



Last updated 9/18/2017

Rich's lesson module checklist

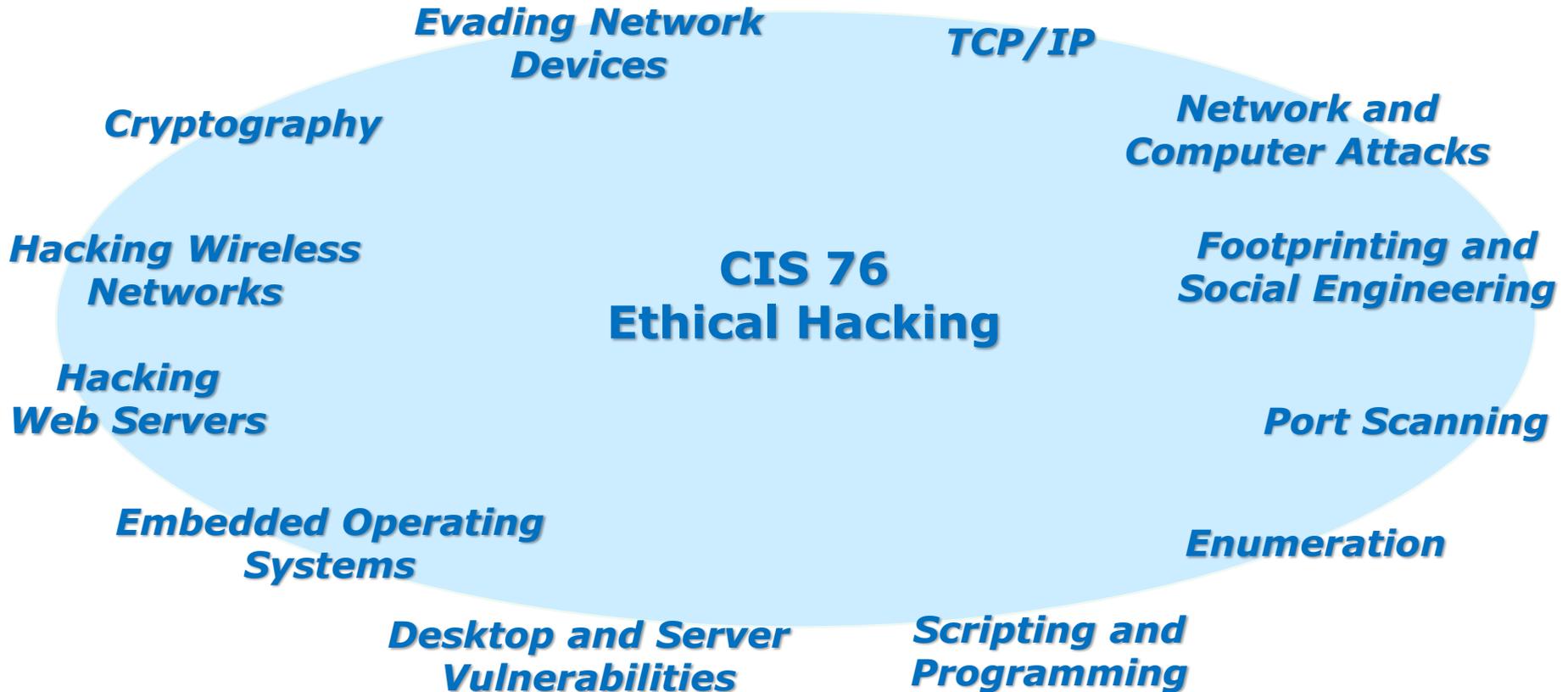
- Slides and lab posted
- WB converted from PowerPoint
- Print out agenda slide and annotate page numbers

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

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

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

- Update CCC Confer and 3C Media portals



Student Learner Outcomes

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

Introductions and Credits



Rich Simms

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

And thanks to:

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



Student checklist for attending class

Rich's Cabrillo College CIS Classes
CIS 90 Calendar

CIS 90 (Fall 2014) Calendar

Course Dates: [Calendar](#)

CIS 76

Lesson	Date	Topics	Link
	9/2	<p>Class and Linux Overview</p> <ul style="list-style-type: none"> Understand how the course will work High-level overview of computers, operating systems, and virtual machines Overview of LINUX/Linux market and architecture Using SSH for remote network logs Using terminals and the command line <p>Methods</p> <p>Presentation slides (download)</p> <p>Supplemental</p> <ul style="list-style-type: none"> PowerPoint: Logging into Opus (command) <p>Assignments</p> <ul style="list-style-type: none"> Student Survey Lab 1 <p>CCS Center</p> <p>Enter virtual classroom</p>	
		<p>Quiz 1</p> <p>Commands</p>	

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

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



Student checklist for suggested screen layout

Google

CCC Confer

Downloaded PDF of Lesson Slides

The screenshot displays a virtual classroom interface. On the left is a Blackboard course page for 'Rich's Cabrillo College CIS 90 Classes'. In the center is a CCC Confer video conference window showing a participant named 'Rich Simms' and a 'PARTICIPANTS' list. Overlaid on the conferencing window is a Google Maps window titled 'Class Activity - Where are you now?'. On the right is an Adobe Acrobat Pro window displaying a PDF titled 'cis90lesson01.pdf - The CIS 90 System Playground'. Below the PDF viewer is a terminal window showing a login session to Opus with a password prompt and a successful login message.

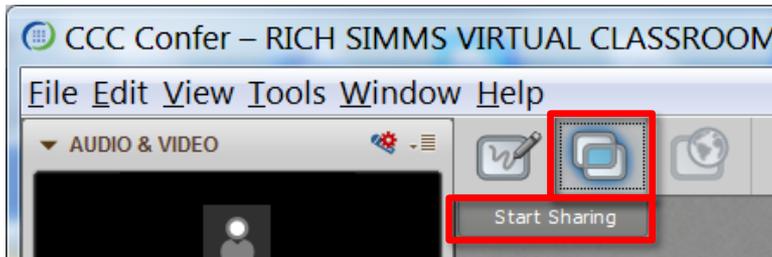
CIS 76 website Calendar page

One or more login sessions to Opus

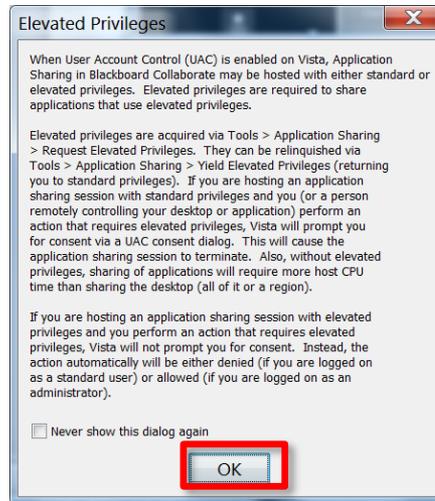


Student checklist for sharing desktop with classmates

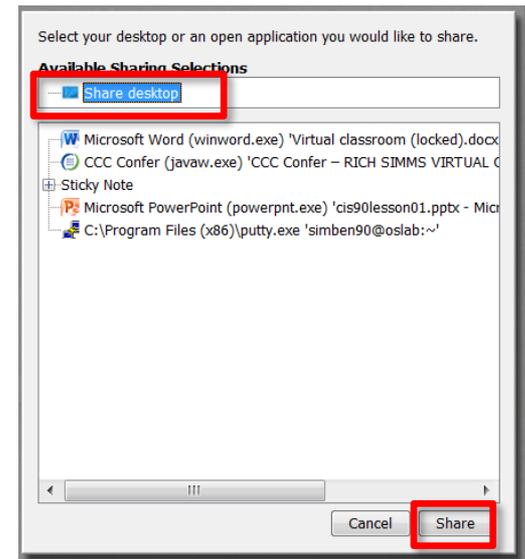
1) Instructor gives you sharing privileges.



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



3) Click OK button.



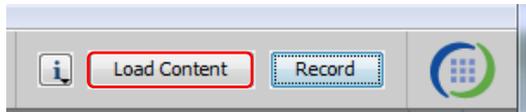
4) Select "Share desktop" and click Share button.



Rich's CCC Confer checklist - setup

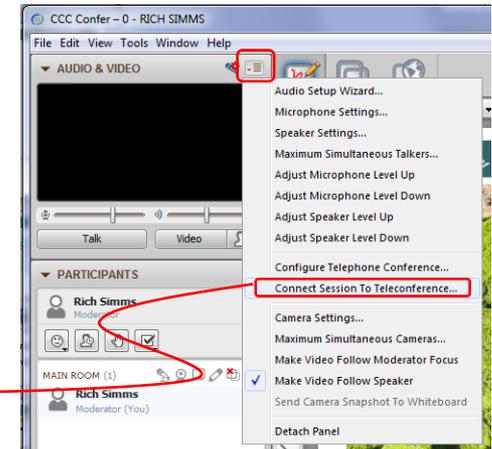
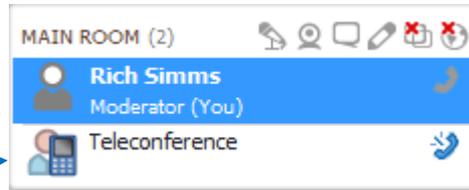


[] Preload White Board

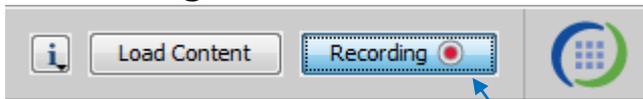


[] Connect session to Teleconference

Session now connected to teleconference



[] Is recording on?



Red dot means recording

[] Use teleconferencing, not mic

Should be grayed out



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



Rich's CCC Confer checklist - screen layout



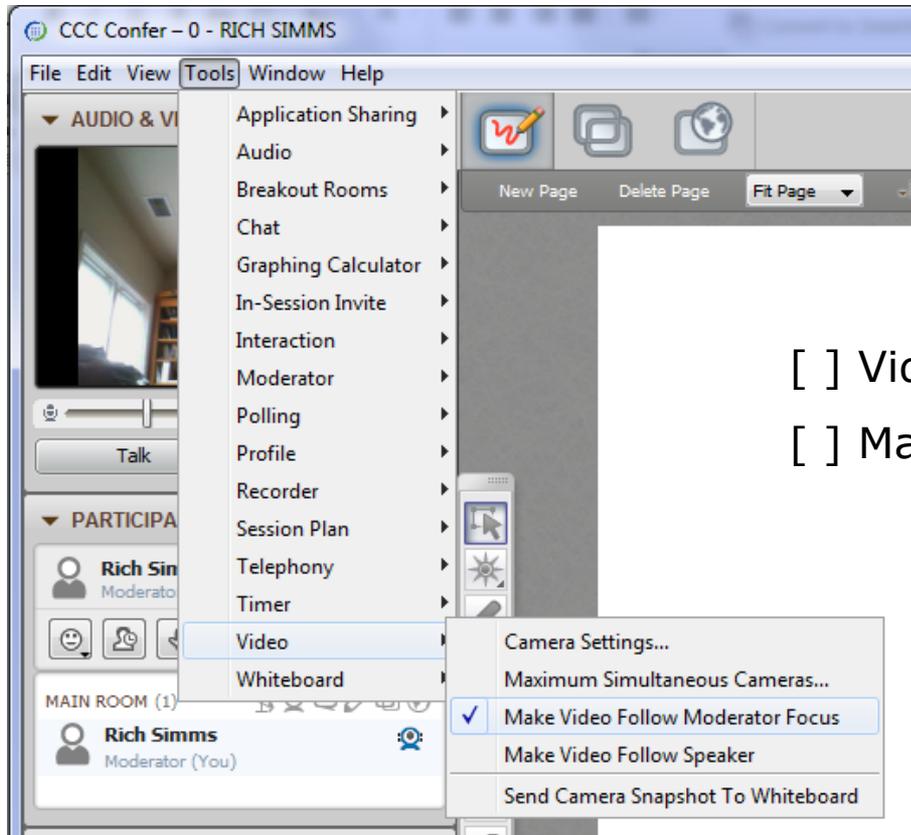
The screenshot displays a Windows desktop with several applications open. On the left is the CCC Confer window, showing a video feed of Rich Simms and a list of participants. In the center is a Chrome browser window displaying a quiz titled 'Part 1 - Flashc (1 point each)'. The quiz questions are: [Q1] What command shows the other users logged in to the computer? and [Q2] What environment variable is used by the shell to determine which directories to search when locating a command? Below the quiz is a Putty terminal window showing a file tree with directories like boot, bin, etc, sbin and files like mail, ls. The terminal prompt is 'simben90@oslab:~'. To the right is the vSphere Client window showing a virtual machine named 'CIS 192'. Red callout boxes with white text label 'foxit for slides' pointing to the PDF viewer, 'chrome' pointing to the browser, and 'vSphere Client' pointing to the vSphere interface.

[] layout and share apps





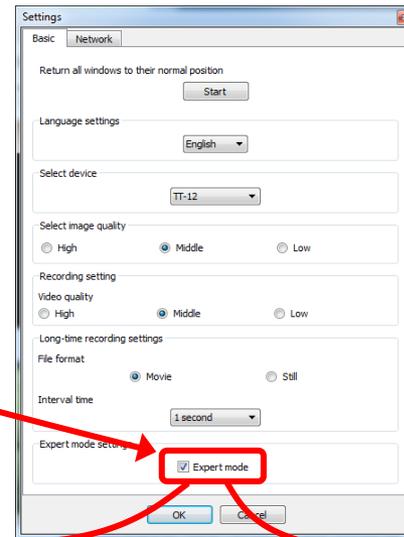
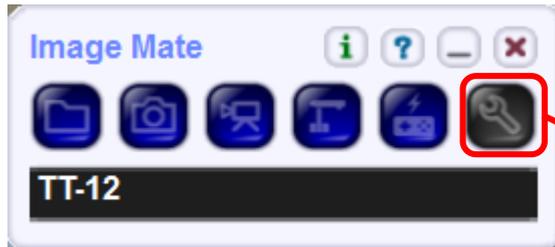
Rich's CCC Confer checklist - webcam setup



- [] Video (webcam)
- [] Make Video Follow Moderator Focus



Rich's CCC Confer checklist - Elmo



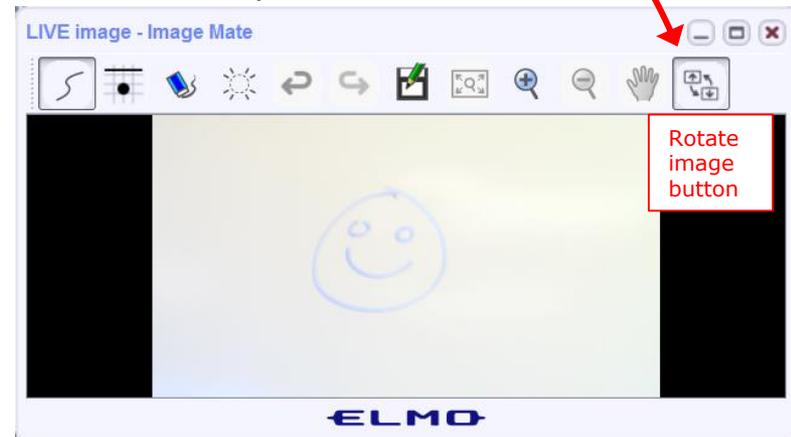
The "rotate image" button is necessary if you use both the side table and the white board.

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

Elmo rotated down to view side table



Elmo rotated up to view white board



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



Rich's CCC Confer checklist - universal fixes

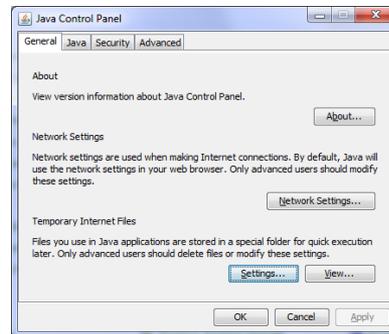
Universal Fix for CCC Confer:

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

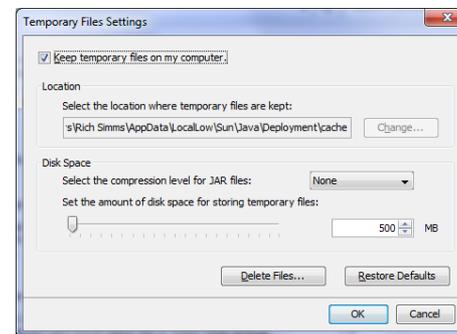
Control Panel (small icons)



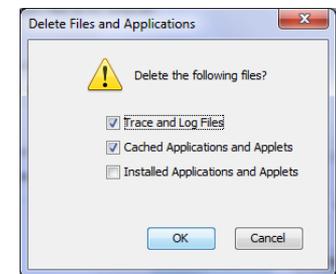
General Tab > Settings...



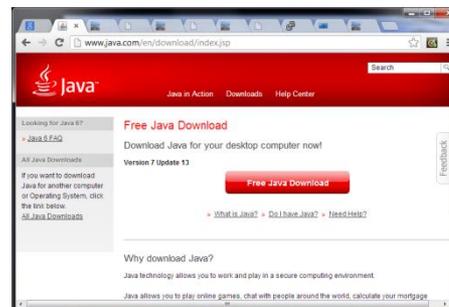
500MB cache size



Delete these



Google Java download





Start

Sound Check

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

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

Volume

**4 - increase conference volume.*

**7 - decrease conference volume.*

**5 - increase your voice volume.*

**8 - decrease your voice volume.*



Instructor: **Rich Simms**

Dial-in: **888-886-3951**

Passcode: **136690**



Philip



Bruce



James



Sam B.



Sam R.



Miguel



Bobby



Garrett



Ryan A.



Aga



Karina



Chris



Corbin



Helen



Xu



Mariano



Cameron



Ryan M.



Tre



May



Karl-Heinz



Remy



Tanner

First Minute Quiz

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

Use CCC Confer White Board

email answers to: risimms@cabrillo.edu

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

Footprinting and Social Engineering

Objectives

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

Agenda

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

Admonition

Unauthorized hacking is a crime.

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

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



Questions

Questions?

Lesson material?

Labs? Tests?

How this course works?

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

Who questions much, shall learn much, and retain much.

- Francis Bacon

If you don't ask, you don't get.

- Mahatma Gandhi

Chinese
Proverb

他問一個問題，五分鐘是個傻子，他不問一個問題仍然是一個傻瓜永遠。

He who asks a question is a fool for five minutes; he who does not ask a question remains a fool forever.

In the news

Recent news

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

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

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

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

3. CVE-2017-5638

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

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

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

Thanks Karina

Recent news

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

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

Housekeeping



If you haven't already

Change your default password on Opus-II

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

Roll Call

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

risimms@cabrillo.edu

to provide roll call attendance.

Housekeeping

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

The screenshot shows a phpBB forum interface. The header includes the site name 'Cabrillo College: Computer and Information Systems' and a search bar. The main content area displays a list of forum topics. A red rectangular box highlights a white text area containing the following instructions:

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

Perkins/VTEA Survey

The screenshot shows a forum post on the 'Cabrillo College: Computer and Information Systems' forum. The post is titled 'Carl D. Perkins Vocational and Technical Education Act' and is posted by Rich Simms on 09/22/2015 at 10:45 pm. The post text explains that the Carl D. Perkins Vocational and Technical Education Act was originally authorized by Congress in 1966, reauthorized in 1991 and again in 2009. It provides federal funding for vocational career technical education (CTE) and the related system in order to help the economy. Cabrillo College is receiving portions of this funding and is looking for interested students to complete a survey. The survey is a confidential questionnaire that will help the college determine the best way to use the funding. The survey can be completed online through a link provided in the post. The post also includes a link to the WIDA website and instructions for logging in as a student or faculty member.

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!***

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

Career Technical Information	
Your answers to these questions will help qualify Cabrillo College for Perkins/VTEA grant funds.	
Are you currently receiving benefits from:	
<input type="radio"/> Yes	TANF/CALWORKS
<input type="radio"/> No	
<input type="radio"/> Yes	SSI (Supplemental Security Income)
<input type="radio"/> No	
<input type="radio"/> Yes	GA (General Assistance)
<input type="radio"/> No	
<input type="radio"/> Yes	Does your <u>income</u> qualify you for a fee waiver?
<input type="radio"/> No	
<input type="radio"/> Yes	Are you a single parent with custody of one or more minor children?
<input type="radio"/> No	
<input type="radio"/> Yes	Are you a <u>displaced homemaker</u> attending Cabrillo to develop job skills?
<input type="radio"/> No	
<input type="radio"/> Yes	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?
<input type="radio"/> No	

Wireshark Class If Interested - Enroll ASAP!

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

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

CIS 140NA Network Analysis using Wireshark

Prerequisite: CIS 82 or CIS 83.

Recommended Preparation: Eligibility for ENGL 100 or ESL 100 and READ 100.

Repeatability: May be taken a total of 1 time.

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

Attack Phases

EC-Council Five Phases of Hacking

Phase 1 - Reconnaissance

Phase 2 - Scanning

Phase 3 - Gaining Access

Phase 4 - Maintaining Access

Phase 5 - Clearing Tracks

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

NSA Intrusion Phases

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

Kill Chain

SANS Talk by Paul A. Henry

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

CYBER KILL CHAIN®

Lockheed Martin's Cyber Kill Chain® and Intelligence Driven Defense® services identify and prevent cyber intrusion activity. The services monitor what the adversaries must complete in order to achieve their objective.

A : ADVANCED

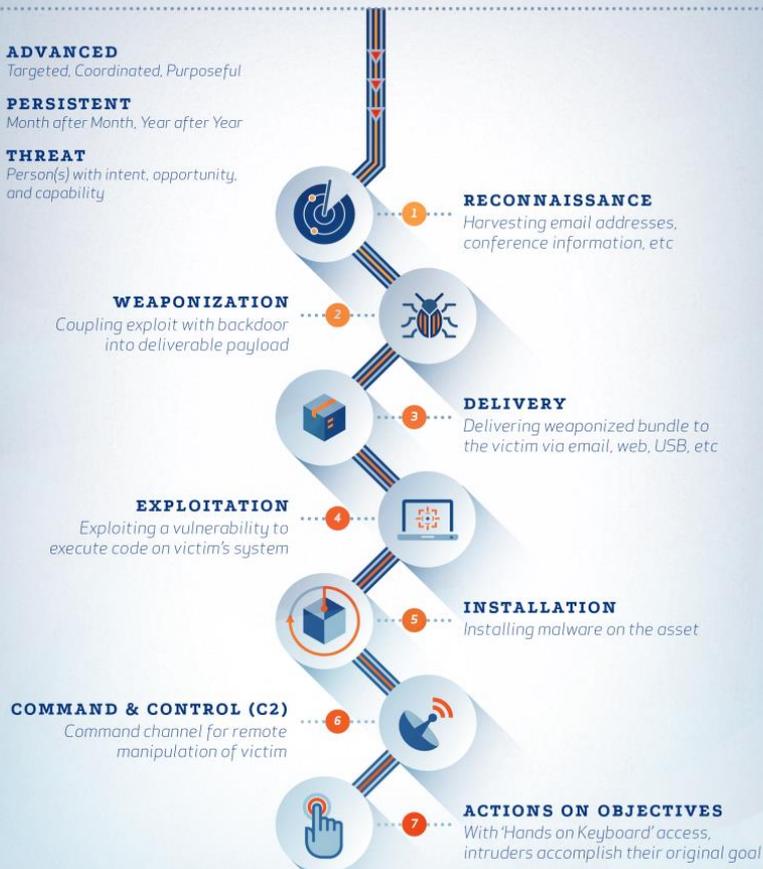
Targeted, Coordinated, Purposeful

P : PERSISTENT

Month after Month, Year after Year

T : THREAT

Person(s) with intent, opportunity, and capability



Learn how defenders have the advantage at:
lockheedmartin.com/cyber



Cyber Kill Chain Lockheed-Martin

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

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



Footprinting and Reconnaissance

Reconnaissance

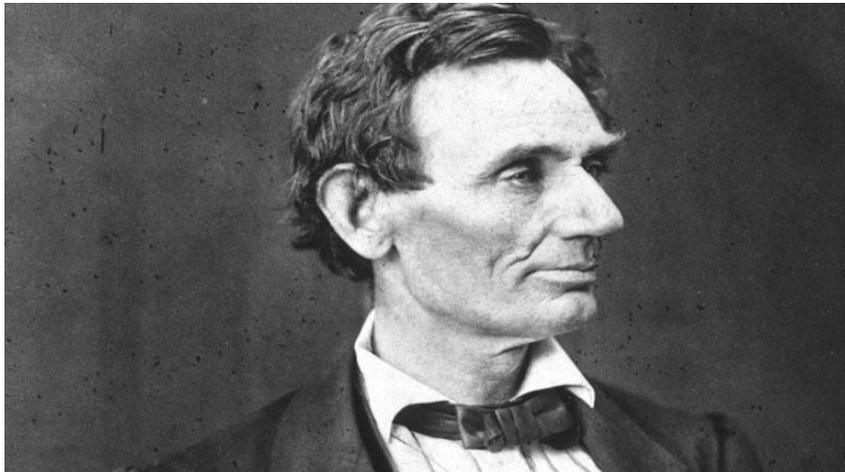
- Also known as "footprinting", "casing the joint", and "information gathering".
- The goal is to learn as much information about the target as possible without being detected.
- Gather information such as:
 - People and organizational structure
 - Related third parties
 - System and network technology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

Reconnaissance

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

Reconnaissance

- One of the most time consuming phases.



