



Rich's lesson module checklist

Last updated 9/16/2016

- 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

- Opus accounts made (with TBDs for walk-ins) and populated
- Netlab+ accounts created
- Forum created with welcome post
- Canvas LMS setup with website links, welcome letter, credentials
- CIS 76 VLAB VMs created and configured
- Lab 1 tested
- Survey posted
- Login credentials document updated and secured

- Welcome letter sent in advance of first class
- Rosters printed
- Add codes printed

- 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

The screenshot shows a web browser window with the address bar containing `simms-teach.com/cis90calendar.php`. The page title is "Rich's Cabrillo College CIS Classes CIS 90 Calendar". The main content area is titled "CIS 90 (Fall 2014) Calendar" and includes a "Calendar" link. A sidebar on the left lists various course sections, with "CIS 76" highlighted. The main content area contains a table with columns for "Lesson", "Date", and "Topics". The "Presentation slides (download)" link is highlighted in a red box. Below the table, there is a section for "Enter virtual classroom" also highlighted in a red box.

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

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

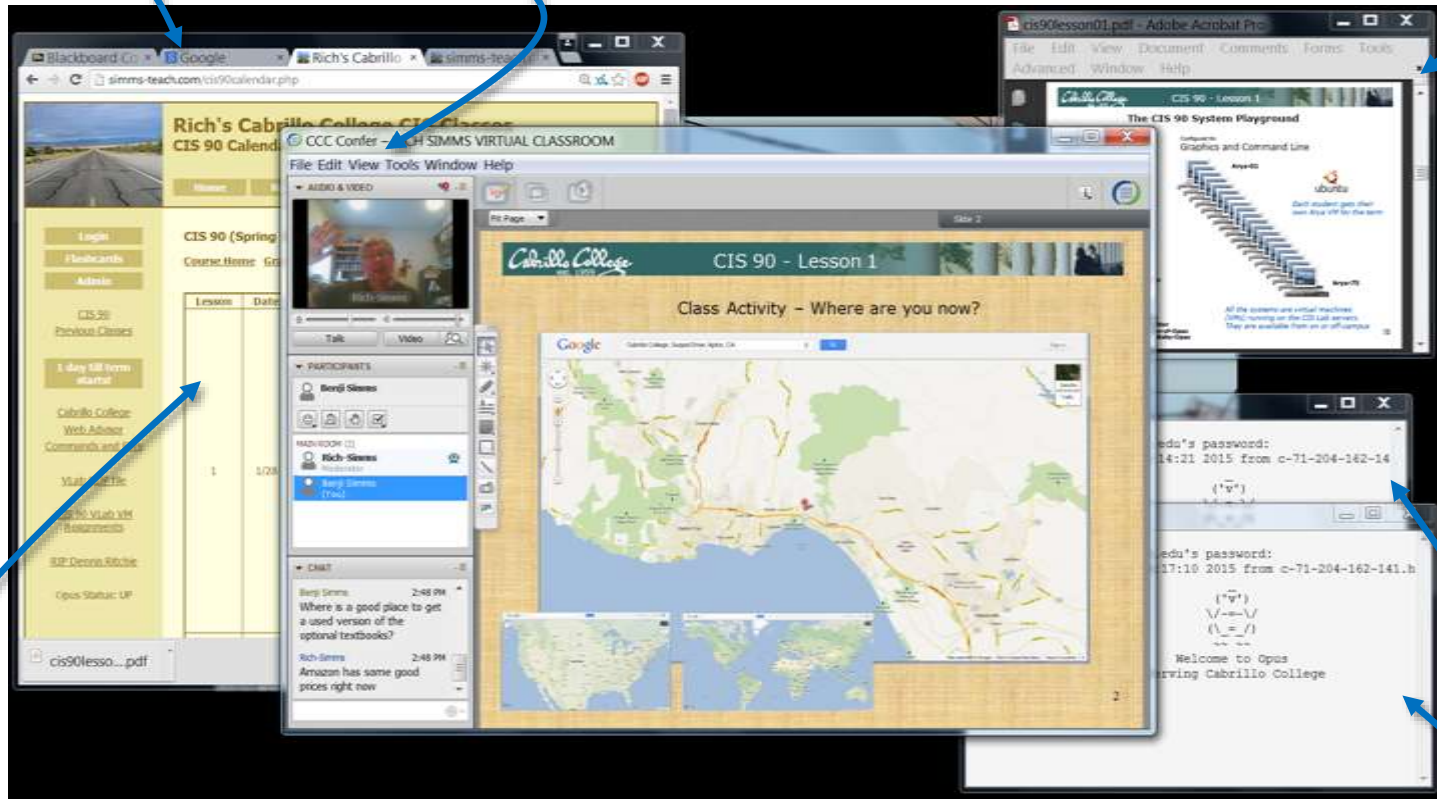


Student checklist for suggested screen layout

Google

CCC Confer

Downloaded PDF of Lesson Slides



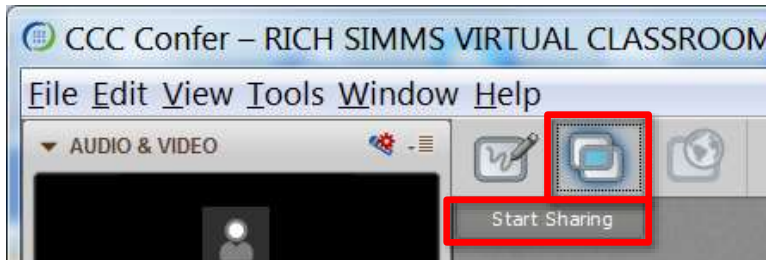
CIS 76 website Calendar page

One or more login sessions to Opus

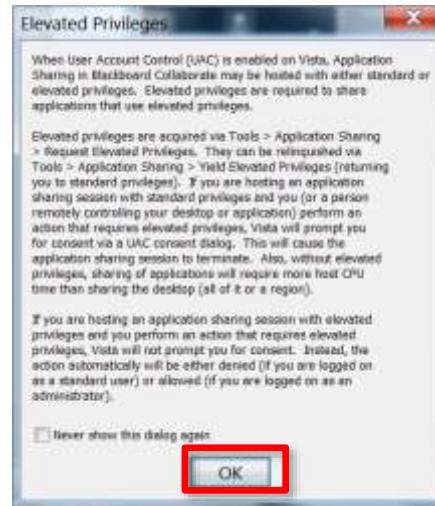


Student checklist for sharing desktop with classmates

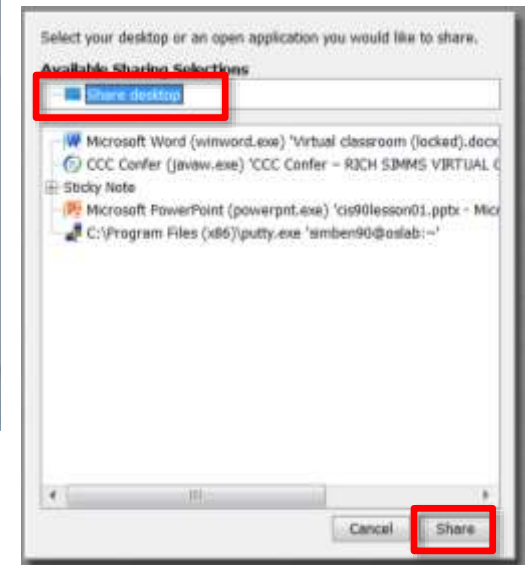
1) Instructor gives you sharing privileges.



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



3) Click OK button.



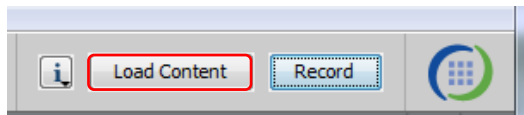
4) Select "Share desktop" and click Share button.



Rich's CCC Confer checklist - setup

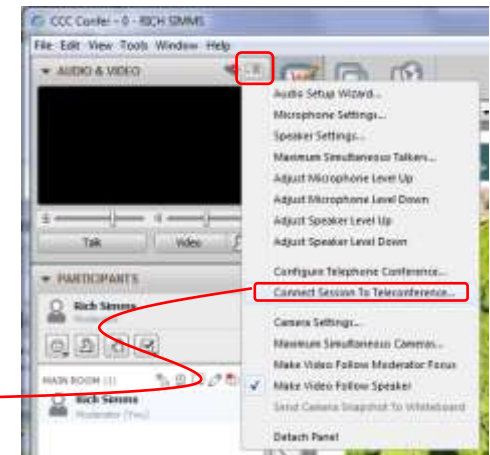
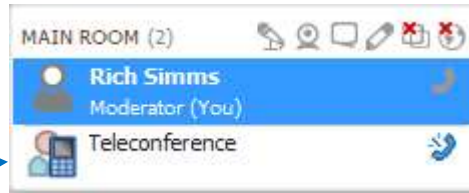


[] Preload White Board



[] Connect session to Teleconference

Session now connected to teleconference



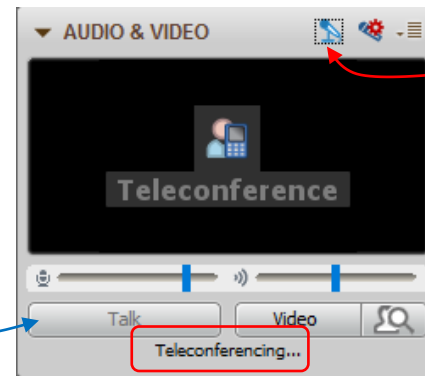
[] Is recording on?



Red dot means recording

[] Use teleconferencing, not mic

Should be grayed out



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



Rich's CCC Confer checklist - screen layout

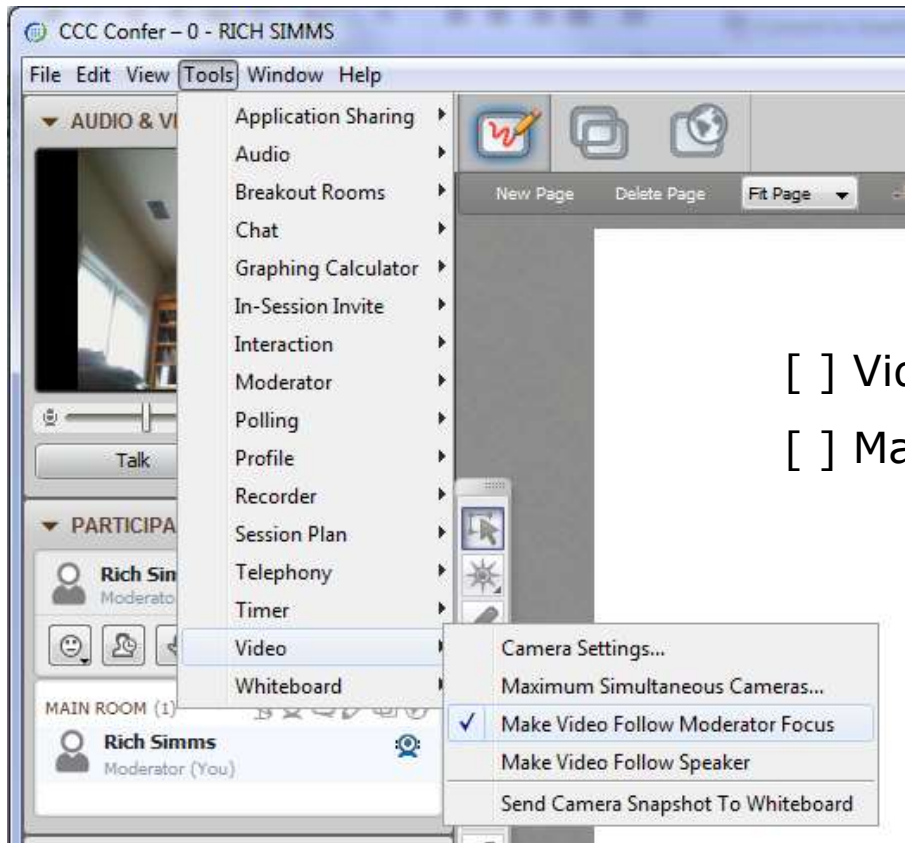


[] layout and share apps





Rich's CCC Confer checklist - webcam setup



[] Video (webcam)

[] Make Video Follow Moderator Focus



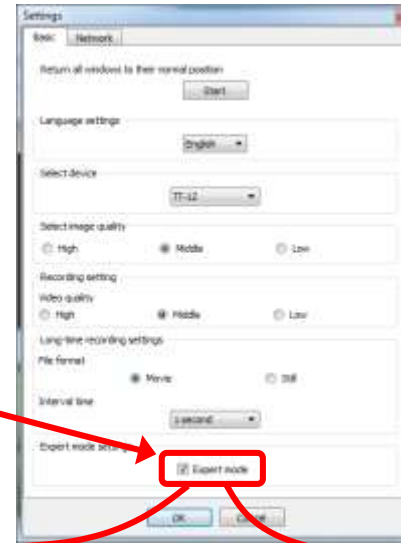
Rich's CCC Confer checklist - Elmo



Elmo rotated down to view side table



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



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 up to view white board



Rich's CCC Confer checklist - universal fixes

Universal Fix for CCC Confer:

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

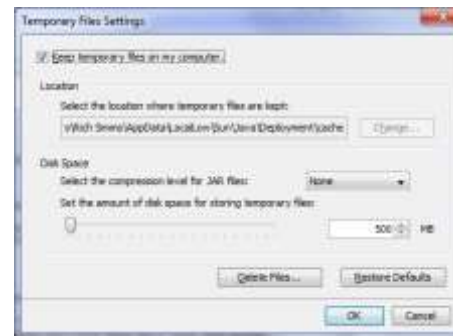
Control Panel (small icons)



General Tab > Settings...



