Rich's lesson module checklist

Last updated 9/4/2017

- □ 24 hours before first class
  - □ Login credentials document updated and secured
  - □ Send out welcome email
  - □ Publish updated Canvas course with links and announcement
  - □ Forum created with welcome post

- □ Opus accounts made (with TBDs for walk-ins) and populated
- □ Netlab+ PE and NetLab+ VE accounts created
- □ VLab accounts created

- □ CIS 76 VLAB Pods and VMs created
- □ Pod assignments published
- □ Lab 1, Pod Setup Guide, CVE-2008-4250 exploit tested and published
- □ Survey posted

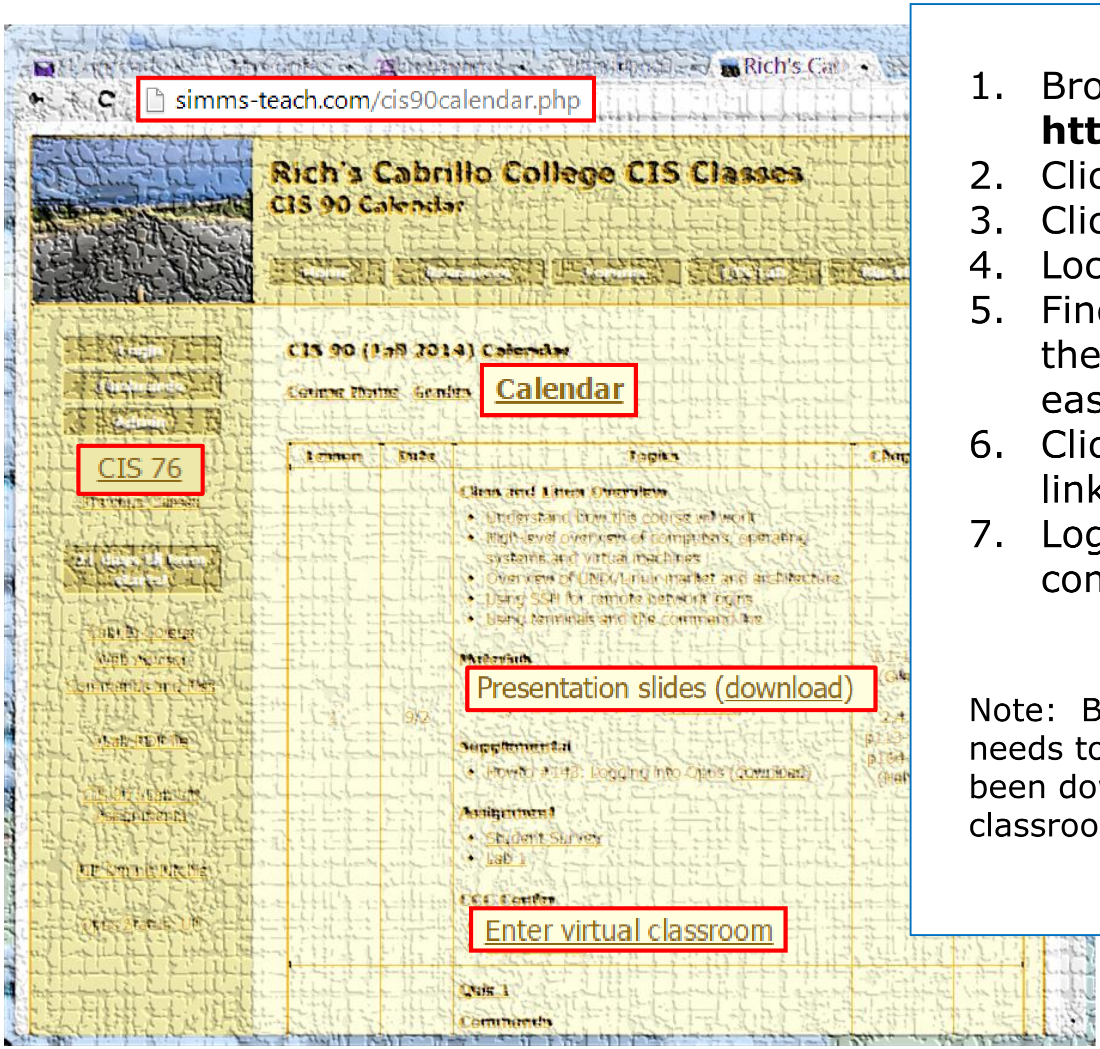
- □ Rosters printed
- □ Add codes printed
- □ Email heads-up to CCC Confer on incoming recordings

- □ 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

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

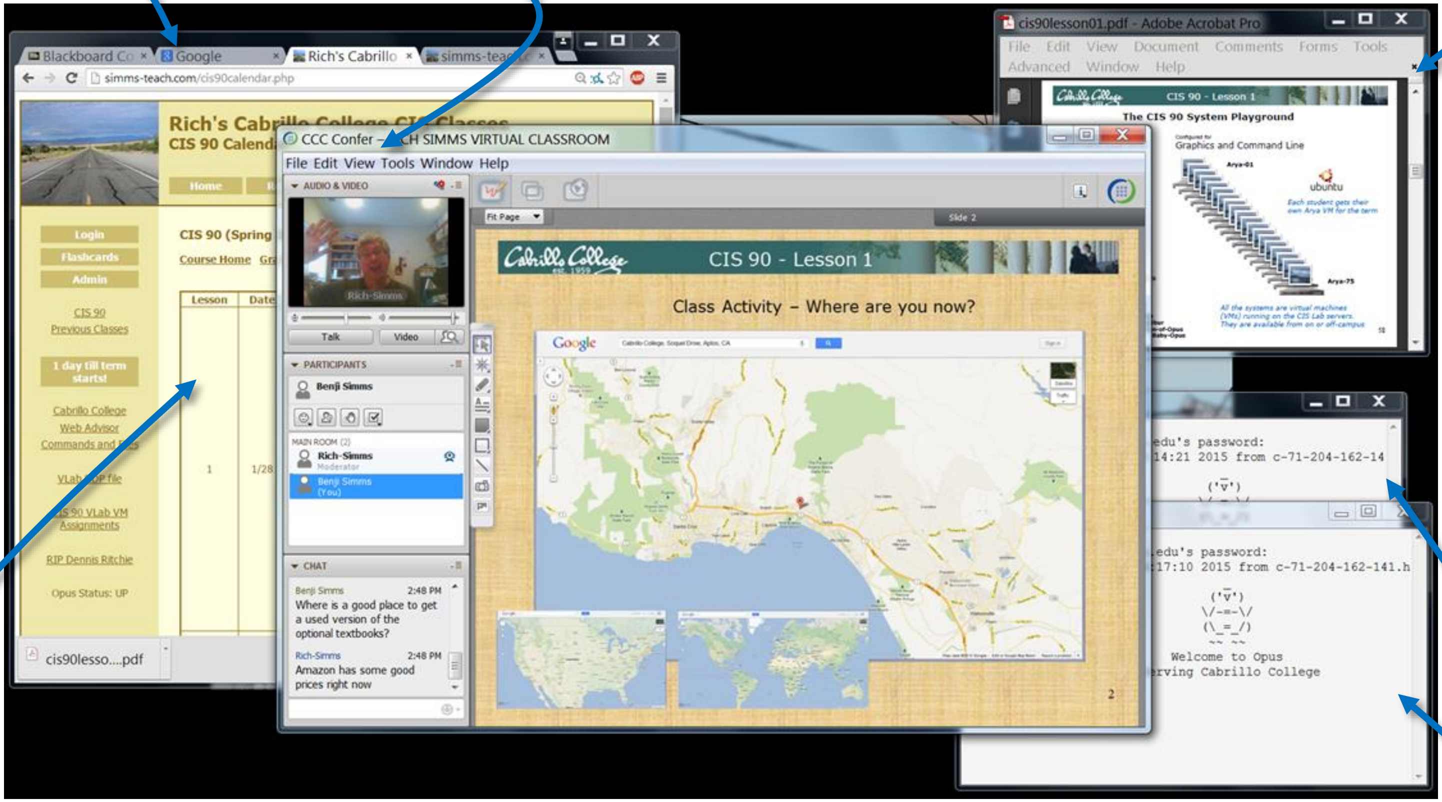
Student checklist for attending class


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

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

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

Student checklist for suggested screen layout


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

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

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

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

        ('v')
```

```
edu's password:
17:10 2015 from c-71-204-162-141.h

        ('v')
       \/-=-\/
       (\_=_/)
        ~~ ~~
   Welcome to Opus
erving Cabrillo College
```

❑ Google

❑ CCC Confer

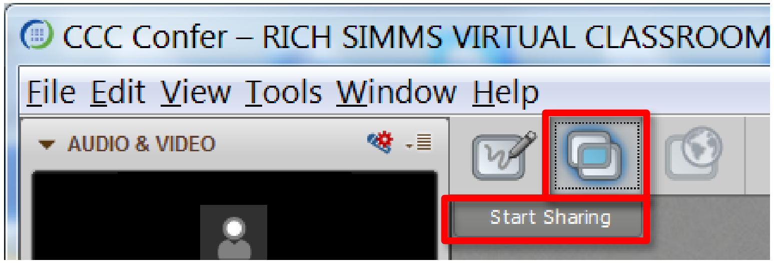
❑ Downloaded PDF of Lesson Slides

❑ CIS 76 website Calendar page

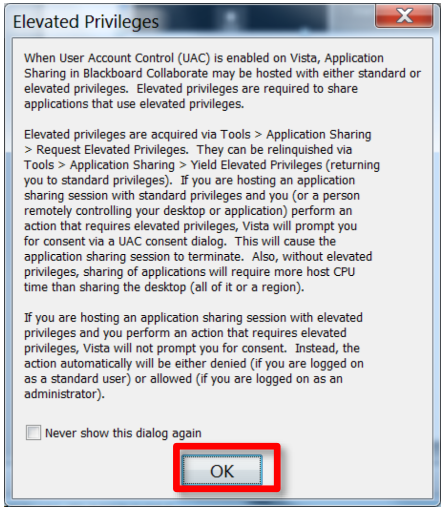
❑ One or more login sessions to Opus

Student checklist for sharing desktop with classmates

1) Instructor gives you sharing privileges.


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

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



Elevated Privileges

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

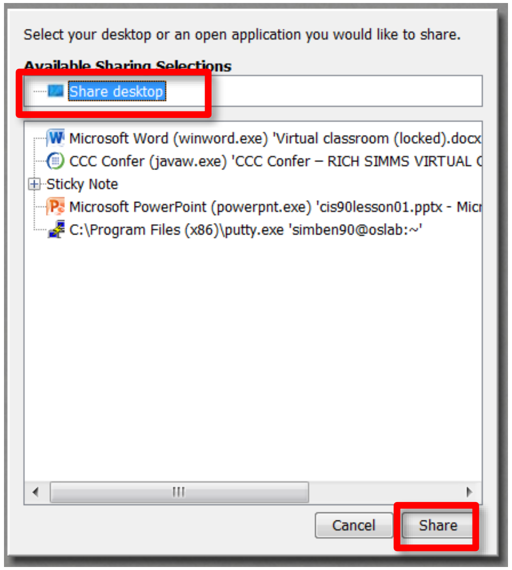
Elevated privileges are acquired via Tools > Application Sharing > Request Elevated Privileges. They can be relinquished via Tools > Application Sharing > Yield Elevated Privileges (returning you to standard privileges). If you are hosting an application sharing session with standard privileges and you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

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

☐ Never show this dialog again

OK

3) Click OK button.



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

Available Sharing Selections

Share desktop

Microsoft Word (winword.exe) 'Virtual classroom (locked).docx

CCC Confer (javaw.exe) 'CCC Confer – RICH SIMMS VIRTUAL C

Sticky Note

Microsoft PowerPoint (powerpnt.exe) 'cis90lesson01.pptx - Micr

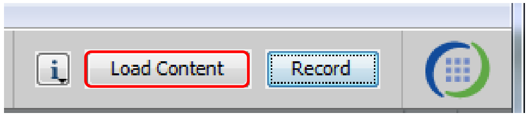
C:\Program Files (x86)\putty.exe 'simben90@oslab:~'

Cancel | Share

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

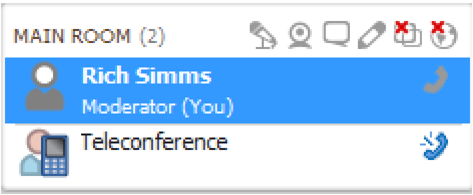
Rich's CCC Confer checklist - setup

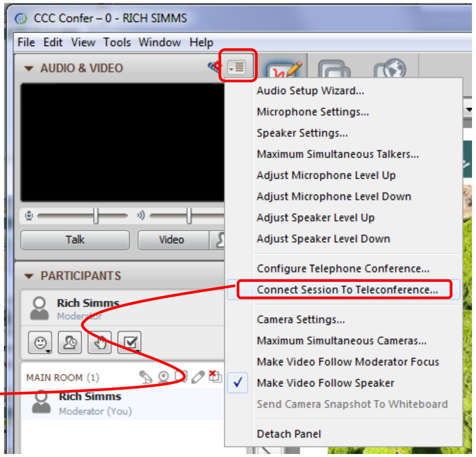
[ ] Preload White Board



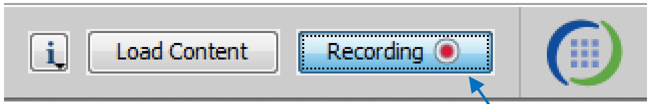
[ ] Connect session to Teleconference

Session now connected to teleconference

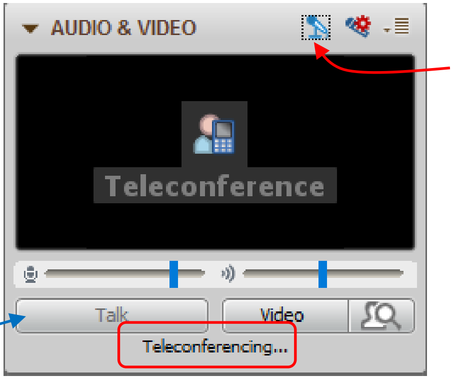



CCC Confer – 0 - RICH SIMMS
File Edit View Tools Window Help
AUDIO & VIDEO
Audio Setup Wizard...
Microphone Settings...
Speaker Settings...
Maximum Simultaneous Talkers...
Adjust Microphone Level Up
Adjust Microphone Level Down
Adjust Speaker Level Up
Adjust Speaker Level Down
Configure Telephone Conference...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

[ ] Is recording on?



Red dot means recording

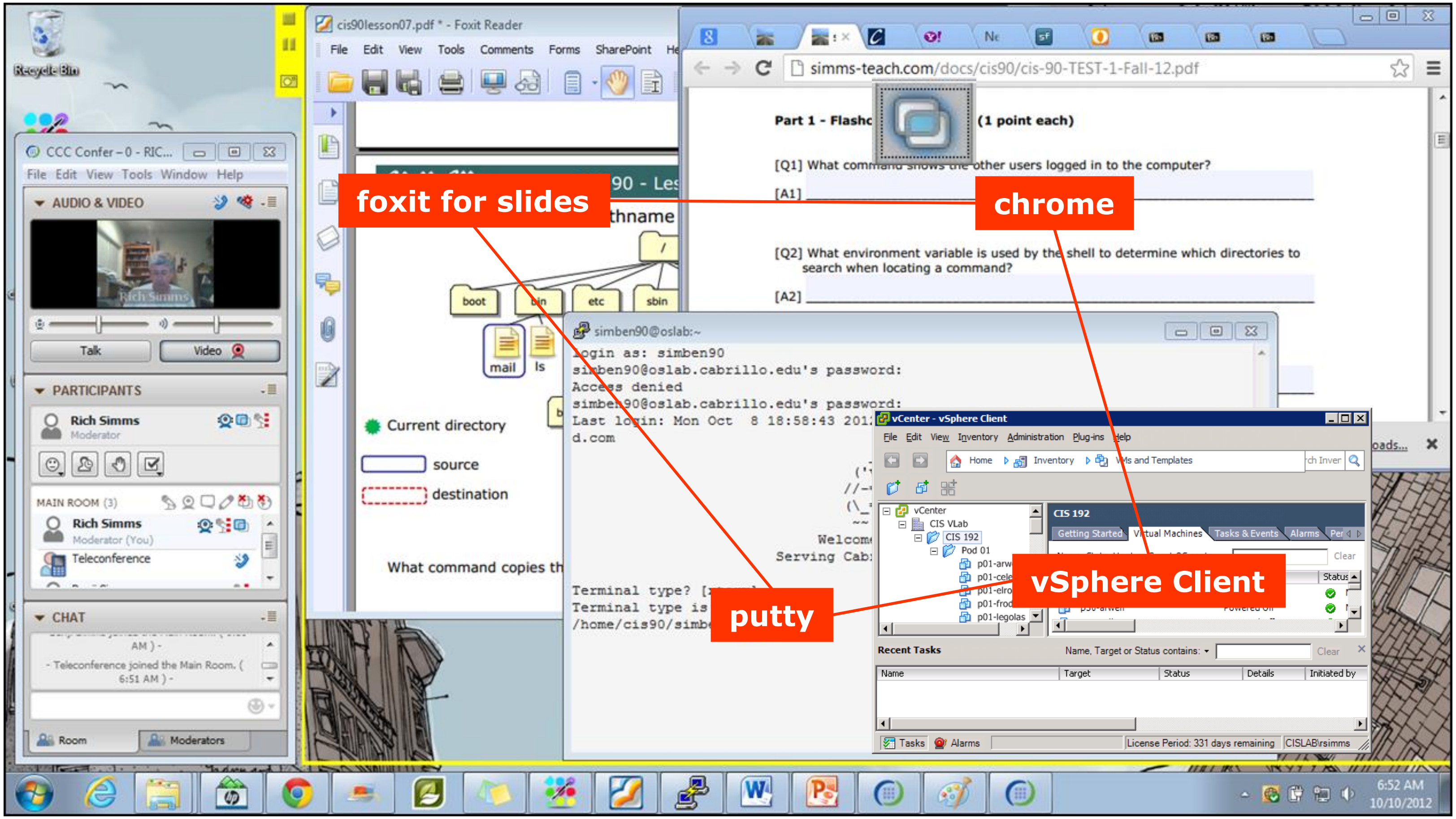


Should change from phone handset icon to little Microphone icon and the Teleconferencing … message displayed

[ ] Use teleconferencing, not mic

Should be grayed out

Rich's CCC Confer checklist - screen layout



Part 1 - Flashc... (1 point each)

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

[A1] ______

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

[A2] ______

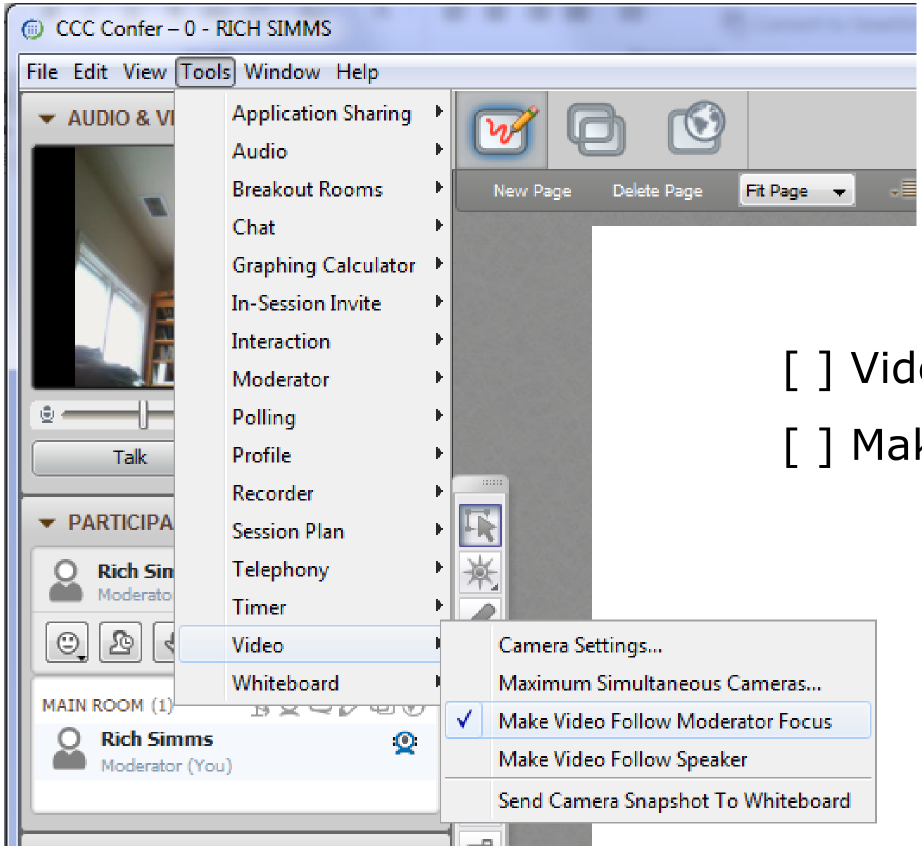
```
login as: simben90
simben90@oslab.cabrillo.edu's password:
Access denied
simben90@oslab.cabrillo.edu's password:
Last login: Mon Oct  8 18:58:43 201
d.com