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

Reconnaissance

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

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

Doxing

The screenshot shows the Wikipedia page for 'Doxing'. The article text is as follows:

Doxing (from *dox*, abbreviation of *documents*),^[1] or **doxxing**,^{[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]

- 1 Etymology
- 2 Common techniques
- 3 Notable examples
 - 3.1 Boston Marathon
 - 3.2 Anonymous
 - 3.3 Human flesh search engine
 - 3.4 Journalists
 - 3.5 Curt Schilling

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

dox

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

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

#lulz #owned #hacker #social engineering #ruin

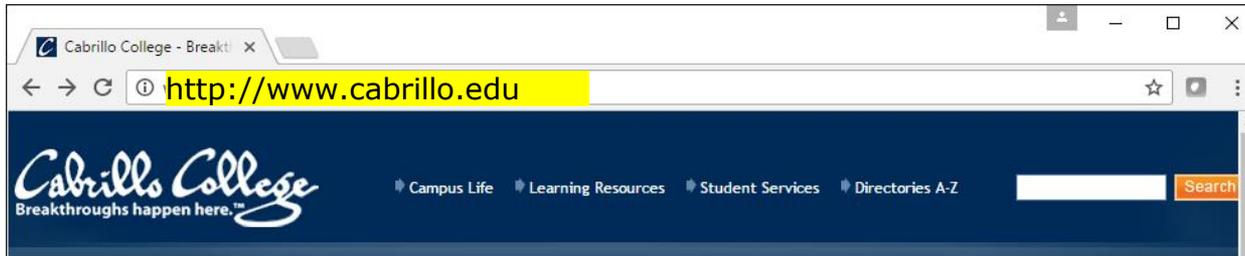
<http://www.urbandictionary.com/define.php?term=dox>

Creating a "dossier" on someone or an organization

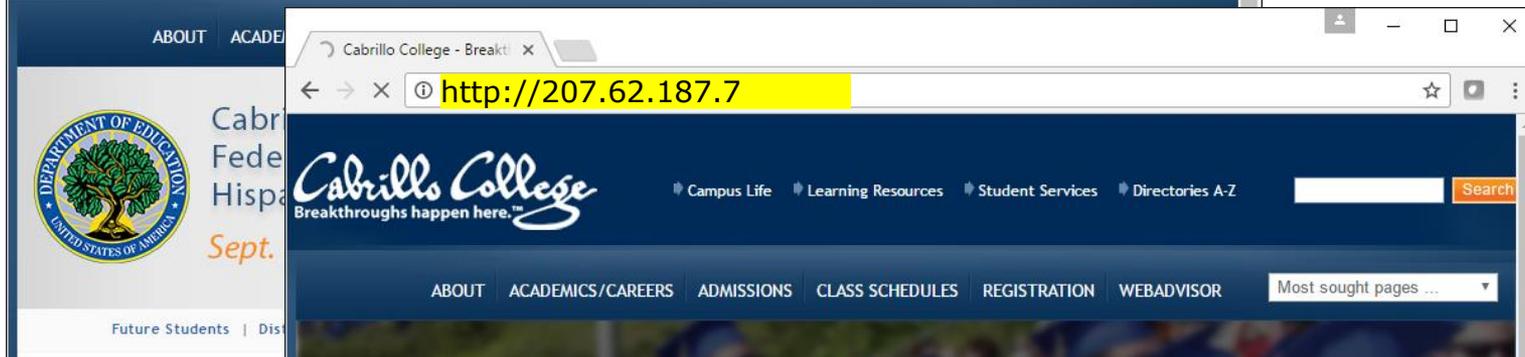
Domain Name System

Overview

DNS - Domain Name System



The world with DNS



The world without DNS

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

But which is easier to remember?



An Overview of Domain Name System

Created in 1983 from the work led by Paul Mockapetris

Improves the deficiencies of the */etc/hosts* file

DNS manages two databases (zones)

Forward lookup zones: for mapping Domain names to IP addresses

Reverse lookup zones: for mapping IP addresses to Domain names

Three components to DNS:

Resolver

The Server

Primary

Secondary

Caching

Database files (*db.domain-name*)

Supports two type of queries:

Recursive

Iterative

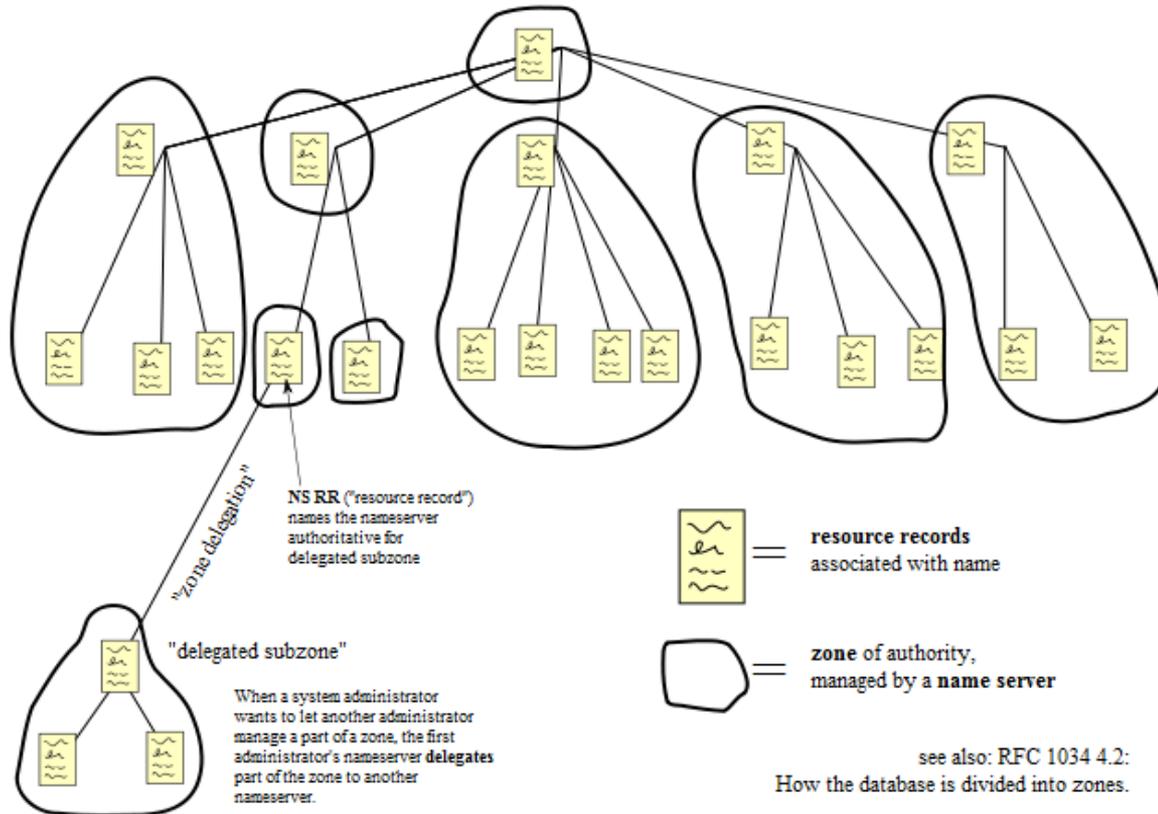
Most popular implementation of DNS is Berkely Internet Name Daemon (BIND)

Maintained by the Internet Systems Consortium: www.isc.org

DNS - Hierarchy of authority

Domain Name Space

Nameless root domain referred to via "."

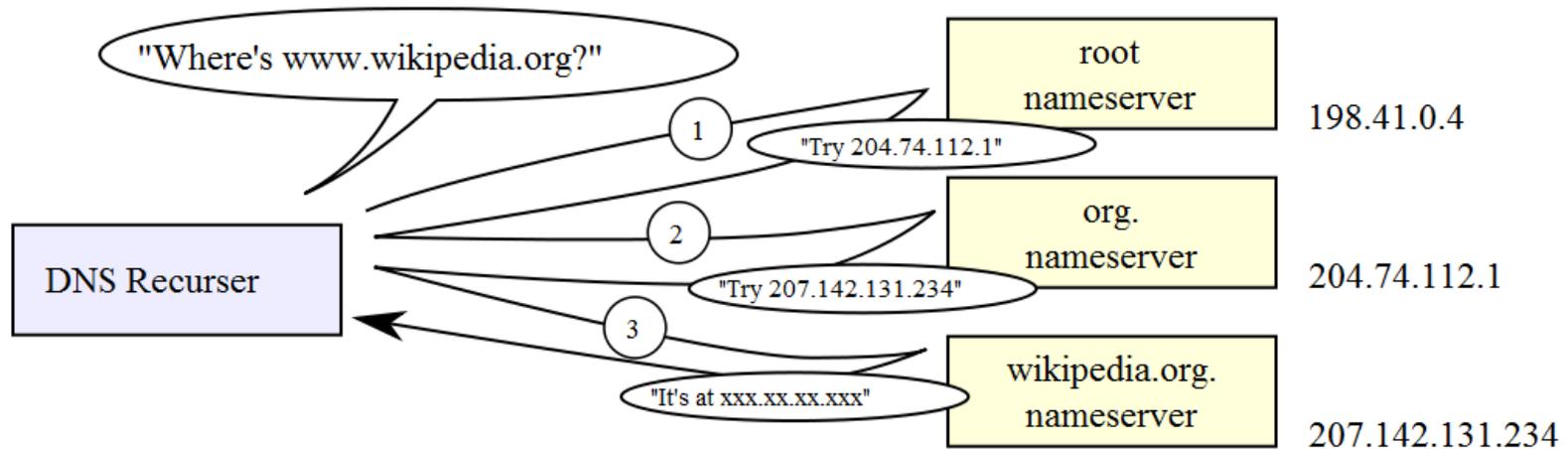


Generic TLD's - Top Level Domains (com, edu, net, org, mil, etc.)

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_DNSBasicNameResolutionTechniquesIterativeandRekurs-4.htm

DNS Database Resource Record types

SOA - Start of Authority

NS - Nameserver

A - IPv4 Address

AAAA - IPv6 Address

PTR - Pointer (for reverse lookups)

CNAME - Aliases

MX - Mail hubs

TXT - associate text strings with a name



Getting a Domain whois command

Anyone can register a domain

The screenshot displays the DreamHost web panel interface for domain registration. The browser address bar shows the URL: <https://panel.dreamhost.com/index.cgi?tree=domain.registration&>. The page title is "Registrations" and includes a "Contact Support" button. The main heading is "Register a New Domain". A search input field contains "mynewdomain.com" and a "Search" button is visible. Below the search field, a promotional banner lists domain extensions and prices: **SALE** .XYZ \$1.95, .CLUB \$0.99, .ONLINE \$4.95, .SITE \$3.95, .STORE \$8.95. A note below the banner states: "Sale prices 1st year only. Additional years charged at regular rates. [See full pricing.](#)". A yellow warning box contains the text: "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](#)." The page also features a sidebar with navigation options: HOME, DOMAINS (Manage Domains, Registrations, Reg. Transfer, Secure Hosting, Remap Sub-Dir, Anonymous FTP, Mongrel and Proxy, Site Statistics), MAIL, GOODIES, DREAMPRESS, VPS, and DEDICATED SERVERS. At the bottom, there is a section titled "Manage Registered Domains on 'Richard's Account'" with a table header including "Domain", "Modify Whois?", "Expires", "Locked?", "Renew Now?", "Auto Renew?", and "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: ~
File Edit View Search Terminal Help
root@eh-kali-05:~# whois simms-teach.com

Whois Server Version 2.0

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

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

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

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

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

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

Domain information fields

Linux whois command

```
root@eh-kali-05: ~  
File Edit View Search Terminal Help  
information purposes only, and to assist persons in obtaining information  
about or related to a domain name registration record. VeriSign does not  
guarantee its accuracy. By submitting a Whois query, you agree to abide  
by the following terms of use: You agree that you may use this Data only  
for lawful purposes and that under no circumstances will you use this Data  
to: (1) allow, enable, or otherwise support the transmission of mass  
unsolicited, commercial advertising or solicitations via e-mail, telephone,  
or facsimile; or (2) enable high volume, automated, electronic processes  
that apply to VeriSign (or its computer systems). The compilation,  
repackaging, dissemination or other use of this Data is expressly  
prohibited without the prior written consent of VeriSign. You agree not to  
use electronic processes that are automated and high-volume to access or  
query the Whois database except as reasonably necessary to register  
domain names or modify existing registrations. VeriSign reserves the right  
to restrict your access to the Whois database in its sole discretion to ensure  
operational stability. VeriSign may restrict or terminate your access to the  
Whois database for failure to abide by these terms of use. VeriSign  
reserves the right to modify these terms at any time.  
  
The Registry database contains ONLY .COM, .NET, .EDU domains and  
Registrars.  
  
Domain Name: SIMMS-TEACH.COM  
Registry Domain ID: 1472785313 DOMAIN COM-VRSN  
Registrar WHOIS Server: whois.dreamhost.com  
Registrar URL: www.dreamhost.com  
Updated Date: 2016-05-17T00:43:20.00Z  
Creation Date: 2008-05-15T11:21:10.00Z  
Registrar Registration Expiration Date: 2017-05-15T18:21:10.00Z  
Registrar: DREAMHOST  
Registrar IANA ID: 431  
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited  
Registry Registrant ID:  
Registrant Name: PRIVATE REGISTRANT  
Registrant Organization: A HAPPY DREAMHOST CUSTOMER  
Registrant Street: 417 ASSOCIATED RD #324  
Registrant Street: C/O SIMMS-TEACH.COM
```

Registrant contact fields

Linux whois command

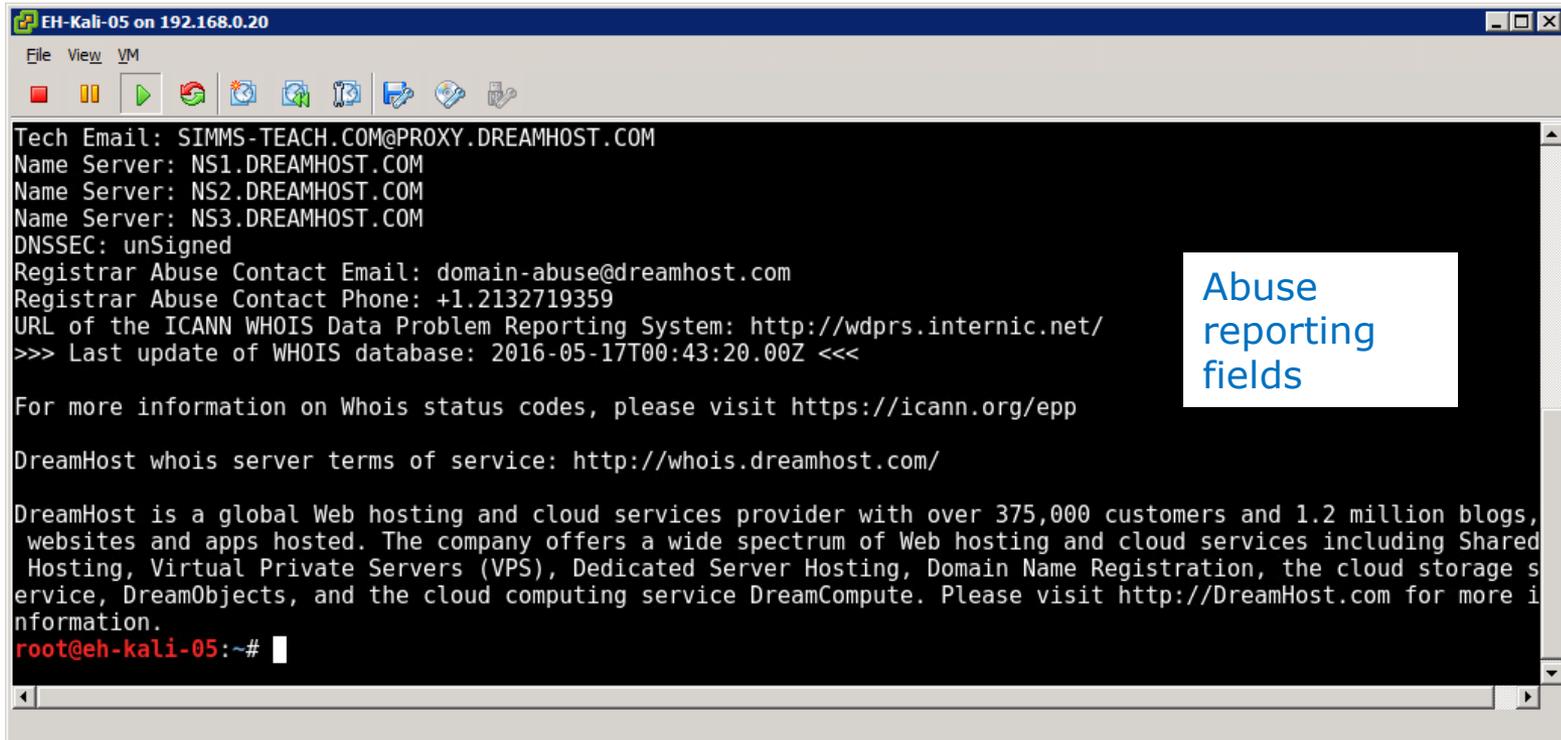
```
root@eh-kali-05: ~  
File Edit View Search Terminal Help  
Registrant Street: C/O SIMMS-TEACH.COM  
Registrant City: BREA  
Registrant State/Province: CA  
Registrant Postal Code: 92821  
Registrant Country: US  
Registrant Phone: +1.7147064182  
Registrant Phone Ext:  
Registrant Fax:  
Registrant Fax Ext:  
Registrant Email: SIMMS-TEACH.COM@PROXY.DREAMHOST.COM  
Registry Admin ID:  
Admin Name: PRIVATE REGISTRANT  
Admin Organization: A HAPPY DREAMHOST CUSTOMER  
Admin Street: 417 ASSOCIATED RD #324  
Admin Street: C/O SIMMS-TEACH.COM  
Admin City: BREA  
Admin State/Province: CA  
Admin Postal Code: 92821  
Admin Country: US  
Admin Phone: +1.7147064182  
Admin Phone Ext:  
Admin Fax:  
Admin Fax Ext:  
Admin Email: SIMMS-TEACH.COM@PROXY.DREAMHOST.COM  
Registry Tech ID:  
Tech Name: PRIVATE REGISTRANT  
Tech Organization: A HAPPY DREAMHOST CUSTOMER  
Tech Street: 417 ASSOCIATED RD #324  
Tech Street: C/O SIMMS-TEACH.COM  
Tech City: BREA  
Tech State/Province: CA  
Tech Postal Code: 92821  
Tech Country: US  
Tech Phone: +1.7147064182  
Tech Phone Ext:  
Tech Fax:  
Tech Fax Ext:  
Tech Email: SIMMS-TEACH.COM@PROXY.DREAMHOST.COM
```

Registrant contact fields

Admin contact fields

Tech contact fields

Linux whois command



```
EH-Kali-05 on 192.168.0.20
File View VM
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:~#
```

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

Activity

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

Write their first names into the chat window.

Domain Information

whois.icann.org

<http://whois.icann.org>

The screenshot shows the ICANN WHOIS website interface. At the top, there is a navigation bar with the ICANN logo and the text "ICANN WHOIS". Below this, there are several menu items: "ABOUT WHOIS", "POLICIES", "GET INVOLVED", "WHOIS COMPLAINTS", and "KNOWLEDGE CENTER". A search bar contains the text "simms-teach.com" and a "Lookup" button. Below the search bar, the text "Showing results for: SIMMS-TEACH.COM" and "Original Query: simms-teach.com" is displayed. The main content area is titled "Contact Information" and is divided into three columns: "Registrant Contact", "Admin Contact", and "Tech Contact". Each column lists contact details such as Name, Organization, Mailing Address, Phone, Ext., Fax, Fax Ext., and Email. To the right of the contact information, there are links for "Submit a Complaint for WHOIS", "WHOIS Inaccuracy Complaint Form", "WHOIS Service Complaint Form", and "WHOIS Compliance FAQs". At the bottom of the page, there are two columns labeled "Registrar" and "Status".

Provides a web interface for getting whois information

<http://whois.icann.org>

The screenshot shows a web browser window with the ICANN WHOIS website. The address bar displays the URL <https://whois.icann.org/en/lookup?name=simms-teach.com>. The search input field contains "simms-teach.com" and a "Lookup" button is visible. The results are displayed in several sections:

- 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>

The screenshot shows a web browser window with the address bar containing `https://whois.icann.org/en/lookup?name=simms-teach.com`. The page features a search input field with `simms-teach.com` and a blue `Lookup` button. Below the search area, the WHOIS data for `simms-teach.com` is displayed in a light gray box. The data is organized into sections for Registry, Admin, and Tech information, each listing various fields such as Name, Organization, Street, City, State, Postal Code, Country, Phone, and Fax.

```
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>

The screenshot shows a web browser window with the URL <https://whois.icann.org/en/lookup?name=simms-teach.com>. The page displays the WHOIS record for the domain `simms-teach.com`. The record includes the following information:

- 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 for the simms-teach.com domain.

What is the email address for the Technical Contact?

Put your answer in the chat window



Domain Information

Domain Dossier

centralops.net

The screenshot shows a web browser window with the URL centralops.net/co/. The page features a blue header with the CentralOps.net logo and the tagline "Advanced online Internet utilities". A navigation menu includes "Utilities" and "About". On the left, a sidebar lists various tools, with "Domain Dossier" highlighted in a red box. The main content area is titled "Free online network tools" and lists several utilities: Domain Dossier, Domain Check, Email Dossier, Browser Mirror, Ping, Traceroute, NsLookup, AutoWhois, and AnalyzePath. Each utility has a brief description. A user information box at the top right shows the user is anonymous with 35 service units remaining. A "How this site works" section explains that tools are free for everyday use, but extended or automated use requires a paid account.

*Free online
anonymous tools*

*Click on the Domain
Dossier link on the
left panel*

<http://centralops.net/co>

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

Domain Dossier Investigate domains and IP addresses

domain or IP address

domain whois record DNS records traceroute
 network whois record service scan

user: anonymous [71.198.222.56]
balance: 44 units
[log in](#) | [account info](#)

Address lookup

canonical name [simms-teach.com](#)
aliases
addresses **208.113.154.64**

Domain Whois record

Queried [whois.internic.net](#) with "dom simms-teach.com"...

```

Domain Name: SIMMS-TEACH.COM
Registry Domain ID: 1472785313_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.dreamhost.com
Registrar URL: http://www.DreamHost.com
Updated Date: 2017-05-16T07:28:52Z
Creation Date: 2008-05-15T18:21:10Z
Registry Expiry Date: 2018-05-15T18:21:10Z
Registrar: DreamHost, LLC
Registrar IANA ID: 431
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: NS1.DREAMHOST.COM
Name Server: NS2.DREAMHOST.COM
Name Server: NS3.DREAMHOST.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicof/
>>> Last update of whois database: 2017-09-18T20:55:19Z <<<

```

Queried [whois.dreamhost.com](#) with "simms-teach.com"...

