Last updated 9/20/2016

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

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

CIS 76
Ethical Hacking

TCP/IP

Network and Computer Attacks

Footprinting and Social Engineering

Port Scanning

Enumeration

Scripting and Programming

Desktop and Server Vulnerabilities

Embedded Operating Systems

Hacking Web Servers

Hacking Wireless Networks

Cryptography

Evading Network Devices

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

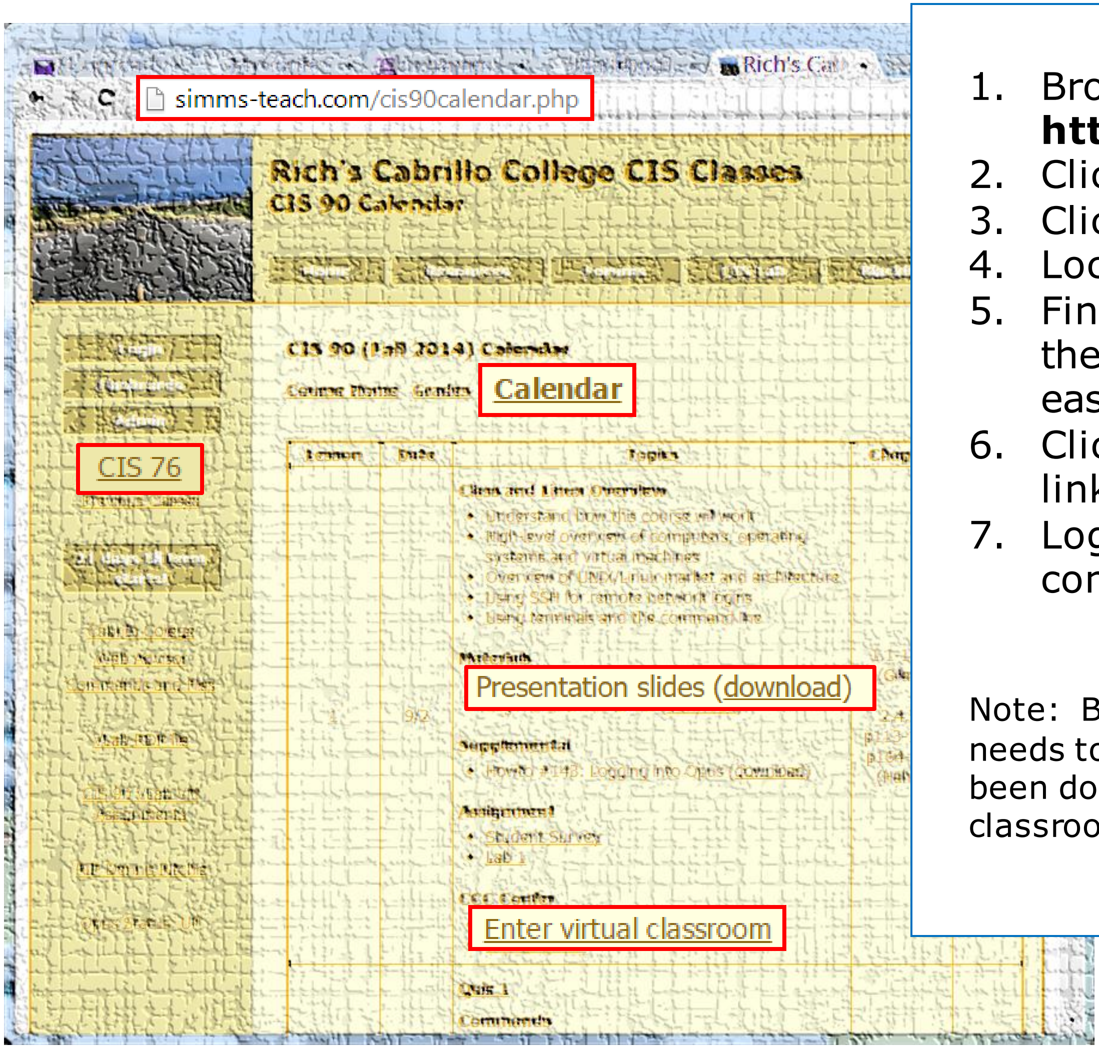
Rich Simms

- 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


simms-teach.com/cis90calendar.php
Rich's Cabrillo College CIS Classes
CIS 90 Calendar
Calendar
CIS 76
Presentation slides (download)
Enter virtual classroom

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 with Putty or ssh command.

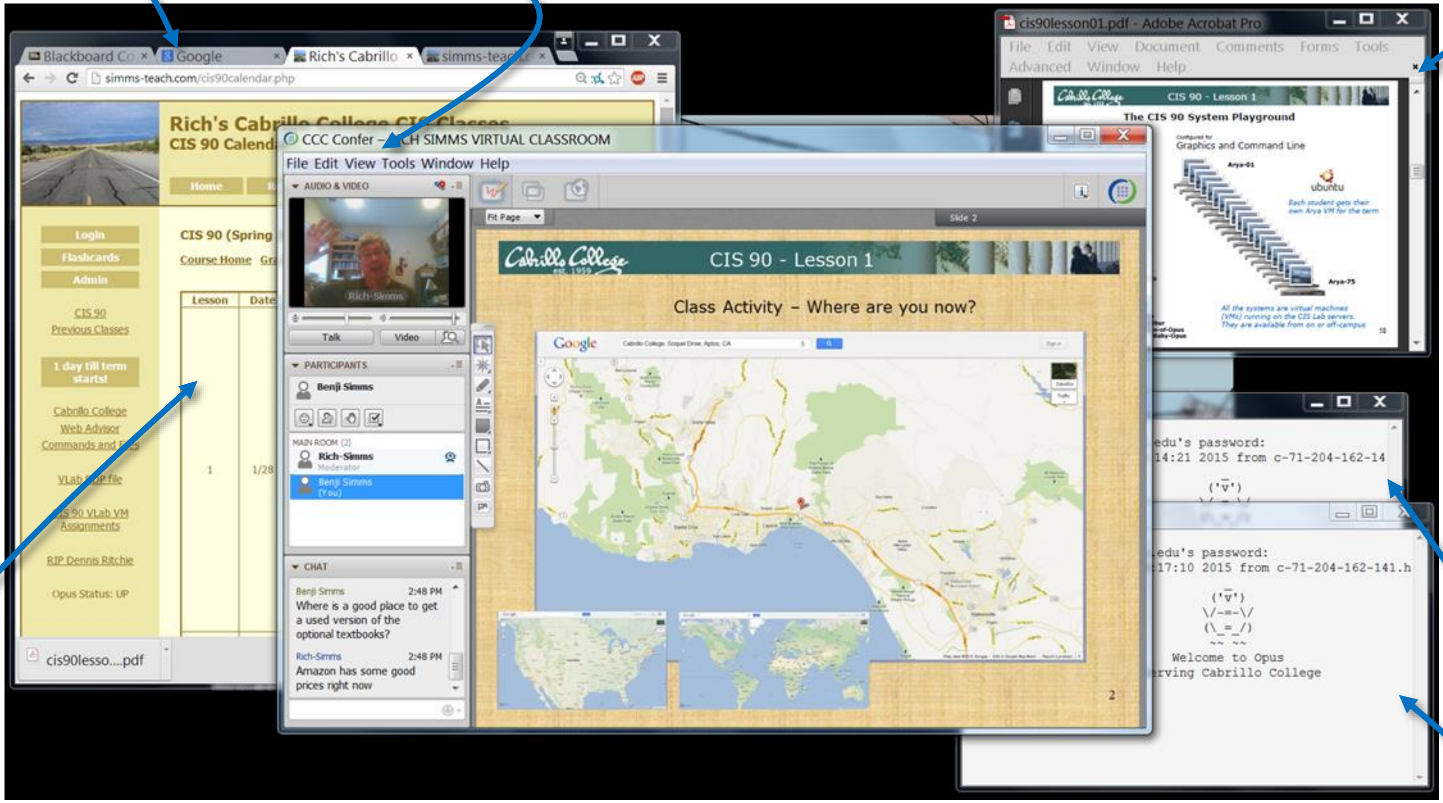
Note: Blackboard Collaborate Launcher only needs to be installed once. It has already been downloaded and installed on the classroom PC's.

Student checklist for suggested screen layout

❑ *Google*

❑ *CCC Confer*

❑ *Downloaded PDF of Lesson Slides*


Blackboard Co
Google
Rich's Cabrillo
simms-teach
simms-teach.com/cis90calendar.php
Rich's Cabrillo College CIS Classes
CIS 90 Calend
Home
Login
Flashcards
Admin
CIS 90
Previous Classes
1 day till term starts!
Cabrillo College
Web Advisor
Commands and Files
VLab RDP file
CIS 90 VLab VM Assignments
RIP Dennis Ritchie
Opus Status: UP
CIS 90 (Spring
Course Home
Lesson
Date
1
1/28
cis90lesso....pdf
CCC Confer – RICH SIMMS VIRTUAL CLASSROOM
File Edit View Tools Window Help
AUDIO & VIDEO
Rich-Simms
Talk
Video
PARTICIPANTS
Benji Simms
MAIN ROOM (2)
Rich-Simms
Moderator
Benji Simms (You)
CHAT
Fit Page
Slide 2
CIS 90 - Lesson 1
Class Activity – Where are you now?
Google
2
cis90lesson01.pdf - Adobe Acrobat Pro
File Edit View Document Comments Forms Tools Advanced Window Help
CIS 90 - Lesson 1
The CIS 90 System Playground
Graphics and Command Line
Arya-01
ubuntu
Each student gets their own Arya VM for the term
Arya-75
All the systems are virtual machines (VMs) running on the CIS Lab servers. They are available from on or off-campus

Benji Simms 2:48 PM
Where is a good place to get a used version of the optional textbooks?

Rich-Simms 2:48 PM
Amazon has some good prices right now

```
edu's password:
14:21 2015 from c-71-204-162-14
  ('v')
```

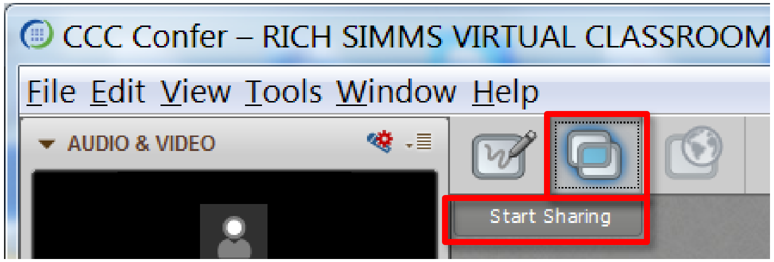
```
edu's password:
17:10 2015 from c-71-204-162-141.h
  ('v')
 \/-=-\/
 (\_=_/)
  ~~ ~~
 Welcome to Opus
erving Cabrillo College
```

❑ *CIS 76 website Calendar page*

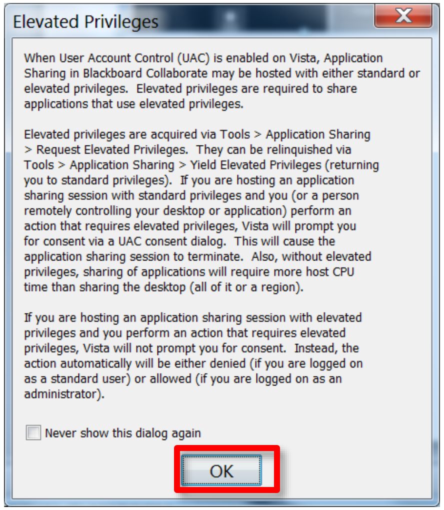
❑ *One or more login sessions to Opus*

Student checklist for sharing desktop with classmates

1) Instructor gives you sharing privileges.


CCC Confer – RICH SIMMS VIRTUAL CLASSROOM
File Edit View Tools Window Help
AUDIO & VIDEO
Start Sharing

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



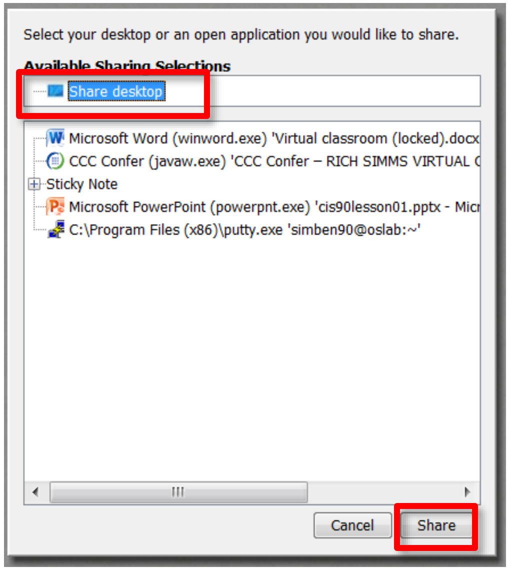
When User Account Control (UAC) is enabled on Vista, Application Sharing in Blackboard Collaborate may be hosted with either standard or elevated privileges. Elevated privileges are required to share applications that use elevated privileges.

Elevated privileges are acquired via Tools > Application Sharing > Request Elevated Privileges. They can be relinquished via Tools > Application Sharing > Yield Elevated Privileges (returning you to standard privileges). If you are hosting an application sharing session with standard privileges and you (or a person remotely controlling your desktop or application) perform an action that requires elevated privileges, Vista will prompt you for consent via a UAC consent dialog. This will cause the application sharing session to terminate. Also, without elevated privileges, sharing of applications will require more host CPU time than sharing the desktop (all of it or a region).

If you are hosting an application sharing session with elevated privileges and you perform an action that requires elevated privileges, Vista will not prompt you for consent. Instead, the action automatically will be either denied (if you are logged on as a standard user) or allowed (if you are logged on as an administrator).

☐ Never show this dialog again

3) Click OK button.



Select your desktop or an open application you would like to share.

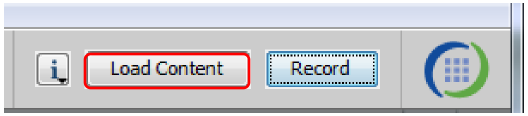
Available Sharing Selections

- Share desktop
- Microsoft Word (winword.exe) 'Virtual classroom (locked).docx
- CCC Confer (javaw.exe) 'CCC Confer – RICH SIMMS VIRTUAL C
- Sticky Note
- Microsoft PowerPoint (powerpnt.exe) 'cis90lesson01.pptx - Micr
- C:\Program Files (x86)\putty.exe 'simben90@oslab:~'

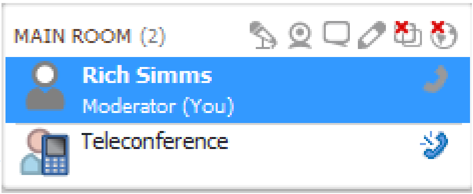
4) Select "Share desktop" and click Share button.

Rich's CCC Confer checklist - setup

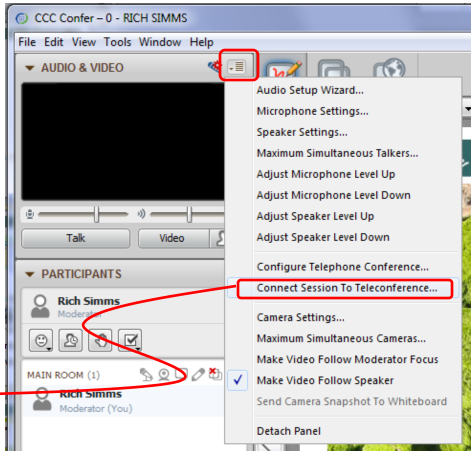
[ ] Preload White Board



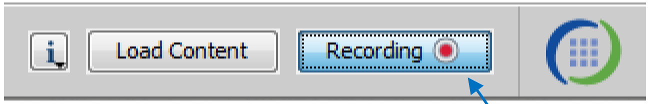
[ ] Connect session to Teleconference



Session now connected to teleconference


CCC Confer – 0 - RICH SIMMS
File Edit View Tools Window Help
AUDIO & VIDEO
Talk
Video
PARTICIPANTS
Rich Simms
Moderator
MAIN ROOM (1)
Rich Simms
Moderator (You)
Audio Setup Wizard...
Microphone Settings...
Speaker Settings...
Maximum Simultaneous Talkers...
Adjust Microphone Level Up
Adjust Microphone Level Down
Adjust Speaker Level Up
Adjust Speaker Level Down
Configure Telephone Conference...
Connect Session To Teleconference...
Camera Settings...
Maximum Simultaneous Cameras...
Make Video Follow Moderator Focus
✓ Make Video Follow Speaker
Send Camera Snapshot To Whiteboard
Detach Panel

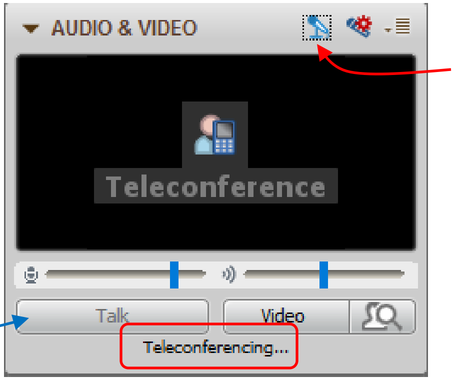
[ ] Is recording on?



Red dot means recording

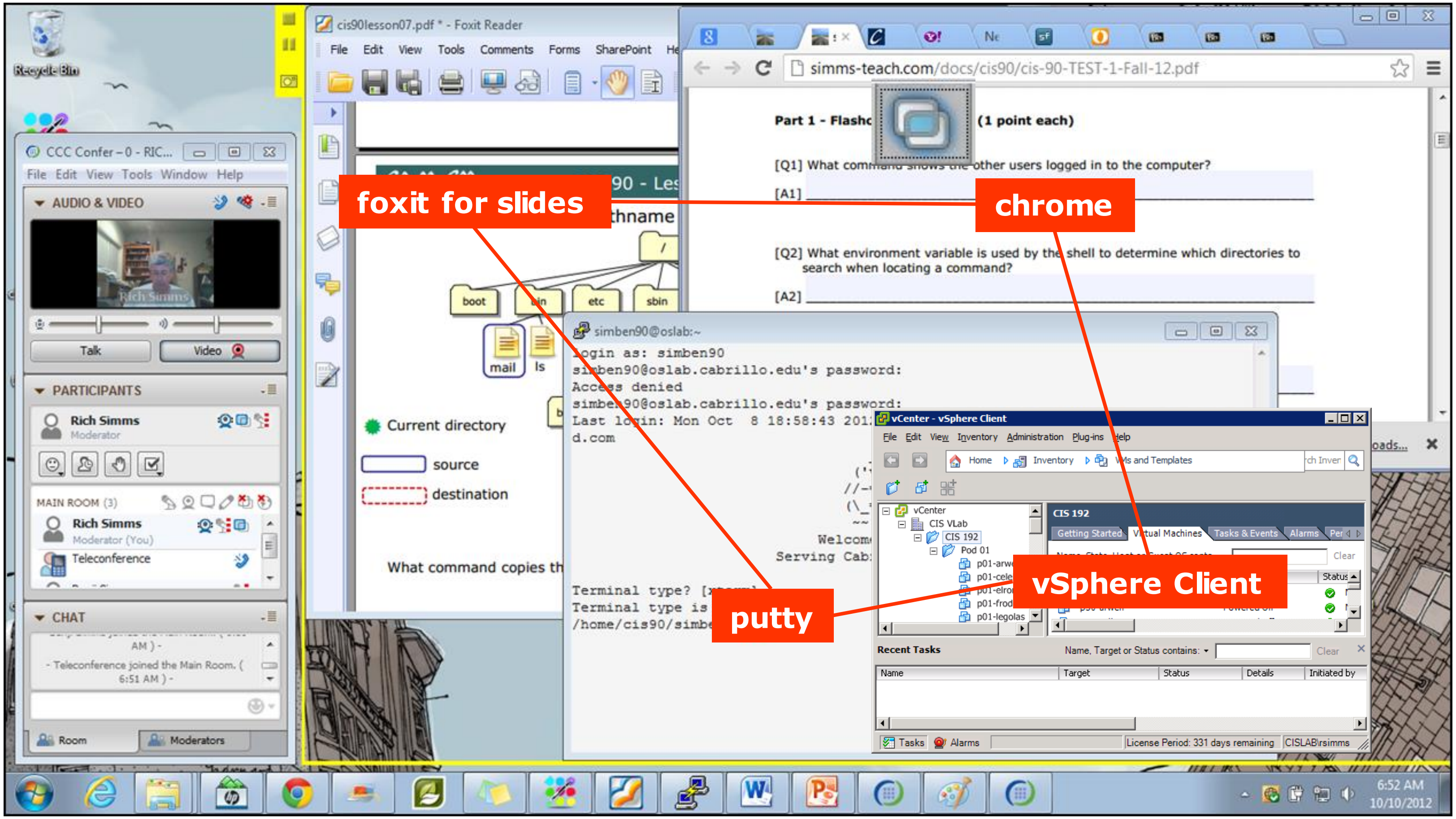
[ ] Use teleconferencing, not mic

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



foxit for slides

chrome

putty

vSphere Client

cis90lesson07.pdf * - Foxit Reader

Current directory

source

destination

What command copies th

simms-teach.com/docs/cis90/cis-90-TEST-1-Fall-12.pdf

Part 1 - Flashc (1 point each)

[Q1] What command shows the other users logged in to the computer?

[A1] ____________________

[Q2] What environment variable is used by the shell to determine which directories to search when locating a command?

[A2] ____________________

simben90@oslab:~

```
login as: simben90
simben90@oslab.cabrillo.edu's password:
Access denied
simben90@oslab.cabrillo.edu's password:
Last login: Mon Oct  8 18:58:43 201
d.com

                              Welcom
                            Serving Cab

Terminal type? [xterm]
Terminal type is
/home/cis90/simbe
```

CCC Confer – 0 - RIC...

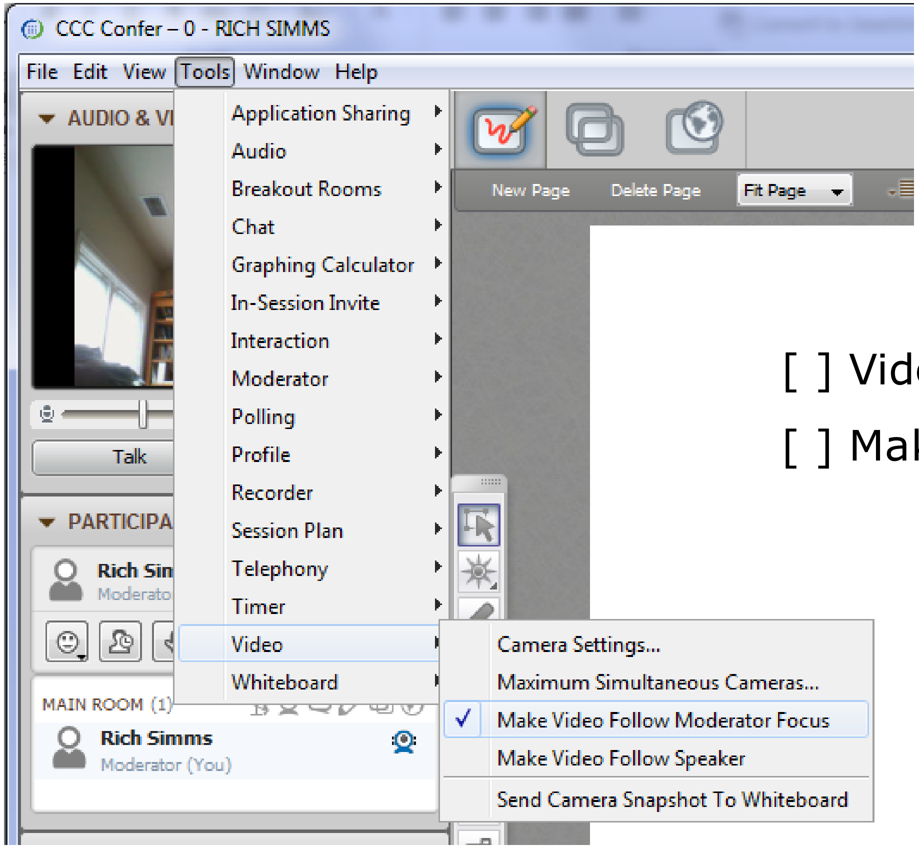
- Teleconference joined the Main Room. (6:51 AM) -

vCenter - vSphere Client

License Period: 331 days remaining CISLAB\rsimms

[ ] layout and share apps

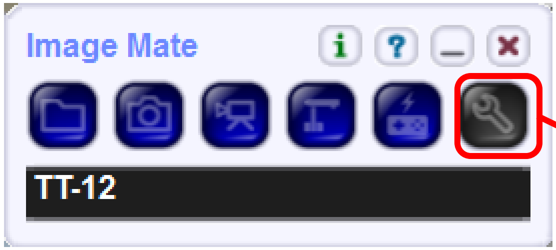
Rich's CCC Confer checklist - webcam setup

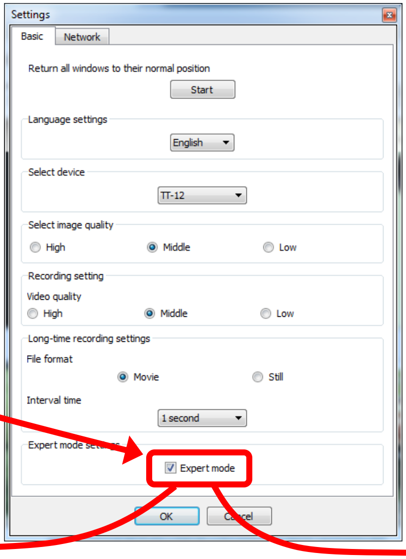


[ ] Video (webcam)

[ ] Make Video Follow Moderator Focus

Rich's CCC Confer checklist - Elmo




Settings

Basic | Network

Return all windows to their normal position

Start

Language settings: English

Select device: TT-12

Select image quality: ○ High ● Middle ○ Low

Recording setting

Video quality: ○ High ● Middle ○ Low

Long-time recording settings

File format: ● Movie ○ Still

Interval time: 1 second

Expert mode settings

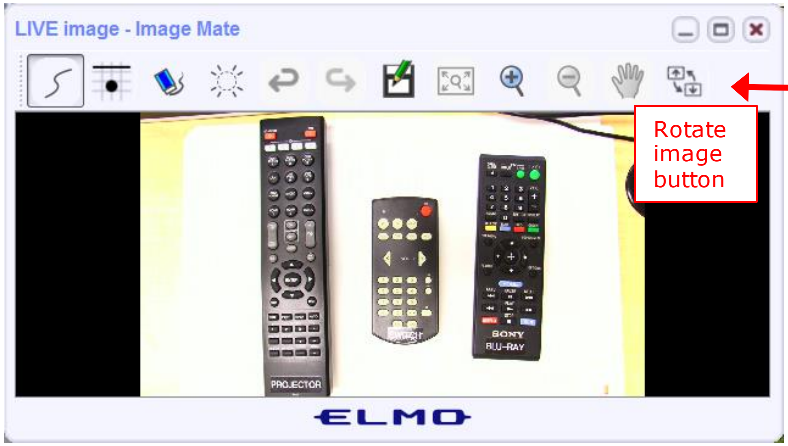
☑ Expert mode

OK | Cancel

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

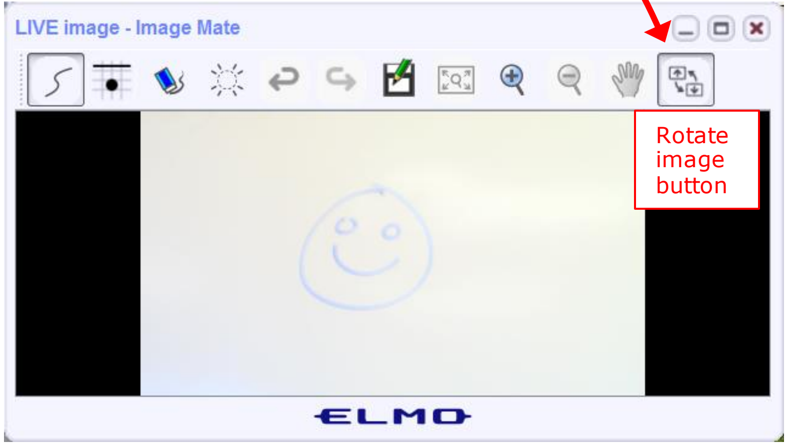
Quite interesting that they consider you to be an "expert" in order to use this button!

Elmo rotated down to view side table



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

Elmo rotated up to view white board

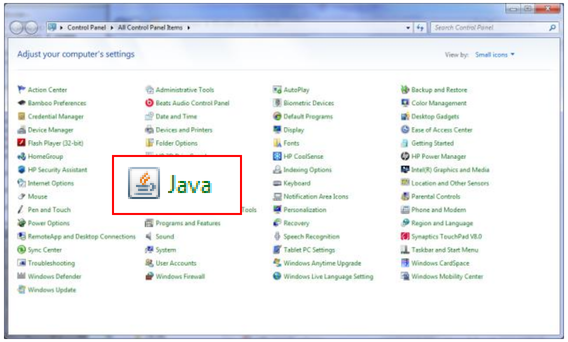


Rich's CCC Confer checklist - universal fixes

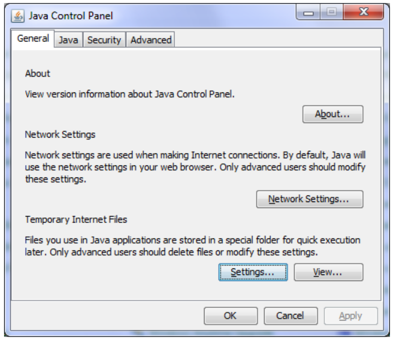
Universal Fix for CCC Confer:

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...


Java Control Panel

General | Java | Security | Advanced

About

View version information about Java Control Panel.

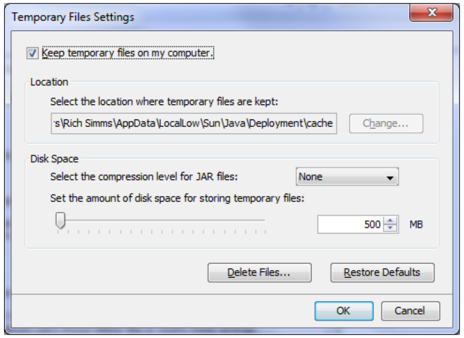
Network Settings

Network settings are used when making Internet connections. By default, Java will use the network settings in your web browser. Only advanced users should modify these settings.

Temporary Internet Files

Files you use in Java applications are stored in a special folder for quick execution later. Only advanced users should delete files or modify these settings.

500MB cache size


Temporary Files Settings

☑ Keep temporary files on my computer.

Location

Select the location where temporary files are kept:

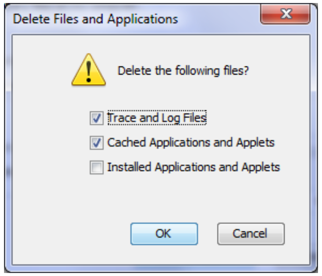
s\Rich Simms\AppData\LocalLow\Sun\Java\Deployment\cache

Disk Space

Select the compression level for JAR files: None

Set the amount of disk space for storing temporary files: 500 MB

Delete these


Delete Files and Applications

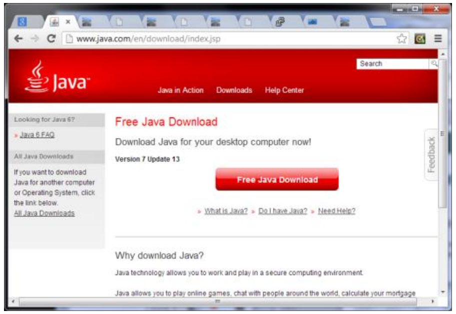
Delete the following files?

☑ Trace and Log Files

☑ Cached Applications and Applets

☐ Installed Applications and Applets

Google Java download


www.java.com/en/download/index.jsp

Free Java Download

Download Java for your desktop computer now!

Version 7 Update 13

Looking for Java 6?

» Java 6 FAQ

All Java Downloads

If you want to download Java for another computer or Operating System, click the link below.

All Java Downloads

Why download Java?

Java technology allows you to work and play in a secure computing environment.

Java allows you to play online games, chat with people around the world, calculate your mortgage

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.*

CIS 76 - Lesson 4

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

Ryan

Jordan

Takashi

Karl-Heinz

Sean

Benji

Joshua

Brian

Tess

Jeremy

David H.

Roberto

Nelli

Mike C.

Deryck

Alex

Michael W.

Carter

Thomas

Wes

Jennifer

Marcos

Tim

Luis

Dave R.

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	Agenda
• 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.	• 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

How this course works?

Past lesson material?

Previous labs?

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.*

Housekeeping

war is not healthy for children and other living things
ICE COLD
Coffee!
You can sleep when you're dead!
LATTE
TOURIST MAP OF THE WORLD
New Z
Sports Blaster
We're Proud To Serv

Housekeeping

1. Send me your student survey & agreement if you haven't already.

2. Lab 3 due by 11:59PM (Opus time) tonight.

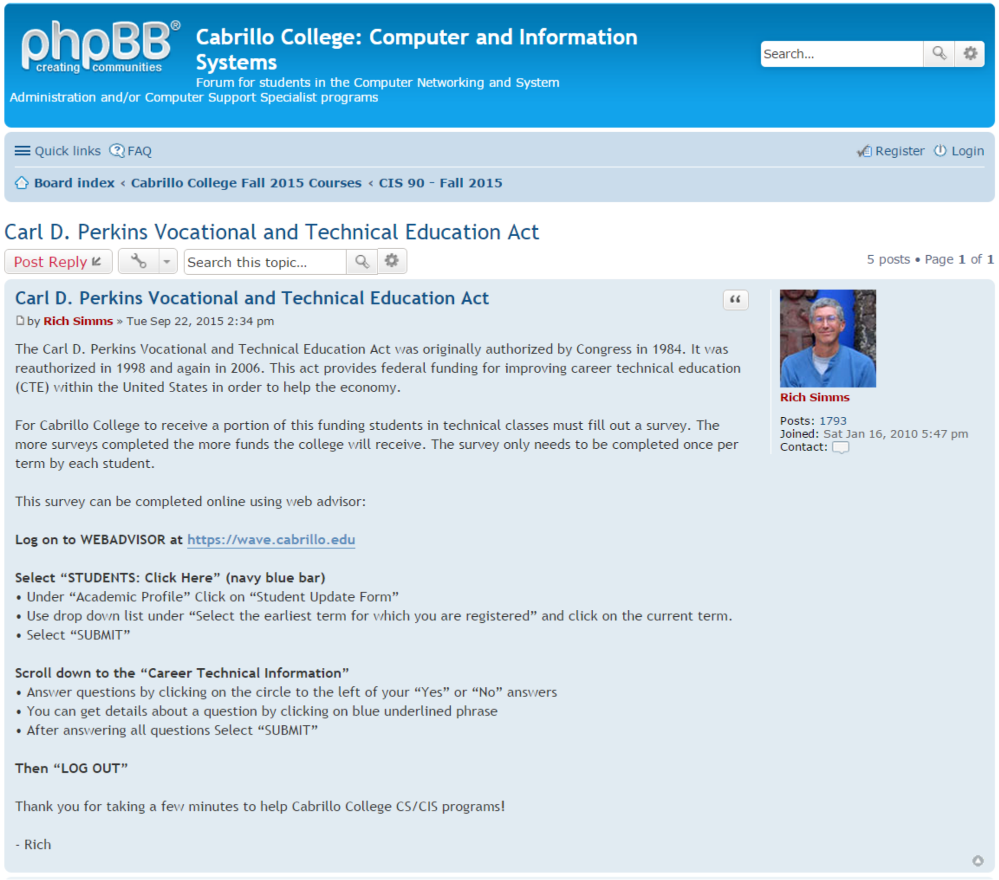
3. Graded labs are placed in your home directory on Opus.

4. Answers to the quizzes are in /home/cis76/answers on Opus.

5. Grades from last week posted on the website.

6. When I get your survey/agreement I will send you your grading codename.

Perkins/VTEA Survey



Cabrillo College: Computer and Information Systems

Forum for students in the Computer Networking and System Administration and/or Computer Support Specialist programs

Board index ‹ Cabrillo College Fall 2015 Courses ‹ CIS 90 - Fall 2015

Carl D. Perkins Vocational and Technical Education Act

5 posts • Page **1** of **1**

Carl D. Perkins Vocational and Technical Education Act

by **Rich Simms** » Tue Sep 22, 2015 2:34 pm

The Carl D. Perkins Vocational and Technical Education Act was originally authorized by Congress in 1984. It was reauthorized in 1998 and again in 2006. This act provides federal funding for improving career technical education (CTE) within the United States in order to help the economy.

For Cabrillo College to receive a portion of this funding students in technical classes must fill out a survey. The more surveys completed the more funds the college will receive. The survey only needs to be completed once per term by each student.

This survey can be completed online using web advisor:

Log on to WEBADVISOR at https://wave.cabrillo.edu

Select "STUDENTS: Click Here" (navy blue bar)
- Under "Academic Profile" Click on "Student Update Form"
- Use drop down list under "Select the earliest term for which you are registered" and click on the current term.
- Select "SUBMIT"

Scroll down to the "Career Technical Information"
- Answer questions by clicking on the circle to the left of your "Yes" or "No" answers
- You can get details about a question by clicking on blue underlined phrase
- After answering all questions Select "SUBMIT"

Then "LOG OUT"

Thank you for taking a few minutes to help Cabrillo College CS/CIS programs!

- Rich

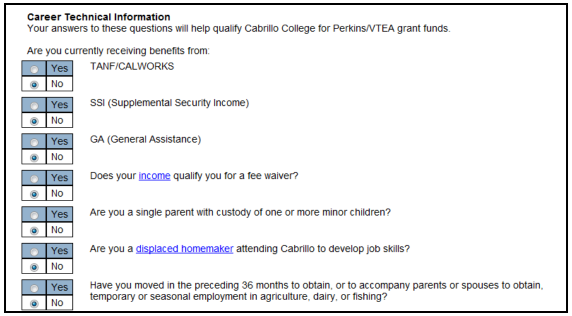
Rich Simms

Posts: 1793
Joined: Sat Jan 16, 2010 5:47 pm
Contact:

http://oslab.cis.cabrillo.edu/forum/viewtopic.php?f=121&t=4176

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?

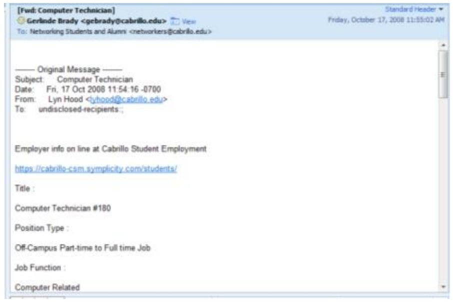
Don't forget to change your default password on Opus

Cabrillo Networking Program Mailing list

Subscribe by sending an email (no subject or body) to:

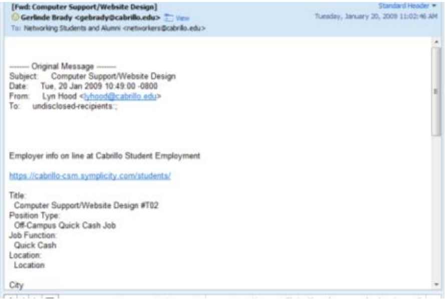
networkers-subscribe@cabrillo.edu

- Program information
- Certification information
- Career and job information
- Short-term classes, events, lectures, tours, etc.
- Surveys
- Networking info and links



[Fwd: Computer Technician]
Gerlinde Brady <gebrady@cabrillo.edu> View
To: Networking Students and Alumni <networkers@cabrillo.edu>
Standard Header
Friday, October 17, 2008 11:55:02 AM

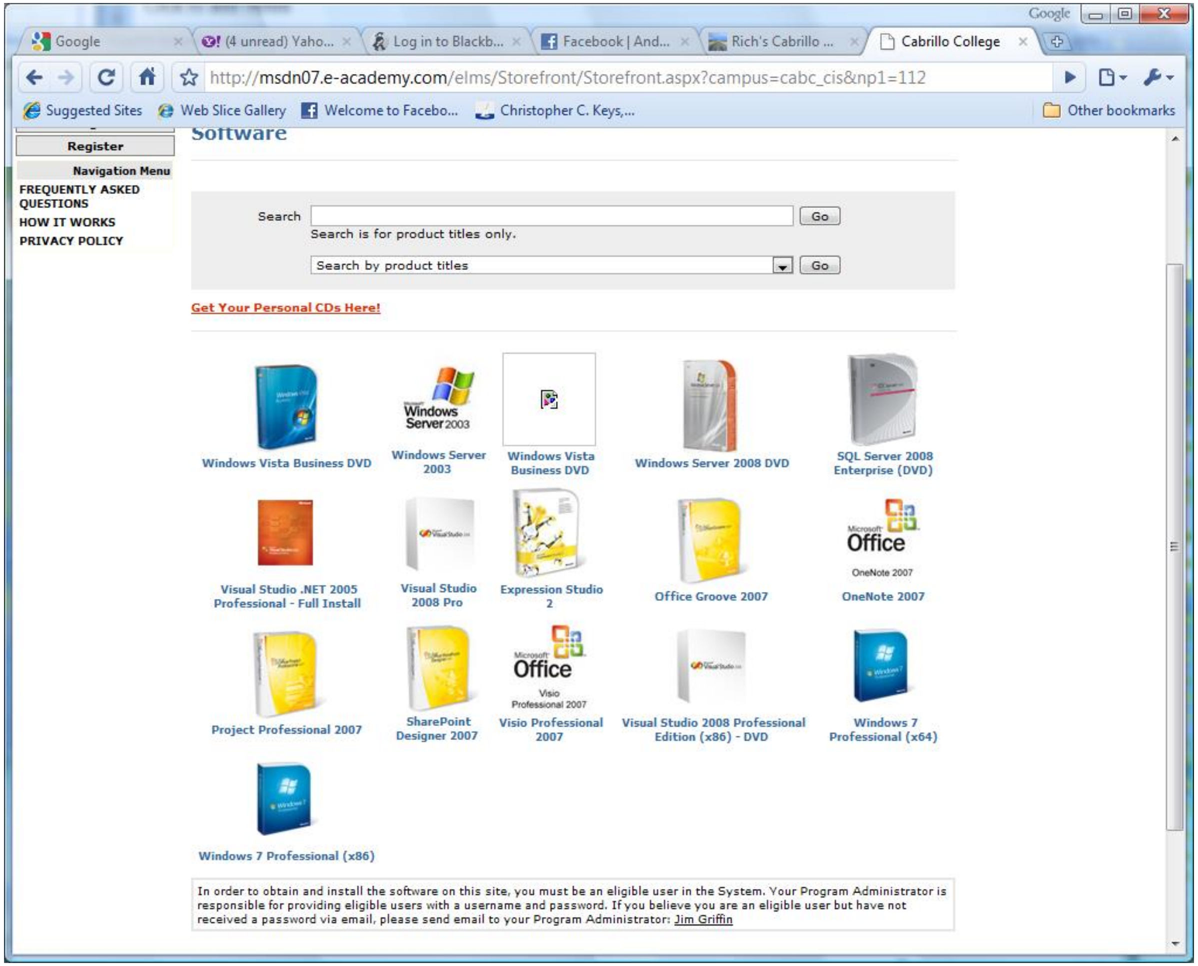
```
-------- Original Message --------
Subject:    Computer Technician
Date:    Fri, 17 Oct 2008 11:54:16 -0700
From:    Lyn Hood <lyhood@cabrillo.edu>
To:    undisclosed-recipients:;


Employer info on line at Cabrillo Student Employment

https://cabrillo-csm.symplicity.com/students/

Title :

Computer Technician #180

Position Type :

Off-Campus Part-time to Full time Job

Job Function :

Computer Related
```



[Fwd: Computer Support/Website Design]
Gerlinde Brady <gebrady@cabrillo.edu> View
To: Networking Students and Alumni <networkers@cabrillo.edu>
Standard Header
Tuesday, January 20, 2009 11:02:46 AM

```
-------- Original Message --------
Subject:    Computer Support/Website Design
Date:    Tue, 20 Jan 2009 10:49:00 -0800
From:    Lyn Hood <lyhood@cabrillo.edu>
To:    undisclosed-recipients:;


Employer info on line at Cabrillo Student Employment

https://cabrillo-csm.symplicity.com/students/

Title:
  Computer Support/Website Design #T02
Position Type:
  Off-Campus Quick Cash Job
Job Function:
  Quick Cash
Location:
  Location

City
```

Microsoft Academic Webstore



Search is for product titles only.

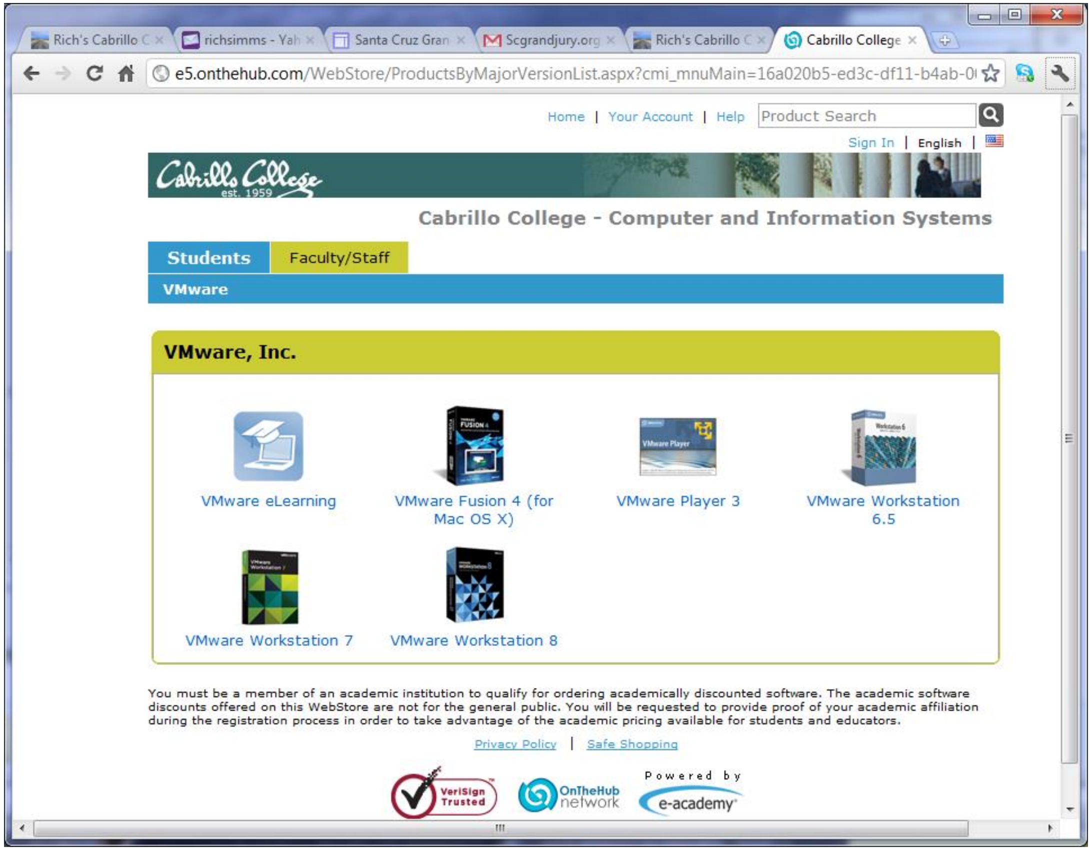
In order to obtain and install the software on this site, you must be an eligible user in the System. Your Program Administrator is responsible for providing eligible users with a username and password. If you believe you are an eligible user but have not received a password via email, please send email to your Program Administrator: Jim Griffin

- Microsoft software for students registered in a CIS or CS class at Cabrillo

- Available after registration is final (two weeks after first class)

To get to this page, go to **http://simms-teach.com/resources** and click on the appropriate link in the Tools and Software section

VMware Academic Webstore



Cabrillo College - Computer and Information Systems

VMware, Inc.

- VMware eLearning
- VMware Fusion 4 (for Mac OS X)
- VMware Player 3
- VMware Workstation 6.5
- VMware Workstation 7
- VMware Workstation 8

You must be a member of an academic institution to qualify for ordering academically discounted software. The academic software discounts offered on this WebStore are not for the general public. You will be requested to provide proof of your academic affiliation during the registration process in order to take advantage of the academic pricing available for students and educators.

- VMware software for students registered in a CIS or CS class at Cabrillo
- Available after registration is final (two weeks after first class)

To get to this page, go to **http://simms-teach.com/resources** and click on the appropriate link in the Tools and Software section

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

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

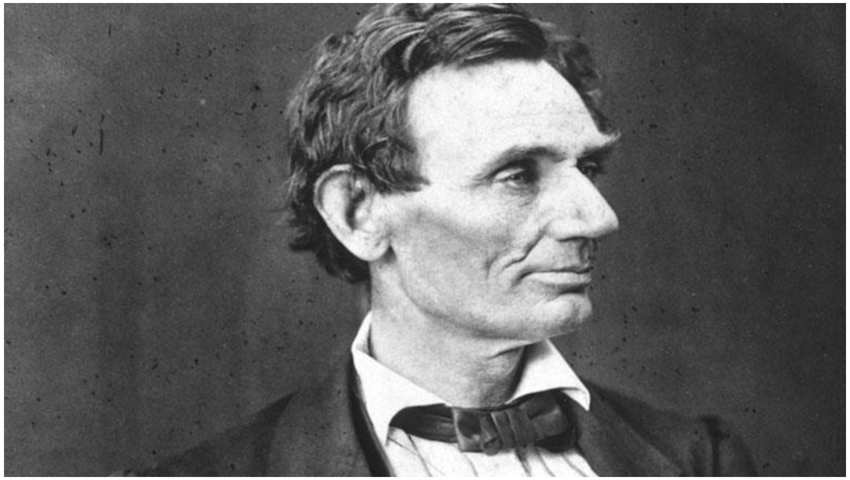
- Not covered in depth by the Netlab+ labs.

- Hard to defend against:
  - Companies need to advertise.
  - Companies need to post job openings.
  - Can't control their employees outside of work.

- Search 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

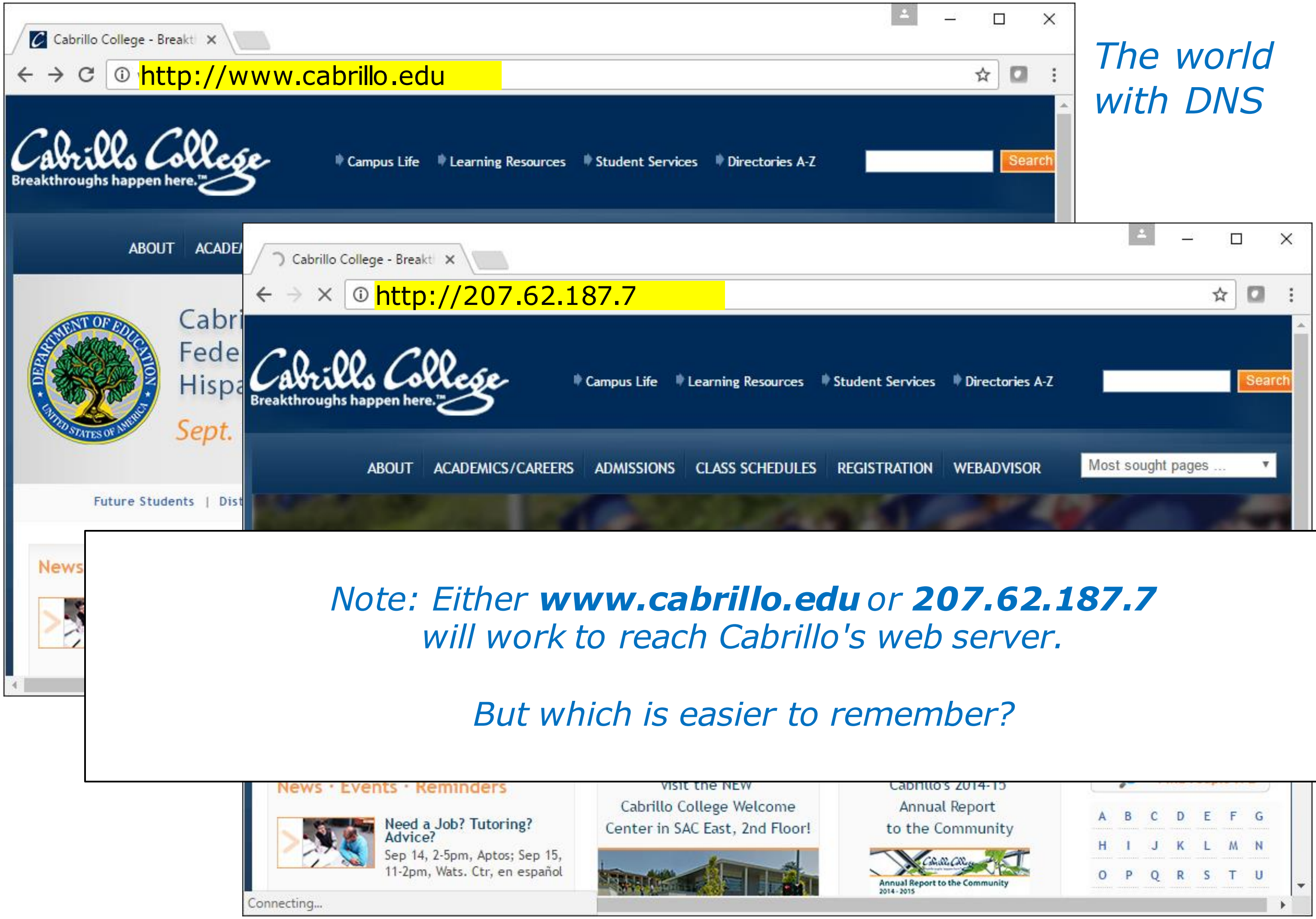
- Active vs. Passive: Have you touched the target?
- Passive: Using methods where you will not be detected by the target.
- Semi-passive: Using methods that appear as normal Internet traffic.
- Active: port scans, vulnerability scans, testing input validation filters, searching for unpublished servers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

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

Domain Name System

DNS

DNS - Domain Name System



http://www.cabrillo.edu

The world with DNS

http://207.62.187.7

The world without DNS

Cabrillo College - Breakt
Cabrillo College Breakthroughs happen here.™
Campus Life
Learning Resources
Student Services
Directories A-Z
Search
ABOUT
ACADEMICS/CAREERS
ADMISSIONS
CLASS SCHEDULES
REGISTRATION
WEBADVISOR
Most sought pages ...
Future Students
News · Events · Reminders
Need a Job? Tutoring? Advice?
Sep 14, 2-5pm, Aptos; Sep 15, 11-2pm, Wats. Ctr, en español
Visit the NEW Cabrillo College Welcome Center in SAC East, 2nd Floor!
Cabrillo's 2014-15 Annual Report to the Community
A B C D E F G
H I J K L M N
O P Q R S T U
Connecting...

