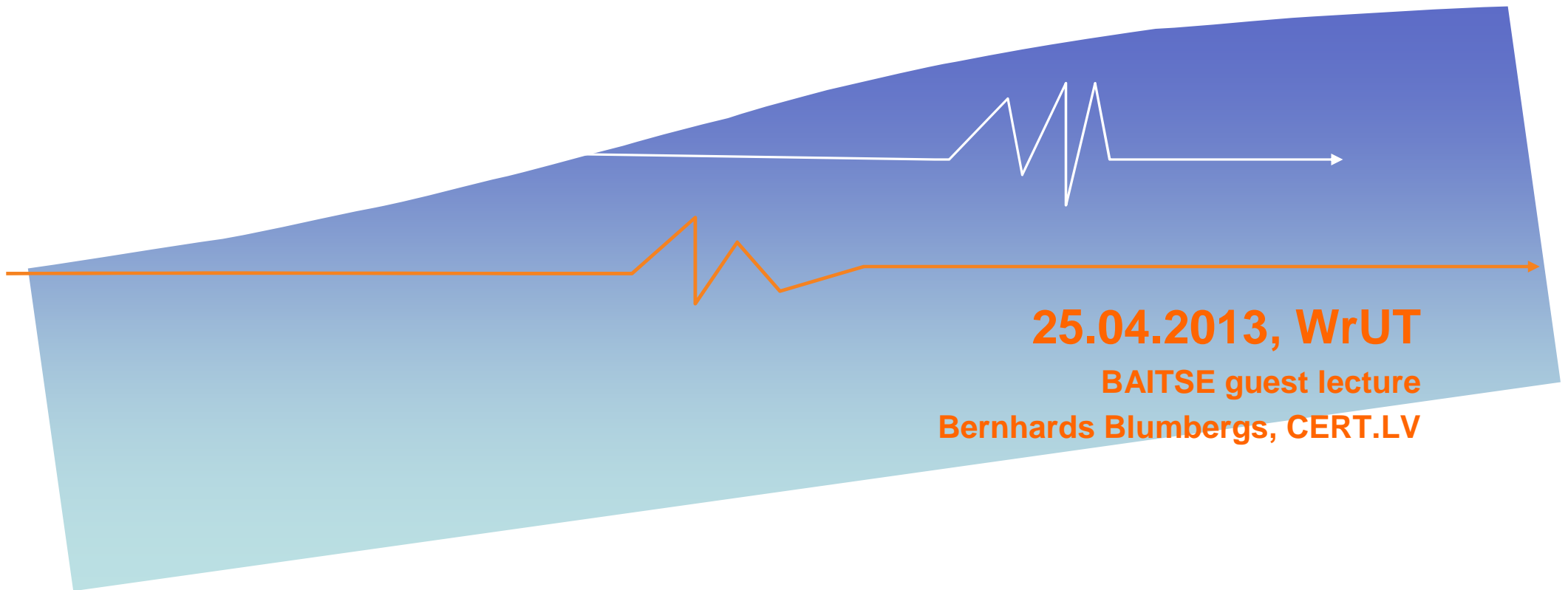




Basics of executing a penetration test



25.04.2013, WrUT

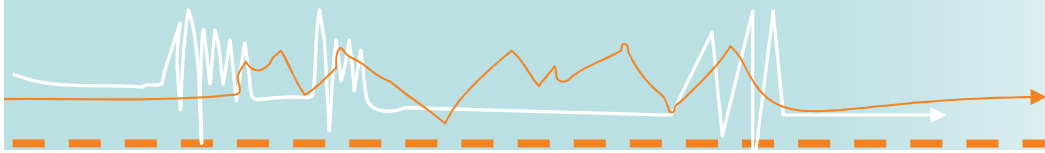
BAITSE guest lecture

Bernhards Blumbergs, CERT.LV

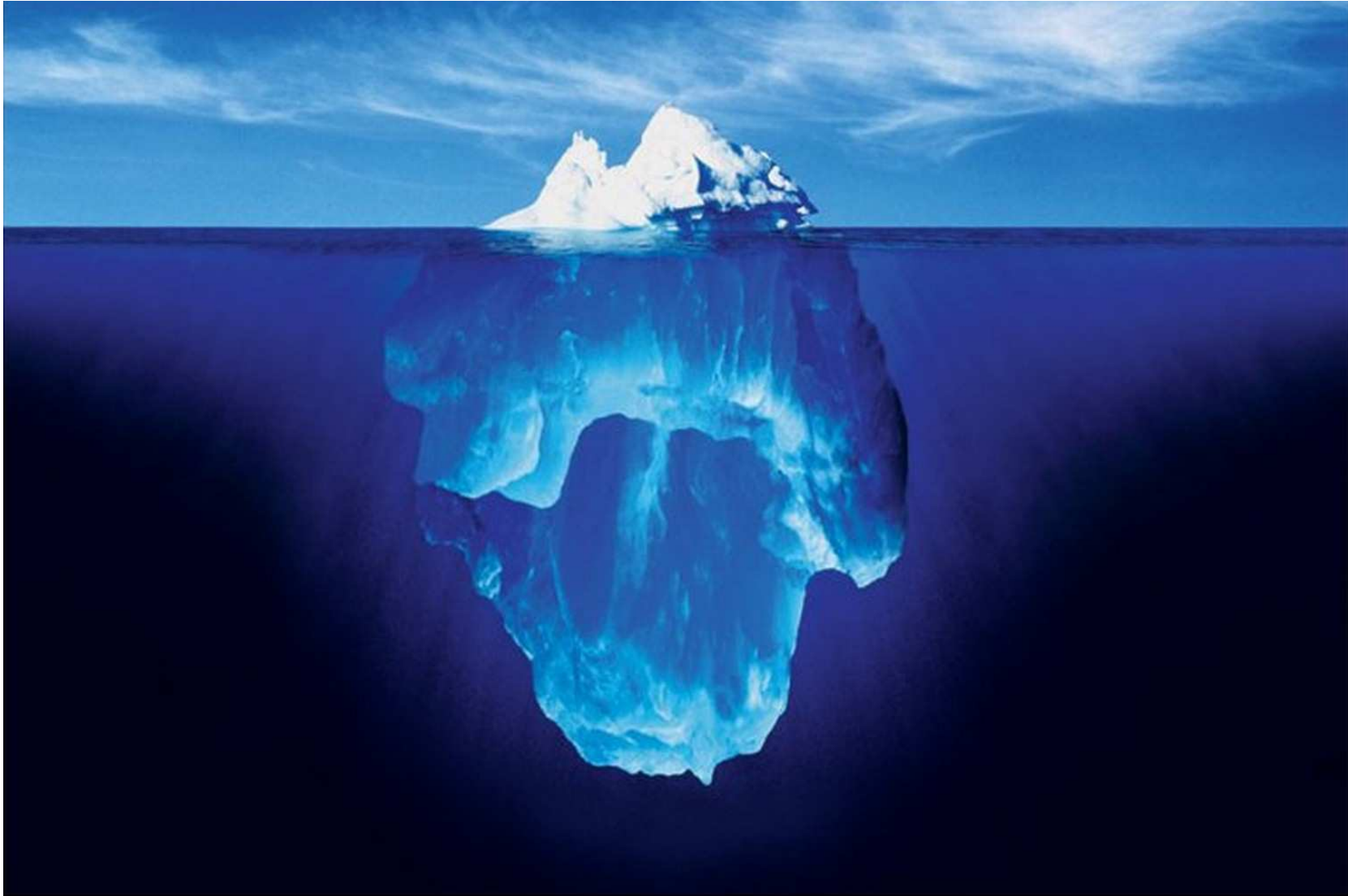
Outline

- Reconnaissance and footprinting
- Scanning and enumeration
- System exploitation





Outline



Reconnaissance and footprinting

What is footprinting?

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



Footprinting types

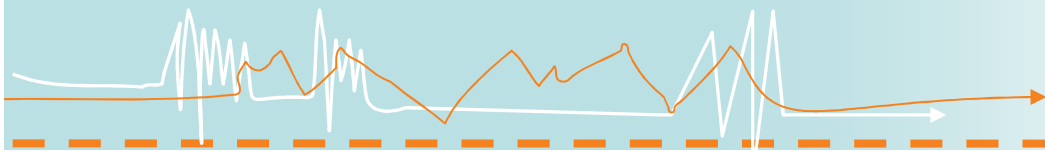
- Internet footprinting
- Organizational footprinting
- Whois footprinting
- DNS footprinting
- Network footprinting
- Website footprinting
- E-mail footprinting
- Google hacking
- Vulnerability identification