                                    Welcom
                                Serving Cab

Terminal type? [
Terminal type is
/home/cis90/simb
```

[ ] layout and share apps

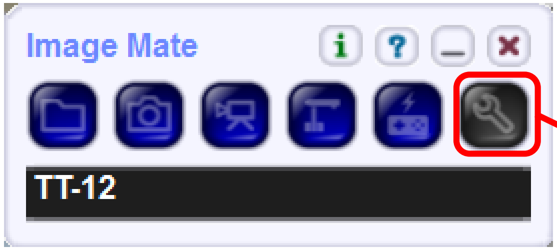
Rich's CCC Confer checklist - webcam setup

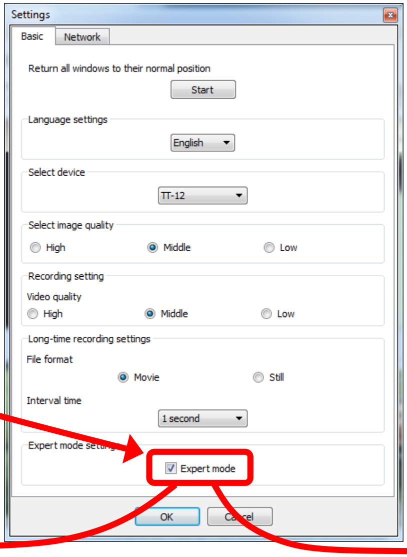


[ ] Video (webcam)

[ ] Make Video Follow Moderator Focus

Rich's CCC Confer checklist - Elmo





Settings

Basic | Network

Return all windows to their normal position

Start

Language settings

English ▾

Select device

TT-12 ▾

Select image quality

○ High ● Middle ○ Low

Recording setting

Video quality

○ High ● Middle ○ Low

Long-time recording settings

File format

● Movie ○ Still

Interval time

1 second ▾

Expert mode setting

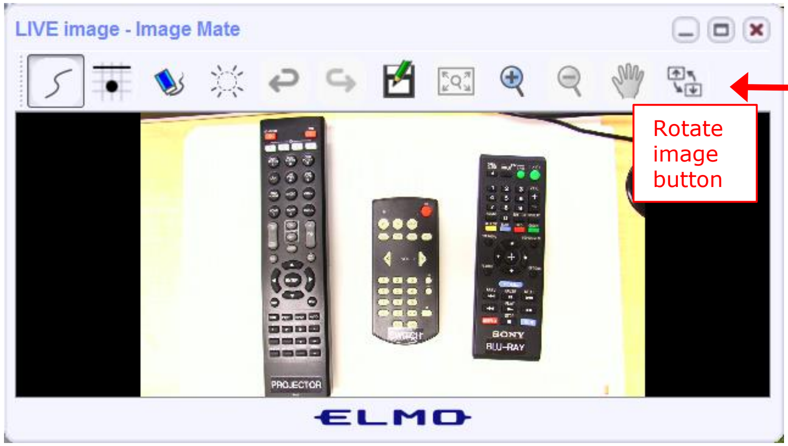
☑ Expert mode

OK | Cancel

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

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

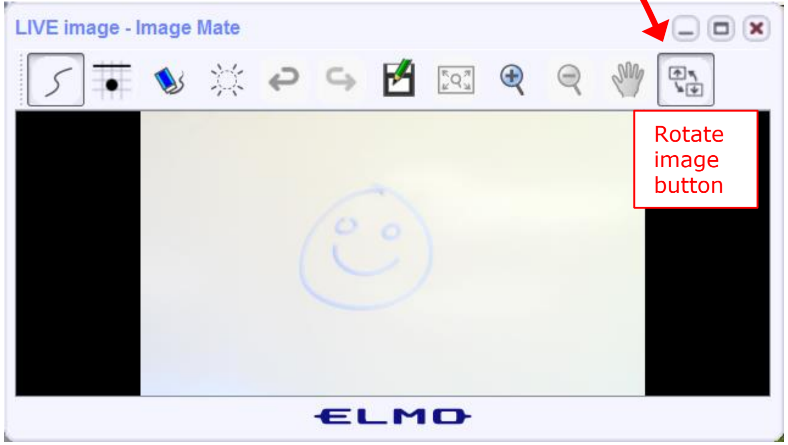
Elmo rotated down to view side table



Rotate image button

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

Elmo rotated up to view white board



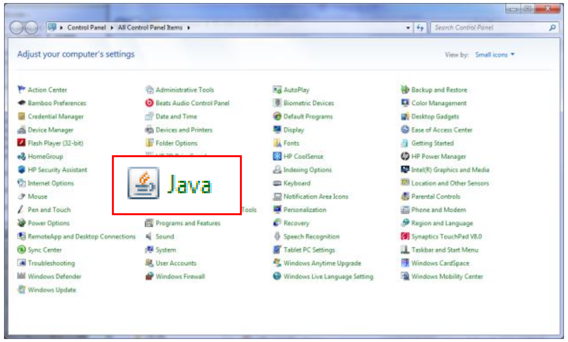
Rotate image button

Rich's CCC Confer checklist - universal fixes

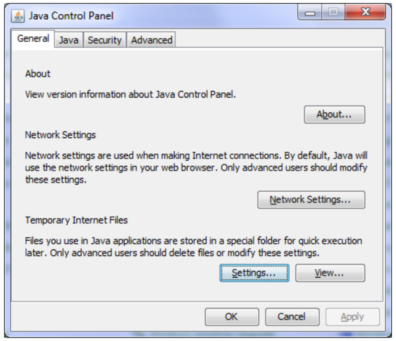
Universal Fix for CCC Confer:

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...



About

View version information about Java Control Panel.

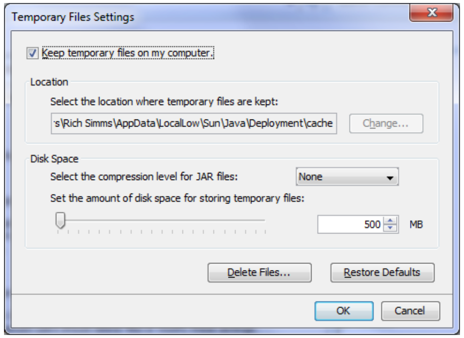
Network Settings

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

Temporary Internet Files

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

500MB cache size



☑ Keep temporary files on my computer.

Location

Select the location where temporary files are kept:

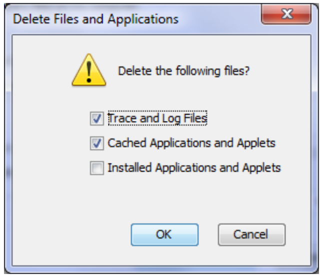
s\Rich Simms\AppData\LocalLow\Sun\Java\Deployment\cache

Disk Space

Select the compression level for JAR files: None

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

Delete these



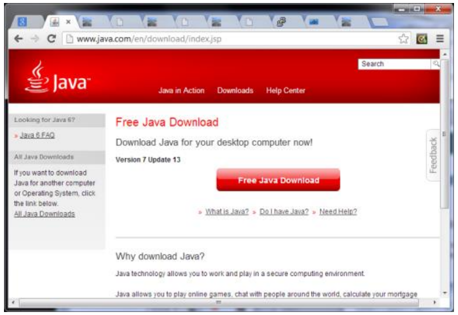
Delete the following files?

☑ Trace and Log Files

☑ Cached Applications and Applets

☐ Installed Applications and Applets

Google Java download



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

Free Java Download

Download Java for your desktop computer now!

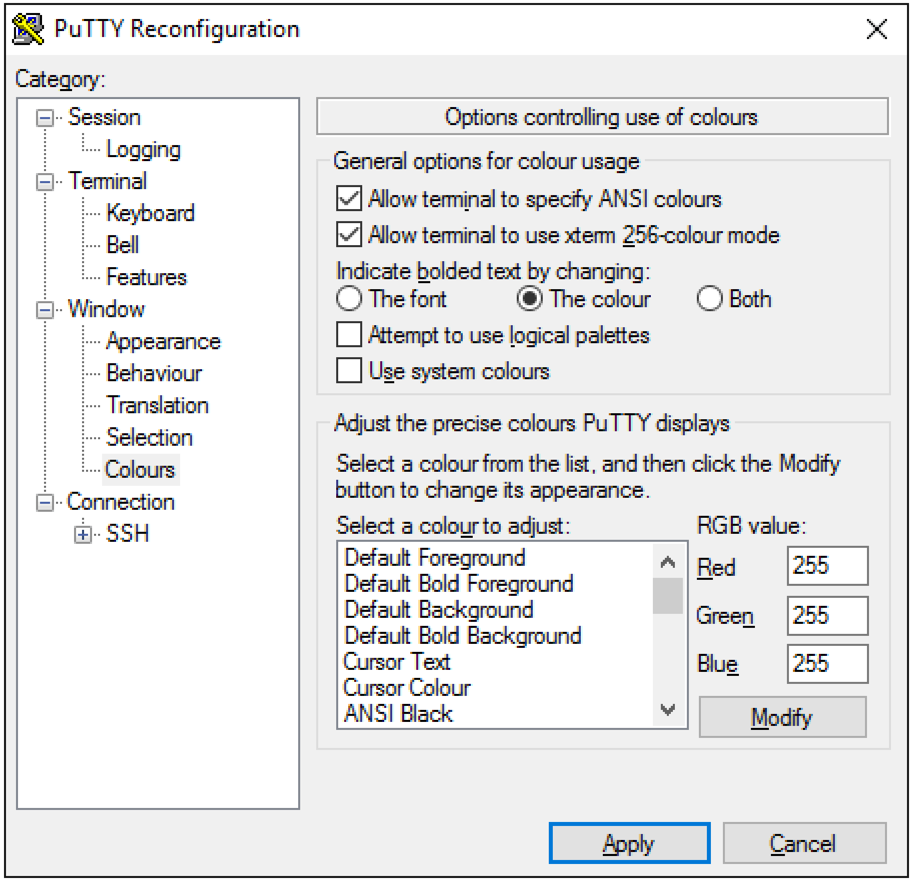
Version 7 Update 13

Why download Java?

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

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

Rich's CCC Confer checklist - Putty Colors



PuTTY Reconfiguration

Category:

Options controlling use of colours

General options for colour usage

☑ Allow terminal to specify ANSI colours

☑ Allow terminal to use xterm 256-colour mode

Indicate bolded text by changing:

○ The font ● The colour ○ Both

□ Attempt to use logical palettes

□ Use system colours

Adjust the precise colours PuTTY displays

Select a colour from the list, and then click the Modify button to change its appearance.

Select a colour to adjust:

Default Foreground
Default Bold Foreground
Default Background
Default Bold Background
Cursor Text
Cursor Colour
ANSI Black

RGB value:

Red 255

Green 255

Blue 255

http://looselytyped.blogspot.com/2013/02/zenburn-pleasant-color-scheme-for-putty.html

Putty Colors

Default Foreground 255 255 255
Default Bold Foreground 255 255 255
Default Background 51 51 51
Default Bold Background 255 2 85
Cursor Text 0 0 0
Cursor Color 0 255 0
ANSI Black 77 77 77
ANSI Black Bold 85 85 85
ANSI Red 187 0 0
ANSI Red Bold 255 85 85
ANSI Green 152 251 152
ANSI Green Bold 85 255 85
ANSI Yellow 240 230 140
ANSI Yellow Bold 255 255 85
ANSI Blue 205 133 63
ANSI Blue Bold 135 206 235
ANSI Magenta 255 222 173
ANSI Magenta Bold 255 85 255
ANSI Cyan 255 160 160
ANSI Cyan Bold 255 215 0
ANSI White 245 222 179
ANSI White Bold 255 255 255

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.*

Ethical Hacking Overview

Objectives

- Describe the roles of security and penetration testers.
- Describe what ethical hackers can and cannot legally do.

Agenda

- Introductions
- Admonition
- How this class works
- Lab resources
- Housekeeping
- Ethical hacking overview
- Laws
- Certifications
- Vocabulary
- Conferences
- Newsletters and Blogs
- MS08-067 (CVE-2008-4250) hack
- VLab pod setup
- Assignment
- Wrap up

Introductions

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!

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

Philip

Bruce

James

Sam B.

Sam R.

Miguel

Bobby

Garrett

Ryan A.

Agnieszka

Efrain A.

Christopher

Adam

Efrain O.

Xu

Mariano

Nicholas

Ryan M.

Cameron

Corbin

Tre

May

Karl-Heinz

Remy

Tanner

Helen

Tyler

TBD

TBD

TBD

TBD

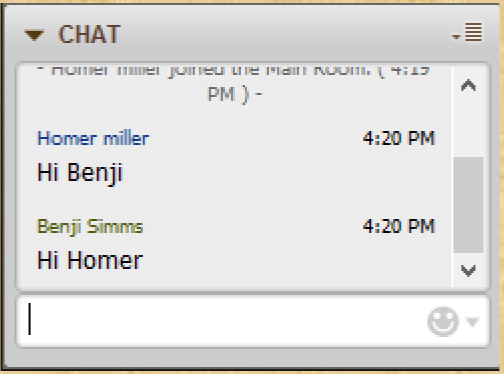
TBD

TBD

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

First Activity

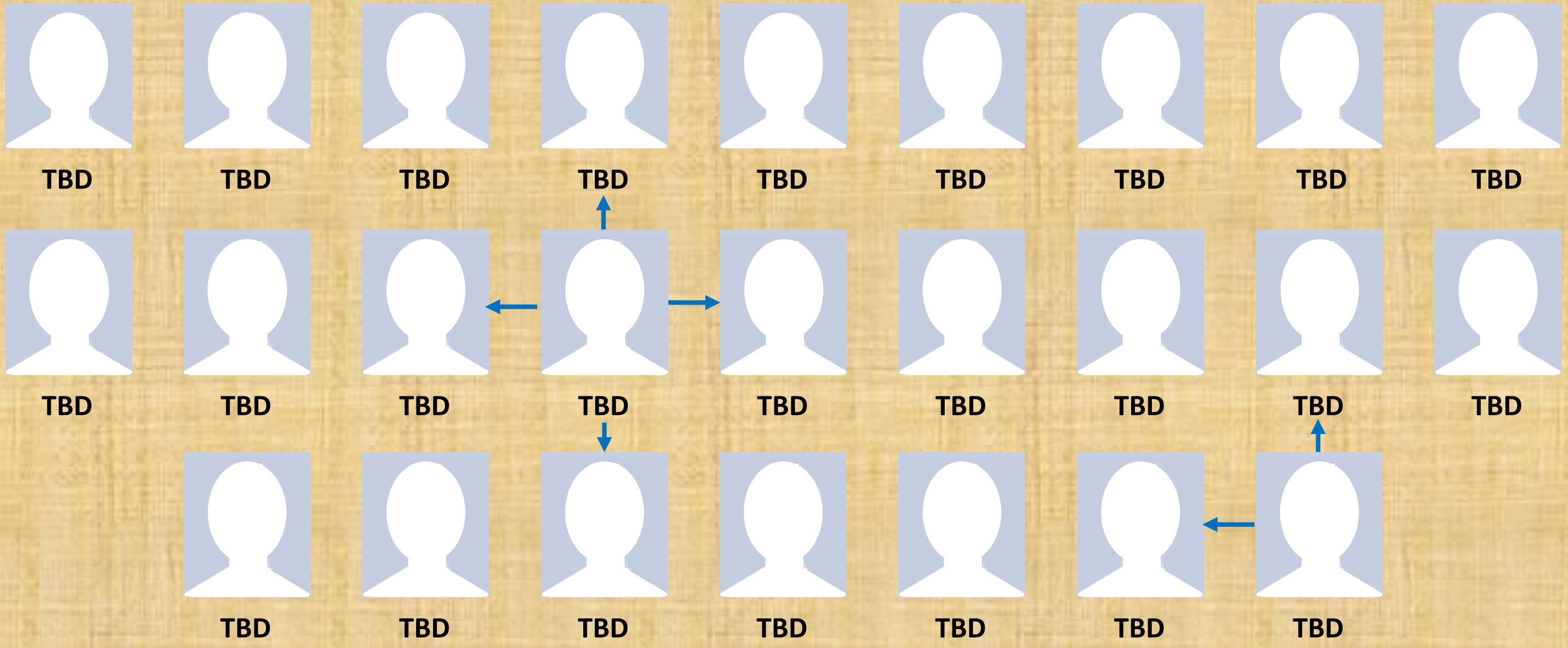
Use the chat window in CCC Confer to say Hi to your adjacent "virtual classmates"



- Homer miller joined the Main Room. (4:19 PM) -

Homer miller 4:20 PM
Hi Benji

Benji Simms 4:20 PM
Hi Homer



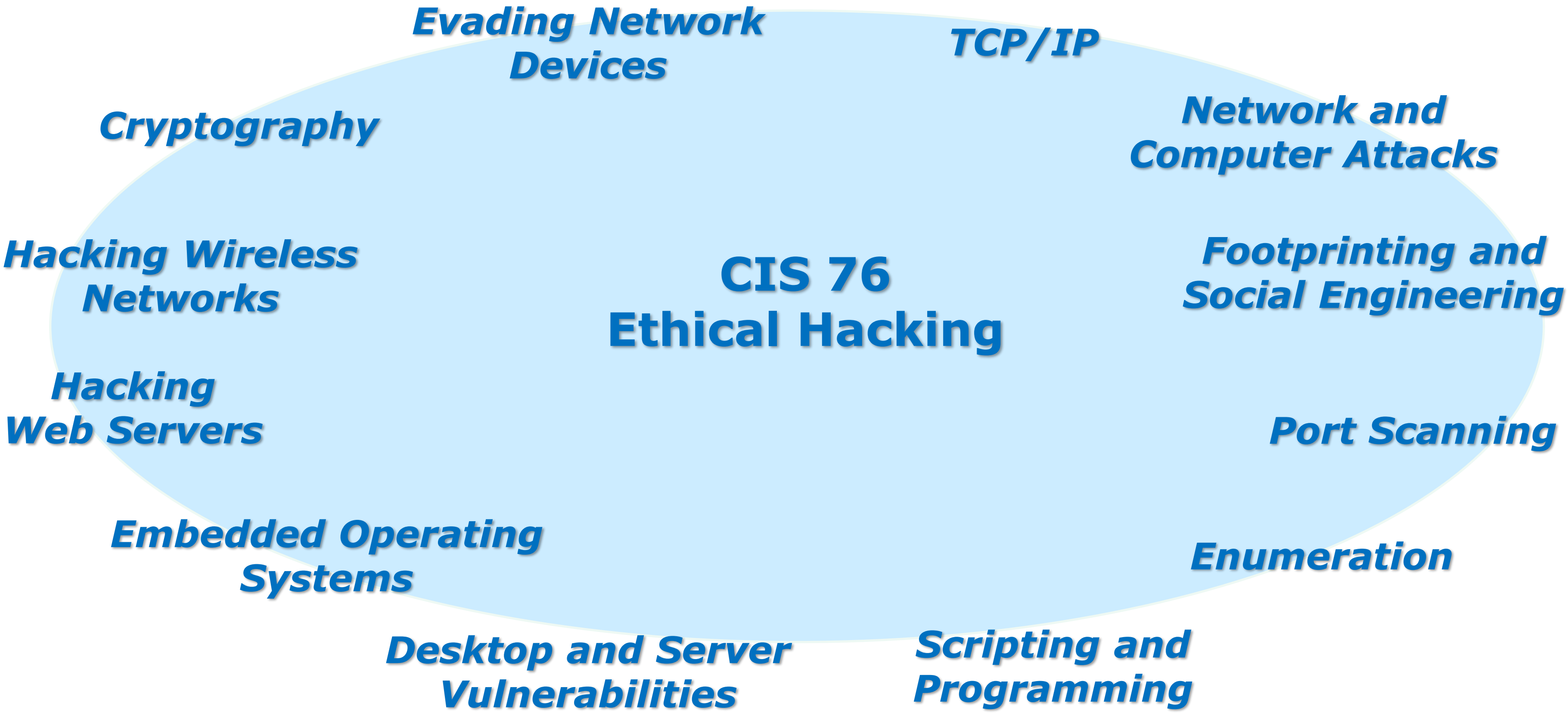
TBD TBD TBD TBD TBD TBD TBD TBD TBD

TBD TBD TBD TBD TBD TBD TBD TBD TBD

TBD TBD TBD TBD TBD TBD TBD

If your name is not listed above you can chat Hi to anyone you want!

What is this class about?



Evading Network Devices
TCP/IP
Cryptography
Network and Computer Attacks
Hacking Wireless Networks
CIS 76 Ethical Hacking
Footprinting and Social Engineering
Hacking Web Servers
Port Scanning
Embedded Operating Systems
Enumeration
Desktop and Server Vulnerabilities
Scripting and Programming

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.

Admonition

Unauthorized hacking is a crime.

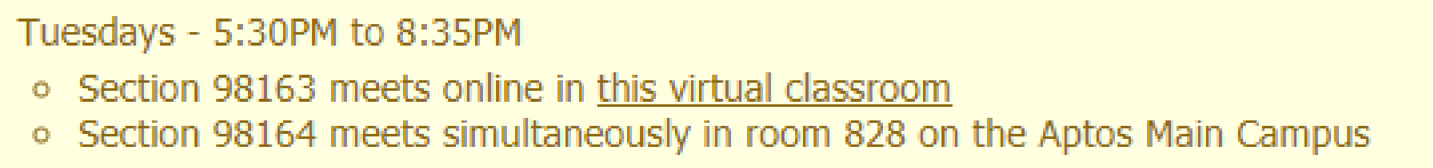
The hacking methods and activities learned in this course can result in prison terms, large fines and lawsuits if used in an unethical manner. They may only be used in a lawful manner on equipment you own or where you have explicit permission from the owner.

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.

How this class works

Attending class

How to attend class each week



Tuesdays - 5:30PM to 8:35PM

- Section 98163 meets online in this virtual classroom
- Section 98164 meets simultaneously in room 828 on the Aptos Main Campus

Option 1: **Online "synchronous"** - from anywhere connect online to the "live" virtual classroom using CCC Confer. Use the "Enter virtual classroom" link on: https://simms-teach.com/cis76calendar.php

Option 2: **Traditional** - drive to campus, find parking, walk to the 800 building and take a seat in the classroom.

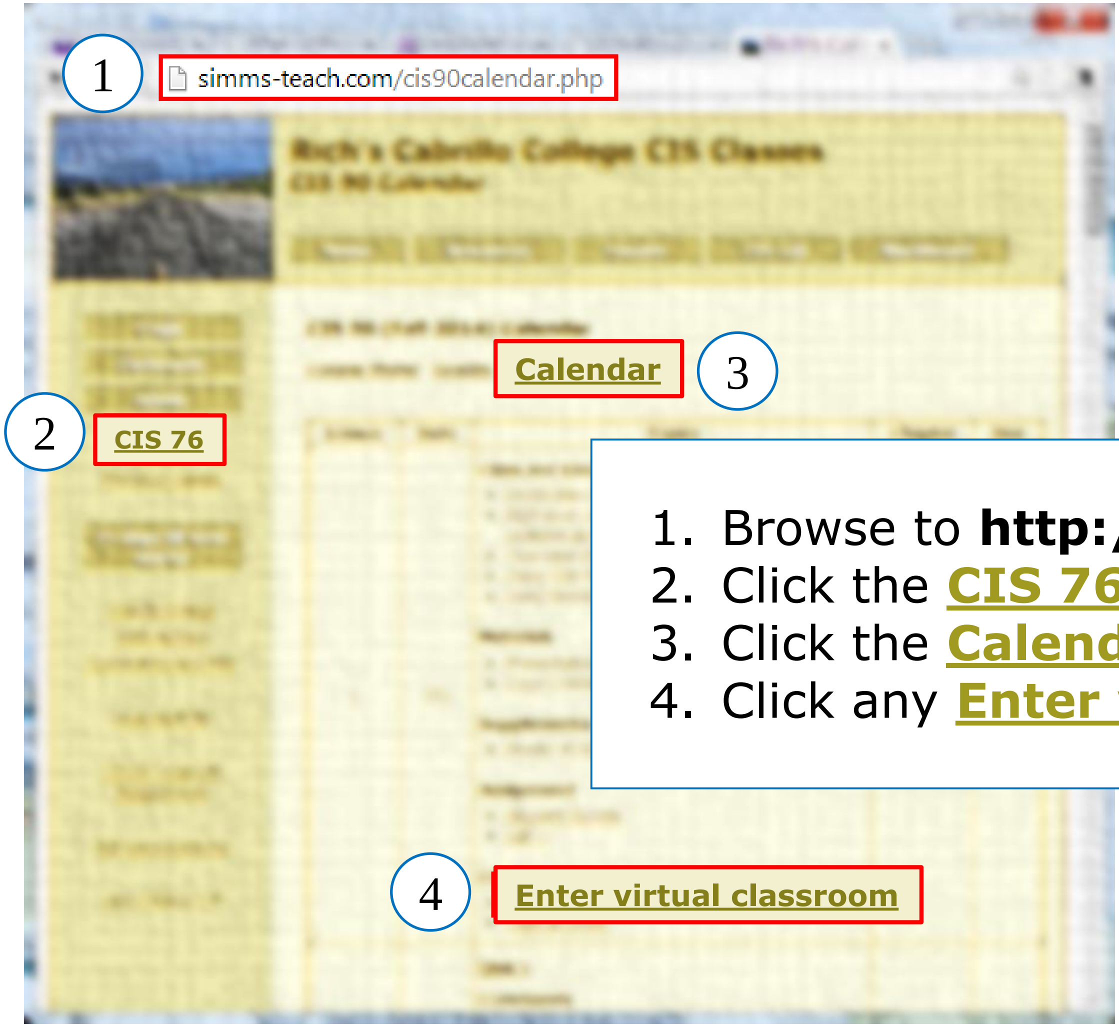
Option 3: **Online archives "asynchronous"** - watch the archived class recording online using CCC Confer at a time that works for you. Use the "Class archives" link on: https://simms-teach.com/cis76calendar.php

*It doesn't matter which section you enrolled in. You can use **any** method of attending for **any** of the classes.*

Attending Class

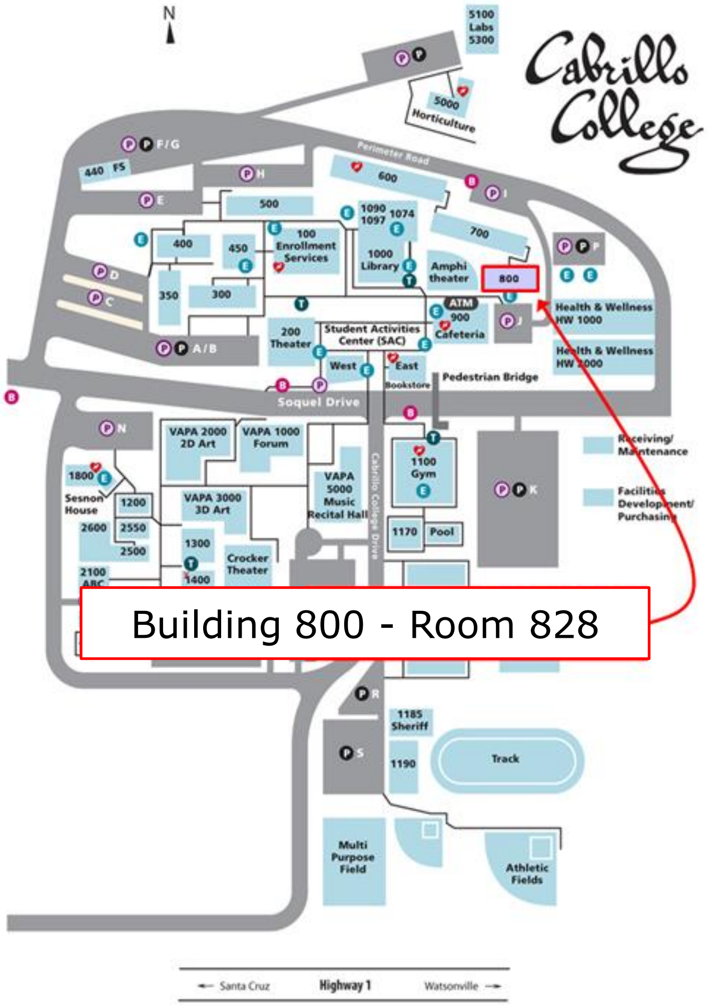
(supplemental)

Option 1: **Online (synchronous)** - from anywhere connect online to the "live" virtual classroom using CCC Confer.


1
simms-teach.com/cis90calendar.php
Rich's Cabrillo College CIS Classes
CIS 90 Calendar
Calendar
3
2
CIS 76
4
Enter virtual classroom

1. Browse to **http://simms-teach.com**
2. Click the **CIS 76** link
3. Click the **Calendar** link
4. Click any **Enter virtual classroom** link

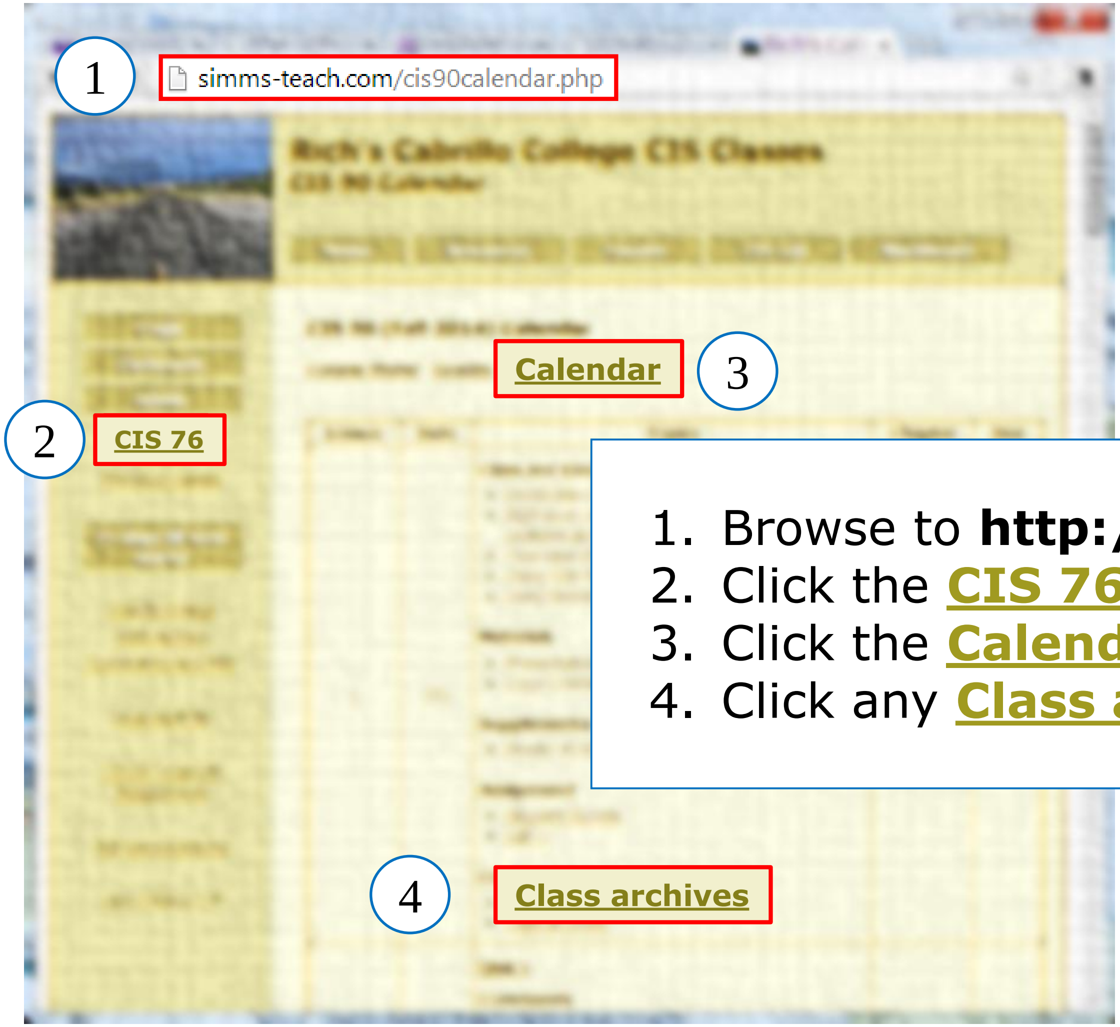
Option 2: **Traditional** - drive to campus, find parking, walk to the 800 building and take a seat in the classroom.



Building 800 - Room 828

Enjoy the ocean view from the classroom windows!

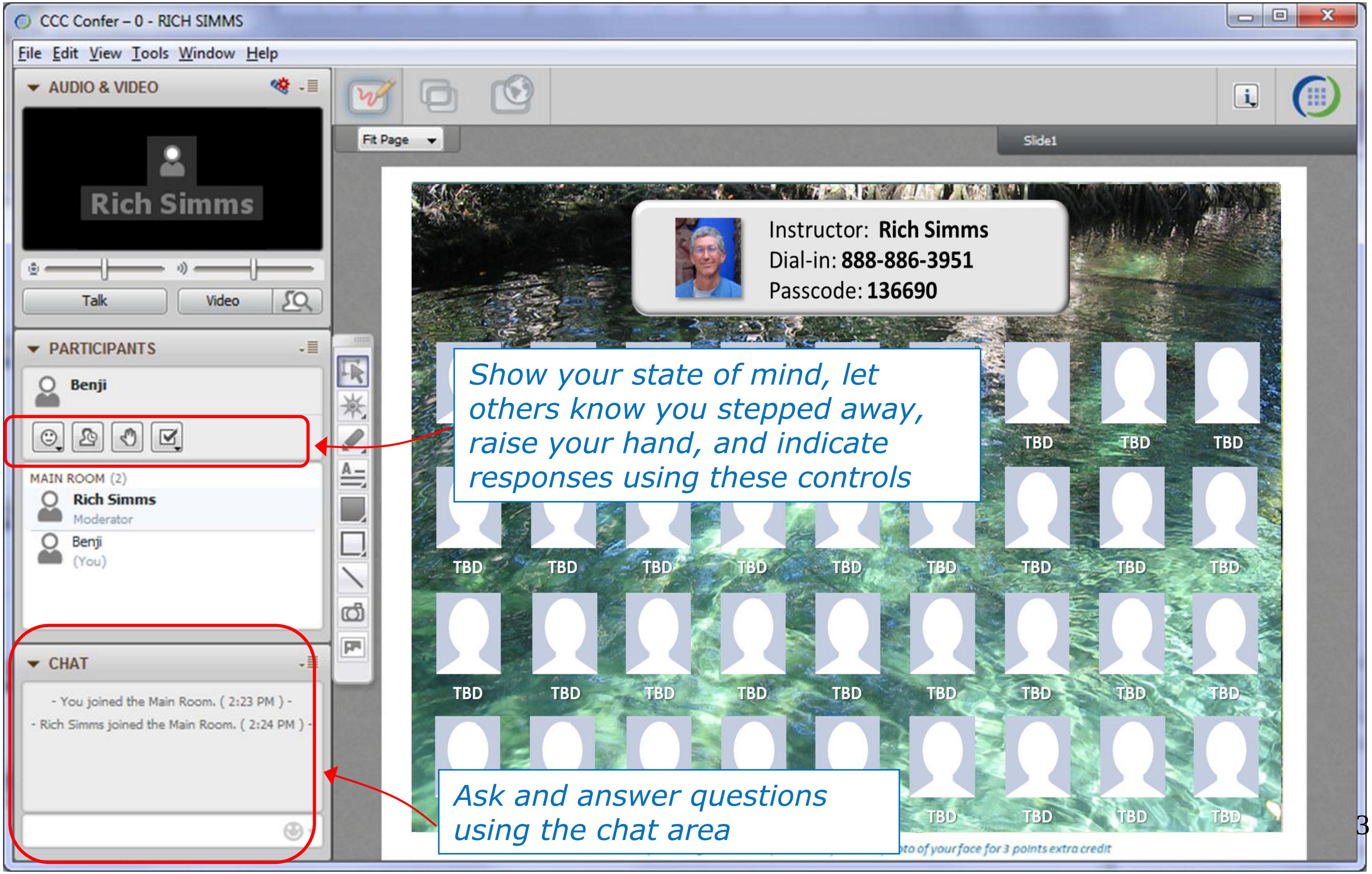
Option 3: **Online archives (asynchronous)** - watch the archived class recording online using CCC Confer at a time that works for you.


1
simms-teach.com/cis90calendar.php
Rich's Cabrillo College CIS Classes
CIS 90 Calendar
2
CIS 76
Calendar
3
4
Class archives

1. Browse to **http://simms-teach.com**
2. Click the **CIS 76** link
3. Click the **Calendar** link
4. Click any **Class archives** link

CCC Confer

CCC Confer - Attending class online



- You joined the Main Room. (2:23 PM) -

- Rich Simms joined the Main Room. (2:24 PM) -

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

Show your state of mind, let others know you stepped away, raise your hand, and indicate responses using these controls

Ask and answer questions using the chat area

CCC Confer - Attending class online

When dialed in by phone you can use:

*0 Contact the operator for assistance.

*6 Mute/unmute your individual line with a private announcement.

This only applies if you dialed in using a phone

Help the Instructor with CCC Confer

Students who attend class on the Aptos campus should still use CCC Confer.

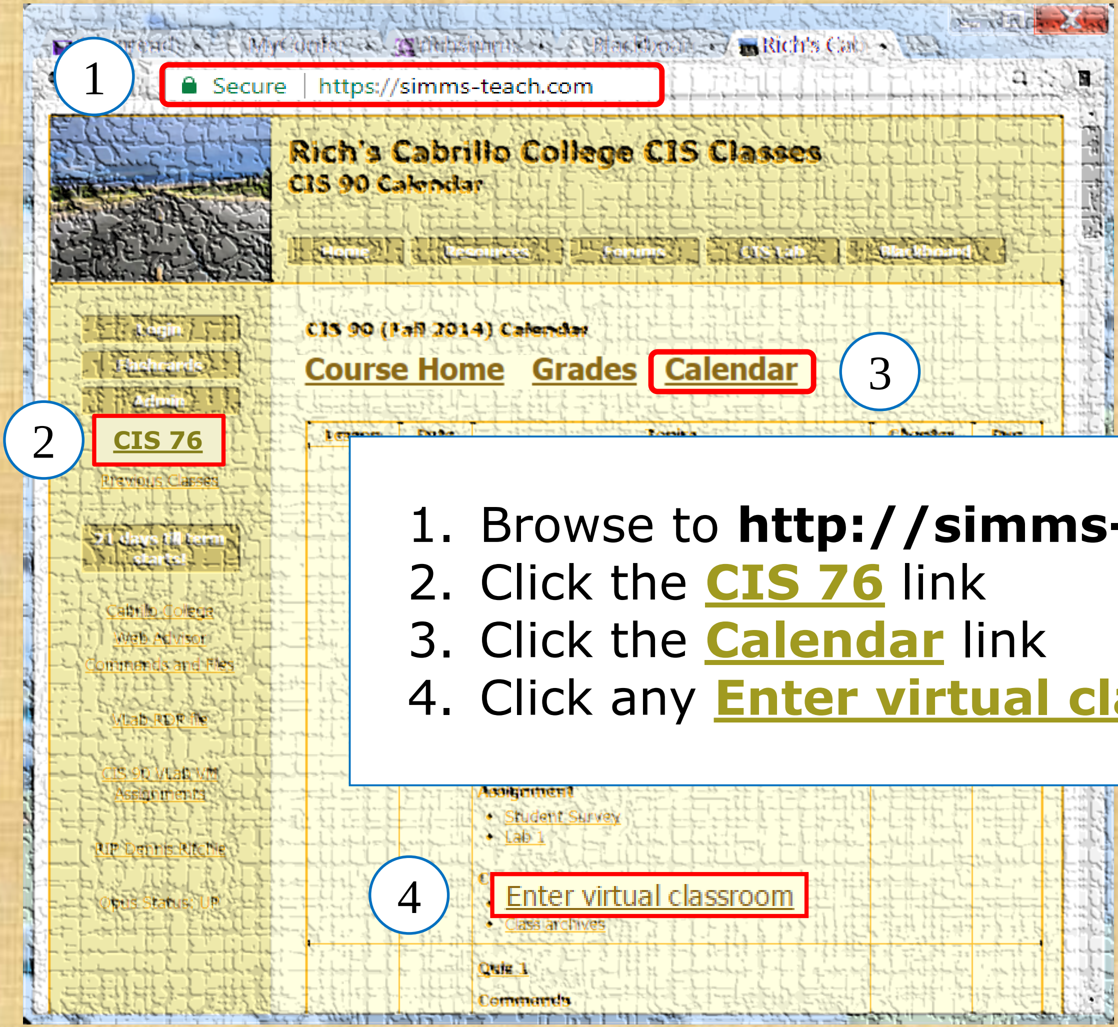
- If you notice **an online student with their electronic hand up that the instructor missed** please let the instructor know.
- If you notice the instructor **forgot to Share the presentation** material please let the instructor know.
- If you notice the instructor **forgot to turn on recording** please jump up and down and wave your arms to let the instructor know!

CCC Confer

(supplemental)

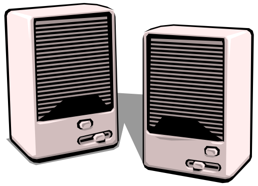
simms-teach.com

Find the CCC Confer virtual room



1. Browse to **http://simms-teach.com**
2. Click the **CIS 76** link
3. Click the **Calendar** link
4. Click any **Enter virtual classroom** link

- Listen using your computer's speakers/headset or with your phone using the dial-in number

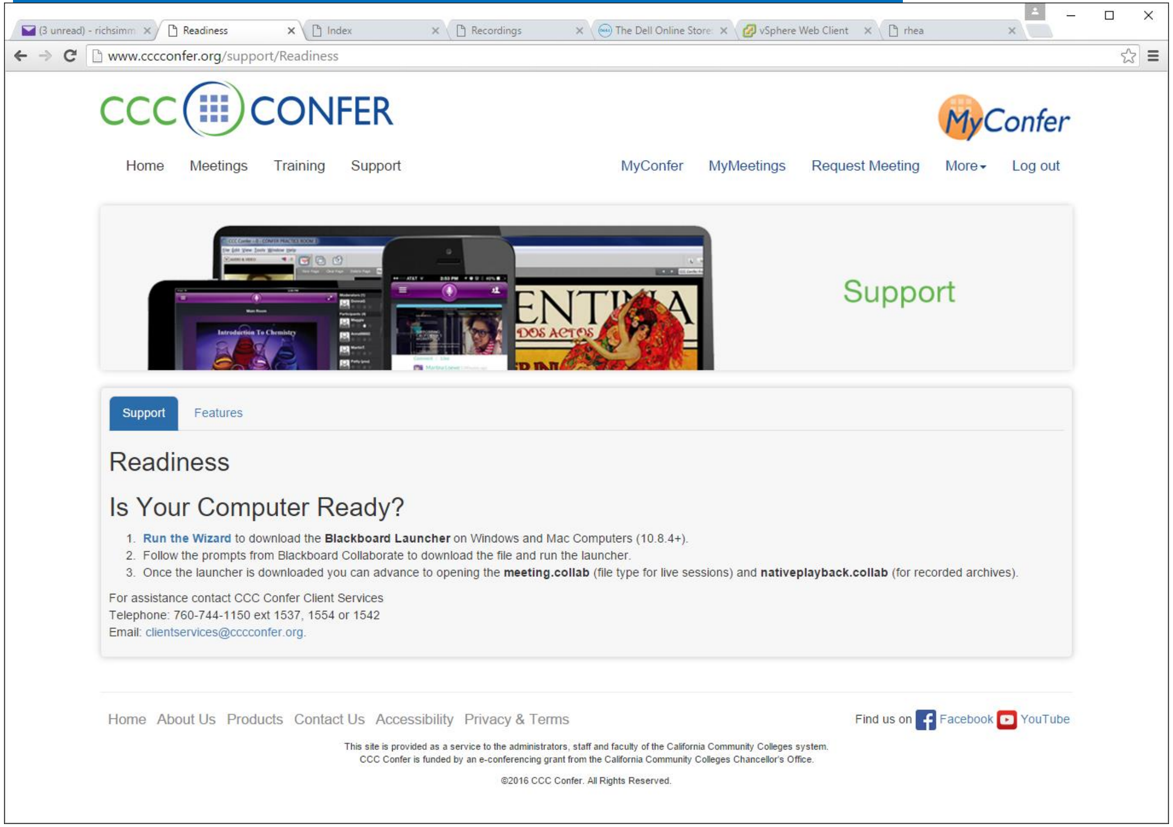


- Ask questions using the chat window or just speak if dialed in with your phone (or Skype)

Dialing in by phone (or Skype) is best because you can ask and answer questions by speaking rather than use the chat window

CCC Confer - Is your computer ready?

http://www.cccconfer.org/support/Readiness



Readiness

Is Your Computer Ready?

1. **Run the Wizard** to download the **Blackboard Launcher** on Windows and Mac Computers (10.8.4+).
2. Follow the prompts from Blackboard Collaborate to download the file and run the launcher.
3. Once the launcher is downloaded you can advance to opening the **meeting.collab** (file type for live sessions) and **nativeplayback.collab** (for recorded archives).

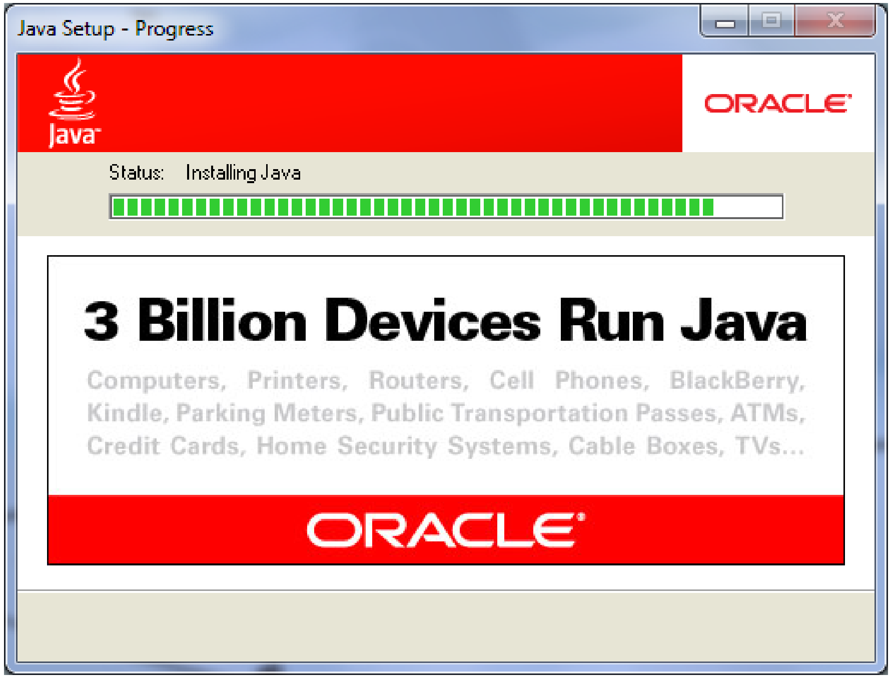
For assistance contact CCC Confer Client Services
Telephone: 760-744-1150 ext 1537, 1554 or 1542
Email: clientservices@cccconfer.org.

This site is provided as a service to the administrators, staff and faculty of the California Community Colleges system.
CCC Confer is funded by an e-conferencing grant from the California Community Colleges Chancellor's Office.

©2016 CCC Confer. All Rights Reserved.

Browse to the link above anytime before the first class. The first time setup for CCC Confer can take several minutes!

CCC Confer - Java may be downloaded the first time you use CCC Confer



Java Setup - Progress

Status: Installing Java

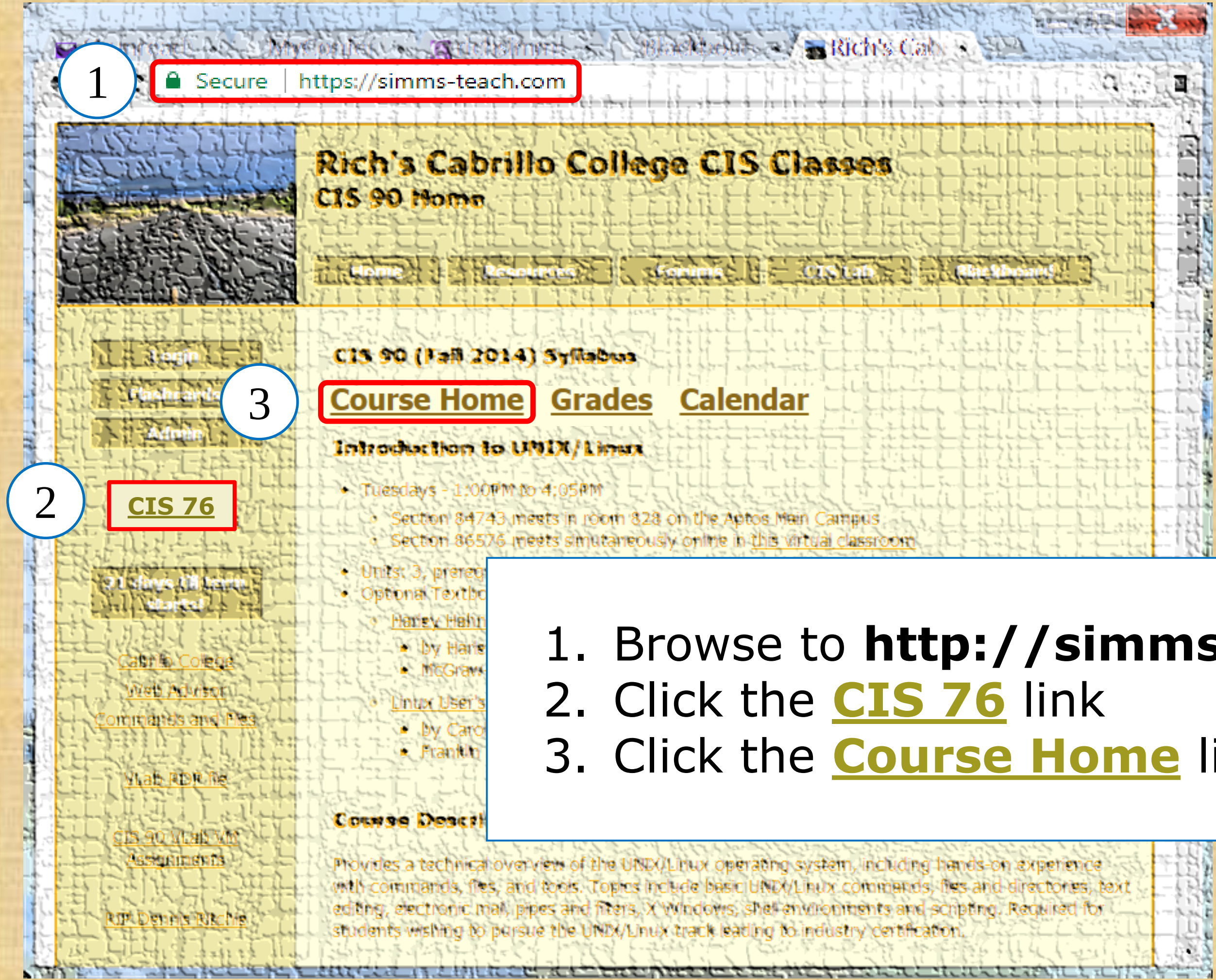
Java
ORACLE
3 Billion Devices Run Java
Computers, Printers, Routers, Cell Phones, BlackBerry, Kindle, Parking Meters, Public Transportation Passes, ATMs, Credit Cards, Home Security Systems, Cable Boxes, TVs...
ORACLE

CCC Confer uses Java which requires a download and installation of the Java Runtime Environment from java.com (Oracle)

Syllabus, Calendar and Grades

simms-teach.com

Find the syllabus



CIS 90 (Fall 2014) Syllabus

Course Home Grades Calendar

Introduction to UNIX/Linux

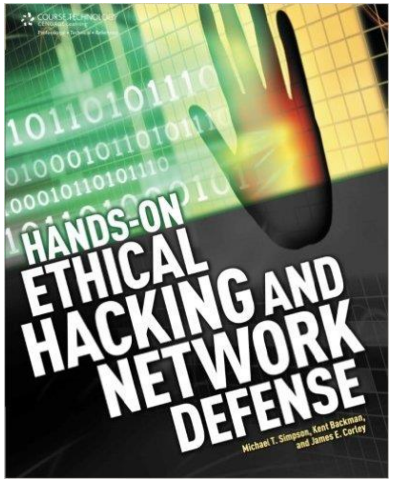
- Tuesdays - 1:00PM to 4:05PM
  - Section 84743 meets in room 828 on the Aptos Main Campus
  - Section 86576 meets simultaneously online in this virtual classroom
- Units: 3, prereq
- Optional Textbo

Course Descri

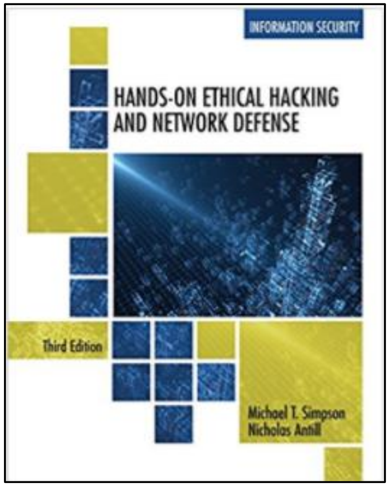
Provides a technical overview of the UNIX/Linux operating system, including hands-on experience with commands, files, and tools. Topics include basic UNIX/Linux commands, files and directories, text editing, electronic mail, pipes and filters, X Windows, shell environments and scripting. Required for students wishing to pursue the UNIX/Linux track leading to industry certification.

1. Browse to **http://simms-teach.com**
2. Click the **CIS 76** link
3. Click the **Course Home** link

CIS 76 Textbook


COURSE TECHNOLOGY
HANDS-ON ETHICAL HACKING AND NETWORK DEFENSE
Michael T. Simpson, Kent Backman, and James E. Corley

OR



Textbook:

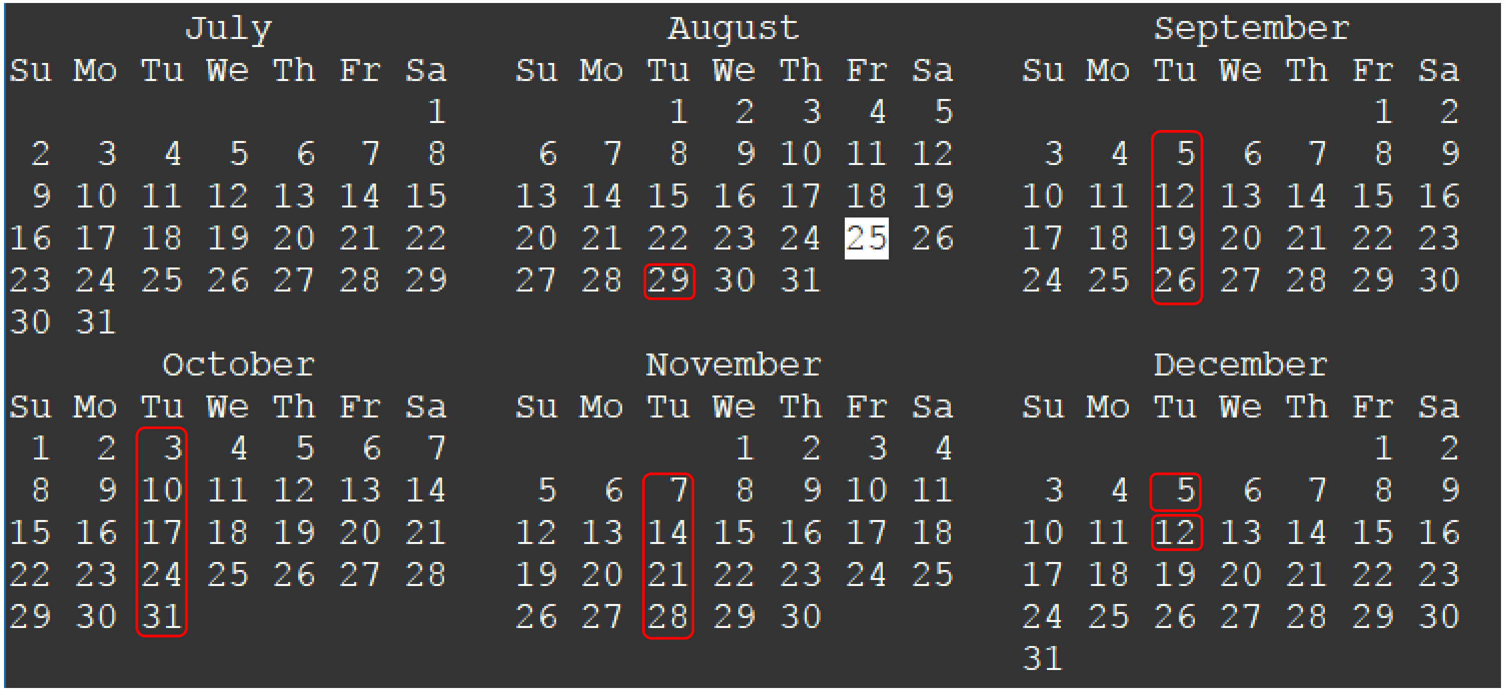
Hands-On Ethical Hacking and Network Defense 1st Edition
by Michael T. Simpson (Author), Kent Backman (Author), James Corley (Author)
ISBN-13: 978-1133935612

Hands-On Ethical Hacking and Network Defense 3rd Edition
by Michael T. Simpson (Author), Nicholas Antill (Author)
ISBN-13: 978-1285454610

CIS 76 Fall 2017

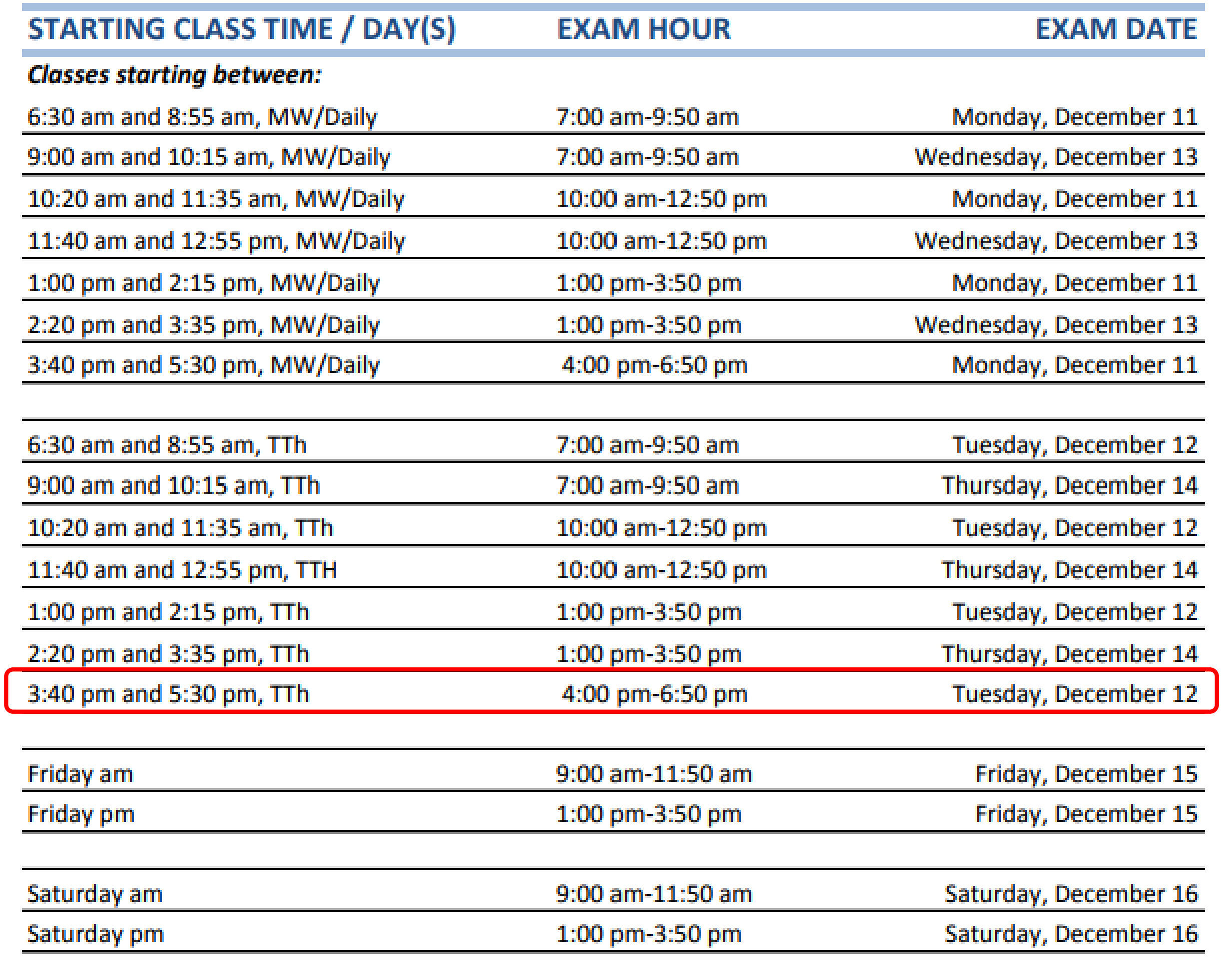
Class meets in room **828** and **online** every **Tuesday evening**:

- 15 lessons: **5:30-8:35 PM**, from **Aug 29th** to **Dec 5th**
- Final exam: **4:00-6:50PM**, on **Tuesday Dec 12th**, in room **828**