*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)

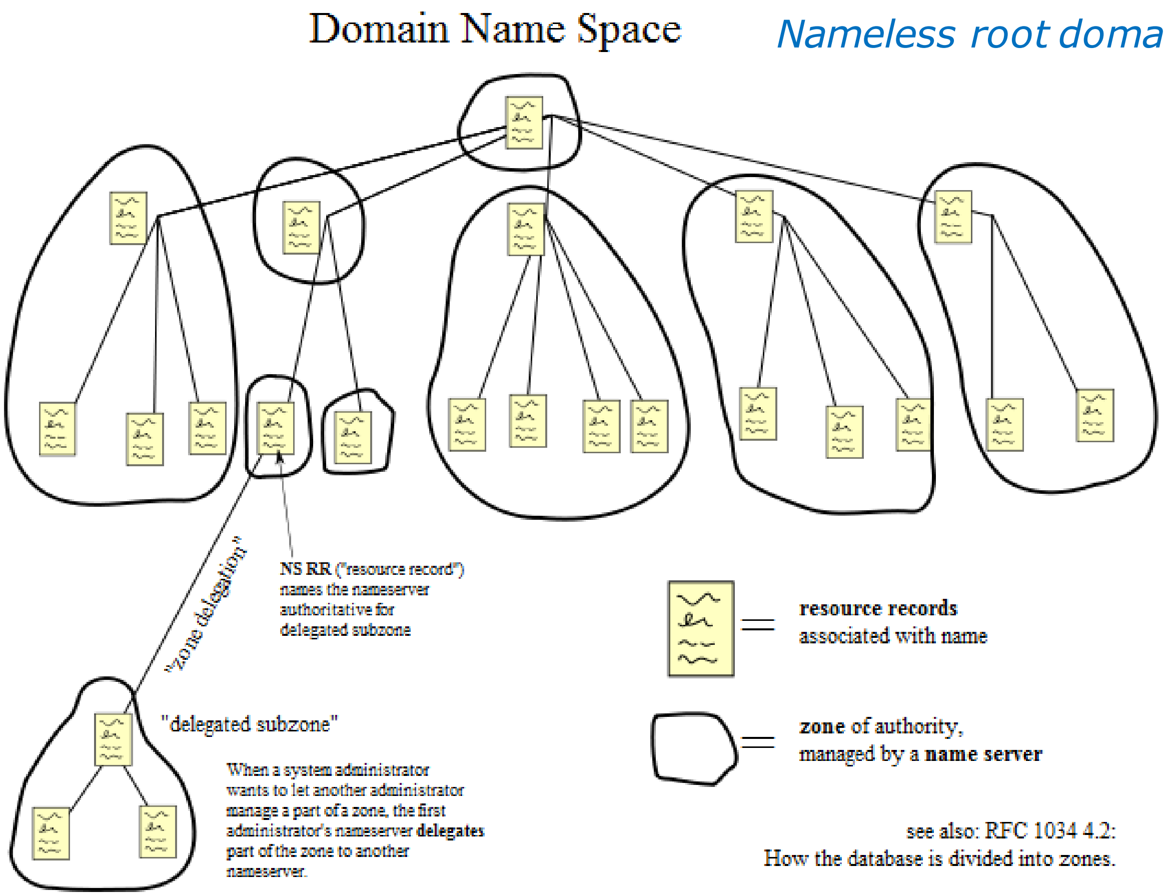
```
root@kali:~# host opus.cis.cabrillo.edu
opus.cis.cabrillo.edu is an alias for oslab.cis.cabrillo.edu.
oslab.cis.cabrillo.edu has address 207.62.187.230
oslab.cis.cabrillo.edu has IPv6 address 2607:f380:80f:f425::230
root@kali:~#
```

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



NS RR ("resource record") names the nameserver authoritative for delegated subzone

When a system administrator wants to let another administrator manage a part of a zone, the first administrator's nameserver **delegates** part of the zone to another nameserver.

resource records associated with name

zone of authority, managed by a **name server**

see also: RFC 1034 4.2: How the database is divided into zones.

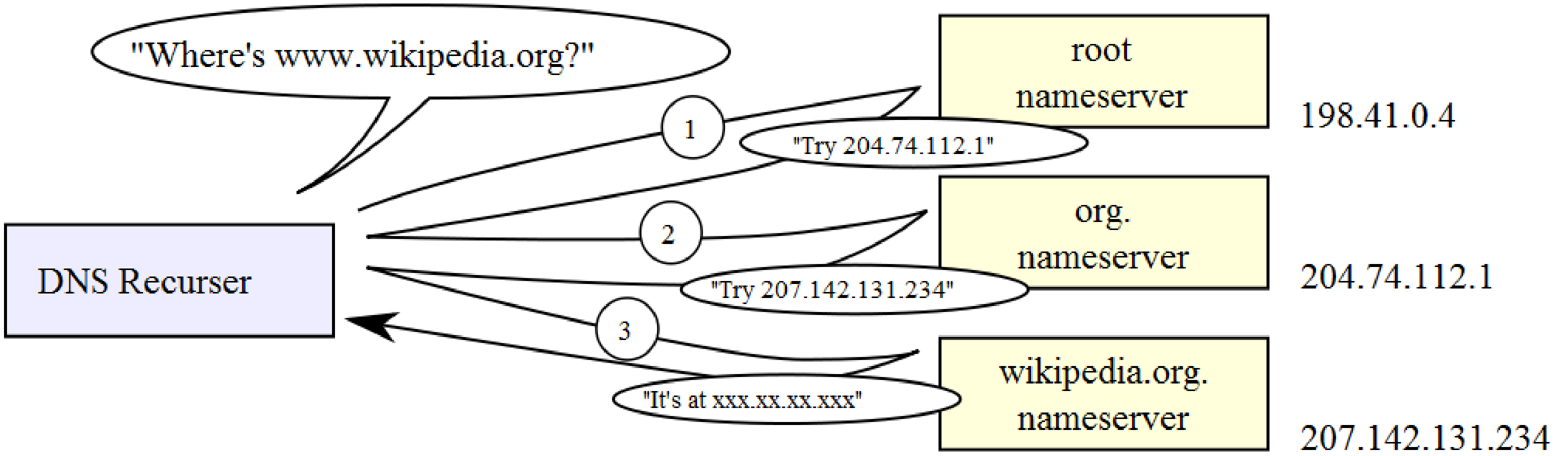
Nameless root domain referred to via "."

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)

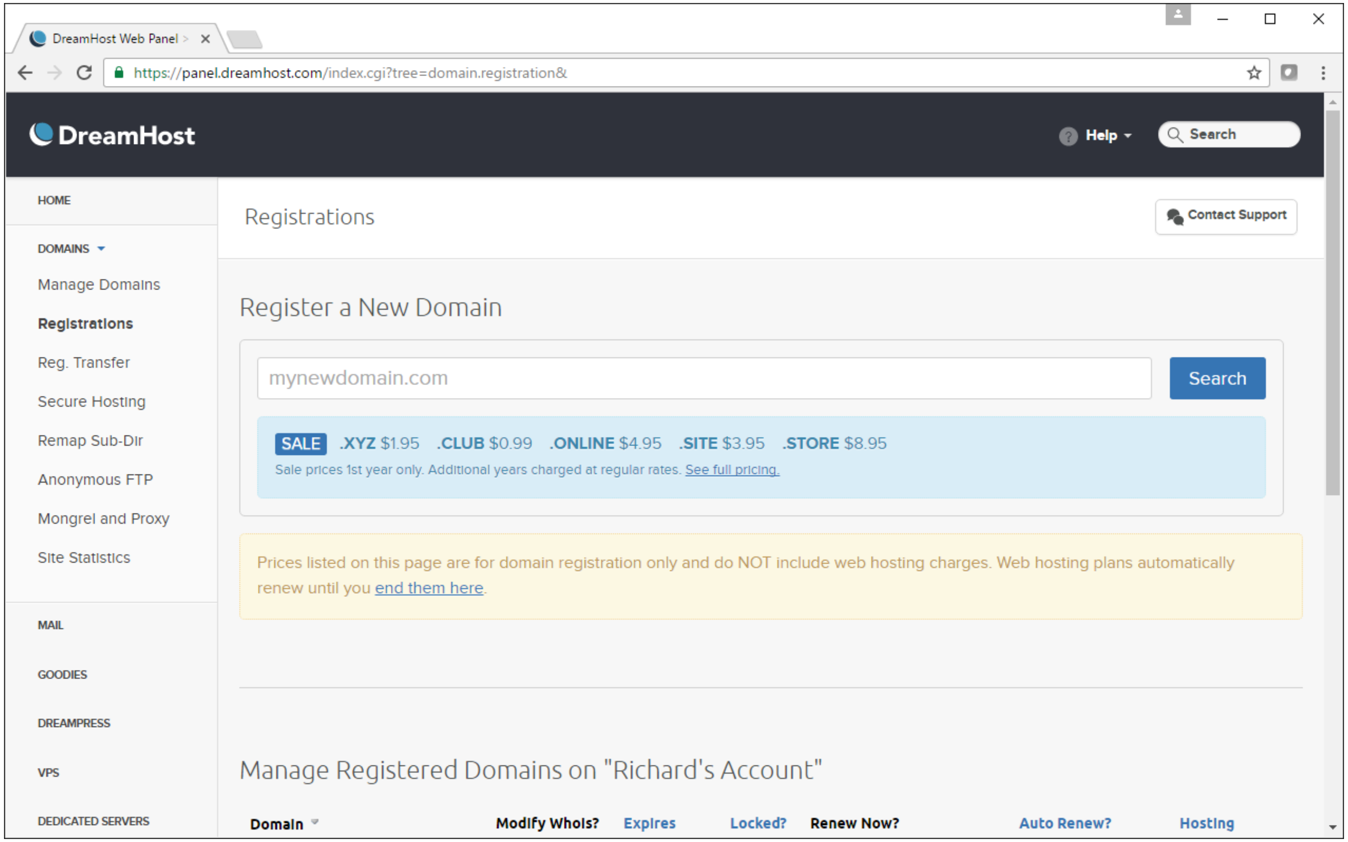
CNAME - Aliases

MX - mail hubs

Domain Owner

whois

Anyone can register a domain



Registrations

Register a New Domain

mynewdomain.com

SALE .XYZ $1.95 .CLUB $0.99 .ONLINE $4.95 .SITE $3.95 .STORE $8.95

Sale prices 1st year only. Additional years charged at regular rates. See full pricing.

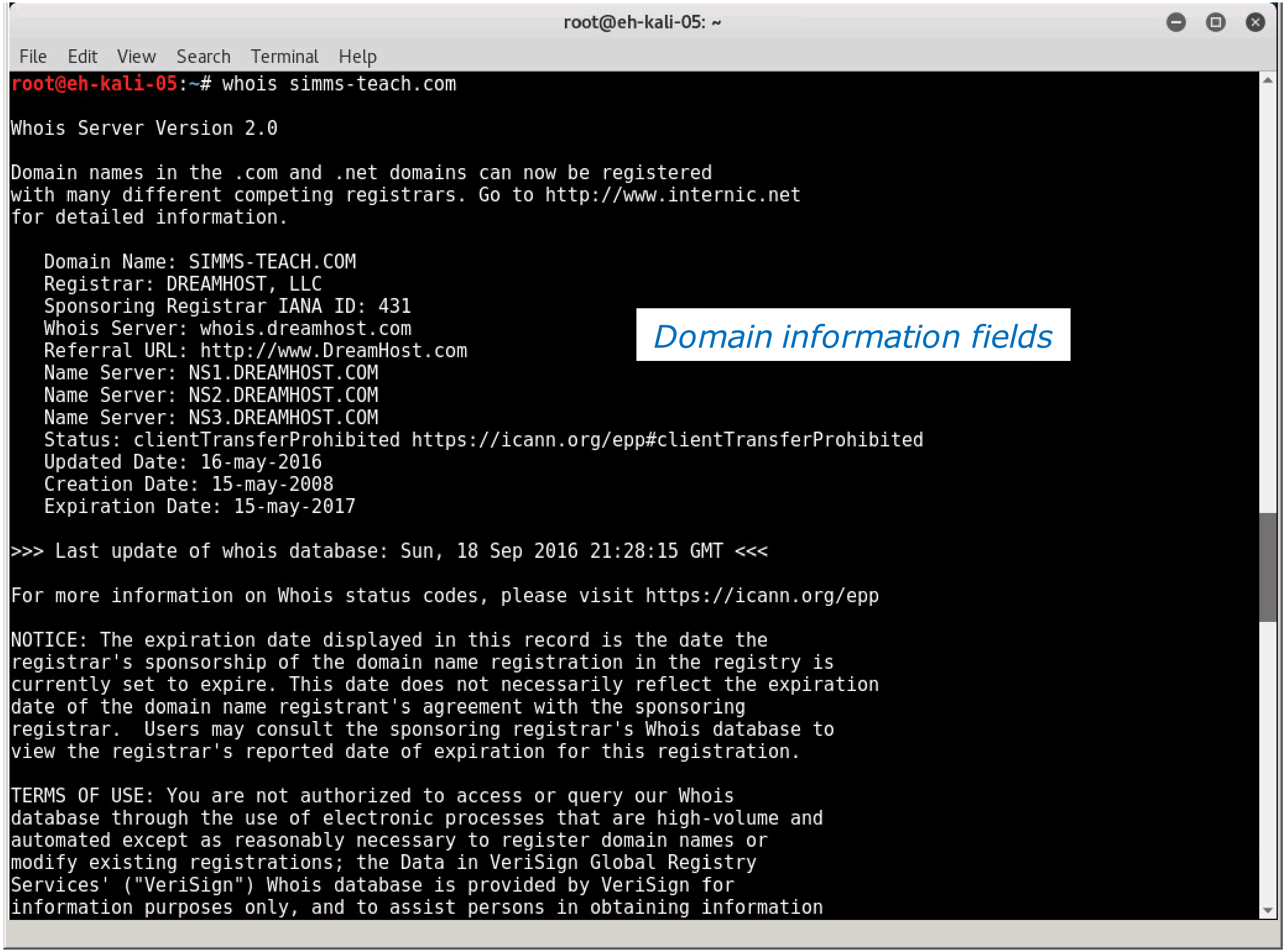
Prices listed on this page are for domain registration only and do NOT include web hosting charges. Web hosting plans automatically renew until you end them here.

Manage Registered Domains on "Richard's Account"

Domain	Modify WhoIs?	Expires	Locked?	Renew Now?	Auto Renew?	Hosting

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

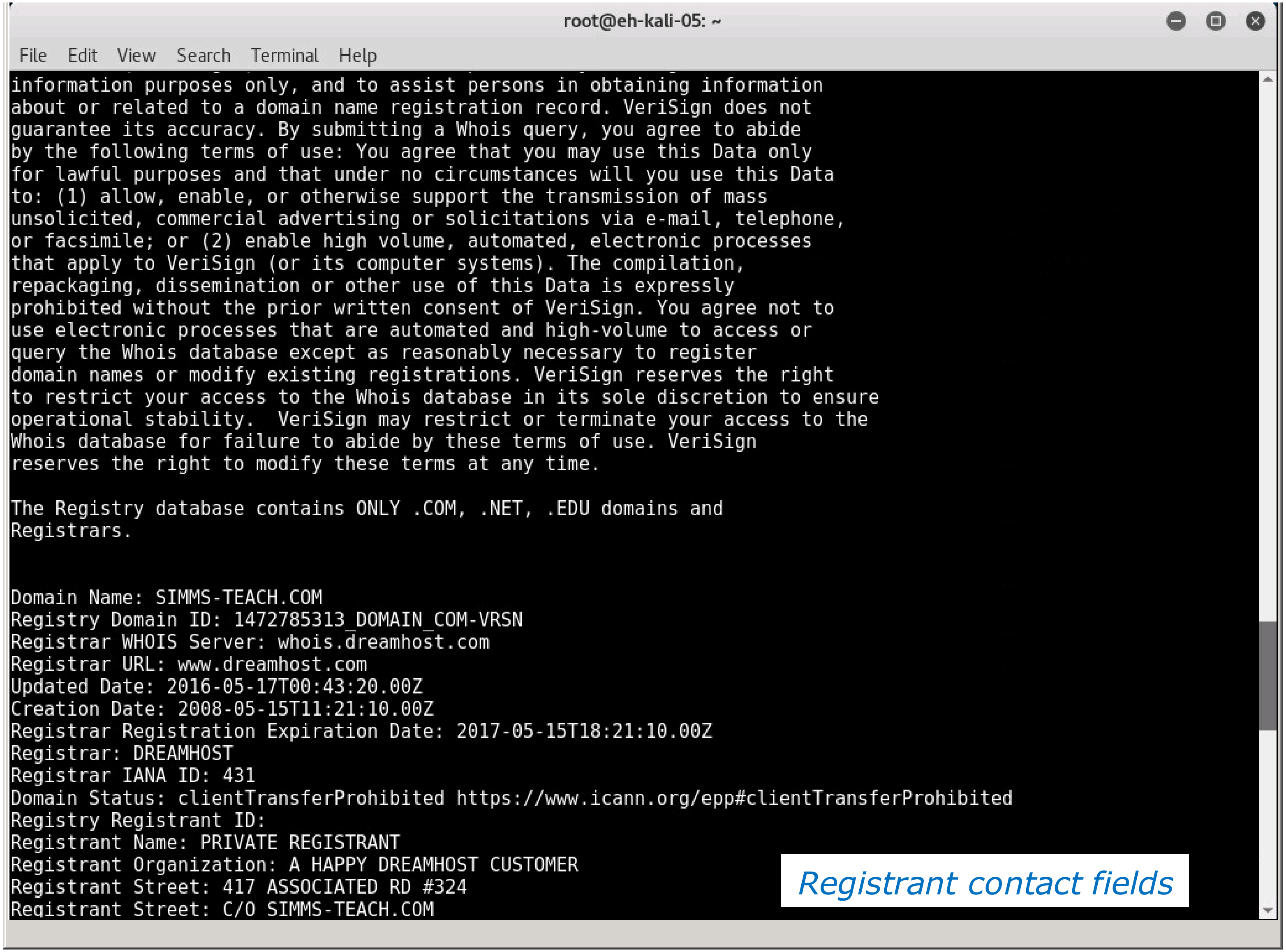
Linux whois command



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

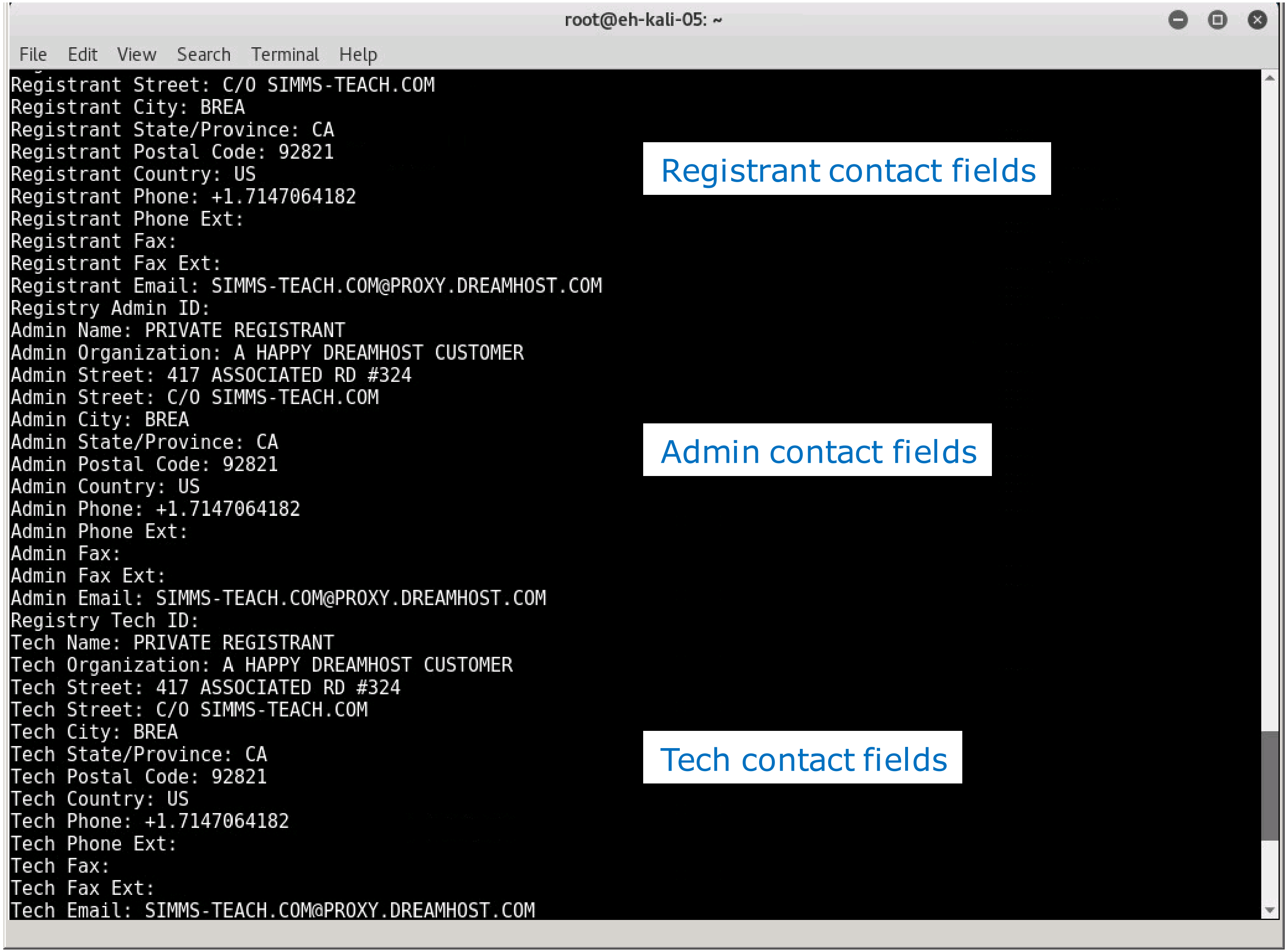
Linux whois command



```
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



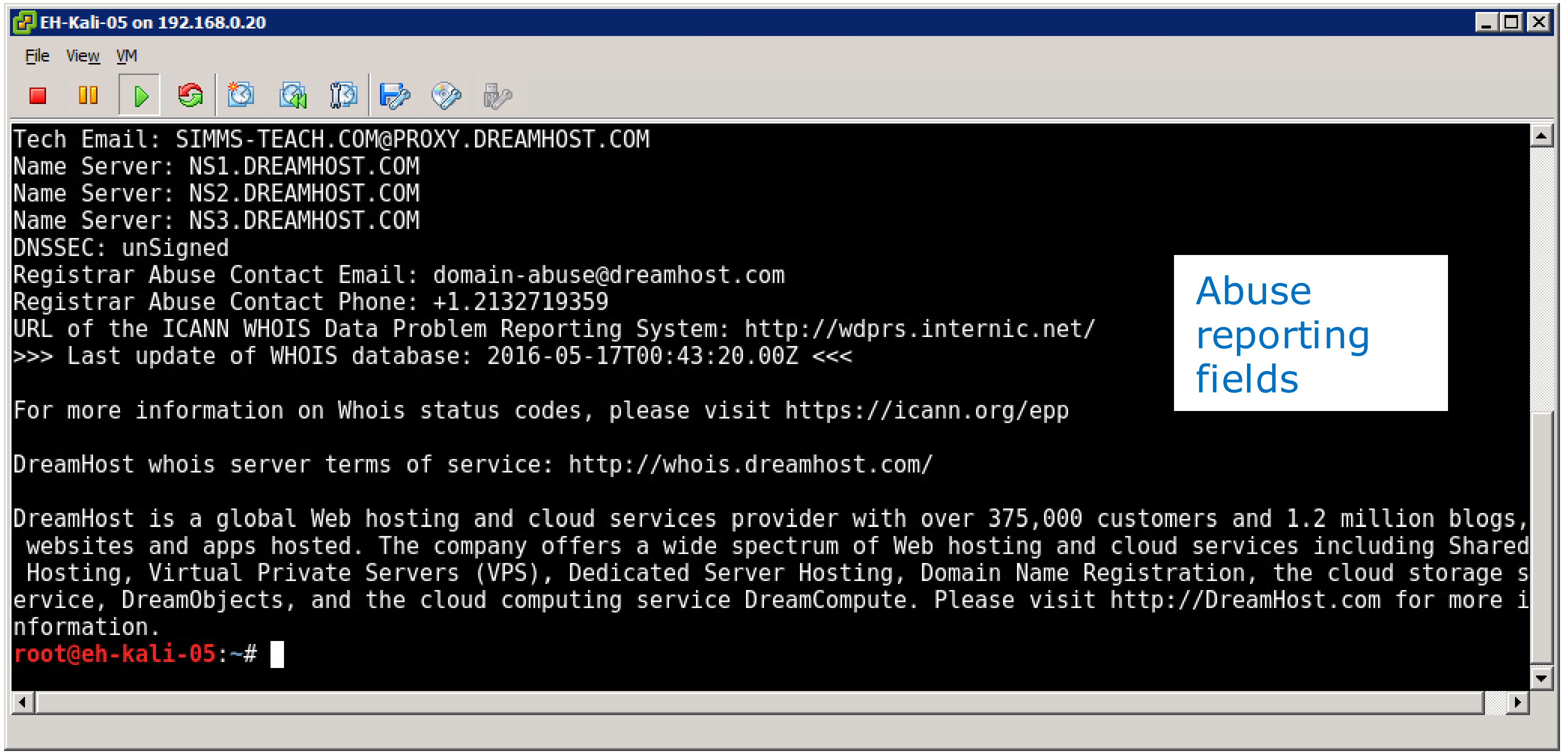
```
Registrant Street: C/O SIMMS-TEACH.COM
Registrant City: BREA
Registrant State/Province: CA
Registrant Postal Code: 92821
Registrant Country: US
Registrant Phone: +1.7147064182
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: SIMMS-TEACH.COM@PROXY.DREAMHOST.COM
Registry 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



```
Tech Email: SIMMS-TEACH.COM@PROXY.DREAMHOST.COM
Name Server: NS1.DREAMHOST.COM
Name Server: NS2.DREAMHOST.COM
Name Server: NS3.DREAMHOST.COM
DNSSEC: unSigned
Registrar Abuse Contact Email: domain-abuse@dreamhost.com
Registrar Abuse Contact Phone: +1.2132719359
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2016-05-17T00:43:20.00Z <<<

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

DreamHost whois server terms of service: http://whois.dreamhost.com/

DreamHost is a global Web hosting and cloud services provider with over 375,000 customers and 1.2 million blogs,
 websites and apps hosted. The company offers a wide spectrum of Web hosting and cloud services including Shared
 Hosting, Virtual Private Servers (VPS), Dedicated Server Hosting, Domain Name Registration, the cloud storage s
ervice, DreamObjects, and the cloud computing service DreamCompute. Please visit http://DreamHost.com for more i
nformation.
root@eh-kali-05:~# 
```

Abuse reporting fields

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

Activity

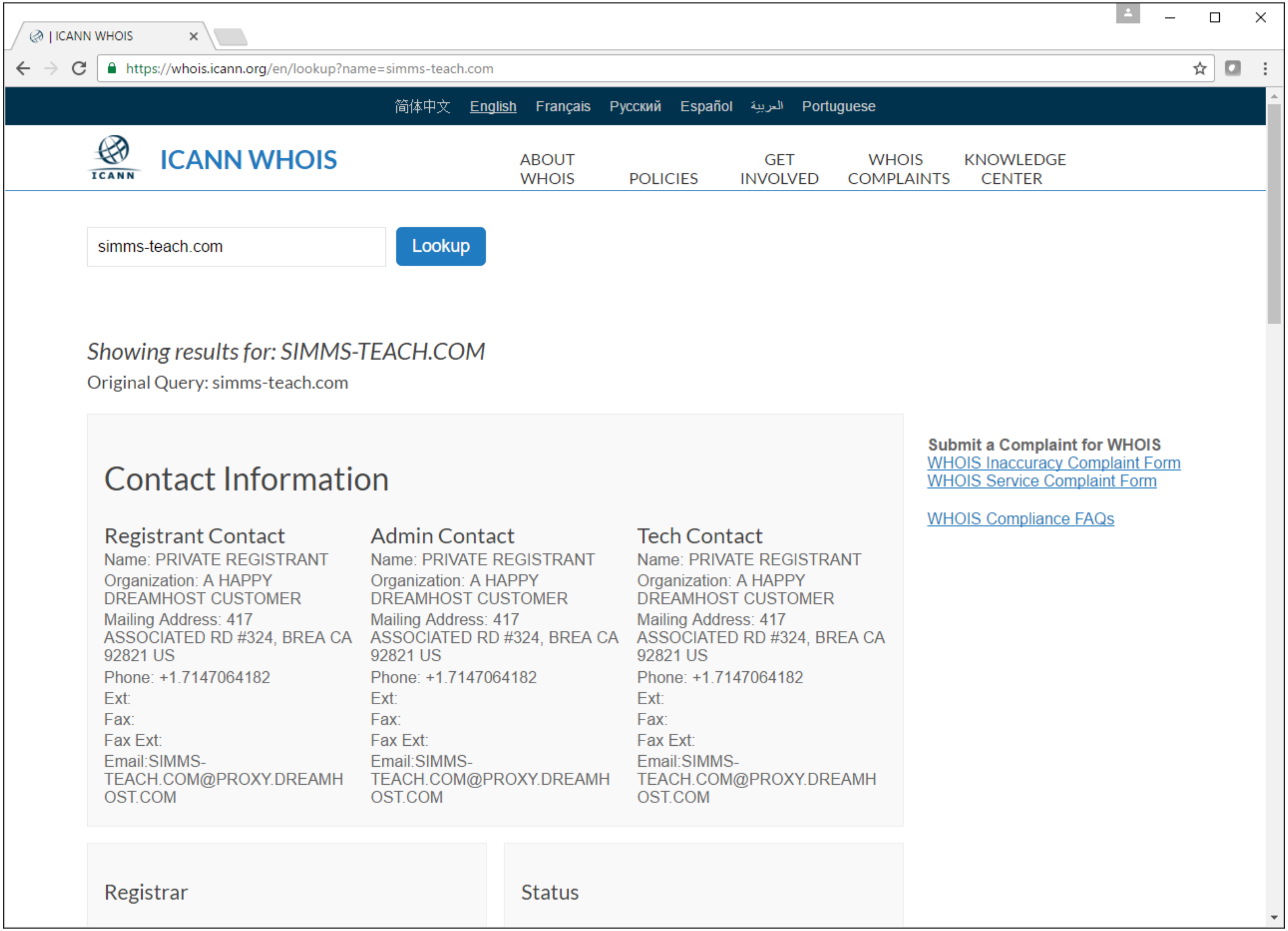
Using only the **whois** command see if you can find two contacts at Beloit College in Wisconsin.

Write their first names into the chat window.

Domain Owner

whois.icann.org

http://whois.icann.org



| ICANN WHOIS
https://whois.icann.org/en/lookup?name=simms-teach.com
简体中文 English Français Русский Español العربية Portuguese
ICANN
ICANN WHOIS
ABOUT WHOIS
POLICIES
GET INVOLVED
WHOIS COMPLAINTS
KNOWLEDGE CENTER
simms-teach.com
Lookup

Showing results for: SIMMS-TEACH.COM

Original Query: simms-teach.com

Contact Information

Registrant Contact
Name: PRIVATE REGISTRANT
Organization: A HAPPY DREAMHOST CUSTOMER
Mailing Address: 417 ASSOCIATED RD #324, BREA CA 92821 US
Phone: +1.7147064182
Ext:
Fax:
Fax Ext:
Email:SIMMS-TEACH.COM@PROXY.DREAMHOST.COM

Admin Contact
Name: PRIVATE REGISTRANT
Organization: A HAPPY DREAMHOST CUSTOMER
Mailing Address: 417 ASSOCIATED RD #324, BREA CA 92821 US
Phone: +1.7147064182
Ext:
Fax:
Fax Ext:
Email:SIMMS-TEACH.COM@PROXY.DREAMHOST.COM

Tech Contact
Name: PRIVATE REGISTRANT
Organization: A HAPPY DREAMHOST CUSTOMER
Mailing Address: 417 ASSOCIATED RD #324, BREA CA 92821 US
Phone: +1.7147064182
Ext:
Fax:
Fax Ext:
Email:SIMMS-TEACH.COM@PROXY.DREAMHOST.COM

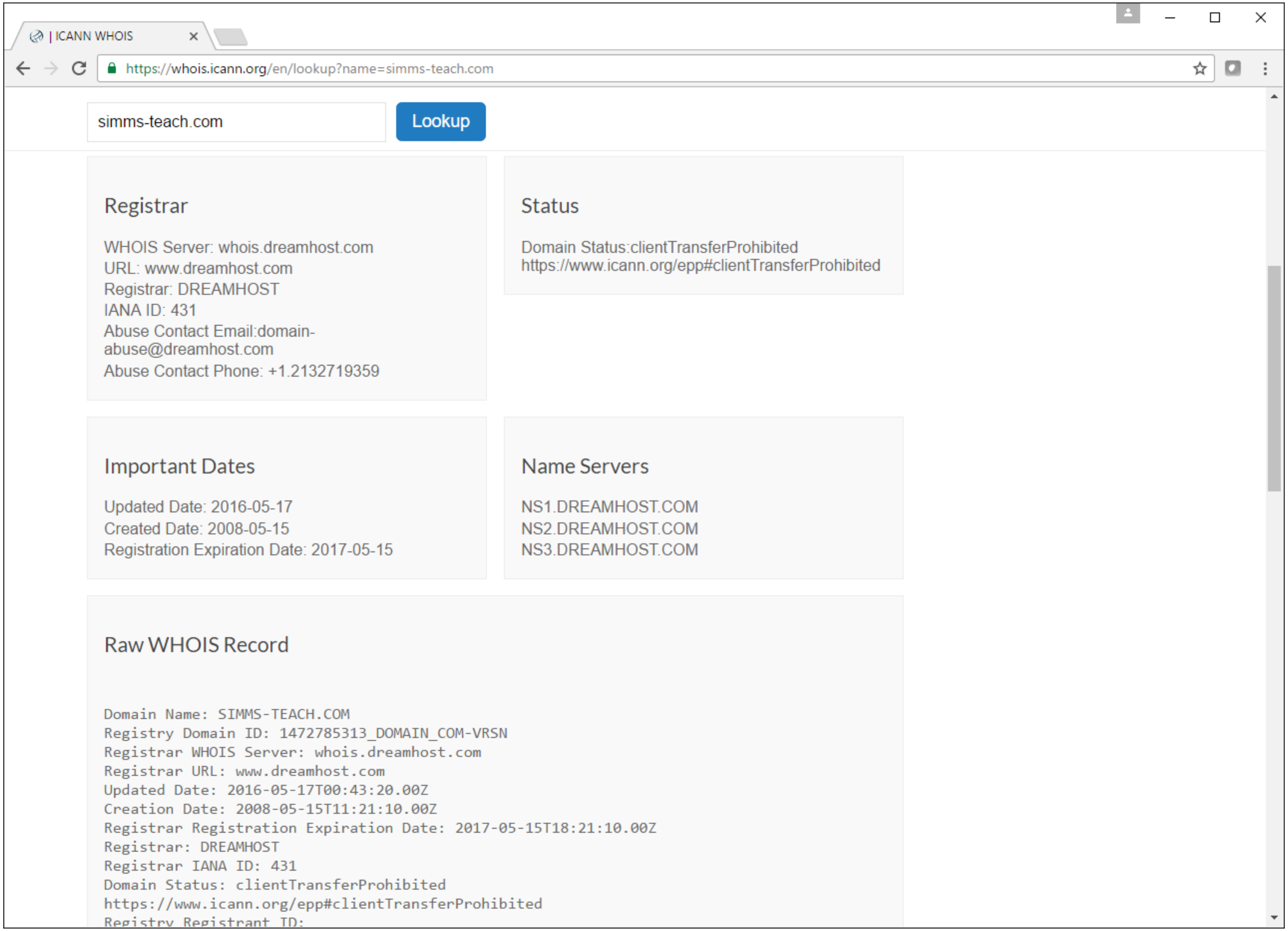
Submit a Complaint for WHOIS
WHOIS Inaccuracy Complaint Form
WHOIS Service Complaint Form

WHOIS Compliance FAQs

Registrar

Status

http://whois.icann.org



Registrar

WHOIS Server: whois.dreamhost.com
URL: www.dreamhost.com
Registrar: DREAMHOST
IANA ID: 431
Abuse Contact Email:domain-abuse@dreamhost.com
Abuse Contact Phone: +1.2132719359

Status

Domain Status:clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited

Important Dates

Updated Date: 2016-05-17
Created Date: 2008-05-15
Registration Expiration Date: 2017-05-15

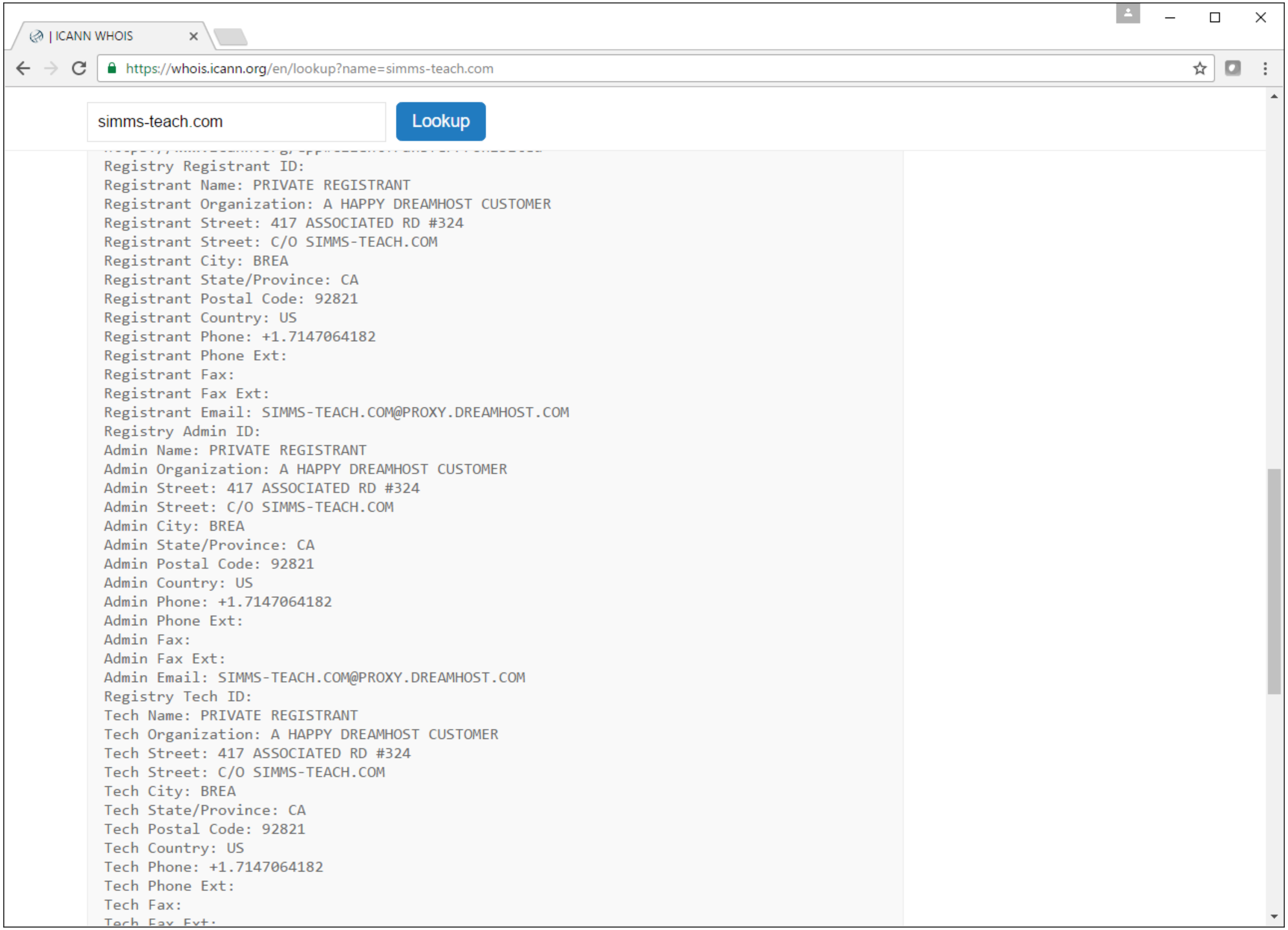
Name Servers

NS1.DREAMHOST.COM
NS2.DREAMHOST.COM
NS3.DREAMHOST.COM

Raw WHOIS Record

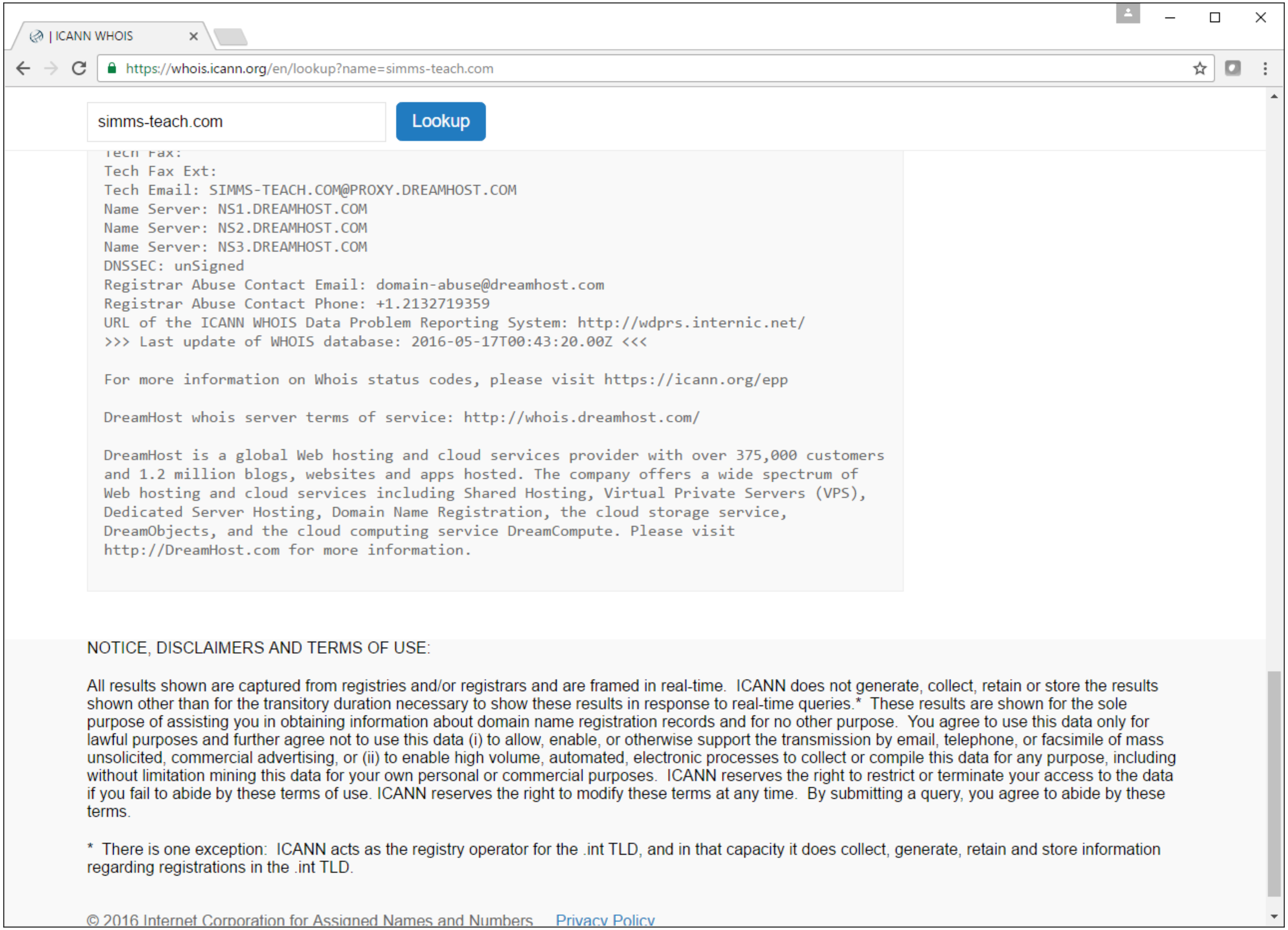
```
Domain Name: SIMMS-TEACH.COM
Registry Domain ID: 1472785313_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.dreamhost.com
Registrar URL: www.dreamhost.com
Updated Date: 2016-05-17T00:43:20.00Z
Creation Date: 2008-05-15T11:21:10.00Z
Registrar Registration Expiration Date: 2017-05-15T18:21:10.00Z
Registrar: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

http://whois.icann.org



```
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 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:
```

http://whois.icann.org



```
Tech Fax:
Tech Fax Ext:
Tech Email: SIMMS-TEACH.COM@PROXY.DREAMHOST.COM
Name Server: NS1.DREAMHOST.COM
Name Server: NS2.DREAMHOST.COM
Name Server: NS3.DREAMHOST.COM
DNSSEC: unSigned
Registrar Abuse Contact Email: domain-abuse@dreamhost.com
Registrar Abuse Contact Phone: +1.2132719359
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2016-05-17T00:43:20.00Z <<<

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

DreamHost whois server terms of service: http://whois.dreamhost.com/

DreamHost is a global Web hosting and cloud services provider with over 375,000 customers
and 1.2 million blogs, websites and apps hosted. The company offers a wide spectrum of
Web hosting and cloud services including Shared Hosting, Virtual Private Servers (VPS),
Dedicated Server Hosting, Domain Name Registration, the cloud storage service,
DreamObjects, and the cloud computing service DreamCompute. Please visit
http://DreamHost.com for more information.
```

NOTICE, DISCLAIMERS AND TERMS OF USE:

All results shown are captured from registries and/or registrars and are framed in real-time. ICANN does not generate, collect, retain or store the results shown other than for the transitory duration necessary to show these results in response to real-time queries.* These results are shown for the sole purpose of assisting you in obtaining information about domain name registration records and for no other purpose. You agree to use this data only for lawful purposes and further agree not to use this data (i) to allow, enable, or otherwise support the transmission by email, telephone, or facsimile of mass unsolicited, commercial advertising, or (ii) to enable high volume, automated, electronic processes to collect or compile this data for any purpose, including without limitation mining this data for your own personal or commercial purposes. ICANN reserves the right to restrict or terminate your access to the data if you fail to abide by these terms of use. ICANN reserves the right to modify these terms at any time. By submitting a query, you agree to abide by these terms.

* There is one exception: ICANN acts as the registry operator for the .int TLD, and in that capacity it does collect, generate, retain and store information regarding registrations in the .int TLD.

© 2016 Internet Corporation for Assigned Names and Numbers Privacy Policy

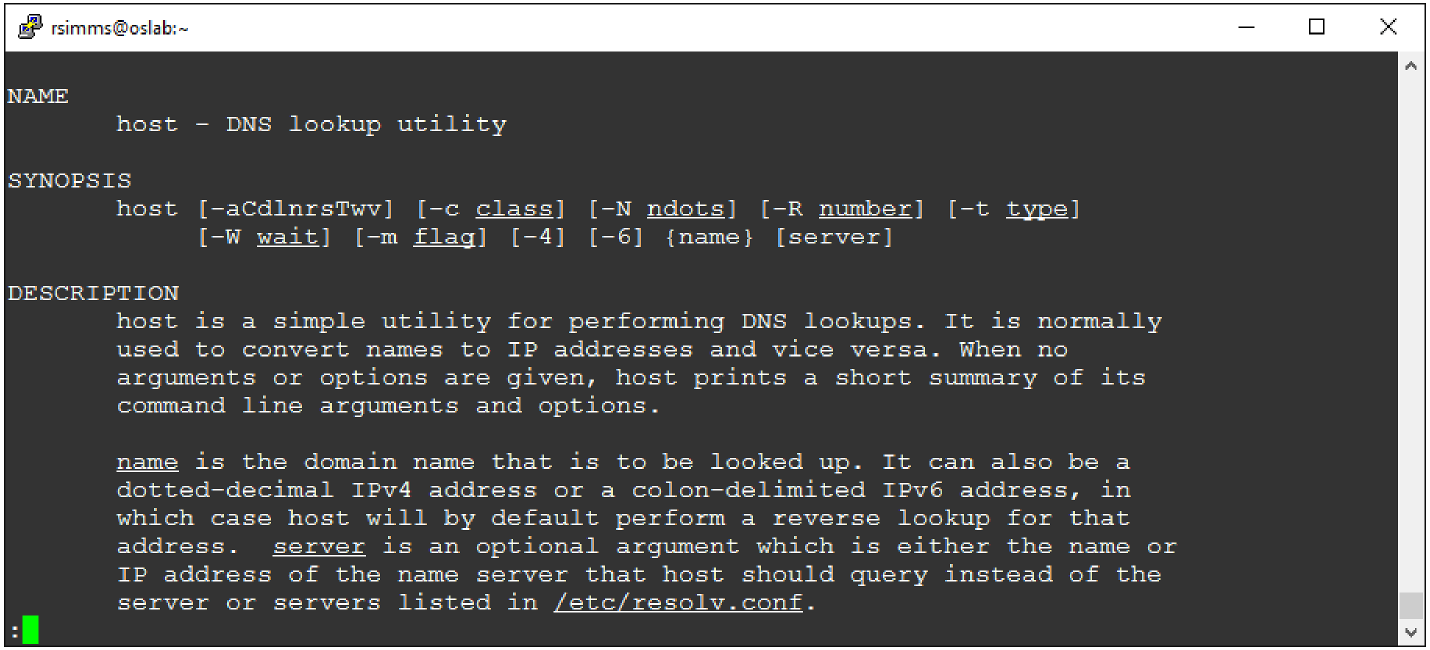
Activity

Using only http://whois.icann.org see if you can find a technical contact at MIT in Cambridge, MA.

Write their first name into the chat window.

Host Command

host command



```
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

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

```
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:~#
```

Specifying a specific name server to do the name resolution

```
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:~#
```

Activity

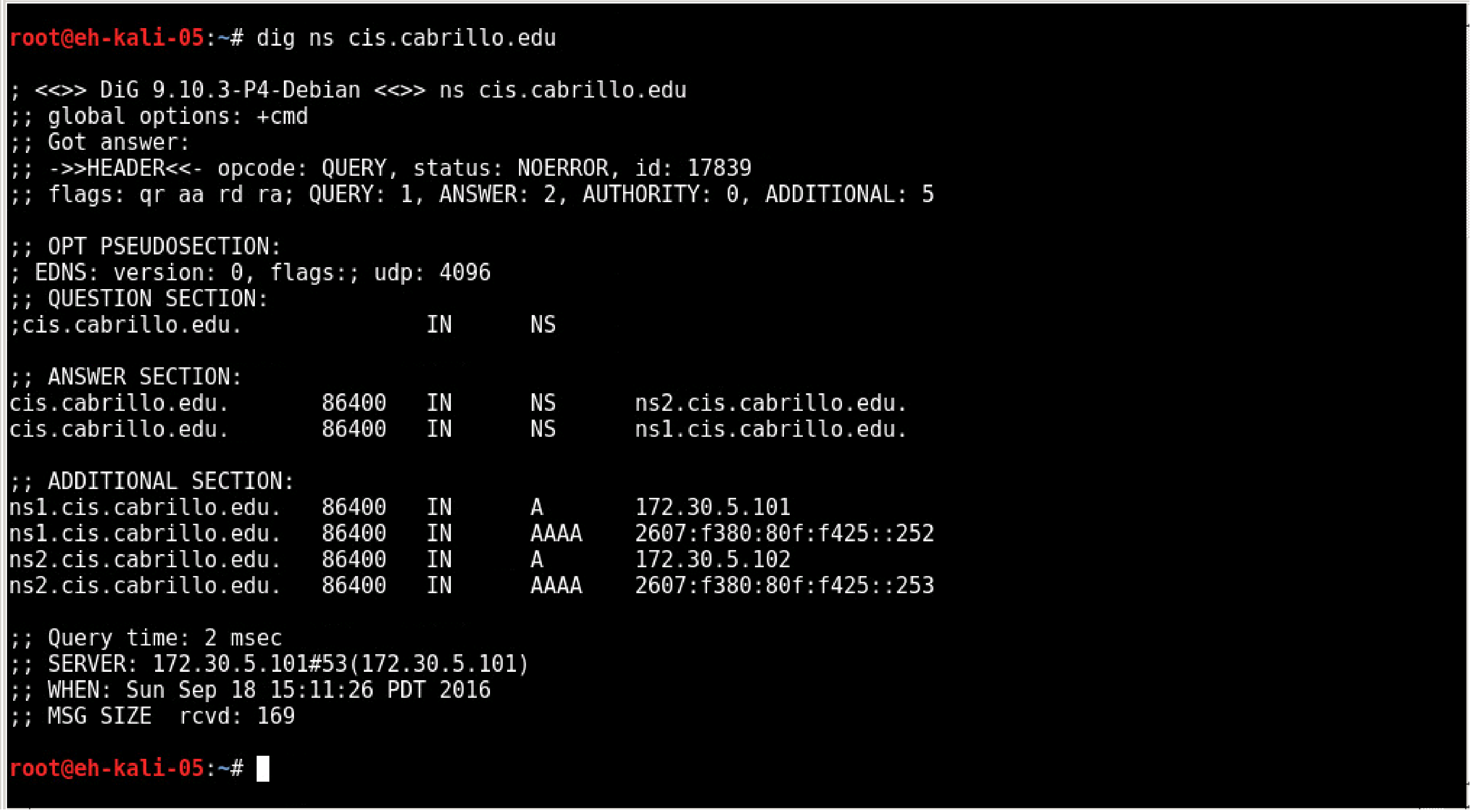
Do a forward and reverse lookup of eh-centos.cis.cabrillo.edu

Write the responses you get in the chat window.

