11. Penetration Testing

Prof. Dr. Marc Rennhard
Institut für angewandte Informationstechnologie InIT
ZHAW School of Engineering
rema@zhaw.ch

Content

- Introduction to Penetration Testing
- Different phases of a penetration test including methods and tools that can be applied
  - Footprinting
  - Scanning
  - Analysis of Scanning Results
  - Finding and Exploiting Vulnerabilities

Goals

- You know what penetration tests are and have learned the basics to perform one yourself
- You know the methods and tools used during a penetration test and know what information the tools can deliver

Software Security (SSI)

Introduction to Penetration Testing

Penetration Testing (1)

- Security testing can mean different things:
  - Review of the security architecture (e.g. using threat modeling)
  - Analyse source code with respect to security
  - Automated security scans
  - Hand-on assessment using manual and semi-automated methods
  - Testing the security awareness of employees by performing social engineering attacks
  - …
- One specific type of security test is a penetration test
  - A penetration test serves to analyse the entire or parts of the IT-environment of a company with the goal to find and exploit vulnerabilities
  - It "simulates" the behaviour of an attacker
    - The spent effort and detected vulnerabilities are an indication of the effort an attacker would have to invest spend to achieve a similar results

Penetration Testing (2)

- Depending on the information given to the tester beforehand, one distinguishes between black-, white-, or grey-box tests
- Black-box test: The tester gets very little information, e.g. just a company name or a range of IP addresses
- White-box test: The tester gets lots of internal information, which may include:
  - Internal system documentation, operation manuals, source code
  - User accounts with different authorisation levels
- In practice, grey-box tests are most frequently used, so the tester gets some but not all information
  - E.g. some user accounts but no additional internal system information

Penetration Testing (3)

Phases of a penetration test:

- Preparation phase: define scope (not discussed here)
- Footprinting: collecting relevant information about the target environment
- Scanning: examine the target networks and hosts in more detail
- Analysis of scanning results: identify the systems that one will attempt to compromise during the following phase
- Finding and exploiting vulnerabilities: identify vulnerabilities and demonstrate proof-of-concept or "real" exploits
- Reporting: Prepare a written report and a presentation, including concrete recommendations (not discussed here)

Software Security (SSI)

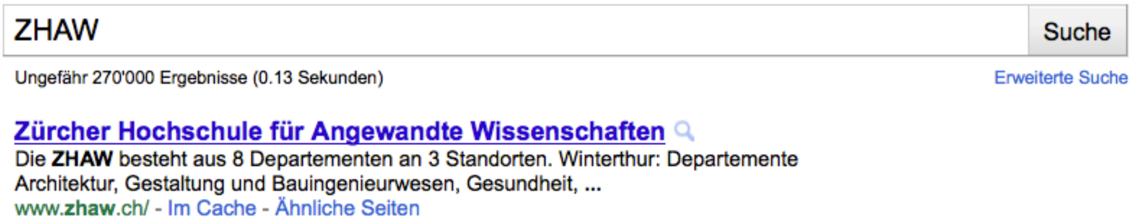
Footprinting

Footprinting

- Footprinting means collecting relevant information of the target and generating a profile of the target's Internet / intranet presence
- Footprinting is the first step a security tester (or attacker) performs when attacking / analysing a target
- The necessary footprinting activities depend on how much information is already available or how focussed the analysis should be
  - One extreme is starting with a company name only
  - The other extreme is being restricted to one or a few specific systems from the beginning and having detailed information about the systems
- What information are we interested in?
  - Domain names, IP address blocks, contact persons
  - Interesting systems (hostnames, IP addresses), internal system configurations

Footprinting – Getting Domain Names

- The first thing to do is getting the domain name(s) of the company
- This can be easily achieved using any search engine



ZHAW

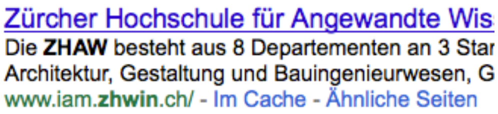
Ungefähr 270'000 Ergebnisse (0.13 Sekunden)

Zürcher Hochschule für Angewandte Wissenschaften

Die **ZHAW** besteht aus 8 Departementen an 3 Standorten. Winterthur: Departemente Architektur, Gestaltung und Bauingenieurwesen, Gesundheit, ...

www.**zhaw**.ch/ - Im Cache - Ähnliche Seiten

- Do not only look at the first entry, maybe there are additional domains available/used for a company name

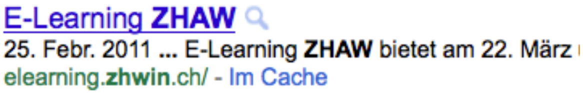


Zürcher Hochschule für Angewandte Wis

Die **ZHAW** besteht aus 8 Departementen an 3 Star

Architektur, Gestaltung und Bauingenieurwesen, G

www.iam.**zhwin**.ch/ - Im Cache - Ähnliche Seiten



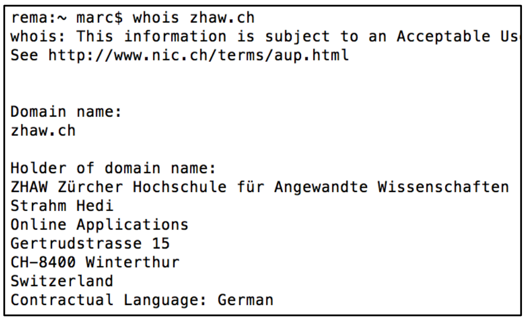
E-Learning ZHAW

25. Febr. 2011 ... E-Learning **ZHAW** bietet am 22. März

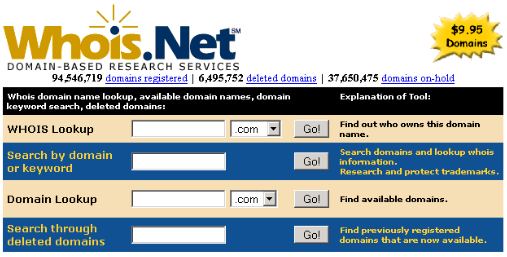
elearning.**zhwin**.ch/ - Im Cache

Footprinting – Whois (1)

- When the domain name is known, the Whois system can be used to get additional details
  - The Whois system is a distributed database, the servers are operated by the ISPs for their respective resources
  - There are various possibilities to query for information
- Command-line client
  - Simple to use
  - But primarily available for *ix systems
- Free web front-ends
  - Also easy to use, but they do not always deliver all information



```
rema:~ marc$ whois zhaw.ch
whois: This information is subject to an Acceptable Us
See http://www.nic.ch/terms/aup.html


Domain name:
zhaw.ch

Holder of domain name:
ZHAW Zürcher Hochschule für Angewandte Wissenschaften
Strahm Hedi
Online Applications
Gertrudstrasse 15
CH-8400 Winterthur
Switzerland
Contractual Language: German
```

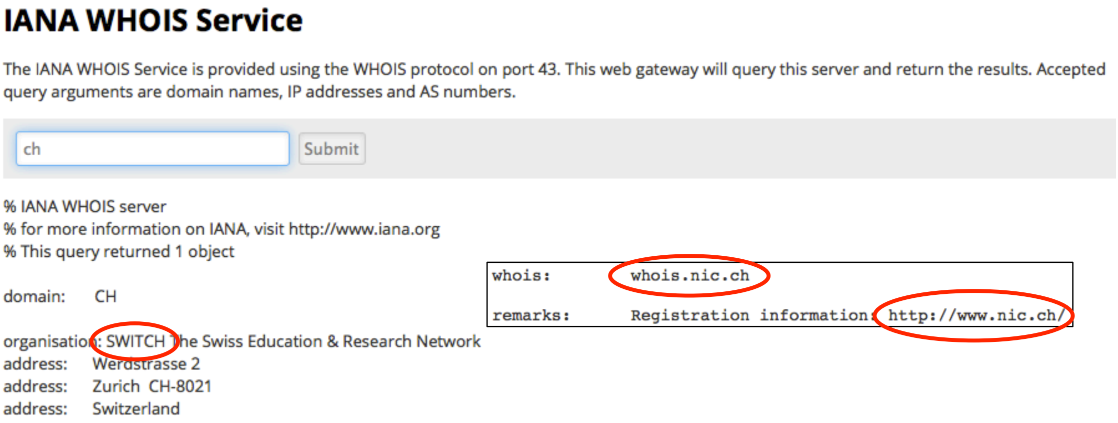


94,546,719 domains registered | 6,495,752 deleted domains | 37,650,475 domains on-hold

Whois domain name lookup, available domain names, domain keyword search, deleted domains:			Explanation of Tool:
WHOIS Lookup	.com	Go!	Find out who owns this domain name.
Search by domain or keyword		Go!	Search domains and lookup whois information. Research and protect trademarks.
Domain Lookup	.com	Go!	Find available domains.
Search through deleted domains		Go!	Find previously registered domains that are now available.

Footprinting – Whois (2)

- Most reliable option: directly querying the Whois databases
  - Start with the database for the top level domains (TLD): whois.iana.org
  - Query for a TLD (e.g. ch) and search for the responsible organisation



IANA WHOIS Service

The IANA WHOIS Service is provided using the WHOIS protocol on port 43. This web gateway will query this server and return the results. Accepted query arguments are domain names, IP addresses and AS numbers.

ch Submit

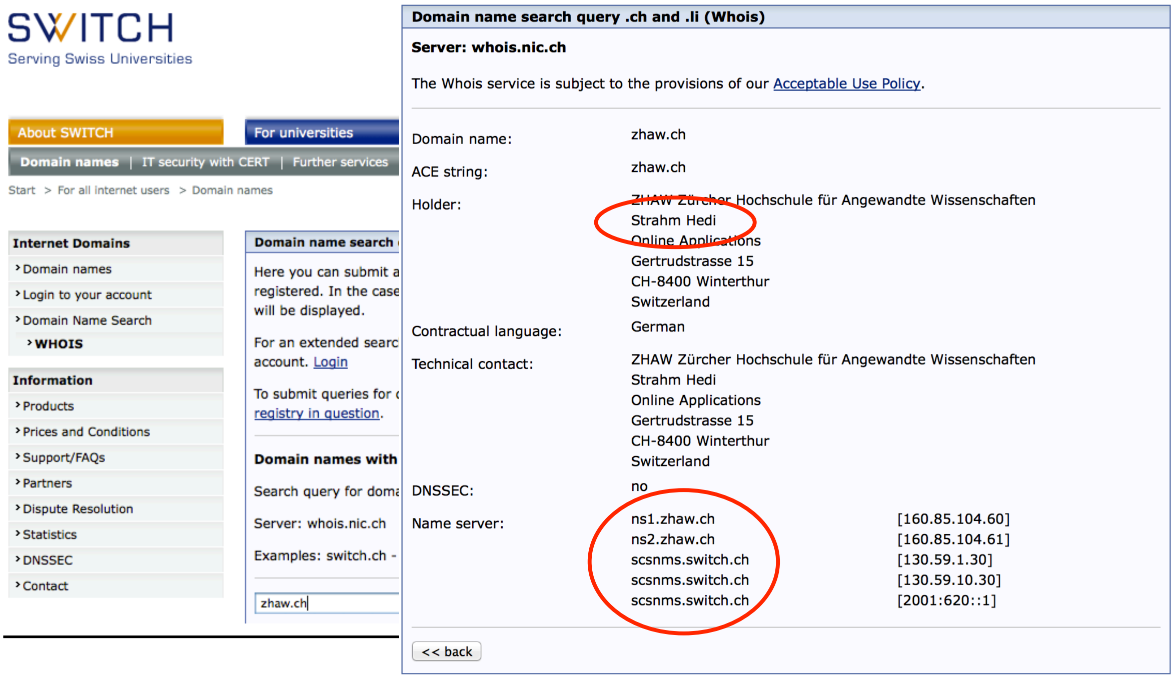
```
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

domain:       CH

organisation: SWITCH The Swiss Education & Research Network
address:      Werdstrasse 2
address:      Zurich  CH-8021
address:      Switzerland
```

```
whois:        whois.nic.ch

remarks:      Registration information: http://www.nic.ch/
```

  - For the ch TLD, this organisation is SWITCH and there is information about the Whois server and a URL for registration services

Footprinting – Whois (3)

- On http://www.nic.ch, a Whois search for zhaw.ch can be performed to find details such as contact persons, name servers etc.