```
         July                  August               September
Su Mo Tu We Th Fr Sa   Su Mo Tu We Th Fr Sa   Su Mo Tu We Th Fr Sa
                   1          1  2  3  4  5                   1  2
 2  3  4  5  6  7  8    6  7  8  9 10 11 12    3  4  5  6  7  8  9
 9 10 11 12 13 14 15   13 14 15 16 17 18 19   10 11 12 13 14 15 16
16 17 18 19 20 21 22   20 21 22 23 24 25 26   17 18 19 20 21 22 23
23 24 25 26 27 28 29   27 28 29 30 31         24 25 26 27 28 29 30
30 31
        October               November              December
Su Mo Tu We Th Fr Sa   Su Mo Tu We Th Fr Sa   Su Mo Tu We Th Fr Sa
 1  2  3  4  5  6  7             1  2  3  4                   1  2
 8  9 10 11 12 13 14    5  6  7  8  9 10 11    3  4  5  6  7  8  9
15 16 17 18 19 20 21   12 13 14 15 16 17 18   10 11 12 13 14 15 16
22 23 24 25 26 27 28   19 20 21 22 23 24 25   17 18 19 20 21 22 23
29 30 31               26 27 28 29 30         24 25 26 27 28 29 30
                                              31
```

Fall 2017
Final Exam Schedule



STARTING CLASS TIME / DAY(S)	EXAM HOUR	EXAM DATE
Classes starting between:		
6:30 am and 8:55 am, MW/Daily	7:00 am-9:50 am	Monday, December 11
9:00 am and 10:15 am, MW/Daily	7:00 am-9:50 am	Wednesday, December 13
10:20 am and 11:35 am, MW/Daily	10:00 am-12:50 pm	Monday, December 11
11:40 am and 12:55 pm, MW/Daily	10:00 am-12:50 pm	Wednesday, December 13
1:00 pm and 2:15 pm, MW/Daily	1:00 pm-3:50 pm	Monday, December 11
2:20 pm and 3:35 pm, MW/Daily	1:00 pm-3:50 pm	Wednesday, December 13
3:40 pm and 5:30 pm, MW/Daily	4:00 pm-6:50 pm	Monday, December 11
6:30 am and 8:55 am, TTh	7:00 am-9:50 am	Tuesday, December 12
9:00 am and 10:15 am, TTh	7:00 am-9:50 am	Thursday, December 14
10:20 am and 11:35 am, TTh	10:00 am-12:50 pm	Tuesday, December 12
11:40 am and 12:55 pm, TTH	10:00 am-12:50 pm	Thursday, December 14
1:00 pm and 2:15 pm, TTh	1:00 pm-3:50 pm	Tuesday, December 12
2:20 pm and 3:35 pm, TTh	1:00 pm-3:50 pm	Thursday, December 14
3:40 pm and 5:30 pm, TTh	4:00 pm-6:50 pm	Tuesday, December 12
Friday am	9:00 am-11:50 am	Friday, December 15
Friday pm	1:00 pm-3:50 pm	Friday, December 15
Saturday am	9:00 am-11:50 am	Saturday, December 16
Saturday pm	1:00 pm-3:50 pm	Saturday, December 16

The typical week

http://simms-teach.com

phpBB creating communities Cabrillo College Linux Classes

Help forum for Rich's students

Board index ‹ CIS 191A - Fall 2008

User Control Panel (0 new messages) • View your posts

Searching files for specific text

First unread post • 3 posts • Page 1 of 1

Searching files for specific text

by Benji Simms on Mon May 26, 2008 11:01 am

I can't remember where I put a file. What is the command to search through the files on my computer to find one with the word "Bones" in it?

Benji Simms

Posts: 4
Joined: Thu May 15, 2008 2:40 pm

Re: Searching files for specific text

by Rich Simms on Mon May 26, 2008 11:44 am

Try:

CODE: SELECT ALL

Rich Simms

Use the

Forum

to collaborate with classmates at any time

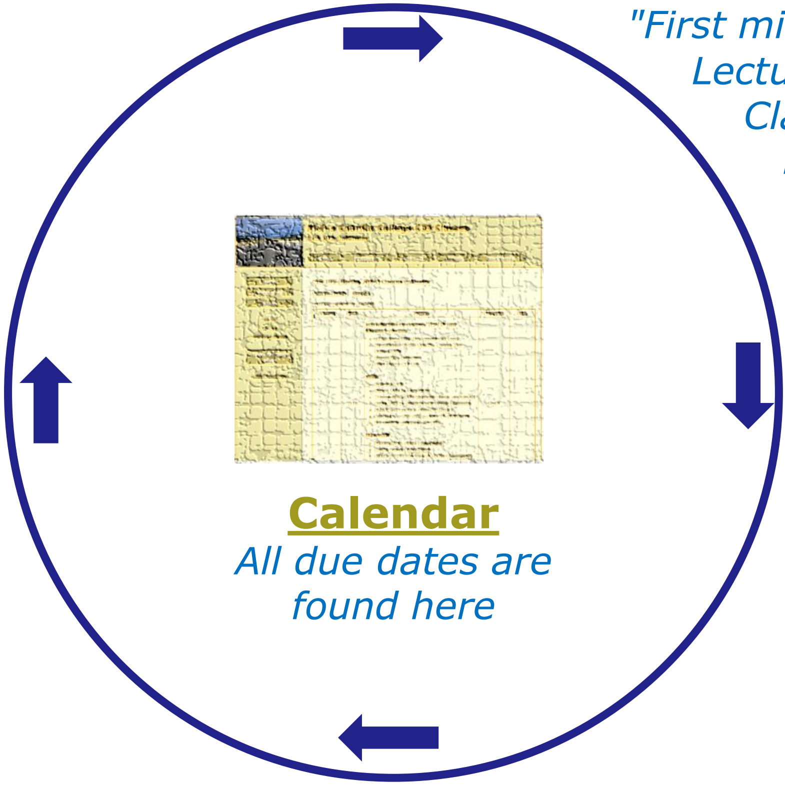
Tuesday

"First minute" quiz

Lecture on new lesson material

Class activities

Previous week lab assignments due 11:59PM (Opus time)

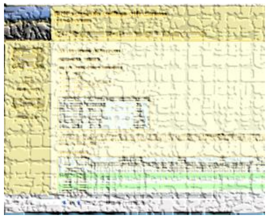


Calendar

All due dates are found here

Thursday

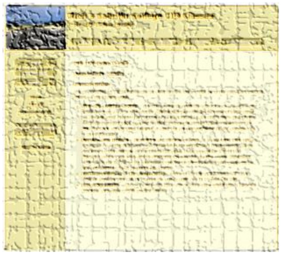
is grading day



Check the **Grades** *page to see grades on labs, quizzes and tests*

Work on labs or practice tests during the week.

All assignments and due dates are on the **Calendar** *page*



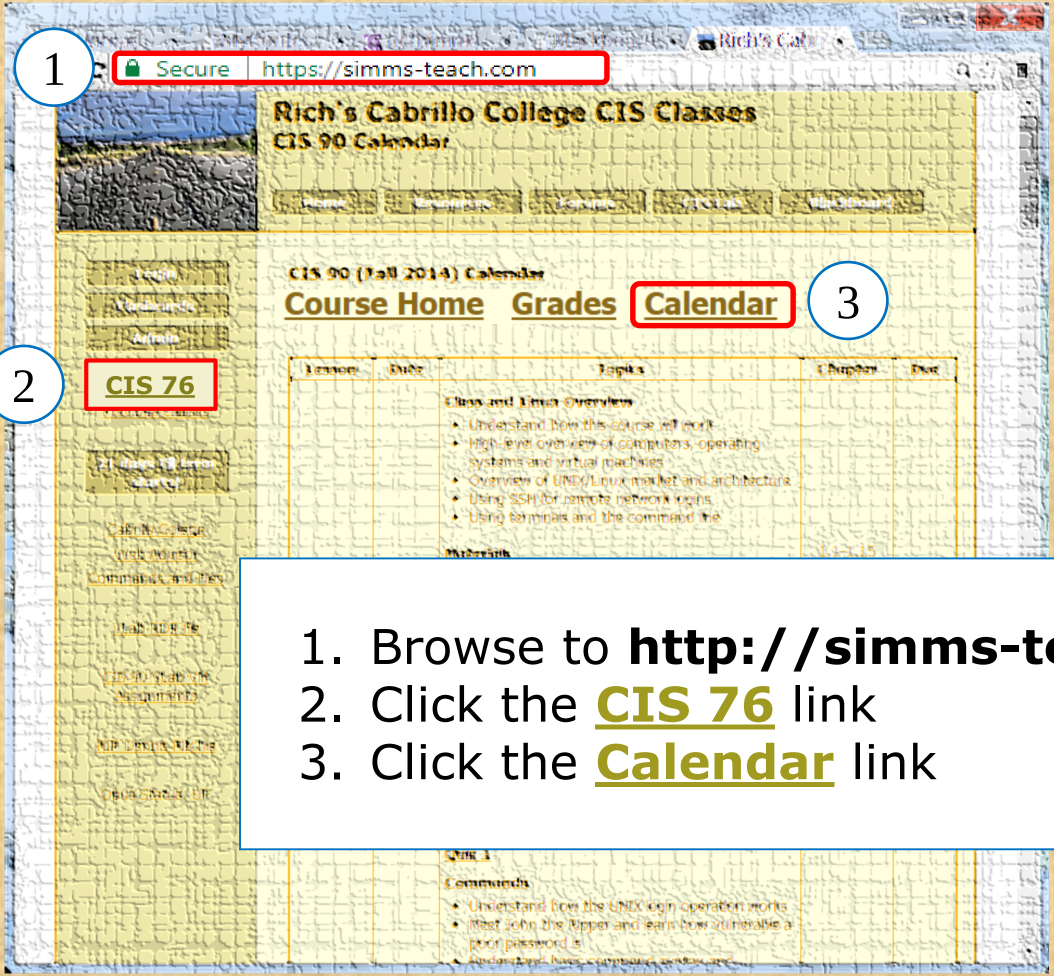
Peek at the **Extra Credit** *page if you need more points*

Contacting the instructor

- Use the forum for the fastest response on technical or class related questions.
- Use email for personal matters. If it's not personal I will probably encourage you to post your question on the forum so I can answer it there. This is preferable because your other classmates can benefit from the answer.
- Weekly office hours: http://babyface.cabrillo.edu/salsa/listing.jsp?staffId=1426
- Avoid leaving a message on voice mail. Checked rarely so don't expect a fast response (if any)!

simms-teach.com

Find the Calendar page



Secure https://simms-teach.com

Rich's Cabrillo College CIS Classes
CIS 90 Calendar

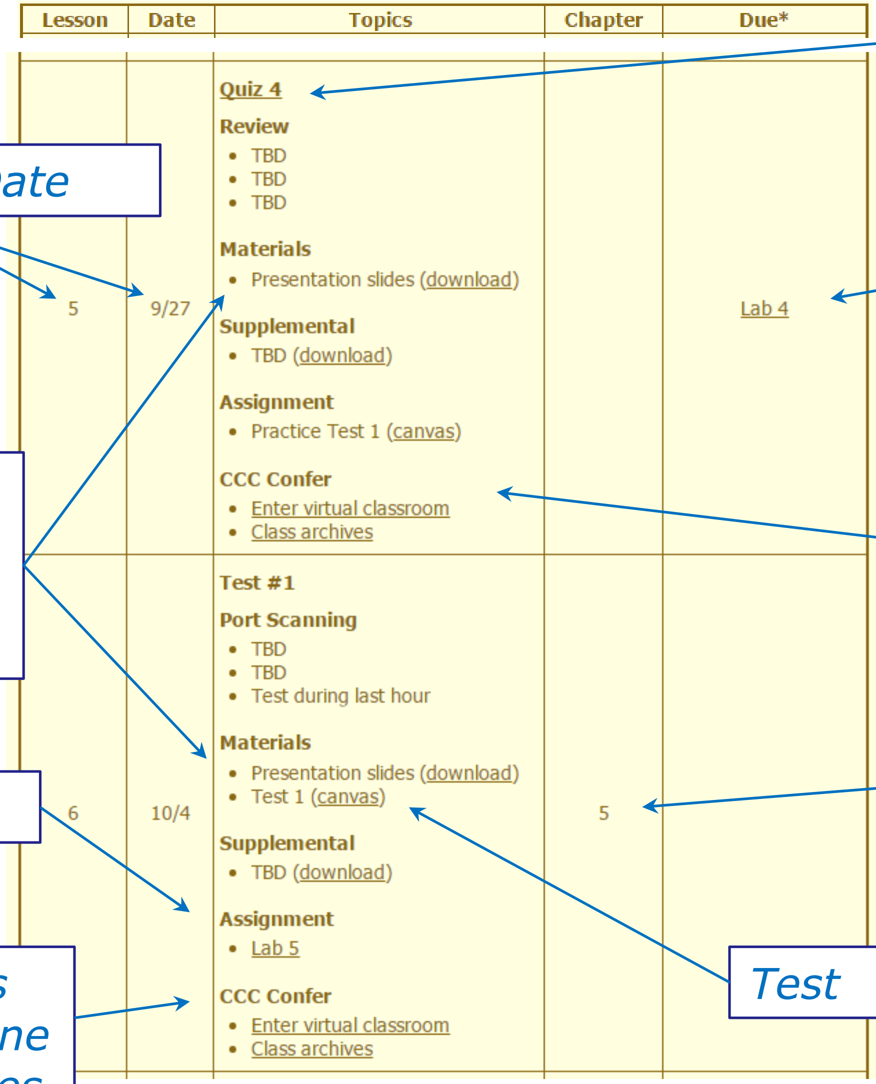
CIS 90 (Fall 2014) Calendar

Course Home Grades Calendar

Lesson	Date	Topics	Chapter	Due
		Class and Linux Overview • Understand how this course will work • High-level overview of computers, operating systems and virtual machines • Overview of UNIX/Linux market and architecture • Using SSH for remote network logins • Using terminals and the command line Materials	1.1-1.15	
		Quiz 1 Commands • Understand how the UNIX login operation works • Meet John the Ripper and learn how vulnerable a poor password is		

1. Browse to **http://simms-teach.com**
2. Click the **CIS 76** link
3. Click the **Calendar** link

Course Calendar



Lesson	Date	Topics	Chapter	Due*
5	9/27	**Quiz 4** **Review** • TBD • TBD • TBD **Materials** • Presentation slides (download) **Supplemental** • TBD (download) **Assignment** • Practice Test 1 (canvas) **CCC Confer** • Enter virtual classroom • Class archives		Lab 4
6	10/4	**Test #1** **Port Scanning** • TBD • TBD • Test during last hour **Materials** • Presentation slides (download) • Test 1 (canvas) **Supplemental** • TBD (download) **Assignment** • Lab 5 **CCC Confer** • Enter virtual classroom • Class archives	5	

First minute quiz

Lesson # and Date

What is due by 11:59PM (Opus time) on that date (LATE WORK IS NOT ACCEPTED)

Lesson slides, feel free to download during class for local viewing

Links to virtual classroom and archived recordings

References to material in the textbook

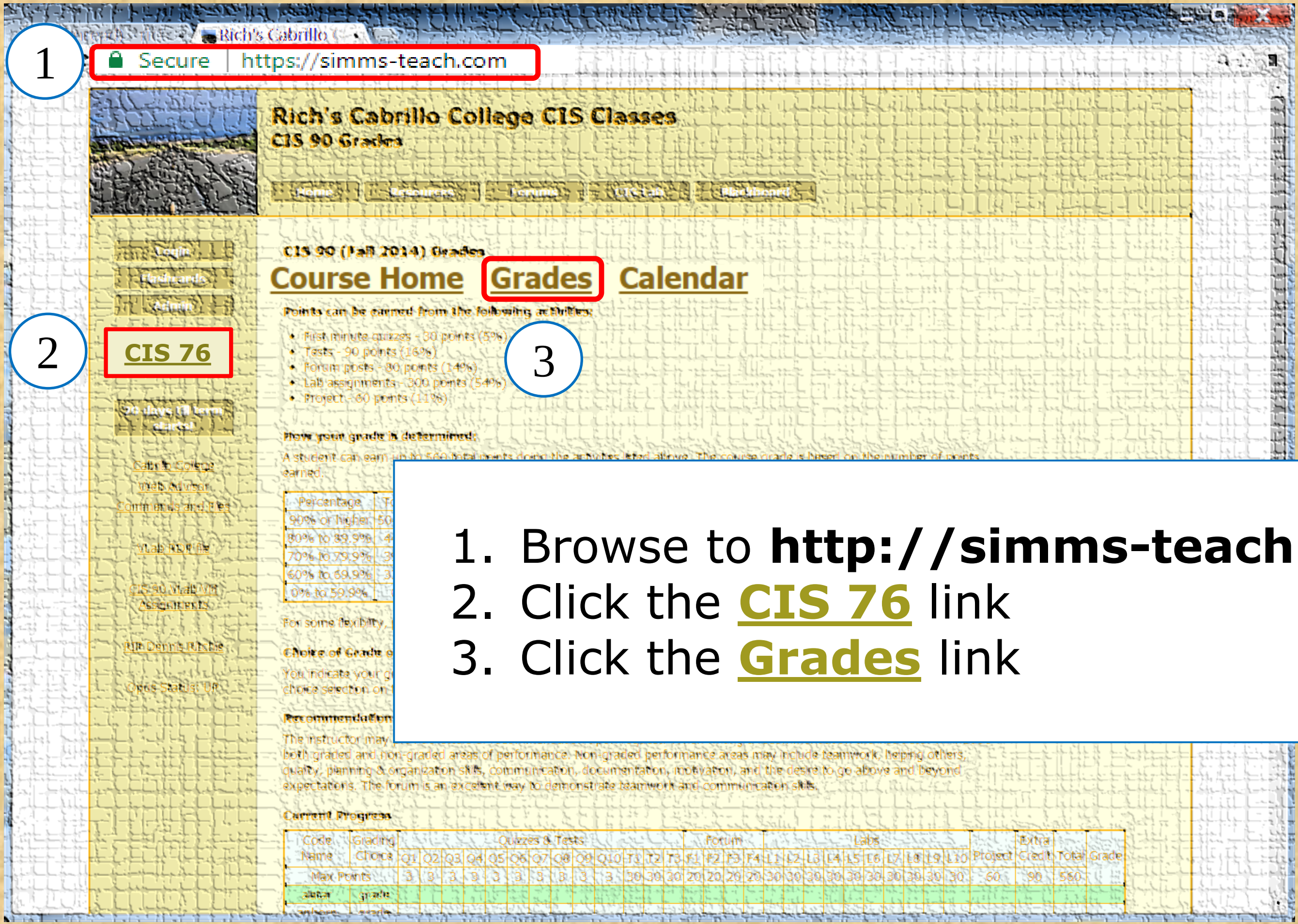
Lab assignment

CCC Confer links to join class online or review archives

Test

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

simms-teach.com
Find the Grades page



Secure | https://simms-teach.com

Rich's Cabrillo College CIS Classes
CIS 90 Grades

CIS 90 (Fall 2014) Grades

Course Home Grades Calendar

CIS 76

Points can be earned from the following activities:

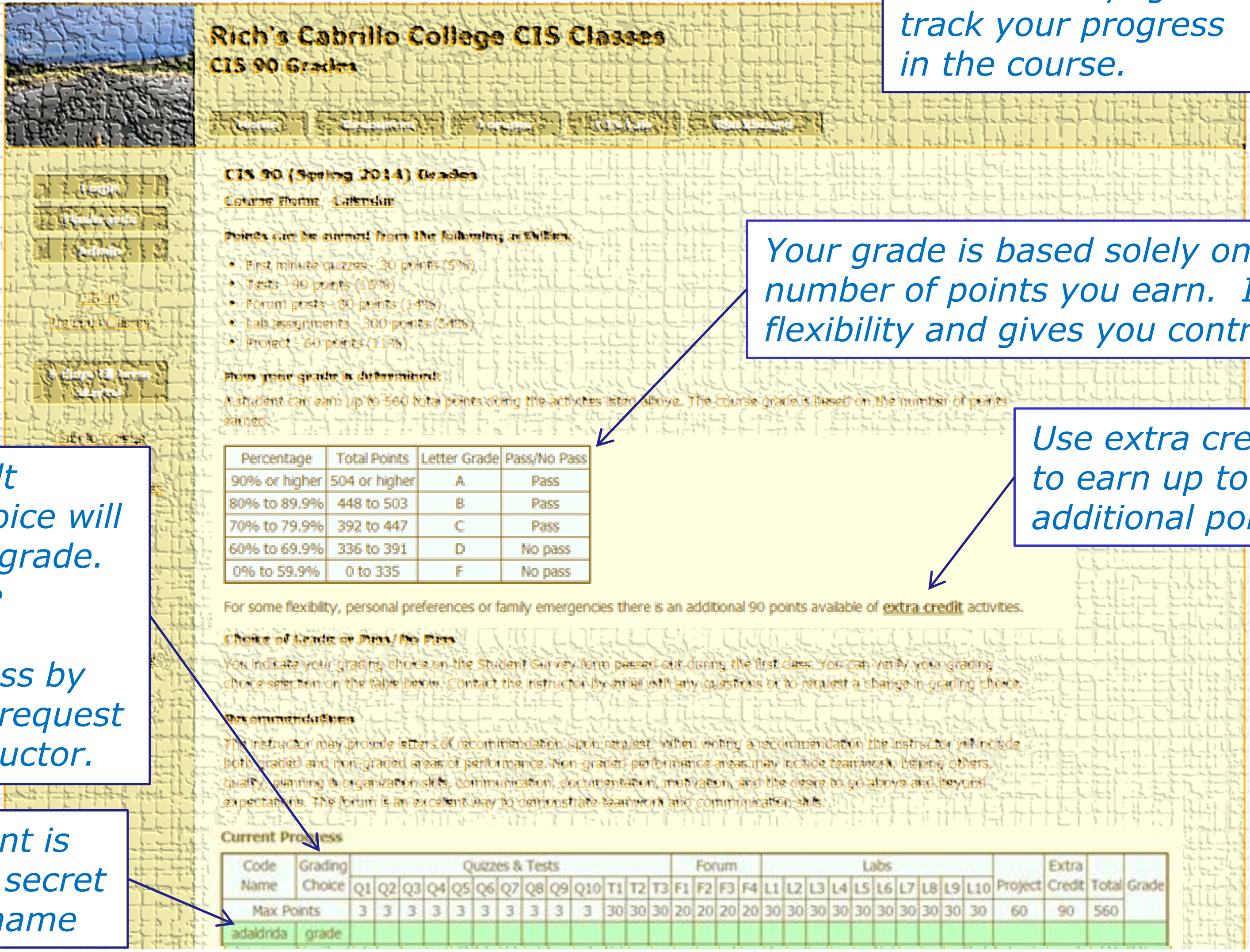
- First minute quizzes - 30 points (5%)
- Tests - 90 points (16%)
- Forum posts - 80 points (14%)
- Lab assignments - 300 points (54%)
- Project - 60 points (11%)

How your grade is determined:

Current Progress

1. Browse to **http://simms-teach.com**
2. Click the **CIS 76** link
3. Click the **Grades** link

Course Grading



Rich's Cabrillo College CIS Classes

CIS 90 Grades

CIS 90 (Spring 2014) Grades

Course Home Calendar

Points can be earned from the following activities:

- First minute quizzes - 30 points (5%)
- Tests - 90 points (16%)
- Forum posts - 80 points (14%)
- Lab assignments - 300 points (54%)
- Project - 60 points (11%)

How your grade is determined:

A student can earn up to 560 total points doing the activites listed above. The course grade is based on the number of points earned.

Percentage	Total Points	Letter Grade	Pass/No Pass
90% or higher	504 or higher	A	Pass
80% to 89.9%	448 to 503	B	Pass
70% to 79.9%	392 to 447	C	Pass
60% to 69.9%	336 to 391	D	No pass
0% to 59.9%	0 to 335	F	No pass

For some flexiblity, personal preferences or family emergencies there is an additional 90 points available of extra credit activities.

Choice of Grade or Pass/No Pass

You indicate your grading choice on the Student Survey form passed out during the first class. You can verify your grading choice selection on the table below. Contact the instructor by email with any questions or to request a change in grading choice.

Recommendations

The instructor may provide letters of recommendation upon request. When writing a recommendation the instructor will include both graded and non-graded areas of performance. Non-graded performance areas may include teamwork, helping others, quality, planning & organization skills, communication, documentation, motivation, and the desire to go above and beyond expectations. The forum is an excellent way to demonstrate teamwork and communication skills.

Current Progress

Code Name	Grading Choice	Quizzes & Tests													Forum				Labs										Project	Extra Credit	Total	Grade
		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	T1	T2	T3	F1	F2	F3	F4	L1	L2	L3	L4	L5	L6	L7	L8	L9	L10				
Max Points		3	3	3	3	3	3	3	3	3	3	30	30	30	20	20	20	20	30	30	30	30	30	30	30	30	30	30	60	90	560	
adaldrida	grade																															

Monitor this page to track your progress in the course.

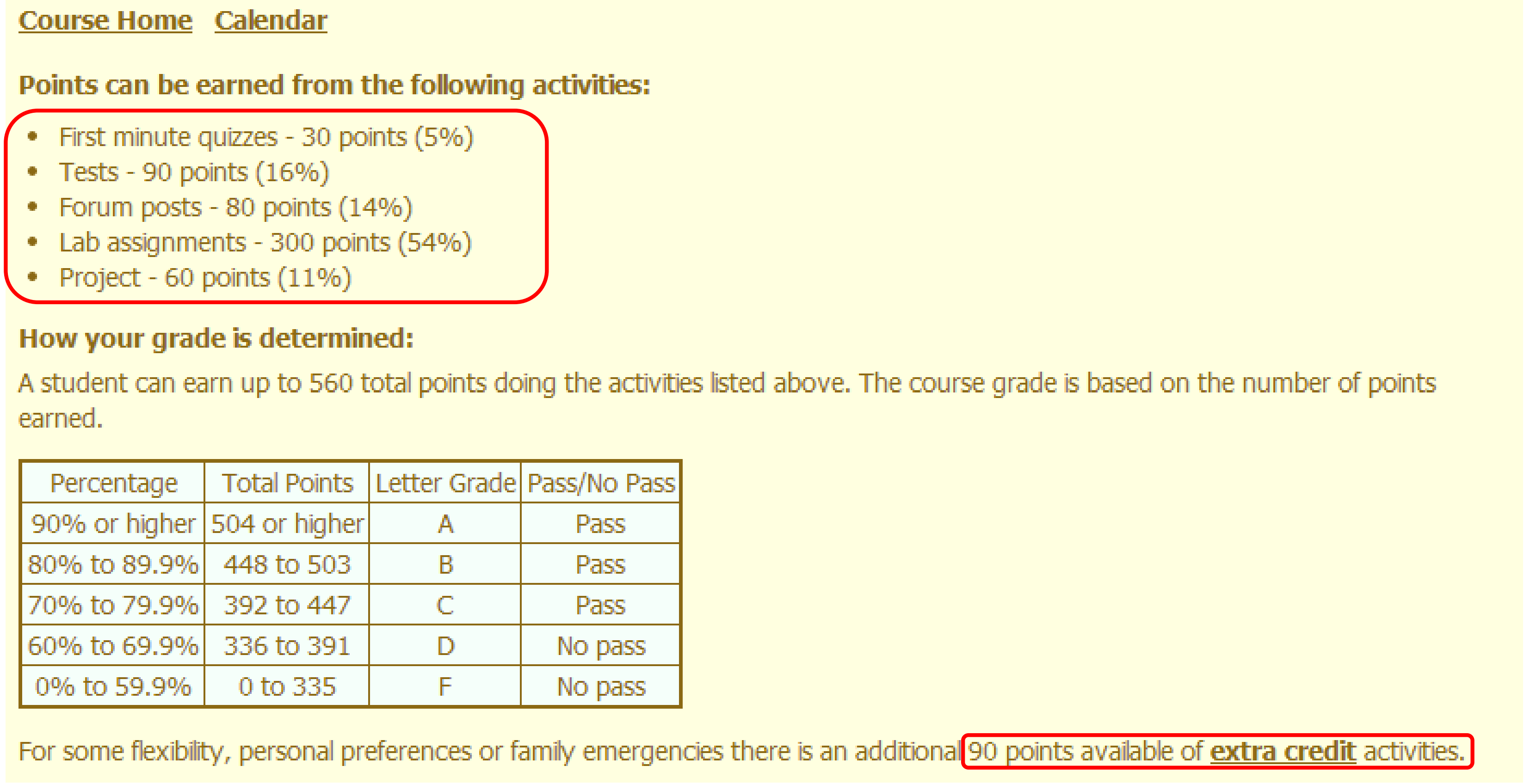
Your grade is based solely on the number of points you earn. It offers flexibility and gives you control.

Use extra credit to earn up to 90 additional points

Your default grading choice will be a letter grade. This can be changed to Pass/No Pass by emailing a request to the instructor.

Each student is assigned a secret LOR code name

More on Grading



Course Home Calendar

Points can be earned from the following activities:

- First minute quizzes - 30 points (5%)
- Tests - 90 points (16%)
- Forum posts - 80 points (14%)
- Lab assignments - 300 points (54%)
- Project - 60 points (11%)

How your grade is determined:

A student can earn up to 560 total points doing the activities listed above. The course grade is based on the number of points earned.

Percentage	Total Points	Letter Grade	Pass/No Pass
90% or higher	504 or higher	A	Pass
80% to 89.9%	448 to 503	B	Pass
70% to 79.9%	392 to 447	C	Pass
60% to 69.9%	336 to 391	D	No pass
0% to 59.9%	0 to 335	F	No pass

For some flexibility, personal preferences or family emergencies there is an additional 90 points available of **extra credit** activities.

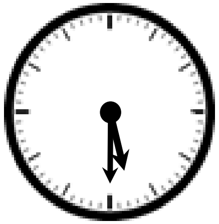
You control your grade. The more points you earn the higher your grade will be.

Grading - Lab Assignments

- 10 labs, 30 points each
- Due at 11:59PM (Opus time) on the date shown on the course Calendar.
- Late work is not accepted. There is no credit for any work turned in after the deadline. If you don't complete a lab assignment, please turn in what you have, by the due date, for partial credit.
- Students may work together and collaborate on labs but they must submit their own work to get credit.
- Lab resources, instructors, and assistants are available in the CIS lab. In addition the Linux Opus server and the CIS VLab may be accessed from anywhere over the Internet.

*A lab assignment due at 11:59PM will get **no credit** if turned in **one minute late** at 12:00AM which is midnight the next day!*

Grading - First Minute Quizzes



- 10 quizzes, 3 points each

- The quiz questions are shown on CCC Confer at 5:30PM sharp. Answers are emailed to the instructor. The order of the questions will not be known until the quiz is given! Emailed answers that are not in order will be marked as incorrect.

- The quiz questions are given out in advance and students can use the forum to collaborate on answers prior to class.

- Quizzes are open book/notes. Students may not give or ask others for assistance while taking a quiz.

- There are NO makeup's for these quizzes and they must be taken and turned in within the first few minutes of class. Answers emailed after the first few minutes of class will not get credit.

- Students that attend by watching the archives can do some extra credit work instead. In the past many working students have joined the class briefly at the start just to take the quiz and then return to work.

An incentive to start class on time

Grading - Tests

- 3 tests, 30 points each
- Tests are timed. ☹
- A practice test will be made available a week before the actual test. ☺
- Tests 1 and 2 will be held during the last hour of class on the days shown on the Calendar.
- Working students have the option to take tests 1 and 2 later in the day but they must be completed no later than 11:59PM (Opus time) on the day of the test.
- Test 3 is the final exam and is mandatory. The time of the final exam is shown on the Calendar.
- Tests are open notes, open book, and open computer.
- Students may not give or ask others for assistance while taking a test.
- Tests may be taken remotely online.

Timed tests are more difficult due to the time pressure! They do help me understand what you have learned so I can adjust the course as needed.

Grading - Forum Posts

- 4 points per post, up to 20 points maximum per "posting quarter".
- The end date for each posting quarter is shown on the course calendar.
- The posts for the quarter will be due at 11:59PM (Opus time) on the date shown on the course Calendar.
- Extra posts in one quarter do not carry over to the next quarter.
- Only posts in the CIS 76 class forum will be counted.

As far as earning points, forum posts are "low hanging fruit" !!

Grading - Extra Credit

- Up to 90 points
- You need to attend to a family emergency and can't turn in a lab assignment on time … don't worry!
- Your schedule/commute doesn't allow you to take any of the "first minute" quizzes …. don't worry!
- You get anxious, panic and forget everything you know on a test … don't worry!
- You just don't like making forum posts … don't worry!

There are ample extra credit opportunities which provide you with the flexibility to get the grade you want.

There is a cap on extra credit points so plan carefully!

Making the fine print LARGE (and red)

Please remember:

1) No makeup's for missed quizzes.

2) Quiz answers in the wrong order or not emailed in the first few minutes will not be accepted.

3) Late work will not be accepted. For example, a lab assignment due at 11:59PM will get no credit if turned in **one minute late** at 12:00AM (midnight) the next day.

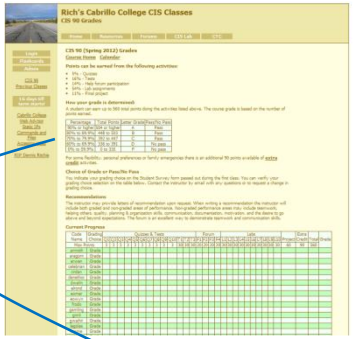
Tip: if you have not completed a lab assignment, **please turn in what you have done for partial credit.**

Don’t panic though -- there are ample extra credit opportunities for students wanting or needing any extra points.

Final word on Grading

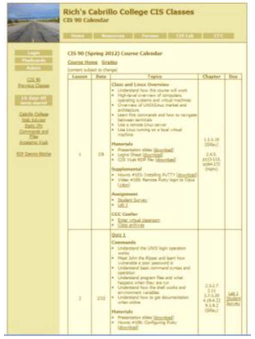
- You control your grade for this course!
- Use the **Grades** web page to plan for the grade you wish to receive and track your progress.
- Use the **Calendar** web page to see due dates for ALL lab assignments, extra credit labs and forum posts. See when EVERY quiz and test is scheduled.

Grades

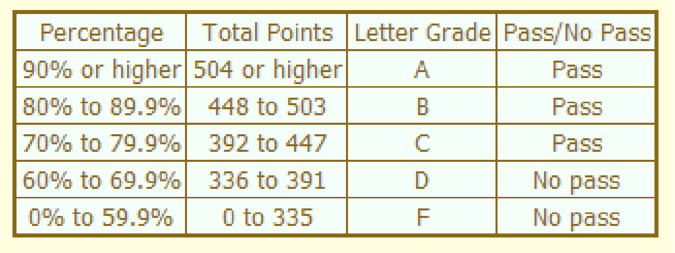


Rich's Cabrillo College CIS Classes
CIS 90 Grades

Calendar



Rich's Cabrillo College CIS Classes
CIS 90 Calendar

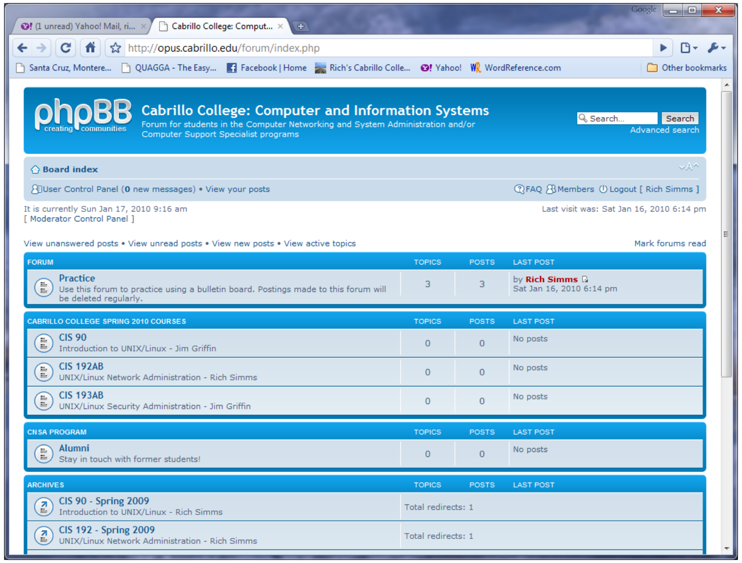


Percentage	Total Points	Letter Grade	Pass/No Pass
90% or higher	504 or higher	A	Pass
80% to 89.9%	448 to 503	B	Pass
70% to 79.9%	392 to 447	C	Pass
60% to 69.9%	336 to 391	D	No pass
0% to 59.9%	0 to 335	F	No pass

At the end of the course the instructor will count the number of points you have earned and use this table on the Grades web page to determine your grade.

Help Forum

Online Help Forum



http://opus.cabrillo.edu/forum/index.php

Cabrillo College: Computer and Information Systems
Forum for students in the Computer Networking and System Administration and/or Computer Support Specialist programs

Board index

User Control Panel (**0** new messages) • View your posts

FAQ Members Logout [Rich Simms]

It is currently Sun Jan 17, 2010 9:16 am
[Moderator Control Panel]

Last visit was: Sat Jan 16, 2010 6:14 pm

View unanswered posts • View unread posts • View new posts • View active topics

Mark forums read

FORUM	TOPICS	POSTS	LAST POST
Practice Use this forum to practice using a bulletin board. Postings made to this forum will be deleted regularly.	3	3	by **Rich Simms** Sat Jan 16, 2010 6:14 pm

CABRILLO COLLEGE SPRING 2010 COURSES	TOPICS	POSTS	LAST POST
CIS 90 Introduction to UNIX/Linux - Jim Griffin	0	0	No posts
CIS 192AB UNIX/Linux Network Administration - Rich Simms	0	0	No posts
CIS 193AB UNIX/Linux Security Administration - Jim Griffin	0	0	No posts

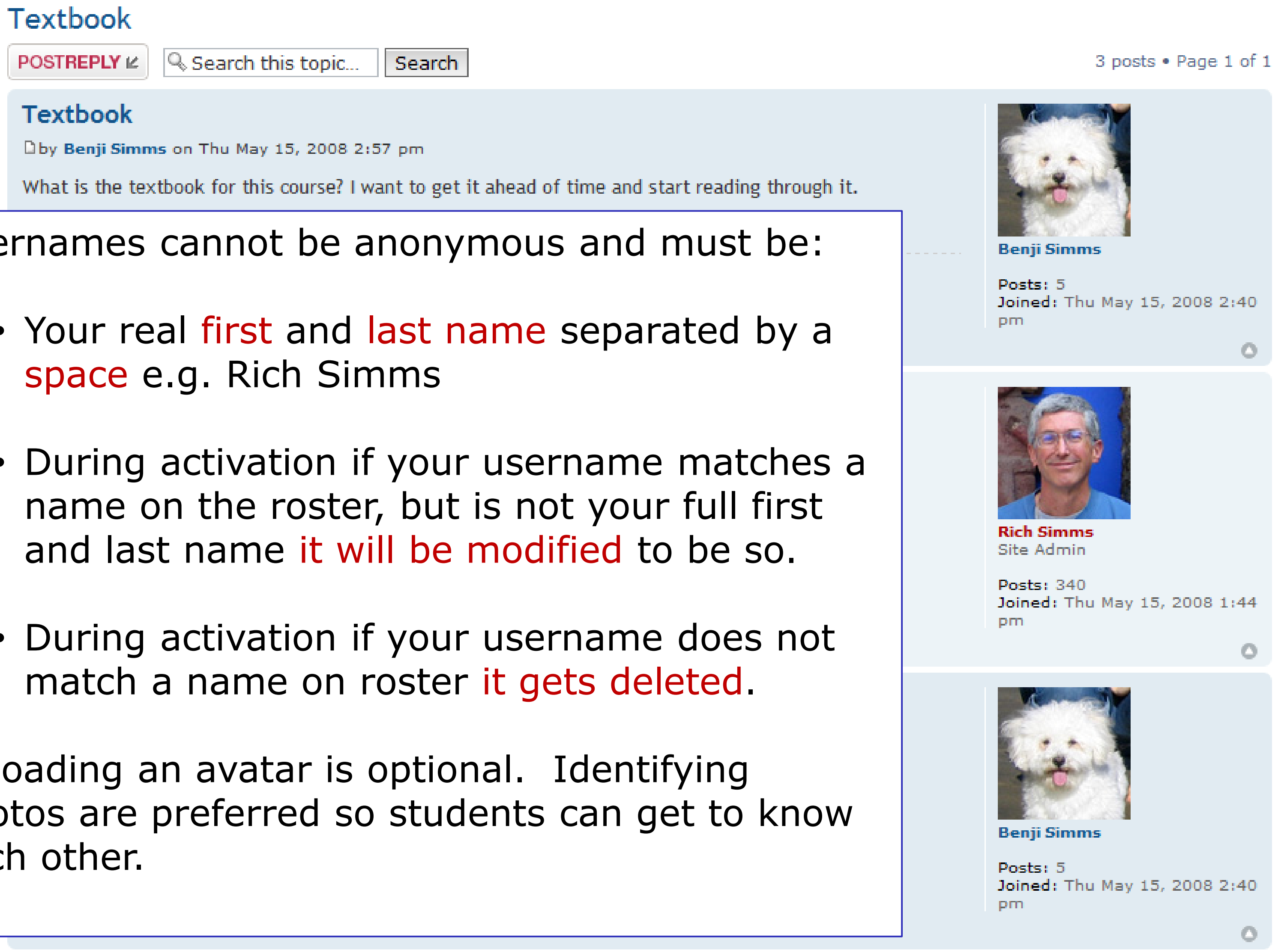
CNSA PROGRAM	TOPICS	POSTS	LAST POST
Alumni Stay in touch with former students!	0	0	No posts

ARCHIVES	TOPICS	POSTS	LAST POST
CIS 90 - Spring 2009 Introduction to UNIX/Linux - Rich Simms	Total redirects: 1		
CIS 192 - Spring 2009 UNIX/Linux Network Administration - Rich Simms	Total redirects: 1		

- Ask and answer questions.
- Get clarifications on assignments.
- Collaborate with classmates on assignments, quizzes and practice tests.
- Share ethical hacking news and ideas.
- Never post passwords!

As an incentive to use the forum - students can earn 4 points per CIS 76 forum post (capped at 20 points for each posting period)

Class Forum



Textbook

3 posts • Page 1 of 1

Textbook

by Benji Simms on Thu May 15, 2008 2:57 pm

What is the textbook for this course? I want to get it ahead of time and start reading through it.

Benji Simms

Posts: 5
Joined: Thu May 15, 2008 2:40 pm

Rich Simms
Site Admin

Posts: 340
Joined: Thu May 15, 2008 1:44 pm

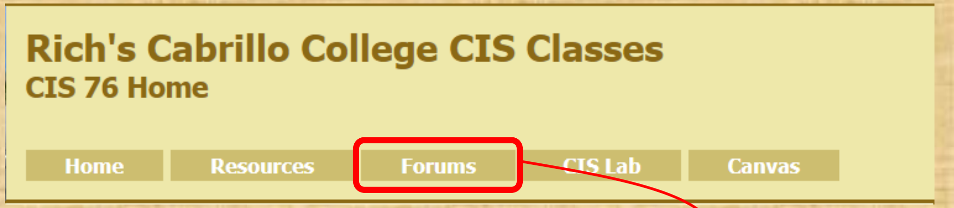
Benji Simms

Posts: 5
Joined: Thu May 15, 2008 2:40 pm

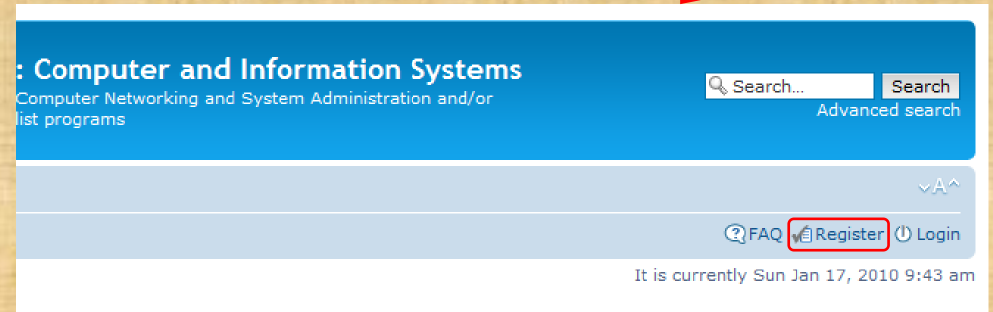
- Usernames cannot be anonymous and must be:
  - Your real first and last name separated by a space e.g. Rich Simms
  - During activation if your username matches a name on the roster, but is not your full first and last name it will be modified to be so.
  - During activation if your username does not match a name on roster it gets deleted.
- Uploading an avatar is optional. Identifying photos are preferred so students can get to know each other.

Class Activity
Forum Registration

Click the Forums link on
http://**simms-teach.com**



Rich's Cabrillo College CIS Classes
CIS 76 Home



: Computer and Information Systems
Computer Networking and System Administration and/or
list programs

It is currently Sun Jan 17, 2010 9:43 am

To Register:

1. Browse to the forum
2. Click on ✓ Register
3. Review and agree to terms
4. Your **Username** must:
   - be your first and last name separated by a space
   - e.g. Benji Simms
   - match a name on the class roster

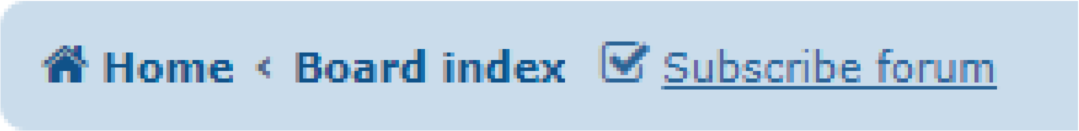
Note: All registrations are manually approved by the instructor. If your username is incomplete or does not match a name of the class roster it will be modified or deleted.

Class Forum

Subscribe to the forum to get email notifications of new posts

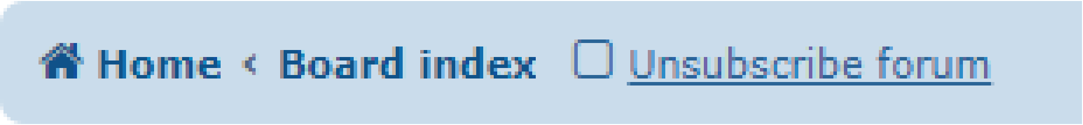
After logging in:

1. Go to the CIS 76 class forum.
2. Click the "Subscribe forum" box at the lower left. When subscribed you get email notifications when new posts are made.
3. To unsubscribe, click it again.



Home ‹ Board index ☑ Subscribe forum

Unsubscribed looks like this.



Home ‹ Board index □ Unsubscribe forum

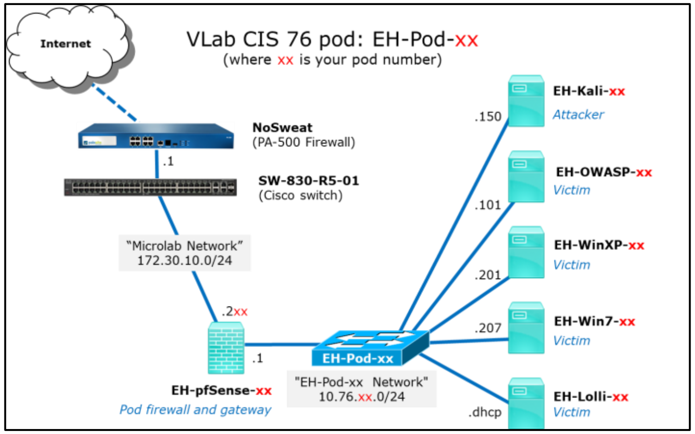
Subscribed looks like this.

Lab Resources

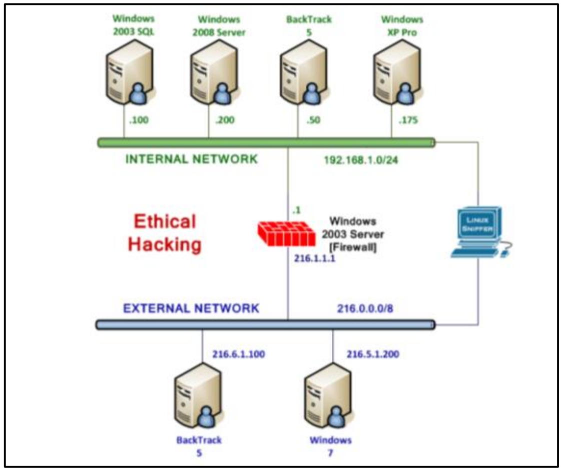
CIS 76 Resources

Opus

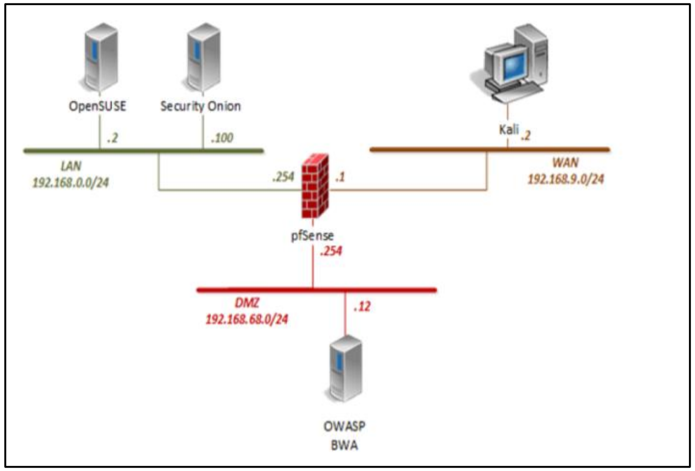
VLab CIS 76 Pod



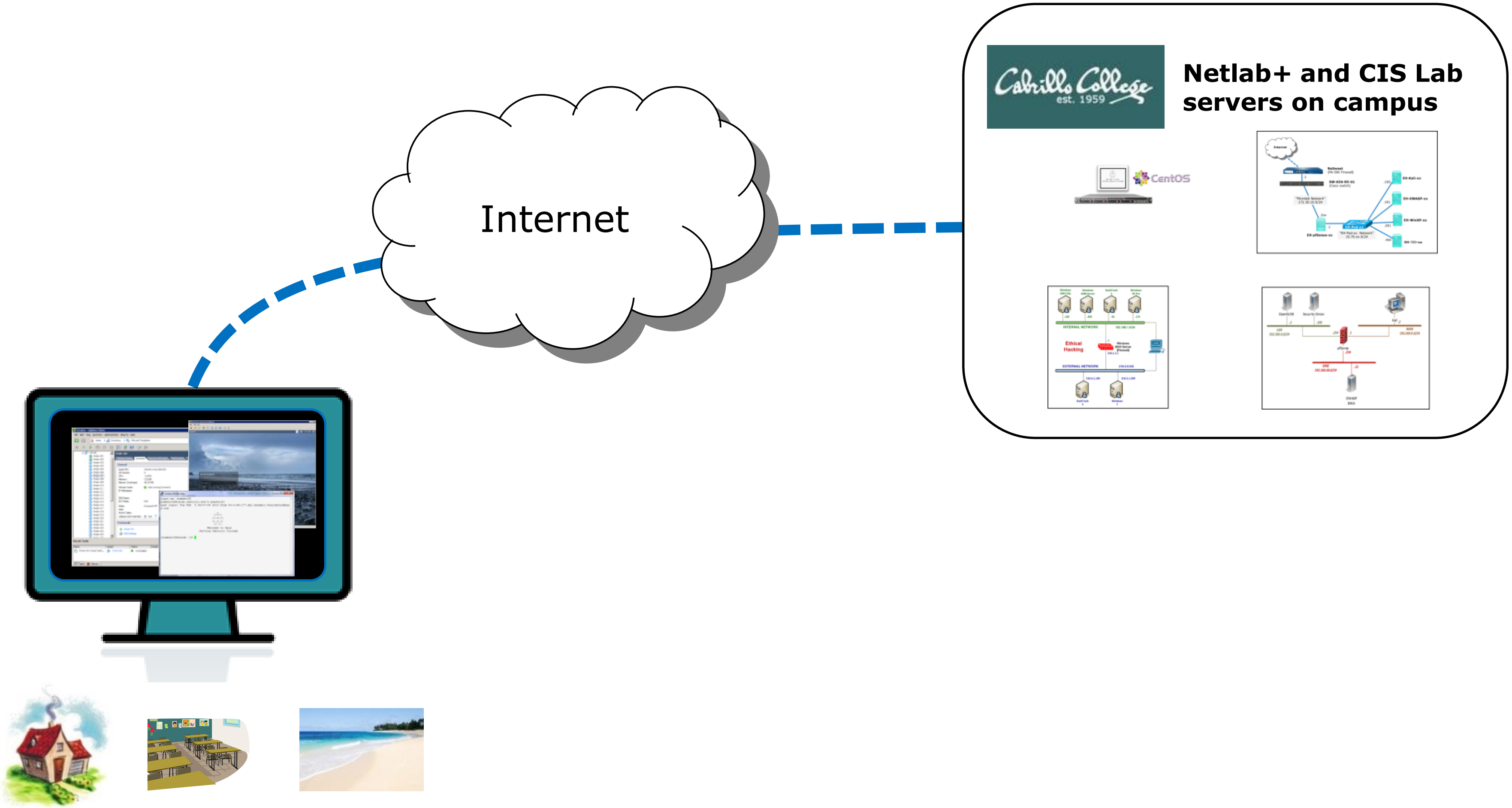
Netlab+ NISGTC Ethical Hacking Pod (2015)



Netlab+ NDG Ethical Hacking Pod (2016)



Option 1: Work on assignments online from anywhere



Internet

Netlab+ and CIS Lab servers on campus

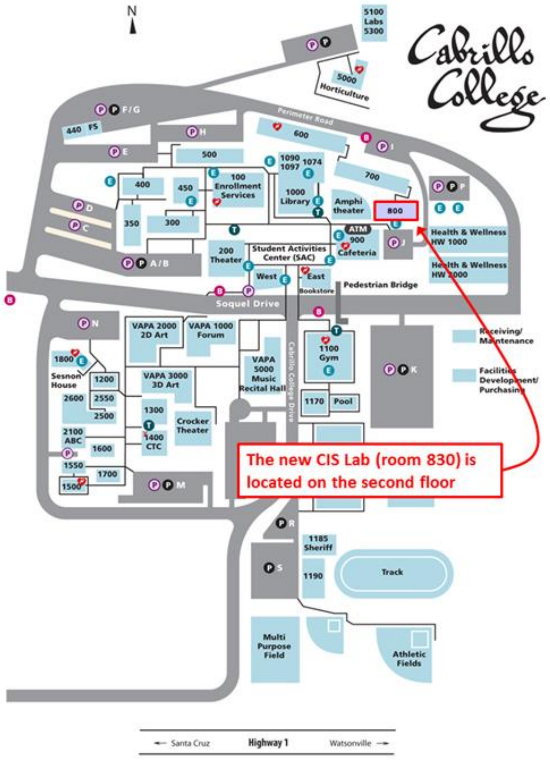
Home

School

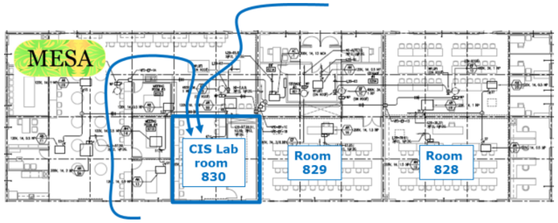
Travel

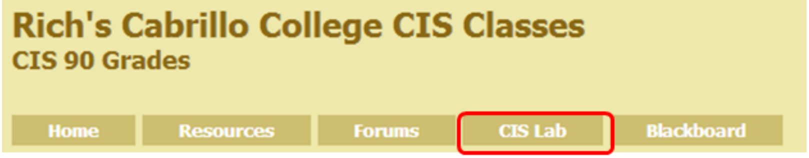
Option 2: Work on assignments in the CIS Lab

Building 800 - Room 830 (in the STEM Center)



The new CIS Lab (room 830) is located on the second floor




Rich's Cabrillo College CIS Classes

CIS 90 Grades

Use this link to see the schedule and location

Instructors, lab assistants and equipment are available CIS students.

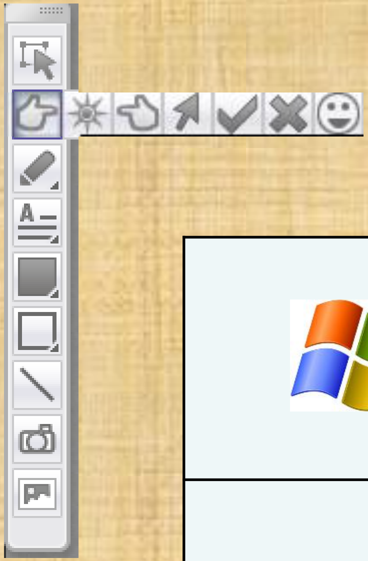
Great place to collaborate with classmates and a place for study groups to meet.

Housekeeping

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

Instructor Note:

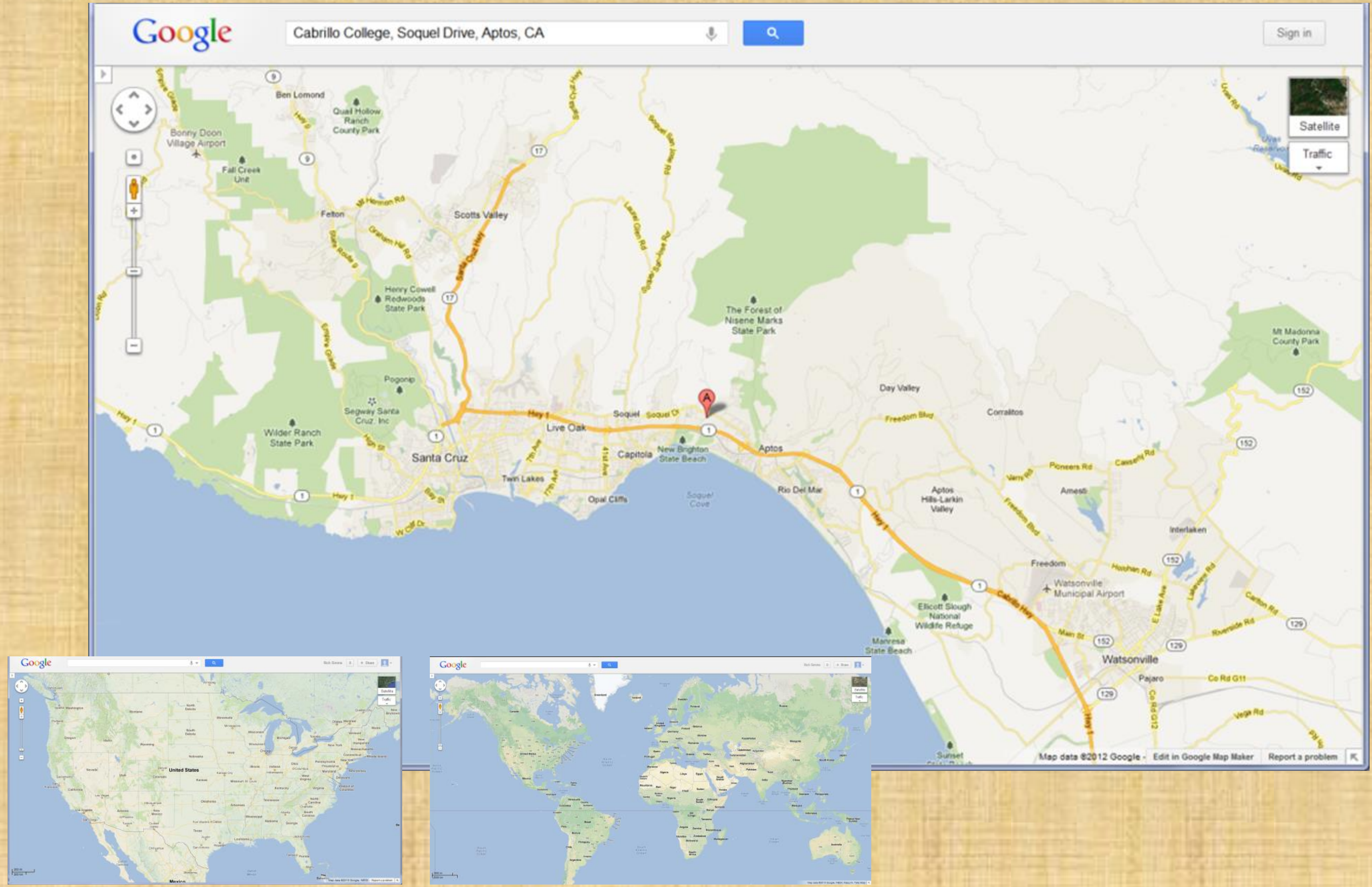
Switch to preloaded whiteboard



Class Activity
What kind of computer did you use to join CCC Confer?

⊞		🐧	Other

Class Activity – Where are you now?



Cabrillo College, Soquel Drive, Aptos, CA

Roll Call

If you are attending class by watching the recordings in the archives, email the instructor at: risimms@cabrillo.edu to provide roll call attendance.

Login Credentials

Usernames and passwords

The Login Credentials are not included in these lesson slides.

To locate a copy, login into Canvas (https://cabrillo.instructure.com) and read the Welcome announcement.

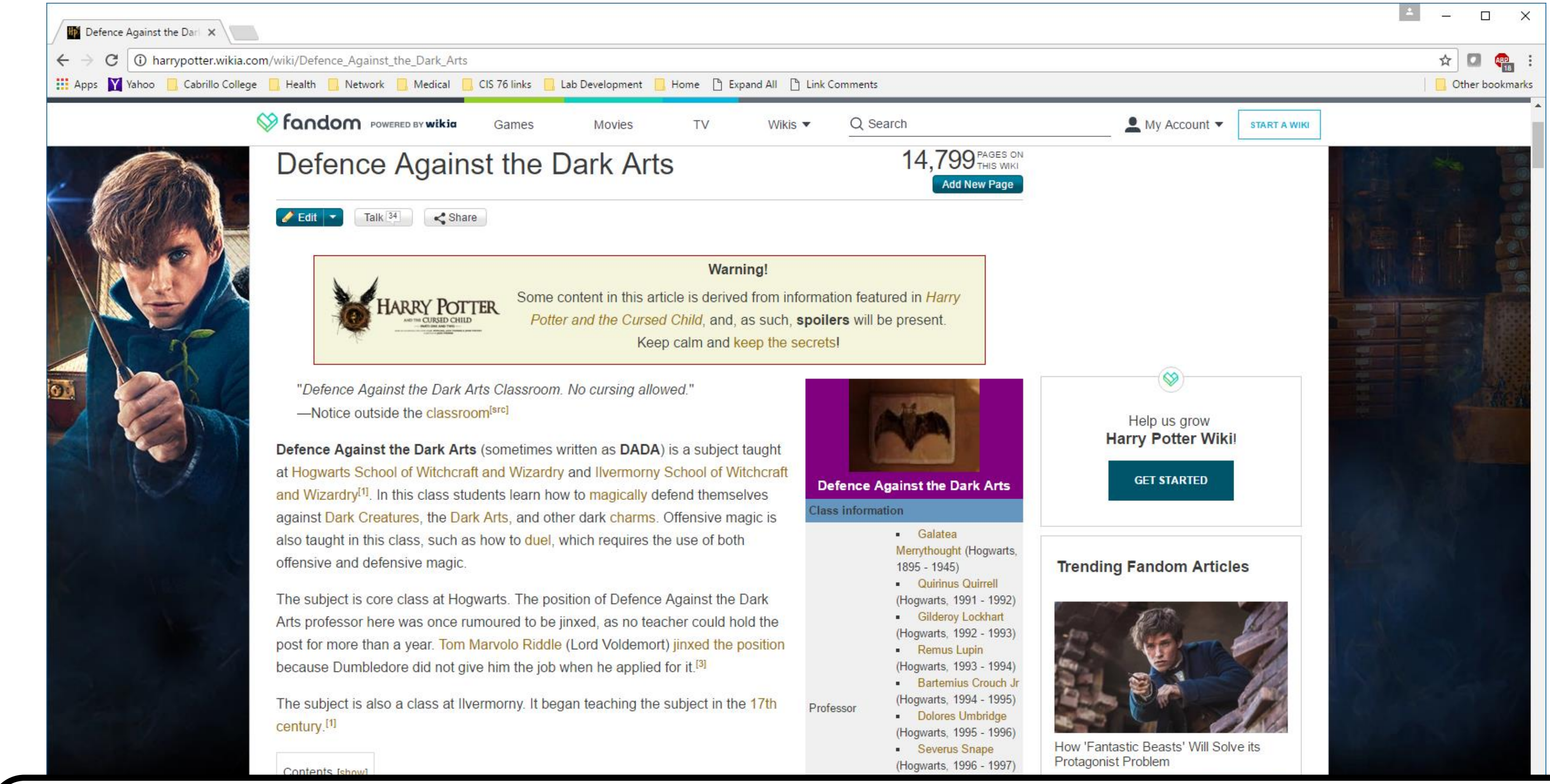
Instructor Note:

Turn Recording On, Switch back to shared slides

Ethical Hacking Overview

WARNING

Cognitive Overload Ahead



Defence Against the Dark Arts

Warning!

Some content in this article is derived from information featured in *Harry Potter and the Cursed Child*, and, as such, **spoilers** will be present.

Keep calm and keep the secrets!

> *"Defence Against the Dark Arts Classroom. No cursing allowed."*
> —Notice outside the classroom[src]

Defence Against the Dark Arts (sometimes written as **DADA**) is a subject taught at Hogwarts School of Witchcraft and Wizardry and Ilvermorny School of Witchcraft and Wizardry[1]. In this class students learn how to magically defend themselves against Dark Creatures, the Dark Arts, and other dark charms. Offensive magic is also taught in this class, such as how to duel, which requires the use of both offensive and defensive magic.

The subject is core class at Hogwarts. The position of Defence Against the Dark Arts professor here was once rumoured to be jinxed, as no teacher could hold the post for more than a year. Tom Marvolo Riddle (Lord Voldemort) jinxed the position because Dumbledore did not give him the job when he applied for it.[3]

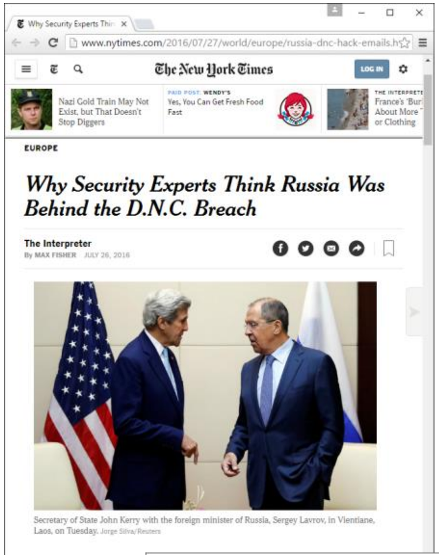
The subject is also a class at Ilvermorny. It began teaching the subject in the 17th century.[1]

Defence Against the Dark Arts	
Class information	
Professor	Galatea Merrythought (Hogwarts, 1895 - 1945) Quirinus Quirrell (Hogwarts, 1991 - 1992) Gilderoy Lockhart (Hogwarts, 1992 - 1993) Remus Lupin (Hogwarts, 1993 - 1994) Bartemius Crouch Jr (Hogwarts, 1994 - 1995) Dolores Umbridge (Hogwarts, 1995 - 1996) Severus Snape (Hogwarts, 1996 - 1997)

"Your defences must therefore be as flexible and inventive as the arts you seek to undo"
—Professor Snape discussing defence during a 1996 lesson

http://harrypotter.wikia.com/wiki/Defence_Against_the_Dark_Arts

In the News



Why Security Experts Thi

www.nytimes.com/2016/07/27/world/europe/russia-dnc-hack-emails.h

The New York Times

Nazi Gold Train May Not Exist, but That Doesn't Stop Diggers

PAID POST: WENDY'S Yes, You Can Get Fresh Food Fast

THE INTERPRETER France's 'Bur About More or Clothing

EUROPE

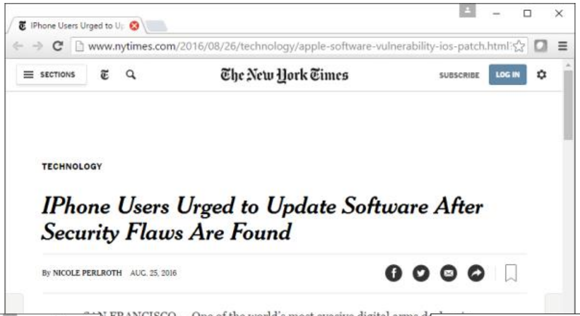
Why Security Experts Think Russia Was Behind the D.N.C. Breach

The Interpreter

By MAX FISHER JULY 26, 2016

Secretary of State John Kerry with the foreign minister of Russia, Sergey Lavrov, in Vientiane, Laos, on Tuesday. Jorge Silva/Reuters

https://http
016/07/27/
dnc-hack-e



IPhone Users Urged to U

www.nytimes.com/2016/08/26/technology/apple-software-vulnerability-ios-patch.html

SECTIONS

The New York Times

SUBSCRIBE LOG IN

TECHNOLOGY

IPhone Users Urged to Update Software After Security Flaws Are Found

By NICOLE PERLROTH AUG. 25, 2016

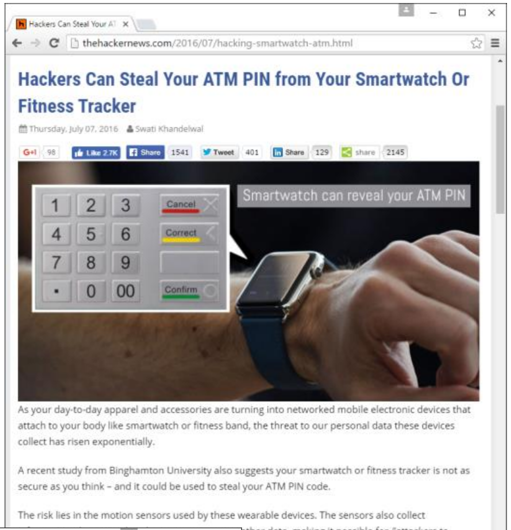
SAN FRANCISCO — One of the world's most evasive digital arms de
eved to have been taking advantage of three security vulnerabili
ular Apple products in its efforts to spy on dissidents and journa

estigators discovered that a company called the NSO Group, an I
fit that sells software that invisibly tracks a target's mobile phon
ponsible for the intrusions. The NSO Group's software can read t
ssages and emails and track calls and contacts. It can even recor
nds, collect passwords and trace the whereabouts of the phone u

esponse, Apple on Thursday released a patched version of its m
ware, iOS 9.3.5. Users can get the patch through a normal softw
late.

ble fixed the holes 10 days after a tip from two researchers, Bill M
John Scott Railton, at Citizen Lab at the University of Toronto's

/http://www.nytimes.com/201
gy/apple-software-vulnerability
tml?_r=0



Hackers Can Steal Your A

thehackernews.com/2016/07/hacking-smartwatch-atm.html

Hackers Can Steal Your ATM PIN from Your Smartwatch Or Fitness Tracker

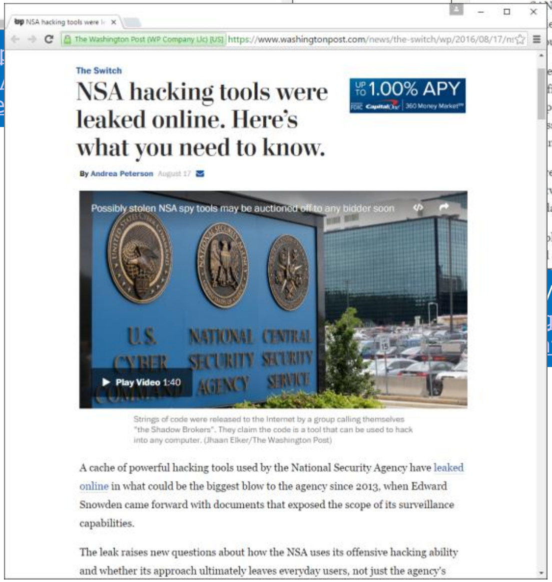
Thursday, July 07, 2016 Swati Khandelwal

As your day-to-day apparel and accessories are turning into networked mobile electronic devices that attach to your body like smartwatch or fitness band, the threat to our personal data these devices collect has risen exponentially.

A recent study from Binghamton University also suggests your smartwatch or fitness tracker is not as secure as you think – and it could be used to steal your ATM PIN code.

The risk lies in the motion sensors used by these wearable devices. The sensors also collect
other data, making it possible for "attackers to
over secret key entries."

ckernews.com/2016/0
ch-atm.html



NSA hacking tools were

The Washington Post (WP Company LLC) [US] https://www.washingtonpost.com/news/the-switch/wp/2016/08/17/n

The Switch

NSA hacking tools were leaked online. Here's what you need to know.

By Andrea Peterson August 17

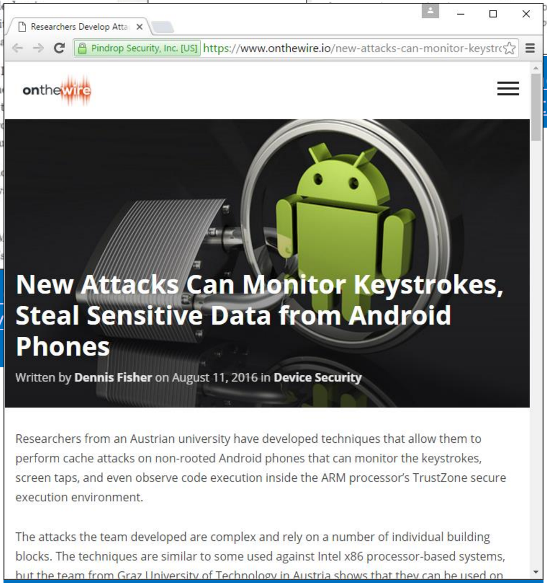
Possibly stolen NSA spy tools may be auctioned off to any bidder soon
Play Video 1:40

Strings of code were released to the Internet by a group calling themselves "the Shadow Brokers". They claim the code is a tool that can be used to hack into any computer. (Jhaan Elker/The Washington Post)

A cache of powerful hacking tools used by the National Security Agency have leaked online in what could be the biggest blow to the agency since 2013, when Edward Snowden came forward with documents that exposed the scope of its surveillance capabilities.

The leak raises new questions about how the NSA uses its offensive hacking ability and whether its approach ultimately leaves everyday users, not just the agency's

https://https://www.washingtonpost.com/news/the-switch/wp/2016/08/17/nsa-hacking-tools-were-leaked-online-heres-what-you-need-to-know/