```

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: 2017-05-17T00:28:06.002Z
Creation Date: 2008-05-15T11:21:10.002Z
Registrar Registration Expiration Date: 2018-05-15T18:21:10.002Z
Registrar: DREAMHOST
Registrar IANA ID: 431

```

The Domain Dossier provides whois info, DNS and service information

Activity

Using the Domain Dossier website:

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

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

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

host & nslookup commmands

Forward and reverse DNS
lookups

host command

```

rsimms@oslab:~
NAME
  host - DNS lookup utility

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

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

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

Easy to use Linux command for resolving names or IP addresses

host command on Linux

Forward lookup

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

Reverse lookup

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

host command on Linux

```
root@kali:~# host opus.cis.cabrillo.edu ns1.cis.cabrillo.edu
```

```
Using domain server:
```

```
Name: ns1.cis.cabrillo.edu
```

```
Address: 2607:f380:80f:f425::252#53
```

```
Aliases:
```

```
opus.cis.cabrillo.edu is an alias for oslab.cis.cabrillo.edu.
```

```
oslab.cis.cabrillo.edu has address 207.62.187.230
```

```
oslab.cis.cabrillo.edu has IPv6 address 2607:f380:80f:f425::230
```

```
root@kali:~#
```

```
root@kali:~# host opus.cis.cabrillo.edu ns2.cis.cabrillo.edu
```

```
Using domain server:
```

```
Name: ns2.cis.cabrillo.edu
```

```
Address: 2607:f380:80f:f425::253#53
```

```
Aliases:
```

```
opus.cis.cabrillo.edu is an alias for oslab.cis.cabrillo.edu.
```

```
oslab.cis.cabrillo.edu has address 207.62.187.230
```

```
oslab.cis.cabrillo.edu has IPv6 address 2607:f380:80f:f425::230
```

```
root@kali:~#
```

*Specifying a
specific name
server to do
the name
resolution*

nslookup command on Windows

Forward lookup

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

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

Reverse lookup

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

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

Activity

Using the host command to do a forward lookup on:

simms-teach.com

Put the IP address in the chat window

Activity

Using the host command to do a reverse lookup on:

208.113.154.64

What ISP am I hosting my website on?

Put your answer in the chat window

Domain Records

dig

dig command

```

rsimms@opus-iii:~
DIG(1)                                BIND9                                DIG(1)
NAME
    dig - DNS lookup utility

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

    dig [-h]

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

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

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

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

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

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

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

```

Find domain name servers

dig ns cis.cabrillo.edu

```

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

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

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

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

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

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

root@eh-kali-05:~# █

```

Find domain mail servers

dig mx cis.cabrillo.edu

```

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

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

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

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

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

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

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

root@eh-kali-05:~# █

```

Find domain administrative contact

dig soa cis.cabrillo.edu

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

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

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

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

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

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

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

*email address of
administrator*

Find domain hosts via zone transfer

dig axfr cis.cabrillo.edu

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

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

snipped

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

[root@ns2 ~]#
```

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

Examine txt records

dig txt cis.cabrillo.edu

```

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

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

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

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

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

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

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

[rsimms@opus-ii ~]$

```

Looking at txt records may reveal network information

Activity

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

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

Activity

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

Write your answer in the chat window

Identifying IP Addresses

whatismyipaddress.com/

<http://whatismyipaddress.com/>

The screenshot shows a web browser window with the URL <http://whatismyipaddress.com/ip/207.62.187.230>. The page features a green header with navigation links: MY IP, IP LOOKUP, SPEED TEST, BLACKLIST CHECK, TRACE EMAIL, CHANGE IP, HIDE IP, IP TOOLS, LEARN, and COMMUNITY. The main content area displays the following information:

- IP Details for 207.62.187.230**
- Warning: 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.
- Input field: 207.62.187.230
- Section: **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](#)
- Section: **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

Additional elements include a search bar, social media links (Facebook, Twitter), and a "Check out our new Learning Center" section with a lightbulb icon and a "Start Here" button.

<http://whatismyipaddress.com/>

The screenshot shows a web browser window with the URL `whatismyipaddress.com/ip/207.62.187.230`. The page displays the following information:

- 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

Geolocation Map

User Comments

No comments. Be the first to add one.

Waiting for partners.tremorhub.com...
acters in your comment about this IP address.

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](#)

Metromile

Car insurance based on the miles you drive.

Paying

[GET A QUOTE](#)

Like this site? Post a review!

<http://whatismyipaddress.com/>

Blacklist Check

How you **connect** to the world

IPv6
WhatIsMyIPAddress.com

IP Address|Search Search

MY IP IP LOOKUP SPEED TEST BLACKLIST CHECK TRACE EMAIL CHANGE IP HIDE IP IP TOOLS LEARN COMMUNITY

Home » IP Tools » Blacklist Check

Blacklist Check

Like Page 244K likes

Blacklist Check

Tweet Share 170

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 Check Blacklists

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

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

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/) vk.org all.s5h.net

Like this site? Post a review!

<http://whatismyipaddress.com/>

Blacklist Status

- access.rethawk.org
- b.barracudacentral.org
- bl.spamcop.net
- blackholes.wirehub.net
- block.dnsbl.sorbs.net
- boqons.cymru.com
- cbl.abuseat.org
- dev.null.dk
- dialups.mail-abuse.org
- dnsbl.abuse.ch
- dnsbl.antisipam.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.apewvs.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
- smp.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.tioan.com
- blacklist.sci.kun.nl
- blocked.hilli.dk
- cart00nev.surriel.com
- cbless.anti-spam.org.cn
- dialup.blacklist.jp.pg.org
- dialups.visi.com
- dnsbl.anticapta.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.jp.pg.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
- xbi.spamhaus.org
- zombie.dnsbl.sorbs.net
- rbl.megarbl.net

Number

- Free Cell Phone Finder
- Tracking Cell Phone
- Find IP Physical Location
- Content Personalization
- Watch: Hillary Will Fail
- Enter Address & Location
- Mktg Automation Checklist
- Remove Malware - Free

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

Like this site? Post a review!

Activity

Top attackers

NoSweat : Sunday, September 17, 2017

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

Pick one of the IP addresses above and using:

<http://whatismyipaddress.com/>

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

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

shodan

SHODAN

Shodan

https://www.shodan.io

SHODAN

Explore Enterprise Access Contact Us

New to Shodan? Login or Register

The search engine for the Internet of Things

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

Create a Free Account Getting Started

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.

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.

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!

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.

SHODAN

The screenshot shows the Shodan search engine interface. The browser address bar displays `https://www.shodan.io/host/207.62.187.230`. The page features a navigation menu with options like 'Explore', 'Downloads', 'Reports', 'Enterprise Access', 'Contact Us', 'My Account', and 'Upgrade'. A satellite map shows the location of the IP address, with a red pin and the label 'FRONT Edu Ctr RD'. Below the map, the IP address `207.62.187.230` is associated with `oslab.cis.cabrillo.edu`. A table lists various details:

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

To the right, the 'Ports' section shows two open ports: 25 and 443. The 'Services' section lists the following:

- 25
- tcp
- smtp

The 'Sendmail' service is identified with version 8.14.4/8.14.4. Below this, a sample SMTP session is shown:

```
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-BBITHIME
250-SIZE
250-DSN
250-ETRN
250-AUTH GSSAPI
```

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"
```

Activity

Use the host command to find the IP address for:

`microlab.simms-teach.com`

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

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

Write those ports in the chat window



Light probing with telnet and nc

telnet command

```

root@eh-kali-05: ~
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

```

root@eh-kali-05: ~
NC (1)          General Commands Manual          NC (1)
NAME
nc - TCP/IP swiss army knife

SYNOPSIS
nc [-options] hostname port[sl] [ports] ...
nc -l -p port [-options] [hostname] [port]

DESCRIPTION
netcat is a simple unix utility which reads and writes data across network connections, using TCP or UDP protocol. It is designed to be a reliable "back-end" tool that can be used directly or easily driven by other programs and scripts. At the same time, it is a feature-rich network debugging and exploration tool, since it can create almost any kind of connection you would need and has several interesting built-in capabilities. Netcat, or "nc" as the actual program is named, should have been supplied long ago as another one of those cryptic but standard Unix tools.

In the simplest usage, "nc host port" creates a TCP connection to the given port on the given target host. Your standard input is then sent to the host, and anything that comes back across the connection is sent to your standard output. This continues indefinitely, until the network side of the connection shuts down. Note that this behavior is different from most other applications which shut everything down and exit after an end-of-file on the standard input.

Netcat can also function as a server, by listening for inbound connections on arbitrary ports and then doing the same reading and writing. With minor limitations, netcat doesn't really care if it runs in "client" or "server" mode -- it still shows 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-address> <port>

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

Probing simms-teach.com (telnet)

telnet simms-teach.com 80

HEAD / HTTP/1.0

(then enter blank line)

```
root@eh-kali-05: ~  
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 simms-teach.com (nc)

nc simms-teach.com 80

HEAD / HTTP/1.0

(then enter blank line)

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

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

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

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

Probing eh-centos VM (telnet)

telnet eh-centos 80

HEAD / HTTP/1.0

(then enter blank line)

```

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 eh-centos VM (nc)

nc eh-centos 80

HEAD / HTTP/1.0

(then enter blank line)

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

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

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

Probing OWASP VM (telnet)