SWITCH
Serving Swiss Universities

Domain name search

Here you can submit a
registered. In the case
will be displayed.

For an extended searc
account. Login

To submit queries for d
registry in question.

Domain names with

Search query for doma

Server: whois.nic.ch

Examples: switch.ch -

zhaw.ch

Domain name search query .ch and .li (Whois)

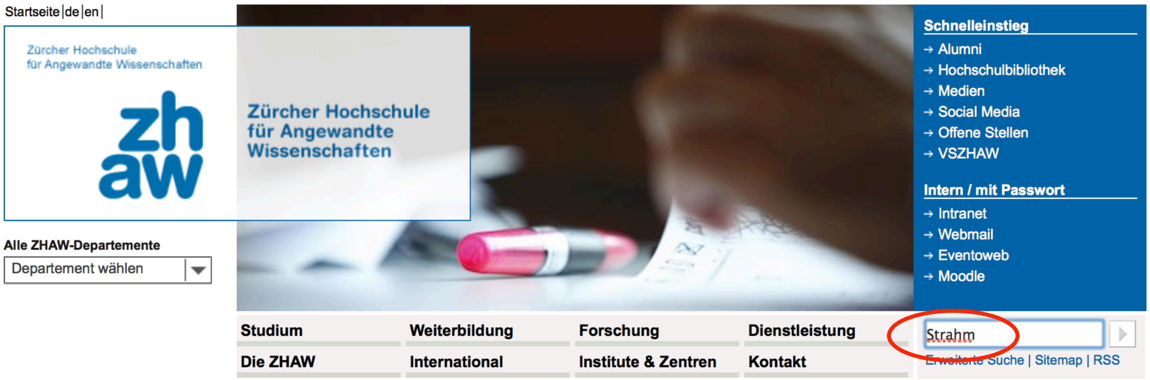
Server: whois.nic.ch

The Whois service is subject to the provisions of our Acceptable Use Policy.

```
Domain name:            zhaw.ch
ACE string:             zhaw.ch
Holder:                 ZHAW Zürcher Hochschule für Angewandte Wissenschaften
                        Strahm Hedi
                        Online Applications
                        Gertrudstrasse 15
                        CH-8400 Winterthur
                        Switzerland
Contractual language:   German
Technical contact:      ZHAW Zürcher Hochschule für Angewandte Wissenschaften
                        Strahm Hedi
                        Online Applications
                        Gertrudstrasse 15
                        CH-8400 Winterthur
                        Switzerland
DNSSEC:                 no
Name server:            ns1.zhaw.ch                    [160.85.104.60]
                        ns2.zhaw.ch                    [160.85.104.61]
                        scsnms.switch.ch               [130.59.1.30]
                        scsnms.switch.ch               [130.59.10.30]
                        scsnms.switch.ch               [2001:620::1]
```

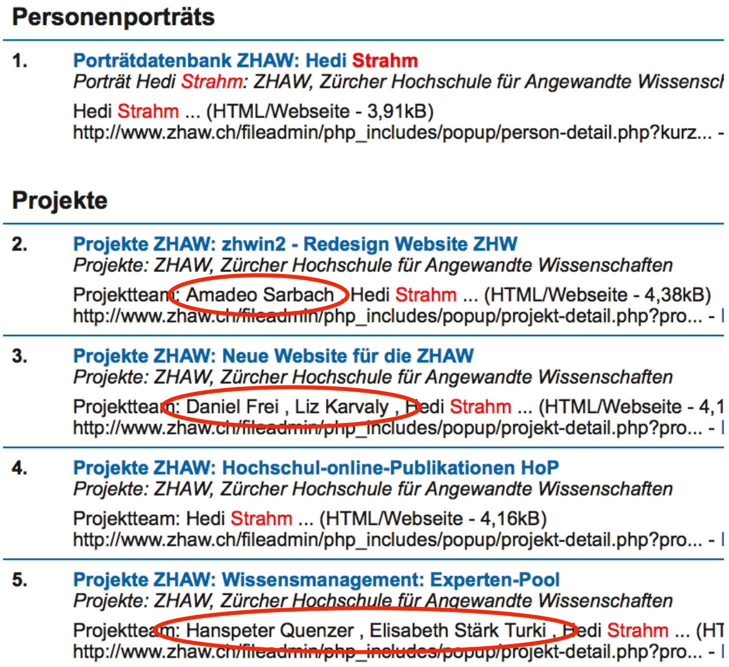
Footprinting – Browsing the Company Website (1)

- The company website itself can provide lots of interesting information, especially with respect to contact persons and their roles
- Example: look for search functions and enter the contact information received by the Whois query



Strahm

Footprinting – Browsing the Company Website (2)



Personenporträts

1. **Porträtdatenbank ZHAW: Hedi Strahm**
Porträt Hedi Strahm: ZHAW, Zürcher Hochschule für Angewandte Wissenscl
Hedi Strahm ... (HTML/Webseite - 3,91kB)
http://www.zhaw.ch/fileadmin/php_includes/popup/person-detail.php?kurz... -

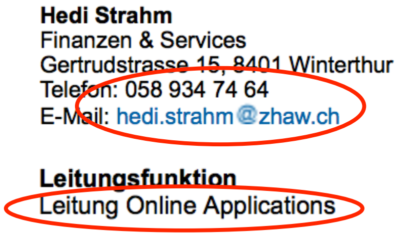
Projekte

2. **Projekte ZHAW: zhwin2 - Redesign Website ZHW**
Projekte: ZHAW, Zürcher Hochschule für Angewandte Wissenschaften
Projektteam: Amadeo Sarbach , Hedi Strahm ... (HTML/Webseite - 4,38kB)
http://www.zhaw.ch/fileadmin/php_includes/popup/projekt-detail.php?pro... - I

3. **Projekte ZHAW: Neue Website für die ZHAW**
Projekte: ZHAW, Zürcher Hochschule für Angewandte Wissenschaften
Projektteam: Daniel Frei , Liz Karvaly , Hedi Strahm ... (HTML/Webseite - 4,1
http://www.zhaw.ch/fileadmin/php_includes/popup/projekt-detail.php?pro... - I

4. **Projekte ZHAW: Hochschul-online-Publikationen HoP**
Projekte: ZHAW, Zürcher Hochschule für Angewandte Wissenschaften
Projektteam: Hedi Strahm ... (HTML/Webseite - 4,16kB)
http://www.zhaw.ch/fileadmin/php_includes/popup/projekt-detail.php?pro... - I

5. **Projekte ZHAW: Wissensmanagement: Experten-Pool**
Projekte: ZHAW, Zürcher Hochschule für Angewandte Wissenschaften
Projektteam: Hanspeter Quenzer , Elisabeth Stärk Turki , Hedi Strahm ... (HT
http://www.zhaw.ch/fileadmin/php_includes/popup/projekt-detail.php?pro... - I



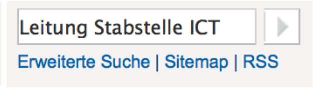
Hedi Strahm
Finanzen & Services
Gertrudstrasse 15, 8401 Winterthur
Telefon: 058 934 74 64
E-Mail: hedi.strahm@zhaw.ch

Leitungsfunktion
Leitung Online Applications

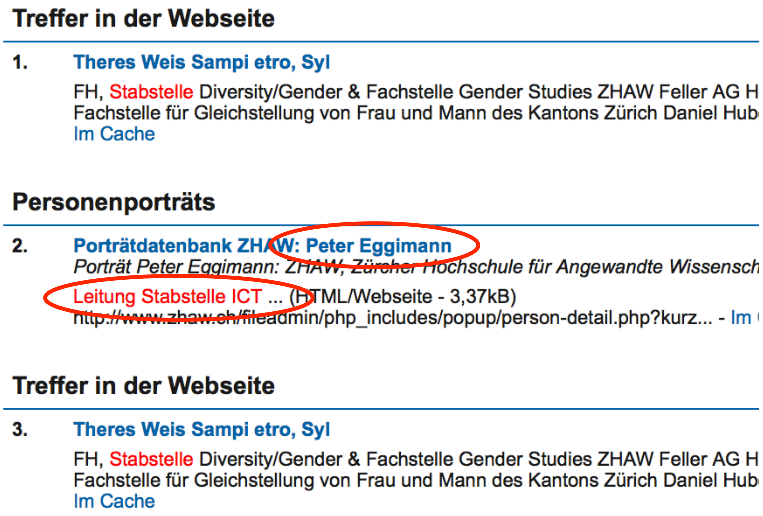
- So we have found additional information:
  - She has a leading position in ICT
  - We know her phone number and e-mail address
  - Valuable for social engineering attacks!
- And the search results deliver various additional, possibly interesting names

Footprinting – Browsing the Company Website (3)

- Searching for job functions is also helpful



Leitung Stabstelle ICT
Erweiterte Suche | Sitemap | RSS



Treffer in der Webseite

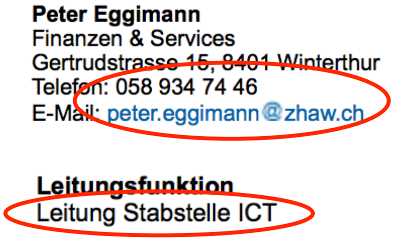
1. **Theres Weis Sampi etro, Syl**
FH, Stabstelle Diversity/Gender & Fachstelle Gender Studies ZHAW Feller AG H
Fachstelle für Gleichstellung von Frau und Mann des Kantons Zürich Daniel Hub
Im Cache

Personenporträts

2. **Porträtdatenbank ZHAW: Peter Eggimann**
Porträt Peter Eggimann: ZHAW, Zürcher Hochschule für Angewandte Wissensch
Leitung Stabstelle ICT ... (HTML/Webseite - 3,37kB)
http://www.zhaw.ch/fileadmin/php_includes/popup/person-detail.php?kurz... - Im

Treffer in der Webseite

3. **Theres Weis Sampi etro, Syl**
FH, Stabstelle Diversity/Gender & Fachstelle Gender Studies ZHAW Feller AG H
Fachstelle für Gleichstellung von Frau und Mann des Kantons Zürich Daniel Hub
Im Cache



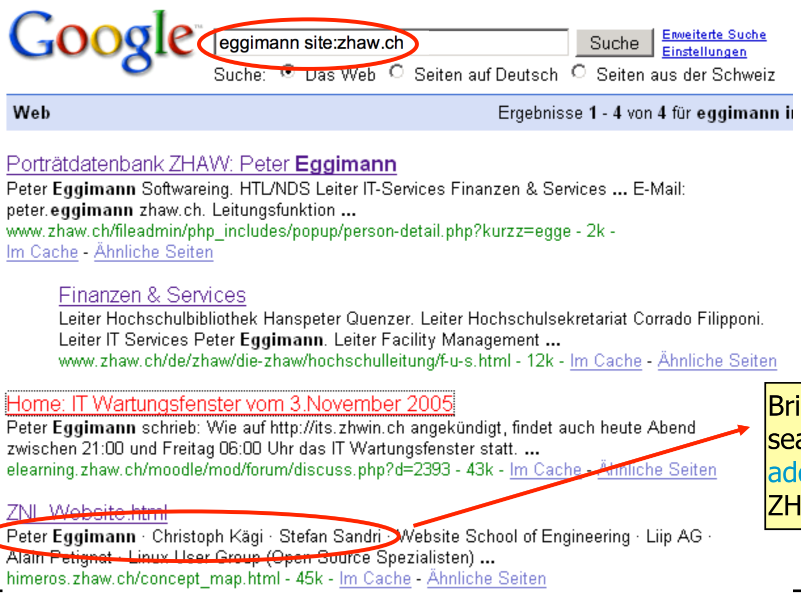
Peter Eggimann
Finanzen & Services
Gertrudstrasse 15, 8401 Winterthur
Telefon: 058 934 74 46
E-Mail: peter.eggimann@zhaw.ch

Leitungsfunktion
Leitung Stabstelle ICT

- That's another interesting person...