Researchers Develop Atta

Pindrop Security, Inc. [US] https://www.onthewire.io/new-attacks-can-monitor-keystro

onthewire

New Attacks Can Monitor Keystrokes, Steal Sensitive Data from Android Phones

Written by Dennis Fisher on August 11, 2016 in Device Security

Researchers from an Austrian university have developed techniques that allow them to perform cache attacks on non-rooted Android phones that can monitor the keystrokes, screen taps, and even observe code execution inside the ARM processor's TrustZone secure execution environment.

The attacks the team developed are complex and rely on a number of individual building blocks. The techniques are similar to some used against Intel x86 processor-based systems, but the team from Graz University of Technology in Austria shows that they can be used on

https://https://www.onthewire.io/new-attacks-can-monitor-keystrokes-steal-sensitive-data-from-android-phones/

In the News

Politics

The curious case of 'Nicole Mincey,' the Trump fan who may actually be a bot

A look at the second half, so far, of President Trump's first year in office

https://https://
s/the-curious-
fan-who-may-
bot/2017/08/0
4a0a64977c92
cf649

12 MAY 17 U.K. Hospitals Hit in Widespread Ransomware Attack

At least 16 hospitals in the United Kingdom are being forced to divert emergency patients today after computer systems there were infected with ransomware, a type of malicious software that encrypts a victim's documents, images, music and other files unless the victim pays for a key to unlock them.

It remains unclear exactly how this ransomware strain is being disseminated and why it appears to have spread so quickly, but there are indications the malware may be spreading to vulnerable systems through a security hole in **Windows** that was recently patched by **Microsoft**.

https://https://krebsonsecurity.com
hospitals-hit-in-widespread-ransom

Critical RCE Vulnerability Found in Cisco WebEx Extensions, Again — Patch Now!

Monday, July 17, 2017 Swati Khandelwal

ns' WebEx browser extension for
ow attackers to remotely execute

017/07/cisco-

Report: Hackers Leak More 'Game Of Thrones' Plot Details

Along with an HBO executive's emails.

By Sara Boboltz

https://http://www.huffingtonpost.com/entry/hackers-leak-more-game-ofthrones-plot-details_us_5988e1b3e4b0a66b8bae06da?g1q

THE WALL STREET JOURNAL.
SUBSCRIBE
SIGN IN
Iraqi Forces Seize Tal Afar From Islamic State
Woman Dies From Injuries in Barcelona Van Attack

WORLD | ASIA

North Korea's Army of Hackers Has a New Target: Bank Accounts

Emphasis on finances represents a significant shift from Pyongyang's prior patterns of attack

By Timothy W. Martin

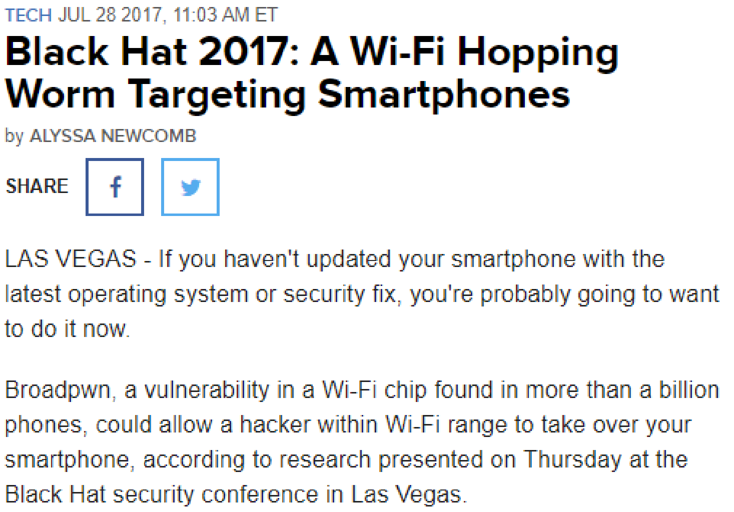
Updated July 27, 2017 2:34 p.m. ET

SEOUL—North Korea's cyberarmy has splintered into multiple groups and is unleashing orchestrated attacks increasingly focused on funneling stolen

https://https://www.wsj.com/articles/north-korean-hackers-hunt-for-cash-1501128326

Recent Conferences

Black Hat July 2017



TECH JUL 28 2017, 11:03 AM ET

Black Hat 2017: A Wi-Fi Hopping Worm Targeting Smartphones

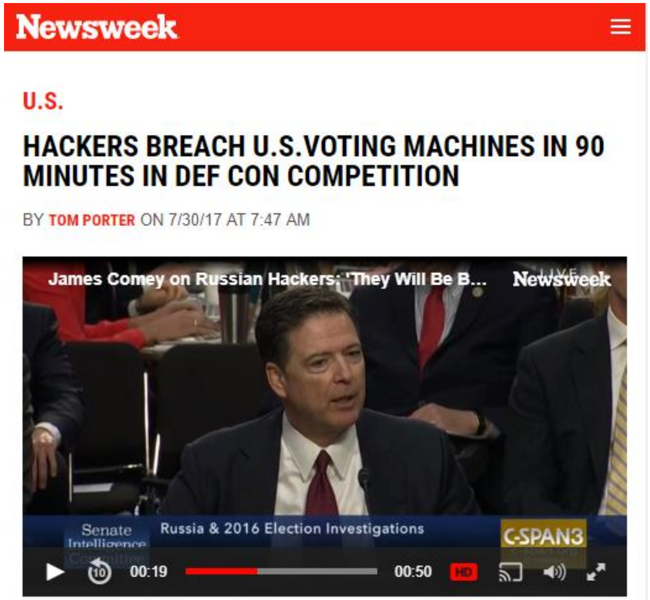
by ALYSSA NEWCOMB

LAS VEGAS - If you haven't updated your smartphone with the latest operating system or security fix, you're probably going to want to do it now.

Broadpwn, a vulnerability in a Wi-Fi chip found in more than a billion phones, could allow a hacker within Wi-Fi range to take over your smartphone, according to research presented on Thursday at the Black Hat security conference in Las Vegas.

https://https://www.nbcnews.com/tech/security/black-hat-2017-wi-fi-hopping-worm-targeting-smartphones-n787301

Def Con July 2017



Newsweek

U.S.

HACKERS BREACH U.S.VOTING MACHINES IN 90 MINUTES IN DEF CON COMPETITION

BY TOM PORTER ON 7/30/17 AT 7:47 AM

James Comey on Russian Hackers: 'They Will Be B...
Newsweek
Senate Intelligence Committee
Russia & 2016 Election Investigations
C-SPAN3
00:19
00:50
HD

https://http://www.newsweek.com/hackers-breach-usvoting-machines-90-minutes-def-con-competition-643858

White Hats

What is an Ethical Hacker?

1. An authorized security professional who uses the same tools as unethical "black hat" hackers to test and evaluate an organization's security infrastructure for vulnerabilities.

2. Also known as a "security tester", "penetration tester" or "white hat" hacker who may also be a member of a "red team".

3. An ethical hacker:
   - Only hacks with "end-to-end" authorization.
   - Abides by all state and federal laws.
   - Respects the privacy and protects any information discovered.
   - Discloses unknown hardware or software product vulnerabilities to the appropriate vendors or authorities.
   - When finished leaves nothing open for themselves or others to exploit in the future.
   - Provides a confidential report to the client on all vulnerabilities found.

References:
http://www.computerhope.com/jargon/e/ethihack.htm
http://panmore.com/ethical-hacking-code-of-ethics-security-risk-issues
https://www.sans.org/reading-room/whitepapers/auditing/red-teaming-art-ethical-hacking-1272

EC-Council Code of Ethics

1. Keep private and confidential information gained in your professional work, (in particular as it pertains to client lists and client personal information). Not collect, give, sell, or transfer any personal information (such as name, e-mail address, Social Security number, or other unique identifier) to a third party without client prior consent.
2. Protect the intellectual property of others by relying on your own innovation and efforts, thus ensuring that all benefits vest with its originator.
3. Disclose to appropriate persons or authorities potential dangers to any ecommerce clients, the Internet community, or the public, that you reasonably believe to be associated with a particular set or type of electronic transactions or related software or hardware.
4. Provide service in your areas of competence, being honest and forthright about any limitations of your experience and education. Ensure that you are qualified for any project on which you work or propose to work by an appropriate combination of education, training, and experience.
5. Never knowingly use software or process that is obtained or retained either illegally or unethically.
6. Not to engage in deceptive financial practices such as bribery, double billing, or other improper financial practices.
7. Use the property of a client or employer only in ways properly authorized, and with the owner’s knowledge and consent.
8. Disclose to all concerned parties those conflicts of interest that cannot reasonably be avoided or escaped.
9. Ensure good management for any project you lead, including effective procedures for promotion of quality and full disclosure of risk.
10. Add to the knowledge of the e-commerce profession by constant study, share the lessons of your experience with fellow EC-Council members, and promote public awareness of benefits of electronic commerce.
11. Conduct oneself in the most ethical and competent manner when soliciting professional service or seeking employment, thus meriting confidence in your knowledge and integrity.
12. Ensure ethical conduct and professional care at all times on all professional assignments without prejudice.
13. Not to neither associate with malicious hackers nor engage in any malicious activities.
14. Not to purposefully compromise or allow the client organization’s systems to be compromised in the course of your professional dealings.
15. Ensure all penetration testing activities are authorized and within legal limits.
16. Not to take part in any black hat activity or be associated with any black hat community that serves to endanger networks.
17. Not to be part of any underground hacking community for purposes of preaching and expanding black hat activities.
18. Not to make inappropriate reference to the certification or misleading use of certificates, marks or logos in publications, catalogues, documents or speeches.
19. Not convicted in any felony, or violated any law of the land.

Source: https://www.eccouncil.org/code-of-ethics/

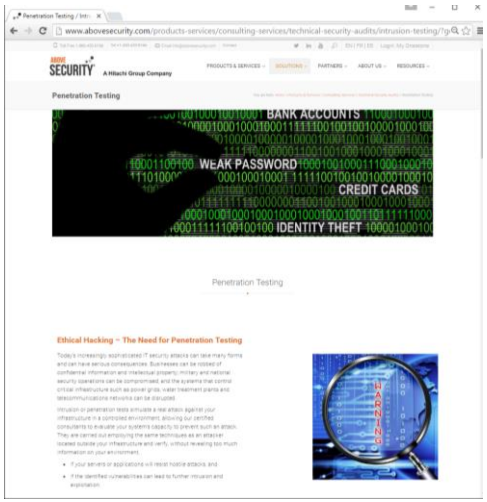
An ethical penetration test involves:

- Written agreements
  - Scope
  - Rules of engagement
  - Testing process
  - Protecting data
  - Attackers knowledge of target: Black/Gray/White box
  - Target's knowledge of attack
  - Liability
  - Report
  - Payment terms
  - And more ...
- Non-disclosure agreements
- Legal review of all agreements

What happens if a critical business server crashes as the result of a penetration test?
How far will social engineering be used and on who?
How will exfiltrated evidence and reports be protected?
Who will be aware of the test?
And so on ...

Example Penetration Testing Services

Above Security



Penetration Testing / Intr...

www.abovesecurity.com/products-services/consulting-services/technical-security-audits/intrusion-testing/?g

Penetration Testing

Penetration Testing

Ethical Hacking – The Need for Penetration Testing

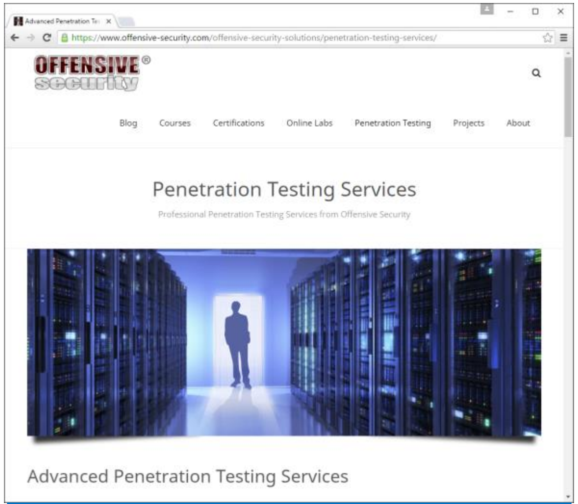
Today's increasingly sophisticated IT security attacks can take many forms and can have serious consequences. Businesses can be robbed of confidential information and intellectual property; military and national security operations can be compromised, and the systems that control critical infrastructure such as power grids, water treatment plants and telecommunications networks can be disrupted.

Intrusion or penetration tests simulate a real attack against your infrastructure in a controlled environment, allowing our certified consultants to evaluate your system's capacity to prevent such an attack. They are carried out employing the same techniques as an attacker located outside your infrastructure and verify, without revealing too much information on your environment:

- If your servers or applications will resist hostile attacks, and
- If the identified vulnerabilities can lead to further intrusion and exploitation.

http://www.abovesecurity.com/products-services/consulting-services/technical-security-audits/intrusion-testing

Offensive Security



Advanced Penetration Te...

https://www.offensive-security.com/offensive-security-solutions/penetration-testing-services/

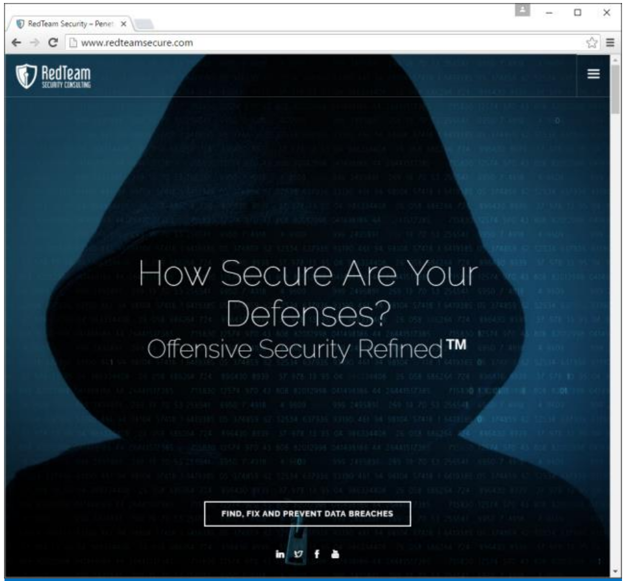
Penetration Testing Services

Professional Penetration Testing Services from Offensive Security

Advanced Penetration Testing Services

https://www.offensive-security.com/offensive-security-solutions/penetration-testing-services/

RedTeam Security



RedTeam Security – Penet...

www.redteamsecure.com

RedTeam SECURITY CONSULTING
FIND, FIX AND PREVENT DATA BREACHES

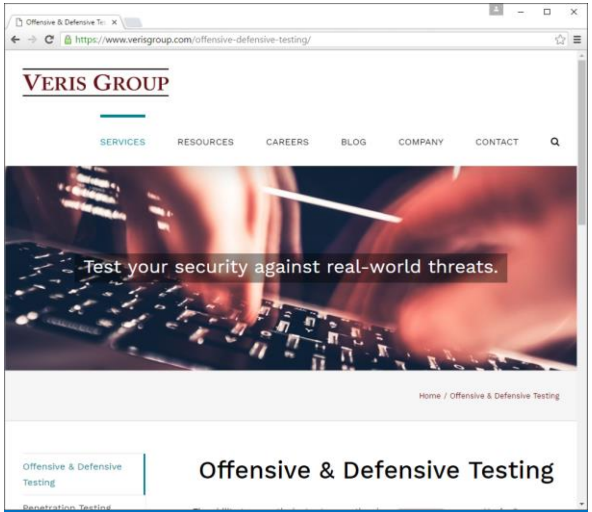
How Secure Are Your Defenses?

Offensive Security Refined™

http://www.redteamsecure.com/

Example Penetration Testing Services

Veris Group

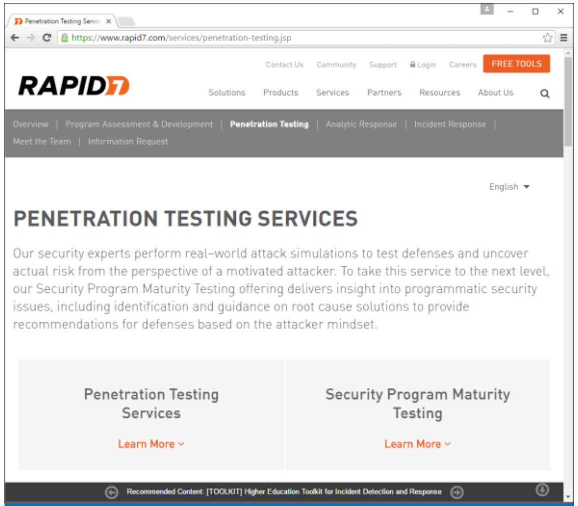

Offensive & Defensive Te
https://www.verisgroup.com/offensive-defensive-testing/
VERIS GROUP
SERVICES
RESOURCES
CAREERS
BLOG
COMPANY
CONTACT
Home / Offensive & Defensive Testing
Offensive & Defensive Testing
Penetration Testing

Test your security against real-world threats.

Offensive & Defensive Testing

https://www.verisgroup.com/offensive-defensive-testing/

Rapid7


Penetration Testing Servic
https://www.rapid7.com/services/penetration-testing.jsp
Contact Us
Community
Support
Login
Careers
FREE TOOLS
RAPID7
Solutions
Products
Services
Partners
Resources
About Us
Overview | Program Assessment & Development | Penetration Testing | Analytic Response | Incident Response | Meet the Team | Information Request
English
Learn More
Learn More

PENETRATION TESTING SERVICES

Our security experts perform real-world attack simulations to test defenses and uncover actual risk from the perspective of a motivated attacker. To take this service to the next level, our Security Program Maturity Testing offering delivers insight into programmatic security issues, including identification and guidance on root cause solutions to provide recommendations for defenses based on the attacker mindset.

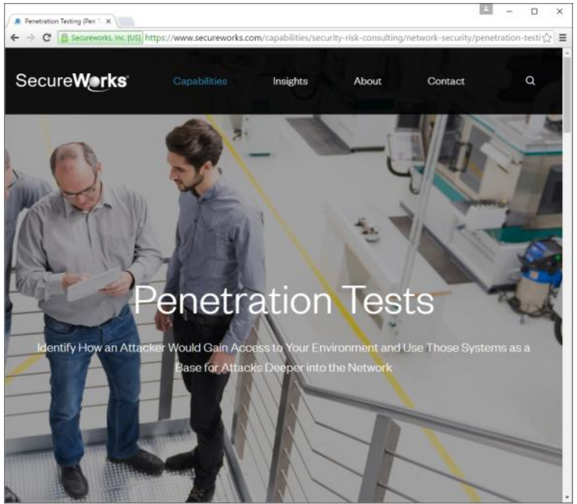
Penetration Testing Services

Security Program Maturity Testing

Recommended Content: [TOOLKIT] Higher Education Toolkit for Incident Detection and Response

https://www.rapid7.com/services/penetration-testing.jsp

SecureWorks

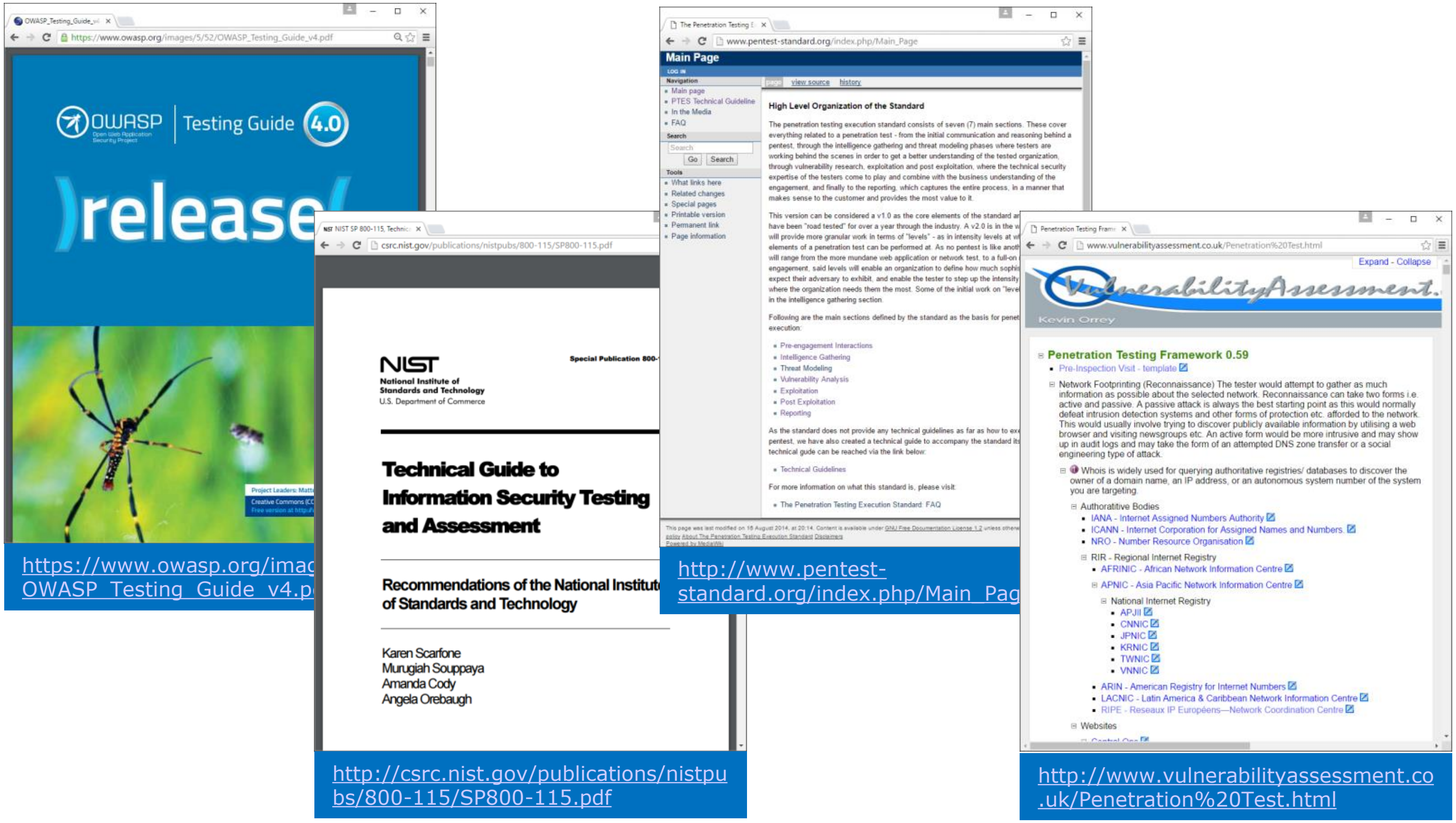

Penetration Testing (Pen T
Secureworks, Inc. [US] https://www.secureworks.com/capabilities/security-risk-consulting/network-security/penetration-testi
SecureWorks
Capabilities
Insights
About
Contact

Penetration Tests

Identify How an Attacker Would Gain Access to Your Environment and Use Those Systems as a Base for Attacks Deeper into the Network

https://www.secureworks.com/capabilities/security-risk-consulting/network-security/penetration-testing

Testing Methodologies



OWASP_Testing_Guide_v4
https://www.owasp.org/images/5/52/OWASP_Testing_Guide_v4.pdf
OWASP Open Web Application Security Project
Testing Guide 4.0
)release(
Project Leaders: Matt
Creative Commons (CC
Free version at http://

https://www.owasp.org/imag OWASP_Testing_Guide_v4.p

NIST SP 800-115, Technic
csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-

Technical Guide to Information Security Testing and Assessment

Recommendations of the National Institute of Standards and Technology

Karen Scarfone
Murugiah Souppaya
Amanda Cody
Angela Orebaugh

http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

High Level Organization of the Standard

The penetration testing execution standard consists of seven (7) main sections. These cover everything related to a penetration test - from the initial communication and reasoning behind a pentest, through the intelligence gathering and threat modeling phases where testers are working behind the scenes in order to get a better understanding of the tested organization, through vulnerability research, exploitation and post exploitation, where the technical security expertise of the testers come to play and combine with the business understanding of the engagement, and finally to the reporting, which captures the entire process, in a manner that makes sense to the customer and provides the most value to it.

This version can be considered a v1.0 as the core elements of the standard ar
have been "road tested" for over a year through the industry. A v2.0 is in the w
will provide more granular work in terms of "levels" - as in intensity levels at w
elements of a penetration test can be performed at. As no pentest is like anoth
will range from the more mundane web application or network test, to a full-on
engagement, said levels will enable an organization to define how much sophis
expect their adversary to exhibit, and enable the tester to step up the intensity
where the organization needs them the most. Some of the initial work on "leve
in the intelligence gathering section.

Following are the main sections defined by the standard as the basis for penet
execution:

- Pre-engagement Interactions
- Intelligence Gathering
- Threat Modeling
- Vulnerability Analysis
- Exploitation
- Post Exploitation
- Reporting

As the standard does not provide any technical guidelines as far as how to exe
pentest, we have also created a technical guide to accompany the standard its
technical gude can be reached via the link below:

- Technical Guidelines

For more information on what this standard is, please visit:

- The Penetration Testing Execution Standard: FAQ

This page was last modified on 16 August 2014, at 20:14. Content is available under GNU Free Documentation License 1.2 unless otherw
policy About The Penetration Testing Execution Standard Disclaimers
Powered by MediaWiki

http://www.pentest-standard.org/index.php/Main_Pag

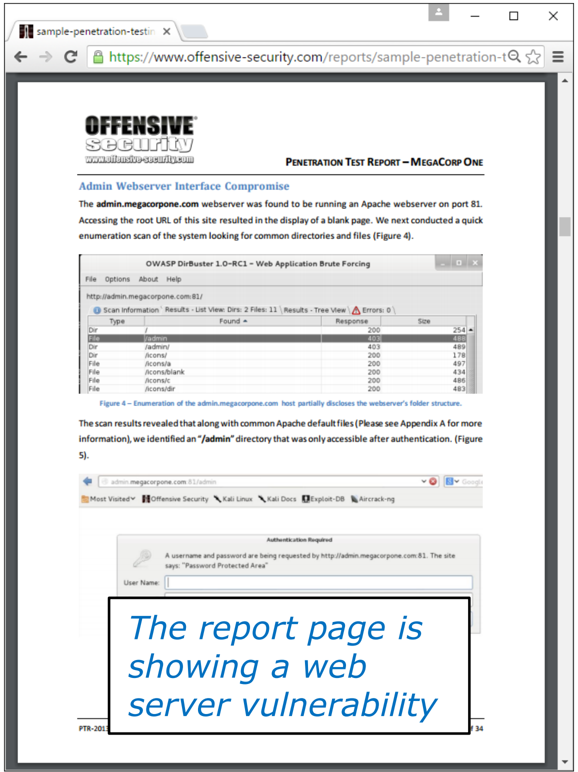
Penetration Testing Frame
www.vulnerabilityassessment.co.uk/Penetration%20Test.html
Expand - Collapse
VulnerabilityAssessment.
Kevin Orrey

Penetration Testing Framework 0.59

- Pre-Inspection Visit - template
- Network Footprinting (Reconnaissance) The tester would attempt to gather as much information as possible about the selected network. Reconnaissance can take two forms i.e. active and passive. A passive attack is always the best starting point as this would normally defeat intrusion detection systems and other forms of protection etc. afforded to the network. This would usually involve trying to discover publicly available information by utilising a web browser and visiting newsgroups etc. An active form would be more intrusive and may show up in audit logs and may take the form of an attempted DNS zone transfer or a social engineering type of attack.
  - Whois is widely used for querying authoritative registries/ databases to discover the owner of a domain name, an IP address, or an autonomous system number of the system you are targeting.
    - Authoratitive Bodies
      - IANA - Internet Assigned Numbers Authority
      - ICANN - Internet Corporation for Assigned Names and Numbers.
      - NRO - Number Resource Organisation
      - RIR - Regional Internet Registry
        - AFRINIC - African Network Information Centre
        - APNIC - Asia Pacific Network Information Centre
          - National Internet Registry
            - APJII
            - CNNIC
            - JPNIC
            - KRNIC
            - TWNIC
            - VNNIC
        - ARIN - American Registry for Internet Numbers
        - LACNIC - Latin America & Caribbean Network Information Centre
        - RIPE - Reseaux IP Européens—Network Coordination Centre
    - Websites

http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html

Example Reports



sample-penetration-testin
https://www.offensive-security.com/reports/sample-penetration-t

OFFENSIVE security www.offensive-security.com

PENETRATION TEST REPORT – MEGACORP ONE

Admin Webserver Interface Compromise

The **admin.megacorpone.com** webserver was found to be running an Apache webserver on port 81. Accessing the root URL of this site resulted in the display of a blank page. We next conducted a quick enumeration scan of the system looking for common directories and files (Figure 4).

OWASP DirBuster 1.0-RC1 – Web Application Brute Forcing

http://admin.megacorpone.com:81/

Scan Information | Results - List View: Dirs: 2 Files: 11 | Results - Tree View | Errors: 0

Type	Found	Response	Size
Dir	/	200	254
File	/admin	403	488
Dir	/admin/	403	489
Dir	/icons/	200	178
File	/icons/a	200	497
File	/icons/blank	200	434
File	/icons/c	200	486
File	/icons/dir	200	483

Figure 4 – Enumeration of the admin.megacorpone.com host partially discloses the webserver's folder structure.

The scan results revealed that along with common Apache default files (Please see Appendix A for more information), we identified an **"/admin"** directory that was only accessible after authentication. (Figure 5).

admin.megacorpone.com:81/admin

Most Visited Offensive Security Kali Linux Kali Docs Exploit-DB Aircrack-ng

Authentication Required

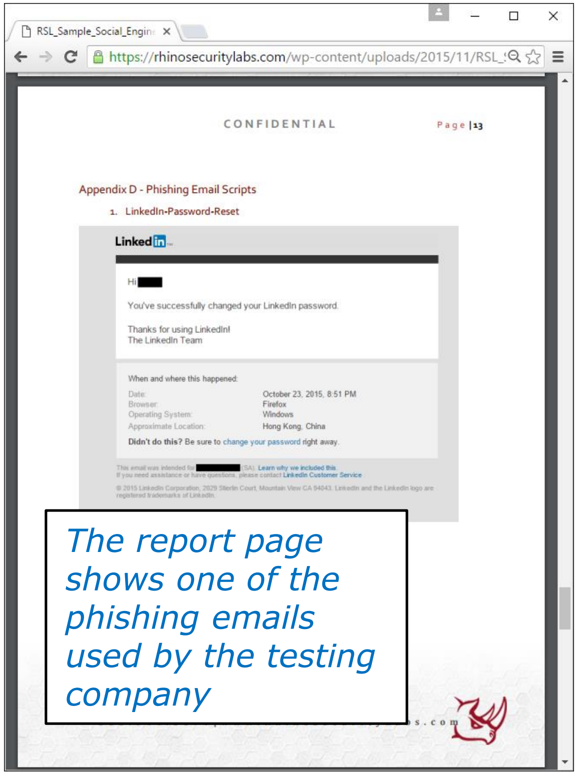
A username and password are being requested by http://admin.megacorpone.com:81. The site says: "Password Protected Area"

User Name:

PTR-2013 f 34

The report page is showing a web server vulnerability

https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf



RSL_Sample_Social_Engin
https://rhinosecuritylabs.com/wp-content/uploads/2015/11/RSL_

CONFIDENTIAL Page |13

Appendix D - Phishing Email Scripts

1. LinkedIn-Password-Reset

LinkedIn

Hi [redacted]

You've successfully changed your LinkedIn password.

Thanks for using LinkedIn!
The LinkedIn Team

When and where this happened:

Date:	October 23, 2015, 8:51 PM
Browser:	Firefox
Operating System:	Windows
Approximate Location:	Hong Kong, China

Didn't do this? Be sure to change your password right away.

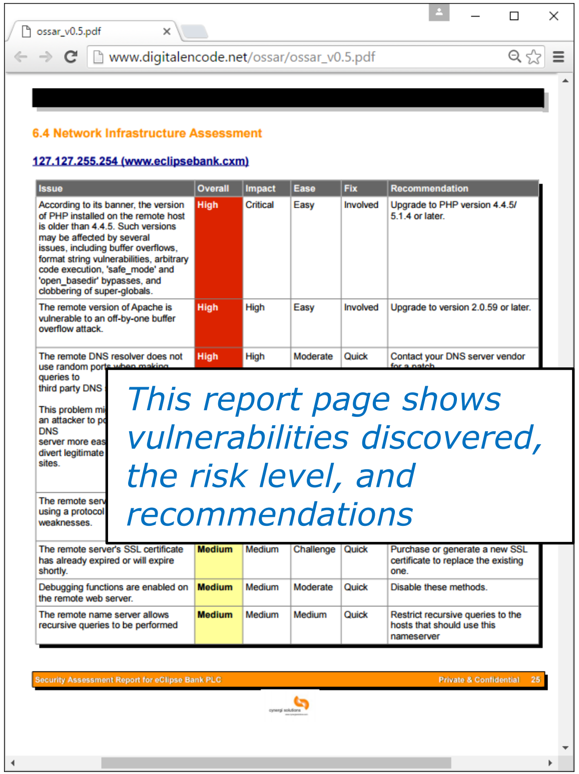
This email was intended for [redacted] (SA). Learn why we included this.
If you need assistance or have questions, please contact LinkedIn Customer Service

© 2015 LinkedIn Corporation, 2029 Stierlin Court, Mountain View CA 94043. LinkedIn and the LinkedIn logo are registered trademarks of LinkedIn.

s.com

The report page shows one of the phishing emails used by the testing company

https://rhinosecuritylabs.com/wp-content/uploads/2015/11/RSL_Sample_Social_Engineering_Report_2.0.pdf



6.4 Network Infrastructure Assessment

127.127.255.254 (www.eclipsebank.cxm)

Issue	Overall	Impact	Ease	Fix	Recommendation
According to its banner, the version of PHP installed on the remote host is older than 4.4.5. Such versions may be affected by several issues, including buffer overflows, format string vulnerabilities, arbitrary code execution, 'safe_mode' and 'open_basedir' bypasses, and clobbering of super-globals.	High	Critical	Easy	Involved	Upgrade to PHP version 4.4.5/ 5.1.4 or later.
The remote version of Apache is vulnerable to an off-by-one buffer overflow attack.	High	High	Easy	Involved	Upgrade to version 2.0.59 or later.
The remote DNS resolver does not use random ports when making queries to third party DNS This problem mi an attacker to p DNS server more eas divert legitimate sites.	High	High	Moderate	Quick	Contact your DNS server vendor for a patch.
The remote serv using a protocol weaknesses.					
The remote server's SSL certificate has already expired or will expire shortly.	Medium	Medium	Challenge	Quick	Purchase or generate a new SSL certificate to replace the existing one.
Debugging functions are enabled on the remote web server.	Medium	Medium	Moderate	Quick	Disable these methods.
The remote name server allows recursive queries to be performed	Medium	Medium	Medium	Quick	Restrict recursive queries to the hosts that should use this nameserver

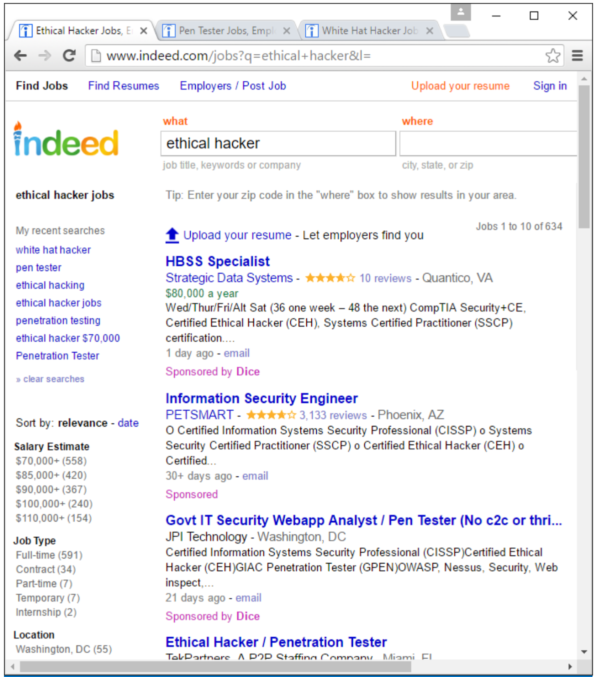
Security Assessment Report for eClipse Bank PLC Private & Confidential 25

This report page shows vulnerabilities discovered, the risk level, and recommendations

http://www.digitalencode.net/ossar/ossar_v0.5.pdf

Ethical Hacker Job Openings (Indeed)

Ethical Hacker job search



ethical hacker

ethical hacker jobs

Tip: Enter your zip code in the "where" box to show results in your area.

My recent searches
white hat hacker
pen tester
ethical hacking
ethical hacker jobs
penetration testing
ethical hacker $70,000
Penetration Tester
» clear searches

Sort by: **relevance** - date

Salary Estimate
$70,000+ (558)
$85,000+ (420)
$90,000+ (367)
$100,000+ (240)
$110,000+ (154)

Job Type
Full-time (591)
Contract (34)
Part-time (7)
Temporary (7)
Internship (2)

Location
Washington, DC (55)

Jobs 1 to 10 of 634

Upload your resume - Let employers find you

HBSS Specialist
Strategic Data Systems - ★★★★☆ 10 reviews - Quantico, VA
$80,000 a year
Wed/Thur/Fri/Alt Sat (36 one week – 48 the next) CompTIA Security+CE, Certified Ethical Hacker (CEH), Systems Certified Practitioner (SSCP) certification....
1 day ago - email
Sponsored by Dice

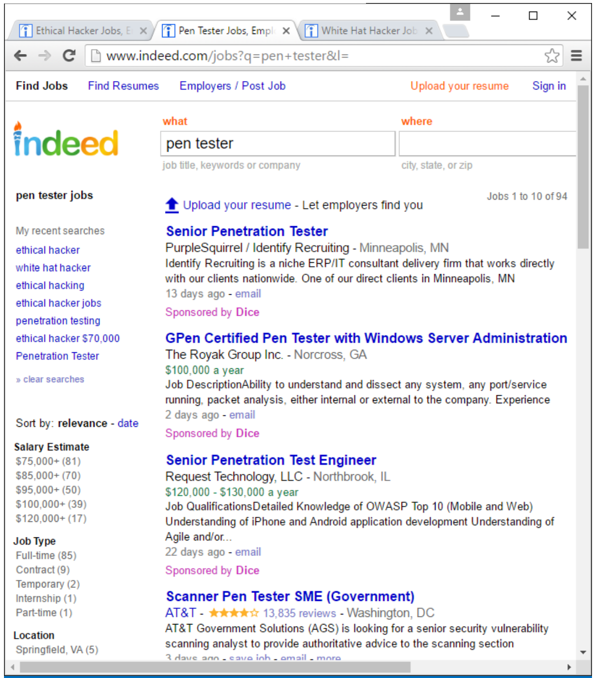
Information Security Engineer
PETSMART - ★★★★☆ 3,133 reviews - Phoenix, AZ
O Certified Information Systems Security Professional (CISSP) o Systems Security Certified Practitioner (SSCP) o Certified Ethical Hacker (CEH) o Certified...
30+ days ago - email
Sponsored

Govt IT Security Webapp Analyst / Pen Tester (No c2c or thri...
JPI Technology - Washington, DC
Certified Information Systems Security Professional (CISSP)Certified Ethical Hacker (CEH)GIAC Penetration Tester (GPEN)OWASP, Nessus, Security, Web inspect,...
21 days ago - email
Sponsored by Dice

Ethical Hacker / Penetration Tester
TekPartners, A P2P Staffing Company - Miami, FL

http://www.indeed.com/jobs?q=ethical+hacker&l=

Pen Tester job search



pen tester

pen tester jobs

My recent searches
ethical hacker
white hat hacker
ethical hacking
ethical hacker jobs
penetration testing
ethical hacker $70,000
Penetration Tester
» clear searches

Sort by: **relevance** - date

Salary Estimate
$75,000+ (81)
$85,000+ (70)
$95,000+ (50)
$100,000+ (39)
$120,000+ (17)

Job Type
Full-time (85)
Contract (9)
Temporary (2)
Internship (1)
Part-time (1)

Location
Springfield, VA (5)

Jobs 1 to 10 of 94

Upload your resume - Let employers find you

Senior Penetration Tester
PurpleSquirrel / Identify Recruiting - Minneapolis, MN
Identify Recruiting is a niche ERP/IT consultant delivery firm that works directly with our clients nationwide. One of our direct clients in Minneapolis, MN
13 days ago - email
Sponsored by Dice

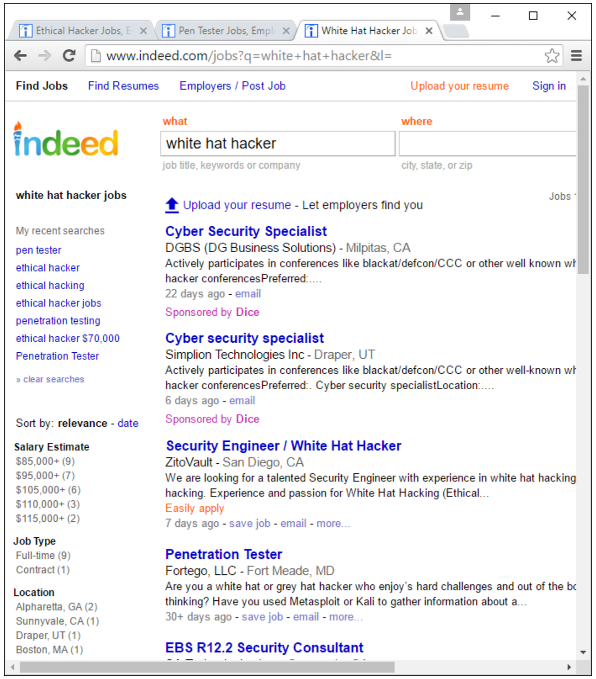
GPen Certified Pen Tester with Windows Server Administration
The Royak Group Inc. - Norcross, GA
$100,000 a year
Job DescriptionAbility to understand and dissect any system, any port/service running, packet analysis, either internal or external to the company. Experience
2 days ago - email
Sponsored by Dice

Senior Penetration Test Engineer
Request Technology, LLC - Northbrook, IL
$120,000 - $130,000 a year
Job QualificationsDetailed Knowledge of OWASP Top 10 (Mobile and Web) Understanding of iPhone and Android application development Understanding of Agile and/or...
22 days ago - email
Sponsored by Dice

Scanner Pen Tester SME (Government)
AT&T - ★★★★☆ 13,835 reviews - Washington, DC
AT&T Government Solutions (AGS) is looking for a senior security vulnerability scanning analyst to provide authoritative advice to the scanning section
3 days ago - save job - email - more

http://www.indeed.com/jobs?q=pen+tester&l=

White Hat Hacker job search



white hat hacker

white hat hacker jobs

My recent searches
pen tester
ethical hacker
ethical hacking
ethical hacker jobs
penetration testing
ethical hacker $70,000
Penetration Tester
» clear searches

Sort by: **relevance** - date

Salary Estimate
$85,000+ (9)
$95,000+ (7)
$105,000+ (6)
$110,000+ (3)
$115,000+ (2)

Job Type
Full-time (9)
Contract (1)

Location
Alpharetta, GA (2)
Sunnyvale, CA (1)
Draper, UT (1)
Boston, MA (1)

Jobs

Upload your resume - Let employers find you

Cyber Security Specialist
DGBS (DG Business Solutions) - Milpitas, CA
Actively participates in conferences like blackat/defcon/CCC or other well known wh hacker conferencesPreferred:....