500MB cache size



Delete these



Google Java download





Start

Sound Check

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

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



Ethical Hacking Overview

Objectives

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

Agenda

- Introductions
- Bait and switch
- 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**

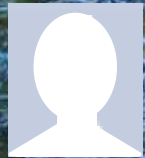
Passcode: **136690**



Sergio



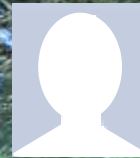
Nicholas



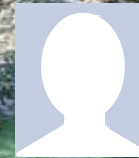
Takashi



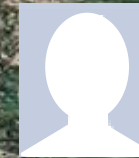
Karl-Heinz



Shahram



Benjamin



Joshua



Brian H.



Brian T.



Jeremy



David H.



Roberto



Dwight



Michael C.



Deryck



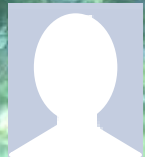
Efrain



Michael W.



Carter



Thomas



Wesley



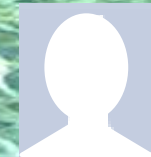
Jennifer



Marcos



Tim



Daniel



Ryan



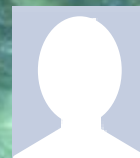
Jordan



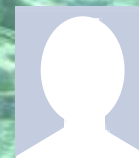
Alex



Tess



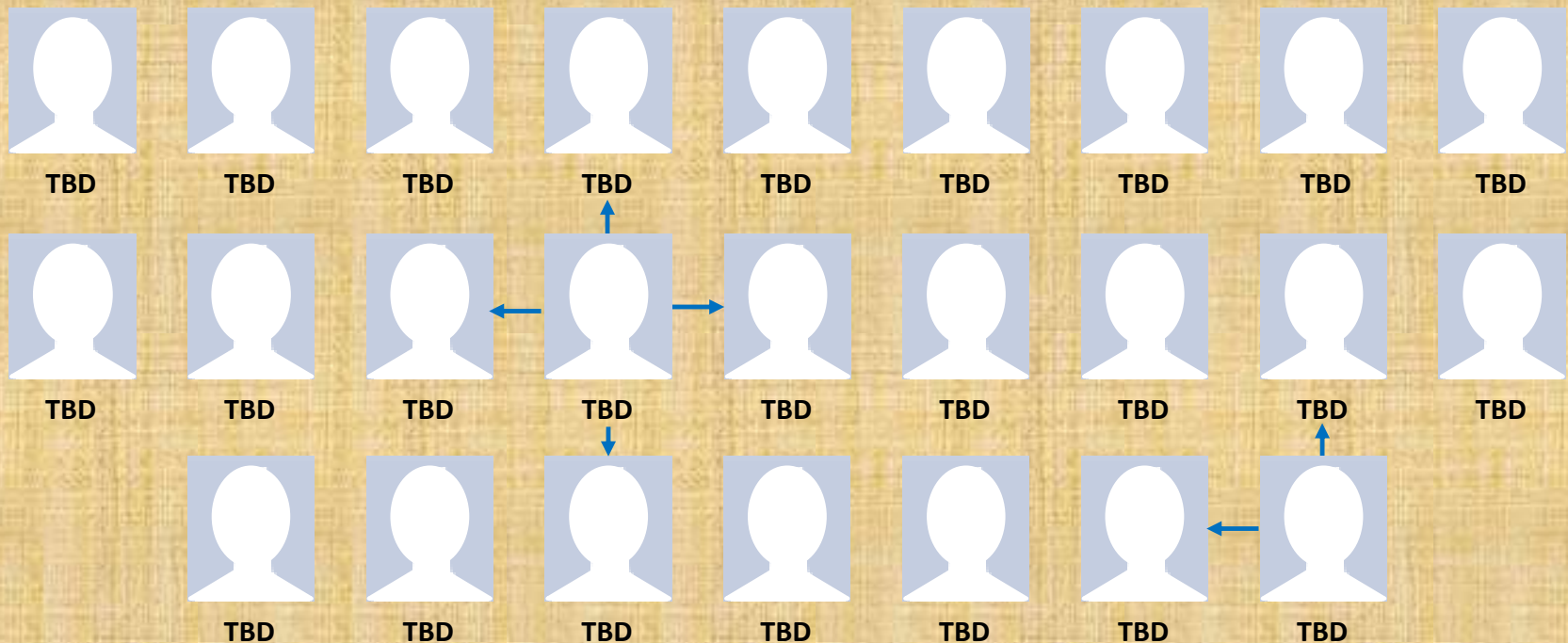
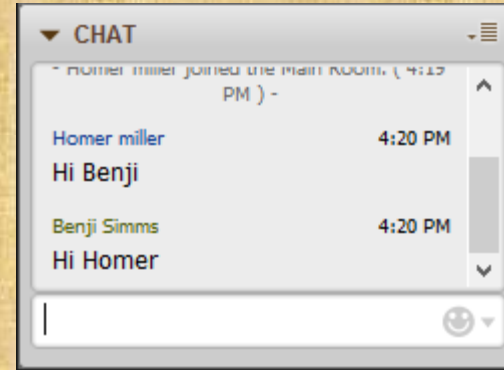
Luis



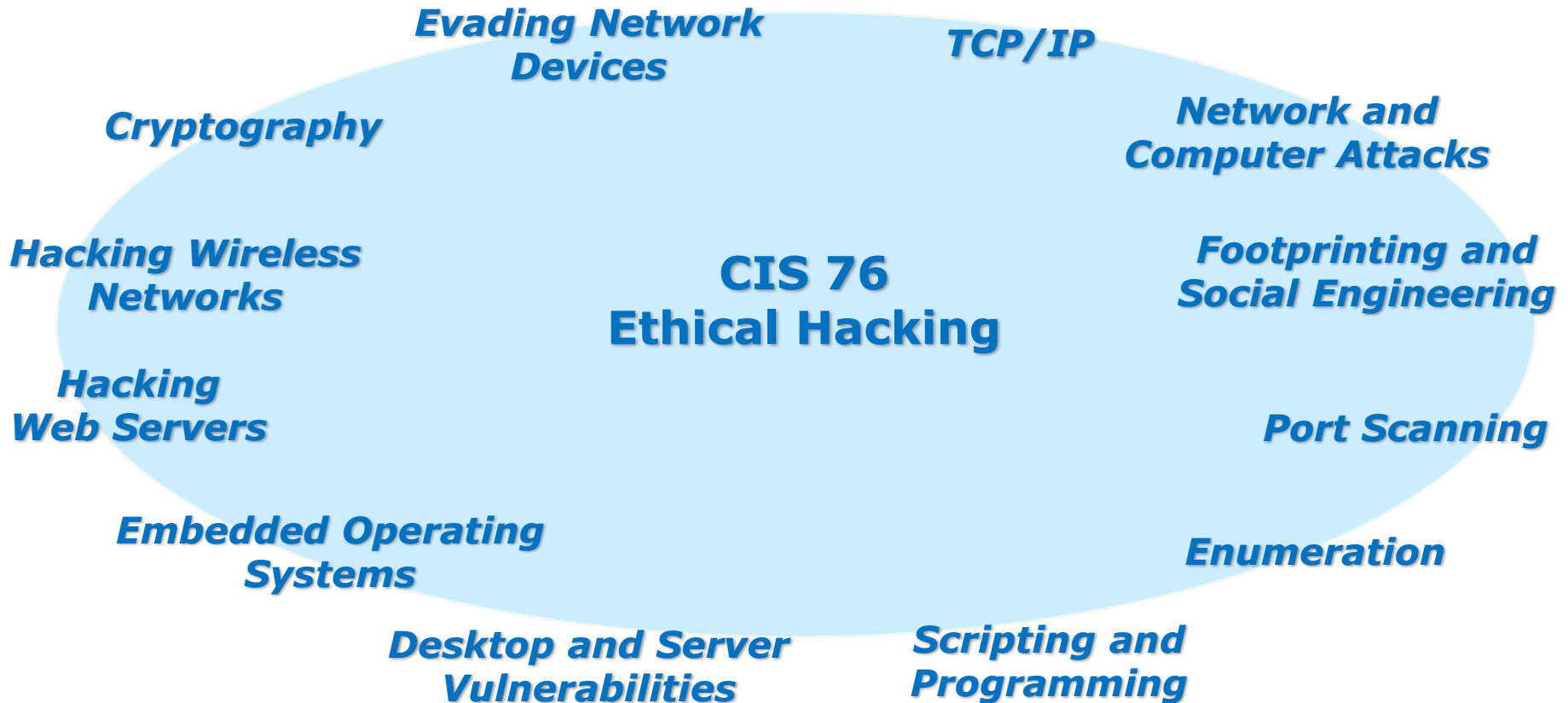
Dave R.

First Activity

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



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



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.



Bait and Switch

This is what is shown in the Schedule

CIS 76 Introduction to Information Assurance

Introduces the various methodologies for attacking a network. Prerequisite: CIS 75.
Transfer Credit: Transfers to CSU

Section	Days	Times	Units	Instructor	Room
95024	Arr.	Arr.	3.00	R.Simms	OL
&	Arr.	Arr.		R.Simms	OL

Section 95024 is an ONLINE course. Meets weekly throughout the semester online by remote technology with an additional 50 min online lab per week. For details, see instructor's web page at go.cabrillo.edu/online.

95025	T	5:30PM-8:35PM	3.00	R.Simms	828
&	Arr.	Arr.		R.Simms	OL

Section 95025 is a Hybrid ONLINE course. Meets weekly throughout the semester at the scheduled times with an additional 50 min online lab per week. For details, see instructor's web page at go.cabrillo.edu/online.

This is what I'm actually teaching and when

CIS 76 Introduction to Cyber Security: Ethical Hacking

Introduces the various methodologies for attacking a network. Prerequisite: CIS 75.
Transfer Credit: Transfers to CSU

Section	Days	Times	Units	Instructor	Room
95024	T	5:30PM-8:35PM	3.00	R.Simms	CCC Confer
&	Arr.	Arr.		R.Simms	OL

Section 95024 is an ONLINE course. Meets weekly throughout the semester online by remote technology with an additional 50 min online lab per week. For details, see instructor's web page at go.cabrillo.edu/online.

95025	T	5:30PM-8:35PM	3.00	R.Simms	828
&	Arr.	Arr.		R.Simms	OL

Section 95025 is a Hybrid ONLINE course. Meets weekly throughout the semester at the scheduled times with an additional 50 min online lab per week. For details, see instructor's web page at go.cabrillo.edu/online.

- Information Assurance is a different subject than Ethical hacking. However they are related and both aim to strengthen security infrastructure.
- The online section will meet at the same time as the classroom section using CCC Confer. Attending live is preferable to watching the recordings at a later date because you can ask questions and participate in class activities.
- If you miss a class (whether online or in the classroom) you can always attend by watching the recordings at a later date.
- If you choose to attend class by only watching the recordings you will need to do some extra credit to make up for the points lost on the first minute quizzes.



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 95024 meets online in [this virtual classroom](#)
- Section 95025 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.

simms-teach.com/cis90calendar.php

Rich's Cabrillo College CIS Classes
CIS 90 Calendar

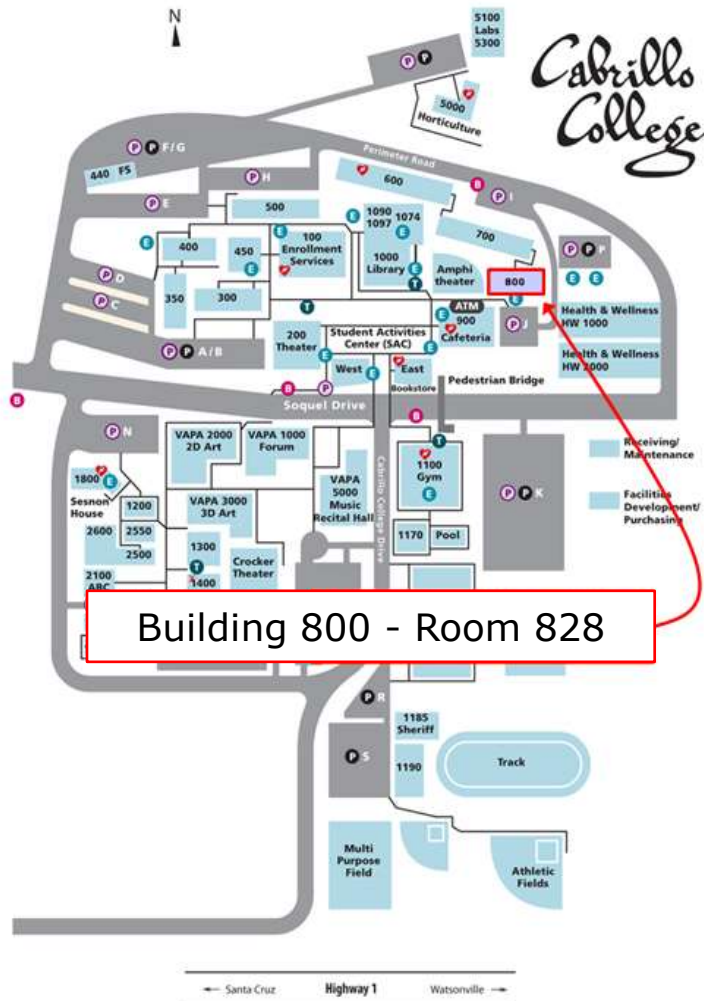
[CIS 76](#)

[Calendar](#)

[Enter virtual classroom](#)