Domain Records

dig

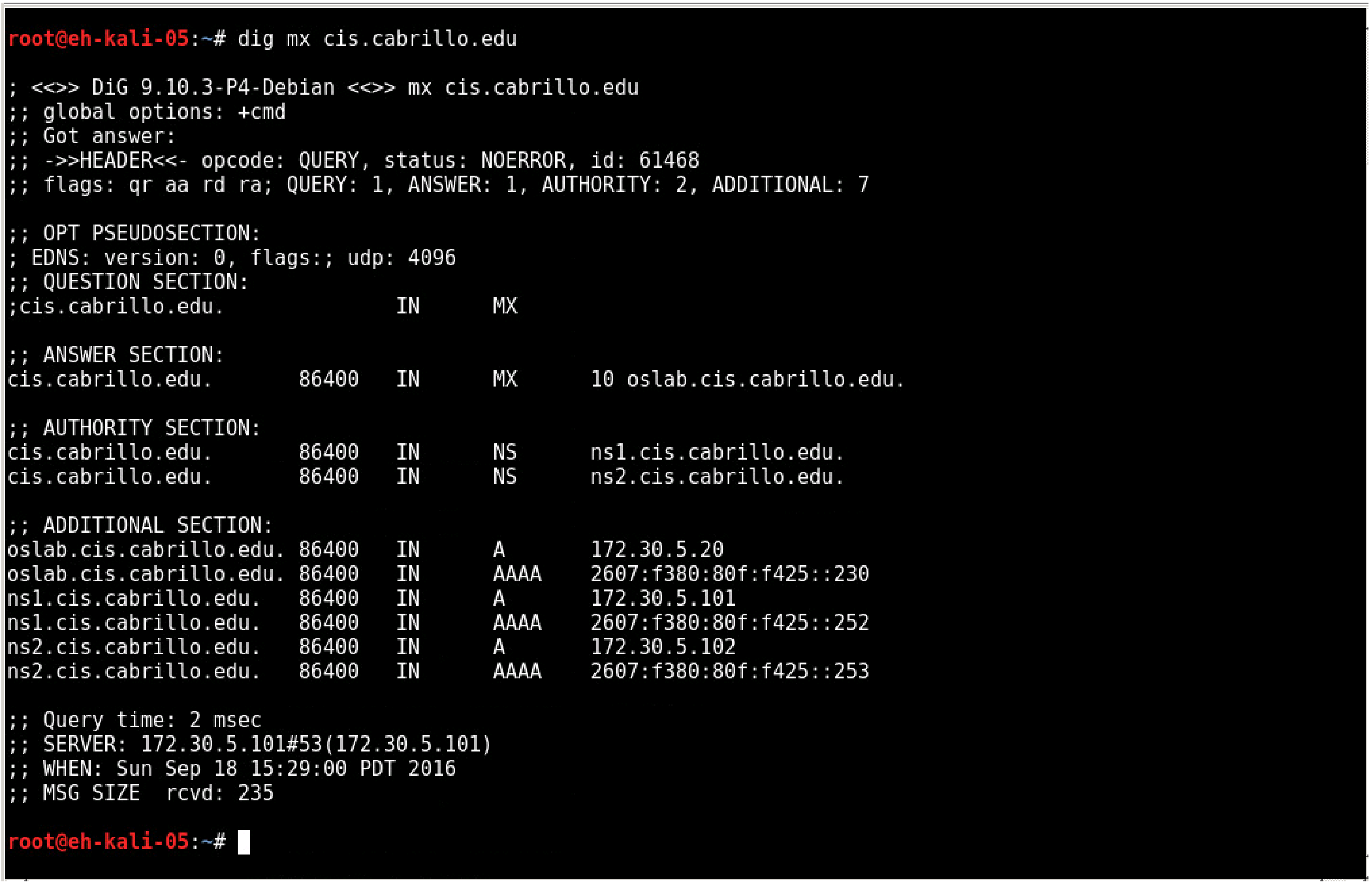
Find domain name servers



```
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:~#
```

dig ns cis.cabrillo.edu

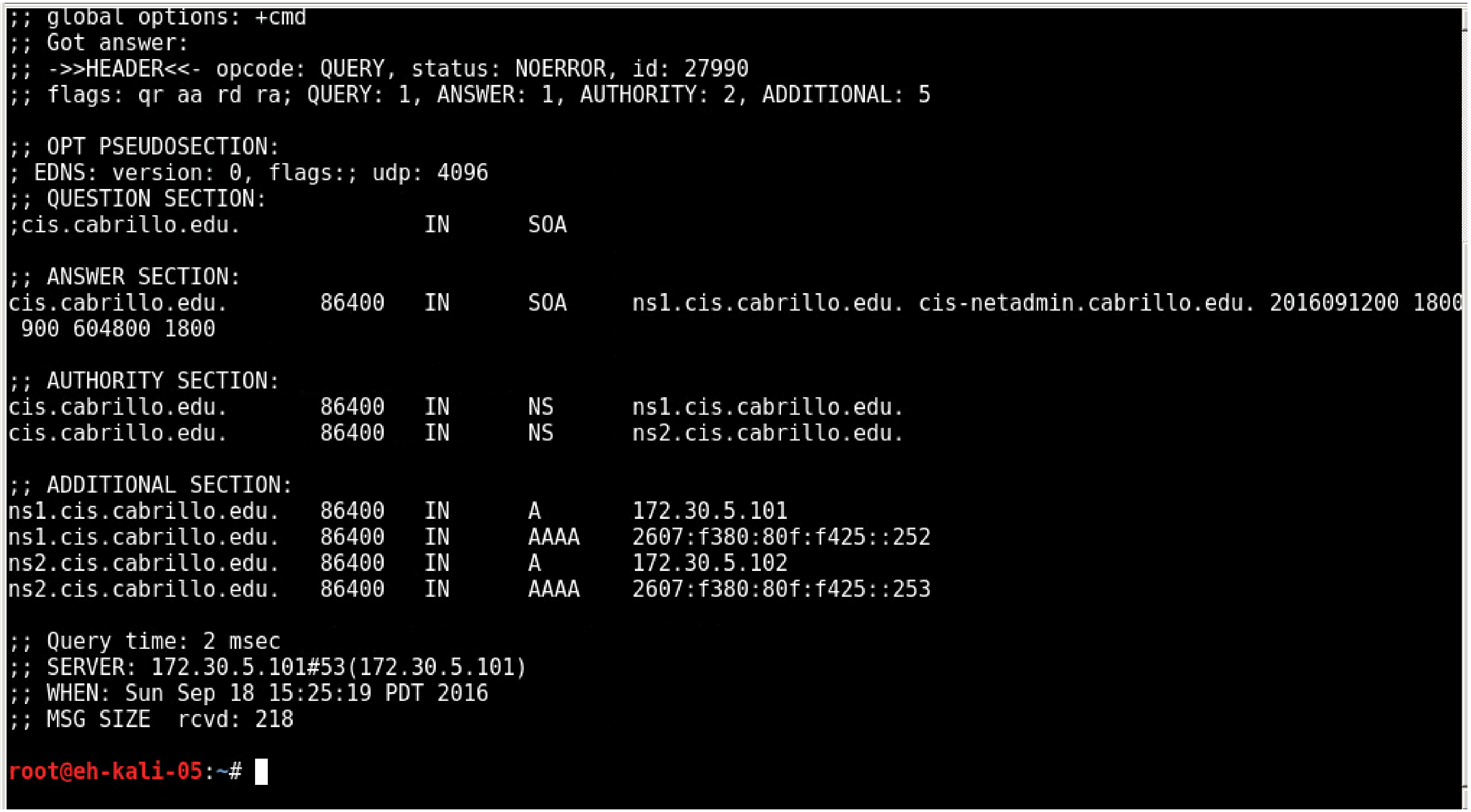
Find domain mail servers



```
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:~#
```

dig mx cis.cabrillo.edu

Find domain administrative contact

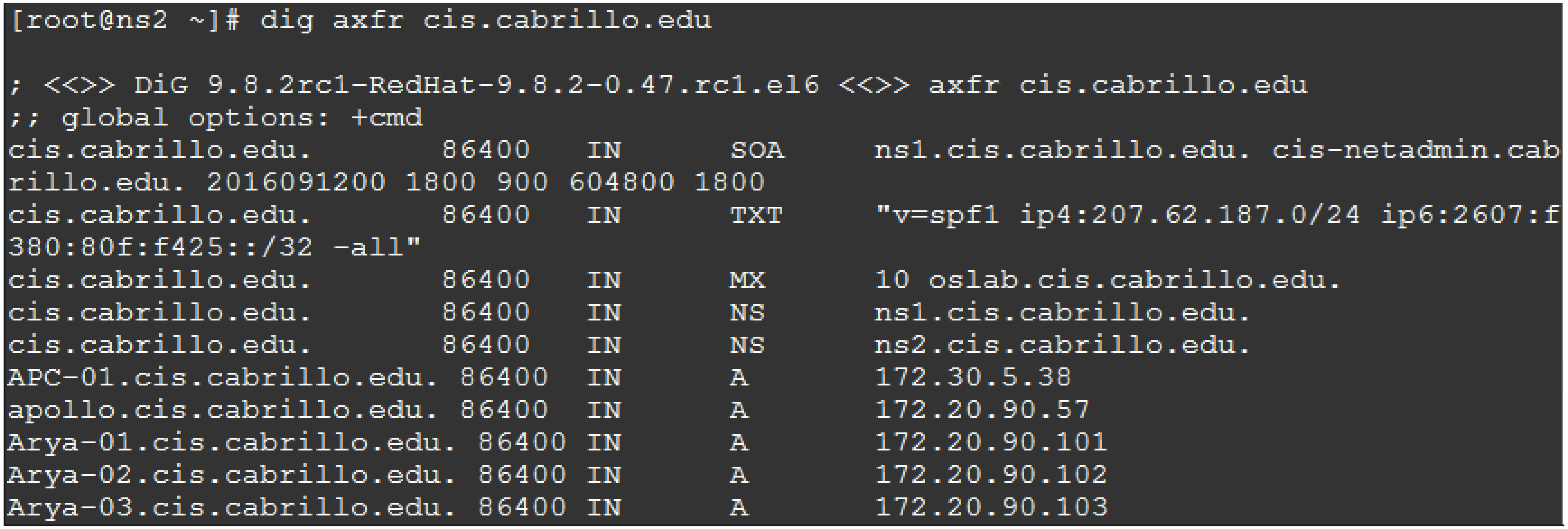


```
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27990
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 5

;; 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:~#
```

dig soa cis.cabrillo.edu

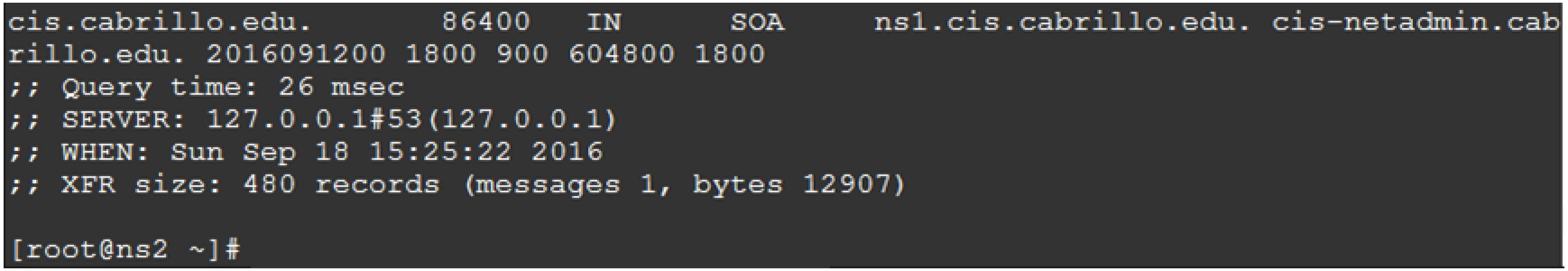
Find domain hosts via zone transfer

Most name servers are configured to never publicly release this information



```
[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 ~]#
```

dig axfr cis.cabrillo.edu

Activity

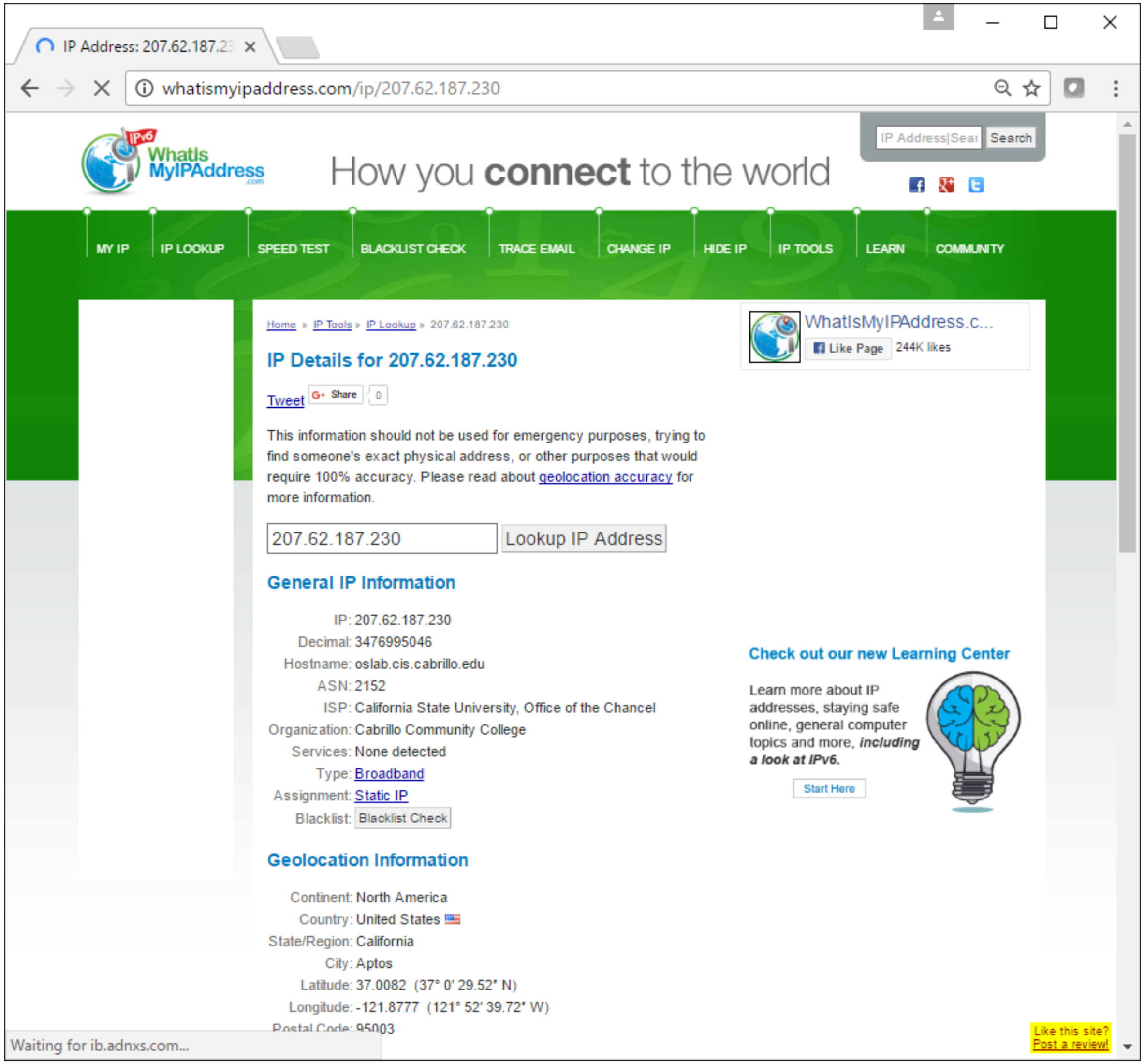
Which domain uses more mx records, google.com or amazon.com?

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

Identifying IP Addresses

whatismyipaddress.com/

http://whatismyipaddress.com/



Home » IP Tools » IP Lookup » 207.62.187.230

IP Details for 207.62.187.230

This information should not be used for emergency purposes, trying to find someone's exact physical address, or other purposes that would require 100% accuracy. Please read about geolocation accuracy for more information.

207.62.187.230

General IP Information

IP: 207.62.187.230
Decimal: 3476995046
Hostname: oslab.cis.cabrillo.edu
ASN: 2152
ISP: California State University, Office of the Chancel
Organization: Cabrillo Community College
Services: None detected
Type: Broadband
Assignment: Static IP
Blacklist: Blacklist Check

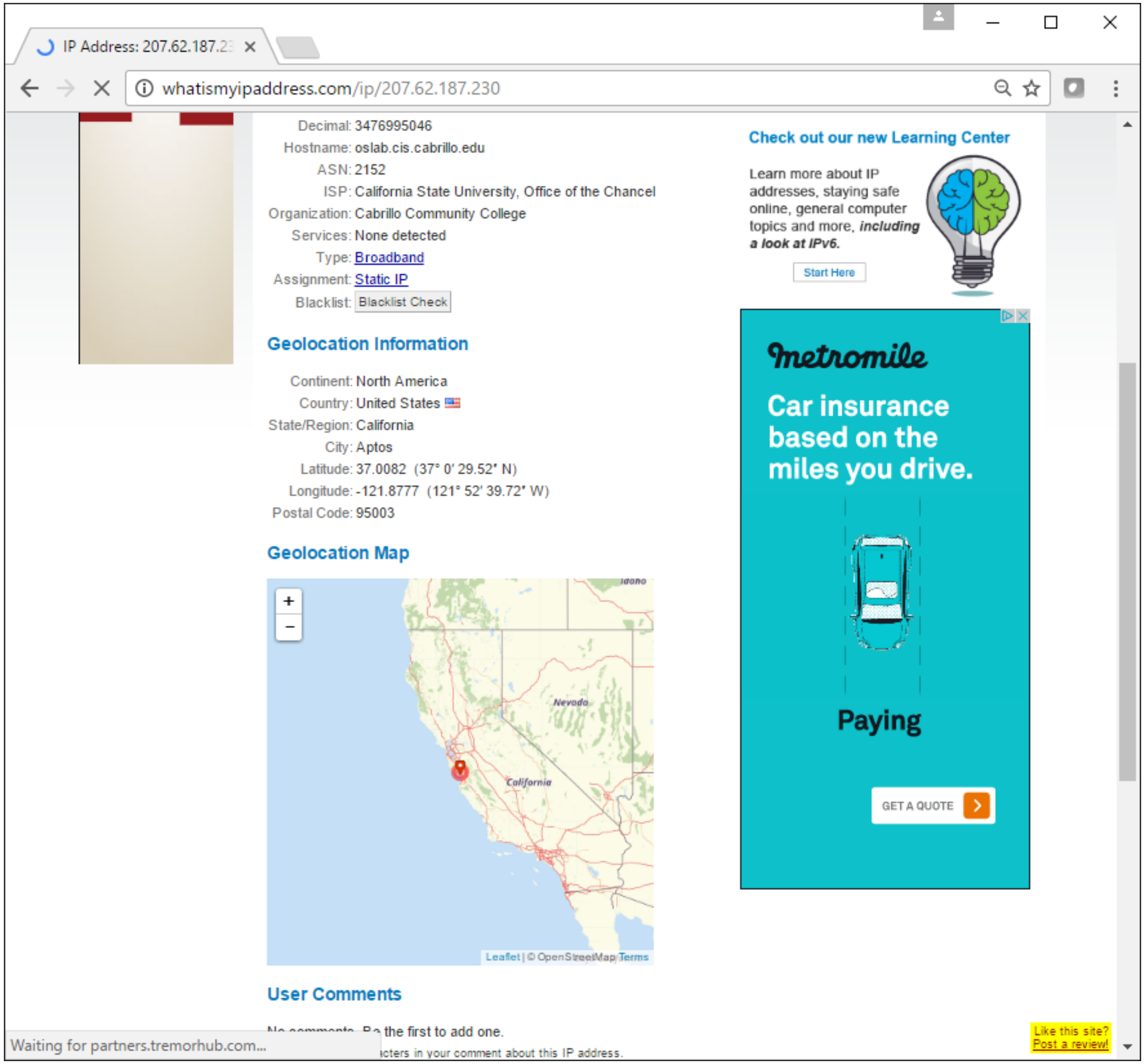
Geolocation Information

Continent: North America
Country: United States
State/Region: California
City: Aptos
Latitude: 37.0082 (37° 0' 29.52" N)
Longitude: -121.8777 (121° 52' 39.72" W)
Postal Code: 95003

Check out our new Learning Center

Learn more about IP addresses, staying safe online, general computer topics and more, ***including a look at IPv6.***

http://whatismyipaddress.com/



Decimal:	3476995046
Hostname:	oslab.cis.cabrillo.edu
ASN:	2152
ISP:	California State University, Office of the Chancel
Organization:	Cabrillo Community College
Services:	None detected
Type:	Broadband
Assignment:	Static IP
Blacklist:	Blacklist Check

Check out our new Learning Center

Learn more about IP addresses, staying safe online, general computer topics and more, *including a look at IPv6.*

Start Here

Geolocation Information

Continent:	North America
Country:	United States
State/Region:	California
City:	Aptos
Latitude:	37.0082 (37° 0' 29.52" N)
Longitude:	-121.8777 (121° 52' 39.72" W)
Postal Code:	95003

Geolocation Map

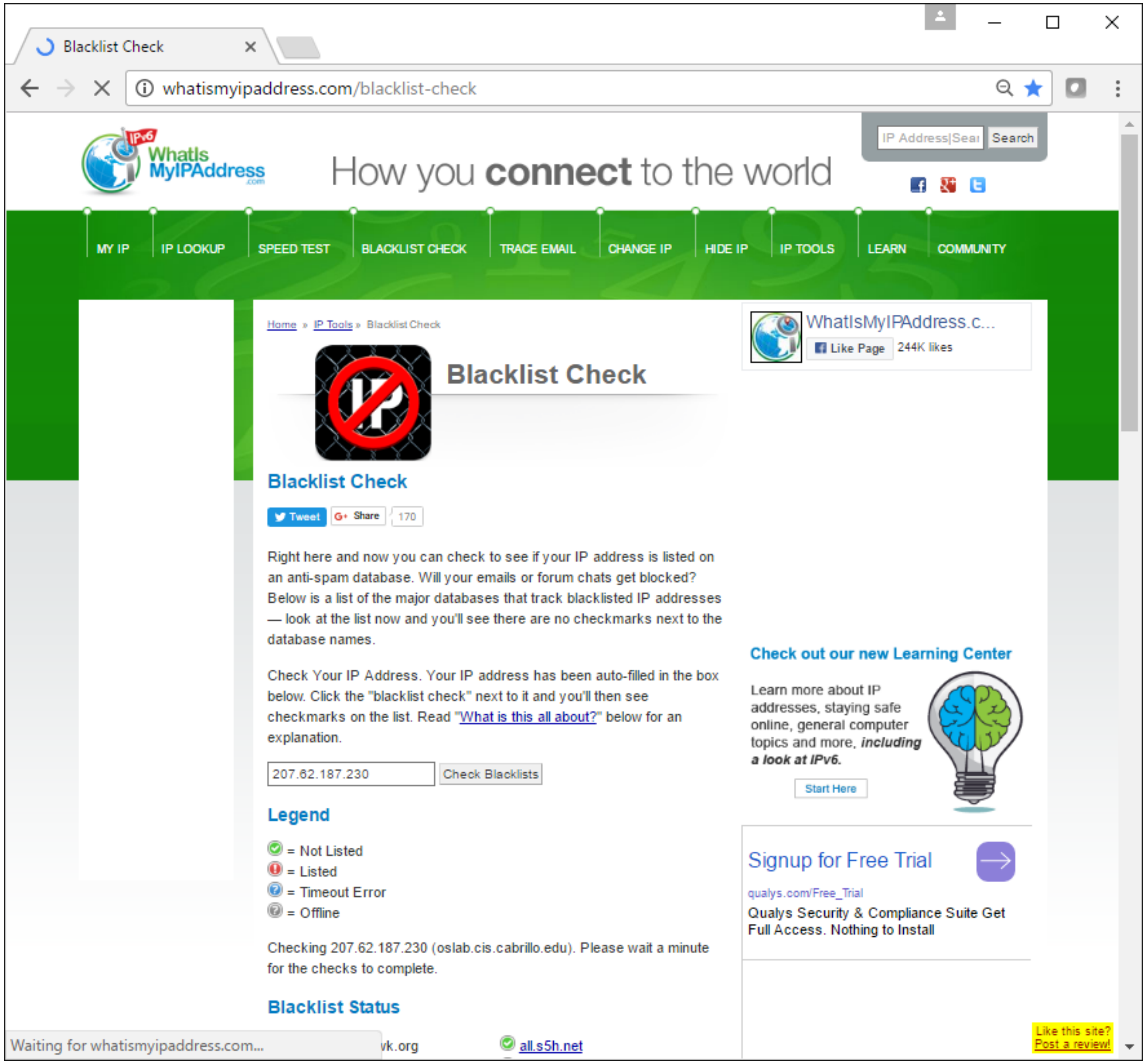
User Comments

No comments. Be the first to add one.

cters in your comment about this IP address.

Like this site? Post a review!
Waiting for partners.tremorhub.com...

http://whatismyipaddress.com/



Blacklist Check

Blacklist Check

Right here and now you can check to see if your IP address is listed on an anti-spam database. Will your emails or forum chats get blocked? Below is a list of the major databases that track blacklisted IP addresses — look at the list now and you'll see there are no checkmarks next to the database names.

Check Your IP Address. Your IP address has been auto-filled in the box below. Click the "blacklist check" next to it and you'll then see checkmarks on the list. Read "What is this all about?" below for an explanation.

207.62.187.230

Legend

✓ = Not Listed
❗ = Listed
? = Timeout Error
● = Offline

Checking 207.62.187.230 (oslab.cis.cabrillo.edu). Please wait a minute for the checks to complete.

Blacklist Status

vk.org ✓ all.s5h.net

Check out our new Learning Center

Learn more about IP addresses, staying safe online, general computer topics and more, ***including a look at IPv6.***

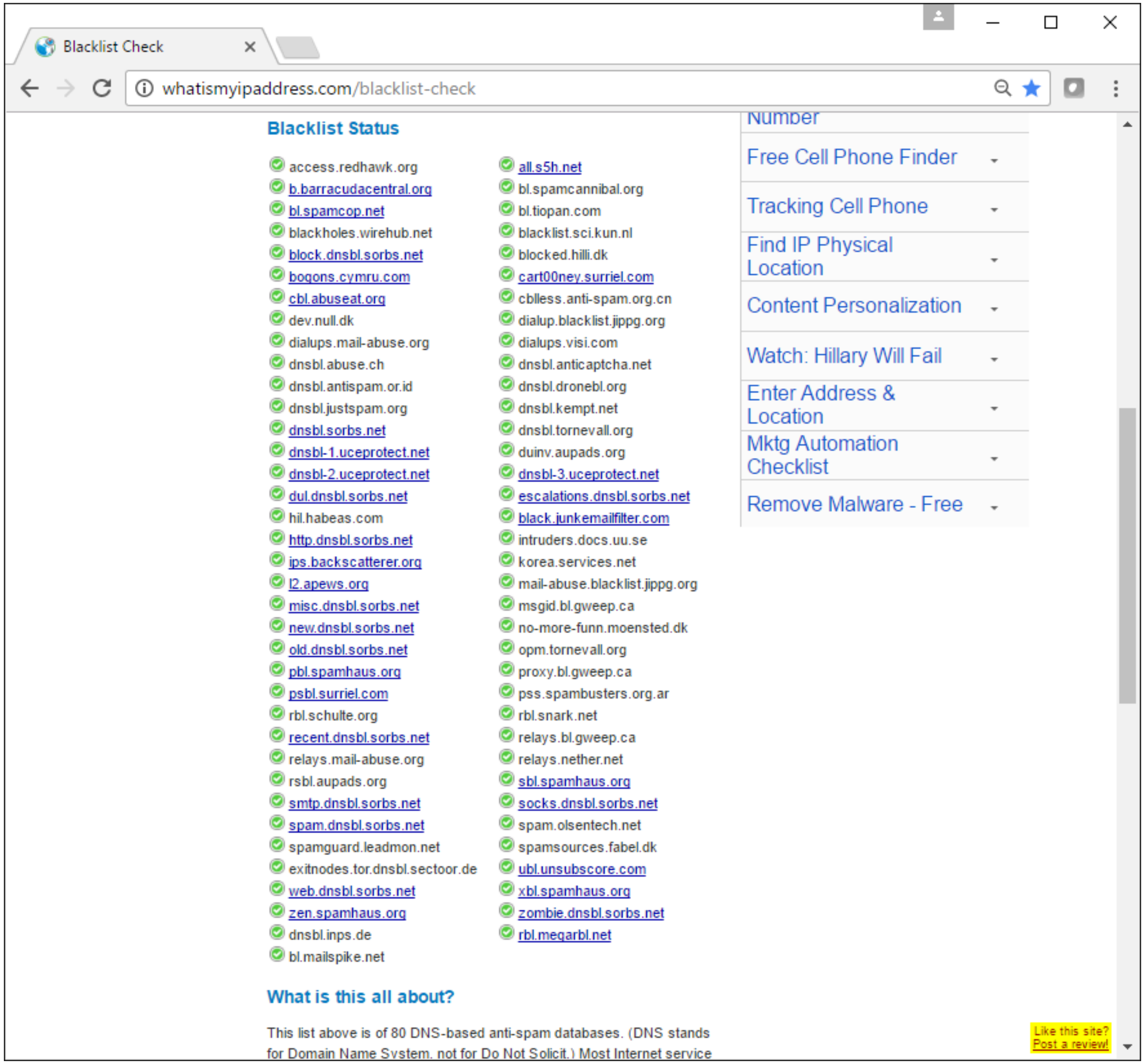
Signup for Free Trial

qualys.com/Free_Trial

Qualys Security & Compliance Suite Get Full Access. Nothing to Install

Waiting for whatismyipaddress.com...

http://whatismyipaddress.com/



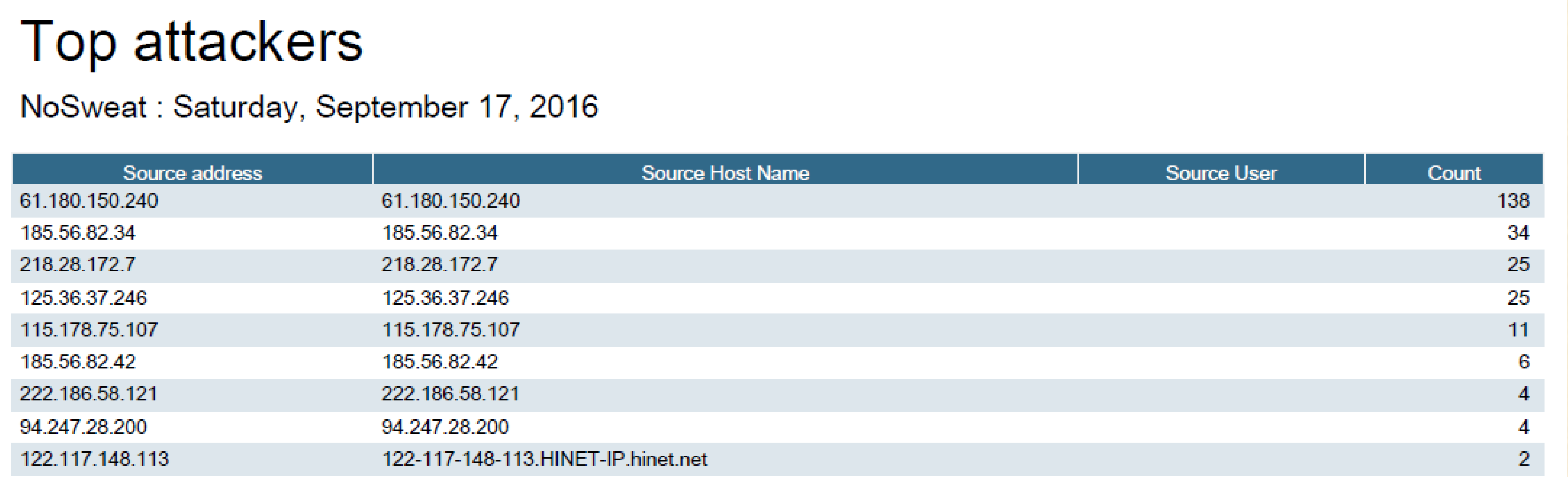
Blacklist Status

- ✓ access.redhawk.org
- ✓ b.barracudacentral.org
- ✓ bl.spamcop.net
- ✓ blackholes.wirehub.net
- ✓ block.dnsbl.sorbs.net
- ✓ bogons.cymru.com
- ✓ cbl.abuseat.org
- ✓ dev.null.dk
- ✓ dialups.mail-abuse.org
- ✓ dnsbl.abuse.ch
- ✓ dnsbl.antispam.or.id
- ✓ dnsbl.justspam.org
- ✓ dnsbl.sorbs.net
- ✓ dnsbl-1.uceprotect.net
- ✓ dnsbl-2.uceprotect.net
- ✓ dul.dnsbl.sorbs.net
- ✓ hil.habeas.com
- ✓ http.dnsbl.sorbs.net
- ✓ ips.backscatterer.org
- ✓ l2.apews.org
- ✓ misc.dnsbl.sorbs.net
- ✓ new.dnsbl.sorbs.net
- ✓ old.dnsbl.sorbs.net
- ✓ pbl.spamhaus.org
- ✓ psbl.surriel.com
- ✓ rbl.schulte.org
- ✓ recent.dnsbl.sorbs.net
- ✓ relays.mail-abuse.org
- ✓ rsbl.aupads.org
- ✓ smtp.dnsbl.sorbs.net
- ✓ spam.dnsbl.sorbs.net
- ✓ spamguard.leadmon.net
- ✓ exitnodes.tor.dnsbl.sectoor.de
- ✓ web.dnsbl.sorbs.net
- ✓ zen.spamhaus.org
- ✓ dnsbl.inps.de
- ✓ bl.mailspike.net
- ✓ all.s5h.net
- ✓ bl.spamcannibal.org
- ✓ bl.tiopan.com
- ✓ blacklist.sci.kun.nl
- ✓ blocked.hilli.dk
- ✓ cart00ney.surriel.com
- ✓ cblless.anti-spam.org.cn
- ✓ dialup.blacklist.jippg.org
- ✓ dialups.visi.com
- ✓ dnsbl.anticaptcha.net
- ✓ dnsbl.dronebl.org
- ✓ dnsbl.kempt.net
- ✓ dnsbl.tornevall.org
- ✓ duinv.aupads.org
- ✓ dnsbl-3.uceprotect.net
- ✓ escalations.dnsbl.sorbs.net
- ✓ black.junkemailfilter.com
- ✓ intruders.docs.uu.se
- ✓ korea.services.net
- ✓ mail-abuse.blacklist.jippg.org
- ✓ msgid.bl.gweep.ca
- ✓ no-more-funn.moensted.dk
- ✓ opm.tornevall.org
- ✓ proxy.bl.gweep.ca
- ✓ pss.spambusters.org.ar
- ✓ rbl.snark.net
- ✓ relays.bl.gweep.ca
- ✓ relays.nether.net
- ✓ sbl.spamhaus.org
- ✓ socks.dnsbl.sorbs.net
- ✓ spam.olsentech.net
- ✓ spamsources.fabel.dk
- ✓ ubl.unsubscore.com
- ✓ xbl.spamhaus.org
- ✓ zombie.dnsbl.sorbs.net
- ✓ rbl.megarbl.net

What is this all about?

This list above is of 80 DNS-based anti-spam databases. (DNS stands for Domain Name System, not for Do Not Solicit.) Most Internet service

Activity



Top attackers

NoSweat : Saturday, September 17, 2016

Source address	Source Host Name	Source User	Count
61.180.150.240	61.180.150.240		138
185.56.82.34	185.56.82.34		34
218.28.172.7	218.28.172.7		25
125.36.37.246	125.36.37.246		25
115.178.75.107	115.178.75.107		11
185.56.82.42	185.56.82.42		6
222.186.58.121	222.186.58.121		4
94.247.28.200	94.247.28.200		4
122.117.148.113	122-117-148-113.HINET-IP.hinet.net		2

Pick one of the IP addresses above and find out who it was assigned to and whether it is blacklisted.

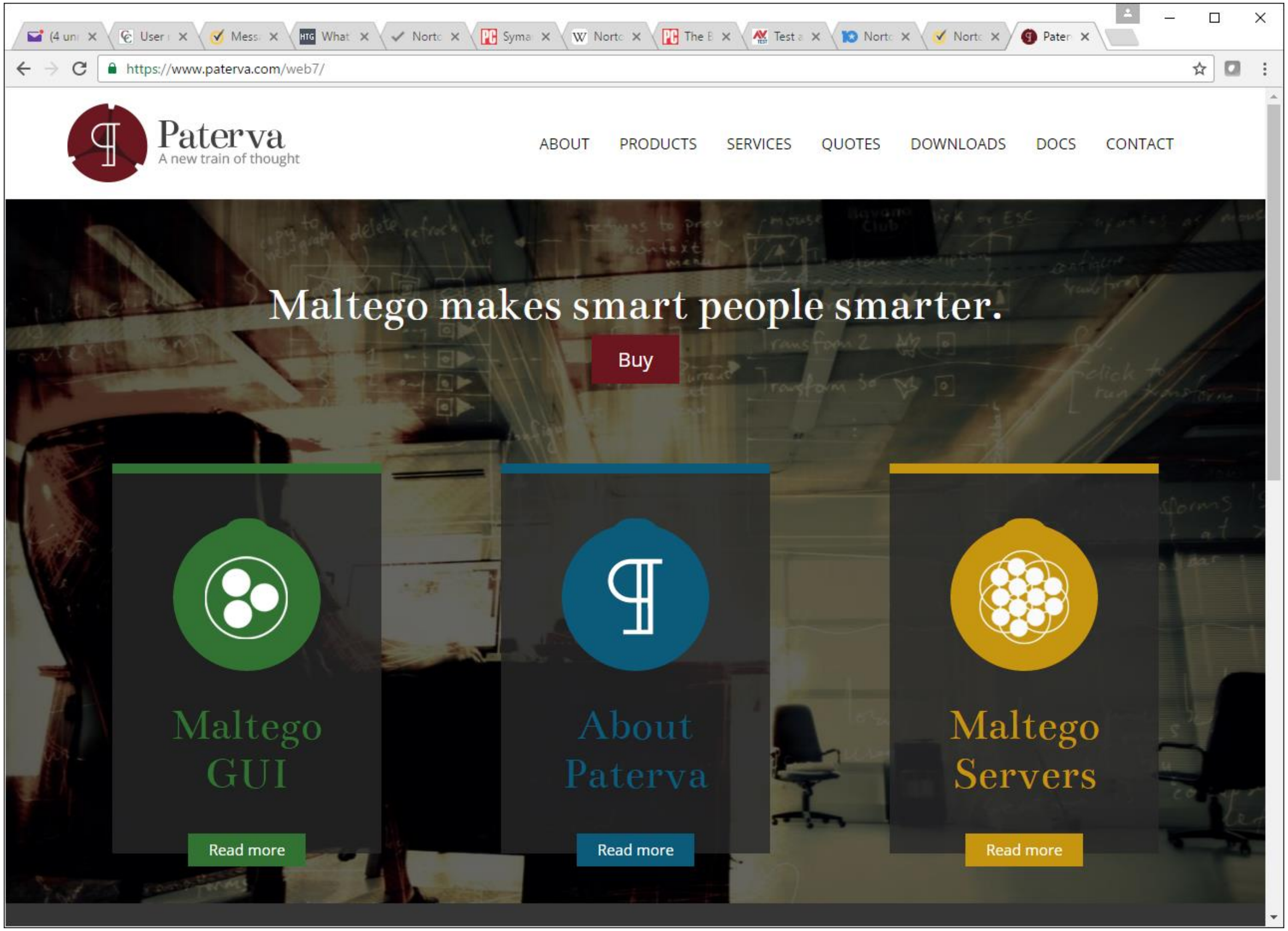
Put the organization name, country, and number of times blacklisted in the chat window.

Maltego

Maltego

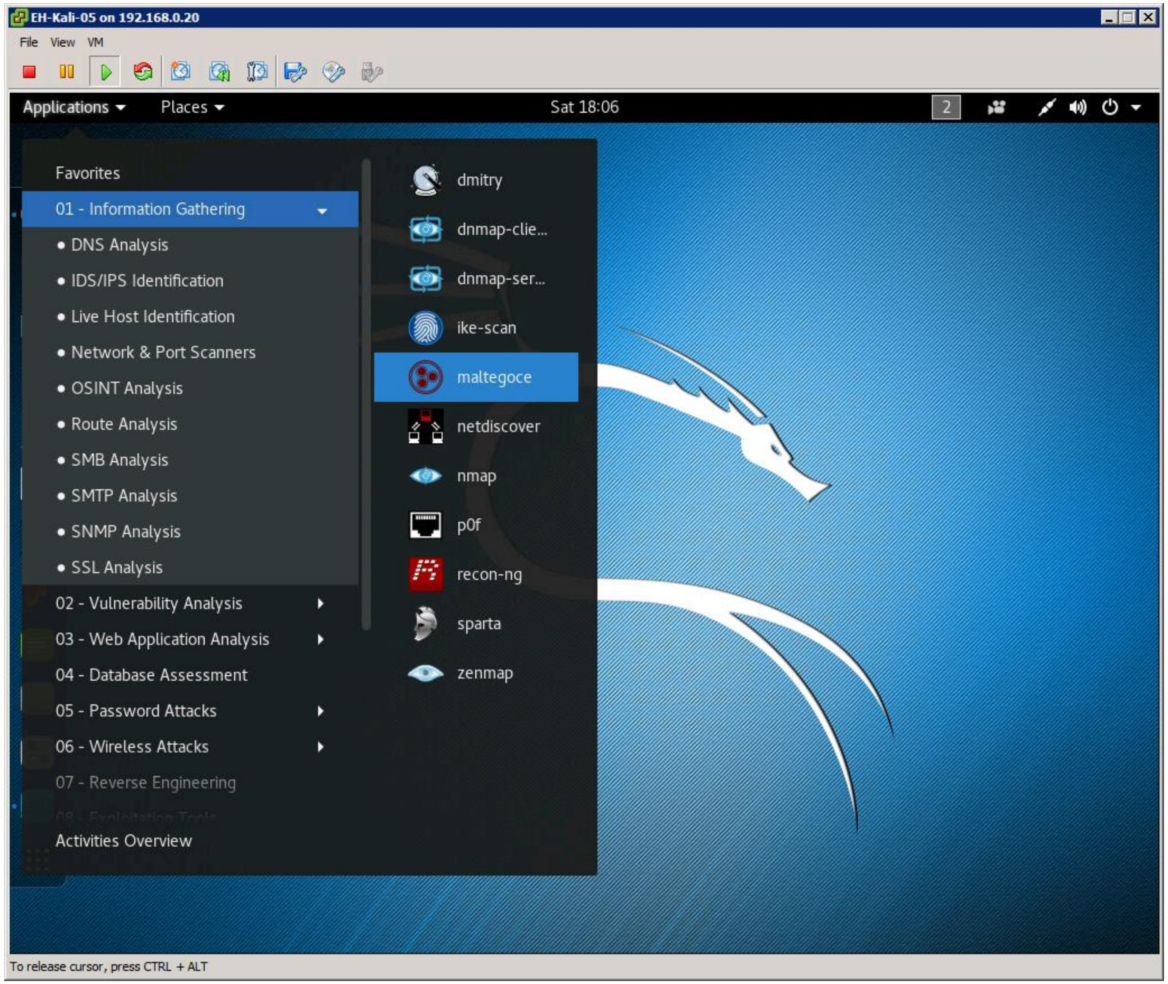
The community edition is a free version of the commercial client Maltego with various limitations.
Limitations :
- Maximum of 12 results per transform
- You need to register on our website to use the client
- API keys expire every couple of days
- Runs on a (slower) server that is shared with all community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

Maltego



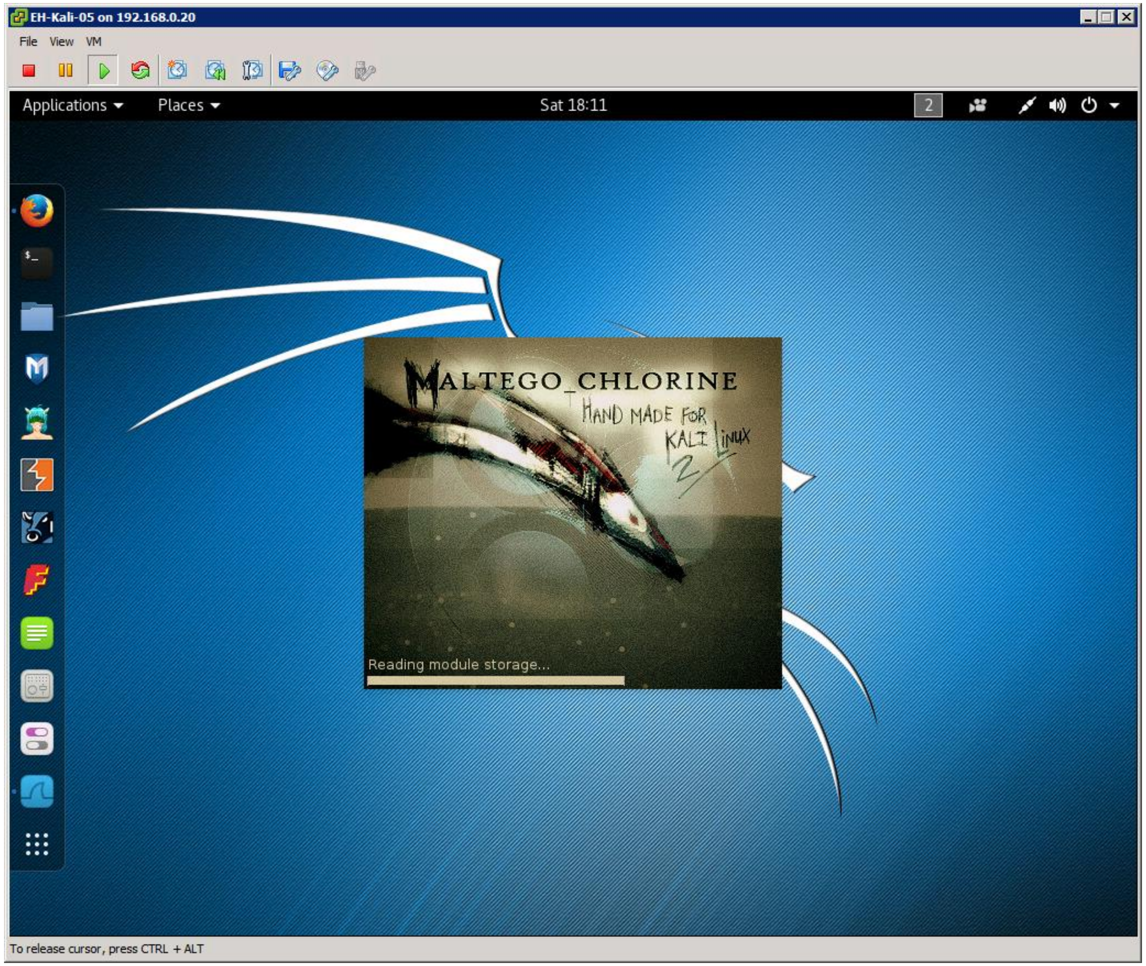
https://www.paterva.com/web7/

Maltego



Applications > 01-Information Gathering > maltegoce

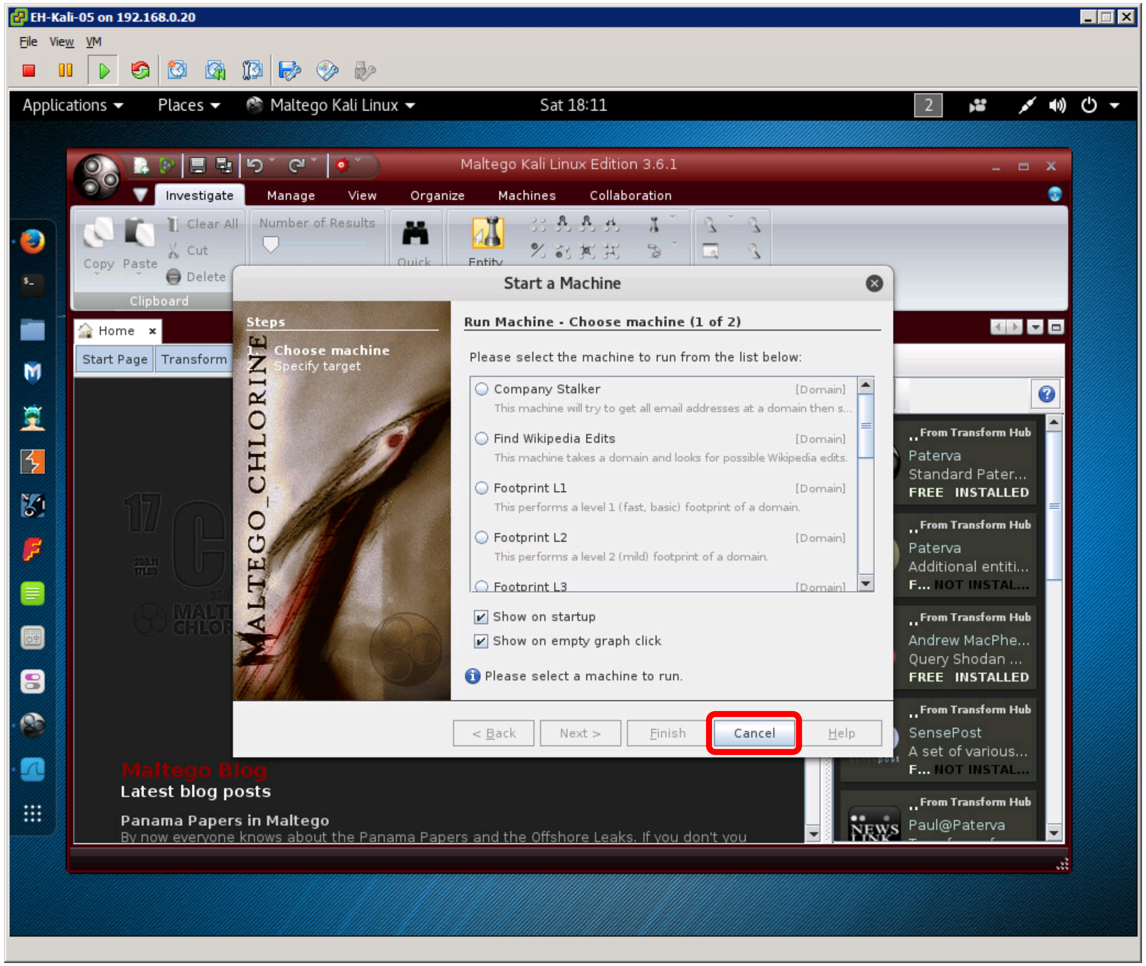
Maltego


EH-Kali-05 on 192.168.0.20
File View VM
Applications
Places
Sat 18:11
2
MALTEGO CHLORINE
HAND MADE FOR KALI LINUX 2

Reading module storage...

To release cursor, press CTRL + ALT

Maltego



Start a Machine

Steps

1. Choose machine
2. Specify target

Run Machine - Choose machine (1 of 2)

Please select the machine to run from the list below:

○ Company Stalker [Domain]
This machine will try to get all email addresses at a domain then s...

○ Find Wikipedia Edits [Domain]
This machine takes a domain and looks for possible Wikipedia edits.

○ Footprint L1 [Domain]
This performs a level 1 (fast, basic) footprint of a domain.

○ Footprint L2 [Domain]
This performs a level 2 (mild) footprint of a domain.

○ Footprint L3 [Domain]

☑ Show on startup

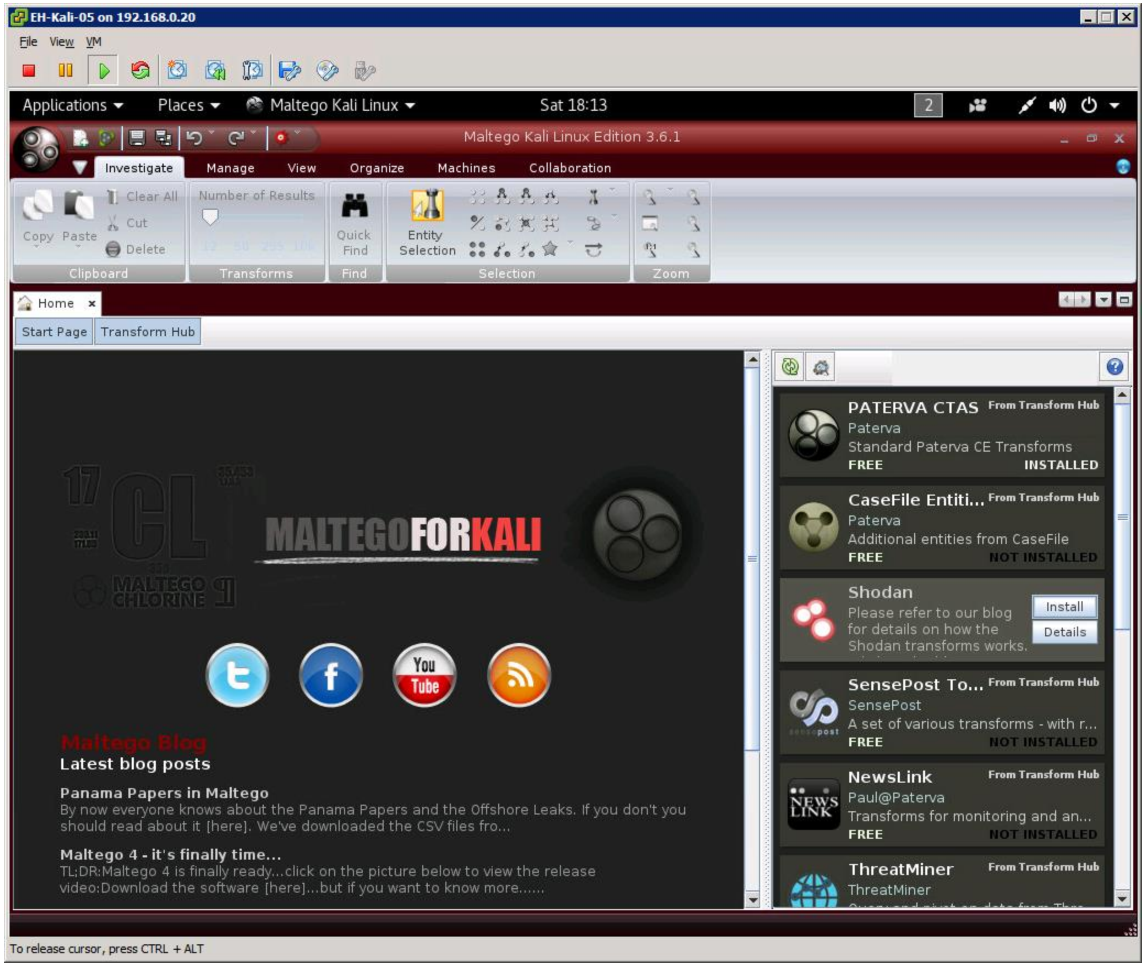
☑ Show on empty graph click

Please select a machine to run.