Footprinting – Using Search Engines (1)

- Search engines – especially Google – are powerful tools to find security-relevant information about a company
  - Using appropriate search options can reveal desired results


Google
eggimann site:zhaw.ch
Suche
Erweiterte Suche
Einstellungen
Suche: ● Das Web ○ Seiten auf Deutsch ○ Seiten aus der Schweiz
Web
Ergebnisse 1 - 4 von 4 für eggimann i

Porträtdatenbank ZHAW: Peter **Eggimann**
Peter **Eggimann** Softwareing. HTL/NDS Leiter IT-Services Finanzen & Services **...** E-Mail: peter.**eggimann** zhaw.ch. Leitungsfunktion **...**
www.zhaw.ch/fileadmin/php_includes/popup/person-detail.php?kurzz=egge - 2k -
Im Cache - Ähnliche Seiten

Finanzen & Services
Leiter Hochschulbibliothek Hanspeter Quenzer. Leiter Hochschulsekretariat Corrado Filipponi. Leiter IT Services Peter **Eggimann**. Leiter Facility Management **...**
www.zhaw.ch/de/zhaw/die-zhaw/hochschulleitung/f-u-s.html - 12k - Im Cache - Ähnliche Seiten

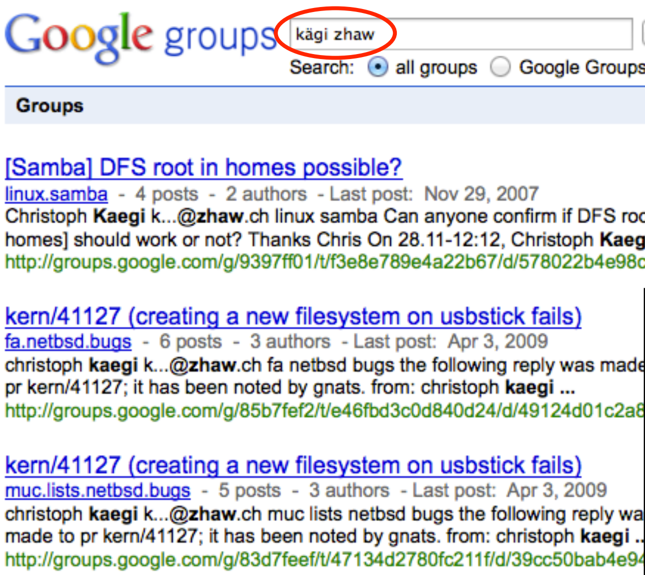
Home: IT Wartungsfenster vom 3.November 2005
Peter **Eggimann** schrieb: Wie auf http://its.zhwin.ch angekündigt, findet auch heute Abend zwischen 21:00 und Freitag 06:00 Uhr das IT Wartungsfenster statt. **...**
elearning.zhaw.ch/moodle/mod/forum/discuss.php?d=2393 - 43k - Im Cache - Ähnliche Seiten

ZNI_Website.html
Peter **Eggimann** · Christoph Kägi · Stefan Sandri · Website School of Engineering · Liip AG · Alain Petignat · Linux User Group (Open Source Spezialisten) **...**
himeros.zhaw.ch/concept_map.html - 45k - Im Cache - Ähnliche Seiten

Briefly analysing this search result reveals two additional members of the ZHAW ICT-Services

Footprinting – Using Search Engines (2)

- The Usenet or web forums provide a wealth of information as well
  - ...and IT personnel needing answers often disclose sensitive information

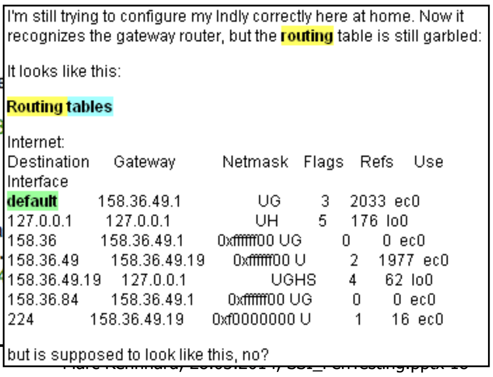


[Samba] DFS root in homes possible?
linux.samba - 4 posts - 2 authors - Last post: Nov 29, 2007
Christoph **Kaegi** k...@**zhaw**.ch linux samba Can anyone confirm if DFS root in [homes] should work or not? Thanks Chris On 28.11-12:12, Christoph **Kaegi** **...**
http://groups.google.com/g/9397ff01/t/f3e8e789e4a22b67/d/578022b4e98cc58f

kern/41127 (creating a new filesystem on usbstick fails)
fa.netbsd.bugs - 6 posts - 3 authors - Last post: Apr 3, 2009
christoph **kaegi** k...@**zhaw**.ch fa netbsd bugs the following reply was made pr kern/41127; it has been noted by gnats. from: christoph **kaegi** **...**
http://groups.google.com/g/85b7fef2/t/e46fbd3c0d840d24/d/49124d01c2a8

kern/41127 (creating a new filesystem on usbstick fails)
muc.lists.netbsd.bugs - 5 posts - 3 authors - Last post: Apr 3, 2009
christoph **kaegi** k...@**zhaw**.ch muc lists netbsd bugs the following reply wa made to pr kern/41127; it has been noted by gnats. from: christoph **kaegi** ..
http://groups.google.com/g/83d7feef/t/47134d2780fc211f/d/39cc50bab4e94

- May disclose internal technical details
- If we are lucky, even things such as (faulty) config files or routing tables:



I'm still trying to configure my Indly correctly here at home. Now it recognizes the gateway router, but the **routing** table is still garbled:

It looks like this:

Routing tables

```
Internet:
Destination     Gateway          Netmask    Flags    Refs    Use
Interface
default         158.36.49.1              UG        3    2033  ec0
127.0.0.1        127.0.0.1               UH        5     176  lo0
158.36          158.36.49.1     0xffffff00 UG       0       0  ec0
158.36.49        158.36.49.19    0xffffff00 U        2    1977  ec0
158.36.49.19     127.0.0.1                UGHS      4      62  lo0
158.36.84        158.36.49.1     0xffffff00 UG       0       0  ec0
224            158.36.49.19     0xf0000000 U        1      16  ec0
```

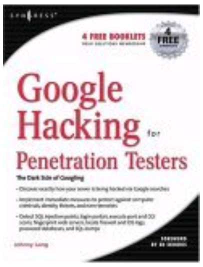
but is supposed to look like this, no?

Footprinting – Using Search Engines (3)

- Don’t restrict your Google search to names only, e.g.:
  - password site:zhaw.ch to get information about passwords
  - manual site:zhaw.ch to get internal technical documentation
  - “vulnerability report” site:zhaw.ch to get internal vulnerability reports (you never know...)

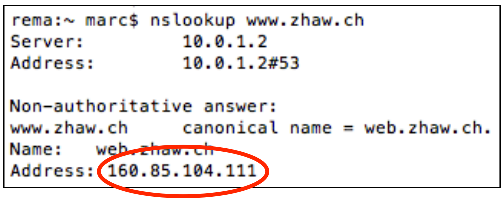
- It may be that Google reports a hit but the information is no longer available on the website
  - In this case you can try to access the version that was cached by Google
  - http://google.com/search?q=cache:www.zhaw.ch/de.html

- There’s in fact an entire website and a book (!) dedicated to such searches, also known as Google Hacking (http://johnny.ihackstuff.com)



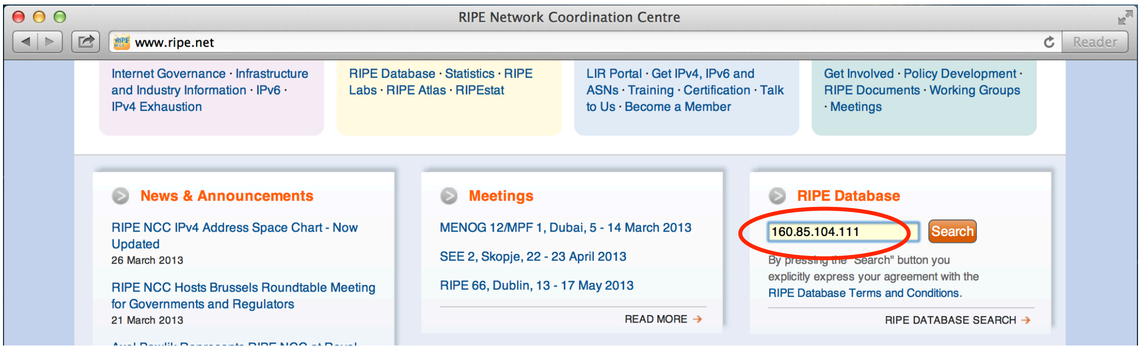
Footprinting – IP Range (1)

- Another question is the IP range used by the target company
  - IP ranges are assigned by the Regional Internet Registries (RIR)
  - ARIN for North America, RIPE for Europe etc.
- To search for the IP range of ZHAW, we just need one IP address of ZHAW
  - Can be done by, e.g. performing an nslookup



```
rema:~ marc$ nslookup www.zhaw.ch
Server:         10.0.1.2
Address:        10.0.1.2#53

Non-authoritative answer:
www.zhaw.ch     canonical name = web.zhaw.ch.
Name:   web.zhaw.ch
Address: 160.85.104.111
```

- Entering this IP address at http://www.ripe.net...


RIPE Network Coordination Centre
www.ripe.net
Reader
Internet Governance · Infrastructure and Industry Information · IPv6 · IPv4 Exhaustion
RIPE Database · Statistics · RIPE Labs · RIPE Atlas · RIPEstat
LIR Portal · Get IPv4, IPv6 and ASNs · Training · Certification · Talk to Us · Become a Member
Get Involved · Policy Development · RIPE Documents · Working Groups · Meetings
News & Announcements
Meetings
RIPE Database
Search
READ MORE →
RIPE DATABASE SEARCH →

RIPE NCC IPv4 Address Space Chart - Now Updated
26 March 2013

RIPE NCC Hosts Brussels Roundtable Meeting for Governments and Regulators
21 March 2013

MENOG 12/MPF 1, Dubai, 5 - 14 March 2013

SEE 2, Skopje, 22 - 23 April 2013

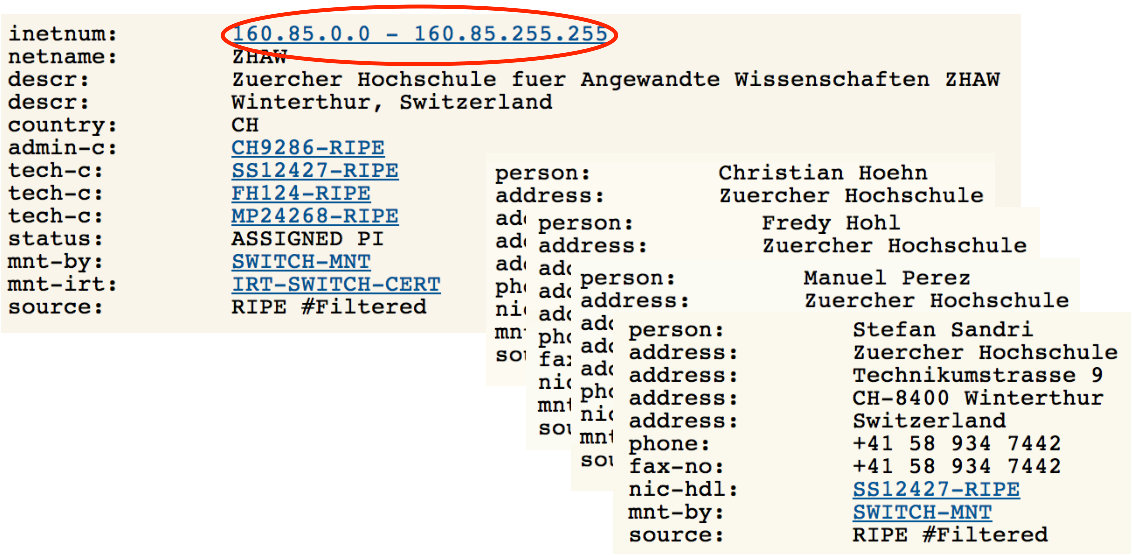
RIPE 66, Dublin, 13 - 17 May 2013

160.85.104.111

By pressing the "Search" button you explicitly express your agreement with the RIPE Database Terms and Conditions.