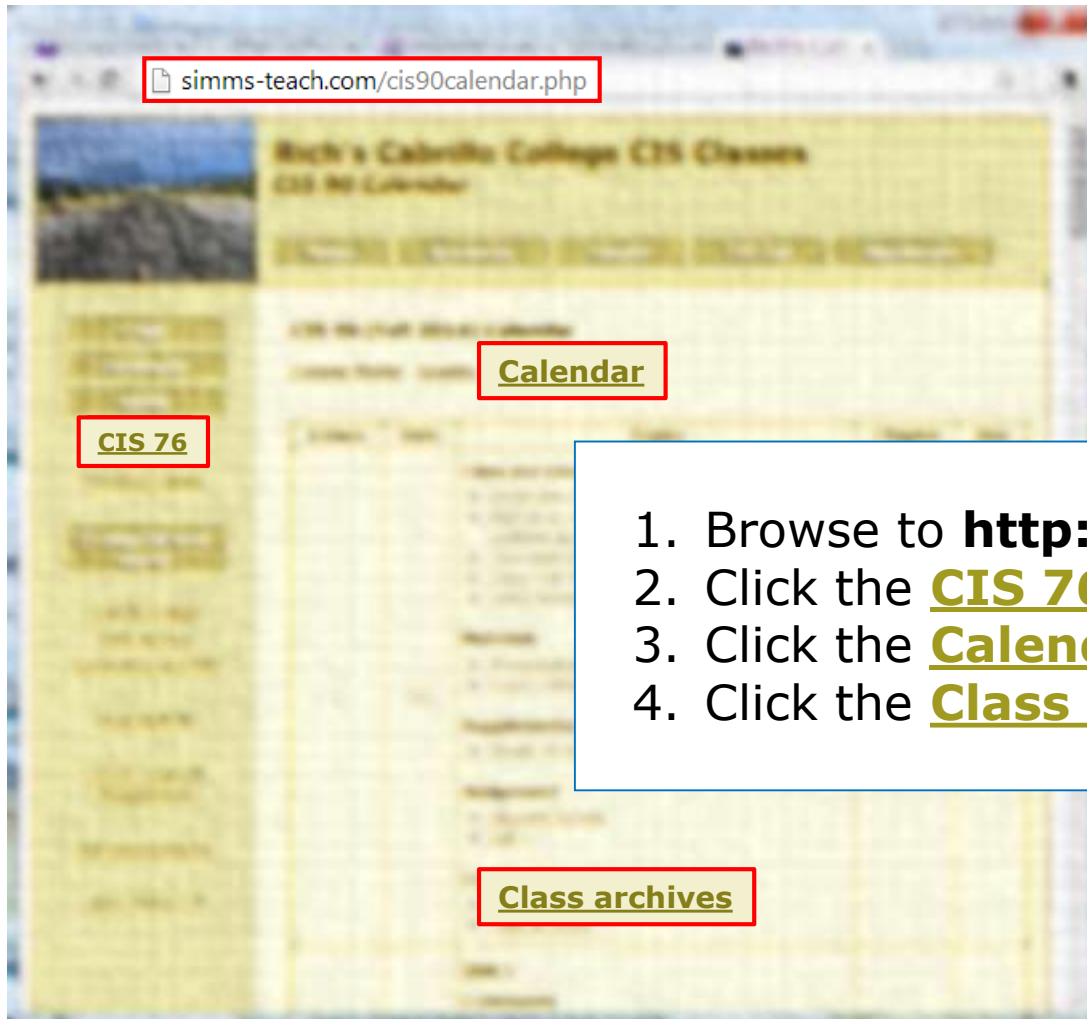
1. Browse to **http://simms-teach.com**
2. Click the **CIS 76** link
3. Click the **Calendar** link
4. Click the **Enter virtual classroom** link

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



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



CCC Confer

CCC Confer - Attending class online

CCC Confer - 0 - RICH SIMMS

File Edit View Tools Window Help

AUDIO & VIDEO

Rich Simms

Talk Video

PARTICIPANTS

Benji

MAIN ROOM (2)

Rich Simms
Moderator

Benji
(You)

CHAT

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

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

Cabrillo College
est. 1959

CIS Linux Classes

Instructor: Rich Simms
Dial-in: 888-450-4821

Fit Page Slide1

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

30

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)

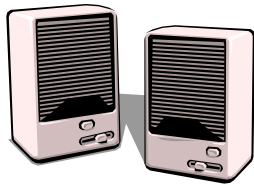
Enter the CCC Confer virtual room

The screenshot shows a web browser window with the address bar containing simms-teach.com/cis90calendar.php. The page title is "Rich's Cabrillo College CIS Classes CIS 90 Calendar". The page content includes a sidebar with a link labeled "CIS 76" and a main content area with a "Calendar" link and an "Enter virtual classroom" link. The "Enter virtual classroom" link is highlighted with a red box.

1. Browse to **<http://simms-teach.com>**
2. Click the **[CIS 76](#)** link
3. Click the **[Calendar](#)** link
4. Click the **[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>

The screenshot shows a web browser window displaying the CCC Confer website. The URL in the address bar is www.cccconfer.org/support/Readiness. The page has a header with the CCC Confer logo on the left and the MyConfer logo on the right. Below the logos are navigation menus for 'Home', 'Meetings', 'Training', 'Support', 'MyConfer', 'MyMeetings', 'Request Meeting', 'More', and 'Log out'. A central banner features images of a laptop, a tablet, and a smartphone, with the word 'Support' in green text. Below the banner, there is a 'Support' tab and a 'Readiness' section. The 'Readiness' section is titled 'Is Your Computer Ready?' and contains a numbered list of instructions: 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.collob (file type for live sessions) and nativeplayback.collob (for recorded archives). Below the list, contact information for CCC Confer Client Services is provided: Telephone: 760-744-1150 ext 1537, 1554 or 1542; Email: clientrelations@cccconfer.org. At the bottom of the page, there are links for 'Home', 'About Us', 'Products', 'Contact Us', 'Accessibility', and 'Privacy & Terms'. There are also social media icons for Facebook and YouTube. A footer note states: 'This site is provided as a service to the administrators, staff and faculty of the Cabrillo Community Colleges system. CCC Confer is funded by an e-learning grant from the Cabrillo Community Colleges Chancellor's Office. ©2013 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



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

Syllabus, Calendar and Grades

Activity

Find the syllabus

Browse to: <http://simms-teach.com>

The screenshot shows a web browser window displaying the website simms-teach.com. The page title is "Rich's Cabrillo College CIS Classes CIS 90 Home". The main content area is titled "CIS 90 (Fall 2014) Syllabus" and includes a "Course Home" link, a "Calendar" link, and a section for "Introduction to UNIX/Linux". The course schedule is listed as "Tuesdays - 1:00PM to 4:05PM". The syllabus content includes:

- Section 84743 meets in room 028 on the Aptos Main Campus
- Section 86576 meets simultaneously online in [this virtual classroom](#)
- UNIX 3 prerequisites: none, recommended: CIS 11 or CIS 172
- OpenStax Textbooks, available:
 - [Harvey Hahn's Guide to UNIX](#)
 - by Harvey Hahn
 - McGraw Hill ISBN 10
 - [Linux User's Guide: D&G](#)
 - by Carolyn Z. Gikley
 - Franklin Beedle & Associates

The "Course Description" section states: "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."

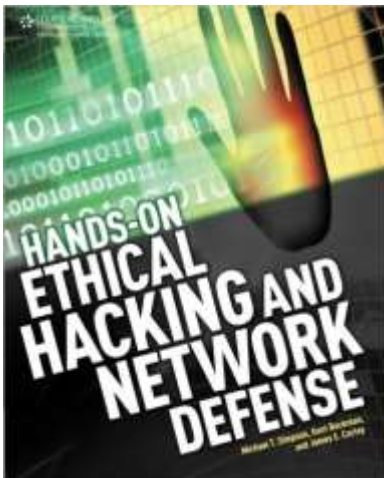
1) Click on **CIS 76**
on left panel

CIS 76

Course Home

2) Then click on
Course Home
to see the Syllabus

CIS 76 Textbook



There are several books and editions with the same title and the same authors. I chose this one because it has the most recent publication date and was recommended by another instructor who has taught Ethical Hacking for many years.

A newer edition is supposedly in the works but not published yet.

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](https://www.amazon.com/Hands-On-Ethical-Hacking-Network-Defense/dp/1133935612)

CIS 76 Fall 2016

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

- 15 lessons: **5:30-8:35 PM**, from **Aug 30th** to **Dec 6th**
- Final exam: **4:00-6:50PM**, on **Thursday Dec 15th**, 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	2	1	2	3	4	5	6					1	2	3	
3	4	5	6	7	8	9	7	8	9	10	11	12	13	4	5	6	7	8	9	10
10	11	12	13	14	15	16	14	15	16	17	18	19	20	11	12	13	14	15	16	17
17	18	19	20	21	22	23	21	22	23	24	25	26	27	18	19	20	21	22	23	24
24	25	26	27	28	29	30	28	29	30	31	25	26	27	28	29	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			1	2	3	4	5					1	2	3
2	3	4	5	6	7	8	6	7	8	9	10	11	12	4	5	6	7	8	9	10
9	10	11	12	13	14	15	13	14	15	16	17	18	19	11	12	13	14	15	16	17
16	17	18	19	20	21	22	20	21	22	23	24	25	26	18	19	20	21	22	23	24
23	24	25	26	27	28	29	27	28	29	30	25	26	27	28	29	30	31			
30	31																			

CIS 76 Fall 2016 Final Exam Schedule

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

The typical week

<http://simms-teach.com>



Use the

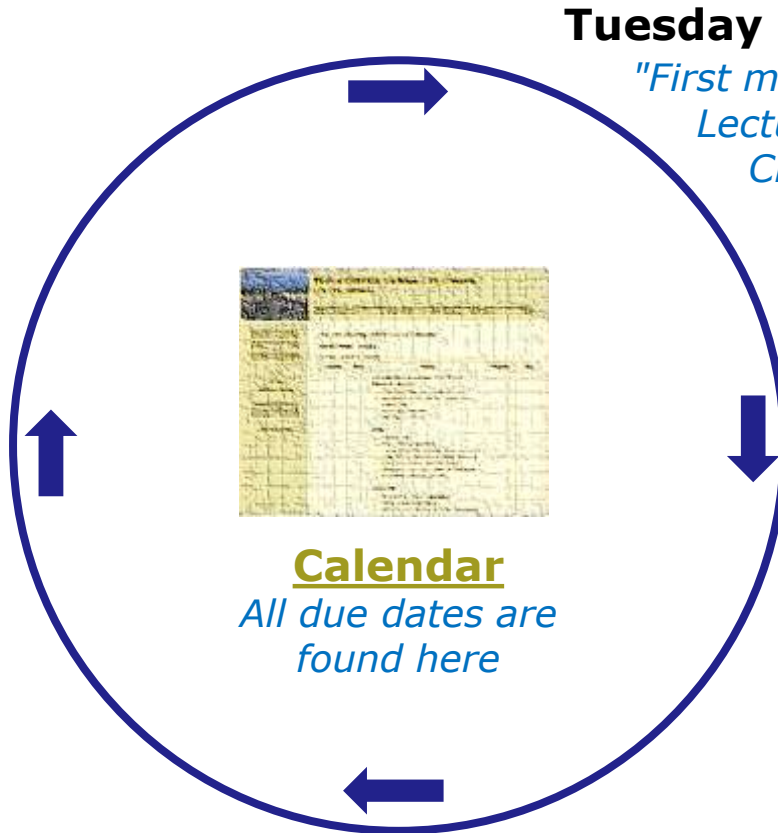
Forum

to collaborate
with classmates
at any time



Work on labs or practice tests
during the week.

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



Calendar

All due dates are
found here



Tuesday

"First minute" quiz

Lecture on new lesson material

Class activities

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



Thursday

is grading day



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

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)!

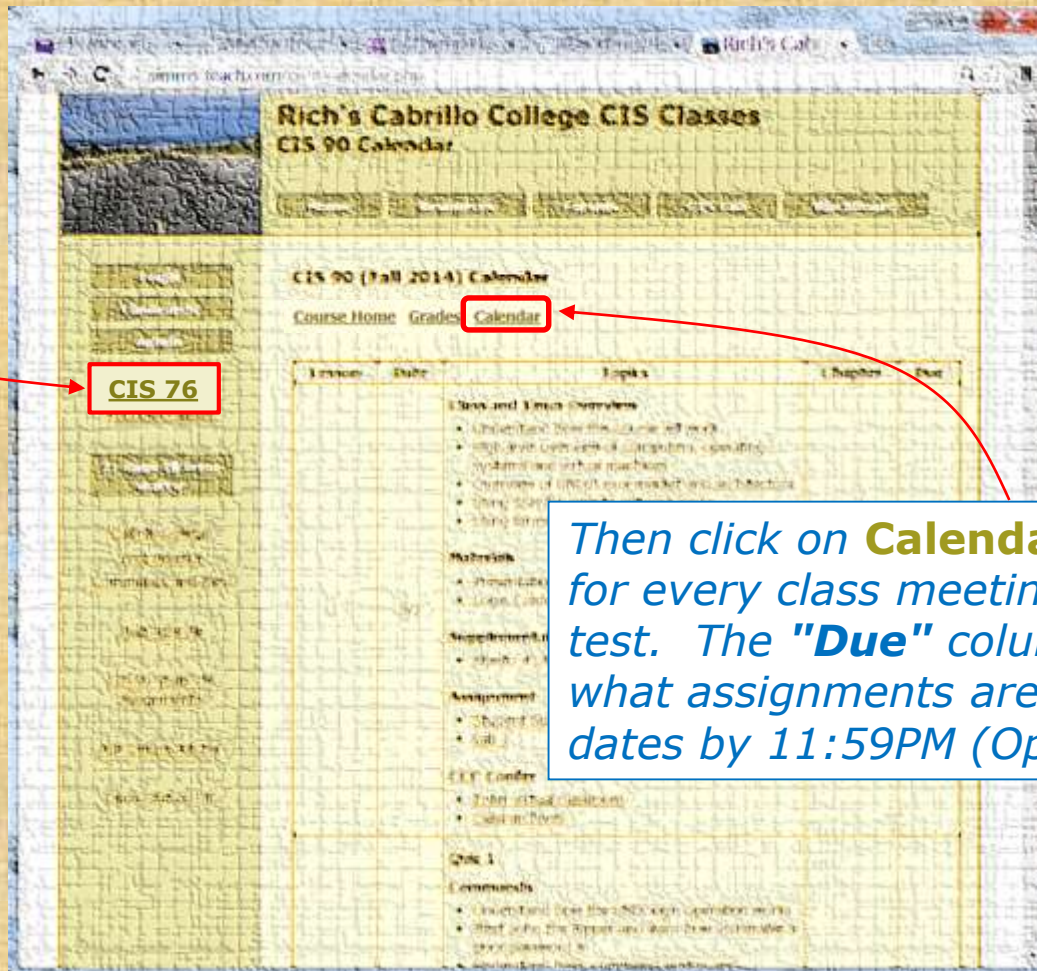


Activity

Find the Calendar page

Please browse to: <http://simms-teach.com>

Click on **CIS 76**
on left panel



Then click on **Calendar** to see dates for every class meeting, quiz, and test. The "**Due**" column indicates what assignments are due on those dates by 11:59PM (Opus time).

