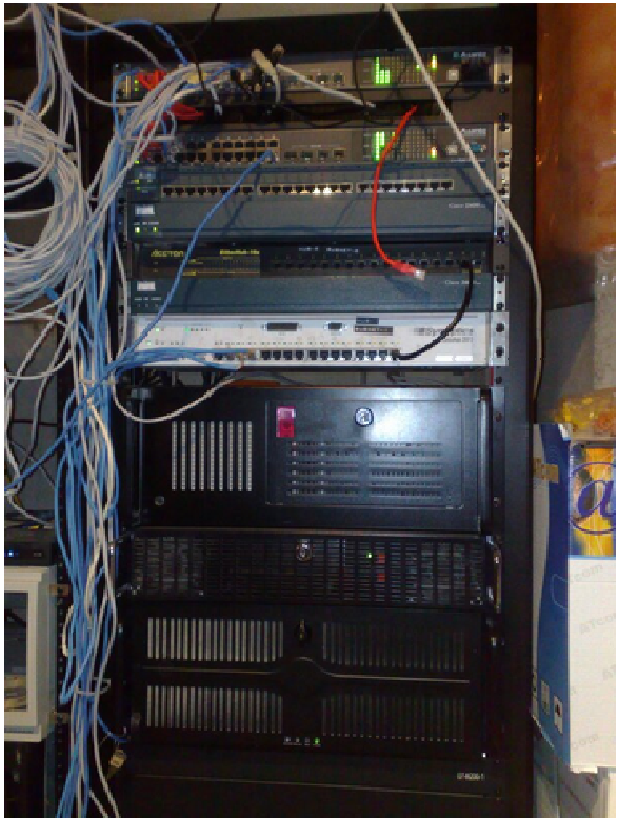
Expand

Tweets

Rita Stiene @zakitis69 8 secs

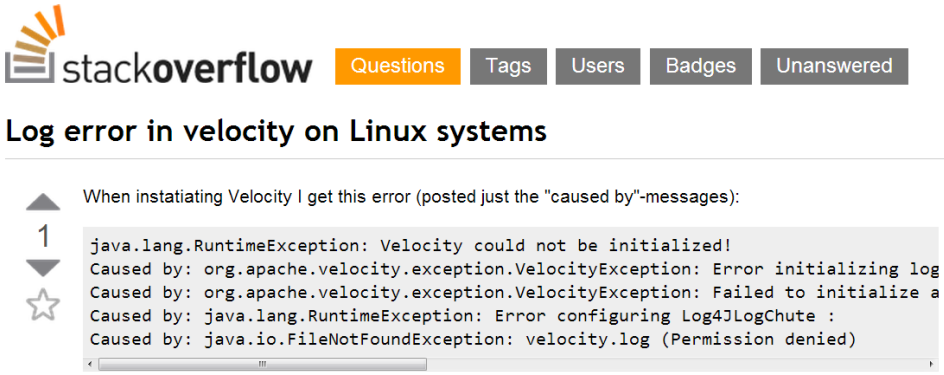
How in the hell will I sort this mess out? Two sleepless weeks here I come! pic.twitter.com/6fIXGf7WLI