Open Source Intelligence

- Reconnaissance information derived from publicly available sources





CERT.LV

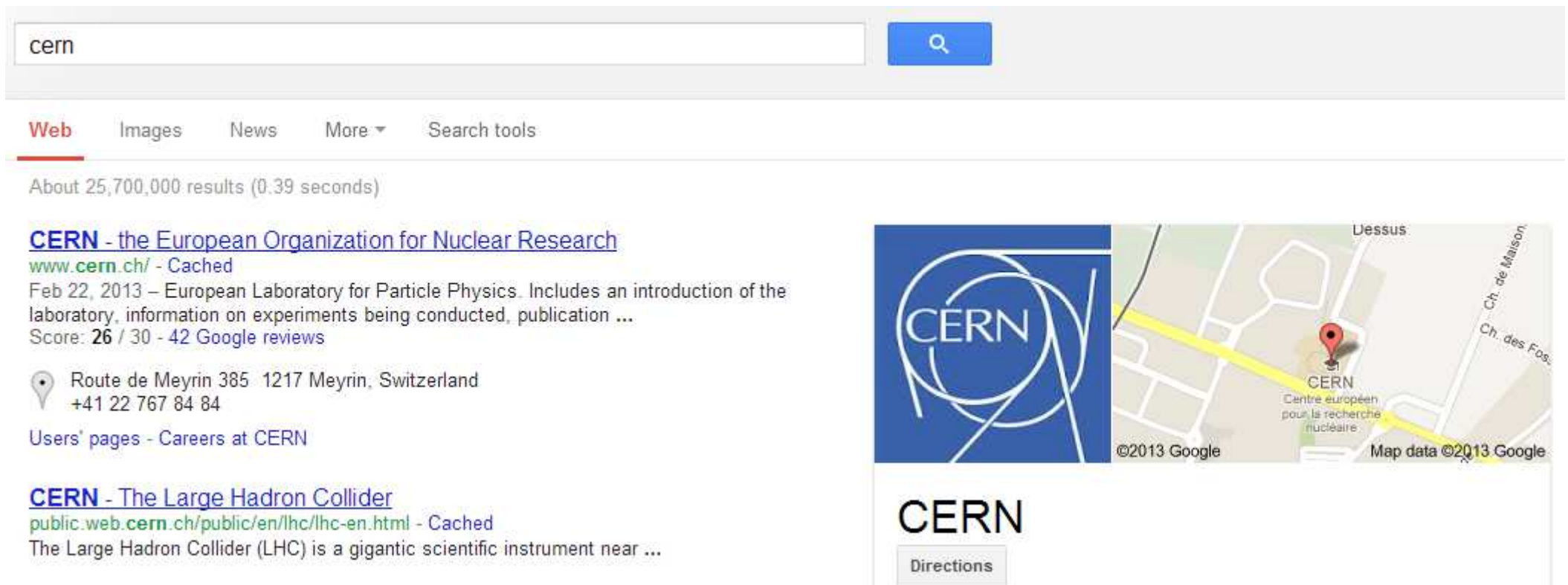
Reconnaissance types

- **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

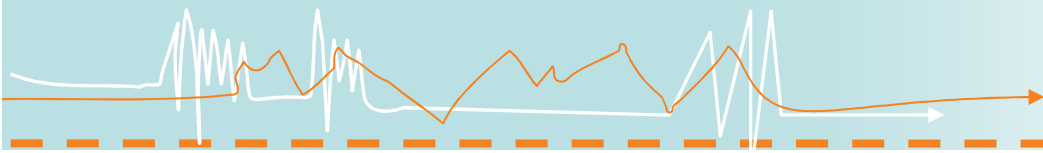
Route de Meyrin 385 1217 Meyrin, Switzerland
+41 22 767 84 84

[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 ...

 
Dessus
Ch. de Maison
Ch. des Fos
CERN
Centre européen pour la recherche nucléaire
©2013 Google Map data ©2013 Google

CERN
Directions



Passive - Internet search

- Public and restricted websites



CERN Single Sign-On

Sign in with a CERN account, a Federation account or a public service account

11 February

Long Shutdown: Exciting times ahead

Over 10,000 high-current splices between LHC magnets will be opened and consolidated during the first Long Shutdown of the LHC. This image shows their installation in 2007 (Image: CERN)

INFORMATION FOR:

- CERN staff and users
- Journalists
- Kids
- Our neighbours

INFORMATION ABOUT:

- CERN in a nutshell
- Science at CERN
- Research at CERN
- The Large Hadron Collider (LHC)
- People at CERN
- Education at CERN
- CERN and the environment

PUBLICATIONS:

- CERN Courier
- CERN Bulletin

Sign in with your CERN account

Reminder: you have agreed to comply with the CERN computing rules

Use credentials

Username or Email address Password

Remember Username or Email Address [Need password help?](#)

Use one-click authentication

[Sign in using your current Windows/Kerberos credentials \[autologon\]](#)
Use your current authentication token. You need Internet Explorer on CERN Windows or Firefox on SLC (Firefox help here).

[Sign in using your Certificate \[autologon\]](#)
Use a EuGridPMA trusted certificate. Don't forget to first map your Certificate to your CERN Account.

Use strong two factor authentication [\[show\]](#)



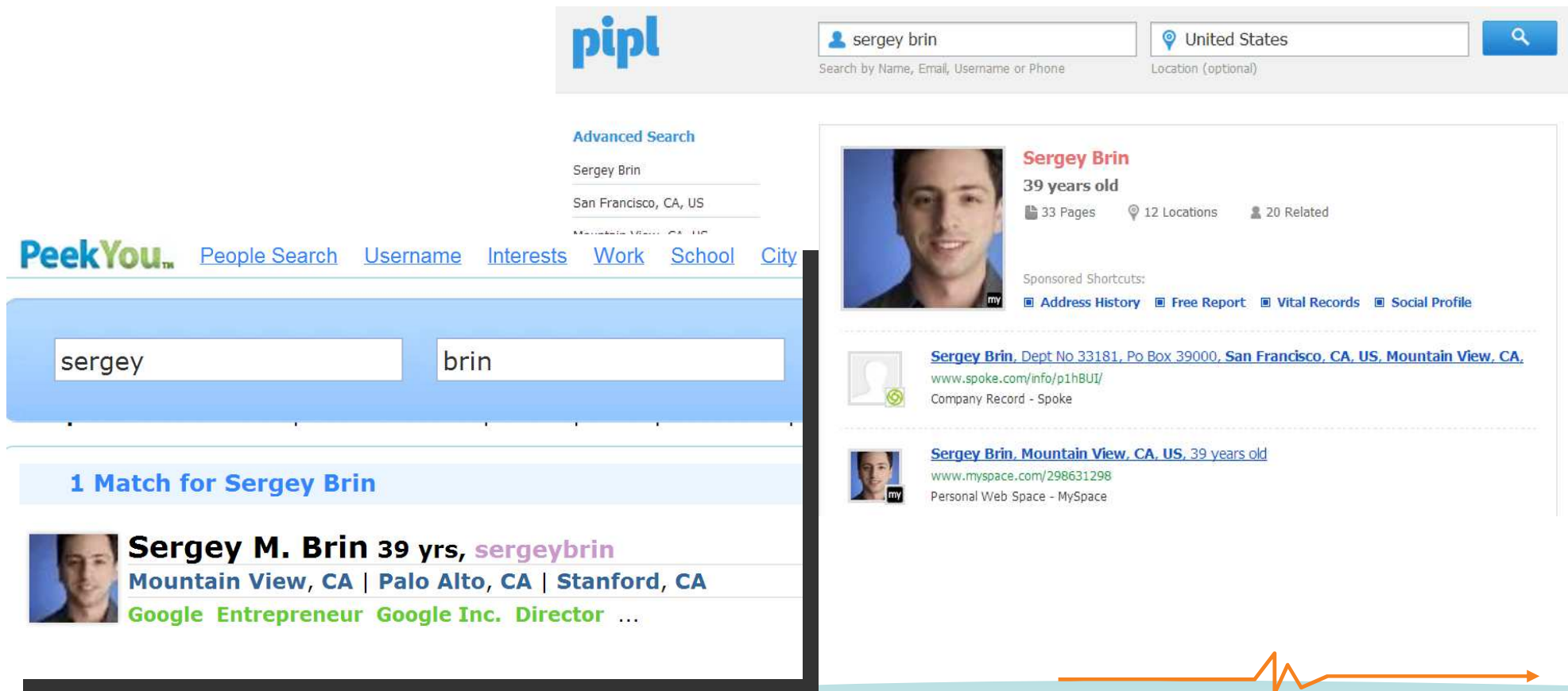
Passive - Internet search

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



Passive - Internet search

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



The image shows a screenshot of the Pipl.com search interface. At the top, the Pipl logo is on the left, and search filters for 'sergey brin' and 'United States' are on the right. Below the search bar, there are tabs for 'Advanced Search', 'People Search', 'Username', 'Interests', 'Work', 'School', and 'City'. The search results show one match for 'Sergey Brin'.

Advanced Search
 Sergey Brin
 San Francisco, CA, US

PeekYou™ People Search Username Interests Work School City

sergey brin

1 Match for Sergey Brin

Sergey M. Brin 39 yrs, sergeybrin
 Mountain View, CA | Palo Alto, CA | Stanford, CA
 Google Entrepreneur Google Inc. Director ...

Sergey Brin
 39 years old
 33 Pages 12 Locations 20 Related

Sponsored Shortcuts:
 Address History Free Report Vital Records Social Profile

Sergey Brin, Dept No 33181, Po Box 39000, San Francisco, CA, US, Mountain View, CA,
www.spoke.com/info/p1hBUI/
 Company Record - Spoke

Sergey Brin, Mountain View, CA, US, 39 years old
www.myspace.com/298631298
 Personal Web Space - MySpace

Passive - Internet search

- Social networks:
- LinkedIn.com

LinkedIn



Pierre Bonnal
Senior Project Engineer at CERN
Geneva Area, Switzerland | Research

Join LinkedIn and access Pierre Bonnal's full profile.

As a LinkedIn member, you'll join 200 million other professionals who are sharing connections, ideas, and opportunities. And it's free! You'll also be able to:

- See who you and **Pierre Bonnal** know in common
- Get introduced to **Pierre Bonnal**
- Contact **Pierre Bonnal** directly

[View full profile](#)

Pierre Bonnal's Overview

| | |
|-------------|--|
| Current | Senior Project Engineer at CERN Senior lecturer at Université de Lausanne / HEC School of Business Senior lecturer at Université de Genève / HEC School of Business |
| Past | Consultant en management at Bonnal & futurs associés Professor; Dean of the Business Administration Department at University of Applied Sciences Western Switzerland / Haute école de gestion de Genève Senior lecturer at Conservatoire National des Arts et Métiers, Paris / Institut International de Management see all ^ |
| Education | Institut National Polytechnique de Toulouse Université Paul Cézanne (Aix-Marseille III) Université du Québec à Trois-Rivières see all ^ |
| Connections | 342 connections |
| Websites | cern.ch/puresafe hec.unil.ch/faculty/pbonnal |

LinkedIn



Tim Smith
IT Group Leader at CERN
Geneva Area, Switzerland | Research

Join LinkedIn and access Tim Smith's full profile.