< Back | Next > | Finish | Cancel | Help

Click Cancel.

Maltego


EH-Kali-05 on 192.168.0.20
File View VM
Applications Places Maltego Kali Linux Sat 18:13
Maltego Kali Linux Edition 3.6.1
Investigate Manage View Organize Machines Collaboration
Copy Paste Clear All Cut Delete Clipboard
Number of Results Transforms
Quick Find Find
Entity Selection Selection
Zoom
Home
Start Page Transform Hub
MALTEGOFORKALI
MALTEGO CHLORINE
Install
Details
To release cursor, press CTRL + ALT

PATERVA CTAS From Transform Hub
Paterva
Standard Paterva CE Transforms
FREE INSTALLED

CaseFile Entiti... From Transform Hub
Paterva
Additional entities from CaseFile
FREE NOT INSTALLED

Shodan
Please refer to our blog for details on how the Shodan transforms works.

SensePost To... From Transform Hub
SensePost
A set of various transforms - with r...
FREE NOT INSTALLED

NewsLink From Transform Hub
Paul@Paterva
Transforms for monitoring and an...
FREE NOT INSTALLED

ThreatMiner From Transform Hub
ThreatMiner

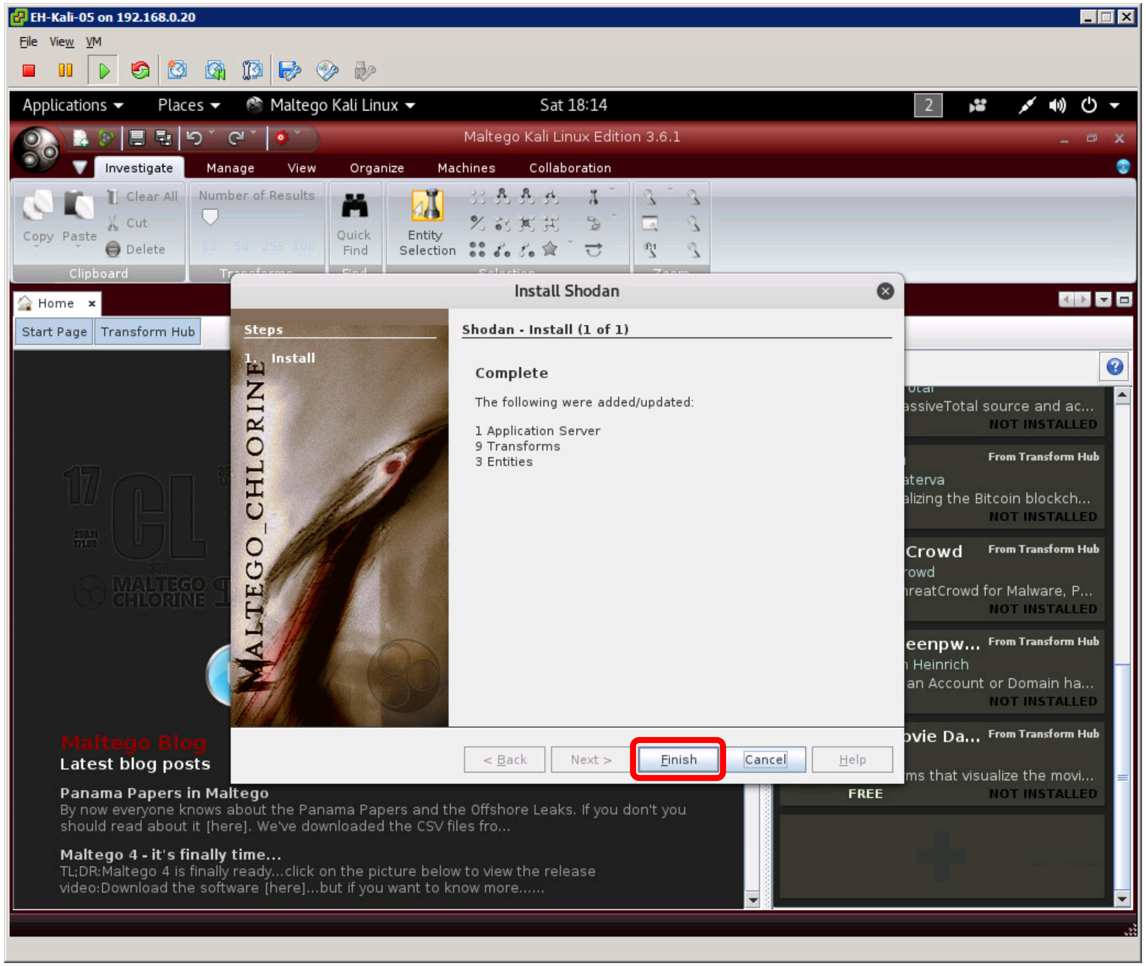
Maltego Blog
Latest blog posts

Panama Papers in Maltego
By now everyone knows about the Panama Papers and the Offshore Leaks. If you don't you should read about it [here]. We've downloaded the CSV files fro...

Maltego 4 - it's finally time...
TL;DR:Maltego 4 is finally ready...click on the picture below to view the release video:Download the software [here]...but if you want to know more......

Install Shodan transform

Maltego


EH-Kali-05 on 192.168.0.20
File View VM
Applications Places Maltego Kali Linux Sat 18:14
Maltego Kali Linux Edition 3.6.1
Investigate Manage View Organize Machines Collaboration
Copy Paste Clear All Cut Delete Clipboard
Number of Results Transforms
Quick Find
Entity Selection
Home
Start Page Transform Hub
Steps
1. Install
MALTEGO_CHLORINE
< Back Next > Finish Cancel Help
From Transform Hub
NOT INSTALLED
FREE

Install Shodan

Shodan - Install (1 of 1)

Complete

The following were added/updated:

1 Application Server
9 Transforms
3 Entities

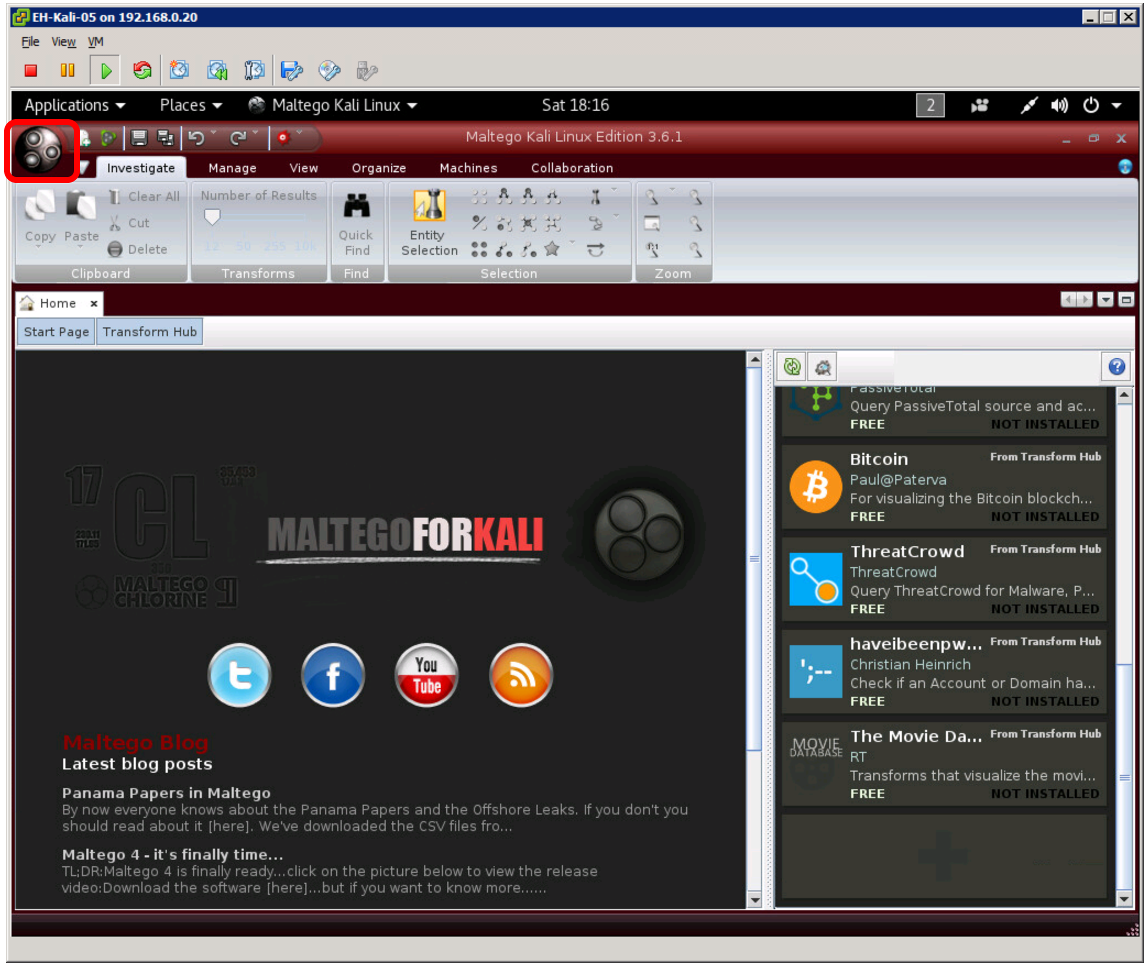
Maltego Blog
Latest blog posts

Panama Papers in Maltego
By now everyone knows about the Panama Papers and the Offshore Leaks. If you don't you should read about it [here]. We've downloaded the CSV files fro...

Maltego 4 - it's finally time...
TL;DR:Maltego 4 is finally ready...click on the picture below to view the release video:Download the software [here]...but if you want to know more......

Click Finish.

Maltego


EH-Kali-05 on 192.168.0.20
File View VM
Applications Places Maltego Kali Linux Sat 18:16
Maltego Kali Linux Edition 3.6.1
Investigate Manage View Organize Machines Collaboration
Copy Paste Clear All Cut Delete Clipboard
Number of Results Transforms
Quick Find Find
Entity Selection Selection
Zoom
Home
Start Page Transform Hub
MALTEGOFORKALI
MALTEGO CHLORINE

Maltego Blog
Latest blog posts

Panama Papers in Maltego
By now everyone knows about the Panama Papers and the Offshore Leaks. If you don't you should read about it [here]. We've downloaded the CSV files fro...

Maltego 4 - it's finally time...
TL;DR:Maltego 4 is finally ready...click on the picture below to view the release video:Download the software [here]...but if you want to know more......

PassiveTotal
Query PassiveTotal source and ac...
FREE NOT INSTALLED

Bitcoin From Transform Hub
Paul@Paterva
For visualizing the Bitcoin blockch...
FREE NOT INSTALLED

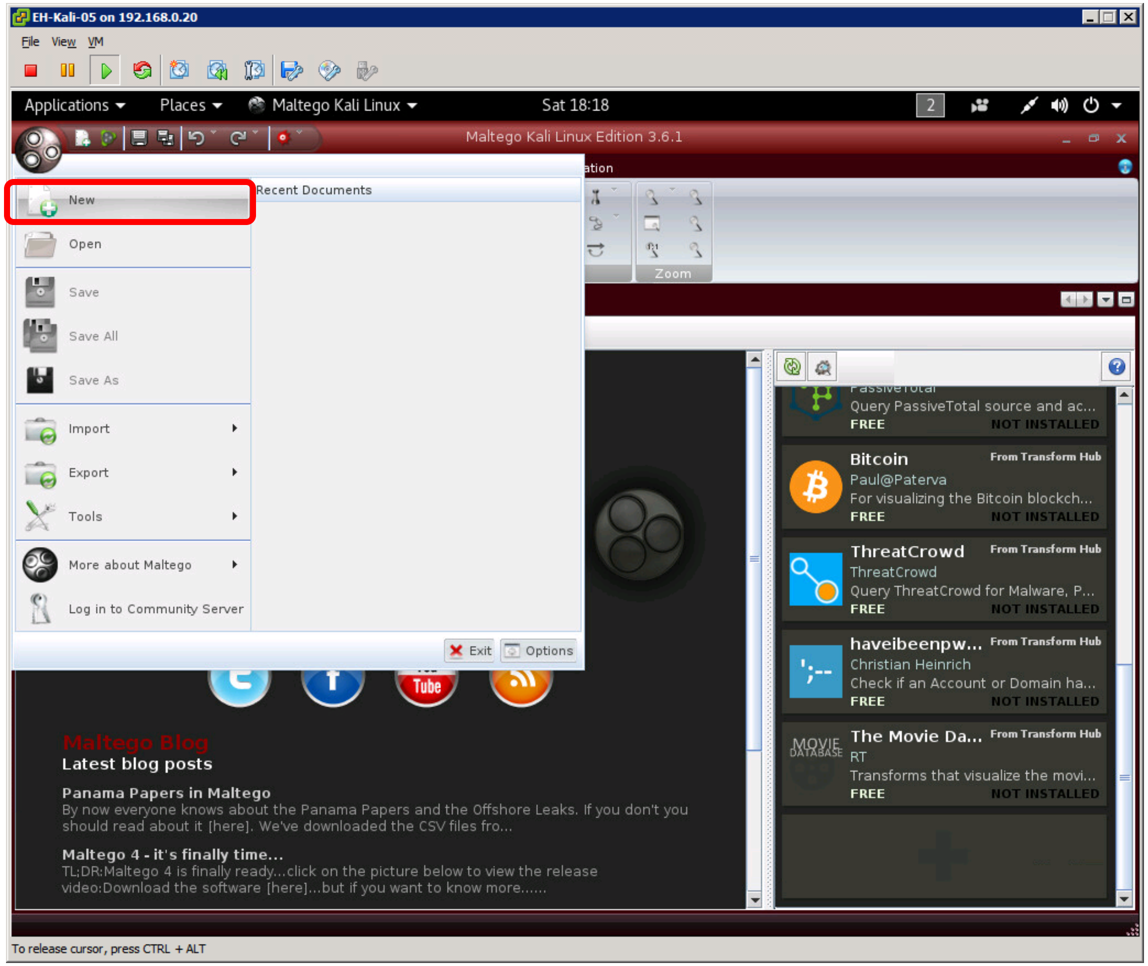
ThreatCrowd From Transform Hub
ThreatCrowd
Query ThreatCrowd for Malware, P...
FREE NOT INSTALLED

haveibeenpw... From Transform Hub
Christian Heinrich
Check if an Account or Domain ha...
FREE NOT INSTALLED

The Movie Da... From Transform Hub
RT
Transforms that visualize the movi...
FREE NOT INSTALLED

Click main Maltego icon.

Maltego

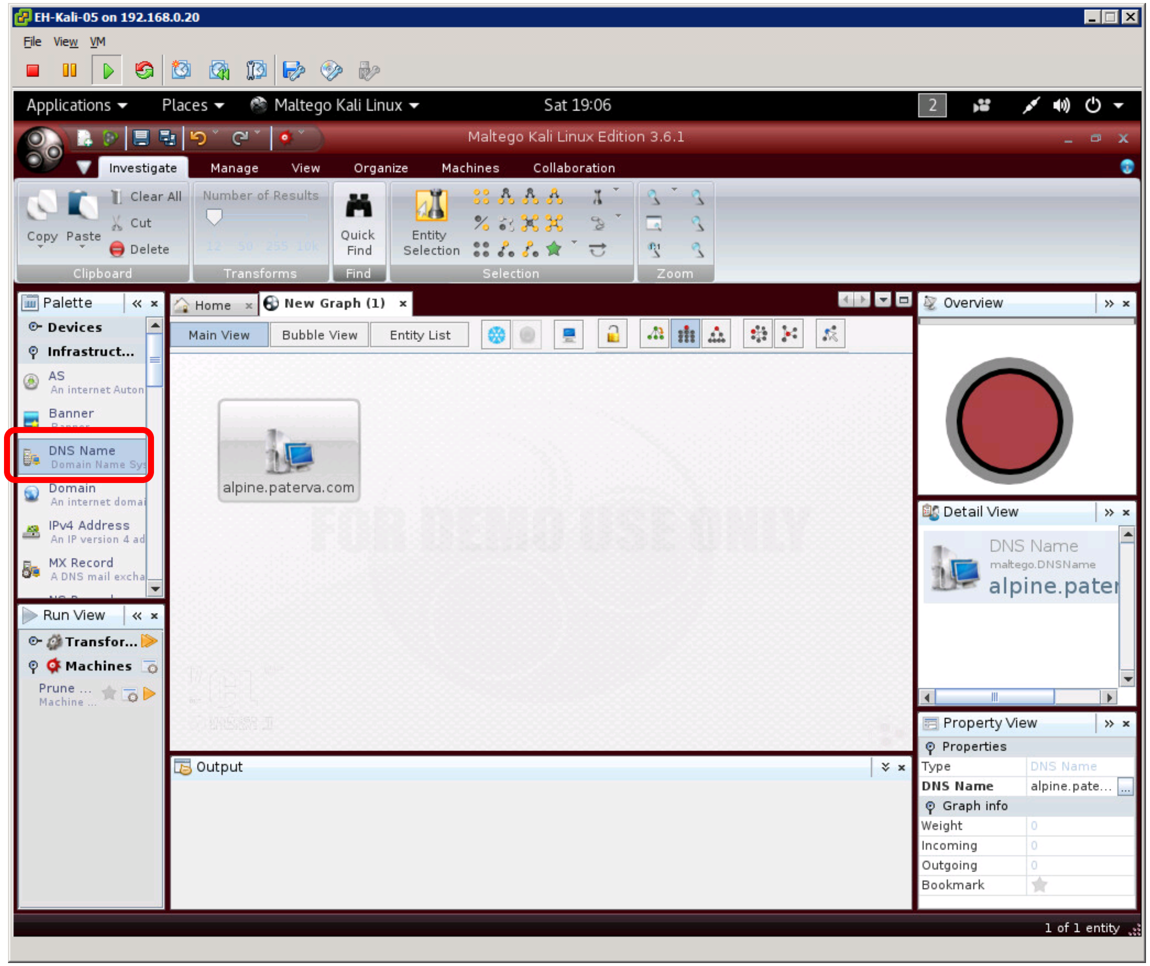


Panama Papers in Maltego
By now everyone knows about the Panama Papers and the Offshore Leaks. If you don't you should read about it [here]. We've downloaded the CSV files fro...

Maltego 4 - it's finally time...
TL;DR:Maltego 4 is finally ready...click on the picture below to view the release video:Download the software [here]...but if you want to know more......

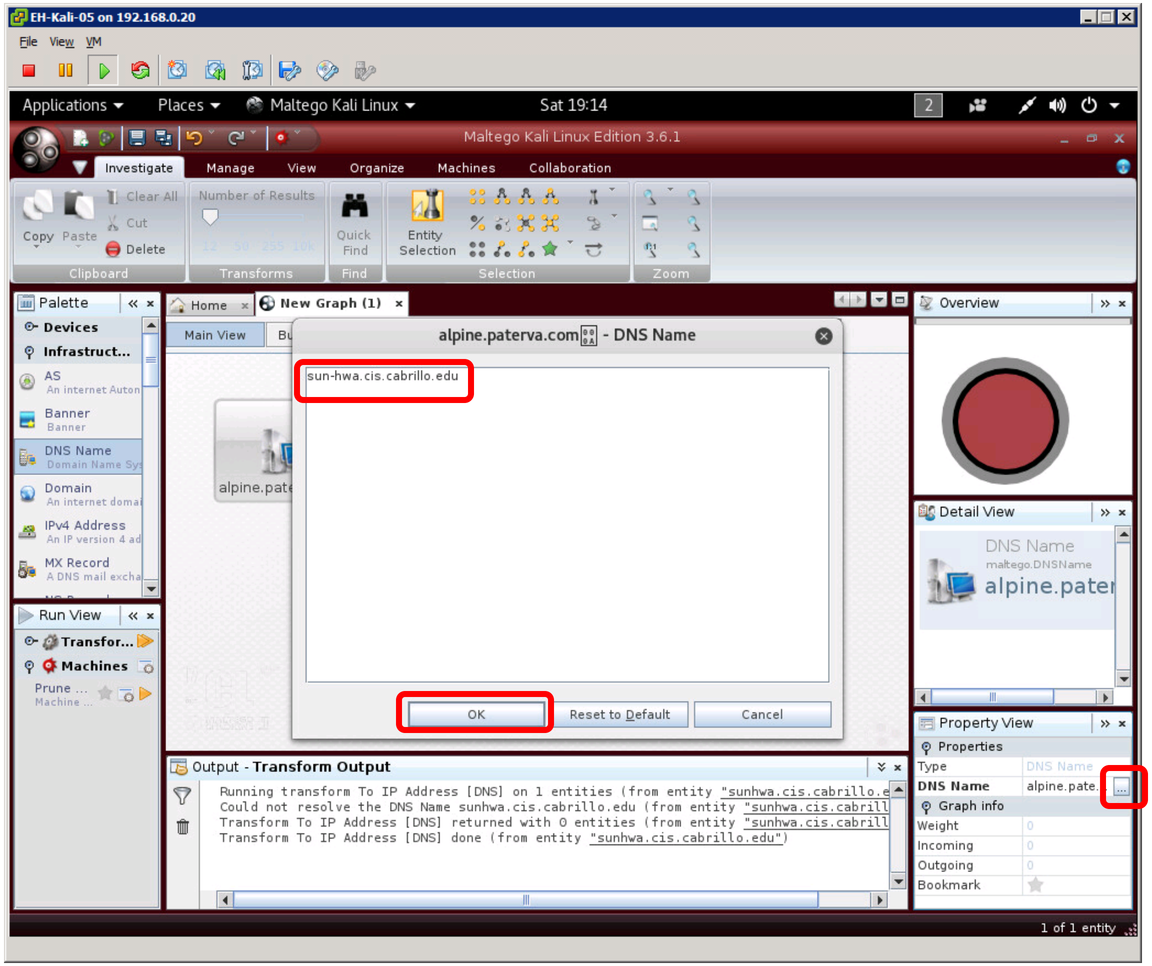
Select New.

Maltego



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

Maltego



alpine.paterva.com - DNS Name

sun-hwa.cis.cabrillo.edu

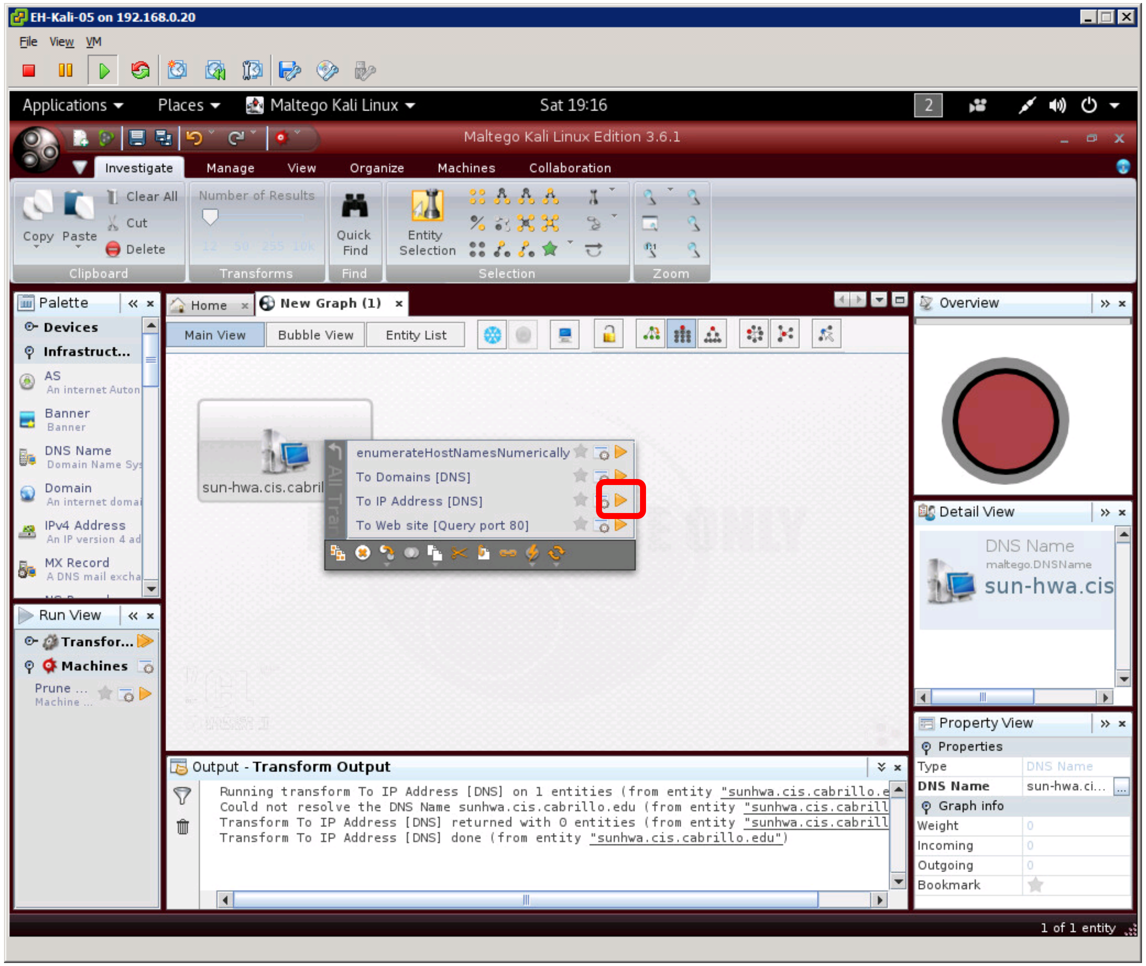
OK | Reset to Default | Cancel

Output - Transform Output

```
Running transform To IP Address [DNS] on 1 entities (from entity "sunhwa.cis.cabrillo.e
Could not resolve the DNS Name sunhwa.cis.cabrillo.edu (from entity "sunhwa.cis.cabrill
Transform To IP Address [DNS] returned with 0 entities (from entity "sunhwa.cis.cabrill
Transform To IP Address [DNS] done (from entity "sunhwa.cis.cabrillo.edu")
```

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

Maltego

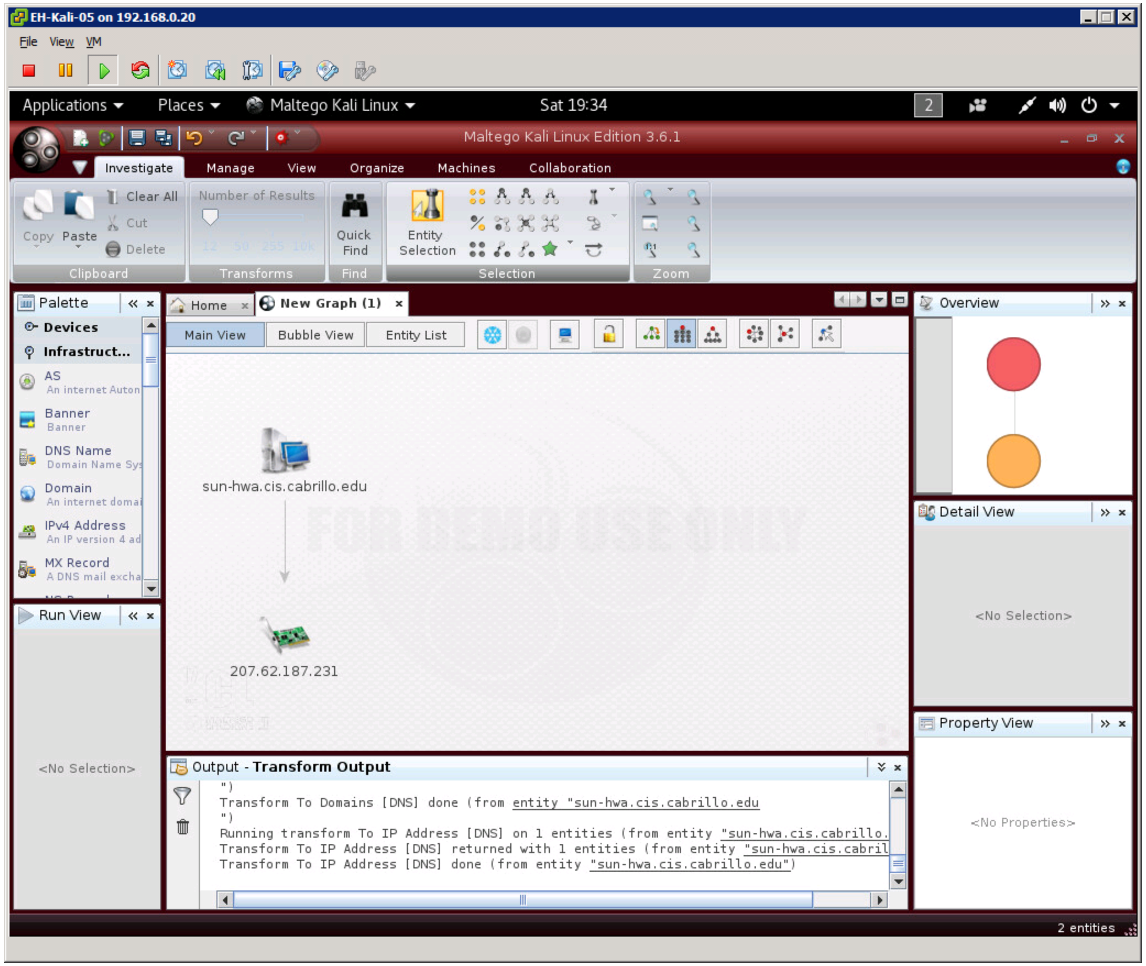


Output - Transform Output

```
Running transform To IP Address [DNS] on 1 entities (from entity "sunhwa.cis.cabrillo.e
Could not resolve the DNS Name sunhwa.cis.cabrillo.edu (from entity "sunhwa.cis.cabrill
Transform To IP Address [DNS] returned with 0 entities (from entity "sunhwa.cis.cabrill
Transform To IP Address [DNS] done (from entity "sunhwa.cis.cabrillo.edu")
```

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

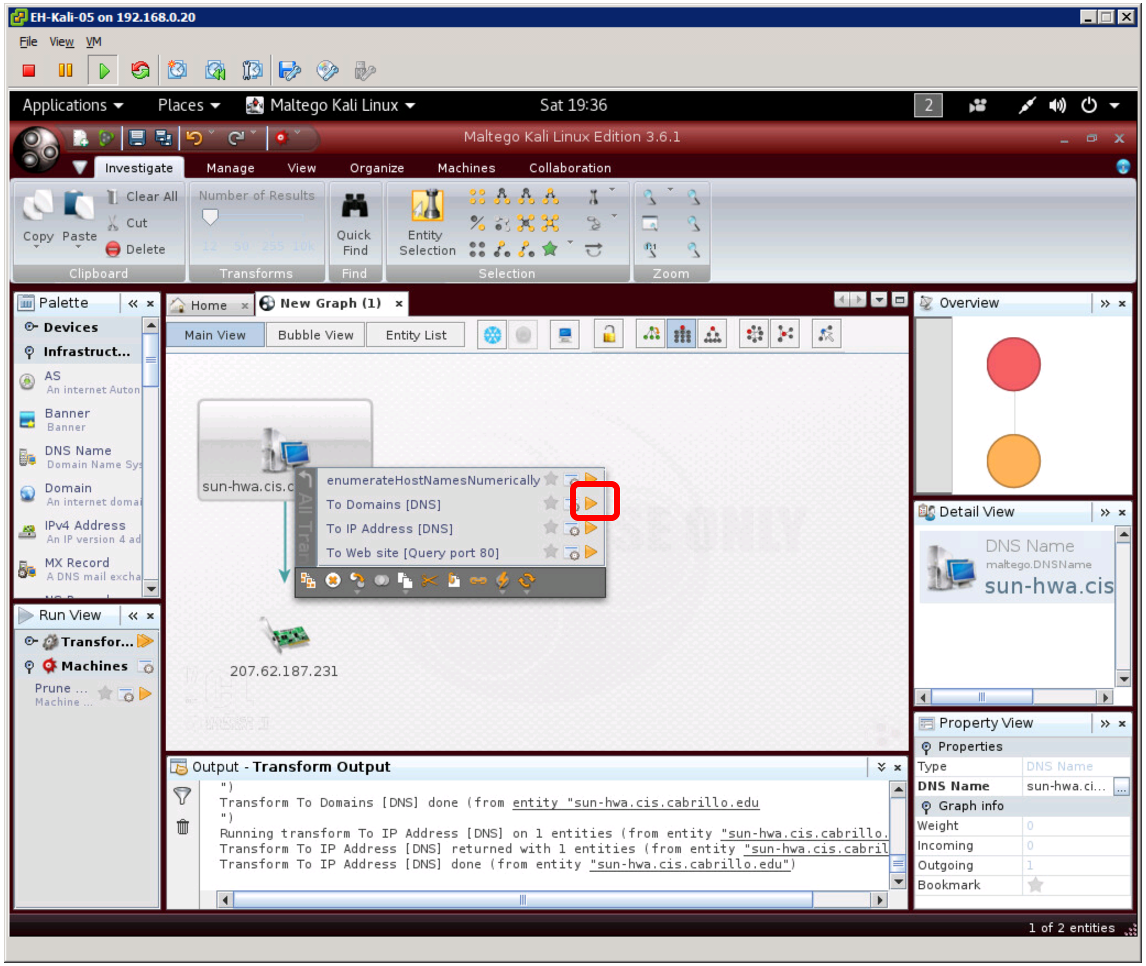
Maltego


EH-Kali-05 on 192.168.0.20
File View VM
Applications Places Maltego Kali Linux Sat 19:34
Maltego Kali Linux Edition 3.6.1
Investigate Manage View Organize Machines Collaboration
Copy Paste Clear All Cut Delete Clipboard
Number of Results Transforms
Quick Find Find
Entity Selection Selection
Zoom
Palette
Devices
Infrastruct...
AS An internet Auton
Banner Banner
DNS Name Domain Name Sys
Domain An internet domai
IPv4 Address An IP version 4 ad
MX Record A DNS mail excha
Run View
<No Selection>
Home New Graph (1)
Main View Bubble View Entity List
sun-hwa.cis.cabrillo.edu
FOR DEMO USE ONLY
207.62.187.231
Overview
Detail View
<No Selection>
Property View
<No Properties>
Output - Transform Output
2 entities

```
")
Transform To Domains [DNS] done (from entity "sun-hwa.cis.cabrillo.edu
")
Running transform To IP Address [DNS] on 1 entities (from entity "sun-hwa.cis.cabrillo.
Transform To IP Address [DNS] returned with 1 entities (from entity "sun-hwa.cis.cabril
Transform To IP Address [DNS] done (from entity "sun-hwa.cis.cabrillo.edu")
```

The IP address shows now below the little NIC icon.

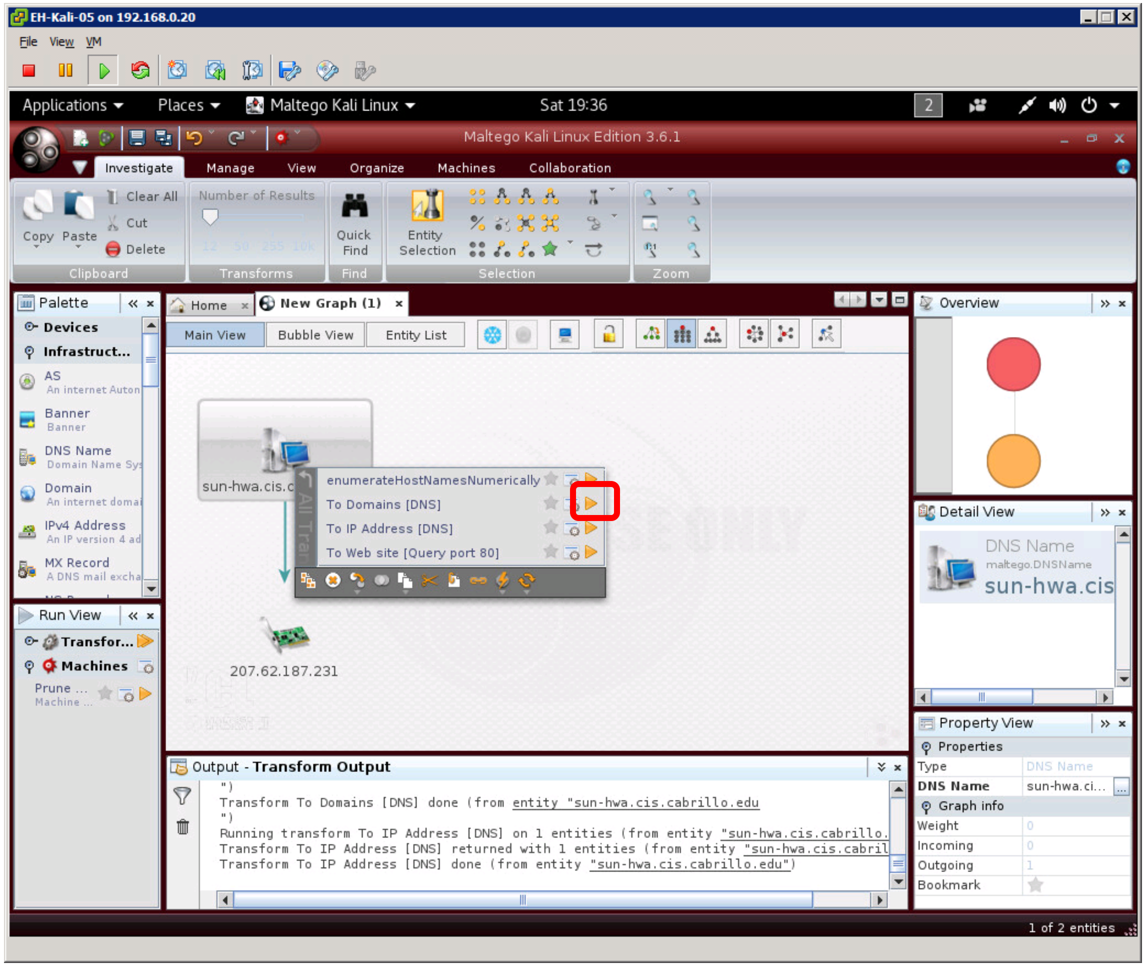
Maltego


EH-Kali-05 on 192.168.0.20
File View VM
Applications Places Maltego Kali Linux Sat 19:36
Maltego Kali Linux Edition 3.6.1
Investigate Manage View Organize Machines Collaboration
Copy Paste Clear All Cut Delete Clipboard
Number of Results Transforms
Quick Find Find
Entity Selection Selection
Zoom
Palette Devices Infrastruct... AS Banner DNS Name Domain IPv4 Address MX Record
Run View Transfor... Machines Prune ...
Home New Graph (1)
Main View Bubble View Entity List
sun-hwa.cis.c
enumerateHostNamesNumerically
To Domains [DNS]
To IP Address [DNS]
To Web site [Query port 80]
207.62.187.231
Overview
Detail View
DNS Name
maltego.DNSName
sun-hwa.cis
Property View
Properties
Type DNS Name
DNS Name sun-hwa.ci...
Graph info
Weight 0
Incoming 0
Outgoing 1
Bookmark
1 of 2 entities
Output - Transform Output

```
")
Transform To Domains [DNS] done (from entity "sun-hwa.cis.cabrillo.edu
")
Running transform To IP Address [DNS] on 1 entities (from entity "sun-hwa.cis.cabrillo.
Transform To IP Address [DNS] returned with 1 entities (from entity "sun-hwa.cis.cabril
Transform To IP Address [DNS] done (from entity "sun-hwa.cis.cabrillo.edu")
```

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

Maltego


EH-Kali-05 on 192.168.0.20
File View VM
Applications Places Maltego Kali Linux Sat 19:36
Maltego Kali Linux Edition 3.6.1
Investigate Manage View Organize Machines Collaboration
Copy Paste Clear All Cut Delete Clipboard
Number of Results Transforms
Quick Find Find
Entity Selection Selection
Zoom
Palette
Devices
Infrastruct...
AS
Banner
DNS Name
Domain
IPv4 Address
MX Record
Run View
Transfor...
Machines
Prune ...
Home
New Graph (1)
Main View Bubble View Entity List
sun-hwa.cis.c
enumerateHostNamesNumerically
To Domains [DNS]
To IP Address [DNS]
To Web site [Query port 80]
207.62.187.231
Overview
Detail View
DNS Name
maltego.DNSName
sun-hwa.cis
Property View
1 of 2 entities

Output - **Transform Output**

```
")
Transform To Domains [DNS] done (from entity "sun-hwa.cis.cabrillo.edu
")
Running transform To IP Address [DNS] on 1 entities (from entity "sun-hwa.cis.cabrillo.
Transform To IP Address [DNS] returned with 1 entities (from entity "sun-hwa.cis.cabril
Transform To IP Address [DNS] done (from entity "sun-hwa.cis.cabrillo.edu")
```

Properties

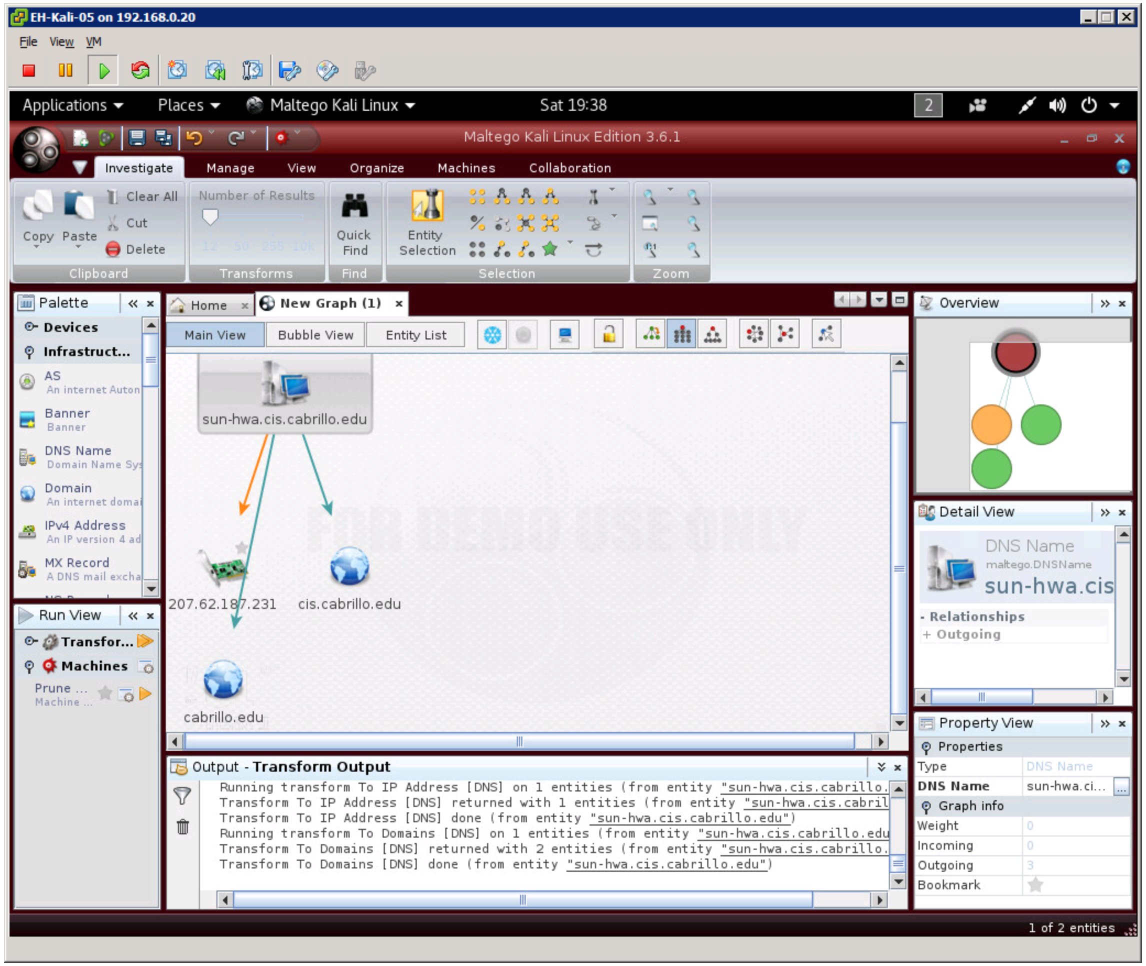
Type	DNS Name
DNS Name	sun-hwa.ci...

Graph info

Weight	0
Incoming	0
Outgoing	1
Bookmark	☆

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

Maltego



Output - Transform Output

```
Running transform To IP Address [DNS] on 1 entities (from entity "sun-hwa.cis.cabrillo.
Transform To IP Address [DNS] returned with 1 entities (from entity "sun-hwa.cis.cabril
Transform To IP Address [DNS] done (from entity "sun-hwa.cis.cabrillo.edu")
Running transform To Domains [DNS] on 1 entities (from entity "sun-hwa.cis.cabrillo.edu
Transform To Domains [DNS] returned with 2 entities (from entity "sun-hwa.cis.cabrillo.
Transform To Domains [DNS] done (from entity "sun-hwa.cis.cabrillo.edu")
```

Properties

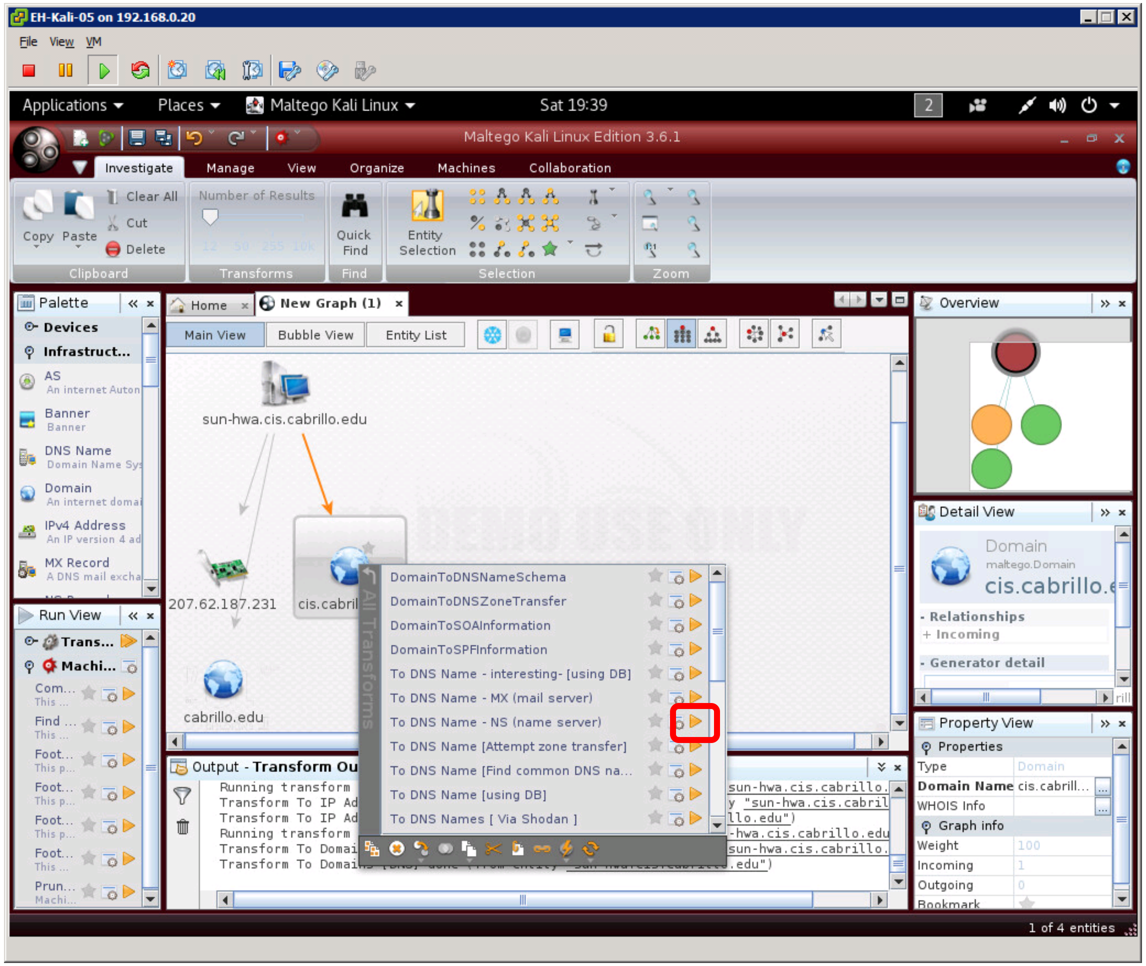
Type	DNS Name
DNS Name	sun-hwa.ci...

Graph info

Weight	0
Incoming	0
Outgoing	3
Bookmark	☆

Notice both the domain and sub-domain appear.

Maltego

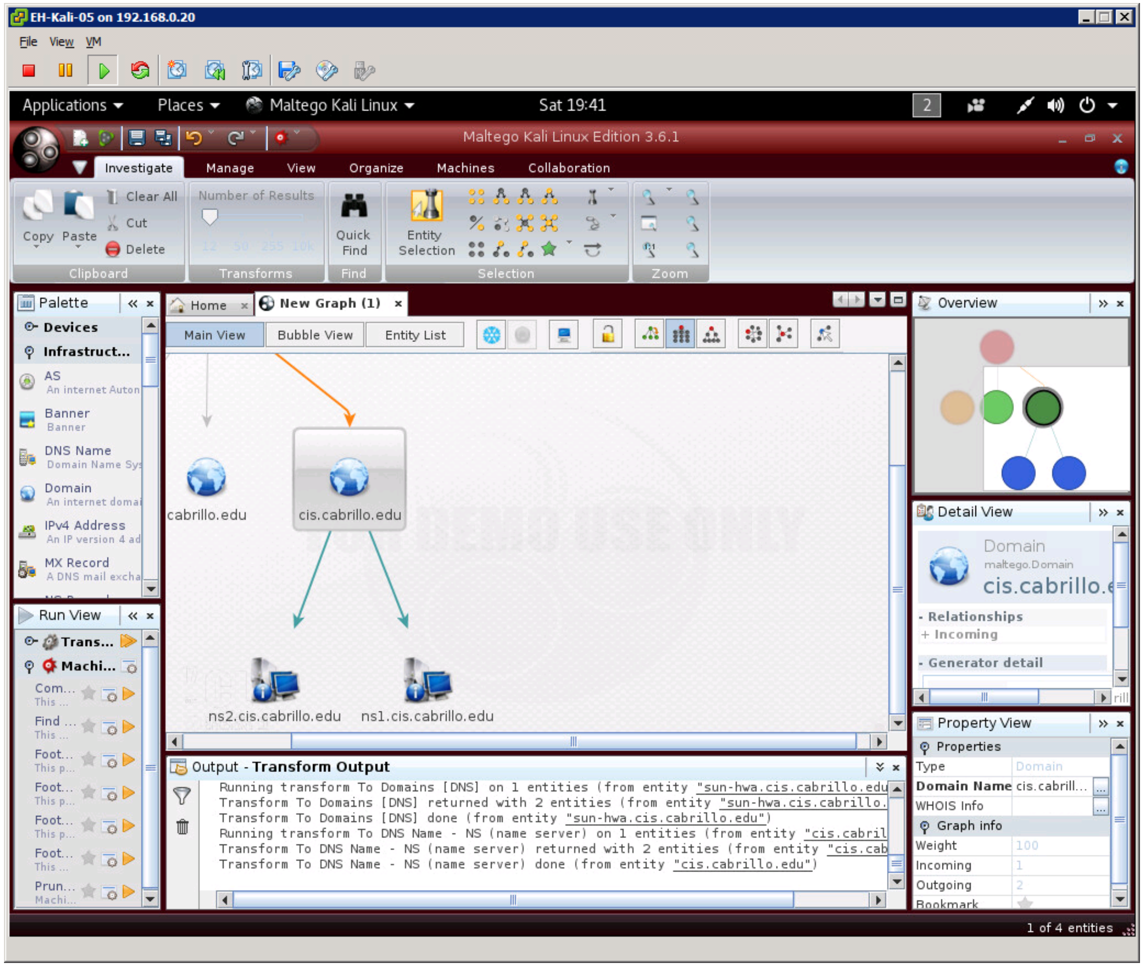

EH-Kali-05 on 192.168.0.20
File View VM
Applications Places Maltego Kali Linux Sat 19:39
Maltego Kali Linux Edition 3.6.1
Investigate Manage View Organize Machines Collaboration
Copy Paste Clear All Cut Delete Clipboard
Number of Results Transforms
Quick Find Find
Entity Selection Selection
Zoom
Palette Devices Infrastruct... AS An internet Auton Banner Banner DNS Name Domain Name Sys Domain An internet domai IPv4 Address An IP version 4 ad MX Record A DNS mail excha
Run View Trans... Machi... Com... Find ... Foot... Foot... Foot... Foot... Foot... Prun...
Home New Graph (1)
Main View Bubble View Entity List
sun-hwa.cis.cabrillo.edu
207.62.187.231
cis.cabril
cabrillo.edu
All Transforms
DomainToDNSNameSchema
DomainToDNSZoneTransfer
DomainToSOAInformation
DomainToSPFInformation
To DNS Name - interesting- [using DB]
To DNS Name - MX (mail server)
To DNS Name - NS (name server)
To DNS Name [Attempt zone transfer]
To DNS Name [Find common DNS na...
To DNS Name [using DB]
To DNS Names [Via Shodan]
Overview
Detail View Domain maltego.Domain cis.cabrillo.e
Relationships Incoming Generator detail
Property View Properties Type Domain Domain Name cis.cabrill... WHOIS Info Graph info Weight 100 Incoming 1 Outgoing 0 Bookmark
1 of 4 entities

Output - Transform Ou

```
Running transform                          sun-hwa.cis.cabrillo.
Transform To IP Ad                         y "sun-hwa.cis.cabril
Transform To IP Ad                         llo.edu")
Running transform                          -hwa.cis.cabrillo.edu
Transform To Domai                         sun-hwa.cis.cabrillo.
Transform To Domain [DNS] done (from entity "sun-hwa.cis.cabrillo.edu")
```

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

Maltego



Output - **Transform Output**

```
Running transform To Domains [DNS] on 1 entities (from entity "sun-hwa.cis.cabrillo.edu
Transform To Domains [DNS] returned with 2 entities (from entity "sun-hwa.cis.cabrillo.
Transform To Domains [DNS] done (from entity "sun-hwa.cis.cabrillo.edu")
Running transform To DNS Name - NS (name server) on 1 entities (from entity "cis.cabril
Transform To DNS Name - NS (name server) returned with 2 entities (from entity "cis.cab
Transform To DNS Name - NS (name server) done (from entity "cis.cabrillo.edu")
```

Properties

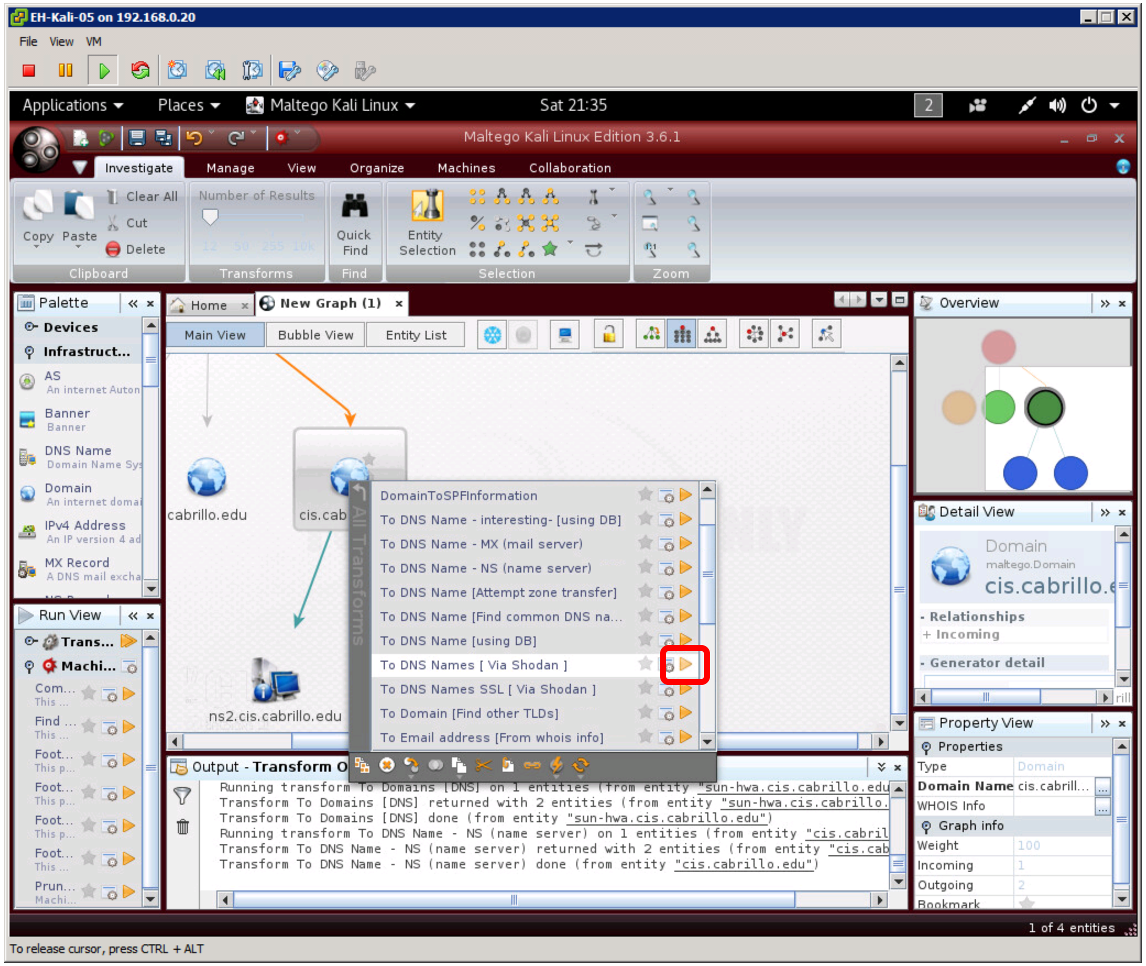
Type	Domain
Domain Name	cis.cabrill...
WHOIS Info	

Graph info

Weight	100
Incoming	1
Outgoing	2
Bookmark	

Notice both the domain and sub-domain appear.