Course Calendar

Lesson	Date	Topics	Chapter	Due*
5	9/27	Quiz 4 Review <ul style="list-style-type: none"> TBD TBD TBD Materials <ul style="list-style-type: none"> Presentation slides (download) Supplemental <ul style="list-style-type: none"> TBD (download) Assignment <ul style="list-style-type: none"> Practice Test 1 (canvas) CCC Confer <ul style="list-style-type: none"> Enter virtual classroom Class archives 		Lab 4
6	10/4	Test #1 Port Scanning <ul style="list-style-type: none"> TBD TBD Test during last hour Materials <ul style="list-style-type: none"> Presentation slides (download) Test 1 (canvas) Supplemental <ul style="list-style-type: none"> TBD (download) Assignment <ul style="list-style-type: none"> Lab 5 CCC Confer <ul style="list-style-type: none"> Enter virtual classroom Class archives 	5	

Lesson # and Date

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

Lab assignment

CCC Confer links to join class online or review archives

First minute quiz

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

Links to virtual classroom and archived recordings

References to material in the textbook

Test

Activity

Find the Grades page

Please browse to: <http://simms-teach.com>

The screenshot shows a web browser window displaying the 'Rich's Cabrillo College CIS Classes' website. The page title is 'Rich's Cabrillo College CIS Classes' and the sub-header is 'CIS 90 Grades'. The main content area is titled 'CIS 90 (Fall 2014) Grades' and includes a 'Course Home' section with a red box around the 'Grades' link. Below this, there is a list of points earned from various activities, a table for 'How your grade is determined', and a section for 'Choice of Grade on Pass/No Pass'. A red arrow points from a callout box on the left to the 'CIS 76' link in the left-hand navigation menu. Another red arrow points from a callout box on the right to the 'Grades' link in the 'Course Home' section.

Click on CIS 76 on left panel

Then click on Grades to see the grading policy and monitor points earned

Course Grading

Monitor this page to track your progress in the course.

Rich's Cabrillo College CIS Classes
CIS 90 Grades

CIS 90 (Spring 2014) Grades
Course Home | Linking

Points can be earned from the following activities:

- First quiz/puzzle - 30 points (5%)
- Tests - 90 points (15%)
- Forum posts - 30 points (5%)
- Lab assignments - 300 points (50%)
- Project - 60 points (10%)

How your grade is determined:
A student can earn up to 504 total points from 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.

Choice of Letter or Pass/No Pass
You indicate your grading choice on the Student Services form passed out during the first class. You can only make grading choices once per term. If you need to contact the instructor by email with any questions or to request a change to your choice.

Extra Credit Activities
The instructor may provide a variety of opportunities to earn extra credit. When asking a question during the instructor's office hours, research and post questions on performance, team work, or for new assignments, or for team work, papers, others, and projects. A grade of 90% or higher is guaranteed for students who complete all extra credit activities. The choice to go above and beyond is up to you. The extra credit is an excellent way to distinguish yourself and demonstrate 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				
adadnda	grade	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	

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.

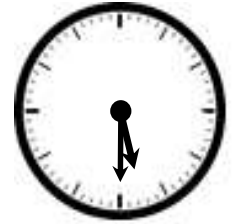
You control your grade. The more points you earn the higher your grade will be.

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.**
- 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

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

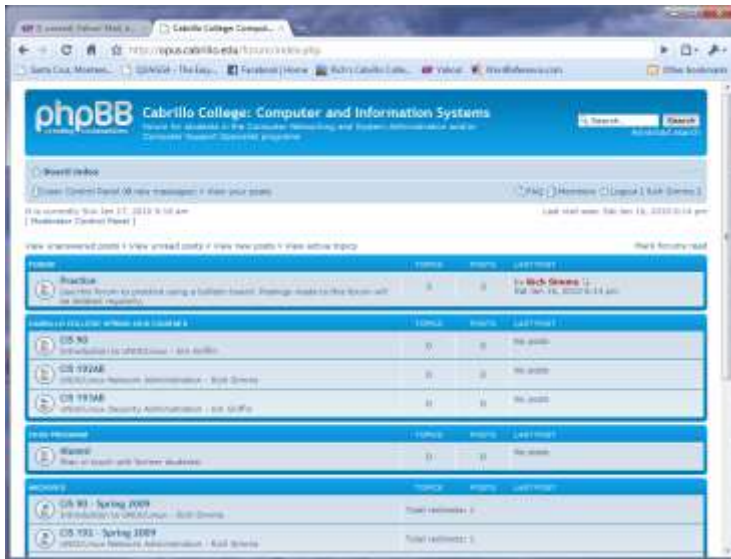
At the end of the course the instructor will count the number of points you have earned and use this table on the Grades web page to determine your grade.

HELEN'S
RESTAURANT

WHERE GOOD
FRIENDS
MEET TO EAT

Help Forum

Online Help Forum



- 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

POSTREPLY ↩

Search this topic...

Search

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.

- 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.



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

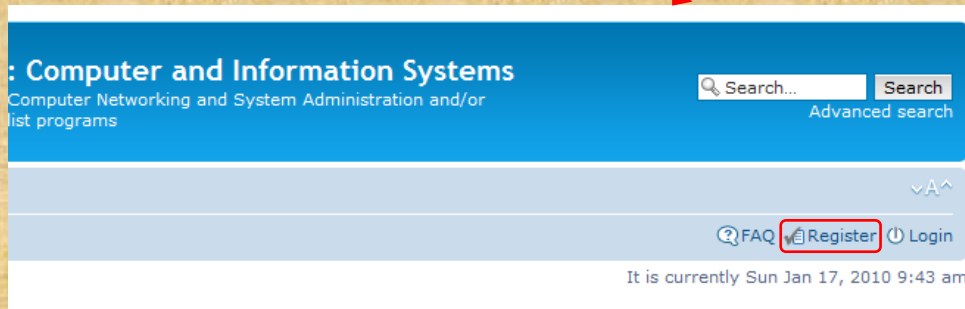


Benji Simms


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

Class Activity Forum Registration

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



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: If you have already registered for a previous CIS course you don't need to do it again.

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.

 Board index Subscribe forum

*Unsubscribed
looks like this.*

 Board index Unsubscribe forum

*Subscribed
looks like this.*

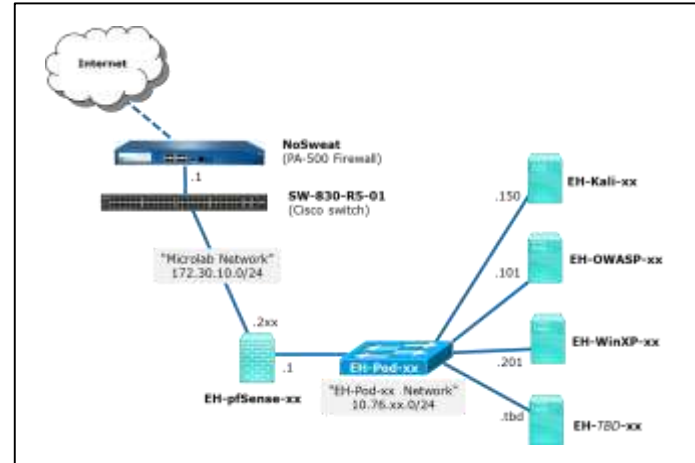


Lab Resources

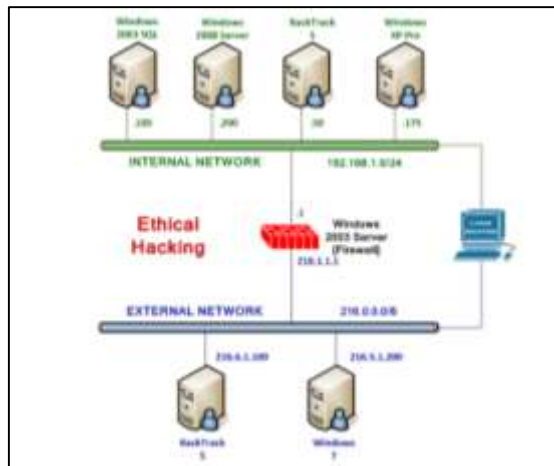
CIS 76 Resources



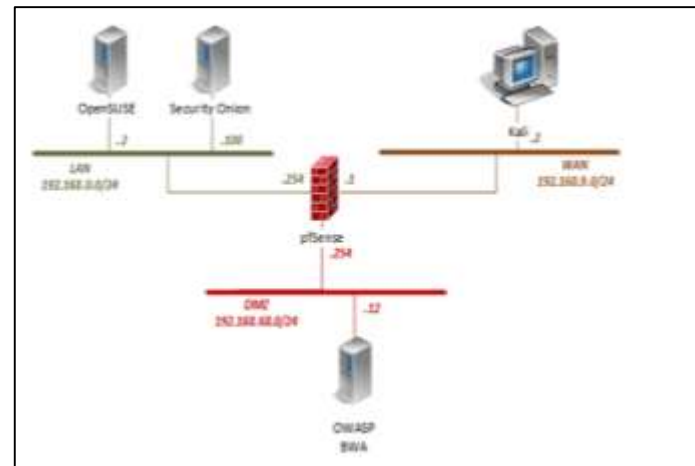
VLab CIS 76 Pod



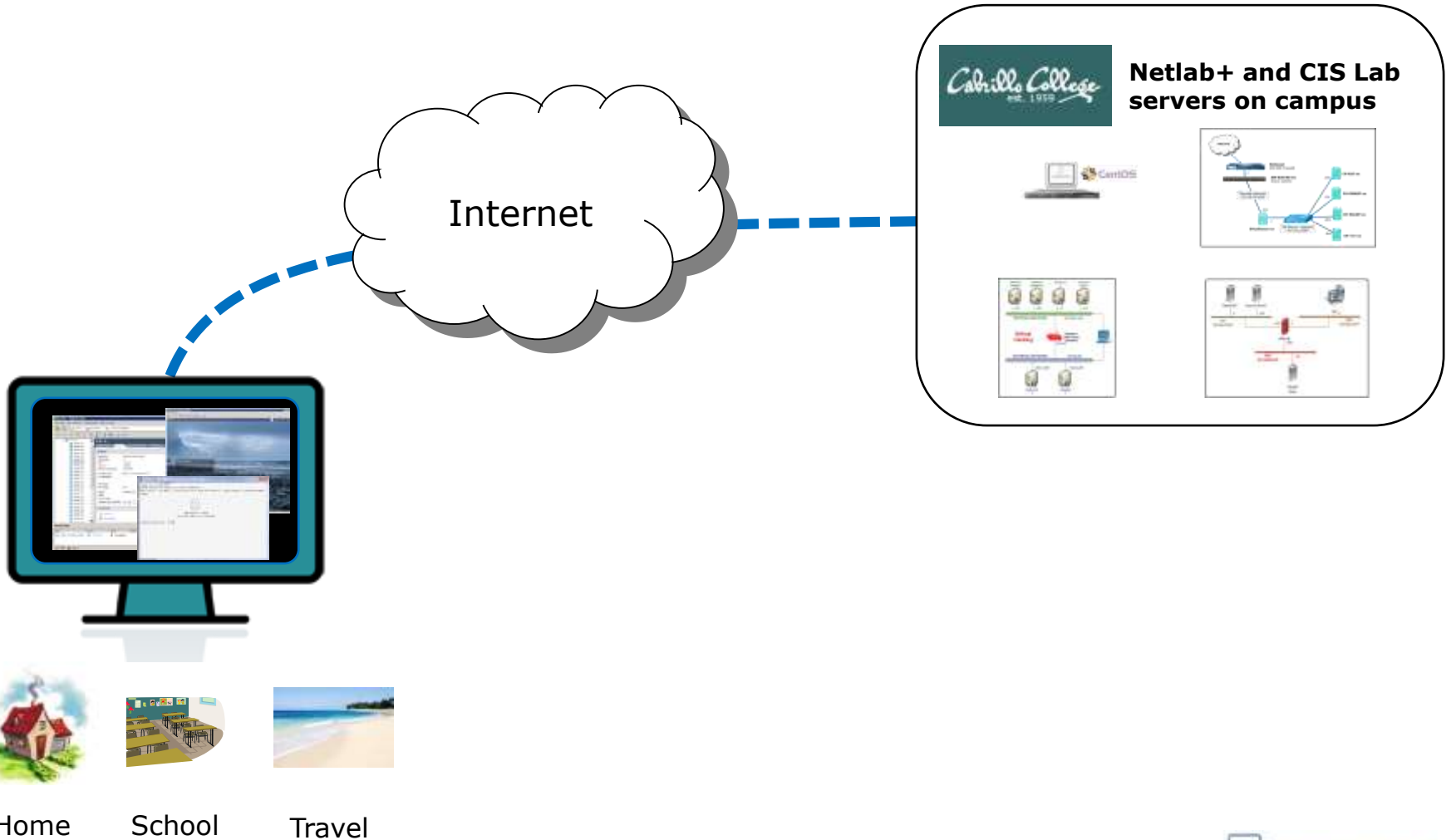
Netlab+ NISGTC Ethical Hacking Pod (2015)



Netlab+ NDG Ethical Hacking Pod (2016)

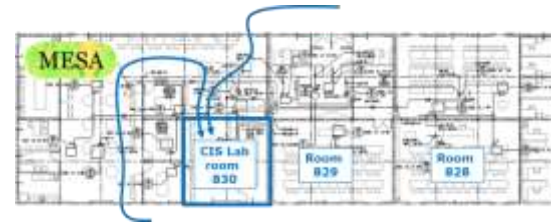
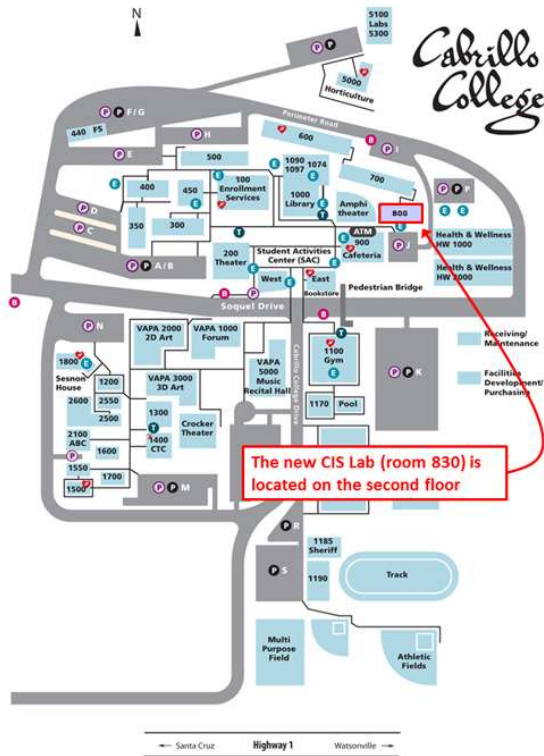


Option 1: Work on assignments online from anywhere



Option 2: Work on assignments in the CIS Lab

Building 800 - Room 830 (in the STEM Center)



Rich's Cabrillo College CIS Classes
CIS 90 Grades

Home	Resources	Forums	CIS Lab	Blackboard
------	-----------	--------	----------------	------------

Instructors, lab assistants and equipment are available CIS students.

