Last updated 9/18/2017

Rich's lesson module checklist

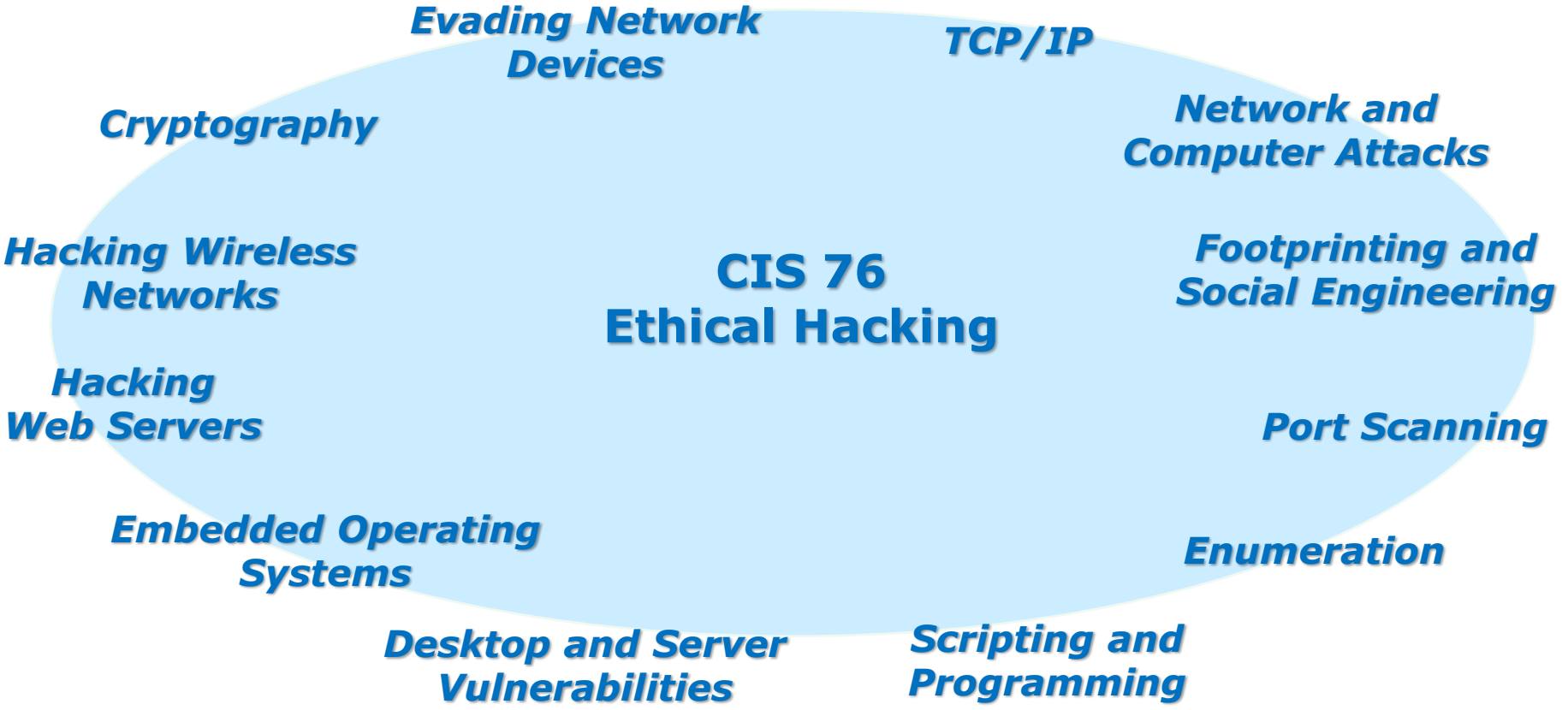
- ❑ Slides and lab posted
- ❑ WB converted from PowerPoint
- ❑ Print out agenda slide and annotate page numbers

- ❑ Flash cards
- ❑ Properties
- ❑ Page numbers
- ❑ 1st minute quiz
- ❑ Web Calendar summary
- ❑ Web book pages
- ❑ Commands

- ❑ Lab 4 posted and tested
- ❑ Microlab site ready
- ❑ PAN firewall adjusted for shodan
- ❑ pic02.jpg uploaded to website

- ❑ Backup slides, whiteboard slides, CCC info, handouts on flash drive
- ❑ Spare 9v battery for mic
- ❑ Key card for classroom door

- ❑ Update CCC Confer and 3C Media portals



Student Learner Outcomes

1. Defend a computer and a LAN against a variety of different types of security attacks using a number of hands-on techniques.

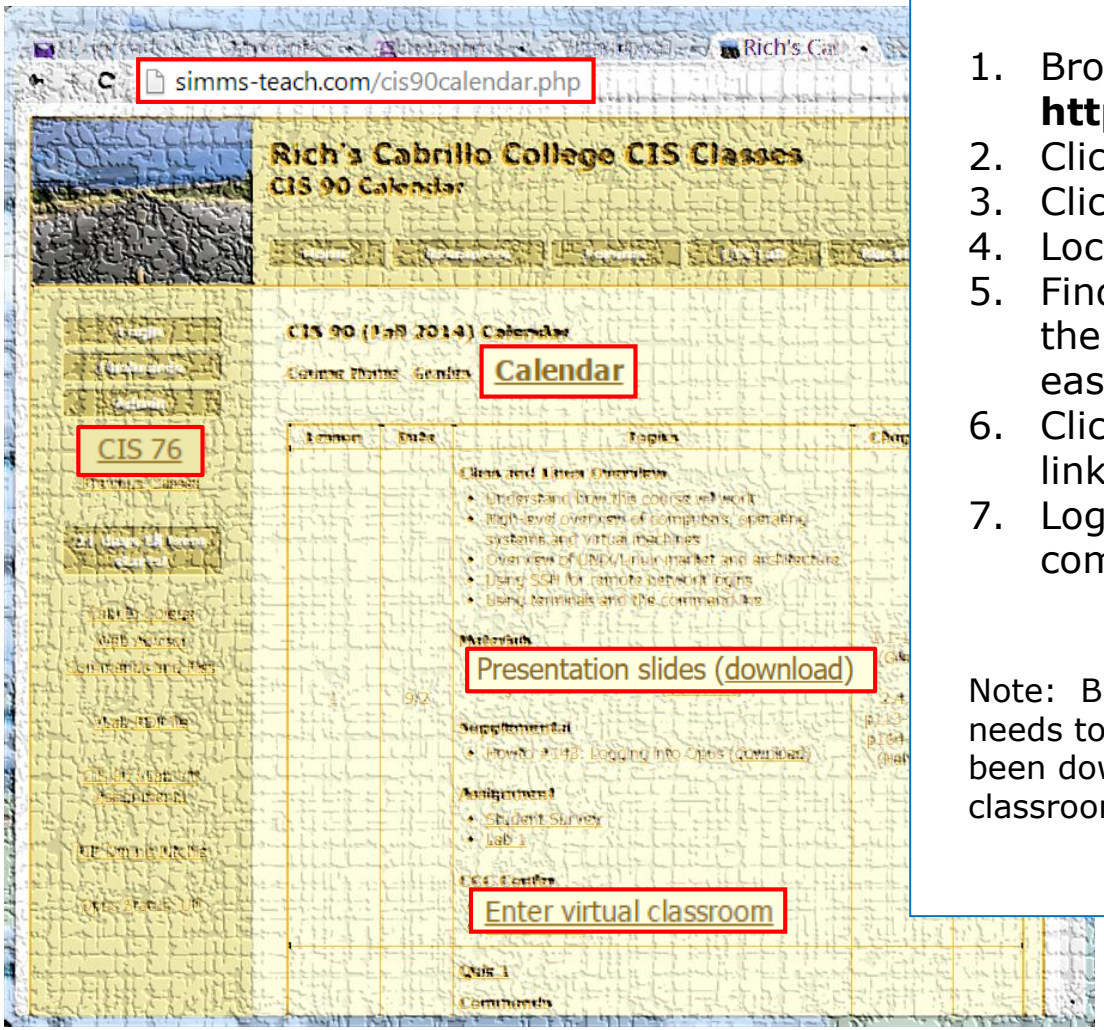
2. Defend a computer and a LAN against a variety of different types of security attacks using a number of hands-on techniques.

Introductions and Credits

Rich Simms
- HP Alumnus.
- Started teaching in 2008 when Jim Griffin went on sabbatical.
- Rich's site: http://simms-teach.com

And thanks to:
- Steven Bolt at for his WASTC EH training.
- Kevin Vaccaro for his CSSIA EH training and Netlab+ pods.
- EC-Council for their online self-paced CEH v9 course.
- Sam Bowne for his WASTC seminars, textbook recommendation and fantastic EH website (https://samsclass.info/).
- Lisa Bock for her great lynda.com EH course.
- John Govsky for many teaching best practices: e.g. the First Minute quizzes, the online forum, and the point grading system (http://teacherjohn.com/).
- Google for everything else!

Student checklist for attending class

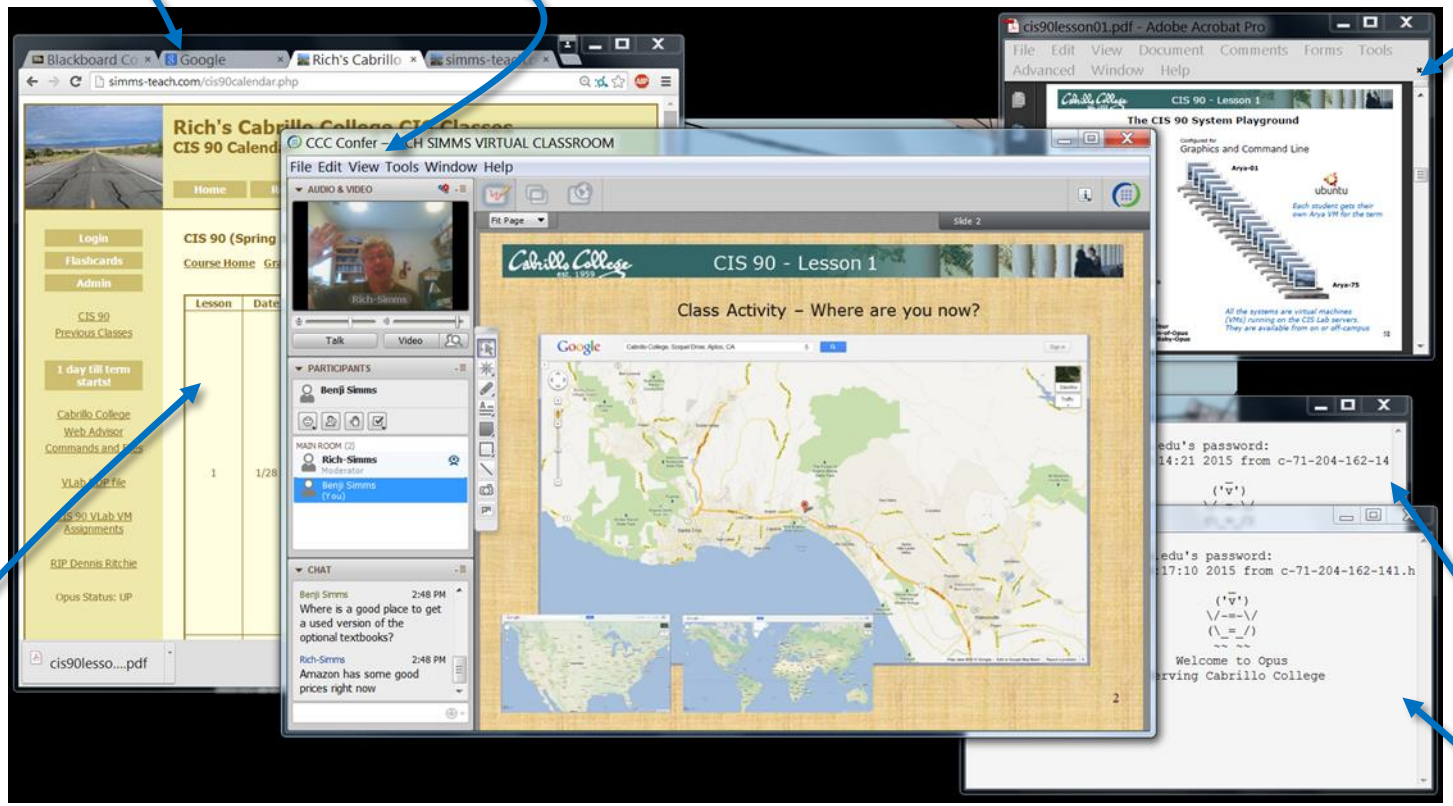


1. Browse to: **http://simms-teach.com**
2. Click the **CIS 76** link.
3. Click the **Calendar** link.
4. Locate today's lesson.
5. Find the **Presentation slides** for the lesson and **download** for easier viewing.
6. Click the **Enter virtual classroom** link to join CCC Confer.
7. Log into Opus-II with Putty or ssh command.

Note: Blackboard Collaborate Launcher only needs to be installed once. It has already been downloaded and installed on the classroom PC's.

Student checklist for suggested screen layout

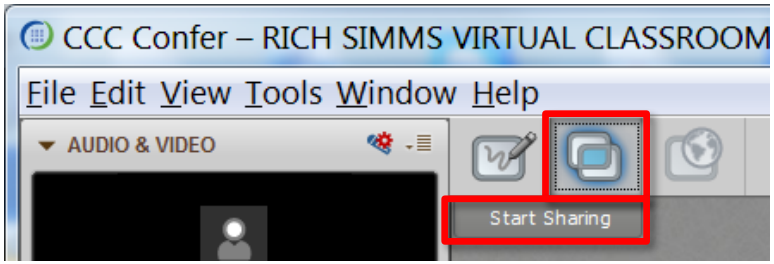
- ❑ *Google*
- ❑ *CCC Confer*
- ❑ *Downloaded PDF of Lesson Slides*



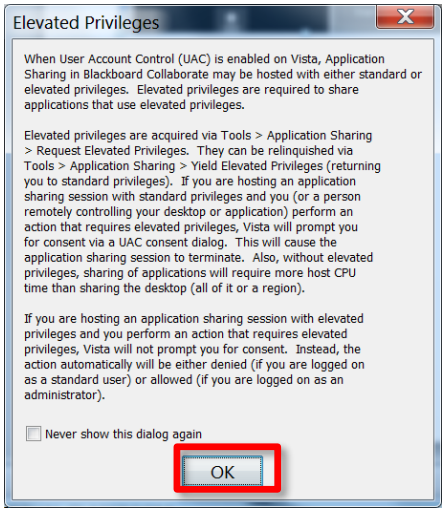
- ❑ *CIS 76 website Calendar page*
- ❑ *One or more login sessions to Opus*

Student checklist for sharing desktop with classmates

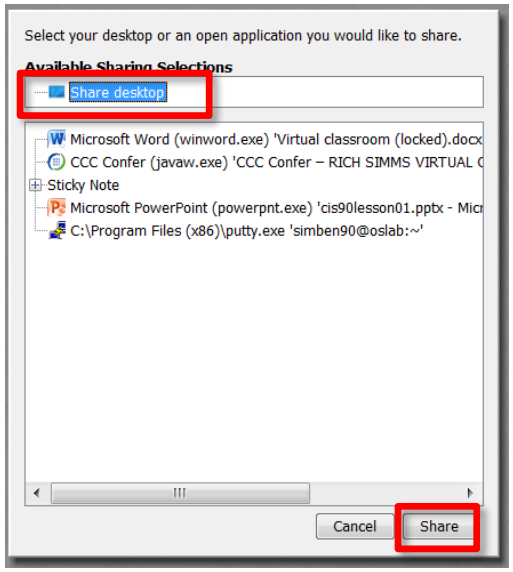
1) Instructor gives you sharing privileges.



2) Click overlapping rectangles icon. If white "Start Sharing" text is present then click it as well.



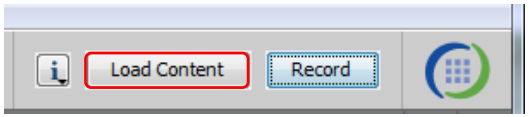
3) Click OK button.



4) Select "Share desktop" and click Share button.

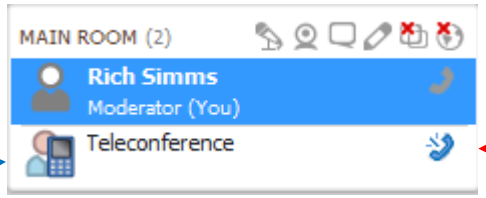
Rich's CCC Confer checklist - setup

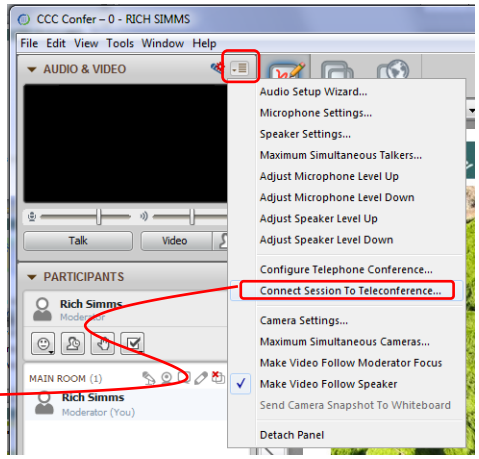
[ ] Preload White Board



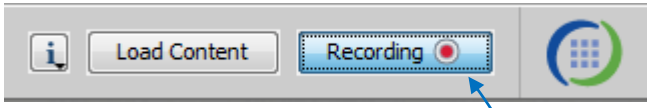
[ ] Connect session to Teleconference

Session now connected to teleconference





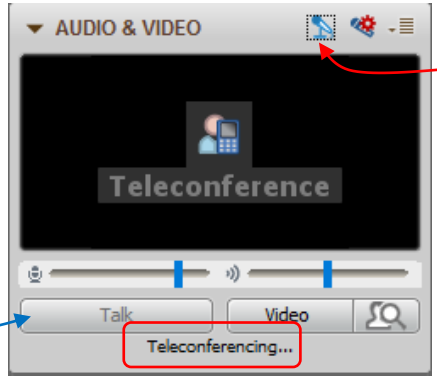
[ ] Is recording on?



Red dot means recording

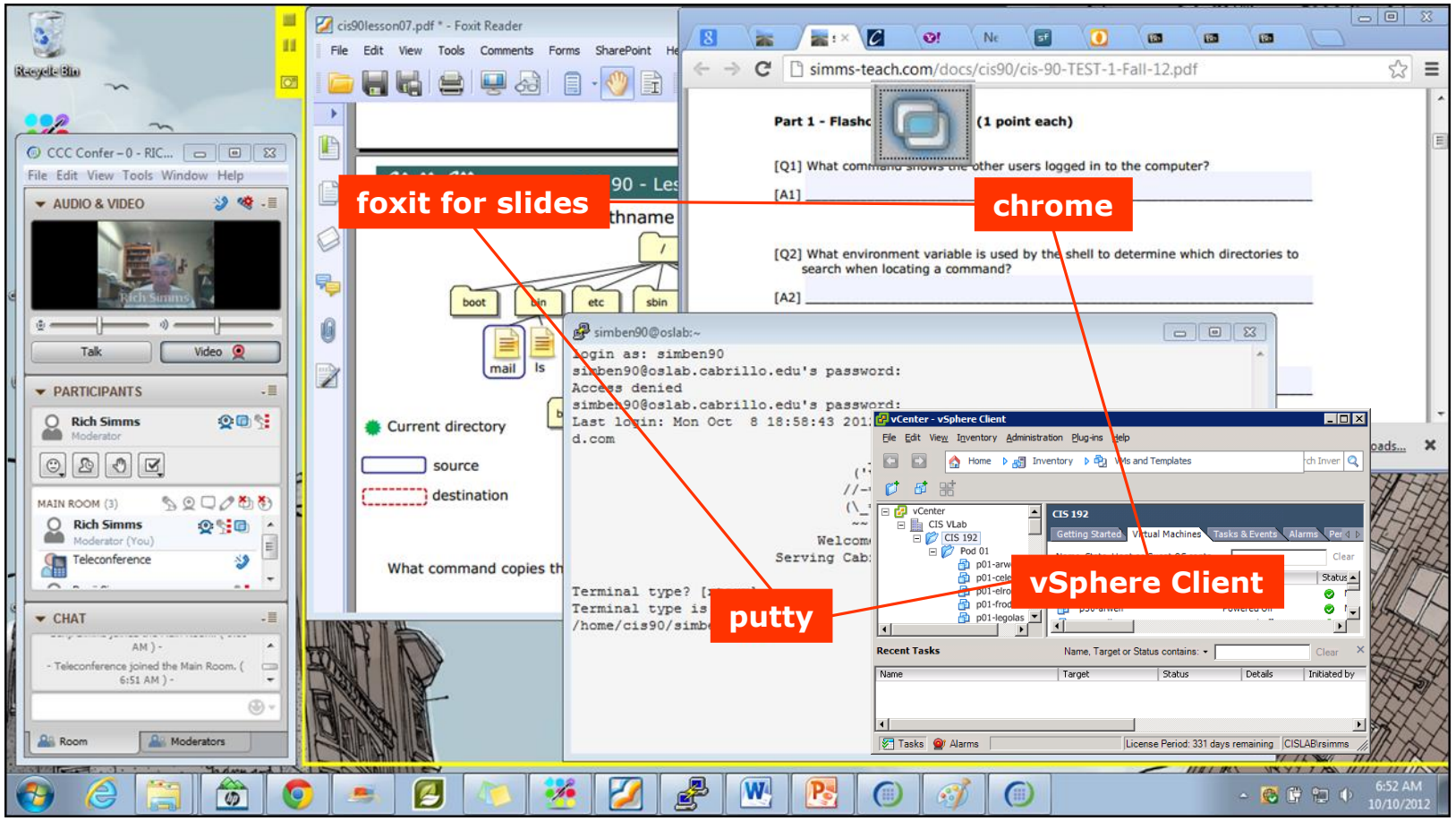
[ ] Use teleconferencing, not mic

Should be grayed out



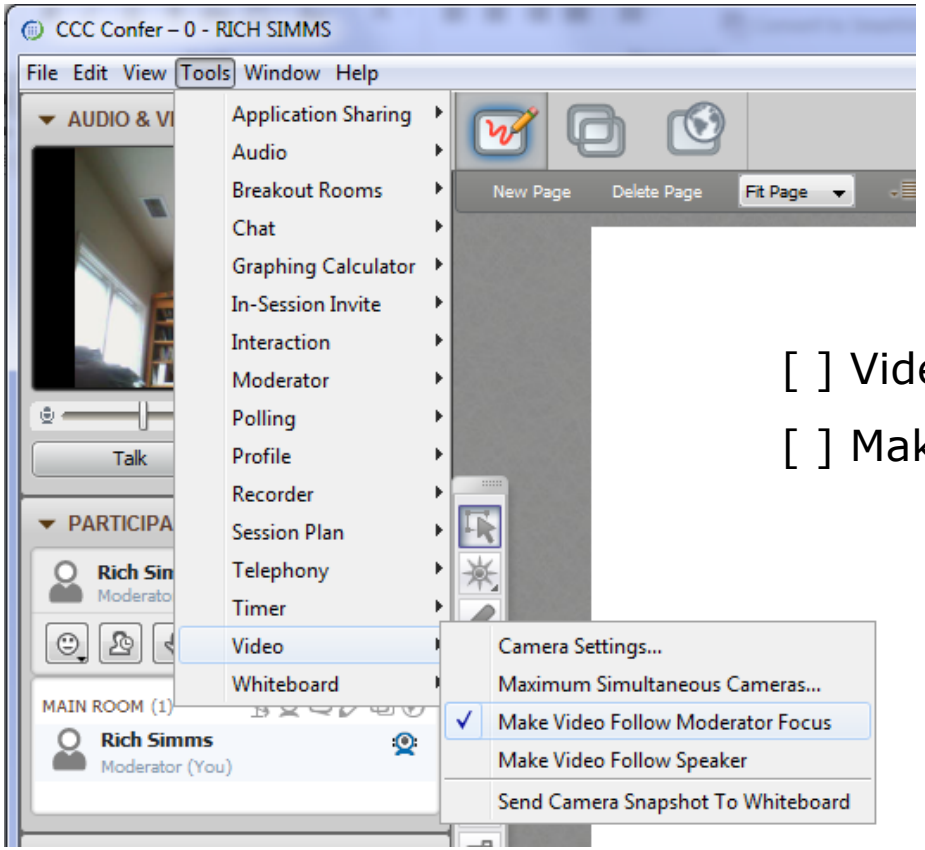
Should change from phone handset icon to little Microphone icon and the Teleconferencing … message displayed

Rich's CCC Confer checklist - screen layout



[ ] layout and share apps

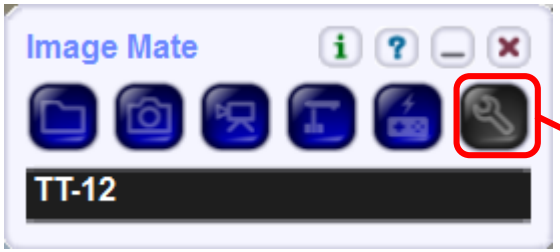
Rich's CCC Confer checklist - webcam setup

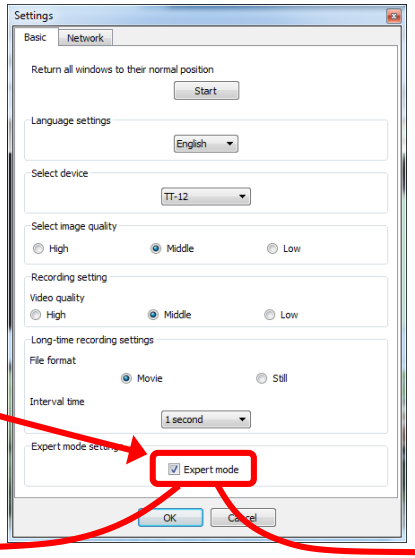


[ ] Video (webcam)

[ ] Make Video Follow Moderator Focus

Rich's CCC Confer checklist - Elmo



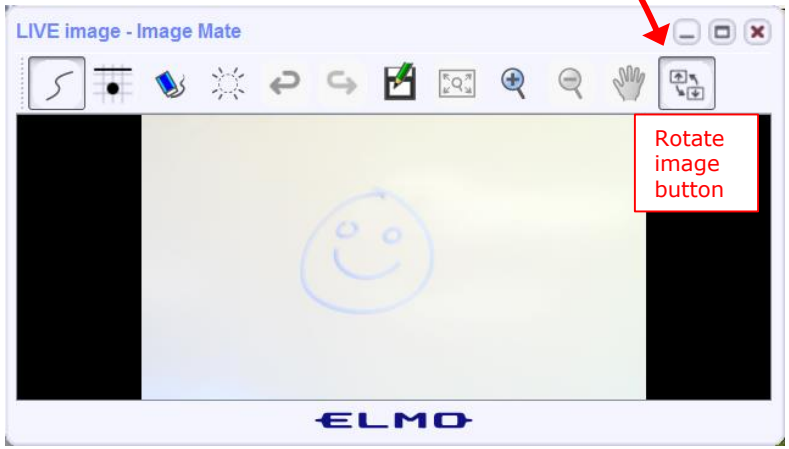


The "rotate image" button is necessary if you use both the side table and the white board.

Quite interesting that they consider you to be an "expert" in order to use this button!

Elmo rotated down to view side table

Elmo rotated up to view white board



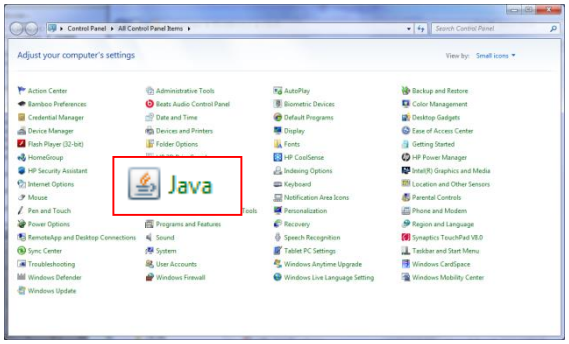
Run and share the Image Mate program just as you would any other app with CCC Confer

Rich's CCC Confer checklist - universal fixes

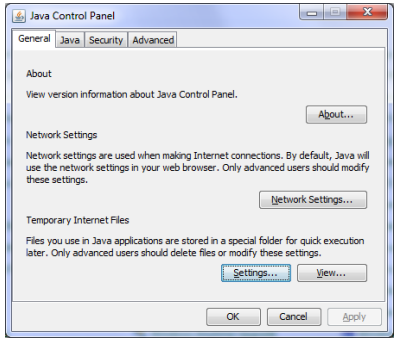
Universal Fix for CCC Confer:

1) Shrink (500 MB) and delete Java cache
2) Uninstall and reinstall latest Java runtime
3) http://www.cccconfer.org/support/technicalSupport.aspx

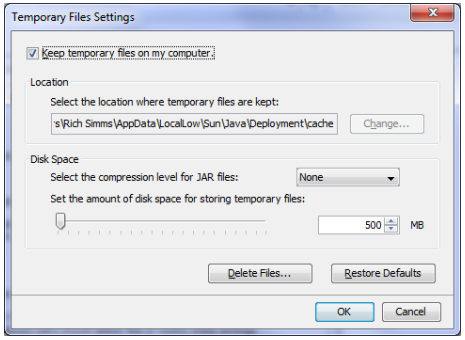
Control Panel (small icons)



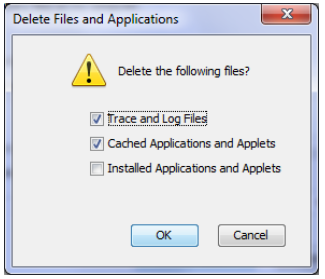
General Tab > Settings…



500MB cache size



Delete these



Google Java download

Start

Sound Check

*Students that dial-in should mute their line using *6 to prevent unintended noises distracting the web conference.*

*Instructor can use *96 to mute all student lines.*

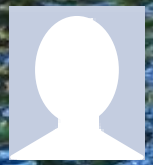
Volume
**4 - increase conference volume.*
**7 - decrease conference volume.*
**5 - increase your voice volume.*
**8 - decrease your voice volume.*

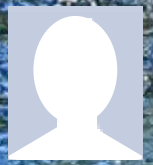
CIS 76 - Lesson 4

Instructor: **Rich Simms**
Dial-in: **888-886-3951**
Passcode: **136690**


Philip


Bruce

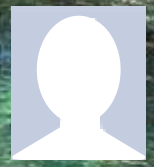

James


Sam B.


Sam R.


Miguel

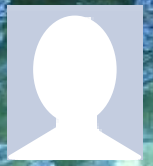

Bobby


Garrett


Ryan A.


Aga


Karina


Chris


Corbin


Helen


Xu


Mariano


Cameron


Ryan M.


Tre


May


Karl-Heinz


Remy


Tanner

Email me (risimms@cabrillo.edu) a relatively current photo of your face for 3 points extra credit

First Minute Quiz

Please answer these questions **in the order** shown:

Use CCC Confer White Board

email answers to: risimms@cabrillo.edu

(answers must be emailed within the first few minutes of class for credit)

Footprinting and Social Engineering

Objectives

- Learn to use various web tools for conducting reconnaissance.
- Explore gathering DNS information.
- Try some Google Hacking.
- Understand what doxing is.
- Understand the different types of social engineering.

Agenda

- Quiz
- Questions
- Housekeeping
- Footprinting and Reconnaissance
- Social Engineering
- Assignment
- Wrap up

Admonition

Unauthorized hacking is a crime.

The hacking methods and activities learned in this course can result in prison terms, large fines and lawsuits if used in an unethical manner. They may only be used in a lawful manner on equipment you own or where you have explicit permission from the owner.

Students that engage in any unethical, unauthorized or illegal hacking may be dropped from the course and will receive no legal protection or help from the instructor or the college.

Questions

Questions?

Lesson material?

Labs? Tests?

How this course works?

- Graded work in home directories
- Answers in /home/cis90/answers

Who questions much, shall learn much, and retain much.
- Francis Bacon

If you don't ask, you don't get.
- Mahatma Gandhi

Chinese Proverb	他問一個問題，五分鐘是個傻子，他不問一個問題仍然是一個傻瓜永遠。 *He who asks a question is a fool for five minutes; he who does not ask a question remains a fool forever.*

In the news

Recent news

1. MUO: Equihax: One of the Most Calamitous Breaches of All Time

   http://www.makeuseof.com/tag/equifax-breach-what-happened/

Thanks Karina

2. ars TECHNICA: Failure to patch two-month-old bug led to massive Equifax breach

   https://arstechnica.com/information-technology/2017/09/massive-equifax-breach-caused-by-failure-to-patch-two-month-old-bug/

3. CVE-2017-5638

   http://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-2017-5638

4. Krebs: Ayuda! (Help!) Equifax Has My Data!

   https://krebsonsecurity.com/2017/09/ayuda-help-equifax-has-my-data/

Recent news

1. Act Now: Hackers Hid Malware in Security App With 2 Billion Downloads

https://www.inc.com/joseph-steinberg/act-now-hackers-hid-malware-in-security-app-with.html

Housekeeping

If you haven't already

Change your default password on Opus-II

```
[simben90@opus-ii ~]$ passwd
Changing password for user simben90.
Changing password for simben90.
(current) UNIX password:
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[simben90@opus-ii ~]$
```

Roll Call

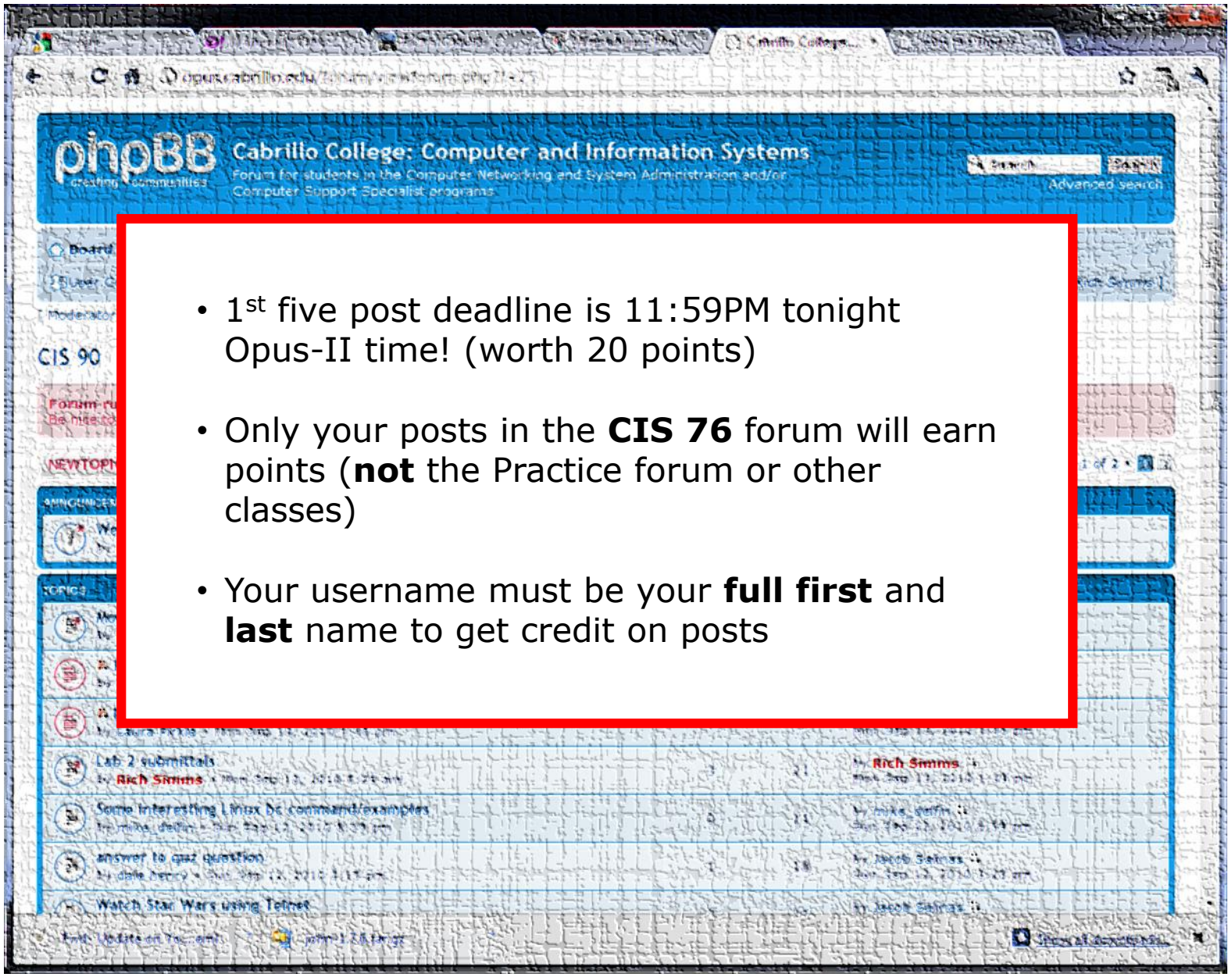
If you are attending class by watching the recordings email the instructor at:

risimms@cabrillo.edu

to provide roll call attendance.

Housekeeping

1. Send me your student survey & agreement if you haven't already.
2. Lab 3 due by 11:59PM (Opus-II time) tonight.
3. Five forum posts due tonight at 11:59PM (Opus-II time).
4. Graded labs are placed in your home directory on Opus-II.
5. Answers to the quizzes are in /home/cis76/answers on Opus-II.
6. Grades from last week posted on the website.
7. When I get your survey/agreement I will send you your grading codename.



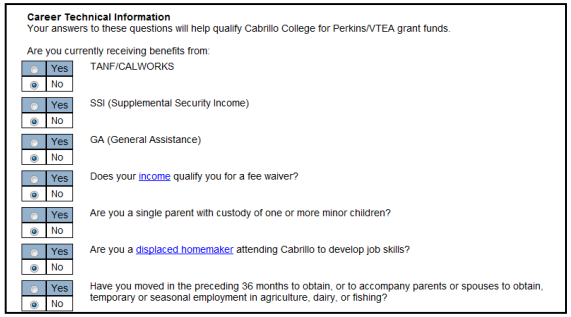
- 1st five post deadline is 11:59PM tonight Opus-II time! (worth 20 points)
- Only your posts in the **CIS 76** forum will earn points (**not** the Practice forum or other classes)
- Your username must be your **full first** and **last** name to get credit on posts

Perkins/VTEA Survey

https://opus-ii.cis.cabrillo.edu/forum/viewtopic.php?f=4&t=80

This is an important source of funding for Cabrillo College.

Send me an email stating you completed this Perkins/VTEA survey for ***three points extra credit!***



Career Technical Information
Your answers to these questions will help qualify Cabrillo College for Perkins/VTEA grant funds.

Are you currently receiving benefits from:

○ Yes ◉ No	TANF/CALWORKS
○ Yes ◉ No	SSI (Supplemental Security Income)
○ Yes ◉ No	GA (General Assistance)
○ Yes ◉ No	Does your income qualify you for a fee waiver?
○ Yes ◉ No	Are you a single parent with custody of one or more minor children?
○ Yes ◉ No	Are you a displaced homemaker attending Cabrillo to develop job skills?
○ Yes ◉ No	Have you moved in the preceding 36 months to obtain, or to accompany parents or spouses to obtain, temporary or seasonal employment in agriculture, dairy, or fishing?

Wireshark Class
If Interested - Enroll ASAP!

HYBRID COURSES
(part face-to-face/part online)

Course	Title	Section #	Dates	# Weeks	Campus	Day/Time	Units
CIS 140NA	Network Analysis using Wireshark	2	9/26-12/12	12	Aptos	Tue 8:00am-10:50am	3.00

CIS 140NA Network Analysis using Wireshark
Prerequisite: CIS 82 or CIS 83.
Recommended Preparation: Eligibility for ENGL 100 or ESL 100 and READ 100.
Repeatability: May be taken a total of 1 time.

Teaches practical network management skills using the Wireshark network analyzer.
Provides a logical troubleshooting approach to capturing and analyzing data frames.
Teaches to effectively troubleshoot, maintain, optimize, and monitor network traffic.
May be offered in a Distance-Learning Format.

Attack Phases

EC-Council Five Phases of Hacking

Phase 1 - Reconnaissance

Phase 2 - Scanning

Phase 3 - Gaining Access

Phase 4 - Maintaining Access

Phase 5 - Clearing Tracks

http://www.techrepublic.com/blog/it-security/the-five-phases-of-a-successful-network-penetration/

INFOSEC
APT (Advanced Persistent Threat) Life Cycle

Phase 1 - Reconnaissance

Phase 2 - Spear phishing attacks

Phase 3 - Establish presence

Phase 4 - Exploration and Pivoting

Phase 5 - Data Extraction

Phase 6 - Maintaining Persistence

http://www.techrepublic.com/blog/it-security/the-five-phases-of-a-successful-network-penetration/

NSA Intrusion Phases

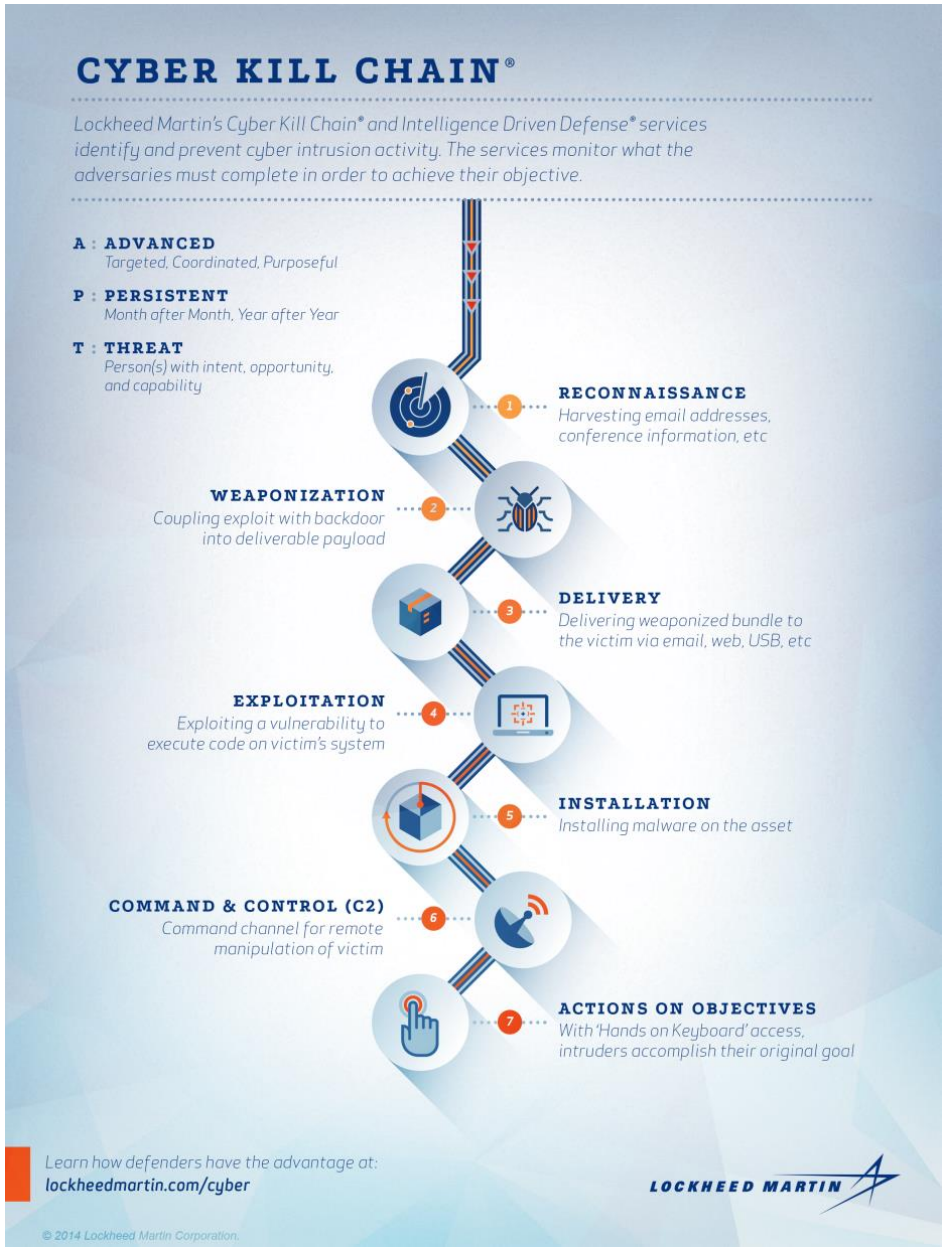
1. Reconnaissance
2. Initial exploitation
3. Establish Persistence
4. Install Tools
5. Move Laterally
6. Collect, "exfil", and exploit

https://www.usenix.org/conference/enigma2016/conference-program/presentation/joyce

Kill Chain
SANS Talk by Paul A. Henry

1. Initial Recon
2. Initial Compromise
3. Establish Foothold
4. Escalate Privileges
5. Internal Recon
6. Move Laterally (Gather PII)
7. Maintain Presence (Prepare for exfiltration)
8. Complete Mission

https://www.sans.org/talks/655/kill-chain-singapore-2017-10-24



Cyber Kill Chain Lockheed-Martin

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command & Control (C2)
7. Action of Objectives

http://www.lockheedmartin.com/us/news/features/2014/isgs-cyber-kill-chain.html

Footprinting and Reconnaissance

Reconnaissance

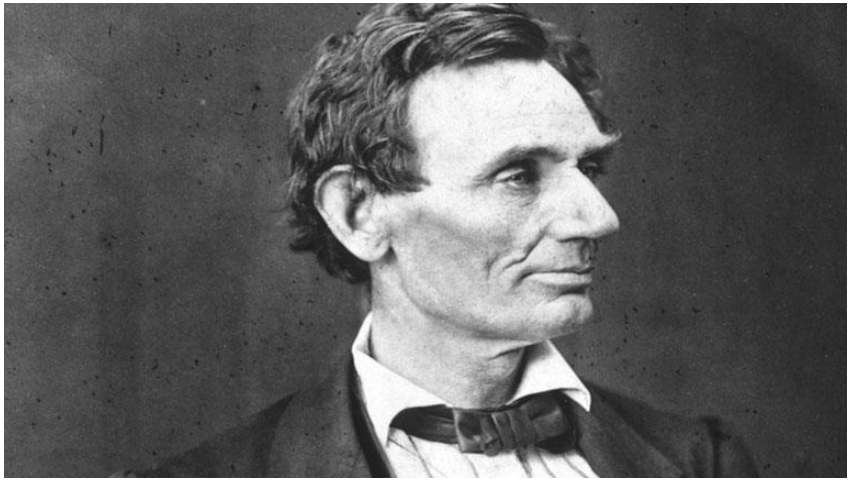
- Also known as "footprinting", "casing the joint", and "information gathering".
- The goal is to learn as much information about the target as possible without being detected.
- Gather information such as:
  - People and organizational structure
  - Related third parties
  - System and network technology used
  - Content of interest
  - Security measures
  - Physical locations and layouts

Reconnaissance

- Not covered in depth by the Netlab+ labs.
- Hard to defend against:
  - Companies need to advertise.
  - Companies need to post job openings.
  - Can't control their employees outside of work.
- Searching the Internet is a legal way to obtain information.

Reconnaissance

- One of the most time consuming phases.



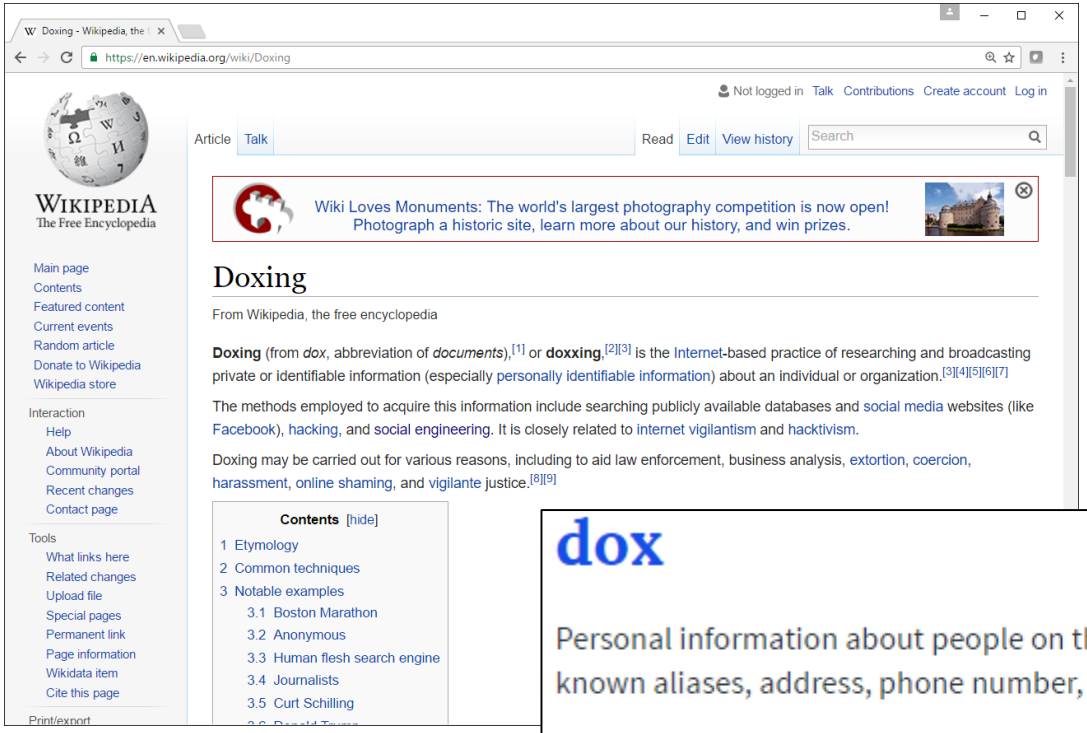
If I had eight hours to chop down a tree, I'd spend the first six hours sharpening my ax.