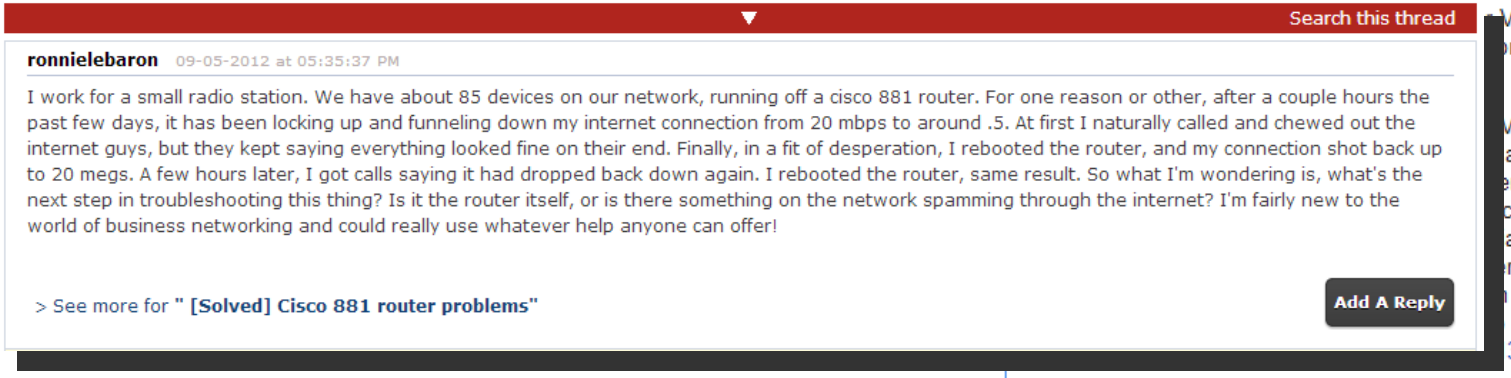
Hide photo Reply Delete Favorite More

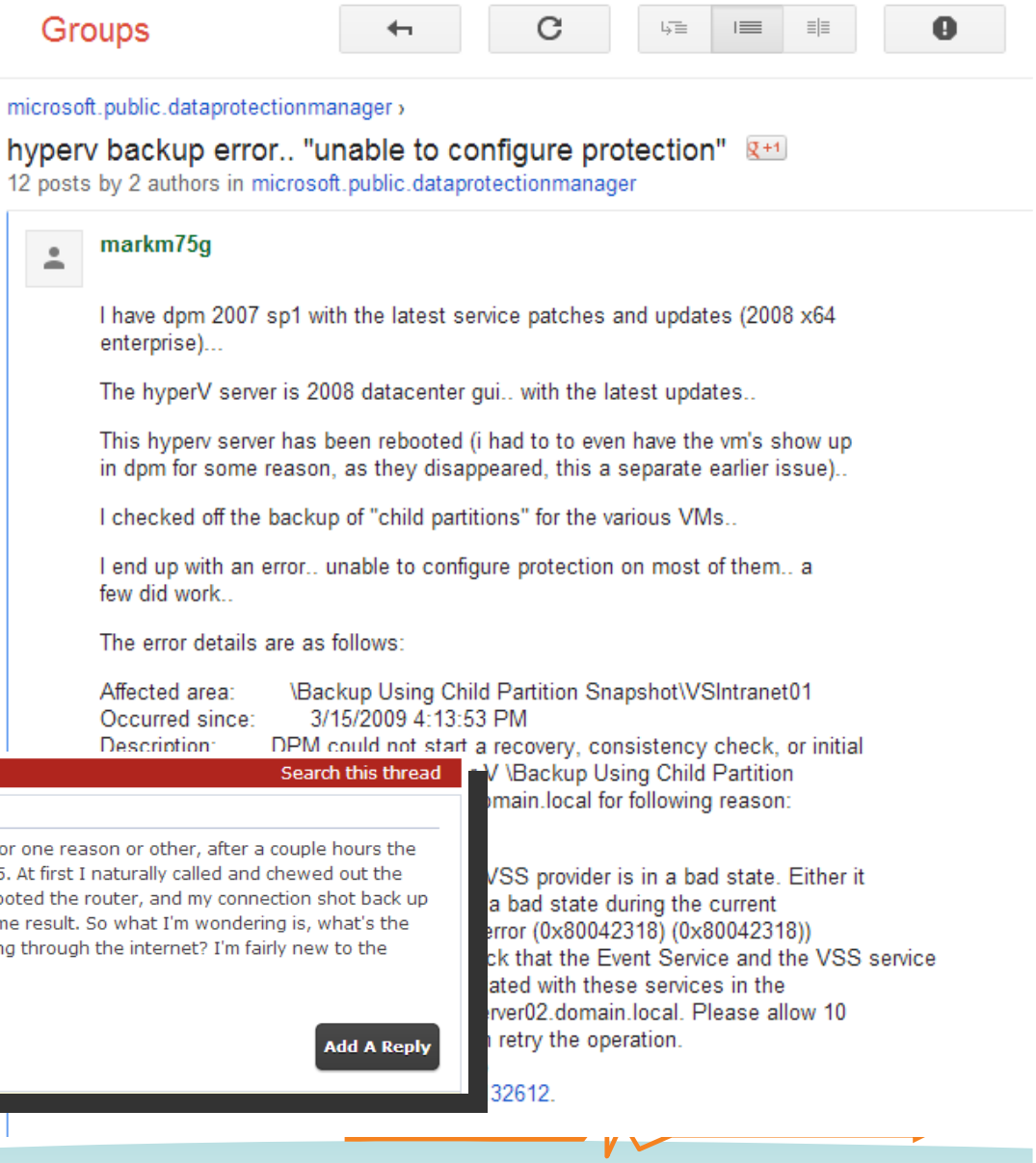


Passive - Internet search

- Social networks:
- Forums and groups

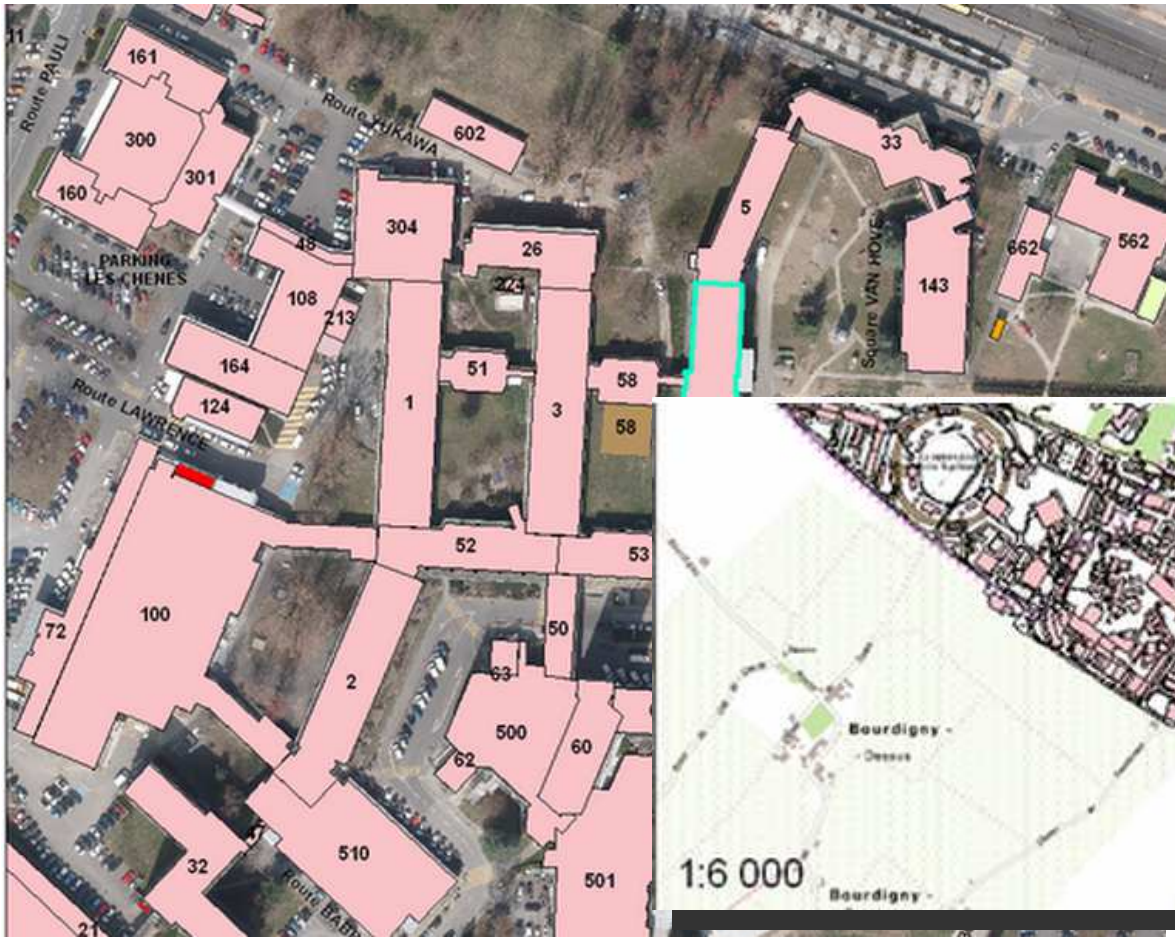


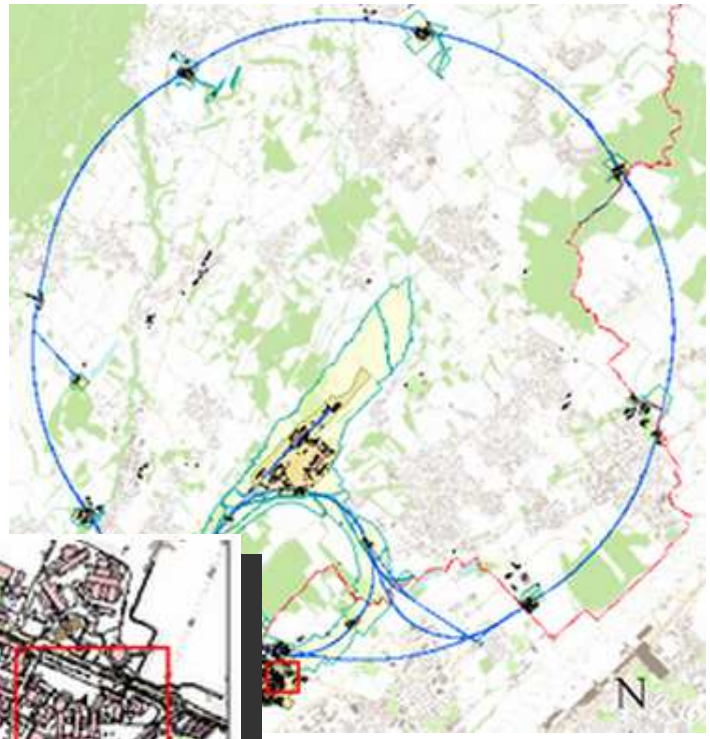




Passive - Internet search

- Location information





Other GIS Portal

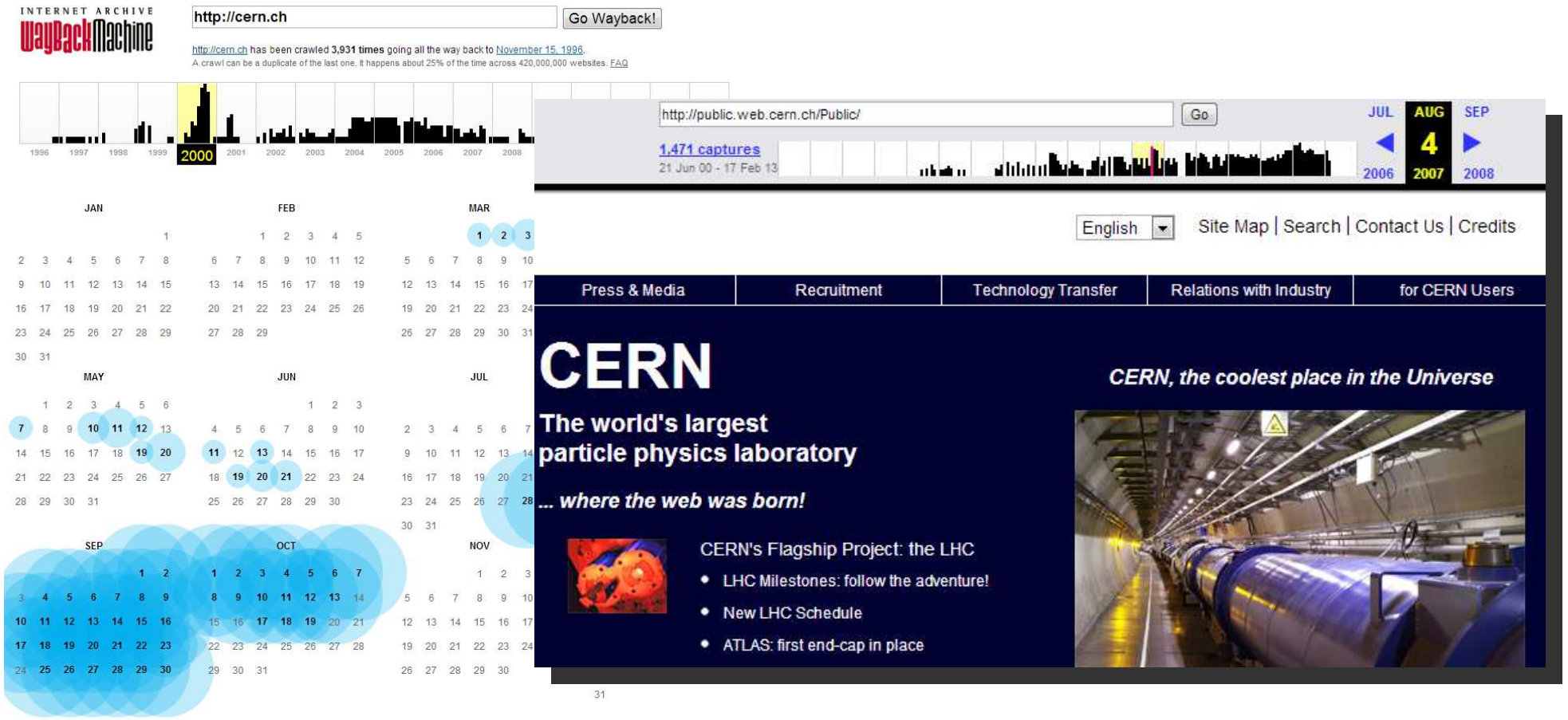
CERN

Passive - Internet search

- Google cache

Passive - Internet search

- Internet Archive – wayback machine



Passive - Internet search

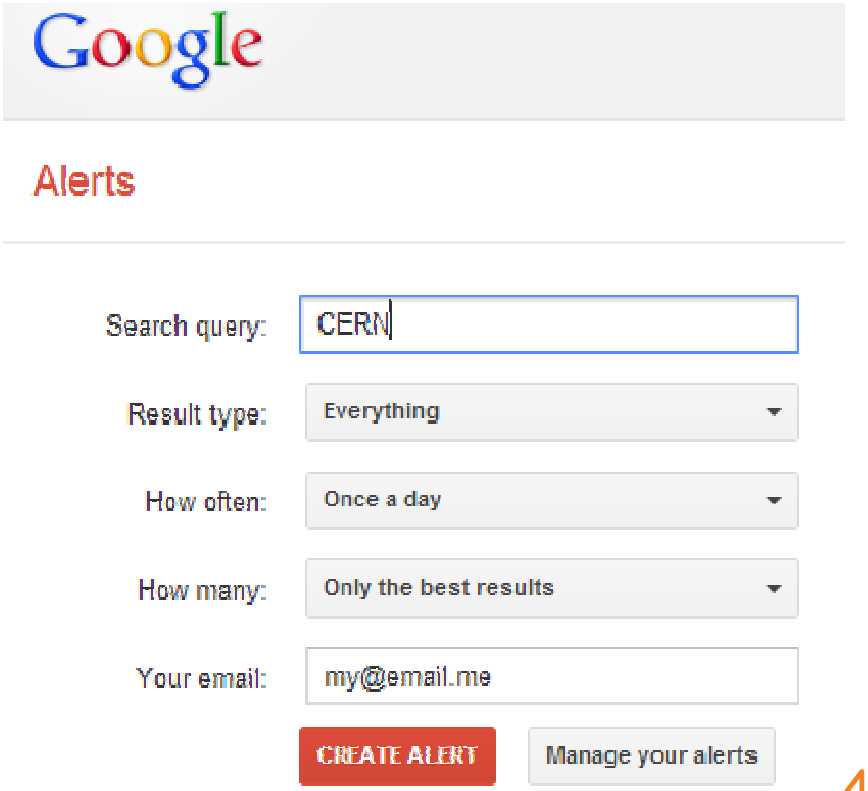
- Google alerts

Monitor the Web for interesting new content

Google Alerts are email updates of the latest relevant Google results (web, news, etc.) based on your queries.

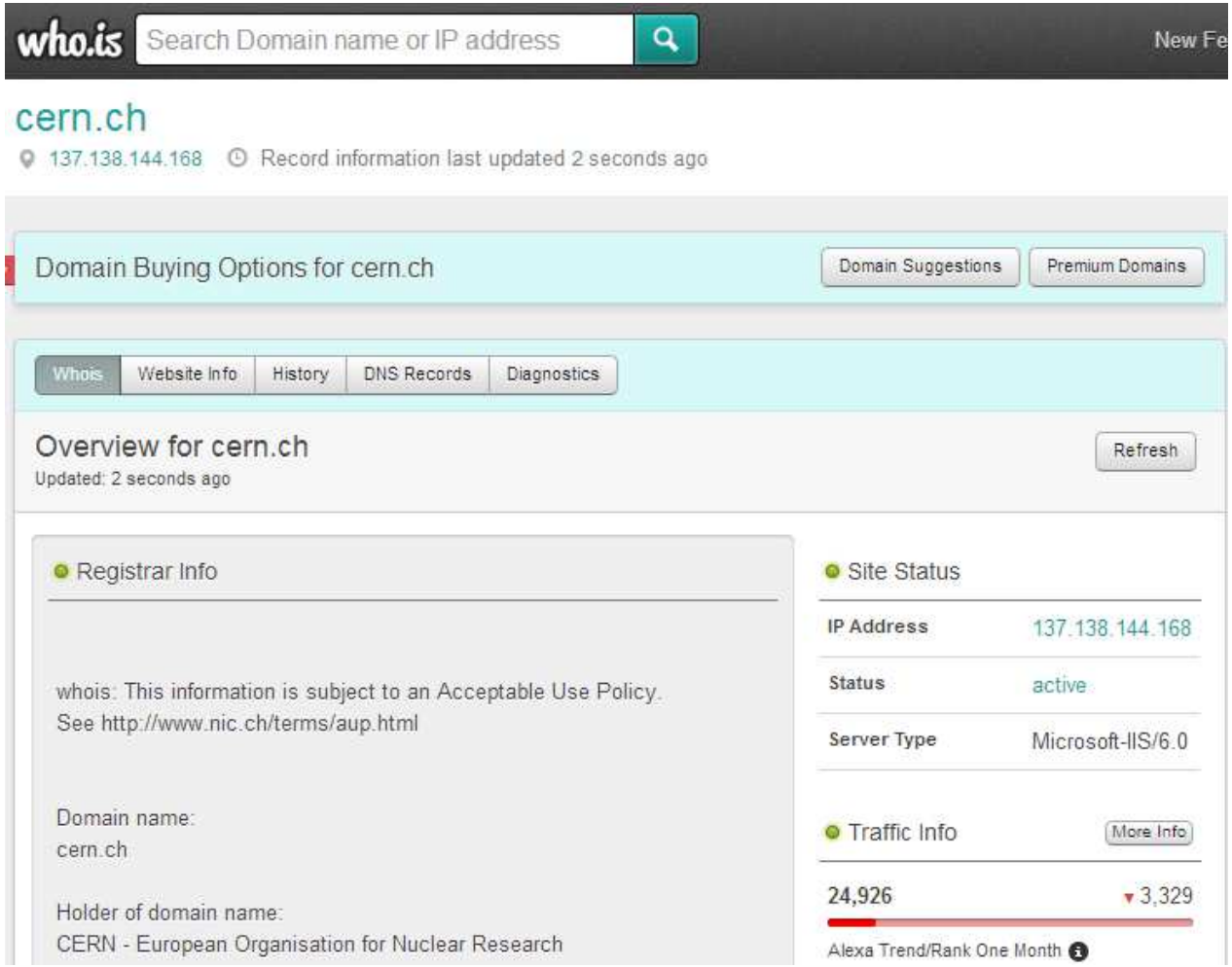
Enter a search query you wish to monitor. You will see a preview of the type of results you'll receive.
Some handy uses of Google Alerts include:

- monitoring a developing news story
- keeping current on a competitor or industry
- getting the latest on a celebrity or event
- keeping tabs on your favorite sports teams



Passive - Whois, domain footprinting

- Whois data



Passive – Whois, domain footprinting

- Regional Internet registries (RIRs)

Search results

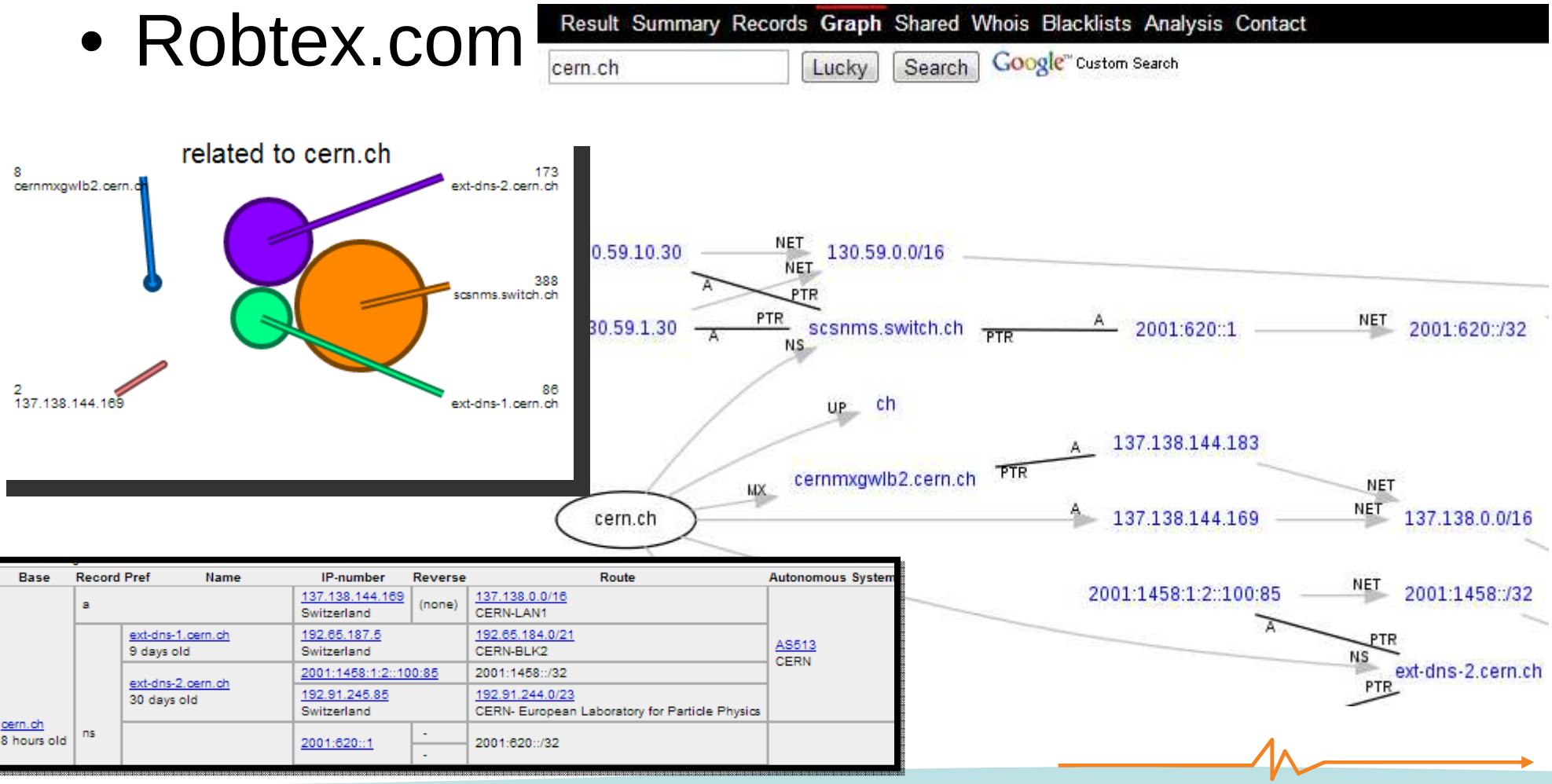
This is the RIPE Database search service.
The objects are in RPSL format.
The RIPE Database is subject to Terms and Conditions.
See http://www.ripe.net/db/support/db-terms-conditions.pdf

```
inetnum:        137.138.0.0 - 137.138.255.255
netname:        CERN-GPN
descr:          CERN- European Organization for Nuclear Research
descr:          CERN Campus Network
descr:          CH-1211 Geneva 23, Switzerland
country:        CH
org:            ORG-CEOf1-RIPE
admin-c:        JIMI1-RIPE
tech-c:         CNOC5-RIPE
status:         EARLY-REGISTRATION
mnt-by:         RIPE-NCC-HM-MNT
mnt-by:         CERN-MNT
mnt-routes:     CERN-MNT
mnt-domains:    CERN-MNT
mnt-irt:        IRT-CERN-CERT
source:         RIPE #Filtered

organisation:   ORG-CEOf1-RIPE
org-name:       CERN - European Organization for Nuclear Research
org-type:       LIR
address:        CERN IT department - CS group CERN CH-1211 Geneva 23
SWITZERLAND
phone:          +41 22 76 74417
fax-no:         +41 22 76 77155
admin-c:        DGR6-RIPE
admin-c:        EM9228
admin-c:        JIMI1-RIPE
mnt-ref:        CERN-MNT
mnt-ref:        RIPE-NCC-HM-MNT
mnt-by:         RIPE-NCC-HM-MNT
source:         RIPE #Filtered
```

Passive – Whois, domain footprinting

- Domain information
- Robtex.com



Base	Record Pref	Name	IP-number	Reverse	Route	Autonomous System
cern.ch 8 hours old	a		137.138.144.169 Switzerland	(none)	137.138.0.0/16 CERN-LAN1	AS513 CERN
	ns	ext-dns-1.cern.ch 9 days old	192.65.187.5 Switzerland		192.65.184.0/21 CERN-BLK2	
		ext-dns-2.cern.ch 30 days old	2001:1458:1:2::100:85		2001:1458::/32	
			192.91.245.85 Switzerland		192.91.244.0/23 CERN- European Laboratory for Particle Physics	
			2001:620::1	- -	2001:620::/32	

Passive – Whois, domain footprinting

- Domain information
- Netcraft.com

Background

Site title	ROOT | A Data Analysis Framework	**Date first seen**	May 1996
Site rank	113128	**Primary language**	English
Description	*Not Present*		
Keywords	*Not Present*		

Network

Site	http://root.cern.ch	**Last Reboot**	*unknown*
Domain	cern.ch	**Netblock Owner**	CERN LCG network
IP address	128.142.172.96	**Nameserver**	ext-dns-1.cern.ch
IPv6 address	*Not Present*	**DNS admin**	external-dns@cern.ch
Domain registrar	nic.ch	**Reverse DNS**	lxroot02.cern.ch
Organisation	CERN - European Organisation for Nuclear Research, route de Meyrin, Genève 23, CH-1211, Switzerland	**Nameserver organisation**	whois.nic.ch
Top Level Domain	Switzerland (.ch)	**Hosting company**	CERN - European Organisation for Nuclear Research
Hosting country	CH	**DNS Security Extensions**	*unknown*

Results for cern.ch

Found 44 sites

	Site	Site Report	First seen	Netblock	OS
1.	public.web.cern.ch		november 2001	cern- european organization for nuclear research	windows server 2008
2.	cern.ch		november 1999	cern- european organization for nuclear research	windows server 2003
3.	root.cern.ch		may 1996	cern lcg network	linux - ubuntu
4.	op-webtools.web.cern.ch		january 2010	cern- european organization for nuclear research	windows server 2008
5.	user.web.cern.ch		may 2001	cern- european organization for nuclear research	windows server 2008

Passive - Whois, domain footprinting

- Domain information
- host, whois, nslookup, dig

```
lockout@ubu1004-64:~$ host cern.ch
cern.ch has address 137.138.144.169
cern.ch mail is handled by 10 cernmxgwlb2.cern.ch.
```

```
oute:           137.138.0.0/16
escr:           CERN-LAN1
rigin:          AS513
rg:             ORG-CEOf1-RIPE
nt-by:          AS513-MNT
nt-lower:       CERN-MNT
nt-routes:      CERN-MNT
ource:          RIPE # Filtered

rganisation:    ORG-CEOf1-RIPE
rg-name:        CERN - European Organization for Nuclear
rg-type:        LIR
ddress:         CERN
                IT department - CS group
                CERN
                CH-1211 Geneva 23
                SWITZERLAND
hone:           +41 22 76 74417
ax-no:          +41 22 76 77155
dmin-c:         DGR6-RIPE
dmin-c:         EM9228
dmin-c:         JIMI1-RIPE
nt-ref:         CERN-MNT
nt-ref:         RIPE-NCC-HM-MNT
nt-by:          RIPE-NCC-HM-MNT
ource:          RIPE # Filtered
```

```
lockout@ubu1004-64:~$ nslookup cern.ch
Server:         91.198.156.8
Address:        91.198.156.8#53

Non-authoritative answer:
Name:   cern.ch
Address: 137.138.144.169
```

```
lockout@ubu1004-64:~$ dig cern.ch ns

; <<>> DiG 9.7.0-P1 <<>> cern.ch ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10923
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;cern.ch.                       IN      NS

;; ANSWER SECTION:
cern.ch.                8391    IN      NS      ext-dns-1.cern.ch.
cern.ch.                8391    IN      NS      scsnms.switch.ch.
cern.ch.                8391    IN      NS      ext-dns-2.cern.ch.
```