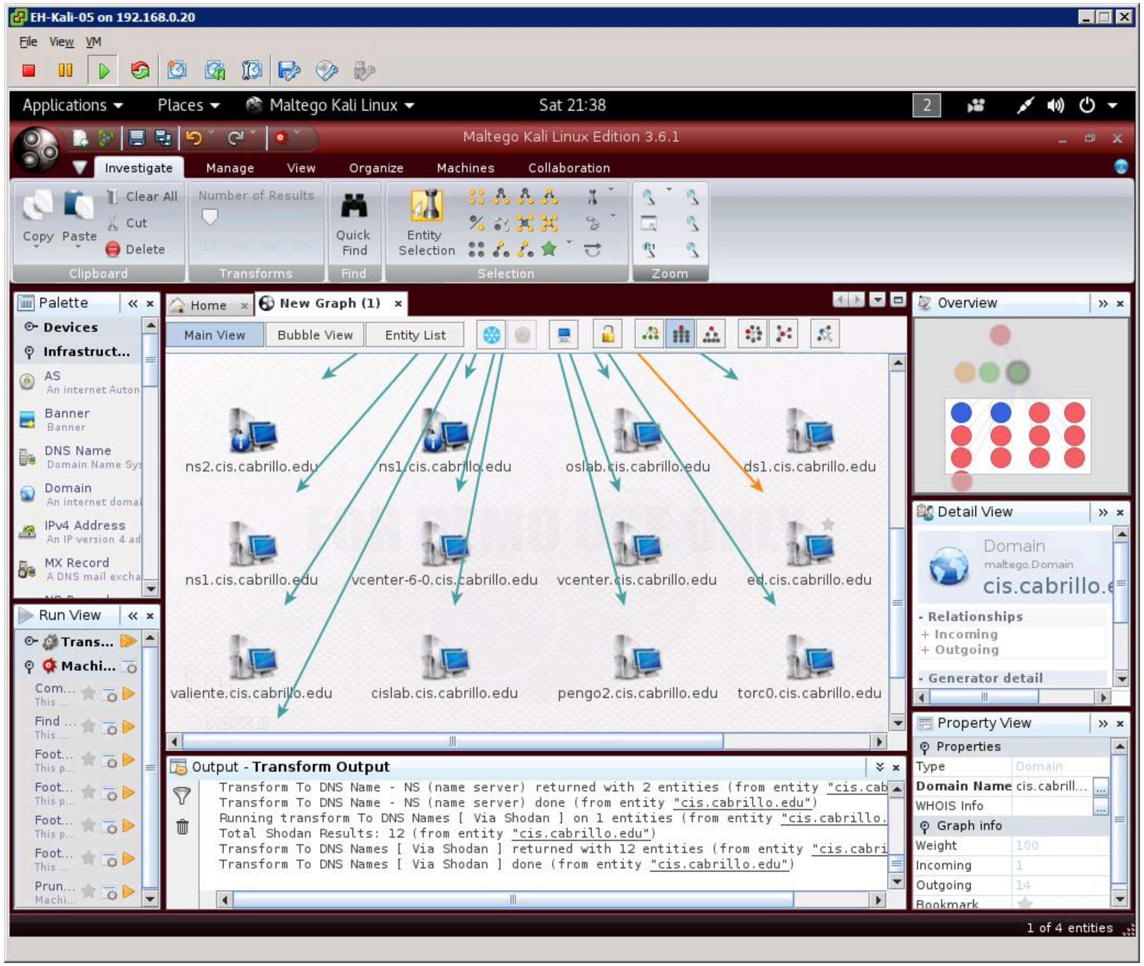
Maltego


EH-Kali-05 on 192.168.0.20
File View VM
Applications Places Maltego Kali Linux Sat 21:35
Maltego Kali Linux Edition 3.6.1
Investigate Manage View Organize Machines Collaboration
Copy Paste Clear All Cut Delete Clipboard
Number of Results 12 50 255 10k Transforms
Quick Find Find
Entity Selection Selection
Zoom
Palette
Devices
Infrastruct...
AS An internet Auton
Banner Banner
DNS Name Domain Name Sys
Domain An internet domai
IPv4 Address An IP version 4 ad
MX Record A DNS mail excha
Run View
Trans...
Machi...
Com... This ...
Find ... This ...
Foot... This p...
Foot... This p...
Foot... This p...
Foot... This ...
Prun... Machi...
Home
New Graph (1)
Main View Bubble View Entity List
cabrillo.edu
cis.cab
ns2.cis.cabrillo.edu
All Transforms
DomainToSPFInformation
To DNS Name - interesting- [using DB]
To DNS Name - MX (mail server)
To DNS Name - NS (name server)
To DNS Name [Attempt zone transfer]
To DNS Name [Find common DNS na...
To DNS Name [using DB]
To DNS Names [Via Shodan]
To DNS Names SSL [Via Shodan]
To Domain [Find other TLDs]
To Email address [From whois info]
Output - Transform O
Overview
Detail View
Domain
maltego.Domain
cis.cabrillo.e
- Relationships
+ Incoming
- Generator detail
Property View
Properties
Type Domain
Domain Name cis.cabrill...
WHOIS Info
Graph info
Weight 100
Incoming 1
Outgoing 2
Bookmark
1 of 4 entities
To release cursor, press CTRL + ALT

```
Running transform To Domains [DNS] on 1 entities (from entity "sun-hwa.cis.cabrillo.edu
Transform To Domains [DNS] returned with 2 entities (from entity "sun-hwa.cis.cabrillo.
Transform To Domains [DNS] done (from entity "sun-hwa.cis.cabrillo.edu")
Running transform To DNS Name - NS (name server) on 1 entities (from entity "cis.cabril
Transform To DNS Name - NS (name server) returned with 2 entities (from entity "cis.cab
Transform To DNS Name - NS (name server) done (from entity "cis.cabrillo.edu")
```

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

Maltego



Output - **Transform Output**

```
Transform To DNS Name - NS (name server) returned with 2 entities (from entity "cis.cab
Transform To DNS Name - NS (name server) done (from entity "cis.cabrillo.edu")
Running transform To DNS Names [ Via Shodan ] on 1 entities (from entity "cis.cabrillo.
Total Shodan Results: 12 (from entity "cis.cabrillo.edu")
Transform To DNS Names [ Via Shodan ] returned with 12 entities (from entity "cis.cabri
Transform To DNS Names [ Via Shodan ] done (from entity "cis.cabrillo.edu")
```

Properties

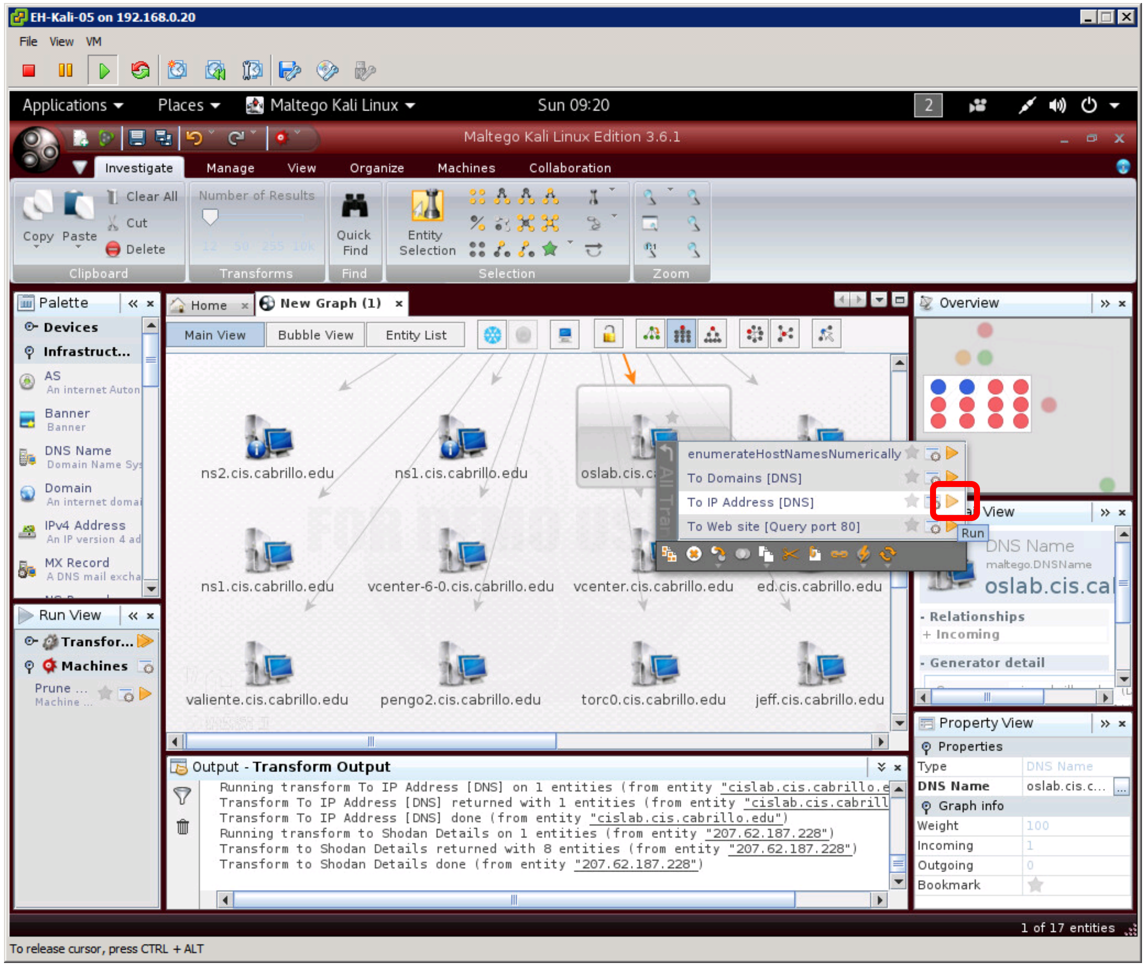
Type	Domain
Domain Name	cis.cabrill...
WHOIS Info	

Graph info

Weight	100
Incoming	1
Outgoing	14
Bookmark	☆

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

Maltego



Output - Transform Output

```
Running transform To IP Address [DNS] on 1 entities (from entity "cislab.cis.cabrillo.e
Transform To IP Address [DNS] returned with 1 entities (from entity "cislab.cis.cabrill
Transform To IP Address [DNS] done (from entity "cislab.cis.cabrillo.edu")
Running transform to Shodan Details on 1 entities (from entity "207.62.187.228")
Transform to Shodan Details returned with 8 entities (from entity "207.62.187.228")
Transform to Shodan Details done (from entity "207.62.187.228")
```

Properties

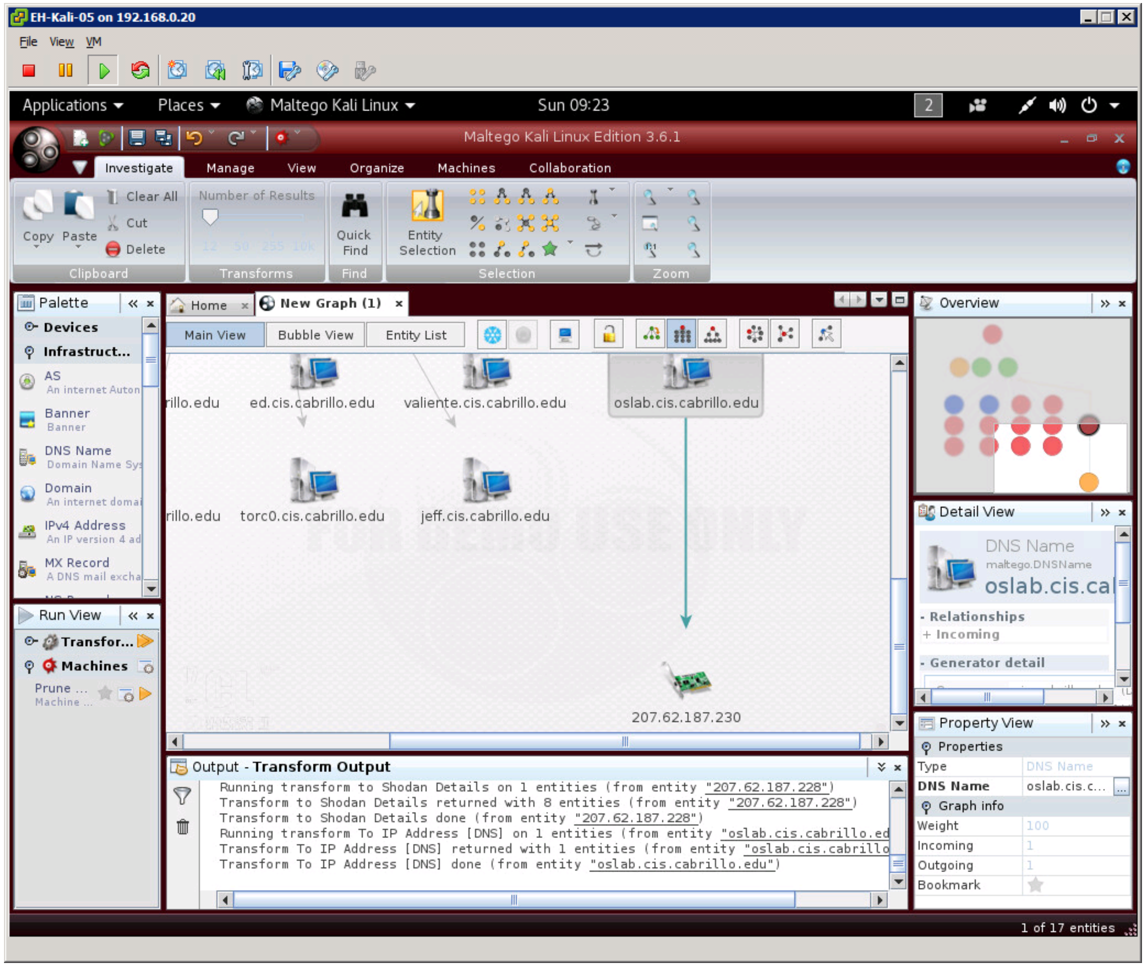
Type	DNS Name
DNS Name	oslab.cis.c...

Graph info

Weight	100
Incoming	1
Outgoing	0
Bookmark	☆

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

Maltego



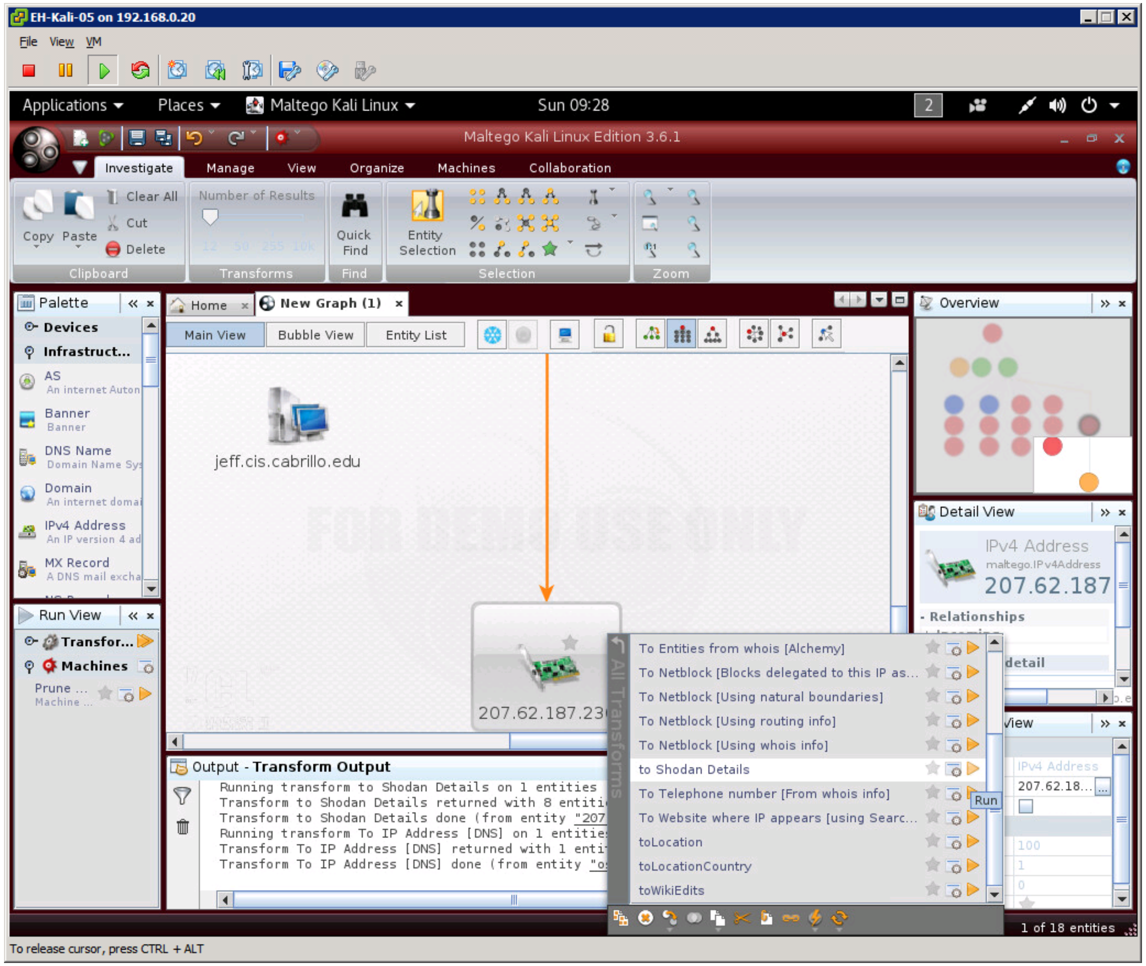
Output - Transform Output

```
Running transform to Shodan Details on 1 entities (from entity "207.62.187.228")
Transform to Shodan Details returned with 8 entities (from entity "207.62.187.228")
Transform to Shodan Details done (from entity "207.62.187.228")
Running transform To IP Address [DNS] on 1 entities (from entity "oslab.cis.cabrillo.ed
Transform To IP Address [DNS] returned with 1 entities (from entity "oslab.cis.cabrillo
Transform To IP Address [DNS] done (from entity "oslab.cis.cabrillo.edu")
```

Type	DNS Name
DNS Name	oslab.cis.c...
Weight	100
Incoming	1
Outgoing	1
Bookmark	☆

Notice we have the external IP address now.

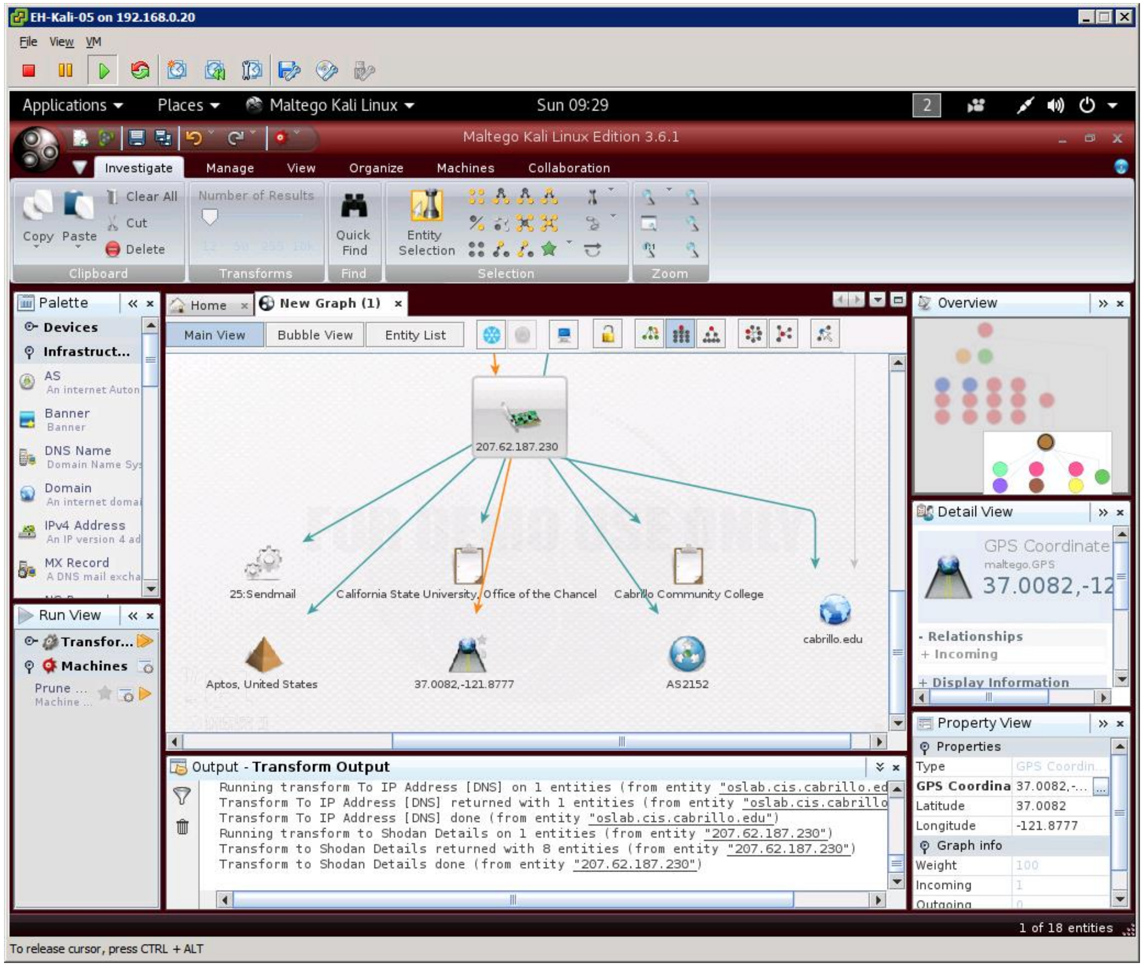
Maltego


EH-Kali-05 on 192.168.0.20
File View VM
Applications Places Maltego Kali Linux Sun 09:28
Maltego Kali Linux Edition 3.6.1
Investigate Manage View Organize Machines Collaboration
Copy Paste Clear All Cut Delete Clipboard
Number of Results Transforms
Quick Find Find
Entity Selection Selection
Zoom
Palette
Devices
Infrastruct...
AS An internet Auton
Banner Banner
DNS Name Domain Name Sys
Domain An internet domai
IPv4 Address An IP version 4 ad
MX Record A DNS mail excha
Run View
Transfor...
Machines
Prune ... Machine ...
Home
New Graph (1)
Main View Bubble View Entity List
jeff.cis.cabrillo.edu
207.62.187.23
All Transforms
To Entities from whois [Alchemy]
To Netblock [Blocks delegated to this IP as...
To Netblock [Using natural boundaries]
To Netblock [Using routing info]
To Netblock [Using whois info]
to Shodan Details
To Telephone number [From whois info]
To Website where IP appears [using Searc...
toLocation
toLocationCountry
toWikiEdits
Run
Overview
Detail View
IPv4 Address
maltego.IPv4Address
207.62.187
Relationships
detail
View
IPv4 Address
207.62.18...
100
1
0
Output - Transform Output
1 of 18 entities
To release cursor, press CTRL + ALT

```
Running transform to Shodan Details on 1 entities
Transform to Shodan Details returned with 8 entiti
Transform to Shodan Details done (from entity "207
Running transform To IP Address [DNS] on 1 entitie
Transform To IP Address [DNS] returned with 1 enti
Transform To IP Address [DNS] done (from entity "o
```

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

Maltego


EH-Kali-05 on 192.168.0.20
File View VM
Applications Places Maltego Kali Linux Sun 09:29
Maltego Kali Linux Edition 3.6.1
Investigate Manage View Organize Machines Collaboration
Copy Paste Clear All Cut Delete Clipboard
Number of Results Transforms
Quick Find Find
Entity Selection Selection
Zoom
Palette
Devices
Infrastruct...
AS An internet Auton
Banner Banner
DNS Name Domain Name Sys
Domain An internet domai
IPv4 Address An IP version 4 ad
MX Record A DNS mail excha
Run View
Transfor...
Machines
Prune ... Machine ...
Home
New Graph (1)
Main View Bubble View Entity List
207.62.187.230
25:Sendmail
California State University, Office of the Chancel
Cabrillo Community College
cabrillo.edu
Aptos, United States
37.0082,-121.8777
AS2152
Overview
Detail View
GPS Coordinate
maltego.GPS
37.0082,-12
- Relationships
+ Incoming
+ Display Information
Property View
1 of 18 entities
To release cursor, press CTRL + ALT

Output - **Transform Output**

```
Running transform To IP Address [DNS] on 1 entities (from entity "oslab.cis.cabrillo.ed
Transform To IP Address [DNS] returned with 1 entities (from entity "oslab.cis.cabrillo
Transform To IP Address [DNS] done (from entity "oslab.cis.cabrillo.edu")
Running transform to Shodan Details on 1 entities (from entity "207.62.187.230")
Transform to Shodan Details returned with 8 entities (from entity "207.62.187.230")
Transform to Shodan Details done (from entity "207.62.187.230")
```

Properties

Type	GPS Coordin...
GPS Coordina	37.0082,-...
Latitude	37.0082
Longitude	-121.8777

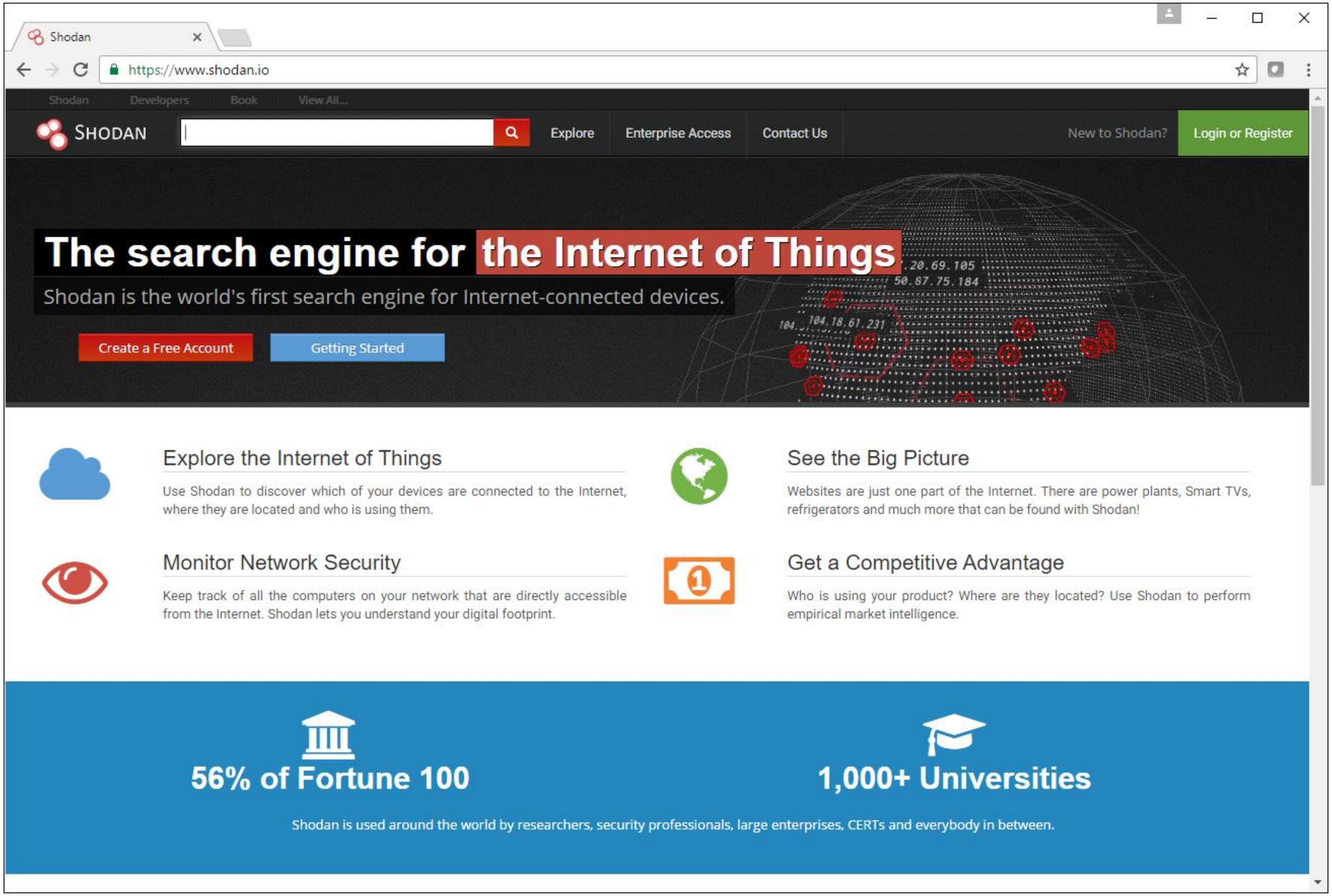
Graph info

Weight	100
Incoming	1
Outgoing	0

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

shodan

SHODAN



The search engine for the Internet of Things

Shodan is the world's first search engine for Internet-connected devices.

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

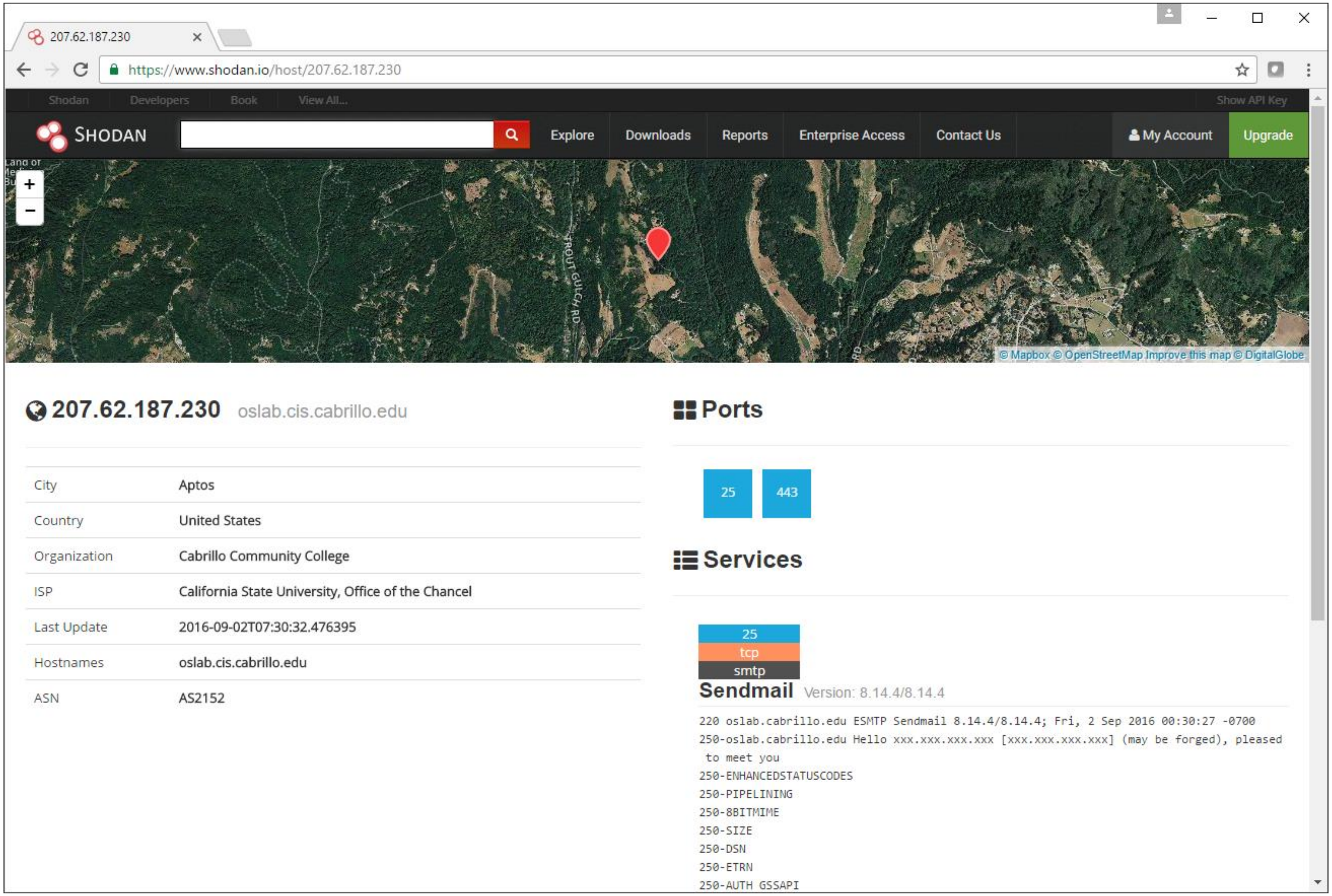
56% of Fortune 100

1,000+ Universities

Shodan is used around the world by researchers, security professionals, large enterprises, CERTs and everybody in between.

https://www.shodan.io/

SHODAN



207.62.187.230 oslab.cis.cabrillo.edu

City	Aptos
Country	United States
Organization	Cabrillo Community College
ISP	California State University, Office of the Chancel
Last Update	2016-09-02T07:30:32.476395
Hostnames	oslab.cis.cabrillo.edu
ASN	AS2152

Ports

25 443

Services

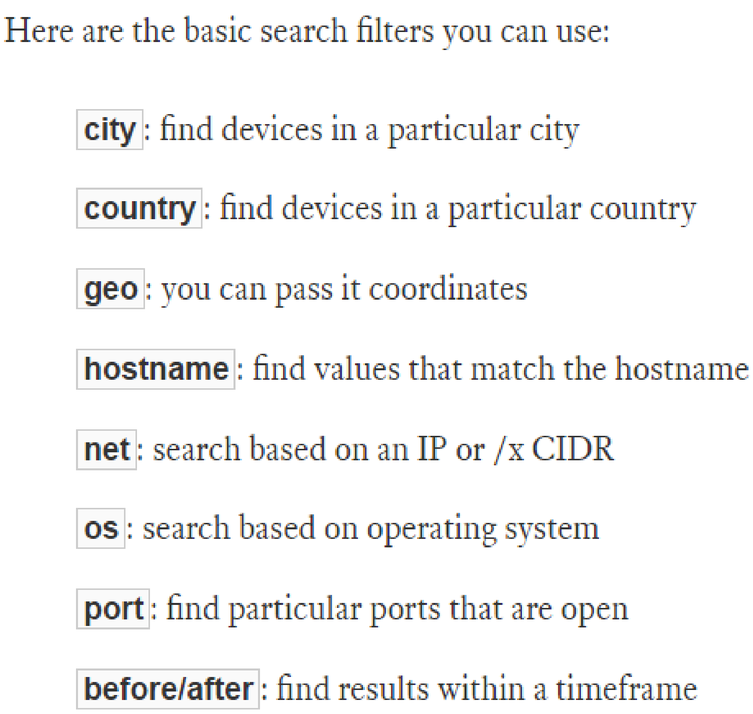
25
tcp
smtp

Sendmail Version: 8.14.4/8.14.4

```
220 oslab.cabrillo.edu ESMTP Sendmail 8.14.4/8.14.4; Fri, 2 Sep 2016 00:30:27 -0700
250-oslab.cabrillo.edu Hello xxx.xxx.xxx.xxx [xxx.xxx.xxx.xxx] (may be forged), pleased
 to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-8BITMIME
250-SIZE
250-DSN
250-ETRN
250-AUTH GSSAPI
```

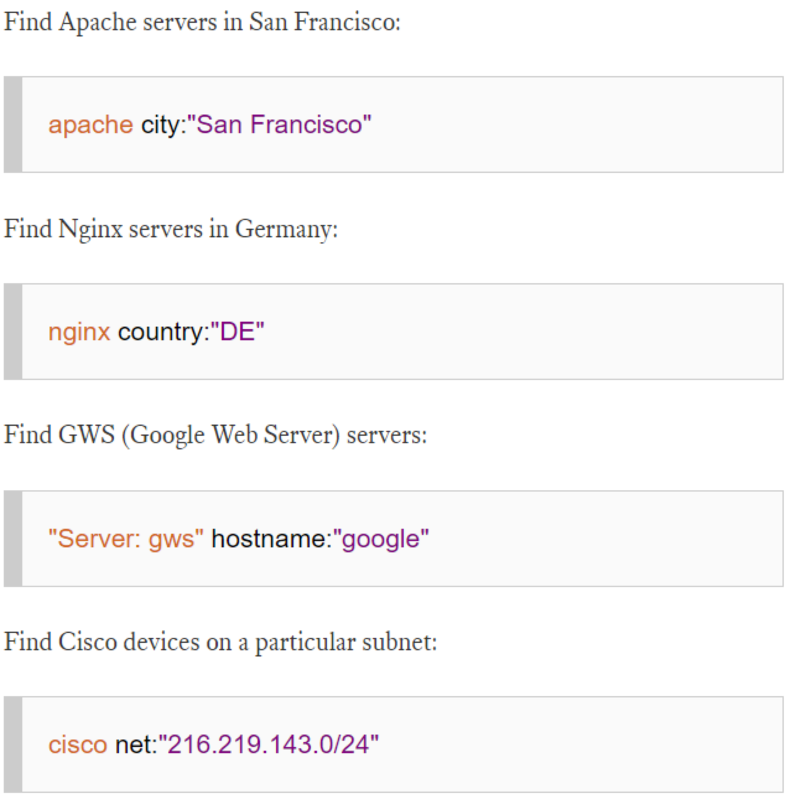
https://www.shodan.io/

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

Find the IP address for sun-hwa.cis.cabrillo.edu and then have SHODAN look at it.

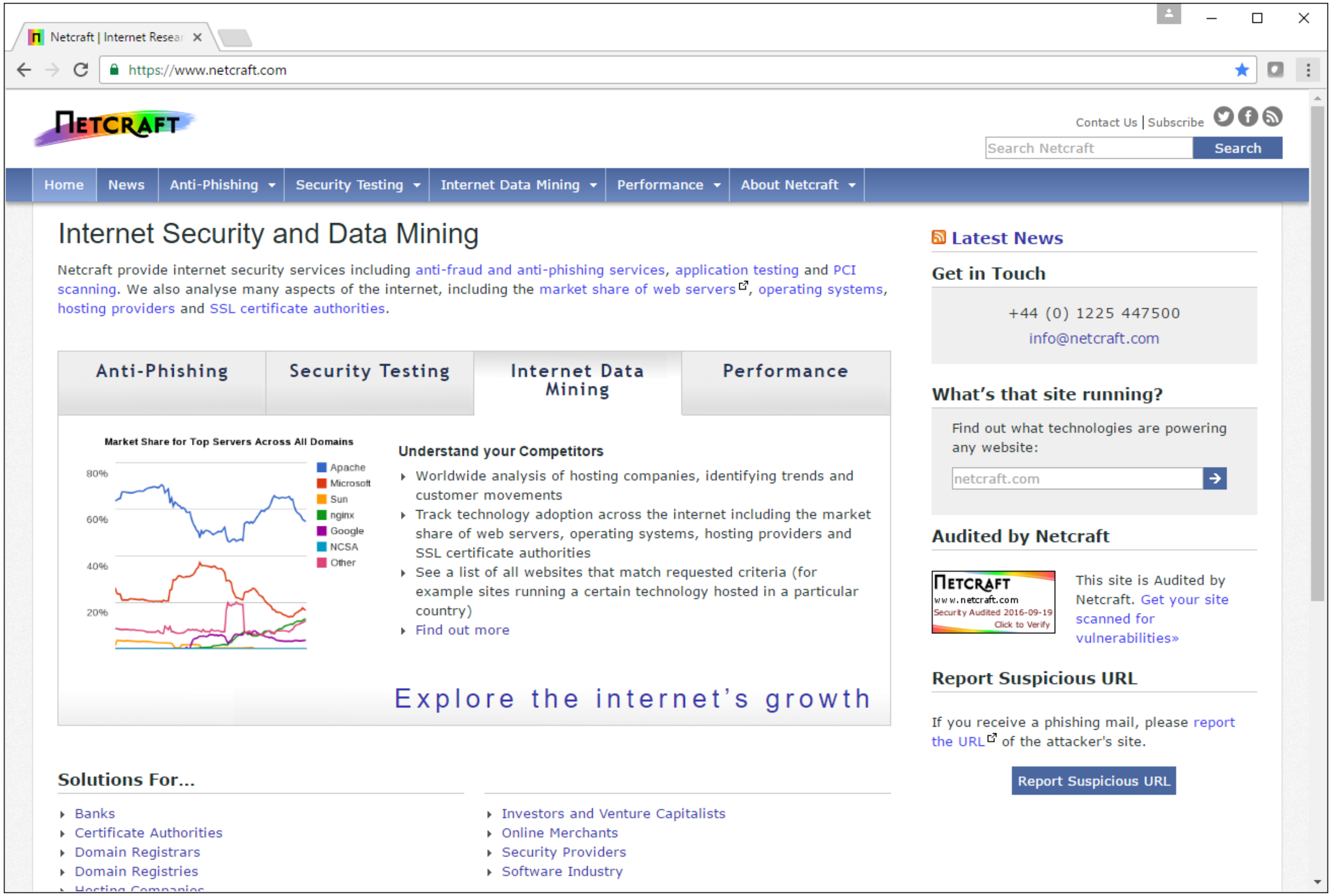
What OS and web server are running on Sun-Hwa?

Write your answer in the chat window

Website Information

Netcraft

Netcraft



Internet Security and Data Mining

Netcraft provide internet security services including anti-fraud and anti-phishing services, application testing and PCI scanning. We also analyse many aspects of the internet, including the market share of web servers, operating systems, hosting providers and SSL certificate authorities.

Understand your Competitors

- Worldwide analysis of hosting companies, identifying trends and customer movements
- Track technology adoption across the internet including the market share of web servers, operating systems, hosting providers and SSL certificate authorities
- See a list of all websites that match requested criteria (for example sites running a certain technology hosted in a particular country)
- Find out more

Explore the internet's growth

Solutions For...

- Banks
- Certificate Authorities
- Domain Registrars
- Domain Registries
- Hosting Companies
- Investors and Venture Capitalists
- Online Merchants
- Security Providers
- Software Industry

Latest News

Get in Touch

+44 (0) 1225 447500
info@netcraft.com

What's that site running?

Find out what technologies are powering any website:

Audited by Netcraft

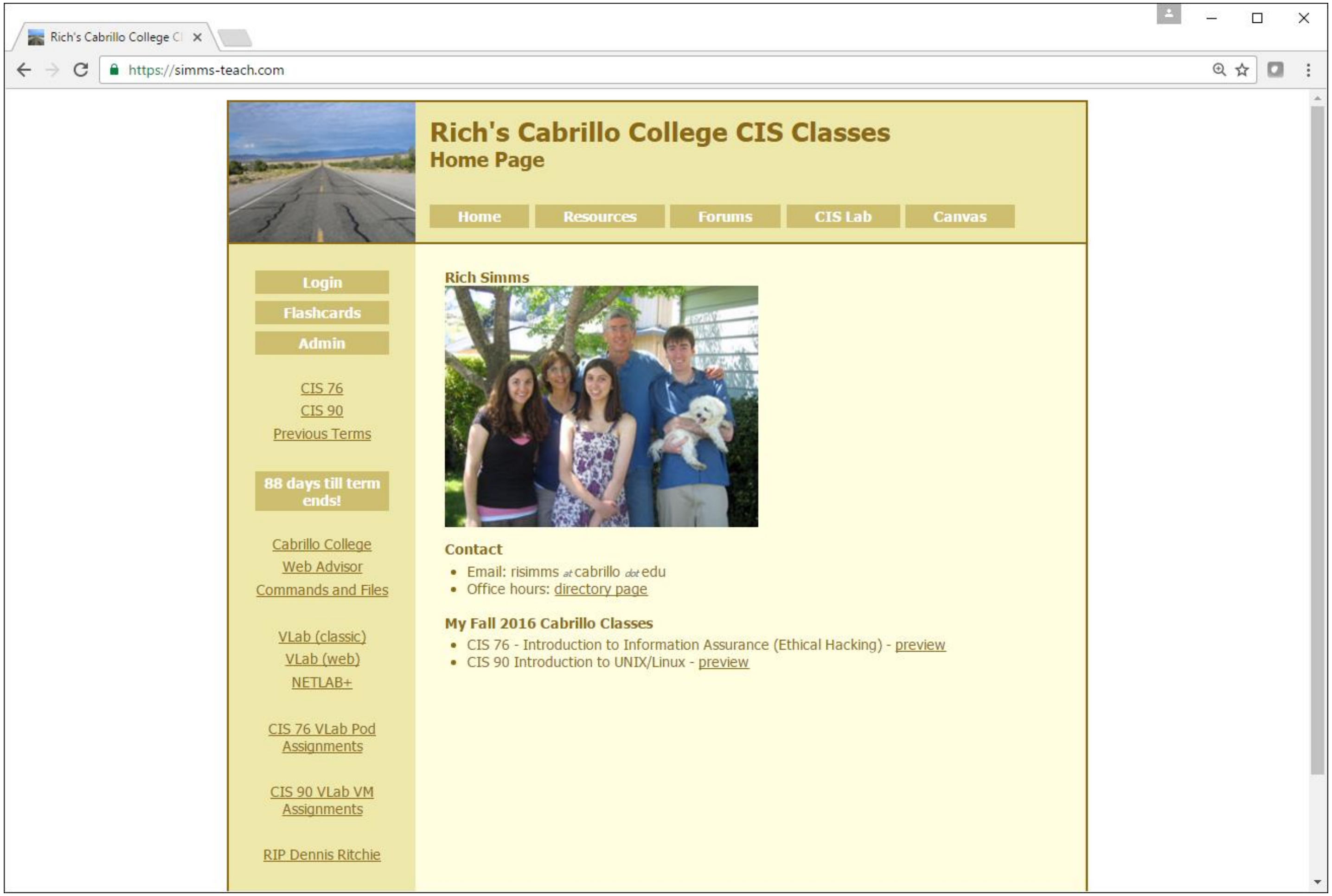
This site is Audited by Netcraft. Get your site scanned for vulnerabilities»

Report Suspicious URL

If you receive a phishing mail, please report the URL of the attacker's site.

https://www.netcraft.com/

My Website



Rich's Cabrillo College CIS Classes

Home Page

Rich Simms

Contact

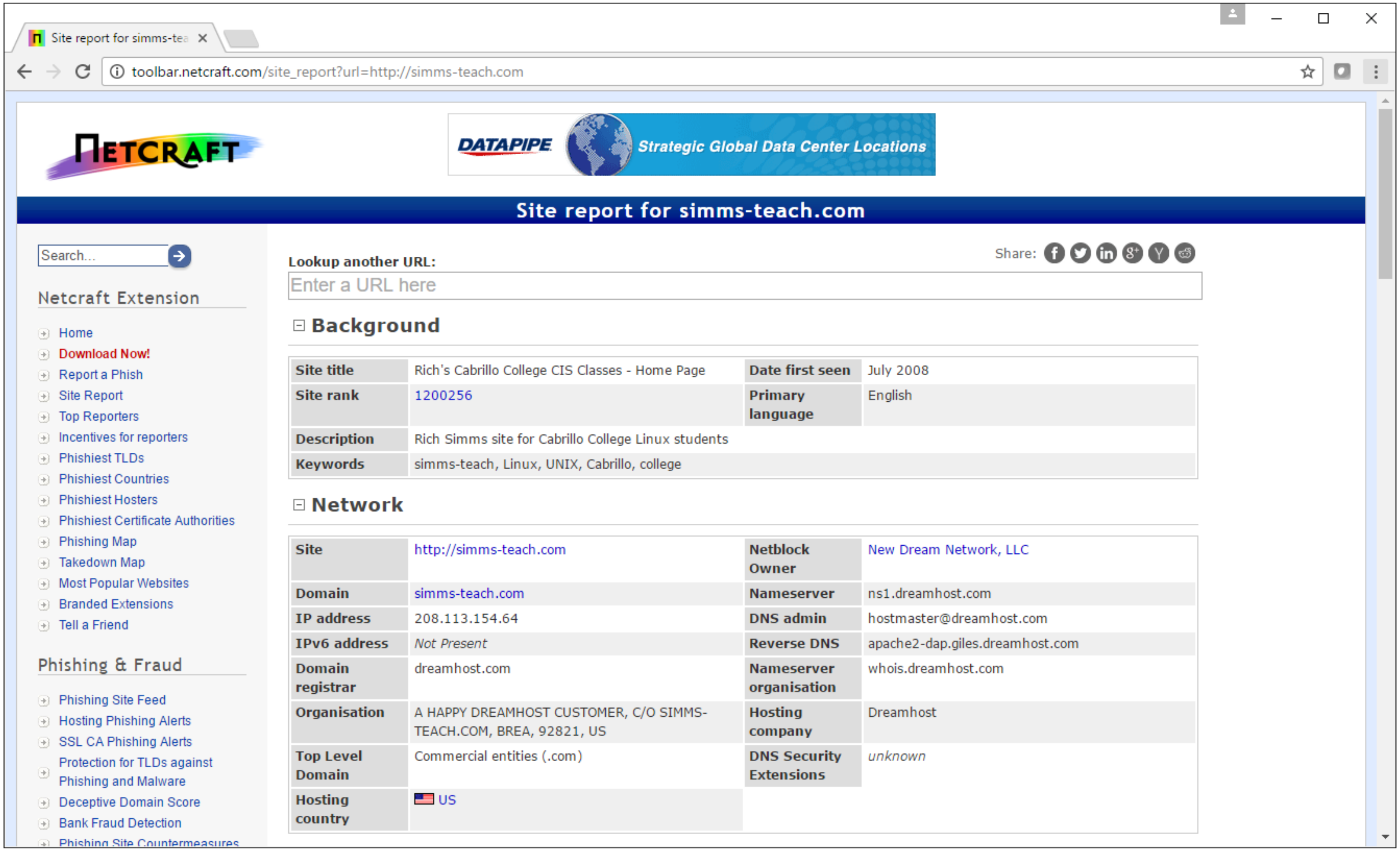
- Email: risimms at cabrillo dot edu
- Office hours: directory page

My Fall 2016 Cabrillo Classes

- CIS 76 - Introduction to Information Assurance (Ethical Hacking) - preview
- CIS 90 Introduction to UNIX/Linux - preview

https://simms-teach.com/

Netcraft



Site report for simms-teach.com

Lookup another URL:

⊟ Background

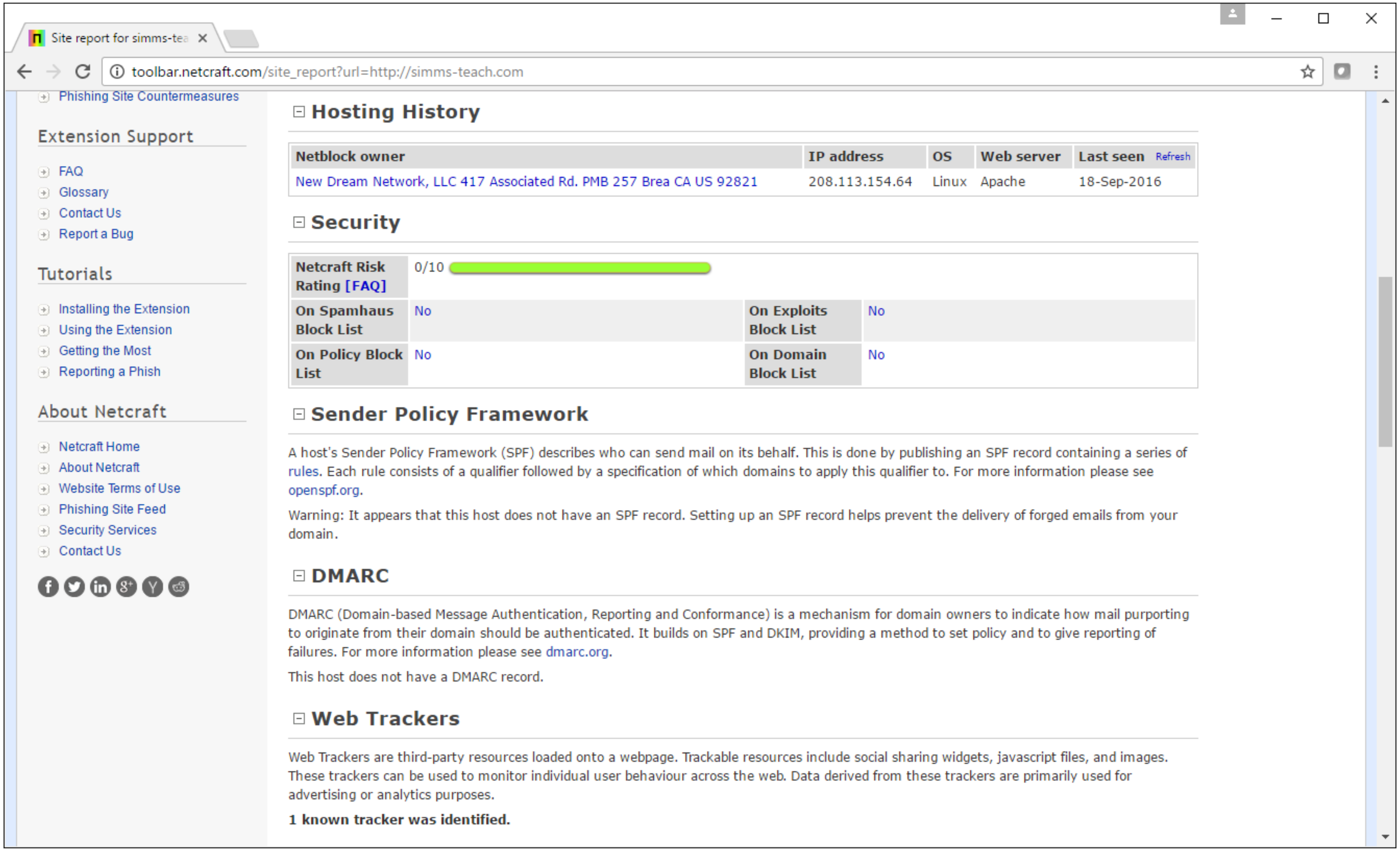
Site title	Rich's Cabrillo College CIS Classes - Home Page	Date first seen	July 2008
Site rank	1200256	Primary language	English
Description	Rich Simms site for Cabrillo College Linux students		
Keywords	simms-teach, Linux, UNIX, Cabrillo, college		

⊟ Network

Site	http://simms-teach.com	Netblock Owner	New Dream Network, LLC
Domain	simms-teach.com	Nameserver	ns1.dreamhost.com
IP address	208.113.154.64	DNS admin	hostmaster@dreamhost.com
IPv6 address	*Not Present*	Reverse DNS	apache2-dap.giles.dreamhost.com
Domain registrar	dreamhost.com	Nameserver organisation	whois.dreamhost.com
Organisation	A HAPPY DREAMHOST CUSTOMER, C/O SIMMS-TEACH.COM, BREA, 92821, US	Hosting company	Dreamhost
Top Level Domain	Commercial entities (.com)	DNS Security Extensions	*unknown*
Hosting country	US		

https://www.netcraft.com/

Netcraft



⊟ Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
New Dream Network, LLC 417 Associated Rd. PMB 257 Brea CA US 92821	208.113.154.64	Linux	Apache	18-Sep-2016

⊟ Security

Netcraft Risk Rating [FAQ]	0/10		
On Spamhaus Block List	No	On Exploits Block List	No
On Policy Block List	No	On Domain Block List	No

⊟ Sender Policy Framework

A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of rules. Each rule consists of a qualifier followed by a specification of which domains to apply this qualifier to. For more information please see openspf.org.