Reconnaissance

- Active vs. Passive: Have you touched the target?
- Passive: Using methods where you will not be detected by the target.
- Semi-passive: Using methods that appear as normal Internet traffic.
- Active: port scans, vulnerability scans, testing input validation filters, searching for unpublished servers or directories.

http://www.securitysift.com/passive-reconnaissance/

Doxing



https://en.wikipedia.org/wiki/Doxing

dox

Personal information about people on the Internet, often including real name, known aliases, address, phone number, SSN, credit card number, etc.

"Someone dropped Bob's dox and the next day, ten pizzas and three tow trucks showed up at his house."

#lulz #owned #hacker #social engineering #ruin

http://www.urbandictionary.com/define.php?term=dox

Creating a "dossier" on someone or an organization

Domain Name System

Overview

DNS - Domain Name System

The world with DNS

The world without DNS

*Note: Either **www.cabrillo.edu** or **207.62.187.7** will work to reach Cabrillo's web server.*

But which is easier to remember?

An Overview of Domain Name System

Created in 1983 from the work led by Paul Mockapetris
Improves the deficiencies of the */etc/hosts* file
DNS manages two databases (zones)
- Forward lookup zones: for mapping Domain names to IP addresses
- Reverse lookup zones: for mapping IP addresses to Domain names

Three components to DNS:
- Resolver
- The Server
  - Primary
  - Secondary
  - Caching
- Database files (db.*domain-name)*

Supports two type of queries:
- Recursive
- Iterative

Most popular implementation of DNS is Berkely Internet Name Daemon (BIND)
Maintained by the Internet Systems Consortium: *www.isc.org*

Source: Jim Griffin's CIS 192 course

DNS - Forward and Reverse Lookups

Forward lookup (Name to IP address)

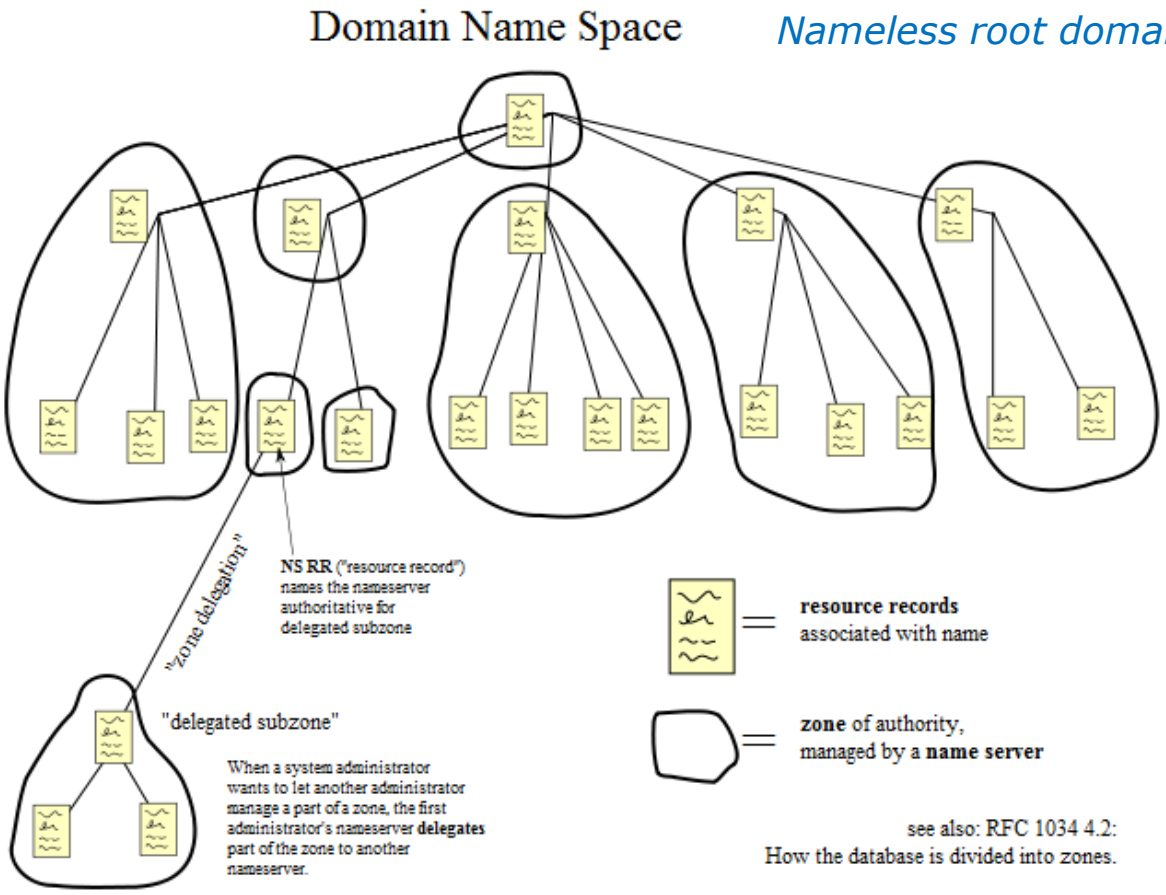
```
root@kali:~# host opus.cis.cabrillo.edu
opus.cis.cabrillo.edu is an alias for oslab.cis.cabrillo.edu.
oslab.cis.cabrillo.edu has address 207.62.187.230
oslab.cis.cabrillo.edu has IPv6 address 2607:f380:80f:f425::230
root@kali:~#
```

Reverse lookup (IP address to name)

```
root@kali:~# host 207.62.187.230
230.187.62.207.in-addr.arpa is an alias for 230.224-27.187.62.207.in-
addr.arpa.
230.224-27.187.62.207.in-addr.arpa domain name pointer
oslab.cis.cabrillo.edu.

root@kali:~# host 2607:f380:80f:f425::230
0.3.2.0.0.0.0.0.0.0.0.0.0.0.0.0.5.2.4.f.f.0.8.0.0.8.3.f.7.0.6.2.ip6.arpa
domain name pointer oslab.cis.cabrillo.edu.
```

DNS works both ways

DNS - Hierarchy of authority



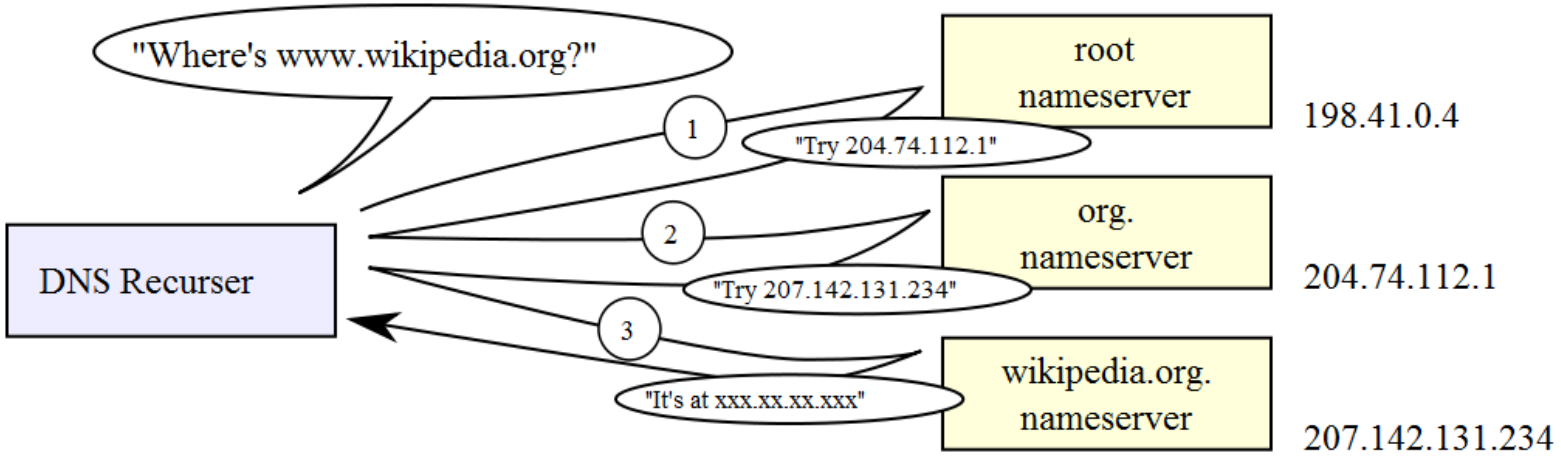
Nameless root domain referred to via "."

Generic TLD's - Top Level Domains (com, edu, net, org, mil, etc.)

Next level domains (e.g. hp.com, cabrillo.edu, yahoo.com, webhawks.org, etc.

source: http://en.wikipedia.org/wiki/File:Domain_name_space.svg

DNS - Queries



http://en.wikipedia.org/wiki/File:An_example_of_theoretical_DNS_recursion.svg

One place where recursion is often used is with the local name server on a network. Rather than making client machine resolvers perform iterative resolution, it is common for the resolver to generate a recursive request to the local DNS server, which then generates iterative requests to other servers as needed. As you can see, recursive and iterative requests can be combined in a single resolution, providing significant flexibility to the process as a whole.

http://www.tcpipguide.com/free/t_DNSBasicNameResolutionTechniquesIterativeandRecurs-4.htm

DNS Database Resource Record types

SOA - Start of Authority

NS - Nameserver

A - IPv4 Address

AAAA - IPv6 Address

PTR - Pointer (for reverse lookups)

CNAME - Aliases

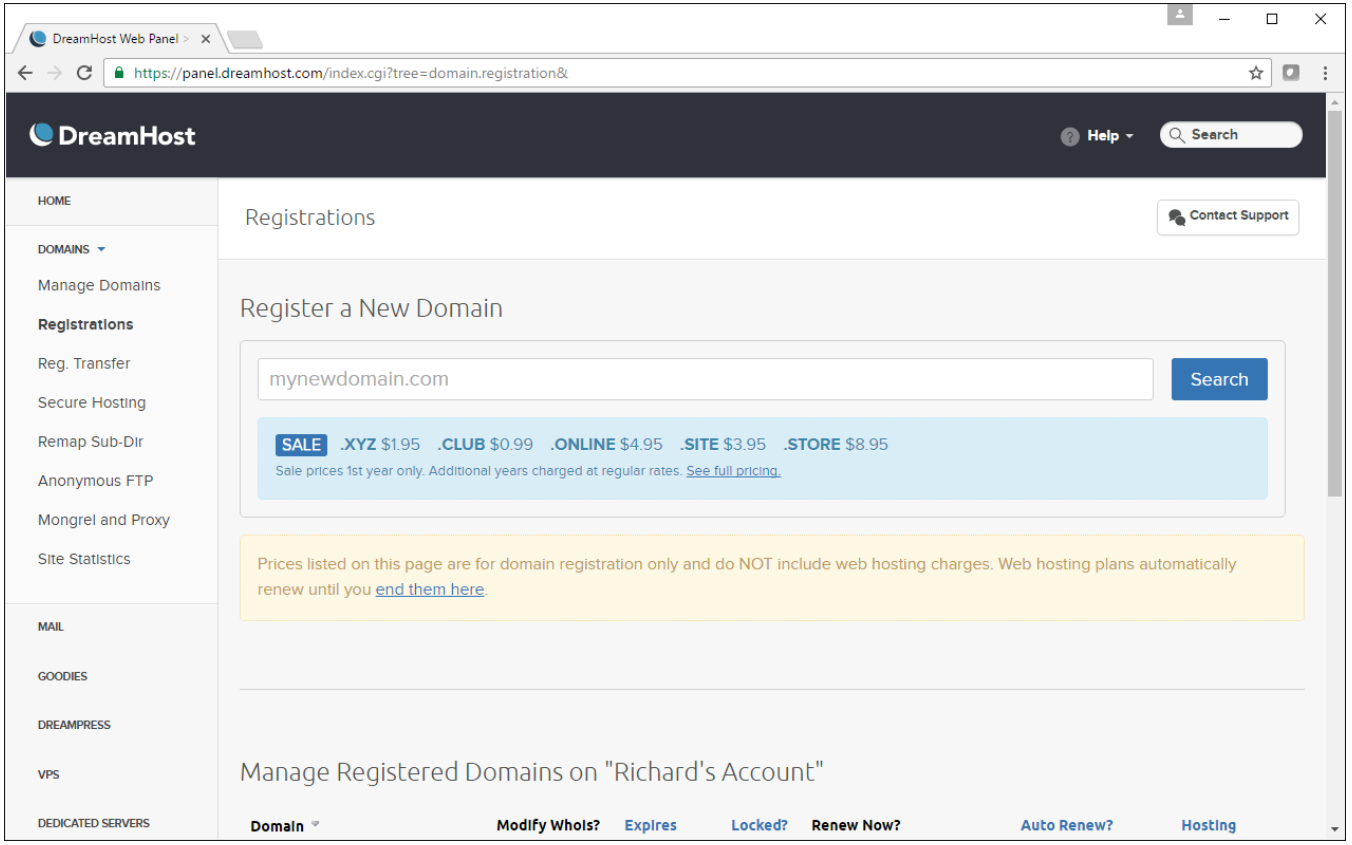
MX - Mail hubs

TXT - associate text strings with a name

Getting a Domain

whois command

Anyone can register a domain



There is a registry of contact information for every domain registered. Often ISPs will let you use their contact information rather than your own.

Linux whois command

root@eh-kali-05: ~

File Edit View Search Terminal Help

```
root@eh-kali-05:~# whois simms-teach.com

Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

   Domain Name: SIMMS-TEACH.COM
   Registrar: DREAMHOST, LLC
   Sponsoring Registrar IANA ID: 431
   Whois Server: whois.dreamhost.com
   Referral URL: http://www.DreamHost.com
   Name Server: NS1.DREAMHOST.COM
   Name Server: NS2.DREAMHOST.COM
   Name Server: NS3.DREAMHOST.COM
   Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Updated Date: 16-may-2016
   Creation Date: 15-may-2008
   Expiration Date: 15-may-2017

>>> Last update of whois database: Sun, 18 Sep 2016 21:28:15 GMT <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
```

Domain information fields

Linux whois command

root@eh-kali-05: ~

File Edit View Search Terminal Help

```
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability.  VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.


Domain Name: SIMMS-TEACH.COM
Registry Domain ID: 1472785313_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.dreamhost.com
Registrar URL: www.dreamhost.com
Updated Date: 2016-05-17T00:43:20.00Z
Creation Date: 2008-05-15T11:21:10.00Z
Registrar Registration Expiration Date: 2017-05-15T18:21:10.00Z
Registrar: DREAMHOST
Registrar IANA ID: 431
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: PRIVATE REGISTRANT
Registrant Organization: A HAPPY DREAMHOST CUSTOMER
Registrant Street: 417 ASSOCIATED RD #324
Registrant Street: C/O SIMMS-TEACH.COM
```

Registrant contact fields

Linux whois command

root@eh-kali-05: ~

File Edit View Search Terminal Help

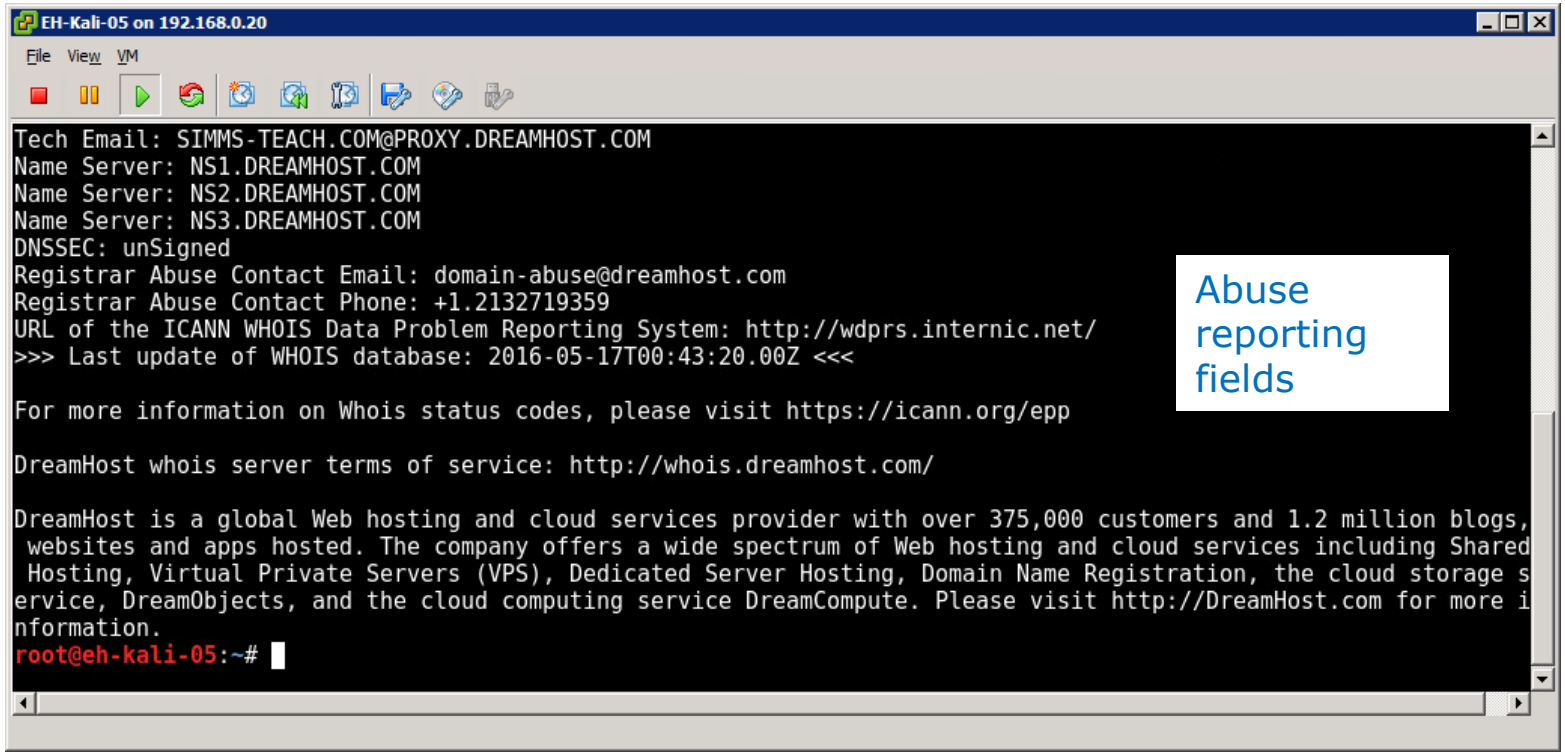
```
Registrant Street: C/O SIMMS-TEACH.COM
Registrant City: BREA
Registrant State/Province: CA
Registrant Postal Code: 92821
Registrant Country: US
Registrant Phone: +1.7147064182
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: SIMMS-TEACH.COM@PROXY.DREAMHOST.COM
Registry Admin ID:
Admin Name: PRIVATE REGISTRANT
Admin Organization: A HAPPY DREAMHOST CUSTOMER
Admin Street: 417 ASSOCIATED RD #324
Admin Street: C/O SIMMS-TEACH.COM
Admin City: BREA
Admin State/Province: CA
Admin Postal Code: 92821
Admin Country: US
Admin Phone: +1.7147064182
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: SIMMS-TEACH.COM@PROXY.DREAMHOST.COM
Registry Tech ID:
Tech Name: PRIVATE REGISTRANT
Tech Organization: A HAPPY DREAMHOST CUSTOMER
Tech Street: 417 ASSOCIATED RD #324
Tech Street: C/O SIMMS-TEACH.COM
Tech City: BREA
Tech State/Province: CA
Tech Postal Code: 92821
Tech Country: US
Tech Phone: +1.7147064182
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: SIMMS-TEACH.COM@PROXY.DREAMHOST.COM
```

Registrant contact fields

Admin contact fields

Tech contact fields

Linux whois command



One of the fields can be use to report abuse coming from hosts on the domain.

Activity

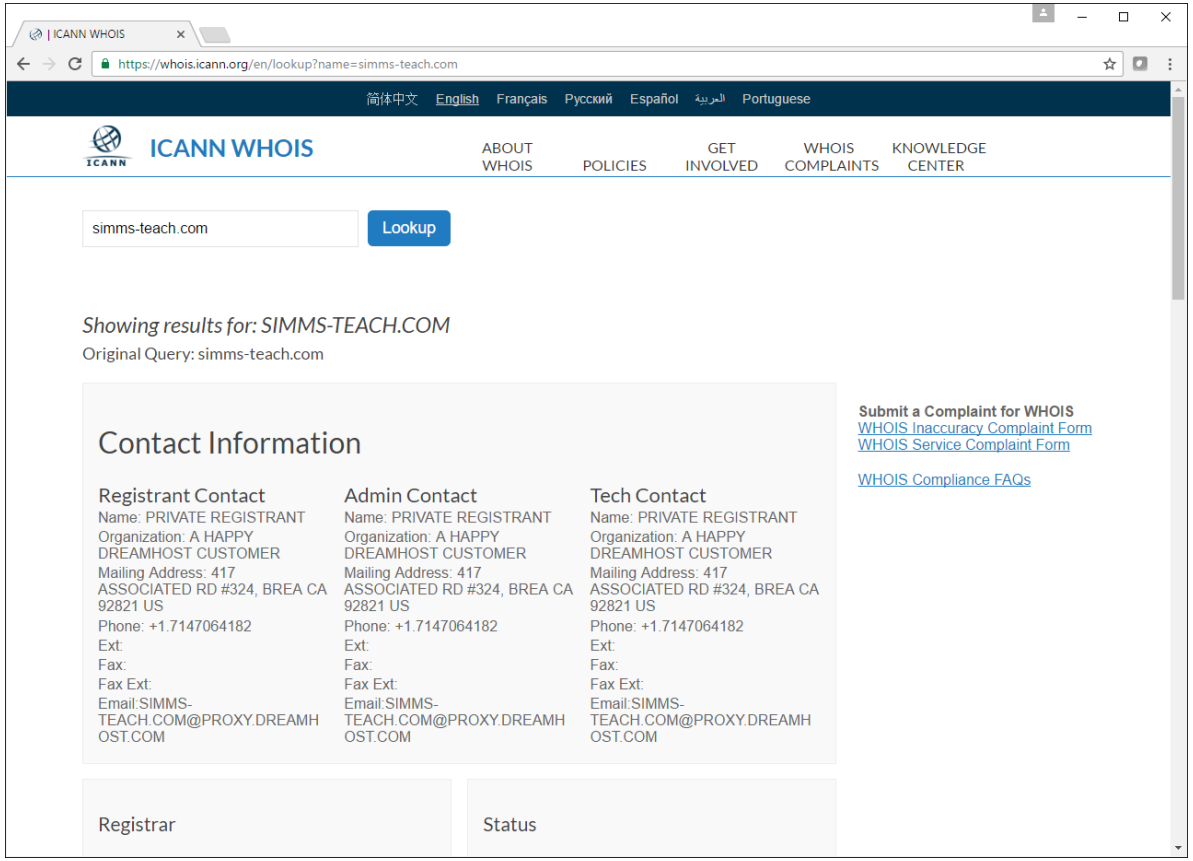
Using only the **whois** command see if you can find two contacts at Beloit College in Wisconsin.

Write their first names into the chat window.

Domain Information

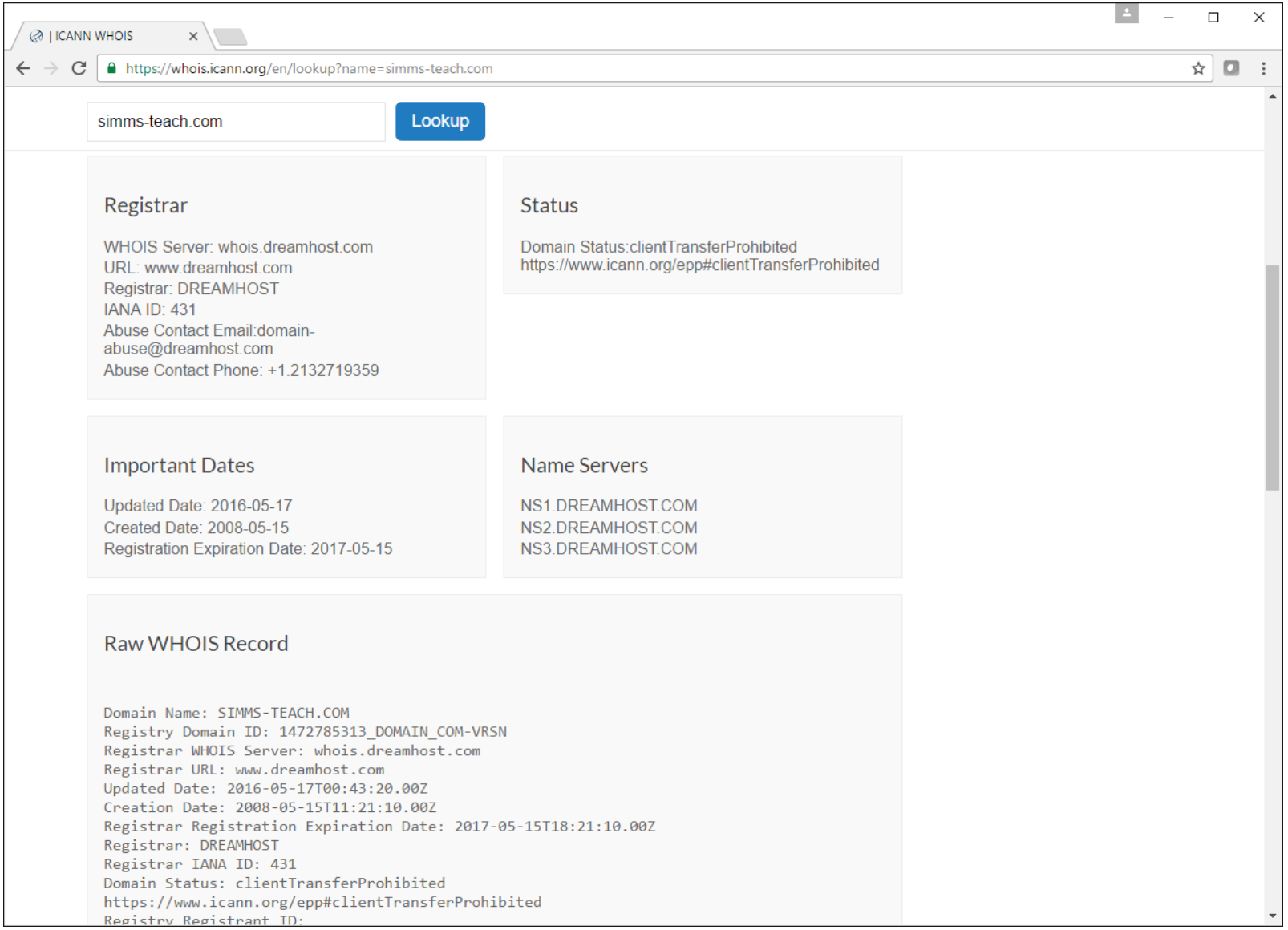
whois.icann.org

http://whois.icann.org

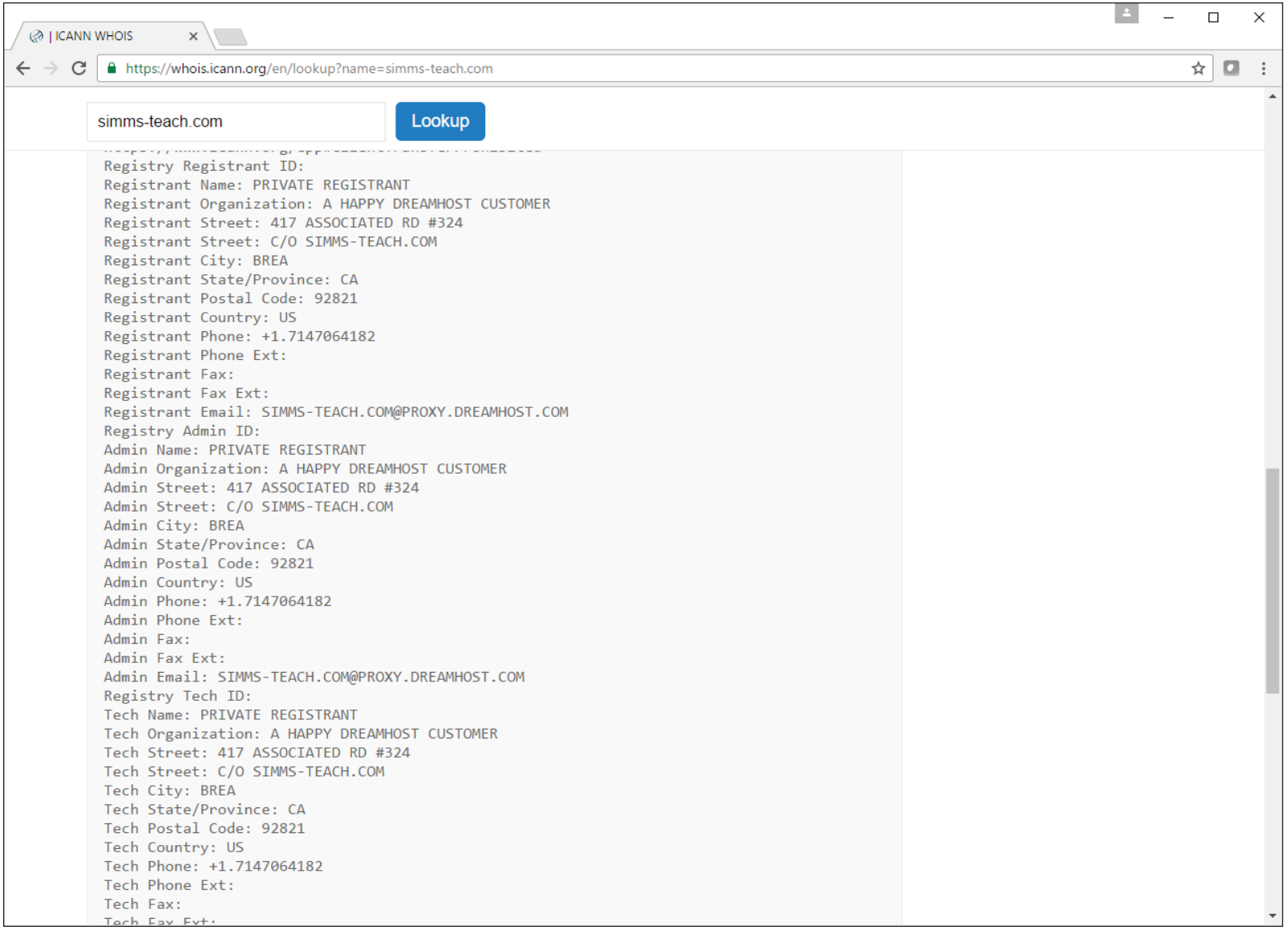


Provides a web interface for getting whois information

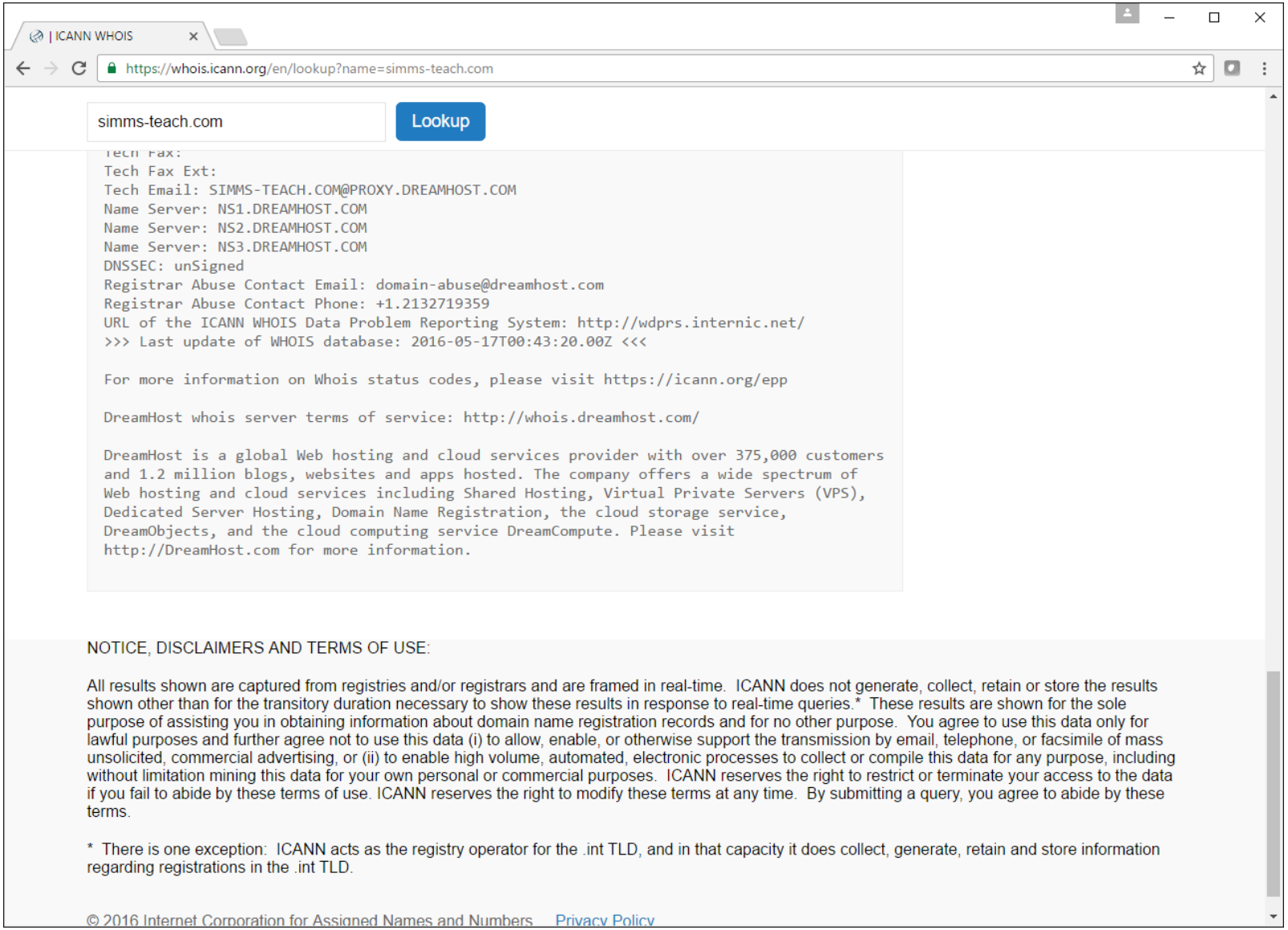
http://whois.icann.org



http://whois.icann.org



http://whois.icann.org



Activity

Using only: http://whois.icann.org

See if you can find a technical contact for the simms-teach.com domain.

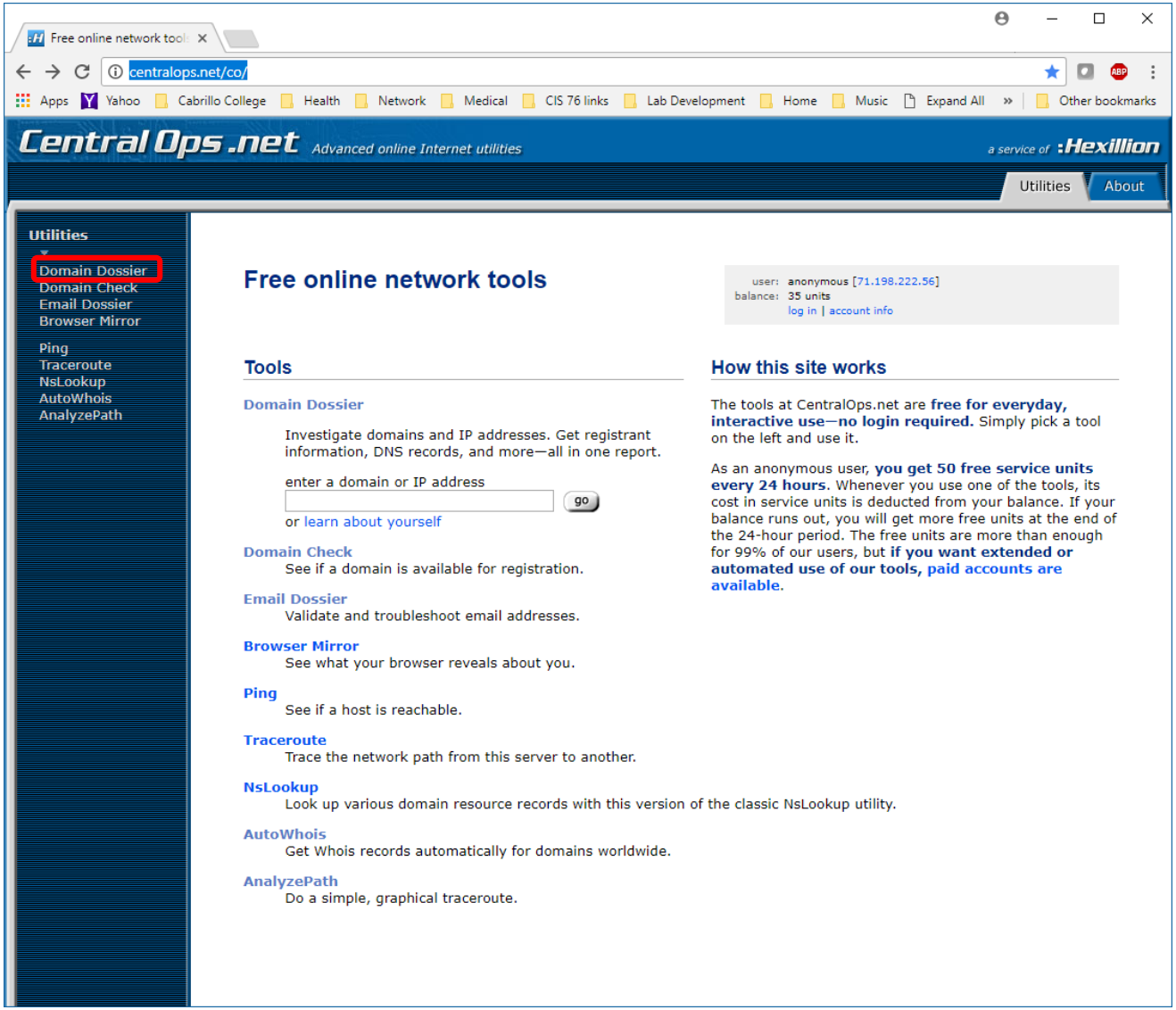
What is the email address for the Technical Contact?

Put your answer in the chat window

Domain Information

Domain Dossier

centralops.net

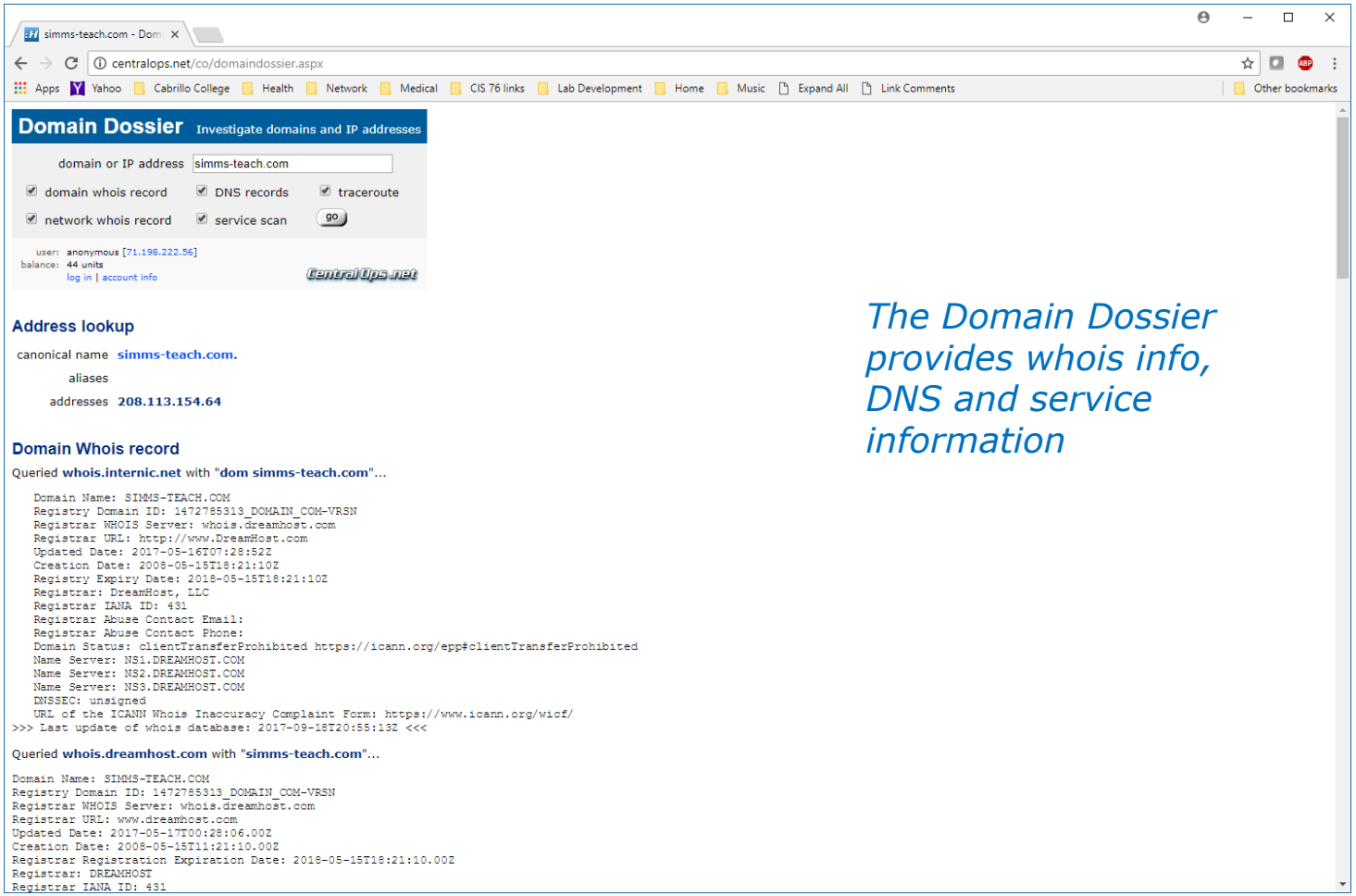


Free online anonymous tools

Click on the Domain Dossier link on the left panel

http://centralops.net/co

http://centralops.net/co/domaindossier.aspx



The Domain Dossier provides whois info, DNS and service information

Activity

Using the Domain Dossier website:

http://centralops.net/co/domaindossier.aspx

See if you can find the administrative contact for the mit.edu domain.

Put their first name and the phone number in the chat window

host & nslookup commands

Forward and reverse DNS lookups

host command

```
rsimms@oslab:~

NAME
       host - DNS lookup utility

SYNOPSIS
       host [-aCdlnrsTwv] [-c class] [-N ndots] [-R number] [-t type]
            [-W wait] [-m flag] [-4] [-6] {name} [server]

DESCRIPTION
       host is a simple utility for performing DNS lookups. It is normally
       used to convert names to IP addresses and vice versa. When no
       arguments or options are given, host prints a short summary of its
       command line arguments and options.

       name is the domain name that is to be looked up. It can also be a
       dotted-decimal IPv4 address or a colon-delimited IPv6 address, in
       which case host will by default perform a reverse lookup for that
       address.  server is an optional argument which is either the name or
       IP address of the name server that host should query instead of the
       server or servers listed in /etc/resolv.conf.
:
```

Easy to use Linux command for resolving names or IP addresses

host command on Linux

Forward lookup

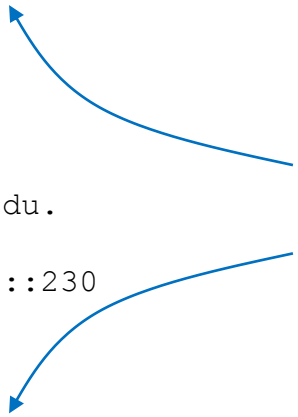
```
[rsimms@oslab ~]$ host www.google.com
www.google.com has address 216.58.193.196
www.google.com has IPv6 address 2607:f8b0:4007:80b::2004
[rsimms@oslab ~]$
```

Reverse lookup

```
[rsimms@oslab ~]$ host 216.58.193.196
196.193.58.216.in-addr.arpa domain name pointer lax02s23-in-f4.1e100.net.
196.193.58.216.in-addr.arpa domain name pointer lax02s23-in-f196.1e100.net.
[rsimms@oslab ~]$
```

host command on Linux

```
root@kali:~# host opus.cis.cabrillo.edu ns1.cis.cabrillo.edu
Using domain server:
Name: ns1.cis.cabrillo.edu
Address: 2607:f380:80f:f425::252#53
Aliases:

opus.cis.cabrillo.edu is an alias for oslab.cis.cabrillo.edu.
oslab.cis.cabrillo.edu has address 207.62.187.230
oslab.cis.cabrillo.edu has IPv6 address 2607:f380:80f:f425::230
root@kali:~#


root@kali:~# host opus.cis.cabrillo.edu ns2.cis.cabrillo.edu
Using domain server:
Name: ns2.cis.cabrillo.edu
Address: 2607:f380:80f:f425::253#53
Aliases:

opus.cis.cabrillo.edu is an alias for oslab.cis.cabrillo.edu.
oslab.cis.cabrillo.edu has address 207.62.187.230
oslab.cis.cabrillo.edu has IPv6 address 2607:f380:80f:f425::230
root@kali:~#
```



Specifying a specific name server to do the name resolution

nslookup command on Windows

Forward lookup

```
C:\Users\rich>nslookup opus-ii.cis.cabrillo.edu
Server:  router.asus.com
Address:  192.168.1.1

Non-authoritative answer:
Name:    opus-ii.cis.cabrillo.edu
Addresses:  2607:f380:80f:f425::244
          207.62.187.244
```

Reverse lookup

```
C:\Users\rich>nslookup 207.62.187.244
Server:  router.asus.com
Address:  192.168.1.1

Name:    opus-ii.cis.cabrillo.edu
Address:  207.62.187.244
Aliases:  244.187.62.207.in-addr.arpa
```

Activity

Using the host command to do a forward lookup on:

`simms-teach.com`

Put the IP address in the chat window

Activity

Using the host command to do a reverse lookup on:

`208.113.154.64`

What ISP am I hosting my website on?