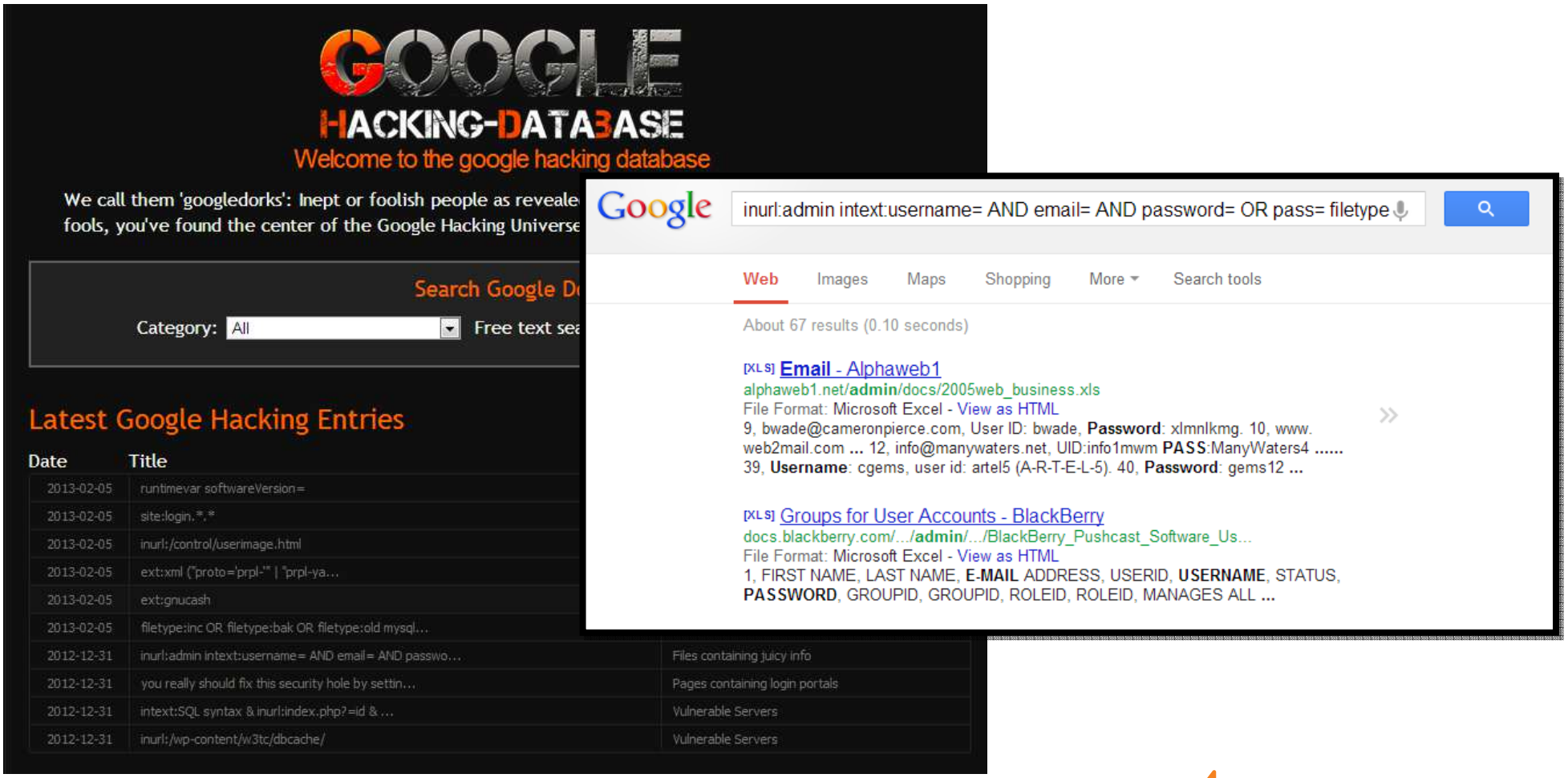
Passive - Google hacking

- Google hacking

Operator	Example	Operator	Example
Using OR or |	hacking http OR ftp	link:	link:cert.lv
" "	"secret document"	cache:	cache:twitter.com
- preceding word	car -golf	related:	related:bbc.com
+ preceding word	car +bmw	intitle:	intitle:"sql error"
- joining words	Brute-forcing	inurl:	inurl:index.php
site:	site:cern.ch	intext:	intext:password.txt
filetype:	filetype:pdf	info:	info:microsoft.com

Passive - Google hacking

- Google hacking database



Passive - Vulnerability databases

- Vulnerability databases

Active – Network, service footprinting

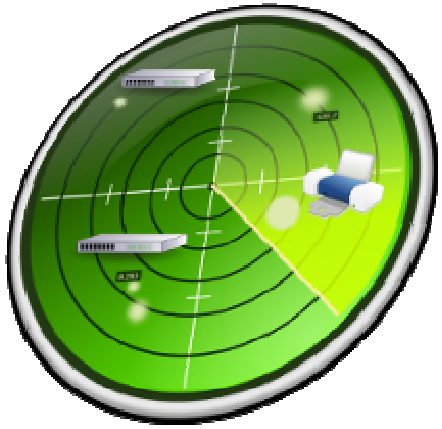
- Active host identification:
  - ping sweep, list scan

```
root@ubu1004-64:/# nmap -sP -n 137.138.144.160-170

Starting Nmap 5.00 ( http://nmap.org ) at 2013-03-05 15:00 EET
Host 137.138.144.161 is up (0.053s latency).
Host 137.138.144.162 is up (0.053s latency).
Host 137.138.144.163 is up (0.053s latency).
Host 137.138.144.164 is up (0.053s latency).
Host 137.138.144.168 is up (0.053s latency).
Host 137.138.144.169 is up (0.053s latency).
Host 137.138.144.170 is up (0.11s latency).
Nmap done: 11 IP addresses (7 hosts up) scanned in 1.44 seconds
```

```
root@ubu1004-64:/# nmap -sL -P0 137.138.144.160-170

Starting Nmap 5.00 ( http://nmap.org ) at 2013-03-05 14:58 EET
Host 137.138.144.160 not scanned
Host webcern01.cern.ch (137.138.144.161) not scanned
Host webredir05.cern.ch (137.138.144.162) not scanned
Host webredir06.cern.ch (137.138.144.163) not scanned
Host webredir07.cern.ch (137.138.144.164) not scanned
Host webredir05-nlb.cern.ch (137.138.144.165) not scanned
Host webredir06-nlb.cern.ch (137.138.144.166) not scanned
Host webredir07-nlb.cern.ch (137.138.144.167) not scanned
Host webr7.cern.ch (137.138.144.168) not scanned
Host webr8.cern.ch (137.138.144.169) not scanned
Host webr9.cern.ch (137.138.144.170) not scanned
Nmap done: 11 IP addresses (0 hosts up) scanned in 1.05 seconds
```



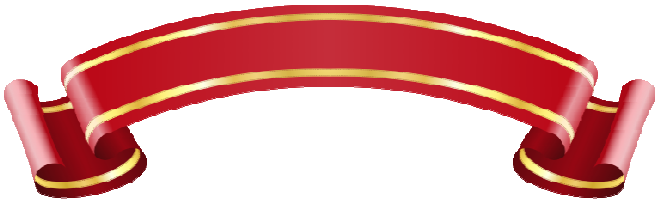
Active – Network, service footprinting

- Traceroute

```
root@ubu1004-64:/# traceroute -T 137.138.144.169
traceroute to 137.138.144.169 (137.138.144.169), 30 hops max, 60 byte packets
 1  85.254.250.126 (85.254.250.126)  0.324 ms  0.377 ms  0.388 ms
 2  85.254.196.234 (85.254.196.234)  0.202 ms  0.203 ms  0.229 ms
 3  sigmanet.mx1.rig.lv.geant.net (62.40.125.157)  0.287 ms  0.272 ms  0.257 ms
 4  so-1-0-0.rt1.tal.ee.geant2.net (62.40.112.205)  8.721 ms  8.709 ms  8.694 ms
 5  xe-1-0-0.mx1.tal.ee.geant.net (62.40.98.0)  8.730 ms  8.721 ms  8.692 ms
 6  so-2-3-0.rt1.cop.dk.geant2.net (62.40.112.121)  21.948 ms  21.938 ms  21.980 ms
 7  as3.rt1.fra.de.geant2.net (62.40.112.49)  35.984 ms  36.010 ms  36.027 ms
 8  ae3.rt1.gen.ch.geant2.net (62.40.112.162)  44.362 ms  44.378 ms  44.401 ms
 9  swiCE2-10GE-1-1.switch.ch (62.40.124.22)  44.353 ms  44.376 ms  44.375 ms
10  e513-e-rbrxl-1-te0.cern.ch (192.65.184.209)  49.974 ms  49.630 ms  49.666 ms
11  e513-e-rbrxl-2-ne0.cern.ch (192.65.184.38)  58.060 ms  53.161 ms  53.164 ms
12  * * *
13  * * *
14  * * *
15  webr8.cern.ch (137.138.144.169)  53.329 ms  53.360 ms  53.301 ms
16  webr8.cern.ch (137.138.144.169)  53.289 ms  53.317 ms  55.750 ms
```

Active – Network, service footprinting

- Banner grabbing



```
root@ubu1004-64:/opt/nmap6/bin# telnet  137.138.144.169 80
Trying 137.138.144.169...
Connected to 137.138.144.169.
Escape character is '^]'.
GET /index.htm HTTP/1.1
host:cern.ch

HTTP/1.1 200 OK
Date: Tue, 05 Mar 2013 13:17:36 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 1.1.4322
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 3650

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
    "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
```

```
root@ubu1004-64:/opt/nmap6/bin# ./nmap -P0 -n -sS -p smtp --script=banner 137.138.144.183

Starting Nmap 6.01 ( http://nmap.org ) at 2013-03-05 15:31 EET
Nmap scan report for 137.138.144.183
Host is up (0.054s latency).
PORT   STATE SERVICE
25/tcp open  smtp
| banner: 220 cernmxgwlb2.cern.ch Microsoft ESMTP MAIL Service ready at T
|_ue, 5 Mar 2013 14:31:13 +0100

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

Active - DNS footprinting

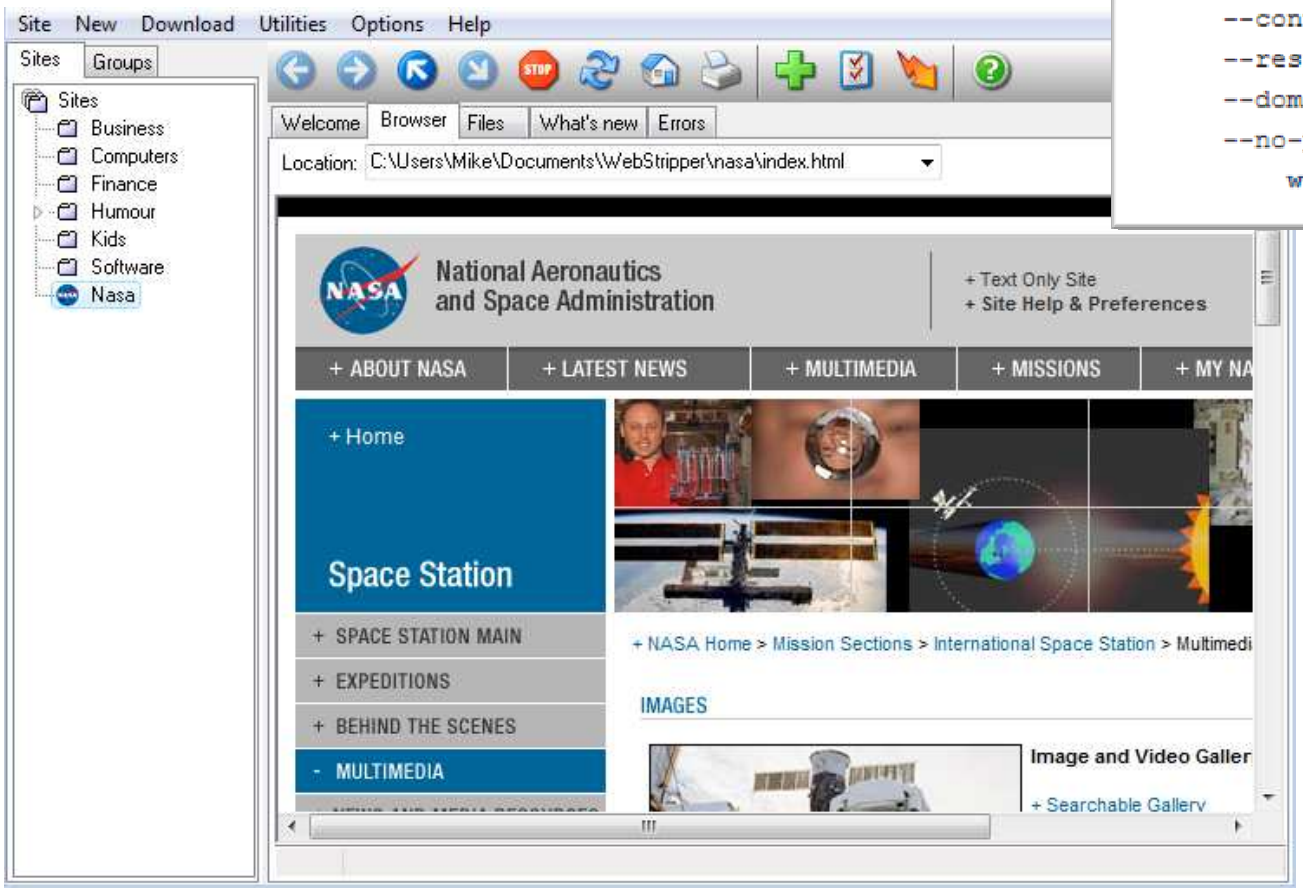
- DNS querying and zone transfer
  - Typical host record types

Type	Description
A	Host address record
MX	Mail exchanger
CNAME	Cannonical host alias
PTR	Pointer record
SOA	Start of authority
NS	Name server
SRV	Service locator

Active - Website footprinting

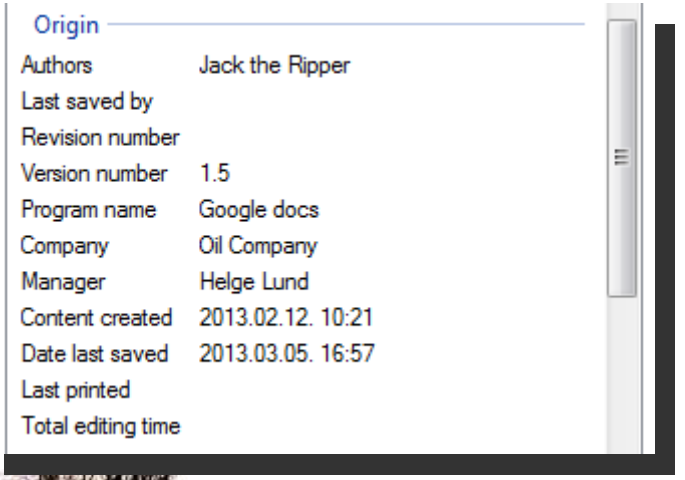
- Offline browsing

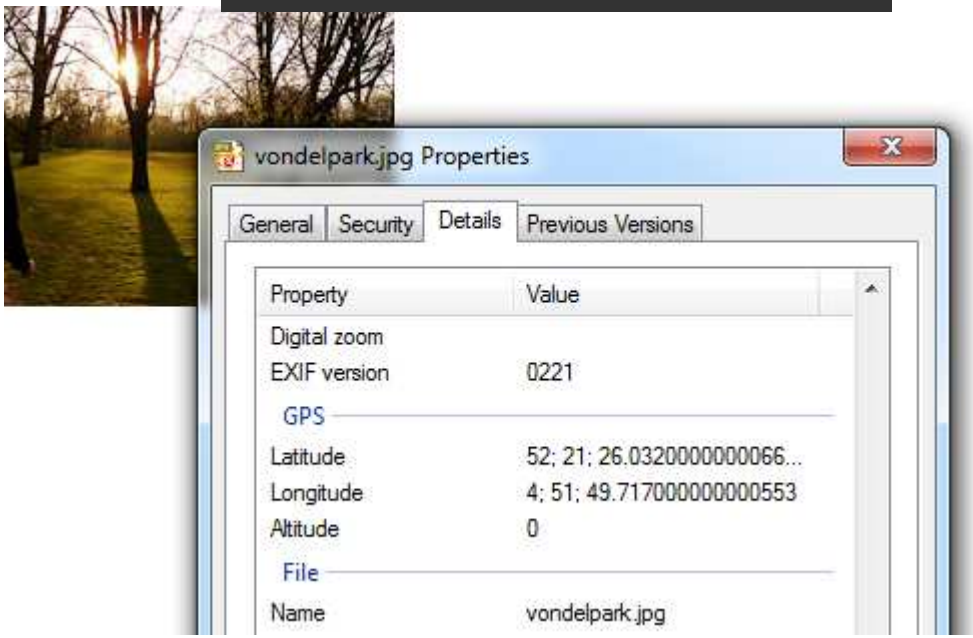
```
$ wget \
      --recursive \
      --no-clobber \
      --page-requisites \
      --html-extension \
      --convert-links \
      --restrict-file-names=windows \
      --domains website.org \
      --no-parent \
          www.website.org/tutorials/html/
```



Active - Website footprinting

- Website data harvesting
  - Documents
  - Document metadata
  - Picture EXIF data
  - E-mail addresses
  - robots.txt