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

Use this link to see the schedule and location

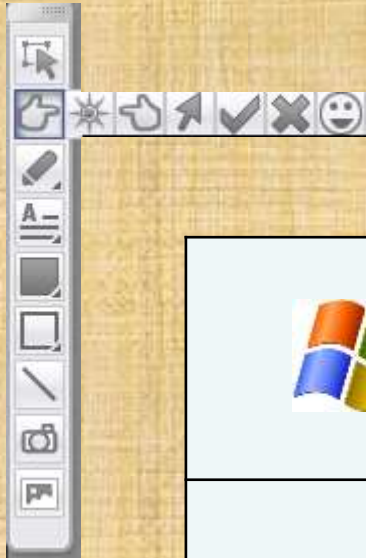
Housekeeping





Instructor Note:

*Switch to
preloaded
whiteboard*

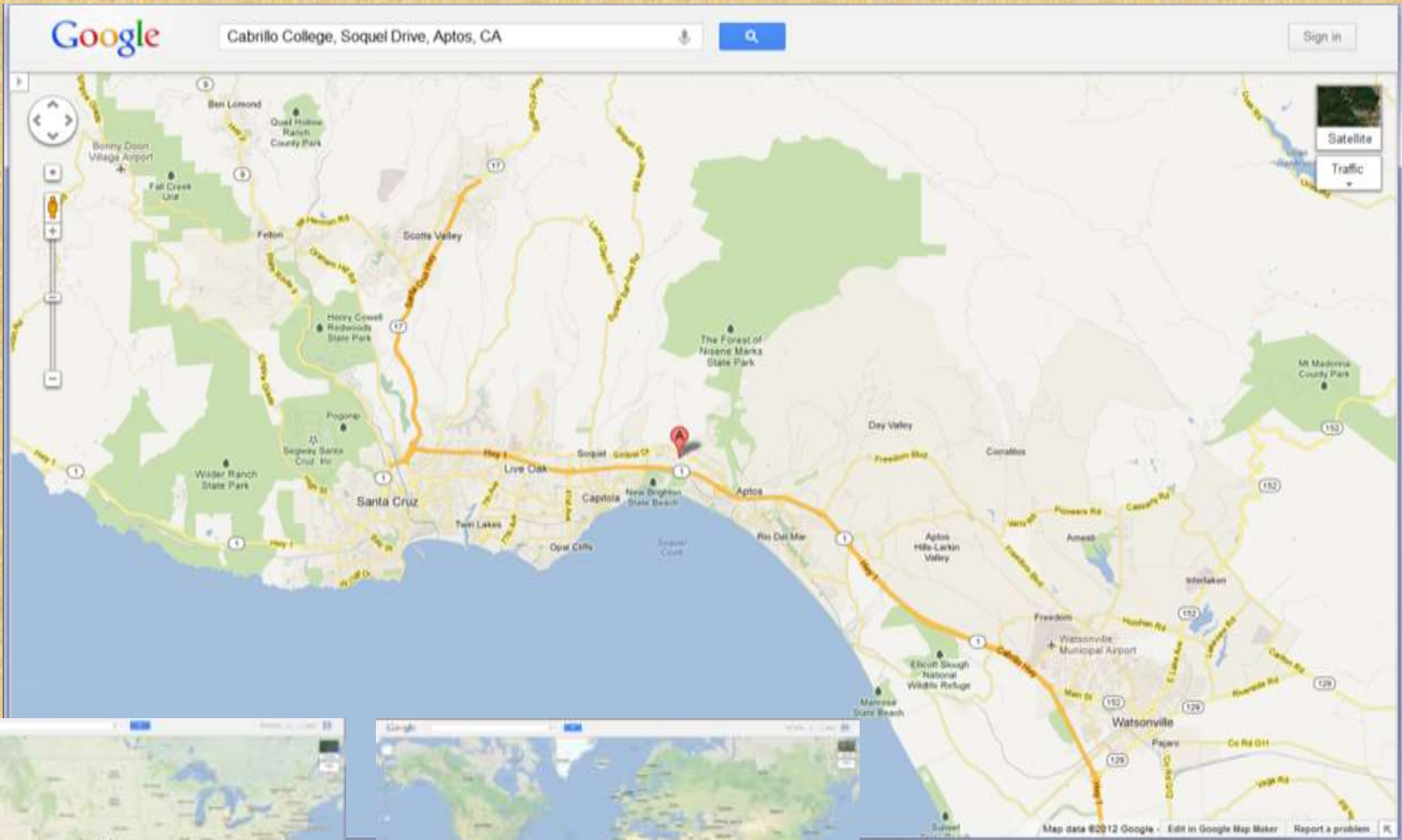


Class Activity

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

			Other

Class Activity – Where are you now?



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

Username and passwords

The Login Credentials slides 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

Recent News



<https://www.nytimes.com/2016/07/27/dnc-hack-e>



http://www.nytimes.com/2016/08/22/technology/apple-software-vulnerability-security-flaws.html?_r=0



<https://www.hackernews.com/2016/07/27/hacking-atm-smartwatch-fitness-tracker.html>



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



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

Yesterday's News



The screenshot shows a web browser window displaying a news article from The Washington Post. The browser's address bar shows the URL: https://www.washingtonpost.com/world/national-security/fbi-is-investigating-foreign-hacks-of-state-election-systems/2016/08/29/6e758ff4-6e00-11e6-8365-b19e428a975e_story.html. The article is categorized under 'National Security' and has the main headline 'Russian hackers targeted Arizona election system'. A sub-headline reads 'FBI: Some voter databases may have been hacked'. The article features a photograph of a large, modern building with a prominent overhang. Below the photo is a video player with a 'Play Video 1:29' button. The text of the article states: 'The FBI says it has found breaches in voter registration systems in Illinois and Arizona, and it's urging states to increase their computer security ahead of the November presidential election. (Reuters)'. The author is listed as 'By Ellen Nakashima' with a date of 'August 29 at 12:00 PM'. At the bottom of the article, a blue banner contains the full URL: https://https://www.washingtonpost.com/world/national-security/fbi-is-investigating-foreign-hacks-of-state-election-systems/2016/08/29/6e758ff4-6e00-11e6-8365-b19e428a975e_story.html

Recent Presentations

Black Hat August 2016



<https://https://www.newscientist.com/article/2101483-scammer-ai-can-tailor-clickbait-to-you-for-phishing-attacks/>

USENIX August 2016



https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_garcia.pdf

Def Con August 2016



<https://http://www.bbc.com/news/technology-36995288>



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.

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



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

Offensive Security



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

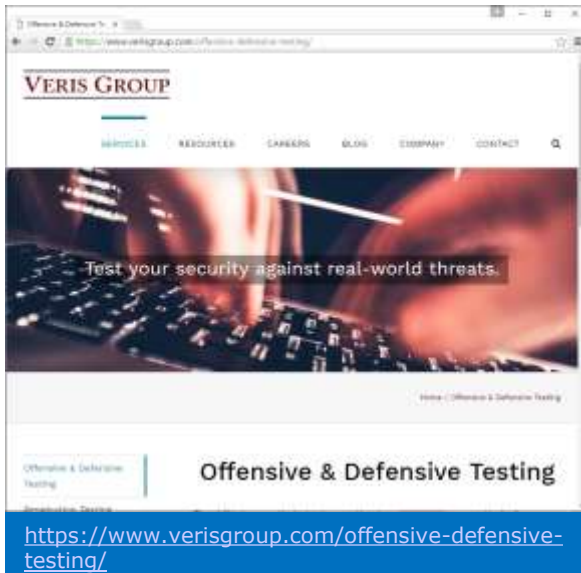
RedTeam Security



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

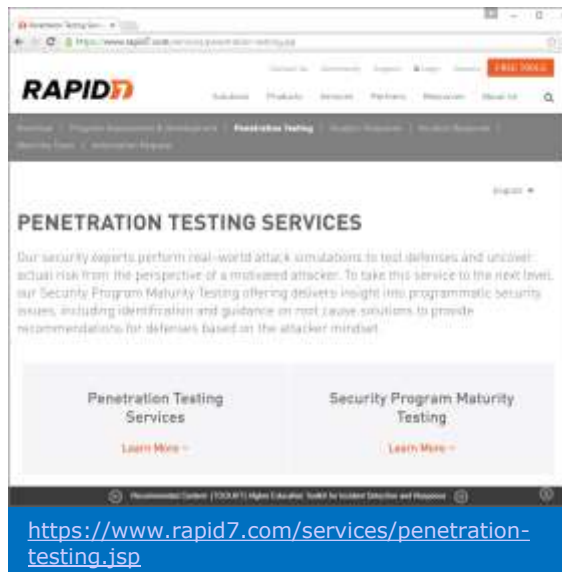
Example Penetration Testing Services

Veris Group



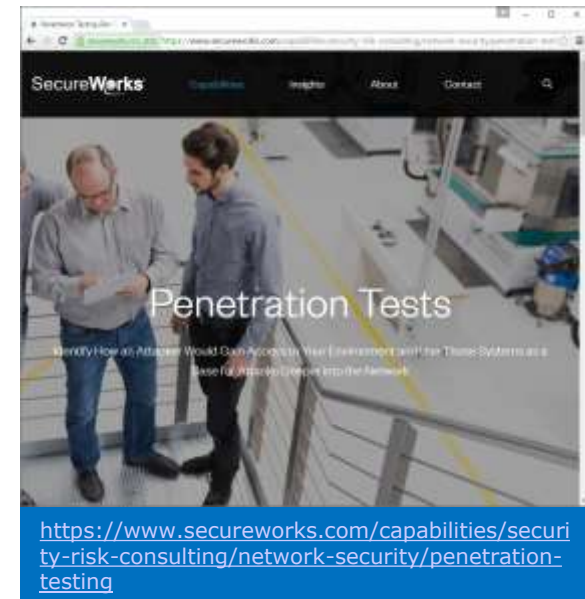
The screenshot shows the Veris Group website. The header includes the company name and navigation links for Home, Services, Careers, Blog, Company, and Contact. A large banner image features a close-up of a computer keyboard with the text "Test your security against real-world threats." Below the banner, the text "Offensive & Defensive Testing" is prominently displayed. A blue URL bar at the bottom contains the link: <https://www.verisgroup.com/offensive-defensive-testing/>

Rapid7



The screenshot shows the Rapid7 website. The header includes the company name and navigation links for Solutions, Products, Services, Partners, Resources, and About Us. A large banner image shows two people in a server room with the text "Penetration Tests" and "Identify How an Attacker Would Gain Access to Your Environment and How Those Systems are at Risk for Attacks Originating from the Network." Below the banner, the text "PENETRATION TESTING SERVICES" is prominently displayed. Two service cards are shown: "Penetration Testing Services" and "Security Program Maturity Testing", each with a "Learn More" link. A blue URL bar at the bottom contains the link: <https://www.rapid7.com/services/penetration-testing.jsp>

SecureWorks

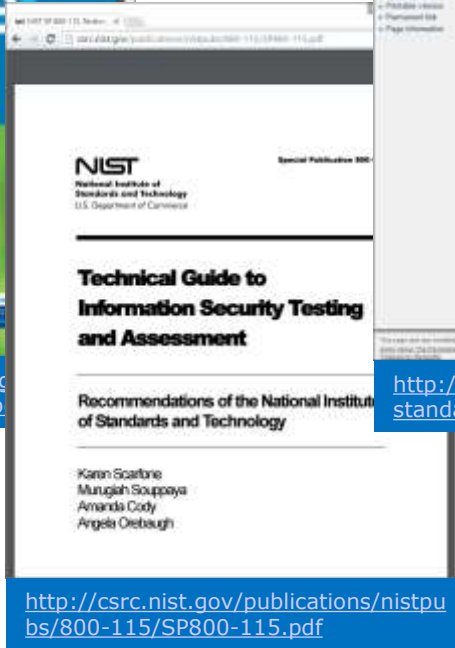


The screenshot shows the SecureWorks website. The header includes the company name and navigation links for Capabilities, Insights, About, and Contact. A large banner image shows two people in a server room with the text "Penetration Tests" and "Identify How an Attacker Would Gain Access to Your Environment and How Those Systems are at Risk for Attacks Originating from the Network." Below the banner, the text "Penetration Tests" is prominently displayed. A blue URL bar at the bottom contains the link: <https://www.secureworks.com/capabilities/security-risk-consulting/network-security/penetration-testing>

Testing Methodologies



https://www.owasp.org/images/OWASP_Testing_Guide_v4.0.pdf



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



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



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

Example Reports

OFFENSIVE SECURITY
Penetration Test Report - MisaCorp Over

Address Webserver Software Compromise

The admin.misaorg.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 6).