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

```

root@eh-kali-05: ~
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

Probing OWASP VM (nc)

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

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

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

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

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

Activity

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

What web server software and version is ruining there?

Put your answer in the chat window

Using telnet for port 25 (SMTP)

Some SMTP commands

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

Probing port 25 on EH-CentOS VM

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

This server is running Postfix as the SMTP service.

You can actually use telnet to send an email!

Checking for new email on EH-CentOS VM

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

What a crazy way to send an email huh?

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

Yep, it really works!

Activity

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

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

Put the mail header which looks like this:

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

into the chat window



Website Information

Netcraft

Netcraft

The screenshot shows the Netcraft website interface. At the top, there is a navigation menu with links for Home, News, Anti-Phishing, Security Testing, Internet Data Mining, Performance, and About Netcraft. The main heading is "Internet Security and Data Mining". Below this, there is a paragraph describing Netcraft's services: "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." To the right, there is a "Latest News" section and a "Get in Touch" section with contact information: "+44 (0) 1225 447500" and "info@netcraft.com". Below the main heading, there are four tabs: "Anti-Phishing", "Security Testing", "Internet Data Mining", and "Performance". Under "Internet Data Mining", there is a line graph titled "Market Share for Top Servers Across All Domains" showing the percentage share of various servers over time. The legend includes Apache, Microsoft, Sun, nginx, Google, NCSA, and Other. Below the graph, there is a section titled "Understand your Competitors" with a list of services: "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)", and "Find out more". At the bottom left, there is a "Solutions For..." section with a list of industries: Banks, Certificate Authorities, Domain Registrars, Domain Registries, and Hosting Companies; Investors and Venture Capitalists, Online Merchants, Security Providers, and Software Industry. On the right, there is a "What's that site running?" section with a search box containing "netcraft.com" and a "Report Suspicious URL" button.

My Website

Rich's Cabrillo College CIS Classes
Home Page

Home Resources Forums CIS Lab Canvas

Login
Flashcards
Admin

CIS 76
CIS 90
Previous Terms

88 days till term ends!

[Cabrillo College Web Advisor](#)
[Commands and Files](#)

[VLab \(classic\)](#)
[VLab \(web\)](#)
[NETLAB+](#)

[CIS 76 VLab Pod Assignments](#)

[CIS 90 VLab VM Assignments](#)

[RIP Dennis Ritchie](#)

Rich Simms

Contact

- Email: risimms@cabrillo.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](#)

Netcraft

Site report for simms-teach.com

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: [f](#) [t](#) [in](#) [g+](#) [Y](#) [e](#)

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		

Netcraft

Site report for simms-teach.com

toolbar.netcraft.com/site_report?url=http://simms-teach.com

Phishing Site Countermeasures

Extension Support

- FAQ
- Glossary
- Contact Us
- Report a Bug

Tutorials

- Installing the Extension
- Using the Extension
- Getting the Most
- Reporting a Phish

About Netcraft

- Netcraft Home
- About Netcraft
- Website Terms of Use
- Phishing Site Feed
- Security Services
- Contact Us

[f](#)
[t](#)
[in](#)
[g+](#)
[y](#)
[es](#)

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.

Netcraft

The screenshot shows a web browser window displaying a Netcraft site report for 'simms-teach.com'. The page is titled 'Web Trackers' and explains that these are third-party resources used for tracking user behavior. It states that one known tracker was identified: W3C. Two pie charts show that 100% of the trackers are from W3C and belong to the 'Widget' category. Below the charts is a table listing the identified tracker. The 'Site Technology' section is also visible, showing server-side technologies like PHP and SSL, and client-side technologies.

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).

Netcraft

Site report for simms-tea x

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

Netcraft

Site report for simms-teach.com

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.iffattoquotidiano.it
HTML	The main markup language used for displaying web pages within browsers	www.amazon.de , www.imdb.com , www.amazon.fr

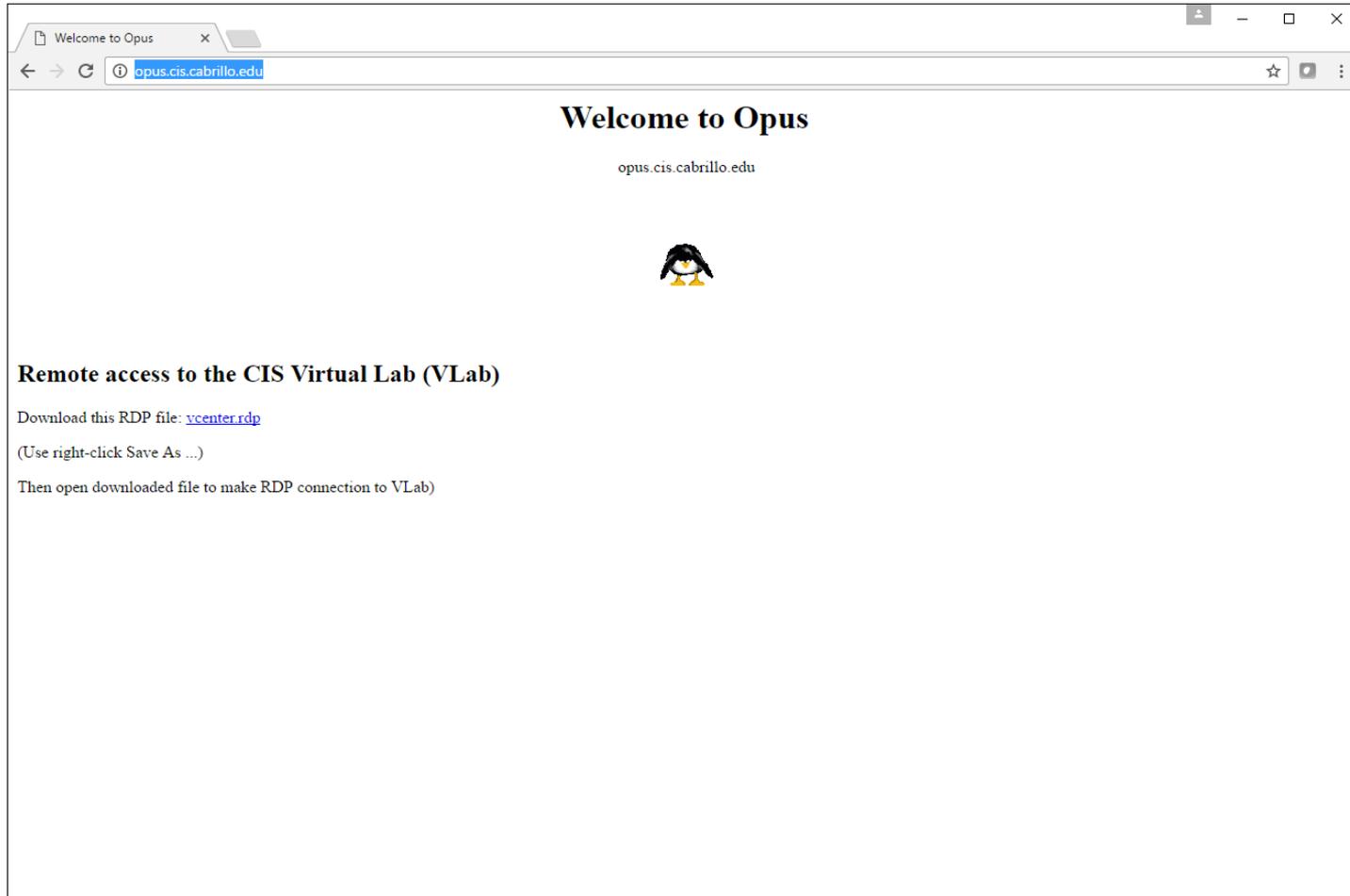
CSS Usage

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	<i>No description</i>	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

COPYRIGHT © NETCRAFT LTD. 2016

Opus website



Netcraft

The screenshot shows a web browser window displaying a Netcraft site report for opus.cis.cabrillo.edu. The page features the Netcraft logo, a search bar, and a navigation menu on the left. The main content area is divided into sections for 'Background' and 'Network' information.

Background Information:

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

Network Information:

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:f425:0:0:230	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		

The right sidebar contains a 'Global Data Center Locations' advertisement for DATAPIPE.

Netcraft

Site report for opus.cis.cabrillo.edu

toolbar.netcraft.com/site_report?url=http://opus.cis.cabrillo.edu/

Phishing Site Countermeasures

Extension Support

- FAQ
- Glossary
- Contact Us
- Report a Bug

Tutorials

- Installing the Extension
- Using the Extension
- Getting the Most
- Reporting a Phish

About Netcraft

- Netcraft Home
- About Netcraft
- Website Terms of Use
- Phishing Site Feed
- Security Services
- Contact Us

Hosting History

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

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.

Netcraft

Site report for opus.cis.cabrillo.edu

toolbar.netcraft.com/site_report?url=http://opus.cis.cabrillo.edu/

- About Netcraft
- Website Terms of Use
- Phishing Site Feed
- Security Services
- Contact Us

f t in g+ Y

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.cnb.com
Apache ↗	Web server software	www.ilsole24ore.com , www.businessinsider.com , www.bom.gov.au

COPYRIGHT © NETCRAFT LTD. 2016

Activity

Using netcraft:

<https://www.netcraft.com/>

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

`opus.cis.cabrillo.edu`

`opus-ii.cis.cabrillo.edu`

Which server uses OpenSSL technology

Write your answer in the chat window

robtex.com

Robtex

The screenshot shows a web browser window with the URL <https://www.robtext.com/dns-lookup/simms-teach.com>. The page title is "simms-teach.com" and the breadcrumb trail is "Robtex >>> DNS >>> com >>> simms-teach".