```
# Robots.txt file for http://www.microsoft.com
#

User-agent: *
Disallow: /*navV3Index=0$
Disallow: /*navV3Index=1$
Disallow: /*navV3Index=2$
Disallow: /*navV3Index=3$
Disallow: /*navV3Index=4$
Disallow: /*mnui=-1$
Disallow: /*mnui=0$
Disallow: /*mnui=1$
```

Active - E-mail tracking

- Email tracking


```
Return-path: <utilities@smiconferences.co.uk>
Envelope-to: bernhards@cert.lv
Delivery-date: Tue, 05 Mar 2013 16:58:58 +0200
Received: from [192.168.165.36] (helo=mx.latnet.lv)
    by mstore113.sigmanet.lv with ESMTP id 1UCtKU-000BNY-35 ; Tue, 05 Mar 201
Received: from localhost (localhost [127.0.0.1])
    by pumpis2.latnet.lv (Postfix) with ESMTP id D3F851780FC
    for <cert@latnet.lv>; Tue,  5 Mar 2013 16:58:57 +0200 (EET)
X-Virus-Scanned: Debian amavisd-new at pumpis2.latnet.lv
X-Spam-Flag: NO
X-Spam-Score: 6.752
X-Spam-Level: ******
X-Spam-Status: No, score=6.752 tagged_above=0 required=7 tests=[AWL=-0.266,
    EXCUSE_10_MV=2.5, F_LOAN2=0.1, HTML_MESSAGE=0.001, HTML_TAG2=0.1,
    ONLINE_IN_BODY=0.1, OPPORTUNITY2_MV=1, RCVD_IN_DNSWL_LOW=-1,
    RCVD_IN_JMF_BL=3, RCVD_IN_SORBS_WEB=1.117, RDNS_NONE=0.1,
    SUSP_URL_MV=0.2, TO_HEADER_EXIST=-0.1, URL_STARTS_WITH_WWW=-0.1]
    autolearn=no
Received: from mx.latnet.lv ([127.0.0.1])
    by localhost (pumpis2.latnet.lv [127.0.0.1]) (amavisd-new, port 11141)
    with ESMTP id DcBGrjXFZpDf for <cert@latnet.lv>;
    Tue,  5 Mar 2013 16:58:53 +0200 (EET)
Received: from mx.latnet.lv (localhost [127.0.0.1])
    by pumpis2.latnet.lv (Postfix) with ESMTP id 61624178106
    for <cert@cert.lv>; Tue,  5 Mar 2013 16:58:53 +0200 (EET)
Received: from groupmail.smiconferences.co.uk (unknown [83.244.251.221])
    by pumpis2.latnet.lv (Postfix) with SMTP id BE8FC1780FC
    for <cert@cert.lv>; Tue,  5 Mar 2013 16:58:52 +0200 (EET)
Received: from groupmail.smiconferences.co.uk[127.0.0.1] by groupmail.smiconferences.co.uk[127.0.0.1]
  (SMTPD32); Tue, 5 Mar 2013 14:58:56 -0000
Organization: SMi Group Ltd
Reply-To: utilities@smiconferences.co.uk
Message-ID: <9d0b069204789ced98a1001b001021b5@smiconferences.co.uk>
From: "Colin Kelly" <utilities@smiconferences.co.uk>
```

Active - Social engineering

- Human-Based social engineering:
  - Calling telephone number
  - Sending e-mail
  - Meeting with employees
  - Applying for job
- Reverse social engineering
- Gaining physical access
- Dumpster diving

Target modeling

- Virtualization for target environment modeling

Windows Hyper-V™

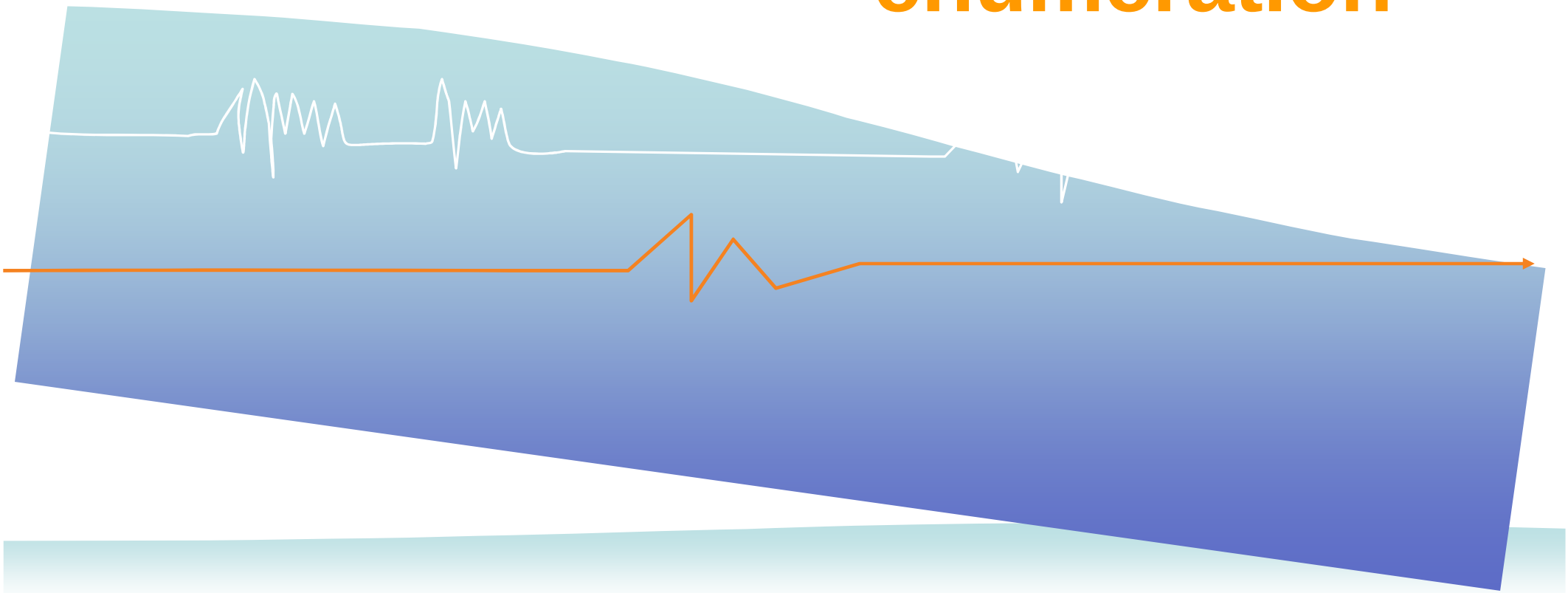
Xen

Target modeling

- Vulnerability identification and testing

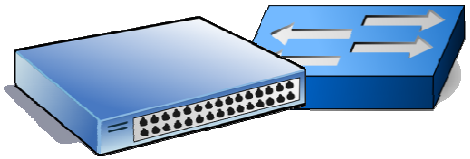
CERT.LV

Scanning and enumeration



Networking devices

- Hub
- Switch