As a LinkedIn member, you'll join 200 million other professionals who are sharing connections, ideas, and opportunities. And it's free! You'll also be able to:

- See who you and **Tim Smith** know in common
- Get introduced to **Tim Smith**
- Contact **Tim Smith** directly

[View full profile](#)

Tim Smith's Overview

| | |
|-------------|--|
| Current | Group Leader, Collaboration and Information Services at CERN Chair, Harassment Investigation Panel at CERN |
| Past | Group Leader, User and Document Services at CERN Chair, Equal Opportunities Advisory Panel at CERN Section Leader, IT Data Services at CERN Section Leader, IT Computing Fabric Services at CERN IT Staff member at CERN Research Associate at University of Victoria Fellow, Physics Research at CERN see less ^ |
| Education | The University of Birmingham The University of Birmingham |
| Connections | 177 connections |
| Websites | Personal Website |



Passive - Internet search

Tweets

- Social networks:
- Facebook, Twitter



Rita Stiene @zakitis69

8 secs

How in the hell will I sort this mess out? Two sleepless weeks here I come! plc.twitter.com/6f1XGf7WLI

Hide photo Reply Delete Favorite More

Tweets



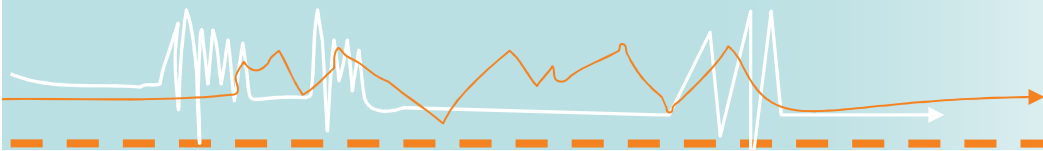
Rita Stiene @zakitis69

now

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

Expand





Passive - Internet search

- Social networks:
- Forums and groups



Log error in velocity on Linux systems

When instatiating Velocity I get this error (posted just the "caused by"-messages):

```
1
java.lang.RuntimeException: Velocity could not be initialized!
Caused by: org.apache.velocity.exception.VelocityException: Error initializing log
Caused by: org.apache.velocity.exception.VelocityException: Failed to initialize a
Caused by: java.lang.RuntimeException: Error configuring Log4JLogChute :
Caused by: java.io.FileNotFoundException: velocity.log (Permission denied)
```

ronnielebaron 09-05-2012 at 05:35:37 PM

I work for a small radio station. We have about 85 devices on our network, running off a cisco 881 router. For one reason or other, after a couple hours the past few days, it has been locking up and funneling down my internet connection from 20 mbps to around .5. At first I naturally called and chewed out the internet guys, but they kept saying everything looked fine on their end. Finally, in a fit of desperation, I rebooted the router, and my connection shot back up to 20 megs. A few hours later, I got calls saying it had dropped back down again. I rebooted the router, same result. So what I'm wondering is, what's the next step in troubleshooting this thing? Is it the router itself, or is there something on the network spanning through the internet? I'm fairly new to the world of business networking and could really use whatever help anyone can offer!

> See more for "[\[Solved\] Cisco 881 router problems](#)"

[Add A Reply](#)

Groups

microsoft.public.dataprotectionmanager >

hyperv backup error.. "unable to configure protection" +1

12 posts by 2 authors in microsoft.public.dataprotectionmanager

markm75g

I have dpm 2007 sp1 with the latest service patches and updates (2008 x64 enterprise)...

The hyperV server is 2008 datacenter gui.. with the latest updates..

This hyperv server has been rebooted (i had to to even have the vm's show up in dpm for some reason, as they disappeared, this a separate earlier issue)..

I checked off the backup of "child partitions" for the various VMs..

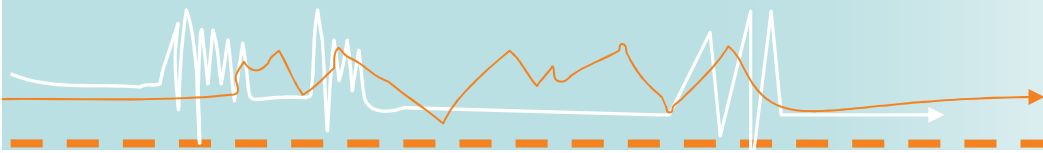
I end up with an error.. unable to configure protection on most of them.. a few did work..

The error details are as follows:

Affected area: \Backup Using Child Partition Snapshot\VSIntranet01
Occurred since: 3/15/2009 4:13:53 PM
Description: DPM could not start a recovery, consistency check, or initial backup of the backup agent on server02.domain.local for following reason:

...VSS provider is in a bad state. Either it is in a bad state during the current backup operation (0x80042318) (0x80042318)) or the backup agent did not check that the Event Service and the VSS service were running on server02.domain.local. Please allow 10 minutes for the backup agent to retry the operation.

32612.



Passive - Internet search

- Location information



Other GIS Portal



Passive - Internet search

- Google cache



The screenshot shows the ATLAS Experiment website. At the top, there is a navigation menu with links: Home, Info, Multimedia, Blogs, Links, Visit ATLAS, Contact, Collaboration Site, Store, Press, and Student/Teach. Below the menu, a news banner reads "Time Magazine Person of the Year Runner-Up: Fabiola Gianotti_". The main content area is split into two columns. The left column features the headline "ATLAS and the Higgs" with a sub-headline "Finding the Higgs boson will change our understanding of the world. ATLAS observed a new particle in". The right column features the headline "2012: A Year for Science - A Year for Discovery" with a sub-headline "Amazing, incredible, emotional. These are". Below the main content, there is a section with a circular particle detector visualization on the left and text on the right that reads "fantastically uncommon year for ATLAS, one of the main experiments at CERN: marvellous machine performance, numerous and interesting physics results, plenty of interactions with students and general public, and - last but not least - a major discovery! More...".

This is Google's cache of <http://atlas.ch/>. It is a snapshot of the page as it appeared on 21 Feb 2013 07:49:09 GMT. The [current page](#) could have changed in the meantime. Tip: To quickly find your search term on this page, press Ctrl+F or ⌘-F (Mac) and use the find bar.

Passive - Internet search

- Internet Archive – wayback machine

INTERNET ARCHIVE
Wayback Machine

<http://cern.ch> has been crawled 3,931 times going all the way back to [November 15, 1996](#).
A crawl can be a duplicate of the last one. It happens about 25% of the time across 420,000,000 websites. [FAQ](#)

1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008

1,471 captures
21 Jun 00 - 17 Feb 13

JUL AUG SEP
2006 2007 2008

English Site Map Search Contact Us Credits

Press & Media Recruitment Technology Transfer Relations with Industry for CERN Users

CERN

The world's largest particle physics laboratory
... where the web was born!

CERN's Flagship Project: the LHC

- LHC Milestones: follow the adventure!
- New LHC Schedule
- ATLAS: first end-cap in place

CERN, the coolest place in the Universe

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



Alerts

Search query:

Result type:

Everything

How often:

Once a day

How many:

Only the best results

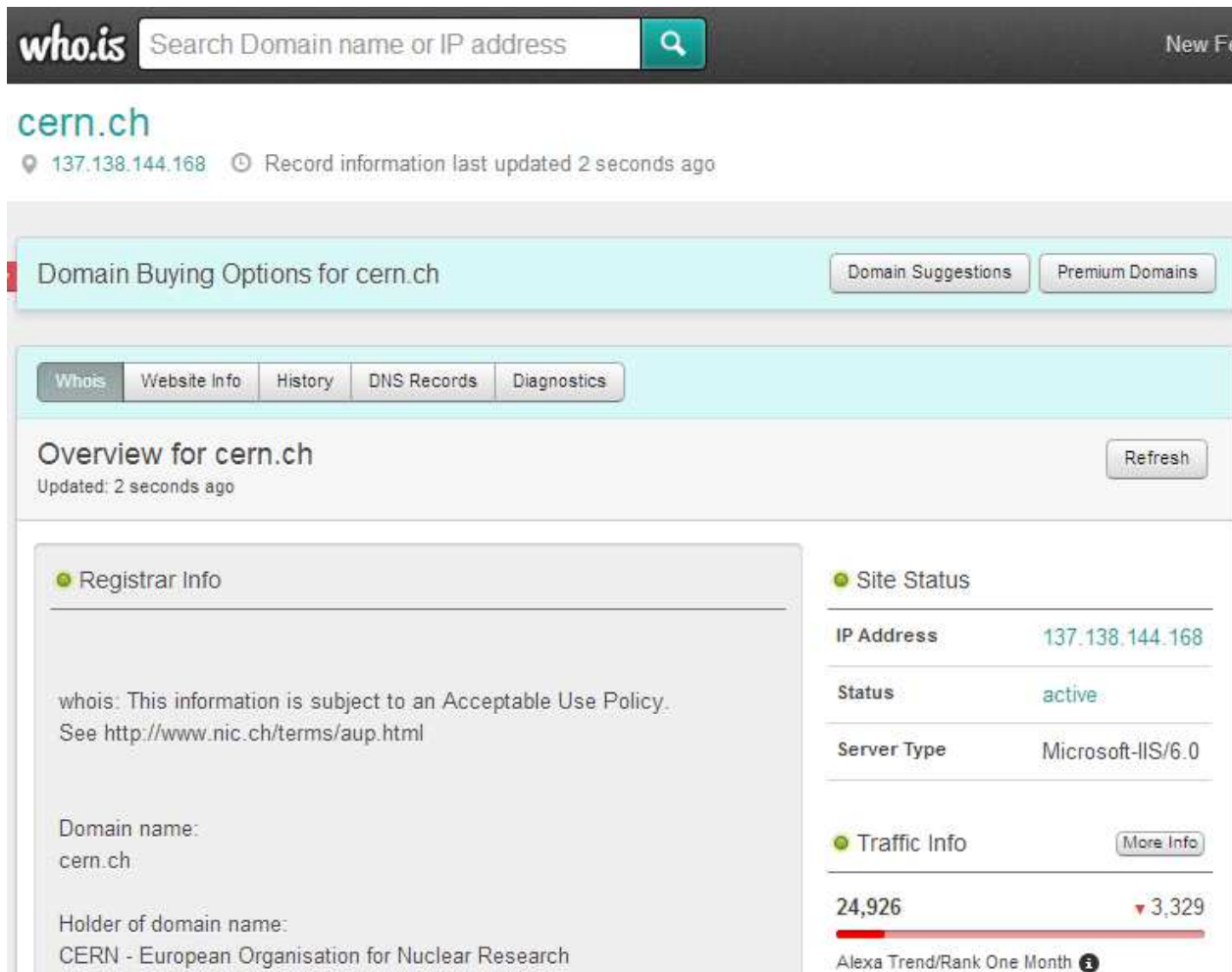
Your email:

CREATE ALERT

Manage your alerts

Passive - Whois, domain footprinting

- Whois data



The screenshot displays the who.is website interface for the domain cern.ch. At the top, there is a search bar with the text "Search Domain name or IP address" and a magnifying glass icon. Below the search bar, the domain "cern.ch" is highlighted in blue, with its IP address "137.138.144.168" and a note "Record information last updated 2 seconds ago" displayed below it. The main content area is divided into several sections:

- Domain Buying Options for cern.ch**: Includes buttons for "Domain Suggestions" and "Premium Domains".
- Navigation Tabs**: "Whois" (selected), "Website Info", "History", "DNS Records", and "Diagnostics".
- Overview for cern.ch**: Updated 2 seconds ago, with a "Refresh" button.
- Registrar Info**: A section with a warning message: "whois: This information is subject to an Acceptable Use Policy. See http://www.nic.ch/terms/aup.html". Below this, it lists "Domain name: cern.ch" and "Holder of domain name: CERN - European Organisation for Nuclear Research".
- Site Status**: A section with the following details:
 - IP Address: 137.138.144.168
 - Status: active
 - Server Type: Microsoft-IIS/6.0
- Traffic Info**: A section with a "More Info" button and a bar chart showing "24,926" (with a downward arrow and "3,329" below it) for "Alexa Trend/Rank One Month".

Passive – Whois, domain footprinting

- Regional Internet registries (RIRs)

RIPE
NCC
RIPE NETWORK COORDINATION CENTRE

RIPE Database | Database Support | DNS | Statistics & Analytics | Projects

NRTM (Mirroring) • Stats • FAQ: RIPE Database • Whois • Tools • Syncupdates • Webupdates

You are here: Home > Data & Tools > RIPE Database > Query

RIPE Database Query

Search details:

You can specify up to five comma separated terms: ?

137.138.144.168

By submitting this form you explicitly express your agreement with the [RIPE Database Terms and Conditions](#)

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-GFN
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

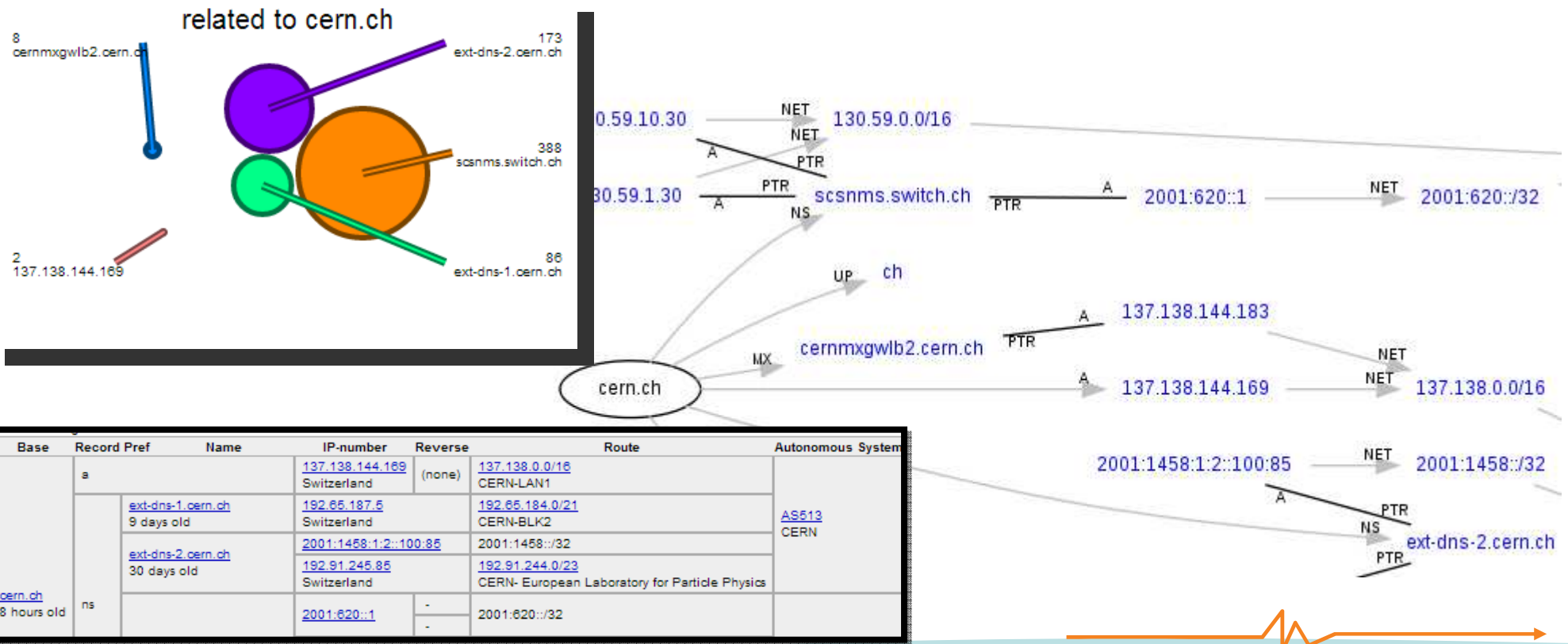
organisation:     ORG-CEOf1-RIPE
org-name:         CERN - European Organization for Nuclear Research
org-type:         LIR
address:          CERN IT department - CS group CERN CH-1211 Geneva 23
                  SWITZERLAND
phone:            +41 22 76 74417
fax-no:           +41 22 76 77155
admin-c:          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

Result Summary Records **Graph** Shared Whois Blacklists Analysis Contact

cern.ch Google™ Custom Search



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.
```

```
route:      137.138.0.0/16
descr:     CERN-LAN1
origin:    AS513
org:       ORG-CEOf1-RIPE
mnt-by:    AS513-MNT
mnt-lower: CERN-MNT
mnt-routes: CERN-MNT
source:    RIPE # Filtered
```

```
organisation: ORG-CEOf1-RIPE
org-name:     CERN - European Organization for Nuclear
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
```

```
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



GOOGLE HACKING-DATABASE
Welcome to the google hacking database

We call them 'googledorks': Inept or foolish people as revealed by fools, you've found the center of the Google Hacking Universe

Search Google Docs

Category:

Latest Google Hacking Entries

| Date | Title | |
|------------|---|--------------------------------|
| 2013-02-05 | runtimevar softwareVersion= | |
| 2013-02-05 | site:login.*.* | |
| 2013-02-05 | inurl:/control/userimage.html | |
| 2013-02-05 | ext:xml ("proto=prpl-" "prpl-ya... | |
| 2013-02-05 | ext:gnucash | |
| 2013-02-05 | filetype:inc OR filetype:bak OR filetype:old mysql... | |
| 2012-12-31 | inurl:admin intext:username= AND email= AND passwo... | Files containing juicy info |
| 2012-12-31 | you really should fix this security hole by settin... | Pages containing login portals |
| 2012-12-31 | intext:SQL syntax & inurl:index.php?id & ... | Vulnerable Servers |
| 2012-12-31 | inurl:/wp-content/w3tc/dbcache/ | Vulnerable Servers |

Google

Web Images Maps Shopping More Search tools

About 67 results (0.10 seconds)

[\[XLS\] Email - Alphaweb1](#)
[alphaweb1.net/admin/docs/2005web_business.xls](#)
 File Format: Microsoft Excel - [View as HTML](#)
 9, bwade@cameronpierce.com, User ID: bwade, **Password:** xlmnlkmg. 10, www.web2mail.com ... 12, info@manywaters.net, UID:info1mwm **PASS:** ManyWaters4 39, **Username:** cgems, user id: artel5 (A-R-T-E-L-5). 40, **Password:** gems12 ...

[\[XLS\] Groups for User Accounts - BlackBerry](#)
[docs.blackberry.com/.../admin/.../BlackBerry_Pushcast_Software_Us...](#)
 File Format: Microsoft Excel - [View as HTML](#)
 1, FIRST NAME, LAST NAME, **E-MAIL ADDRESS**, USERID, **USERNAME**, STATUS, **PASSWORD**, GROUPID, GROUPID, ROLEID, ROLEID, MANAGES ALL ...

Passive - Vulnerability databases

- Vulnerability databases

EXPLOIT DATABASE

Currently Archiving **21257** Exploits
Updated (CVE And Archive): **Sun Mar 3 2013**

HOME BLOG GHDB ABOUT REMOTE LOCAL WEB DOS SHELLCODE PAPERS SEARCH SUBMIT

The Exploit Data

The Exploit Database (EDB) - an ultimate repository of vulnerable software. A great resource for vulnerability researchers, and security professionals. Collect exploits from submittals and store them in one, easy to navigate database.



Sponsored by
DHS National Cyber Security Division/US-CERT

NIST
National Institute of Standards and Technology

National Vulnerability Database
automating vulnerability management, security measurement, and compliance checking

| | | | | | | |
|-----------------|------------|----------------------|--------------------|----------------|------------|-----------------|
| Vulnerabilities | Checklists | 800-53/800-53A | Product Dictionary | Impact Metrics | Data Feeds | Statistics |
| Home | SCAP | SCAP Validated Tools | SCAP Events | About | Contact | Vendor Comments |

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance checking.