IP	Port	Service	Version
10.10.10.10	81	Apache/2.4.18 (Ubuntu)	2.4.18-1ubuntu3.1
10.10.10.10	80	Apache/2.4.18 (Ubuntu)	2.4.18-1ubuntu3.1
10.10.10.10	443	Apache/2.4.18 (Ubuntu)	2.4.18-1ubuntu3.1
10.10.10.10	22	OpenSSH_6.7p1 Ubuntu-1ubuntu0.2	6.7p1-1ubuntu0.2
10.10.10.10	25	Postfix smtpd	
10.10.10.10	53	ISC BIND 9.10.3	9.10.3-4ubuntu1
10.10.10.10	111	rpcbind	
10.10.10.10	135	Microsoft Exchange (AuthAs: Anonymous)	
10.10.10.10	139	Microsoft Exchange (AuthAs: Anonymous)	
10.10.10.10	445	Microsoft Exchange (AuthAs: Anonymous)	
10.10.10.10	593	Microsoft Exchange (AuthAs: Anonymous)	
10.10.10.10	8080	Apache/2.4.18 (Ubuntu)	2.4.18-1ubuntu3.1

Figure 6 - Enumeration of the admin.misaorg.com host quickly identifies the webserver's vulnerable version.

The scan results revealed that along with common Apache default files (the use see Appendix A for more information), we identified an "admin" directory that was only accessible after authentication (Figure 7).

The report page is showing a web server vulnerability

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

CONFIDENTIAL Page 106

Appendix D - Phishing Email Scripts

1. LinkedIn-Password-Reset

LinkedIn

We've successfully changed your LinkedIn password.

Thanks for using LinkedIn! The LinkedIn Team

When did you see this happened?

Link: October 23, 2015, 8:51 PM
Profile: Profile
Location: Hong Kong, China

Search on Bing to see if your account might have been compromised.

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

3.4 Network Infrastructure Assessment

127.127.255.254 (www.eclipsebank.com)

Issue	Charact	Impact	Explo	Resolv	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 containing of rogue plugins.	High	Critical	Easy	Resolved	Upgrade to PHP version 4.4.5 or later.
The remote version of Apache is vulnerable to an off-by-one buffer overflow attack.	High	High	Easy	Resolved	Upgrade to version 2.2.39 or later.
The remote DNS resolver does not use random port queries to third party DNS.	High	High	Moderate	Quick	Contact your DNS server vendor.
The remote servers 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 remote server allows recursive queries to be performed.	Medium	Medium	Medium	Quick	Restrict recursive queries to the hosts that should use this functionality.

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

The screenshot shows the Indeed search results for 'ethical hacker'. The search bar contains 'ethical hacker' and the location is set to 'where'. The results are sorted by relevance. The top job listing is for 'HBSS Specialist' at Strategic Data Systems, with a salary of \$80,000 a year. Other listings include 'Information Security Engineer' at PETSINWART and 'Govt IT Security Webapp Analyst / Pen Tester' at JPI Technology.

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

Pen Tester job search

The screenshot shows the Indeed search results for 'pen tester'. The search bar contains 'pen tester' and the location is set to 'where'. The results are sorted by relevance. The top job listing is for 'Senior Penetration Tester' at PurpleSquamel / Identify Recruiting, with a salary of \$100,000 a year. Other listings include 'GPen Certified Pen Tester with Windows Server Administration' at The Royal Group Inc. and 'Senior Penetration Test Engineer' at Request Technology, LLC.

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

White Hat Hacker job search

The screenshot shows the Indeed search results for 'white hat hacker'. The search bar contains 'white hat hacker' and the location is set to 'where'. The results are sorted by relevance. The top job listing is for 'Cyber Security Specialist' at DOBS (DG Business Solutions) in Milpitas, CA. Other listings include 'Cyber security specialist' at Simplion Technologies Inc. and 'Security Engineer / White Hat Hacker' at ZhoVauR.

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

Ethical Hacker Job Openings (Monster)

Ethical Hacker in CA job search

The screenshot shows a search results page on the Monster website. The search criteria are 'Ethical Hacking' and 'California'. The results list several job openings, including 'Lead Network Information Security Specialist' at Verizon in Irvine, CA, and 'Security Engineer / White Hat Hacker' at ZitoVault in San Diego, CA. A blue sidebar on the left contains a promotional offer for a \$500 reward card and a 2-year price guarantee.

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

Job opening in San Diego

The screenshot displays a detailed job listing for 'Security Engineer / White Hat Hacker' at ZitoVault in San Diego, CA. The job was posted on 8/10/2016. The description seeks a talented professional with experience in white hat hacking and ethical hacking, passionate about understanding cyber security attacks. It highlights the company's focus on the Internet of Things (IoT) and offers an opportunity for career growth. The listing includes a 'Requirements' section and a 'Required Skills' list.

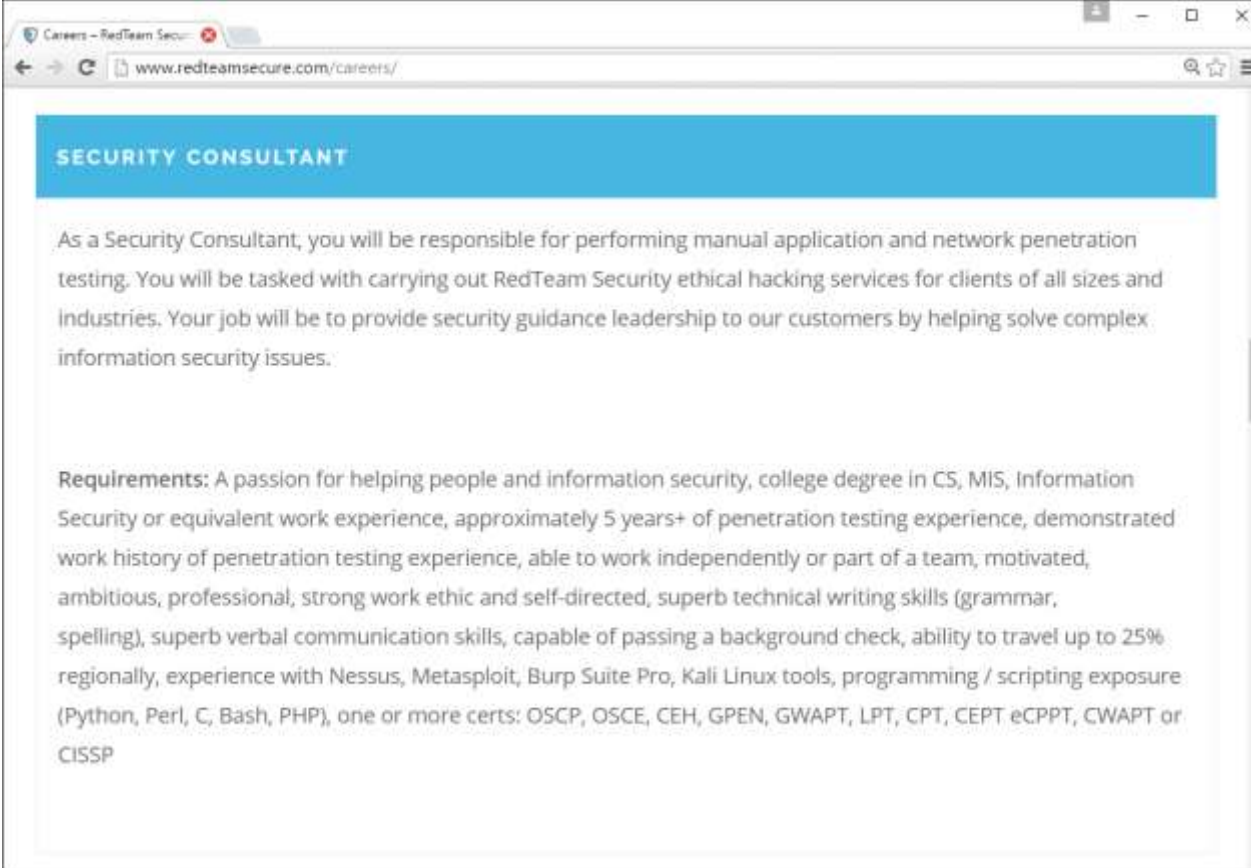
Requirements

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?mescooid=1500125001001&jobPosition=9#>

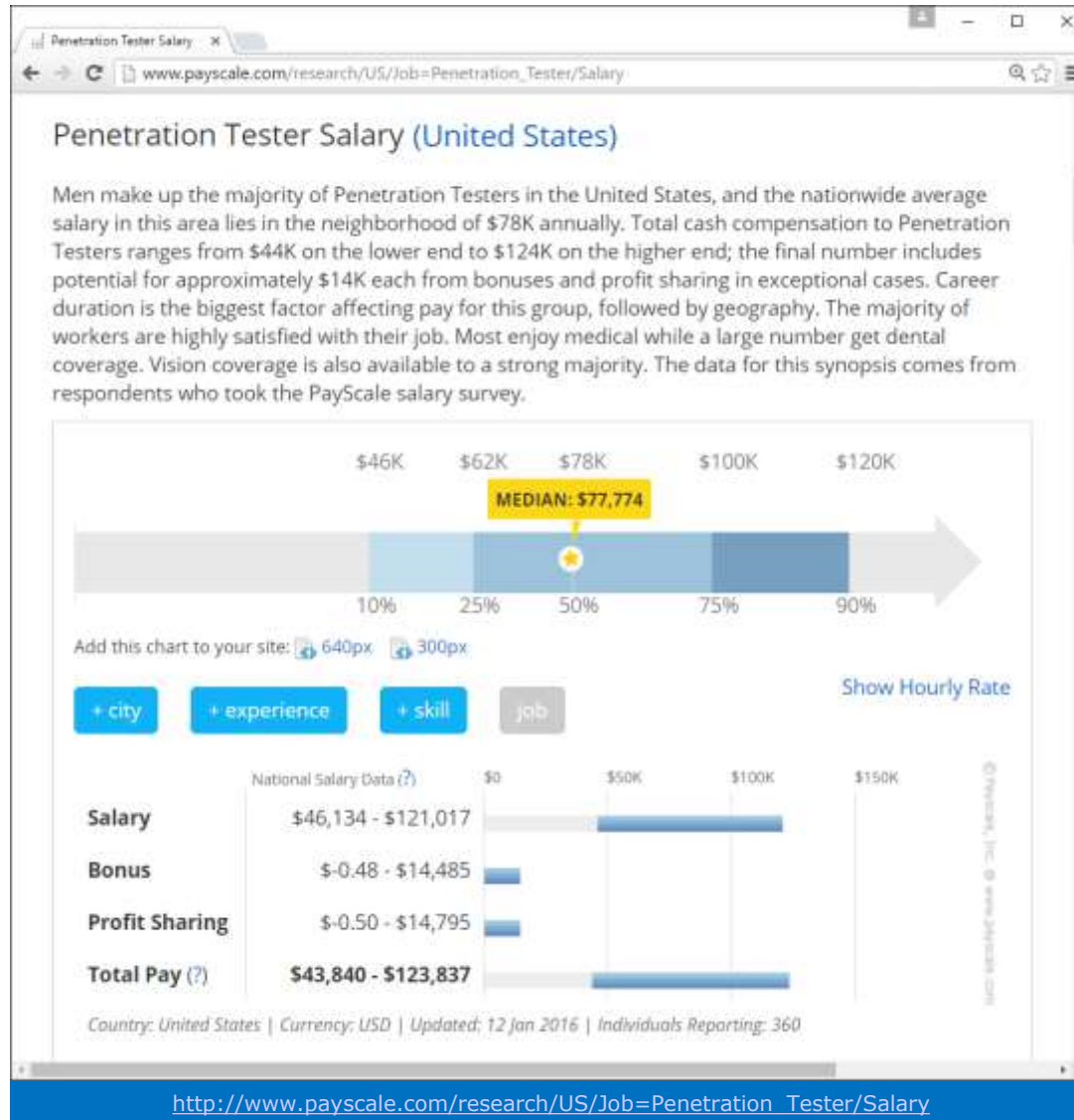
Ethical Hacker Job Openings (On careers page of testing company)



The screenshot shows a web browser window with the URL www.redteamsecure.com/careers/. The page title is "Careers - RedTeam Security". The main heading is "SECURITY CONSULTANT". The job description states: "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." The requirements listed are: "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.