Footprinting – IP Range (2)

- ...delivers the information we are interested in
  - And in addition further information about contact persons



```
inetnum:        160.85.0.0 - 160.85.255.255
netname:        ZHAW
descr:          Zuercher Hochschule fuer Angewandte Wissenschaften ZHAW
descr:          Winterthur, Switzerland
country:        CH
admin-c:        CH9286-RIPE
tech-c:         SS12427-RIPE
tech-c:         FH124-RIPE
tech-c:         MP24268-RIPE
status:         ASSIGNED PI
mnt-by:         SWITCH-MNT
mnt-irt:        IRT-SWITCH-CERT
source:         RIPE #Filtered
```

```
person:         Christian Hoehn
address:        Zuercher Hochschule
```

```
person:         Fredy Hohl
address:        Zuercher Hochschule
```

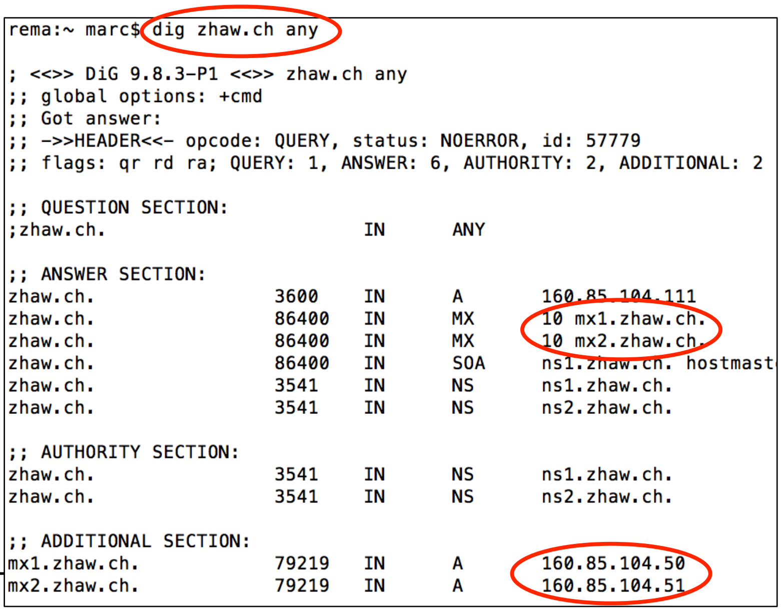
```
person:         Manuel Perez
address:        Zuercher Hochschule
```

```
person:         Stefan Sandri
address:        Zuercher Hochschule
address:        Technikumstrasse 9
address:        CH-8400 Winterthur
address:        Switzerland
phone:          +41 58 934 7442
fax-no:         +41 58 934 7442
nic-hdl:        SS12427-RIPE
mnt-by:         SWITCH-MNT
source:         RIPE #Filtered
```

Footprinting – Information from Name Servers (1)

- Name servers contain hostname to IP address mappings for some company hosts
  - This provides information about used hosts and the hostnames may hint at the purpose of the hosts

- A good start is the dig command line tool (*ix)
  - Which – in this case – reveals the hostnames and IP addresses of the mail servers

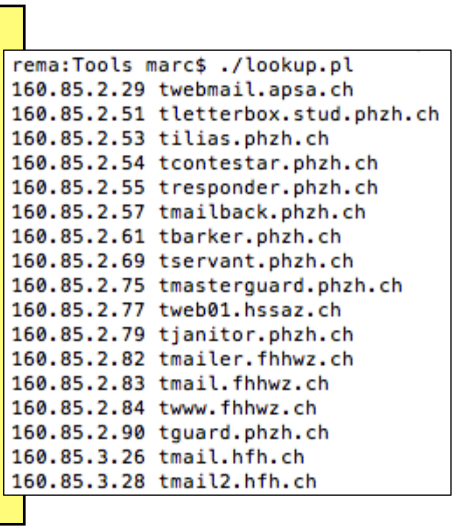


```
rema:~ marc$ dig zhaw.ch any

; <<>> DiG 9.8.3-P1 <<>> zhaw.ch any
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57779
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;zhaw.ch.                       IN      ANY

;; ANSWER SECTION:
zhaw.ch.                3600    IN      A       160.85.104.111
zhaw.ch.                86400   IN      MX      10 mx1.zhaw.ch.
zhaw.ch.                86400   IN      MX      10 mx2.zhaw.ch.
zhaw.ch.                86400   IN      SOA     ns1.zhaw.ch. hostmast
zhaw.ch.                3541    IN      NS      ns1.zhaw.ch.
zhaw.ch.                3541    IN      NS      ns2.zhaw.ch.

;; AUTHORITY SECTION:
zhaw.ch.                3541    IN      NS      ns1.zhaw.ch.
zhaw.ch.                3541    IN      NS      ns2.zhaw.ch.

;; ADDITIONAL SECTION:
mx1.zhaw.ch.            79219   IN      A       160.85.104.50
mx2.zhaw.ch.            79219   IN      A       160.85.104.51
```

Footprinting – Information from Name Servers (2)

- Knowing the IP range, one can easily get all hostnames and IP addresses using inverse DNS lookups
- E.g. with a perl script for class B (/16) networks:

```
#! /usr/bin/perl

Use Socket;

$b_net = "160.85";

for ($i=0; $i<255; $i++) {
  for ($j=0; $j<255; $j++) {
    $ip = "$b_net.$i.$j";
    $ipaddr = inet_aton($ip);
    $name = gethostbyaddr($ipaddr, AF_INET);
    if ($name) {
      print "${ip}\t${name}\n";
    }
  }
}
```



```
rema:Tools marc$ ./lookup.pl
160.85.2.29 twebmail.apsa.ch
160.85.2.51 tletterbox.stud.phzh.ch
160.85.2.53 tilias.phzh.ch
160.85.2.54 tcontestar.phzh.ch
160.85.2.55 tresponder.phzh.ch
160.85.2.57 tmailback.phzh.ch
160.85.2.61 tbarker.phzh.ch
160.85.2.69 tservant.phzh.ch
160.85.2.75 tmasterguard.phzh.ch
160.85.2.77 tweb01.hssaz.ch
160.85.2.79 tjanitor.phzh.ch
160.85.2.82 tmailer.fhhwz.ch
160.85.2.83 tmail.fhhwz.ch
160.85.2.84 twww.fhhwz.ch
160.85.2.90 tguard.phzh.ch
160.85.3.26 tmail.hfh.ch
160.85.3.28 tmail2.hfh.ch
```

Footprinting – Summary

- Footprinting is the first step performed by a penetration tester (or attacker)
- After footprinting, you know general, IT-related information about the target company
  - Domain names
  - IP ranges
  - Technical contact persons
  - Hostnames and IP addresses of some systems
- If you are lucky, you have discovered additional valuable information
  - E.g. Critical information (internal system configurations etc.) that has been voluntarily disclosed by the employees
- There are further information sources
  - Social Networks (Facebook, XING...), Blogs, Twitter, 123People…

Scanning

Scanning

Based on the footprinting results, the target company's networks and hosts are examined in more detail during scanning

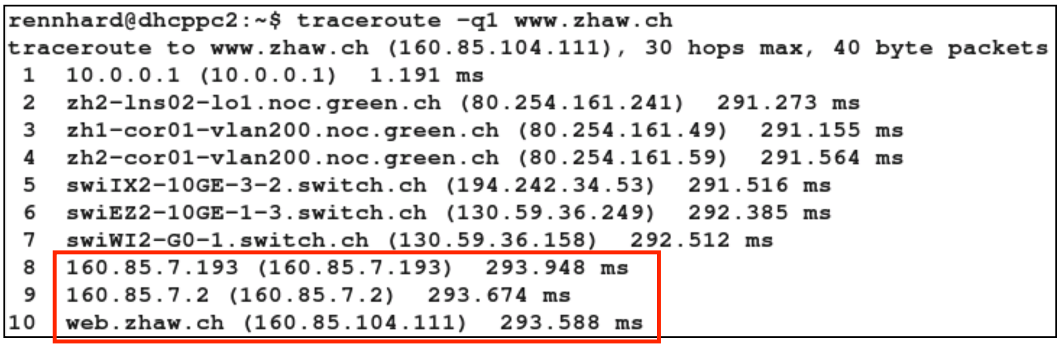
- Determine the network structure, especially when analysing larger environments
- Find hosts that are reachable / visible by the tester
  - Depends on the location of the tester, e.g. inside or outside the company
- Analyse the hosts in detail
  - Identify operating systems
  - Determine services running on the hosts and the corresponding software products
  - This can give hints at possible vulnerabilities present on a target host
- Perform vulnerability scans
  - To identify possible vulnerabilities on hosts that may be exploited

Scanning – Network Structure (1)

- Determining the network structure is relevant when analysing larger environments
  - Provides information about interesting "areas" of a network (e.g. a DMZ)
    - Helps to prioritize which areas to analyse in detail during host scanning
  - It may provide "attack paths" into the network
    - Assume you want to compromise an important host that cannot be reached directly from your location
    - Knowing the network structure helps to identify other, maybe less protected hosts, which may then be used to get better access to the target host
- Traditionally, traceroute is the tool of choice to analyse the network structure
  - Lists all hops (IP addresses) to the target system
  - There are different traceroute variants that use UDP or ICMP packets
  - On *ix systems, UDP is usually the default and ICMP can be used with the `-I` option
  - Its a good idea to use both options, especially if one is not successful

Scanning – Network Structure (2)

- Let's start with a traceroute to www.zhaw.ch

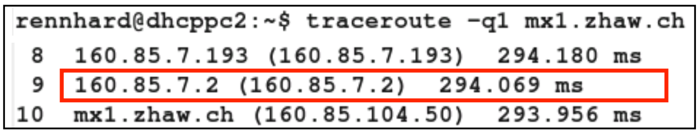


```
rennhard@dhcppc2:~$ traceroute -q1 www.zhaw.ch
traceroute to www.zhaw.ch (160.85.104.111), 30 hops max, 40 byte packets
 1  10.0.0.1 (10.0.0.1)  1.191 ms
 2  zh2-lns02-lo1.noc.green.ch (80.254.161.241)  291.273 ms
 3  zh1-cor01-vlan200.noc.green.ch (80.254.161.49)  291.155 ms
 4  zh2-cor01-vlan200.noc.green.ch (80.254.161.59)  291.564 ms
 5  swiIX2-10GE-3-2.switch.ch (194.242.34.53)  291.516 ms
 6  swiEZ2-10GE-1-3.switch.ch (130.59.36.249)  292.385 ms
 7  swiWI2-G0-1.switch.ch (130.59.36.158)  292.512 ms
 8  160.85.7.193 (160.85.7.193)  293.948 ms
 9  160.85.7.2 (160.85.7.2)  293.674 ms
10  web.zhaw.ch (160.85.104.111)  293.588 ms
```

- What do we learn here?
  - Three ZHAW hosts are visible
  - Probably two routers and the web server itself
  - So we have learned a small part of the internal network structure and IP addresses
  - But we have no clue yet about network sizes etc.