National Vulnerability Database Version 2.2

NVD is the U.S. government repository of standards based vulnerability management data represented using the [Security Content Automation Protocol \(SCAP\)](#). This data enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics.

Active – Network, service footprinting

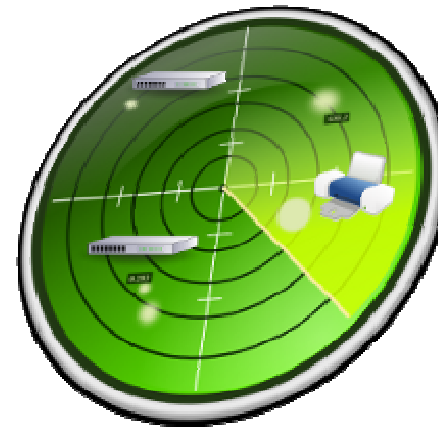
- Active host identification:
 - ping sweep, list scan

```
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

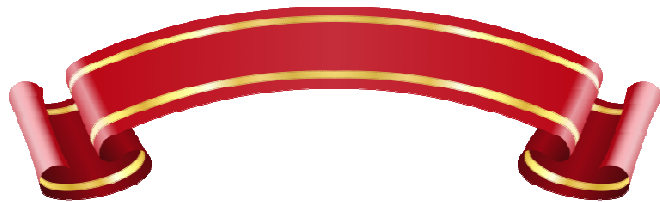
- Traceroute



```
root@ubul004-64:/# 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 fingerprinting

- Banner grabbing



```
root@ubul004-64:/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@ubul004-64:/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 cernmxgwl2.cern.ch Microsoft ESMTTP 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
```