Warning: It appears that this host does not have an SPF record. Setting up an SPF record helps prevent the delivery of forged emails from your domain.

⊟ DMARC

DMARC (Domain-based Message Authentication, Reporting and Conformance) is a mechanism for domain owners to indicate how mail purporting to originate from their domain should be authenticated. It builds on SPF and DKIM, providing a method to set policy and to give reporting of failures. For more information please see dmarc.org.

This host does not have a DMARC record.

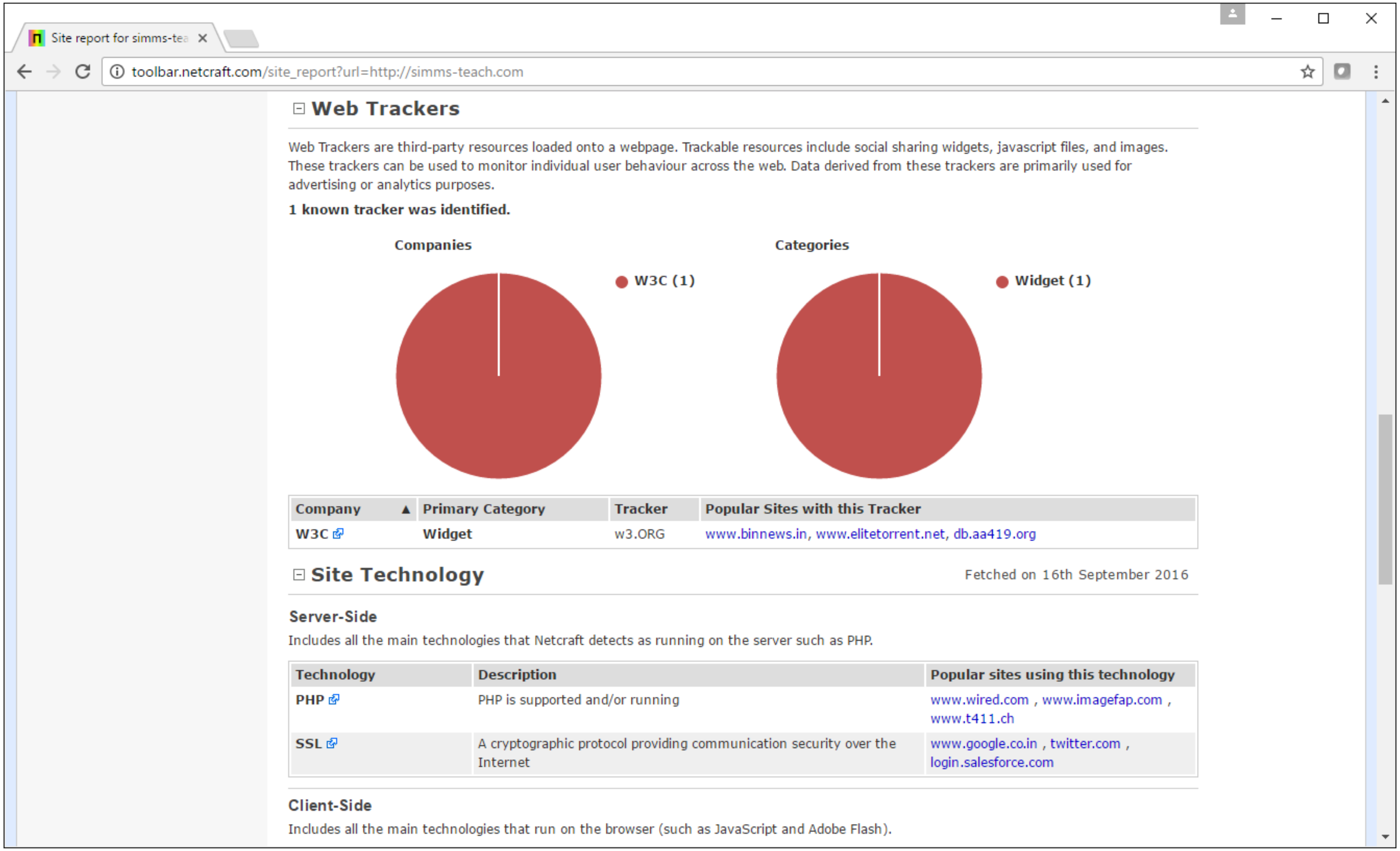
⊟ Web Trackers

Web Trackers are third-party resources loaded onto a webpage. Trackable resources include social sharing widgets, javascript files, and images. These trackers can be used to monitor individual user behaviour across the web. Data derived from these trackers are primarily used for advertising or analytics purposes.

1 known tracker was identified.

https://www.netcraft.com/

Netcraft


Site report for simms-tea
toolbar.netcraft.com/site_report?url=http://simms-teach.com

⊟ Web Trackers

Web Trackers are third-party resources loaded onto a webpage. Trackable resources include social sharing widgets, javascript files, and images. These trackers can be used to monitor individual user behaviour across the web. Data derived from these trackers are primarily used for advertising or analytics purposes.

1 known tracker was identified.

Companies
● W3C (1)
Categories
● Widget (1)

Company ▲	Primary Category	Tracker	Popular Sites with this Tracker
W3C	**Widget**	w3.ORG	www.binnews.in, www.elitetorrent.net, db.aa419.org

⊟ Site Technology

Fetched on 16th September 2016

Server-Side

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

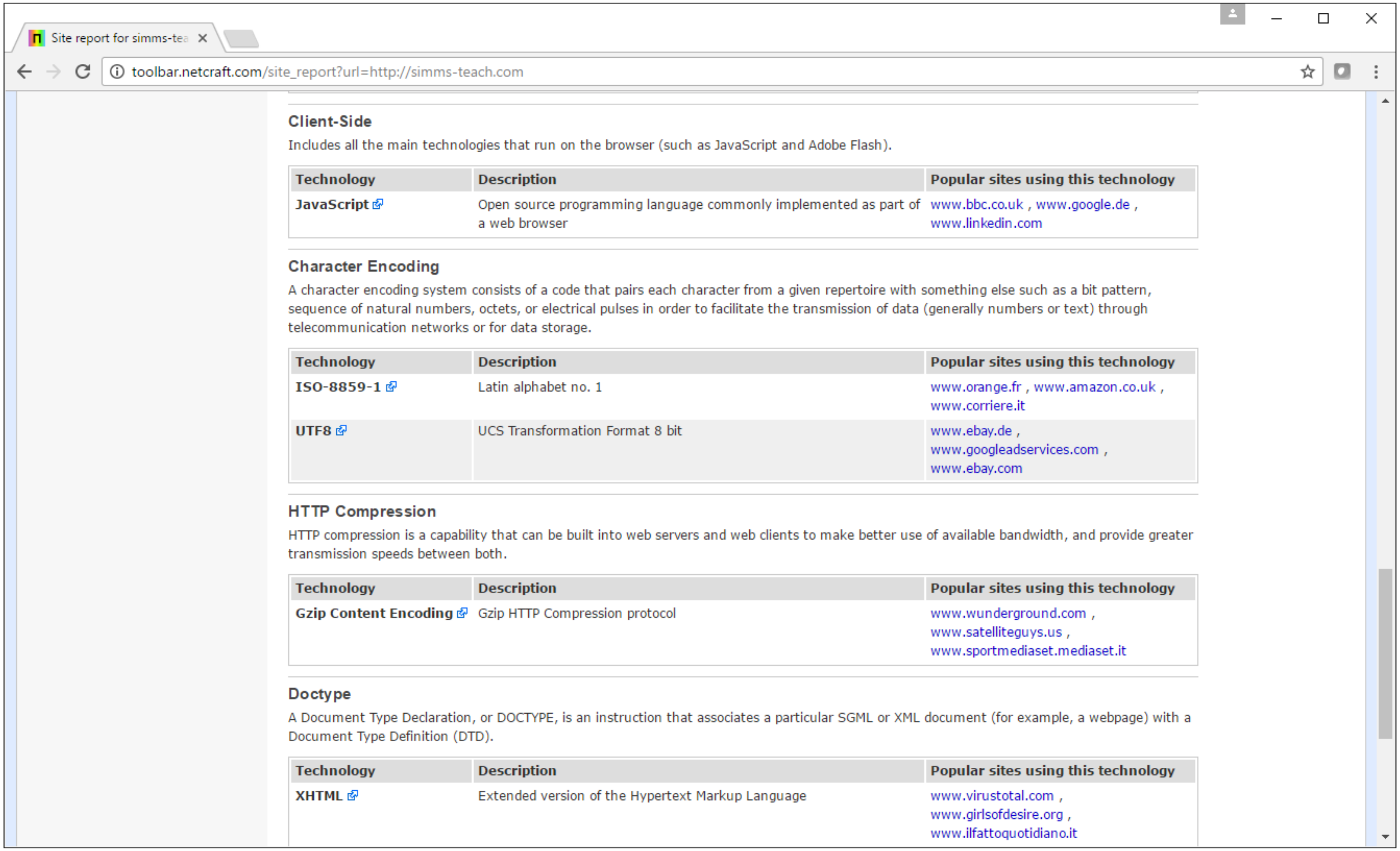
Technology	Description	Popular sites using this technology
PHP	PHP is supported and/or running	www.wired.com , www.imagefap.com , www.t411.ch
SSL	A cryptographic protocol providing communication security over the Internet	www.google.co.in , twitter.com , login.salesforce.com

Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

https://www.netcraft.com/

Netcraft



Site report for simms-tea
toolbar.netcraft.com/site_report?url=http://simms-teach.com

Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

Technology	Description	Popular sites using this technology
JavaScript	Open source programming language commonly implemented as part of a web browser	www.bbc.co.uk , www.google.de , www.linkedin.com

Character Encoding

A character encoding system consists of a code that pairs each character from a given repertoire with something else such as a bit pattern, sequence of natural numbers, octets, or electrical pulses in order to facilitate the transmission of data (generally numbers or text) through telecommunication networks or for data storage.

Technology	Description	Popular sites using this technology
ISO-8859-1	Latin alphabet no. 1	www.orange.fr , www.amazon.co.uk , www.corriere.it
UTF8	UCS Transformation Format 8 bit	www.ebay.de , www.googleadservices.com , www.ebay.com

HTTP Compression

HTTP compression is a capability that can be built into web servers and web clients to make better use of available bandwidth, and provide greater transmission speeds between both.

Technology	Description	Popular sites using this technology
Gzip Content Encoding	Gzip HTTP Compression protocol	www.wunderground.com , www.satelliteguys.us , www.sportmediaset.mediaset.it

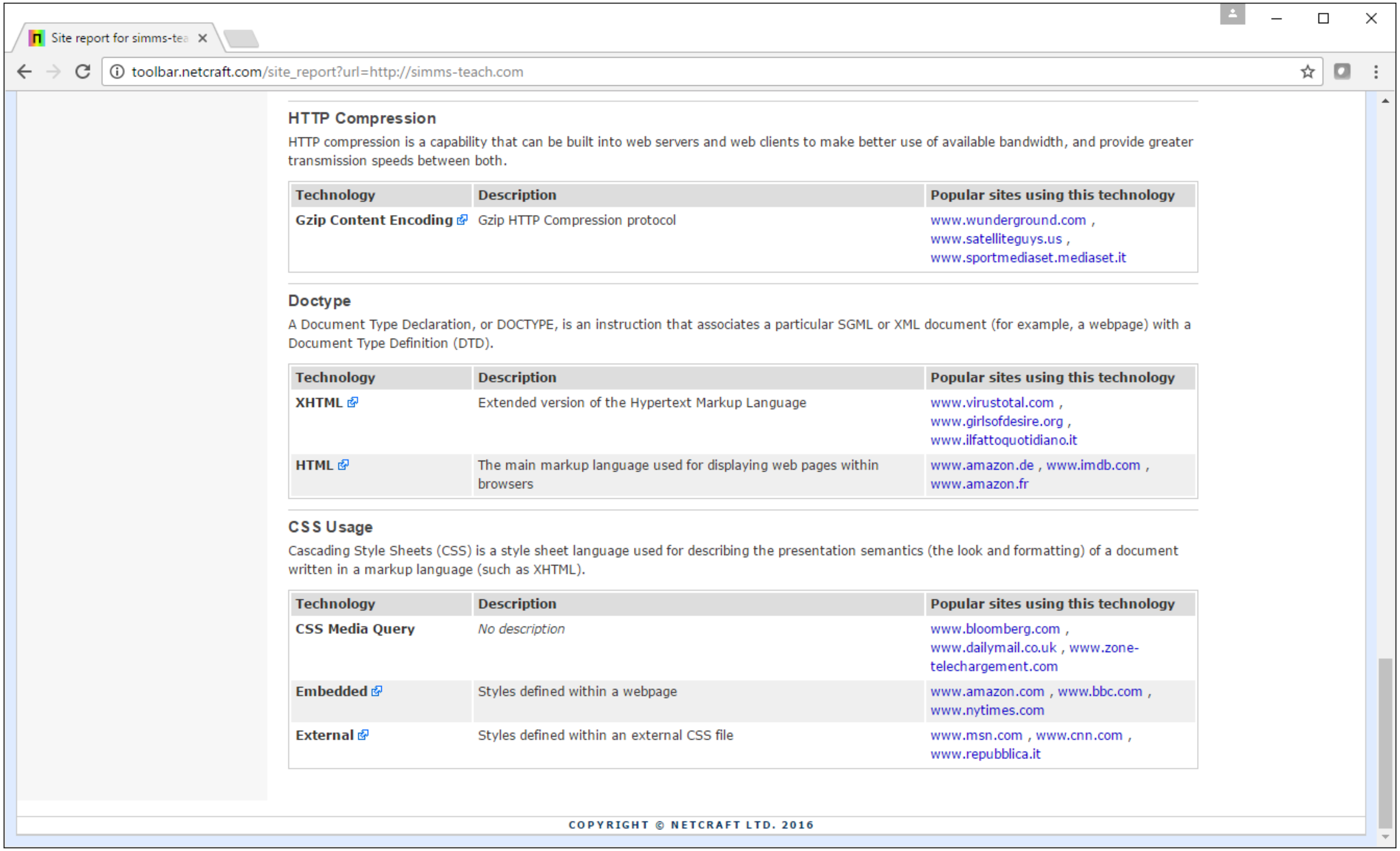
Doctype

A Document Type Declaration, or DOCTYPE, is an instruction that associates a particular SGML or XML document (for example, a webpage) with a Document Type Definition (DTD).

Technology	Description	Popular sites using this technology
XHTML	Extended version of the Hypertext Markup Language	www.virustotal.com , www.girlsofdesire.org , www.ilfattoquotidiano.it

https://www.netcraft.com/

Netcraft


Site report for simms-tea
toolbar.netcraft.com/site_report?url=http://simms-teach.com

HTTP Compression

HTTP compression is a capability that can be built into web servers and web clients to make better use of available bandwidth, and provide greater transmission speeds between both.

Technology	Description	Popular sites using this technology
Gzip Content Encoding	Gzip HTTP Compression protocol	www.wunderground.com , www.satelliteguys.us , www.sportmediaset.mediaset.it

Doctype

A Document Type Declaration, or DOCTYPE, is an instruction that associates a particular SGML or XML document (for example, a webpage) with a Document Type Definition (DTD).

Technology	Description	Popular sites using this technology
XHTML	Extended version of the Hypertext Markup Language	www.virustotal.com , www.girlsofdesire.org , www.ilfattoquotidiano.it
HTML	The main markup language used for displaying web pages within browsers	www.amazon.de , www.imdb.com , www.amazon.fr

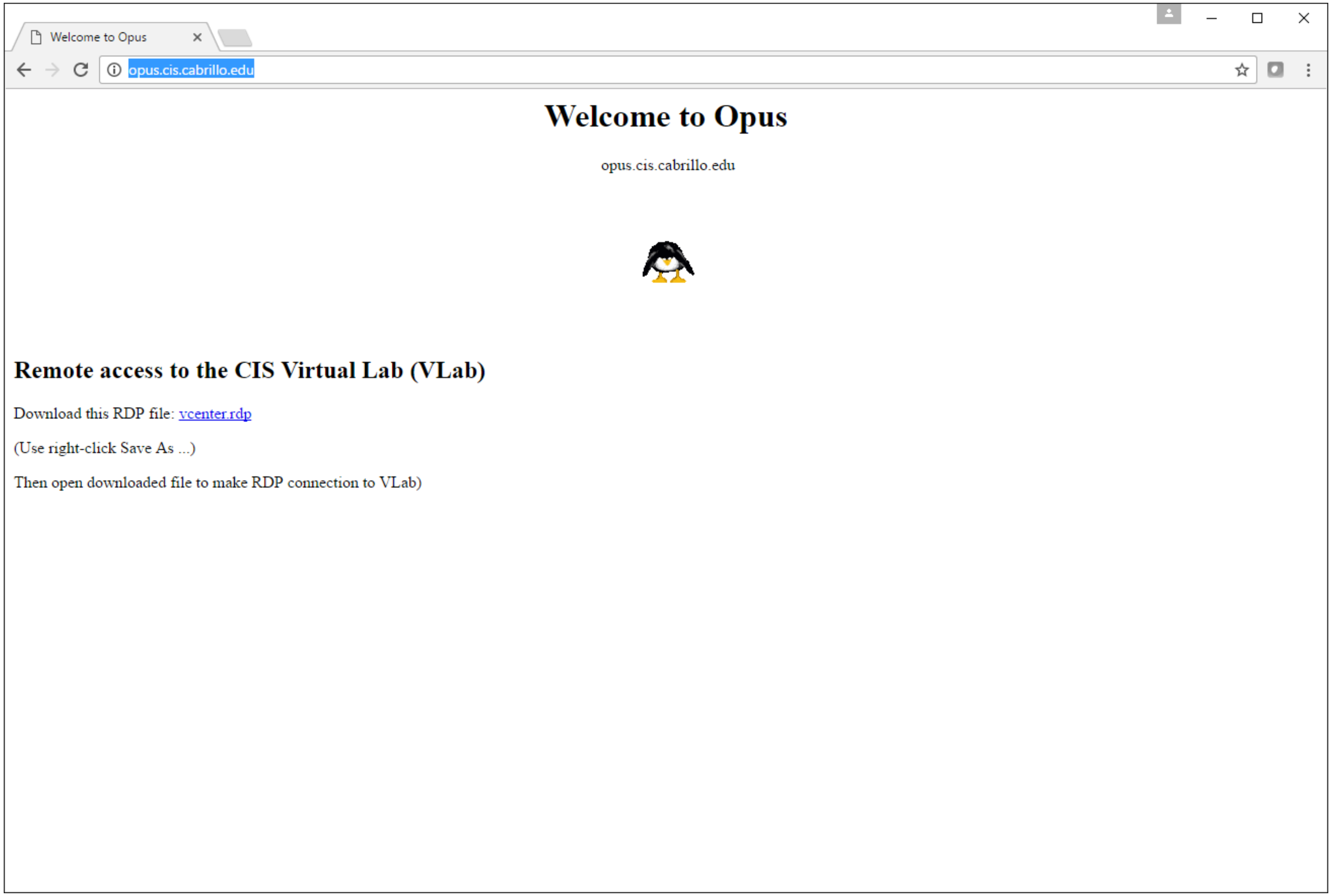
CSS Usage

Cascading Style Sheets (CSS) is a style sheet language used for describing the presentation semantics (the look and formatting) of a document written in a markup language (such as XHTML).

Technology	Description	Popular sites using this technology
CSS Media Query	*No description*	www.bloomberg.com , www.dailymail.co.uk , www.zone-telechargement.com
Embedded	Styles defined within a webpage	www.amazon.com , www.bbc.com , www.nytimes.com
External	Styles defined within an external CSS file	www.msn.com , www.cnn.com , www.repubblica.it

https://www.netcraft.com/

Opus website



Welcome to Opus

opus.cis.cabrillo.edu

Remote access to the CIS Virtual Lab (VLab)

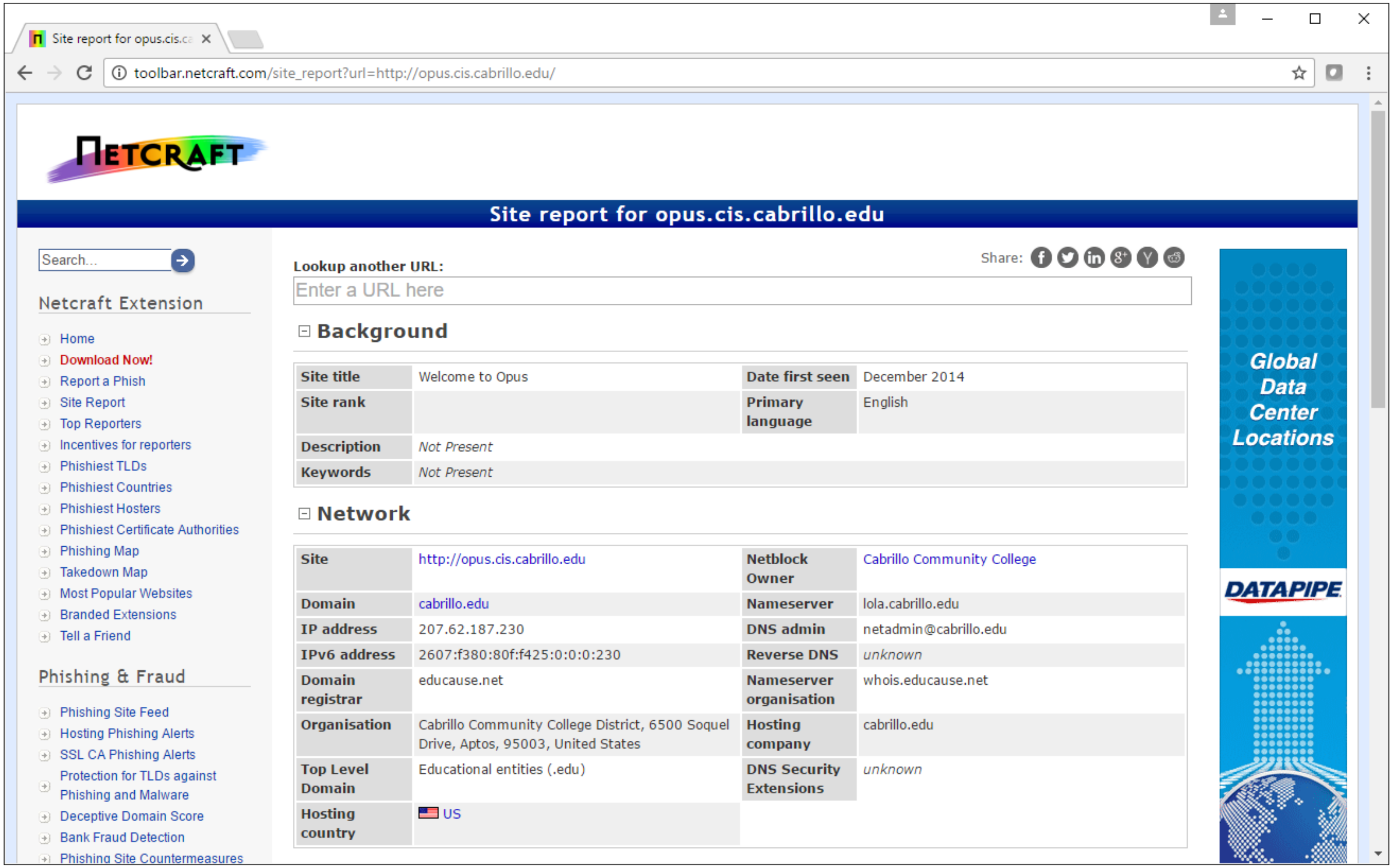
Download this RDP file: vcenter.rdp

(Use right-click Save As ...)

Then open downloaded file to make RDP connection to VLab)

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

Netcraft



Site report for opus.cis.ca
toolbar.netcraft.com/site_report?url=http://opus.cis.cabrillo.edu/
NETCRAFT

Site report for opus.cis.cabrillo.edu

Search...

Netcraft Extension

- Home
- Download Now!
- Report a Phish
- Site Report
- Top Reporters
- Incentives for reporters
- Phishiest TLDs
- Phishiest Countries
- Phishiest Hosters
- Phishiest Certificate Authorities
- Phishing Map
- Takedown Map
- Most Popular Websites
- Branded Extensions
- Tell a Friend

Phishing & Fraud

- Phishing Site Feed
- Hosting Phishing Alerts
- SSL CA Phishing Alerts
- Protection for TLDs against Phishing and Malware
- Deceptive Domain Score
- Bank Fraud Detection
- Phishing Site Countermeasures

Lookup another URL:

Enter a URL here

Share:

⊟ Background

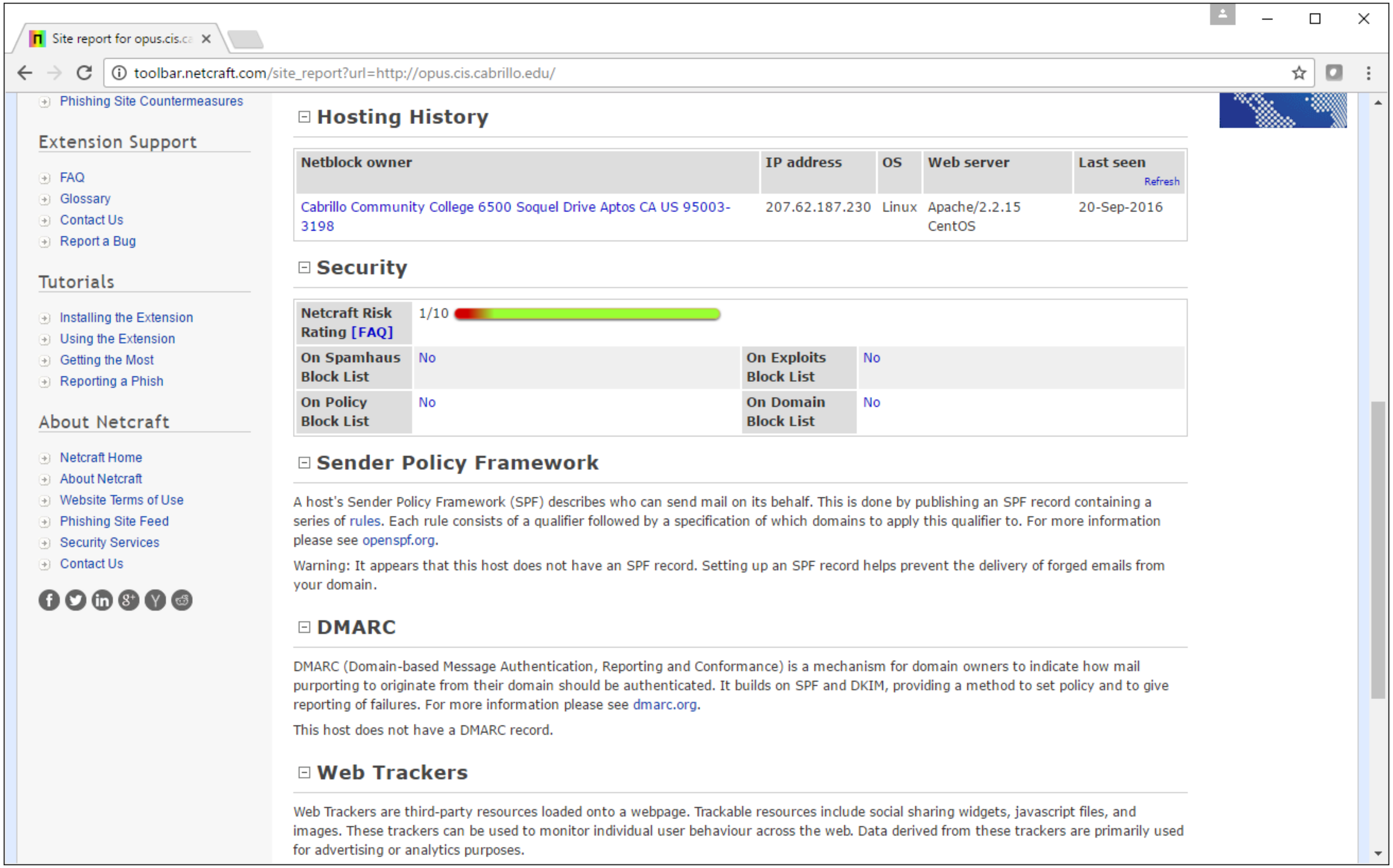
Site title	Welcome to Opus	**Date first seen**	December 2014
Site rank		**Primary language**	English
Description	*Not Present*		
Keywords	*Not Present*		

⊟ Network

Site	http://opus.cis.cabrillo.edu	**Netblock Owner**	Cabrillo Community College
Domain	cabrillo.edu	**Nameserver**	lola.cabrillo.edu
IP address	207.62.187.230	**DNS admin**	netadmin@cabrillo.edu
IPv6 address	2607:f380:80f:f425:0:0:0:230	**Reverse DNS**	*unknown*
Domain registrar	educause.net	**Nameserver organisation**	whois.educause.net
Organisation	Cabrillo Community College District, 6500 Soquel Drive, Aptos, 95003, United States	**Hosting company**	cabrillo.edu
Top Level Domain	Educational entities (.edu)	**DNS Security Extensions**	*unknown*
Hosting country	US		

https://www.netcraft.com/

Netcraft



⊟ Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
Cabrillo Community College 6500 Soquel Drive Aptos CA US 95003-3198	207.62.187.230	Linux	Apache/2.2.15 CentOS	20-Sep-2016

⊟ Security

Netcraft Risk Rating [FAQ]	1/10		
On Spamhaus Block List	No	On Exploits Block List	No
On Policy Block List	No	On Domain Block List	No

⊟ Sender Policy Framework

A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of rules. Each rule consists of a qualifier followed by a specification of which domains to apply this qualifier to. For more information please see openspf.org.

Warning: It appears that this host does not have an SPF record. Setting up an SPF record helps prevent the delivery of forged emails from your domain.

⊟ DMARC

DMARC (Domain-based Message Authentication, Reporting and Conformance) is a mechanism for domain owners to indicate how mail purporting to originate from their domain should be authenticated. It builds on SPF and DKIM, providing a method to set policy and to give reporting of failures. For more information please see dmarc.org.

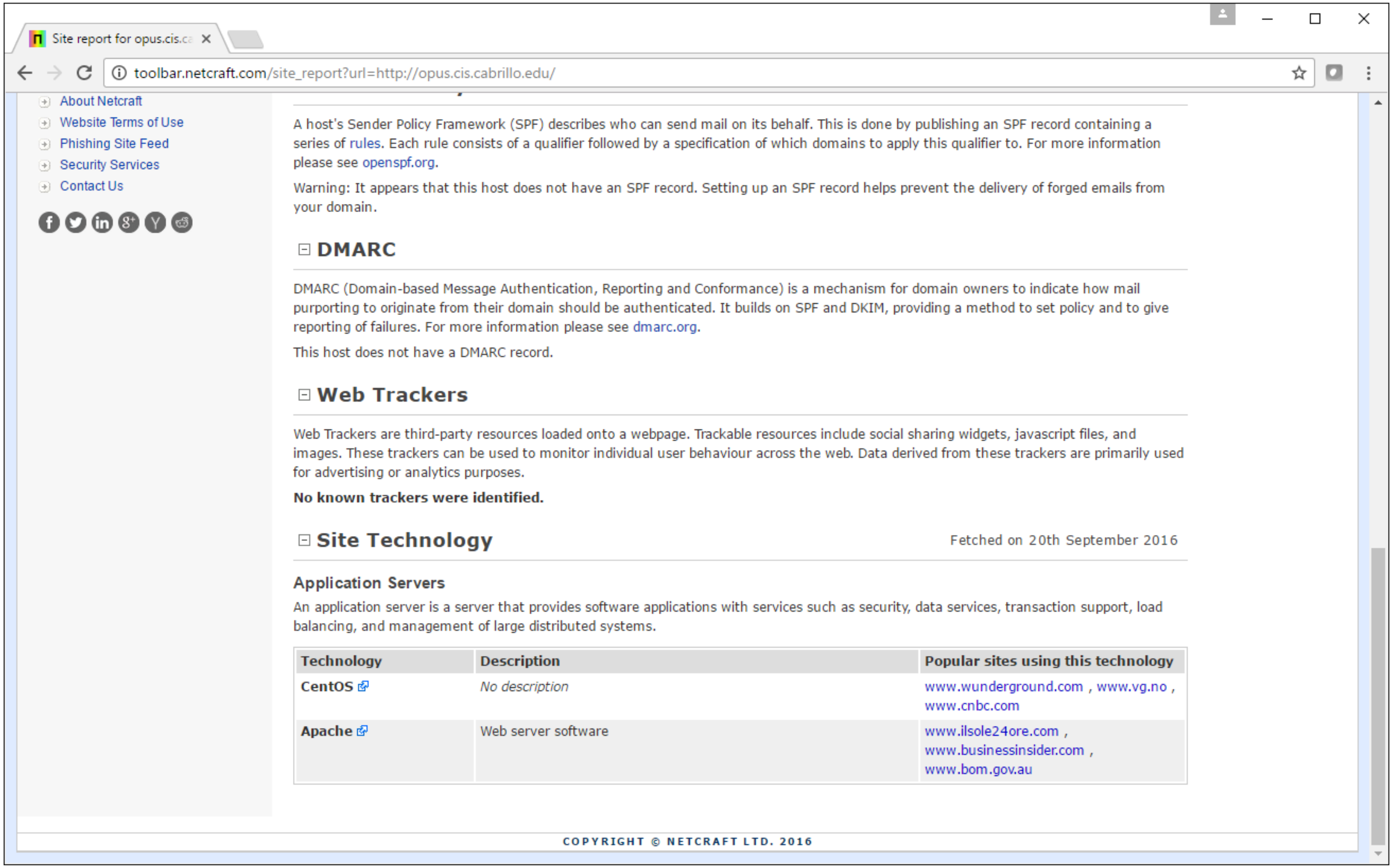
This host does not have a DMARC record.

⊟ Web Trackers

Web Trackers are third-party resources loaded onto a webpage. Trackable resources include social sharing widgets, javascript files, and images. These trackers can be used to monitor individual user behaviour across the web. Data derived from these trackers are primarily used for advertising or analytics purposes.

https://www.netcraft.com/

Netcraft



Site report for opus.cis.c
toolbar.netcraft.com/site_report?url=http://opus.cis.cabrillo.edu/
About Netcraft
Website Terms of Use
Phishing Site Feed
Security Services
Contact Us

A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of rules. Each rule consists of a qualifier followed by a specification of which domains to apply this qualifier to. For more information please see openspf.org.

Warning: It appears that this host does not have an SPF record. Setting up an SPF record helps prevent the delivery of forged emails from your domain.

⊟ DMARC

DMARC (Domain-based Message Authentication, Reporting and Conformance) is a mechanism for domain owners to indicate how mail purporting to originate from their domain should be authenticated. It builds on SPF and DKIM, providing a method to set policy and to give reporting of failures. For more information please see dmarc.org.

This host does not have a DMARC record.

⊟ Web Trackers

Web Trackers are third-party resources loaded onto a webpage. Trackable resources include social sharing widgets, javascript files, and images. These trackers can be used to monitor individual user behaviour across the web. Data derived from these trackers are primarily used for advertising or analytics purposes.

No known trackers were identified.

⊟ Site Technology

Fetched on 20th September 2016

Application Servers

An application server is a server that provides software applications with services such as security, data services, transaction support, load balancing, and management of large distributed systems.

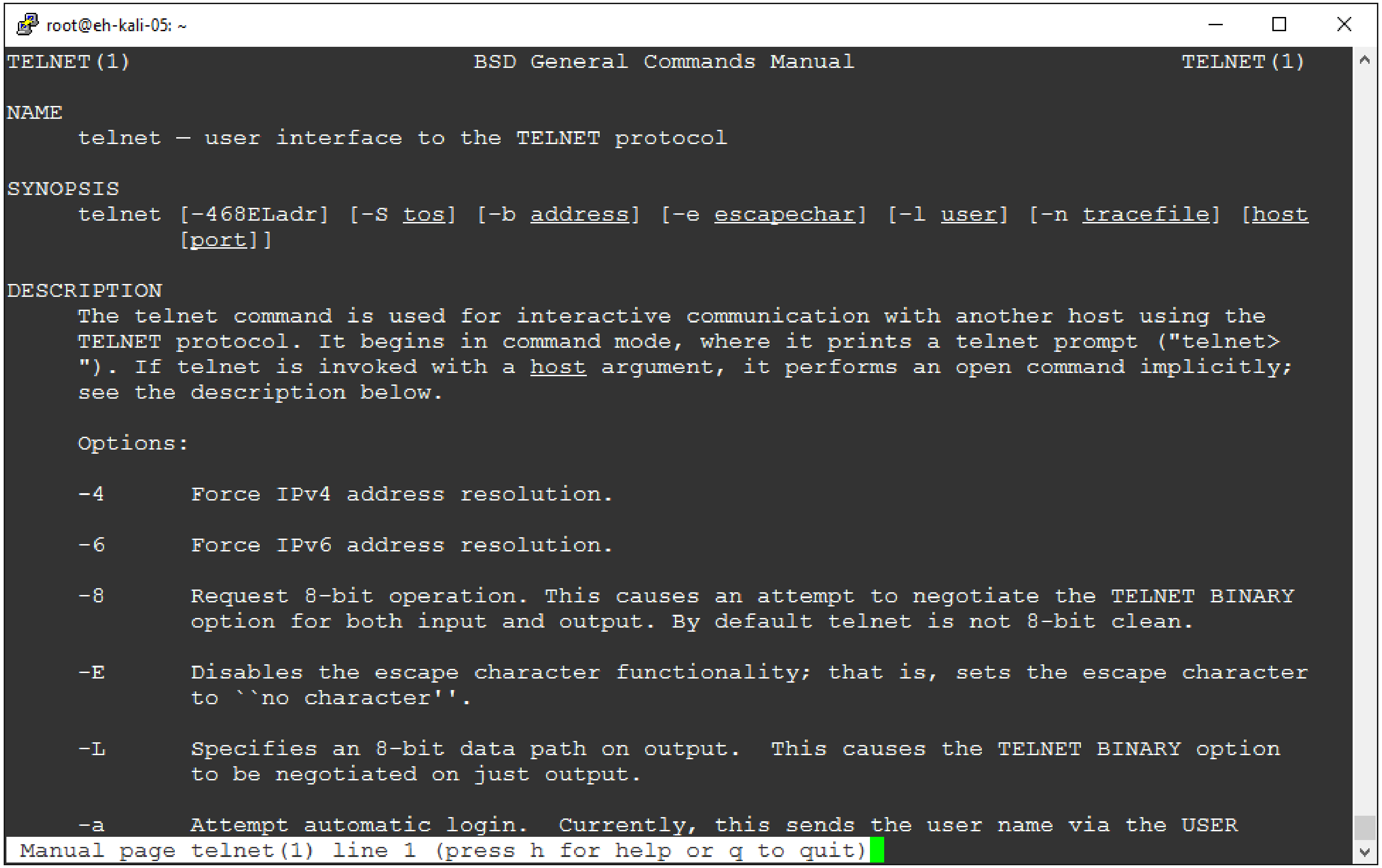
Technology	Description	Popular sites using this technology
CentOS	*No description*	www.wunderground.com , www.vg.no , www.cnbc.com
Apache	Web server software	www.ilsole24ore.com , www.businessinsider.com , www.bom.gov.au

COPYRIGHT © NETCRAFT LTD. 2016

https://www.netcraft.com/

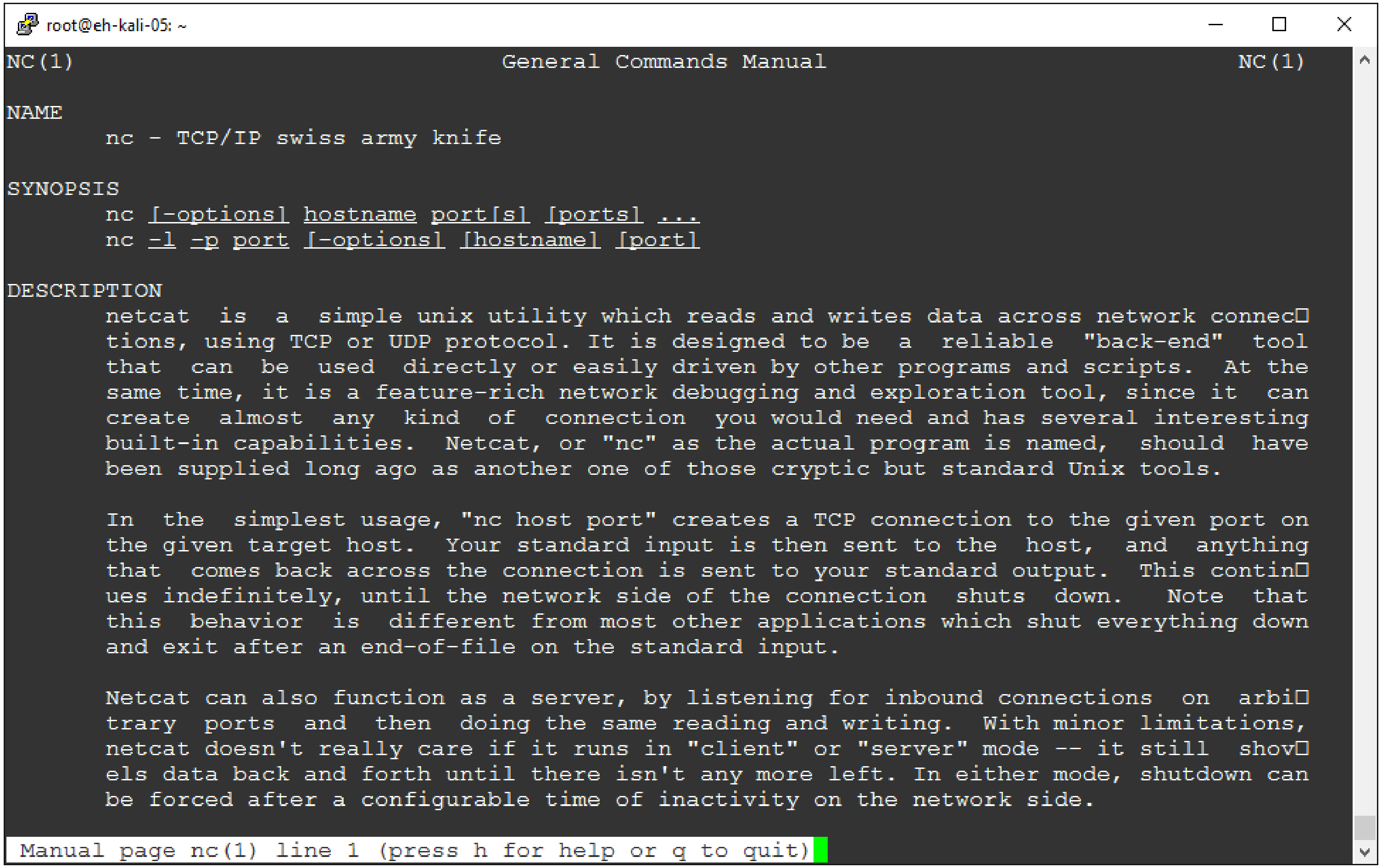
Light probing with telnet

telnet command



```
TELNET(1)                  BSD General Commands Manual                 TELNET(1)

NAME
     telnet — user interface to the TELNET protocol

SYNOPSIS
     telnet [-468ELadr] [-S tos] [-b address] [-e escapechar] [-l user] [-n tracefile] [host
            [port]]

DESCRIPTION
     The telnet command is used for interactive communication with another host using the
     TELNET protocol. It begins in command mode, where it prints a telnet prompt ("telnet>
     "). If telnet is invoked with a host argument, it performs an open command implicitly;
     see the description below.

     Options:

     -4      Force IPv4 address resolution.

     -6      Force IPv6 address resolution.

     -8      Request 8-bit operation. This causes an attempt to negotiate the TELNET BINARY
             option for both input and output. By default telnet is not 8-bit clean.

     -E      Disables the escape character functionality; that is, sets the escape character
             to ``no character''.

     -L      Specifies an 8-bit data path on output.  This causes the TELNET BINARY option
             to be negotiated on just output.

     -a      Attempt automatic login.  Currently, this sends the user name via the USER
 Manual page telnet(1) line 1 (press h for help or q to quit)
```

netcat



```
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 connec□
       tions, 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 contin□
       ues 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  arbi□
       trary  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  shov□
       els 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

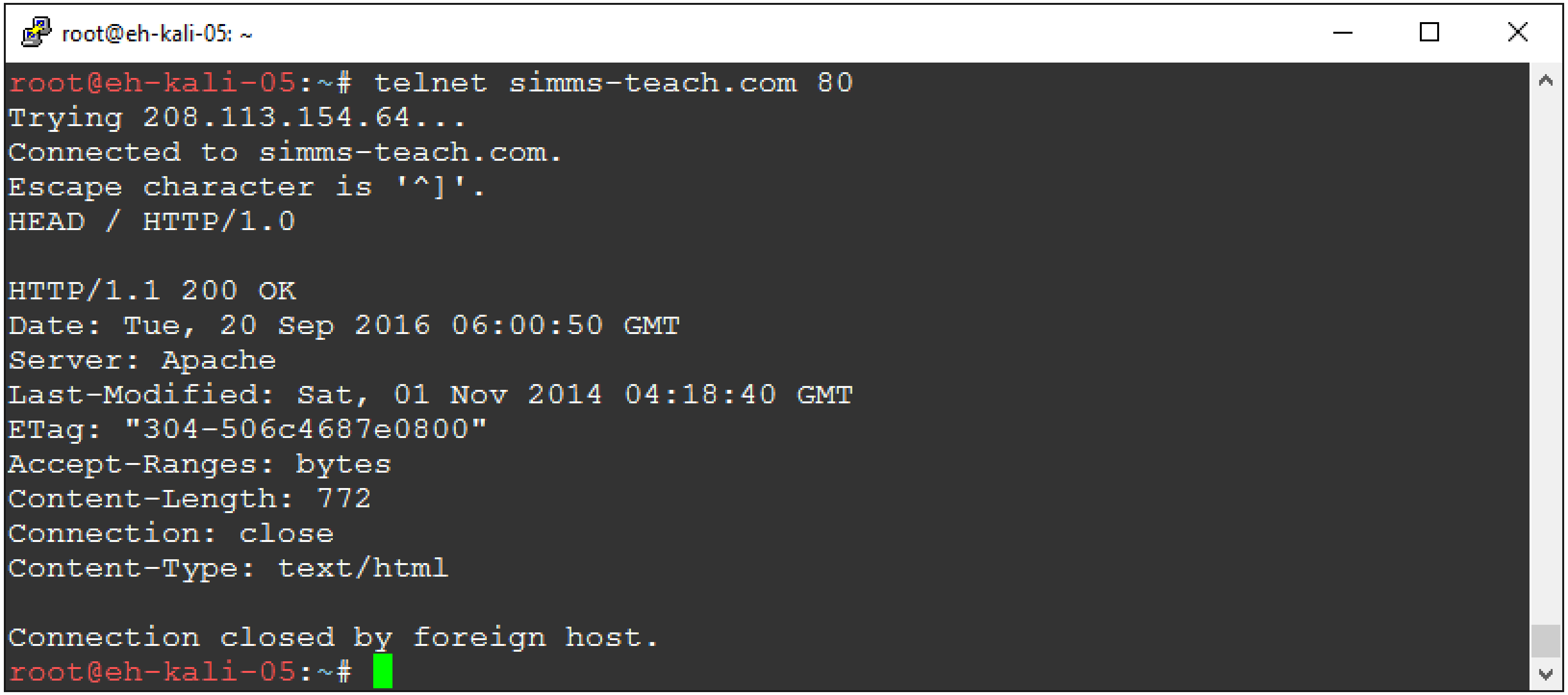
telnet <host-or-IP-addess> <port>

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

Probing simms-teach.com

telnet simms-teach.com 80

nc -v simms-teach.com 80



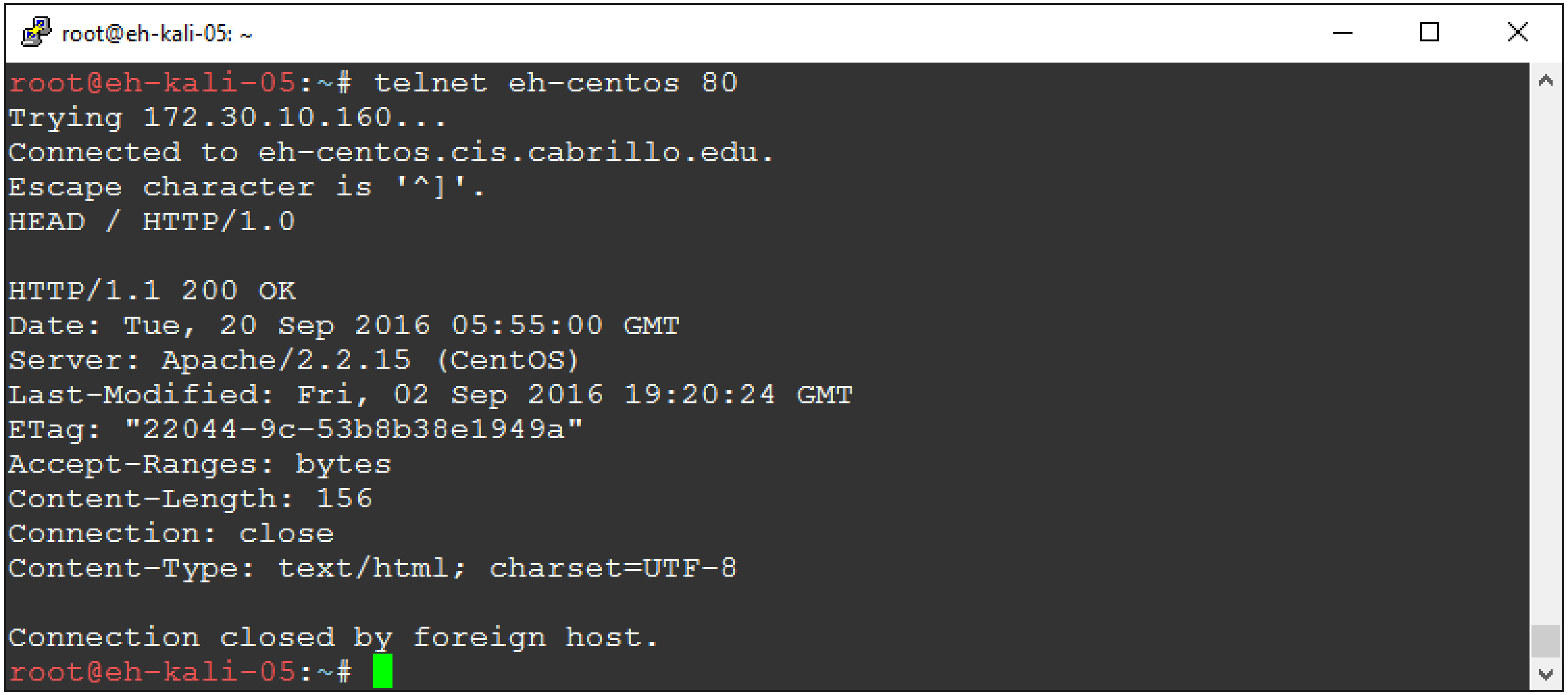
```
root@eh-kali-05:~# telnet simms-teach.com 80
Trying 208.113.154.64...
Connected to simms-teach.com.
Escape character is '^]'.
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Date: Tue, 20 Sep 2016 06:00:50 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

Connection closed by foreign host.
root@eh-kali-05:~#
```

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

Probing eh-centos VM

telnet eh-centos 80

nc -v eh-centos 80



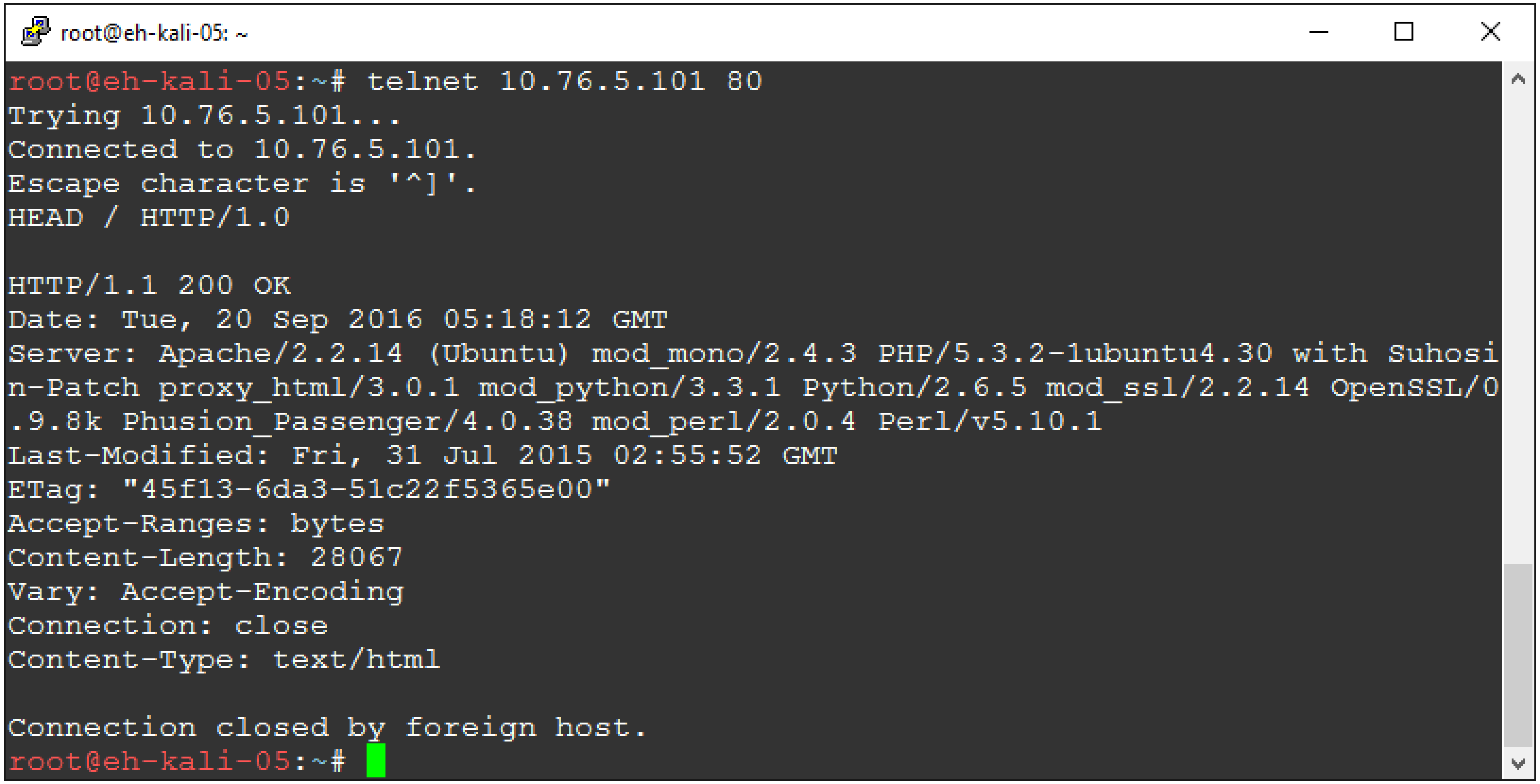
root@eh-kali-05: ~

```
root@eh-kali-05:~# telnet eh-centos 80
Trying 172.30.10.160...
Connected to eh-centos.cis.cabrillo.edu.
Escape character is '^]'.
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Date: Tue, 20 Sep 2016 05:55:00 GMT
Server: Apache/2.2.15 (CentOS)
Last-Modified: Fri, 02 Sep 2016 19:20:24 GMT
ETag: "22044-9c-53b8b38e1949a"
Accept-Ranges: bytes
Content-Length: 156
Connection: close
Content-Type: text/html; charset=UTF-8

Connection closed by foreign host.
root@eh-kali-05:~#
```

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

Probing OWASP VM

telnet 10.76.5.101 80 **nc -v 10.76.5.101 80**



```
root@eh-kali-05:~# telnet 10.76.5.101 80
Trying 10.76.5.101...
Connected to 10.76.5.101.
Escape character is '^]'.
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Date: Tue, 20 Sep 2016 05:18:12 GMT
Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosi
n-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

Connection closed by foreign host.
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.