22 days ago - email
Sponsored by Dice

Cyber security specialist
Simplion Technologies Inc - Draper, UT
Actively participates in conferences like blackat/defcon/CCC or other well-known wh hacker conferencesPreferred:. Cyber security specialistLocation:....
6 days ago - email
Sponsored by Dice

Security Engineer / White Hat Hacker
ZitoVault - San Diego, CA
We are looking for a talented Security Engineer with experience in white hat hacking hacking. Experience and passion for White Hat Hacking (Ethical...
Easily apply
7 days ago - save job - email - more...

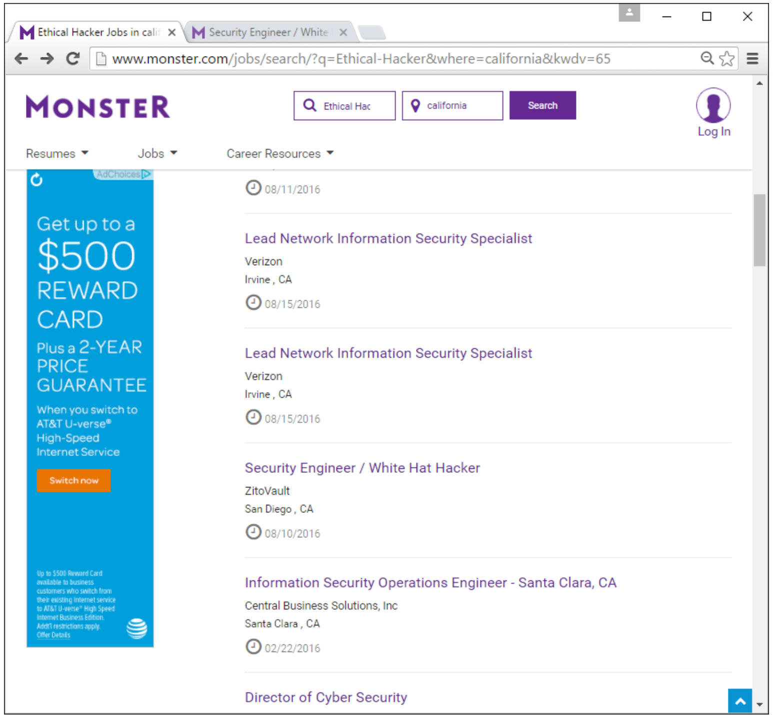
Penetration Tester
Fortego, LLC - Fort Meade, MD
Are you a white hat or grey hat hacker who enjoy's hard challenges and out of the bo thinking? Have you used Metasploit or Kali to gather information about a...
30+ days ago - save job - email - more...

EBS R12.2 Security Consultant

http://www.indeed.com/jobs?q=white+hat+hacker&l=

Ethical Hacker Job Openings (Monster)

Ethical Hacker in CA job search


Ethical Hacker Jobs in cali
Security Engineer / White
www.monster.com/jobs/search/?q=Ethical-Hacker&where=california&kwdv=65
MONSTER
Ethical Hac
california
Search
Log In
Resumes
Jobs
Career Resources

08/11/2016

Lead Network Information Security Specialist
Verizon
Irvine , CA
08/15/2016

Lead Network Information Security Specialist
Verizon
Irvine , CA
08/15/2016

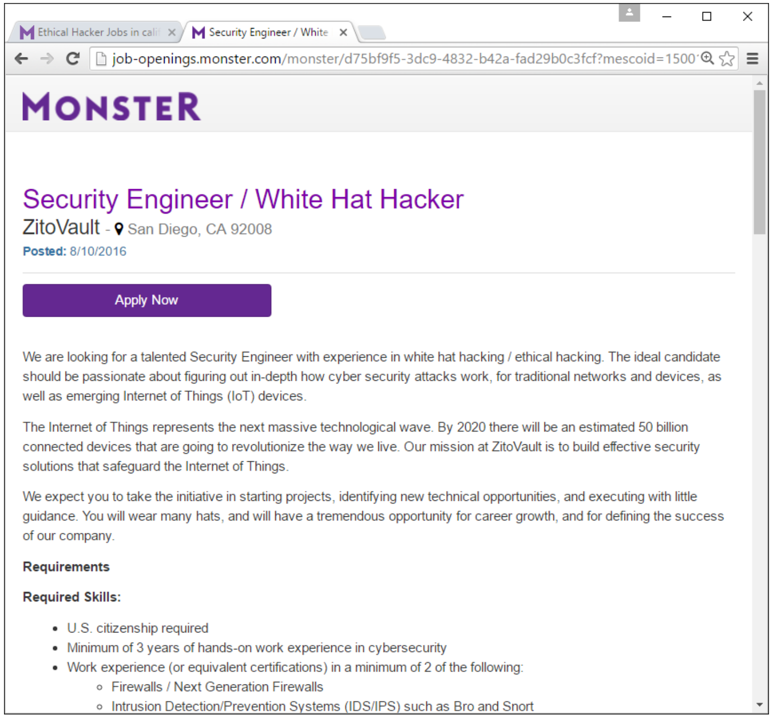
Security Engineer / White Hat Hacker
ZitoVault
San Diego , CA
08/10/2016

Information Security Operations Engineer - Santa Clara, CA
Central Business Solutions, Inc
Santa Clara , CA
02/22/2016

Director of Cyber Security

http://www.monster.com/jobs/search/?q=Ethical-Hacker&where=california&kwdv=65

Job opening in San Diego


Ethical Hacker Jobs in cali
Security Engineer / White
job-openings.monster.com/monster/d75bf9f5-3dc9-4832-b42a-fad29b0c3fcf?mescoid=1500
MONSTER
Apply Now

Security Engineer / White Hat Hacker
ZitoVault - San Diego, CA 92008
Posted: 8/10/2016

We are looking for a talented Security Engineer with experience in white hat hacking / ethical hacking. The ideal candidate should be passionate about figuring out in-depth how cyber security attacks work, for traditional networks and devices, as well as emerging Internet of Things (IoT) devices.

The Internet of Things represents the next massive technological wave. By 2020 there will be an estimated 50 billion connected devices that are going to revolutionize the way we live. Our mission at ZitoVault is to build effective security solutions that safeguard the Internet of Things.

We expect you to take the initiative in starting projects, identifying new technical opportunities, and executing with little guidance. You will wear many hats, and will have a tremendous opportunity for career growth, and for defining the success of our company.

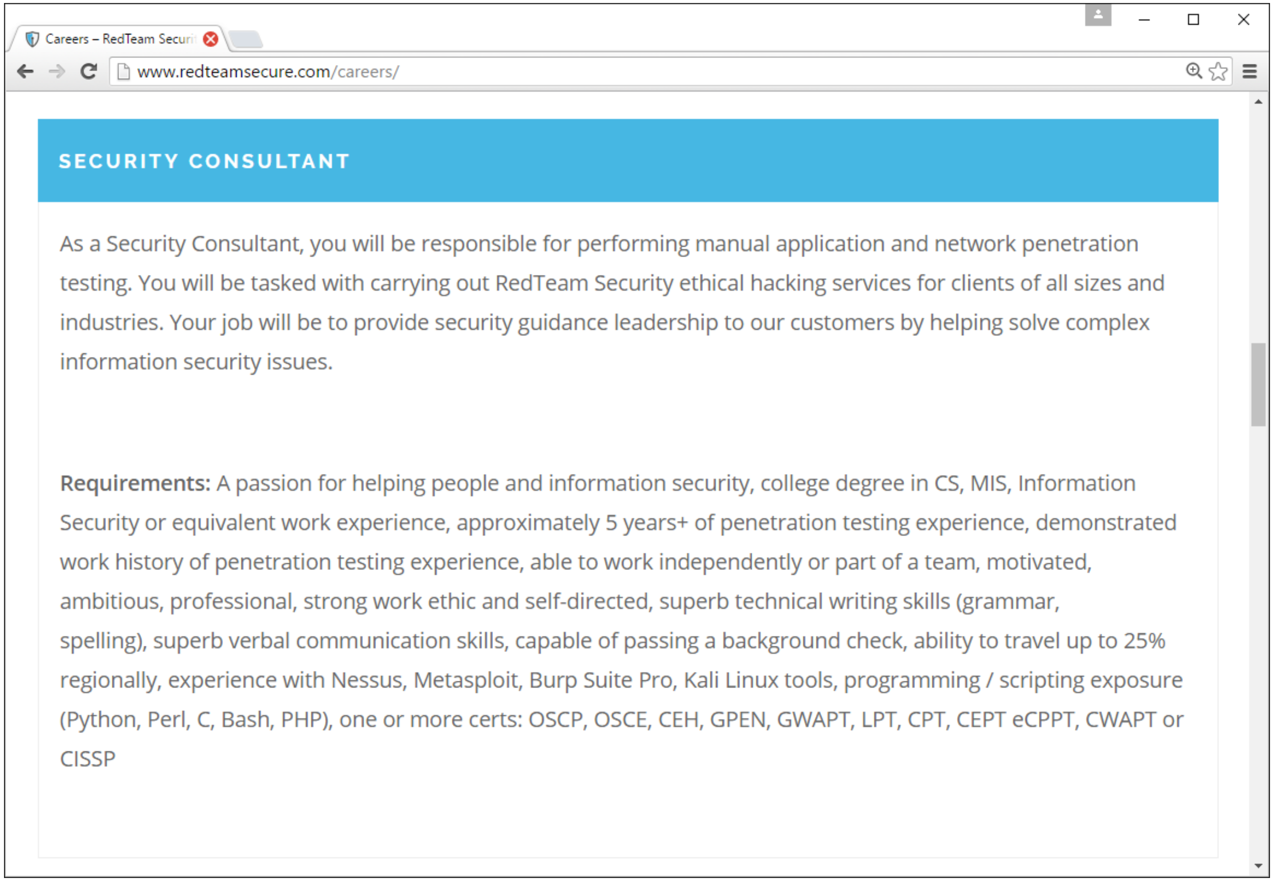
Requirements

Required Skills:

- U.S. citizenship required
- Minimum of 3 years of hands-on work experience in cybersecurity
- Work experience (or equivalent certifications) in a minimum of 2 of the following:
  - Firewalls / Next Generation Firewalls
  - Intrusion Detection/Prevention Systems (IDS/IPS) such as Bro and Snort

http://job-openings.monster.com/monster/d75bf9f5-3dc9-4832-b42a-fad29b0c3fcf?mescoid=1500125001001&jobPosition=9#

Ethical Hacker Job Openings (On careers page of testing company)



SECURITY CONSULTANT

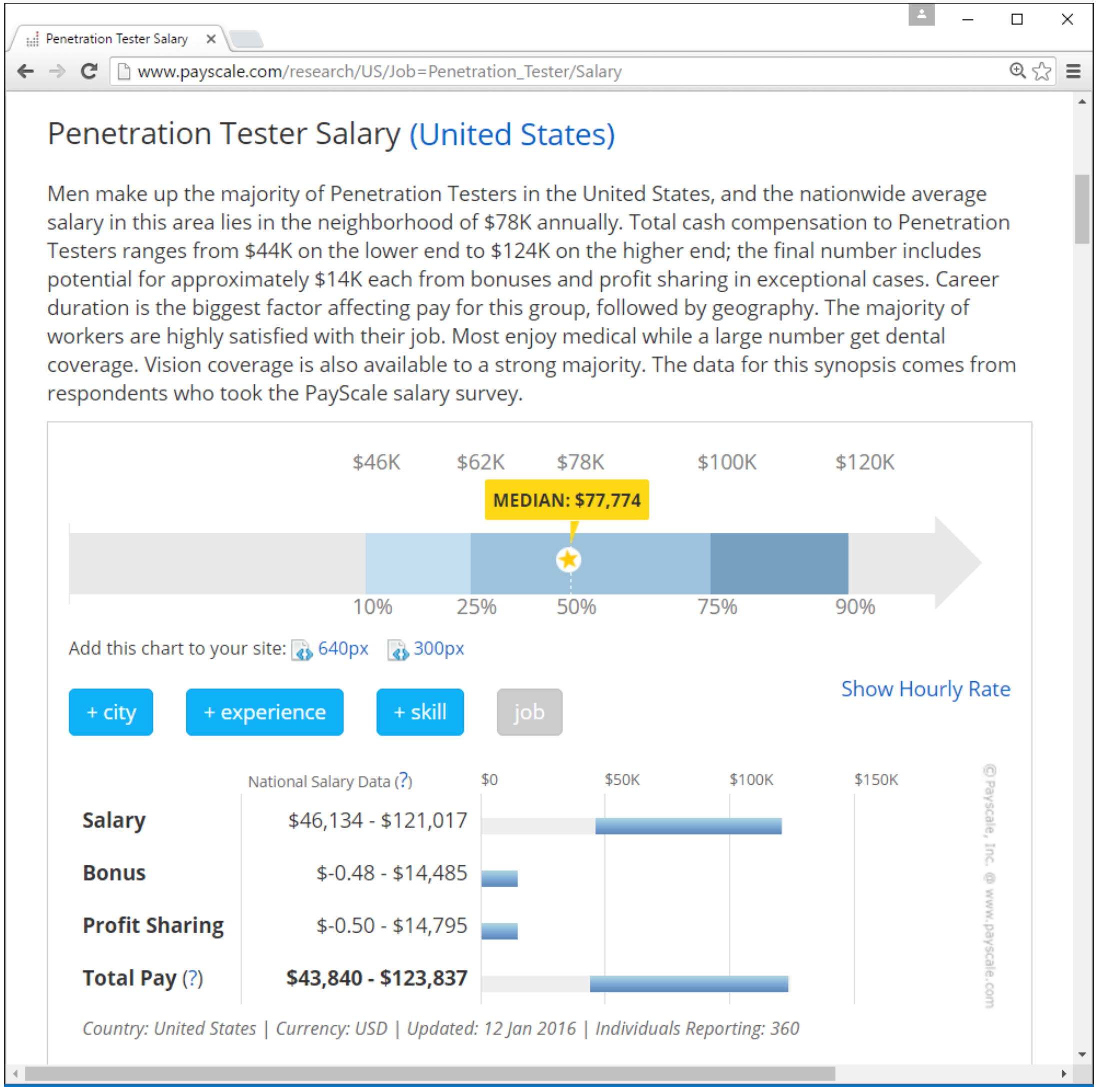
As a Security Consultant, you will be responsible for performing manual application and network penetration testing. You will be tasked with carrying out RedTeam Security ethical hacking services for clients of all sizes and industries. Your job will be to provide security guidance leadership to our customers by helping solve complex information security issues.

Requirements: A passion for helping people and information security, college degree in CS, MIS, Information Security or equivalent work experience, approximately 5 years+ of penetration testing experience, demonstrated work history of penetration testing experience, able to work independently or part of a team, motivated, ambitious, professional, strong work ethic and self-directed, superb technical writing skills (grammar, spelling), superb verbal communication skills, capable of passing a background check, ability to travel up to 25% regionally, experience with Nessus, Metasploit, Burp Suite Pro, Kali Linux tools, programming / scripting exposure (Python, Perl, C, Bash, PHP), one or more certs: OSCP, OSCE, CEH, GPEN, GWAPT, LPT, CPT, CEPT eCPPT, CWAPT or CISSP

Security testing firms will often post job openings such as this.

http://www.redteamsecure.com/careers/

Salary survey of 360 Pen Testers


Penetration Tester Salary
www.payscale.com/research/US/Job=Penetration_Tester/Salary
$46K
$62K
$78K
$100K
$120K
MEDIAN: $77,774
10%
25%
50%
75%
90%
+ city
+ experience
+ skill
job
Show Hourly Rate
$0
$50K
$100K
$150K
© Payscale, Inc. @ www.payscale.com

Penetration Tester Salary (United States)

Men make up the majority of Penetration Testers in the United States, and the nationwide average salary in this area lies in the neighborhood of $78K annually. Total cash compensation to Penetration Testers ranges from $44K on the lower end to $124K on the higher end; the final number includes potential for approximately $14K each from bonuses and profit sharing in exceptional cases. Career duration is the biggest factor affecting pay for this group, followed by geography. The majority of workers are highly satisfied with their job. Most enjoy medical while a large number get dental coverage. Vision coverage is also available to a strong majority. The data for this synopsis comes from respondents who took the PayScale salary survey.

Add this chart to your site: 640px 300px

	National Salary Data (?)
Salary	$46,134 - $121,017
Bonus	$-0.48 - $14,485
Profit Sharing	$-0.50 - $14,795
Total Pay (?)	**$43,840 - $123,837**

Country: United States | Currency: USD | Updated: 12 Jan 2016 | Individuals Reporting: 360

http://www.payscale.com/research/US/Job=Penetration_Tester/Salary

This website shows salary information for pen testers: $44 to $124 thousand per year.

Black Hats

Malicious Unethical Hacking

- Malicious hackers (black hats) are the "bad guys". They include criminals, con artists, disgruntled employees, hacktivists, spies and nation states. They range from careless youthful stunts to organized crime and nation states.

- Some will try and get services without paying. See: captain crunch

- Some will steal PII (Personally Identifiable Information) like financial data, personal data, or credit cards to sell, commit fraud or identity theft. See: target

- Some will try to make money through extortion of random individuals or companies. See: ransomware

- Some will attempt to spy on government and corporations to steal technology, manufacturing processes, intellectual property, or top secret information. See: national security

- Some will expose, vandalize, disrupt or tamper with information or services to harm organizations they oppose. See: anonymous

- Some will use hacking as a weapon to disrupt or destroy services, industrial machinery, or infrastructure (such as electrical grids, banking and financial systems, communication, transportation). See: ukraine power grid

- Targets include computers, networks, mobile devices, industrial control systems, point of sale devices, automobiles, ATMs, all kinds of public infrastructure, and now IoT (Internet of Things). See: smart watch

Hacktivists

Politically motivated attacks against governments, organizations, groups, and people they don't agree with.

- Vandalize websites.
- Break into servers and expose private and confidential information.
- DDoS (Distributed Denial of Service Attacks).

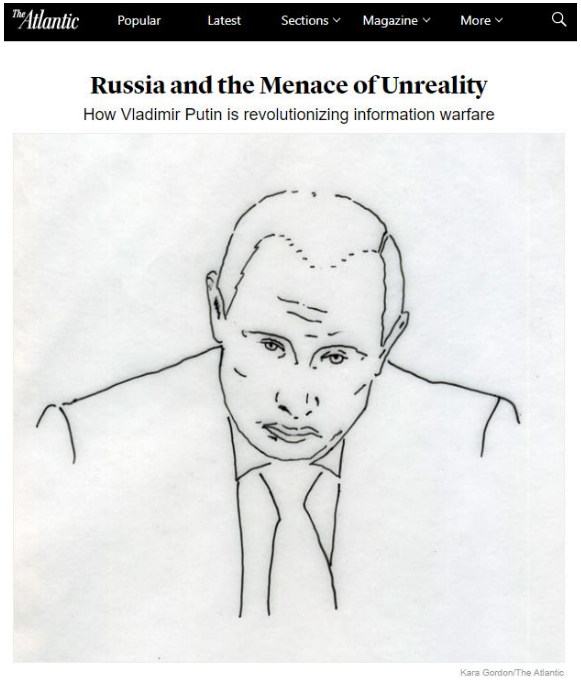
ISIS social media getting "Rick-Rolled" by Anonymous

http://www.nydailynews.com/news/world/activist-group-anonymous-rickrolling-isis-article-1.2445685

Anonymous hackers with the "headless figure" emblem and Guy Fawkes mask.

http://www.cbsnews.com/news/anonymous-hackers-isis-donald-trump-2015/

Weaponization of Information



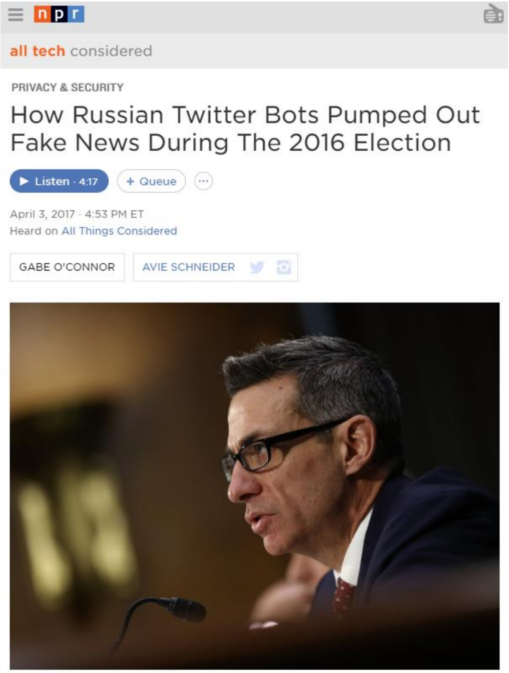
Russia and the Menace of Unreality

How Vladimir Putin is revolutionizing information warfare

Kara Gordon/The Atlantic

At the NATO summit in Wales last week, General Philip Breedlove, the military alliance’s top commander, made a bold declaration. Russia, he said, is waging “the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare.”

https://www.theatlantic.com/international/archive/2014/09/russia-putin-revolutionizing-information-warfare/379880/



PRIVACY & SECURITY

How Russian Twitter Bots Pumped Out Fake News During The 2016 Election

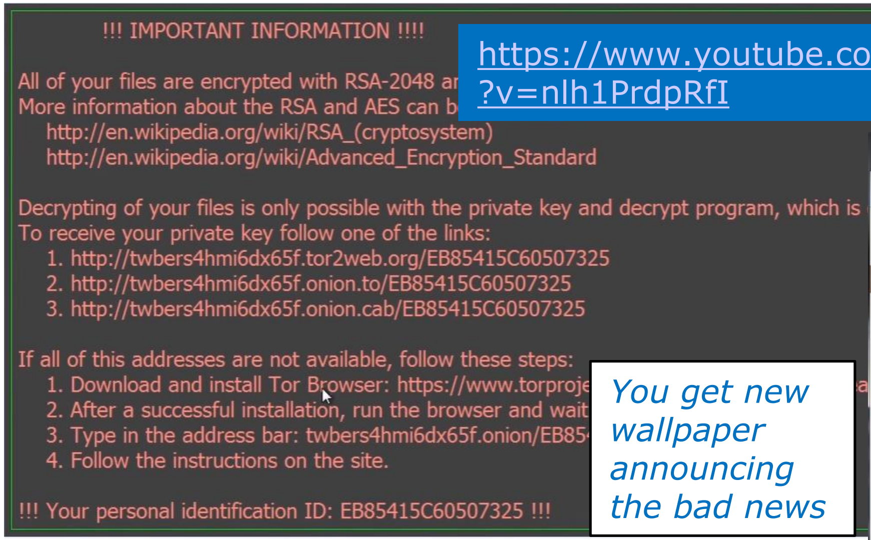
April 3, 2017 · 4:53 PM ET
Heard on All Things Considered

GABE O'CONNOR AVIE SCHNEIDER

Watts says the effort is being conducted by a "very diffuse network." It involves competing efforts "even amongst hackers between different parts of Russian intelligence and propagandists — all with general guidelines about what to pursue, but doing it at different times and paces and rhythms."

http://www.npr.org/sections/alltechconsidered/2017/04/03/522503844/how-russian-twitter-bots-pumped-out-fake-news-during-the-2016-election

Cyber Criminals



!!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 ar
More information about the RSA and AES can b
http://en.wikipedia.org/wiki/RSA_(cryptosystem)
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is
To receive your private key follow one of the links:
1. http://twbers4hmi6dx65f.tor2web.org/EB85415C60507325
2. http://twbers4hmi6dx65f.onion.to/EB85415C60507325
3. http://twbers4hmi6dx65f.onion.cab/EB85415C60507325

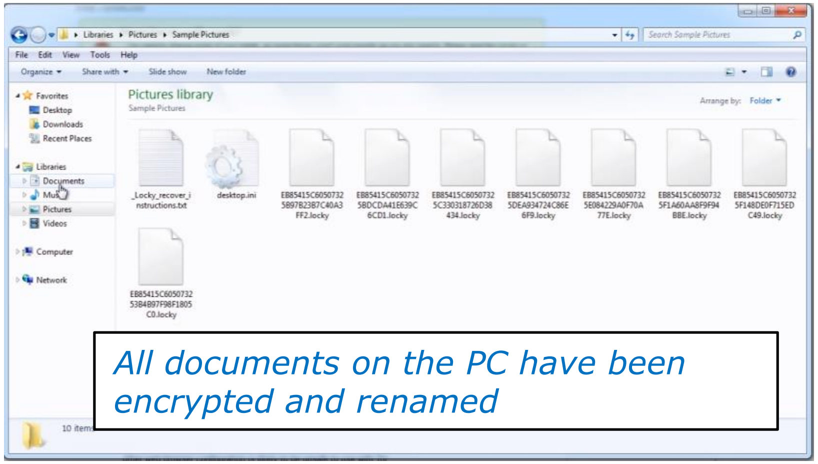
If all of this addresses are not available, follow these steps:
1. Download and install Tor Browser: https://www.torproje
2. After a successful installation, run the browser and wait
3. Type in the address bar: twbers4hmi6dx65f.onion/EB85
4. Follow the instructions on the site.

!!! Your personal identification ID: EB85415C60507325 !!!

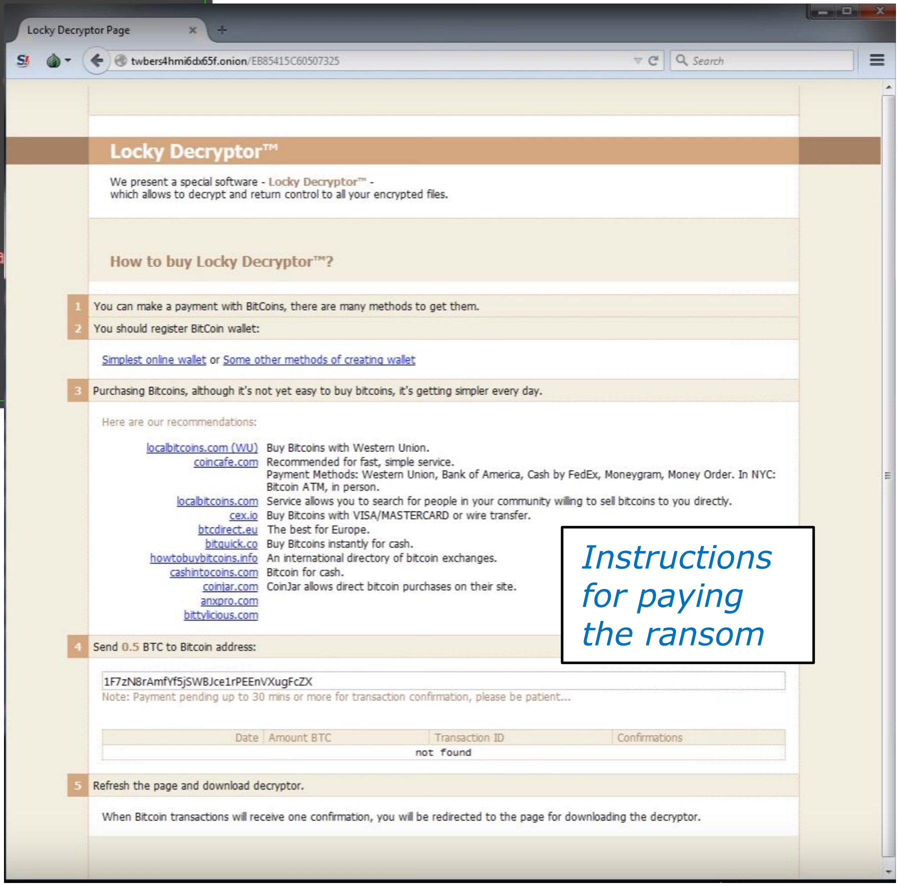
https://www.youtube.com/watch?v=nlh1PrdpRfI

You get new wallpaper announcing the bad news

Opening a word doc attachment from an unknown sender can get quite expensive!


Libraries ▸ Pictures ▸ Sample Pictures
Search Sample Pictures
File Edit View Tools Help
Organize ▾ Share with ▾ Slide show New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Mus
Pictures
Videos
Computer
Network
Pictures library
Sample Pictures
Arrange by: Folder ▾
_Locky_recover_instructions.txt
desktop.ini
EB85415C60507325B97B23B7C40A3FF2.locky
EB85415C60507325BDCDA41E639C6CD1.locky
EB85415C60507325C330318726D38434.locky
EB85415C60507325DEA934724C86E6F9.locky
EB85415C60507325E084229A0F70A77E.locky
EB85415C60507325F1A60AA8F9F94BBE.locky
EB85415C60507325F148DE0F715EDC49.locky
EB85415C6050732538 4B97F98F1805C0.locky
10 item

All documents on the PC have been encrypted and renamed



Locky Decryptor™

We present a special software - Locky Decryptor™ -
which allows to decrypt and return control to all your encrypted files.

How to buy Locky Decryptor™?

1 You can make a payment with BitCoins, there are many methods to get them.

2 You should register BitCoin wallet:

Simplest online wallet or Some other methods of creating wallet

3 Purchasing Bitcoins, although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:

localbitcoins.com (WU)	Buy Bitcoins with Western Union.
coincafe.com	Recommended for fast, simple service. Payment Methods: Western Union, Bank of America, Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, in person.
localbitcoins.com	Service allows you to search for people in your community willing to sell bitcoins to you directly.
cex.io	Buy Bitcoins with VISA/MASTERCARD or wire transfer.
btcdirect.eu	The best for Europe.
bitquick.co	Buy Bitcoins instantly for cash.
howtobuybitcoins.info	An international directory of bitcoin exchanges.
cashintocoins.com	Bitcoin for cash.
coinjar.com	CoinJar allows direct bitcoin purchases on their site.
anxpro.com	
bittylicious.com	

4 Send 0.5 BTC to Bitcoin address:

1F7zN8rAmfYf5jSWBJce1rPEEnVXugFcZX
Note: Payment pending up to 30 mins or more for transaction confirmation, please be patient...

Date	Amount BTC	Transaction ID	Confirmations
	not found		

5 Refresh the page and download decryptor.

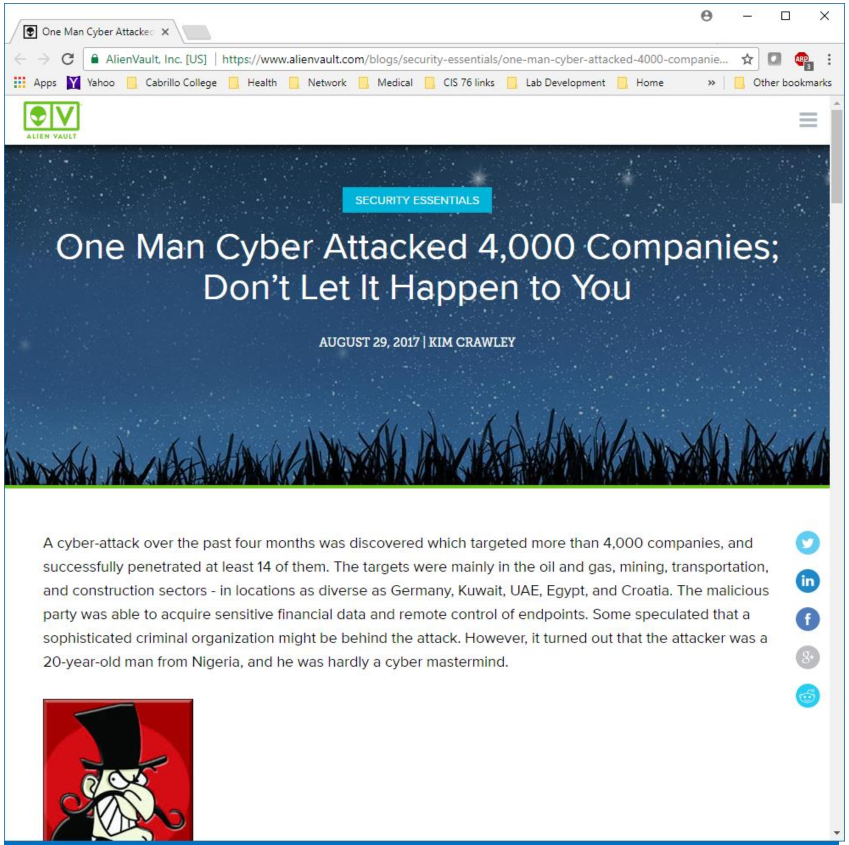
When Bitcoin transactions will receive one confirmation, you will be redirected to the page for downloading the decryptor.

Instructions for paying the ransom

A recent survey by Malwarebytes of 500 businesses found 40% had experienced a ransomware attack.

https://www.theguardian.com/technology/2016/aug/03/ransomware-threat-on-the-rise-as-40-of-businesses-attacked

Cyber Criminals


One Man Cyber Attacke
AlienVault, Inc. [US] | https://www.alienvault.com/blogs/security-essentials/one-man-cyber-attacked-4000-companie...
Apps Yahoo Cabrillo College Health Network Medical CIS 76 links Lab Development Home » Other bookmarks
ALIEN VAULT
SECURITY ESSENTIALS

One Man Cyber Attacked 4,000 Companies; Don't Let It Happen to You

AUGUST 29, 2017 | KIM CRAWLEY

A cyber-attack over the past four months was discovered which targeted more than 4,000 companies, and successfully penetrated at least 14 of them. The targets were mainly in the oil and gas, mining, transportation, and construction sectors - in locations as diverse as Germany, Kuwait, UAE, Egypt, and Croatia. The malicious party was able to acquire sensitive financial data and remote control of endpoints. Some speculated that a sophisticated criminal organization might be behind the attack. However, it turned out that the attacker was a 20-year-old man from Nigeria, and he was hardly a cyber mastermind.

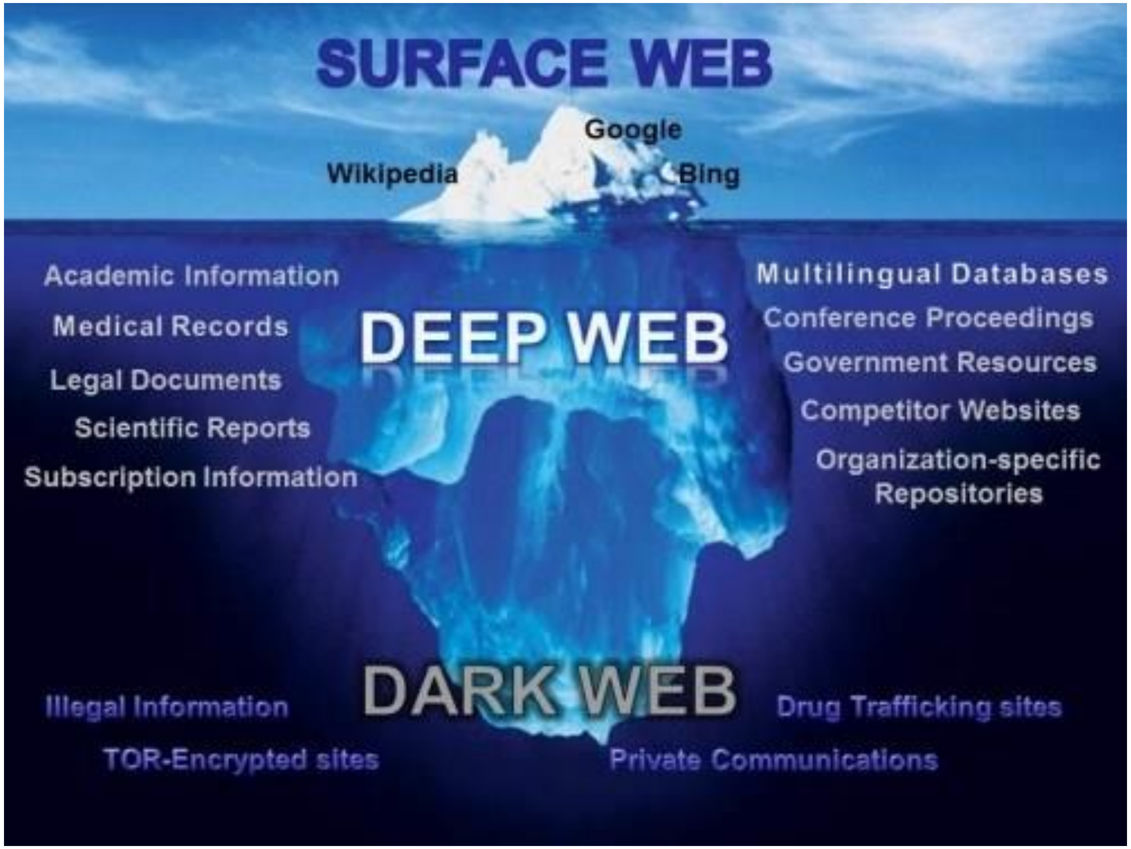
https://www.alienvault.com/blogs/security-essentials/one-man-cyber-attacked-4000-companies-dont-let-it-happen-to-you

"A cyber-attack over the past four months was discovered which targeted more than 4,000 companies, and successfully penetrated at least 14 of them."

"However, it turned out that the attacker was a 20-year-old man from Nigeria, and he was hardly a cyber mastermind."

"HawkEye is another malware which is sold in the Dark Web to be distributed as an email attachment Trojan. Its payload is a DOCX file, which can then acquire email and web browser passwords and engage in keylogger spyware functions."

The Dark Web
A portion of the non-indexed Deep Web



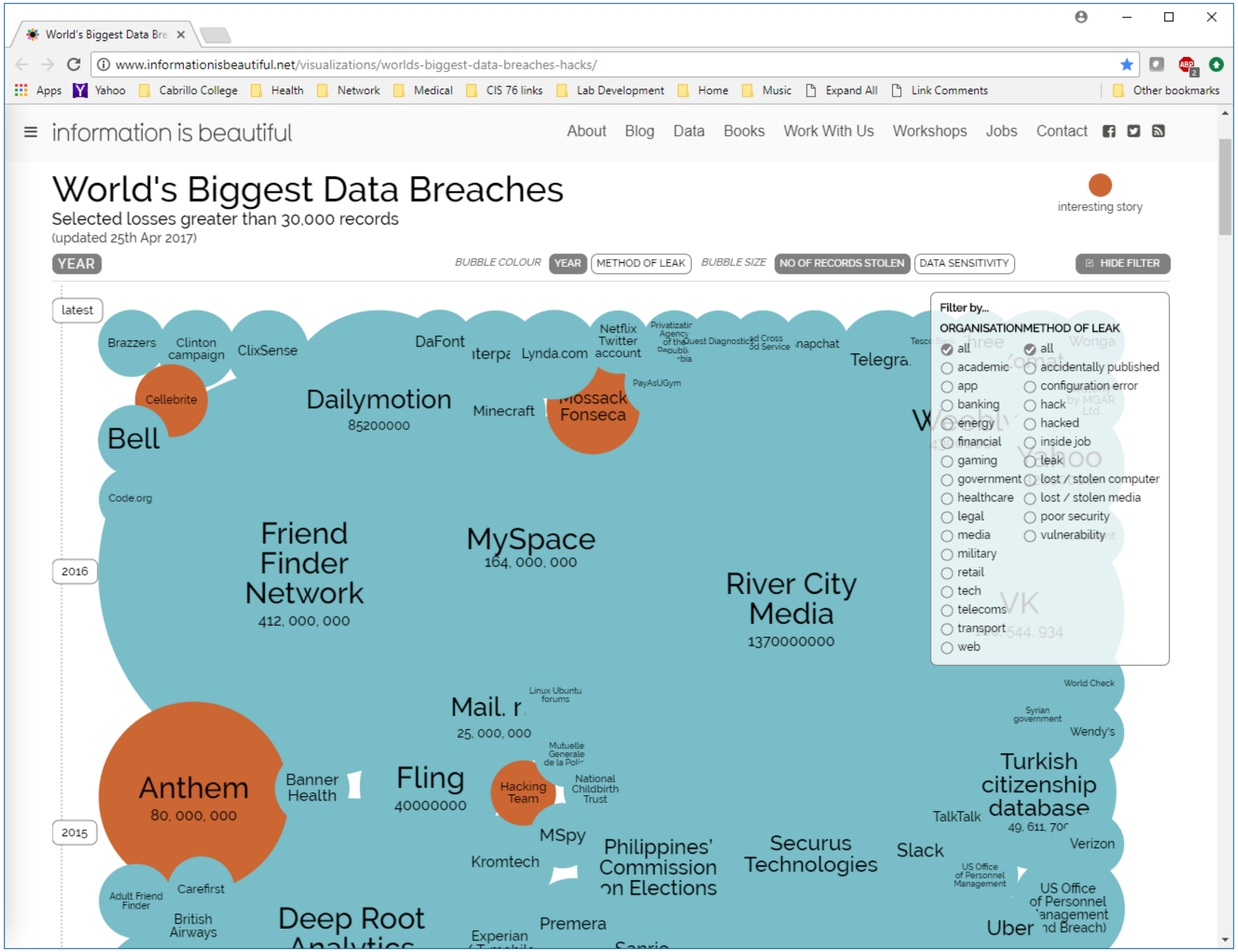
The Dark Web

- 2.5 Million daily visitors.
- 57 percent of the dark web has illegal content (drugs, child porn, terrorist communications, human trafficking, counterfeit currencies, ...)
- 30,00-40,000 estimated number of dark web pages.
- 1.2 billion in total sales by Silk Road site before shutdown by the FBI.
- $7.00 price of stolen credit card.

From "*The Man Who Lit the Dark Web*" by Charles Graeber (Popular Science Sept/Oct 2016)

https://www.quora.com/Is-it-safe-to-browse-the-dark-web

Timeline of Major Hacks



World's Biggest Data Breaches

Selected losses greater than 30,000 records
(updated 25th Apr 2017)

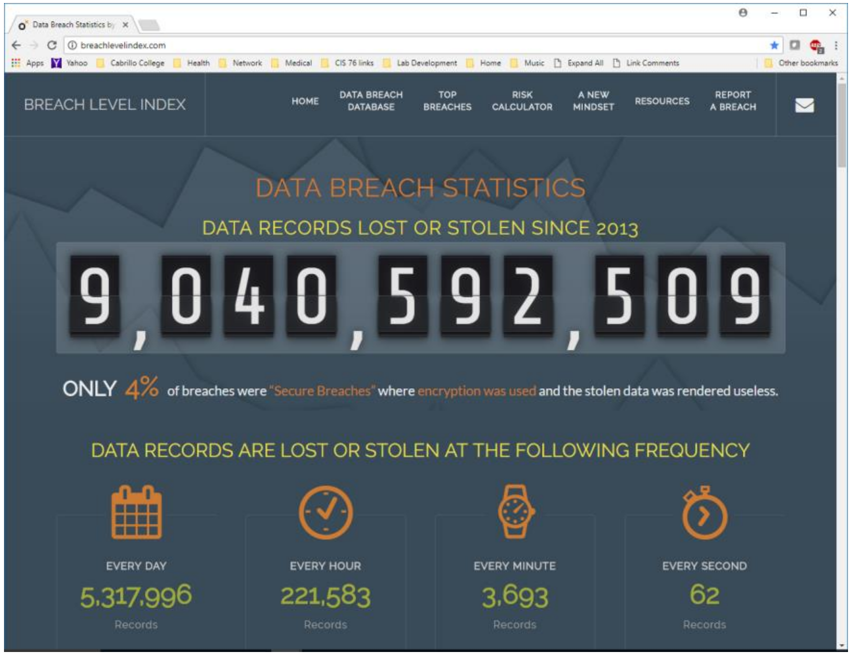
Filter by...

ORGANISATION	METHOD OF LEAK
☑ all	☑ all
○ academic	○ accidentally published
○ app	○ configuration error
○ banking	○ hack
○ energy	○ hacked
○ financial	○ inside job
○ gaming	○ leak
○ government	○ lost / stolen computer
○ healthcare	○ lost / stolen media
○ legal	○ poor security
○ media	○ vulnerability
○ military	
○ retail	
○ tech	
○ telecoms	
○ transport	
○ web	

This website shows a timeline of major data breaches. You can view the data in different ways.

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Data Breach Database



DATA BREACH STATISTICS

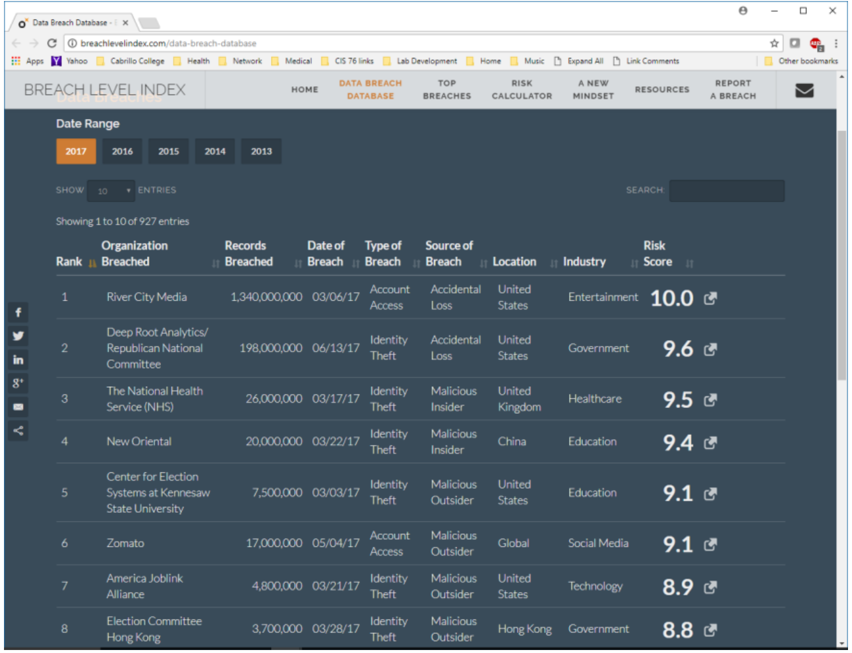
DATA RECORDS LOST OR STOLEN SINCE 2013

9,040,592,509

ONLY 4% of breaches were "Secure Breaches" where encryption was used and the stolen data was rendered useless.

DATA RECORDS ARE LOST OR STOLEN AT THE FOLLOWING FREQUENCY

EVERY DAY	EVERY HOUR	EVERY MINUTE	EVERY SECOND
5,317,996 Records	221,583 Records	3,693 Records	62 Records



Date Range

2017 2016 2015 2014 2013

SHOW 10 ENTRIES SEARCH:

Showing 1 to 10 of 927 entries

Rank	Organization Breached	Records Breached	Date of Breach	Type of Breach	Source of Breach	Location	Industry	Risk Score
1	River City Media	1,340,000,000	03/06/17	Account Access	Accidental Loss	United States	Entertainment	10.0
2	Deep Root Analytics/ Republican National Committee	198,000,000	06/13/17	Identity Theft	Accidental Loss	United States	Government	9.6
3	The National Health Service (NHS)	26,000,000	03/17/17	Identity Theft	Malicious Insider	United Kingdom	Healthcare	9.5
4	New Oriental	20,000,000	03/22/17	Identity Theft	Malicious Insider	China	Education	9.4
5	Center for Election Systems at Kennesaw State University	7,500,000	03/03/17	Identity Theft	Malicious Outsider	United States	Education	9.1
6	Zomato	17,000,000	05/04/17	Account Access	Malicious Outsider	Global	Social Media	9.1
7	America Joblink Alliance	4,800,000	03/21/17	Identity Theft	Malicious Outsider	United States	Technology	8.9
8	Election Committee Hong Kong	3,700,000	03/28/17	Identity Theft	Malicious Outsider	Hong Kong	Government	8.8

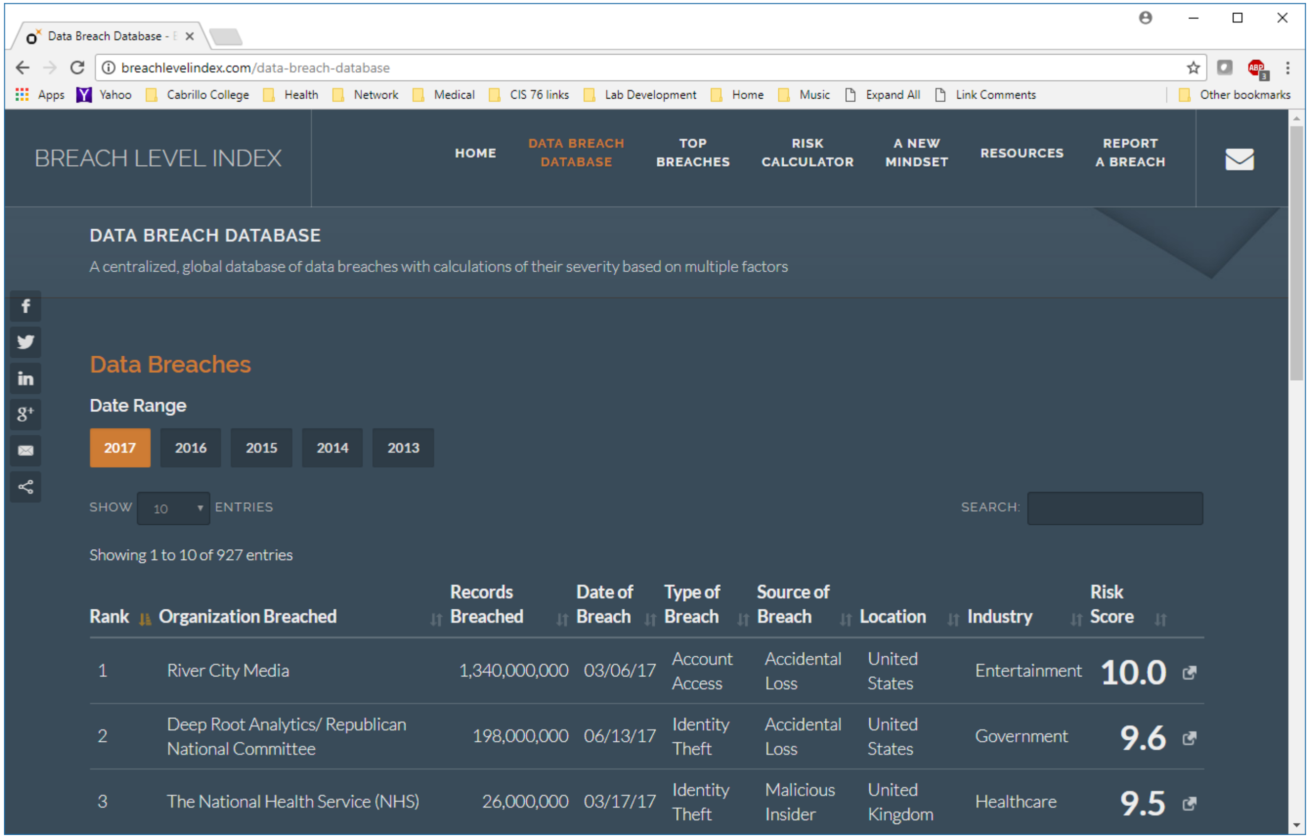
http://breachlevelindex.com/

http://breachlevelindex.com/data-breach-database

This website has a database of breaches and link to descriptive articles. The breach data can be sorted multiple ways and searched.

Data Breaches

This website has a database of breaches you can explore.



DATA BREACH DATABASE

A centralized, global database of data breaches with calculations of their severity based on multiple factors

Data Breaches

Date Range

2017 2016 2015 2014 2013

SHOW 10 ENTRIES SEARCH:

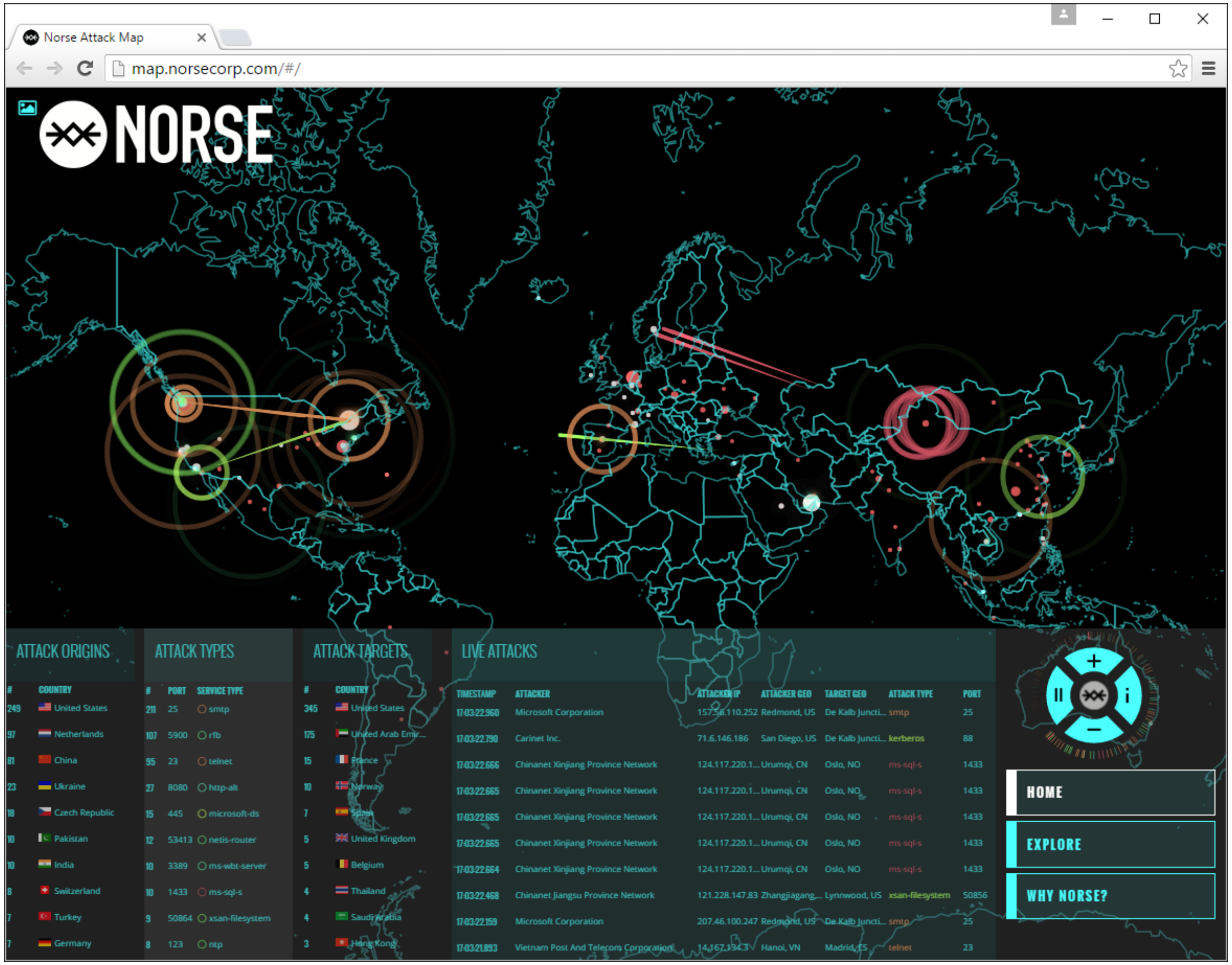
Showing 1 to 10 of 927 entries

Rank	Organization Breached	Records Breached	Date of Breach	Type of Breach	Source of Breach	Location	Industry	Risk Score
1	River City Media	1,340,000,000	03/06/17	Account Access	Accidental Loss	United States	Entertainment	10.0
2	Deep Root Analytics/ Republican National Committee	198,000,000	06/13/17	Identity Theft	Accidental Loss	United States	Government	9.6
3	The National Health Service (NHS)	26,000,000	03/17/17	Identity Theft	Malicious Insider	United Kingdom	Healthcare	9.5

http://breachlevelindex.com/data-breach-database

Live Attack Monitor

This live map graphically depicts attacks taking place across the world



ATTACK ORIGINS

#	COUNTRY
249	United States
97	Netherlands
81	China
23	Ukraine
18	Czech Republic
10	Pakistan
10	India
8	Switzerland
7	Turkey
7	Germany

ATTACK TYPES

#	PORT	SERVICE TYPE
211	25	○ smtp
107	5900	○ rfb
95	23	○ telnet
27	8080	○ http-alt
15	445	○ microsoft-ds
12	53413	○ netis-router
10	3389	○ ms-wbt-server
10	1433	○ ms-sql-s
9	50864	○ xsan-filesystem
8	123	○ ntp

ATTACK TARGETS

#	COUNTRY
345	United States
175	United Arab Emir...
15	France
10	Norway
7	Spain
5	United Kingdom
5	Belgium
4	Thailand
4	Saudi Arabia
3	Hong Kong

LIVE ATTACKS

TIMESTAMP	ATTACKER	ATTACKER IP	ATTACKER GEO	TARGET GEO	ATTACK TYPE	PORT
17-03-22.960	Microsoft Corporation	157.56.110.252	Redmond, US	De Kalb Juncti...	smtp	25
17-03-22.790	Carinet Inc.	71.6.146.186	San Diego, US	De Kalb Juncti...	kerberos	88
17-03-22.666	Chinanet Xinjiang Province Network	124.117.220.1...	Urumqi, CN	Oslo, NO	ms-sql-s	1433
17-03-22.665	Chinanet Xinjiang Province Network	124.117.220.1...	Urumqi, CN	Oslo, NO	ms-sql-s	1433
17-03-22.665	Chinanet Xinjiang Province Network	124.117.220.1...	Urumqi, CN	Oslo, NO	ms-sql-s	1433
17-03-22.665	Chinanet Xinjiang Province Network	124.117.220.1...	Urumqi, CN	Oslo, NO	ms-sql-s	1433
17-03-22.664	Chinanet Xinjiang Province Network	124.117.220.1...	Urumqi, CN	Oslo, NO	ms-sql-s	1433
17-03-22.468	Chinanet Jiangsu Province Network	121.228.147.83	Zhangjiagang,...	Lynnwood, US	xsan-filesystem	50856
17-03-22.159	Microsoft Corporation	207.46.100.247	Redmond, US	De Kalb Juncti...	smtp	25
17-03-21.893	Vietnam Post And Telecom Corporation	14.167.134.3	Hanoi, VN	Madrid, ES	telnet	23

http://map.norsecorp.com/#/

Nation-State Actors

Nation-State Actors

Government sponsored cyber espionage attacks

- Obtain intelligence on adversaries to know what they have and what they are planning.
- Steal industrial, technical, and military secrets.
- Disrupt or damage infrastructure.
- Obtain PII (Personally Identifiable Information).
- Push propaganda and disinformation via social media.
- Leaking confidential information to influence events.

Ugly Gorilla Flying Kitten Berserk Bear

APT 1 Hurricane Panda Fancy Bear APT 29

http://www.darkreading.com/attacks-breaches/nation-state-cyber-espionage-targeted-attacks-becoming-global-norm/d/d-id/1319025

http://www.techinsider.io/advanced-persistent-threats-2016-7/#the-exploits-are-called-zero-day-since-no-one-knows-about-them-until-they-are-actually-used-for-the-first-time-the-software-bugs-were-unknown-and-the-victim-has-had-zero-days-to-develop-a-solution-to-it-4

USENIX Enigma 2016 - NSA TAO Chief on Disrupting Nation State Hackers

- Rob Joyce, Chief, Tailored Access Operations, National Security Agency

  https://www.youtube.com/watch?v=bDJb8WOJYdA

APT1 Exposing One of China’s Cyber Espionage Units

- Mandiant Report

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

All Signs Point to Russia Being Behind the DNC Hack

- Thomas Rid

  http://motherboard.vice.com/en_uk/read/all-signs-point-to-russia-being-behind-the-dnc-hack

Findings from Analysis of DNC Intrusion Malware

- Michael Buratowski, senior vice president, Security Consulting Services

  https://www.fidelissecurity.com/threatgeek/2016/06/findings-analysis-dnc-intrusion-malware

NSA Red Team and more ...

USENIX Enigma 2016 - NSA TAO Chief on Disrupting Nation State Hackers

- Rob Joyce, Chief, Tailored Access Operations, National Security Agency

https://www.youtube.com/watch?v=bDJb8WOJYdA

- Six intrusion phases: Reconnaissance > Initial Exploitation > Establish Persistence > Install Tools > Move Laterally > Collect, Exfil, and Exploit

- Bottom line: A good attacker will know your network better than you do. You know the technologies you intended to use. They know the technologies you ACTUALLY use. They will also know the security functionality, at a very deep level, of your devices better than the people who designed them.

- The NSA runs red team testing against US government agency networks as a information assurance testing service.

- Dropping the firewall temporarily for vendor support? There is a reason nation-state attackers called Advanced Persistent Threats (APT). They will wait and wait and wait until the moment a door is briefly cracked open ...

- Persistence and focus will get you in without the zero-day exploits. There are so many other vectors that are easier, less risky, and more productive.

- The Big 3 intrusions are Email (phishing), (malicious) website, or removable (infected) media. People, even when highly trained, still make mistakes.

USENIX Enigma 2016 - NSA TAO Chief on Disrupting Nation State Hackers

- Rob Joyce, Chief, Tailored Access Operations, National Security Agency
- https://www.youtube.com/watch?v=bDJb8WOJYdA

- "Pass-the-Hash" allows you to grab a credential and pivot like mad laterally across the network.

- Intrusions can go undetected for months, even years.

- With BYOD and Internet of Things it is much easier to go after an employee's laptop rather than a professionally administered corporate PC.

APT1
Ugly Gorilla

MANDIANT

APT1

Exposing One of China's Cyber Espionage Units

APT1 Exposing One of China’s Cyber Espionage Units

- Mandiant Report

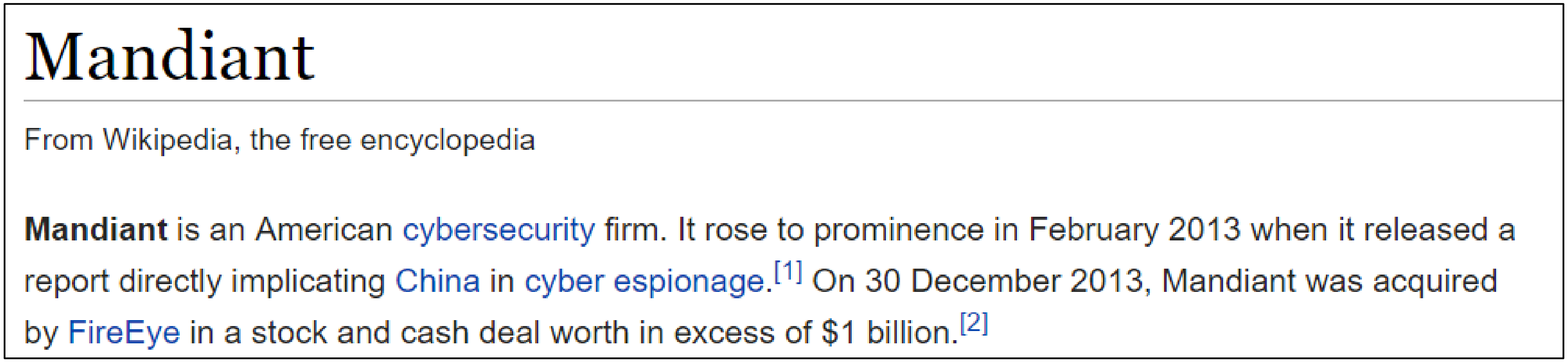
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

"Our analysis has led us to conclude that APT1 is likely government-sponsored and one of the most persistent of China’s cyber threat actors. We believe that APT1 is able to wage such a long-running and extensive cyber espionage campaign in large part because it receives direct government support. In seeking to identify the organization behind this activity, our research found that People’s Liberation Army (PLA’s) Unit 61398 is similar to APT1 in its mission, capabilities, and resources. PLA Unit 61398 is also located in precisely the same area from which APT1 activity appears to originate."

MANDIANT

APT1

Exposing One of China's Cyber Espionage Units



Mandiant

From Wikipedia, the free encyclopedia

Mandiant is an American cybersecurity firm. It rose to prominence in February 2013 when it released a report directly implicating China in cyber espionage.[1] On 30 December 2013, Mandiant was acquired by FireEye in a stock and cash deal worth in excess of $1 billion.[2]

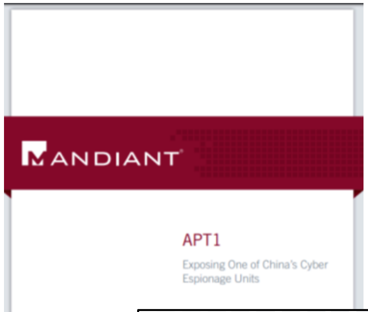
https://en.wikipedia.org/wiki/Mandiant

MANDIANT

APT1

Exposing One of China's Cyber Espionage Units

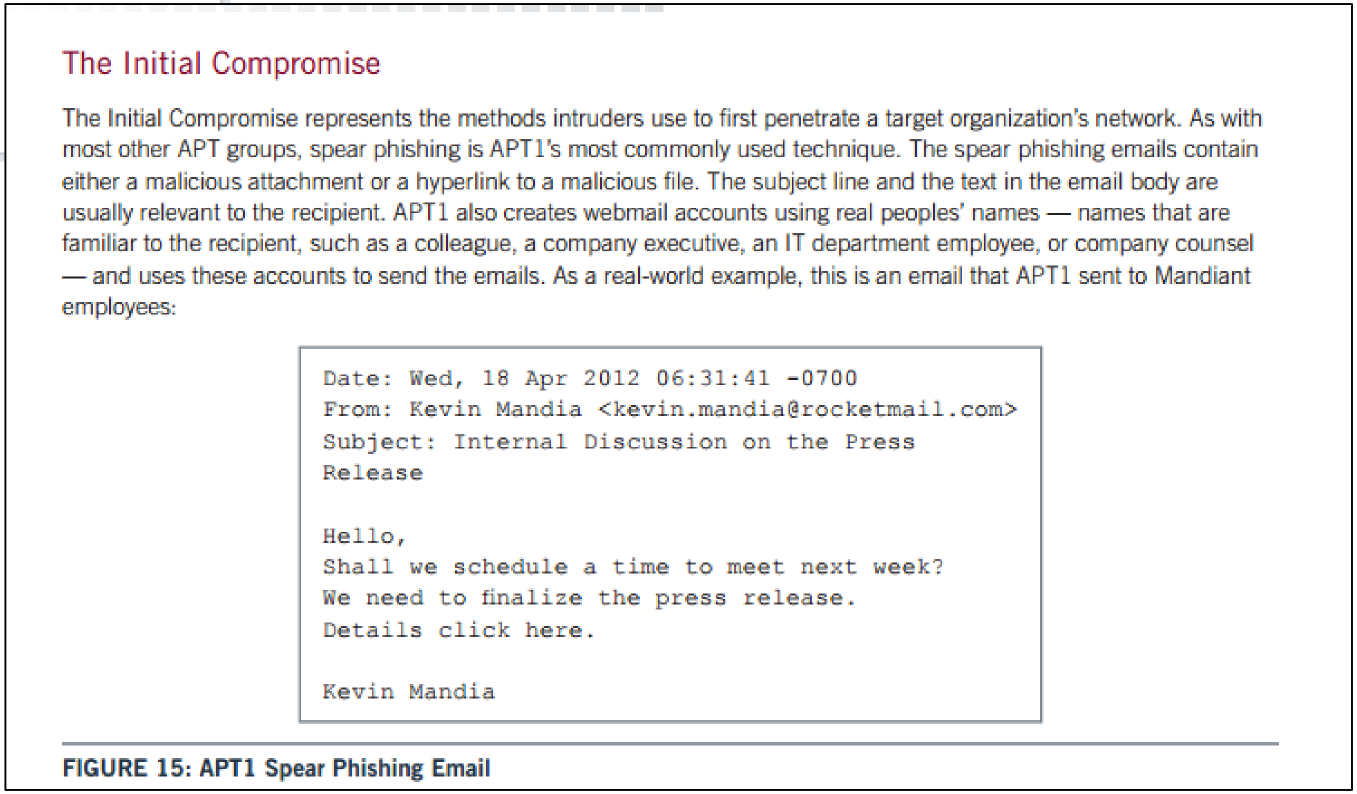
"APT1 has systematically stolen hundreds of terabytes of data from at least 141 organizations, and has demonstrated the capability and intent to steal from dozens of organizations simultaneously."



MANDIANT

APT1

Exposing One of China's Cyber Espionage Units



The Initial Compromise

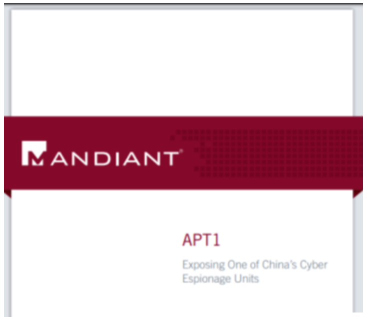
The Initial Compromise represents the methods intruders use to first penetrate a target organization's network. As with most other APT groups, spear phishing is APT1's most commonly used technique. The spear phishing emails contain either a malicious attachment or a hyperlink to a malicious file. The subject line and the text in the email body are usually relevant to the recipient. APT1 also creates webmail accounts using real peoples' names — names that are familiar to the recipient, such as a colleague, a company executive, an IT department employee, or company counsel — and uses these accounts to send the emails. As a real-world example, this is an email that APT1 sent to Mandiant employees:

```
Date: Wed, 18 Apr 2012 06:31:41 -0700
From: Kevin Mandia <kevin.mandia@rocketmail.com>
Subject: Internal Discussion on the Press
Release

Hello,
Shall we schedule a time to meet next week?
We need to finalize the press release.
Details click here.

Kevin Mandia
```

FIGURE 15: APT1 Spear Phishing Email



MANDIANT

APT1

Exposing One of China's Cyber Espionage Units

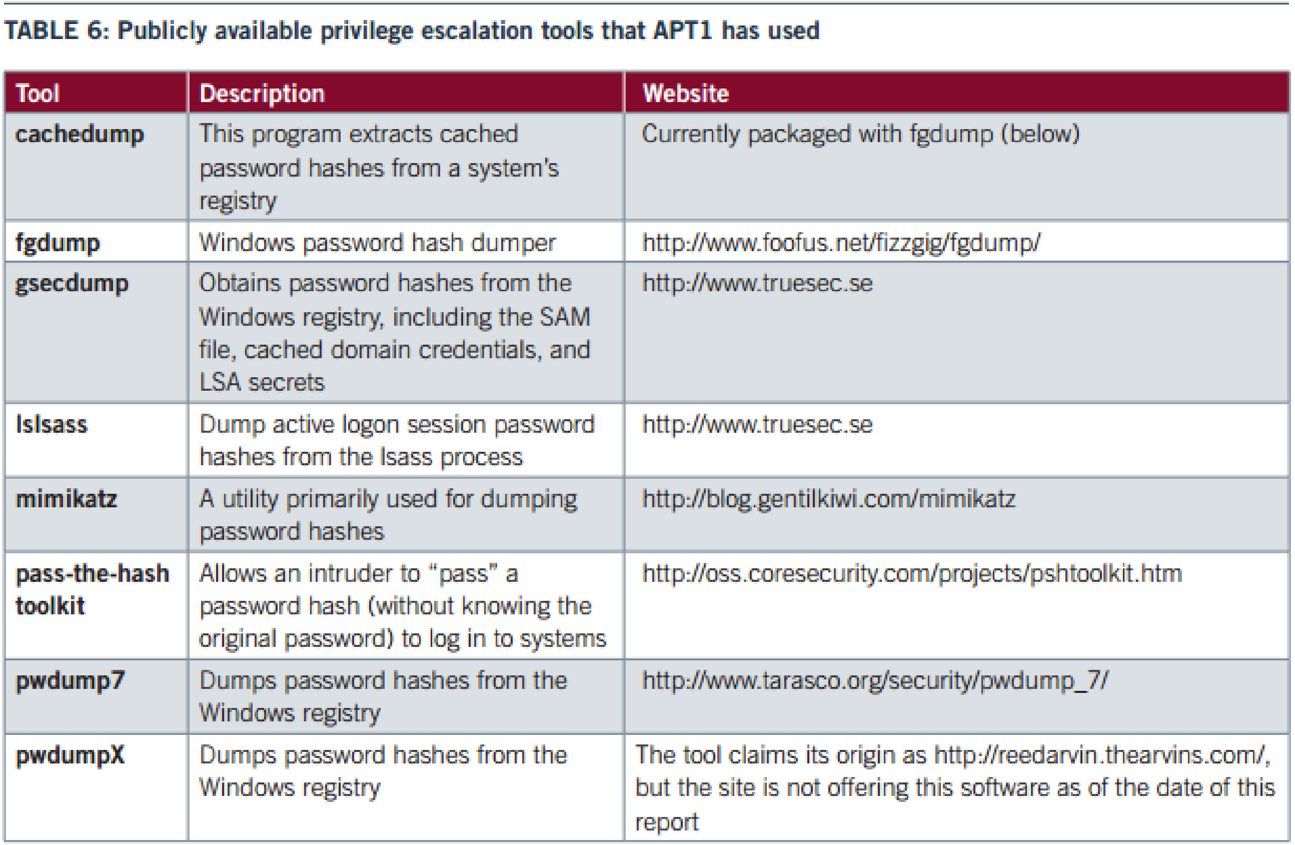


TABLE 6: Publicly available privilege escalation tools that APT1 has used

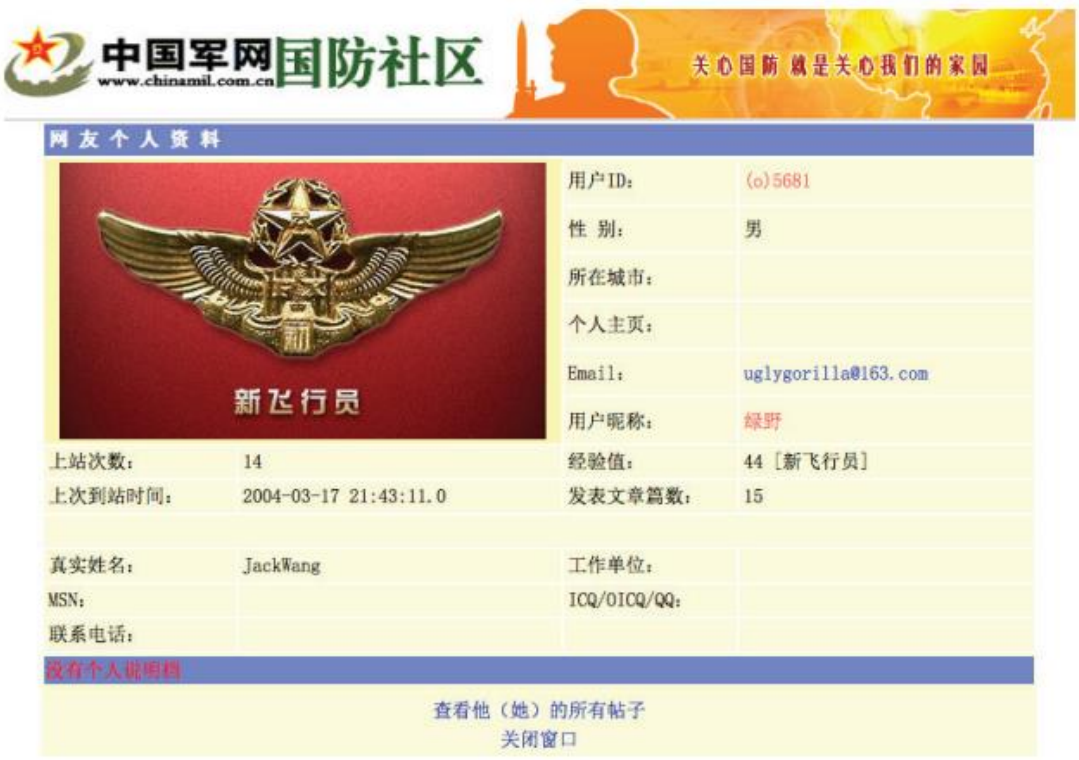
Tool	Description	Website
cachedump	This program extracts cached password hashes from a system's registry	Currently packaged with fgdump (below)
fgdump	Windows password hash dumper	http://www.foofus.net/fizzgig/fgdump/
gsecdump	Obtains password hashes from the Windows registry, including the SAM file, cached domain credentials, and LSA secrets	http://www.truesec.se
lslsass	Dump active logon session password hashes from the lsass process	http://www.truesec.se
mimikatz	A utility primarily used for dumping password hashes	http://blog.gentilkiwi.com/mimikatz
pass-the-hash toolkit	Allows an intruder to "pass" a password hash (without knowing the original password) to log in to systems	http://oss.coresecurity.com/projects/pshtoolkit.htm
pwdump7	Dumps password hashes from the Windows registry	http://www.tarasco.org/security/pwdump_7/
pwdumpX	Dumps password hashes from the Windows registry	The tool claims its origin as http://reedarvin.thearvins.com/, but the site is not offering this software as of the date of this report

MANDIANT

APT1

Exposing O

Espionage



中国军网 www.chinamil.com.cn 国防社区

关心国防 就是关心我们的家园

网友个人资料

新飞行员

		用户ID:	(o)5681
		性 别:	男
		所在城市:	
		个人主页:	
		Email:	uglygorilla@163.com
		用户昵称:	绿野
上站次数:	14	经验值:	44 [新飞行员]
上次到站时间:	2004-03-17 21:43:11.0	发表文章篇数:	15
真实姓名:	JackWang	工作单位:	
MSN:		ICQ/OICQ/QQ:	
联系电话:			

没有个人说明档

查看他（她）的所有帖子

关闭窗口

FIGURE 27: UglyGorilla chinamil profile, source: http://bbs.chinamil.com.cn/forum/bbsui.jsp?id=(o)5681

Chinese Hacker Slang

Search the Mandiant APT1 Report for "meat chicken".

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

What is a "meat chicken"?

Put your answer in the chat window

肉鸡 "rou ji"

DNC Hack

All Signs Point to Russia
motherboard.vice.com/en_uk/read/all-signs-point-to-russia-being-behind-the-dnc-hack
MOTHERBOARD
Watch
Sections

THE HACKS WE CAN'T SEE

All Signs Point to Russia Being Behind the DNC Hack

WRITTEN BY THOMAS RID

25 July 2016 // 01:38 PM CET

All Signs Point to Russia Being Behind the DNC Hack

- By Thomas Rid

http://motherboard.vice.com/en_uk/read/all-signs-point-to-russia-being-behind-the-dnc-hack

"It began ominously. Nearly two months earlier, in April, the Democrats had noticed that something was wrong in their networks. Then, in early May, the DNC called in CrowdStrike, a security firm that specializes in countering advanced network threats. After deploying their tools on the DNC's machines, and after about two hours of work, CrowdStrike found "two sophisticated adversaries" on the Committee's network. The two groups were well-known in the security industry as "APT 28" and "APT 29." APT stands for Advanced Persistent Threat—usually jargon for spies."

All Signs Point to Russia l
motherboard.vice.com/en_uk/read/all-signs-point-to-russia-being-behind-the-dnc-hack
MOTHERBOARD
Watch
Sections

- THE HACKS WE CAN'T SEE -

All Signs Point to Russia Being Behind the DNC Hack

WRITTEN BY THOMAS RID

25 July 2016 // 01:58 PM CET

All Signs Point to Russia Being Behind the DNC Hack

- By Thomas Rid

http://motherboard.vice.com/en_uk/read/all-signs-point-to-russia-being-behind-the-dnc-hack

"The forensic evidence linking the DNC breach to known Russian operations is very strong. On June 20, two competing cybersecurity companies, Mandiant (part of FireEye) and Fidelis, confirmed CrowdStrike's initial findings that Russian intelligence indeed hacked Clinton's campaign. The forensic evidence that links network breaches to known groups is solid: used and reused tools, methods, infrastructure, even unique encryption keys. For example: in late March the attackers registered a domain with a typo—misdepatrment[.]com—to look suspiciously like the company hired by the DNC to manage its network, MIS Department. They then linked this deceptive domain to a long-known APT 28 so-called X-Tunnel command-and-control IP address, 45.32.129[.]185."

All Signs Point to Russia Being Behind the DNC Hack

WRITTEN BY THOMAS RID

All Signs Point to Russia Being Behind the DNC Hack

- By Thomas Rid

http://motherboard.vice.com/en_uk/read/all-signs-point-to-russia-being-behind-the-dnc-hack

On June 15 a Wordpress blog popped up out of nowhere. And, soon, a Twitter account, @GUCCIFER_2. The first post and tweet were clumsily titled: "DNC's servers hacked by a lone hacker." The message: that it was not hacked by Russian intelligence. The mysterious online persona claimed to have given "thousands of files and mails" to Wikileaks, while mocking the firm investigating the case: "I guess CrowdStrike customers should think twice about company's competence," the post said, adding "Fbleepk CrowdStrike!!!!!!!!!"

MOTHERBOARD

All Signs Point to Russia Being Behind the DNC Hack

WRITTEN BY THOMAS RID

All Signs Point to Russia Being Behind the DNC Hack

- By Thomas Rid

http://motherboard.vice.com/en_uk/read/all-signs-point-to-russia-being-behind-the-dnc-hack

The larger operation, with its manipulative traits, fits well into the wider framework of Russia's evolving military doctrine, known as New Generation Warfare or the "Gerasimov Doctrine," named after Valery Gerasimov, the current Chief of the General Staff of the Armed Forces. This new mindset drastically expands what qualifies as a military target, and it expands what qualifies as military tactic. Deception and disinformation are part and parcel of this new approach, as are "camouflage and concealment," as the Israeli analyst Dima Adamsky pointed out in an important study of Russia's evolving strategic art published in November last year.

"Informational struggle," Adamsky observes, is at the center of New Generation Warfare. Informational struggle means "technological and psychological components designed to manipulate the adversary's picture of reality, misinform it, and eventually interfere with the decision-making process of individuals, *organizations, governments, and societies."*

Findings from Analysis of DNC Intrusion Malware

- Michael Buratowski, senior vice president, Security Consulting Services

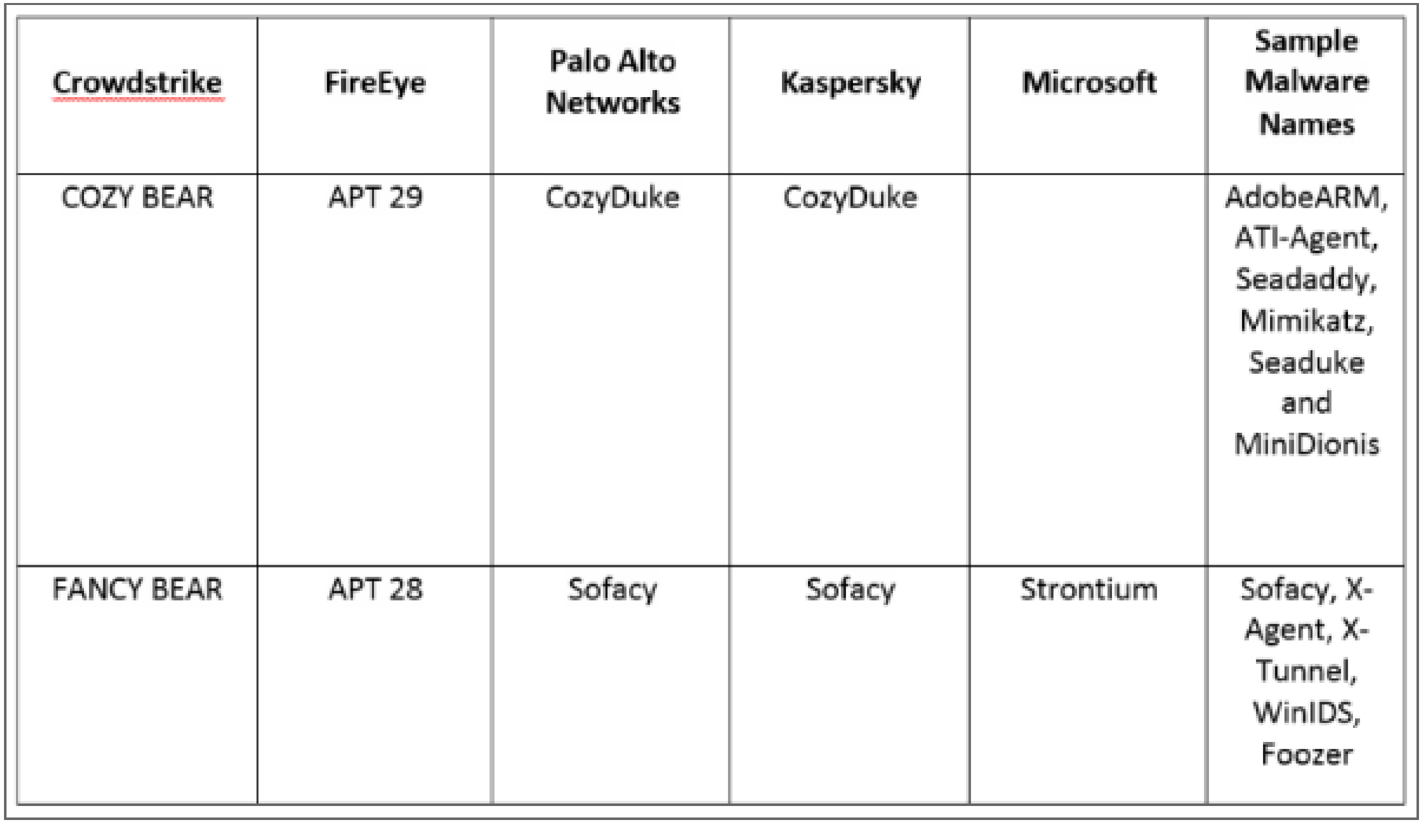
https://www.fidelissecurity.com/threatgeek/2016/06/findings-analysis-dnc-intrusion-malware

"So what does this mean? Who is responsible for the DNC hack? Based on our comparative analysis we agree with CrowdStrike and believe that the COZY BEAR and FANCY BEAR APT groups were involved in successful intrusions at the DNC. The malware samples contain data and programing elements that are similar to malware that we have encountered in past incident response investigations and are linked to similar threat actors."

Findings from Analysis of DNC Intrusion Malware

- Michael Buratowski, senior vice president, Security Consulting Services

https://www.fidelissecurity.com/threatgeek/2016/06/findings-analysis-dnc-intrusion-malware



Crowdstrike	FireEye	Palo Alto Networks	Kaspersky	Microsoft	Sample Malware Names
COZY BEAR	APT 29	CozyDuke	CozyDuke		AdobeARM, ATI-Agent, Seadaddy, Mimikatz, Seaduke and MiniDionis
FANCY BEAR	APT 28	Sofacy	Sofacy	Strontium	Sofacy, X-Agent, X-Tunnel, WinIDS, Foozer

Laws

- ❑ Federal laws
- ❑ State laws
- ❑ Is port scanning legal?
- ❑ Is Wi-Fi monitoring legal?
- ❑ Acceptable use policies

Hacking without permission is a crime and you could go to prison.

Important Federal Laws

Computer Fraud and Abuse Act

- Amended several times including by the USA Patriot Act
- Makes it illegal to access a computer without authorization
- https://www.law.cornell.edu/uscode/text/18/1030

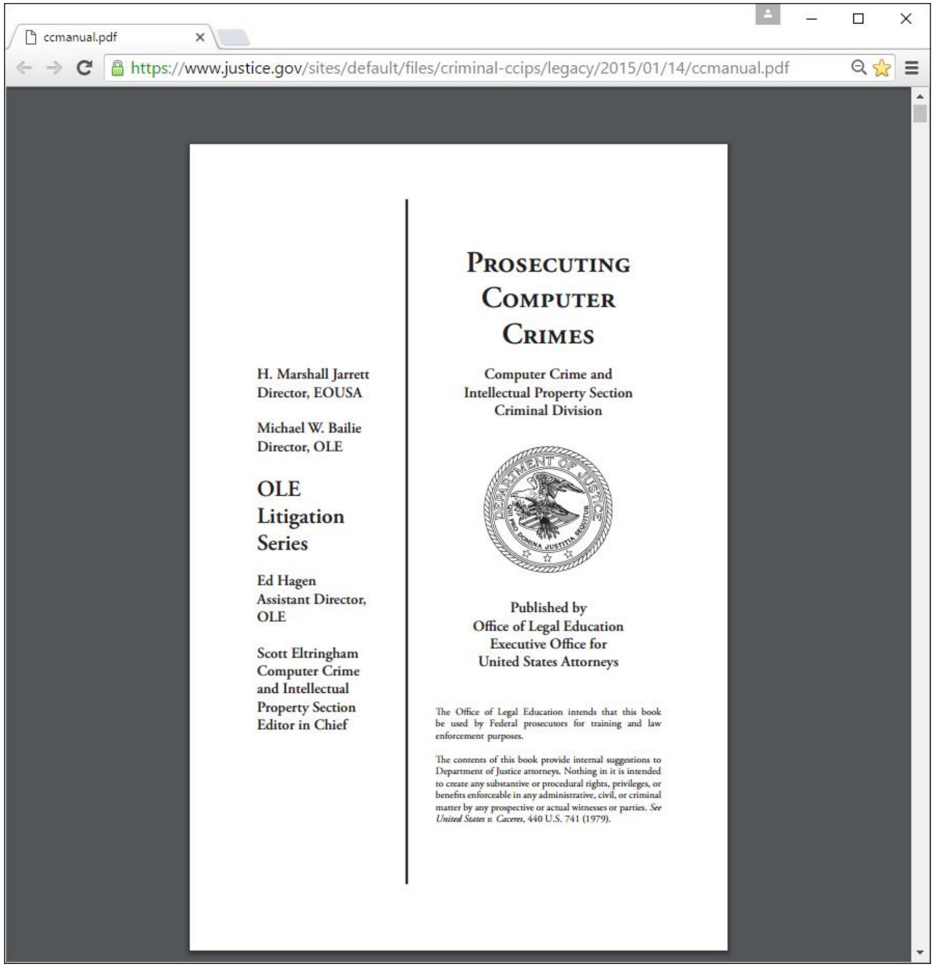
Digital Millennium Copyright Act

- Regulates reverse engineering
- https://www.law.cornell.edu/uscode/text/17/1201

Electronic Communications Privacy Act

- Updated the Wiretap Act of 1968
- Makes it illegal to intercept electronic communications
- https://www.law.cornell.edu/uscode/text/18/2511

Prosecuting Federal Laws


ccmanual.pdf
https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf

H. Marshall Jarrett
Director, EOUSA

Michael W. Bailie
Director, OLE

OLE
Litigation
Series

Ed Hagen
Assistant Director,
OLE

Scott Eltringham
Computer Crime
and Intellectual
Property Section
Editor in Chief

PROSECUTING
COMPUTER
CRIMES

Computer Crime and
Intellectual Property Section
Criminal Division

Published by
Office of Legal Education
Executive Office for
United States Attorneys

The Office of Legal Education intends that this book be used by Federal prosecutors for training and law enforcement purposes.

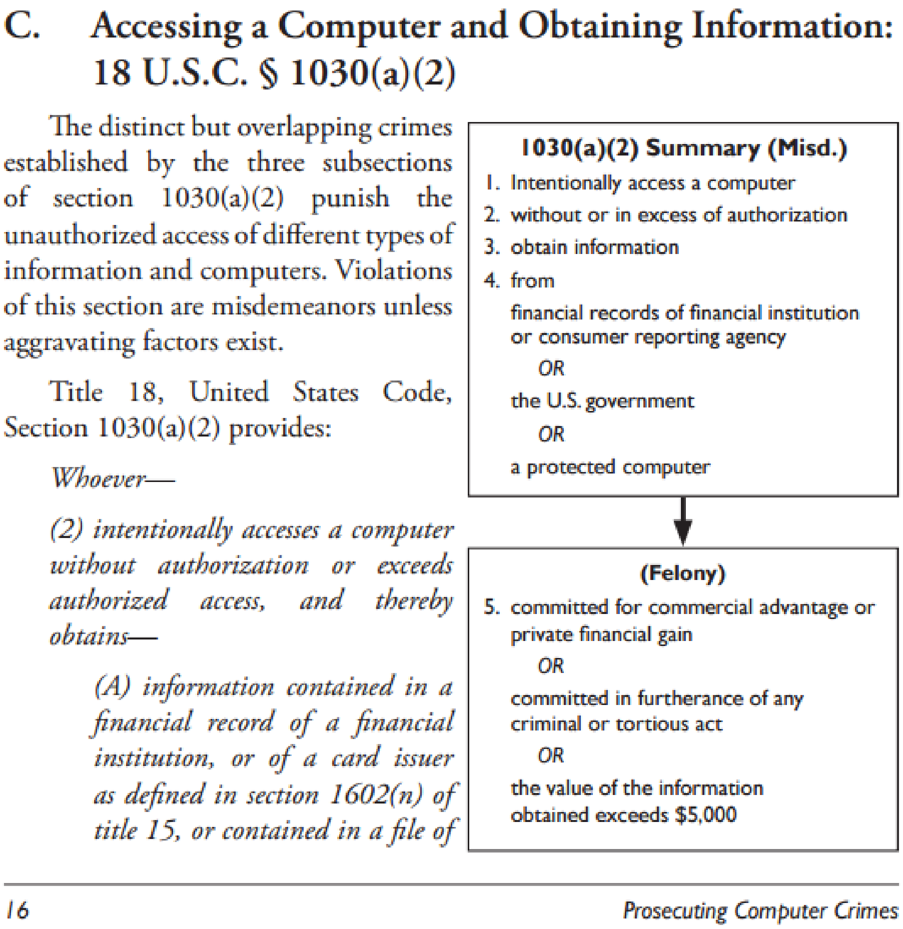
The contents of this book provide internal suggestions to Department of Justice attorneys. Nothing in it is intended to create any substantive or procedural rights, privileges, or benefits enforceable in any administrative, civil, or criminal matter by any prospective or actual witnesses or parties. *See United States v. Caceres*, 440 U.S. 741 (1979).

The suggested guidelines for US Attorneys in prosecuting computer crimes

https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf

Federal

The Computer Fraud and Abuse Act



C. Accessing a Computer and Obtaining Information: 18 U.S.C. § 1030(a)(2)

The distinct but overlapping crimes established by the three subsections of section 1030(a)(2) punish the unauthorized access of different types of information and computers. Violations of this section are misdemeanors unless aggravating factors exist.

Title 18, United States Code, Section 1030(a)(2) provides:

Whoever—

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of

1030(a)(2) Summary (Misd.)

1. Intentionally access a computer
2. without or in excess of authorization
3. obtain information
4. from

financial records of financial institution or consumer reporting agency

OR

the U.S. government

OR

a protected computer

(Felony)

5. committed for commercial advantage or private financial gain

OR

committed in furtherance of any criminal or tortious act

OR

the value of the information obtained exceeds $5,000

16 *Prosecuting Computer Crimes*

Misdemeanor

Felony

https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf

Federal Law

Open the Department of Justice "Prosecuting Computer Crimes" document at:

https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf

Search for the "Summary of CFAA Penalties" table. What is the maximum prison sentence for the offense "Accessing a Computer and Obtaining Information"?

Put your answer in the chat window

Now consider all offenses covered by the CFAA, what is the maximum prison sentence for a violation?

Put your answer in the chat window

Federal

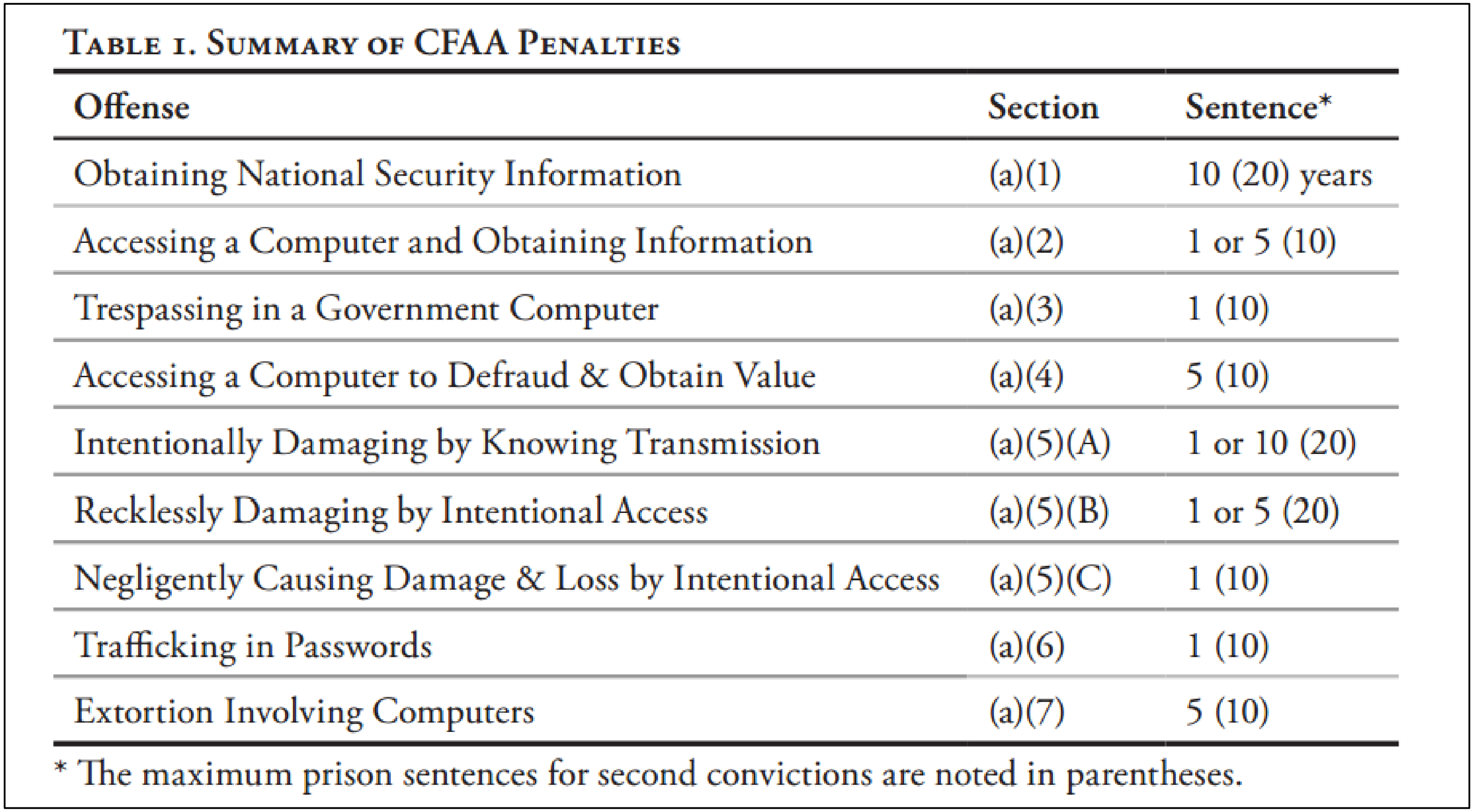


Table 1. Summary of CFAA Penalties

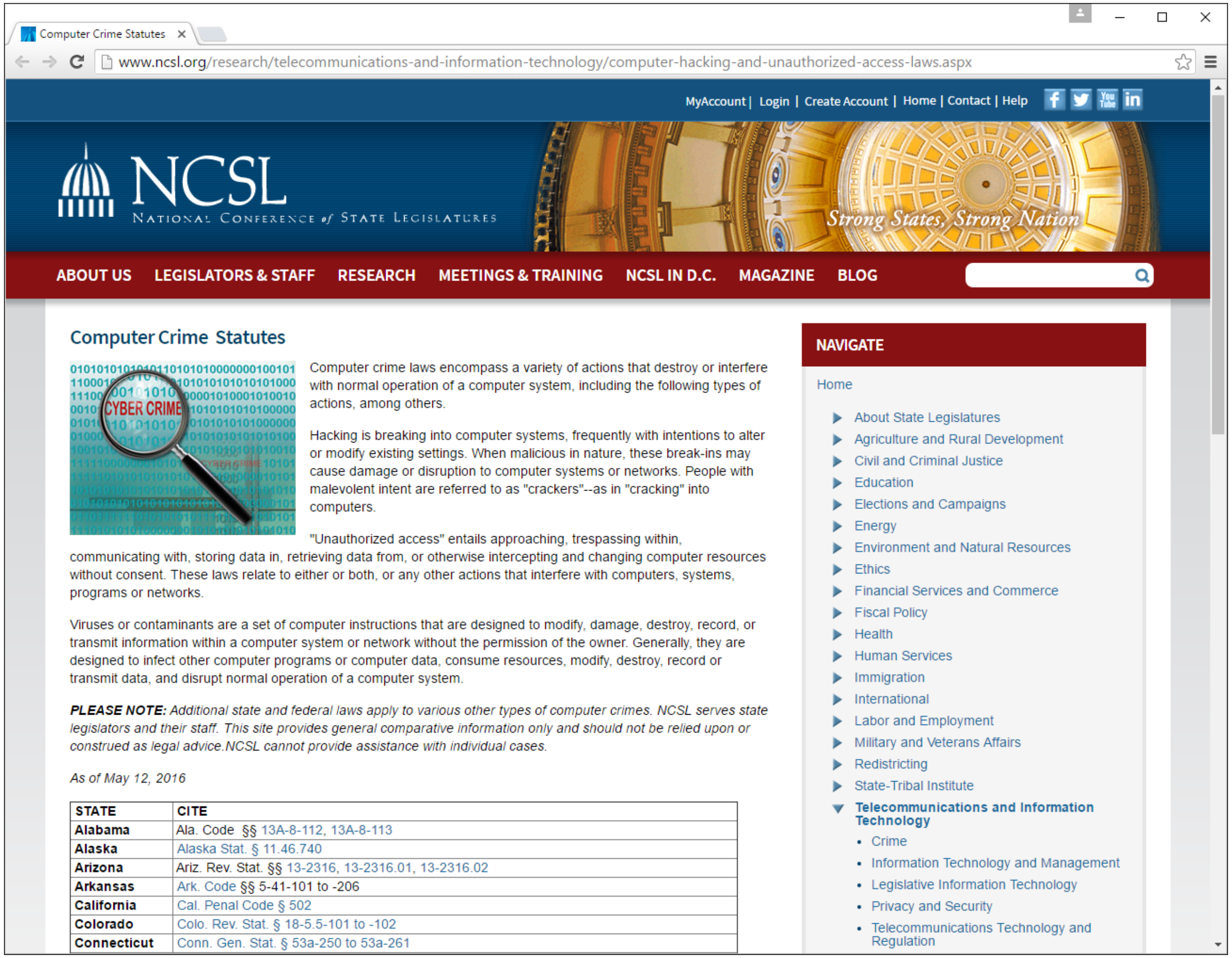
Offense	Section	Sentence*
Obtaining National Security Information	(a)(1)	10 (20) years
Accessing a Computer and Obtaining Information	(a)(2)	1 or 5 (10)
Trespassing in a Government Computer	(a)(3)	1 (10)
Accessing a Computer to Defraud & Obtain Value	(a)(4)	5 (10)
Intentionally Damaging by Knowing Transmission	(a)(5)(A)	1 or 10 (20)
Recklessly Damaging by Intentional Access	(a)(5)(B)	1 or 5 (20)
Negligently Causing Damage & Loss by Intentional Access	(a)(5)(C)	1 (10)
Trafficking in Passwords	(a)(6)	1 (10)
Extortion Involving Computers	(a)(7)	5 (10)

* The maximum prison sentences for second convictions are noted in parentheses.

Prison sentences for violations of the CFAA range from 1 to 20 years.

https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf

State


Computer Crime Statutes
www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx
MyAccount | Login | Create Account | Home | Contact | Help
NCSL
National Conference of State Legislatures
Strong States, Strong Nation
ABOUT US
LEGISLATORS & STAFF
RESEARCH
MEETINGS & TRAINING
NCSL IN D.C.
MAGAZINE
BLOG
CYBER CRIME
NAVIGATE
Home
About State Legislatures
Agriculture and Rural Development
Civil and Criminal Justice
Education
Elections and Campaigns
Energy
Environment and Natural Resources
Ethics
Financial Services and Commerce
Fiscal Policy
Health
Human Services
Immigration
International
Labor and Employment
Military and Veterans Affairs
Redistricting
State-Tribal Institute
Telecommunications and Information Technology
Crime
Information Technology and Management
Legislative Information Technology
Privacy and Security
Telecommunications Technology and Regulation

Computer Crime Statutes

Computer crime laws encompass a variety of actions that destroy or interfere with normal operation of a computer system, including the following types of actions, among others.

Hacking is breaking into computer systems, frequently with intentions to alter or modify existing settings. When malicious in nature, these break-ins may cause damage or disruption to computer systems or networks. People with malevolent intent are referred to as "crackers"--as in "cracking" into computers.

"Unauthorized access" entails approaching, trespassing within, communicating with, storing data in, retrieving data from, or otherwise intercepting and changing computer resources without consent. These laws relate to either or both, or any other actions that interfere with computers, systems, programs or networks.

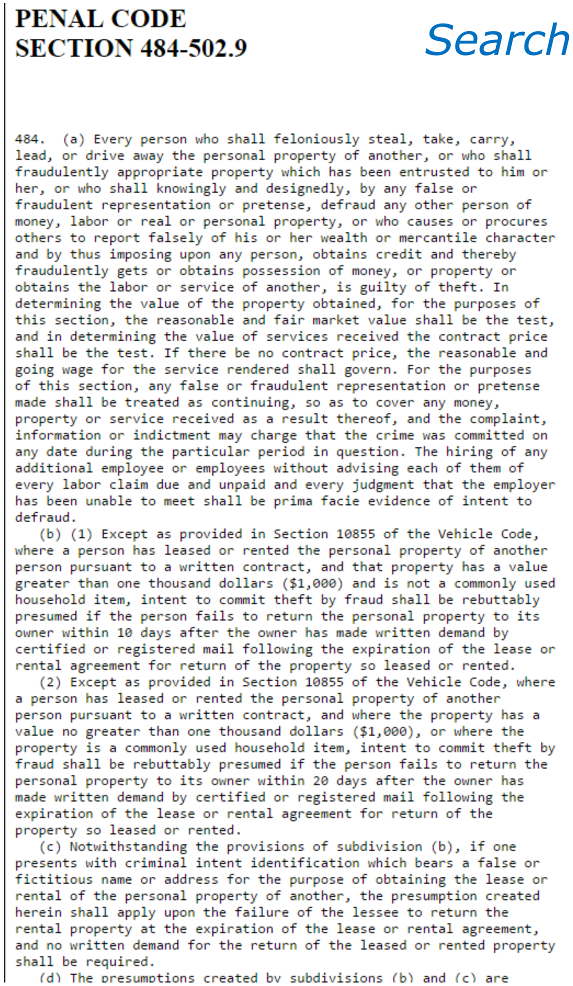
Viruses or contaminants are a set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer system or network without the permission of the owner. Generally, they are designed to infect other computer programs or computer data, consume resources, modify, destroy, record or transmit data, and disrupt normal operation of a computer system.

PLEASE NOTE: *Additional state and federal laws apply to various other types of computer crimes. NCSL serves state legislators and their staff. This site provides general comparative information only and should not be relied upon or construed as legal advice.NCSL cannot provide assistance with individual cases.*

As of May 12, 2016

STATE	CITE
Alabama	Ala. Code §§ 13A-8-112, 13A-8-113
Alaska	Alaska Stat. § 11.46.740
Arizona	Ariz. Rev. Stat. §§ 13-2316, 13-2316.01, 13-2316.02
Arkansas	Ark. Code §§ 5-41-101 to -206
California	Cal. Penal Code § 502
Colorado	Colo. Rev. Stat. § 18-5.5-101 to -102
Connecticut	Conn. Gen. Stat. § 53a-250 to 53a-261

California Penal Code 484-502.9



PENAL CODE
SECTION 484-502.9

484. (a) Every person who shall feloniously steal, take, carry, lead, or drive away the personal property of another, or who shall fraudulently appropriate property which has been entrusted to him or her, or who shall knowingly and designedly, by any false or fraudulent representation or pretense, defraud any other person of money, labor or real or personal property, or who causes or procures others to report falsely of his or her wealth or mercantile character and by thus imposing upon any person, obtains credit and thereby fraudulently gets or obtains possession of money, or property or obtains the labor or service of another, is guilty of theft. In determining the value of the property obtained, for the purposes of this section, the reasonable and fair market value shall be the test, and in determining the value of services received the contract price shall be the test. If there be no contract price, the reasonable and going wage for the service rendered shall govern. For the purposes of this section, any false or fraudulent representation or pretense made shall be treated as continuing, so as to cover any money, property or service received as a result thereof, and the complaint, information or indictment may charge that the crime was committed on any date during the particular period in question. The hiring of any additional employee or employees without advising each of them of every labor claim due and unpaid and every judgment that the employer has been unable to meet shall be prima facie evidence of intent to defraud.

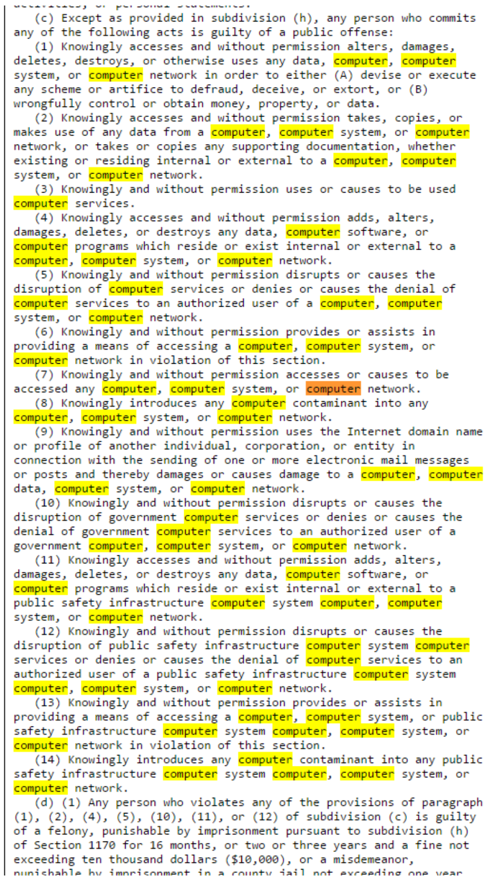
(b) (1) Except as provided in Section 10855 of the Vehicle Code, where a person has leased or rented the personal property of another person pursuant to a written contract, and that property has a value greater than one thousand dollars ($1,000) and is not a commonly used household item, intent to commit theft by fraud shall be rebuttably presumed if the person fails to return the personal property to its owner within 10 days after the owner has made written demand by certified or registered mail following the expiration of the lease or rental agreement for return of the property so leased or rented.

(2) Except as provided in Section 10855 of the Vehicle Code, where a person has leased or rented the personal property of another person pursuant to a written contract, and where the property has a value no greater than one thousand dollars ($1,000), or where the property is a commonly used household item, intent to commit theft by fraud shall be rebuttably presumed if the person fails to return the personal property to its owner within 20 days after the owner has made written demand by certified or registered mail following the expiration of the lease or rental agreement for return of the property so leased or rented.

(c) Notwithstanding the provisions of subdivision (b), if one presents with criminal intent identification which bears a false or fictitious name or address for the purpose of obtaining the lease or rental of the personal property of another, the presumption created herein shall apply upon the failure of the lessee to return the rental property at the expiration of the lease or rental agreement, and no written demand for the return of the leased or rented property shall be required.

(d) The presumptions created by subdivisions (b) and (c) are

Search document for computer



activities, or personal statements.

(c) Except as provided in subdivision (h), any person who commits any of the following acts is guilty of a public offense:

(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.

(2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.

(3) Knowingly and without permission uses or causes to be used computer services.

(4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.

(5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.

(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.

(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

(8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

(9) Knowingly and without permission uses the Internet domain name or profile of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages or posts and thereby damages or causes damage to a computer, computer data, computer system, or computer network.

(10) Knowingly and without permission disrupts or causes the disruption of government computer services or denies or causes the denial of government computer services to an authorized user of a government computer, computer system, or computer network.

(11) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a public safety infrastructure computer system computer, computer system, or computer network.

(12) Knowingly and without permission disrupts or causes the disruption of public safety infrastructure computer system computer services or denies or causes the denial of computer services to an authorized user of a public safety infrastructure computer system computer, computer system, or computer network.

(13) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or public safety infrastructure computer system computer, computer system, or computer network in violation of this section.

(14) Knowingly introduces any computer contaminant into any public safety infrastructure computer system computer, computer system, or computer network.

(d) (1) Any person who violates any of the provisions of paragraph (1), (2), (4), (5), (10), (11), or (12) of subdivision (c) is guilty of a felony, punishable by imprisonment pursuant to subdivision (h) of Section 1170 for 16 months, or two or three years and a fine not exceeding ten thousand dollars ($10,000), or a misdemeanor, punishable by imprisonment in a county jail not exceeding one year

https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=PEN&division=&title=13.&part=1.&chapter=5.&article=

California Penal Code § 502 (c)

CALIFORNIA PENAL CODE 502(c)
"COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT"

(c) Except as provided in subdivision (h), any person who commits any of the following acts is guilty of a public offense:

(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.

(2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.

(3) Knowingly and without permission uses or causes to be used computer services.

(4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.

(5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.

(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.

https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=502.&lawCode=PEN

(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

(8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

(9) Knowingly and without permission uses the Internet domain name of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages, and thereby damages or causes damage to a computer, computer system, or computer network.

(10) Knowingly and without permission disrupts or causes the disruption of government computer services or denies or causes the denial of government computer services to an authorized user of a government computer, computer system, or computer network.

(11) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a public safety infrastructure computer system computer, computer system, or computer network.

(12) Knowingly and without permission disrupts or causes the disruption of public safety infrastructure computer system computer services or denies or causes the denial of computer services to an authorized user of a public safety infrastructure computer system computer, computer system, or computer network.

(13) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or public safety infrastructure computer system computer, computer system, or computer network in violation of this section.

(14) Knowingly introduces any computer contaminant into any public safety infrastructure computer system computer, computer system, or computer network

California Law Activity

Open the California Penal Code at:

https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=502.&lawCode=PEN

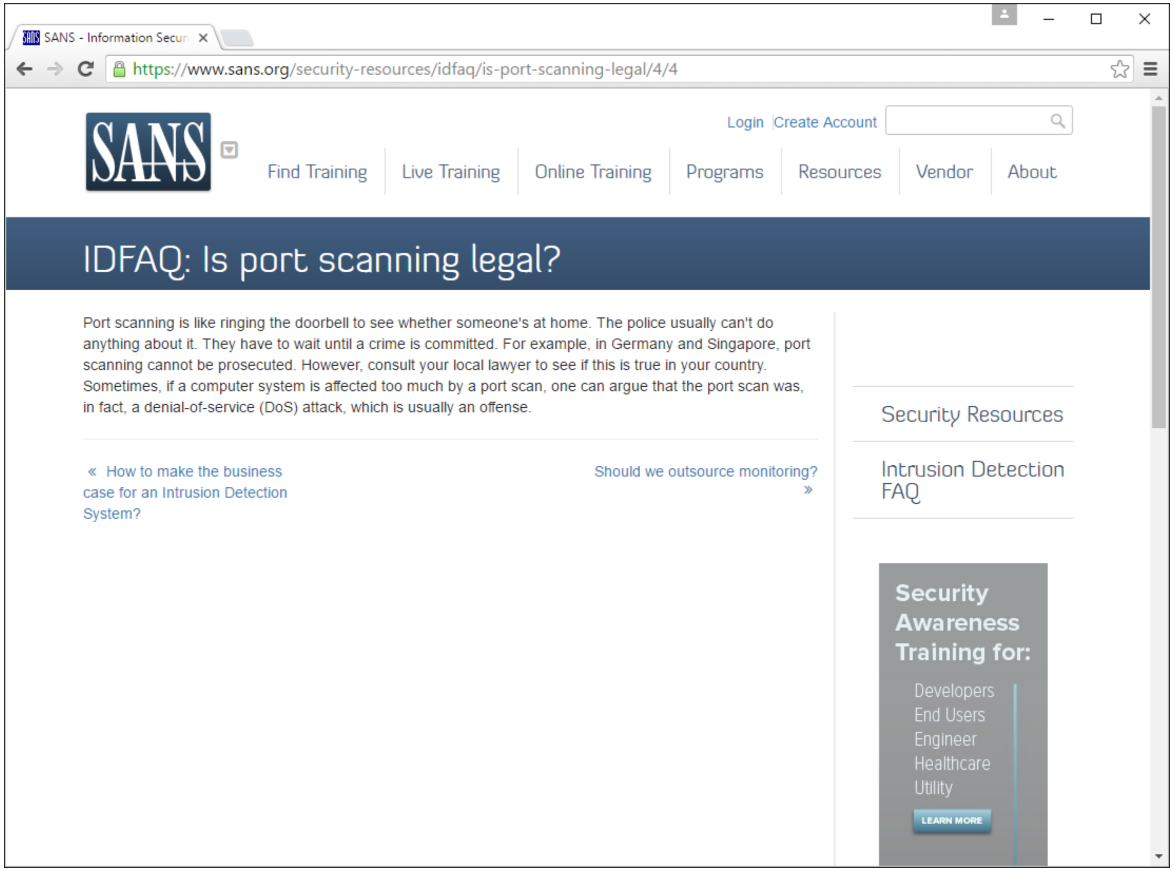
and locate § 502 (c) (1-14).

Which sub clause, 1-14, may be applicable to unintentionally crashing a target computer system while doing a vulnerability scan.

Put your answer in the chat window

Are port scans legal?

Is port scanning legal?



IDFAQ: Is port scanning legal?