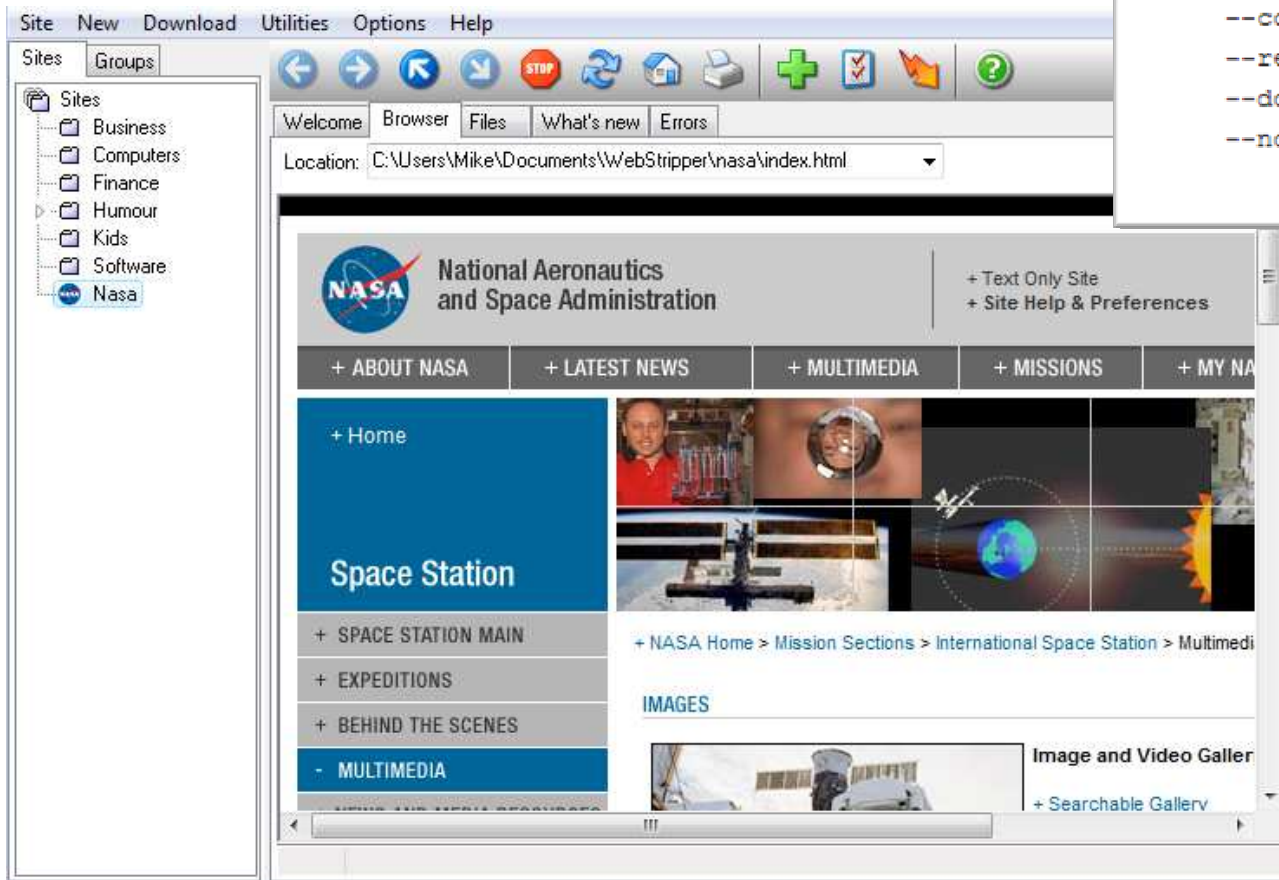
Active - DNS footprinting

- 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: /*mnu=-1$
Disallow: /*mnu=0$
Disallow: /*mnu=1$

```

| Origin | |
|--------------------|-------------------|
| Authors | Jack the Ripper |
| Last saved by | |
| Revision number | |
| Version number | 1.5 |
| Program name | Google docs |
| Company | Oil Company |
| Manager | Helge Lund |
| Content created | 2013.02.12. 10:21 |
| Date last saved | 2013.03.05. 16:57 |
| Last printed | |
| Total editing time | |



| vondelpark.jpg Properties | |
|--|------------------------------|
| General Security Details Previous Versions | |
| Property | Value |
| Digital zoom | |
| EXIF version | 0221 |
| GPS | |
| Latitude | 52; 21; 26.03200000000066... |
| Longitude | 4; 51; 49.717000000000553 |
| Altitude | 0 |
| File | |
| Name | vondelpark.jpg |

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 ESMTTP id 1UctKU-000BNY-35 ; Tue, 05 Mar 2013 16:58:58 +0200
Received: from localhost (localhost [127.0.0.1])
    by pumpis2.latnet.lv (Postfix) with ESMTTP 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 ESMTTP 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 ESMTTP 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



Target modeling

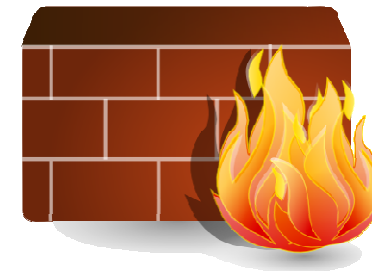
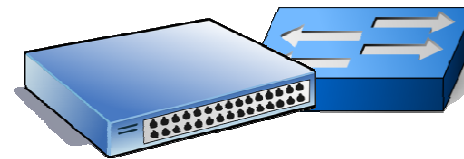
- Vulnerability identification and testing



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



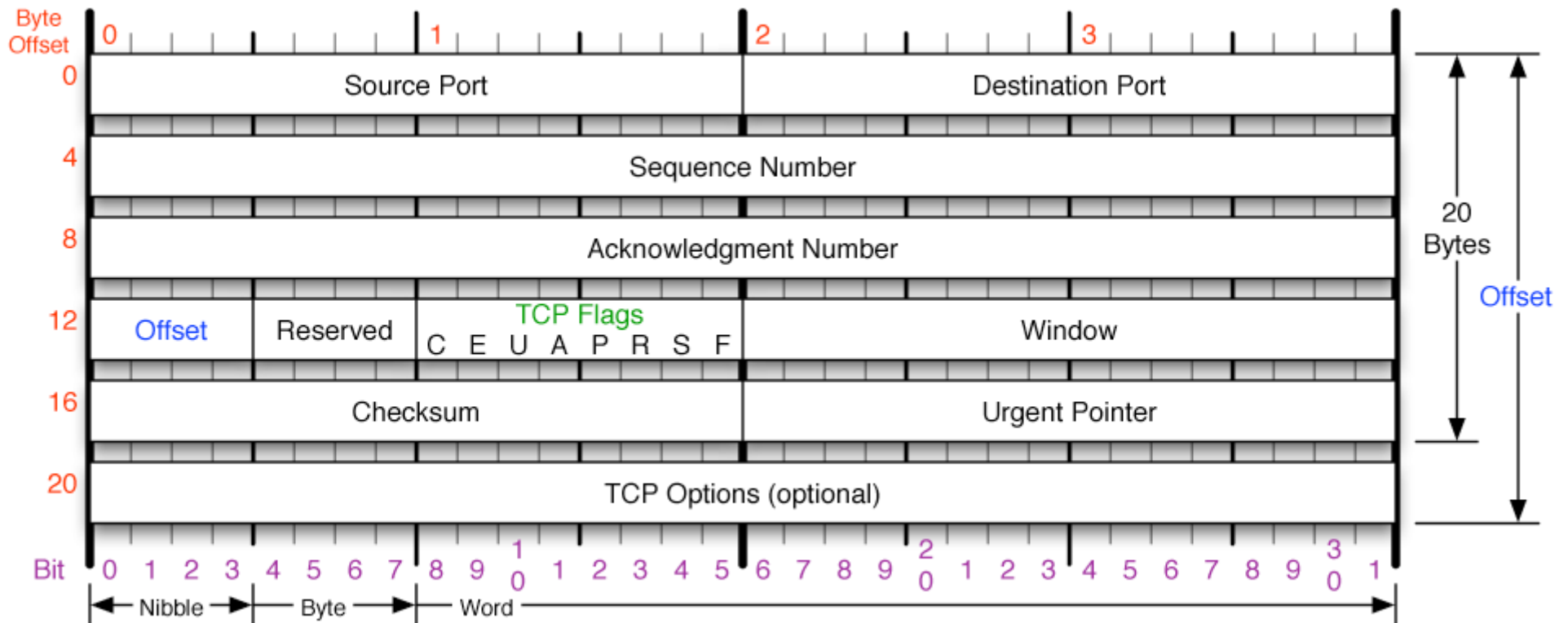
Network models and protocols

- 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



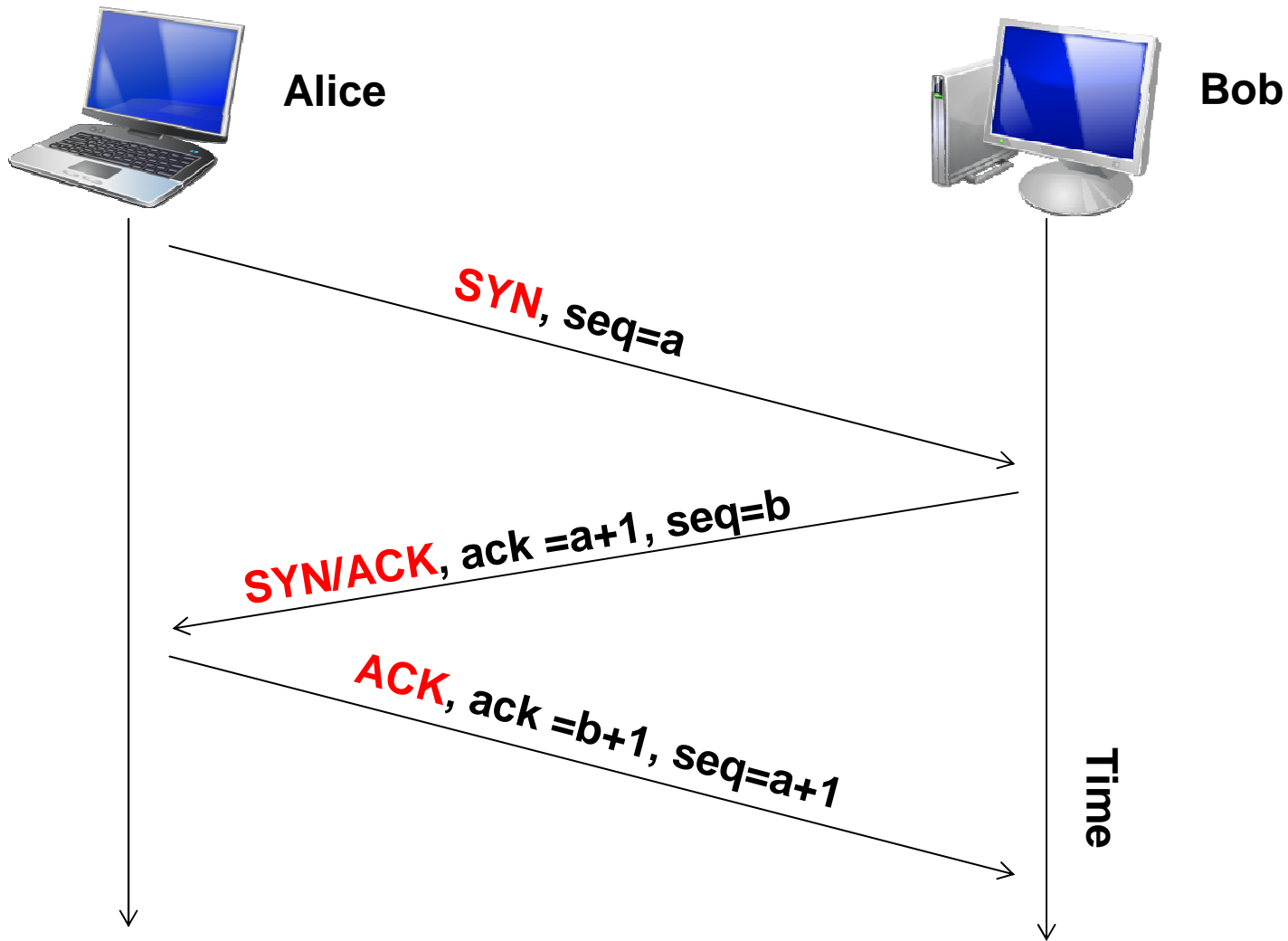
Protocol structure

- 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



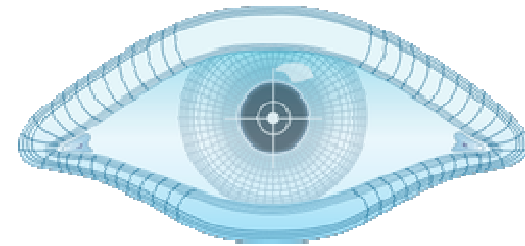
Scanning approach

- 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



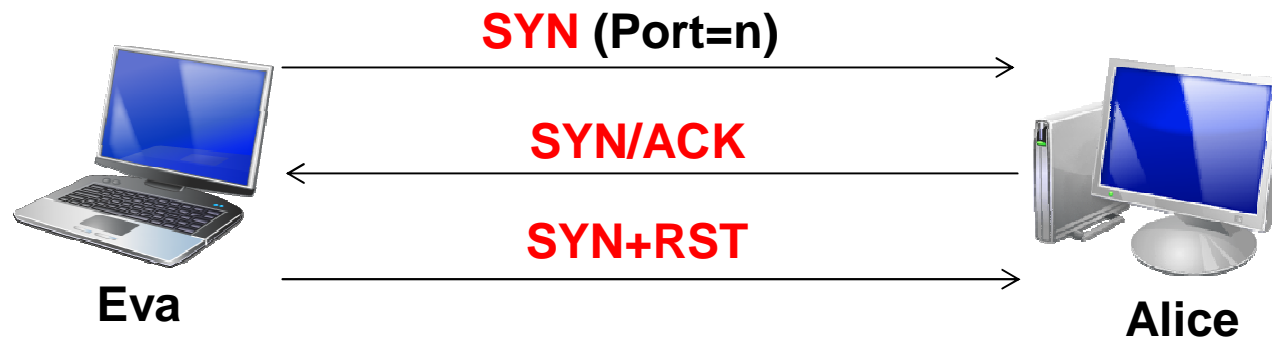
Scan types

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



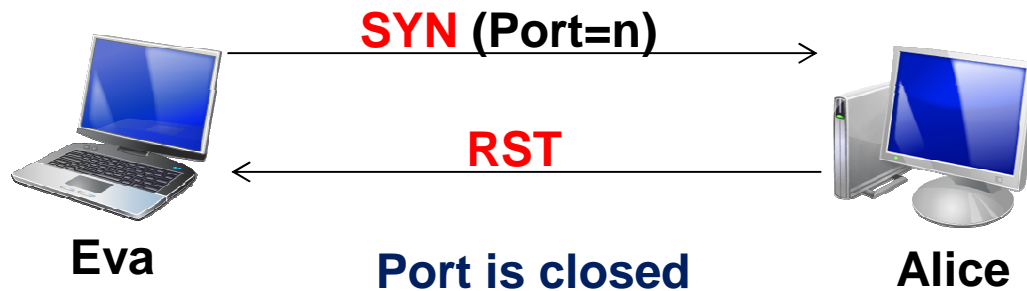
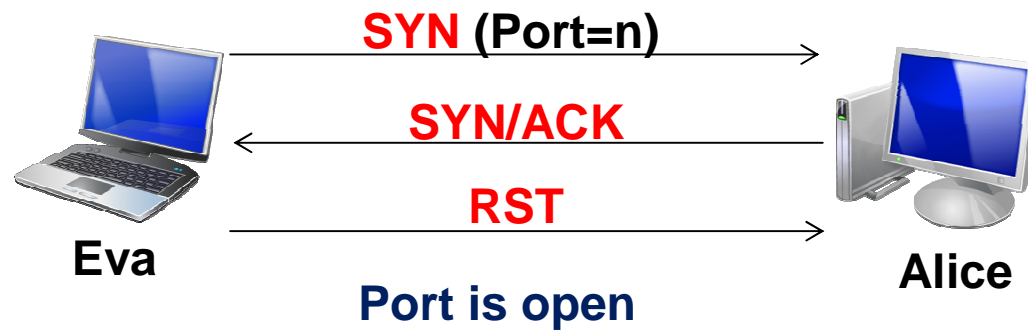
Normal scan

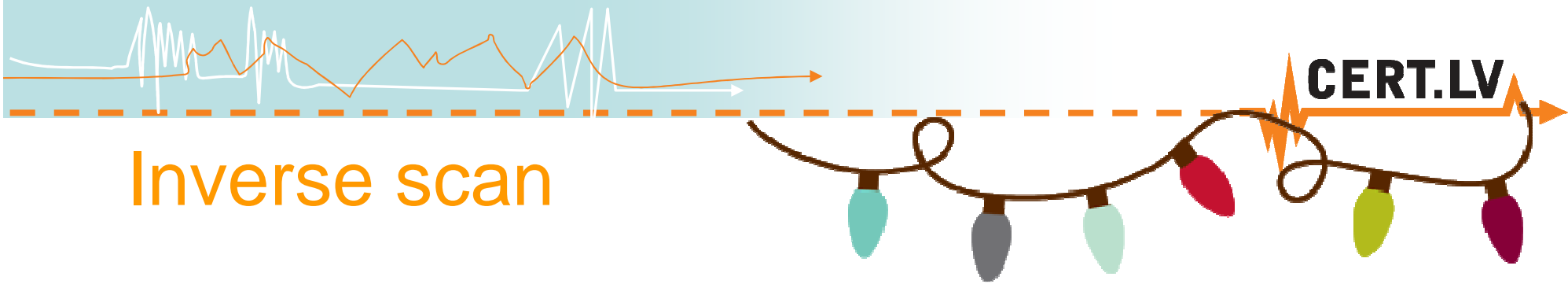
- TCP connect scan (full-open)



Normal scan

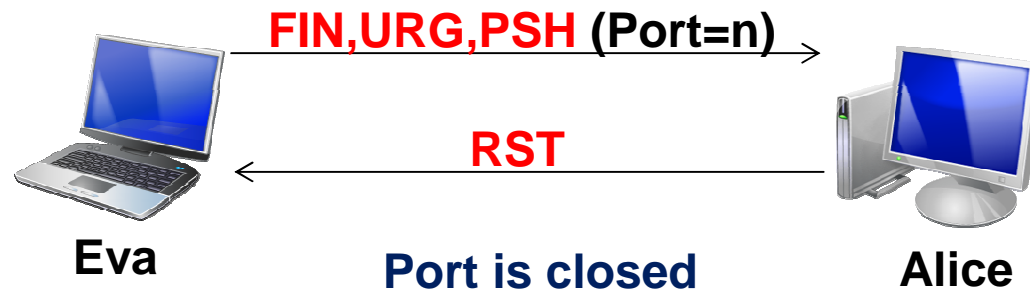
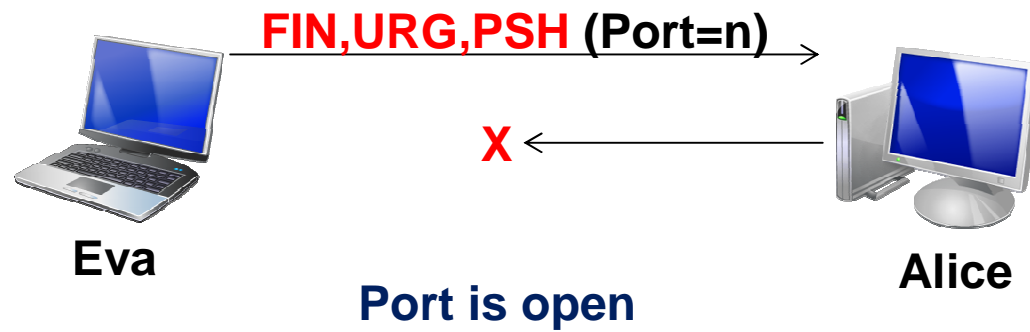
- SYN stealth scan (half-open)





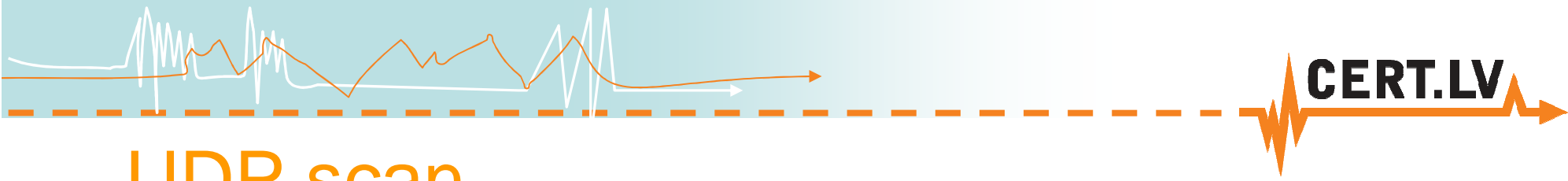
Inverse scan

- Xmas scan

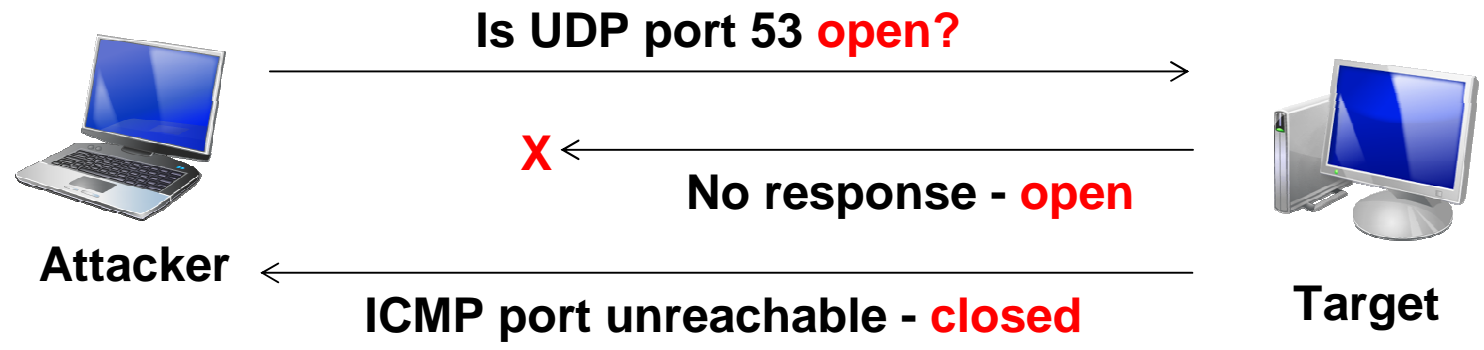


Works against RFC793 TCP/IP compliant OS!





UDP scan



ICMP echo and List scan

- ICMP echo
 - «ping» hosts on network
- List scan
 - do a DNS resolution on hosts



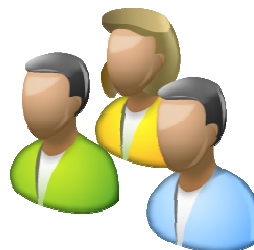
Enumeration

- 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

- SMTP enumeration:
 - SMTP address list enumeration