Put your answer in the chat window

Domain Records

dig

dig command

rsimms@opus-ii:~

```
DIG(1)                                    BIND9                                    DIG(1)

NAME
       dig - DNS lookup utility

SYNOPSIS
       dig [@server] [-b address] [-c class] [-f filename] [-k filename] [-m] [-p port#] [-q name] [-t type]
           [-x addr] [-y [hmac:]name:key] [-4] [-6] [name] [type] [class] [queryopt...]

       dig [-h]

       dig [global-queryopt...] [query...]

DESCRIPTION
       dig (domain information groper) is a flexible tool for interrogating DNS name servers. It performs DNS
       lookups and displays the answers that are returned from the name server(s) that were queried. Most DNS
       administrators use dig to troubleshoot DNS problems because of its flexibility, ease of use and clarity
       of output. Other lookup tools tend to have less functionality than dig.

       Although dig is normally used with command-line arguments, it also has a batch mode of operation for
       reading lookup requests from a file. A brief summary of its command-line arguments and options is
       printed when the -h option is given. Unlike earlier versions, the BIND 9 implementation of dig allows
       multiple lookups to be issued from the command line.

       Unless it is told to query a specific name server, dig will try each of the servers listed in
       /etc/resolv.conf. If no usable server addreses are found, dig will send the query to the local host.

       When no command line arguments or options are given, dig will perform an NS query for "." (the root).

       It is possible to set per-user defaults for dig via ${HOME}/.digrc. This file is read and any options
       in it are applied before the command line arguments.

 Manual page dig(1) line 1 (press h for help or q to quit)
```

Get DNS records from name servers

Find domain name servers

dig ns cis.cabrillo.edu

```
root@eh-kali-05:~# dig ns cis.cabrillo.edu

; <<>> DiG 9.10.3-P4-Debian <<>> ns cis.cabrillo.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17839
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;cis.cabrillo.edu.              IN      NS

;; ANSWER SECTION:
cis.cabrillo.edu.       86400   IN      NS      ns2.cis.cabrillo.edu.
cis.cabrillo.edu.       86400   IN      NS      ns1.cis.cabrillo.edu.

;; ADDITIONAL SECTION:
ns1.cis.cabrillo.edu.   86400   IN      A       172.30.5.101
ns1.cis.cabrillo.edu.   86400   IN      AAAA    2607:f380:80f:f425::252
ns2.cis.cabrillo.edu.   86400   IN      A       172.30.5.102
ns2.cis.cabrillo.edu.   86400   IN      AAAA    2607:f380:80f:f425::253

;; Query time: 2 msec
;; SERVER: 172.30.5.101#53(172.30.5.101)
;; WHEN: Sun Sep 18 15:11:26 PDT 2016
;; MSG SIZE  rcvd: 169

root@eh-kali-05:~#
```

Finding the name servers (ns records) for the cabrillo.edu domain

Find domain mail servers

dig mx cis.cabrillo.edu

```
root@eh-kali-05:~# dig mx cis.cabrillo.edu

; <<>> DiG 9.10.3-P4-Debian <<>> mx cis.cabrillo.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61468
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 7

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;cis.cabrillo.edu.              IN      MX

;; ANSWER SECTION:
cis.cabrillo.edu.       86400   IN      MX      10 oslab.cis.cabrillo.edu.

;; AUTHORITY SECTION:
cis.cabrillo.edu.       86400   IN      NS      ns1.cis.cabrillo.edu.
cis.cabrillo.edu.       86400   IN      NS      ns2.cis.cabrillo.edu.

;; ADDITIONAL SECTION:
oslab.cis.cabrillo.edu. 86400   IN      A       172.30.5.20
oslab.cis.cabrillo.edu. 86400   IN      AAAA    2607:f380:80f:f425::230
ns1.cis.cabrillo.edu.   86400   IN      A       172.30.5.101
ns1.cis.cabrillo.edu.   86400   IN      AAAA    2607:f380:80f:f425::252
ns2.cis.cabrillo.edu.   86400   IN      A       172.30.5.102
ns2.cis.cabrillo.edu.   86400   IN      AAAA    2607:f380:80f:f425::253

;; Query time: 2 msec
;; SERVER: 172.30.5.101#53(172.30.5.101)
;; WHEN: Sun Sep 18 15:29:00 PDT 2016
;; MSG SIZE  rcvd: 235

root@eh-kali-05:~#
```

Finding the mail servers (mx records) for the cis.cabrillo.edu domain

Find domain administrative contact

dig soa cis.cabrillo.edu

```
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27990
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;cis.cabrillo.edu.              IN      SOA

;; ANSWER SECTION:
cis.cabrillo.edu.       86400   IN      SOA     ns1.cis.cabrillo.edu. cis-netadmin.cabrillo.edu. 2016091200 1800
 900 604800 1800

;; AUTHORITY SECTION:
cis.cabrillo.edu.       86400   IN      NS      ns1.cis.cabrillo.edu.
cis.cabrillo.edu.       86400   IN      NS      ns2.cis.cabrillo.edu.

;; ADDITIONAL SECTION:
ns1.cis.cabrillo.edu.   86400   IN      A       172.30.5.101
ns1.cis.cabrillo.edu.   86400   IN      AAAA    2607:f380:80f:f425::252
ns2.cis.cabrillo.edu.   86400   IN      A       172.30.5.102
ns2.cis.cabrillo.edu.   86400   IN      AAAA    2607:f380:80f:f425::253

;; Query time: 2 msec
;; SERVER: 172.30.5.101#53(172.30.5.101)
;; WHEN: Sun Sep 18 15:25:19 PDT 2016
;; MSG SIZE  rcvd: 218

root@eh-kali-05:~#
```

email address of administrator

Finding the Start of Authority records for the cis.cabrillo.edu domain

Find domain hosts via zone transfer

dig axfr cis.cabrillo.edu

```
[root@ns2 ~]# dig axfr cis.cabrillo.edu

; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.47.rc1.el6 <<>> axfr cis.cabrillo.edu
;; global options: +cmd
cis.cabrillo.edu.       86400   IN      SOA     ns1.cis.cabrillo.edu. cis-netadmin.cab
rillo.edu. 2016091200 1800 900 604800 1800
cis.cabrillo.edu.       86400   IN      TXT     "v=spf1 ip4:207.62.187.0/24 ip6:2607:f
380:80f:f425::/32 -all"
cis.cabrillo.edu.       86400   IN      MX      10 oslab.cis.cabrillo.edu.
cis.cabrillo.edu.       86400   IN      NS      ns1.cis.cabrillo.edu.
cis.cabrillo.edu.       86400   IN      NS      ns2.cis.cabrillo.edu.
APC-01.cis.cabrillo.edu. 86400  IN      A       172.30.5.38
apollo.cis.cabrillo.edu. 86400  IN      A       172.20.90.57
Arya-01.cis.cabrillo.edu. 86400 IN      A       172.20.90.101
Arya-02.cis.cabrillo.edu. 86400 IN      A       172.20.90.102
Arya-03.cis.cabrillo.edu. 86400 IN      A       172.20.90.103
```

snipped

```
cis.cabrillo.edu.       86400   IN      SOA     ns1.cis.cabrillo.edu. cis-netadmin.cab
rillo.edu. 2016091200 1800 900 604800 1800
;; Query time: 26 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sun Sep 18 15:25:22 2016
;; XFR size: 480 records (messages 1, bytes 12907)

[root@ns2 ~]#
```

Getting a zone transfer of all hosts. Note: most name servers are configured to never publicly release this information

Examine txt records

dig txt cis.cabrillo.edu

```
rsimms@opus-ii:~
[rsimms@opus-ii ~]$ dig txt cis.cabrillo.edu

; <<>> DiG 9.9.4-RedHat-9.9.4-51.el7 <<>> txt cis.cabrillo.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8167
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;cis.cabrillo.edu.              IN      TXT

;; ANSWER SECTION:
cis.cabrillo.edu.       86400   IN      TXT     "v=spf1 ip4:207.62.187.0/24 ip6:2607:f380:80f::/48 -all"

;; AUTHORITY SECTION:
cis.cabrillo.edu.       86400   IN      NS      ns2.cis.cabrillo.edu.
cis.cabrillo.edu.       86400   IN      NS      ns1.cis.cabrillo.edu.

;; ADDITIONAL SECTION:
ns1.cis.cabrillo.edu.   86400   IN      A       172.30.5.101
ns1.cis.cabrillo.edu.   86400   IN      AAAA    2607:f380:80f:f425::252
ns2.cis.cabrillo.edu.   86400   IN      A       172.30.5.102
ns2.cis.cabrillo.edu.   86400   IN      AAAA    2607:f380:80f:f425::253

;; Query time: 0 msec
;; SERVER: 172.30.5.101#53(172.30.5.101)
;; WHEN: Mon Sep 18 19:20:23 PDT 2017
;; MSG SIZE  rcvd: 236

[rsimms@opus-ii ~]$
```

Looking at txt records may reveal network information

Activity

Using the dig command which domain uses more mx records, google.com or amazon.com?

Write your answer, including the count of mx records, in the chat window.

Activity

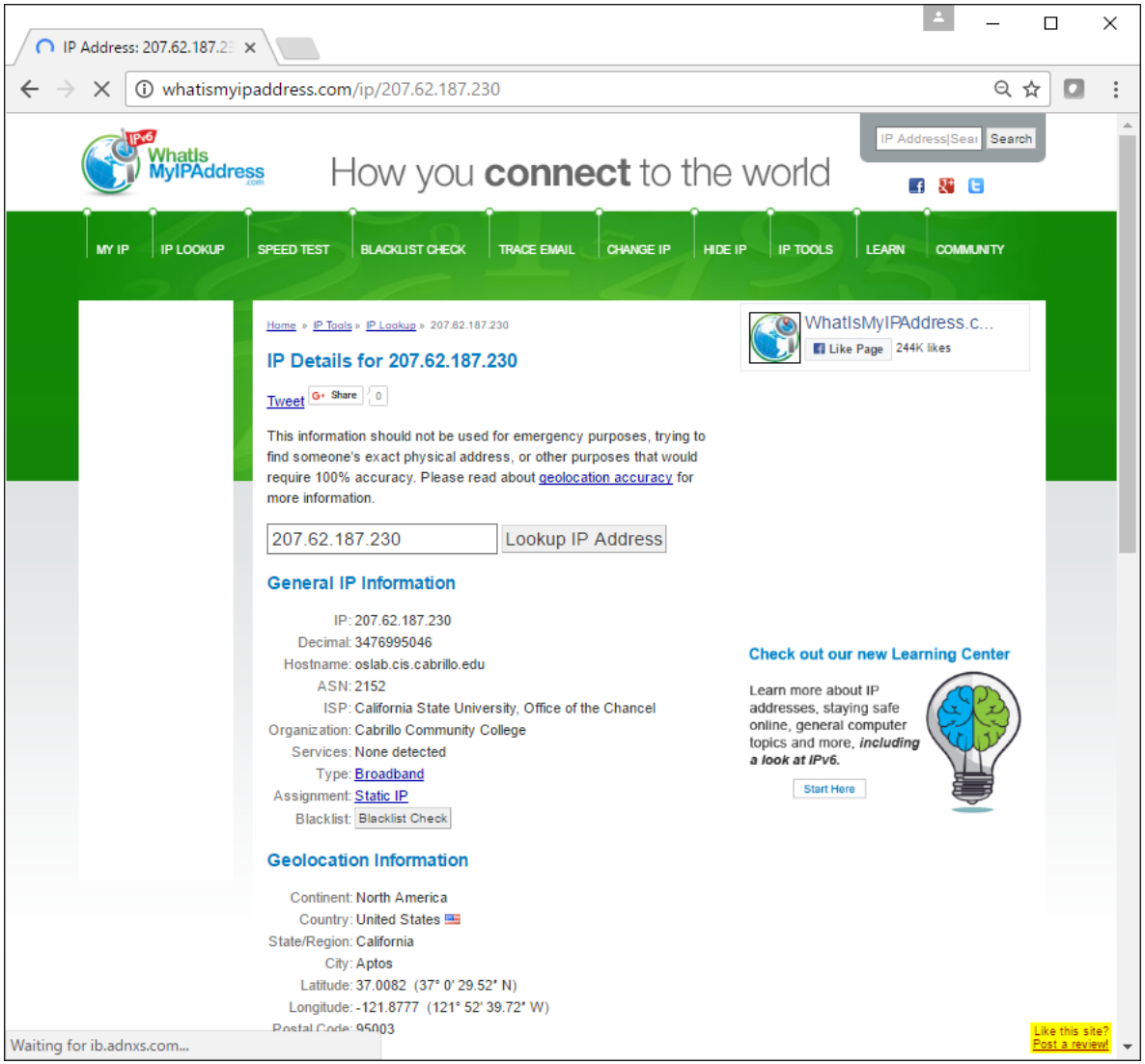
Using the dig command what is the email address of the network contact for umich.edu?

Write your answer in the chat window

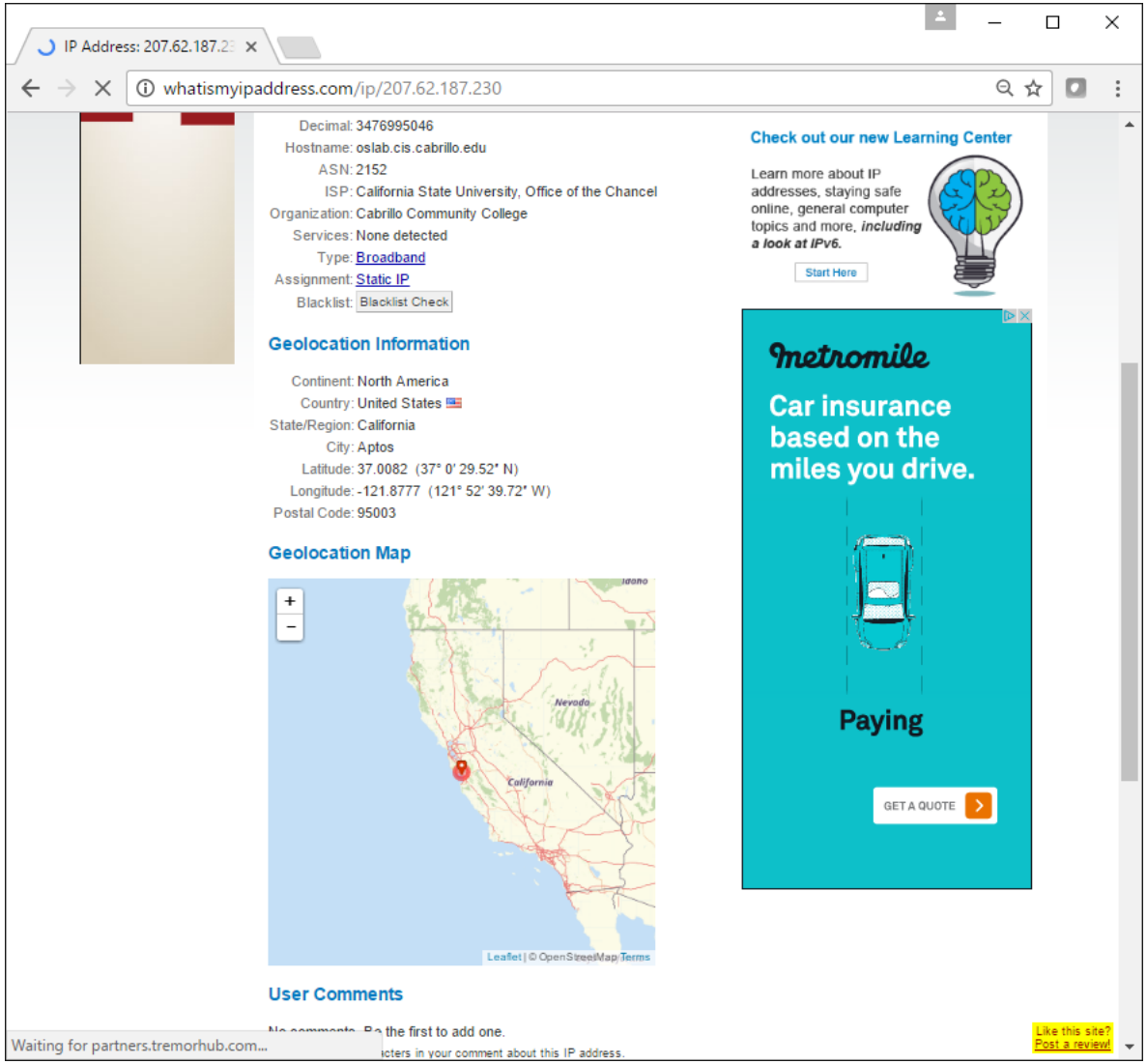
Identifying IP Addresses

whatismyipaddress.com/

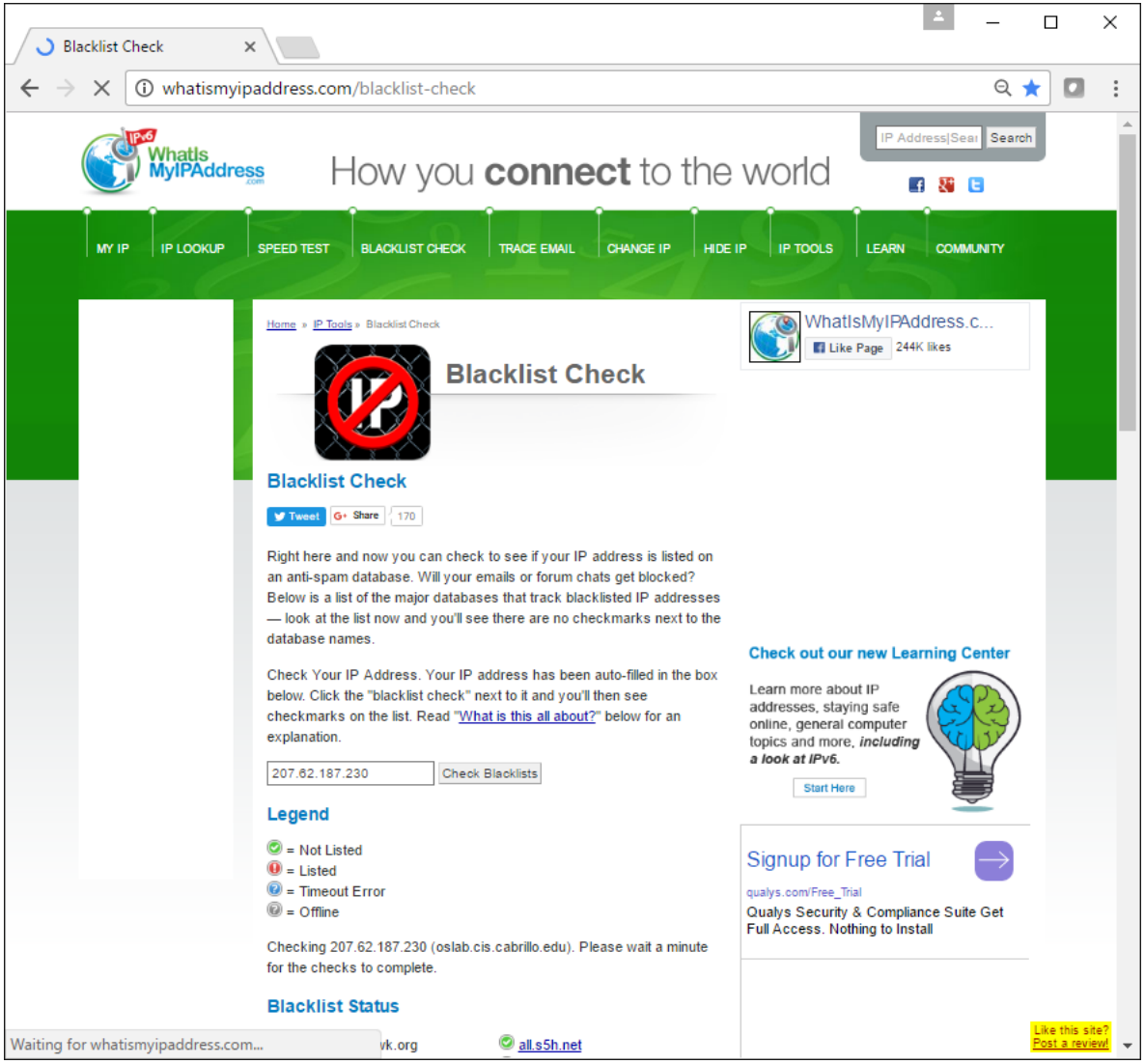
http://whatismyipaddress.com/



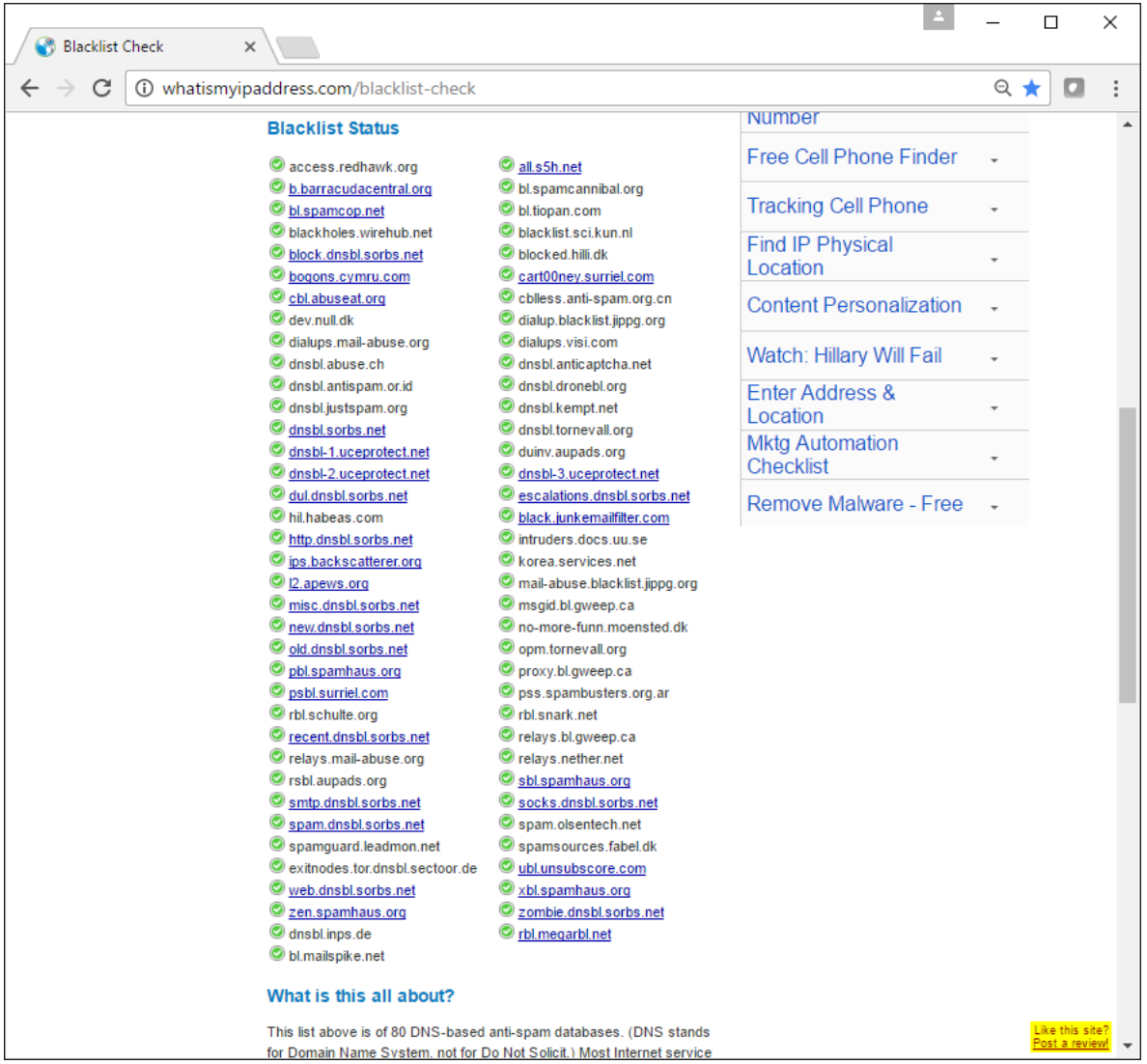
http://whatismyipaddress.com/



http://whatismyipaddress.com/



http://whatismyipaddress.com/



Activity

Top attackers

NoSweat : Sunday, September 17, 2017

Source address	Source Host Name	Source User	Count
203.157.175.9	203.157.175.9		13.61 k
18.220.249.81	ec2-18-220-249-81.us-east-2.compute.amazonaws.com		197
118.69.40.250	lamson.vn		114
62.81.86.6	atf-icfr179036-ovie.red.retevision.es		98
80.241.254.178	host-80-241-254-178.customer.co.ge		70
112.64.33.92	112.64.33.92		4
121.254.231.225	121.254.231.225		2
77.72.82.19	77.72.82.19		1

Pick one of the IP addresses above and using:

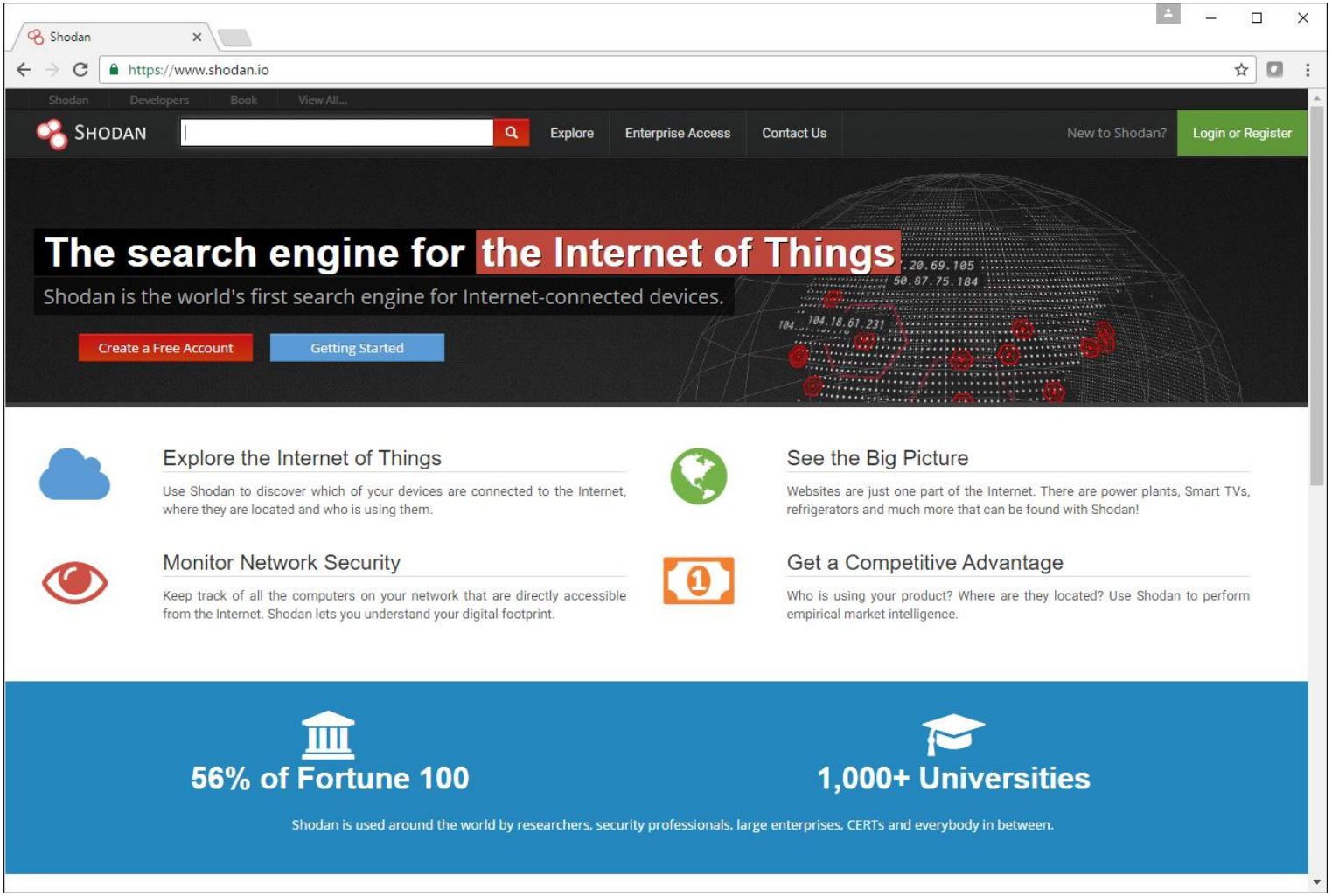
http://whatismyipaddress.com/

Find out who it was assigned to and whether it is blacklisted.

Put the organization name, country, and number of times blacklisted in the chat window

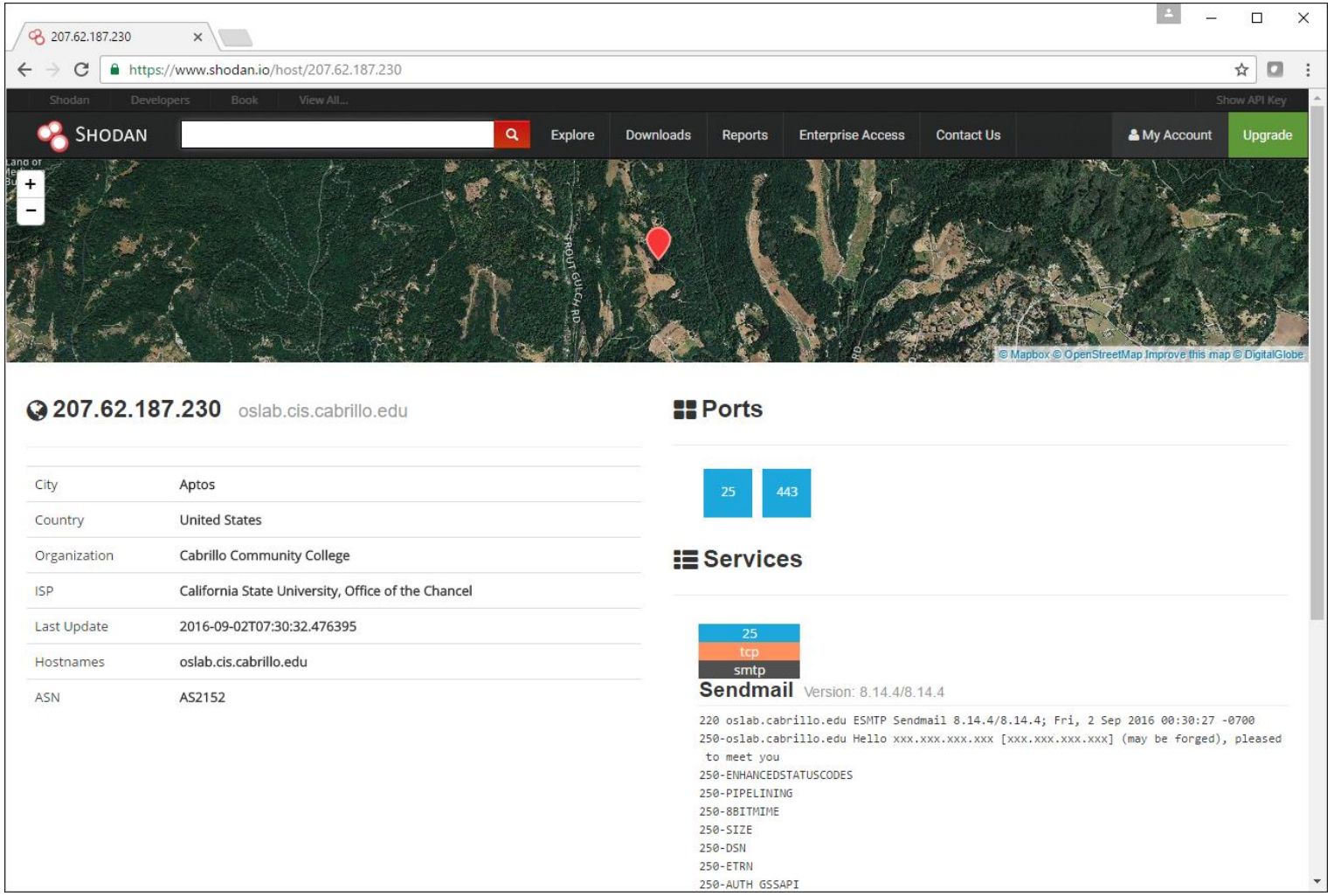
shodan

SHODAN



https://www.shodan.io/

SHODAN



https://www.shodan.io/

SHODAN search filters

Here are the basic search filters you can use:

- **city**: find devices in a particular city
- **country**: find devices in a particular country
- **geo**: you can pass it coordinates
- **hostname**: find values that match the hostname
- **net**: search based on an IP or /x CIDR
- **os**: search based on operating system
- **port**: find particular ports that are open
- **before/after**: find results within a timeframe

Find Apache servers in San Francisco:

```
apache city:"San Francisco"
```

Find Nginx servers in Germany:

```
nginx country:"DE"
```

Find GWS (Google Web Server) servers:

```
"Server: gws" hostname:"google"
```

Find Cisco devices on a particular subnet:

```
cisco net:"216.219.143.0/24"
```

https://danielmiessler.com/study/shodan/

Activity

Use the host command to find the IP address for:

`microlab.simms-teach.com`

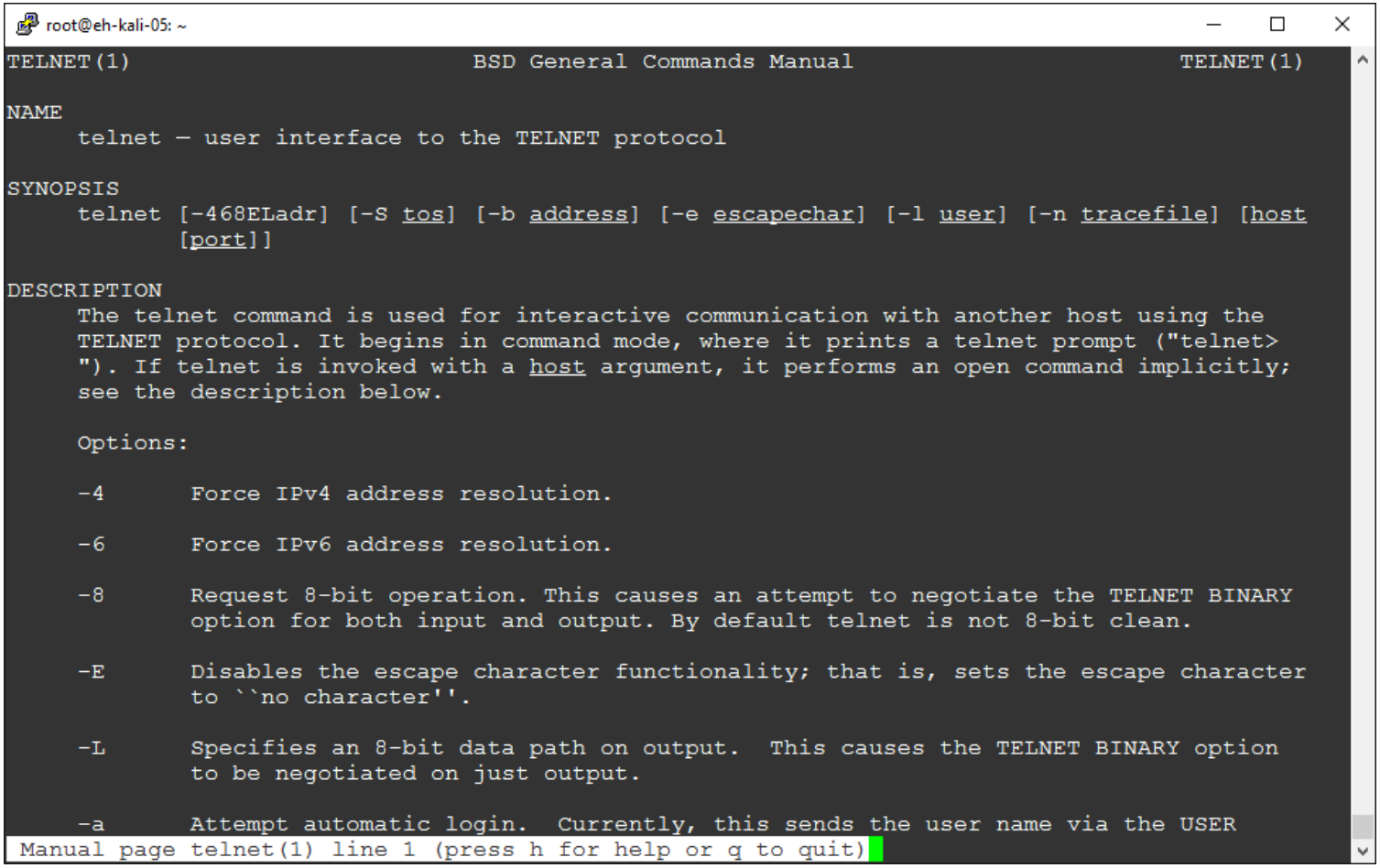
Use shodan: https://www.shodan.io/

to discover passively which ports are open on that IP address.

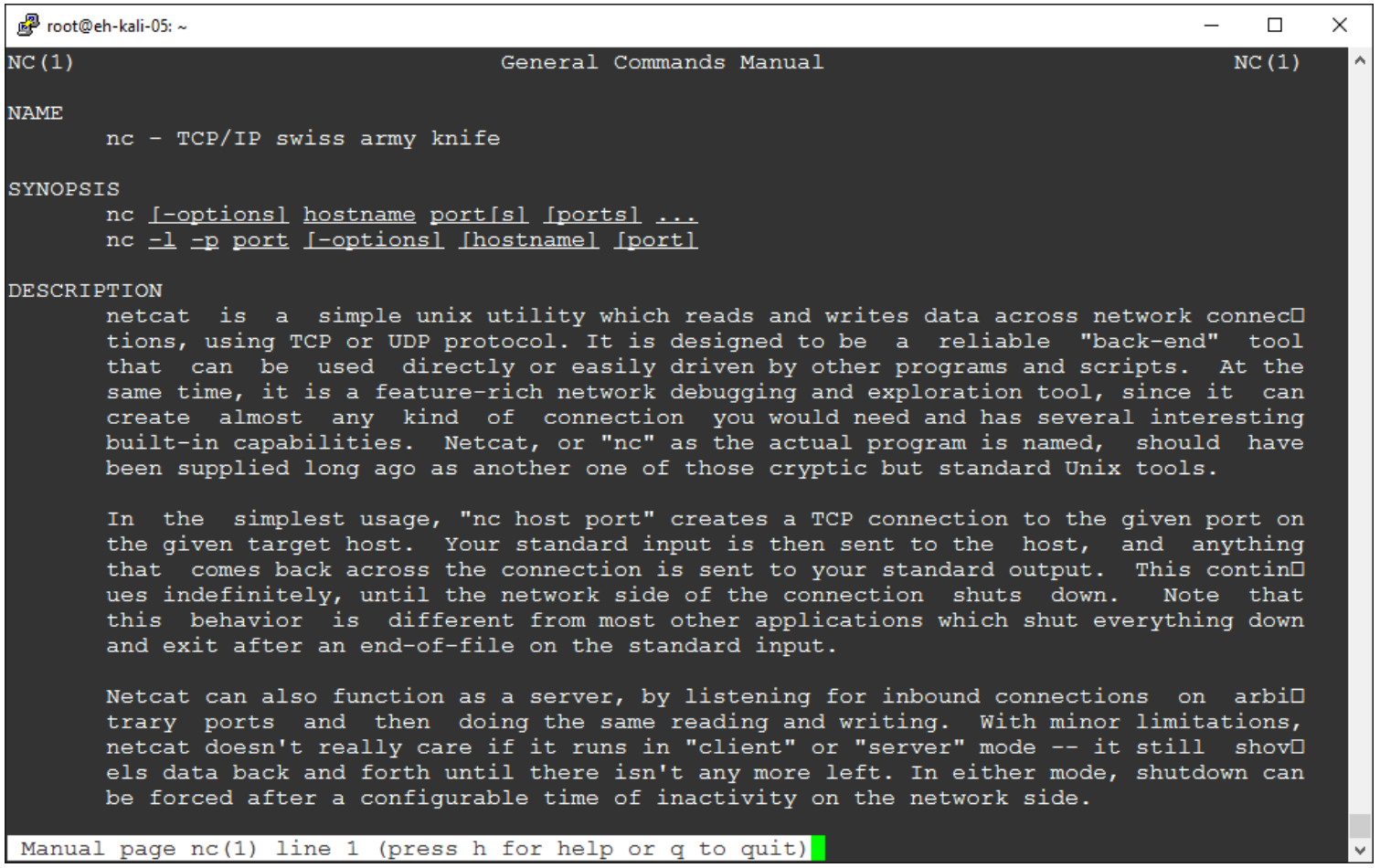
Write those ports in the chat window

Light probing with telnet and nc

telnet command



netcat


root@eh-kali-05: ~
NC(1) General Commands Manual NC(1)
NAME
nc - TCP/IP swiss army knife
SYNOPSIS
nc [-options] hostname port[s] [ports] ...
nc -l -p port [-options] [hostname] [port]
DESCRIPTION
netcat is a simple unix utility which reads and writes data across network connections, using TCP or UDP protocol. It is designed to be a reliable "back-end" tool that can be used directly or easily driven by other programs and scripts. At the same time, it is a feature-rich network debugging and exploration tool, since it can create almost any kind of connection you would need and has several interesting built-in capabilities. Netcat, or "nc" as the actual program is named, should have been supplied long ago as another one of those cryptic but standard Unix tools.
In the simplest usage, "nc host port" creates a TCP connection to the given port on the given target host. Your standard input is then sent to the host, and anything that comes back across the connection is sent to your standard output. This continues indefinitely, until the network side of the connection shuts down. Note that this behavior is different from most other applications which shut everything down and exit after an end-of-file on the standard input.
Netcat can also function as a server, by listening for inbound connections on arbitrary ports and then doing the same reading and writing. With minor limitations, netcat doesn't really care if it runs in "client" or "server" mode -- it still shovels data back and forth until there isn't any more left. In either mode, shutdown can be forced after a configurable time of inactivity on the network side.
Manual page nc(1) line 1 (press h for help or q to quit)

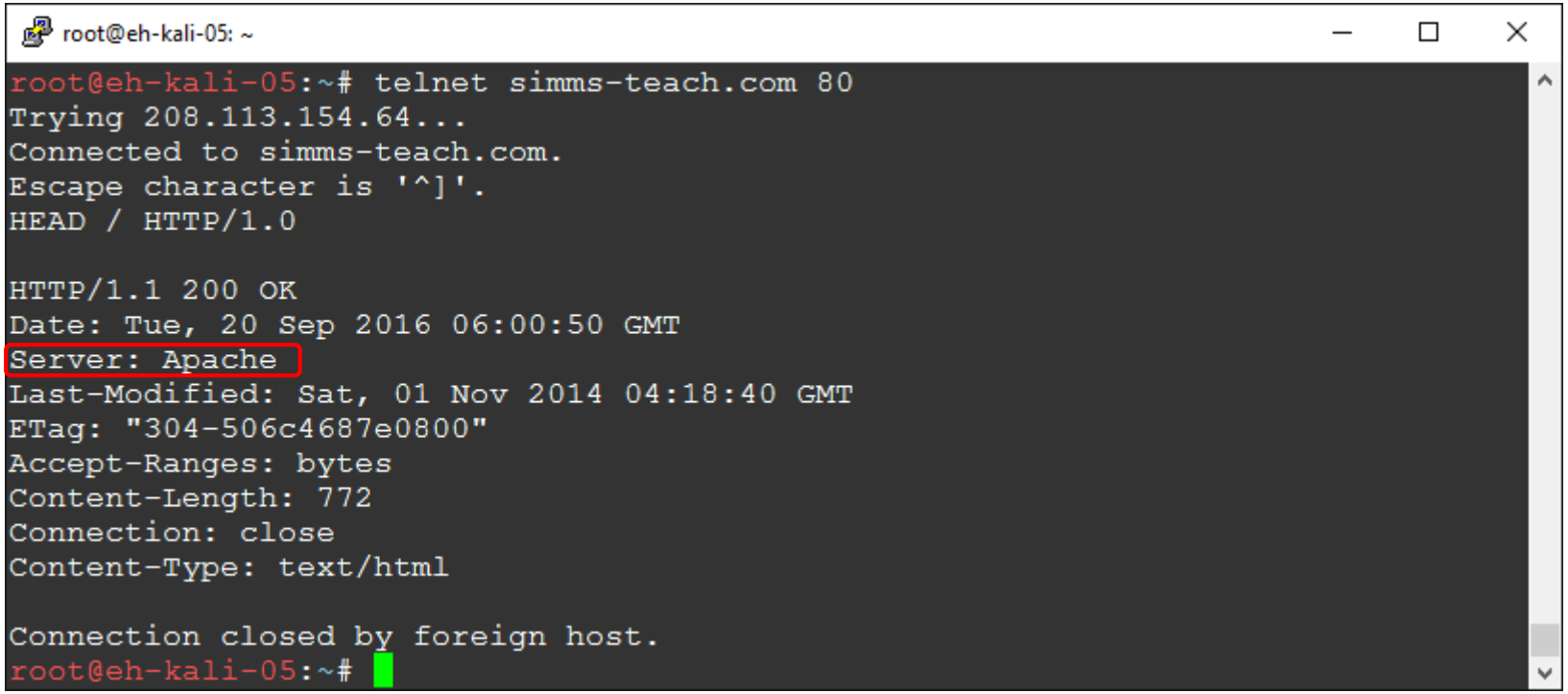
telnet and nc commands

telnet <host-or-IP-addess> <port>

nc <host-or-IP-addess> <port>

Probing simms-teach.com (telnet)

telnet simms-teach.com 80
HEAD / HTTP/1.0
(then enter blank line)



We know it is an Apache web server but not much else

Probing simms-teach.com (nc)

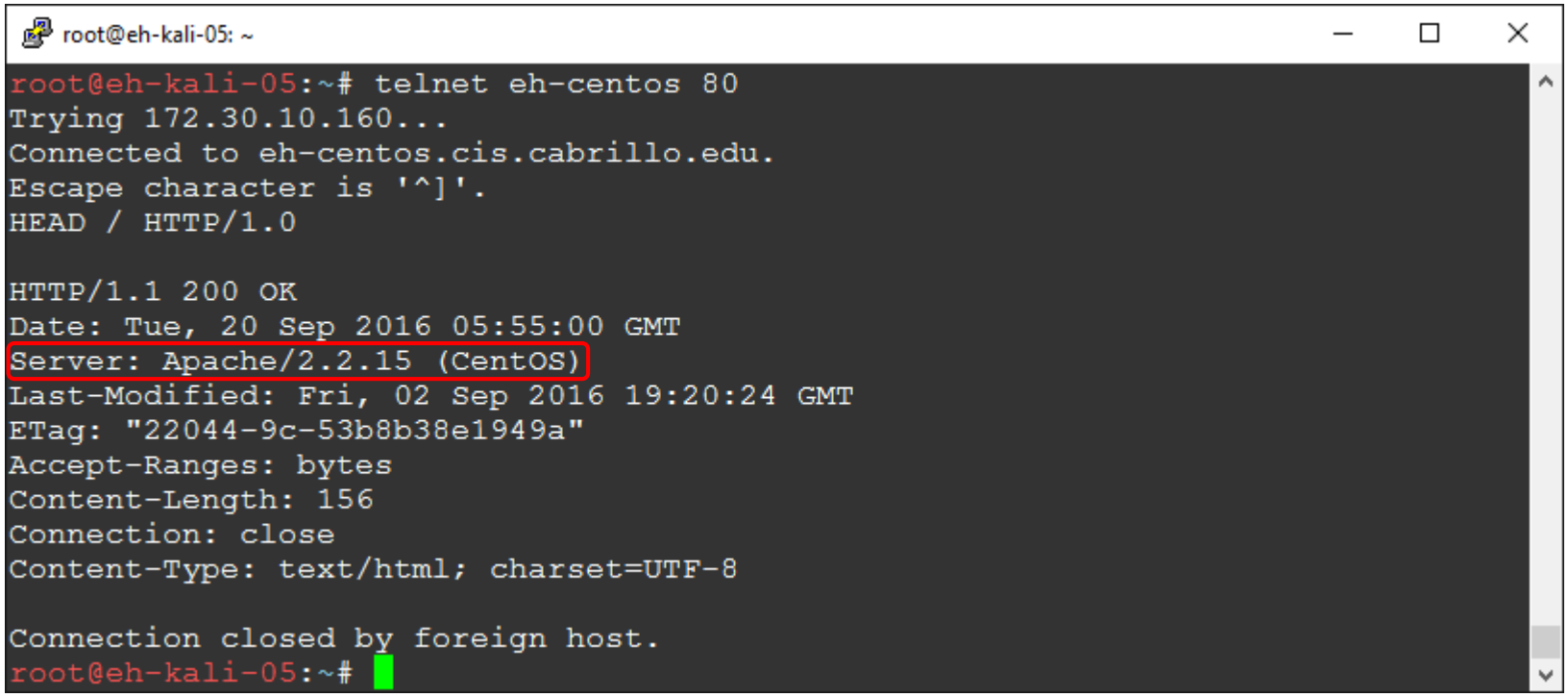
nc simms-teach.com 80
HEAD / HTTP/1.0
(then enter blank line)

```
root@eh-kali-05:~# nc simms-teach.com  80
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Date: Tue, 19 Sep 2017 17:57:21 GMT
Server: Apache
Last-Modified: Sat, 01 Nov 2014 04:18:40 GMT
ETag: "304-506c4687e0800"
Accept-Ranges: bytes
Content-Length: 772
Connection: close
Content-Type: text/html

root@eh-kali-05:~#
```

We know it is an Apache web server but not much else

Probing eh-centos VM (telnet)

telnet eh-centos 80
HEAD / HTTP/1.0
(then enter blank line)



We know it is an Apache web server version 2.2.15 on Centos

Probing eh-centos VM (nc)

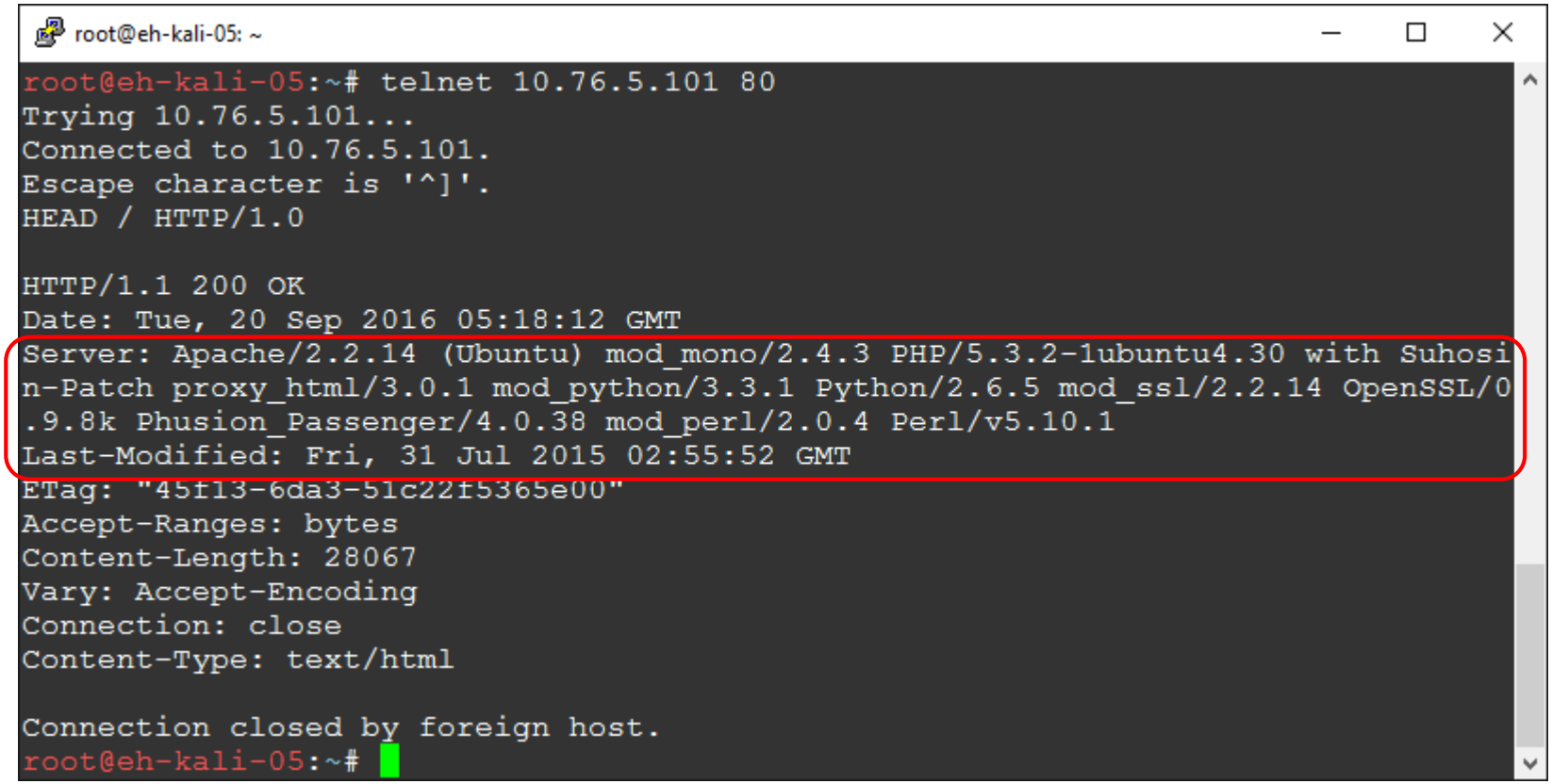
nc eh-centos 80
HEAD / HTTP/1.0
(then enter blank line)

```
root@eh-kali-05:~# nc eh-centos.cis.cabrillo.edu 80
HEAD / HTTP/1.0
HTTP/1.1 400 Bad Request
Date: Tue, 19 Sep 2017 16:28:14 GMT
Server: Apache/2.2.15 (CentOS)
Content-Length: 301
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.2.15 (CentOS) Server at 127.0.0.1 Port 80</address>
</body></html>
root@eh-kali-05:~#
```

We know it is an Apache web server version 2.2.15 on Centos

Probing OWASP VM (telnet)

telnet 10.76.5.101 80
HEAD / HTTP/1.0
(then enter blank line)



We know it is an Apache web server version 2.2.14 on Ubuntu as well as various modules that are loaded

Probing OWASP VM (nc)

nc 10.76.5.101 80
HEAD / HTTP/1.0
(then enter blank line)

```
root@eh-kali-05:~# nc 10.76.5.101 80
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Date: Tue, 19 Sep 2017 17:37:46 GMT
Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3
.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/
2.0.4 Perl/v5.10.1
Last-Modified: Fri, 31 Jul 2015 02:55:52 GMT
ETag: "45f13-6da3-51c22f5365e00"
Accept-Ranges: bytes
Content-Length: 28067
Vary: Accept-Encoding
Connection: close
Content-Type: text/html

root@eh-kali-05:~#
```

We know it is an Apache web server version 2.2.14 on Ubuntu as well as various modules that are loaded

Activity

Use telnet to get header information from the microsoft.com webserver.