Salary survey of 360 Pen Testers



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



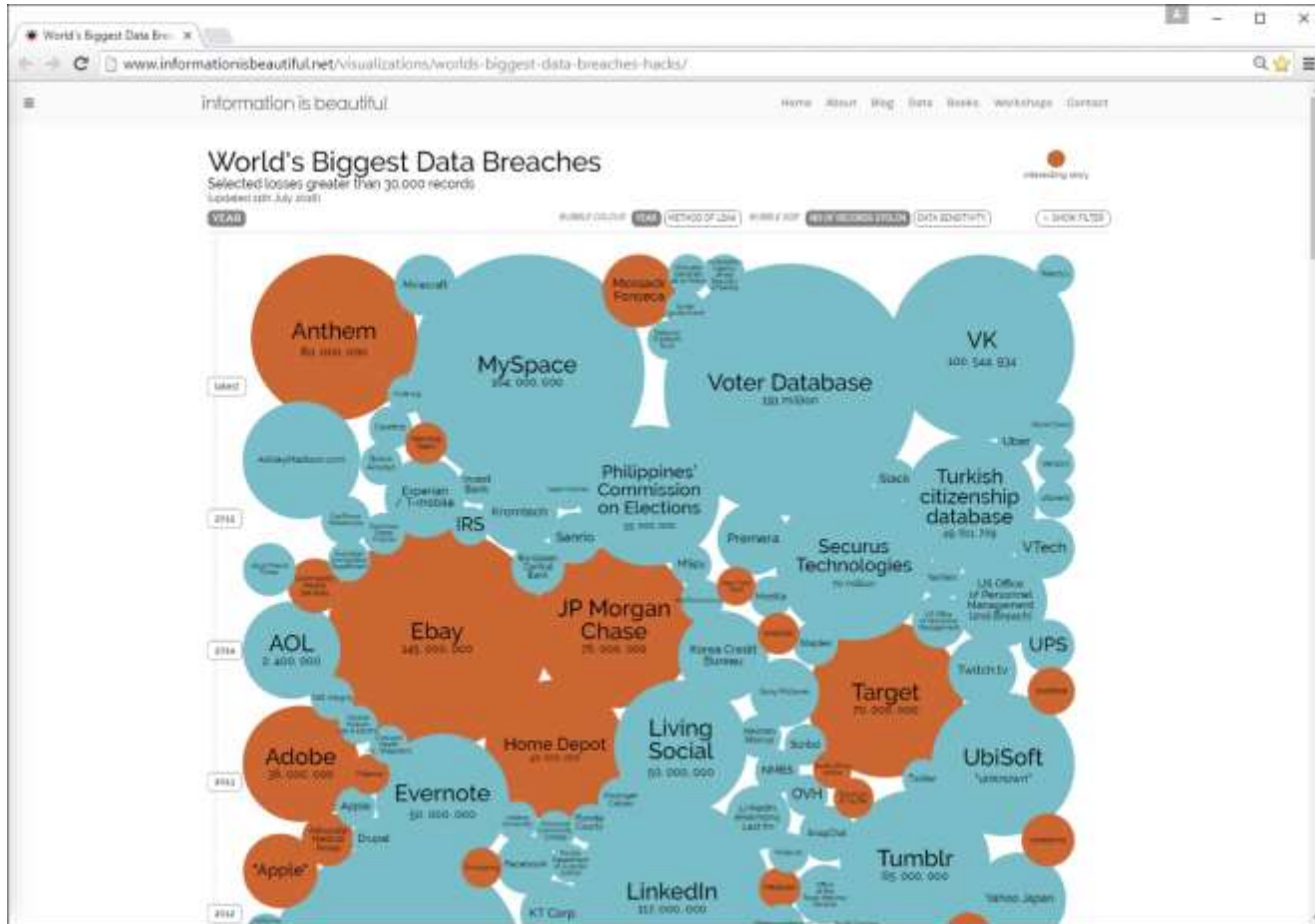
Black Hats

Malicious Unethical Hacking

- Malicious hackers (black hats) are the "bad guys". They include criminals, con artists, disgruntled employees, spies, and hacktivists. 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](#)

Timeline of Major Hacks

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



Live Attack Monitor



This live map graphically depicts attacks taking place across the world

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

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>

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/>



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).
- Propaganda via disinformation and social media.
- Leaking confidential information to influence events.

Ugly Gorilla

Flying Kitten

Berserk Bear

APT 1

Hurricane Panda

Fancy Bear

APT 29



Nation-State Actors

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

<http://www.threatgeek.com/advanced-persistent-threat/>



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



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

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>



"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."



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



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
lsass	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



A screenshot of a user profile on the China Military Network Defense Community (chinamil.com.cn) website. The profile is for a user named '新飞行员' (New Pilot). The profile includes a gold pilot's wings badge, a bio, and various statistics and contact information.

中国军网国防社区
www.chinamil.com.cn

关心国防 就是关心我们的家园

网友个人资料

	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:			

[查看个人资料](#)

[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](http://bbs.chinamil.com.cn/forum/bbsui.jsp?id=(o)5681)

Chinese Hacker Slang

Search the Mandiant APT1 Report for "meat chicken".

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

What is a "meat chicken"?

Put your answer in the chat window

肉鸡 "rou ji"

DNC Hack



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 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

- 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 “Fleep CrowdStrike!!!!!!!!!!”



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

<http://www.threatgeek.com/advanced-persistent-threat/>

"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 programming 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

<http://www.threatgeek.com/advanced-persistent-threat/>

<u>CrowdStrike</u>	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>

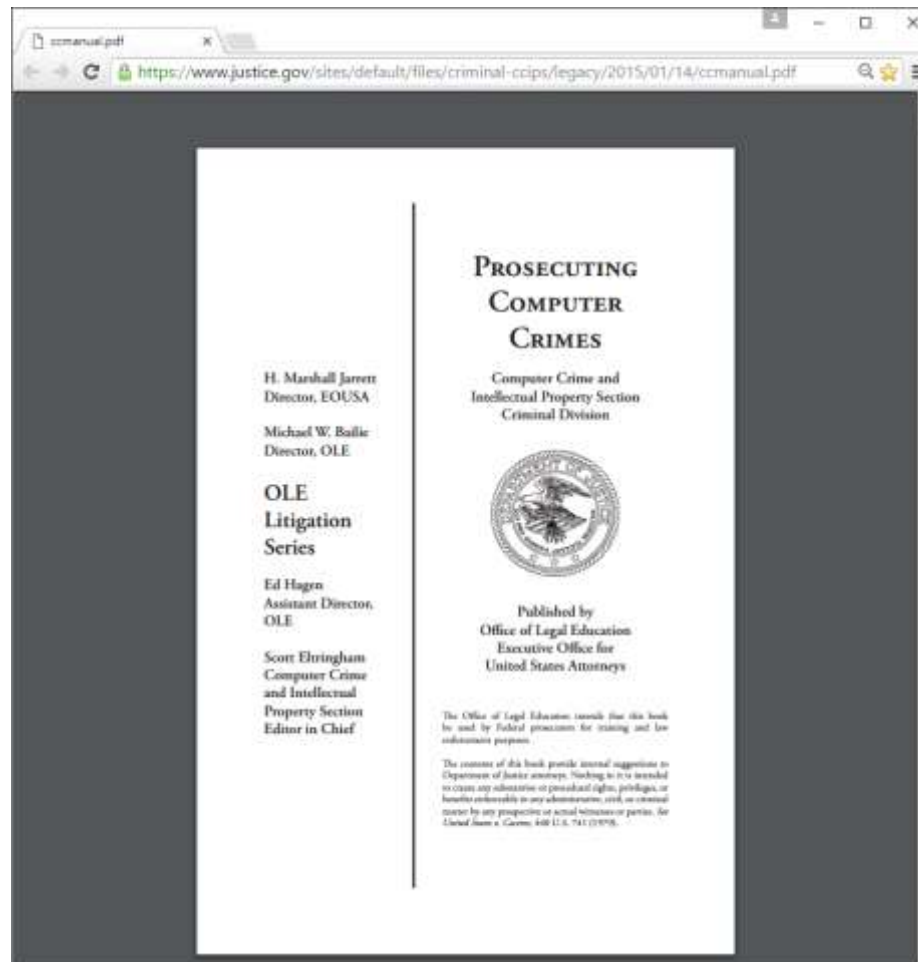
Digital Millennium Copyright Act

- 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



The suggested guidelines for US Attorneys in prosecuting computer crimes

Federal

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

The Computer Fraud and Abuse Act

Misdemeanor

Felony

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 I. 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.

State

The screenshot shows a web browser window displaying the NCSL website. The page title is 'Computer Crime Statutes'. The NCSL logo is visible at the top left, with the tagline 'Strong States, Strong Nation'. A navigation menu includes 'ABOUT US', 'LEGISLATORS & STAFF', 'RESEARCH', 'MEETINGS & TRAINING', 'NCSL IN D.C.', 'MAGAZINE', and 'BLOG'. The main content area features a magnifying glass over a 'CYBER CRIME' graphic. The text explains that computer crime laws encompass actions that destroy or interfere with normal operation of a computer system. It defines hacking as breaking into computer systems and unauthorized access as approaching, trespassing, or transmitting data without consent. A table at the bottom lists state-specific laws for Alabama, Alaska, Arizona, Arkansas, California, Colorado, and Connecticut.

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. § 18-6.3-101 to -102
Connecticut	Conn. Gen. Stat. § 53a-250 to 53a-261

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

California Penal Code 484-502.9

**PENAL CODE
SECTION 484-502.9**

Search document for computer

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 18855 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 18855 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

- (1) 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) deceive or execute any scheme or artifice to defraud, deceive, or entice, 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 program** 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 program** which reside or exist internal or external to a public safety infrastructure **computer system**, **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 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 system**, or **computer network** in violation of this section.
 - (14) knowingly introduces any **computer contaminant** into any public safety infrastructure **computer system**, **computer system**, or **computer network**.
- (8) (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

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.

(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:

<http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=484-502.9>

and locate § 502 (c) (1-14).

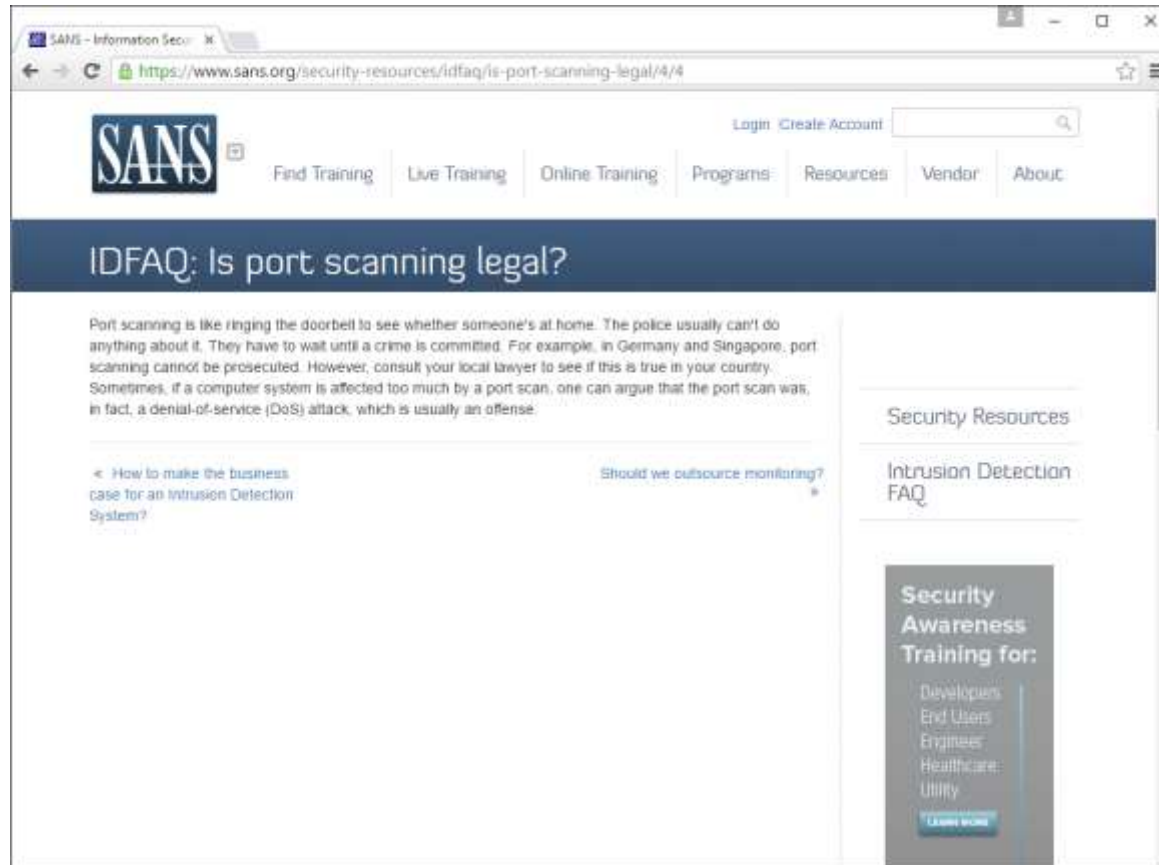
Which sub clause, 1-14, may be applicable to unintentionally crashing a target computer system while doing a vulnerability scan.

Put your answer in the chat window



Are port
scans legal?

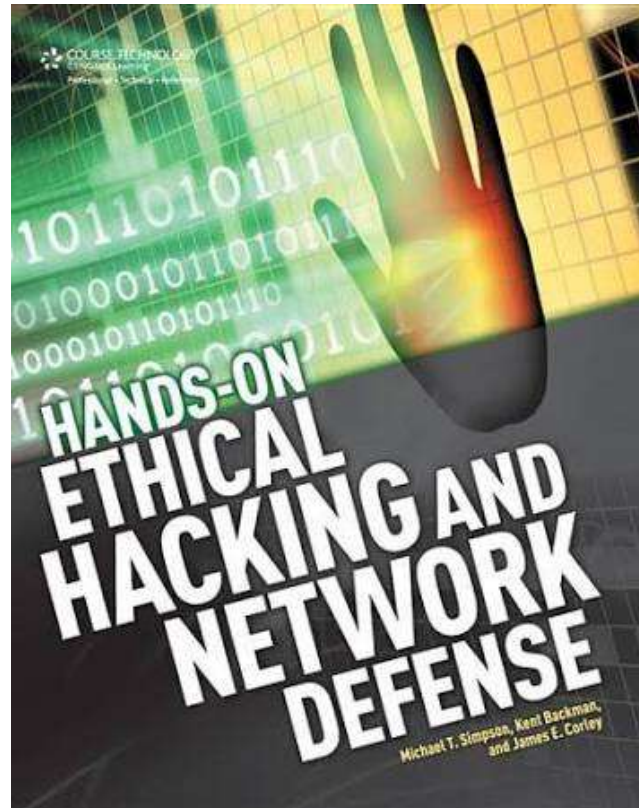
Is port scanning legal?