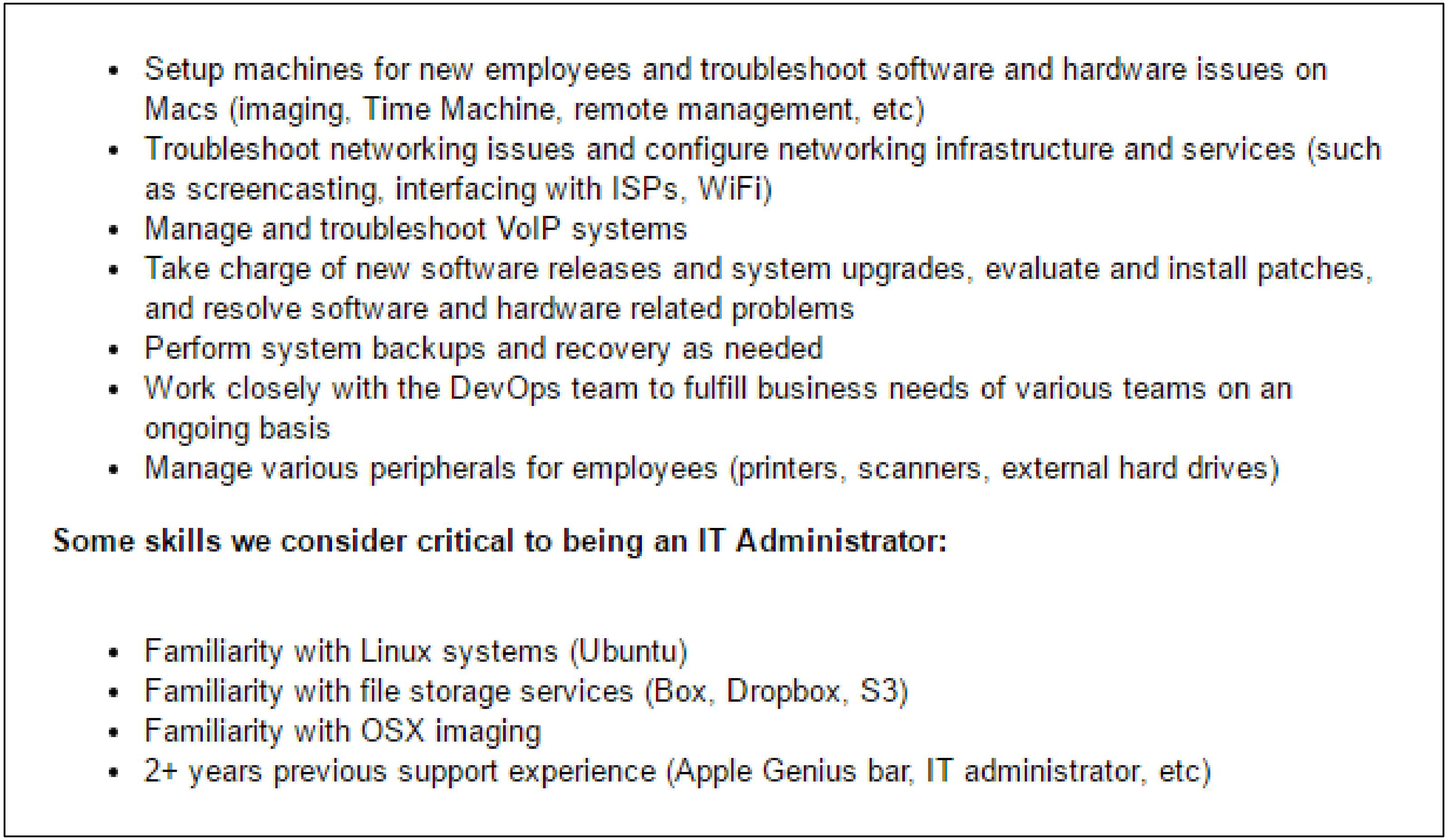
Put the mail header which looks like this:

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

into the chat window

Job Openings

Job title: IT Administrator



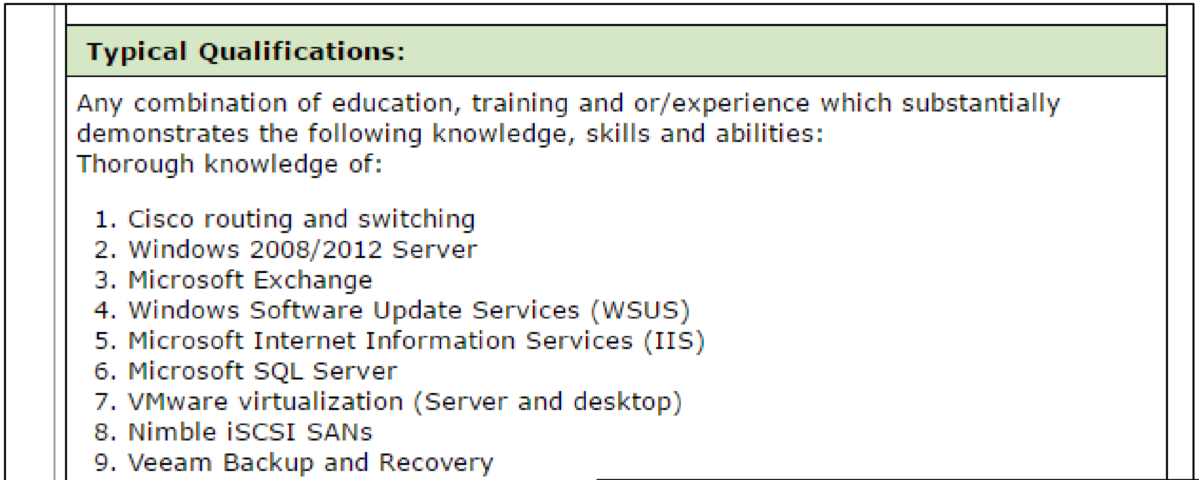
- Setup machines for new employees and troubleshoot software and hardware issues on Macs (imaging, Time Machine, remote management, etc)
- Troubleshoot networking issues and configure networking infrastructure and services (such as screencasting, interfacing with ISPs, WiFi)
- Manage and troubleshoot 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/

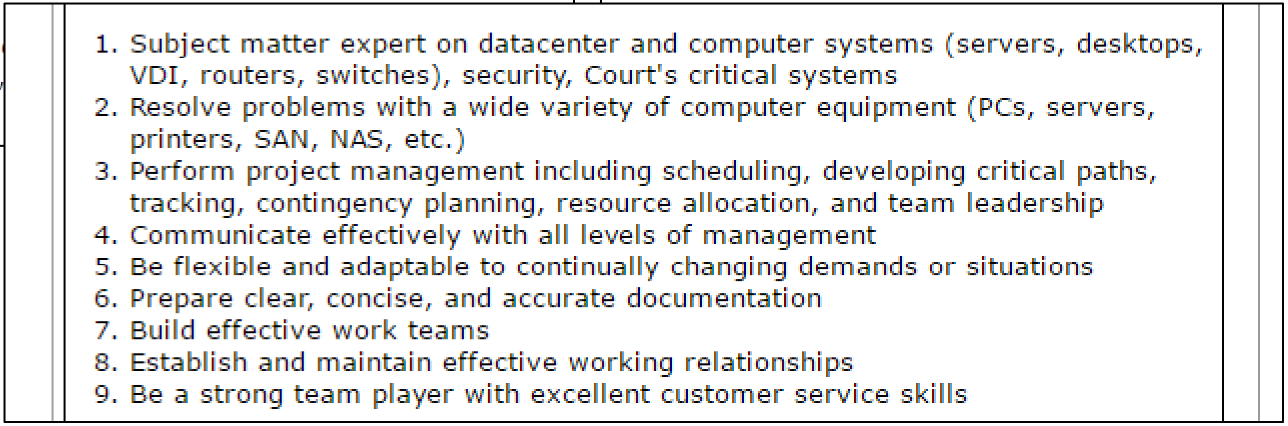
Job title: System Administrator



Typical Qualifications:

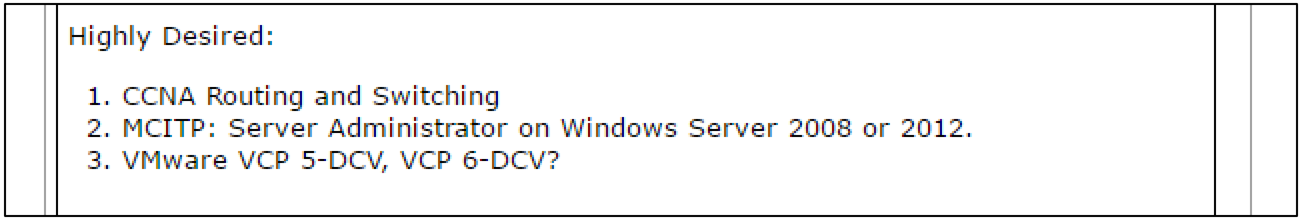
Any combination of education, training and or/experience which substantially demonstrates the following knowledge, skills and abilities:
Thorough knowledge of:

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,



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

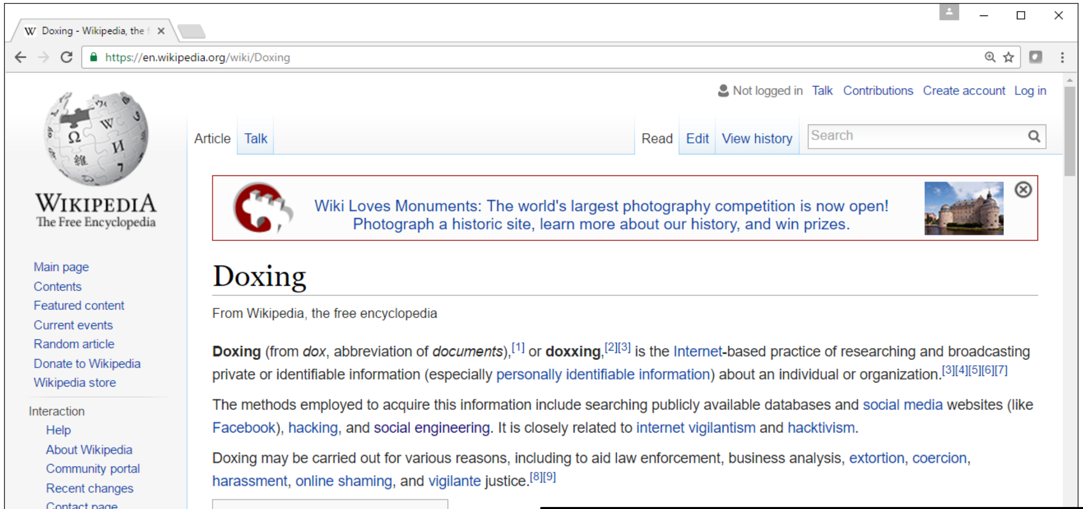
Browse the technical job listings on monster.com or indeed.com.

Did you find any specific system or network information?

If so put what you found in the chat window

doxing and pipl

Doxing



Doxing - Wikipedia, the f

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

Not logged in Talk Contributions Create account Log in

Article Talk Read Edit View history Search

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools
What links here
Related changes
Upload file
Special pages
Permanent link
Page information
Wikidata item
Cite this page

Print/export

Wiki Loves Monuments: The world's largest photography competition is now open!
Photograph a historic site, learn more about our history, and win prizes.

Doxing

From Wikipedia, the free encyclopedia

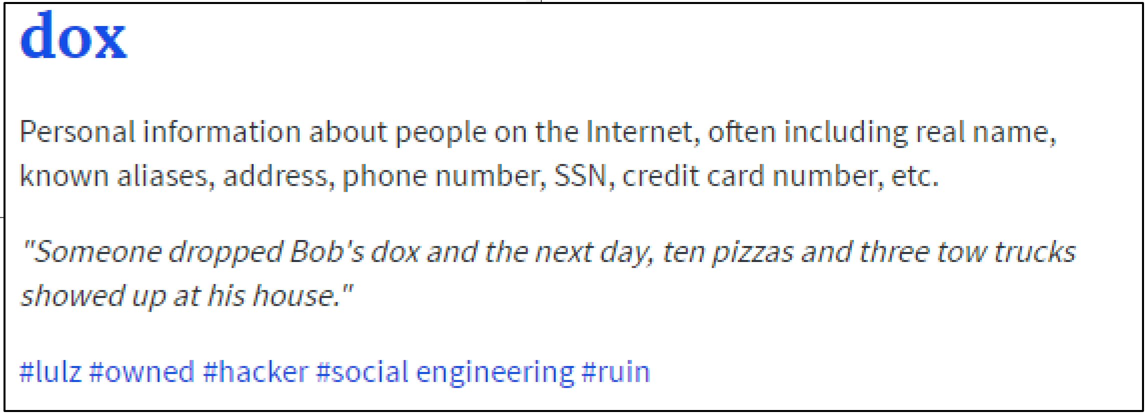
Doxing (from *dox*, abbreviation of *documents*),[1] or **doxing**,[2][3] is the Internet-based practice of researching and broadcasting private or identifiable information (especially personally identifiable information) about an individual or organization.[3][4][5][6][7]

The methods employed to acquire this information include searching publicly available databases and social media websites (like Facebook), hacking, and social engineering. It is closely related to internet vigilantism and hacktivism.

Doxing may be carried out for various reasons, including to aid law enforcement, business analysis, extortion, coercion, harassment, online shaming, and vigilante justice.[8][9]

Contents [hide]

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.

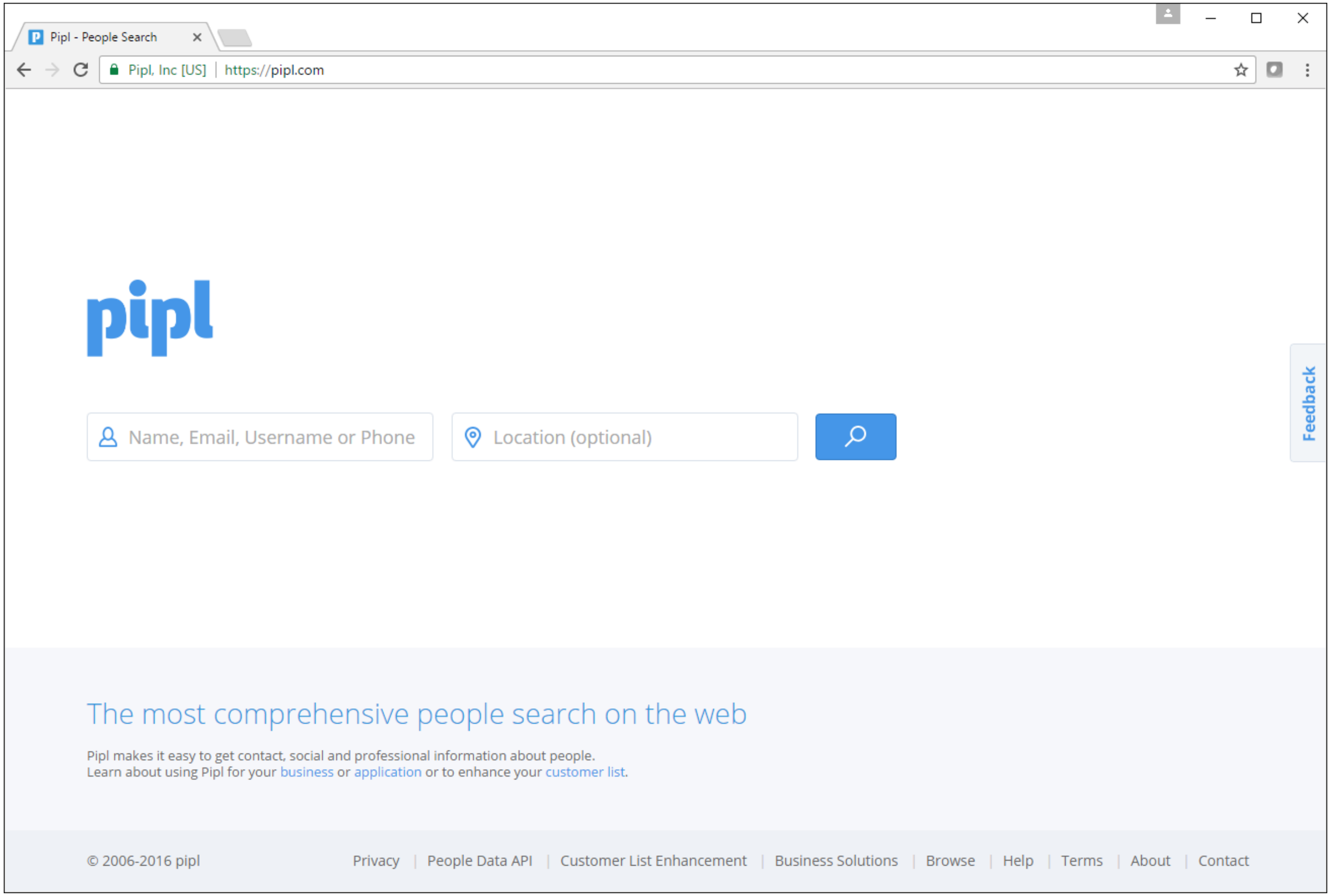
"Someone dropped Bob's dox and the next day, ten pizzas and three tow trucks showed up at his house."

#lulz #owned #hacker #social engineering #ruin

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

Creating a "dossier" on someone or an organization

pipl



Pipl - People Search
Pipl, Inc [US] | https://pipl.com
pipl
Name, Email, Username or Phone
Location (optional)
Feedback

The most comprehensive people search on the web

Pipl makes it easy to get contact, social and professional information about people.
Learn about using Pipl for your business or application or to enhance your customer list.

© 2006-2016 pipl

Privacy | People Data API | Customer List Enhancement | Business Solutions | Browse | Help | Terms | About | Contact

Lookup information on people

Activity

pipl yourself to see how effective this web site is.

Did it find more about you than you expected?

Write your answer in the chat window

Website Information

firebug

Web Data Extractor

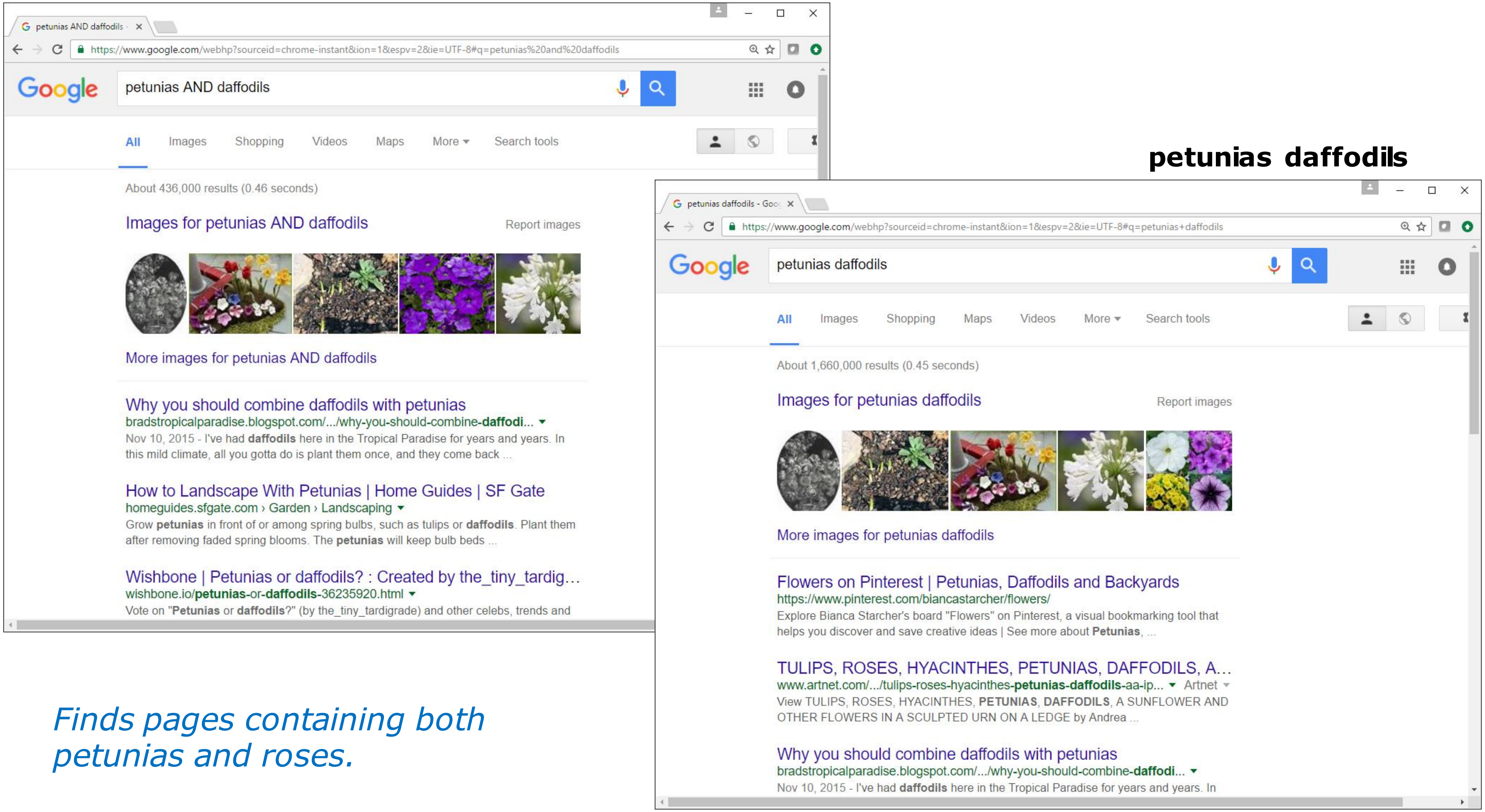
diggity

Google Hacking

Google Hacking with AND (or space) operator

petunias AND daffodils

petunias daffodils



petunias AND daffodils -
https://www.google.com/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=petunias%20and%20daffodils
Google
petunias AND daffodils
All
Images
Shopping
Videos
Maps
More
Search tools

About 436,000 results (0.46 seconds)

Images for petunias AND daffodils

Report images

More images for petunias AND daffodils

Why you should combine daffodils with petunias
bradstropicalparadise.blogspot.com/.../why-you-should-combine-daffodi...
Nov 10, 2015 - I've had **daffodils** here in the Tropical Paradise for years and years. In this mild climate, all you gotta do is plant them once, and they come back ...

How to Landscape With Petunias | Home Guides | SF Gate
homeguides.sfgate.com › Garden › Landscaping
Grow **petunias** in front of or among spring bulbs, such as tulips or **daffodils**. Plant them after removing faded spring blooms. The **petunias** will keep bulb beds ...

Wishbone | Petunias or daffodils? : Created by the_tiny_tardig...
wishbone.io/**petunias**-or-**daffodils**-36235920.html
Vote on "**Petunias** or **daffodils**?" (by the_tiny_tardigrade) and other celebs, trends and

petunias daffodils - Goo
https://www.google.com/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=petunias+daffodils
Google
petunias daffodils
All
Images
Shopping
Maps
Videos
More
Search tools

About 1,660,000 results (0.45 seconds)

Images for petunias daffodils

Report images

More images for petunias daffodils

Flowers on Pinterest | Petunias, Daffodils and Backyards
https://www.pinterest.com/biancastarcher/flowers/
Explore Bianca Starcher's board "Flowers" on Pinterest, a visual bookmarking tool that helps you discover and save creative ideas | See more about **Petunias**, ...

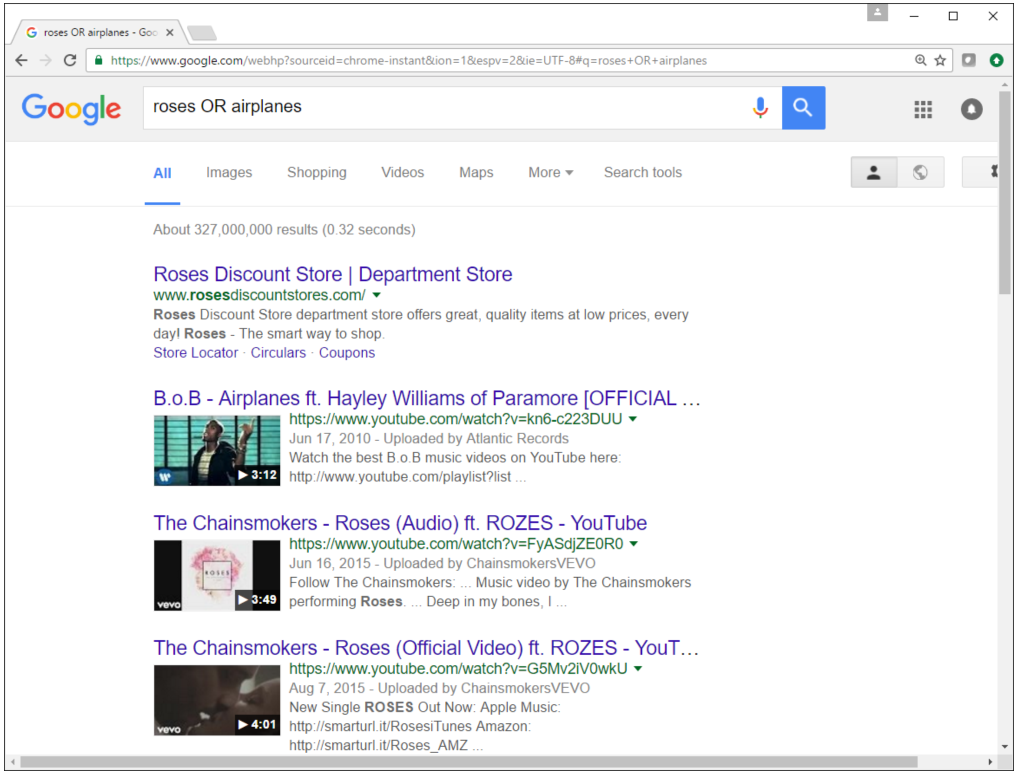
TULIPS, ROSES, HYACINTHES, PETUNIAS, DAFFODILS, A...
www.artnet.com/.../tulips-roses-hyacinthes-**petunias-daffodils**-aa-ip... ▾ Artnet ▾
View TULIPS, ROSES, HYACINTHES, **PETUNIAS**, **DAFFODILS**, A SUNFLOWER AND OTHER FLOWERS IN A SCULPTED URN ON A LEDGE by Andrea ...

Why you should combine daffodils with petunias
bradstropicalparadise.blogspot.com/.../why-you-should-combine-daffodi...
Nov 10, 2015 - I've had **daffodils** here in the Tropical Paradise for years and years. In

Finds pages containing both petunias and roses.

Google Hacking with OR (or |) operator

roses OR airplanes



roses OR airplanes - Goo
https://www.google.com/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=roses+OR+airplanes
Google
All
Images
Shopping
Videos
Maps
More
Search tools

roses OR airplanes

About 327,000,000 results (0.32 seconds)

Roses Discount Store | Department Store
www.rosesdiscountstores.com/
Roses Discount Store department store offers great, quality items at low prices, every day! Roses - The smart way to shop.
Store Locator · Circulars · Coupons

B.o.B - Airplanes ft. Hayley Williams of Paramore [OFFICIAL ...
https://www.youtube.com/watch?v=kn6-c223DUU
Jun 17, 2010 - Uploaded by Atlantic Records
Watch the best B.o.B music videos on YouTube here: http://www.youtube.com/playlist?list ...
3:12

The Chainsmokers - Roses (Audio) ft. ROZES - YouTube
https://www.youtube.com/watch?v=FyASdjZE0R0
Jun 16, 2015 - Uploaded by ChainsmokersVEVO
Follow The Chainsmokers: ... Music video by The Chainsmokers performing Roses. ... Deep in my bones, I ...
3:49

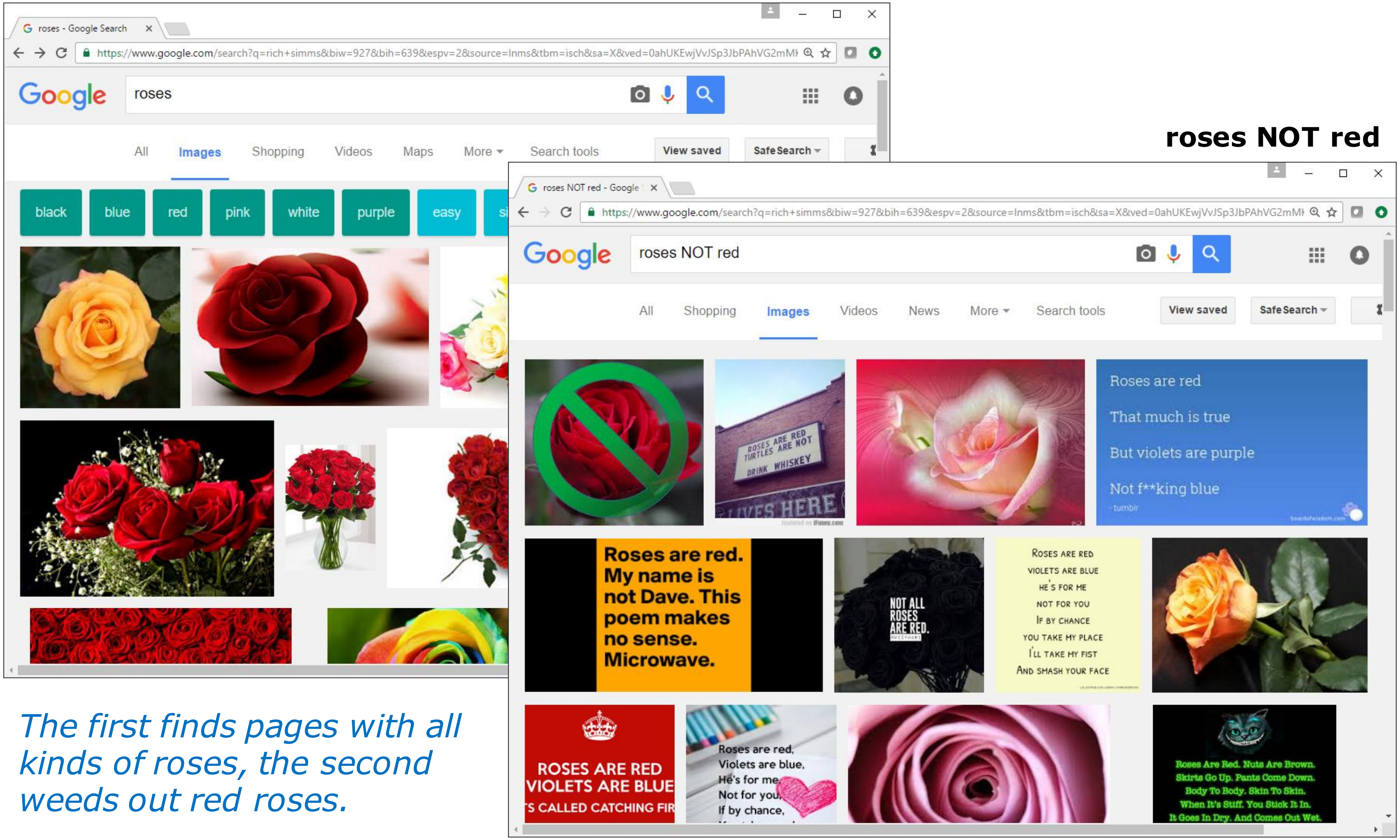
The Chainsmokers - Roses (Official Video) ft. ROZES - YouT...
https://www.youtube.com/watch?v=G5Mv2iV0wkU
Aug 7, 2015 - Uploaded by ChainsmokersVEVO
New Single ROSES Out Now: Apple Music: http://smarturl.it/RosesiTunes Amazon: http://smarturl.it/Roses_AMZ ...
4:01

Finds pages with roses or pages with airplanes.

Google Hacking with NOT (or -) operator

roses

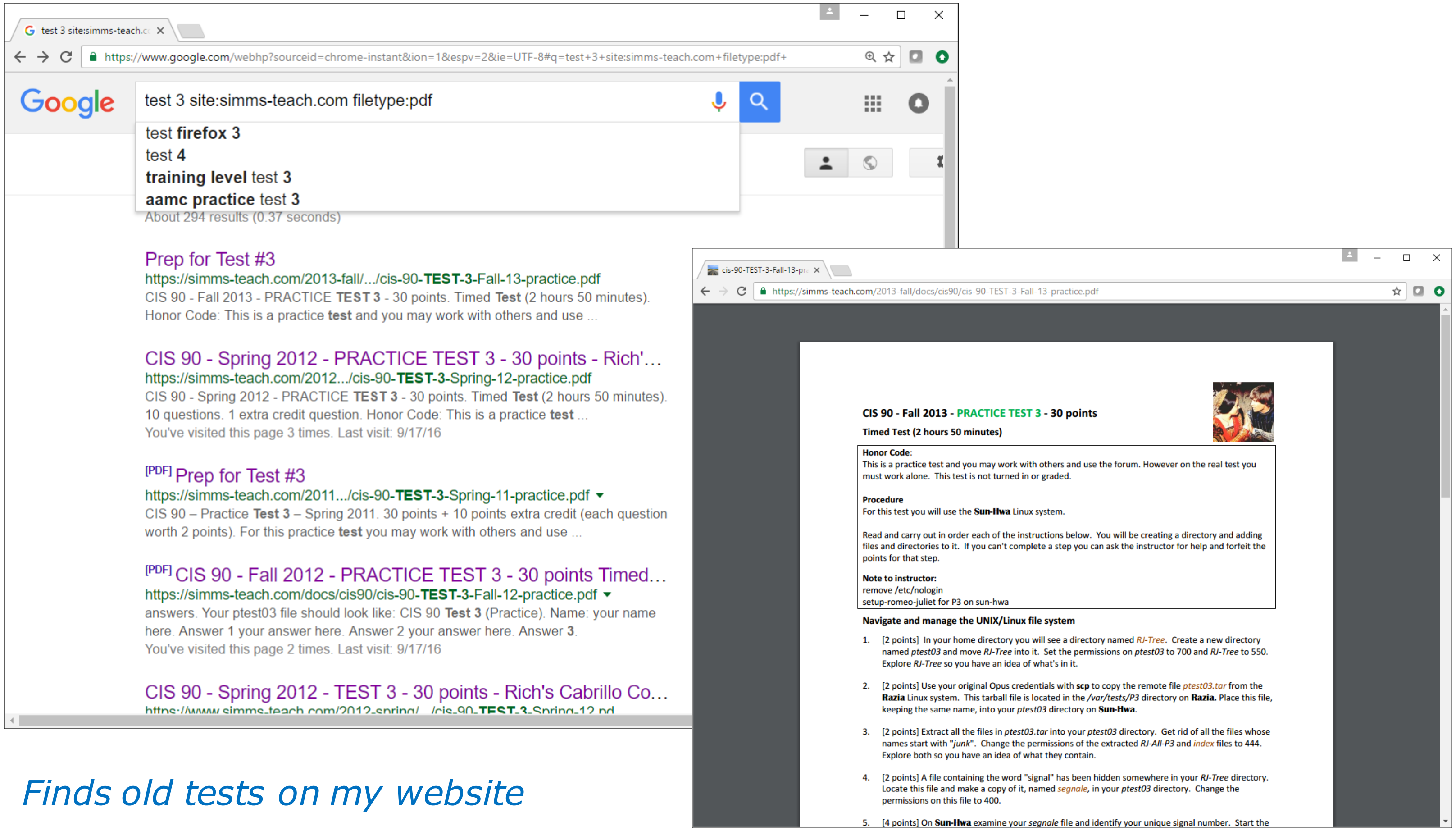
roses NOT red



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



https://www.google.com/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=test+3+site:simms-teach.com+filetype:pdf+

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

test **firefox 3**
test **4**
training level test **3**
aamc practice test **3**

About 294 results (0.37 seconds)

Prep for Test #3
https://simms-teach.com/2013-fall/.../cis-90-**TEST-3**-Fall-13-practice.pdf
CIS 90 - Fall 2013 - PRACTICE **TEST 3** - 30 points. Timed **Test** (2 hours 50 minutes). Honor Code: This is a practice **test** and you may work with others and use ...

CIS 90 - Spring 2012 - PRACTICE TEST 3 - 30 points - Rich'...
https://simms-teach.com/2012.../cis-90-**TEST-3**-Spring-12-practice.pdf
CIS 90 - Spring 2012 - PRACTICE **TEST 3** - 30 points. Timed **Test** (2 hours 50 minutes). 10 questions. 1 extra credit question. Honor Code: This is a practice **test** ...
You've visited this page 3 times. Last visit: 9/17/16

[PDF] Prep for Test #3
https://simms-teach.com/2011.../cis-90-**TEST-3**-Spring-11-practice.pdf ▾
CIS 90 – Practice **Test 3** – Spring 2011. 30 points + 10 points extra credit (each question worth 2 points). For this practice **test** you may work with others and use ...

[PDF] CIS 90 - Fall 2012 - PRACTICE TEST 3 - 30 points Timed...
https://simms-teach.com/docs/cis90/cis-90-**TEST-3**-Fall-12-practice.pdf ▾
answers. Your ptest03 file should look like: CIS 90 **Test 3** (Practice). Name: your name here. Answer 1 your answer here. Answer 2 your answer here. Answer **3**.
You've visited this page 2 times. Last visit: 9/17/16

CIS 90 - Spring 2012 - TEST 3 - 30 points - Rich's Cabrillo Co...
https://www.simms-teach.com/2012-spring/.../cis-90-**TEST-3**-Spring-12.pd

https://simms-teach.com/2013-fall/docs/cis90/cis-90-TEST-3-Fall-13-practice.pdf

CIS 90 - Fall 2013 - PRACTICE TEST 3 - 30 points

Timed Test (2 hours 50 minutes)

Honor Code:
This is a practice test and you may work with others and use the forum. However on the real test you must work alone. This test is not turned in or graded.

Procedure
For this test you will use the **Sun-Hwa** Linux system.

Read and carry out in order each of the instructions below. You will be creating a directory and adding files and directories to it. If you can't complete a step you can ask the instructor for help and forfeit the points for that step.

Note to instructor:
remove /etc/nologin
setup-romeo-juliet for P3 on sun-hwa

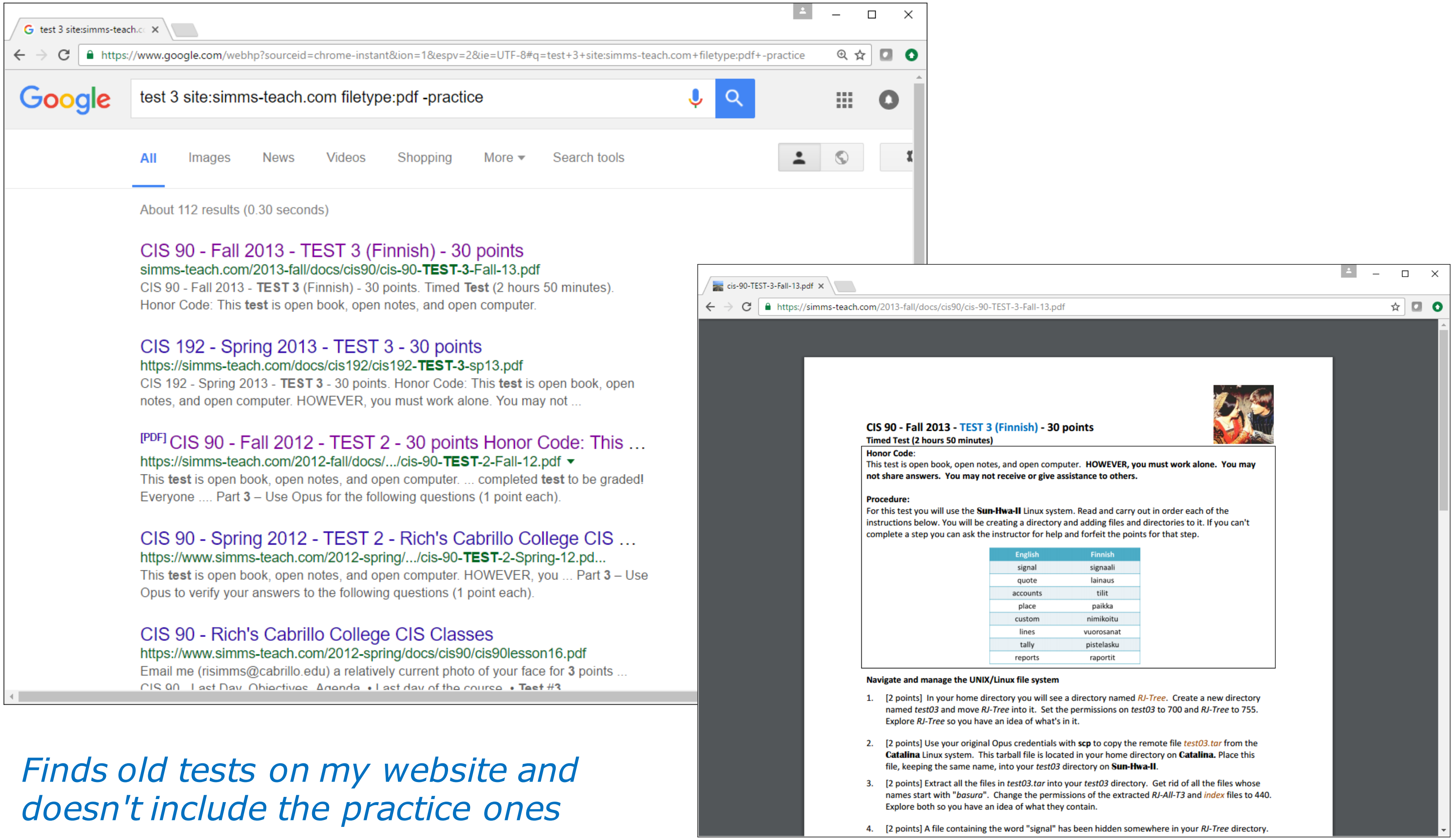
Navigate and manage the UNIX/Linux file system

1. [2 points] In your home directory you will see a directory named *RJ-Tree*. Create a new directory named *ptest03* and move *RJ-Tree* into it. Set the permissions on *ptest03* to 700 and *RJ-Tree* to 550. Explore *RJ-Tree* so you have an idea of what's in it.
2. [2 points] Use your original Opus credentials with **scp** to copy the remote file *ptest03.tar* from the **Razia** Linux system. This tarball file is located in the */var/tests/P3* directory on **Razia.** Place this file, keeping the same name, into your *ptest03* directory on **Sun-Hwa**.
3. [2 points] Extract all the files in *ptest03.tar* into your *ptest03* directory. Get rid of all the files whose names start with "*junk*". Change the permissions of the extracted *RJ-All-P3* and *index* files to 444. Explore both so you have an idea of what they contain.
4. [2 points] A file containing the word "signal" has been hidden somewhere in your *RJ-Tree* directory. Locate this file and make a copy of it, named *segnale*, in your *ptest03* directory. Change the permissions on this file to 400.
5. [4 points] On **Sun-Hwa** examine your *segnale* file and identify your unique signal number. Start the

Finds old tests on my website

Google Hacking with site: and filetype: operators

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


test 3 site:simms-teach.c ×
https://www.google.com/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=test+3+site:simms-teach.com+filetype:pdf+-practice
Google
All
Images
News
Videos
Shopping
More ▾
Search tools

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

About 112 results (0.30 seconds)

CIS 90 - Fall 2013 - TEST 3 (Finnish) - 30 points
simms-teach.com/2013-fall/docs/cis90/cis-90-**TEST**-3-Fall-13.pdf
CIS 90 - Fall 2013 - **TEST 3** (Finnish) - 30 points. Timed **Test** (2 hours 50 minutes). Honor Code: This **test** is open book, open notes, and open computer.

CIS 192 - Spring 2013 - TEST 3 - 30 points
https://simms-teach.com/docs/cis192/cis192-**TEST**-3-sp13.pdf
CIS 192 - Spring 2013 - **TEST 3** - 30 points. Honor Code: This **test** is open book, open notes, and open computer. HOWEVER, you must work alone. You may not ...

[PDF] CIS 90 - Fall 2012 - TEST 2 - 30 points Honor Code: This ...
https://simms-teach.com/2012-fall/docs/.../cis-90-**TEST**-2-Fall-12.pdf ▾
This **test** is open book, open notes, and open computer. ... completed **test** to be graded! Everyone .... Part **3** – Use Opus for the following questions (1 point each).

CIS 90 - Spring 2012 - TEST 2 - Rich's Cabrillo College CIS ...
https://www.simms-teach.com/2012-spring/.../cis-90-**TEST**-2-Spring-12.pd...
This **test** is open book, open notes, and open computer. HOWEVER, you ... Part **3** – Use Opus to verify your answers to the following questions (1 point each).

CIS 90 - Rich's Cabrillo College CIS Classes
https://www.simms-teach.com/2012-spring/docs/cis90/cis90lesson16.pdf
Email me (risimms@cabrillo.edu) a relatively current photo of your face for **3** points ...
CIS 90 ... Last Day Objectives Agenda • Last day of the course • **Test** #3

cis-90-TEST-3-Fall-13.pdf ×
https://simms-teach.com/2013-fall/docs/cis90/cis-90-TEST-3-Fall-13.pdf

CIS 90 - Fall 2013 - TEST 3 (Finnish) - 30 points
Timed Test (2 hours 50 minutes)

Honor Code:
This test is open book, open notes, and open computer. **HOWEVER, you must work alone. You may not share answers. You may not receive or give assistance to others.**

Procedure:
For this test you will use the **Sun-Hwa-II** Linux system. Read and carry out in order each of the instructions below. You will be creating a directory and adding files and directories to it. If you can't complete a step you can ask the instructor for help and forfeit the points for that step.

English	Finnish
signal	signaali
quote	lainaus
accounts	tilit
place	paikka
custom	nimikoitu
lines	vuorosanat
tally	pistelasku
reports	raportit

Navigate and manage the UNIX/Linux file system

1. [2 points] In your home directory you will see a directory named *RJ-Tree*. Create a new directory named *test03* and move *RJ-Tree* into it. Set the permissions on *test03* to 700 and *RJ-Tree* to 755. Explore *RJ-Tree* so you have an idea of what's in it.