```
lletotajs@ubuntu:/etc/bind$ telnet oilcompany.tk 25
Trying 85.254.250.85...
Connected to oilcompany.tk.
Escape character is '^]'.
220 OILcompany ESMTF 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 cernmxgwl2.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
```


Vulnerability exploitation

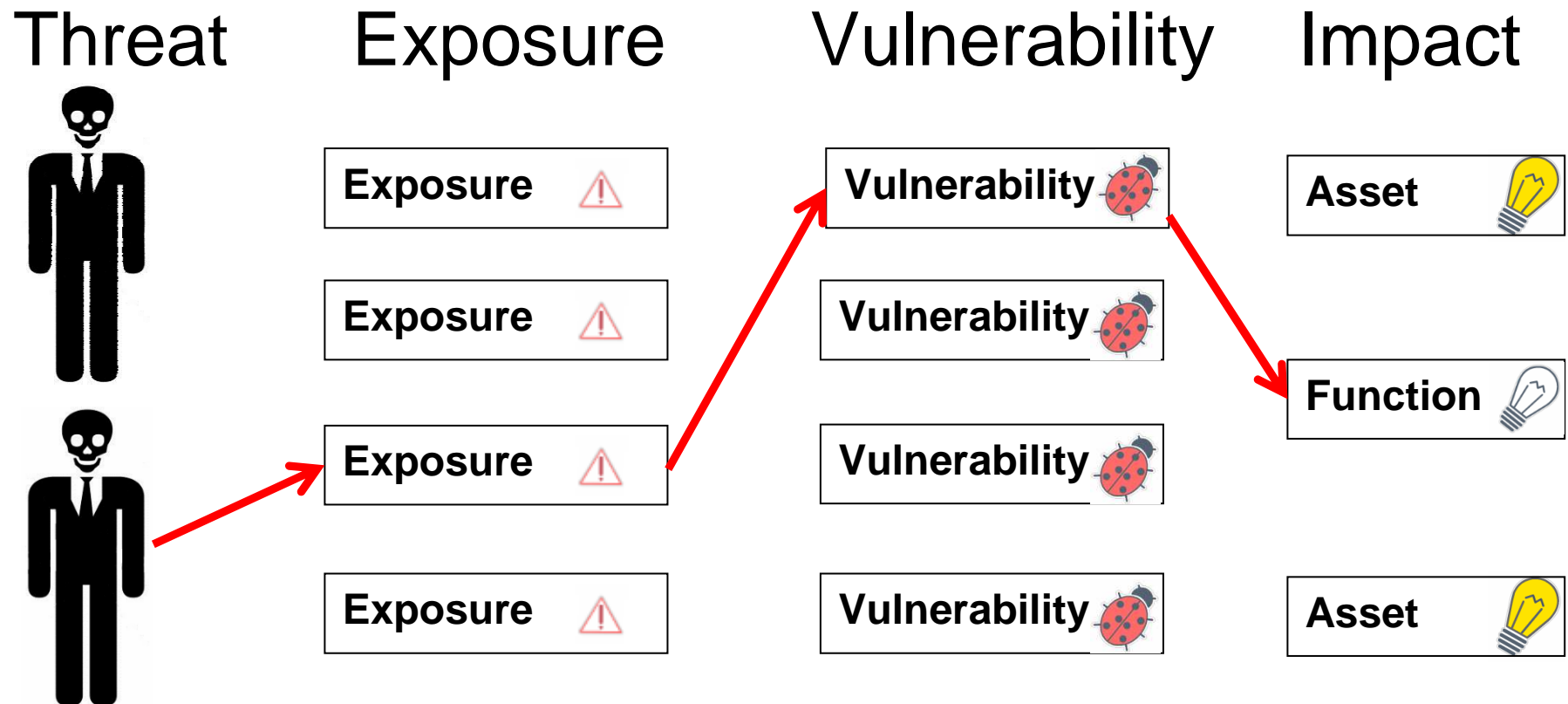
Exploit databases

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

The screenshot displays the top navigation bar of the Security Database website, featuring the logo "SECURITY DATABASE BEFORE IT COMES UPON YOU" and a menu with links for HOME, SERVICES, ALERTS, RESSOURCES, BLOG, and ABOUT US. Below the navigation bar is the "CVSS Calculator" section. On the left, there is a "CVSS Base Score : Not Defined" label next to a horizontal color scale bar ranging from green to red. On the right, a blue information box contains the text: "The CVSS Calculator can be used [Freely](#) via our vDNA API. For more informations, check [here](#)".

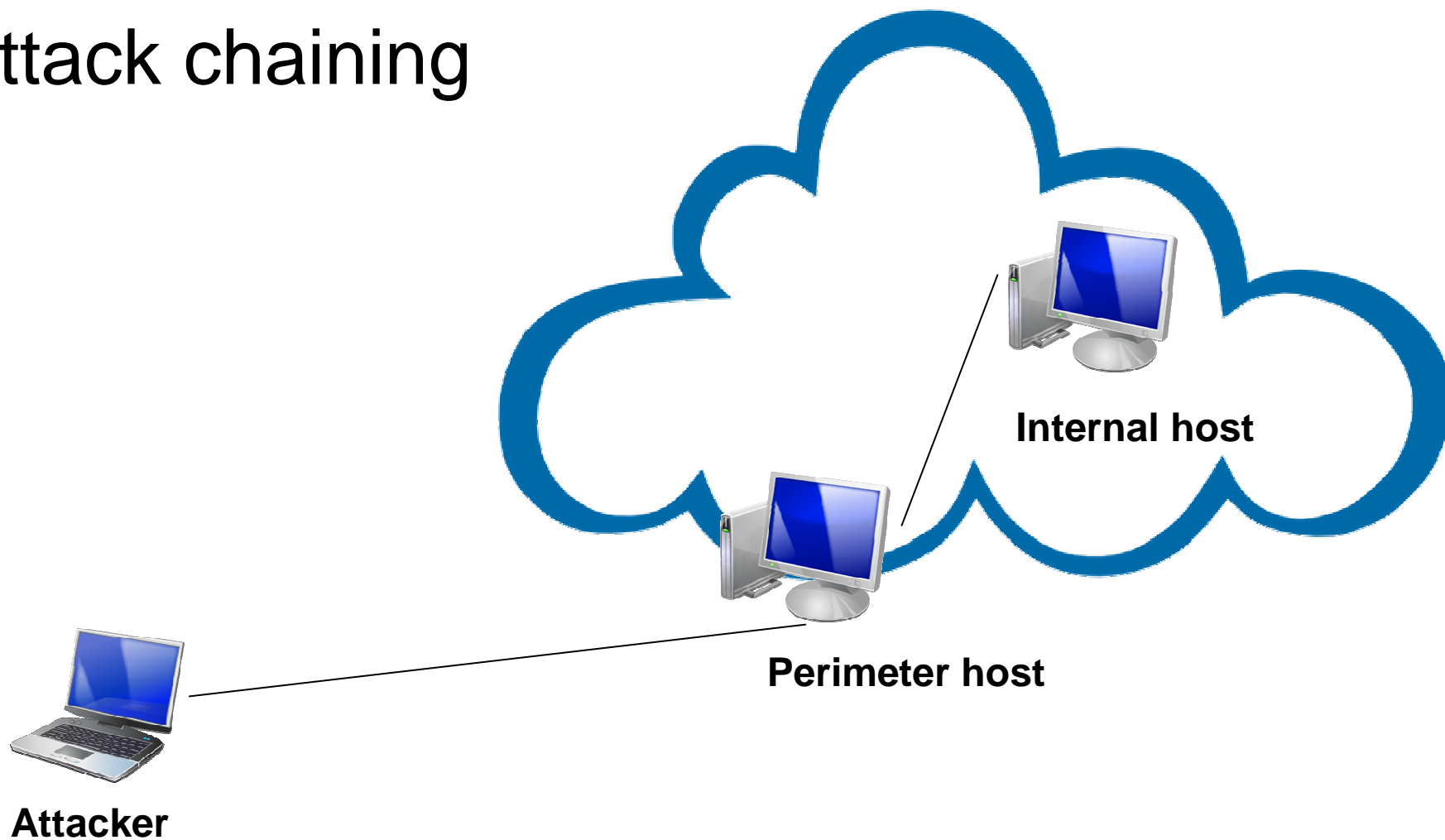
Attack staging

- 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

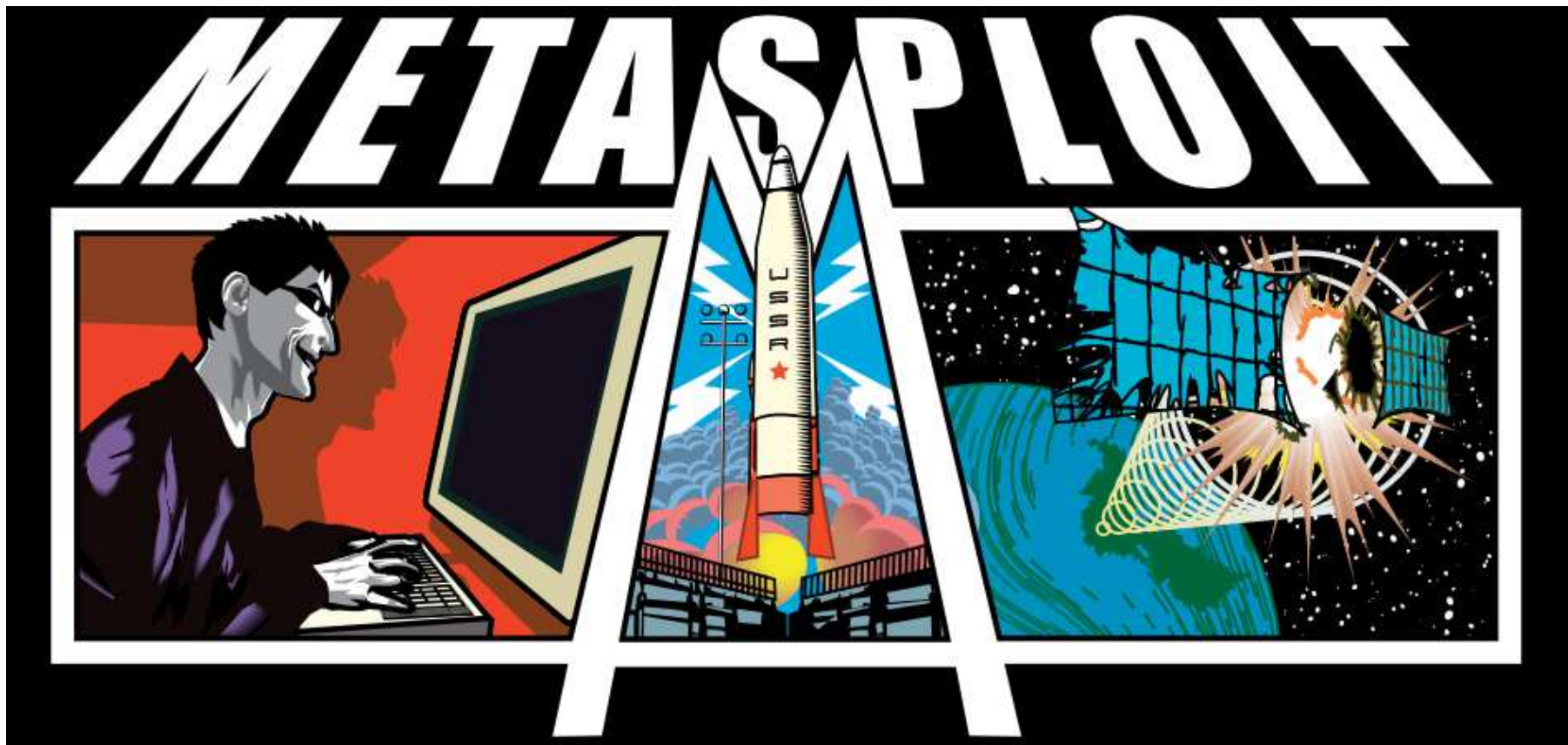
- Shellcode
 - code executed in target system