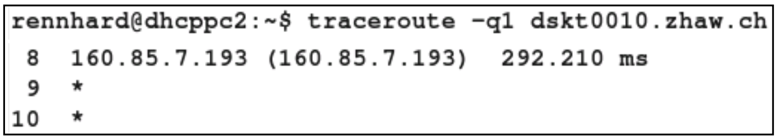
Scanning – Network Structure (3)

- traceroute to mx1.zhaw.ch



```
rennhard@dhcppc2:~$ traceroute -q1 mx1.zhaw.ch
 8  160.85.7.193 (160.85.7.193)  294.180 ms
 9  160.85.7.2 (160.85.7.2)  294.069 ms
10  mx1.zhaw.ch (160.85.104.50)  293.956 ms
```

  - www and mx1 sit behind the same router
  - It's likely (though not guaranteed) that the hosts are in the same network
  - If they are in the same network, their IP addresses (104.50 and 104.111) tell us that the network is at least a /25 network
- Traceroute has its limits with firewalls that filter UDP or ICMP packets

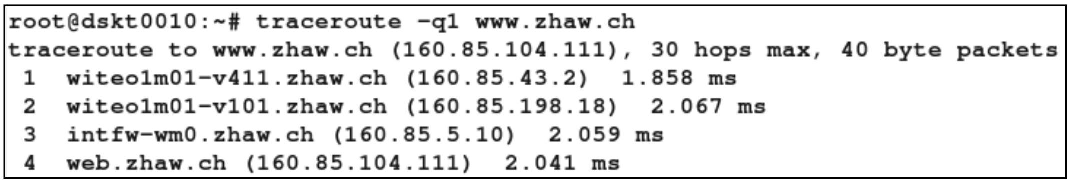


```
rennhard@dhcppc2:~$ traceroute -q1 dskt0010.zhaw.ch
 8  160.85.7.193 (160.85.7.193)  292.210 ms
 9  *
10  *
```

  - An asterisk indicates that no answer was received from the host
  - So all we learn here is that "some filtering takes place" on the hop following 160.85.7.193

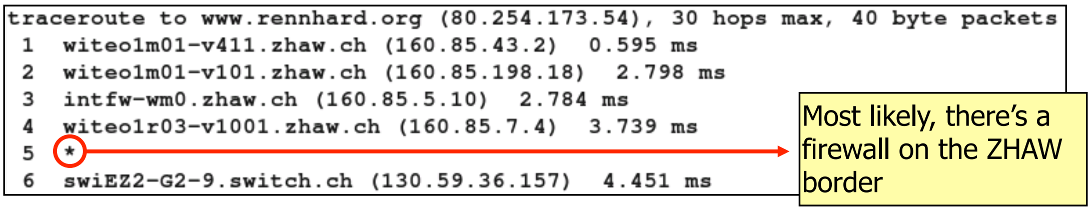
Scanning – Network Structure (4)

- If possible, don't forget to scan from internal hosts
  - Maybe you have access to one or have compromised one



```
root@dskt0010:~# traceroute -q1 www.zhaw.ch
traceroute to www.zhaw.ch (160.85.104.111), 30 hops max, 40 byte packets
 1  witeo1m01-v411.zhaw.ch (160.85.43.2)  1.858 ms
 2  witeo1m01-v101.zhaw.ch (160.85.198.18)  2.067 ms
 3  intfw-wm0.zhaw.ch (160.85.5.10)  2.059 ms
 4  web.zhaw.ch (160.85.104.111)  2.041 ms
```

- Also, scan from internal to external:



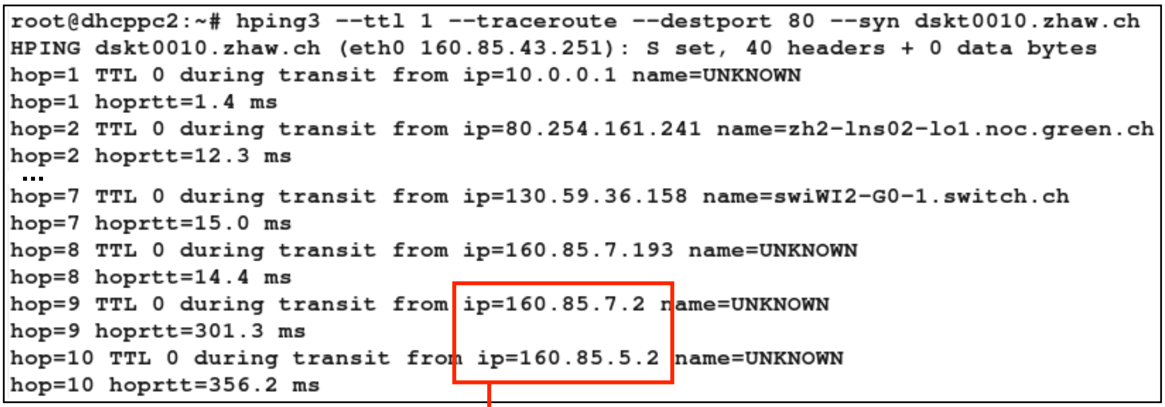
```
traceroute to www.rennhard.org (80.254.173.54), 30 hops max, 40 byte packets
 1  witeo1m01-v411.zhaw.ch (160.85.43.2)  0.595 ms
 2  witeo1m01-v101.zhaw.ch (160.85.198.18)  2.798 ms
 3  intfw-wm0.zhaw.ch (160.85.5.10)  2.784 ms
 4  witeo1r03-v1001.zhaw.ch (160.85.7.4)  3.739 ms
 5  *
 6  swiEZ2-G2-9.switch.ch (130.59.36.157)  4.451 ms
```

Most likely, there's a firewall on the ZHAW border

- Over time, this gives more and more information about hosts, routers and firewalls

Scanning – Network Structure (5)

- An even more flexible tool than traceroute is hping3
  - Allows to specify protocol (ICMP/UDP/TCP) and destination port to be used
- Example: trace the route to dskt0010.zhaw.ch using TCP port 80 SYN probes:
  - TCP port 80 is more likely to get through firewalls than UDP or ICMP

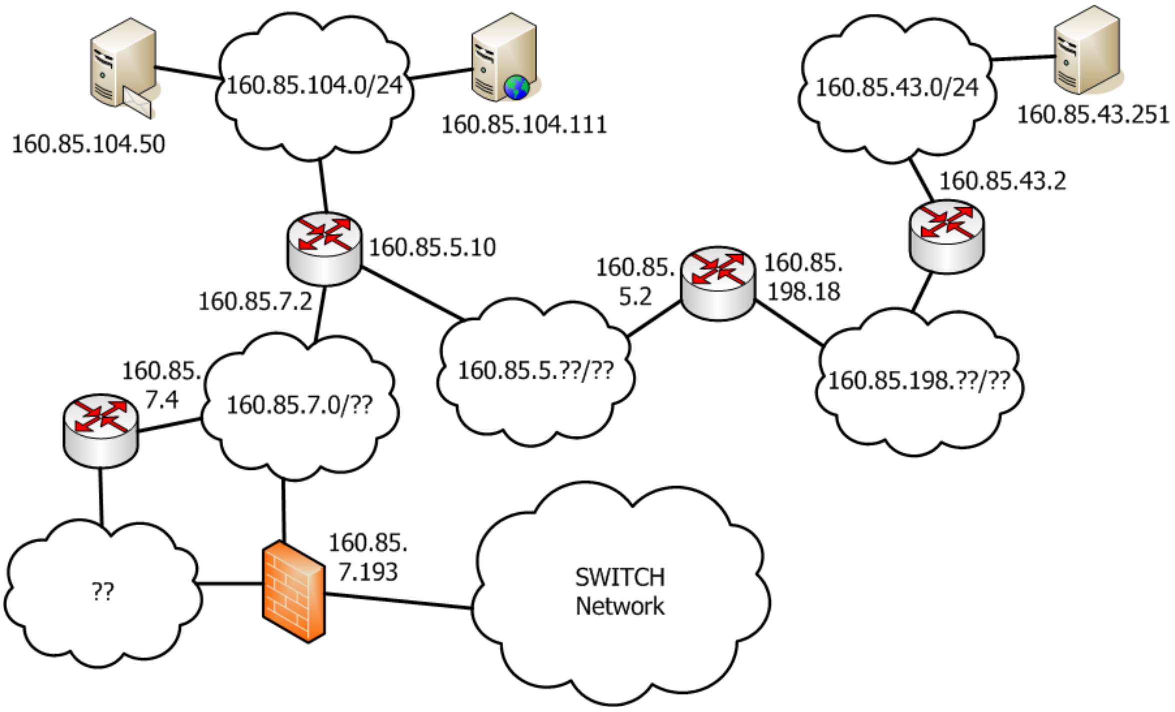


```
root@dhcppc2:~# hping3 --ttl 1 --traceroute --destport 80 --syn dskt0010.zhaw.ch
HPING dskt0010.zhaw.ch (eth0 160.85.43.251): S set, 40 headers + 0 data bytes
hop=1 TTL 0 during transit from ip=10.0.0.1 name=UNKNOWN
hop=1 hoprtt=1.4 ms
hop=2 TTL 0 during transit from ip=80.254.161.241 name=zh2-lns02-lo1.noc.green.ch
hop=2 hoprtt=12.3 ms
…
hop=7 TTL 0 during transit from ip=130.59.36.158 name=swiWI2-G0-1.switch.ch
hop=7 hoprtt=15.0 ms
hop=8 TTL 0 during transit from ip=160.85.7.193 name=UNKNOWN
hop=8 hoprtt=14.4 ms
hop=9 TTL 0 during transit from ip=160.85.7.2 name=UNKNOWN
hop=9 hoprtt=301.3 ms
hop=10 TTL 0 during transit from ip=160.85.5.2 name=UNKNOWN
hop=10 hoprtt=356.2 ms
```

Two additional hops compared to traceroute

Scanning – Network Structure (6)

- Possible network structure based on the currently available information:



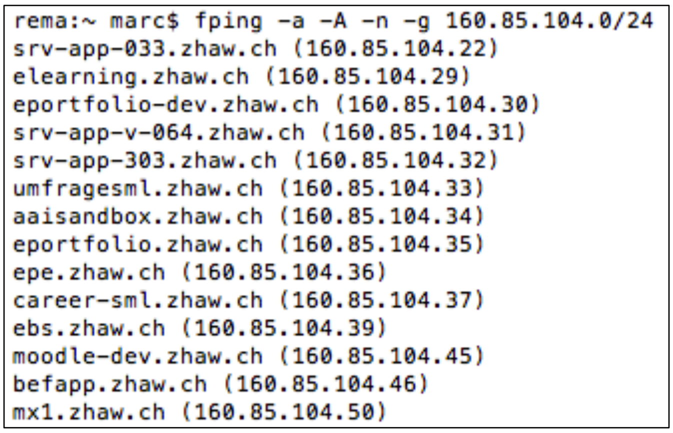
Scanning – Host Search (1)

- Searching for hosts is of course very important because in the end, it's the hosts we are likely going to attack
  - We have already accumulated a host list when performing DNS queries during footprinting, but not all hosts have DNS entries

- The primary used tools for host searching are fping and nmap
  - fping is very similar to ping, but allows "pinging" entire networks
  - nmap has more scanning options than fping and can therefore perform successful host searches where fping cannot

Scanning – Host Search (2)

- Performing a host search in an entire network with fping:

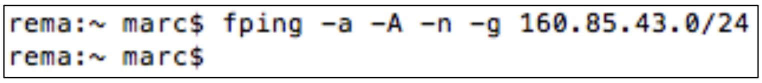


```
rema:~ marc$ fping -a -A -n -g 160.85.104.0/24
srv-app-033.zhaw.ch (160.85.104.22)
elearning.zhaw.ch (160.85.104.29)
eportfolio-dev.zhaw.ch (160.85.104.30)
srv-app-v-064.zhaw.ch (160.85.104.31)
srv-app-303.zhaw.ch (160.85.104.32)
umfragesml.zhaw.ch (160.85.104.33)
aaisandbox.zhaw.ch (160.85.104.34)
eportfolio.zhaw.ch (160.85.104.35)
epe.zhaw.ch (160.85.104.36)
career-sml.zhaw.ch (160.85.104.37)
ebs.zhaw.ch (160.85.104.39)
moodle-dev.zhaw.ch (160.85.104.45)
befapp.zhaw.ch (160.85.104.46)
mx1.zhaw.ch (160.85.104.50)
```

  - Displays both hostnames and IP addresses of the found hosts
- fping (just like ping) has its limitations
  - It works using ICMP ECHO messages
  - If there's a firewall blocking the probes, no results will be found

Scanning – Host Search (3)

- Performing a host search in another network with fping:



```
rema:~ marc$ fping -a -A -n -g 160.85.43.0/24
rema:~ marc$
```

  - There are either no hosts up or a firewall is blocking the ping probes
- In these cases, nmap is usually the better choice
  - nmap not only supports ICMP, but also TCP to perform host scanning
  - The idea is to establish TCP connections to ports that are often not filtered by firewalls, e.g. ssh or web
- nmap scan by trying to connect to ports 22 and 80:

```
rema:~ marc$ nmap -sP -PS[22,80] 160.85.43.0/24

Starting Nmap 5.51 ( http://nmap.org ) at 2012-03-20 13:18 CET
Nmap scan report for 160.85.43.238
Nmap scan report for edu-43.243.zhaw.ch (160.85.43.243)
Nmap scan report for edu-43.249.zhaw.ch (160.85.43.249)
Nmap scan report for edu-43.251.zhaw.ch (160.85.43.251)
Nmap done: 256 IP addresses (4 hosts up) scanned in 40.08 seconds
```

  - So there are indeed (at least) four hosts available!

Scanning – Port Scanning (1)

- Once hosts have been discovered, the next question to answer is what services are running on them
- The tool to perform this is a port scanner and the most popular and powerful scanner is nmap
- nmap can do the following:
  - Host scanning (as we have done before)
  - Various methods of TCP scanning (TCP connect, SYN, ACK, FIN, NUL, Xmas scan...) and UDP scans
  - Determine the products and versions of the OS and exposed services
- Which hosts to scan?
  - Depends on the time and effort you want to invest
  - Focus on the hosts that are “valuable” (e.g. web servers, mail servers, file servers, DNS servers etc.)
  - Other servers or user computers may be interesting, too, as they are often less well maintained (and may provide access to further hosts)

Scanning – Port Scanning (2)

- Let’s start with a TCP scan (SYN scan as root) of www.zhaw.ch
  - -PN is needed when pings are blocked
  - No port range specified: tests 1000 “typical” ports

```
root@octopus:~# nmap -PN www.zhaw.ch

Starting Nmap 5.00 ( http://nmap.org ) at 2011-03-03 13:41 CET
Interesting ports on web.zhaw.ch (160.85.104.111):
Not shown: 999 filtered ports
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 16.18 seconds
```

- Interpretation
  - Only one port (HTTP) is open
  - All other ports are somewhere filtered by a firewall (no reply)
  - Ports that reply with a TCP RST would be marked closed

Scanning – Port Scanning (3)

- nmap can also be used to detect the OS and software versions of the installed services
  - This is done by looking for banners, TCP sequence number analysis etc.
  - Using the -O and -sV options (or -A, which combines them)

```
root@octopus:~# nmap -PN -p1-65535 -O -sV www.zhaw.ch

Starting Nmap 5.00 ( http://nmap.org ) at 2011-03-03 15:19 CET
Interesting ports on web.zhaw.ch (160.85.104.111):
Not shown: 65534 filtered ports
PORT     STATE SERVICE
80/tcp   open  http    Apache httpd
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: phone|switch|WAP
Running (JUST GUESSING) : Nokia Symbian OS (97%), HP embedded (96%), D-Link embedded
(94%), TRENDnet embedded (94%)
Aggressive OS guesses: Nokia E70 mobile phone (Symbian OS) (97%), HP 4000M ProCurve
switch (J4121A) (96%), D-Link DWL-624+ or DWL-2000AP, or TRENDnet TEW-432BRP WAP (94%)
No exact OS matches for host (test conditions non-ideal).

OS and Service detection performed. Please report any incorrect results at http://
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5148.52 seconds
```

- Not much more information in this case...

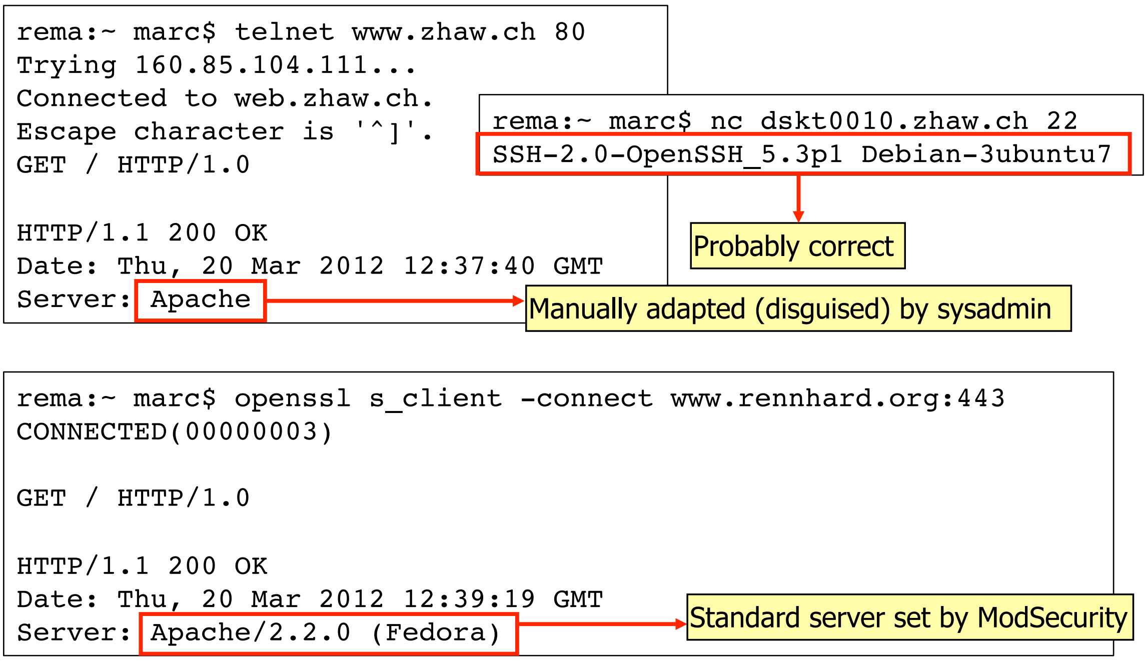
Scanning – Port Scanning (4)

- In some cases, OS and software version detection works much better:

```
rema:~ marc$ sudo nmap -PN -O -sV dskt0010.zhaw.ch

Starting Nmap 5.51 ( http://nmap.org ) at 2012-03-20 13:32 CET
Nmap scan report for dskt0010.zhaw.ch (160.85.43.251)
Host is up (0.034s latency).
rDNS record for 160.85.43.251: edu-43.251.zhaw.ch
Not shown: 998 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.3p1 Debian 3ubuntu7 (protocol 2.0)
80/tcp open  http    Apache httpd 2.2.14 ((Ubuntu))
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: terminal|general purpose
Running (JUST GUESSING): IGEL Linux 2.6.X (86%), Linux 2.6.X (86%)
Aggressive OS guesses: IGEL UD3 thin client (Linux 2.6) (86%), Linux 2.6.32
(86%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Linux

OS and Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.21 seconds
```

Scanning – Manual Banner Grabbing

- Manual methods are also well suited to determine software versions
  - By, e.g., using telnet, netcat or openssl (for SSL/TLS communications)



```
rema:~ marc$ telnet www.zhaw.ch 80
Trying 160.85.104.111...
Connected to web.zhaw.ch.
Escape character is '^]'.
GET / HTTP/1.0

HTTP/1.1 200 OK
Date: Thu, 20 Mar 2012 12:37:40 GMT
Server: Apache
```

```
rema:~ marc$ nc dskt0010.zhaw.ch 22
SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7
```

Probably correct

Manually adapted (disguised) by sysadmin

```
rema:~ marc$ openssl s_client -connect www.rennhard.org:443
CONNECTED(00000003)

GET / HTTP/1.0

HTTP/1.1 200 OK
Date: Thu, 20 Mar 2012 12:39:19 GMT
Server: Apache/2.2.0 (Fedora)
```

Standard server set by ModSecurity

Scanning – Vulnerability Scanning (1)

- nmap and banner grabbing help to identify software versions with possible vulnerabilities
  - But the interpretation of the results and attempts to verify/exploit vulnerabilities are left to the attacker/tester
- Vulnerability Scanners go further
  - They first also perform port scans and try to detect software versions
  - In addition, they contain large databases of known vulnerabilities of specific software versions and can therefore help to interpret the results
  - They also can detect configuration flaws (e.g. weak ciphers) and attempt to automatically exploit some vulnerabilities (e.g. try default passwords)
- Vulnerability Scanners are powerful tools, but:
  - Their database of known vulnerabilities must be constantly updated
  - Often produce false positives (e.g. by identifying the wrong software version and drawing wrong conclusions)
  - The results therefore still require manual interpretation and verification
  - They are usually limited to detecting publicly known vulnerabilities and misconfigurations

Scanning – Vulnerability Scanning (2)

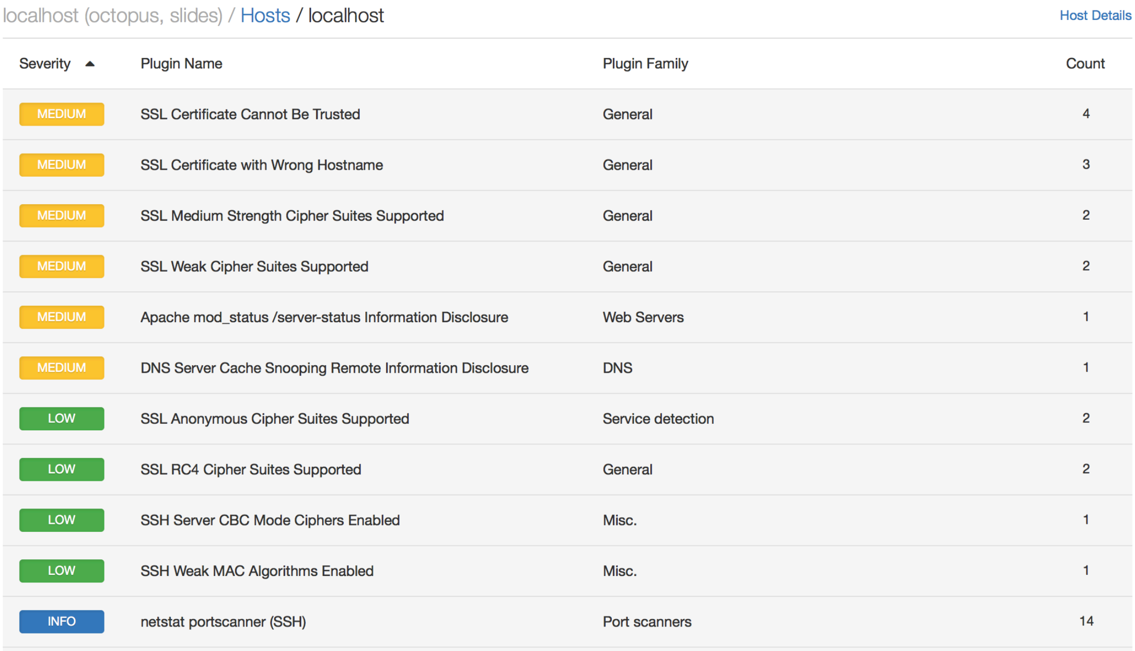
- The most popular general vulnerability scanner is Nessus
  - "General" in the sense that it tests at a wide range of "layers"
  - From OS vulnerabilities to server and web application vulnerabilities
- The vulnerability tests in Nessus are performed by so-called plugins
  - There are more than 50'000 official plugins (distributed with Nessus) available
  - It's also possible to write own plugins
  - Nessus can be configured to auto-update its plugins regularly
- Nessus was originally free and open source, but has turned into a commercial product
  - Maintained by Tenable Network Security
  - Can still be used for free to scan own systems (e.g. at home) but not to offer commercial services