- Router
- Firewall
- NIDS
- Proxy
- Honeypot



Networking devices

- Firewall types:
  - packet filter
  - stateful packet inspection
- Network intrusion system types:
  - detection
  - prevention
- Deep packet inspection
  - DPI = IDS + IPS + SPI

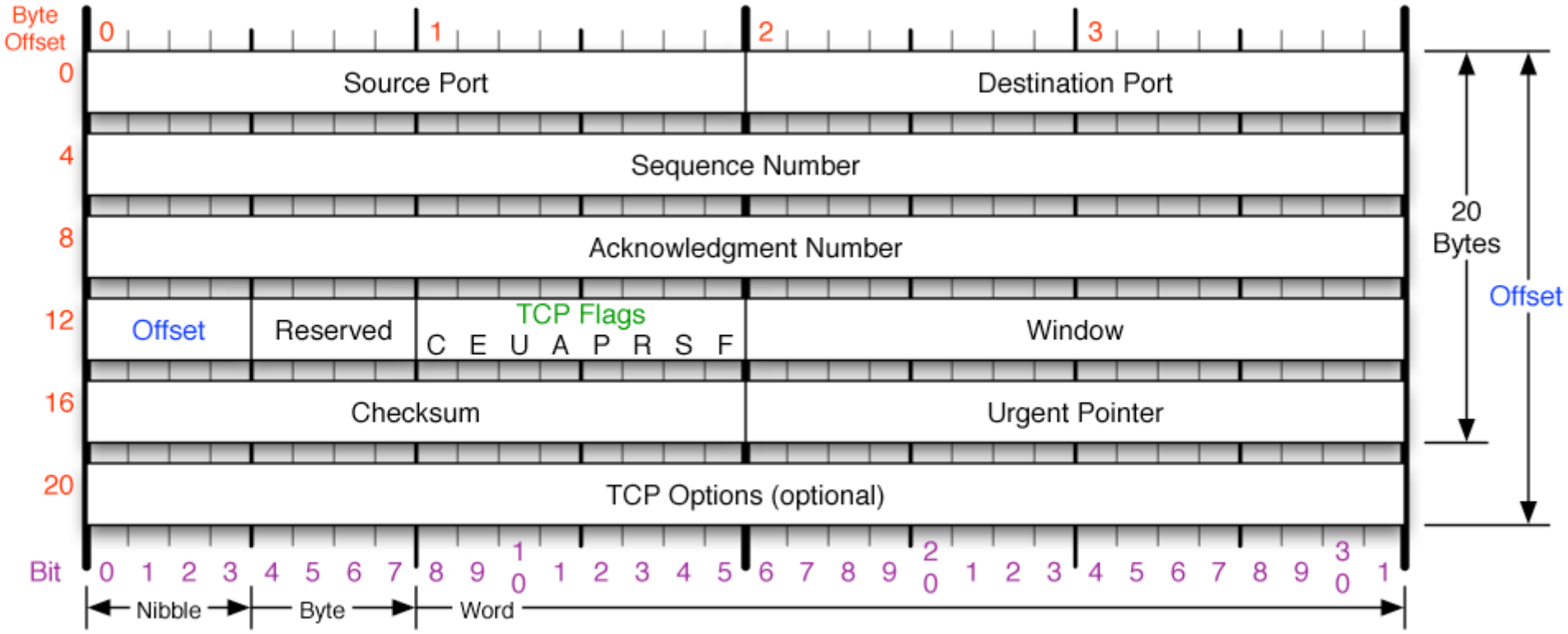
Network models and protocols

- ISO:OSI7 and TCP/IP models

OSI7	TCP/IP
Application layer	Application layer
Presentation layer	
Session layer	
Transport layer	Transport layer
Network layer	Network layer
Data link layer	Network access layer
Physical layer	

Protocol structure

- TCP header



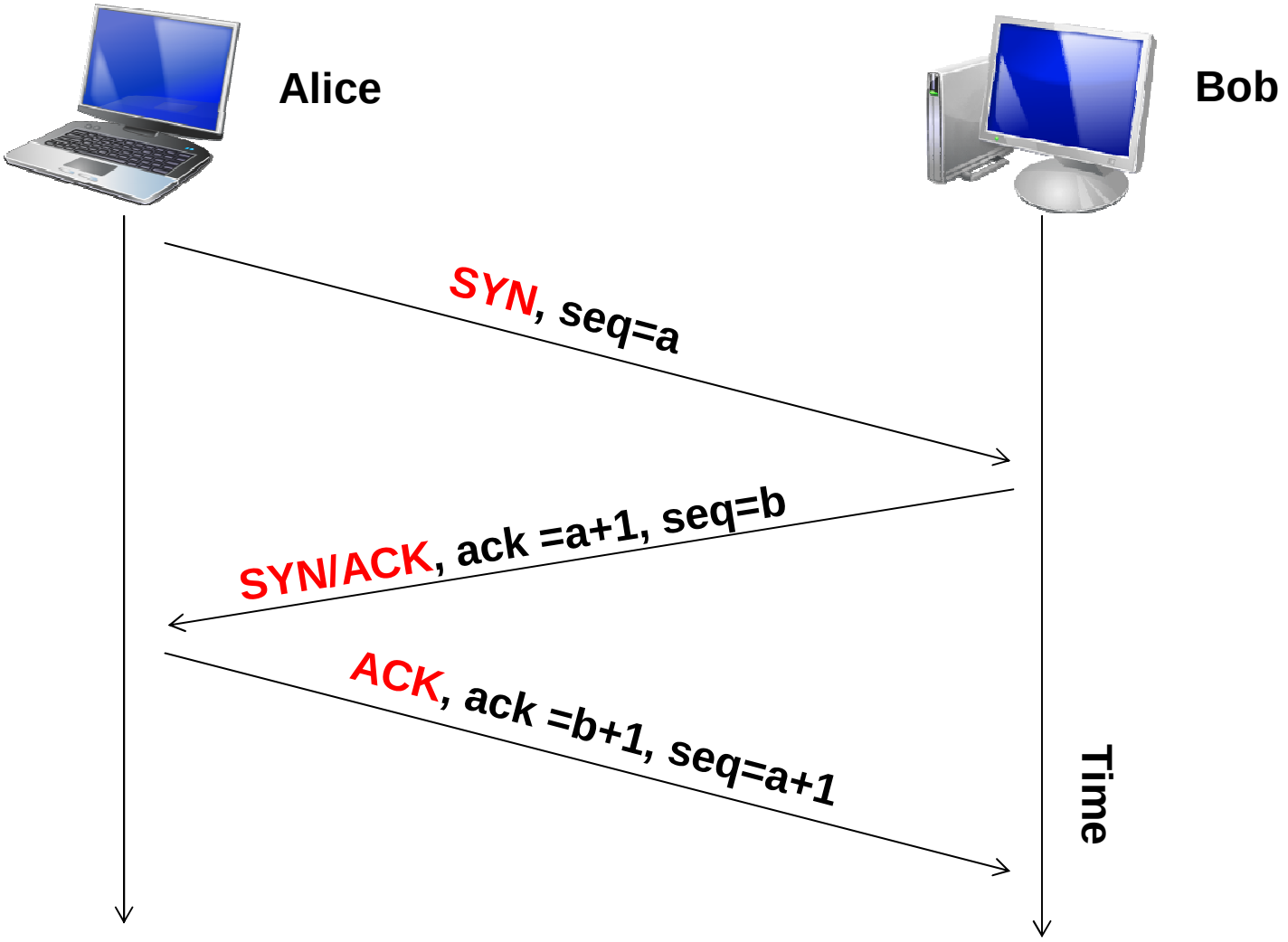
Protocol structure

- TCP flags:

7	6	5	4	3	2	1	0
0	0	URG	ACK	PSH	RST	SYN	FIN

  - FIN – no more data
  - SYN – synchronize sequence numbers
  - RST – reset the connection
  - PSH – push buffered data
  - ACK – acknowledge packet reception
  - URG – process packet immediately

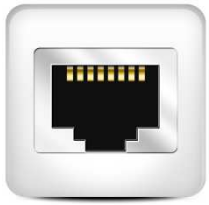
TCP Three-way handshake



Types of scanning

- Network scanning
  - detect active hosts

- Port scanning
  - discover network services



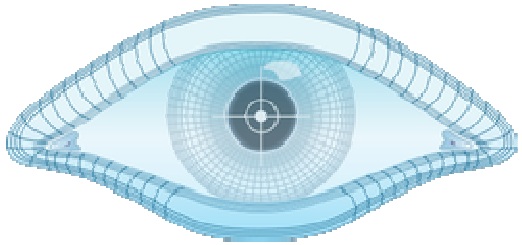
- Vulnerability scanning
  - identify vulnerabilities automatically

Scanning approach

- Identify live systems
- Check for open ports
- Banner grabbing
- Scan for vulnerabilities
- Draw network diagrams
- Prepare proxies

Network mapper - Nmap

- What is Nmap?
  - Host discovery
  - Port scanning
  - Version detection
  - OS detection
  - Advanced scanning
  - Nmap Scripting Engine
    - Vulnerability scanner

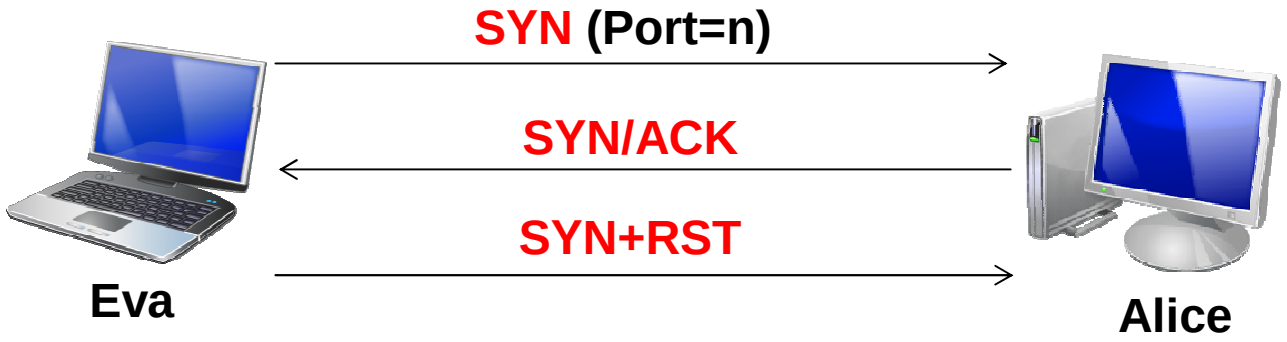


Scan types

- Normal scan
- Inverse scan
- UDP scan
- ICMP echo / List scan

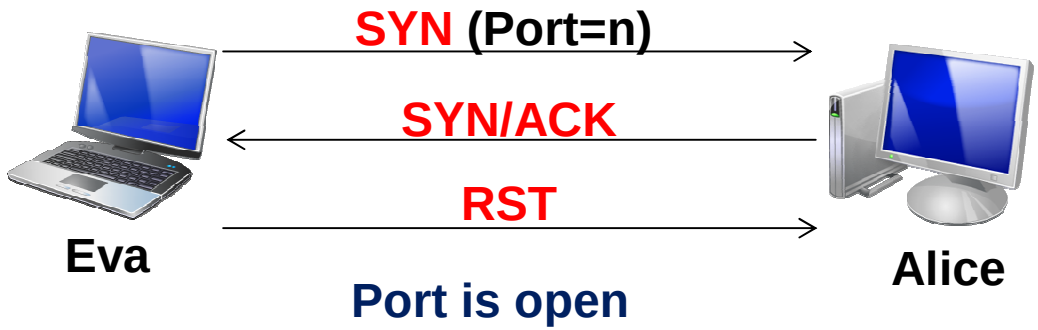
Normal scan

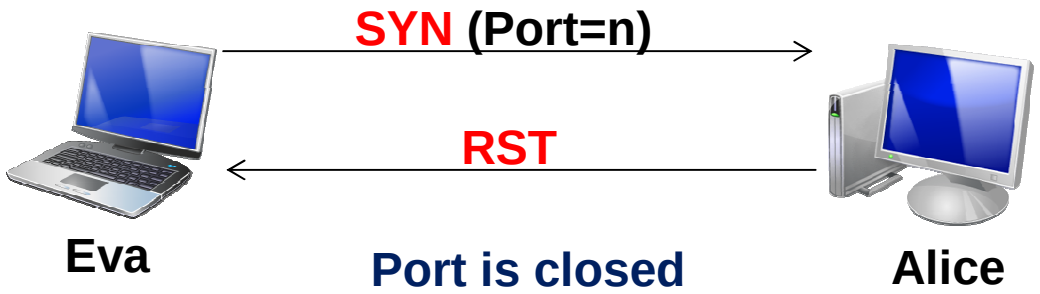
- TCP connect scan (full-open)



Normal scan

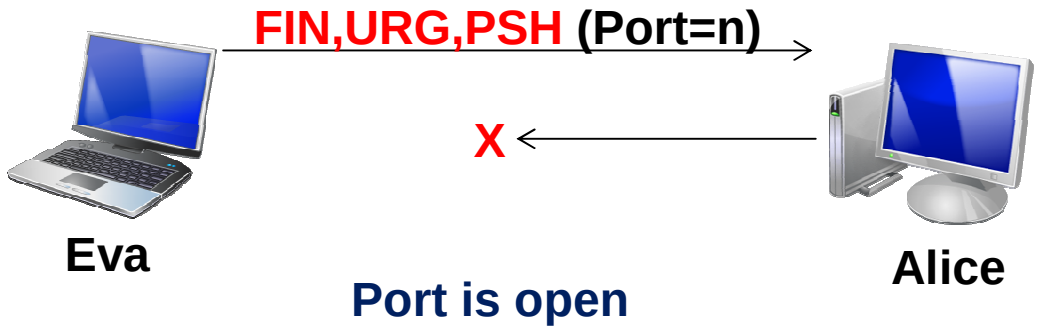
- SYN stealth scan (half-open)

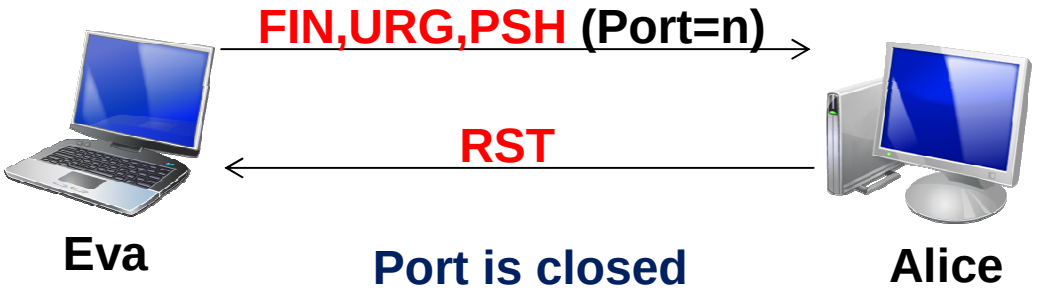




Inverse scan

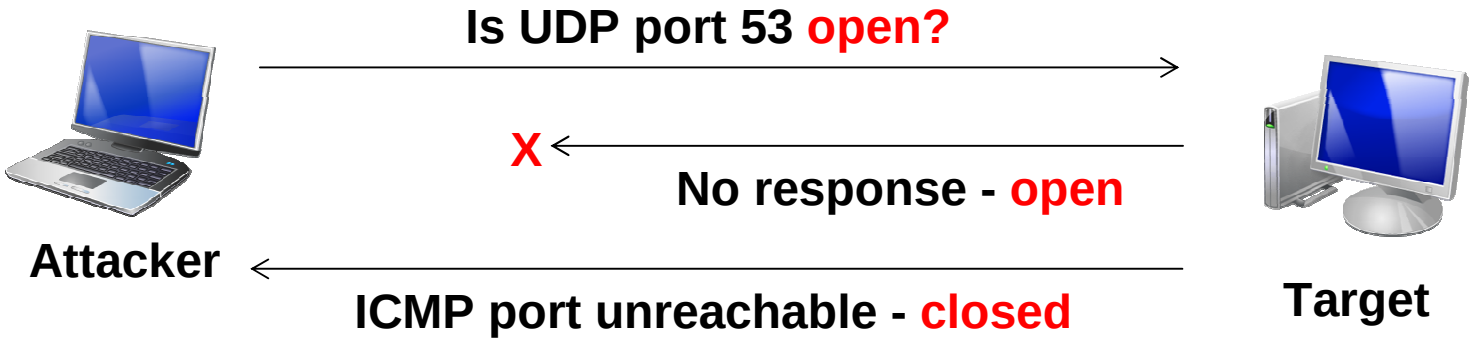
- Xmas scan





Works against RFC793 TCP/IP compliant OS!

UDP scan


Is UDP port 53 open?
X
No response - open
Attacker
ICMP port unreachable - closed
Target

ICMP echo and List scan

- ICMP echo
  - «ping» hosts on network

- List scan
  - do a DNS resolution on hosts

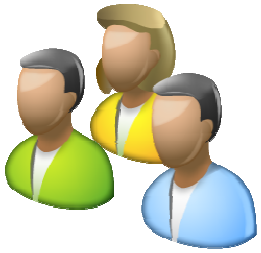
Enumeration

- Extracting and listing information from a system

Enumeration

- Enumeration information types:
  - network resources and shares

  - users and groups



  - applications and banners

  - audit settings

Enumeration

- Types of enumeration:
  - NetBIOS
  - SNMP
  - DNS
  - LDAP
  - SMTP
  - NTP
  - Password

Enumeration

- SMPT enumeration:
  - SMTP address list enumeration