What web server software and version is ruining there?

Put your answer in the chat window

Using telnet for port 25 (SMTP)

Some SMTP commands

HELO <*sending-hostname*>	*Initiate SMTP conversation*
EHLO <*sending-hostname*>	*Initiate extended SMTP conversation*
MAIL From: <*source email address*>	*Source*
RCPT To: <*destination email address*>	*Destination*
DATA	*Message body*
QUIT	*End connection*

Probing port 25 on EH-Centos VM

```
root@eh-kali-05:~# telnet eh-centos 25
Trying 172.30.10.160...
Connected to eh-centos.cis.cabrillo.edu.
Escape character is '^]'.
220 eh-centos.cis.cabrillo.edu ESMTP Postfix
EHLO eh-kali-05.cis.cabrillo.edu
250-eh-centos.cis.cabrillo.edu
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
MAIL From: root@eh-kali-05.cis.cabrillo.edu
250 2.1.0 Ok
RCPT To: cis76@eh-centos.cis.cabrillo.edu
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
What a crazy way to send an email huh?
.
250 2.0.0 Ok: queued as 5B9B76A97
quit
221 2.0.0 Bye
Connection closed by foreign host.
root@eh-kali-05:~#
```

This server is running Postfix as the SMTP service.

You can actually use telnet to send an email!

Checking for new email on EH-Centos VM

```
[cis76@EH-Centos ~]$ mail
Heirloom Mail version 12.4 7/29/08.  Type ? for help.
"/var/spool/mail/cis76": 1 message 1 new
>N  1 root@eh-kali-05.cis.  Tue Sep 20 10:12  10/484
& 1
Message  1:
From root@eh-kali-05.cis.cabrillo.edu  Tue Sep 20 10:12:30 2016
Return-Path: <root@eh-kali-05.cis.cabrillo.edu>
X-Original-To: cis76@eh-centos.cis.cabrillo.edu
Delivered-To: cis76@eh-centos.cis.cabrillo.edu
Status: R

What a crazy way to send an email huh?

& quit
Held 1 message in /var/spool/mail/cis76
[cis76@EH-Centos ~]$
```

Yep, it really works!

Activity

Using the example above use telnet to send a super simple message to cis76@eh-cenos.cis.cabrillo.edu

Next login to EH-Centos as the cis76 user and check your mail.

Put the mail header which looks like this:

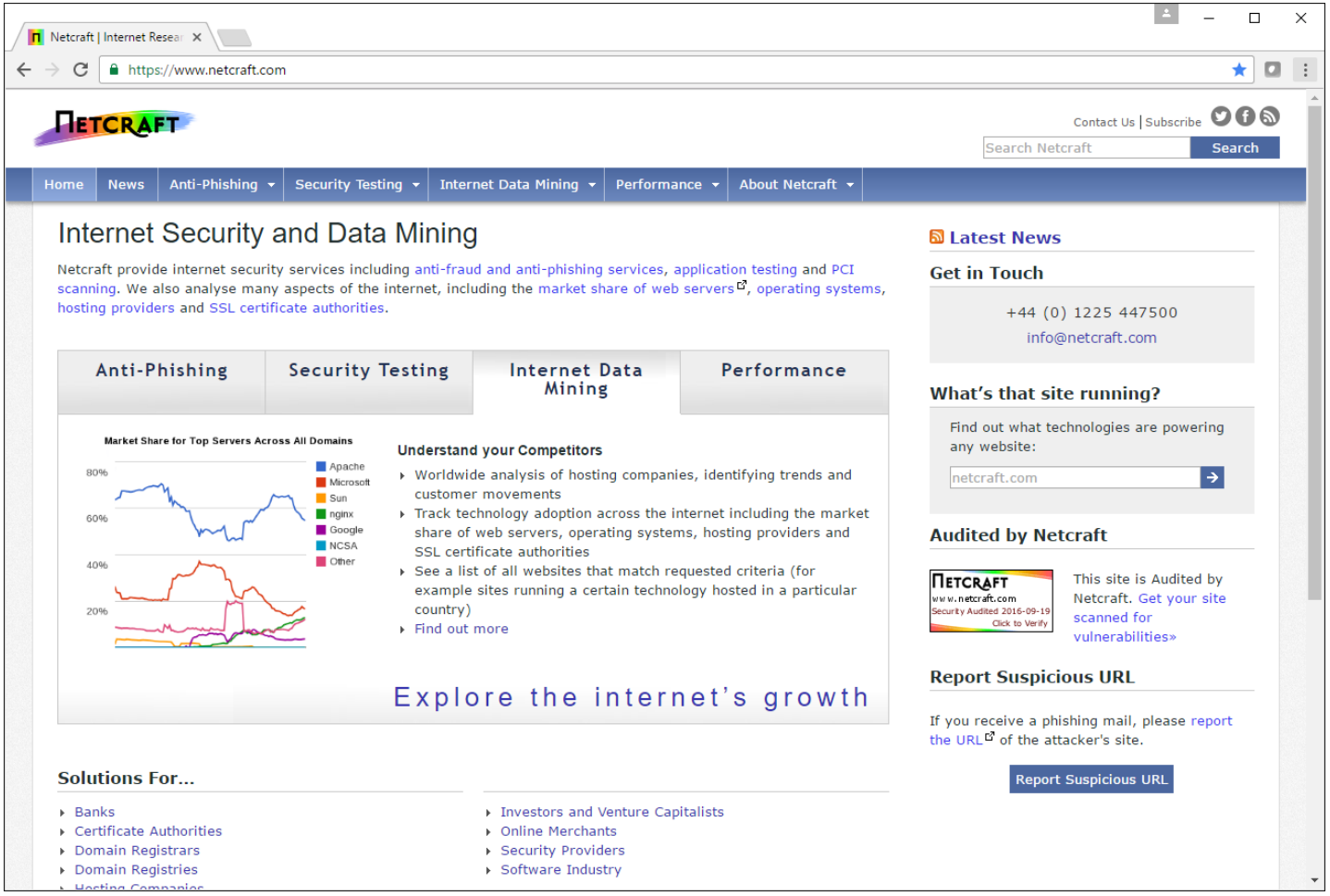
root@eh-kali-05.cis. Tue Sep 20 10:12 10/484

into the chat window

Website Information

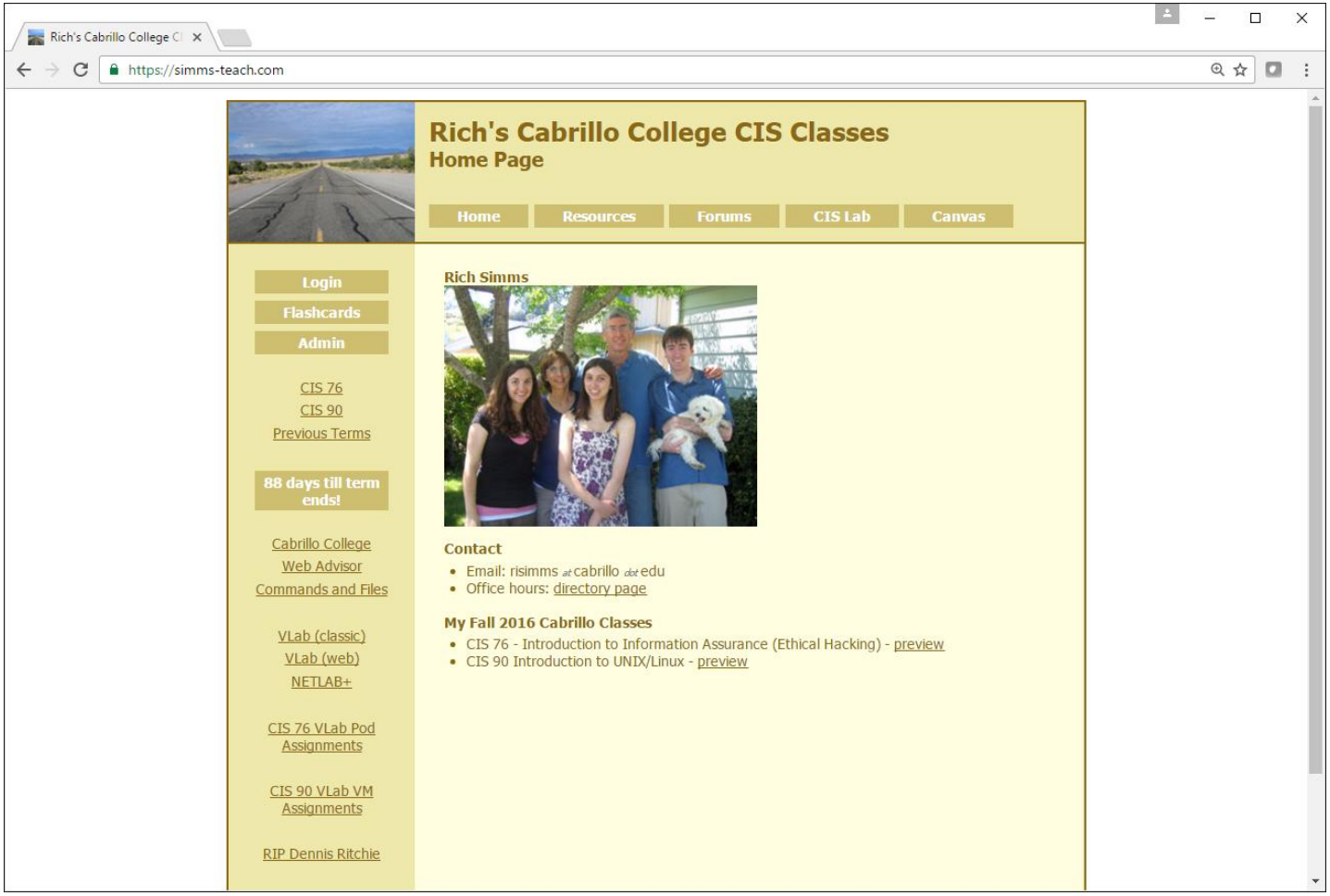
Netcraft

Netcraft



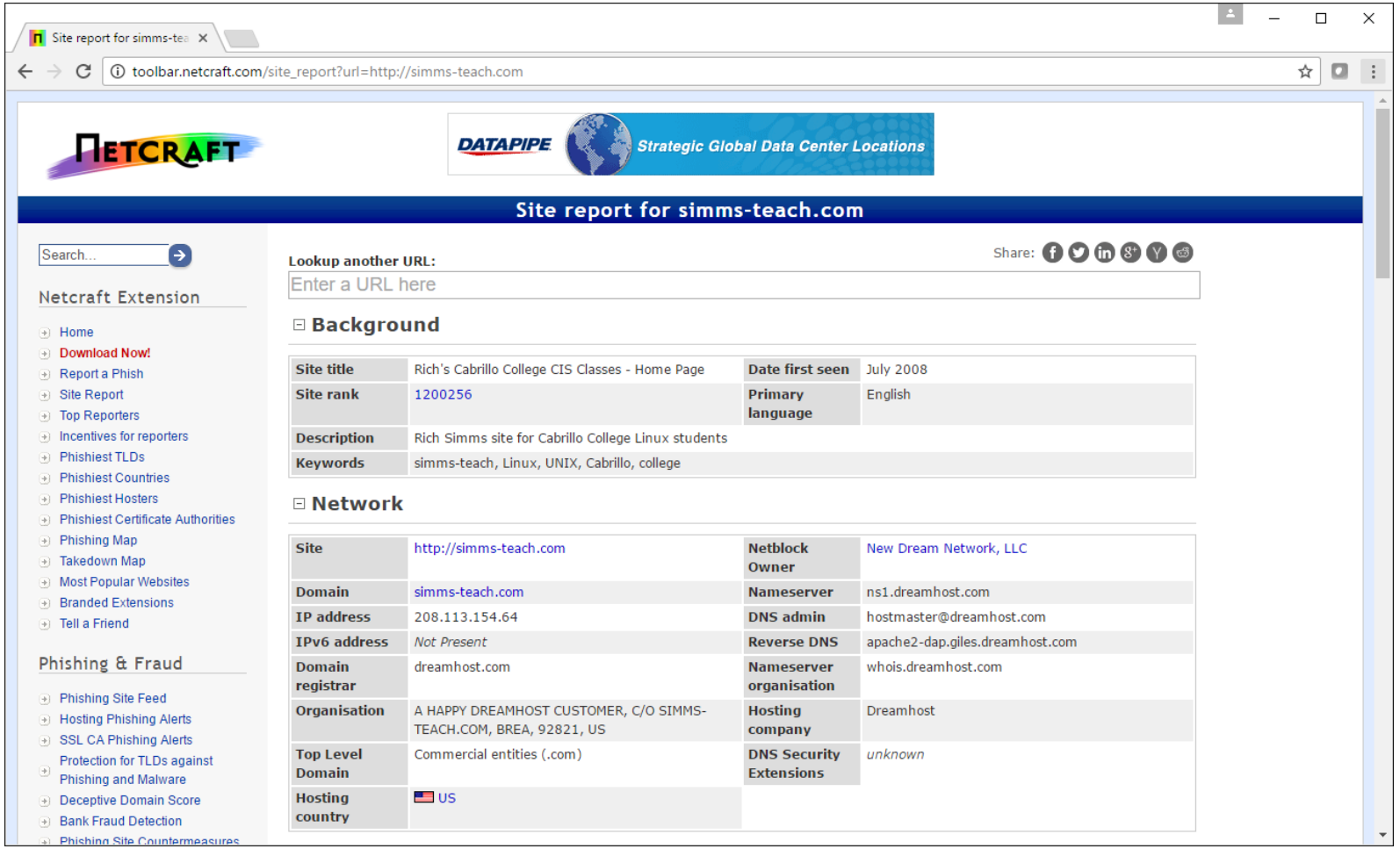
https://www.netcraft.com/

My Website



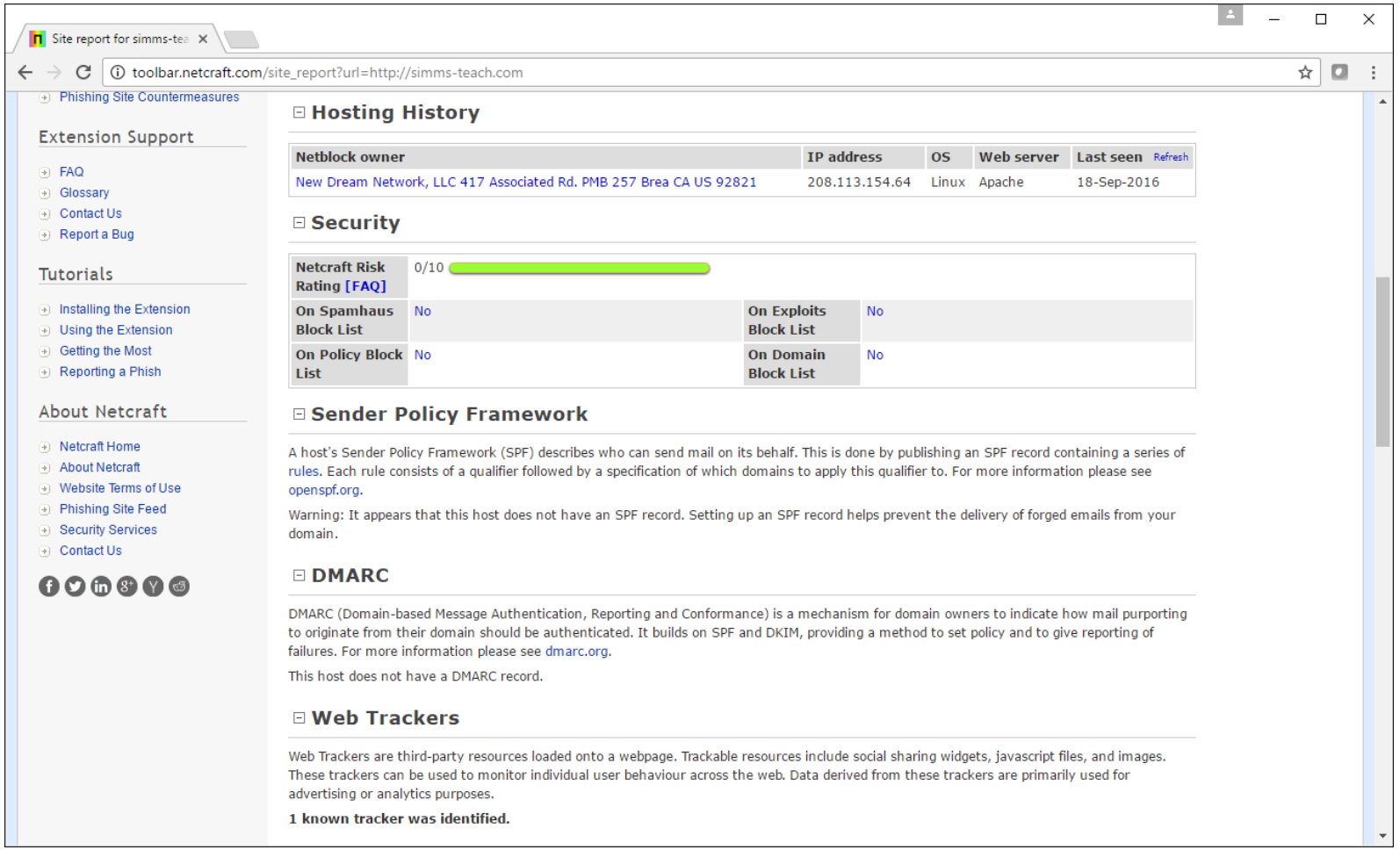
https://simms-teach.com/

Netcraft



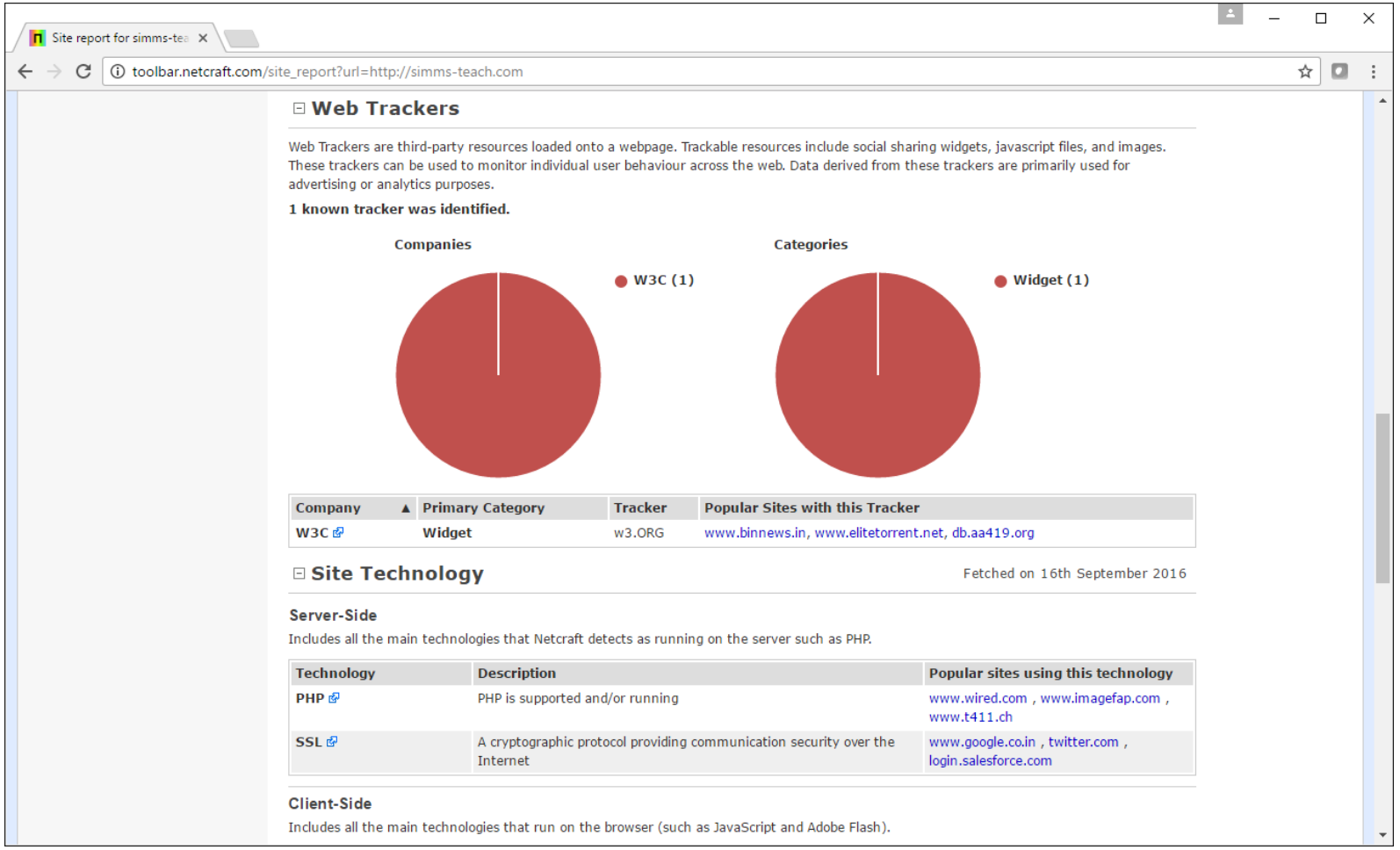
https://www.netcraft.com/

Netcraft



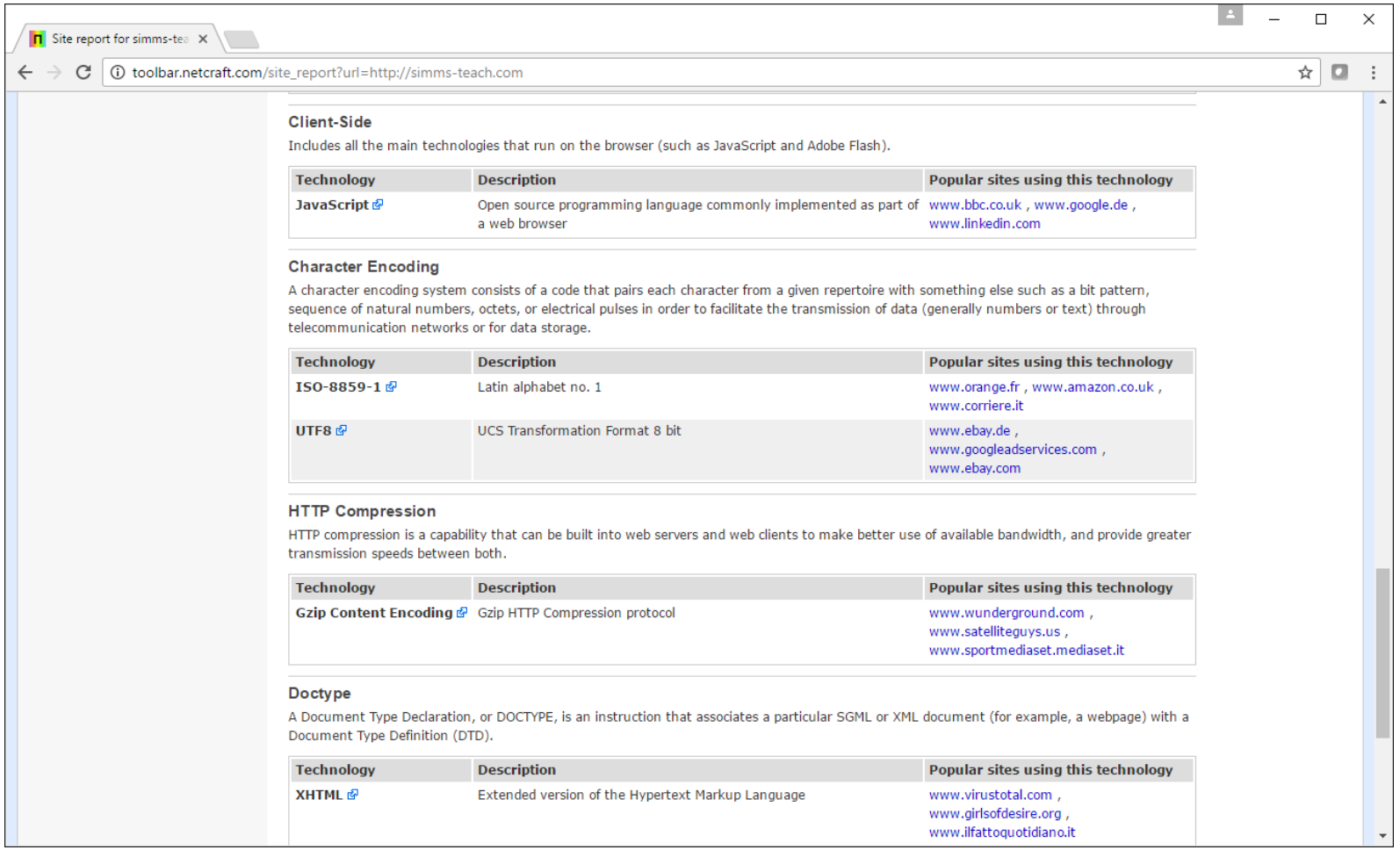
https://www.netcraft.com/

Netcraft



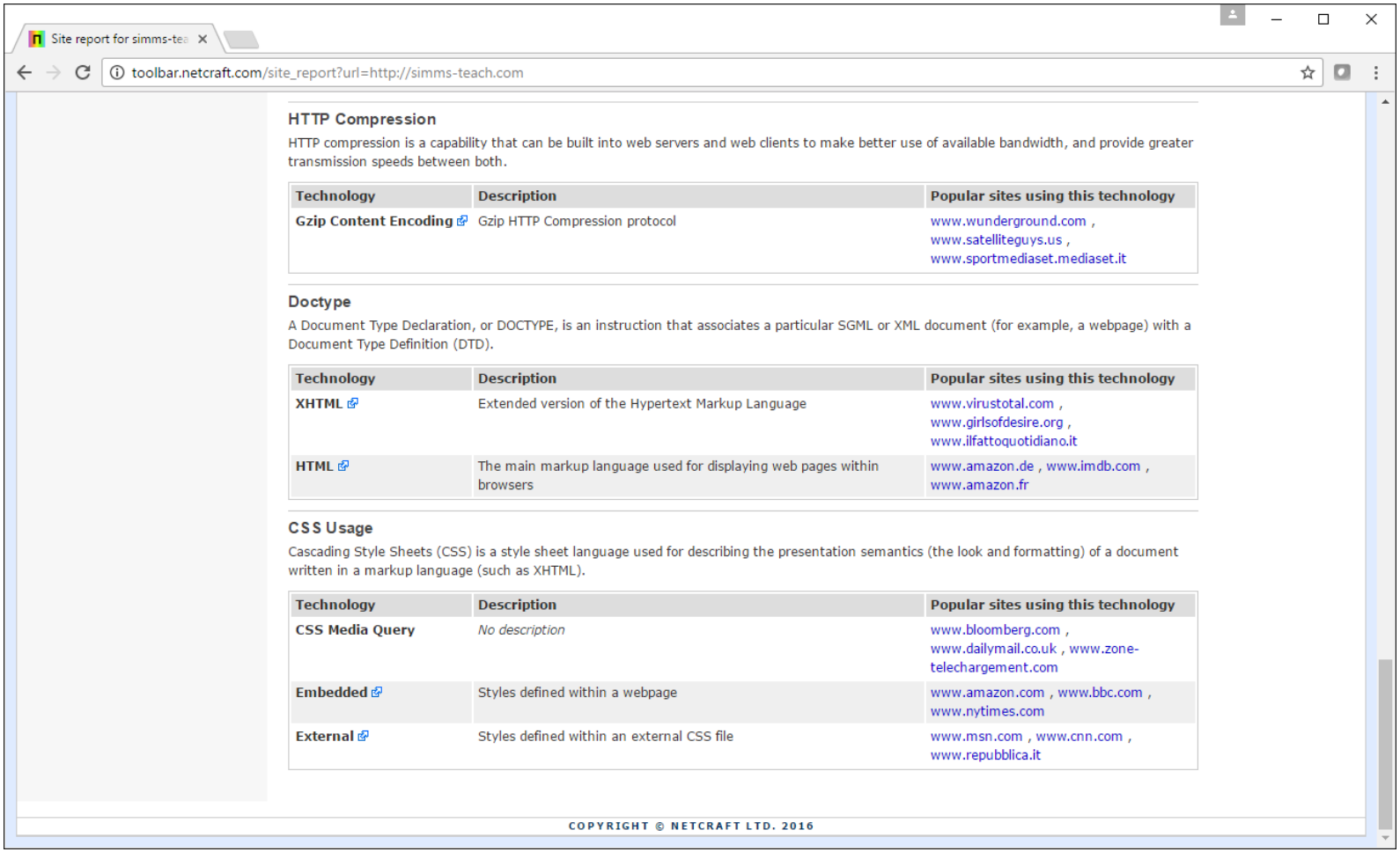
https://www.netcraft.com/

Netcraft



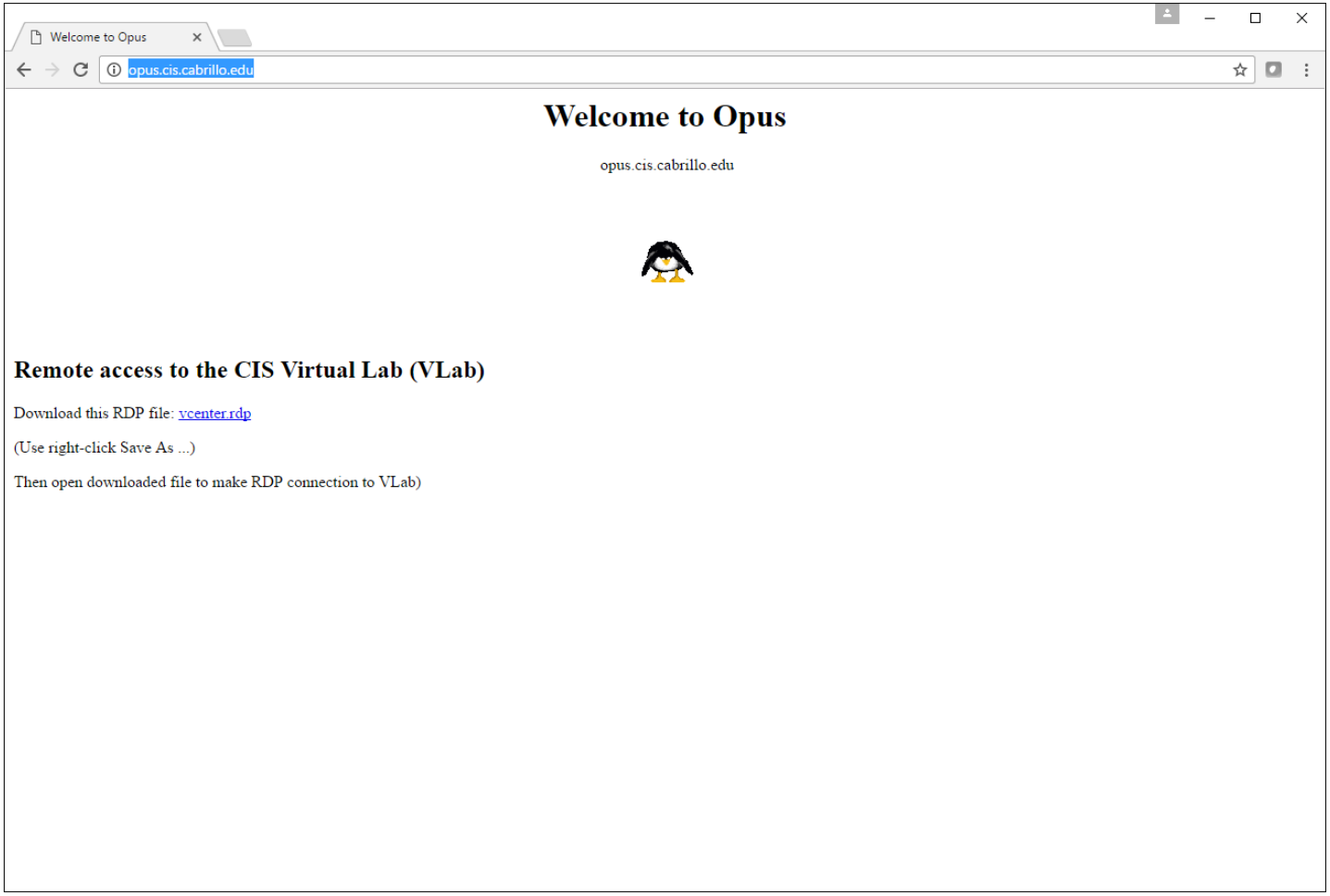
https://www.netcraft.com/

Netcraft



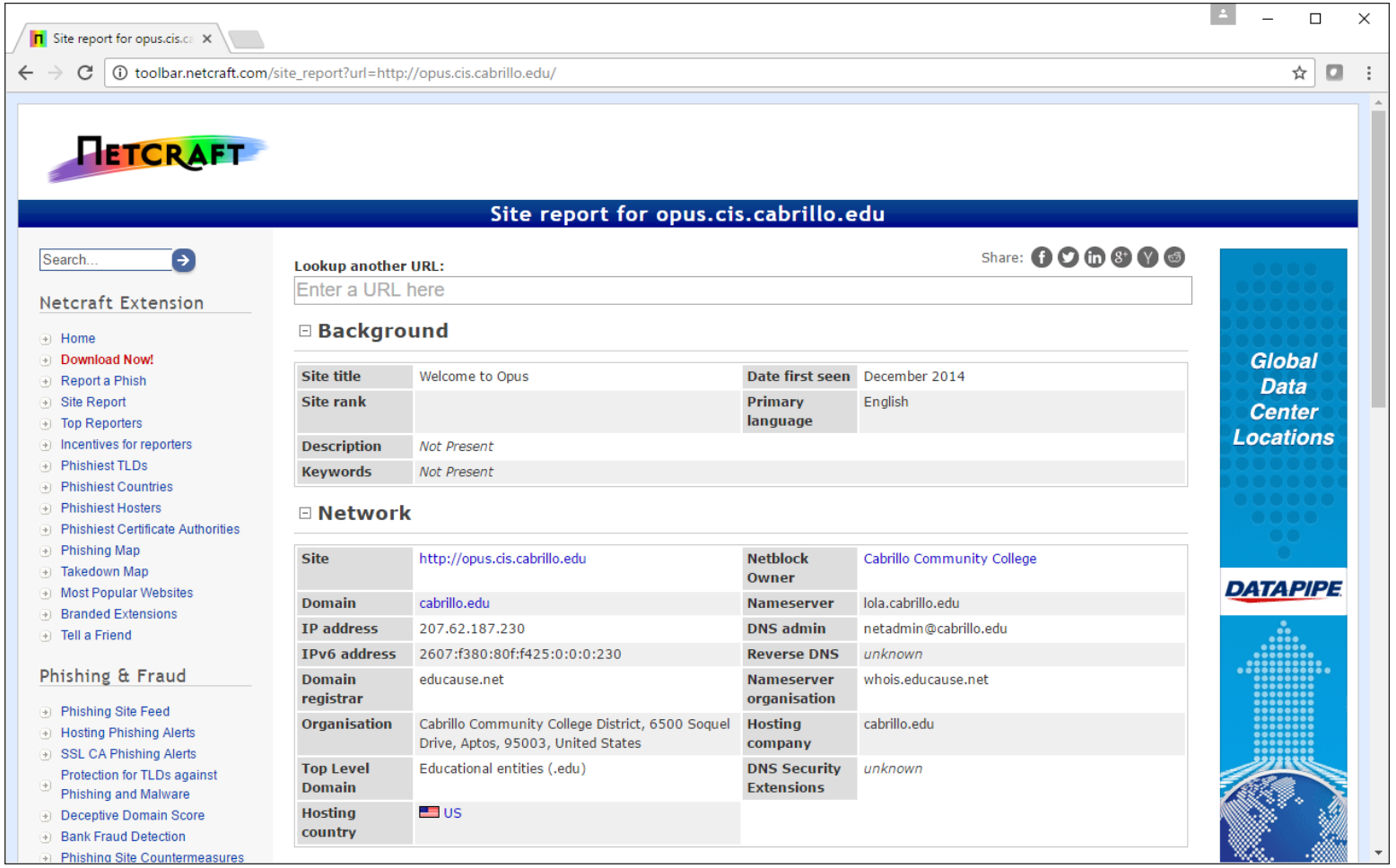
https://www.netcraft.com/

Opus website



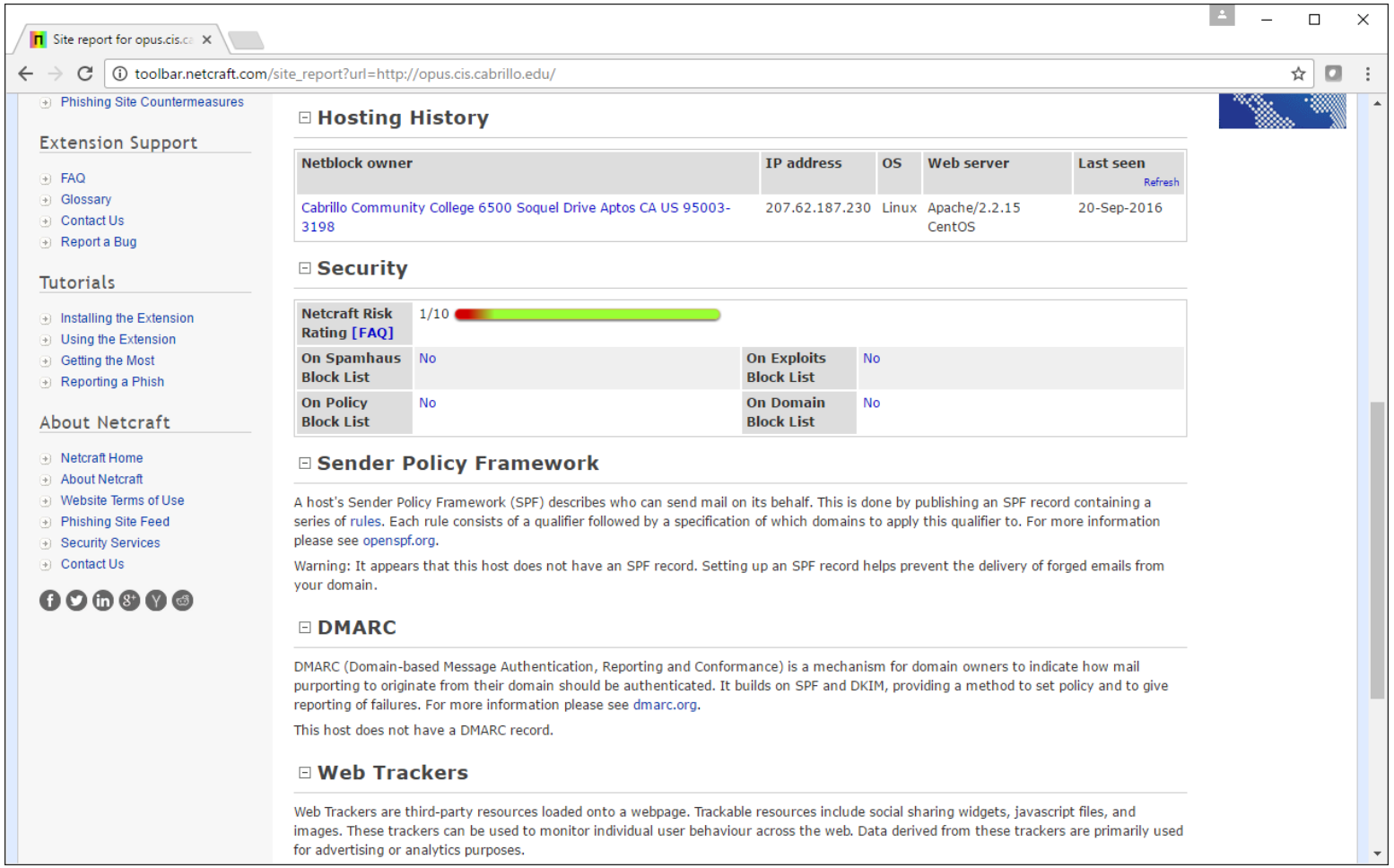
http://opus.cis.cabrillo.edu/

Netcraft



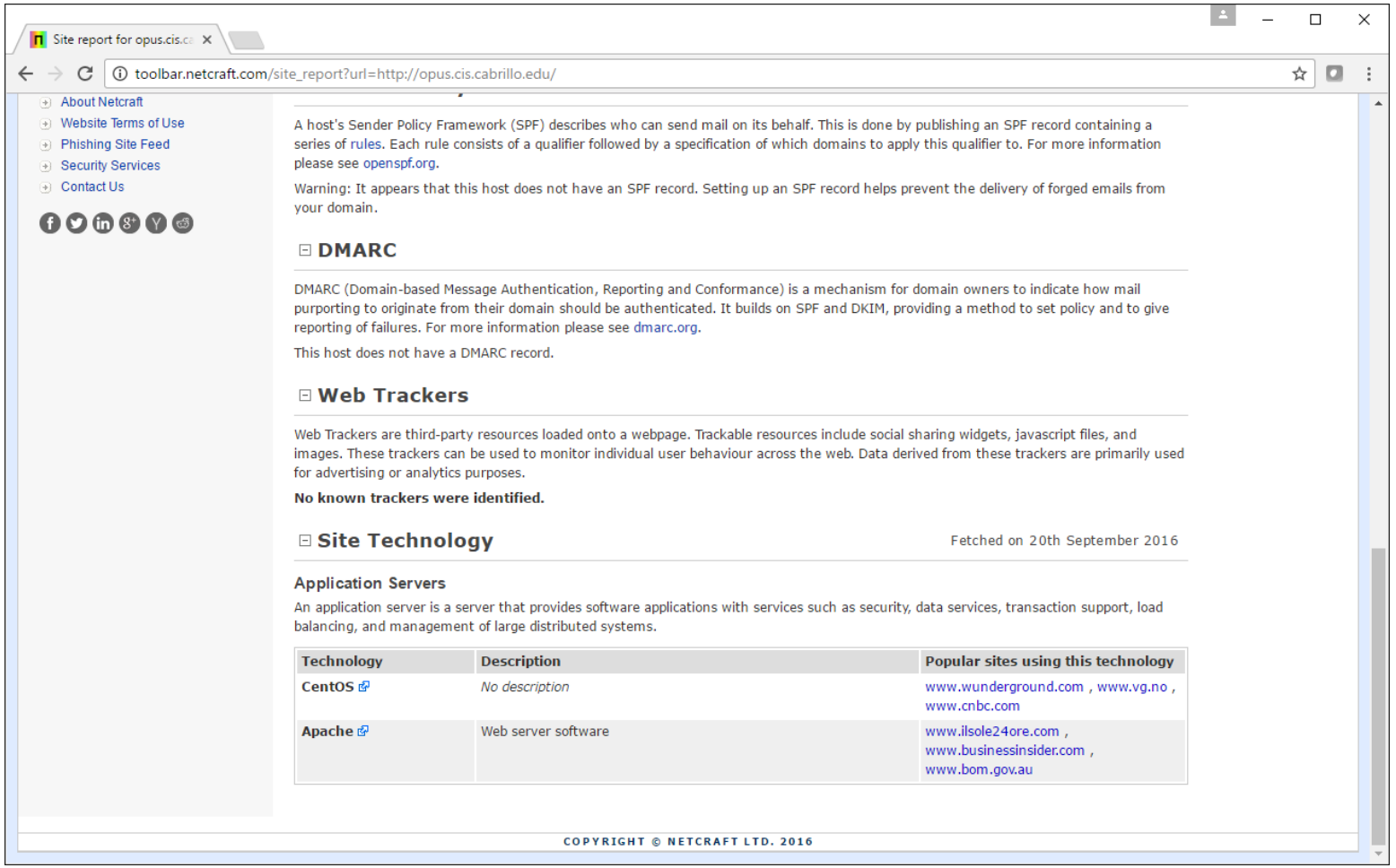
https://www.netcraft.com/

Netcraft



https://www.netcraft.com/

Netcraft



https://www.netcraft.com/

Activity

Using netcraft:

https://www.netcraft.com/

To passively compare the Opus and Opus-II servers without visiting them:

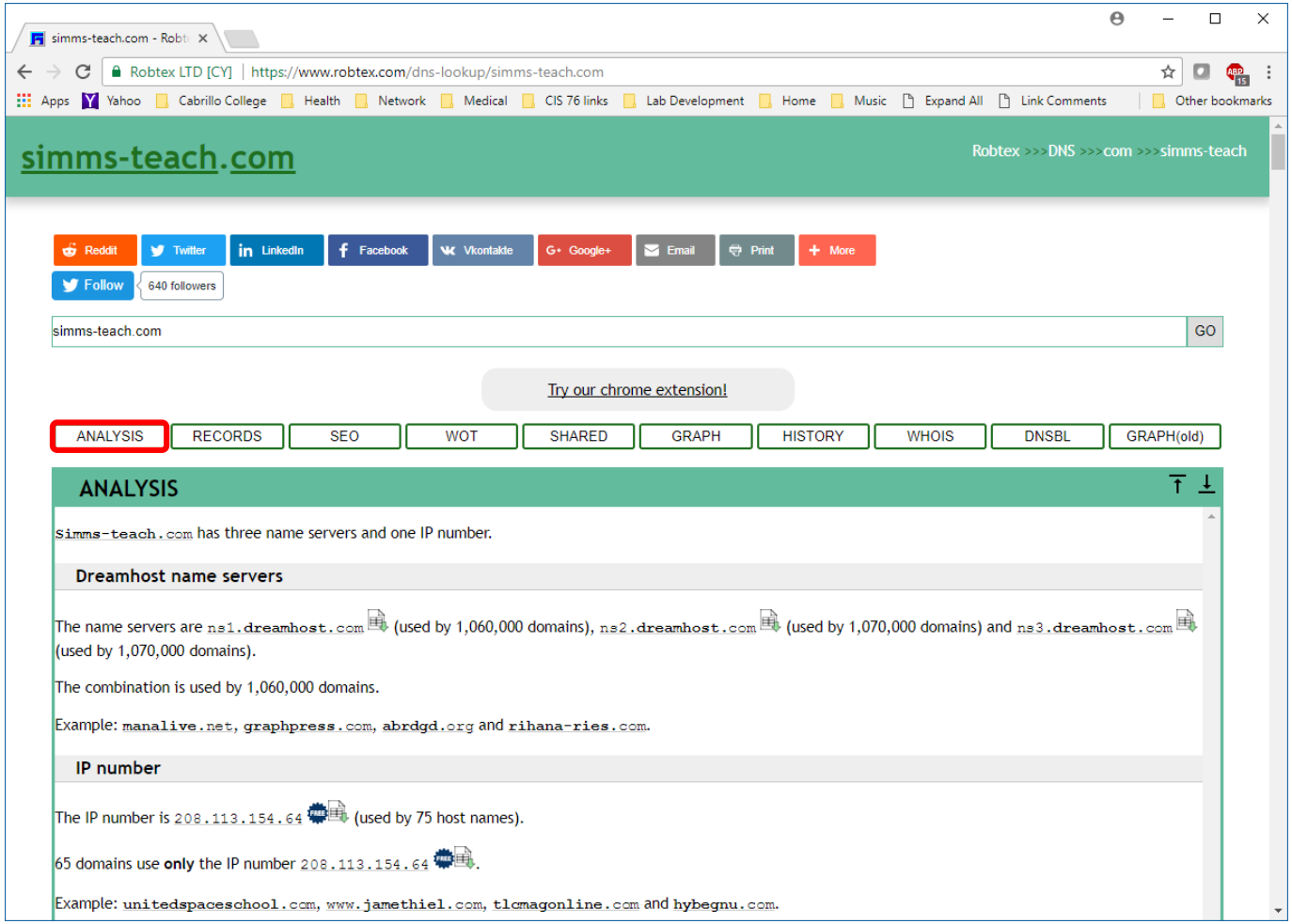
`opus.cis.cabrillo.edu`
`opus-ii.cis.cabrillo.edu`

Which server uses OpenSSL technology

Write your answer in the chat window

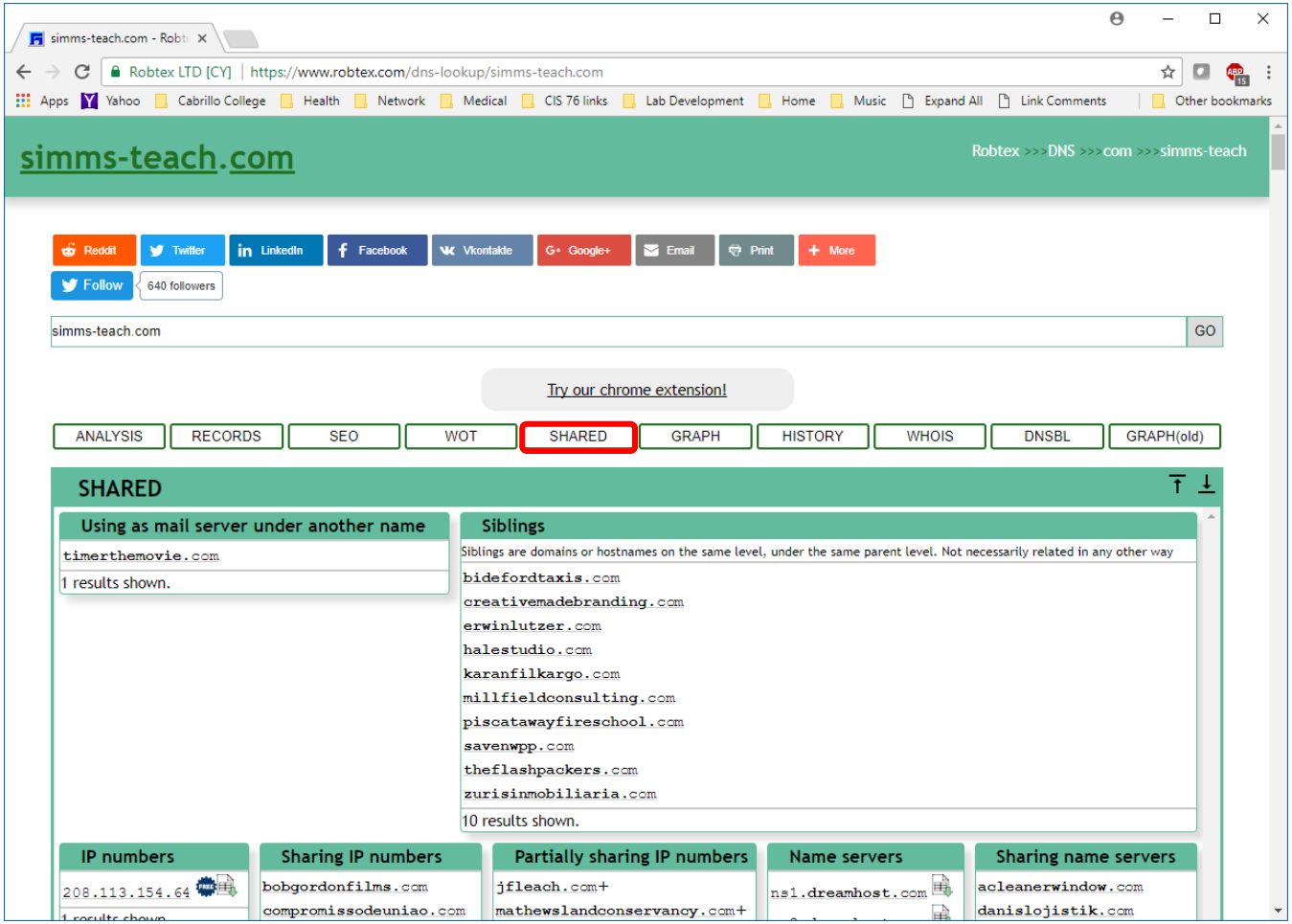
robtex.com

Robtex



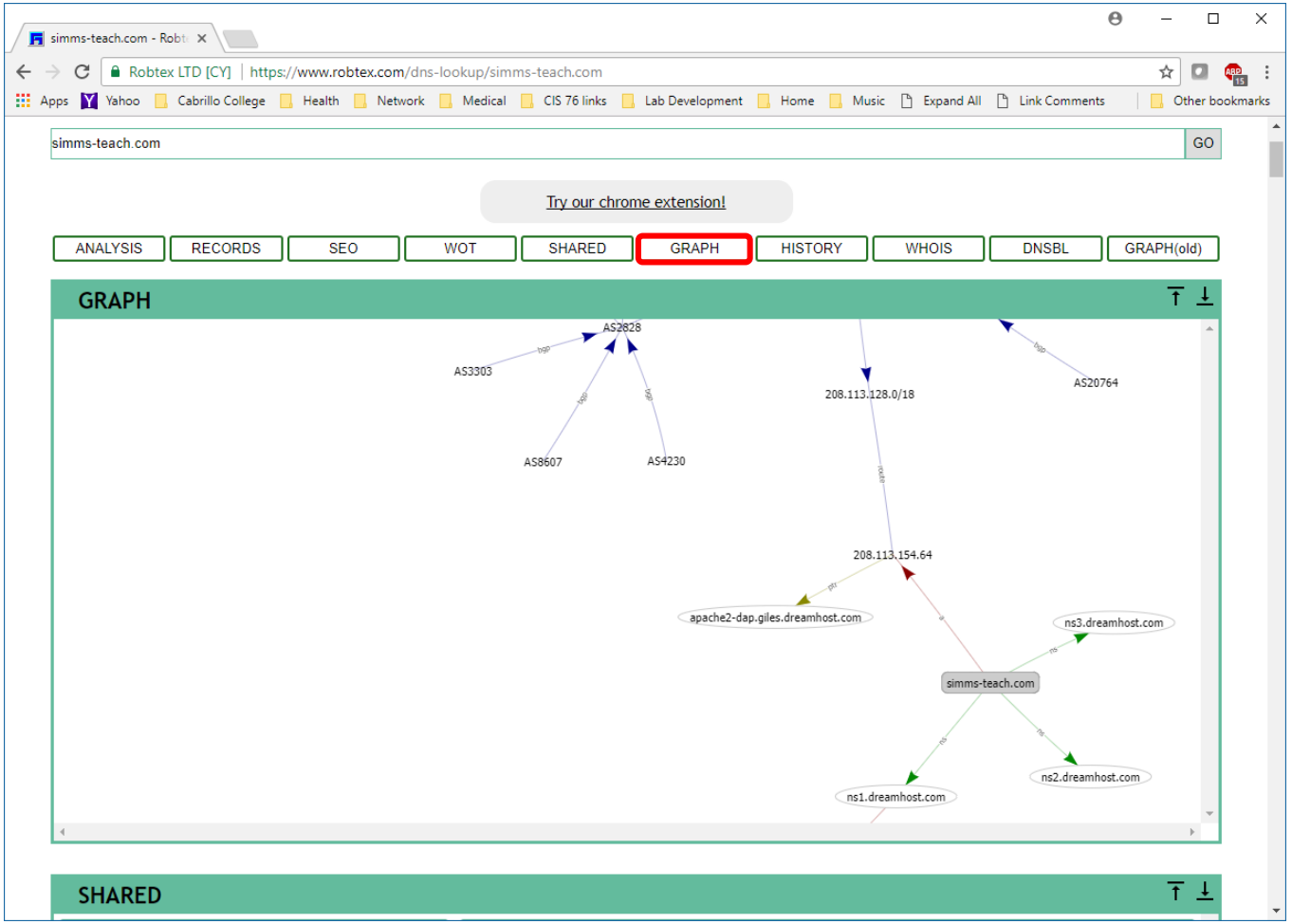
https://www.robtex.com

Robtex



https://www.robtex.com

Robtex



https://www.robtex.com

Activity

Use robtex https://www.robtex.com on:

`www.shodan.io`

Using the "Shared" view what are some other websites that use the same IP address?

Write your answer in the chat window

Maltego

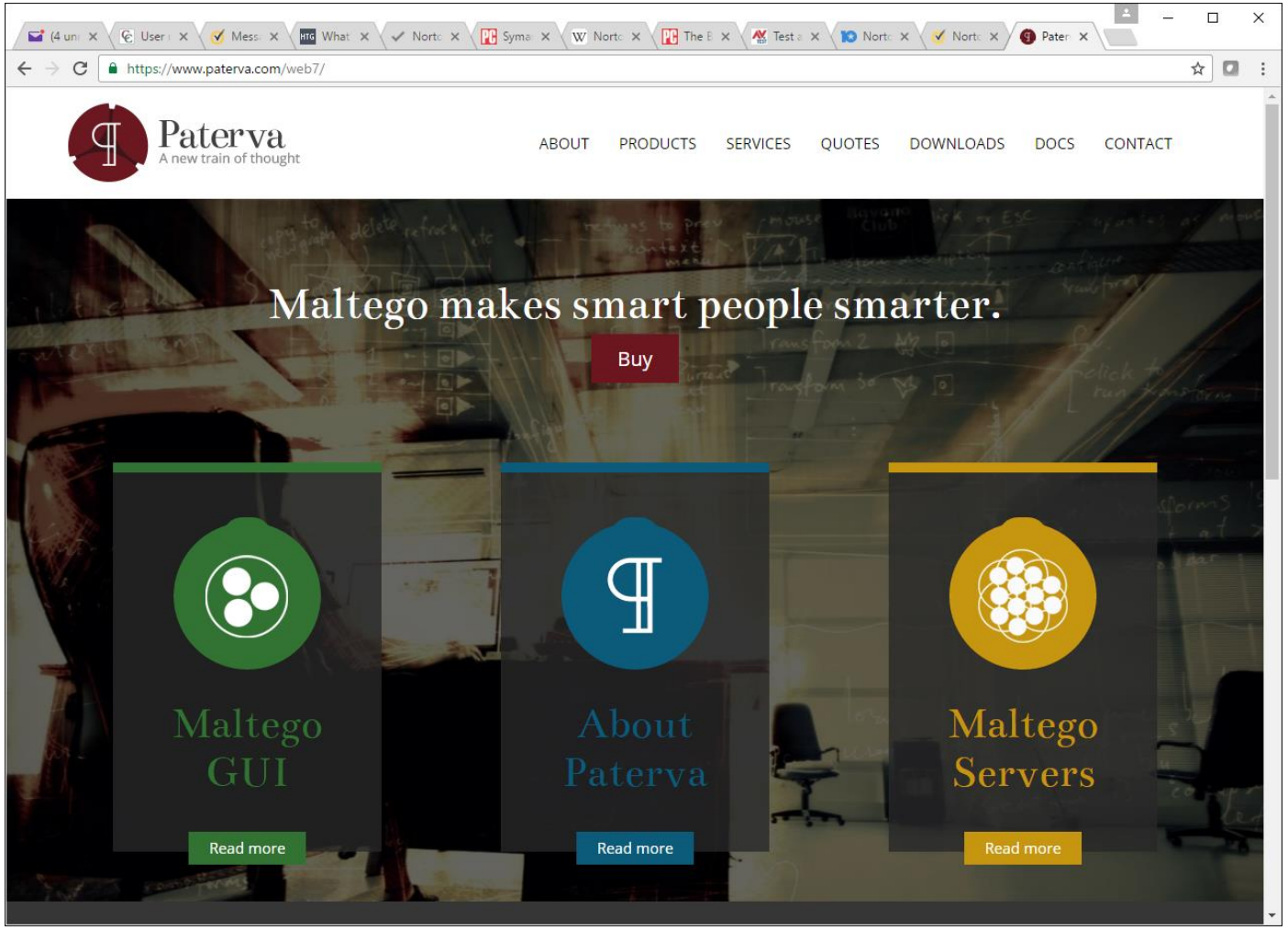
TNT Major Crimes TV Series

https://www.pinterest.com/pin/108438303502515403/

Maltego

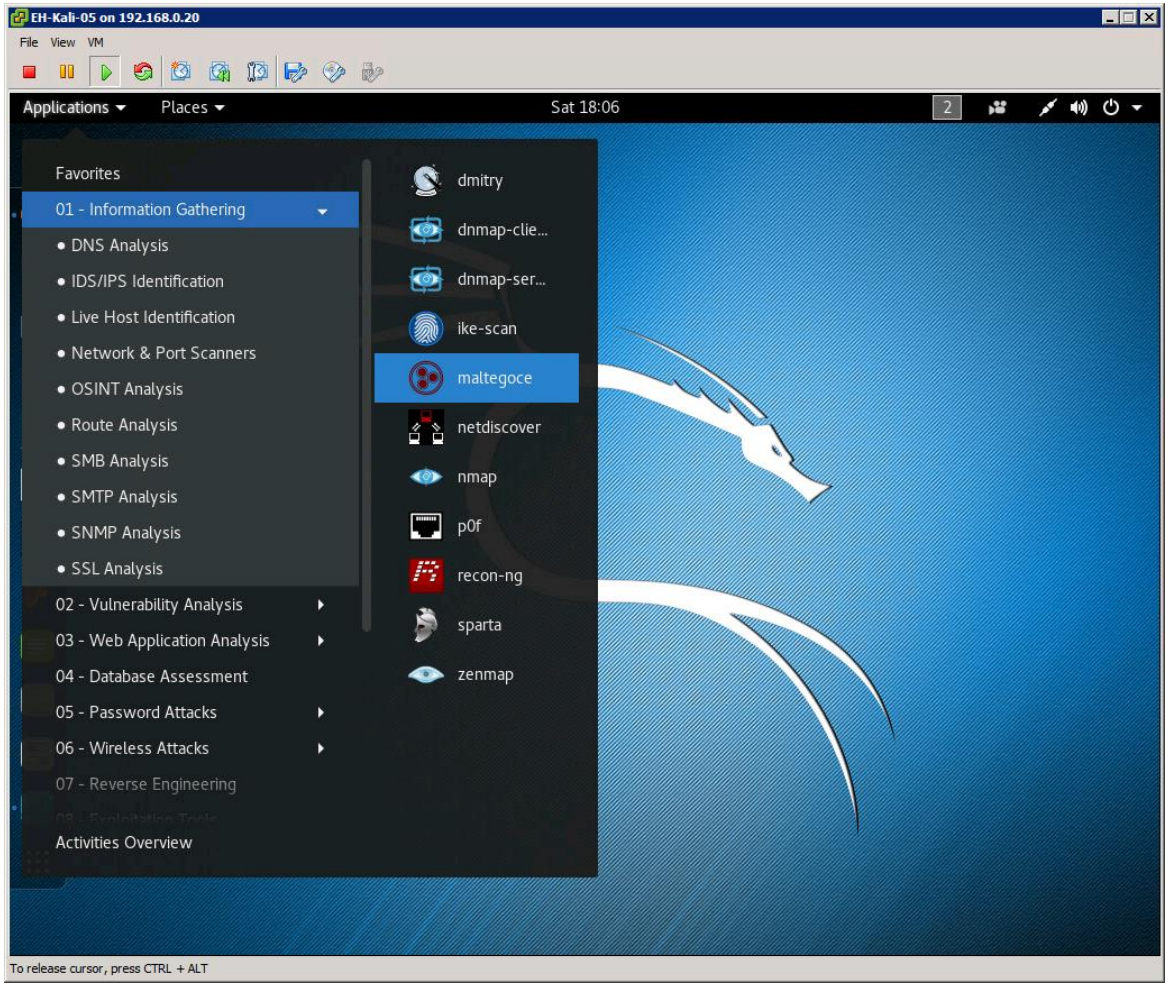
The community edition is a free version of the commercial client Maltego with various limitations.
Limitations :
- Maximum of 12 results per transform
- You need to register on our website to use the client
- API keys expire every couple of days
- Runs on a (slower) server that is shared with all community users
- Communication between client as server is not encrypted

Maltego



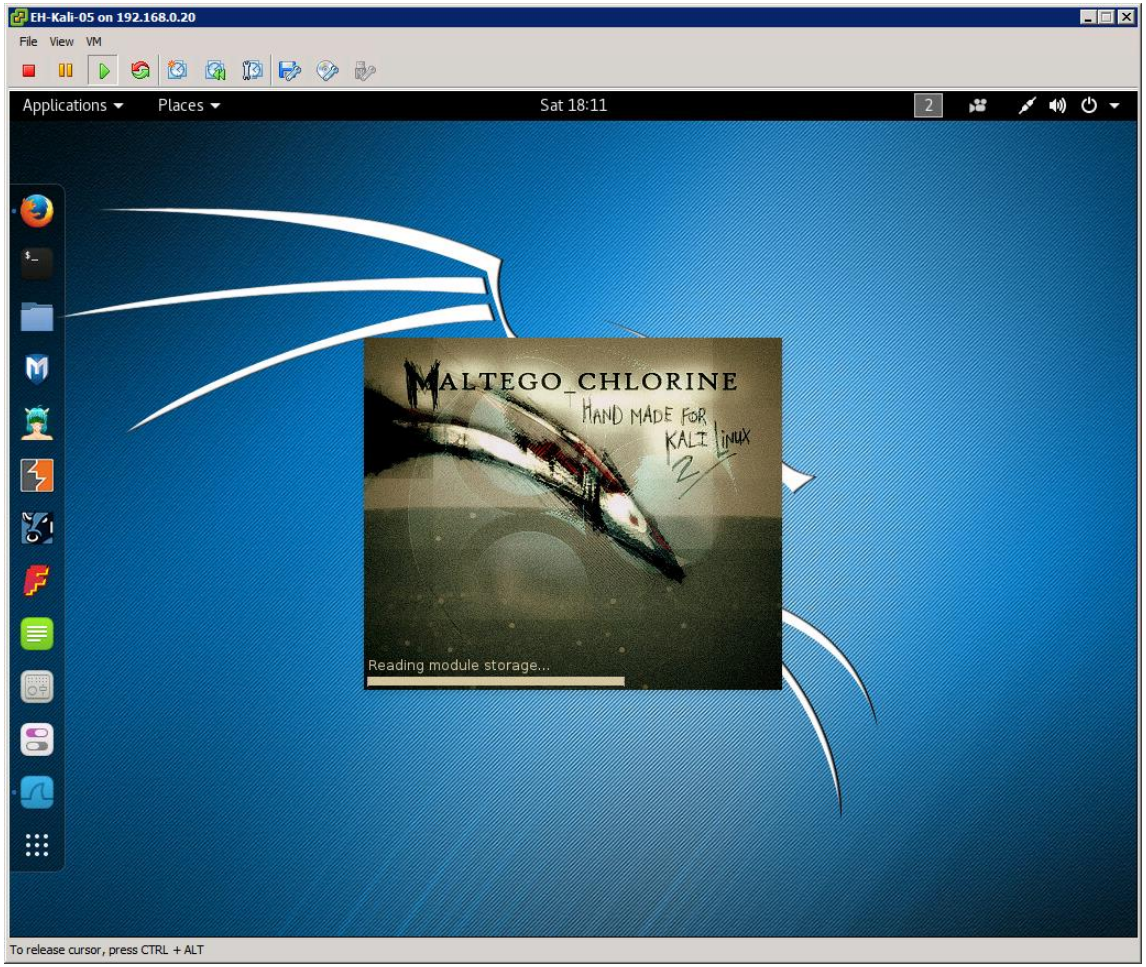
https://www.paterva.com/web7/

Maltego

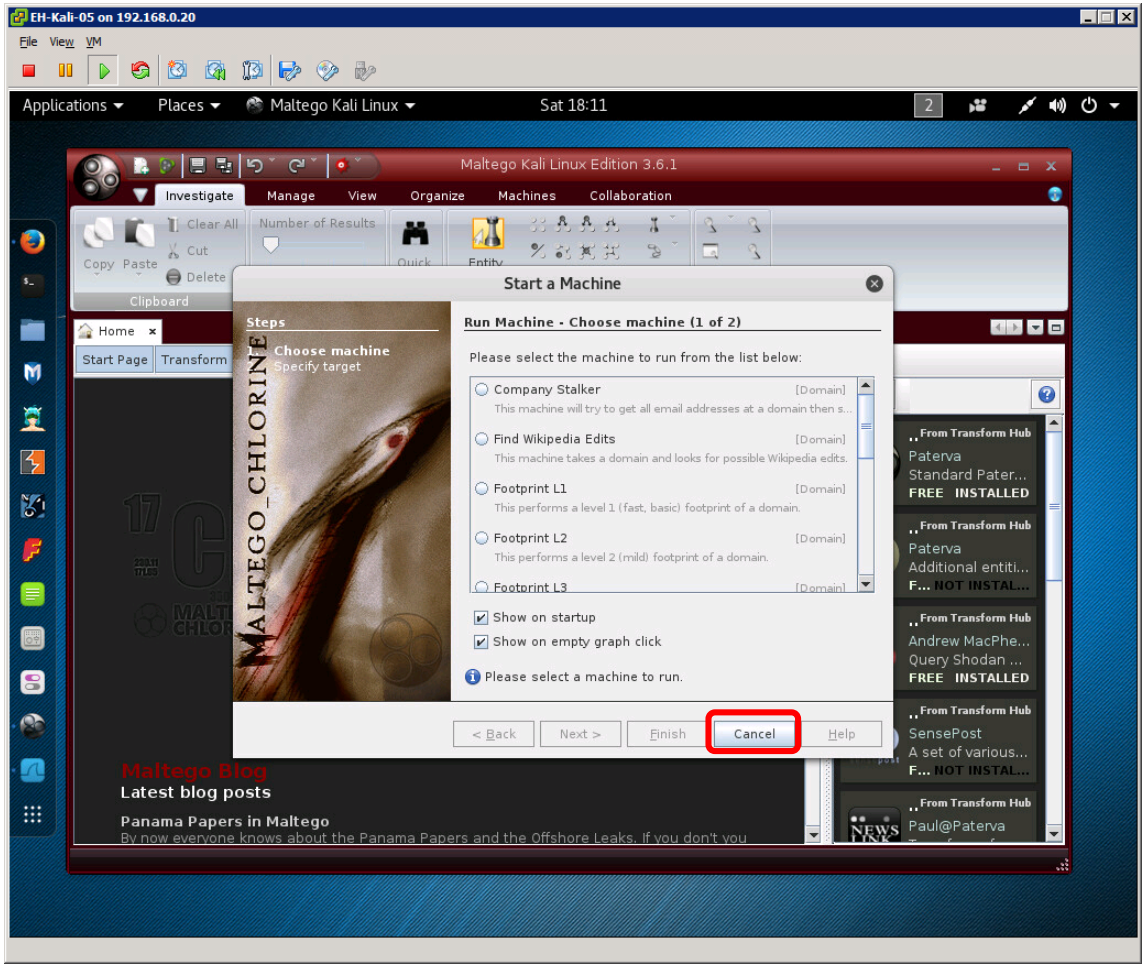


Applications > 01-Information Gathering > maltegoce

Maltego

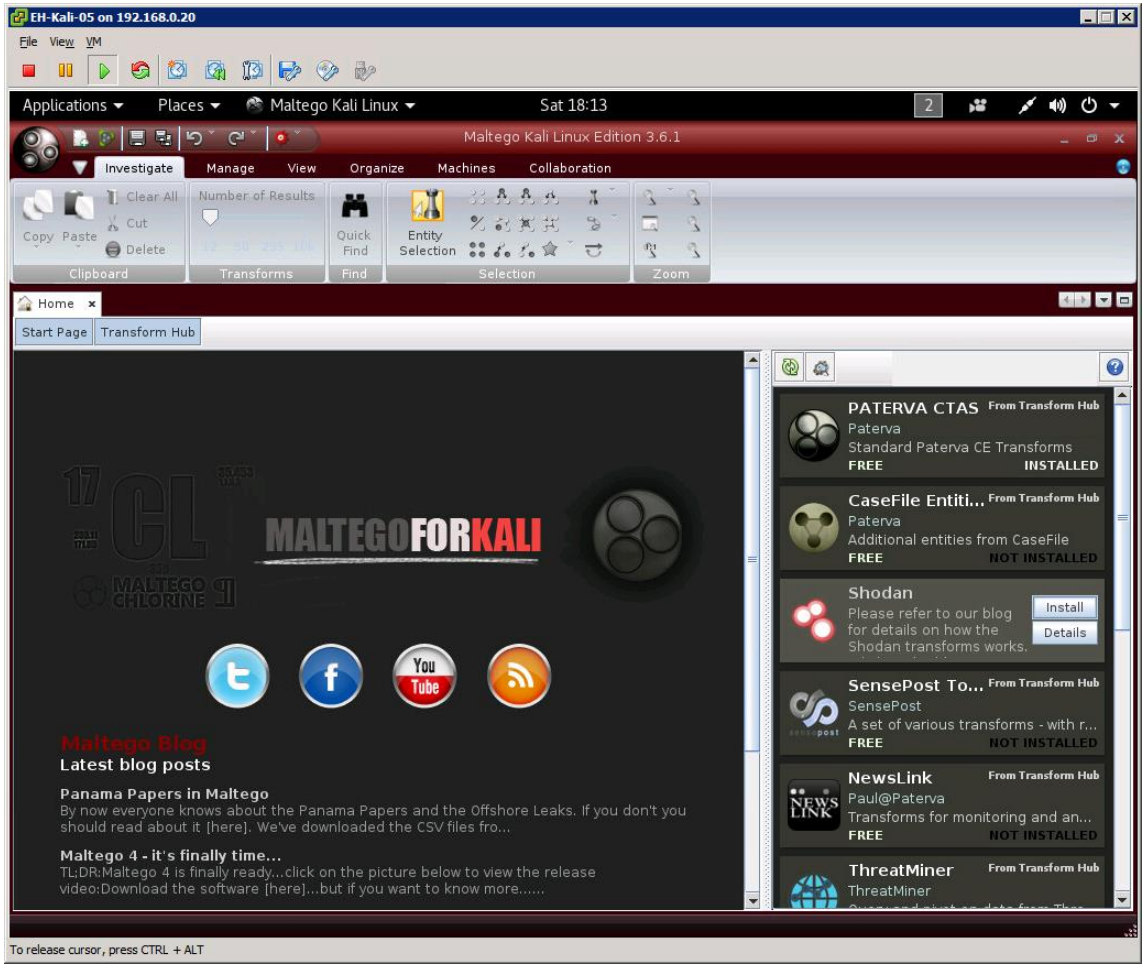

EH-Kali-05 on 192.168.0.20
File View VM
Applications Places Sat 18:11
MALTEGO_CHLORINE
HAND MADE FOR KALI LINUX
Reading module storage...
To release cursor, press CTRL + ALT

Maltego



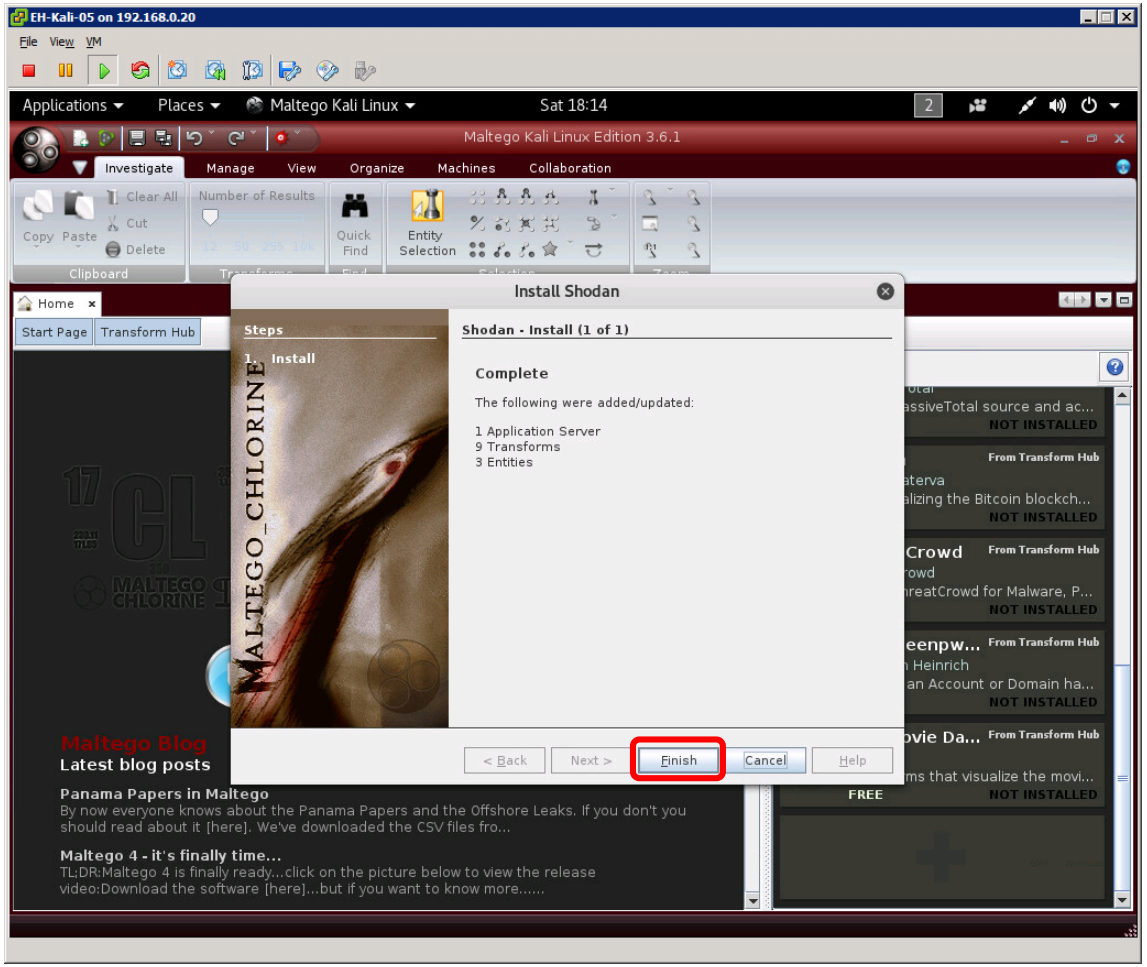
Click Cancel.

Maltego



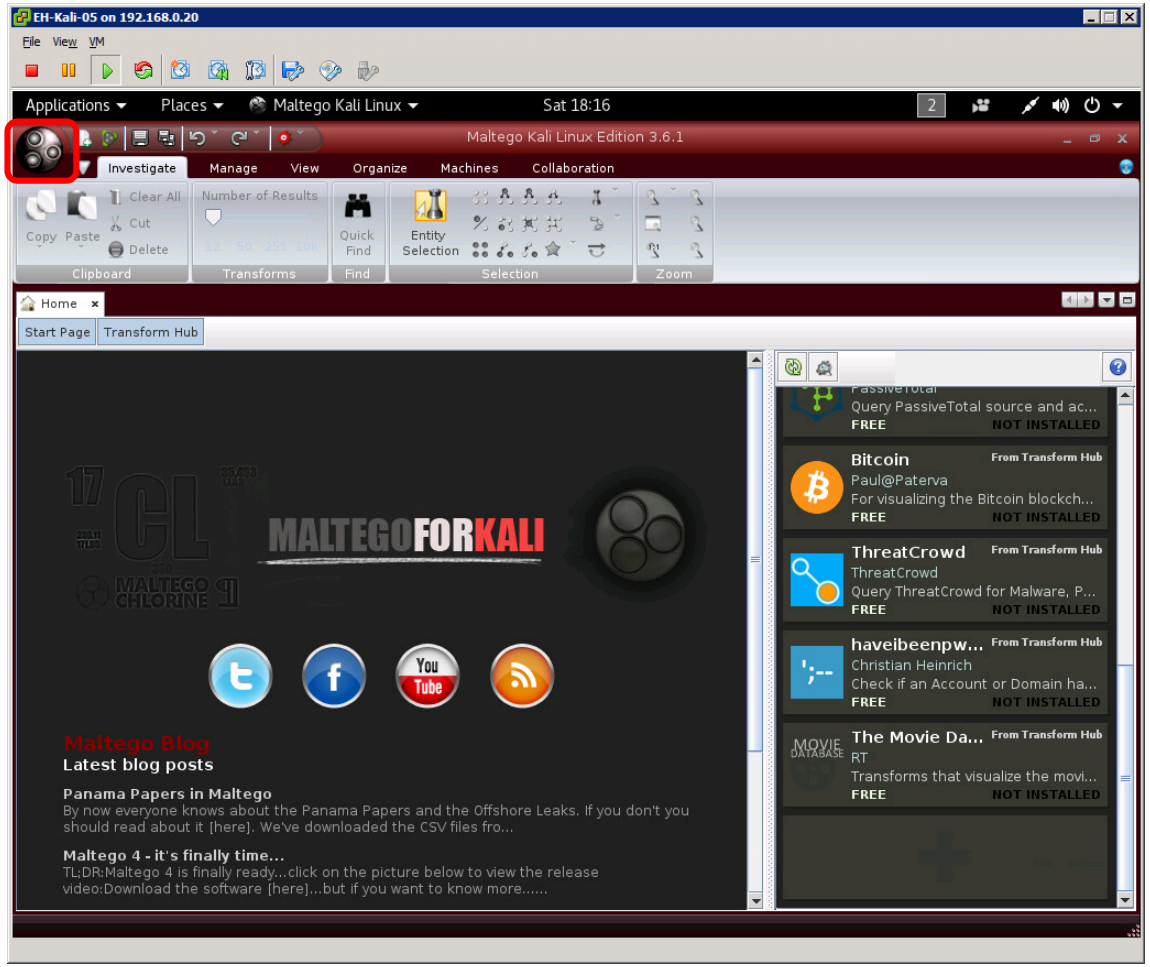
Install Shodan transform

Maltego



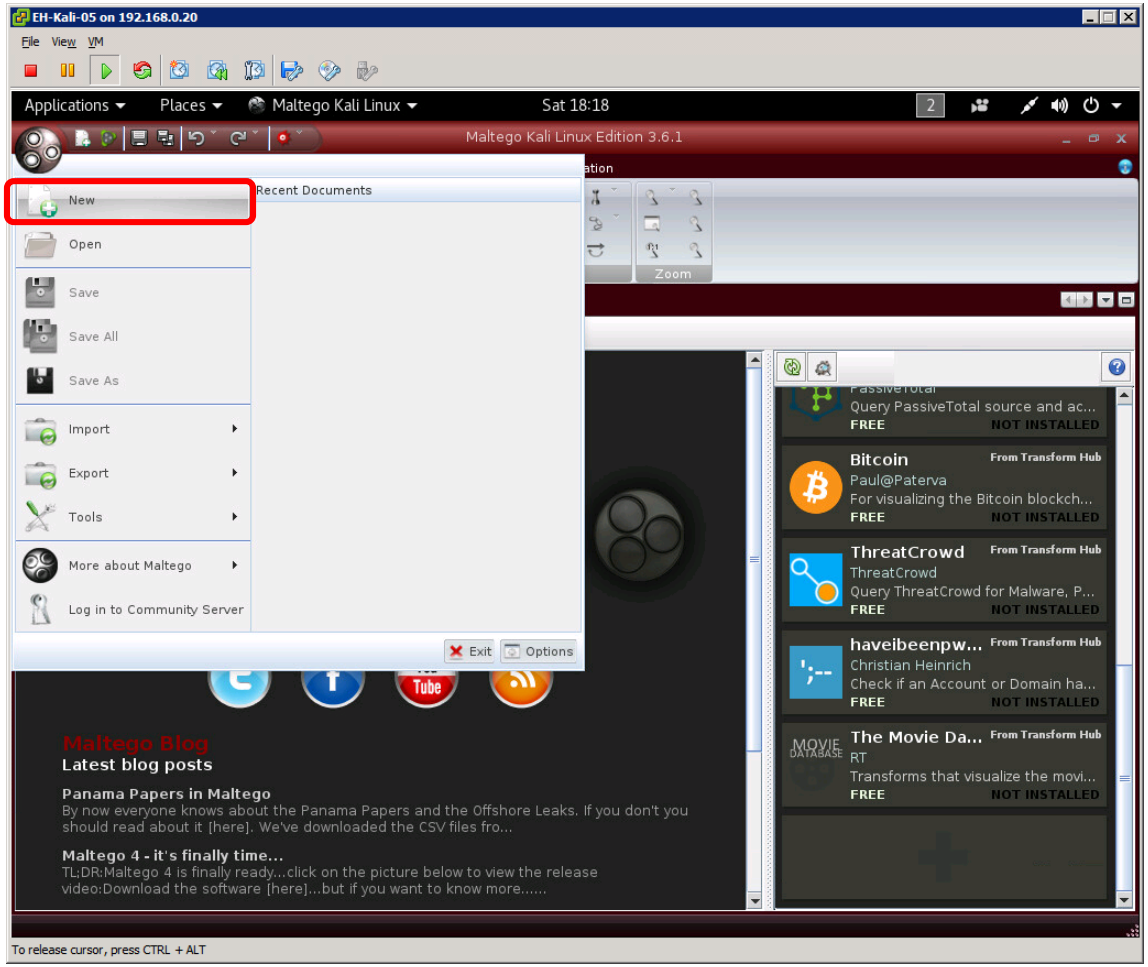
Click Finish.

Maltego



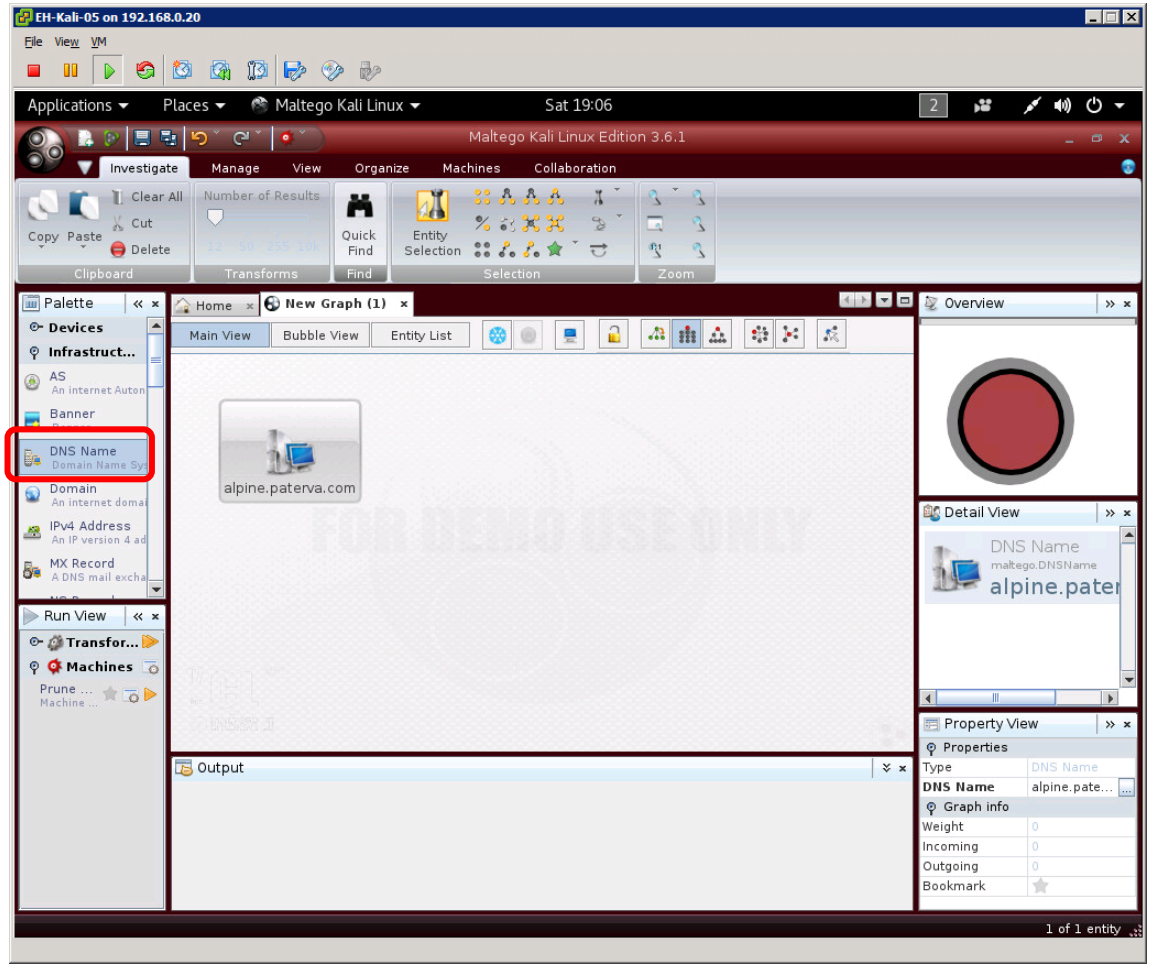
Click main Maltego icon.

Maltego



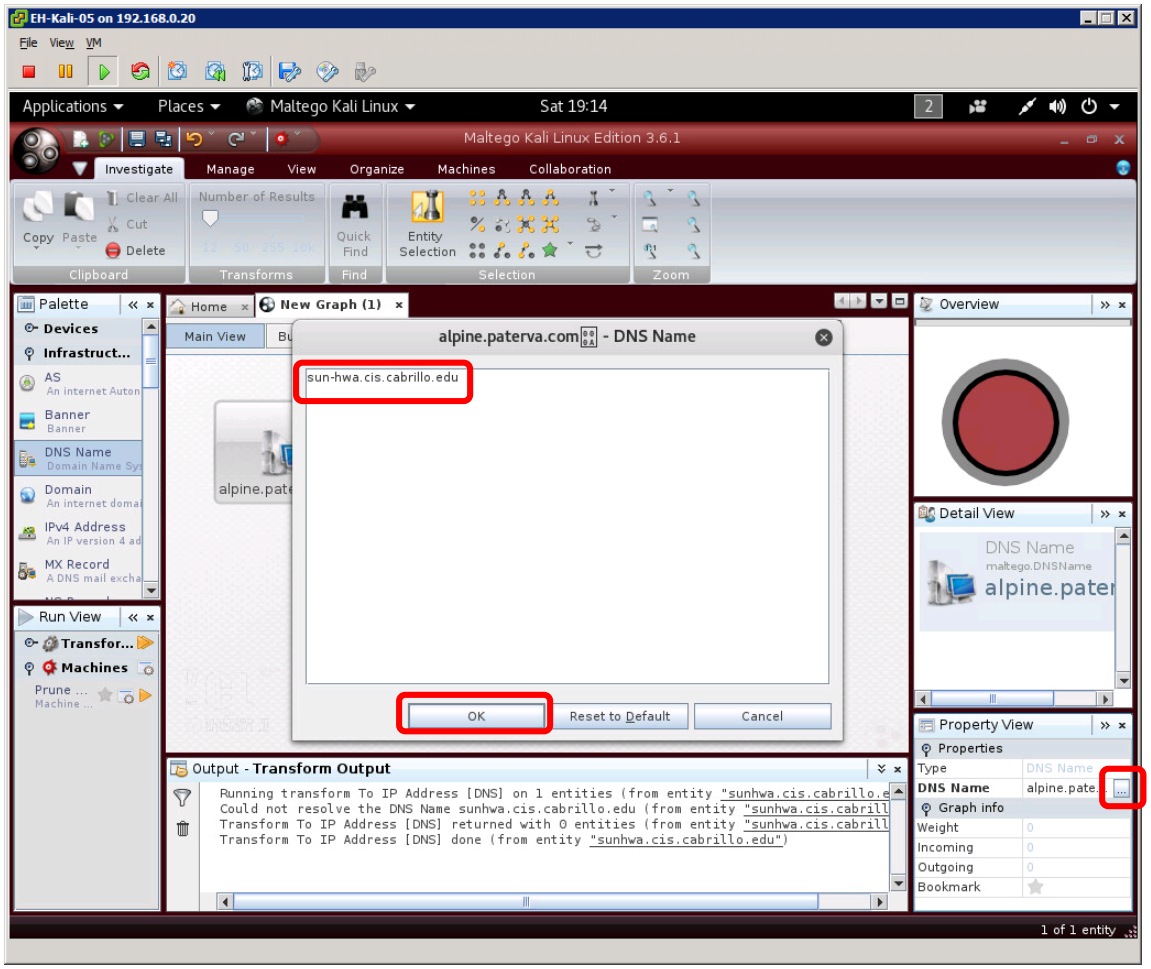
Select New.