Scanning – Vulnerability Scanning (3)

- The core of Nessus is the Nessus daemon (nessusd), which performs the scans
  - Can be installed on any system (local, scanning server...)
- Configuring scans and viewing results is done via the browser from anywhere
  - There also exists a command line client
- Besides performing scans, Nessus supports several features
  - Supports multiple users that are granted access using username/password over TLS
  - An authorization mechanism allows to configure who is allowed to do what (configure scans, execute scans...)
  - Scan profiles can be configured and easily reused in different scans
  - Reports can be exported in various formats for further processing

Scanning – Vulnerability Scanning (4)

- Example scan of a Linux server:



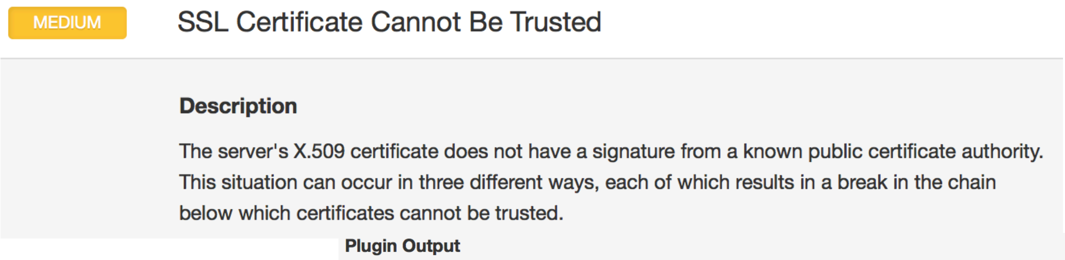
localhost (octopus, slides) / Hosts / localhost

Host Details

Severity ▲	Plugin Name	Plugin Family	Count
MEDIUM	SSL Certificate Cannot Be Trusted	General	4
MEDIUM	SSL Certificate with Wrong Hostname	General	3
MEDIUM	SSL Medium Strength Cipher Suites Supported	General	2
MEDIUM	SSL Weak Cipher Suites Supported	General	2
MEDIUM	Apache mod_status /server-status Information Disclosure	Web Servers	1
MEDIUM	DNS Server Cache Snooping Remote Information Disclosure	DNS	1
LOW	SSL Anonymous Cipher Suites Supported	Service detection	2
LOW	SSL RC4 Cipher Suites Supported	General	2
LOW	SSH Server CBC Mode Ciphers Enabled	Misc.	1
LOW	SSH Weak MAC Algorithms Enabled	Misc.	1
INFO	netstat portscanner (SSH)	Port scanners	14

Scanning – Vulnerability Scanning (5)

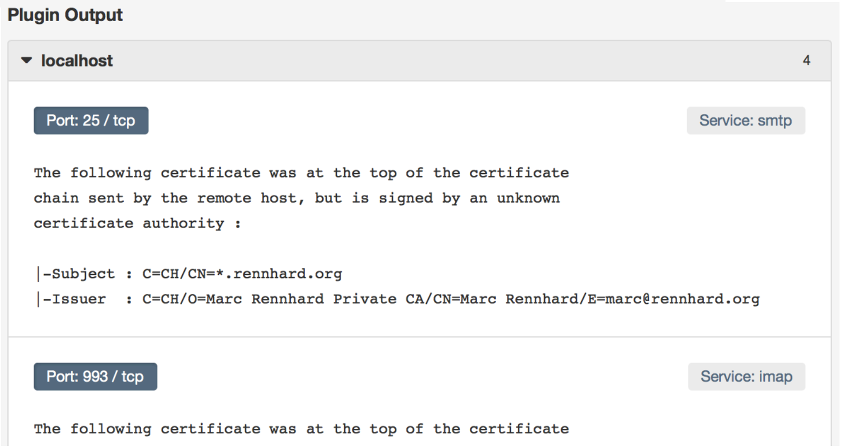
- Nessus provides detailed information about the problems detected:



MEDIUM SSL Certificate Cannot Be Trusted

Description

The server's X.509 certificate does not have a signature from a known public certificate authority. This situation can occur in three different ways, each of which results in a break in the chain below which certificates cannot be trusted.



Plugin Output

▾ localhost 4

Port: 25 / tcp Service: smtp

```
The following certificate was at the top of the certificate
chain sent by the remote host, but is signed by an unknown
certificate authority :

|-Subject  : C=CH/CN=*.rennhard.org
|-Issuer   : C=CH/O=Marc Rennhard Private CA/CN=Marc Rennhard/E=marc@rennhard.org
```

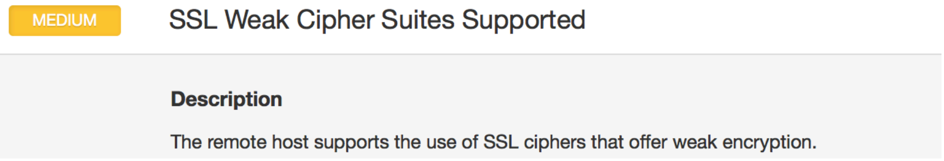
Port: 993 / tcp Service: imap

```
The following certificate was at the top of the certificate
```

- For Nessus, this is a Medium Risk, but in fact it is "wanted behaviour"
  - False positive in this case
  - But it may be a true positive in other cases

Scanning – Vulnerability Scanning (6)

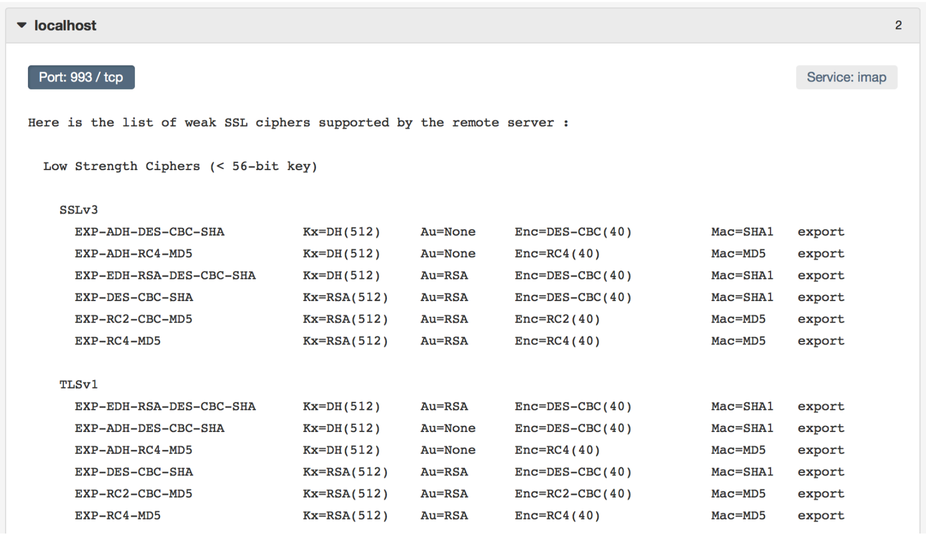
- Example of a true positive:



MEDIUM SSL Weak Cipher Suites Supported

Description

The remote host supports the use of SSL ciphers that offer weak encryption.



▾ localhost 2

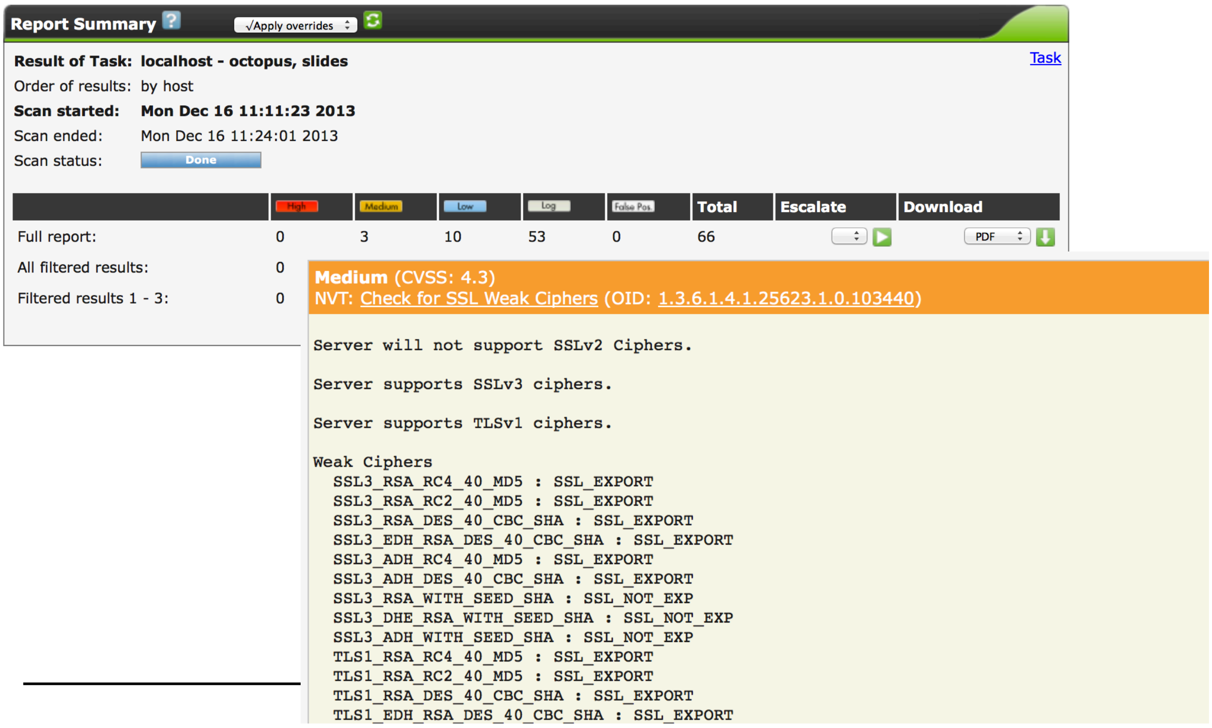
Port: 993 / tcp Service: imap

```
Here is the list of weak SSL ciphers supported by the remote server :

  Low Strength Ciphers (< 56-bit key)

    SSLv3
      EXP-ADH-DES-CBC-SHA          Kx=DH(512)    Au=None   Enc=DES-CBC(40)       Mac=SHA1   export
      EXP-ADH-RC4-MD5              Kx=DH(512)    Au=None   Enc=RC4(40)           Mac=MD5    export
      EXP-EDH-RSA-DES-CBC-SHA      Kx=DH(512)    Au=RSA    Enc=DES-CBC(40)       Mac=SHA1   export
      EXP-DES-CBC-SHA              Kx=RSA(512)   Au=RSA    Enc=DES-CBC(40)       Mac=SHA1   export
      EXP-RC2-CBC-MD5              Kx=RSA(512)   Au=RSA    Enc=RC2(40)           Mac=MD5    export
      EXP-RC4-MD5                  Kx=RSA(512)   Au=RSA    Enc=RC4(40)           Mac=MD5    export

    TLSv1
      EXP-EDH-RSA-DES-CBC-SHA      Kx=DH(512)    Au=RSA    Enc=DES-CBC(40)       Mac=SHA1   export
      EXP-ADH-DES-CBC-SHA          Kx=DH(512)    Au=None   Enc=DES-CBC(40)       Mac=SHA1   export
      EXP-ADH-RC4-MD5              Kx=DH(512)    Au=None   Enc=RC4(40)           Mac=MD5    export
      EXP-DES-CBC-SHA              Kx=RSA(512)   Au=RSA    Enc=DES-CBC(40)       Mac=SHA1   export
      EXP-RC2-CBC-MD5              Kx=RSA(512)   Au=RSA    Enc=RC2-CBC(40)       Mac=MD5    export
      EXP-RC4-MD5                  Kx=RSA(512)   Au=RSA    Enc=RC4(40)           Mac=MD5    export
```