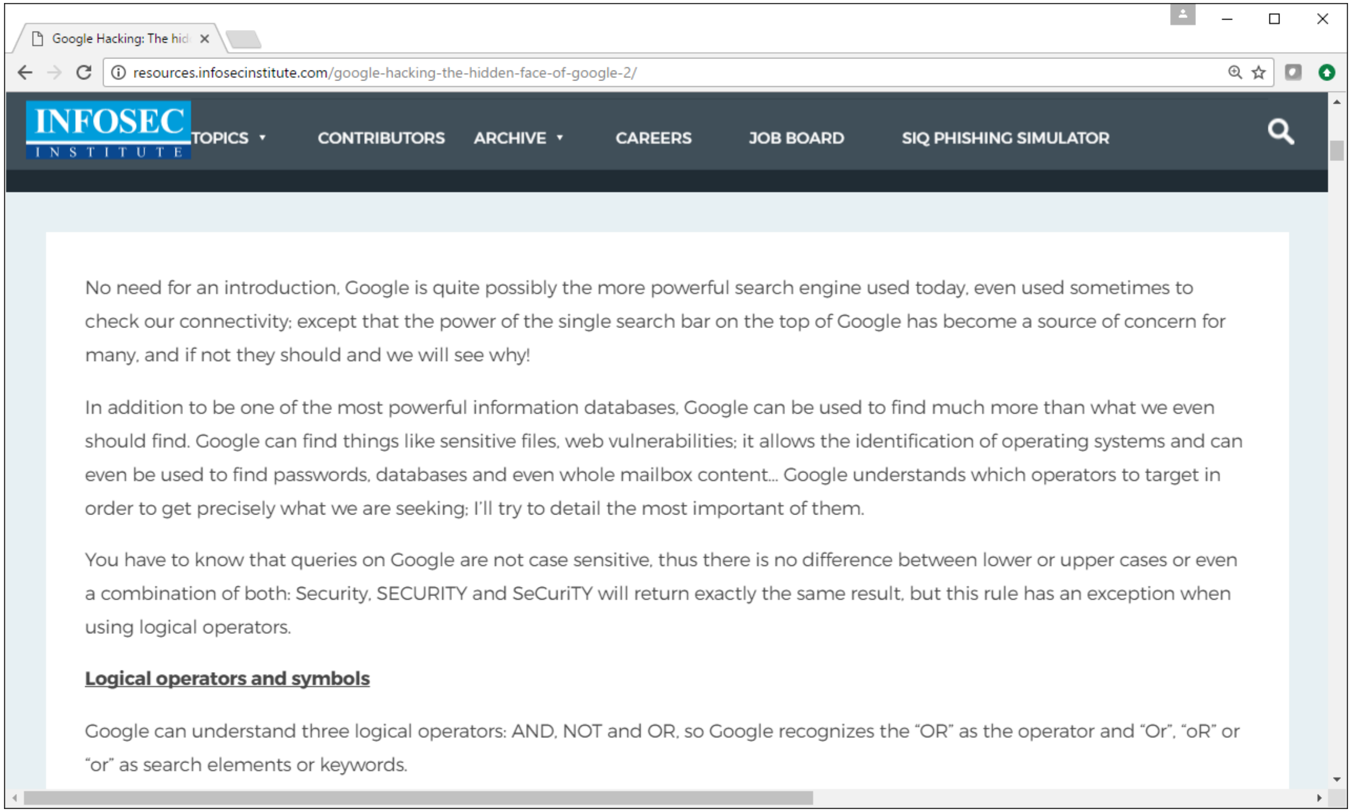
2. [2 points] Use your original Opus credentials with **scp** to copy the remote file *test03.tar* from the **Catalina** Linux system. This tarball file is located in your home directory on **Catalina.** Place this file, keeping the same name, into your *test03* directory on **Sun-Hwa-II**.

3. [2 points] Extract all the files in *test03.tar* into your *test03* directory. Get rid of all the files whose names start with "*basura*". Change the permissions of the extracted *RJ-All-T3* and *index* files to 440. Explore both so you have an idea of what they contain.

4. [2 points] A file containing the word "signal" has been hidden somewhere in your *RJ-Tree* directory.

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

Google Hacking: The hidden face of Google



No need for an introduction, Google is quite possibly the more powerful search engine used today, even used sometimes to check our connectivity; except that the power of the single search bar on the top of Google has become a source of concern for many, and if not they should and we will see why!

In addition to be one of the most powerful information databases, Google can be used to find much more than what we even should find. Google can find things like sensitive files, web vulnerabilities; it allows the identification of operating systems and can even be used to find passwords, databases and even whole mailbox content… Google understands which operators to target in order to get precisely what we are seeking; I'll try to detail the most important of them.

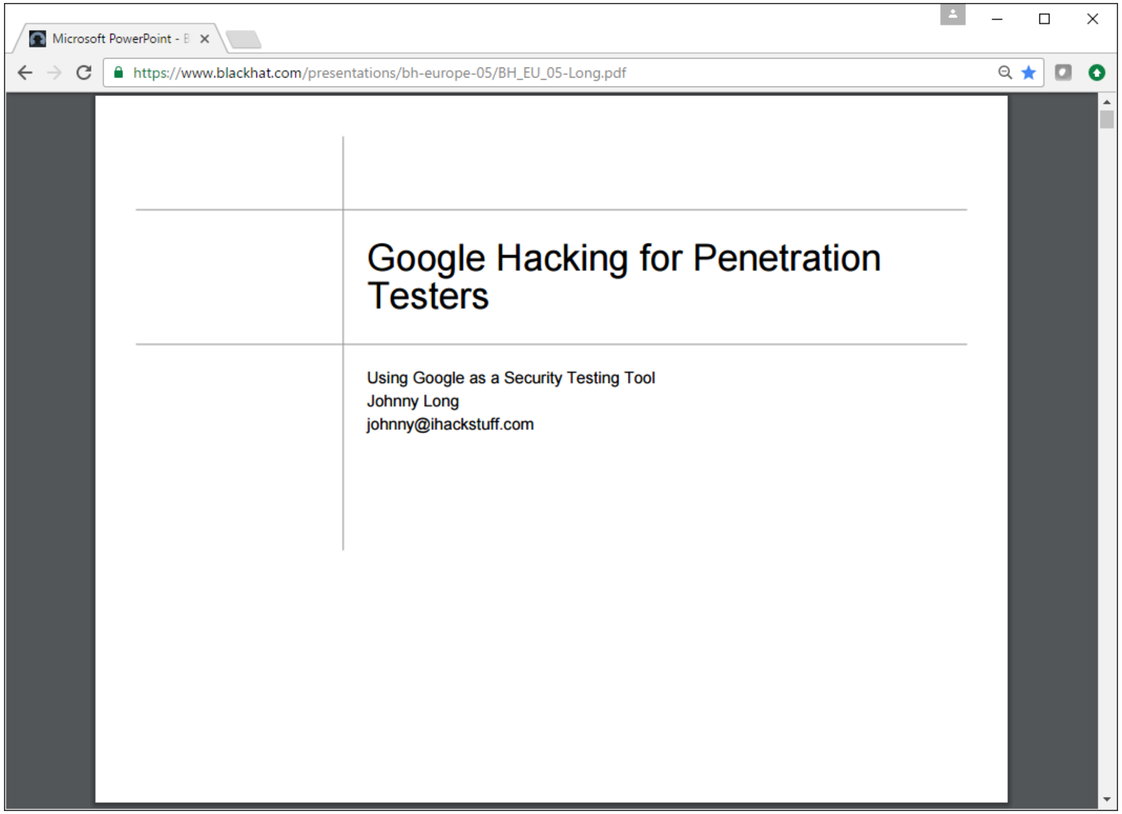
You have to know that queries on Google are not case sensitive, thus there is no difference between lower or upper cases or even a combination of both: Security, SECURITY and SeCuriTY will return exactly the same result, but this rule has an exception when using logical operators.

Logical operators and symbols

Google can understand three logical operators: AND, NOT and OR, so Google recognizes the "OR" as the operator and "Or", "oR" or "or" as search elements or keywords.

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

Google Hacking by Johnny Long

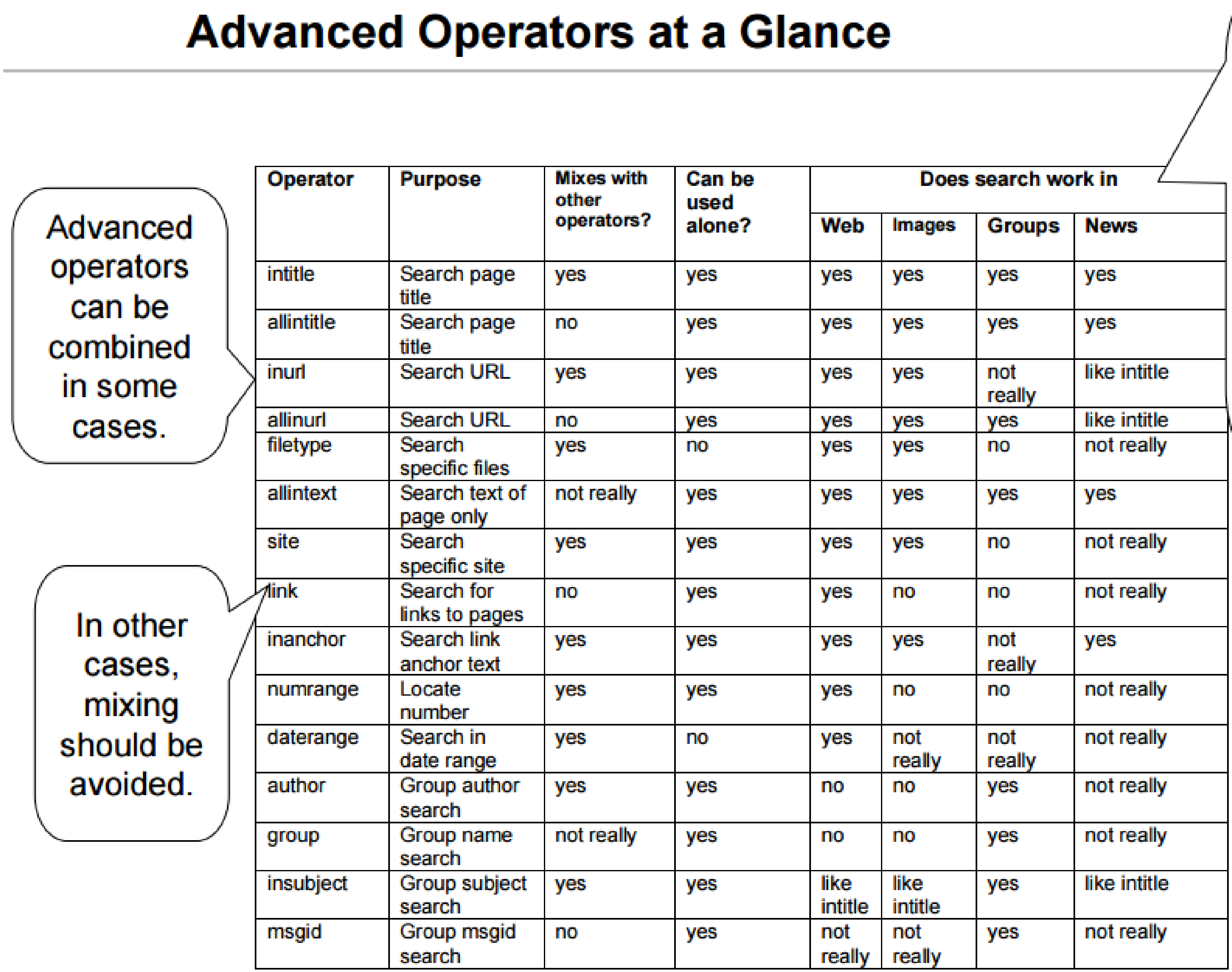


Microsoft PowerPoint - B
https://www.blackhat.com/presentations/bh-europe-05/BH_EU_05-Long.pdf

Google Hacking for Penetration Testers

Using Google as a Security Testing Tool
Johnny Long
johnny@ihackstuff.com

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



Advanced Operators at a Glance

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

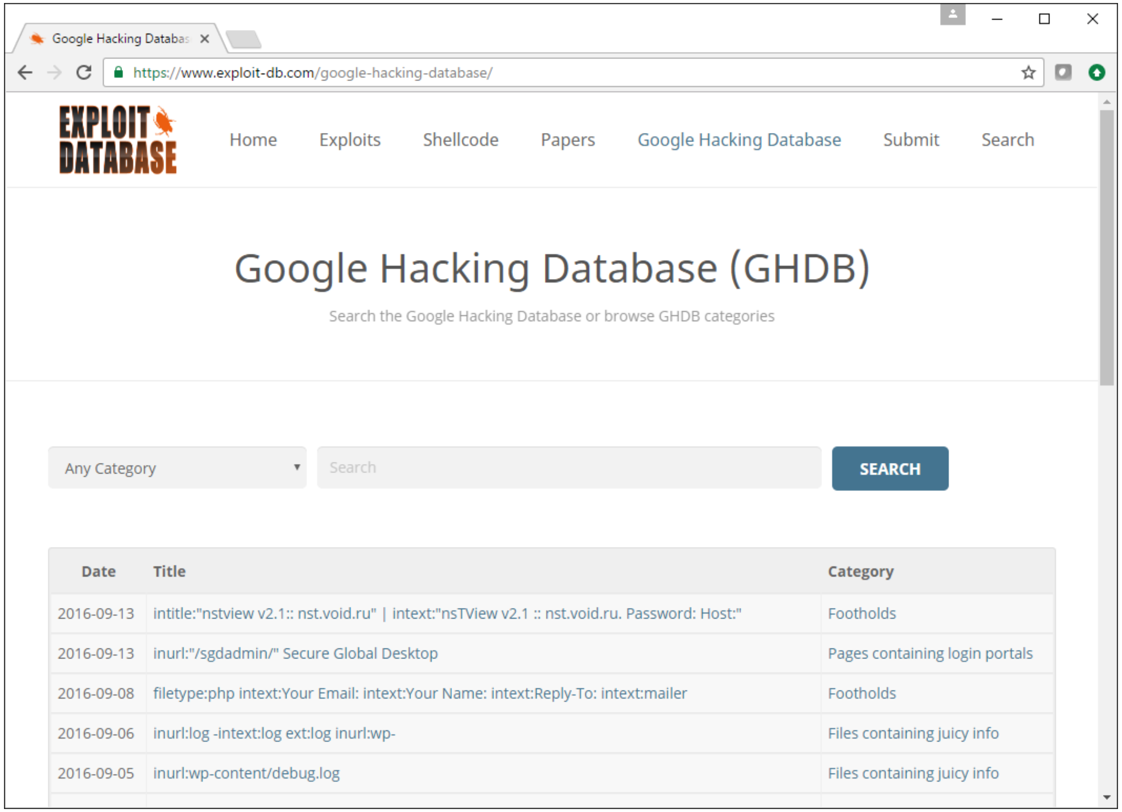
Advanced operators can be combined in some cases.

In other cases, mixing should be avoided.

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

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

Google Hacking On Exploit Database



Google Hacking Database (GHDB)

Search the Google Hacking Database or browse GHDB categories

Date	Title	Category
2016-09-13	intitle:"nstview v2.1:: nst.void.ru" | intext:"nsTView v2.1 :: nst.void.ru. Password: Host:"	Footholds
2016-09-13	inurl:"/sgdadmin/" Secure Global Desktop	Pages containing login portals
2016-09-08	filetype:php intext:Your Email: intext:Your Name: intext:Reply-To: intext:mailer	Footholds
2016-09-06	inurl:log -intext:log ext:log inurl:wp-	Files containing juicy info
2016-09-05	inurl:wp-content/debug.log	Files containing juicy info

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

Google Hacking Database Activity

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

Break-out rooms for the following GHDB categories:

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

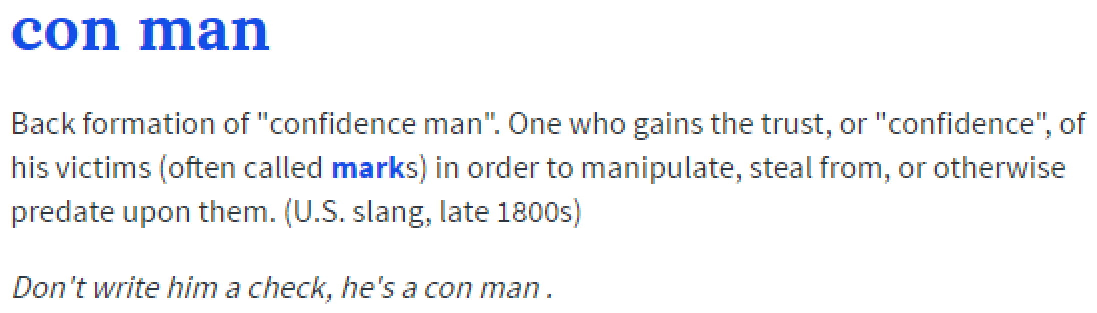
Instructions: Introduce yourself to the others in your online break-out room. Divvy up some of the Google searches in your categories to find 1 - 3 interesting sites to share with the class. Only select sites that are "appropriate" to share in a college class environment.

Each group will present the tops 1-3 sites they found

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 **marks**) 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:

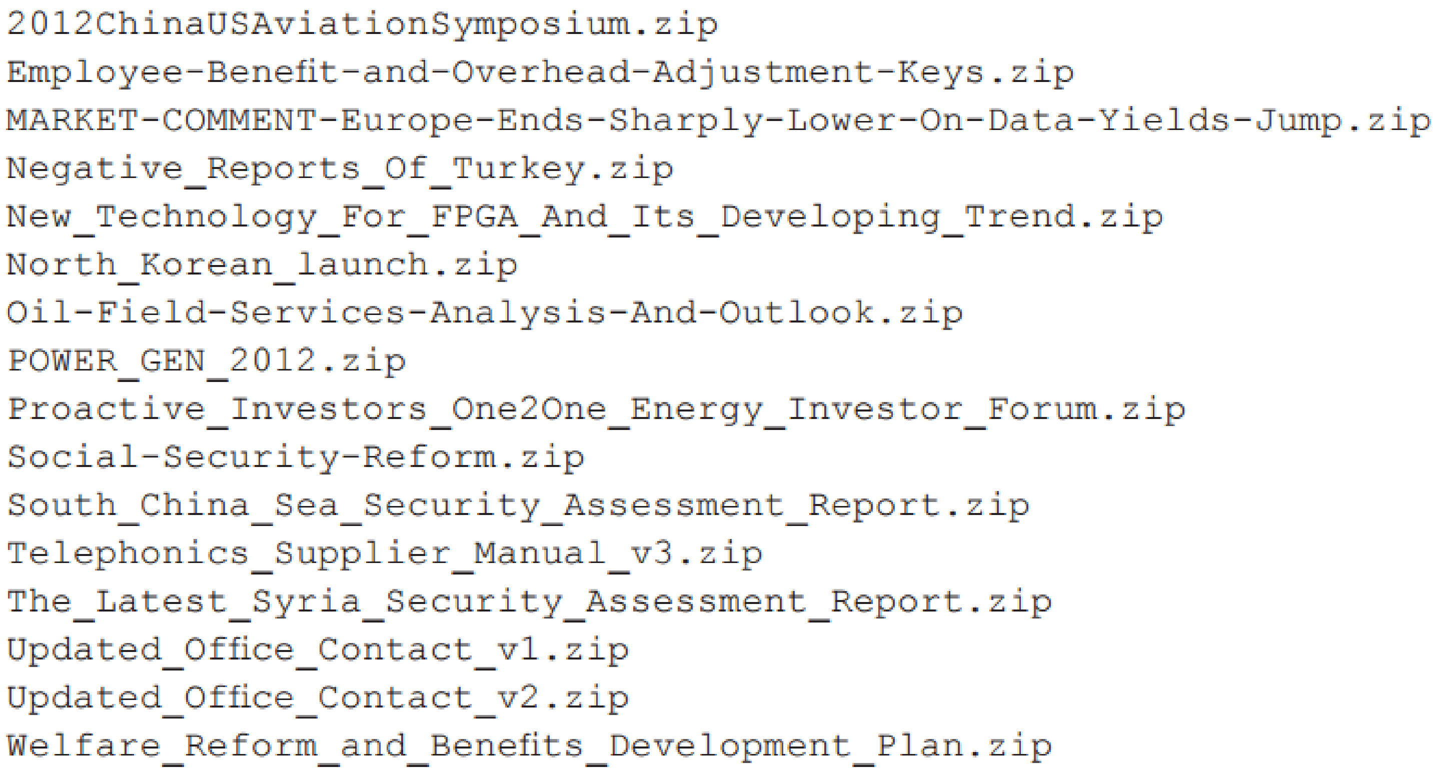
- Spy gear - impersonating a IT staff member then placing a hardware key logger on a sensitive computer.

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:

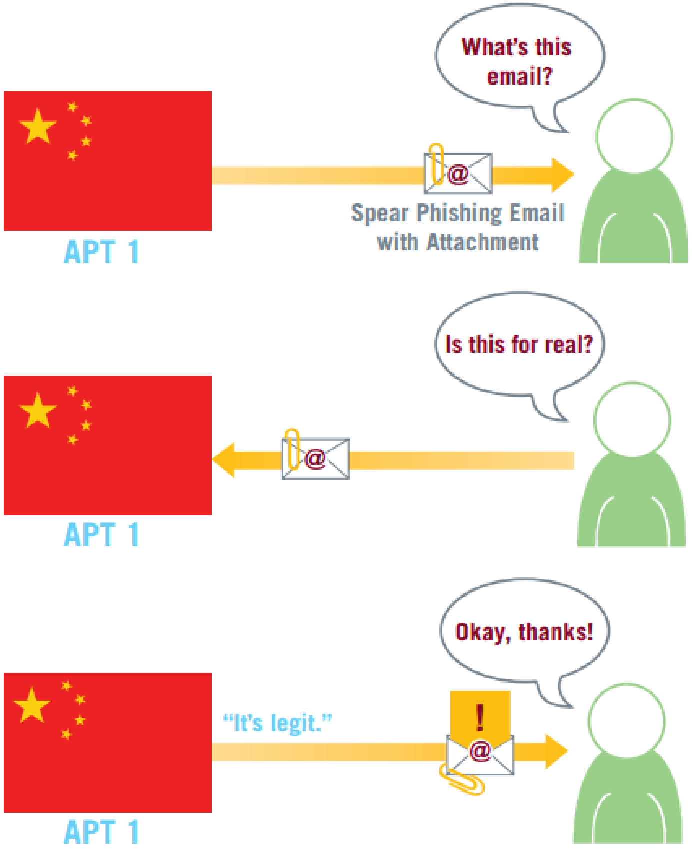


```
2012ChinaUSAviationSymposium.zip
Employee-Benefit-and-Overhead-Adjustment-Keys.zip
MARKET-COMMENT-Europe-Ends-Sharply-Lower-On-Data-Yields-Jump.zip
Negative_Reports_Of_Turkey.zip
New_Technology_For_FPGA_And_Its_Developing_Trend.zip
North_Korean_launch.zip
Oil-Field-Services-Analysis-And-Outlook.zip
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

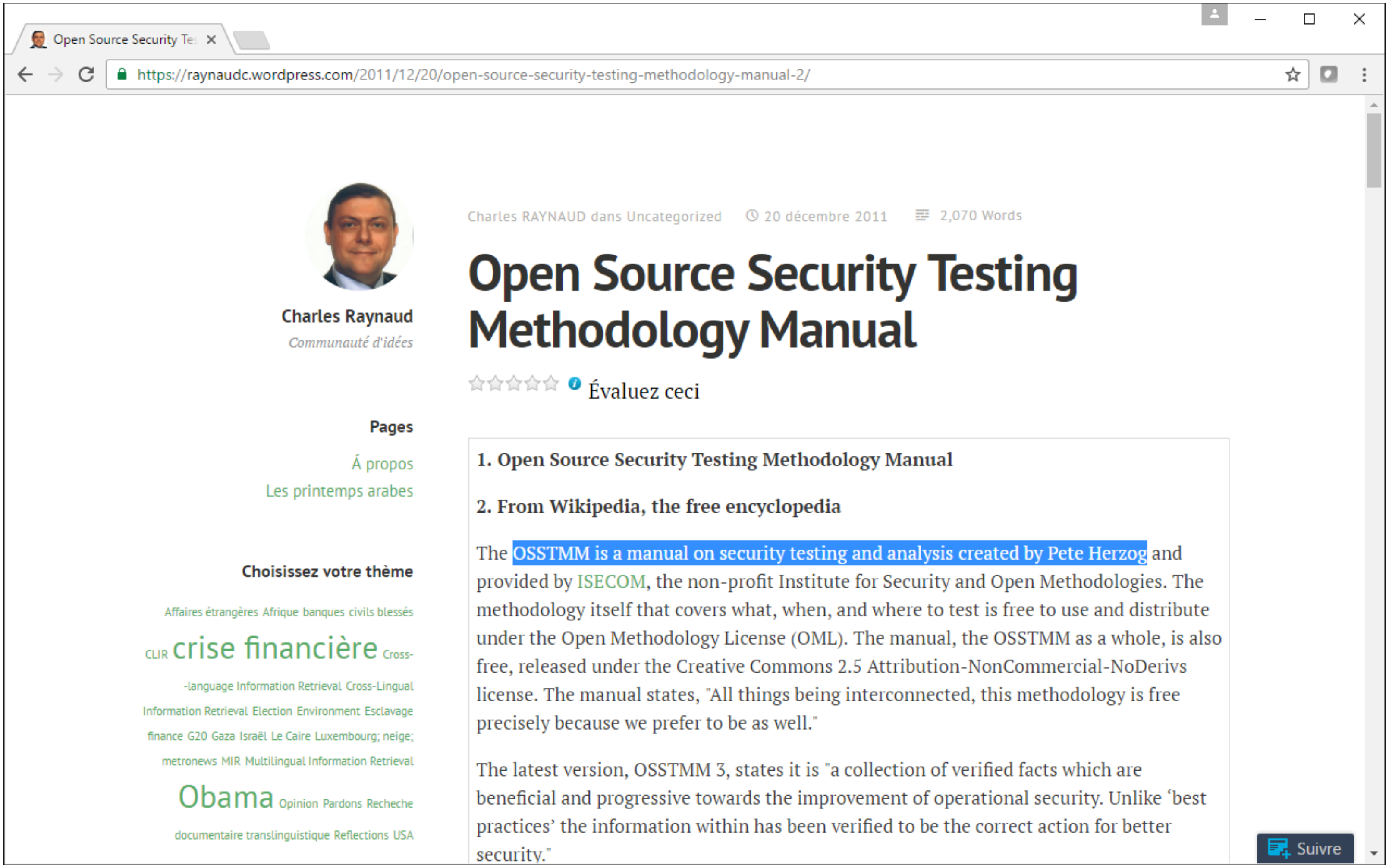
Mandiant APT1 phishing observations:



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



Open Source Security Te
https://raynaudc.wordpress.com/2011/12/20/open-source-security-testing-methodology-manual-2/
Charles Raynaud
Communauté d'idées
Pages
Á propos
Les printemps arabes
Choisissez votre thème
Affaires étrangères Afrique banques civils blessés CLIR crise financière Cross--language Information Retrieval Cross-Lingual Information Retrieval Election Environment Esclavage finance G20 Gaza Israël Le Caire Luxembourg; neige; metronews MIR Multilingual Information Retrieval Obama Opinion Pardons Recheche documentaire translinguistique Reflections USA
Charles RAYNAUD dans Uncategorized
20 décembre 2011
2,070 Words
☆☆☆☆☆ Évaluez ceci
Suivre

Open Source Security Testing Methodology Manual

1. Open Source Security Testing Methodology Manual

2. From Wikipedia, the free encyclopedia

The OSSTMM is a manual on security testing and analysis created by Pete Herzog and provided by ISECOM, the non-profit Institute for Security and Open Methodologies. The methodology itself that covers what, when, and where to test is free to use and distribute under the Open Methodology License (OML). The manual, the OSSTMM as a whole, is also free, released under the Creative Commons 2.5 Attribution-NonCommercial-NoDerivs license. The manual states, "All things being interconnected, this methodology is free precisely because we prefer to be as well."

The latest version, OSSTMM 3, states it is "a collection of verified facts which are beneficial and progressive towards the improvement of operational security. Unlike 'best practices' the information within has been verified to be the correct action for better security."

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."

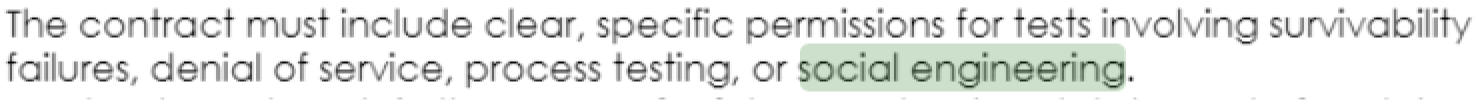
Rules of Engagement

...

3. Contracts and Negotiations

...

3.6



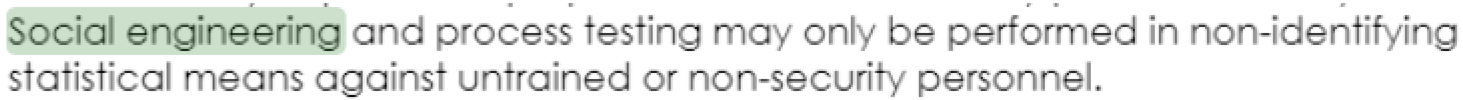
The contract must include clear, specific permissions for tests involving survivability failures, denial of service, process testing, or social engineering.

...

7. Testing

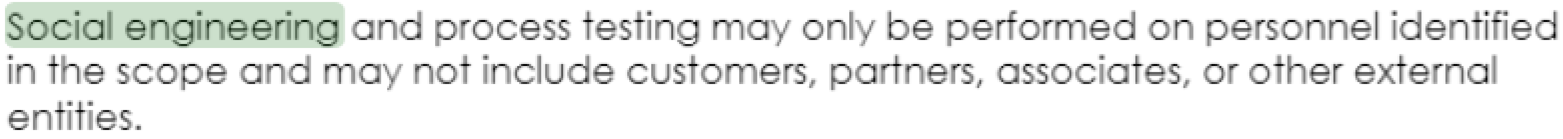
...

7.3



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

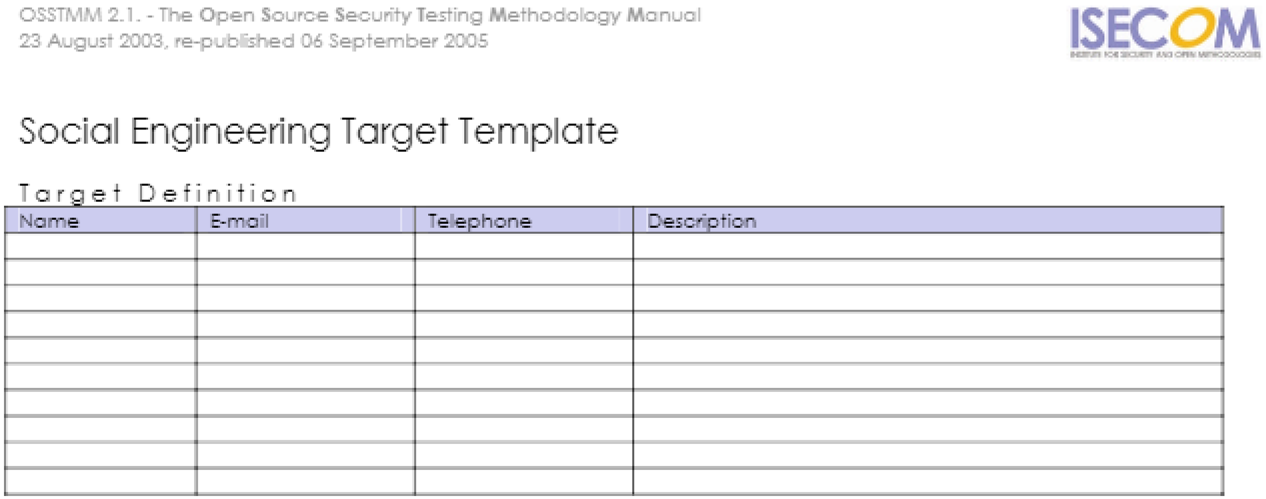
7.4



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

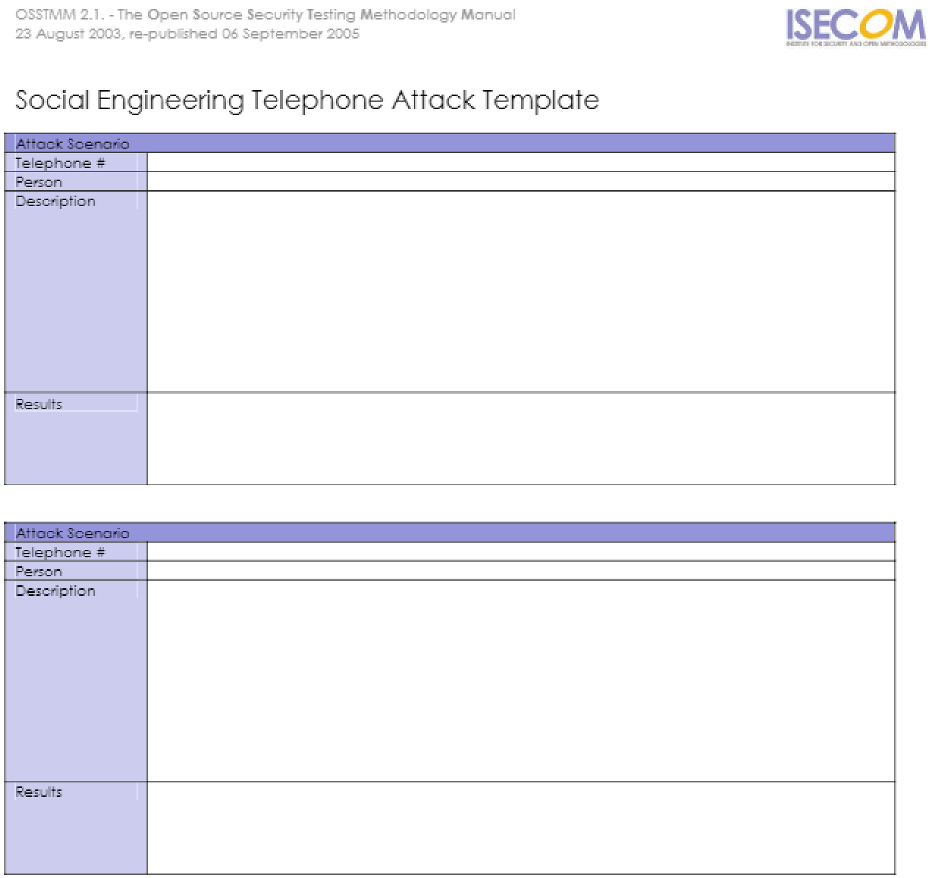
Social Engineering Target Template

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

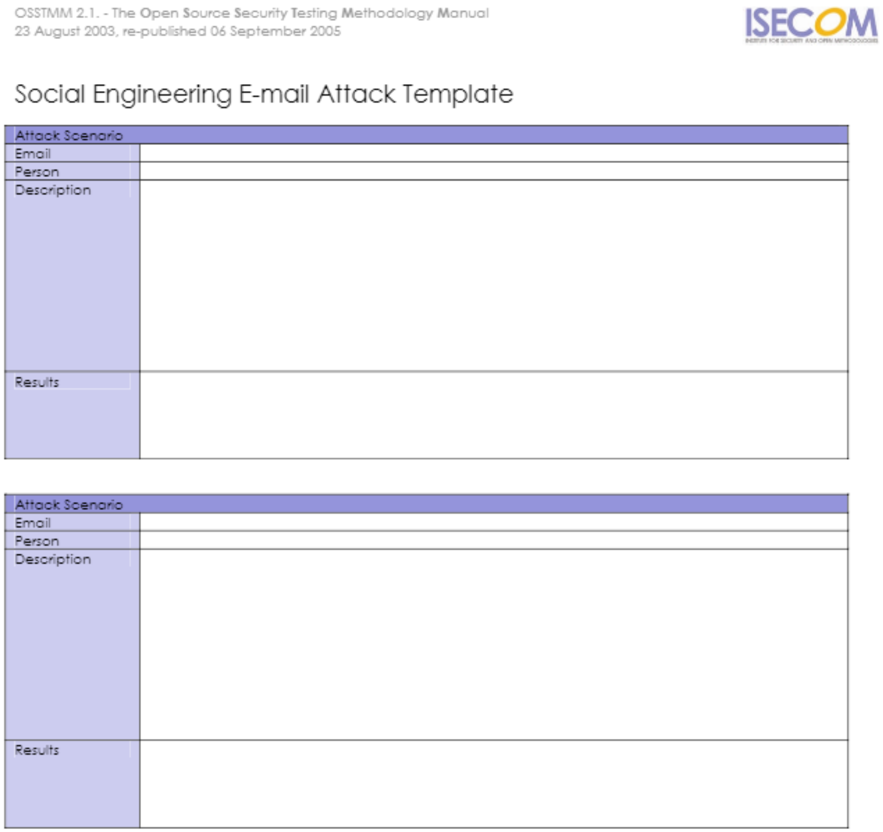
Social Engineering Telephone Attack Template

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

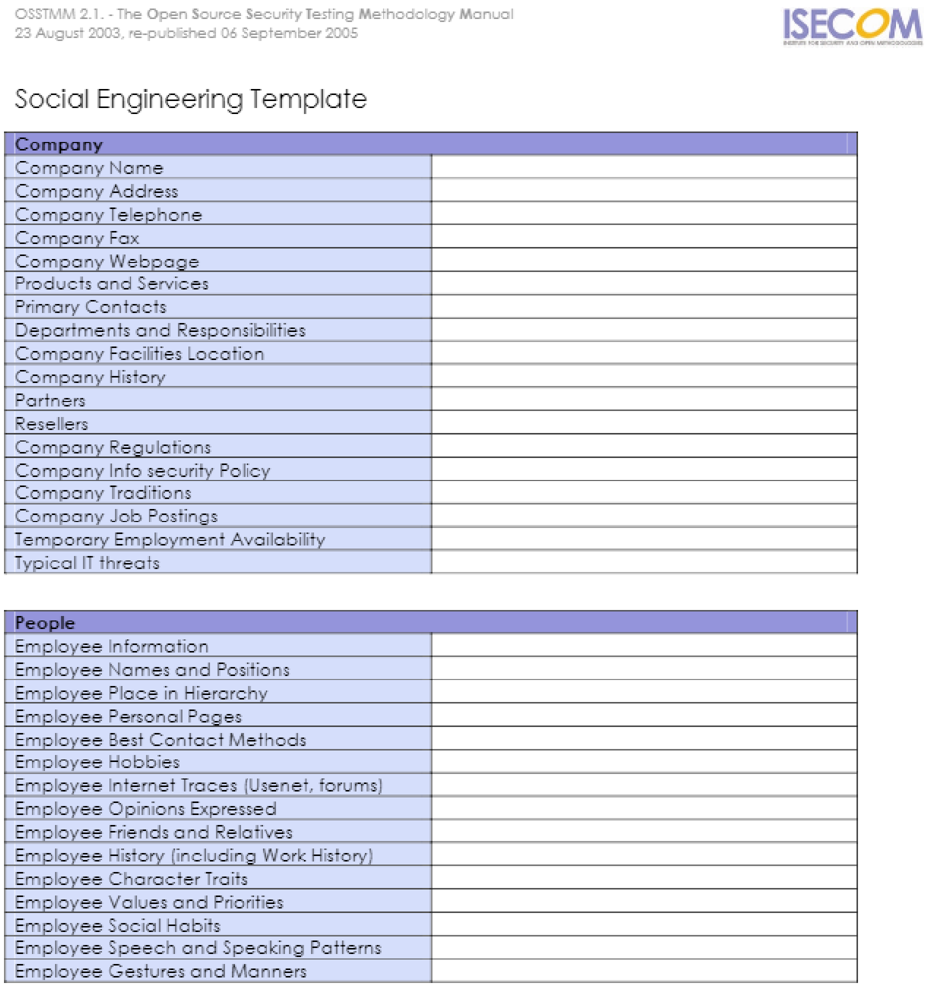
Social Engineering E-mail Attack Template

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

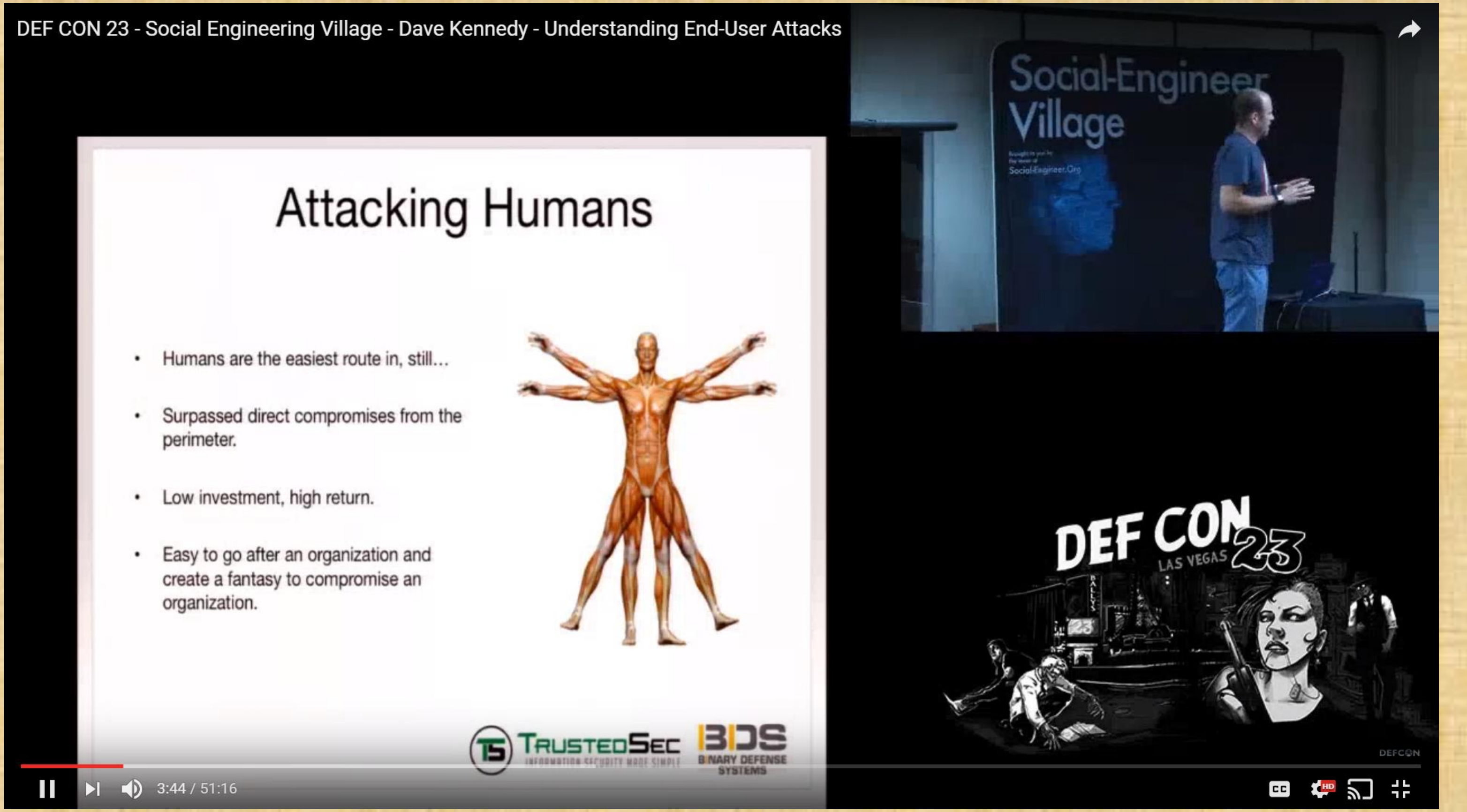
Company	
Company Name	
Company Address	
Company Telephone	
Company Fax	
Company Webpage	
Products and Services	
Primary Contacts	
Departments and Responsibilities	
Company Facilities Location	
Company History	
Partners	
Resellers	
Company Regulations	
Company Info security Policy	
Company Traditions	
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



DEF CON 23 - Social Engineering Village - Dave Kennedy - Understanding End-User Attacks

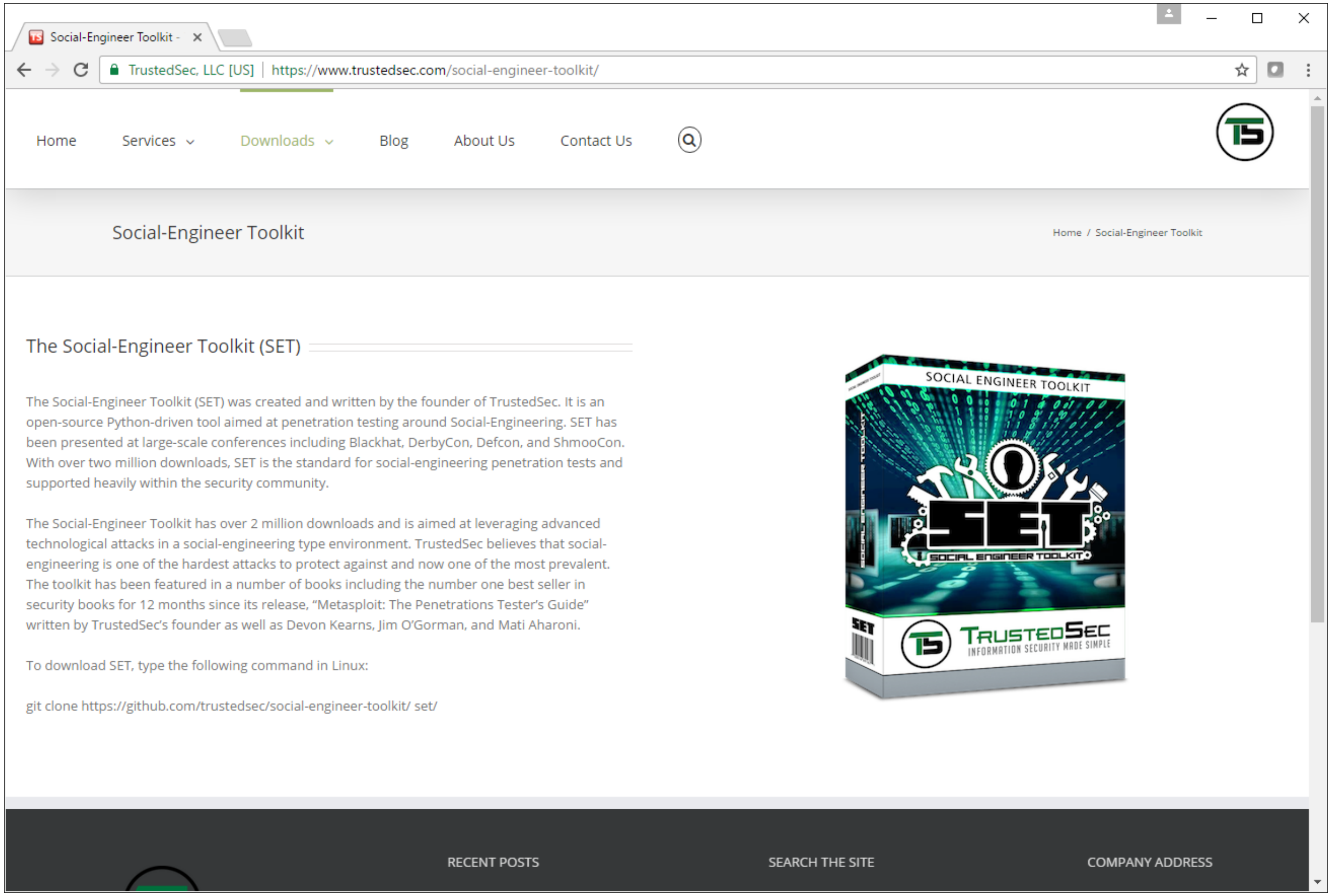
Attacking Humans

- Humans are the easiest route in, still…
- Surpassed direct compromises from the perimeter.
- Low investment, high return.
- Easy to go after an organization and create a fantasy to compromise an organization.

David Kennedy created the Social Engineering Toolkit (SET)

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

Social Engineering Toolkit



Social-Engineer Toolkit -
TrustedSec, LLC [US] | https://www.trustedsec.com/social-engineer-toolkit/
Home
Services
Downloads
Blog
About Us
Contact Us
Home / Social-Engineer Toolkit
SOCIAL ENGINEER TOOLKIT
SET
SOCIAL ENGINEER TOOLKIT
TRUSTEDSEC
INFORMATION SECURITY MADE SIMPLE
RECENT POSTS
SEARCH THE SITE
COMPANY ADDRESS

Social-Engineer Toolkit

The Social-Engineer Toolkit (SET)

The Social-Engineer Toolkit (SET) was created and written by the founder of TrustedSec. It is an open-source Python-driven tool aimed at penetration testing around Social-Engineering. SET has been presented at large-scale conferences including Blackhat, DerbyCon, Defcon, and ShmooCon. With over two million downloads, SET is the standard for social-engineering penetration tests and supported heavily within the security community.

The Social-Engineer Toolkit has over 2 million downloads and is aimed at leveraging advanced technological attacks in a social-engineering type environment. TrustedSec believes that social-engineering is one of the hardest attacks to protect against and now one of the most prevalent. The toolkit has been featured in a number of books including the number one best seller in security books for 12 months since its release, “Metasploit: The Penetrations Tester’s Guide” written by TrustedSec’s founder as well as Devon Kearns, Jim O’Gorman, and Mati Aharoni.

To download SET, type the following command in Linux:

```
git clone https://github.com/trustedsec/social-engineer-toolkit/ set/
```

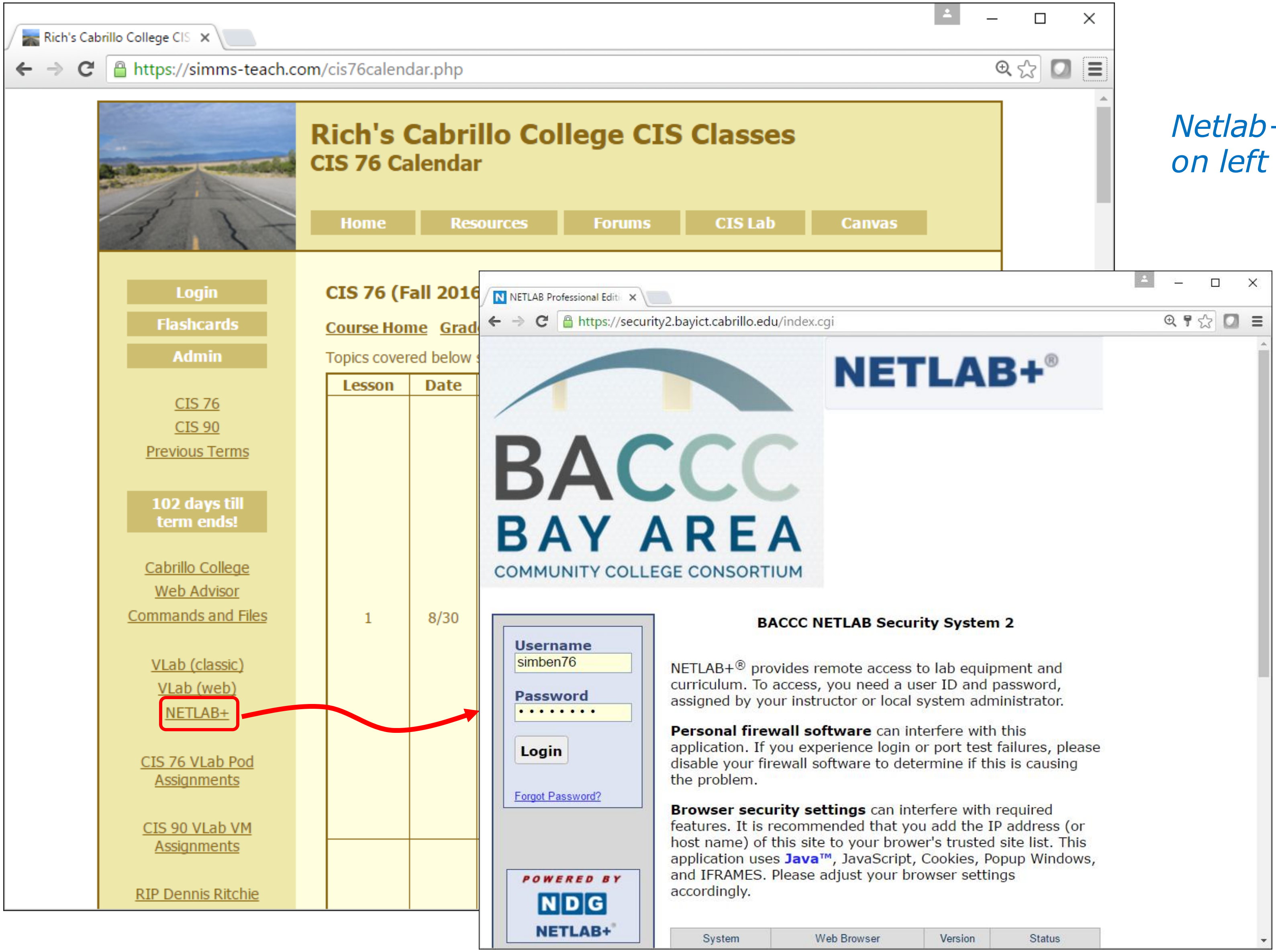
David Kennedy created the Social Engineering Toolkit (SET)

Netlab+ Activity

NDG EH Lab 2

Social Engineering Toolkit

Assignment



Rich's Cabrillo College CIS

https://simms-teach.com/cis76calendar.php

Rich's Cabrillo College CIS Classes

CIS 76 Calendar

CIS 76 (Fall 2016

Course Home Grad

Topics covered below

Lesson	Date
1	8/30

NETLAB Professional Edit

https://security2.bayict.cabrillo.edu/index.cgi

Username: simben76

Password: ••••••••

BACCC NETLAB Security System 2

NETLAB+® provides remote access to lab equipment and curriculum. To access, you need a user ID and password, assigned by your instructor or local system administrator.

Personal firewall software can interfere with this application. If you experience login or port test failures, please disable your firewall software to determine if this is causing the problem.

Browser security settings can interfere with required features. It is recommended that you add the IP address (or host name) of this site to your brower's trusted site list. This application uses **Java™**, JavaScript, Cookies, Popup Windows, and IFRAMES. Please adjust your browser settings accordingly.

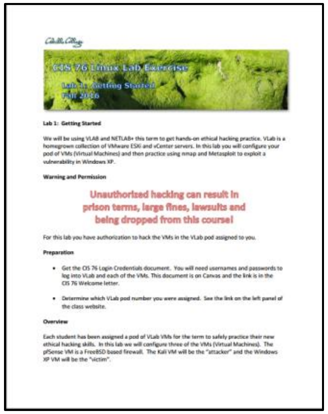
System	Web Browser	Version	Status

Netlab+ link on left panel

Lab Assignments

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.



Cabrillo College

CIS 76 Linux Lab Exercise

Lab 1: Getting Started
Fall 2016

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 pod 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 pod 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 pod 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".

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