```
lietotajs@ubuntu:/etc/bind$ telnet oilcompany.tk 25
Trying 85.254.250.85...
Connected to oilcompany.tk.
Escape character is '^]'.
220 OILcompany ESMTP Postfix (OIL Company)
VRFY ROOT
252 2.0.0 ROOT
VRFY HELGE
252 2.0.0 HELGE
VRFY JIMMY
550 5.1.1 <JIMMY>: Recipient address rejected: User unknown in local recipient table
VRFY ADMINISTRATOR
550 5.1.1 <ADMINISTRATOR>: Recipient address rejected: User unknown in local recipient table
VRFY FELIX
252 2.0.0 FELIX
```

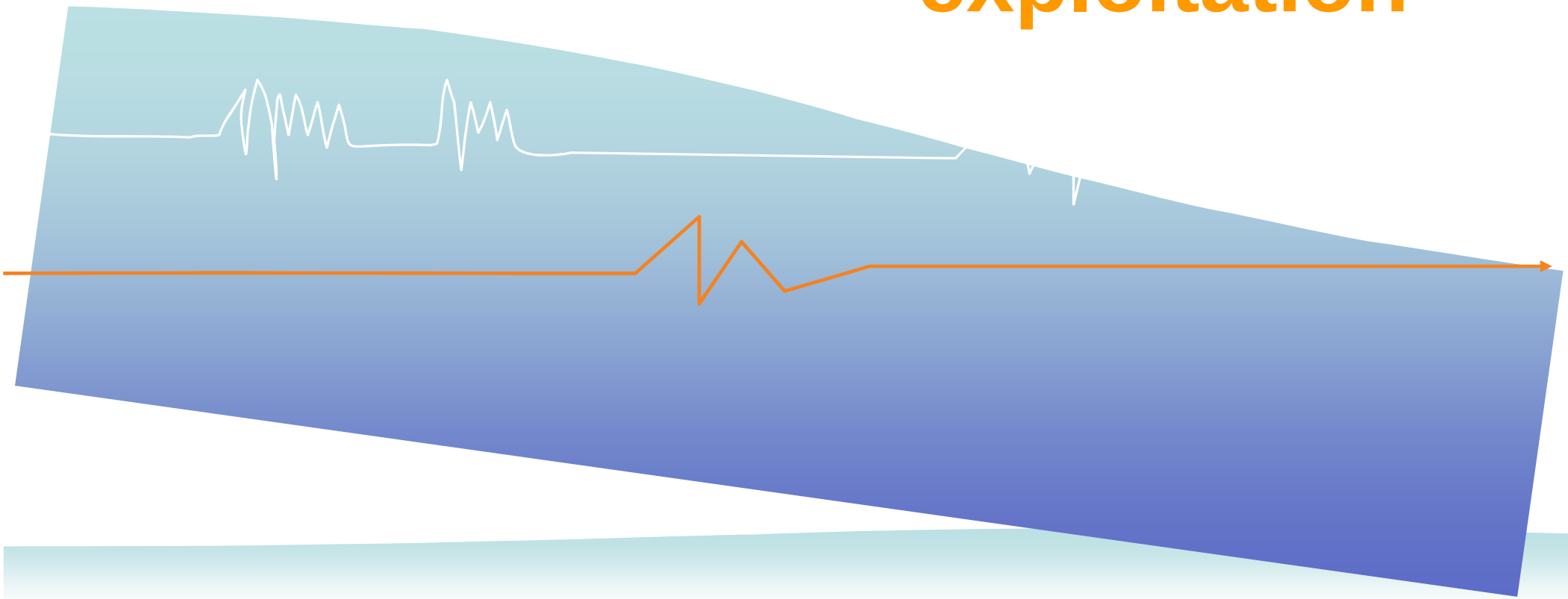
Enumeration

- DNS enumeration:
  - DNS host list enumeration