Below the breadcrumb trail, there are social media sharing buttons for Reddit, Twitter, LinkedIn, Facebook, VKontakte, Google+, Email, Print, and More. A "Follow" button for Twitter shows 640 followers. A search bar contains "simms-teach.com" and a "GO" button.

A button labeled "Try our chrome extension!" is centered below the search bar.

A row of navigation tabs includes "ANALYSIS" (highlighted with a red box), "RECORDS", "SEO", "WOT", "SHARED", "GRAPH", "HISTORY", "WHOIS", "DNSBL", and "GRAPH(old)".

The "ANALYSIS" section is active, showing the following information:

- ANALYSIS** (with up/down arrows)
- simms-teach.com** has three name servers and one IP number.
- Dreamhost name servers**
 - The name servers are `ns1.dreamhost.com` (used by 1,060,000 domains), `ns2.dreamhost.com` (used by 1,070,000 domains) and `ns3.dreamhost.com` (used by 1,070,000 domains).
 - The combination is used by 1,060,000 domains.
 - Example: `manalive.net`, `graphpress.com`, `abrdgd.org` and `rihana-ries.com`.
- IP number**
 - The IP number is `208.113.154.64` (used by 75 host names).
 - 65 domains use **only** the IP number `208.113.154.64`.
 - Example: `unitedspaceschool.com`, `www.jamethiel.com`, `tlcmagonline.com` and `hybegnu.com`.

Robtex

The screenshot shows a web browser window with the URL <https://www.robtex.com/dns-lookup/simms-teach.com>. The page title is "simms-teach.com" and the breadcrumb trail is "Robtex >>> DNS >>> com >>> simms-teach".

Navigation links include: [Reddit](#), [Twitter](#), [LinkedIn](#), [Facebook](#), [Vkontakte](#), [G+ Google+](#), [Email](#), [Print](#), and [More](#). A "Follow" button shows 640 followers.

A search bar contains "simms-teach.com" and a "GO" button.

A button labeled "Try our chrome extension!" is present.

Navigation tabs include: ANALYSIS, RECORDS, SEO, WOT, **SHARED** (highlighted with a red box), GRAPH, HISTORY, WHOIS, DNSBL, and GRAPH(old).

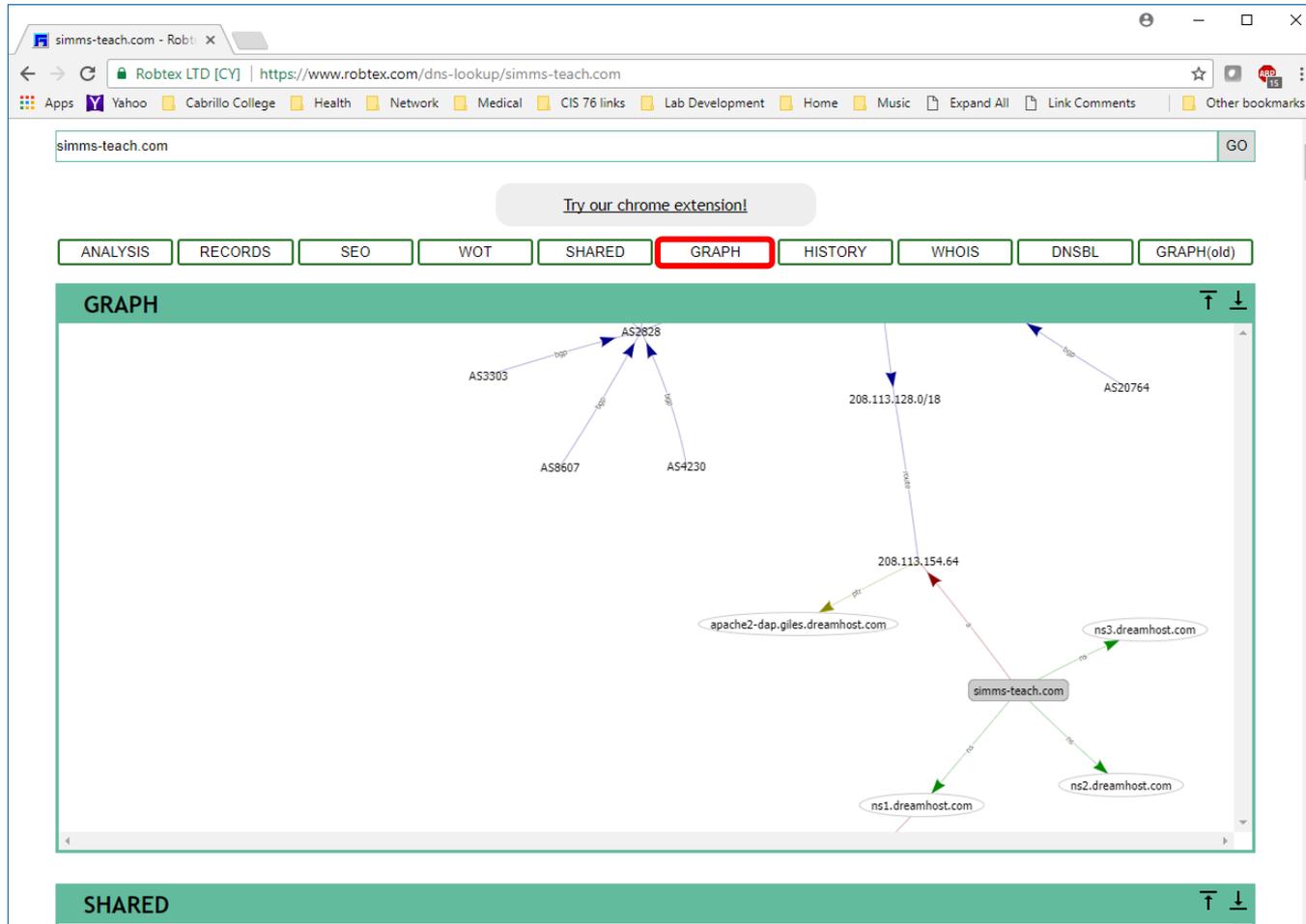
The "SHARED" section is active and displays two panels:

- Using as mail server under another name:** Shows "timmerthemovie.com" and "1 results shown."
- Siblings:** Lists domains: bidefordtaxi.com, creativemadebranding.com, erwinlutzer.com, halestudio.com, karanfalkargo.com, millfieldconsulting.com, piscatawayfireschool.com, savenwpp.com, theflashpackers.com, zurisinmobiliaria.com. Shows "10 results shown."

Other panels at the bottom include:

- IP numbers:** 208.113.154.64
- Sharing IP numbers:** bobgordonfilms.com, compromissodeuniaio.com
- Partially sharing IP numbers:** jfleach.com+, mathewslandconservancy.com+
- Name servers:** ns1.dreamhost.com
- Sharing name servers:** acleanerwindow.com, danislojistik.com

Robtex



Activity

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

www.shodan.io

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

Write your answer in the chat window

Maltego

TNT Major Crimes TV Series



Maltego

The community edition is a free version of the commercial client Maltego with various limitations.

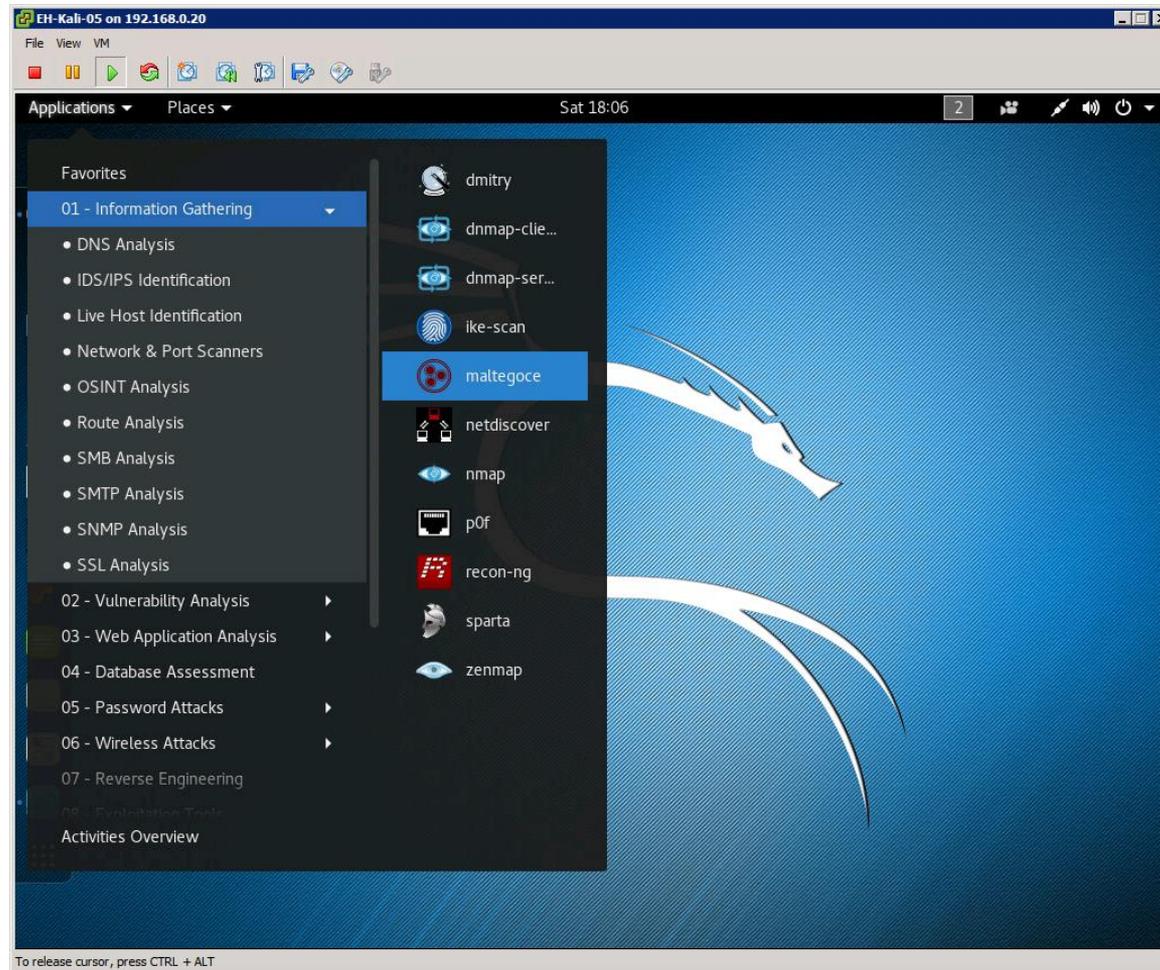
Limitations :

- 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

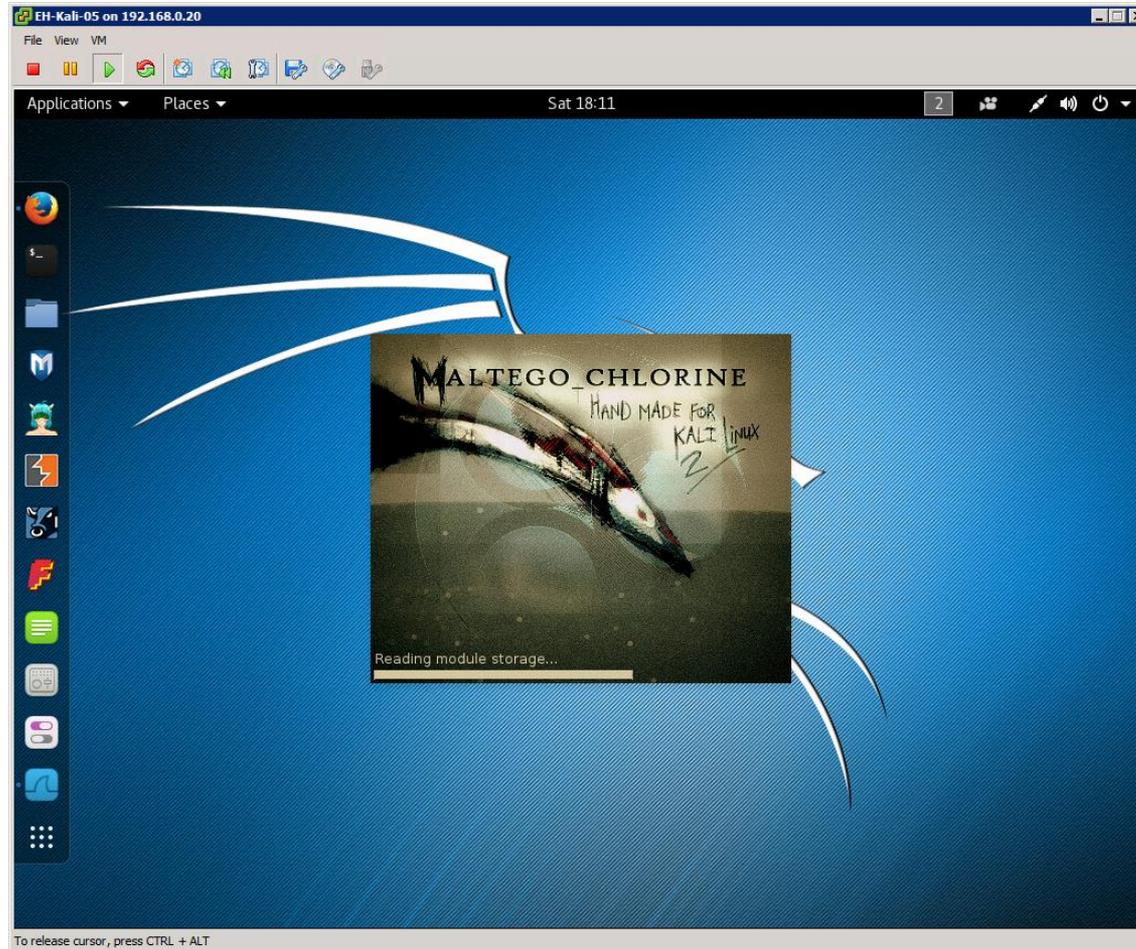
The screenshot shows a web browser window displaying the Paterva website. The browser's address bar shows the URL <https://www.paterva.com/web7/>. The website header features the Paterva logo (a stylized 'P' in a circle) and the tagline "A new train of thought". Navigation links include ABOUT, PRODUCTS, SERVICES, QUOTES, DOWNLOADS, DOCS, and CONTACT. The main content area has a dark background with a chalkboard and the text "Maltego makes smart people smarter." Below this is a red "Buy" button. Three product cards are displayed: "Maltego GUI" with a green circular icon, "About Paterva" with a blue circular icon, and "Maltego Servers" with a yellow circular icon. Each card has a "Read more" button at the bottom.

Maltego

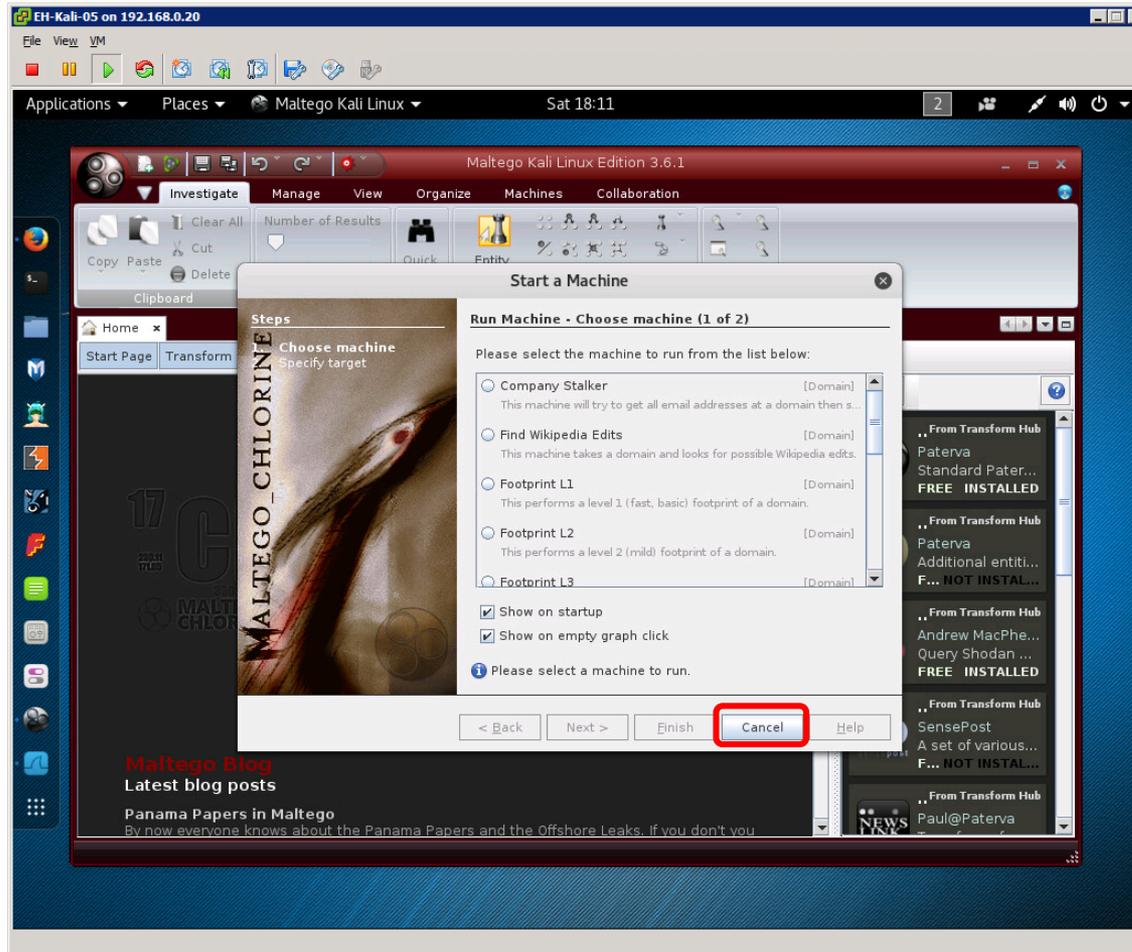


Applications > 01-Information Gathering > maltego

Maltego

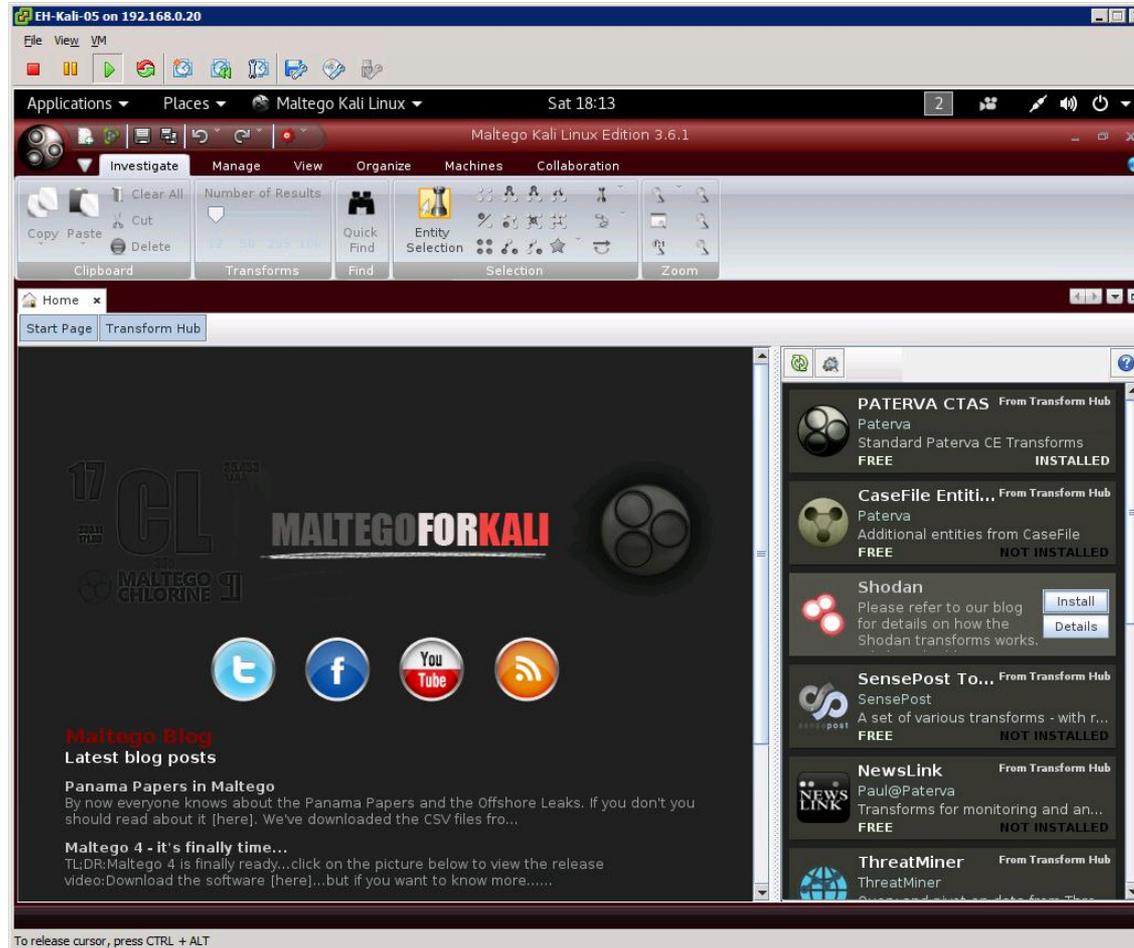


Maltego



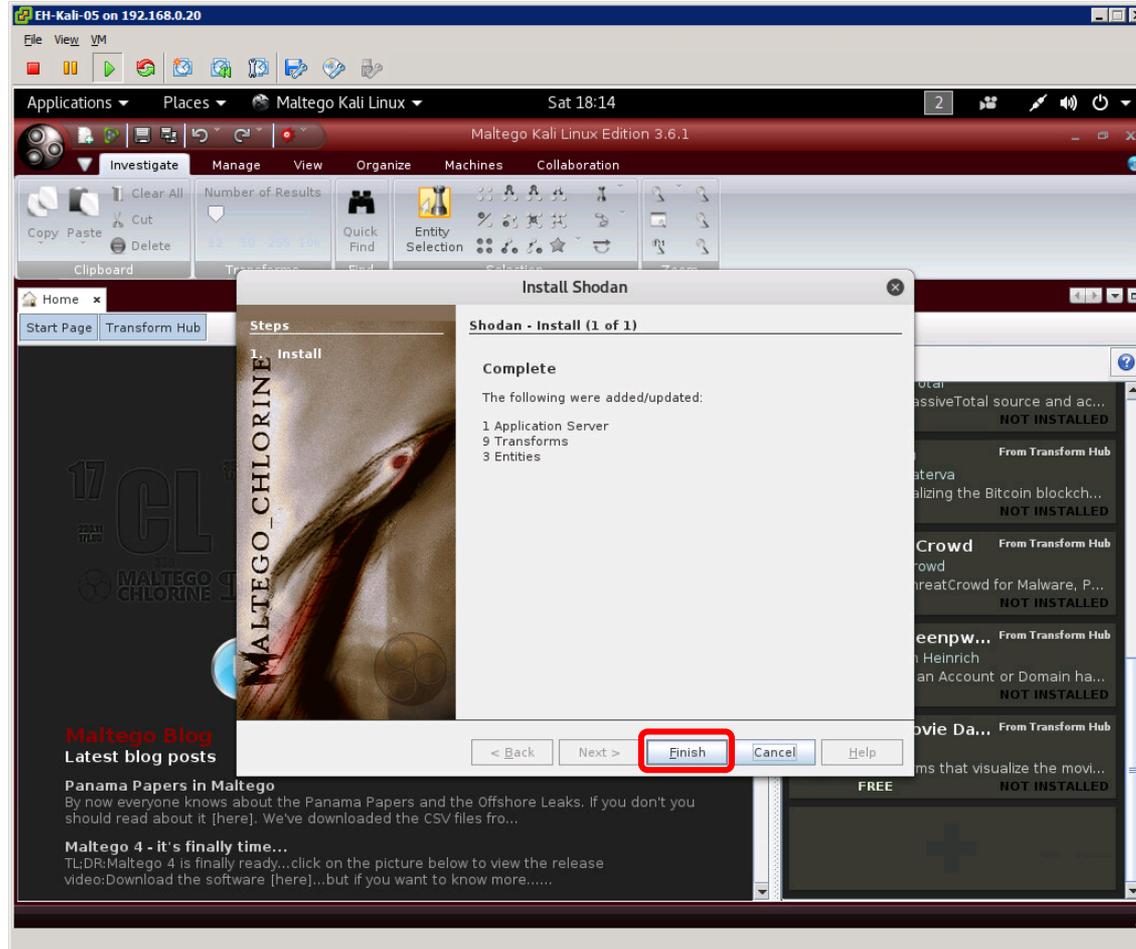
Click Cancel.

Maltego



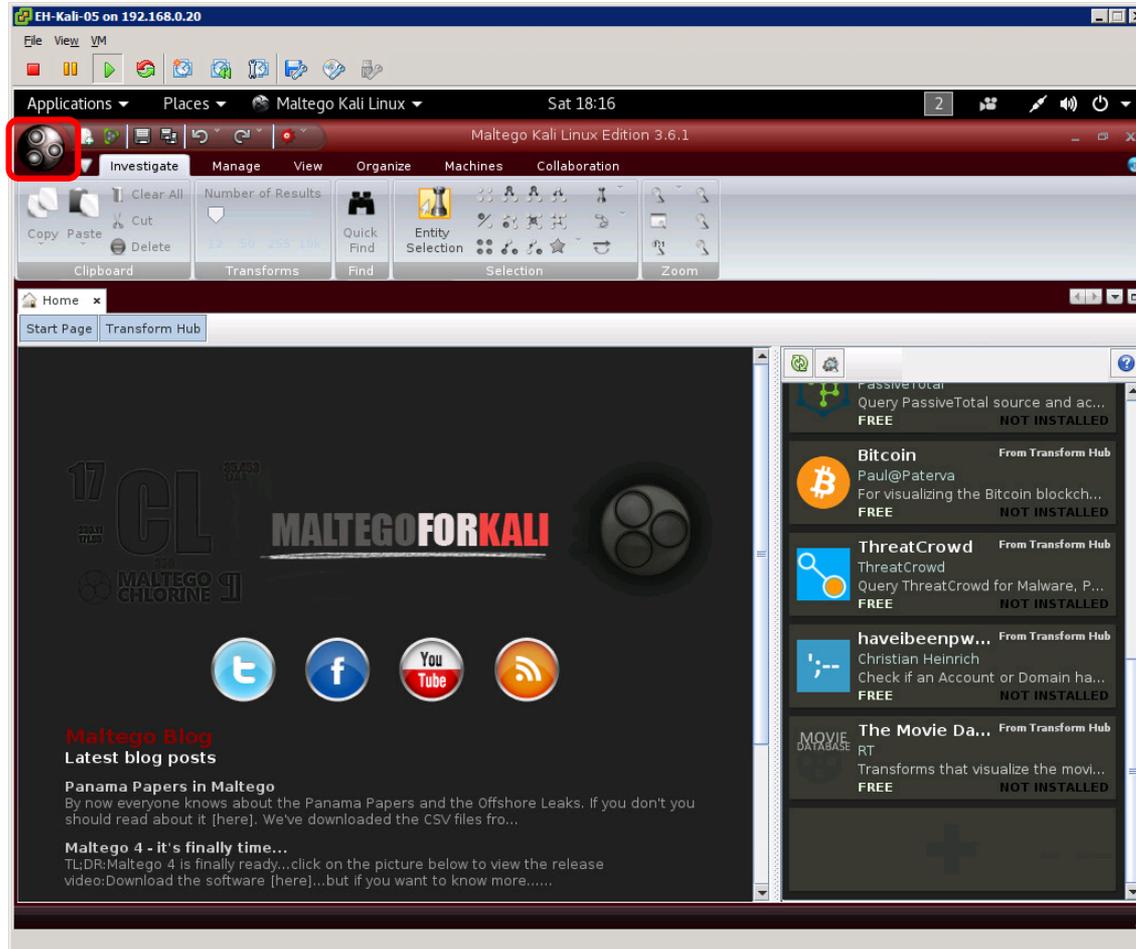
Install Shodan transform

Maltego



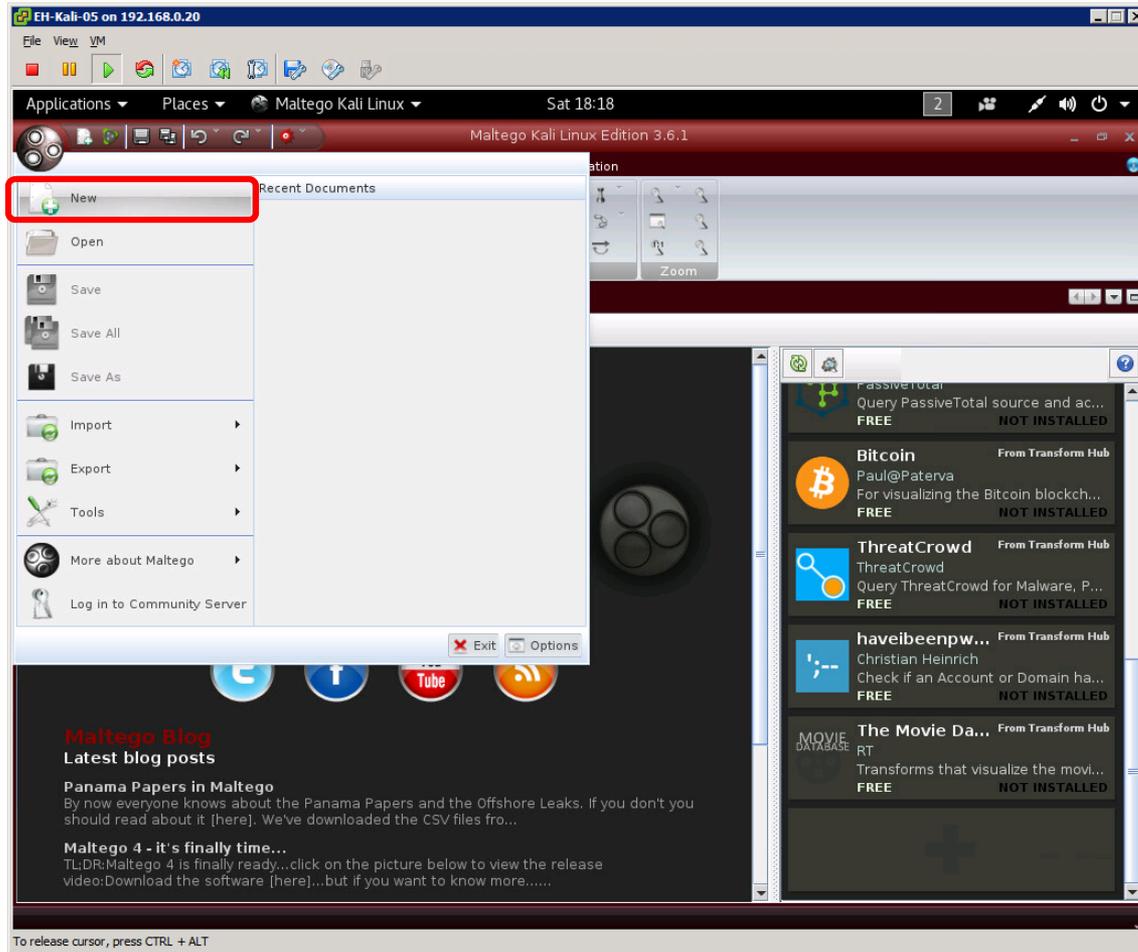
Click Finish.

Maltego



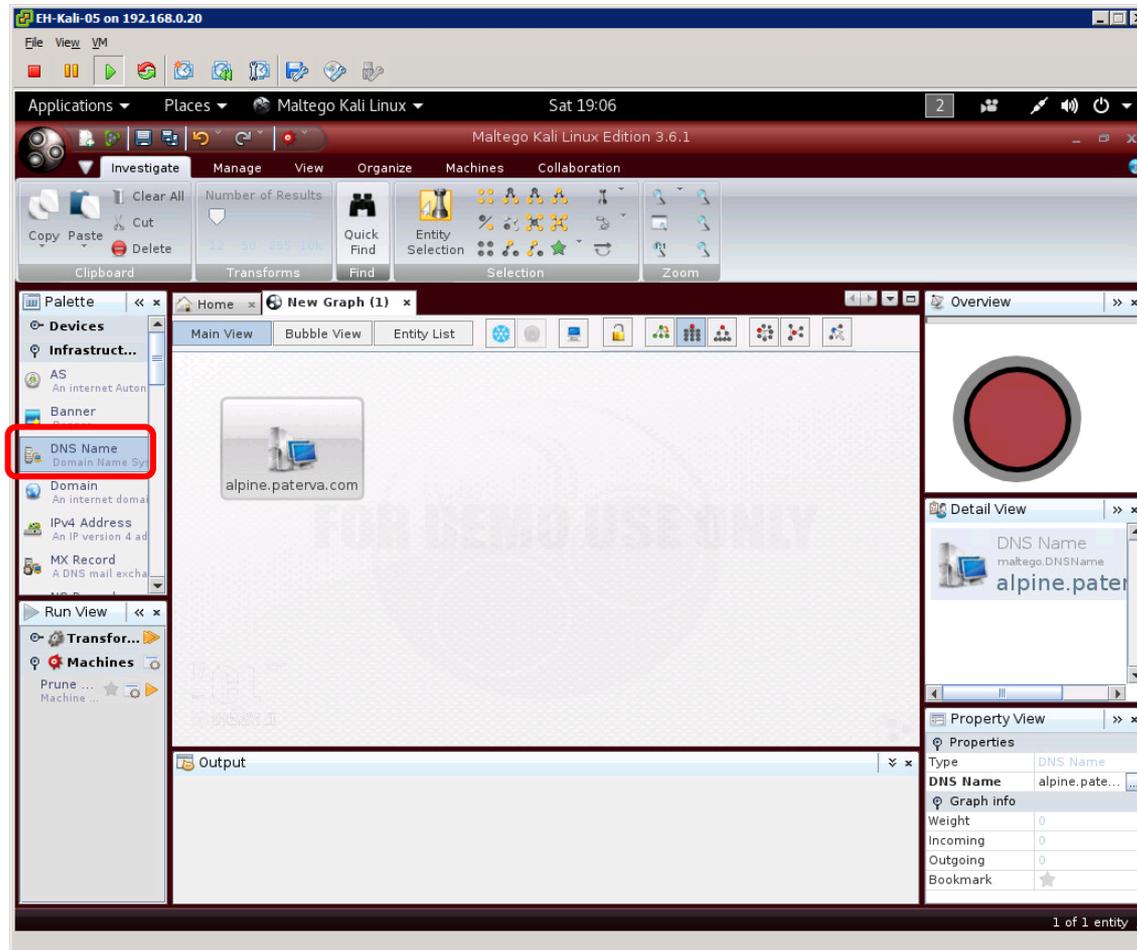
Click main Maltego icon.

Maltego



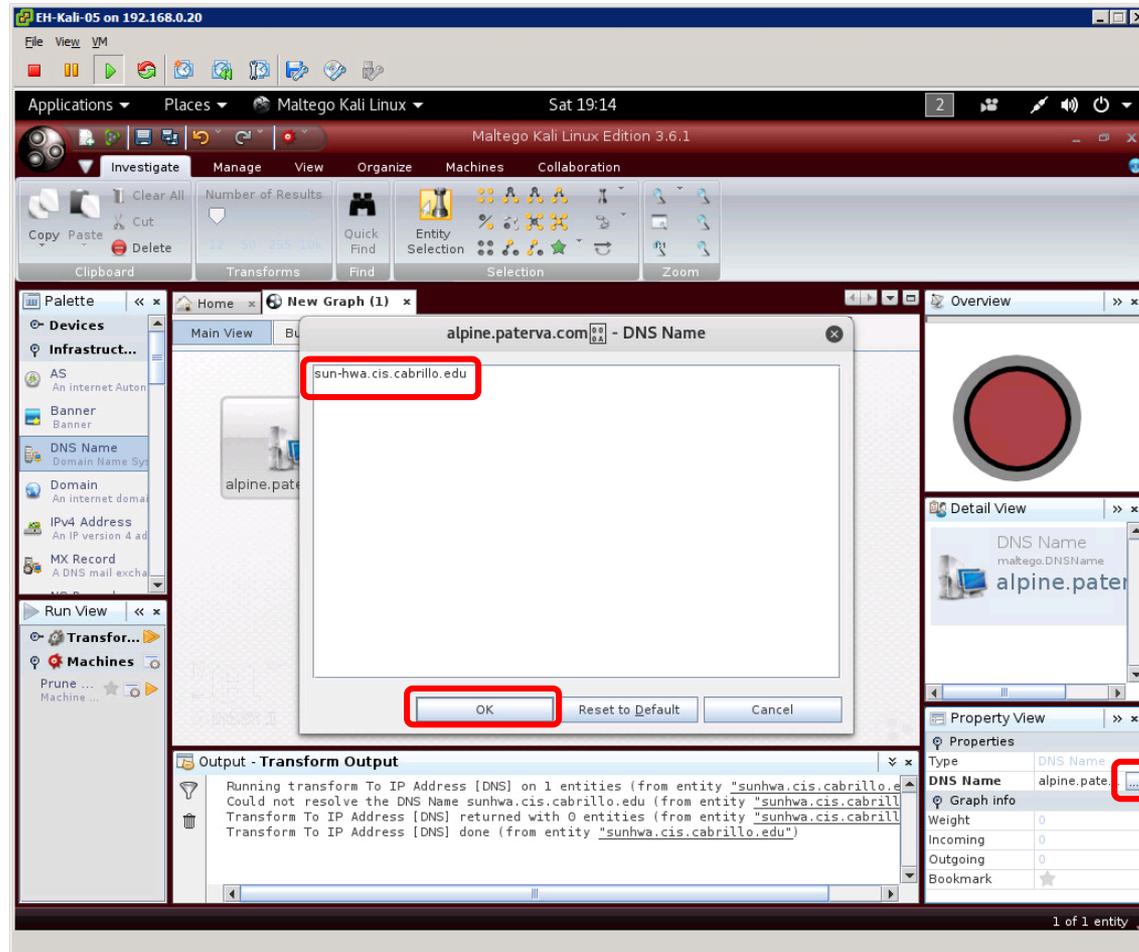
Select New.

Maltego



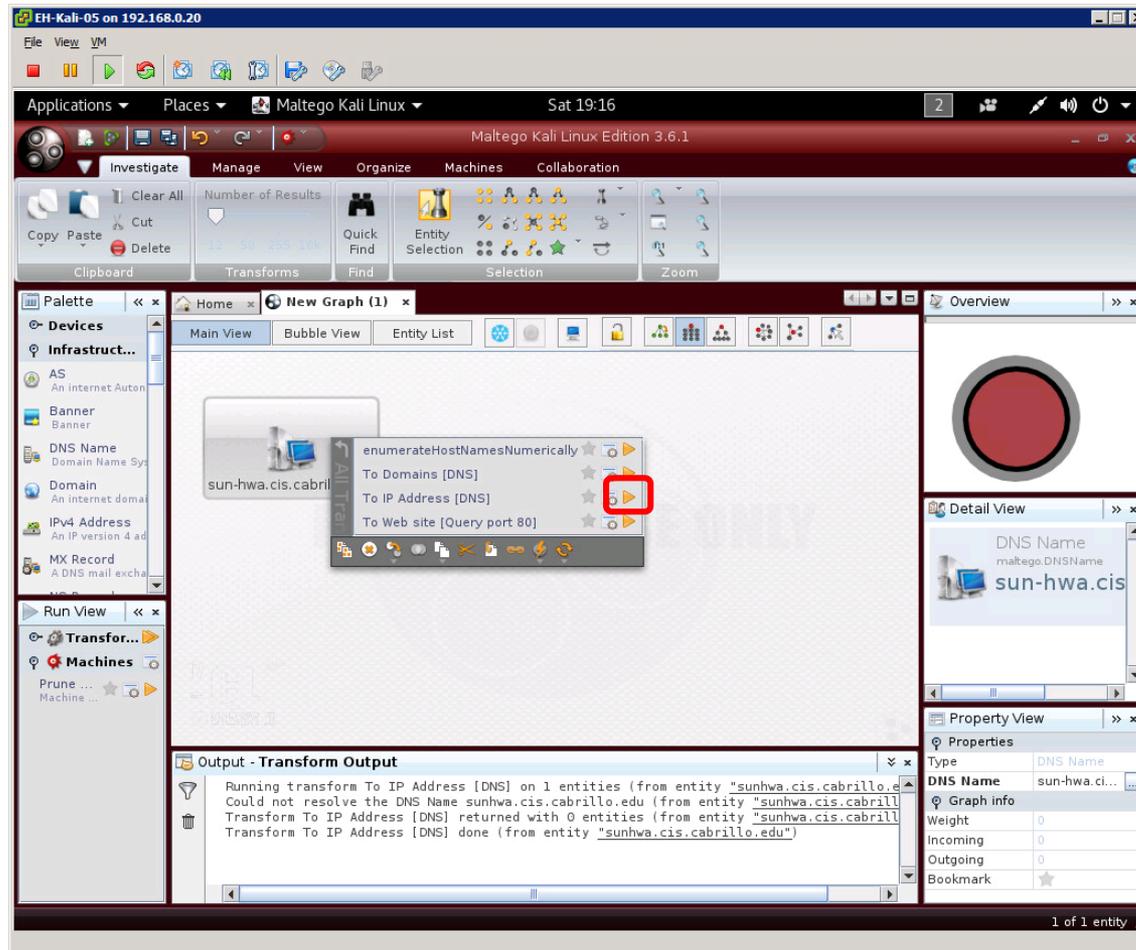
Click on DNS Name in the Infrastructure Palette and drag to the New Graph.

Maltego



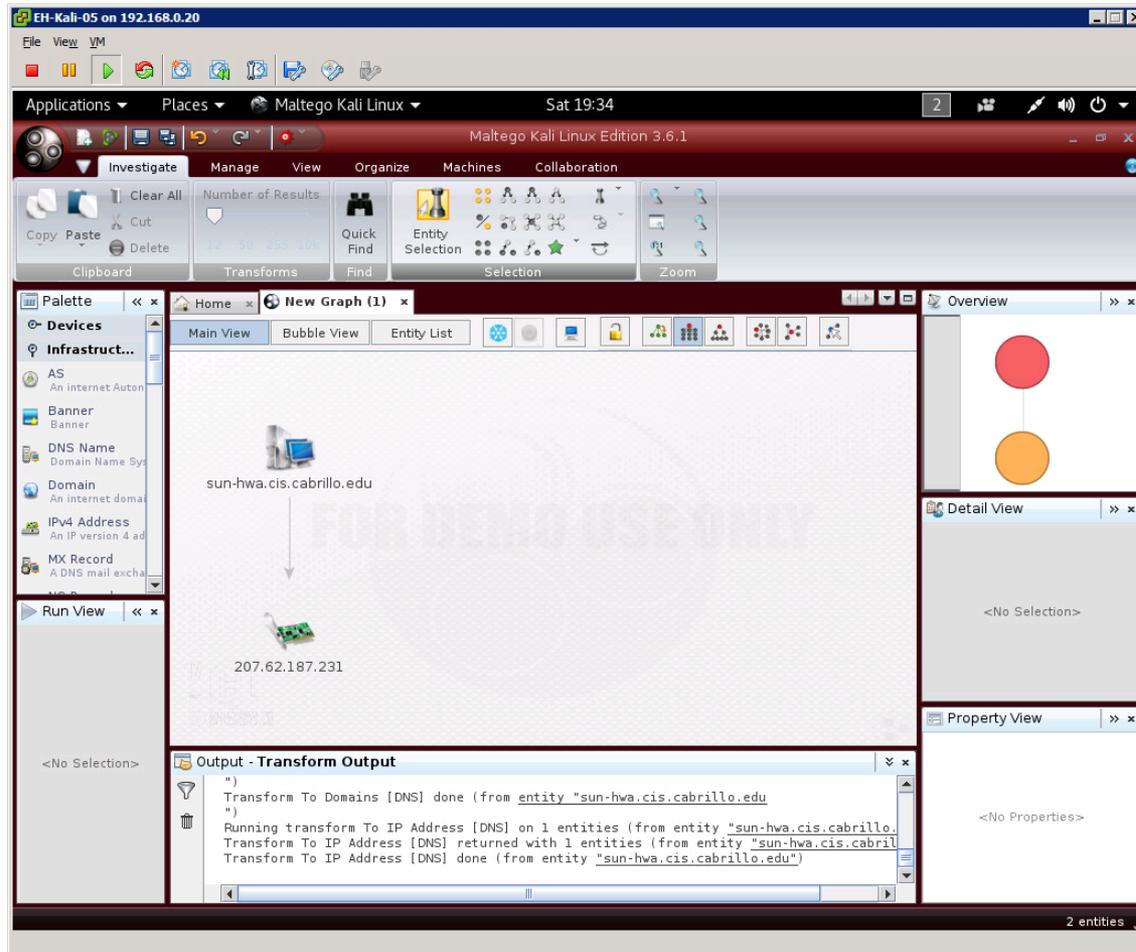
Click the "... " icon in the Property View to change the DNS Name to sun-hwa.cis.cabrillo.edu then click OK.

Maltego



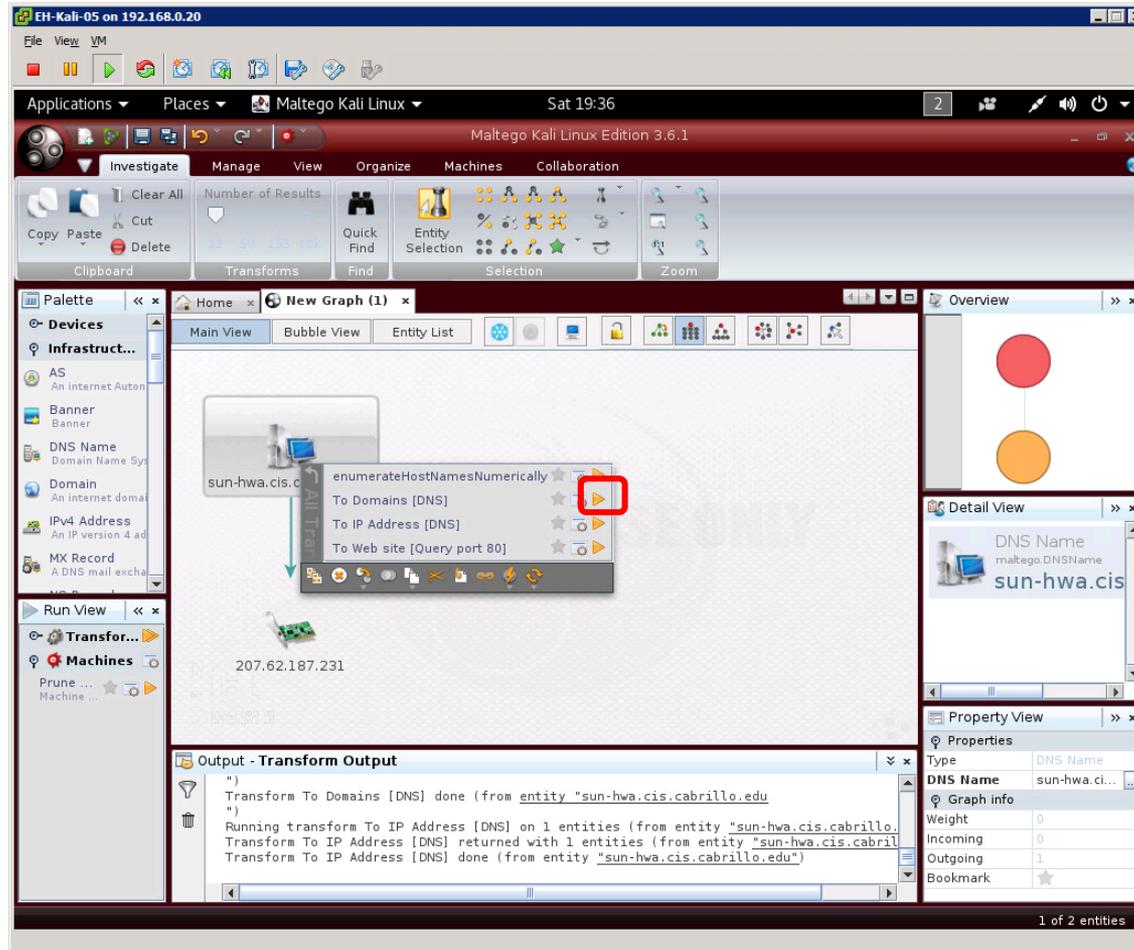
Run the "To IP Address [DNS]" transform to get the IP address.

Maltego



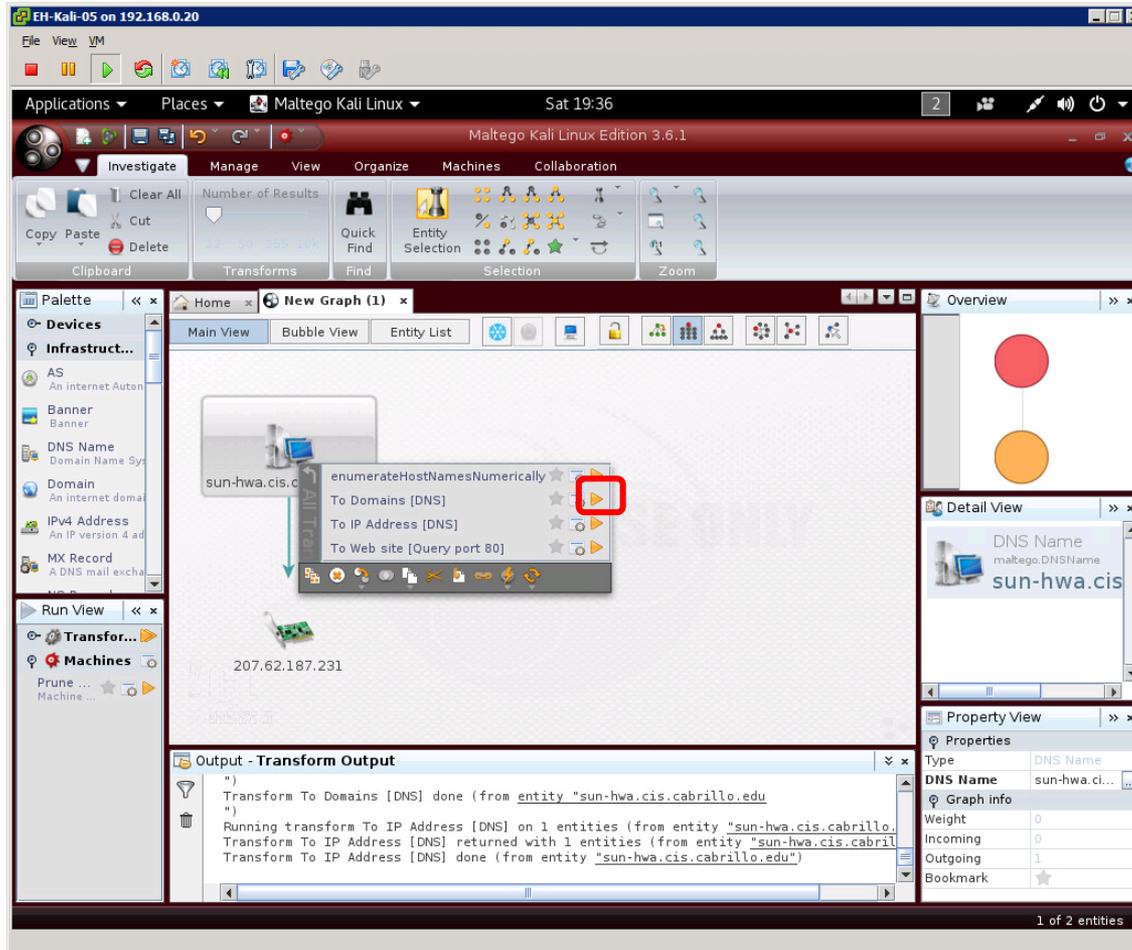
The IP address shows now below the little NIC icon.

Maltego



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

Maltego



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

Maltego

The screenshot displays the Maltego Kali Linux Edition 3.6.1 interface. The main window shows a graph with the following entities and relationships:

- Entity: `sun-hwa.cis.cabrillo.edu` (Computer icon)
- Entity: `207.62.187.231` (IP Address icon)
- Entity: `cis.cabrillo.edu` (Domain icon)
- Entity: `cabrillo.edu` (Domain icon)

Relationships are shown as arrows:

- From `sun-hwa.cis.cabrillo.edu` to `207.62.187.231` (orange arrow)
- From `sun-hwa.cis.cabrillo.edu` to `cis.cabrillo.edu` (blue arrow)
- From `207.62.187.231` to `cabrillo.edu` (green arrow)

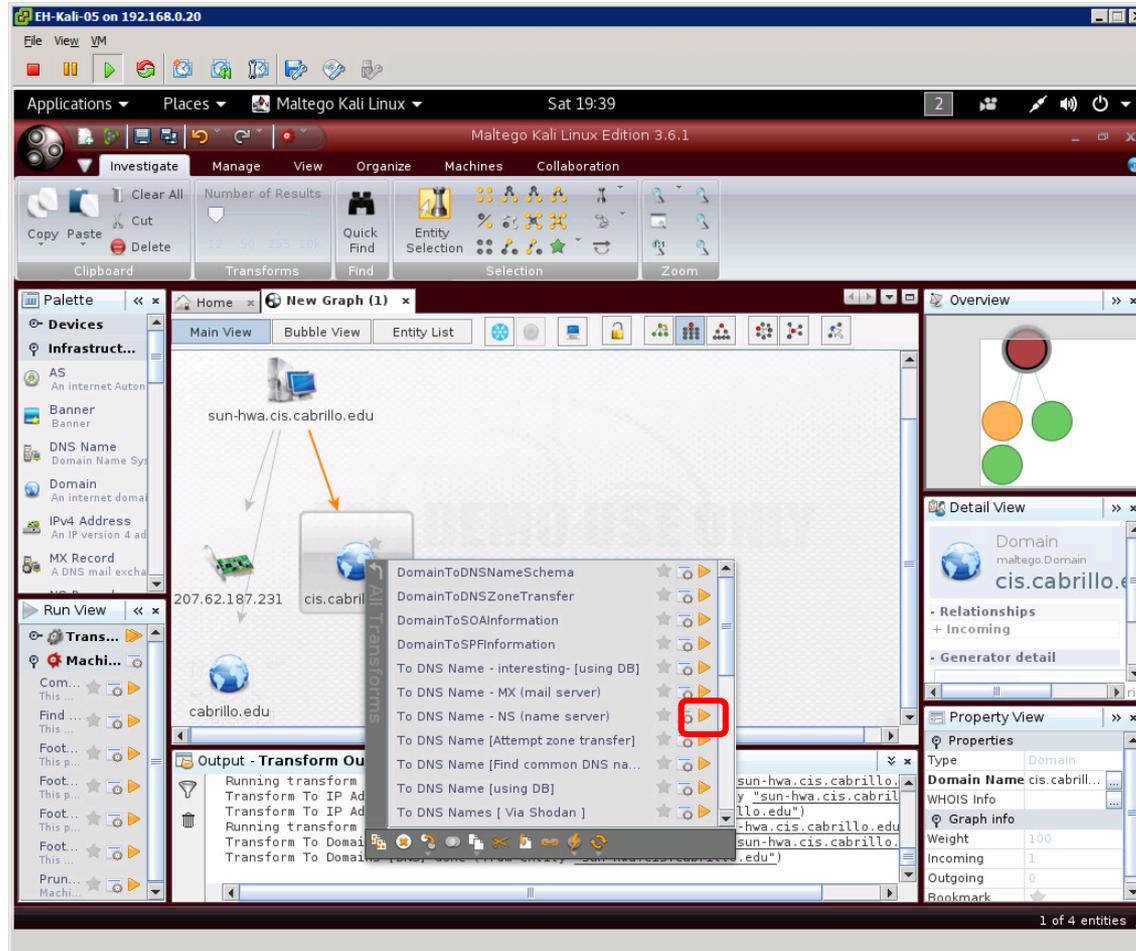
The interface includes a left sidebar with a 'Run View' and 'Transform...' sections. The 'Output - Transform Output' window at the bottom shows the following text:

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

The right sidebar shows an 'Overview' window with a graph icon, a 'Detail View' window showing the 'DNS Name' property of `sun-hwa.cis.cabrillo.edu`, and a 'Property View' window showing the 'DNS Name' property.

Notice both the domain and sub-domain appear.

Maltego



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

Maltego

The screenshot displays the Maltego interface within a Kali Linux virtual machine. The main window shows a graph with the following entities and relationships:

- cabrillo.edu** (Domain) is connected to **cis.cabrillo.edu** (Domain) via an orange arrow.
- cis.cabrillo.edu** is connected to **ns2.cis.cabrillo.edu** (Name Server) and **ns1.cis.cabrillo.edu** (Name Server) via blue arrows.

The left sidebar contains a 'Palette' with various entity types like 'AS', 'Banner', 'DNS Name', 'Domain', 'IPv4 Address', and 'MX Record'. The bottom panel shows the 'Output - Transform Output' window with the following text:

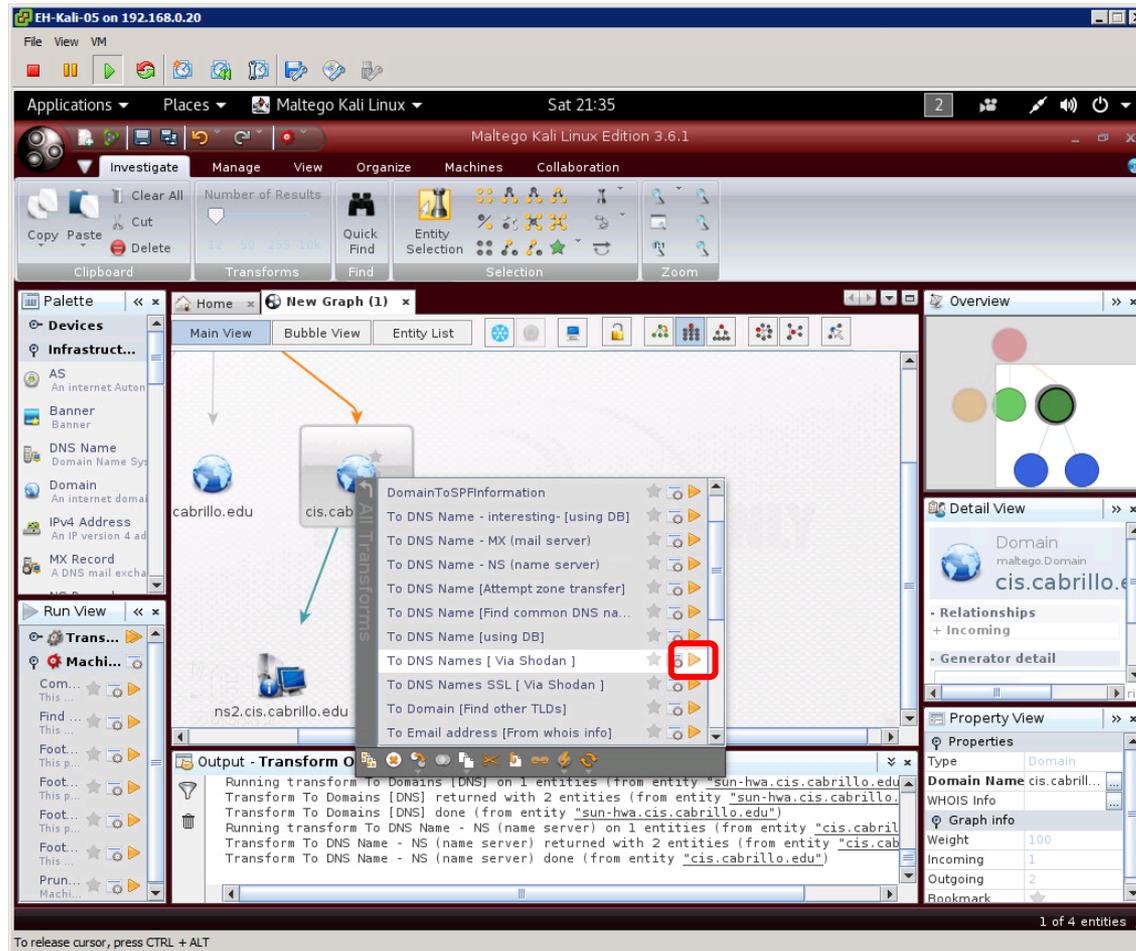
```
Running transform To Domains [DNS] on 1 entities (from entity "sun-hwa.cis.cabrillo.edu")
Transform To Domains [DNS] returned with 2 entities (from entity "sun-hwa.cis.cabrillo.edu")
Transform To Domains [DNS] done (from entity "sun-hwa.cis.cabrillo.edu")
Running transform To DNS Name - NS (name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