- Ciphers with 40-bit keys are indeed supported
- Medium risk is a reasonable classification because it is not something an attacker can easily exploit

Scanning – Vulnerability Scanning (7)

- A free, open source alternative to Nessus: OpenVAS
  - Provides results similar to Nessus



Result of Task: **localhost - octopus, slides**
Order of results: by host
Scan started: **Mon Dec 16 11:11:23 2013**
Scan ended: Mon Dec 16 11:24:01 2013
Scan status: Done

	High	Medium	Low	Log	False Pos.	Total	Escalate	Download
Full report:	0	3	10	53	0	66		PDF
All filtered results:	0							
Filtered results 1 - 3:	0							

Medium (CVSS: 4.3)
NVT: Check for SSL Weak Ciphers (OID: 1.3.6.1.4.1.25623.1.0.103440)

```
Server will not support SSLv2 Ciphers.

Server supports SSLv3 ciphers.

Server supports TLSv1 ciphers.

Weak Ciphers
  SSL3_RSA_RC4_40_MD5 : SSL_EXPORT
  SSL3_RSA_RC2_40_MD5 : SSL_EXPORT
  SSL3_RSA_DES_40_CBC_SHA : SSL_EXPORT
  SSL3_EDH_RSA_DES_40_CBC_SHA : SSL_EXPORT
  SSL3_ADH_RC4_40_MD5 : SSL_EXPORT
  SSL3_ADH_DES_40_CBC_SHA : SSL_EXPORT
  SSL3_RSA_WITH_SEED_SHA : SSL_NOT_EXP
  SSL3_DHE_RSA_WITH_SEED_SHA : SSL_NOT_EXP
  SSL3_ADH_WITH_SEED_SHA : SSL_NOT_EXP
  TLS1_RSA_RC4_40_MD5 : SSL_EXPORT
  TLS1_RSA_RC2_40_MD5 : SSL_EXPORT
  TLS1_RSA_DES_40_CBC_SHA : SSL_EXPORT
  TLS1_EDH_RSA_DES_40_CBC_SHA : SSL_EXPORT
```

Scanning – Summary

- Scanning serves to analyse the network structure and the individual hosts in detail

- After scanning, you know the following information
  - Parts or all of the network structure
  - Hosts that are reachable from your location

- Of a subset of all hosts (or of all hosts if the analysed environment is small) you know more detailed information
  - Operating system
  - Available services (that are visible from your location)
  - Software versions of the services
  - Potential vulnerabilities that may be exploited

Software Security (SSI)

Analysis of Scanning Results

Analysis of Scanning Results (1)

- After "Footprinting and Scanning", a large number of host, services and even potential vulnerabilities are known
- The goal of this phase is to identify the systems that are interesting to be analyzed further, i.e. that one attempts to compromise
- Trying to compromise every possible system is usually not an option, so focussing on some systems is important
- In practice – especially with large environments – this may be a multi-step process
  - Start with the most promising systems and try to compromise them
  - Depending on these results, further systems may have to be considered
  - It can also be that compromising a system provides access to further, previously inaccessible systems, and it may then be reasonable to analyse / scan these systems as well and so on…

Analysis of Scanning Results (2)

What targets are interesting to compromise?

- Again, this depends very much on the available time and the goals that should be reached with the penetration test

In general, focus on the following two types of targets:

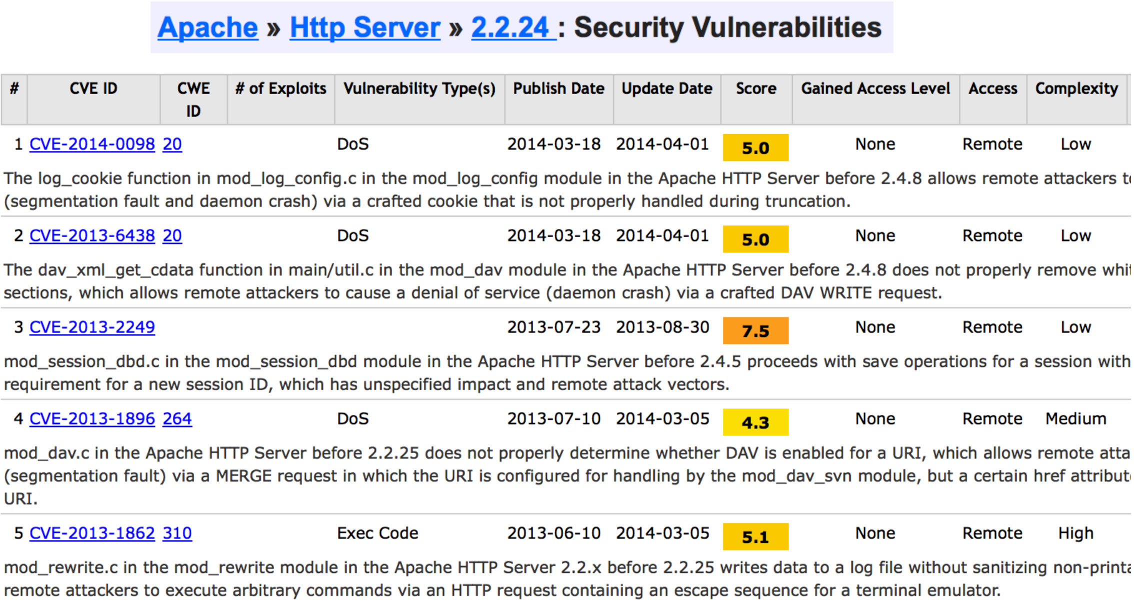
- Any host that is of "high value"
  - Even if no potential vulnerabilities have been identified so far
  - E.g. web (application) servers that provide access to valuable data
- Any "easy targets"
  - E.g. host where Nessus / OpenVAS reported significant problems, e.g.
    - Configuration flaws (e.g. a server component that uses the default admin password)
    - Any known vulnerabilities (e.g. an unpatched windows system that allows remote administrator access)

Analysis of Scanning Results (3)

- One should also consult publicly available vulnerability databases to check whether the analysed hosts contain known vulnerabilities
  - Typically done based on identified versions of OS and services
  - Vulnerability scanners may have reported some known vulnerabilities, but they can only detect a vulnerability if a corresponding plugin exists
- The most prominent is Common Vulnerabilities and Exposures (CVE)
  - Collects known security vulnerabilities
  - Assigns each with a unique number, e.g. CVE-2006-0067, consisting of the year (2006) and a vulnerability "number" (0067) within that year
  - Vulnerability scanners usually report the CVE number (if it exists) of a known vulnerability – and it makes sense to verify them manually (possibility of false positives)

Analysis of Scanning Results – CVE

- Original site: http://cve.mitre.org, but only poor searching possibilities
- Better suited to search for versions: http://www.cvedetails.com



Apache » Http Server » 2.2.24 : Security Vulnerabilities

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity
1	CVE-2014-0098	20		DoS	2014-03-18	2014-04-01	5.0	None	Remote	Low
The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers t (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.										
2	CVE-2013-6438	20		DoS	2014-03-18	2014-04-01	5.0	None	Remote	Low
The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whi sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.										
3	CVE-2013-2249				2013-07-23	2013-08-30	7.5	None	Remote	Low
mod_session_dbd.c in the mod_session_dbd module in the Apache HTTP Server before 2.4.5 proceeds with save operations for a session with requirement for a new session ID, which has unspecified impact and remote attack vectors.										
4	CVE-2013-1896	264		DoS	2013-07-10	2014-03-05	4.3	None	Remote	Medium
mod_dav.c in the Apache HTTP Server before 2.2.25 does not properly determine whether DAV is enabled for a URI, which allows remote atta (segmentation fault) via a MERGE request in which the URI is configured for handling by the mod_dav_svn module, but a certain href attribut URI.										
5	CVE-2013-1862	310		Exec Code	2013-06-10	2014-03-05	5.1	None	Remote	High
mod_rewrite.c in the mod_rewrite module in the Apache HTTP Server 2.2.x before 2.2.25 writes data to a log file without sanitizing non-printa remote attackers to execute arbitrary commands via an HTTP request containing an escape sequence for a terminal emulator.										

Analysis of Scanning Results – Summary

- The results of this analysis is a set of host and services that one attempts to compromise in the next step
  - For some of these systems, vulnerabilities have already been identified (esp. well-known vulnerabilities and configuration flaws)
- Information about known-vulnerabilities can stem from different sources
  - Vulnerability scanners
  - Manual searches in public databases
- Prioritisation of targets is important
  - Which targets are valuable to compromise?
  - What is the estimated effort for a target to successfully compromising it (especially compared to the "value" of the target)
  - Which targets are prioritised according to my task as a tester?

Finding and Exploiting Vulnerabilities

Finding and Exploiting Vulnerabilities

- The goal of this phase is to compromise systems
  - By using the already found well-known vulnerabilities…
  - … and finding further (unknown) vulnerabilities…
  - … and exploiting them
- The thoroughness of this phase again depends on the available time and the goals of the penetration test
  - Sometimes, one only focuses on known vulnerabilities and in other cases (esp. with web application penetration tests), lots of effort is spent to uncover unknown vulnerabilities
  - Sometimes, it's enough to identify a vulnerability and tell the client "what could be done" (without actual exploitation)
  - In other cases, a proof-of-concept exploit is used or developed to show the practical exploitability of a vulnerability
  - And sometimes, "realistic exploits" are presented

→ In general, the more "complete and realistic" an exploit is presented, the more convincing it is for the client – and the more satisfying it is for the tester

Finding Unknown Vulnerabilities

How to find unknown vulnerabilities?

- Source Code Analysis
  - Usually not done manually but with Static Code Analysis Tools such as Findbugs or Fortify SCA
  - Modern tools are powerful, but prone to false positives
- Use a vulnerability scanner that targets specific types of applications
  - In contrast to Nessus / OpenVAS, they are optimized to find unknown vulnerabilities
  - Popular to assess web applications (e.g. w3af, OWASP ZAP, Burp Suite...)
  - Well suited to find some vulnerabilities, but also prone to false positives
- Manual interaction with the target application
  - Very typical for web applications (hands-on assessment)
  - Can produce very good results – provided the tester is skilled
- …

Exploiting Vulnerabilities

Depending on the type of a vulnerability, exploitation is possible in different ways:

- For some basic configuration flaws, exploitation is usually easy (e.g. log into a service using the default password)
- For many known vulnerabilities, there exist pre-fabricated proof-of-concept exploits which are freely available
  - The proof-of-concept exploits allow to verify whether a suspected vulnerability can indeed be exploited
  - This is often done by using the Metasploit framework, which itself contains many proof-of-concept exploits
- With web application vulnerabilities, exploitation is often possible, but requires significant skills with respect to web technologies
- …

Summary

- A penetration test serves to analyse the entire or parts of the IT-environment of a company with the goal to find and exploit vulnerabilities
  - It "simulates" the behaviour of an attacker

- A penetration test consists of several phases
  - Preparation phase: define scope
  - Footprinting: collecting relevant information about the target environment
  - Scanning: examine the target networks and hosts in more detail
  - Analysis of scanning results: identify the systems that will be analyzed in detail during the following phase
  - Finding and exploiting vulnerabilities: identify vulnerable systems and demonstrate proof-of-concept or "real" exploits
  - Reporting: Prepare a written report and an oral presentation, including concrete recommendations