```
root@bt:/pentest/enumeration/dns/dnsrecon# ./dnsrecon.py -t std -d cern.ch
[*] Performing General Enumeration of Domain:
[-] DNSSEC is not configured for cern.ch
[*]      SOA ext-dns-1.cern.ch 192.65.187.5
[*]      NS scsnms.switch.ch 130.59.1.30
[*]      NS scsnms.switch.ch 130.59.10.30
[*]      NS scsnms.switch.ch 2001:620::1
[*]      NS ext-dns-1.cern.ch 192.65.187.5
[*]      NS ext-dns-2.cern.ch 192.91.245.85
[*]      NS ext-dns-2.cern.ch 2001:1458:1:2::100:85
[*]      MX cernmxgwlb2.cern.ch 137.138.144.183
[*]      A cern.ch 137.138.144.169
[*]      TXT cern.ch v=spf1 a:cernmx30.cern.ch a:cernmx31.cern.ch a:cernmx32.cern.ch a:cernmx33.c
ern.ch a:cernmx34.cern.ch ?all
[*] Enumerating SRV Records
[*]      SRV _kerberos._tcp.cern.ch cerndc.cern.ch 137.138.20.248 88 100
[*]      SRV _kerberos._tcp.cern.ch cerndc.cern.ch 137.138.20.249 88 100
[*]      SRV _kerberos._udp.cern.ch cerndc.cern.ch 137.138.20.249 88 100
[*]      SRV _kerberos._udp.cern.ch cerndc.cern.ch 137.138.20.248 88 100
[*]      SRV _sip._tls.cern.ch sip.cern.ch 137.138.21.216 443 0
[*]      SRV _sip._tls.cern.ch sip.cern.ch 137.138.20.216 443 0
[*]      SRV _sipfederationtls._tcp.cern.ch sip.cern.ch 137.138.20.216 5061 0
[*]      SRV _sipfederationtls._tcp.cern.ch sip.cern.ch 137.138.21.216 5061 0
[*] 8 Records Found
```

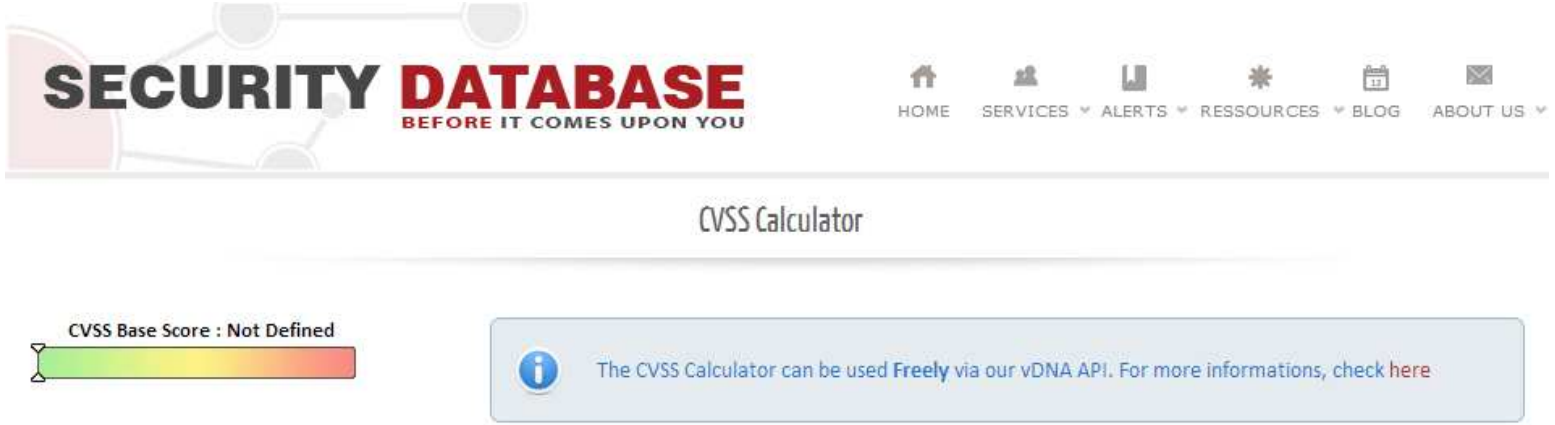
CERT.LV

Vulnerability exploitation



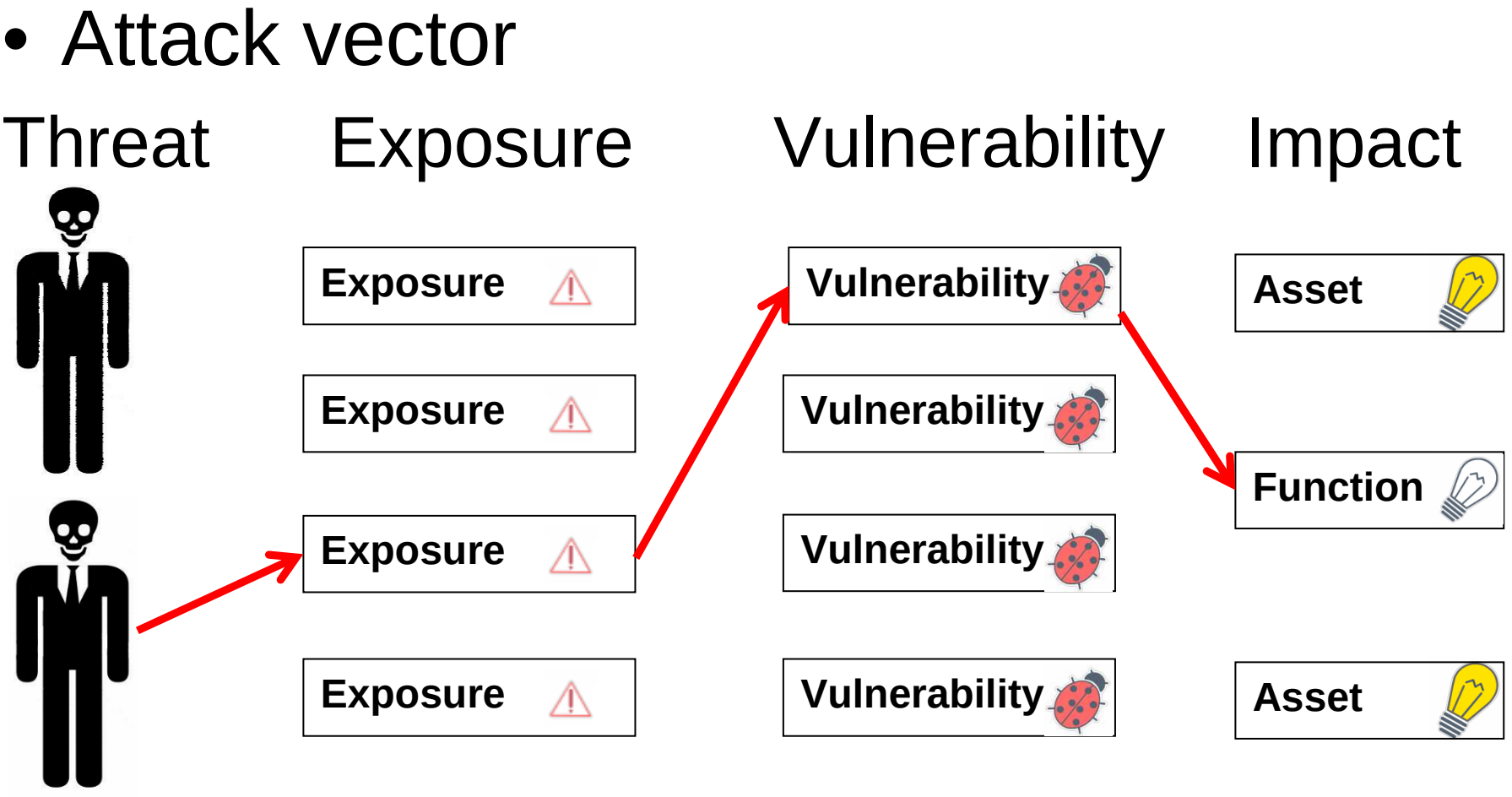
Exploit databases

- Vulnerability identification:
  - Exploit-DB
  - NIST NVD
- CVSS – Common vulnerability scoring system



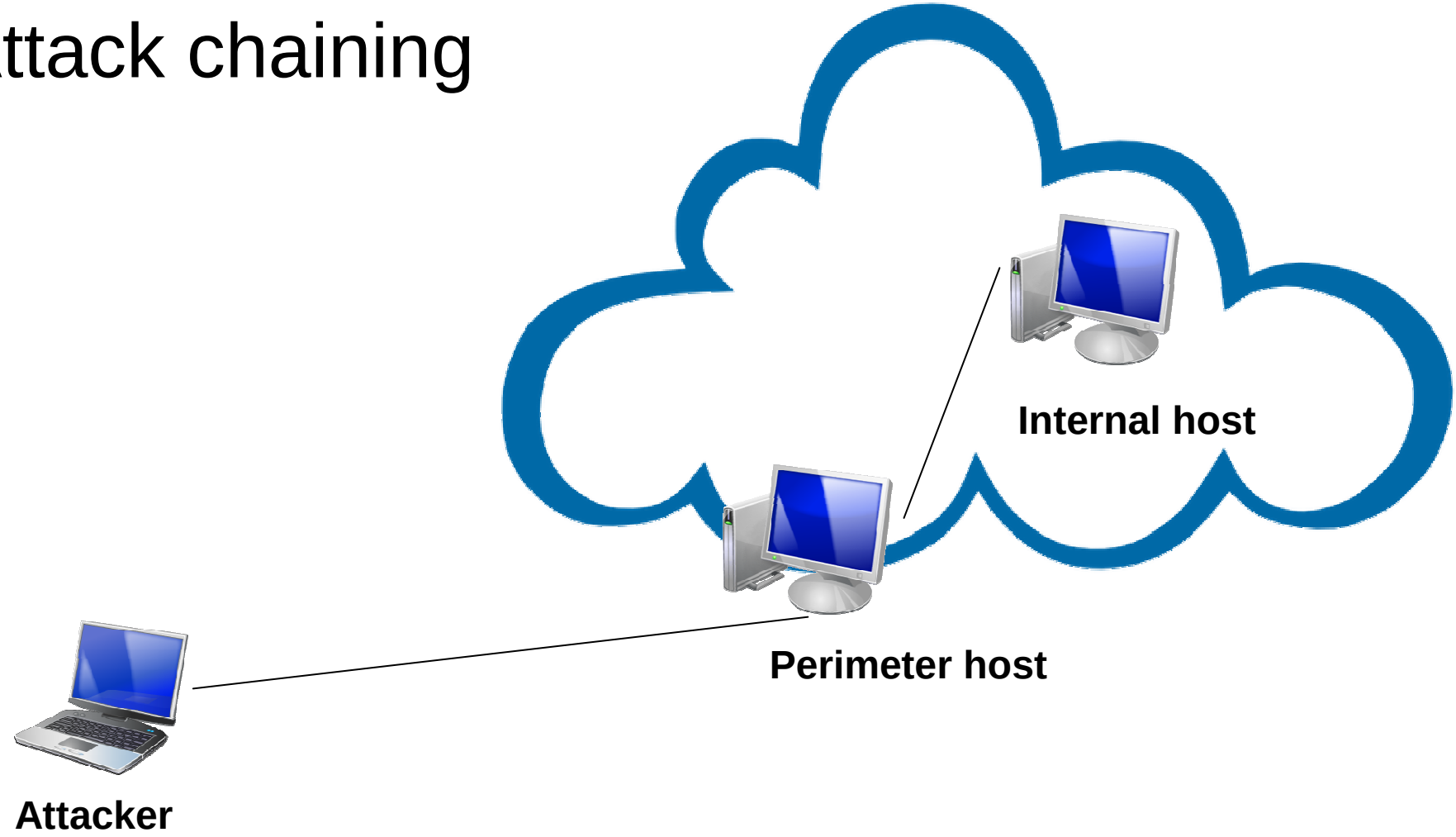
Attack staging

- Attack vector



Attack staging

- Attack chaining



Buffer overflows

- The sample code

```
#include <stdio.h>
main() {
    char *name;
    char *danger;
    name = (char *) malloc(10);
    danger = (char *) malloc(128);
    printf ("Address of name is %d\n", name);
    printf ("Address of command is %d\n", danger);
    printf ("Address difference is %d bytes \n", danger-name);
    sprintf (danger, "echo %s", "Hello world!");
    printf ("Enter your name:");
    gets (name);
    system (danger); }
```

Buffer overflows

- The memory stack

Content	Memory address
	500
	..
Instructions	..
	...
	1500
Variables	..
	1750
Registers	... (ESP)
	1850

Buffer overflows

- Shellcode
  - code executed in target system

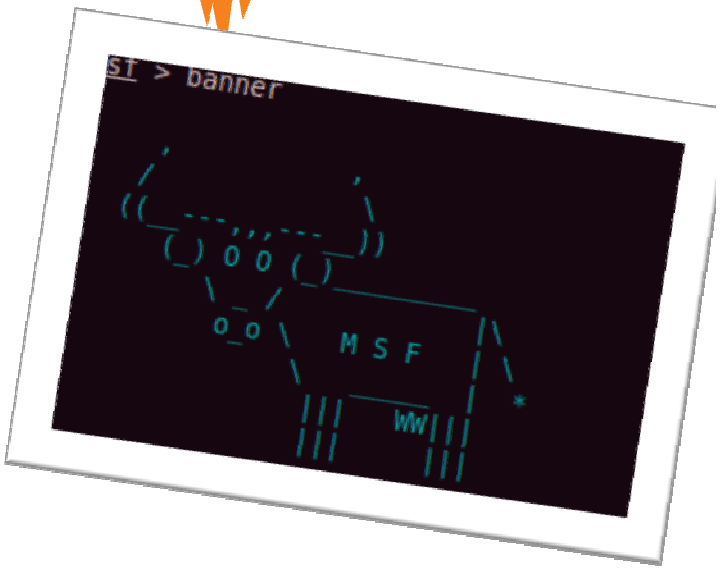
```
char shellcode[] =
"\x31\xc0\x31\xdb\x31\xd2\x53\x68\x69\x74\x79\x0a\x68\x65\x63"
"\x75\x72\x68\x44\x4c\x20\x53\x89\xe1\xb2\x0f\xb0\x04\xcd\x80"
"\x31\xc0\x31\xdb\x31\xc9\xb0\x17\xcd\x80\x31\xc0\x50\x68\x6e"
"\x2f\x73\x68\x68\x2f\x2f\x62\x69\x89\xe3\x8d\x54\x24\x08\x50\x53"
"\x8d\x0c\x24\xb0\x0b\xcd\x80\x31\xc0\xb0\x01\xcd\x80";
```

- Wrapper
  - Means of delivering shellcode to target system

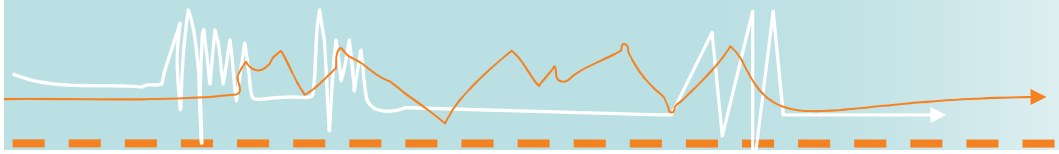
Metasploit

- What is Metasploit?

What is Metasploit?



- Vulnerability database
- OPcode database
- Shellcode database
- Choose and configure exploit
- Configure payload
- Execute the exploit
- Manage target system via Meterpreter
- Attack chaining



CERT.LV

Thank you!

http://www.cert.lv/

cert@cert.lv