The right sidebar shows the 'Overview' and 'Detail View' panels. The 'Detail View' for 'Domain cis.cabrillo.edu' includes sections for 'Relationships' and 'Generator detail'. The 'Property View' shows the following 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



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

Maltego

The screenshot displays the Maltego interface with a graph of entities for the domain cis.cabrillo.edu. The graph shows a hierarchy of entities, including ns2.cis.cabrillo.edu, ns1.cis.cabrillo.edu, oslab.cis.cabrillo.edu, ds1.cis.cabrillo.edu, ns1.cis.cabrillo.edu, vcenter-6-0.cis.cabrillo.edu, vcenter.cis.cabrillo.edu, eq.cis.cabrillo.edu, valiente.cis.cabrillo.edu, cislab.cis.cabrillo.edu, pengo2.cis.cabrillo.edu, and torc0.cis.cabrillo.edu. The interface also shows a 'Run View' panel on the left, an 'Output - Transform Output' panel at the bottom, and a 'Detail View' panel on the right.

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")
    
```

Detail View

Domain
maltego.Domain
cis.cabrillo.edu

- Relationships
 - + Incoming
 - + Outgoing
- Generator detail

Property View

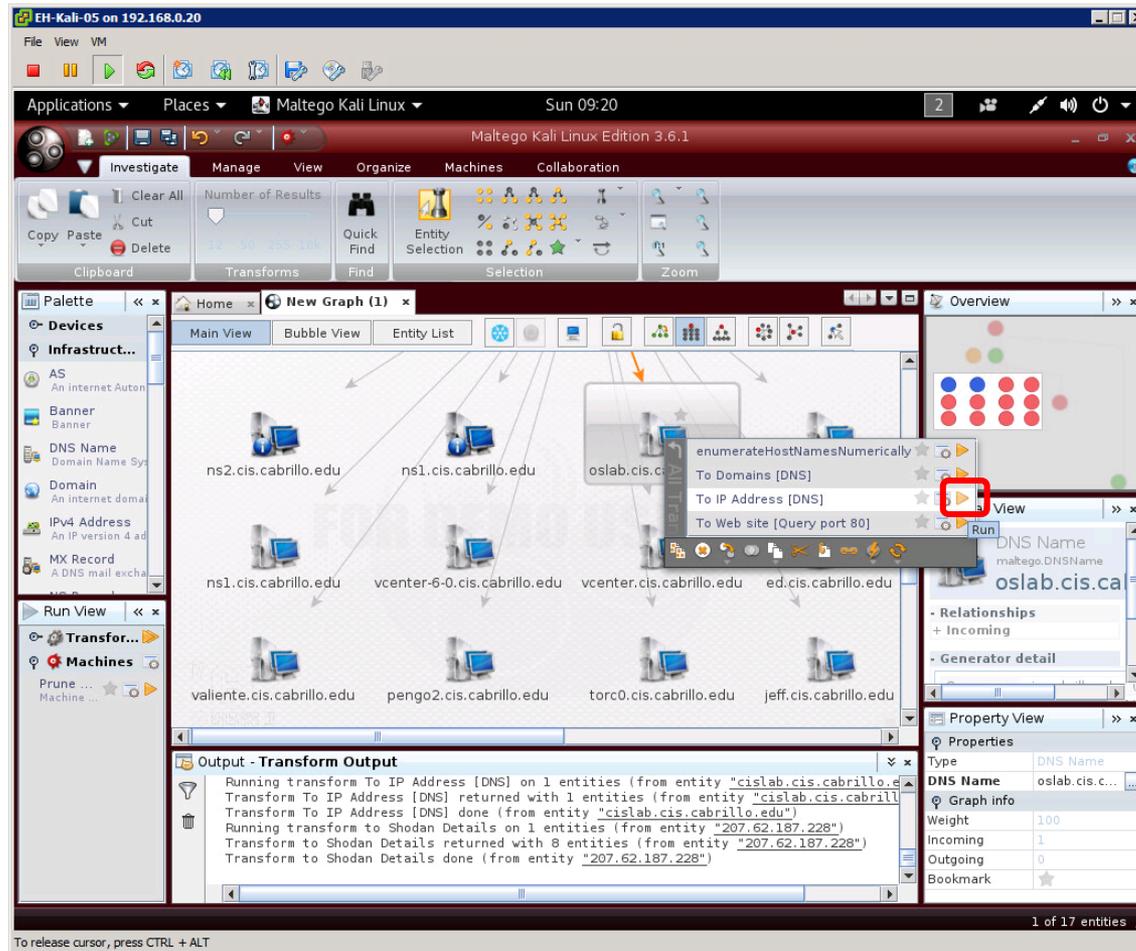
Properties

Type	Domain
Domain Name	cis.cabrill...
WHOIS Info	
Graph info	
Weight	100
Incoming	1
Outgoing	14
Bookmark	

1 of 4 entities

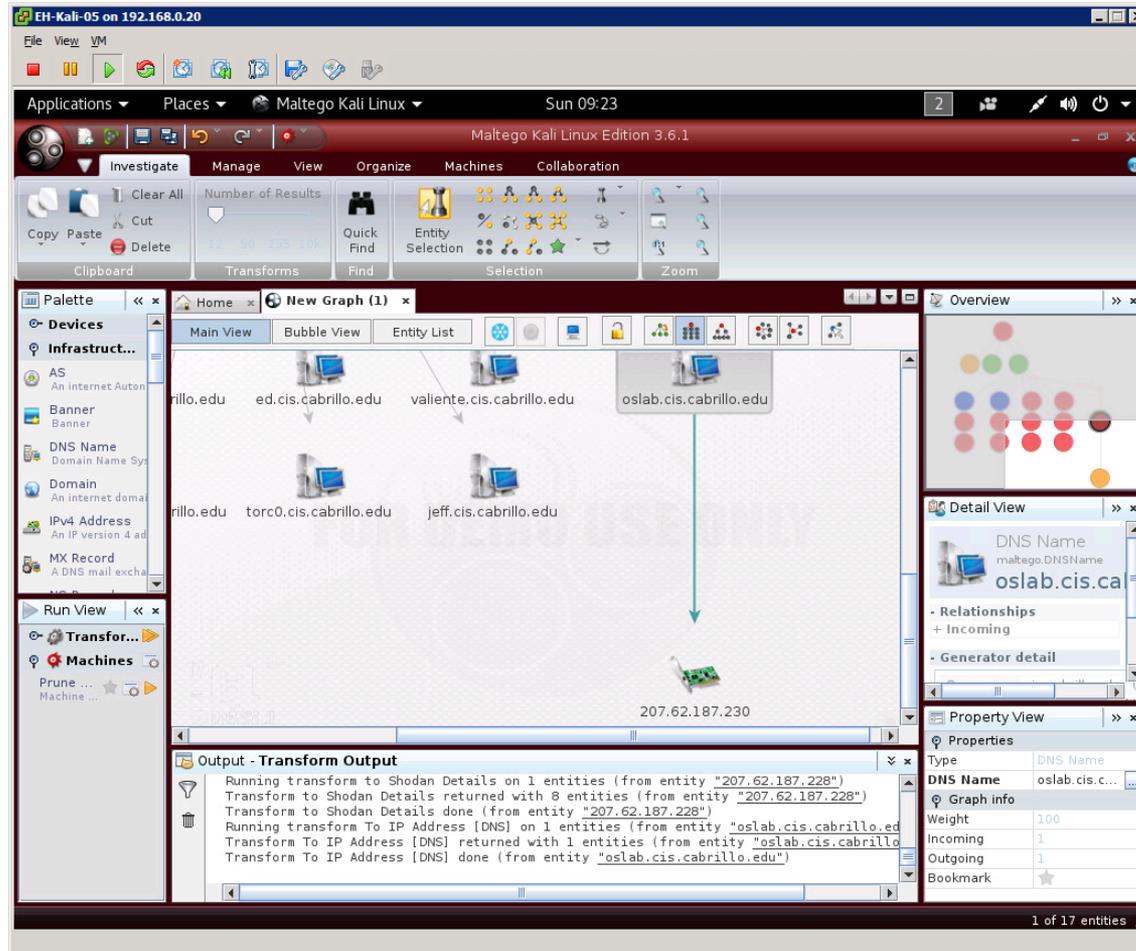
Notice we get 12 (the limit of the free version) hosts on the sub-domain.

Maltego



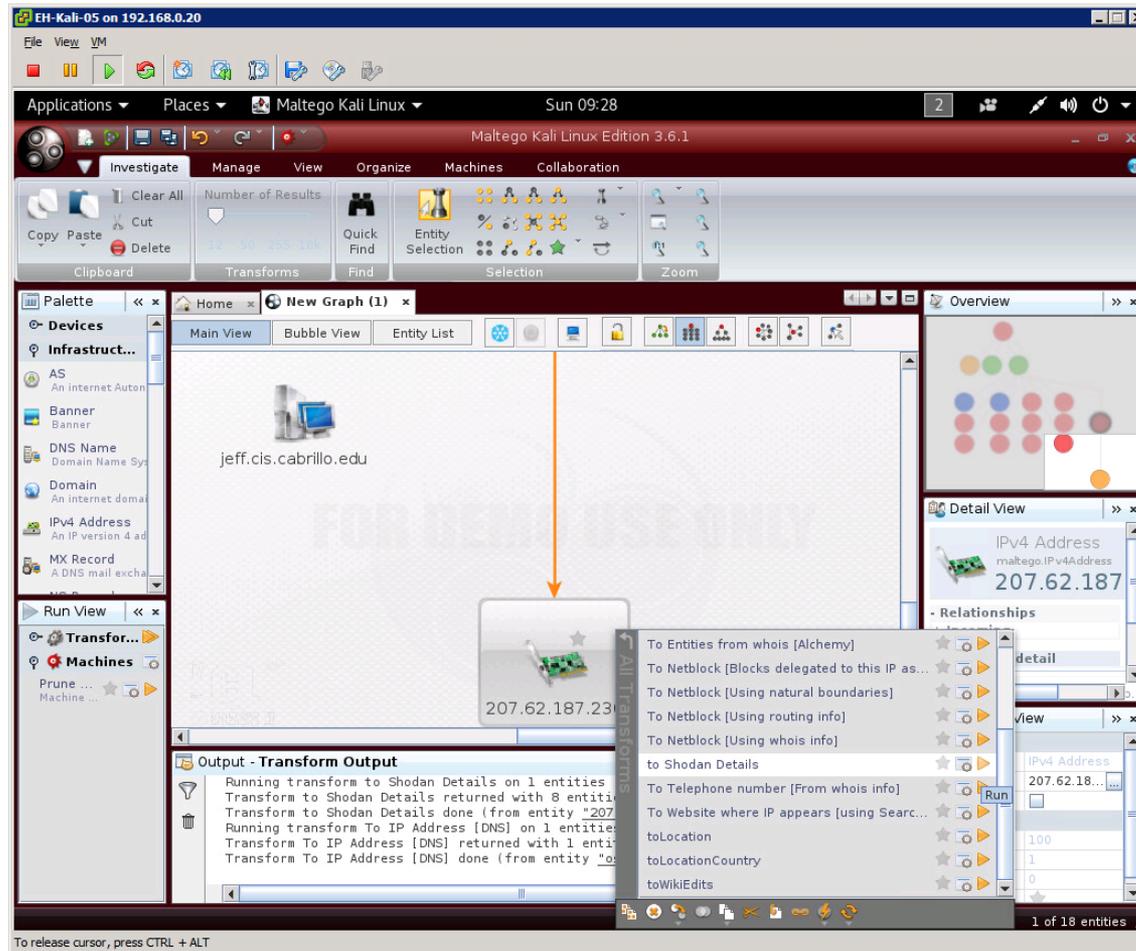
Select oslab and run the "To IP Address [DNS]" to get the IP address.

Maltego



Notice we have the external IP address now.

Maltego



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

Maltego

The screenshot displays the Maltego Kali Linux Edition 3.6.1 interface. The main window shows a graph with a central entity '207.62.187.230' connected to several other entities: '25:Sendmail', 'California State University, Office of the Chancel', 'Cabrillo Community College', 'Aptos, United States', '37.0082, -121.8777', and 'AS2152'. The interface includes a Palette on the left with categories like Devices, Infrastruct..., AS, Banner, DNS Name, Domain, IPv4 Address, and MX Record. Below the Palette is the Run View section with Transform... and Machines. The bottom of the window shows the Output - Transform Output section with the following text:

```

Running transform To IP Address [DNS] on 1 entities (from entity "oslab.cis.cabrillo.edu")
Transform To IP Address [DNS] returned with 1 entities (from entity "oslab.cis.cabrillo.edu")
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")
    
```

The Property View on the right shows the following information for the selected entity:

```

Properties
Type: GPS Coordin...
GPS Coordina: 37.0082, -121.8777
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.

Job Openings

Job title: IT Administrator

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

Some skills we consider critical to being an IT Administrator:

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

<http://www.indeed.com/>

*Job openings can
reveal internal IT
infrastructure*

Job title: System Administrator

Typical Qualifications:

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

Thorough knowledge of:

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

Job openings can reveal internal IT infrastructure

<http://www.indeed.com/>

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

Highly Desired:

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

Activity

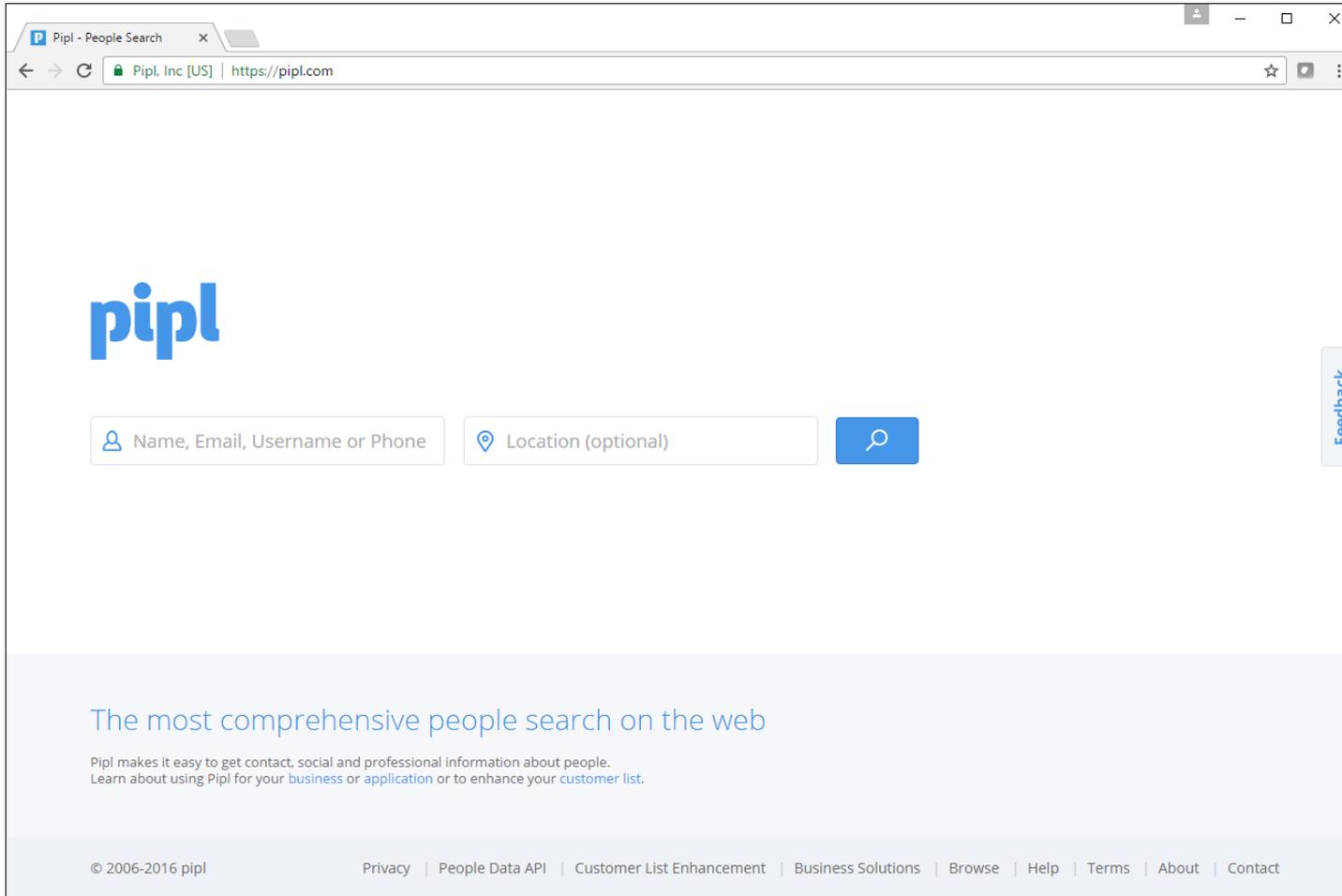
Browse the *System Administrator* job listings on monster.com or indeed.com.

Did you find any specific system or network information?

If so put what you found in the chat window

pipl

pipl



*Lookup
information
on people*

<https://pipl.com/>

Activity

Try using pipi:

<https://pipi.com/>

on yourself.

Try it on your:

- name
- phone number
- email address
- username

Any observations?

Write any observations in the chat window

IntelTechniques

IntelTechniques

OSINT Training by Micha x

Secure | <https://inteltechniques.com/experience.html>

Apps Yahoo Cabrillo College Health Network Medical CIS 76 links Lab Development Home Music Expand All Other bookmarks

INTELTECHNIQUES.com

Online Training Live Training Consultation Tools Forum Blog Podcast

Michael Bazzell

Michael Bazzell spent 18 years as a government computer crime investigator. During the majority of that time, he was assigned to the FBI's Cyber Crimes Task Force where he focused on computer crime investigations. As an active investigator, he has been involved in numerous major criminal investigations including online child solicitation, child abduction, kidnapping, cold-case homicide, terrorist threats, and computer intrusions. He has trained thousands of individuals in the use of his investigative techniques. He also served as the technical advisor for the television hacker drama "Mr. Robot". His books "**Open Source Intelligence Techniques**" and "**Hiding from the Internet**" have been best sellers in both the United States and Europe. Michael currently works and resides in Washington, D.C., and also serves as an advisor for the privacy app Sudo.

IntelTechniques

The screenshot shows a web browser window displaying the IntelTechniques website. The browser's address bar shows the URL <https://inteltechniques.com/menu.html>. The website header features the title "INTELTECHNIQUES SEARCH TOOL" and the name "MICHAEL BAZZELL OSINT TRAINER & PRIVACY CONSULTANT" next to a man in a suit. A navigation menu includes "Online Training", "Live Training", "Consultation", "Tools" (highlighted with a red box), "Forum", "Blog", "Podcast", "Books", "Bio", and "Contact". On the left sidebar, "OSINT LINKS" is also highlighted with a red box. Below this, a list of search engines is provided, including "IntelTechniques Custom Search Tools", "Search Engines", "Facebook", "Twitter", "Periscope", "Social Networks & Forums", "Photographs", "Videos", "Documents", "User Names", "Email Addresses", "People Search Engines", and "Businesses & Professionals". On the right, there is a section titled "OSINT Search Guide" with a promotional text: "The Fifth Edition of my book on internet search techniques is now available. Click the book below for details." Below the text is an image of the book cover for "OPEN SOURCE INTELLIGENCE TECHNIQUES: RESOURCES FOR SEARCHING AND ANALYZING ONLINE INFORMATION, FIFTH EDITION" by Michael Bazzell.

<https://inteltechniques.com/>

Lots and lots and lots of open source tools!