Port scanning is like ringing the doorbell to see whether someone's at home. The police usually can't do anything about it. They have to wait until a crime is committed. For example, in Germany and Singapore, port scanning cannot be prosecuted. However, consult your local lawyer to see if this is true in your country. Sometimes, if a computer system is affected too much by a port scan, one can argue that the port scan was, in fact, a denial-of-service (DoS) attack, which is usually an offense.

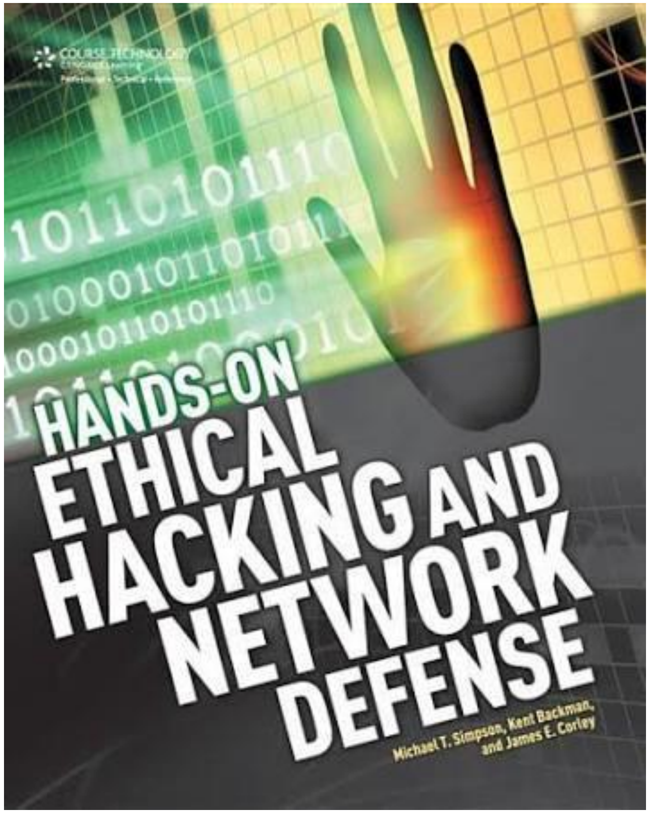
« How to make the business case for an Intrusion Detection System?

Should we outsource monitoring? »

https://www.sans.org/security-resources/idfaq/is-port-scanning-legal/4/4

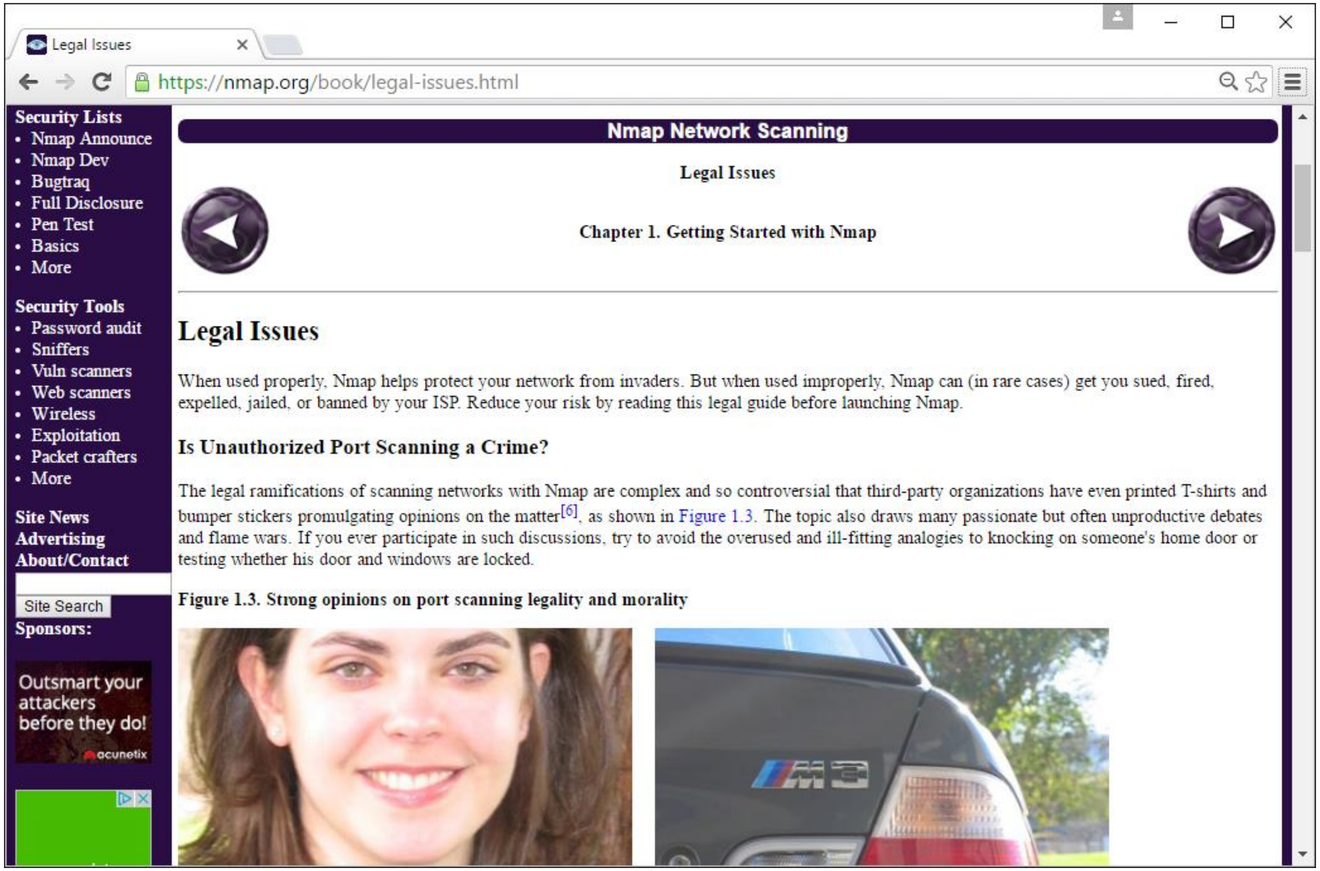
This SANS FAQ says that laws on port scans vary by country. However it could be argued that a port scan caused a DoS which could be prosecuted.

Is port scanning legal?



Our textbook says it is legal in some states but could still result in expensive lawsuits. Each state has different laws.

Is port scanning legal?



Nmap Network Scanning

Legal Issues

Chapter 1. Getting Started with Nmap

Legal Issues

When used properly, Nmap helps protect your network from invaders. But when used improperly, Nmap can (in rare cases) get you sued, fired, expelled, jailed, or banned by your ISP. Reduce your risk by reading this legal guide before launching Nmap.

Is Unauthorized Port Scanning a Crime?

The legal ramifications of scanning networks with Nmap are complex and so controversial that third-party organizations have even printed T-shirts and bumper stickers promulgating opinions on the matter[6], as shown in Figure 1.3. The topic also draws many passionate but often unproductive debates and flame wars. If you ever participate in such discussions, try to avoid the overused and ill-fitting analogies to knocking on someone's home door or testing whether his door and windows are locked.

Figure 1.3. Strong opinions on port scanning legality and morality

https://www.sans.org/security-resources/idfaq/is-port-scanning-legal/4/4

The nmap site urges always getting written permission from the target network and to check your ISP Acceptable Use Policy.

Is port scanning legal?

- Port scanning is often compared to knocking on the doors of all houses in a neighborhood to see if anyone answers.

- A US District Court in Georgia ruled that the port scans conducted by Scott Mouton did not violate the CFAA (18 U.S.C. Section 1030) or the Georgia Computer Systems Protection Act. http://www.internetlibrary.com/cases/lib_case37.cfm

- Your ISP can terminate your service if you violate their Acceptable Use Policies.

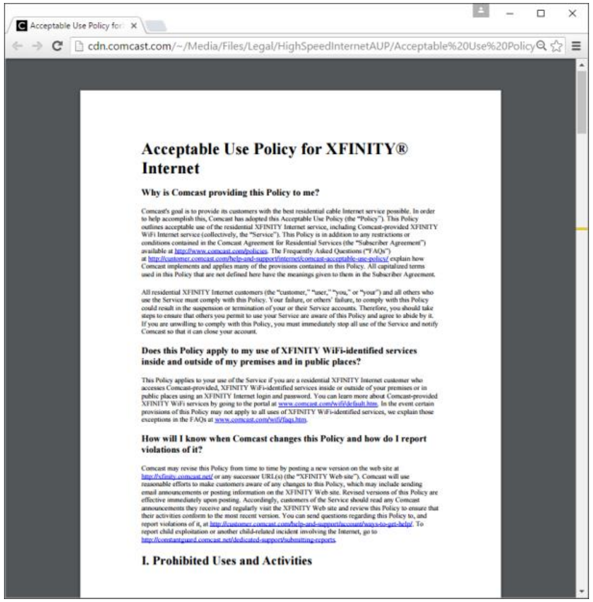
- Defending against lawsuits can be expensive and harm your reputation.

- Remember an ethical hacker will not conduct any hacking activities without explicit permission from the owners of the equipment being used (at both ends).

ISP Acceptable Use Policies

Is port scanning legal?

Comcast XFINITY


Acceptable Use Policy for
cdn.comcast.com/~/Media/Files/Legal/HighSpeedInternetAUP/Acceptable%20Use%20Policy

Acceptable Use Policy for XFINITY® Internet

Why is Comcast providing this Policy to me?

Comcast's goal is to provide its customers with the best residential cable Internet service possible. In order to help accomplish this, Comcast has adopted this Acceptable Use Policy (the "Policy"). This Policy outlines acceptable use of the residential XFINITY Internet service, including Comcast-provided XFINITY WiFi Internet service (collectively, the "Service"). This Policy is in addition to any restrictions or conditions contained in the Comcast Agreement for Residential Services (the "Subscriber Agreement") available at http://www.comcast.com/policies. The Frequently Asked Questions ("FAQs") at http://customer.comcast.com/help-and-support/internet/comcast-acceptable-use-policy/ explain how Comcast implements and applies many of the provisions contained in this Policy. All capitalized terms used in this Policy that are not defined here have the meanings given to them in the Subscriber Agreement.

All residential XFINITY Internet customers (the "customer," "user," "you," or "your") and all others who use the Service must comply with this Policy. Your failure, or others' failure, to comply with this Policy could result in the suspension or termination of your or their Service accounts. Therefore, you should take steps to ensure that others you permit to use your Service are aware of this Policy and agree to abide by it. If you are unwilling to comply with this Policy, you must immediately stop all use of the Service and notify Comcast so that it can close your account.

Does this Policy apply to my use of XFINITY WiFi-identified services inside and outside of my premises and in public places?

This Policy applies to your use of the Service if you are a residential XFINITY Internet customer who accesses Comcast-provided, XFINITY WiFi-identified services inside or outside of your premises or in public places using an XFINITY Internet login and password. You can learn more about Comcast-provided XFINITY WiFi services by going to the portal at www.comcast.com/wifi/default.htm. In the event certain provisions of this Policy may not apply to all uses of XFINITY WiFi-identified services, we explain those exceptions in the FAQs at www.comcast.com/wifi/faqs.htm.

How will I know when Comcast changes this Policy and how do I report violations of it?

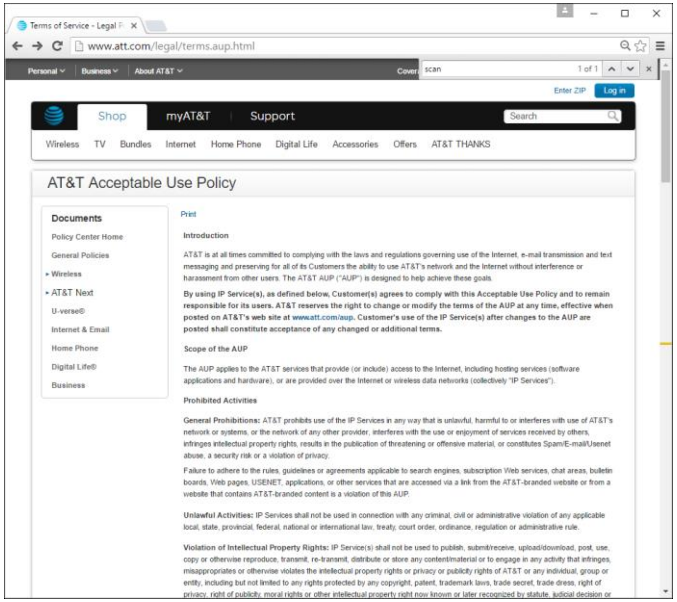
Comcast may revise this Policy from time to time by posting a new version on the web site at http://xfinity.comcast.net/ or any successor URL(s) (the "XFINITY Web site"). Comcast will use reasonable efforts to make customers aware of any changes to this Policy, which may include sending email announcements or posting information on the XFINITY Web site. Revised versions of this Policy are effective immediately upon posting. Accordingly, customers of the Service should read any Comcast announcements they receive and regularly visit the XFINITY Web site and review this Policy to ensure that their activities conform to the most recent version. You can send questions regarding this Policy to, and report violations of it, at http://customer.comcast.com/help-and-support/account/ways-to-get-help/. To report child exploitation or another child-related incident involving the Internet, go to http://constantguard.comcast.net/dedicated-support/submitting-reports.

I. Prohibited Uses and Activities

http://www.xfinity.com/Corporate/Customers/Policies/HighSpeedInternetAUP.html

"Unauthorized port scanning is strictly prohibited;"

AT&T



AT&T Acceptable Use Policy

Introduction

AT&T is at all times committed to complying with the laws and regulations governing use of the Internet, e-mail transmission and text messaging and preserving for all of its Customers the ability to use AT&T's network and the Internet without interference or harassment from other users. The AT&T AUP ("AUP") is designed to help achieve these goals.

By using IP Service(s), as defined below, Customer(s) agrees to comply with this Acceptable Use Policy and to remain responsible for its users. AT&T reserves the right to change or modify the terms of the AUP at any time, effective when posted on AT&T's web site at www.att.com/aup. Customer's use of the IP Service(s) after changes to the AUP are posted shall constitute acceptance of any changed or additional terms.

Scope of the AUP

The AUP applies to the AT&T services that provide (or include) access to the Internet, including hosting services (software applications and hardware), or are provided over the Internet or wireless data networks (collectively "IP Services").

Prohibited Activities

General Prohibitions: AT&T prohibits use of the IP Services in any way that is unlawful, harmful to or interferes with use of AT&T's network or systems, or the network of any other provider, interferes with the use or enjoyment of services received by others, infringes intellectual property rights, results in the publication of threatening or offensive material, or constitutes Spam/E-mail/Usenet abuse, a security risk or a violation of privacy.

Failure to adhere to the rules, guidelines or agreements applicable to search engines, subscription Web services, chat areas, bulletin boards, Web pages, USENET, applications, or other services that are accessed via a link from the AT&T-branded website or from a website that contains AT&T-branded content is a violation of this AUP.

Unlawful Activities: IP Services shall not be used in connection with any criminal, civil or administrative violation of any applicable local, state, provincial, federal, national or international law, treaty, court order, ordinance, regulation or administrative rule.

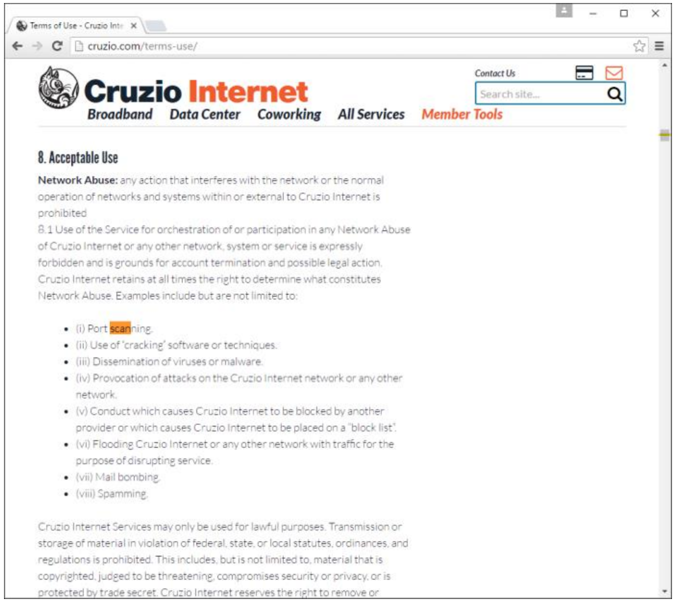
Violation of Intellectual Property Rights: IP Service(s) shall not be used to publish, submit/receive, upload/download, post, use, copy or otherwise reproduce, transmit, re-transmit, distribute or store any content/material or to engage in any activity that infringes, misappropriates or otherwise violates the intellectual property rights or privacy or publicity rights of AT&T or any individual, group or entity, including but not limited to any rights protected by any copyright, patent, trademark laws, trade secret, trade dress, right of privacy, right of publicity, moral rights or other intellectual property right now known or later recognized by statute, judicial decision or

http://www.att.com/legal/terms.internetAttTermsOfService.html

"Examples of system or network security violations include but are not limited to unauthorized monitoring, scanning or probing of network or system ..."

Is port scanning legal?

Cruzio



8. Acceptable Use

Network Abuse: any action that interferes with the network or the normal operation of networks and systems within or external to Cruzio Internet is prohibited
8.1 Use of the Service for orchestration of or participation in any Network Abuse of Cruzio Internet or any other network, system or service is expressly forbidden and is grounds for account termination and possible legal action. Cruzio Internet retains at all times the right to determine what constitutes Network Abuse. Examples include but are not limited to:

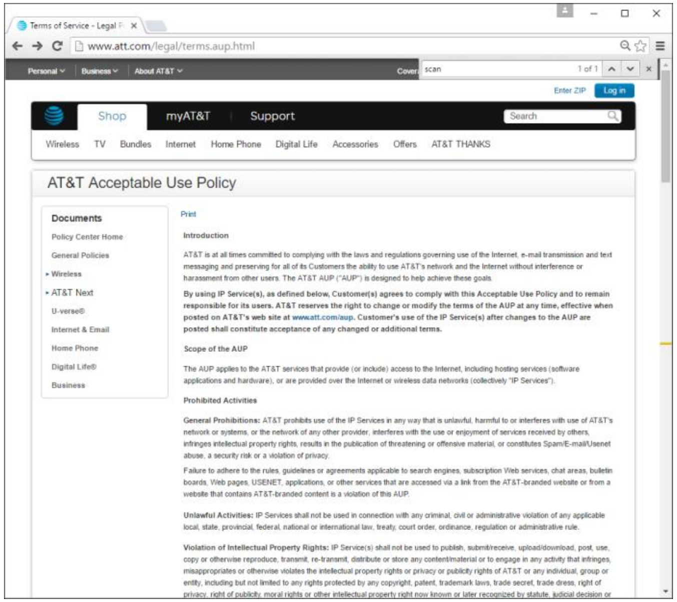
- (i) Port scanning.
- (ii) Use of 'cracking' software or techniques.
- (iii) Dissemination of viruses or malware.
- (iv) Provocation of attacks on the Cruzio Internet network or any other network.
- (v) Conduct which causes Cruzio Internet to be blocked by another provider or which causes Cruzio Internet to be placed on a "block list".
- (vi) Flooding Cruzio Internet or any other network with traffic for the purpose of disrupting service.
- (vii) Mail bombing.
- (viii) Spamming.

Cruzio Internet Services may only be used for lawful purposes. Transmission or storage of material in violation of federal, state, or local statutes, ordinances, and regulations is prohibited. This includes, but is not limited to, material that is copyrighted, judged to be threatening, compromises security or privacy, or is protected by trade secret. Cruzio Internet reserves the right to remove or

http://cruzio.com/terms-use/

"... Network Abuse. Examples include but are not limited to: (i) Port scanning ..."

Charter



AT&T Acceptable Use Policy

Introduction

AT&T is at all times committed to complying with the laws and regulations governing use of the Internet, e-mail transmission and text messaging and preserving for all of its Customers the ability to use AT&T's network and the Internet without interference or harassment from other users. The AT&T AUP ("AUP") is designed to help achieve these goals.

By using IP Service(s), as defined below, Customer(s) agrees to comply with this Acceptable Use Policy and to remain responsible for its users. AT&T reserves the right to change or modify the terms of the AUP at any time, effective when posted on AT&T's web site at www.att.com/aup. Customer's use of the IP Service(s) after changes to the AUP are posted shall constitute acceptance of any changed or additional terms.

Scope of the AUP

The AUP applies to the AT&T services that provide (or include) access to the Internet, including hosting services (software applications and hardware), or are provided over the Internet or wireless data networks (collectively "IP Services").

Prohibited Activities

General Prohibitions: AT&T prohibits use of the IP Services in any way that is unlawful, harmful to or interferes with use of AT&T's network or systems, or the network of any other provider, interferes with the use or enjoyment of services received by others, infringes intellectual property rights, results in the publication of threatening or offensive material, or constitutes Spam/E-mail/Usenet abuse, a security risk or a violation of privacy.

Failure to adhere to the rules, guidelines or agreements applicable to search engines, subscription Web services, chat areas, bulletin boards, Web pages, USENET, applications, or other services that are accessed via a link from the AT&T-branded website or from a website that contains AT&T-branded content is a violation of this AUP.

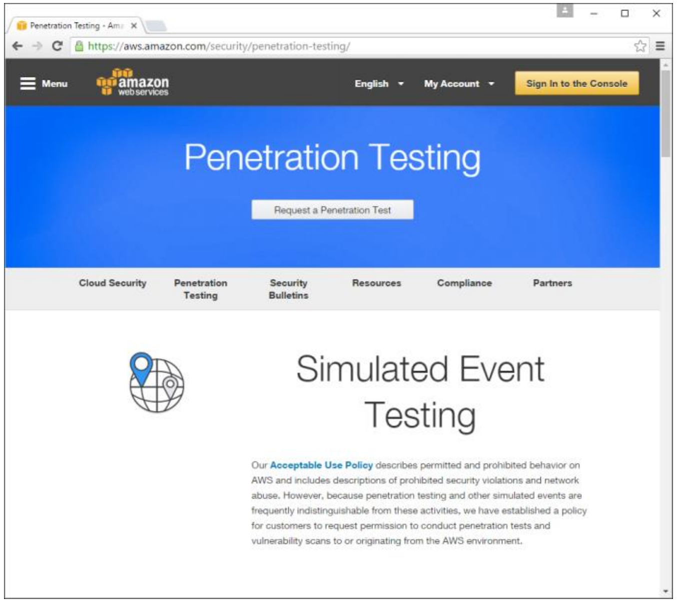
Unlawful Activities: IP Services shall not be used in connection with any criminal, civil or administrative violation of any applicable local, state, provincial, federal, national or international law, treaty, court order, ordinance, regulation or administrative rule.

Violation of Intellectual Property Rights: IP Service(s) shall not be used to publish, submit/receive, upload/download, post, use, copy or otherwise reproduce, transmit, re-transmit, distribute or store any content/material or to engage in any activity that infringes, misappropriates or otherwise violates the intellectual property rights or privacy or publicity rights of AT&T or any individual, group or entity, including but not limited to any rights protected by any copyright, patent, trademark laws, trade secret, trade dress, right of privacy, right of publicity, moral rights or other intellectual property right now known or later recognized by statute, judicial decision or

https://www.charter.com/browse/content/policies-comm-acceptable-use

"PROHIBITED ACTIVITIES ... Unauthorized access to or use of data, systems, or networks, including any attempt to probe, scan, or test the vulnerability of a system or network,"

Is port scanning legal?



Penetration Testing

Simulated Event Testing

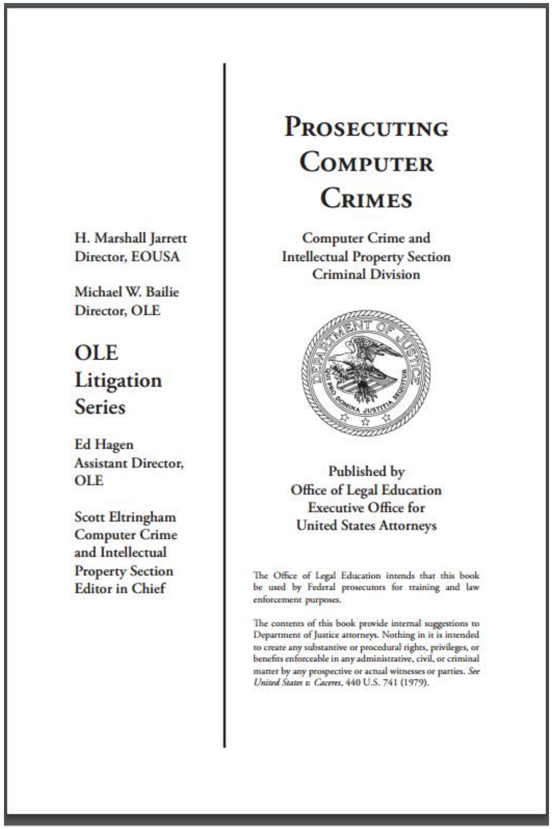
Our **Acceptable Use Policy** describes permitted and prohibited behavior on AWS and includes descriptions of prohibited security violations and network abuse. However, because penetration testing and other simulated events are frequently indistinguishable from these activities, we have established a policy for customers to request permission to conduct penetration tests and vulnerability scans to or originating from the AWS environment.

https://aws.amazon.com/security/penetration-testing/

Note: AWS does allow penetration testing but you must get prior permission!

Is Wi-Fi sniffing legal?

Is Wi-Fi sniffing legal?



H. Marshall Jarrett
Director, EOUSA

Michael W. Bailie
Director, OLE

OLE
Litigation
Series

Ed Hagen
Assistant Director,
OLE

Scott Eltringham
Computer Crime
and Intellectual
Property Section
Editor in Chief

PROSECUTING
COMPUTER
CRIMES

Computer Crime and
Intellectual Property Section
Criminal Division

Published by
Office of Legal Education
Executive Office for
United States Attorneys

The Office of Legal Education intends that this book be used by Federal prosecutors for training and law enforcement purposes.

The contents of this book provide internal suggestions to Department of Justice attorneys. Nothing in it is intended to create any substantive or procedural rights, privileges, or benefits enforceable in any administrative, civil, or criminal matter by any prospective or actual witnesses or parties. *See United States v. Caceres*, 440 U.S. 741 (1979).

"Intercepting a Communication: 18 U.S.C. § 2511(1)(a)
Except as otherwise specifically provided in this chapter any person who—(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication
. . .
shall be punished as provided in subsection (4)."

"A Wiretap Act violation is a Class D felony; the maximum authorized penalties for a violation of section 2511(1) of the Wiretap Act are imprisonment of not more than five years and a fine under Title 18."

https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf

June 2011 - A Silicon Valley federal judge rules Google can be sued for violating the Wiretap act by sniffing personal WiFi network data by its fleet of Smart Cars mapping the Earth.

https://www.wired.com/2011/06/google-wiretap-breach/

April 2012 - Google fined $25,000 by FCC for impeding FCC probe of WiFi sniffing.

http://philadelphia.cbslocal.com/2012/04/16/google-fined-25000-for-impeding-fccs-probe-of-wi-fi-sniffing-case/

September 2012 - An Illinois federal judge rules sniffing open WiFi networks is not wiretapping.

http://arstechnica.com/tech-policy/2012/09/sniffing-open-wifi-networks-is-not-wiretapping-judge-says/

April 2014 - Google asks the Supreme Court to reverse the earlier decision that it could be liable for sniffing unencrypted WiFi network data.

http://arstechnica.com/tech-policy/2014/04/google-tells-supreme-court-its-legal-to-packet-sniff-open-wi-fi-networks/

Certifications

	SB	KV	Simpson Textbook	Concise Cybersecurity
A+ (CompTIA)		1		
Linux Essentials (LPI)		3		
Linux+ (CompTIA)	x			
Network+ (CompTIA)		2	x	
Security+ (CompTIA)	1	4	x	x
CISSP (ISC^2)		6a	x	
CEH (EC-Council)	2	5	x	x
GPEN (SANS/GIAC)	3	6b	x	x
OPST (ISECOM)			x	
OSCP (Offensive Security)	x			x

Vocabulary

Some Terminology

- □ Hacking
- □ Cracking
- □ White hat hacker
- □ Grey hat hacker
- □ Black hat hacker
- □ Nation-state actors
- □ Cybercriminals
- □ Adversary
- □ Hacktivist
- □ Pen Test
- □ Security audit
- □ White box testing
- □ Grey box testing
- □ White box testing
- □ Red Team
- □ Blue Team

- □ Vulnerability
- □ Exploit
- □ Threat
- □ Denial of Service attack
- □ Brute force attack
- □ Buffer overflow
- □ Spoofing
- □ Zero-day
- □ Botnet
- □ Ransomware (link)
- □ Watering hole attack (link)
- □ Man in the middle attack
- □ Fuzzing (link)
- □ Drive-by-download (link)
- □ Cross-side scripting (link)
- □ SQL injection (link)

- □ Malware
- □ Virus
- □ Trojan (link)
- □ Worm (link)
- □ Spyware
- □ Rootkit (link)
- □ Firewall
- □ Signatures (link)
- □ Polymorphism
- □ Exfiltrate
- □ Social engineering
- □ Phishing
- □ Vishing (listen)
- □ Spear-phishing

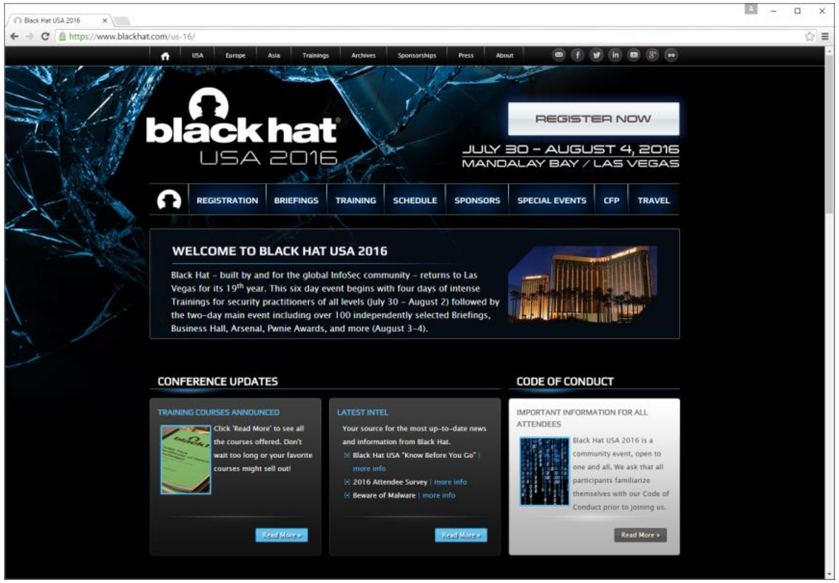
Acronyms

- CVE (Common Vulnerabilities and Exposures)
- DoS (Denial of Service attack)
- DDoS (Distributed Denial of Service attack)
- XSS (Cross-Side Scripting)
- IDS (Intrusion Detection System)
- IPS (Intrusion Prevention System)
- C&C (Command and Control)
- AV (Anti-Virus)
- APT (Advanced Persistent Threat)
- RAT (Remote Access Trojan)

Slang

- ❑ Owned
- ❑ Pwned
- ❑ Meat chicken ("rouji" in Chinese)
- ❑ Doxing
- ❑ Script Kiddie
- ❑ Packet Monkey

Conferences



WELCOME TO BLACK HAT USA 2016

Black Hat – built by and for the global InfoSec community – returns to Las Vegas for its 19th year. This six day event begins with four days of intense Trainings for security practitioners of all levels (July 30 – August 2) followed by the two-day main event including over 100 independently selected Briefings, Business Hall, Arsenal, Pwnie Awards, and more (August 3–4).

CONFERENCE UPDATES

TRAINING COURSES ANNOUNCED

Click 'Read More' to see all the courses offered. Don't wait too long or your favorite courses might sell out!

LATEST INTEL

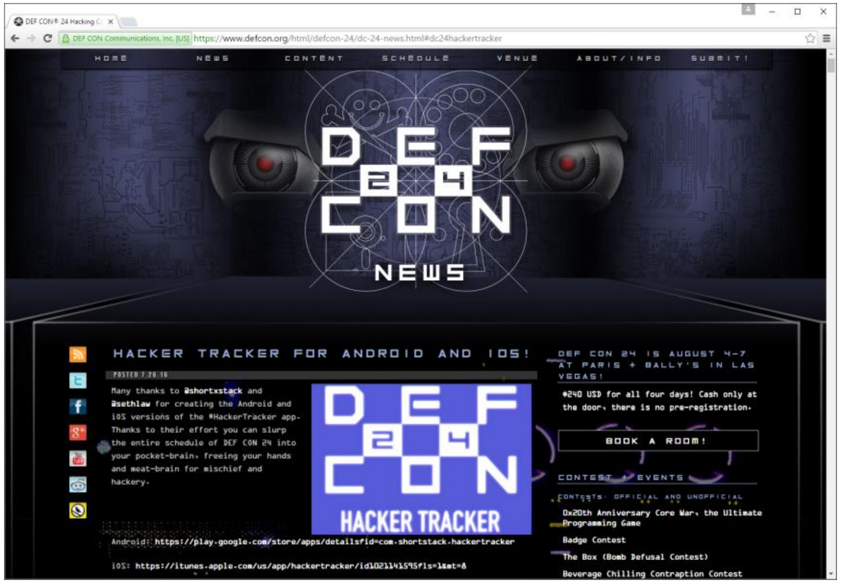
Your source for the most up-to-date news and information from Black Hat.

- Black Hat USA "Know Before You Go" | more info
- 2016 Attendee Survey | more info
- Beware of Malware | more info

CODE OF CONDUCT

IMPORTANT INFORMATION FOR ALL ATTENDEES

Black Hat USA 2016 is a community event, open to one and all. We ask that all participants familiarize themselves with our Code of Conduct prior to joining us.



HACKER TRACKER FOR ANDROID AND IOS!

POSTED 7.26.16

Many thanks to @shortxstack and @sethlaw for creating the Android and iOS versions of the #HackerTracker app. Thanks to their effort you can slurp the entire schedule of DEF CON 24 into your pocket-brain, freeing your hands and meat-brain for mischief and hackery.

Android: https://play.google.com/store/apps/details?id=com.shortstack.hackertracker

iOS: https://itunes.apple.com/us/app/hackertracker/id1021141595?ls=1&mt=8

DEF CON 24 IS AUGUST 4-7 AT PARIS + BALLY'S IN LAS VEGAS!

$240 USD for all four days! Cash only at the door, there is no pre-registration.

CONTEST + EVENTS

CONTESTS: OFFICIAL AND UNOFFICIAL

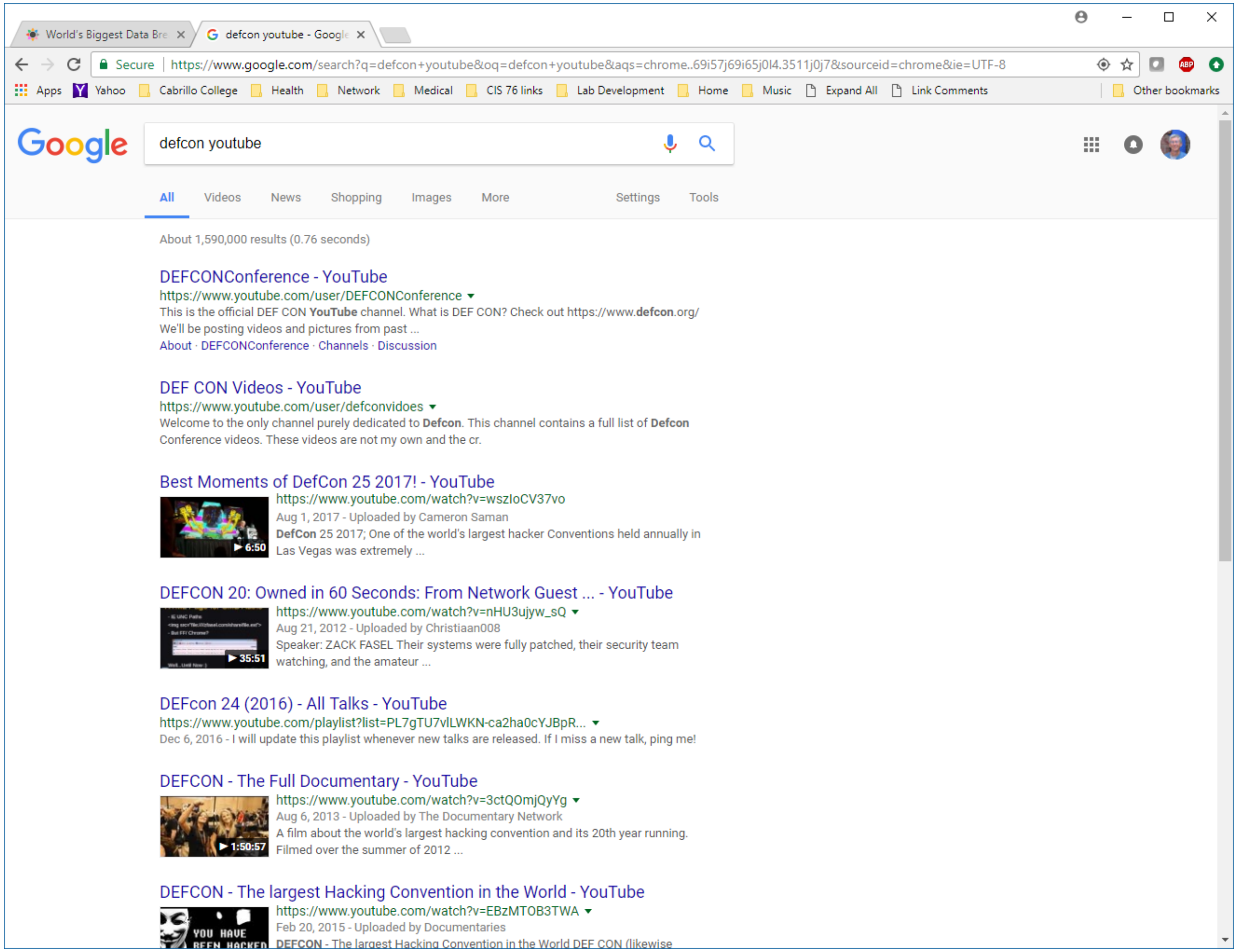
- 0x20th Anniversary Core War, the Ultimate Programming Game
- Badge Contest
- The Box (Bomb Defusal Contest)
- Beverage Chilling Contraption Contest

Black Hat

DEF CON

And many more: ToorCon, Hackers Halted, RSA, OWASP events, ShmooCon, DerbyCon, Thotcon, USENIX...

Google: youtube defcon



About 1,590,000 results (0.76 seconds)

DEFCONConference - YouTube
https://www.youtube.com/user/DEFCONConference ▾
This is the official DEF CON **YouTube** channel. What is DEF CON? Check out https://www.**defcon**.org/ We'll be posting videos and pictures from past ...
About · DEFCONConference · Channels · Discussion

DEF CON Videos - YouTube
https://www.youtube.com/user/defconvidoes ▾
Welcome to the only channel purely dedicated to **Defcon**. This channel contains a full list of **Defcon** Conference videos. These videos are not my own and the cr.

Best Moments of DefCon 25 2017! - YouTube
▶ 6:50
https://www.youtube.com/watch?v=wszIoCV37vo
Aug 1, 2017 - Uploaded by Cameron Saman
DefCon 25 2017; One of the world's largest hacker Conventions held annually in Las Vegas was extremely ...

DEFCON 20: Owned in 60 Seconds: From Network Guest ... - YouTube
▶ 35:51
https://www.youtube.com/watch?v=nHU3ujyw_sQ ▾
Aug 21, 2012 - Uploaded by Christiaan008
Speaker: ZACK FASEL Their systems were fully patched, their security team watching, and the amateur ...

DEFcon 24 (2016) - All Talks - YouTube
https://www.youtube.com/playlist?list=PL7gTU7vlLWKN-ca2ha0cYJBpR... ▾
Dec 6, 2016 - I will update this playlist whenever new talks are released. If I miss a new talk, ping me!

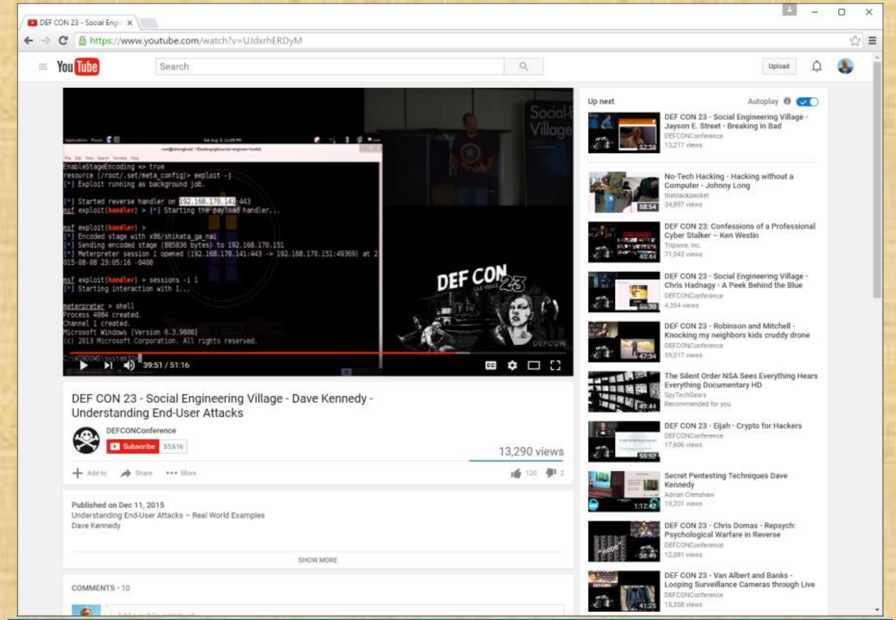
DEFCON - The Full Documentary - YouTube
▶ 1:50:57
https://www.youtube.com/watch?v=3ctQOmjQyYg ▾
Aug 6, 2013 - Uploaded by The Documentary Network
A film about the world's largest hacking convention and its 20th year running. Filmed over the summer of 2012 ...

DEFCON - The largest Hacking Convention in the World - YouTube
YOU HAVE BEEN HACKED
https://www.youtube.com/watch?v=EBzMTOB3TWA ▾
Feb 20, 2015 - Uploaded by Documentaries
DEFCON - The largest Hacking Convention in the World DEF CON (likewise

Conferences like DEFCON publish lots of videos on hacking topics

An Expert at Work Activity

David Kennedy at Def Con 23 hacking a PC with the
Social Engineering Toolkit and Metasploit