Maltego



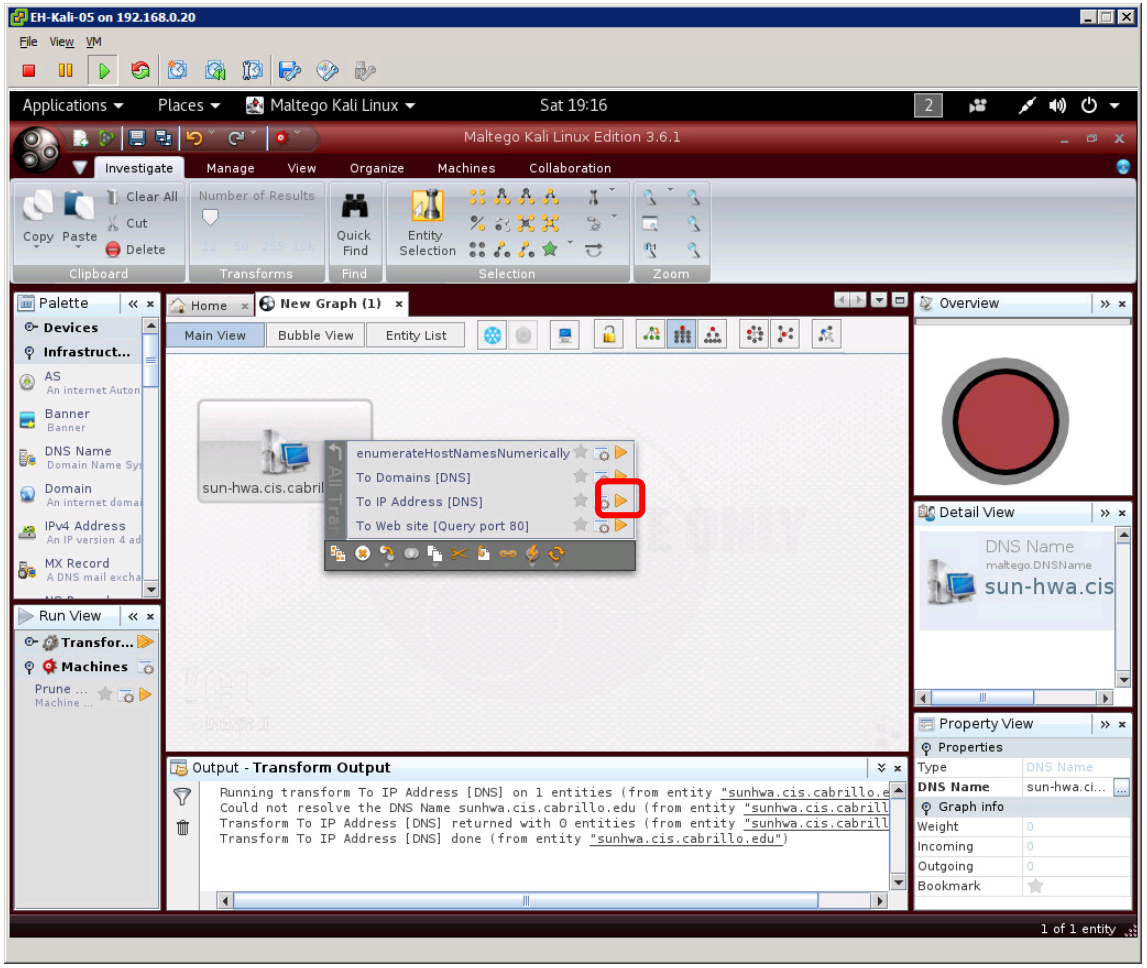
Click on DNS Name in the Infrastructure Palette and drag to the New Graph.

Maltego



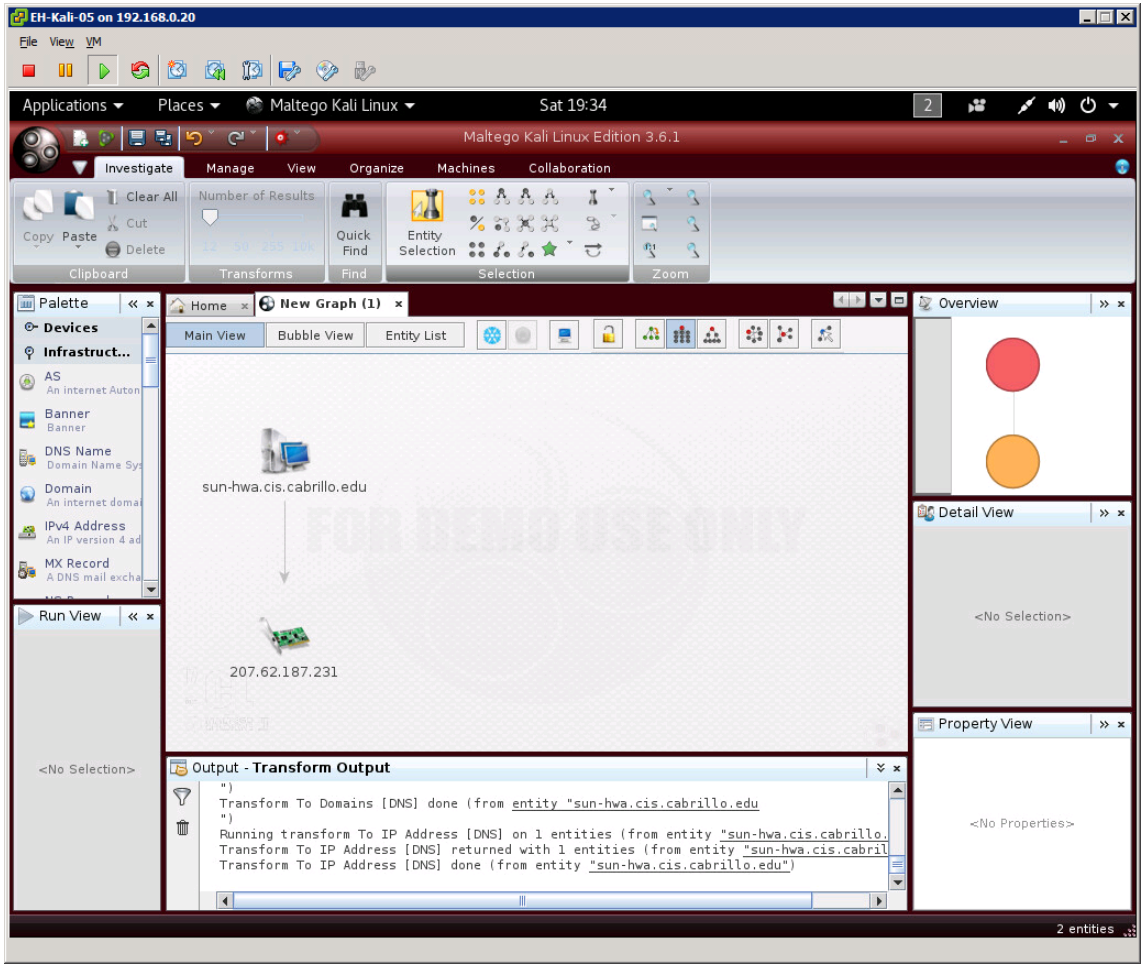
Click the "..." icon in the Property View to change the DNS Name to sun-hwa.cis.cabrillo.edu then click OK.

Maltego



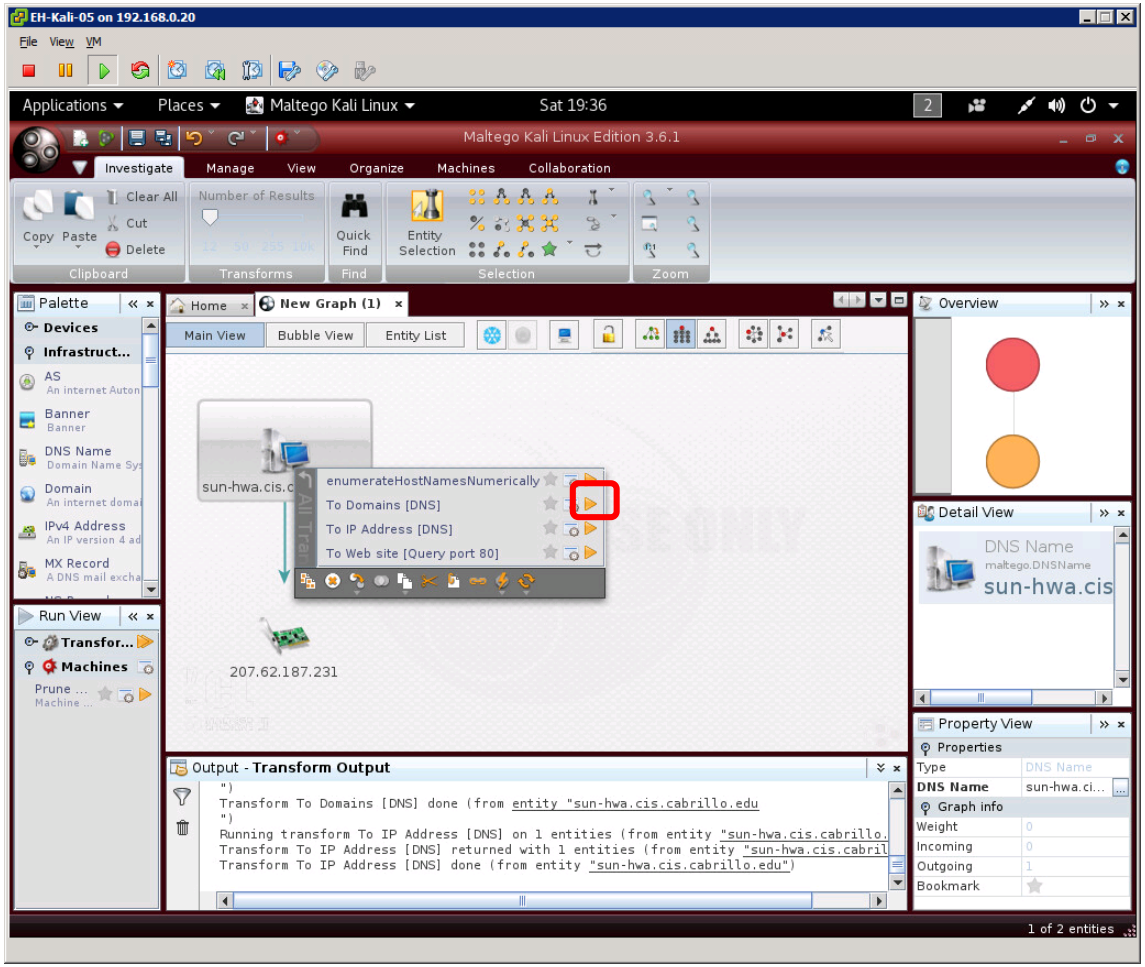
Run the "To IP Address [DNS]" transform to get the IP address.

Maltego



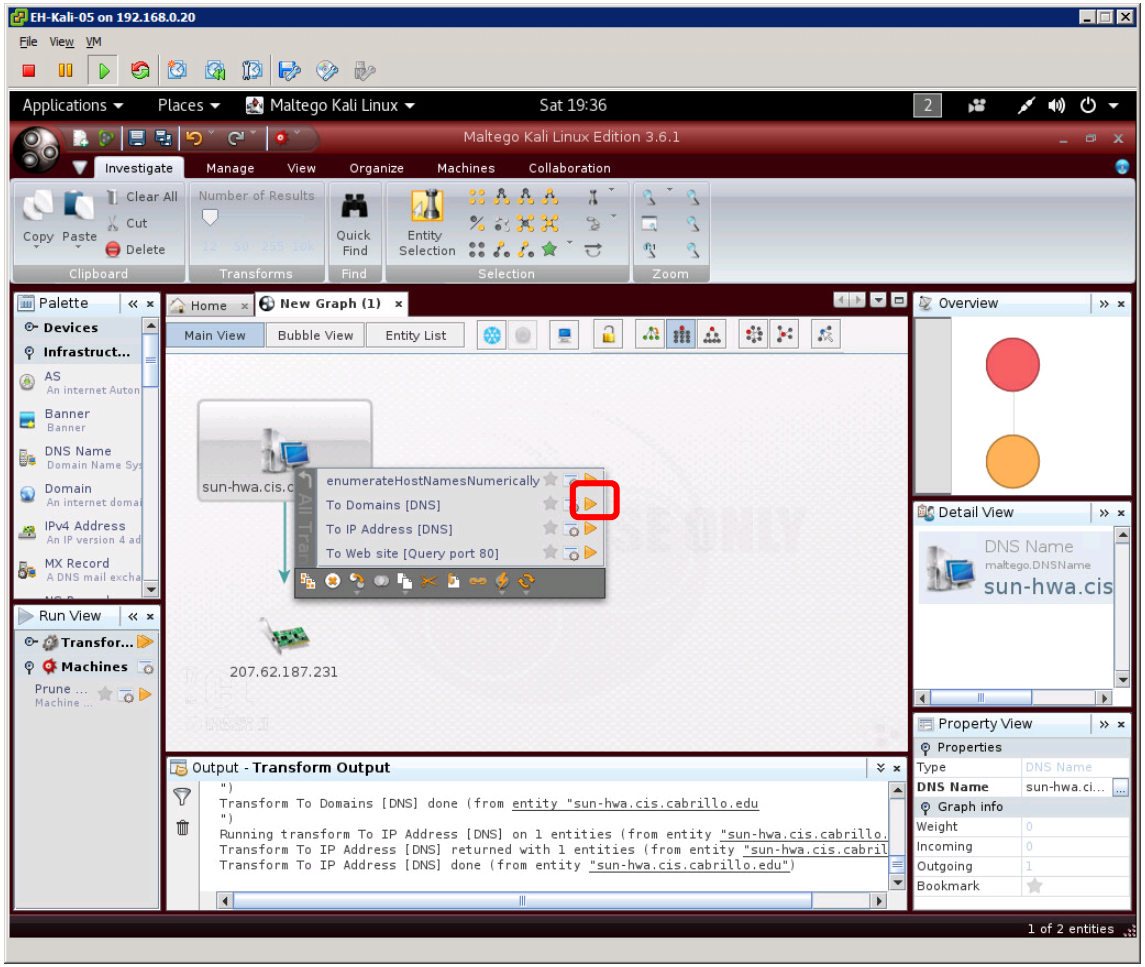
The IP address shows now below the little NIC icon.

Maltego



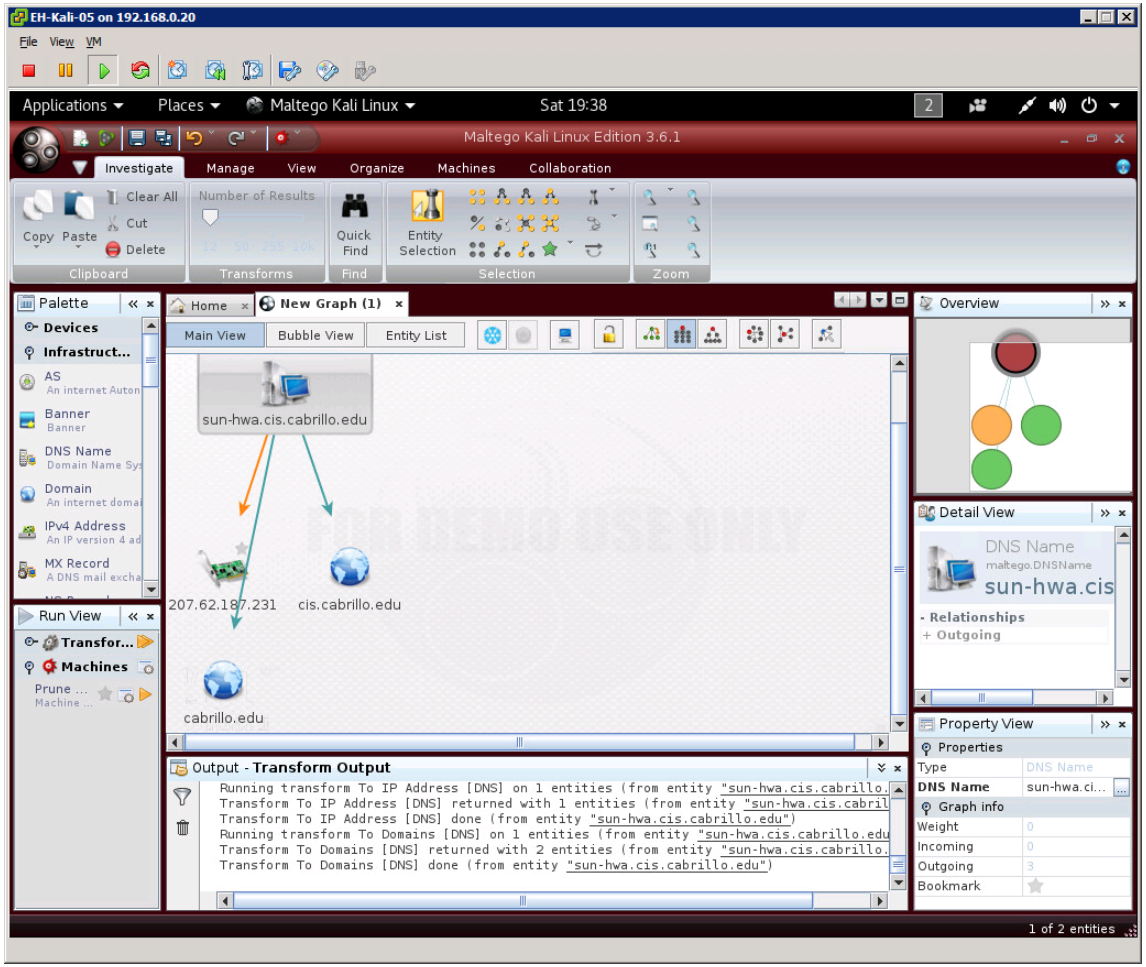
Run the To Domains [DNS] transform to get the domain.

Maltego



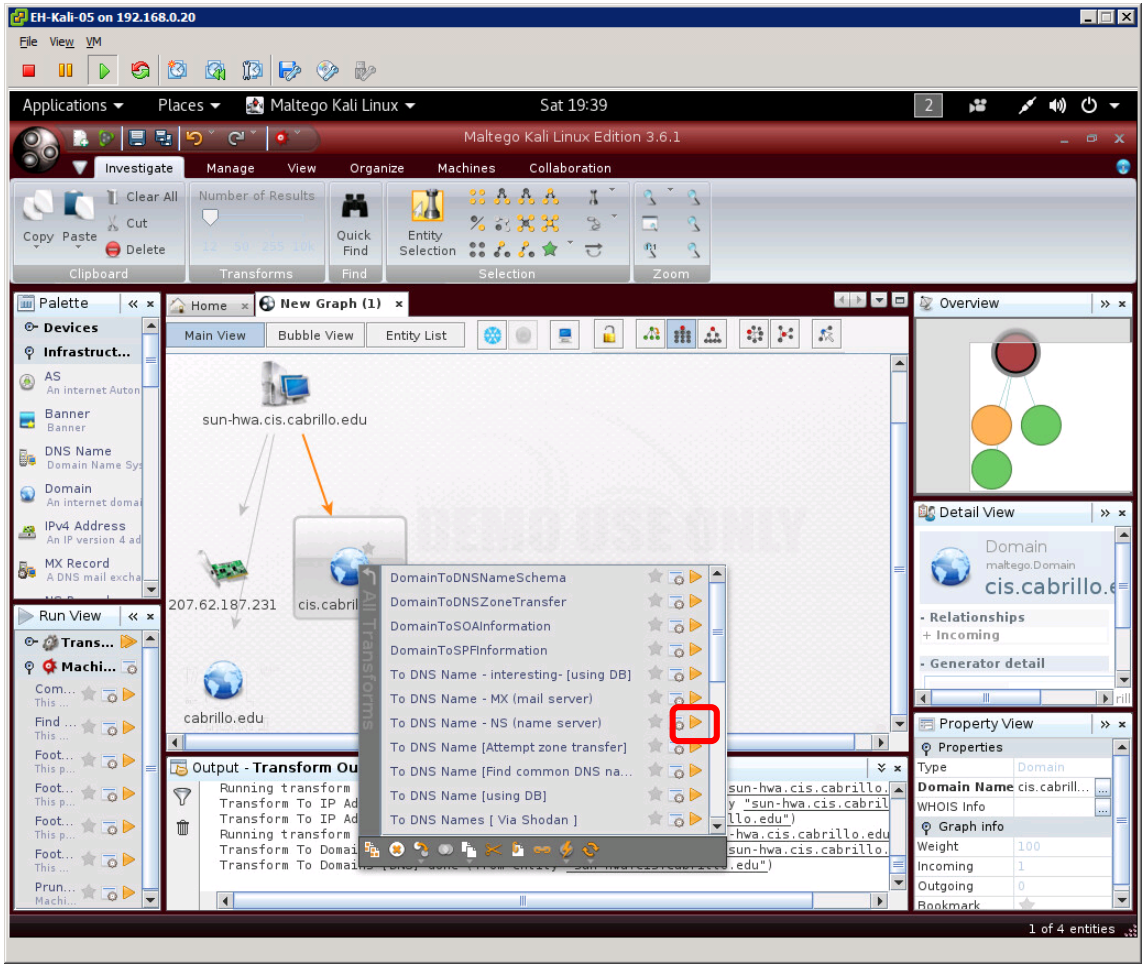
Run the "To Domains [DNS]" transform to get the domains.

Maltego



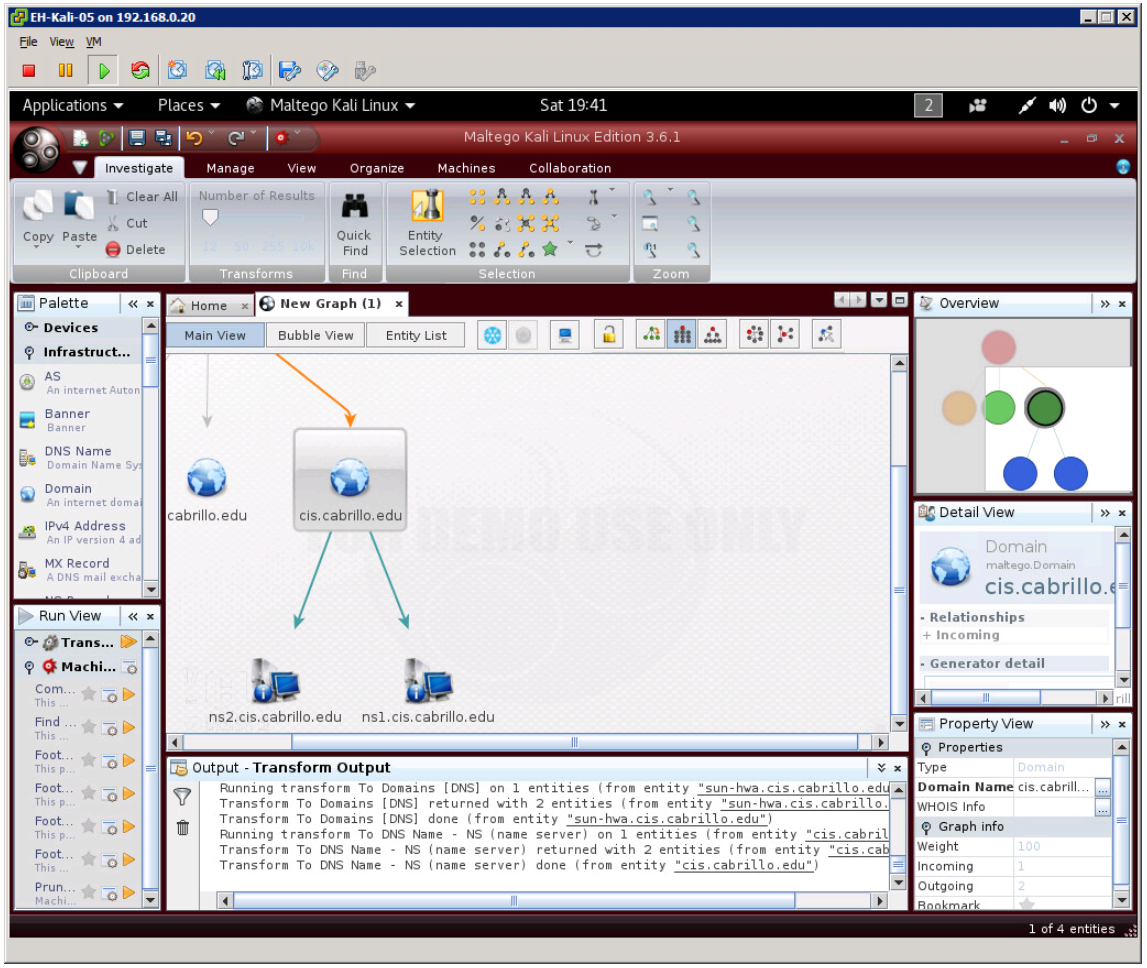
Notice both the domain and sub-domain appear.

Maltego



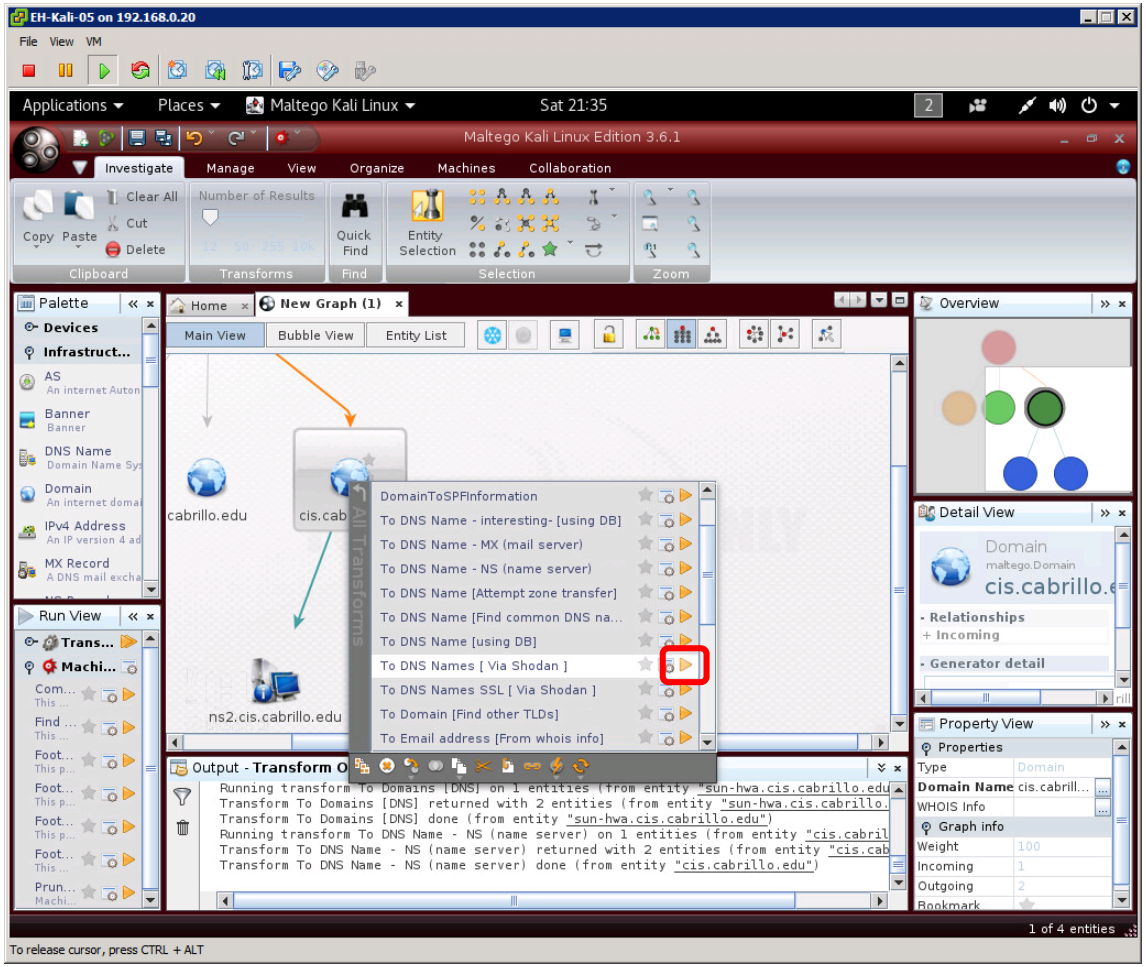
Select the sub-domain and run the "To DNS Name - NS (Name Server)" transform to get the name servers.

Maltego



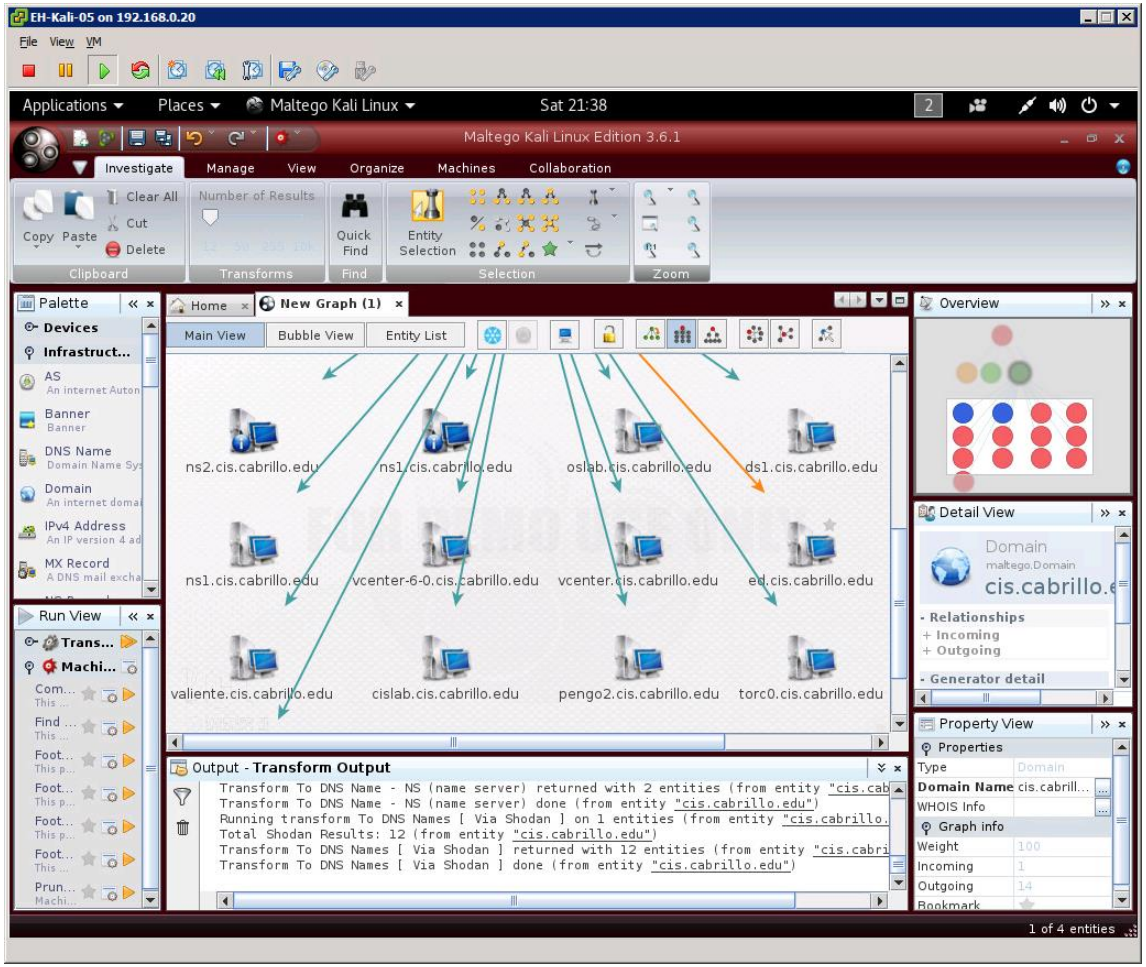
Notice both the domain and sub-domain appear.

Maltego



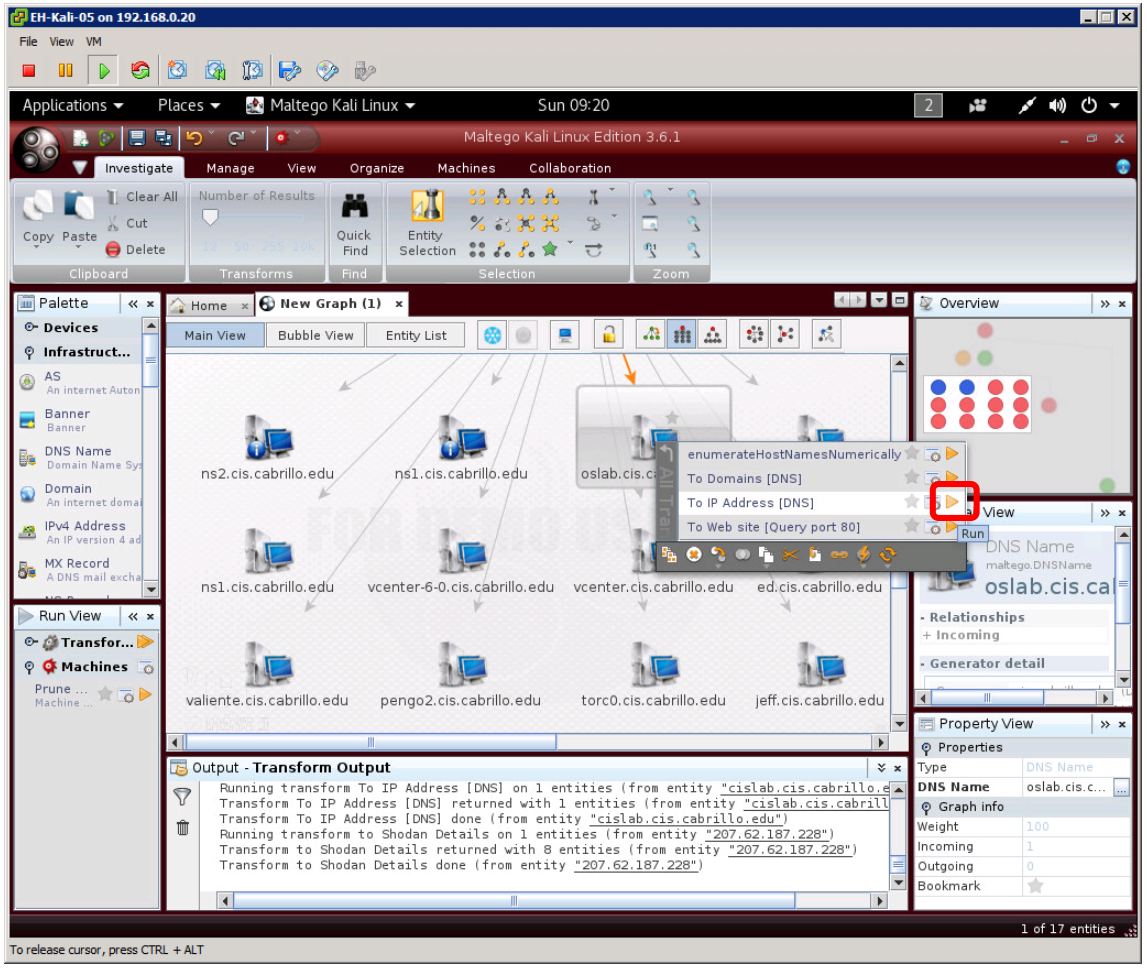
Select the sub-domain and run the "To DNS Names [Via Shodan]" to get the names of other hosts in the sub-domain.

Maltego



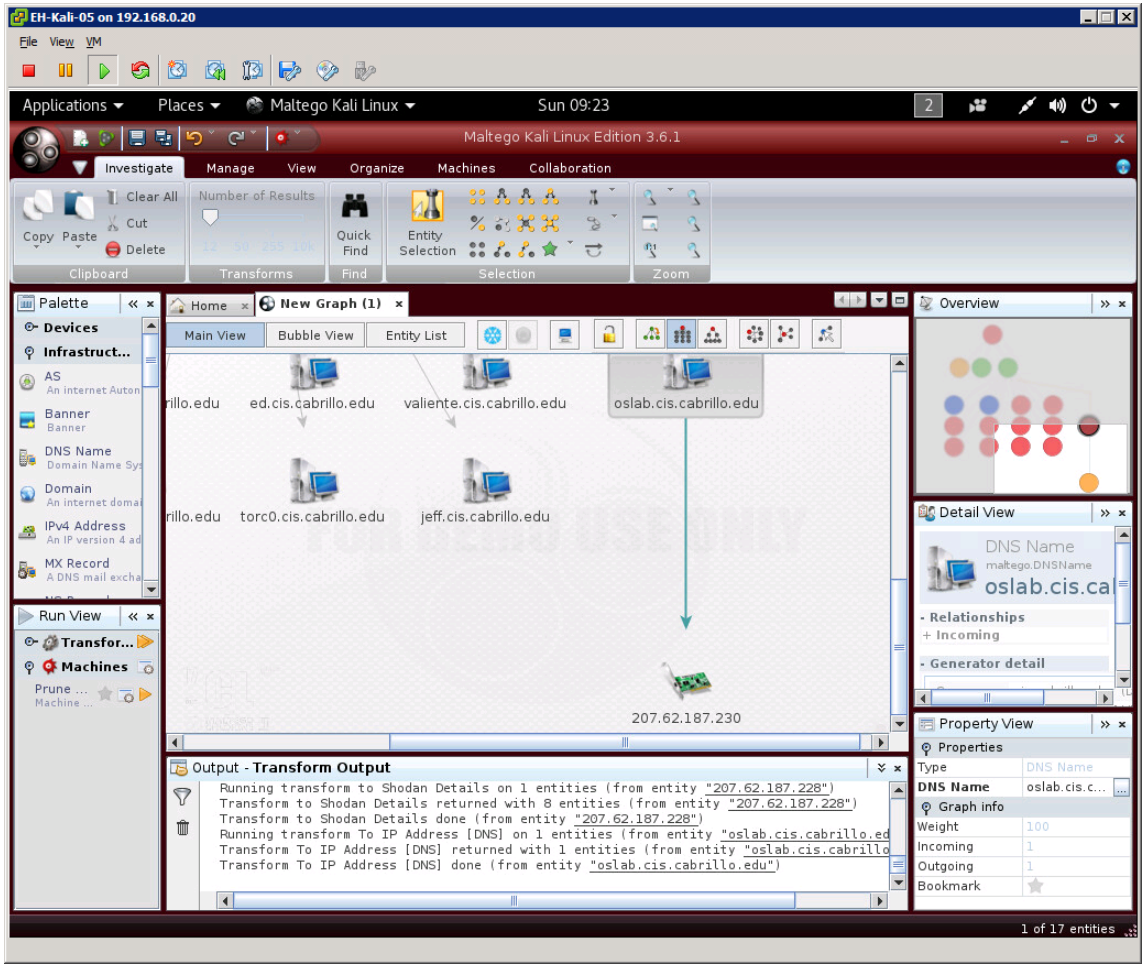
Notice we get 12 (the limit of the free version) hosts on the sub-domain.

Maltego



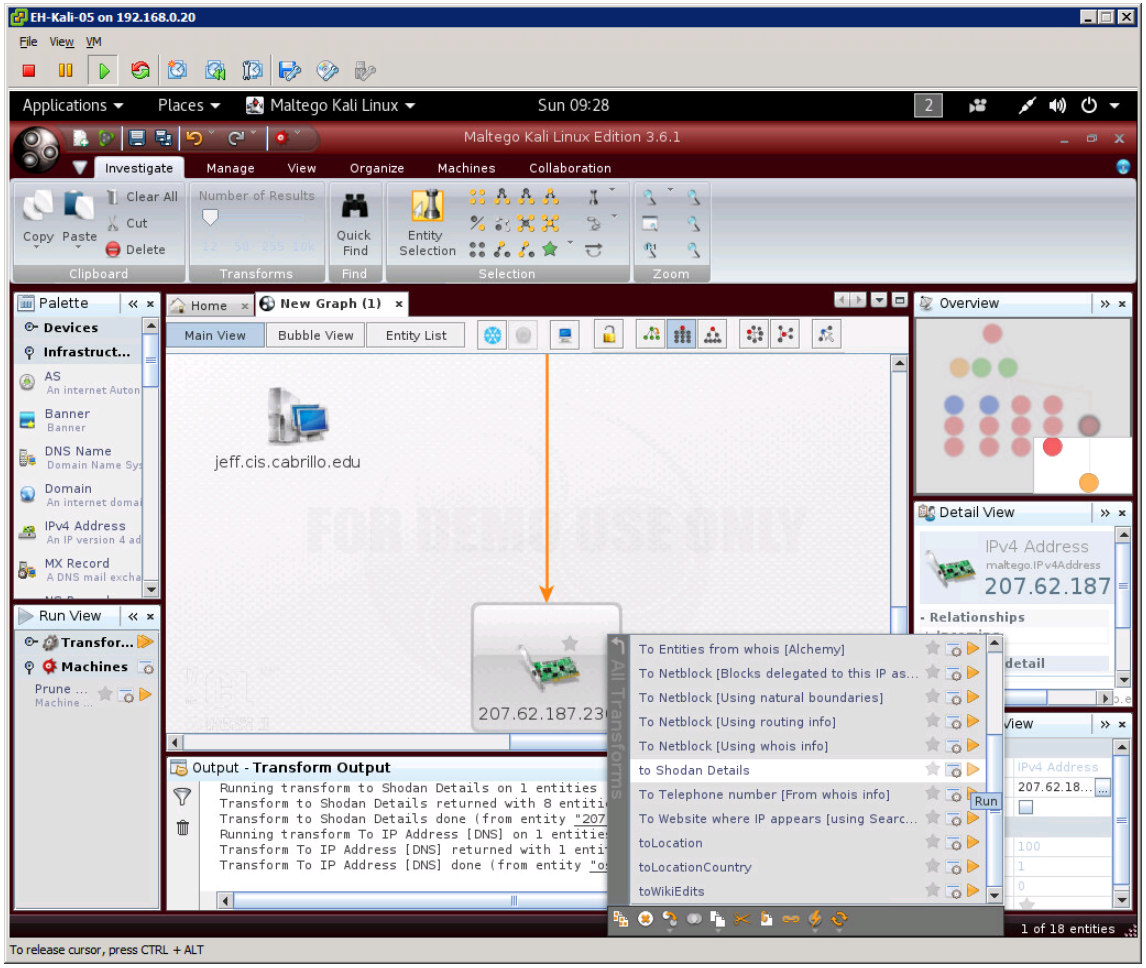
Select oslab and run the "To IP Address [DNS]" to get the IP address.

Maltego



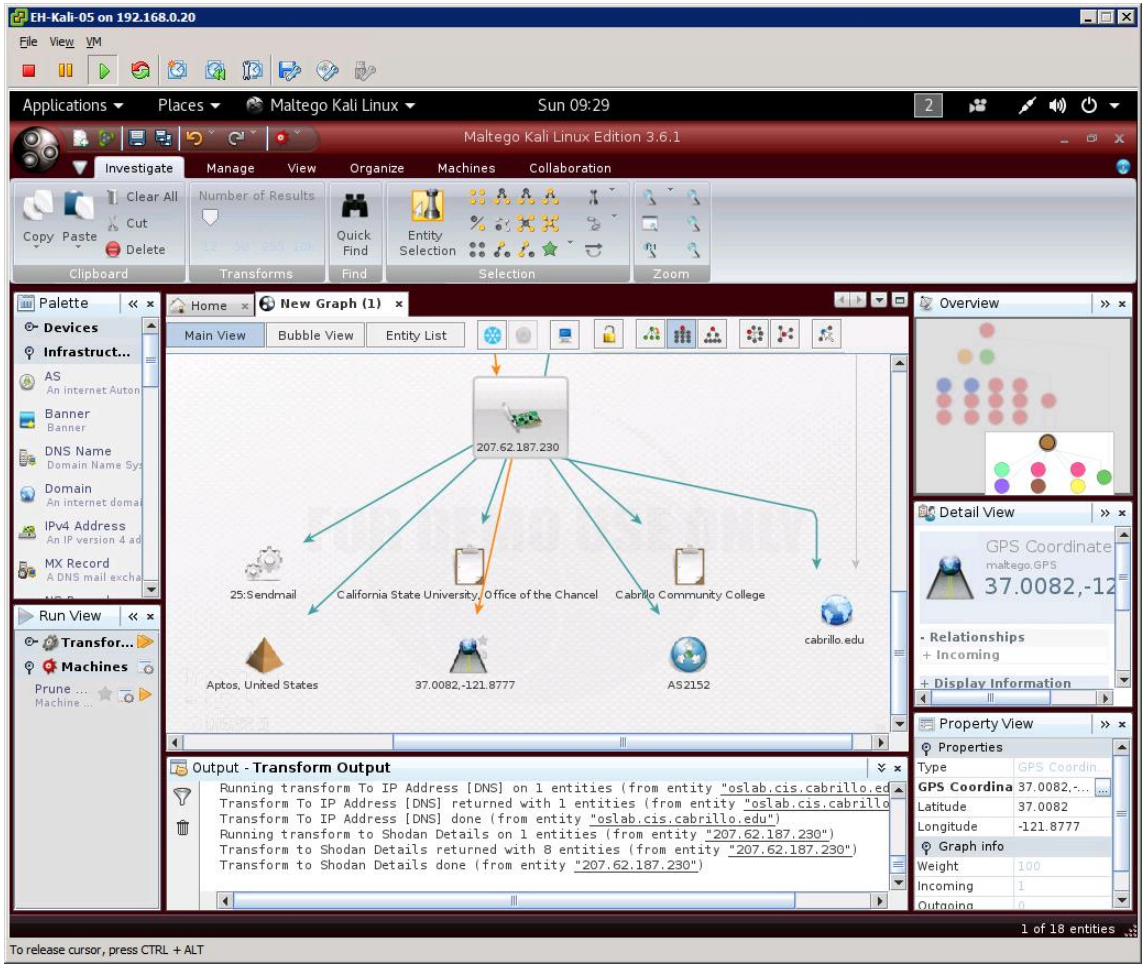
Notice we have the external IP address now.

Maltego



Select oslab and run the "To IP Address [DNS]" to get the IP address.

Maltego



Notice we have related port 25 (SMTP) info, geographic location, organizations, autonomous system number information.

Job Openings

Job title: IT Administrator

- Setup machines for new employees and troubleshoot software and hardware issues on Macs (imaging, Time Machine, remote management, etc)
- Troubleshoot networking issues and configure networking infrastructure and services (such as screencasting, interfacing with ISPs, WiFi)
- Manage and troubleshoot VoIP systems
- Take charge of new software releases and system upgrades, evaluate and install patches, and resolve software and hardware related problems
- Perform system backups and recovery as needed
- Work closely with the DevOps team to fulfill business needs of various teams on an ongoing basis
- Manage various peripherals for employees (printers, scanners, external hard drives)

Some skills we consider critical to being an IT Administrator:

- Familiarity with Linux systems (Ubuntu)
- Familiarity with file storage services (Box, Dropbox, S3)
- Familiarity with OSX imaging
- 2+ years previous support experience (Apple Genius bar, IT administrator, etc)

http://www.indeed.com/

Job openings can reveal internal IT infrastructure

Job title: System Administrator

Typical Qualifications:

Any combination of education, training and or/experience which substantially demonstrates the following knowledge, skills and abilities:
Thorough knowledge of:

1. Cisco routing and switching
2. Windows 2008/2012 Server
3. Microsoft Exchange
4. Windows Software Update Services (WSUS)
5. Microsoft Internet Information Services (IIS)
6. Microsoft SQL Server
7. VMware virtualization (Server and desktop)
8. Nimble iSCSI SANs
9. Veeam Backup and Recovery
10. ShoreTel VoIP phone system
11. Desktop and server system deploym
12. Principles, practices, and techniques,

Job openings can reveal internal IT infrastructure

1. Subject matter expert on datacenter and computer systems (servers, desktops, VDI, routers, switches), security, Court's critical systems
2. Resolve problems with a wide variety of computer equipment (PCs, servers, printers, SAN, NAS, etc.)
3. Perform project management including scheduling, developing critical paths, tracking, contingency planning, resource allocation, and team leadership
4. Communicate effectively with all levels of management
5. Be flexible and adaptable to continually changing demands or situations
6. Prepare clear, concise, and accurate documentation
7. Build effective work teams
8. Establish and maintain effective working relationships
9. Be a strong team player with excellent customer service skills

http://www.indeed.com/

Highly Desired:

1. CCNA Routing and Switching
2. MCITP: Server Administrator on Windows Server 2008 or 2012.
3. VMware VCP 5-DCV, VCP 6-DCV?