IntelTechniques

The screenshot shows the IntelTechniques website interface. At the top, the title "INTELTECHNIQUES SEARCH TOOL" is displayed in large white letters on a dark background. To the right, a man in a suit is shown, and the text "MICHAEL BAZZELL OSINT TRAINER & PRIVACY CONSULTANT" is visible. Below the header is a navigation menu with items: Online Training, Live Training, Consultation, **Tools** (highlighted with a red box), Forum, Blog, Podcast, Books, Bio, and Contact. On the left side, there is a sidebar menu with categories: OSINT LINKS, SEARCH ENGINES, FACEBOOK, TWITTER, INSTAGRAM, USER NAME, **REAL NAME** (highlighted with a red box), EMAIL ADDRESS, TELEPHONE NUMBER, DOMAIN NAME, IP ADDRESS, YOUTUBE, REVERSE IMAGE, REVERSE VIDEO, DOCUMENTS, and PASTEBINS. The main content area is titled "Custom Person Search Tools" and contains a table of search tools. Each tool has input fields for "First Name" and "Last Name", and a "Populate All" button. The tools listed are: Pipl, ThatsThem, Spokeo, Reverse Genie, Advanced Check, Yasni, Radaris, ZabaSearch, Intelius, OneRep, FamilyTreeNow, TruePeople, Quanki, PeekYou, WebMii, LinkedIn, and Twitter. At the bottom of the table, there are additional input fields for "First Name" and "Last Name" and a "Submit All" button.

First Name	Last Name	Populate All
First Name	Last Name	Pipl
First Name	Last Name	ThatsThem
First Name	Last Name	Spokeo
First Name	Last Name	Reverse Genie
First Name	Last Name	Advanced Check
First Name	Last Name	Yasni
First Name	Last Name	Radaris
First Name	Last Name	ZabaSearch
First Name	Last Name	Intelius
First Name	Last Name	OneRep
First Name	Last Name	FamilyTreeNow
First Name	Last Name	TruePeople
First Name	Last Name	Quanki
First Name	Last Name	PeekYou
First Name	Last Name	WebMii
First Name	Last Name	LinkedIn
First Name	Last Name	Twitter
First Name	Last Name	Submit All

<https://inteltechniques.com/>

*Lots and lots and lots of
open source tools!*

Activity

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

Select:

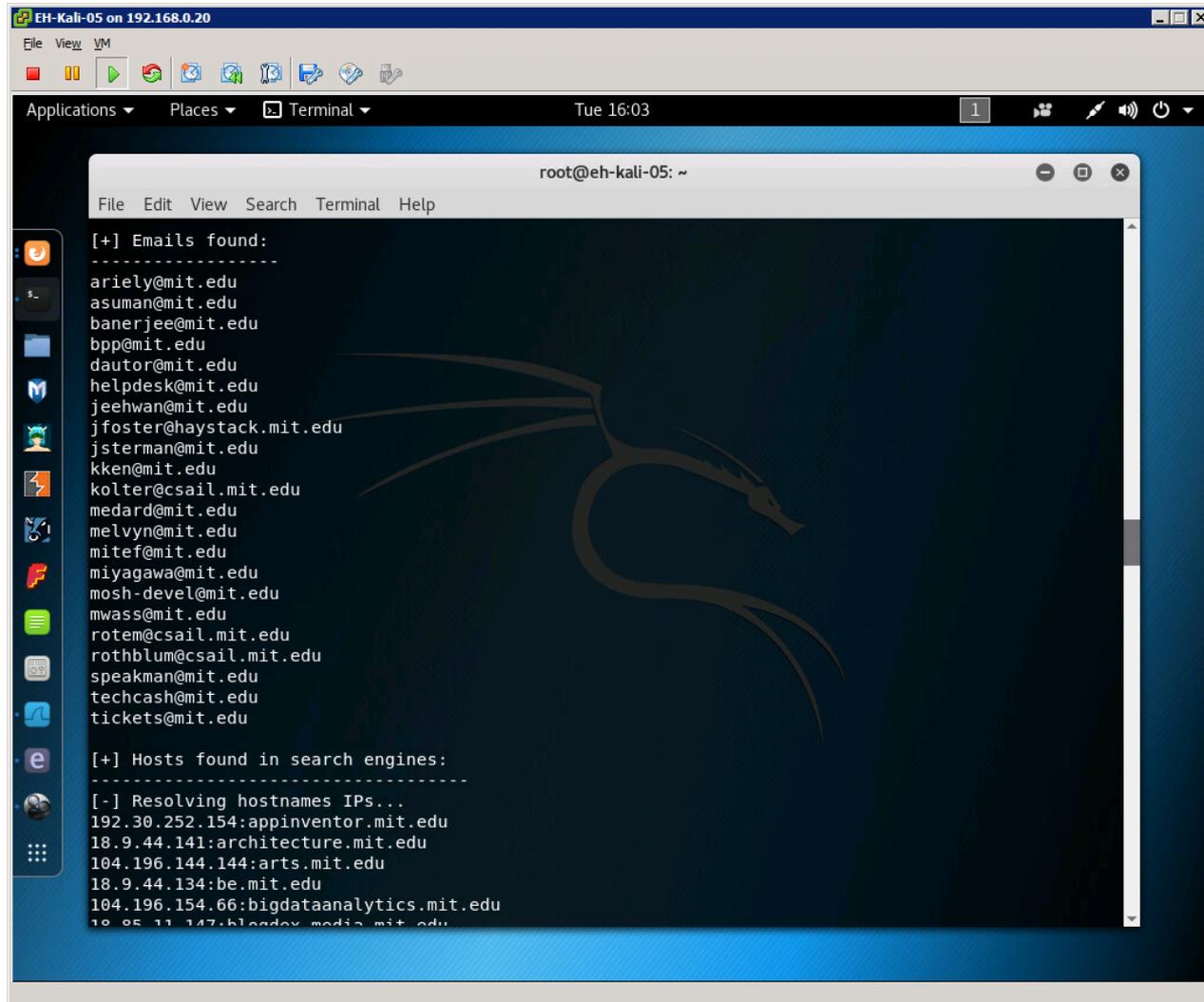
- OSINT LINKS (on left panel)
- Then select: Photographs (in middle pane)
- Then scroll down and select: Foto Forensics

Upload this photograph:

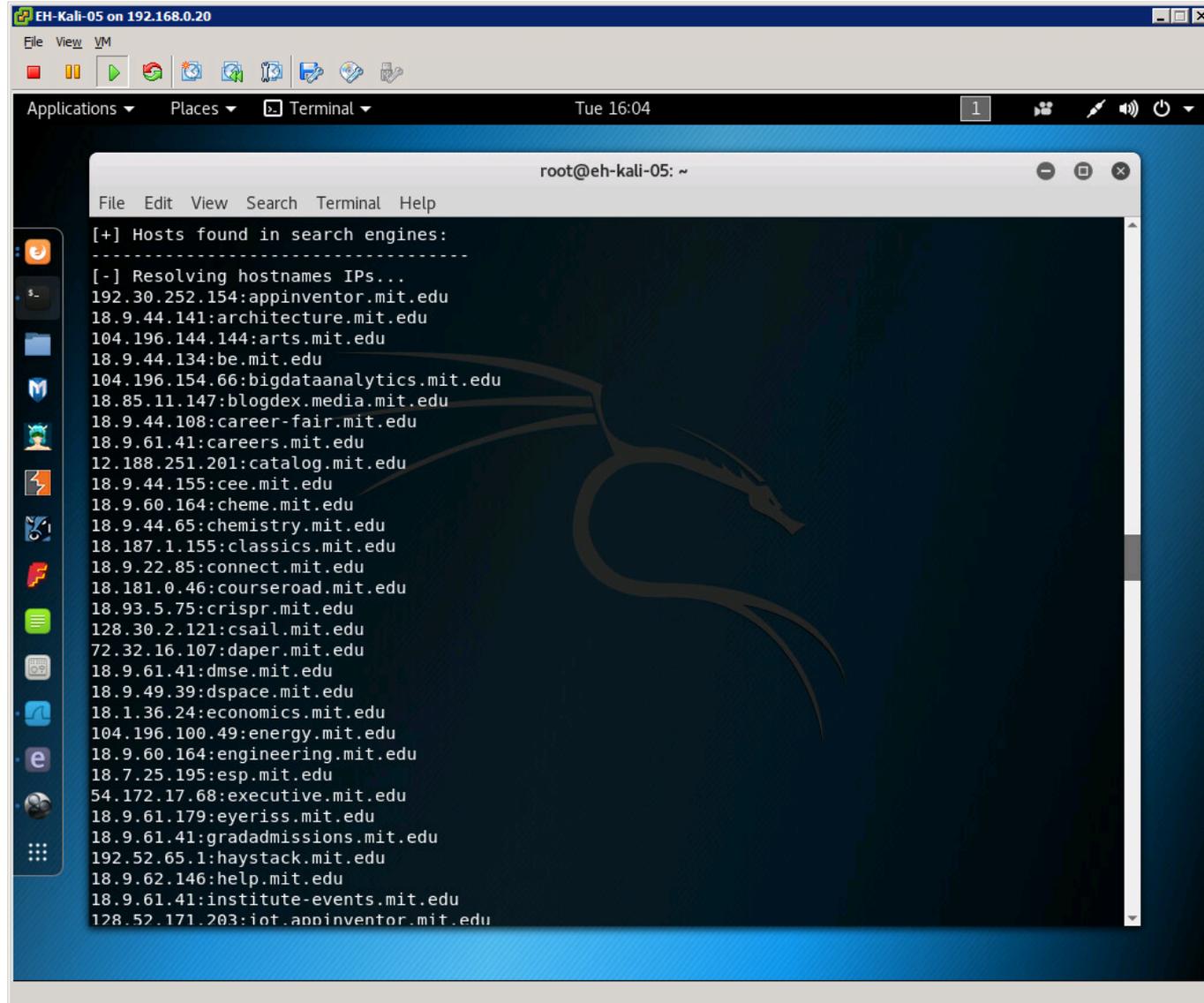
<https://simms-teach.com/docs/cis76/pic02.jpg>

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

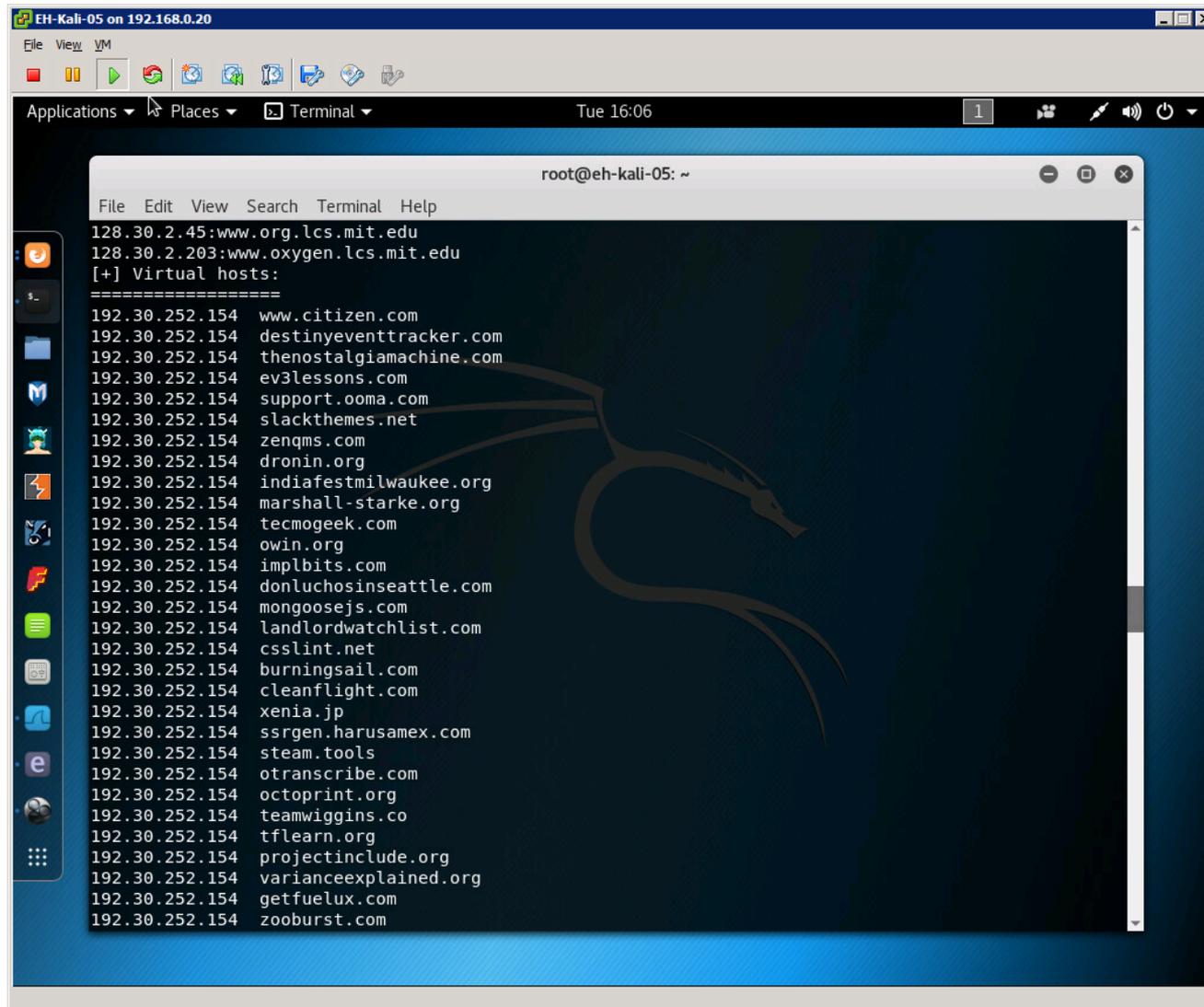
Harvester



emails found



hosts found in search engines



The image shows a terminal window on a Kali Linux system. The terminal title is "root@eh-kali-05: ~". The terminal output displays a list of virtual hosts, each with an IP address and a domain name. The list starts with "128.30.2.45:www.org.lcs.mit.edu" and "128.30.2.203:www.oxygen.lcs.mit.edu", followed by a section for "Virtual hosts:" which lists 25 additional domains, all mapped to the IP address "192.30.252.154".

```
root@eh-kali-05: ~  
File Edit View Search Terminal Help  
128.30.2.45:www.org.lcs.mit.edu  
128.30.2.203:www.oxygen.lcs.mit.edu  
[+] Virtual hosts:  
=====  
192.30.252.154 www.citizen.com  
192.30.252.154 destinyeventtracker.com  
192.30.252.154 thenostalgiamachine.com  
192.30.252.154 ev3lessons.com  
192.30.252.154 support.ooma.com  
192.30.252.154 slackthemes.net  
192.30.252.154 zenqms.com  
192.30.252.154 dronin.org  
192.30.252.154 indiafestmilwaukee.org  
192.30.252.154 marshall-starke.org  
192.30.252.154 tecmogeek.com  
192.30.252.154 owin.org  
192.30.252.154 implbits.com  
192.30.252.154 donluchosinseattle.com  
192.30.252.154 mongoosejs.com  
192.30.252.154 landlordwatchlist.com  
192.30.252.154 csslint.net  
192.30.252.154 burningsail.com  
192.30.252.154 cleanflight.com  
192.30.252.154 xenia.jp  
192.30.252.154 sssrgen.harusamex.com  
192.30.252.154 steam.tools  
192.30.252.154 otranscribe.com  
192.30.252.154 octoprint.org  
192.30.252.154 teamwiggins.co  
192.30.252.154 tflern.org  
192.30.252.154 projectinclude.org  
192.30.252.154 varianceexplained.org  
192.30.252.154 getfuelux.com  
192.30.252.154 zooburst.com
```

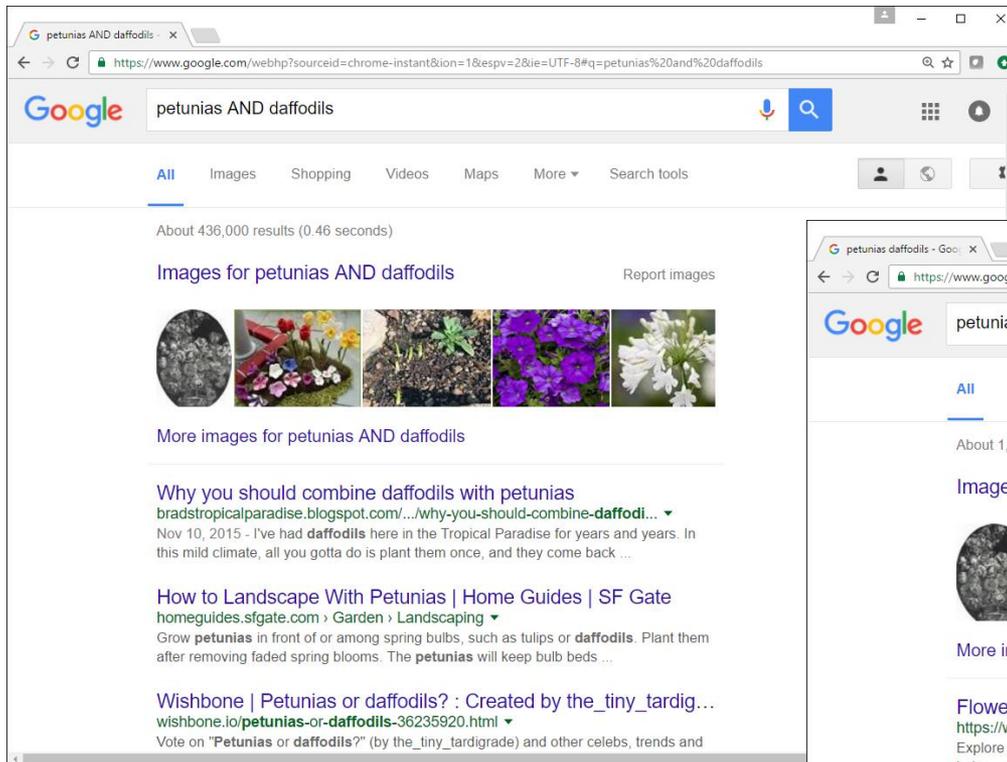
virtual hosts



Google Hacking

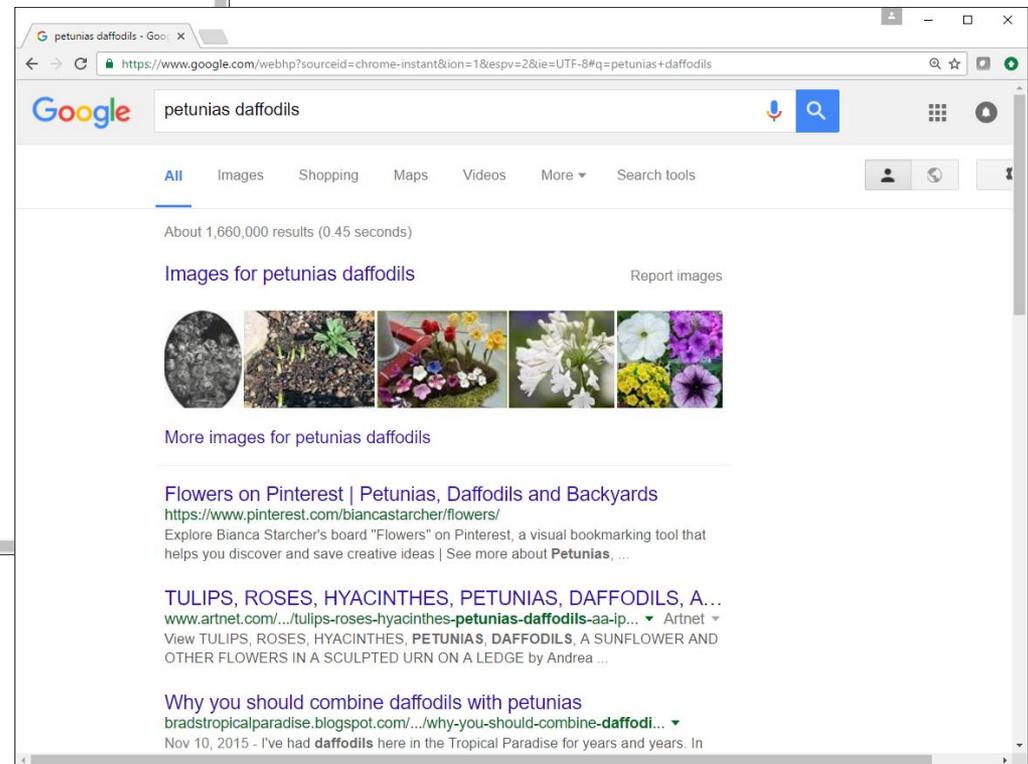
Google Hacking with AND (or space) operator

petunias AND daffodils



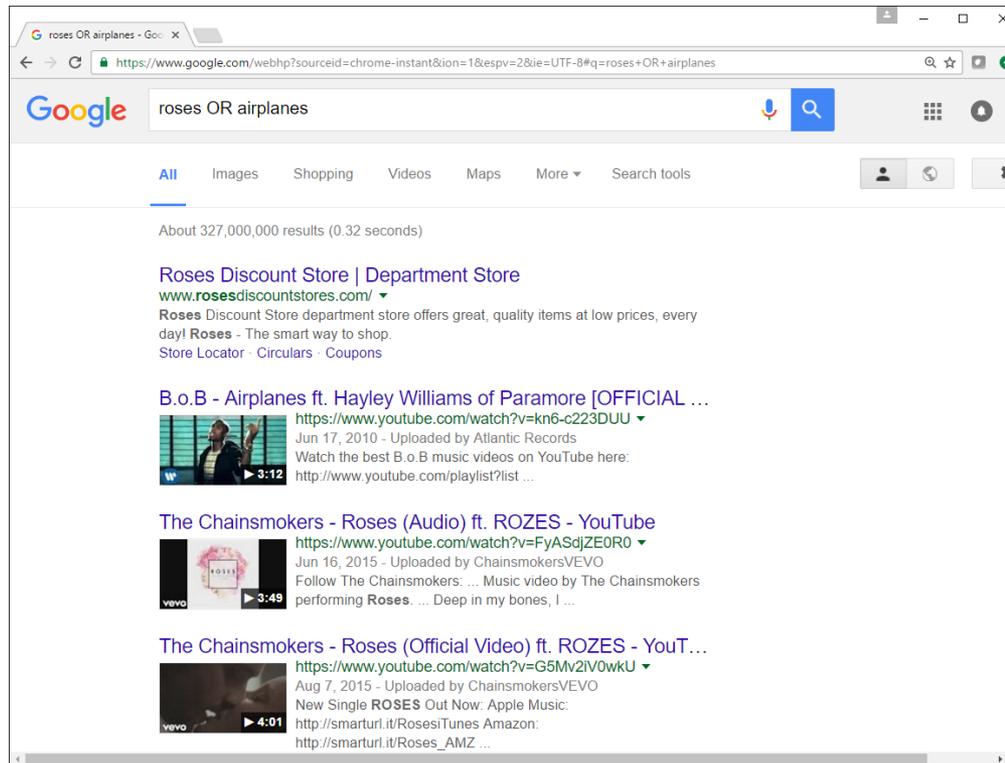
Finds pages containing both petunias and roses.

petunias daffodils



Google Hacking with OR (or |) operator

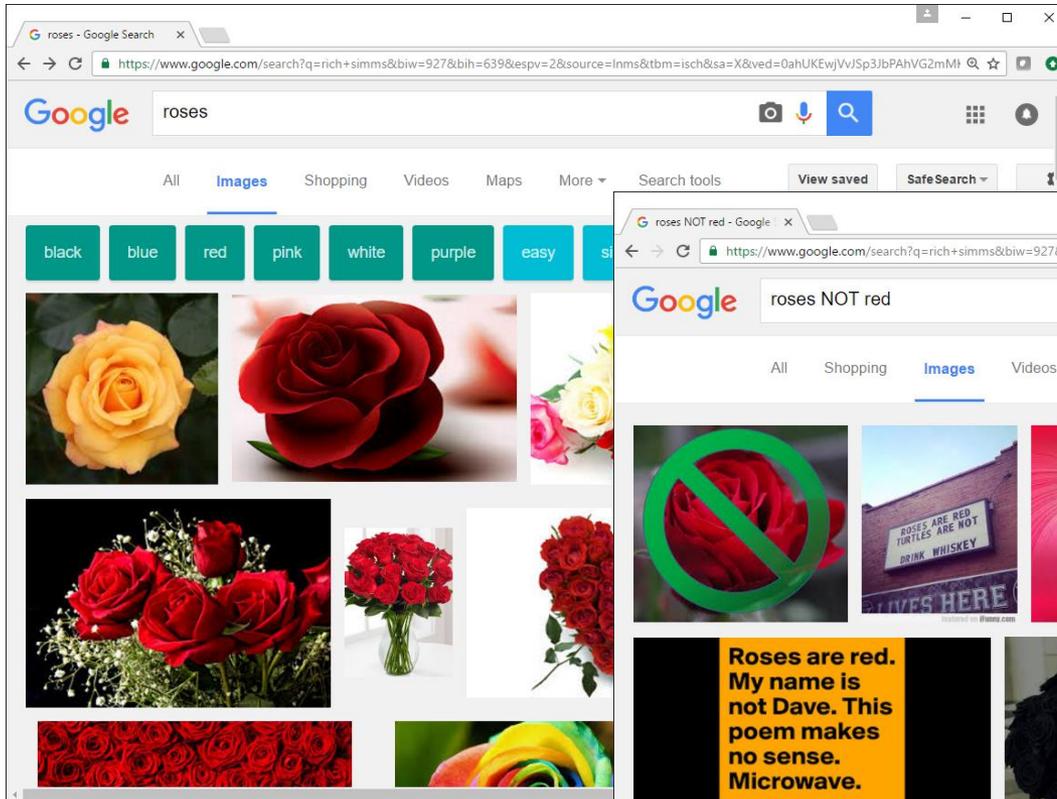
roses OR airplanes



Finds pages with roses or pages with airplanes.