```
EnableStageEncoding => true
resource (/root/.set/meta_config)> exploit -j
[*] Exploit running as background job.

[*] Started reverse handler on 192.168.170.141:443
msf exploit(handler) > [*] Starting the payload handler...

msf exploit(handler) >
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (885836 bytes) to 192.168.170.151
[*] Meterpreter session 1 opened (192.168.170.141:443 -> 192.168.170.151:49369) at 2
015-08-08 23:05:16 -0400

msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > shell
Process 4084 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>
```

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

DEFCONConference Subscribe 53,616

13,290 views

Add to Share More 120 2

Published on Dec 11, 2015
Understanding End-User Attacks – Real World Examples
Dave Kennedy

SHOW MORE

COMMENTS • 10

Up next Autoplay

- DEF CON 23 - Social Engineering Village - Jayson E. Street - Breaking in Bad — DEFCONConference — 13,217 views — 52:38
- No-Tech Hacking - Hacking without a Computer - Johnny Long — theblackpacket — 34,897 views — 58:54
- DEF CON 23: Confessions of a Professional Cyber Stalker – Ken Westin — Tripwire, Inc. — 71,043 views — 40:44
- DEF CON 23 - Social Engineering Village - Chris Hadnagy - A Peek Behind the Blue — DEFCONConference — 4,354 views — 55:30
- DEF CON 23 - Robinson and Mitchell - Knocking my neighbors kids cruddy drone — DEFCONConference — 39,017 views — 47:34
- The Silent Order NSA Sees Everything Hears Everything Documentary HD — SpyTechGears — Recommended for you — 49:44
- DEF CON 23 - Eijah - Crypto for Hackers — DEFCONConference — 17,606 views — 55:52
- Secret Pentesting Techniques Dave Kennedy — Adrian Crenshaw — 19,201 views — 1:12:42
- DEF CON 23 - Chris Domas - Repsych: Psychological Warfare in Reverse — DEFCONConference — 12,081 views — 58:49
- DEF CON 23 - Van Albert and Banks - Looping Surveillance Cameras through Live — DEFCONConference — 15,358 views — 41:25

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

1. Watch a portion of this video (34:00-39:45). In the HTA attack what did he mean when he said "there we go, we get our shell"?
   (put your answer in the chat window)

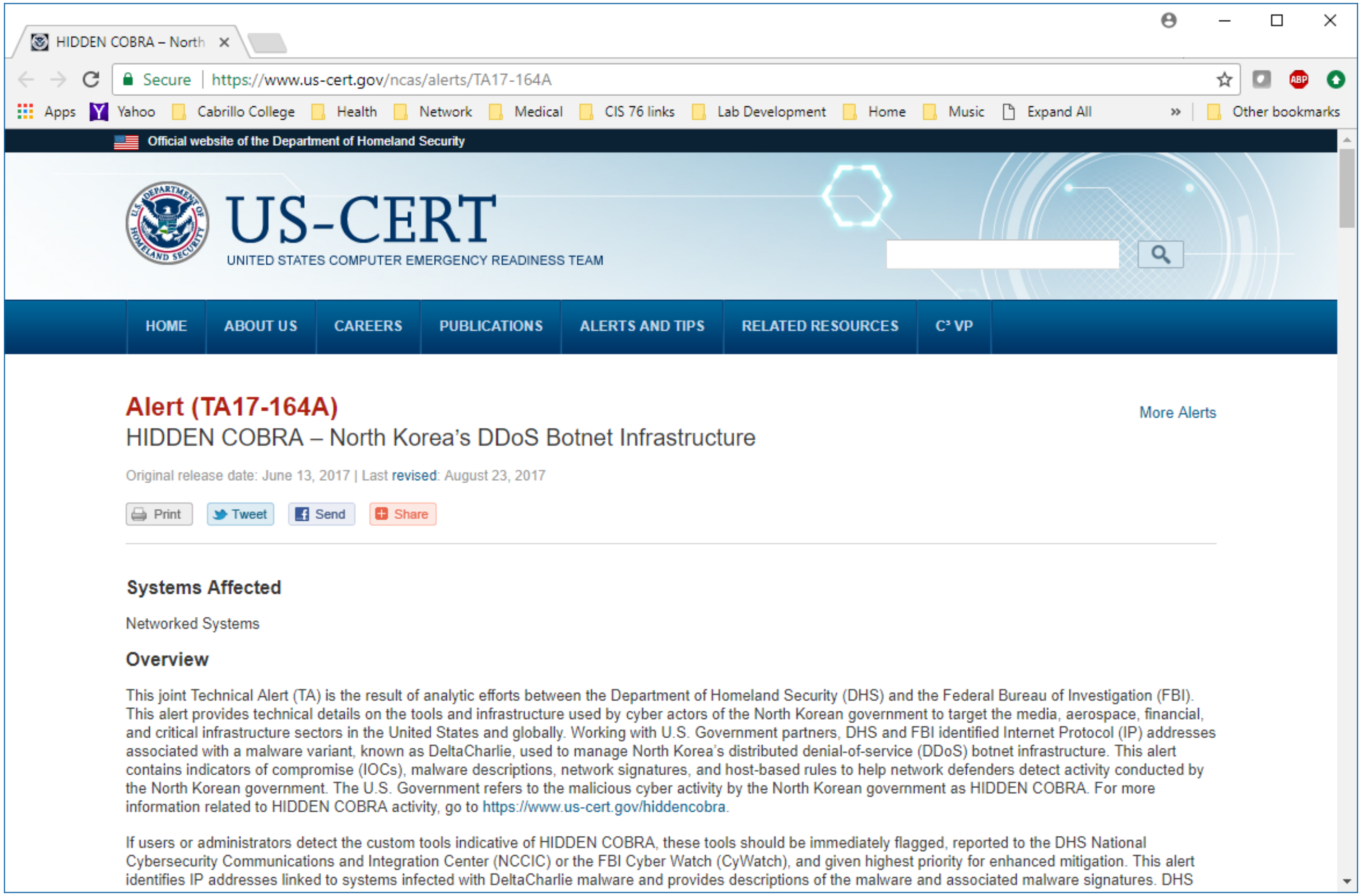
2. Watch a portion of this video (39:45-44:18). In the web-jacking attack what was he able to accomplish?
   (put your answer in the chat window)

Newsletters
and
Blogs

Subscribe or sign up for cyber security newsletters, alerts, blogs and feeds

□ US-CERT
□ SANS
□ Cybrary
□ FireEye
□ CrowdStrike
□ HackerNews
□ Many more ...

Department of Homeland Security - US-CERT


HIDDEN COBRA – North
Secure https://www.us-cert.gov/ncas/alerts/TA17-164A
Apps Yahoo Cabrillo College Health Network Medical CIS 76 links Lab Development Home Music Expand All Other bookmarks
Official website of the Department of Homeland Security
US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM
HOME ABOUT US CAREERS PUBLICATIONS ALERTS AND TIPS RELATED RESOURCES C³ VP
More Alerts
Print Tweet Send Share

Alert (TA17-164A)

HIDDEN COBRA – North Korea's DDoS Botnet Infrastructure

Original release date: June 13, 2017 | Last revised: August 23, 2017

Systems Affected

Networked Systems

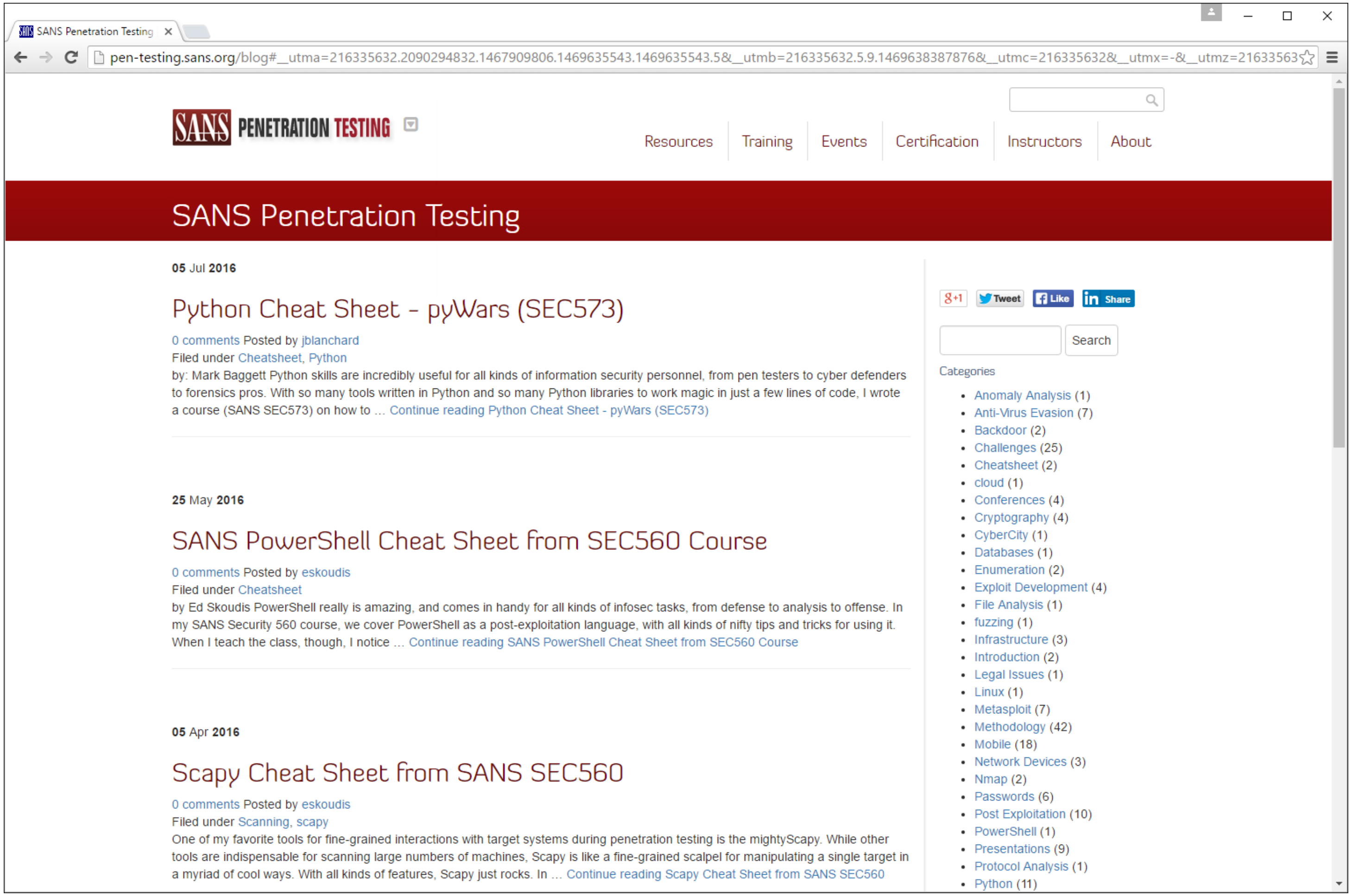
Overview

This joint Technical Alert (TA) is the result of analytic efforts between the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). This alert provides technical details on the tools and infrastructure used by cyber actors of the North Korean government to target the media, aerospace, financial, and critical infrastructure sectors in the United States and globally. Working with U.S. Government partners, DHS and FBI identified Internet Protocol (IP) addresses associated with a malware variant, known as DeltaCharlie, used to manage North Korea's distributed denial-of-service (DDoS) botnet infrastructure. This alert contains indicators of compromise (IOCs), malware descriptions, network signatures, and host-based rules to help network defenders detect activity conducted by the North Korean government. The U.S. Government refers to the malicious cyber activity by the North Korean government as HIDDEN COBRA. For more information related to HIDDEN COBRA activity, go to https://www.us-cert.gov/hiddencobra.

If users or administrators detect the custom tools indicative of HIDDEN COBRA, these tools should be immediately flagged, reported to the DHS National Cybersecurity Communications and Integration Center (NCCIC) or the FBI Cyber Watch (CyWatch), and given highest priority for enhanced mitigation. This alert identifies IP addresses linked to systems infected with DeltaCharlie malware and provides descriptions of the malware and associated malware signatures. DHS

https://www.us-cert.gov/mailing-lists-and-feeds

SANS Blogs


SANS Penetration Testing
pen-testing.sans.org/blog#__utma=216335632.2090294832.1467909806.1469635543.1469635543.5&__utmb=216335632.5.9.1469638387876&__utmc=216335632&__utmx=-&__utmz=21633563
SANS PENETRATION TESTING
Resources
Training
Events
Certification
Instructors
About
8+1
Tweet
Like
Share
Search

SANS Penetration Testing

05 Jul **2016**

Python Cheat Sheet – pyWars (SEC573)

0 comments Posted by jblanchard
Filed under Cheatsheet, Python

by: Mark Baggett Python skills are incredibly useful for all kinds of information security personnel, from pen testers to cyber defenders to forensics pros. With so many tools written in Python and so many Python libraries to work magic in just a few lines of code, I wrote a course (SANS SEC573) on how to … Continue reading Python Cheat Sheet - pyWars (SEC573)

25 May **2016**

SANS PowerShell Cheat Sheet from SEC560 Course

0 comments Posted by eskoudis
Filed under Cheatsheet

by Ed Skoudis PowerShell really is amazing, and comes in handy for all kinds of infosec tasks, from defense to analysis to offense. In my SANS Security 560 course, we cover PowerShell as a post-exploitation language, with all kinds of nifty tips and tricks for using it. When I teach the class, though, I notice … Continue reading SANS PowerShell Cheat Sheet from SEC560 Course

05 Apr **2016**

Scapy Cheat Sheet from SANS SEC560

0 comments Posted by eskoudis
Filed under Scanning, scapy

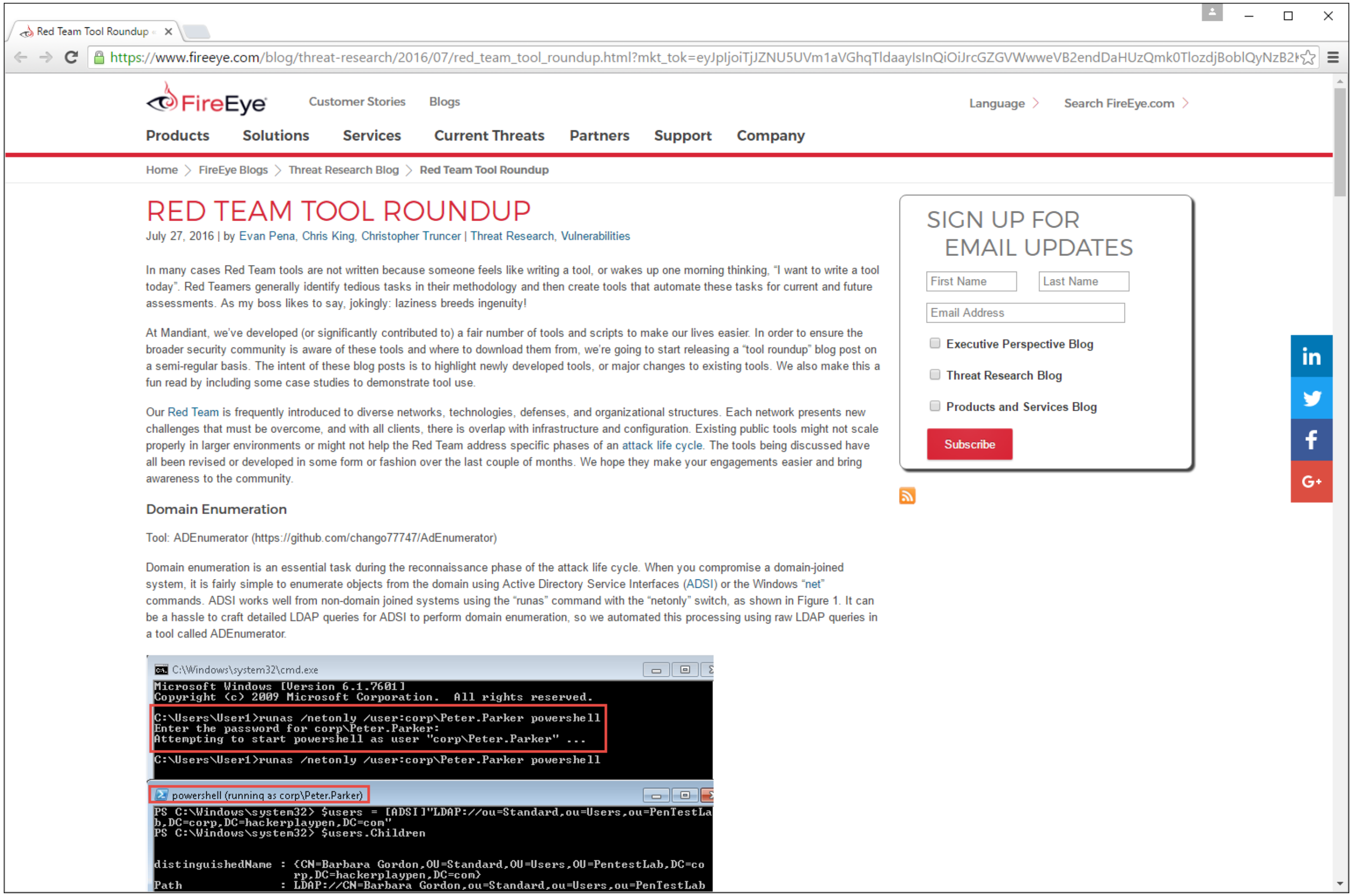
One of my favorite tools for fine-grained interactions with target systems during penetration testing is the mightyScapy. While other tools are indispensable for scanning large numbers of machines, Scapy is like a fine-grained scalpel for manipulating a single target in a myriad of cool ways. With all kinds of features, Scapy just rocks. In … Continue reading Scapy Cheat Sheet from SANS SEC560

Categories

- Anomaly Analysis (1)
- Anti-Virus Evasion (7)
- Backdoor (2)
- Challenges (25)
- Cheatsheet (2)
- cloud (1)
- Conferences (4)
- Cryptography (4)
- CyberCity (1)
- Databases (1)
- Enumeration (2)
- Exploit Development (4)
- File Analysis (1)
- fuzzing (1)
- Infrastructure (3)
- Introduction (2)
- Legal Issues (1)
- Linux (1)
- Metasploit (7)
- Methodology (42)
- Mobile (18)
- Network Devices (3)
- Nmap (2)
- Passwords (6)
- Post Exploitation (10)
- PowerShell (1)
- Presentations (9)
- Protocol Analysis (1)
- Python (11)

https://www.sans.org/security-resources/blogs

FireEye Blogs



RED TEAM TOOL ROUNDUP

July 27, 2016 | by Evan Pena, Chris King, Christopher Truncer | Threat Research, Vulnerabilities

In many cases Red Team tools are not written because someone feels like writing a tool, or wakes up one morning thinking, "I want to write a tool today". Red Teamers generally identify tedious tasks in their methodology and then create tools that automate these tasks for current and future assessments. As my boss likes to say, jokingly: laziness breeds ingenuity!

At Mandiant, we've developed (or significantly contributed to) a fair number of tools and scripts to make our lives easier. In order to ensure the broader security community is aware of these tools and where to download them from, we're going to start releasing a "tool roundup" blog post on a semi-regular basis. The intent of these blog posts is to highlight newly developed tools, or major changes to existing tools. We also make this a fun read by including some case studies to demonstrate tool use.

Our Red Team is frequently introduced to diverse networks, technologies, defenses, and organizational structures. Each network presents new challenges that must be overcome, and with all clients, there is overlap with infrastructure and configuration. Existing public tools might not scale properly in larger environments or might not help the Red Team address specific phases of an attack life cycle. The tools being discussed have all been revised or developed in some form or fashion over the last couple of months. We hope they make your engagements easier and bring awareness to the community.

Domain Enumeration

Tool: ADEnumerator (https://github.com/chango77747/AdEnumerator)

Domain enumeration is an essential task during the reconnaissance phase of the attack life cycle. When you compromise a domain-joined system, it is fairly simple to enumerate objects from the domain using Active Directory Service Interfaces (ADSI) or the Windows "net" commands. ADSI works well from non-domain joined systems using the "runas" command with the "netonly" switch, as shown in Figure 1. It can be a hassle to craft detailed LDAP queries for ADSI to perform domain enumeration, so we automated this processing using raw LDAP queries in a tool called ADEnumerator.

C:\Windows\system32\cmd.exe

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\User1>runas /netonly /user:corp\Peter.Parker powershell
Enter the password for corp\Peter.Parker:
Attempting to start powershell as user "corp\Peter.Parker" ...

C:\Users\User1>runas /netonly /user:corp\Peter.Parker powershell
```

powershell (running as corp\Peter.Parker)

```
PS C:\Windows\system32> $users = [ADSI]"LDAP://ou=Standard,ou=Users,ou=PenTestLa
b,DC=corp,DC=hackerplaypen,DC=com"
PS C:\Windows\system32> $users.Children


distinguishedName : {CN=Barbara Gordon,OU=Standard,OU=Users,OU=PentestLab,DC=co
                    rp,DC=hackerplaypen,DC=com}
Path              : LDAP://CN=Barbara Gordon,ou=Standard,ou=Users,ou=PenTestLab
```

SIGN UP FOR EMAIL UPDATES

First Name

Last Name

Email Address

□ Executive Perspective Blog

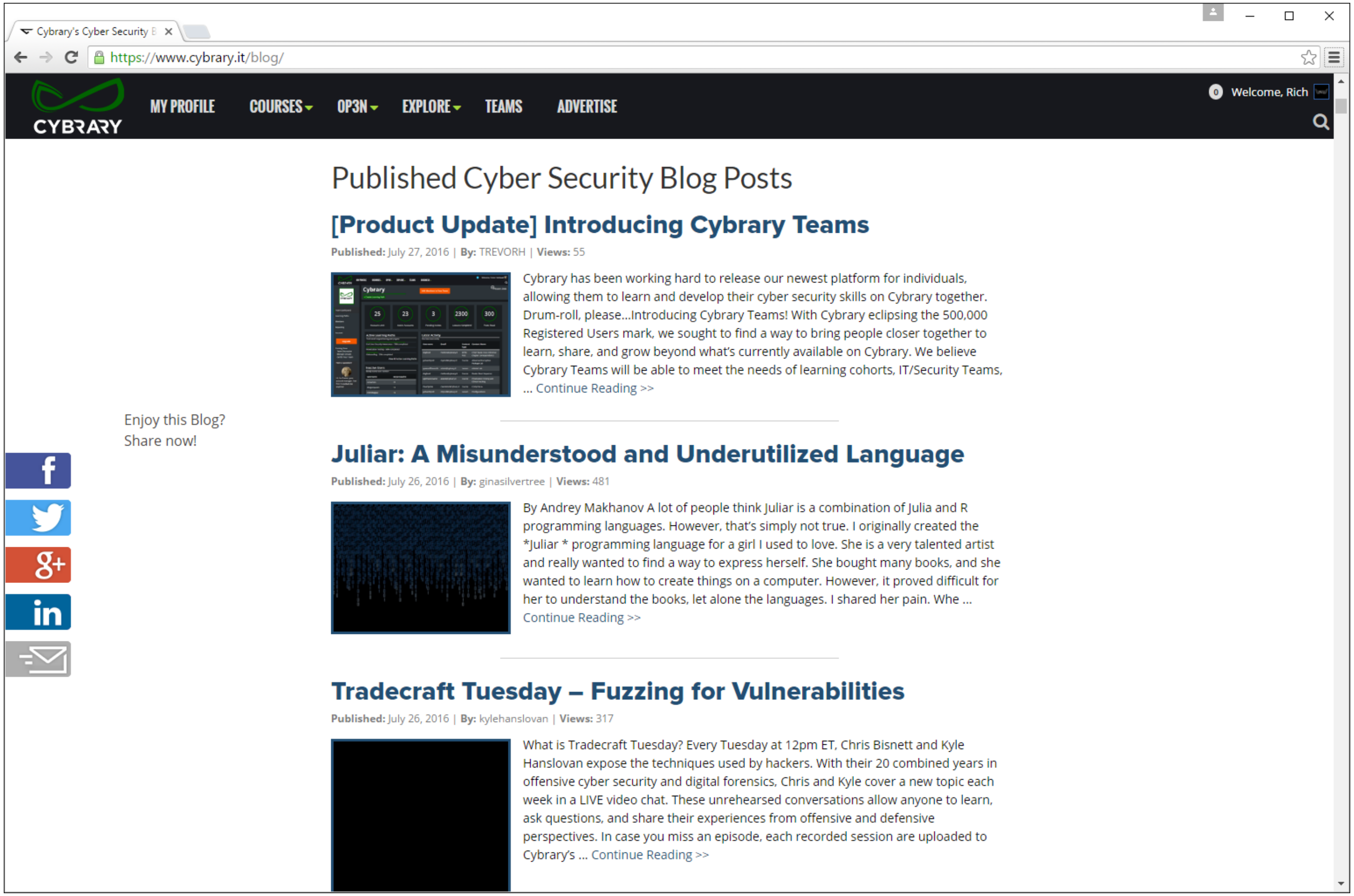
□ Threat Research Blog

□ Products and Services Blog

Subscribe

https://www.fireeye.com/blog/threat-research.html

Cybrary



Published Cyber Security Blog Posts

[Product Update] Introducing Cybrary Teams

Published: July 27, 2016 | **By:** TREVORH | **Views:** 55

Cybrary has been working hard to release our newest platform for individuals, allowing them to learn and develop their cyber security skills on Cybrary together. Drum-roll, please...Introducing Cybrary Teams! With Cybrary eclipsing the 500,000 Registered Users mark, we sought to find a way to bring people closer together to learn, share, and grow beyond what's currently available on Cybrary. We believe Cybrary Teams will be able to meet the needs of learning cohorts, IT/Security Teams, ... Continue Reading >>

Enjoy this Blog?
Share now!

Juliar: A Misunderstood and Underutilized Language

Published: July 26, 2016 | **By:** ginasilvertree | **Views:** 481

By Andrey Makhanov A lot of people think Juliar is a combination of Julia and R programming languages. However, that's simply not true. I originally created the *Juliar * programming language for a girl I used to love. She is a very talented artist and really wanted to find a way to express herself. She bought many books, and she wanted to learn how to create things on a computer. However, it proved difficult for her to understand the books, let alone the languages. I shared her pain. Whe ... Continue Reading >>

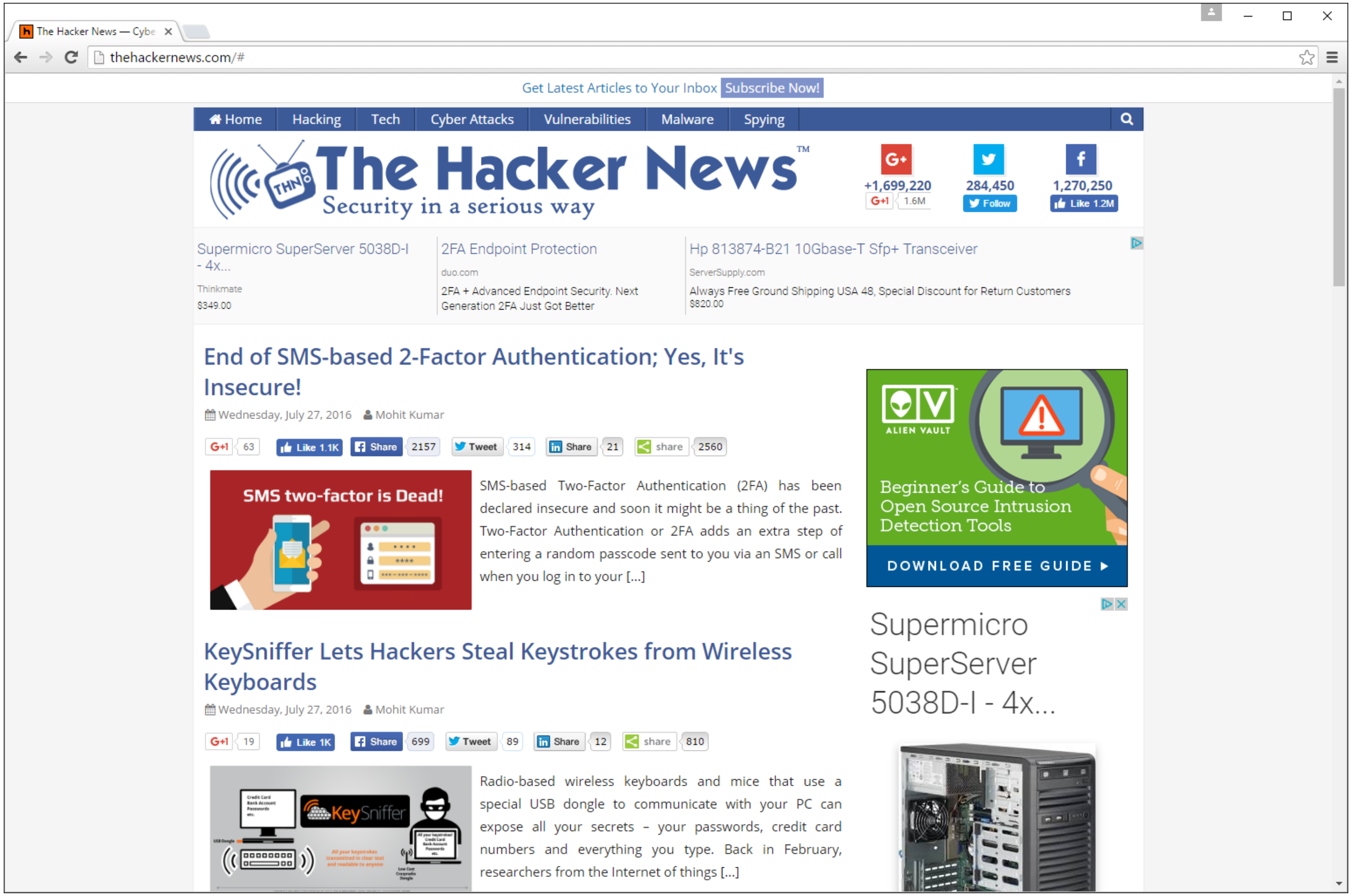
Tradecraft Tuesday – Fuzzing for Vulnerabilities

Published: July 26, 2016 | **By:** kylehanslovan | **Views:** 317

What is Tradecraft Tuesday? Every Tuesday at 12pm ET, Chris Bisnett and Kyle Hanslovan expose the techniques used by hackers. With their 20 combined years in offensive cyber security and digital forensics, Chris and Kyle cover a new topic each week in a LIVE video chat. These unrehearsed conversations allow anyone to learn, ask questions, and share their experiences from offensive and defensive perspectives. In case you miss an episode, each recorded session are uploaded to Cybrary's ... Continue Reading >>

https://www.cybrary.it/blog/

Hacker News



Get Latest Articles to Your Inbox Subscribe Now!

Home | Hacking | Tech | Cyber Attacks | Vulnerabilities | Malware | Spying

The Hacker News™
Security in a serious way

End of SMS-based 2-Factor Authentication; Yes, It's Insecure!

Wednesday, July 27, 2016 Mohit Kumar

SMS-based Two-Factor Authentication (2FA) has been declared insecure and soon it might be a thing of the past. Two-Factor Authentication or 2FA adds an extra step of entering a random passcode sent to you via an SMS or call when you log in to your [...]

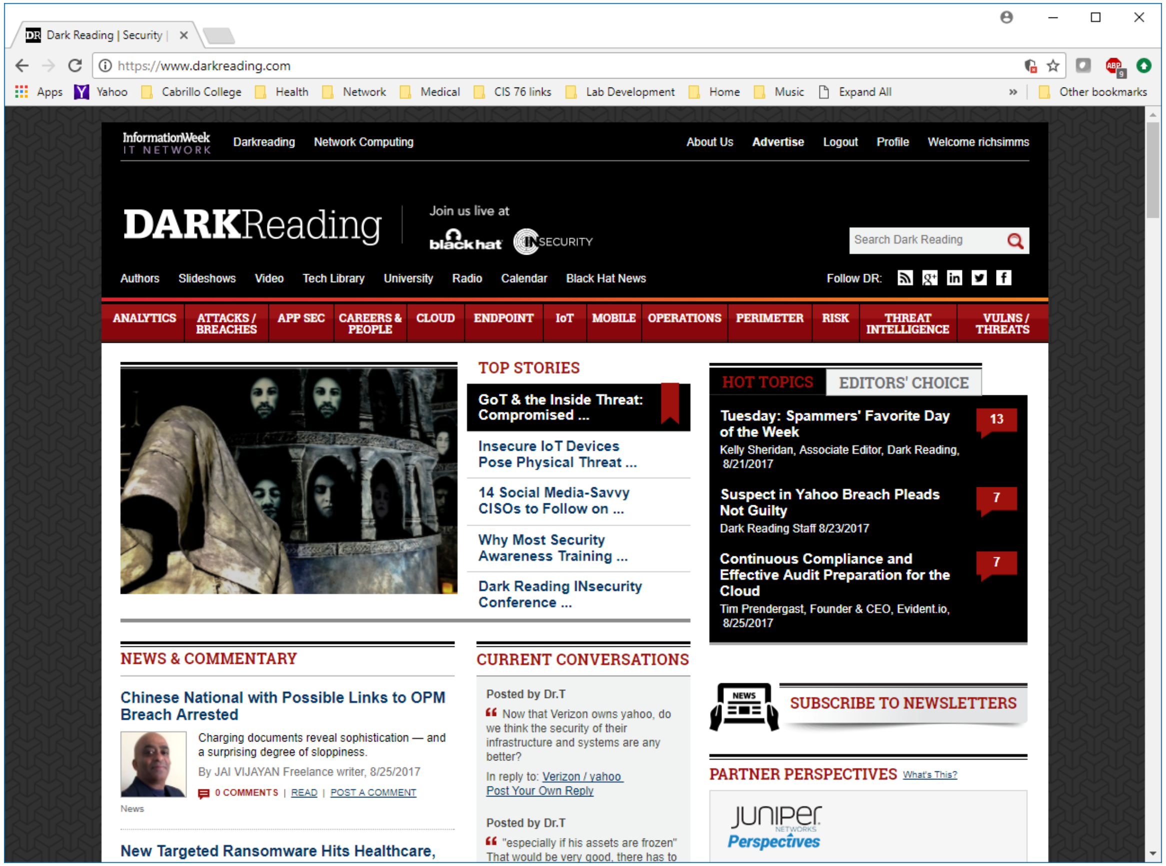
KeySniffer Lets Hackers Steal Keystrokes from Wireless Keyboards

Wednesday, July 27, 2016 Mohit Kumar

Radio-based wireless keyboards and mice that use a special USB dongle to communicate with your PC can expose all your secrets – your passwords, credit card numbers and everything you type. Back in February, researchers from the Internet of things [...]

http://thehackernews.com/

DARK Reading



InformationWeek IT NETWORK Darkreading Network Computing About Us Advertise Logout Profile Welcome richsimms

DARKReading Join us live at black hat INSECURITY

Search Dark Reading

Authors Slideshows Video Tech Library University Radio Calendar Black Hat News Follow DR:

ANALYTICS ATTACKS / BREACHES APP SEC CAREERS & PEOPLE CLOUD ENDPOINT IoT MOBILE OPERATIONS PERIMETER RISK THREAT INTELLIGENCE VULNS / THREATS

TOP STORIES

GoT & the Inside Threat: Compromised ...

Insecure IoT Devices Pose Physical Threat ...

14 Social Media-Savvy CISOs to Follow on ...

Why Most Security Awareness Training ...

Dark Reading INsecurity Conference ...

HOT TOPICS EDITORS' CHOICE

Tuesday: Spammers' Favorite Day of the Week 13
Kelly Sheridan, Associate Editor, Dark Reading, 8/21/2017

Suspect in Yahoo Breach Pleads Not Guilty 7
Dark Reading Staff 8/23/2017

Continuous Compliance and Effective Audit Preparation for the Cloud 7
Tim Prendergast, Founder & CEO, Evident.io, 8/25/2017

NEWS & COMMENTARY

Chinese National with Possible Links to OPM Breach Arrested

Charging documents reveal sophistication — and a surprising degree of sloppiness.

By JAI VIJAYAN Freelance writer, 8/25/2017

0 COMMENTS | READ | POST A COMMENT

News

New Targeted Ransomware Hits Healthcare,

CURRENT CONVERSATIONS

Posted by Dr.T
" Now that Verizon owns yahoo, do we think the security of their infrastructure and systems are any better?
In reply to: Verizon / yahoo
Post Your Own Reply

Posted by Dr.T
" "especially if his assets are frozen" That would be very good, there has to

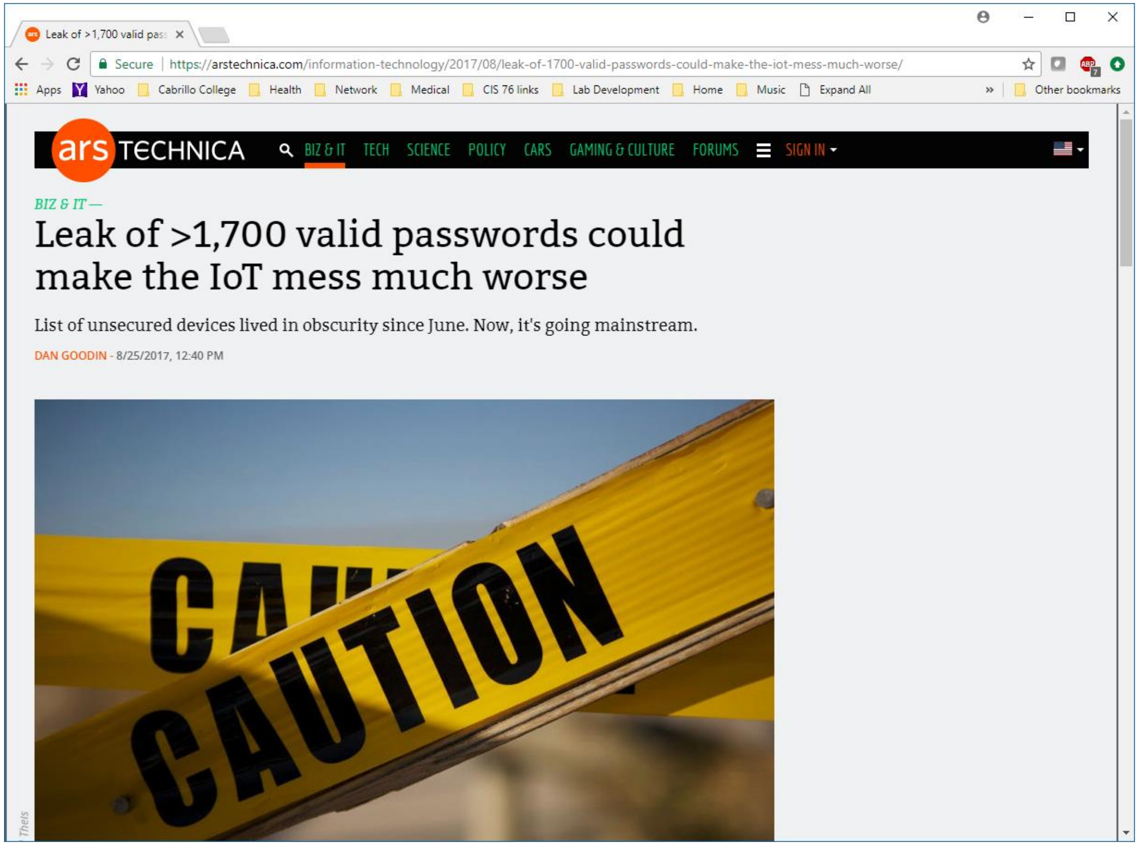
SUBSCRIBE TO NEWSLETTERS

PARTNER PERSPECTIVES What's This?

JUNIPER NETWORKS Perspectives

https://www.darkreading.com/

ars TECHNICA



https://arstechnica.com/information-technology/2017/08/leak-of-1700-valid-passwords-could-make-the-iot-mess-much-worse/

BIZ & IT —

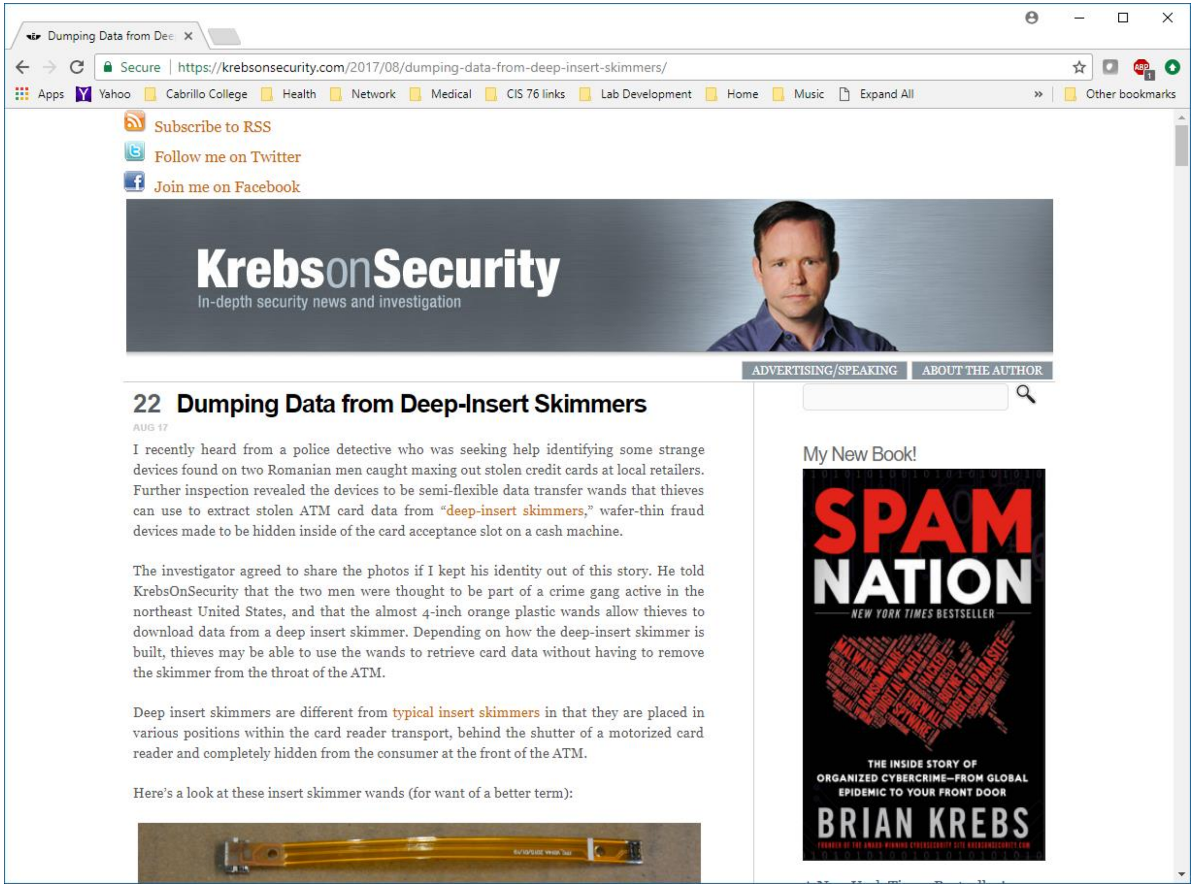
Leak of >1,700 valid passwords could make the IoT mess much worse

List of unsecured devices lived in obscurity since June. Now, it's going mainstream.

DAN GOODIN - 8/25/2017, 12:40 PM

https://arstechnica.com/

Krebs on Security



22 **Dumping Data from Deep-Insert Skimmers**

AUG 17

I recently heard from a police detective who was seeking help identifying some strange devices found on two Romanian men caught maxing out stolen credit cards at local retailers. Further inspection revealed the devices to be semi-flexible data transfer wands that thieves can use to extract stolen ATM card data from "deep-insert skimmers," wafer-thin fraud devices made to be hidden inside of the card acceptance slot on a cash machine.

The investigator agreed to share the photos if I kept his identity out of this story. He told KrebsOnSecurity that the two men were thought to be part of a crime gang active in the northeast United States, and that the almost 4-inch orange plastic wands allow thieves to download data from a deep insert skimmer. Depending on how the deep-insert skimmer is built, thieves may be able to use the wands to retrieve card data without having to remove the skimmer from the throat of the ATM.

Deep insert skimmers are different from typical insert skimmers in that they are placed in various positions within the card reader transport, behind the shutter of a motorized card reader and completely hidden from the consumer at the front of the ATM.

Here's a look at these insert skimmer wands (for want of a better term):

https://krebsonsecurity.com/

VLab Pod Setup

Live demo

https://simms-teach.com/docs/cis76/cis76-podSetup.pdf

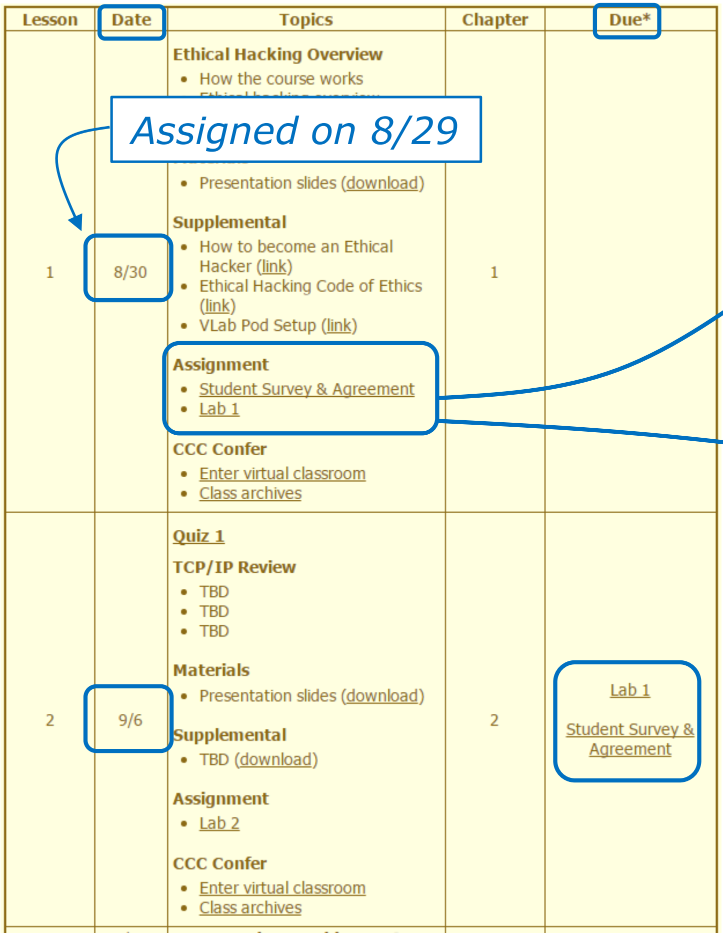
MS08-067
CVE-2008-4250
Hack

Live demo

https://simms-teach.com/docs/cis76/cis76-CVE-2008-4250.pdf

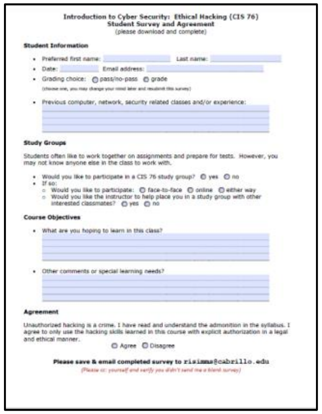
Assignment

Assignments and Due Dates



Lesson	Date	Topics	Chapter	Due*
1	8/30	**Ethical Hacking Overview** • How the course works • Ethical hacking overview **Materials** • Presentation slides (download) **Supplemental** • How to become an Ethical Hacker (link) • Ethical Hacking Code of Ethics (link) • VLab Pod Setup (link) **Assignment** • Student Survey & Agreement • Lab 1 **CCC Confer** • Enter virtual classroom • Class archives	1	
2	9/6	**Quiz 1** **TCP/IP Review** • TBD • TBD • TBD **Materials** • Presentation slides (download) **Supplemental** • TBD (download) **Assignment** • Lab 2 **CCC Confer** • Enter virtual classroom • Class archives	2	Lab 1 Student Survey & Agreement

Assigned on 8/29



Introduction to Cyber Security: Ethical Hacking (CIS 76)
Student Survey and Agreement
(please download and complete)

Student Information

- Preferred first name: Last name:
- Date: Email address:
- Grading choice: ○ pass/no-pass ○ grade
  (choose one, you may change your mind later and resubmit this survey)
- Previous computer, network, security related classes and/or experience:

Study Groups

Students often like to work together on assignments and prepare for tests. However, you may not know anyone else in the class to work with.

- Would you like to participate in a CIS 76 study group? ○ yes ○ no
- If so:
  - Would you like to participate: ○ face-to-face ○ online ○ either way
  - Would you like the instructor to help place you in a study group with other interested classmates? ○ yes ○ no

Course Objectives

- What are you hoping to learn in this class?
- Other comments or special learning needs?

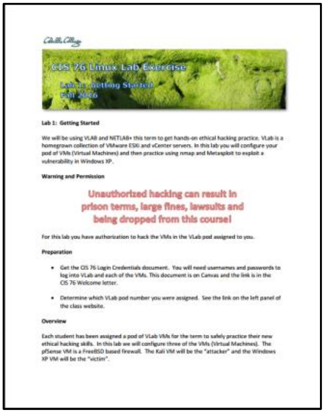
Agreement

Unauthorized hacking is a crime. I have read and understand the admonition in the syllabus. I agree to only use the hacking skills learned in this course with explicit authorization in a legal and ethical manner.

○ Agree ○ Disagree

Please save & email completed survey to risimms@cabrillo.edu
(Please cc: yourself and verify you didn't send me a blank survey)

Survey & Agreement



Lab 1: Getting Started

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

Warning and Permission

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

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

Preparation

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

Overview

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

Lab 1

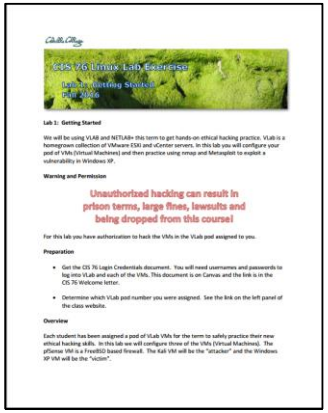
Both due by 11:59PM (Opus Time) on Tuesday 9/5

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

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.



CIS 76 Linux Lab Exercise

Lab 1: Getting Started

Fall 2016

Lab 1: Getting Started

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

Warning and Permission

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

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

Preparation

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

Overview

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

Wrap up

Next Class

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

Lab 1,
Survey & Agreement

Quiz questions for next class:

- What makes ethical hacking different from malicious hacking?
- If convicted of hacking that violates the Federal CFAA (Computer Fraud and Abuse Act) you could serve up to 20 years in prison. True or False?
- What does the Chinese hacker slang "meat chicken" refer to?

Backup