Activity

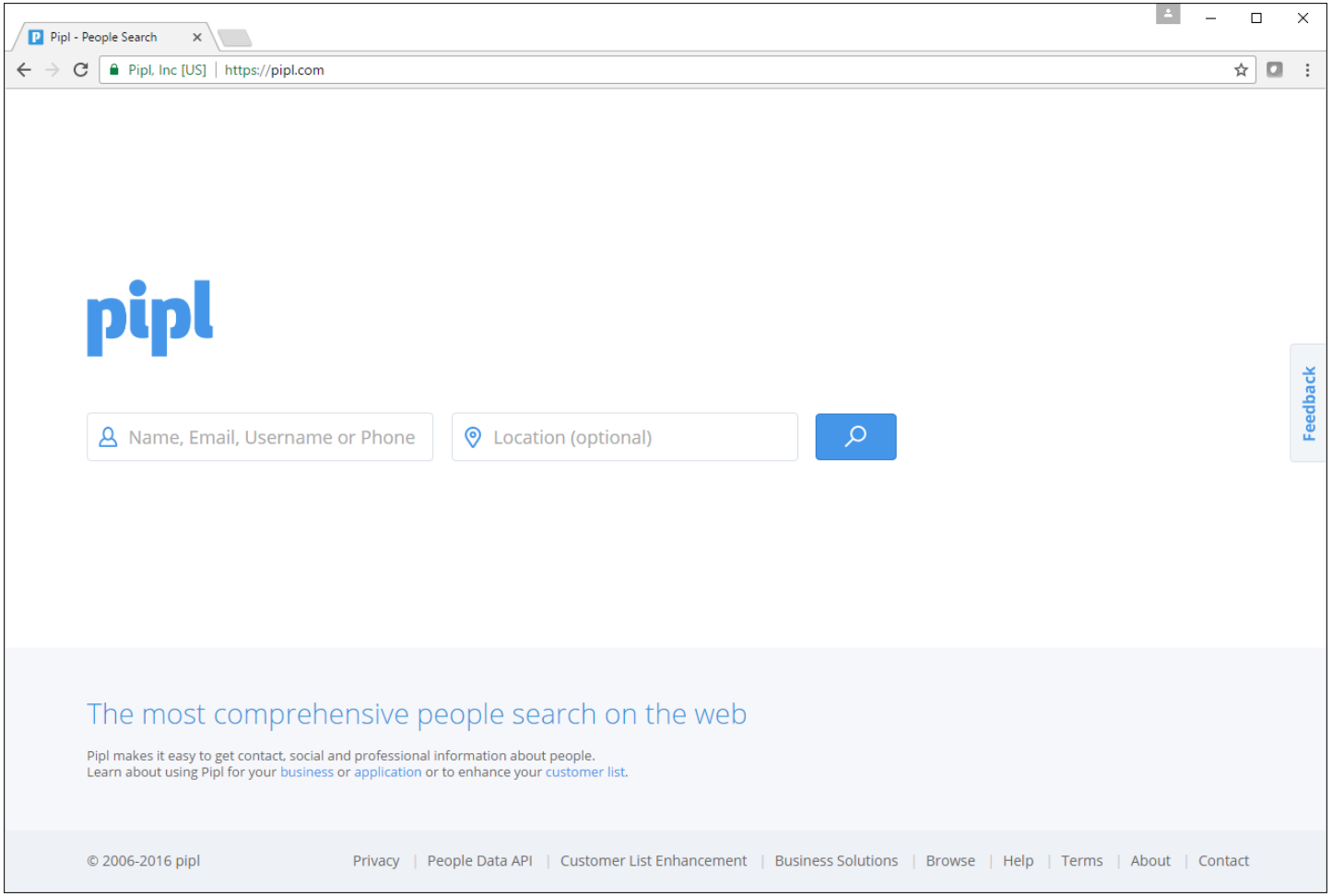
Browse the *System Administrator* job listings on monster.com or indeed.com.

Did you find any specific system or network information?

If so put what you found in the chat window

pipl

pipl



Lookup information on people

https://pipl.com/

Activity

Try using pipl:

https://pipl.com/

on yourself.

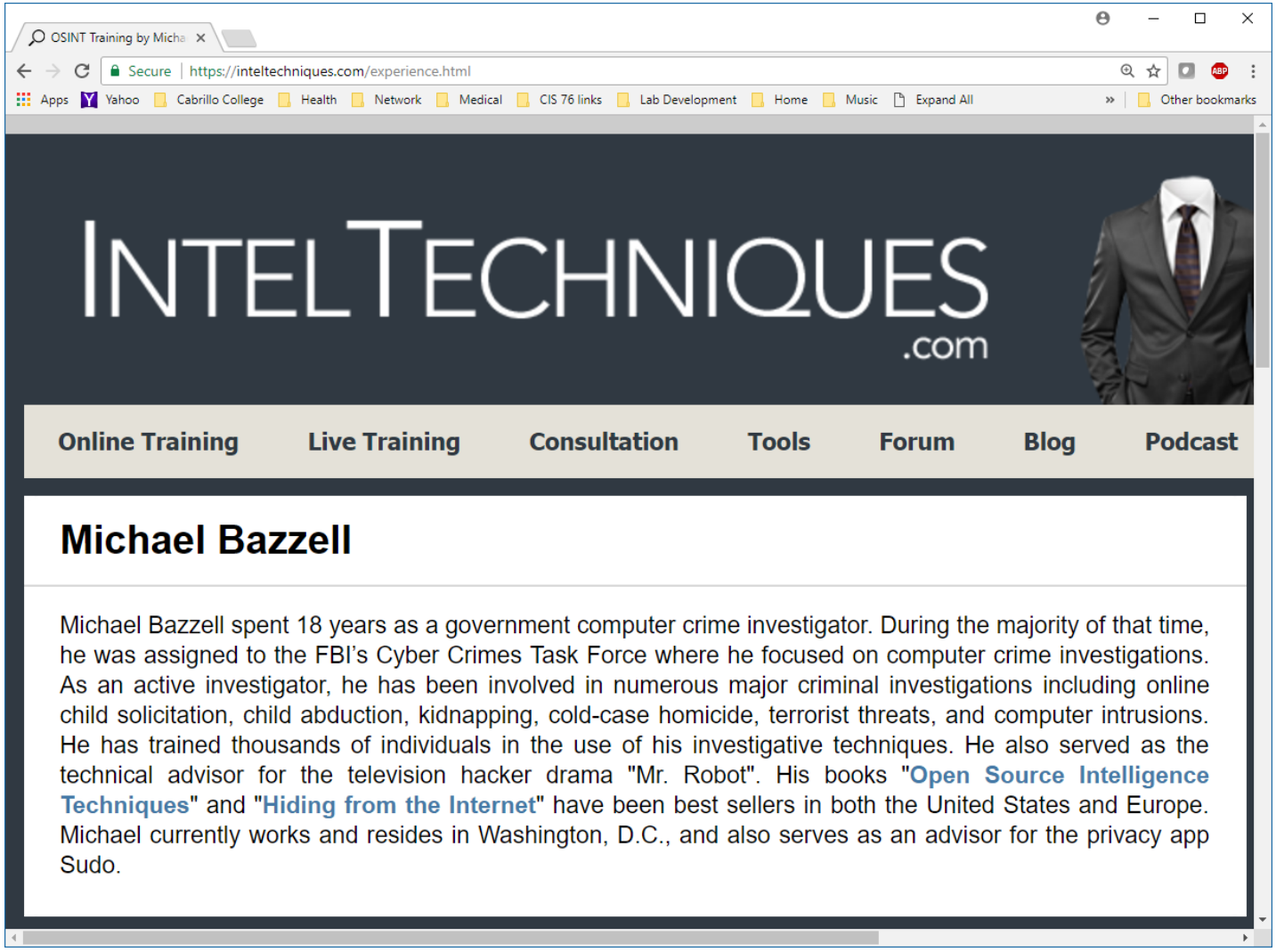
Try it on your:
- name
- phone number
- email address
- username

Any observations?

Write any observations in the chat window

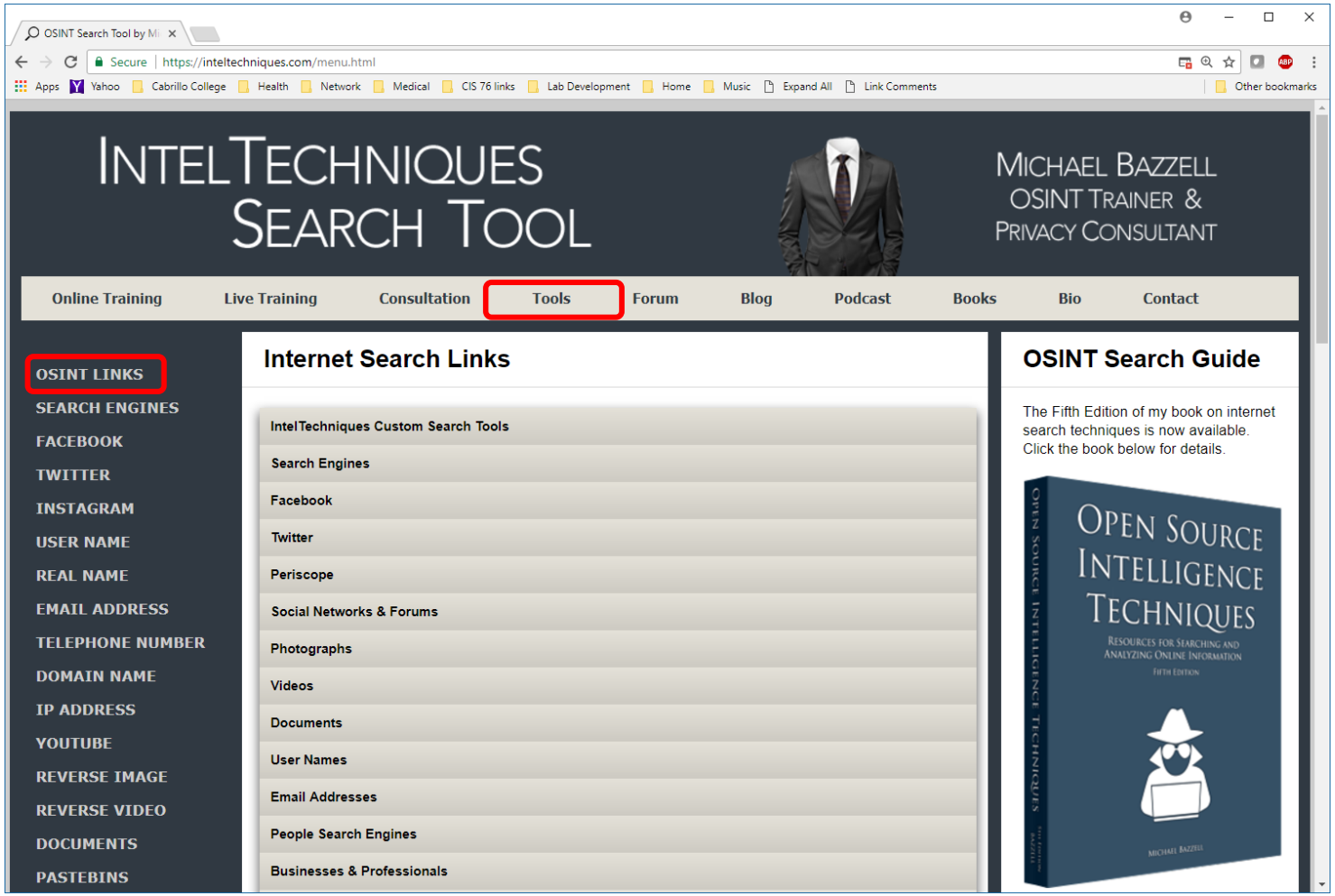
IntelTechniques

IntelTechniques



https://inteltechniques.com/

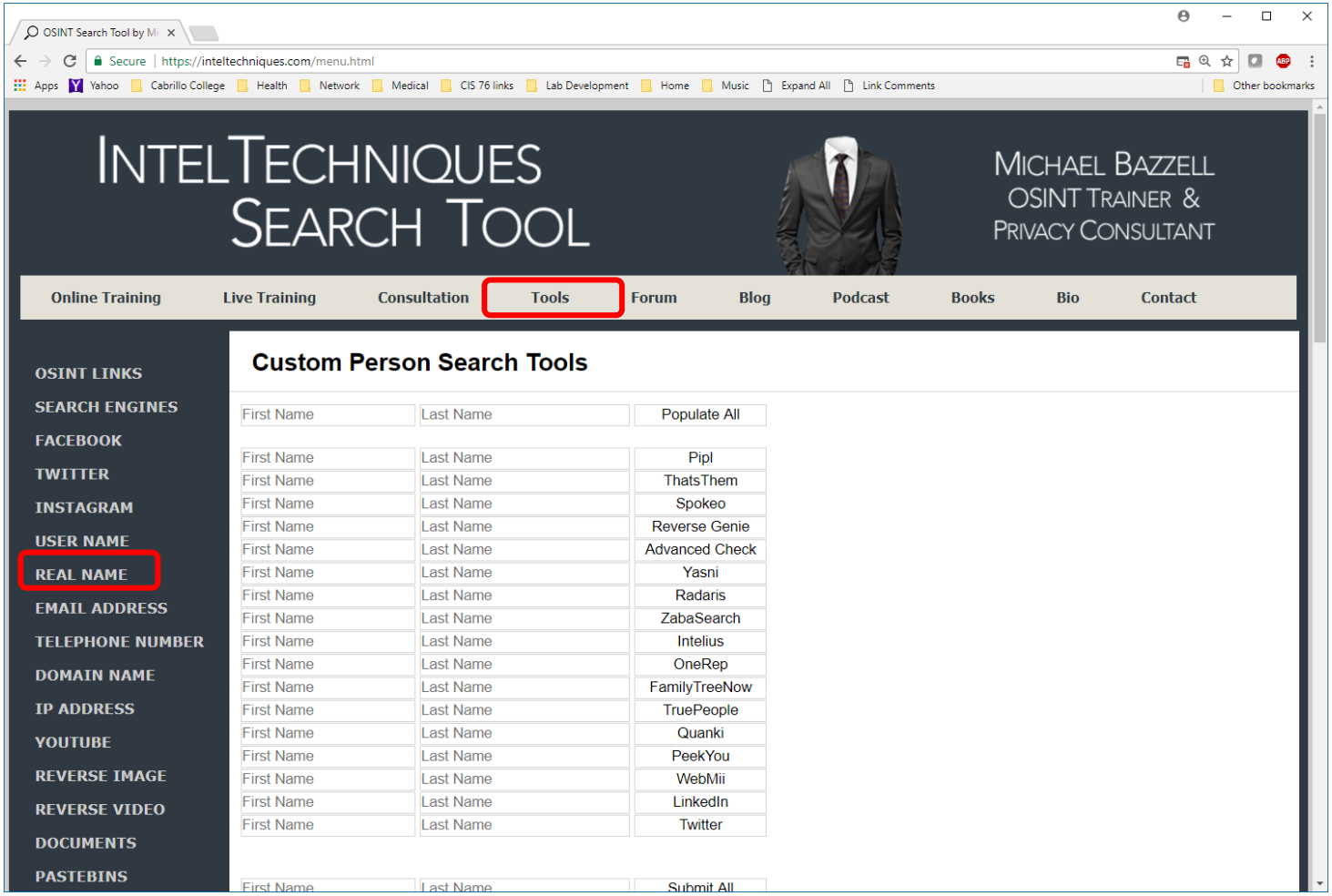
IntelTechniques



https://inteltechniques.com/

Lots and lots and lots of open source tools!

IntelTechniques



https://inteltechniques.com/

Lots and lots and lots of open source tools!

Activity

Try https://inteltechniques.com/menu.html

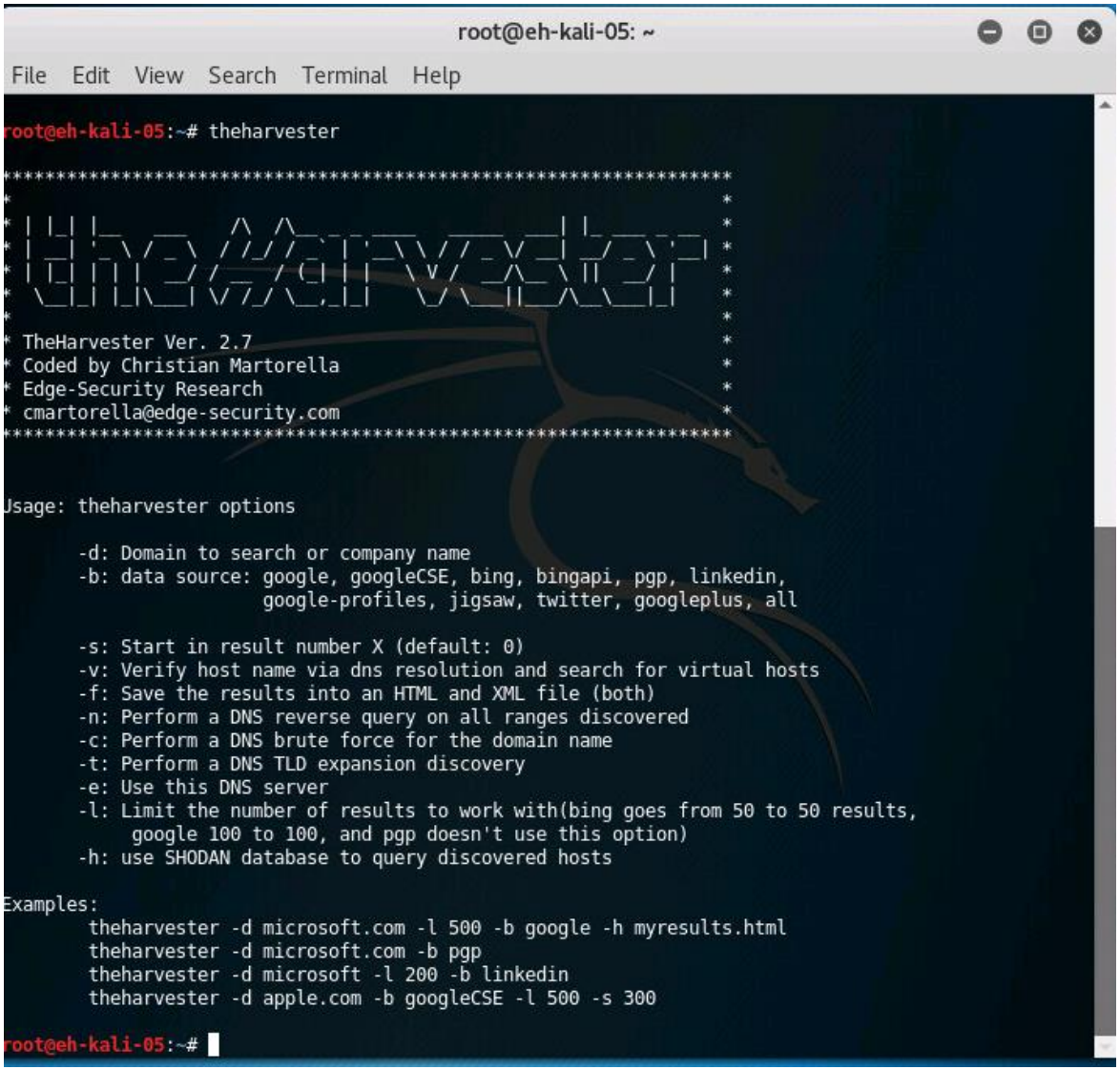
Select:
- OSINT LINKS (on left panel)
- Then select: Photographs (in middle pane)
- Then scroll down and select: Foto Forensics

Upload this photograph:
https://simms-teach.com/docs/cis76/pic02.jpg

Put the date and time that photo was taken and the camera model in the chat window

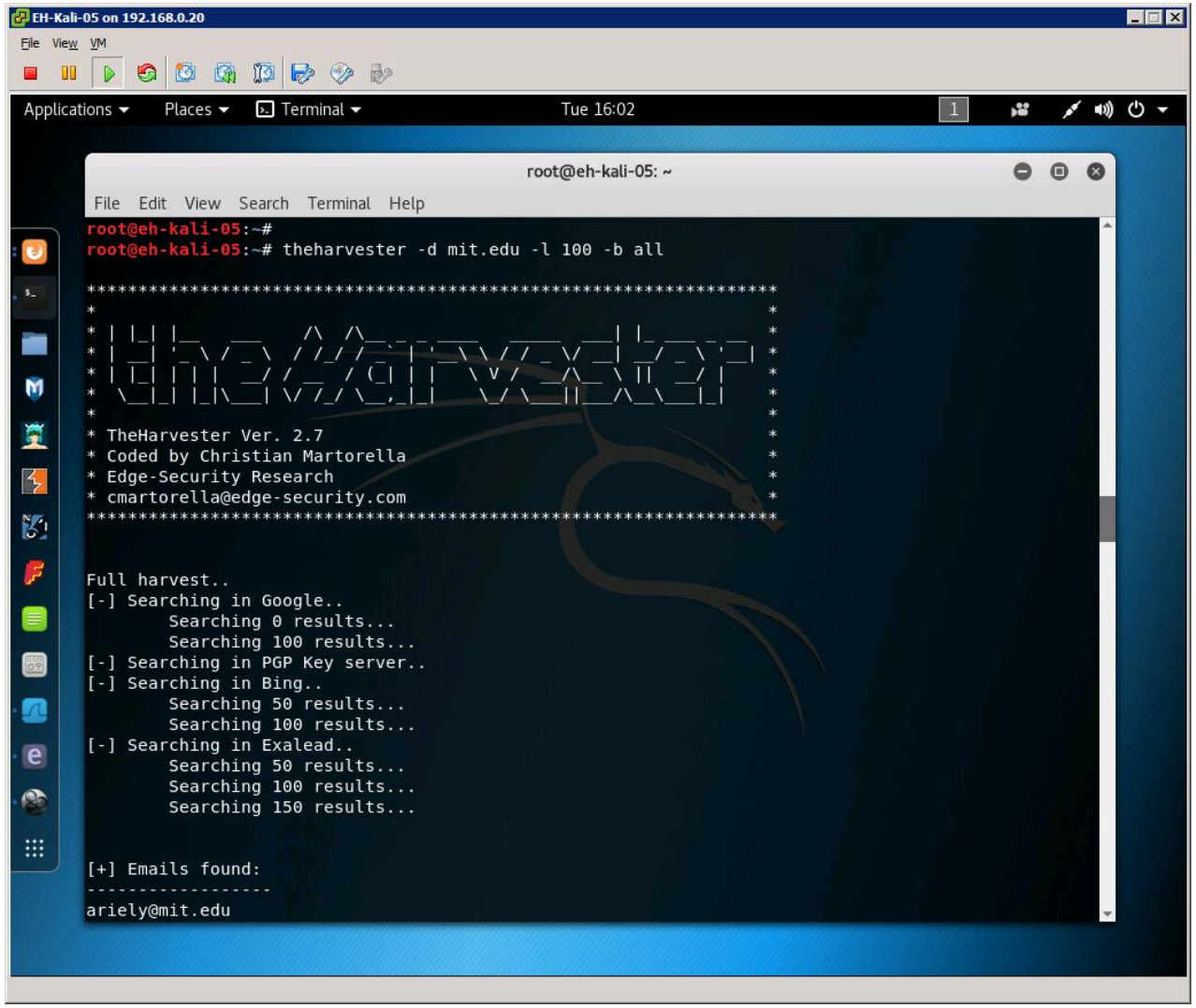
Harvester

theharvester



The Harvester is run from the command line on Kali

theharvester -d mit.edu -l 100 -b all

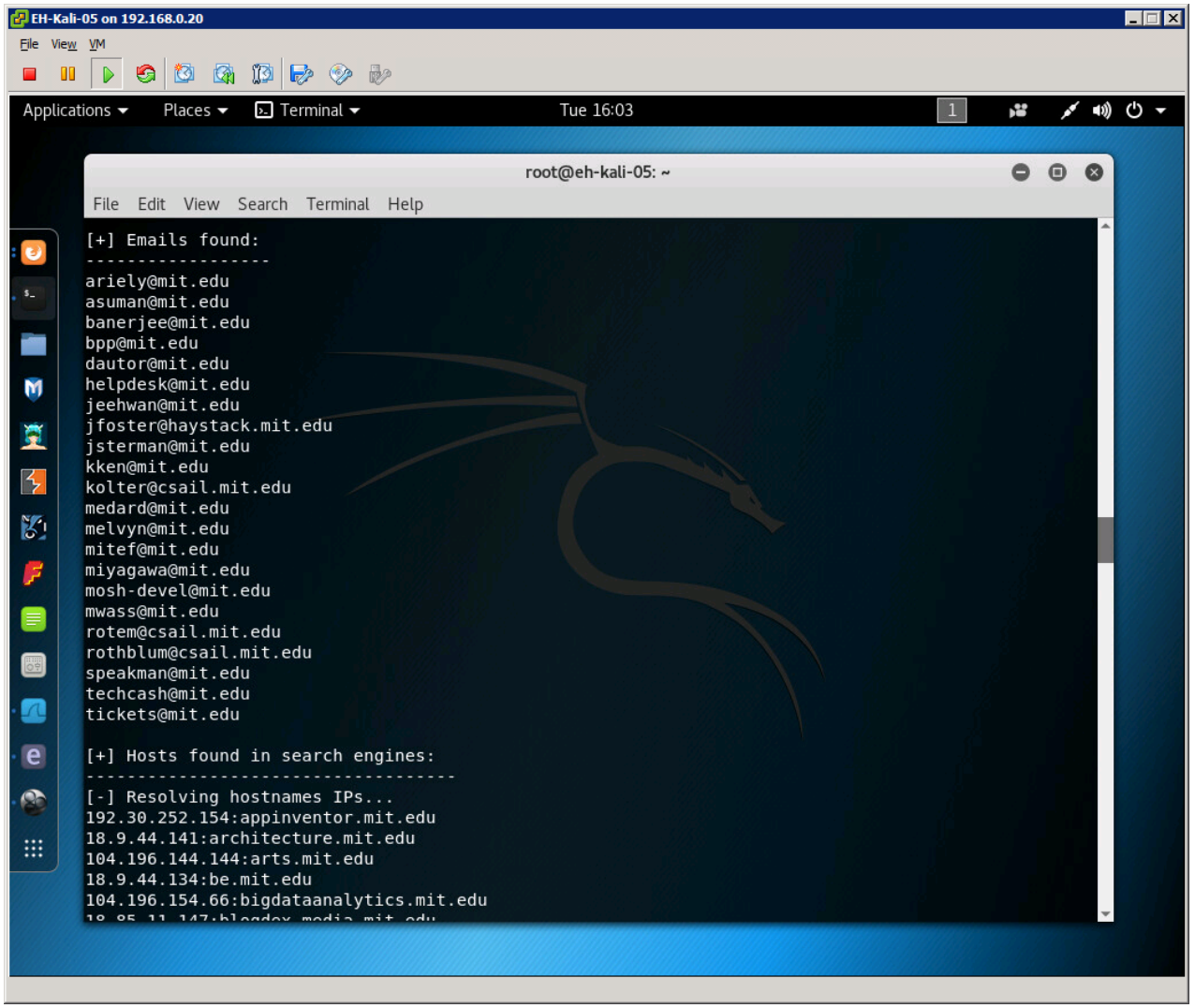


Options:

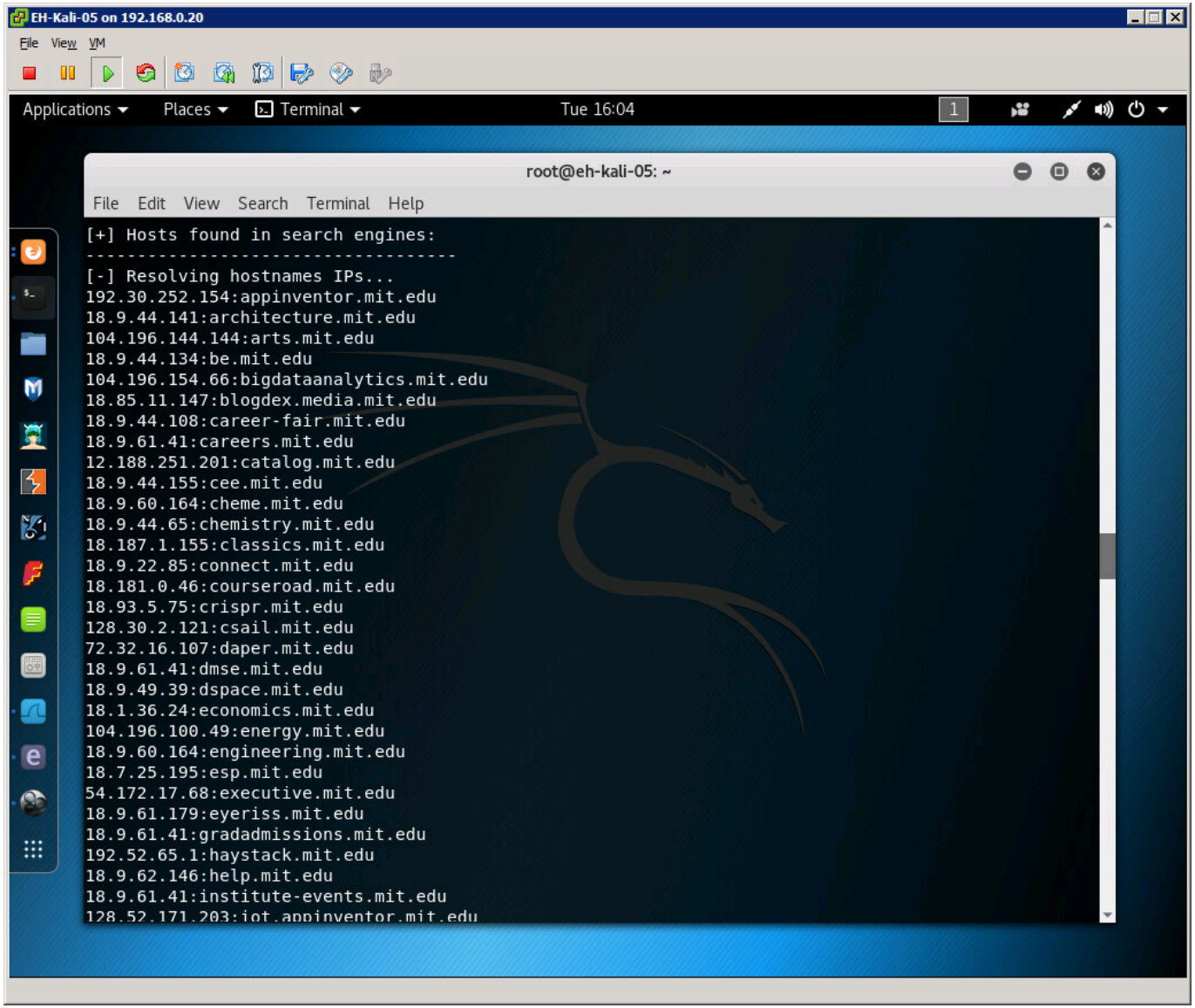
-d specifies the domain

-l limits the number of results

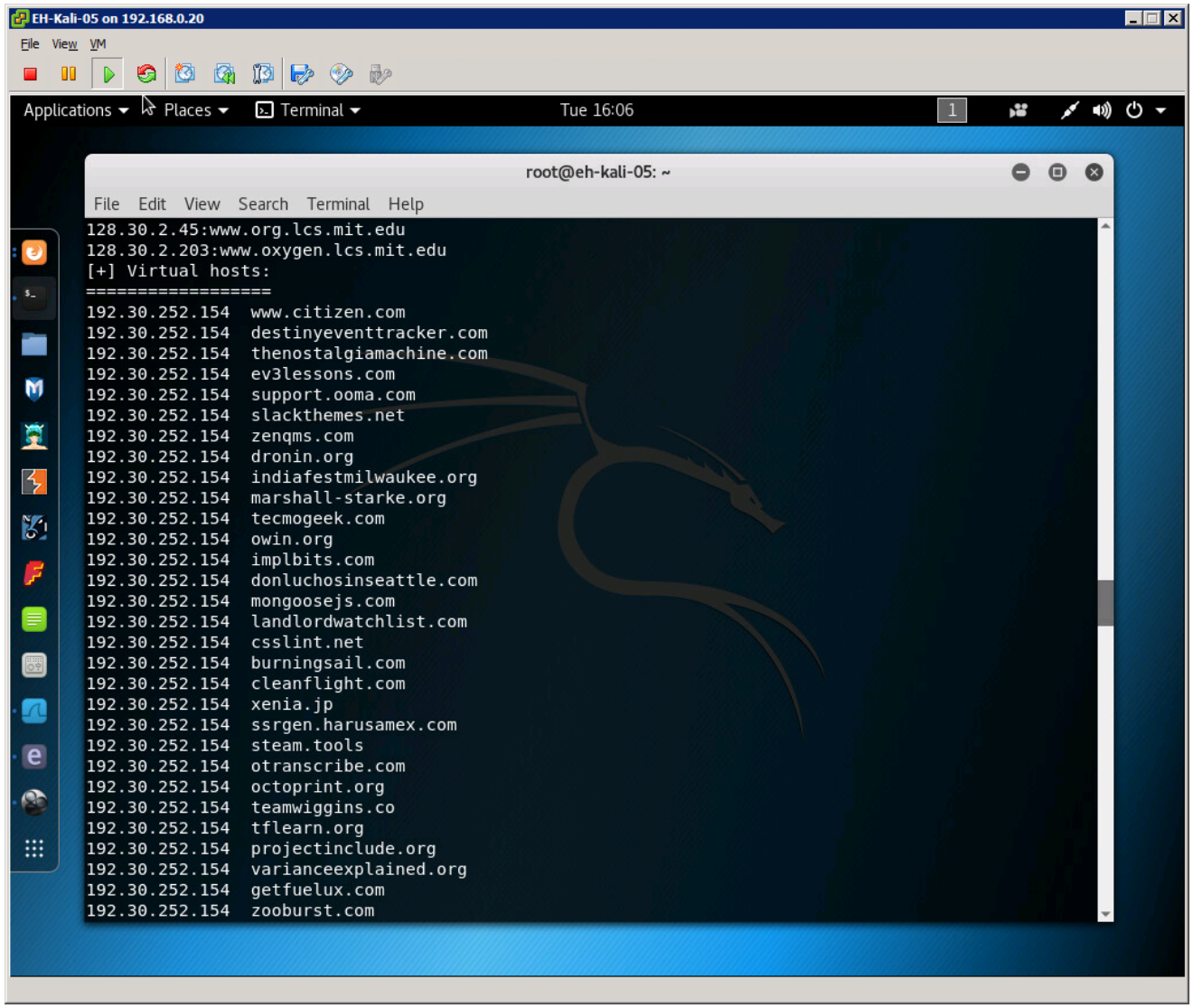
-b selects the data source



emails found



hosts found in search engines

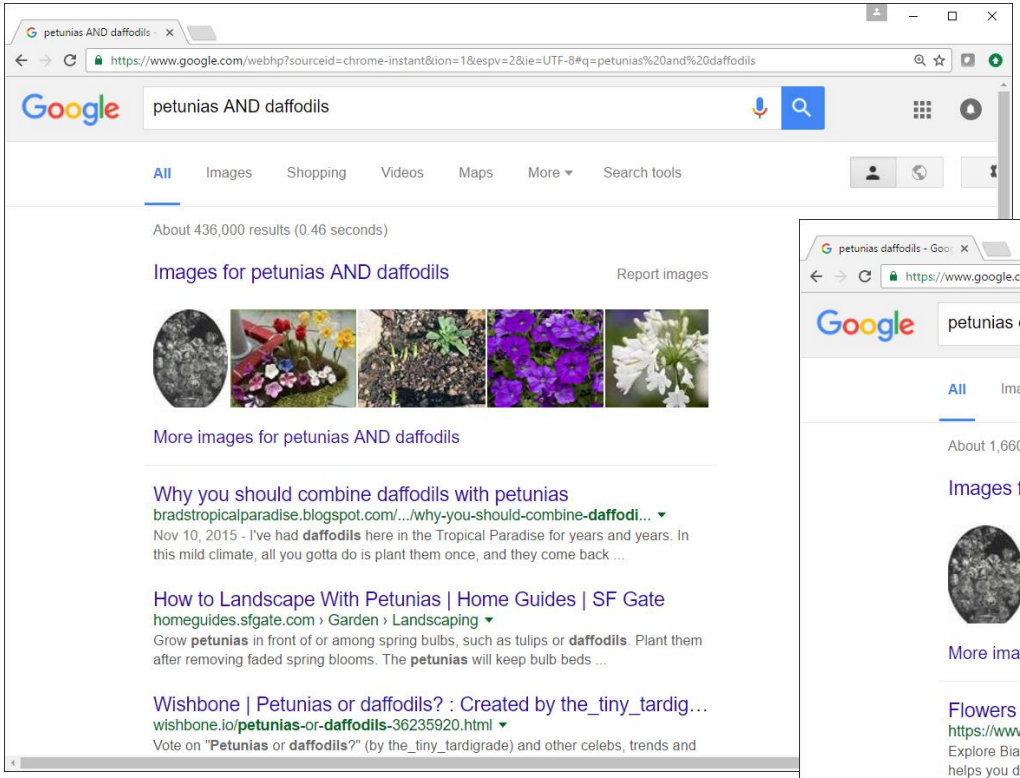


virtual hosts

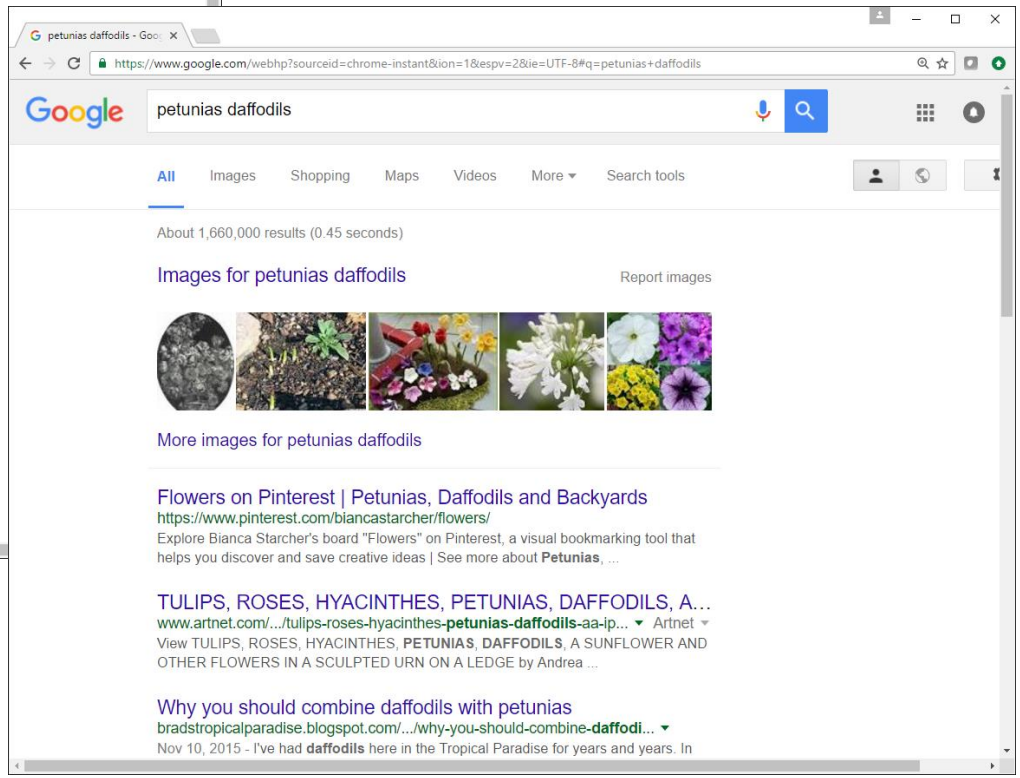
Google Hacking

Google Hacking with AND (or space) operator

petunias AND daffodils



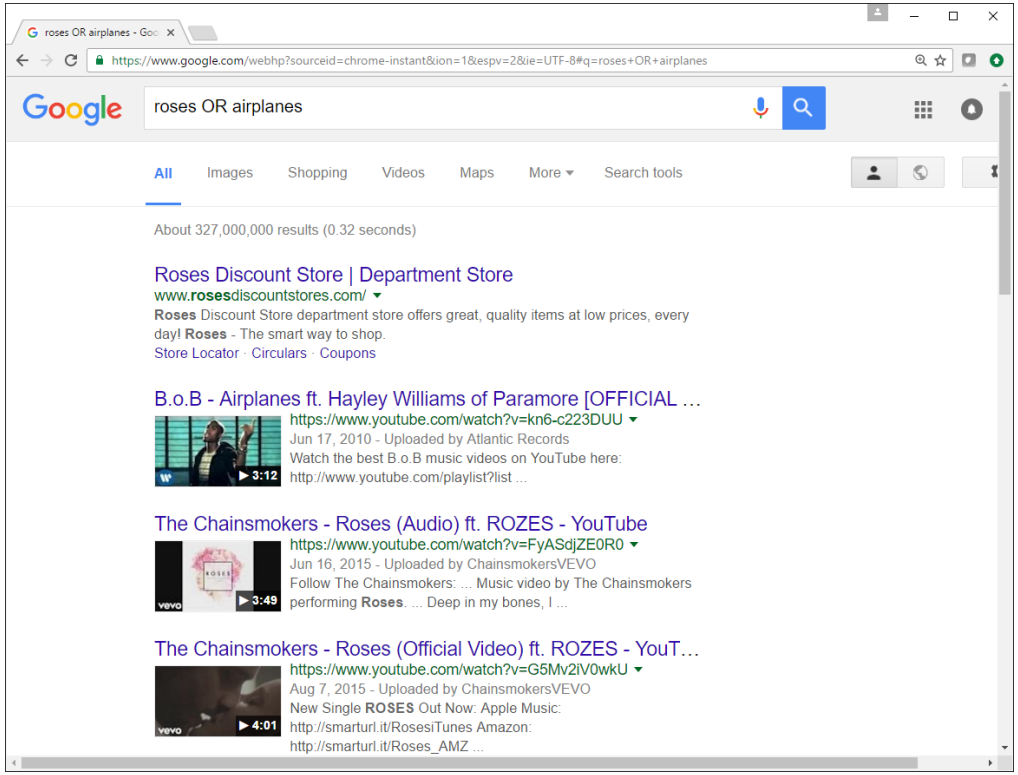
petunias daffodils



Finds pages containing both petunias and roses.

Google Hacking with OR (or |) operator

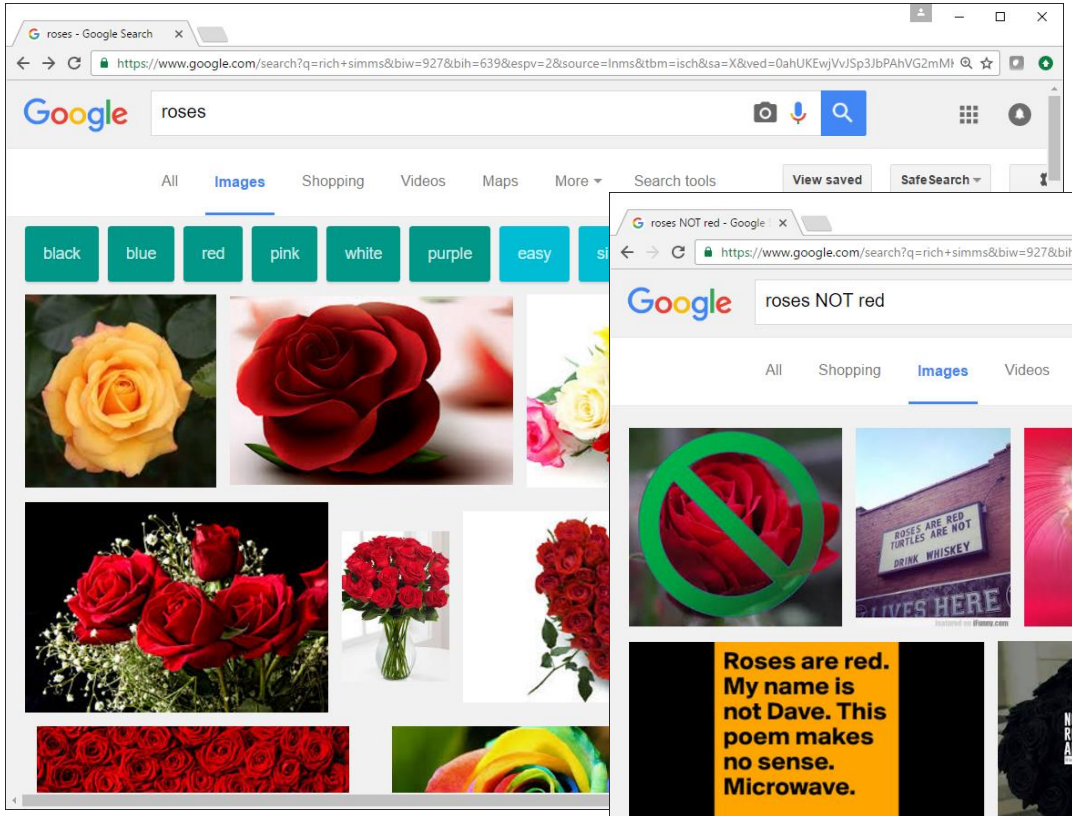
roses OR airplanes



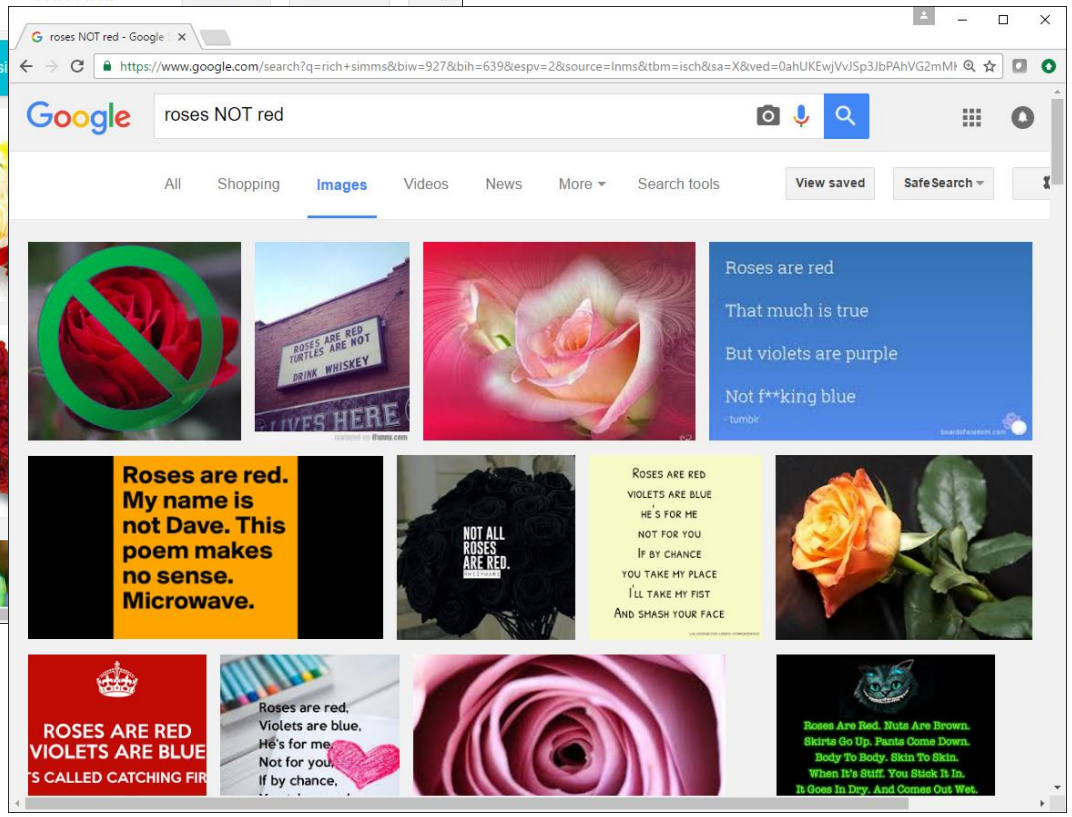
Finds pages with roses or pages with airplanes.