```
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\x04xcd\x80"  
"\x31\xc0\x31\xdb\x31\xc9\xb0\x17xcd\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\x0bxcd\x80\x31\xc0\xb0\x01xcd\x80";
```

- Wrapper
 - Means of delivering shellcode to target system

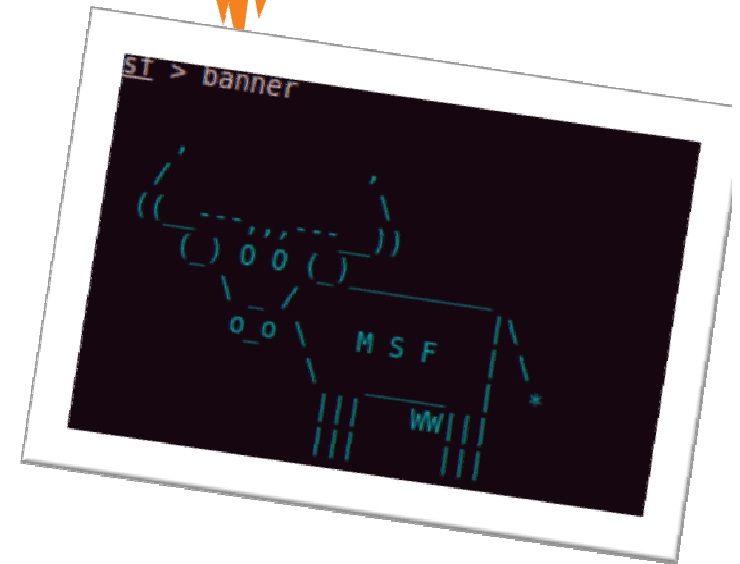
Metasploit

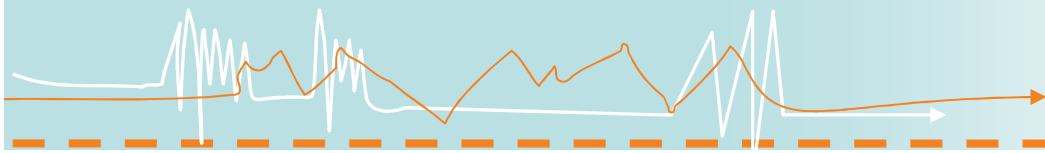
- What is Metasploit?



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**