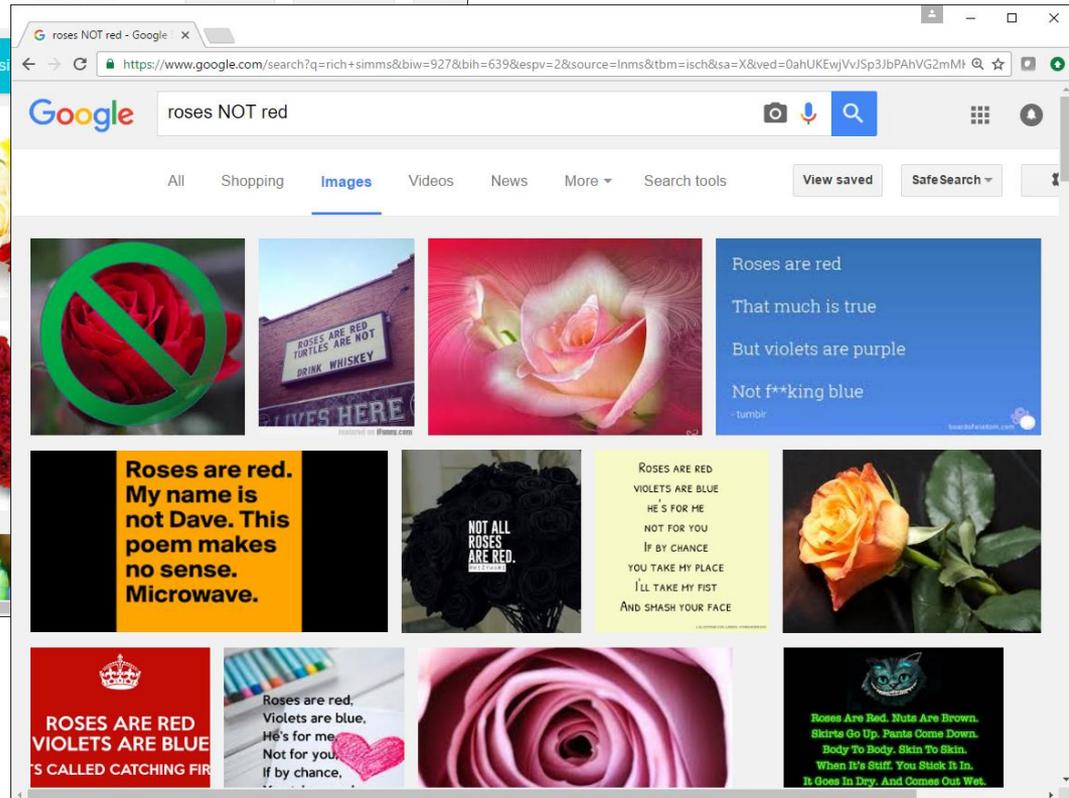
Google Hacking with NOT (or -) operator

roses



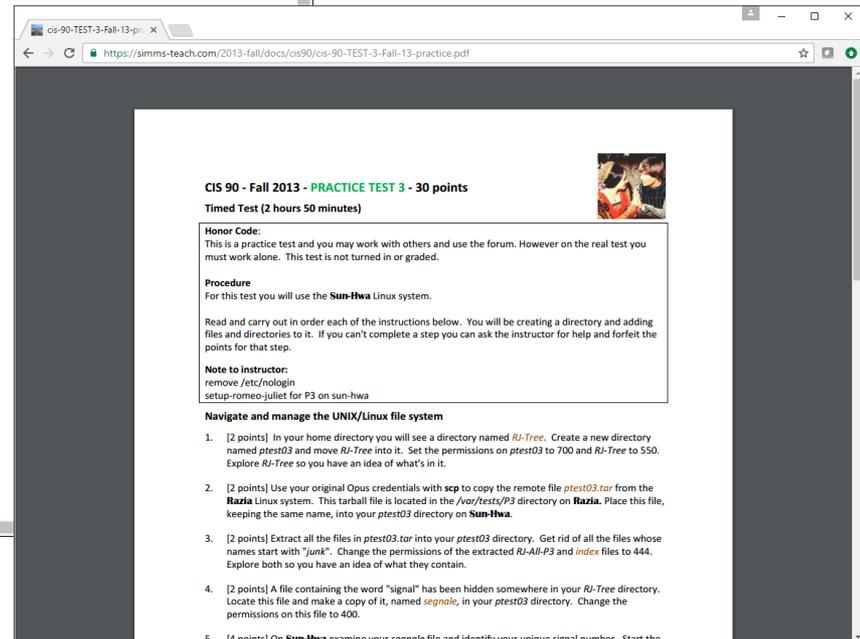
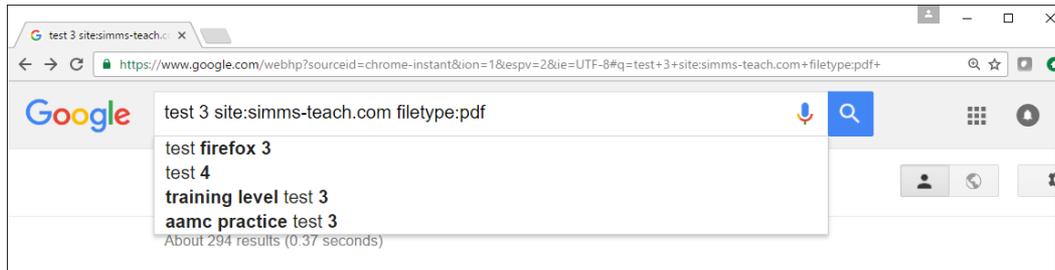
The first finds pages with all kinds of roses, the second weeds out red roses.

roses NOT red



Google Hacking with site: and filetype: operators

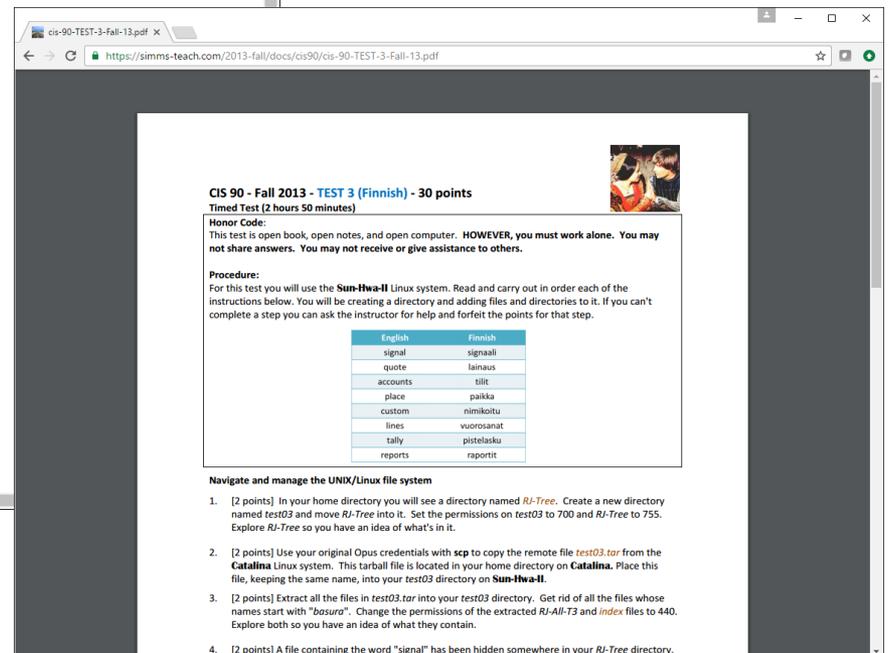
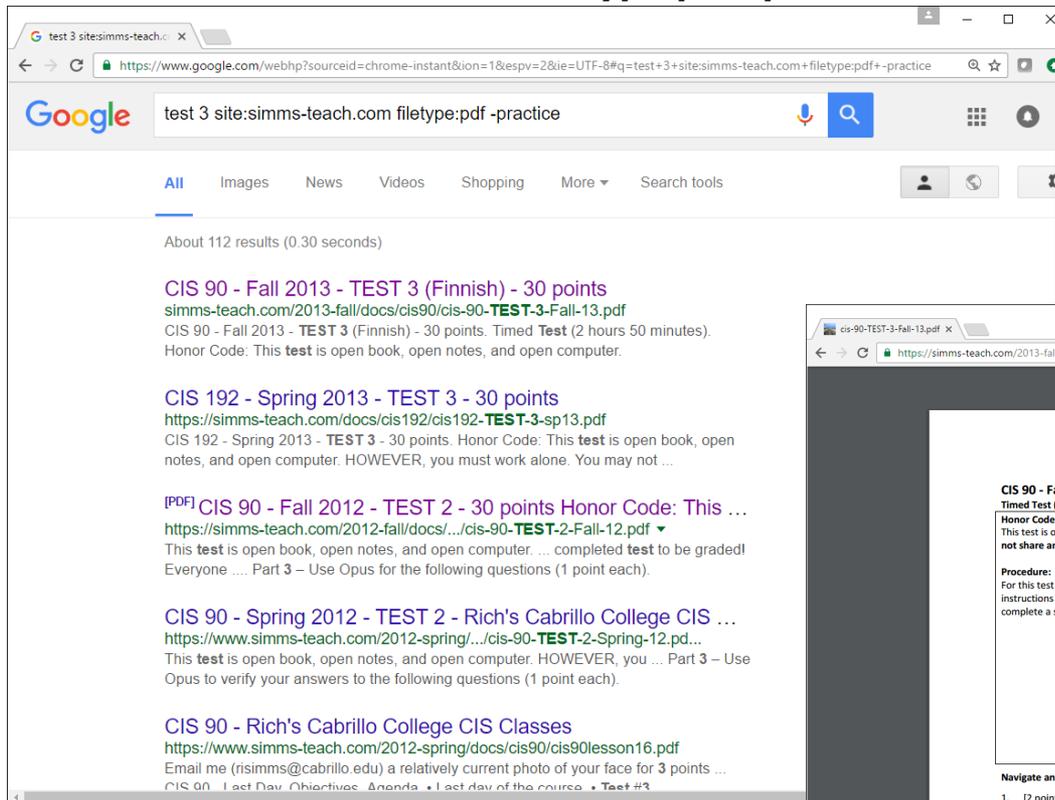
test 3 site:simms-teach.com filetype:pdf



Finds old tests on my website

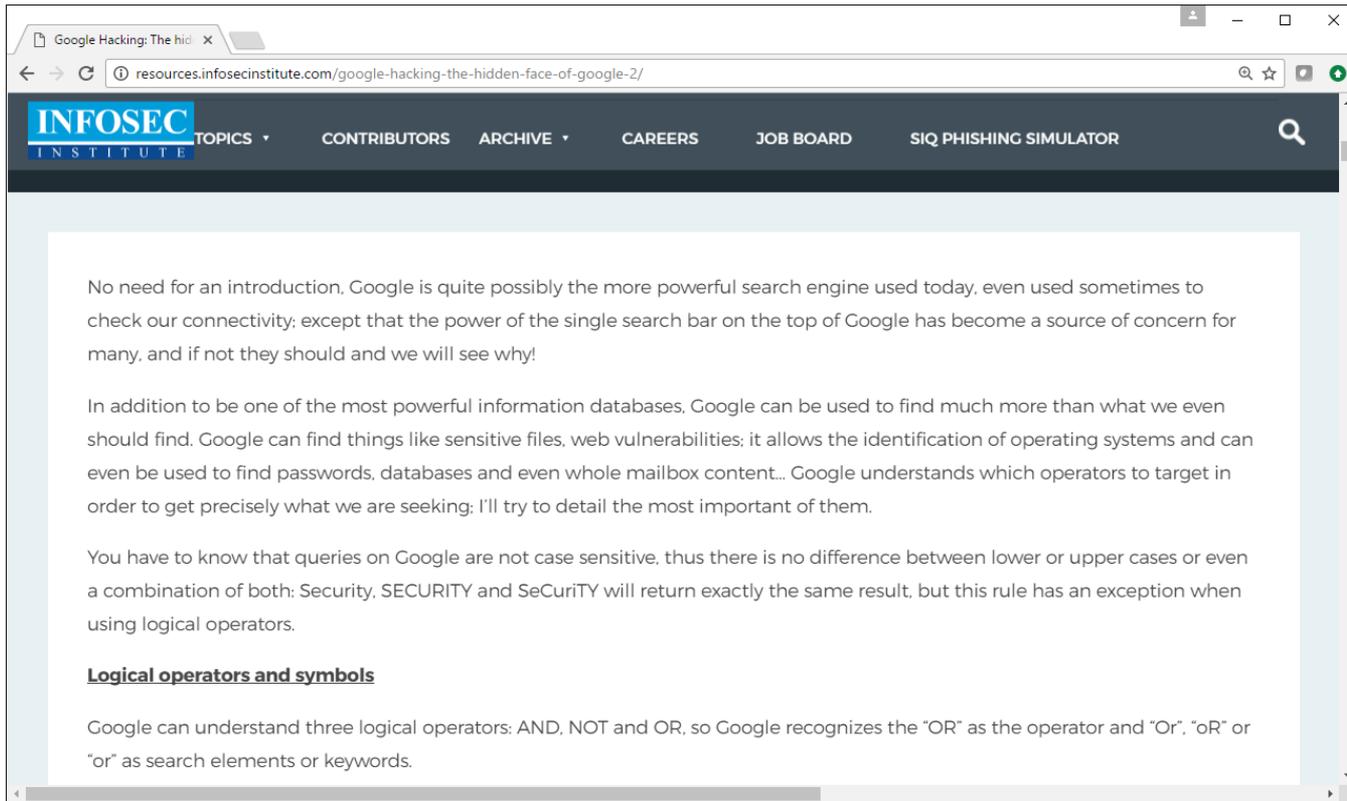
Google Hacking with site: and filetype: operators

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

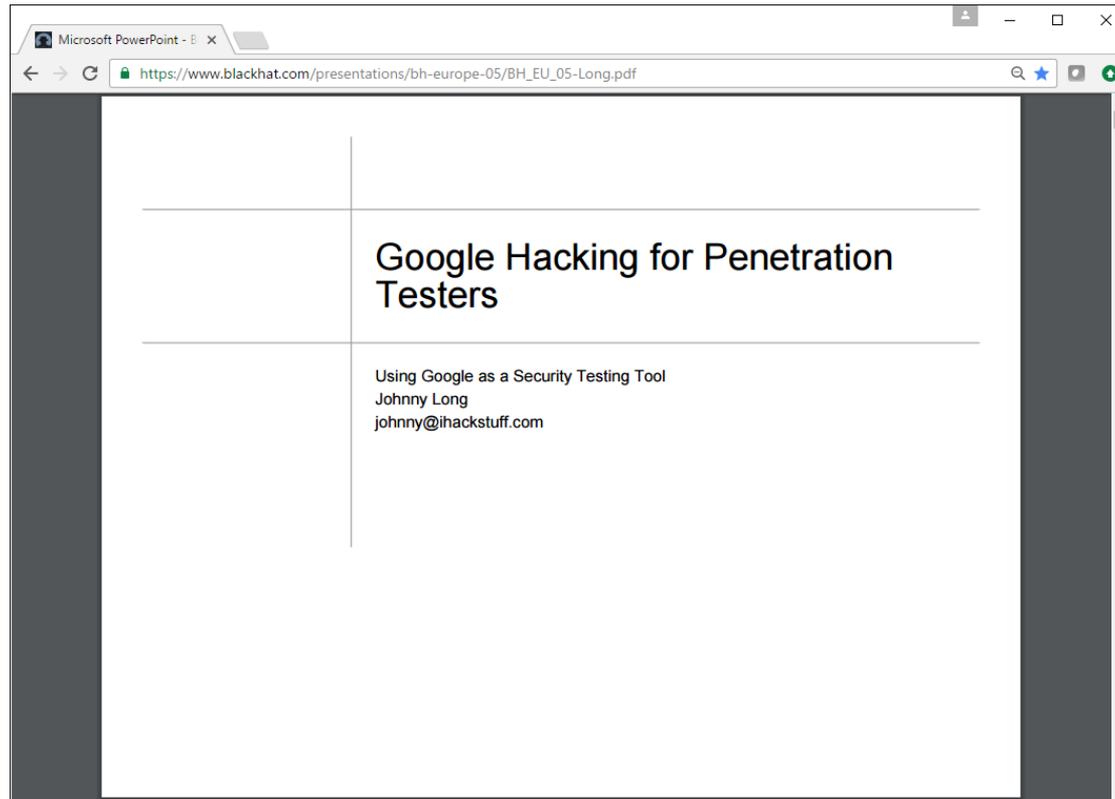


Finds old tests on my website and doesn't include the practice ones

Google Hacking: The hidden face of Google



Google Hacking by Johnny Long



Advanced Operators at a Glance

Advanced operators can be combined in some cases.

In other cases, mixing should be avoided.

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

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

Google Hacking On Exploit Database

The screenshot shows the Exploit Database (GHDB) website. The browser address bar displays <https://www.exploit-db.com/google-hacking-database/>. The website header includes the Exploit Database logo and navigation links: Home, Exploits, Shellcode, Papers, Google Hacking Database, Submit, and Search. The main heading is "Google Hacking Database (GHDB)" with the subtitle "Search the Google Hacking Database or browse GHDB categories". Below this is a search interface with a dropdown menu set to "Any Category", a search input field, and a "SEARCH" button. The search results are displayed in a table with columns for Date, Title, and Category.

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

Google Hacking Database Activity

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

Pick one of the Google Hacking categories such as:

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

Start exploring.

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



Social Engineering

Social Engineering

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

con man

Back formation of "confidence man". One who gains the trust, or "confidence", of his victims (often called **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.
- (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)



<https://www.keelog.com/>

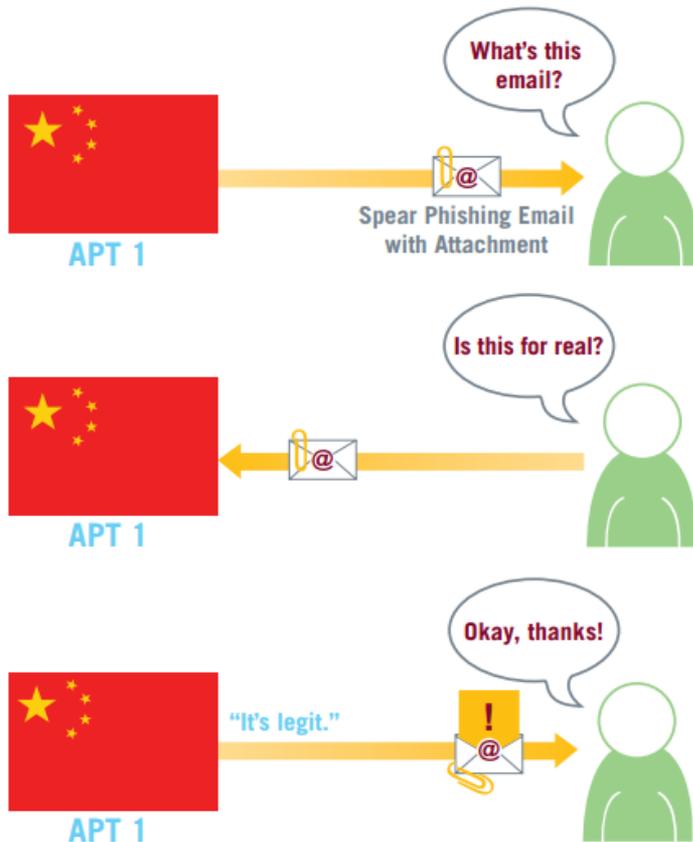
Social Engineering

Mandiant sampling of APT1 malicious zip file attachments:

2012ChinaUSAaviationSymposium.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

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.”

Open-Source Security Testing Methodology Manual

The screenshot shows a web browser window displaying a WordPress blog post. The browser's address bar shows the URL: <https://raynaudc.wordpress.com/2011/12/20/open-source-security-testing-methodology-manual-2/>. The page features a profile picture of Charles Raynaud, a man with short dark hair, wearing a dark jacket over a light-colored shirt. Below the photo, his name 'Charles Raynaud' and the tagline 'Communauté d'idées' are visible. The post title is 'Open Source Security Testing Methodology Manual', and it is dated '20 décembre 2011' with a word count of '2,070 Words'. A rating system shows five stars, with the first four filled and the fifth empty, followed by the text 'Évaluez ceci'. The main content area contains two numbered sections: '1. Open Source Security Testing Methodology Manual' and '2. From Wikipedia, the free encyclopedia'. The text in section 2 describes the OSSTMM as a manual on security testing and analysis created by Pete Herzog and provided by ISECOM. A blue highlight is present under the sentence: '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 sidebar on the left includes a 'Pages' section with links for 'À propos' and 'Les printemps arabes', and a 'Choisissez votre thème' section with various theme options like 'Affaires étrangères', 'crise financière', and 'Obama'. A 'Suivre' button is located at the bottom right of the main content area.

Open-Source Security Testing Methodology Manual

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.

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



Open-Source Security Testing Methodology Manual

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



Social Engineering Target Template

Target Definition

Name	E-mail	Telephone	Description

Open-Source Security Testing Methodology Manual

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



Social Engineering Telephone Attack Template

Attack Scenario	
Telephone #	
Person	
Description	
Results	

Attack Scenario	
Telephone #	
Person	
Description	
Results	

Open-Source Security Testing Methodology Manual

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



Social Engineering E-mail Attack Template

Attack Scenario	
Email	
Person	
Description	
Results	

Attack Scenario	
Email	
Person	
Description	
Results	

Open-Source Security Testing Methodology Manual

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



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	

"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.



3:44 / 51:16



David Kennedy created the Social Engineering Toolkit (SET)

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

Social Engineering Toolkit

Social-Engineer Toolkit - x

TrustedSec, LLC [US] | <https://www.trustedsec.com/social-engineer-toolkit/>

Home Services Downloads Blog About Us Contact Us

Social-Engineer Toolkit Home / 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/
```

RECENT POSTS SEARCH THE SITE COMPANY ADDRESS

David Kennedy created the Social Engineering Toolkit (SET)

Netlab+ Activity

NDG EH Lab 2

Social Engineering Toolkit

Assignment



Rich's Cabrillo College CIS Classes
CIS 76 Calendar

Home Resources Forums CIS Lab Canvas

Login
Flashcards
Admin

CIS 76
CIS 90
Previous Terms

102 days till term ends!

Cabrillo College
Web Advisor
Commands and Files

VLab (classic)
VLab (web)
NETLAB+

CIS 76 VLab Pod Assignments

CIS 90 VLab VM Assignments

RIP Dennis Ritchie

CIS 76 (Fall 2016)
Course Home Grad

Topics covered below

Lesson	Date
1	8/30

Netlab+ link on left panel

BACCC BAY AREA
COMMUNITY COLLEGE CONSORTIUM

NETLAB+

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 browser's trusted site list. This application uses **Java™**, JavaScript, Cookies, Popup Windows, and IFRAMES. Please adjust your browser settings accordingly.

POWERED BY
NDG
NETLAB+®

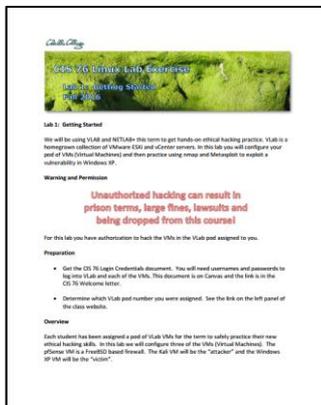
System Web Browser Version Status

Username: simben76
Password: [masked]
Login
Forgot Password?

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.



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