Google Hacking with NOT (or -) operator

roses



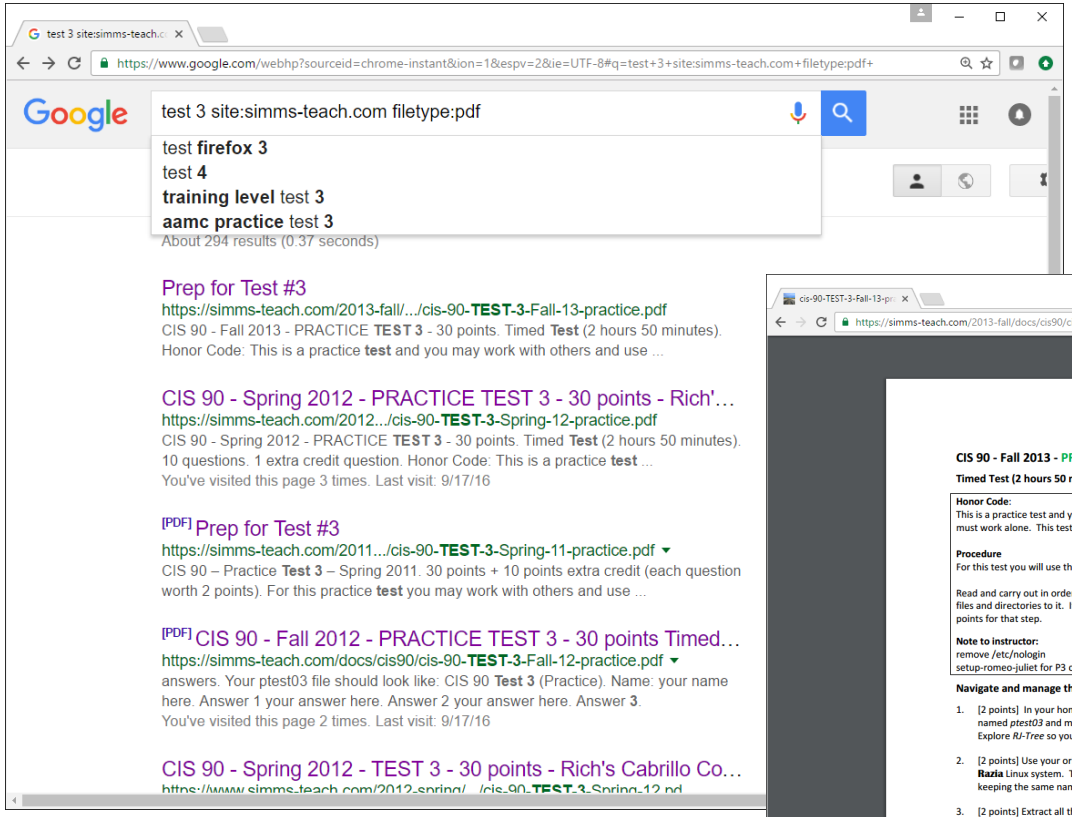
roses NOT red

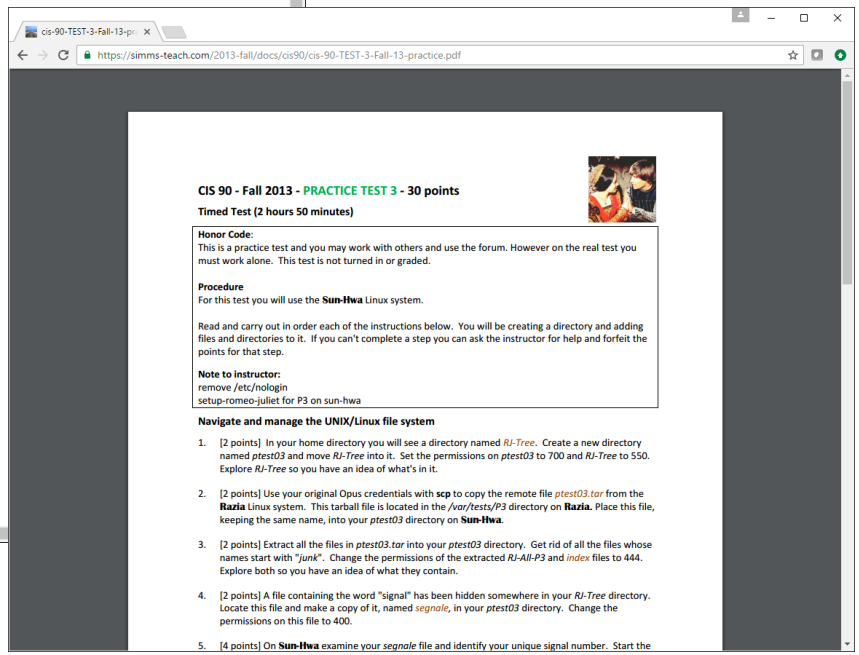


The first finds pages with all kinds of roses, the second weeds out red roses.

Google Hacking with site: and filetype: operators

test 3 site:simms-teach.com filetype:pdf

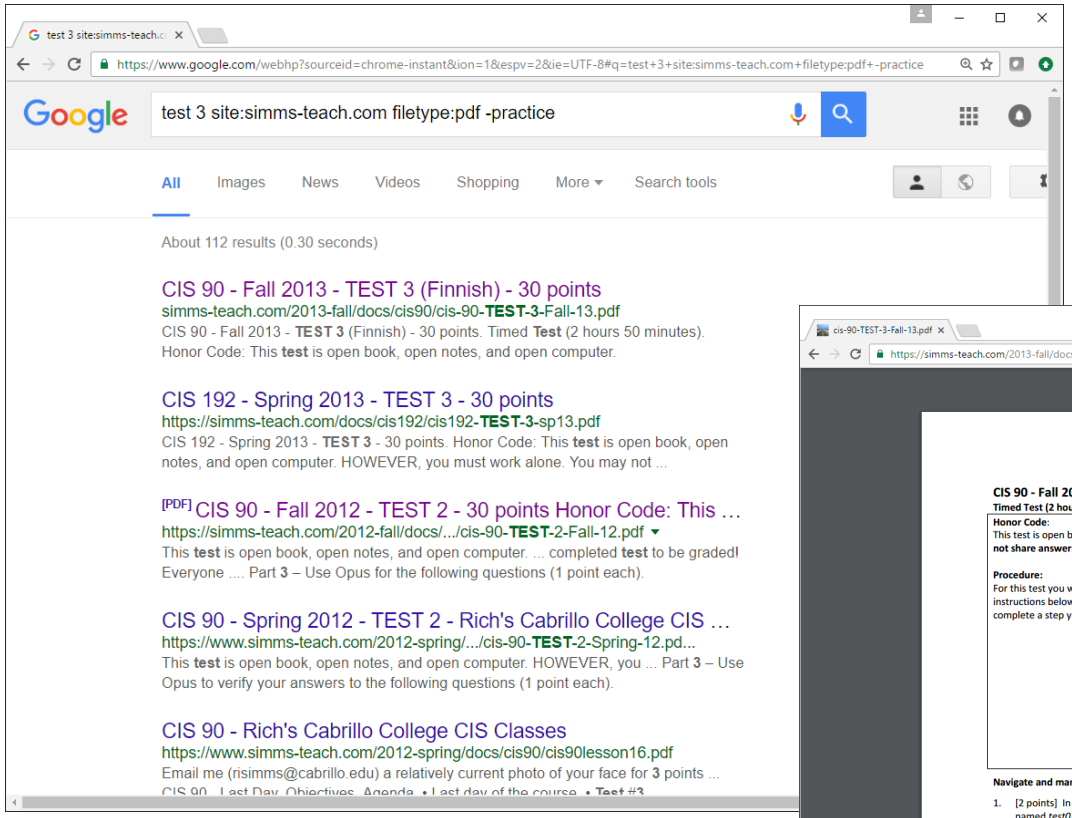


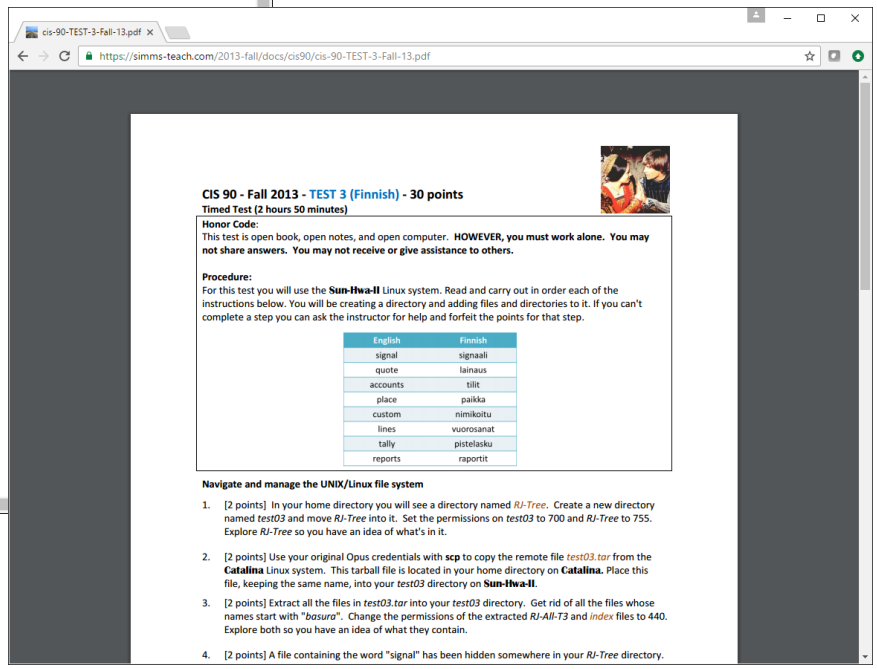


Finds old tests on my website

Google Hacking with site: and filetype: operators

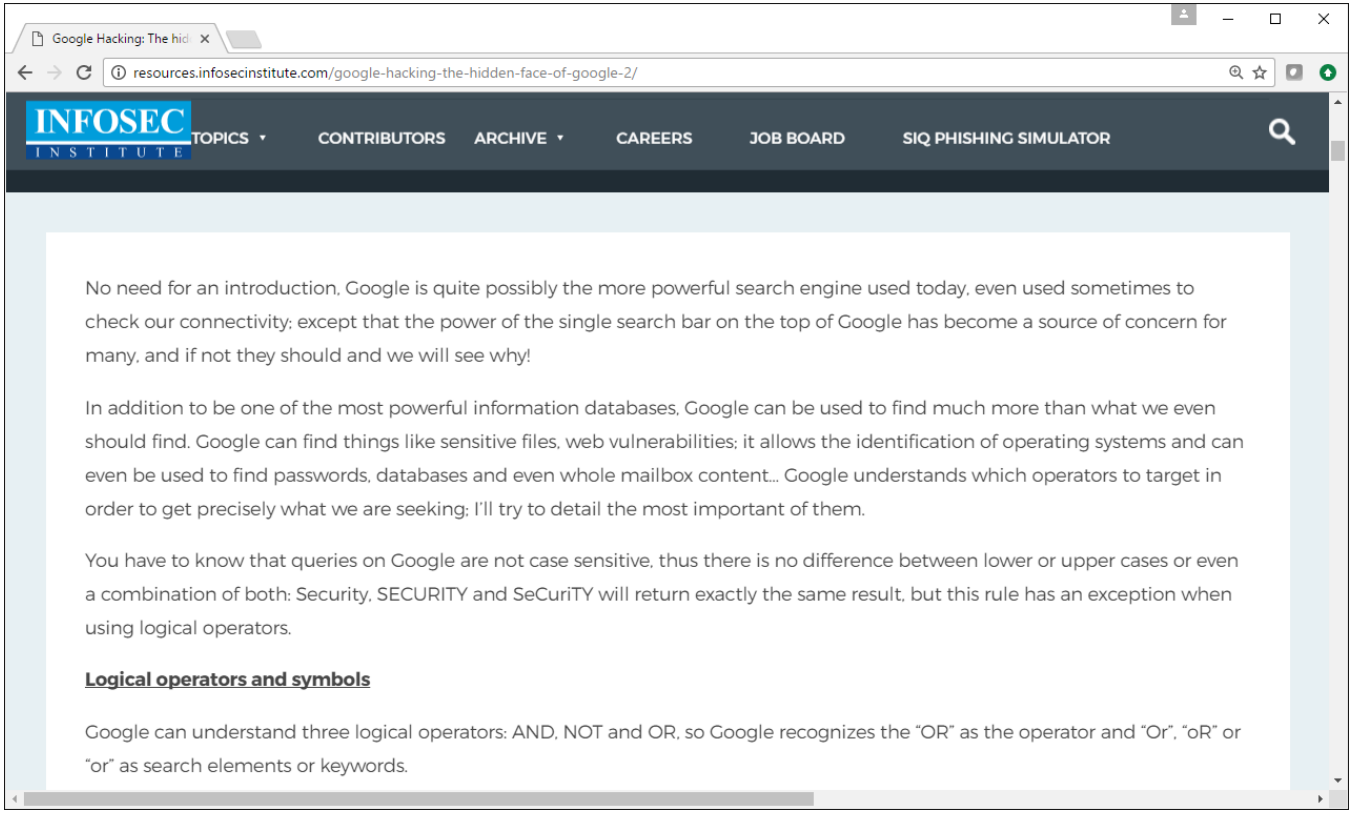
test 3 site:simms-teach.com filetype:pdf -practice





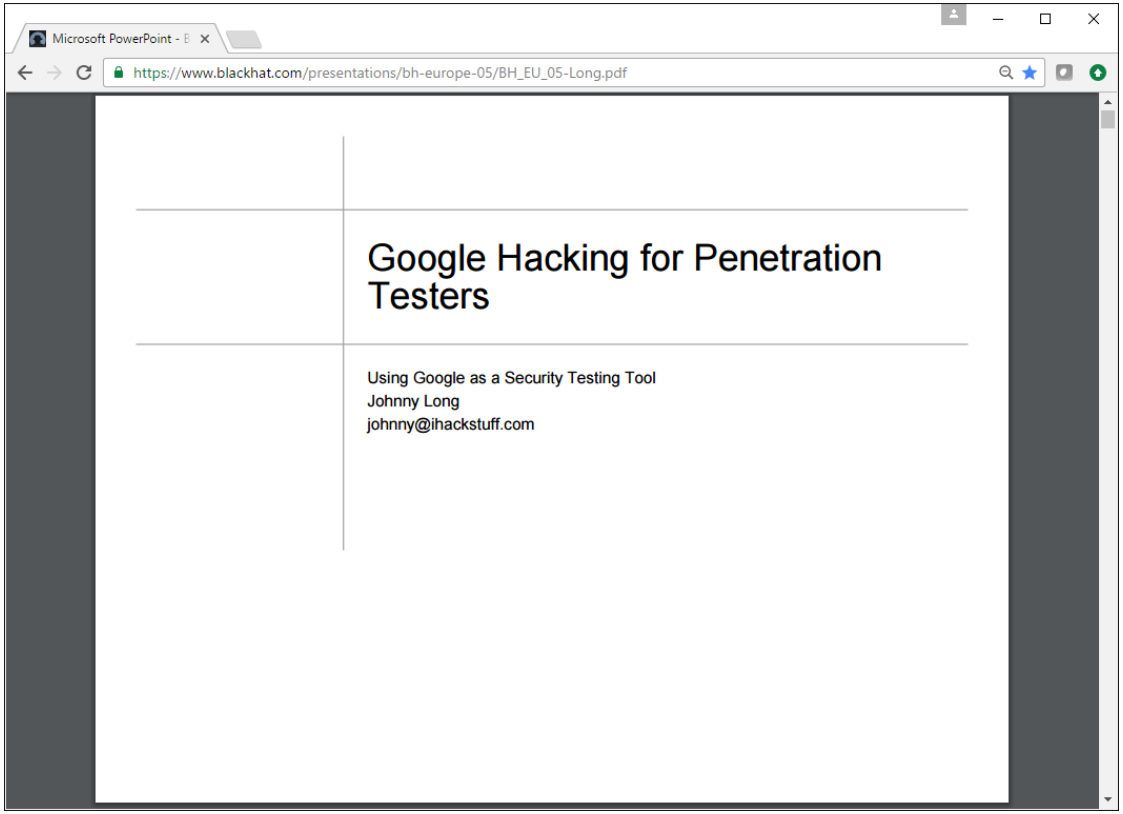
Finds old tests on my website and doesn't include the practice ones

Google Hacking: The hidden face of Google



http://resources.infosecinstitute.com/google-hacking-the-hidden-face-of-google-2/

Google Hacking by Johnny Long



https://www.blackhat.com/presentations/bh-europe-05/BH_EU_05-Long.pdf

Advanced Operators at a Glance

Advanced operators can be combined in some cases.

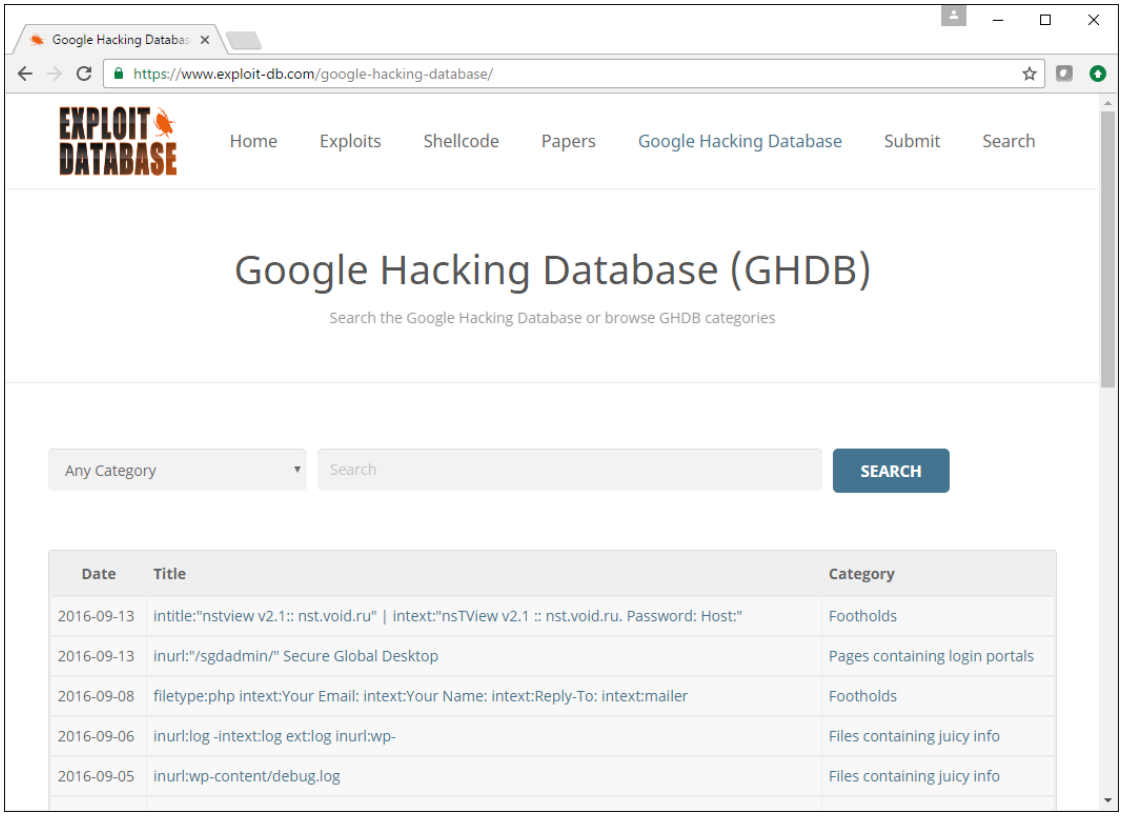
In other cases, mixing should be avoided.

Some operators can only be used to search specific areas of Google, as these columns show.

Operator	Purpose	Mixes with other operators?	Can be used alone?	Does search work in			
				Web	Images	Groups	News
intitle	Search page title	yes	yes	yes	yes	yes	yes
allintitle	Search page title	no	yes	yes	yes	yes	yes
inurl	Search URL	yes	yes	yes	yes	not really	like intitle
allinurl	Search URL	no	yes	yes	yes	yes	like intitle
filetype	Search specific files	yes	no	yes	yes	no	not really
allintext	Search text of page only	not really	yes	yes	yes	yes	yes
site	Search specific site	yes	yes	yes	yes	no	not really
link	Search for links to pages	no	yes	yes	no	no	not really
inanchor	Search link anchor text	yes	yes	yes	yes	not really	yes
numrange	Locate number	yes	yes	yes	no	no	not really
daterange	Search in date range	yes	no	yes	not really	not really	not really
author	Group author search	yes	yes	no	no	yes	not really
group	Group name search	not really	yes	no	no	yes	not really
insubject	Group subject search	yes	yes	like intitle	like intitle	yes	like intitle
msgid	Group msgid search	no	yes	not really	not really	yes	not really

https://www.blackhat.com/presentations/bh-europe-05/BH_EU_05-Long.pdf

Google Hacking On Exploit Database



https://www.exploit-db.com/google-hacking-database/

Google Hacking Database Activity

https://www.exploit-db.com/google-hacking-database/

Pick one of the Google Hacking categories such as:

1. Sensitive directories
2. Network or vulnerability data
3. Various online devices
4. Web server detection
5. Files containing passwords
6. File containing juicy information
7. Or any of the other categories ...

Start exploring.

Put anything you find that is interesting (and not offensive) in the chat window

Social Engineering

Social Engineering

- Manipulating humans to get information or access.
- Fraud, scams and con artists have been around a long time. Way before computers were invented
- Difficult to protect against. Because they take advantage of a false trust their targets have in them.

con man

Back formation of "confidence man". One who gains the trust, or "confidence", of his victims (often called **mark**s) in order to manipulate, steal from, or otherwise predate upon them. (U.S. slang, late 1800s)

Don't write him a check, he's a con man .

http://www.urbandictionary.com/define.php?term=con%20man%20

Social Engineering

Social engineering is easier, faster and far less costly than:

- Researching, reverse-engineering, and exploiting zero-day vulnerabilities.
- Purchasing zero-day exploits on the dark web.
- Conducting time-consuming brute force wordlist or namespace attacks.
- Waiting months for a firewall to be temporarily turned off.
- Doing network vulnerability scans and searching exploit databases to find one that actually works.

Social Engineering

Some examples:

- Spy gear - impersonating a IT staff member then placing a hardware key logger on a sensitive computer.

https://www.keelog.com/

- (Spear) phishing - crafting authentic looking scam emails with malicious links or attachments.
- Vishing - impersonating traveling company VIP calling "their" help desk to urgently get login credentials for an important meeting.
- Shoulder surfing (also with binoculars, telescopes)
- Dumpster diving (waste baskets, trash cans)
- Tailgating (piggybacking)

Social Engineering

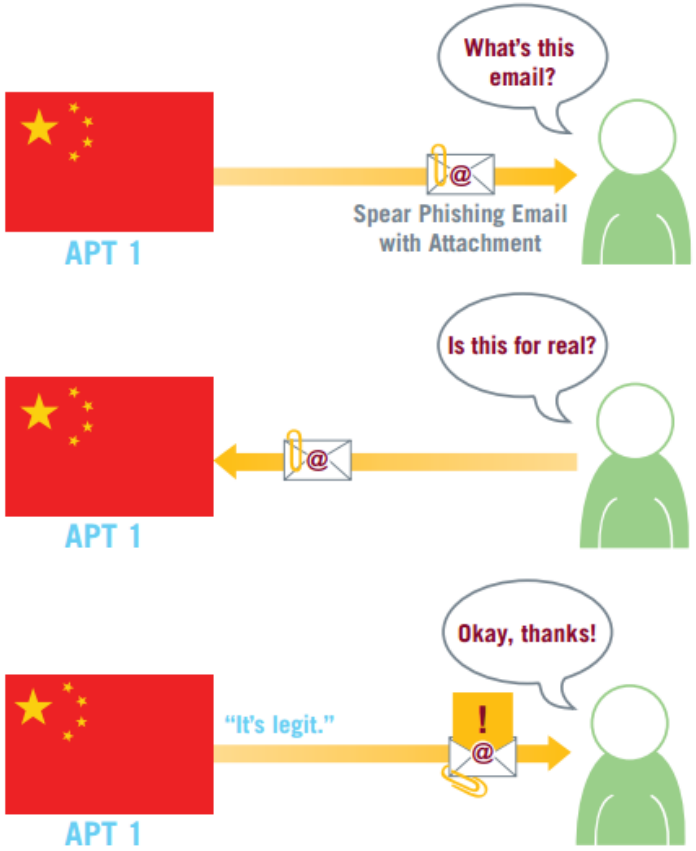
Mandiant sampling of APT1 malicious zip file attachments:

```
2012ChinaUSAviationSymposium.zip
Employee-Benefit-and-Overhead-Adjustment-Keys.zip
MARKET-COMMENT-Europe-Ends-Sharply-Lower-On-Data-Yields-Jump.zip
Negative_Reports_Of_Turkey.zip
New_Technology_For_FPGA_And_Its_Developing_Trend.zip
North_Korean_launch.zip
Oil-Field-Services-Analysis-And-Outlook.zip
POWER_GEN_2012.zip
Proactive_Investors_One2One_Energy_Investor_Forum.zip
Social-Security-Reform.zip
South_China_Sea_Security_Assessment_Report.zip
Telephonics_Supplier_Manual_v3.zip
The_Latest_Syria_Security_Assessment_Report.zip
Updated_Office_Contact_v1.zip
Updated_Office_Contact_v2.zip
Welfare_Reform_and_Benefits_Development_Plan.zip
```

https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Social Engineering

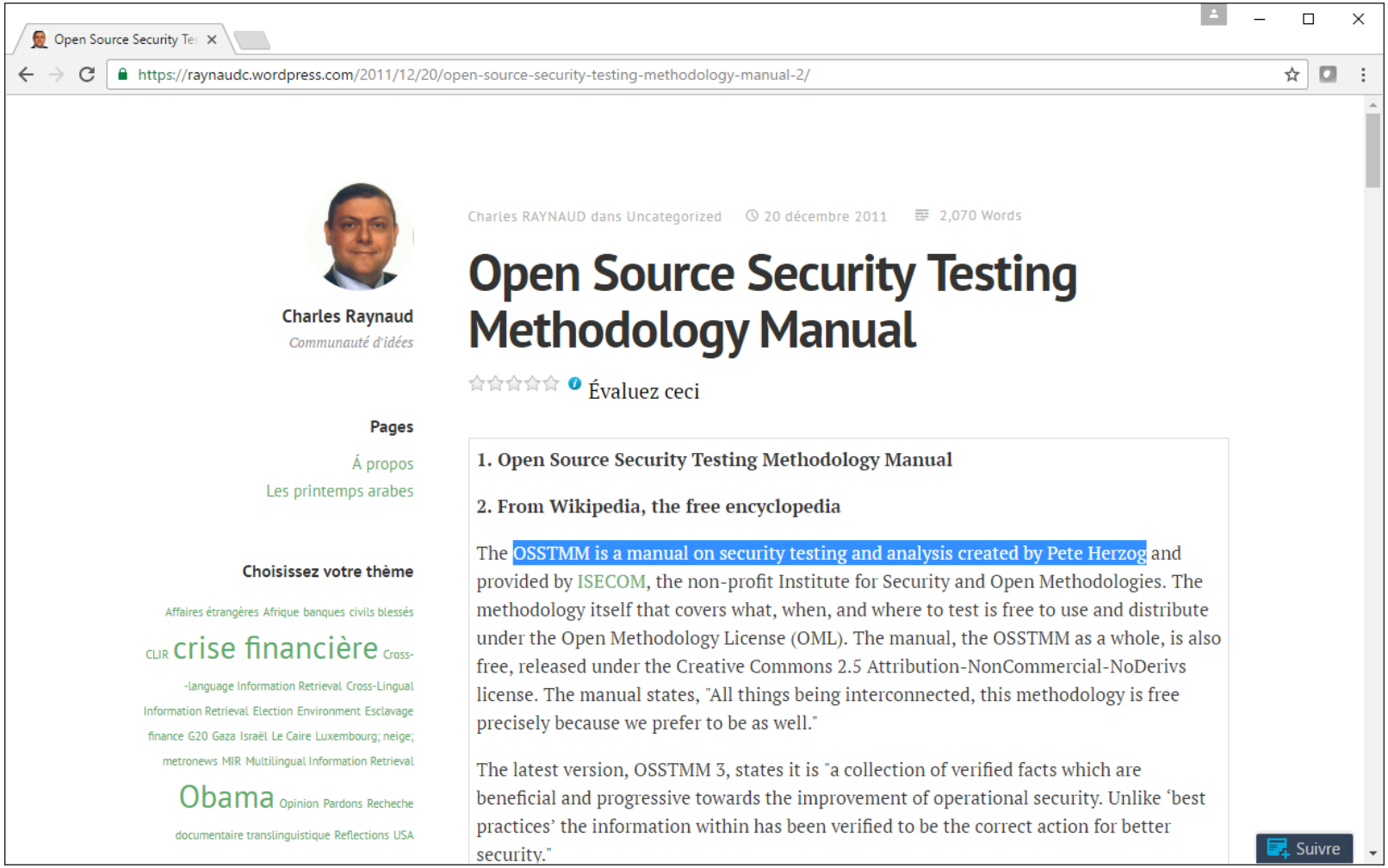
Mandiant APT1 phishing observations:



The example file names include military, economic, and diplomatic themes, suggesting the wide range of industries that APT1 targets. Some names are also generic (e.g., "updated_office_contact_v1.zip") and could be used for targets in any industry. On some occasions, unsuspecting email recipients have replied to the spear phishing messages, believing they were communicating with their acquaintances. In one case a person replied, "I'm not sure if this is legit, so I didn't open it." Within 20 minutes, someone in APT1 responded with a terse email back: "It's legit."

https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Open-Source Security Testing Methodology Manual



https://raynaudc.wordpress.com/2011/12/20/open-source-security-testing-methodology-manual-2/

Open-Source Security Testing Methodology Manual

From our textbook: "As a security tester never use social engineering tactics without written permission from the person that hired you."

Rules of Engagement

...

3. Contracts and Negotiations

...

3.6 The contract must include clear, specific permissions for tests involving survivability failures, denial of service, process testing, or social engineering.

...

7. Testing

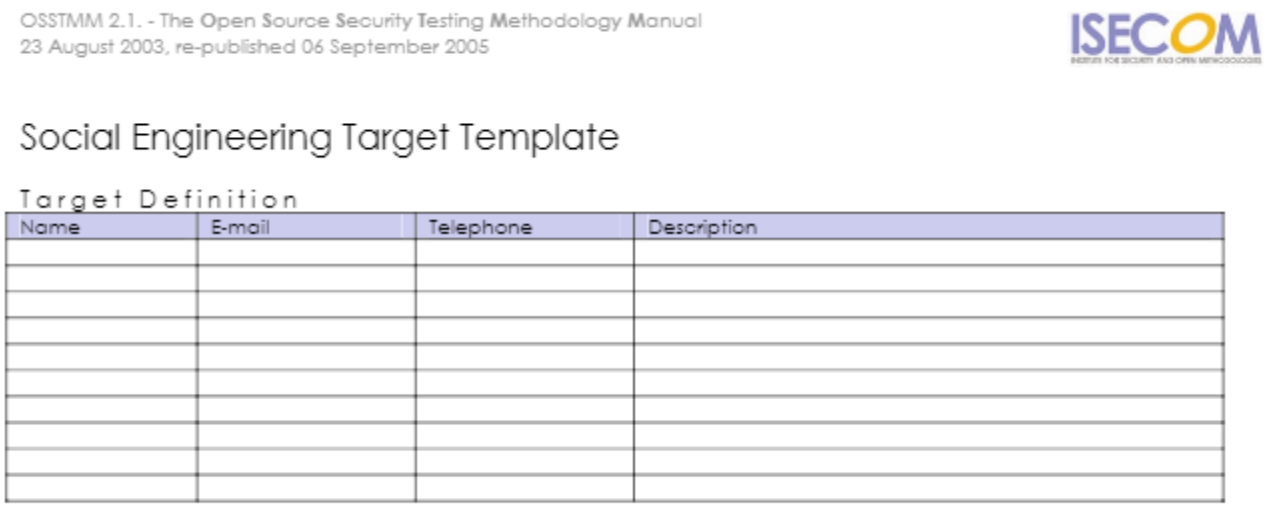
...

7.3 Social engineering and process testing may only be performed in non-identifying statistical means against untrained or non-security personnel.

7.4 Social engineering and process testing may only be performed on personnel identified in the scope and may not include customers, partners, associates, or other external entities.

http://docplayer.net/1016862-Open-source-security-testing-methodology-manual.html

Open-Source Security Testing Methodology Manual



OSSTMM 2.1. - The Open Source Security Testing Methodology Manual
23 August 2003, re-published 06 September 2005

ISECOM

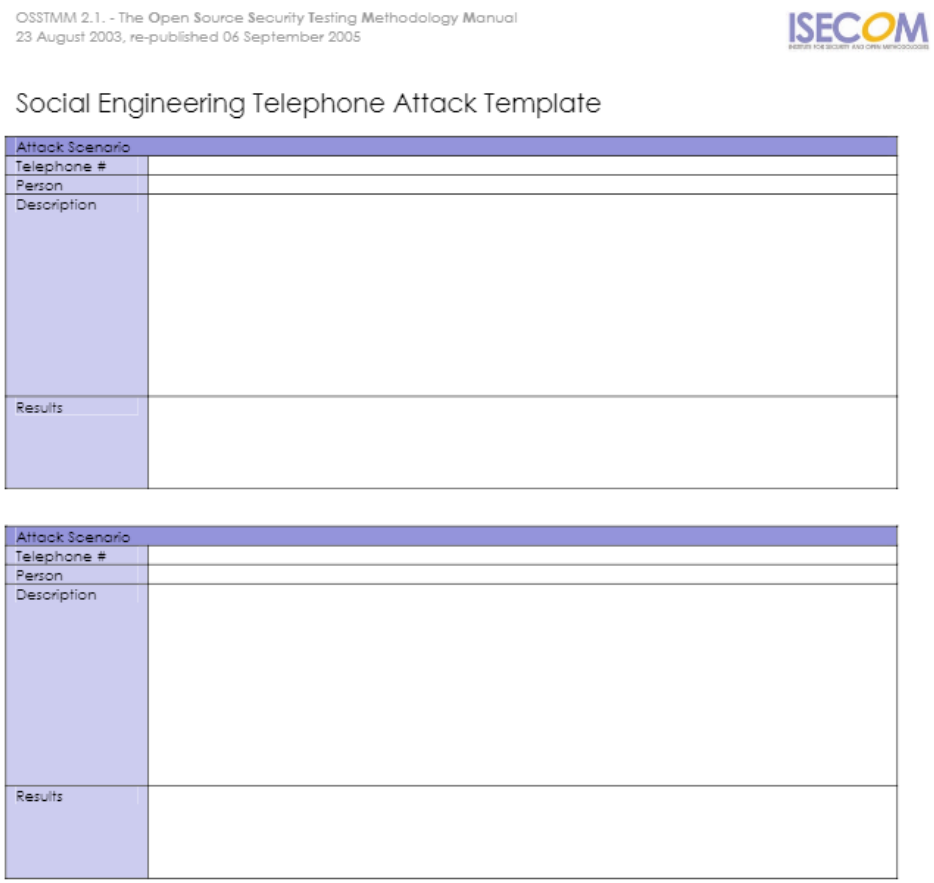
Social Engineering Target Template

Target Definition

Name	E-mail	Telephone	Description

http://docplayer.net/1016862-Open-source-security-testing-methodology-manual.html

Open-Source Security Testing Methodology Manual



OSSTMM 2.1. - The Open Source Security Testing Methodology Manual
23 August 2003, re-published 06 September 2005

ISECOM

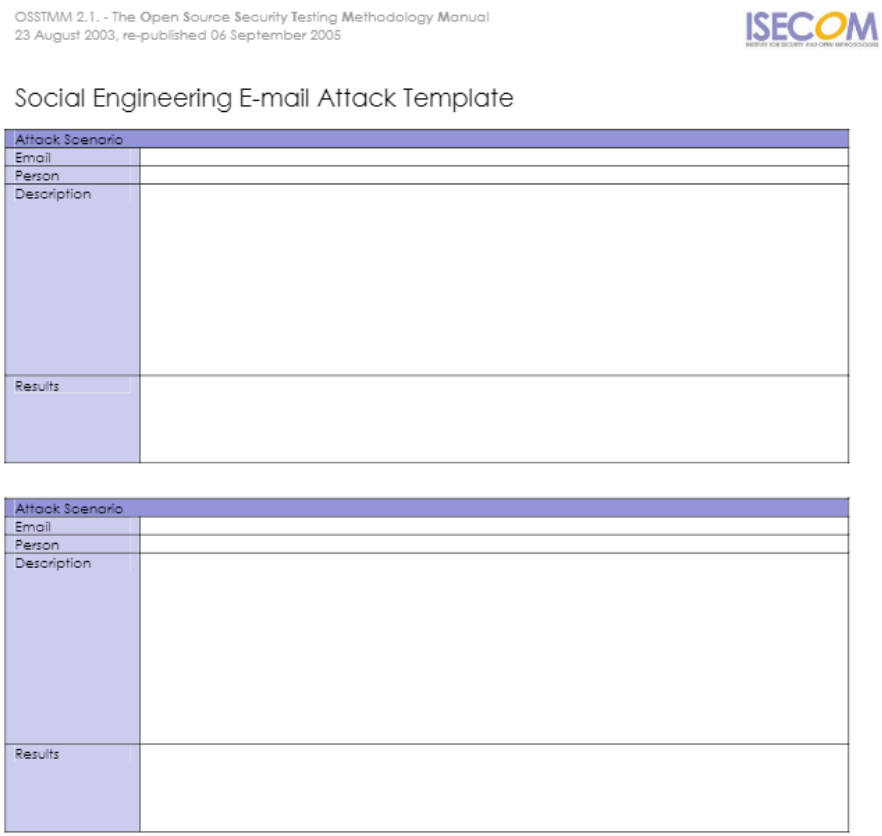
Social Engineering Telephone Attack Template

Attack Scenario	
Telephone #	
Person	
Description	
Results	

Attack Scenario	
Telephone #	
Person	
Description	
Results	

http://docplayer.net/1016862-Open-source-security-testing-methodology-manual.html

Open-Source Security Testing Methodology Manual



OSSTMM 2.1. - The Open Source Security Testing Methodology Manual
23 August 2003, re-published 06 September 2005

ISECOM

Social Engineering E-mail Attack Template

Attack Scenario	
Email	
Person	
Description	
Results	

Attack Scenario	
Email	
Person	
Description	
Results	

http://docplayer.net/1016862-Open-source-security-testing-methodology-manual.html

Open-Source Security Testing Methodology Manual

OSSTMM 2.1. - The Open Source Security Testing Methodology Manual
23 August 2003, re-published 06 September 2005

ISECOM

Social Engineering Template

Company	
Company Name	
Company Address	
Company Telephone	
Company Fax	
Company Webpage	
Products and Services	
Primary Contacts	
Departments and Responsibilities	
Company Facilities Location	
Company History	
Partners	
Resellers	
Company Regulations	
Company Info security Policy	
Company Traditions	
Company Job Postings	
Temporary Employment Availability	
Typical IT threats	

People	
Employee Information	
Employee Names and Positions	
Employee Place in Hierarchy	
Employee Personal Pages	
Employee Best Contact Methods	
Employee Hobbies	
Employee Internet Traces (Usenet, forums)	
Employee Opinions Expressed	
Employee Friends and Relatives	
Employee History (including Work History)	
Employee Character Traits	
Employee Values and Priorities	
Employee Social Habits	
Employee Speech and Speaking Patterns	
Employee Gestures and Manners	

http://docplayer.net/1016862-Open-source-security-testing-methodology-manual.html

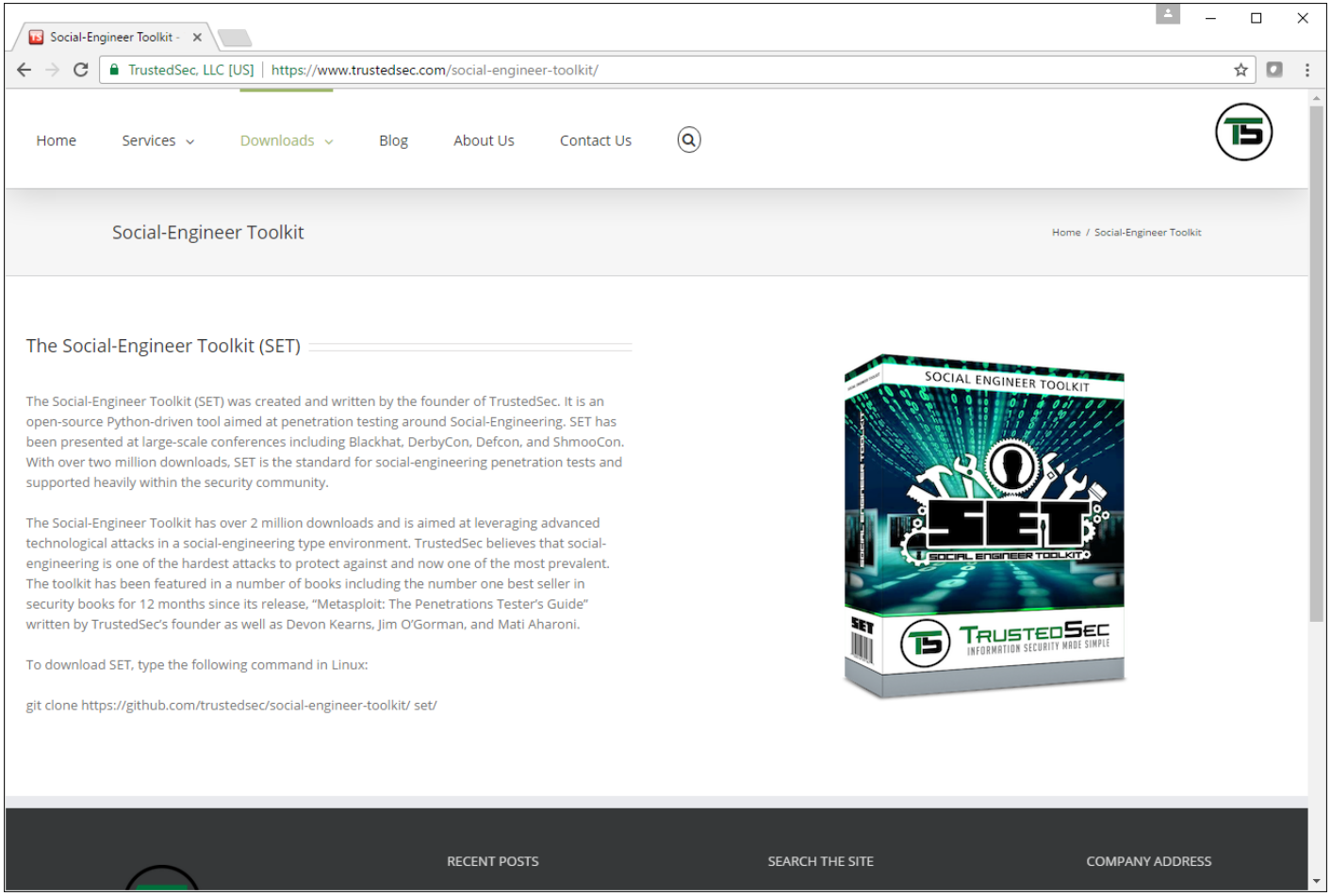
"Katie guest" hack: 3:30 to 9:55
"Help desk" hack: 9:55 to 10:46
Advice: 10:46 to 11:28

"Sales" hack: 11:28 to 12:44
More advice: 12:44 to 13:51

David Kennedy created the Social Engineering Toolkit (SET)

https://www.youtube.com/watch?v=UJdxrhERDyM

Social Engineering Toolkit



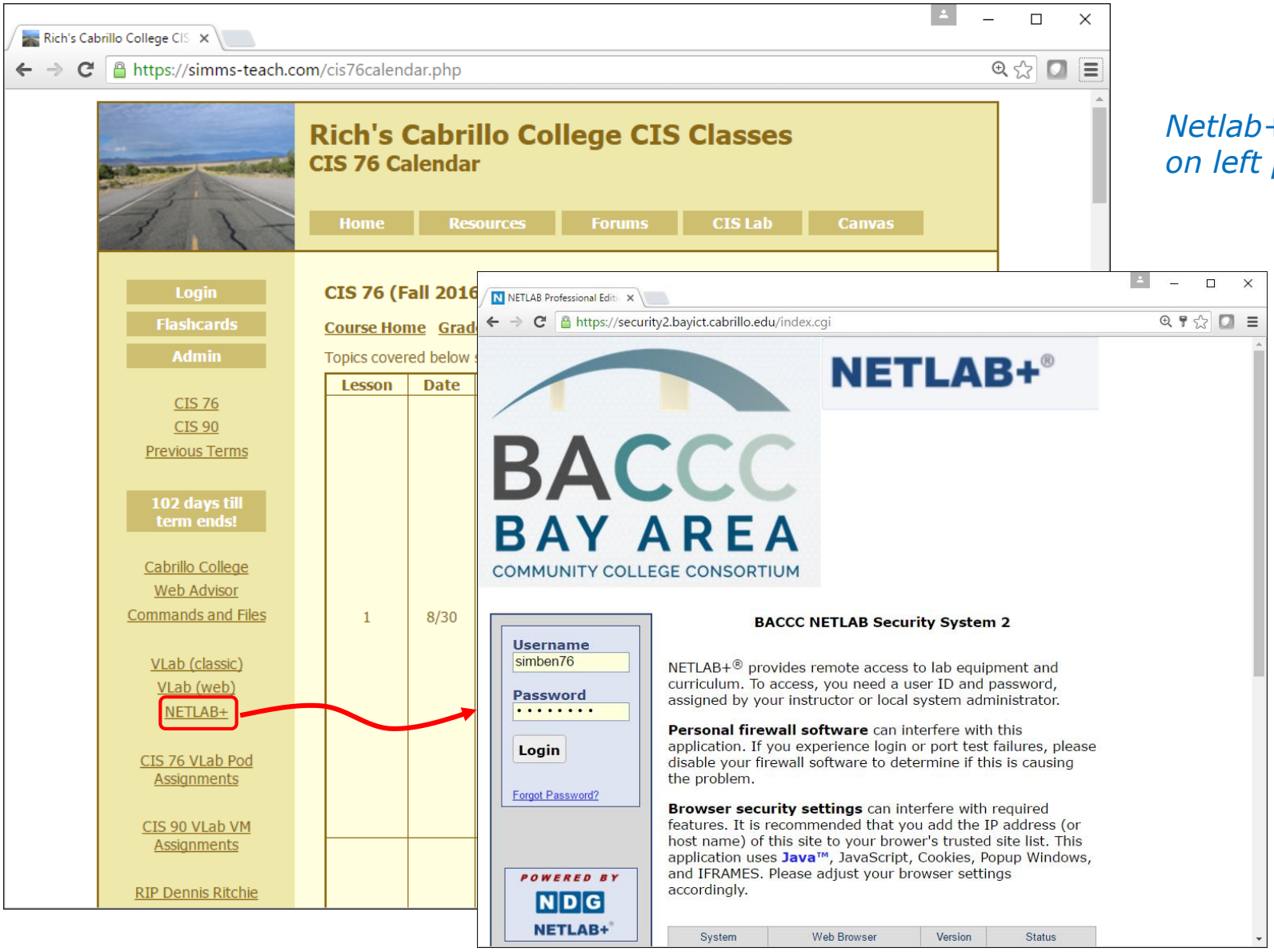
David Kennedy created the Social Engineering Toolkit (SET)

Netlab+ Activity

NDG EH Lab 2

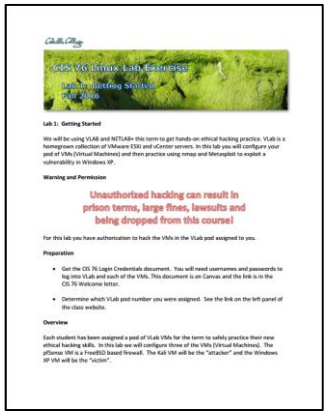
Social Engineering Toolkit


Assignment



Netlab+ link on left panel

Lab Assignments


CIS 76 Linux Lab Exercise

Lab 1: Getting Started

We will be using VLAB and NETLAB+ this term to get hands-on ethical hacking practice. VLab is a homegrown collection of VMware ESXi and vCenter servers. In this lab you will configure your pool of VMs (Virtual Machines) and then practice using nmap and Metasploit to exploit a vulnerability in Windows XP.

Warning and Permission

Unauthorized hacking can result in prison terms, large fines, lawsuits and being dropped from this course!

For this lab you have authorization to hack the VMs in the VLab pool assigned to you.

Preparation

- Get the CIS 76 Login Credentials document. You will need usernames and passwords to log into VLab and each of the VMs. This document is on Canvas and the link is in the CIS 76 Welcome letter.
- Determine which VLab pod number you were assigned. See the link on the left panel of the class website.

Overview

Each student has been assigned a pool of VLab VMs for the term to safely practice their new ethical hacking skills. In this lab we will configure three of the VMs (Virtual Machines). The pfSense VM is a FreeBSD based firewall. The Kali VM will be the "attacker" and the Windows XP VM will be the "victim".

Pearls of Wisdom:

- Don't wait till the last minute to start.
- The *slower* you go the *sooner* you will be finished.
- A few minutes reading the forum can save you hour(s).
- Line up materials, references, equipment, and software ahead of time.
- It's best if you fully understand each step as you do it. Refer back to lesson slides to understand the commands you are using.
- Use Google for trouble-shooting and looking up supplemental info.
- Keep a growing cheat sheet of commands and examples.
- Study groups are very productive and beneficial.
- Use the forum to collaborate, ask questions, get clarifications, and share tips you learned while doing a lab.
- Plan for things to go wrong and give yourself time to ask questions and get answers.
- Late work is not accepted so submit what you have for partial credit.


Wrap up

Next Class

Assignment: Check the Calendar Page on the web site to see what is due next week.

Lab 4

Quiz questions for next class:

- Use telnet to check the headers on the umich.edu web server. What is the value of the X-Powered-By header?
- What city and country is the IPv4 address 61.180.150.240 associated with?
- What is the name of the person who authored the SET (Social Engineering Toolkit)?

Backup