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

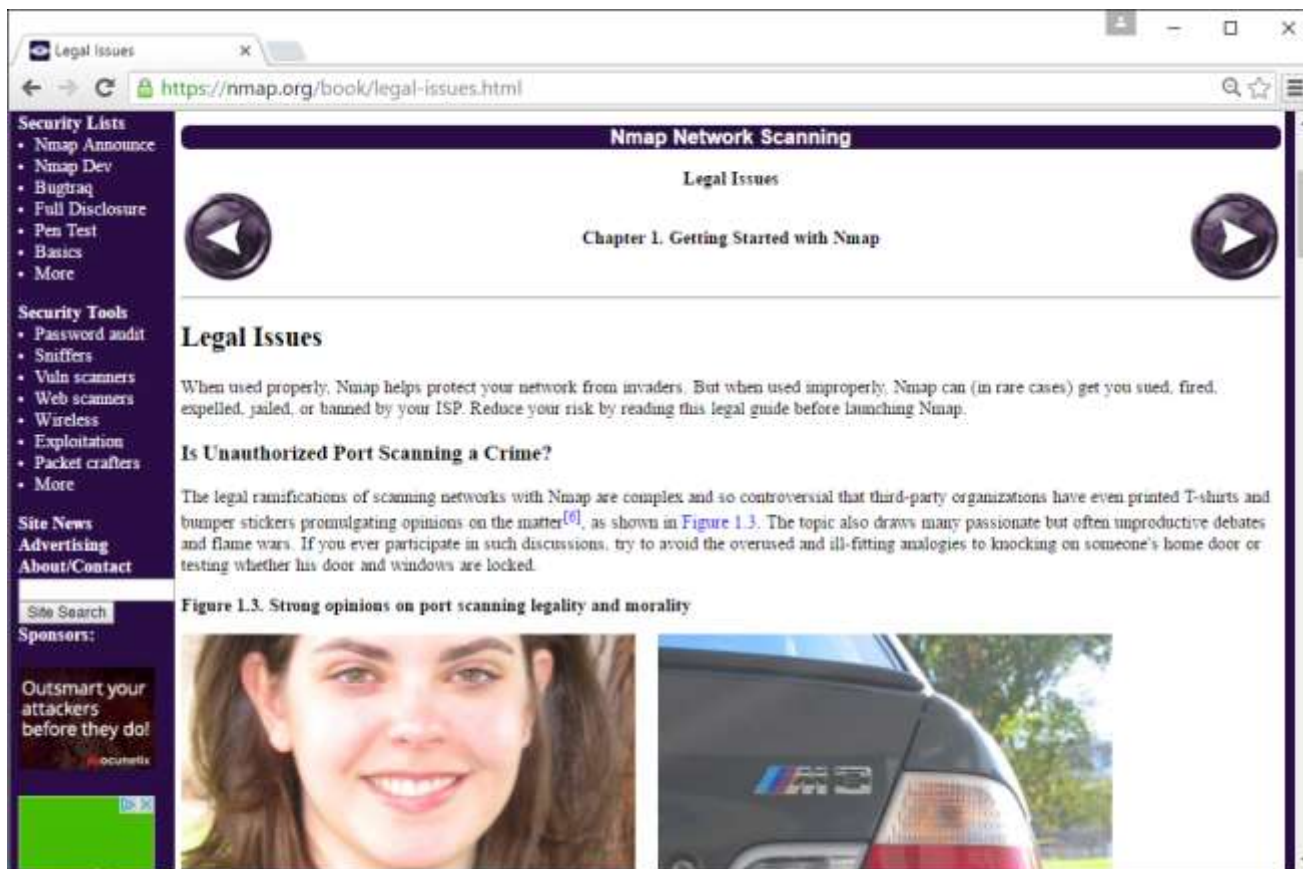
This SANS FAQ says that laws on port scans vary by country. However it could be argued that a port scan caused a DoS which could be prosecuted.

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?



<https://www.sans.org/security-resources/ifaq/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



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

"Unauthorized port scanning is strictly prohibited;"

AT&T



<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



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

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

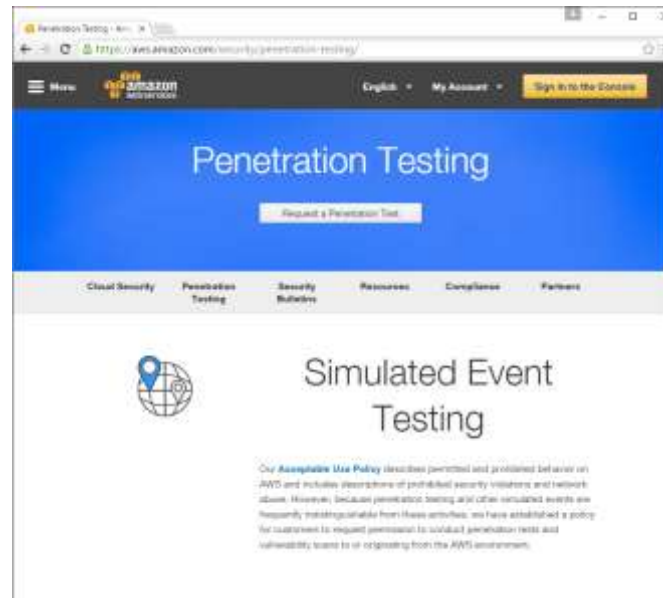
Charter



<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?



<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?



"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."



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	<u>Concise Cybersecurity</u>
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

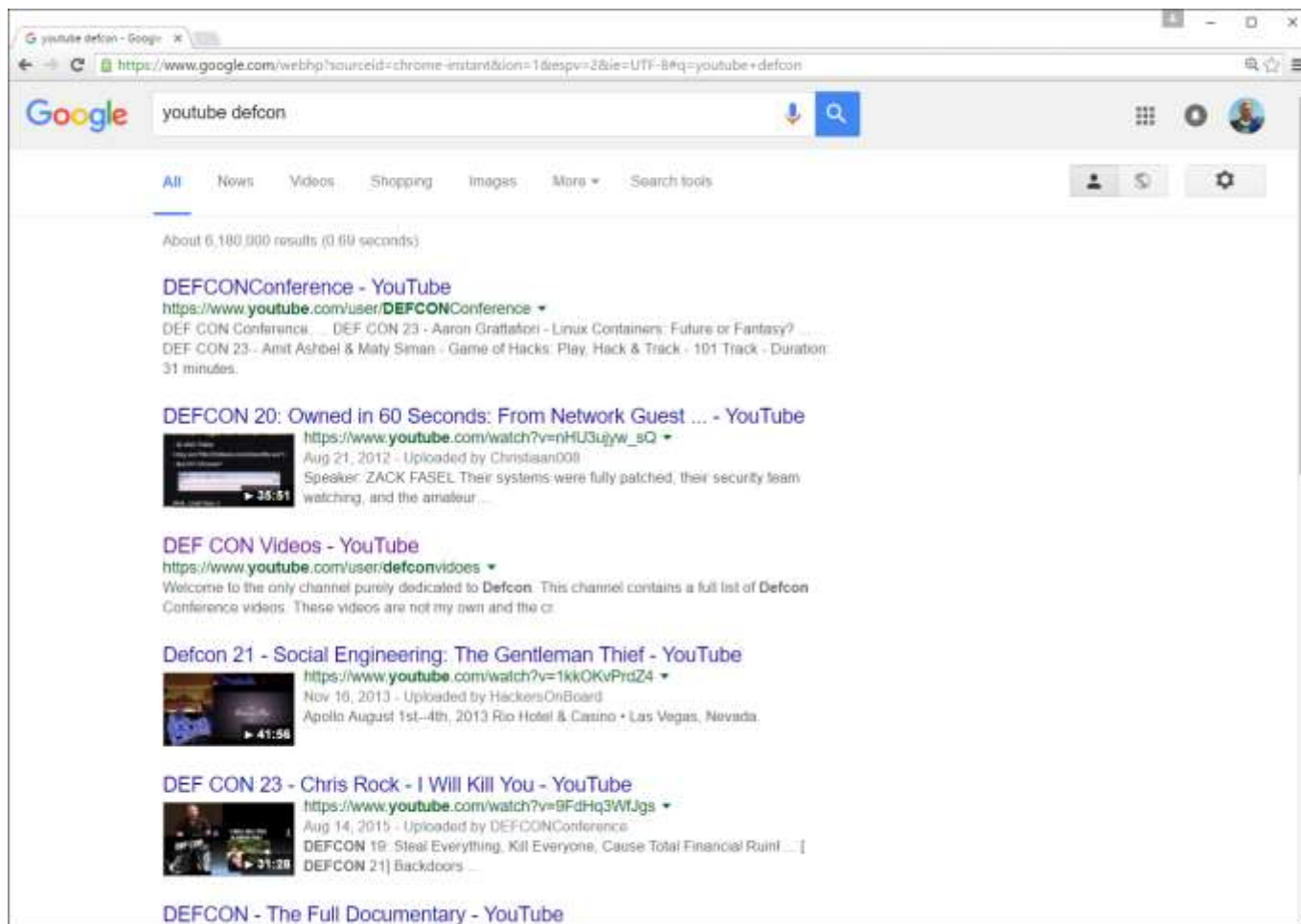


Black Hat

DEF CON

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

Google: youtube defcon



Looking ahead ...

Sept 10-19 2016, SANS Network Security 2016 Las Vegas

July 22-27 2017, Black Hat USA 2017 Las Vegas

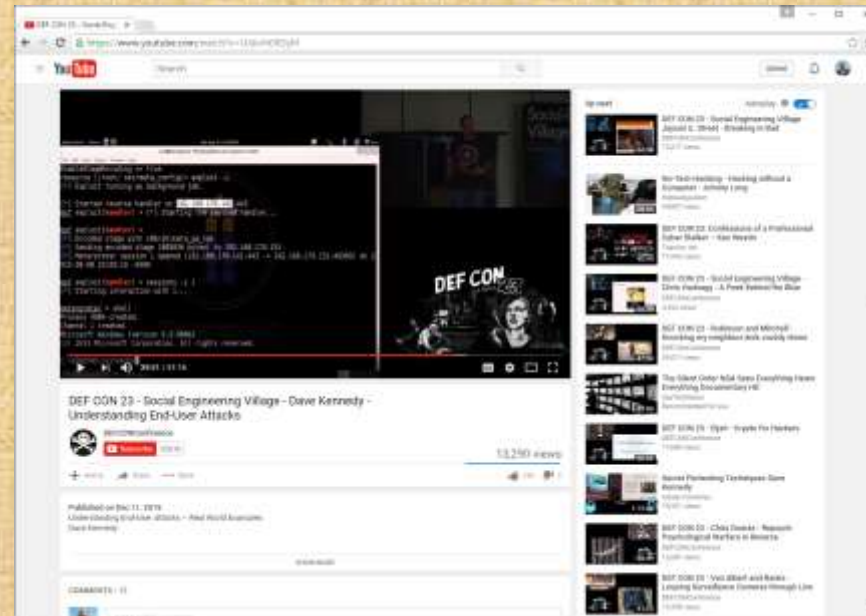
July 27-30 2017, DEF CON 25 Las Vegas

<https://www.concise-courses.com/security/conferences-of-2016/>

<https://www.concise-courses.com/security/conferences-of-2017/>

An Expert at Work Activity

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



<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 (39:45-44:00). 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

Bulletin (SB16-207)
Vulnerability Summary for the Week of July 18, 2016
Original release date: July 20, 2016

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The divisions of high, medium, and low severities correspond to the following scores:

- High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletin is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities				
Primary Vendor - Product	Description	Published	CVSS Score	Source & Patch Info
cisco - ios_xr	Cisco IOS XR 5.x through 5.2.5 on NCS 6000 devices allows remote attackers to cause a denial of service (timer consumption and Route Processor reload) via crafted SSH traffic. aka Bug ID CSCux76819	2016-07-15	7.8	CVE-2016-1426 CISCO #
cisco - ios_xr	The CLI in Cisco IOS XR 6.x through 6.0.1 allows local users to execute arbitrary OS commands in a privileged context by leveraging unspecified container access.	2016-07-15	7.2	CVE-2016-1430 CISCO #

SANS Blogs

The screenshot shows the SANS Penetration Testing website. The header includes the SANS logo and navigation links for Resources, Training, Events, Certification, Instructors, and About. A search bar is located in the top right. The main content area features three blog posts:

- 05 Jul 2016**
Python Cheat Sheet - pyWars (SEC573)
0 comments Posted by blanchard
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 eskoutis
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 eskoutis
Filed under: Scanning, scapy
One of my favorite tools for fine-grained interactions with target systems during penetration testing is the mighty Scapy. 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](#)

On the right side, there is a social media sharing section with buttons for Facebook, Twitter, LinkedIn, and StumbleUpon. Below that is a search bar and a categories list:

- Anomaly Analysis (1)
- Anti-Virus Evasion (7)
- Backdoor (2)
- Challenges (23)
- 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 (8)
- Protocol Analysis (1)
- Python (11)

Cybrary

The screenshot shows a web browser window displaying the Cybrary website. The browser's address bar shows the URL <https://www.cybrary.it/blog/>. The website's navigation bar includes links for 'MY PROFILE', 'COURSES', 'OPIN', 'EXPLORE', 'TEAMS', and 'ADVERTISE'. A search bar on the right says 'Welcome, Rich'. The main content area is titled 'Published Cyber Security Blog Posts' and features three articles:

- [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 edpsing 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 >>
- Julia: A Misunderstood and Underutilized Language**
Published: July 26, 2016 | By: gromitvortex | Views: 401
By Andrey Makhanzov A lot of people think julia is a combination of julia and R programming languages. However, that's simply not true. I originally created the "julia" 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: kyleharrington | Views: 317
What is Tradecraft Tuesday? Every Tuesday at 12pm ET, Chris Bisnett and Kyle Harrington 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 >>

On the left side of the page, there is a 'Share now!' section with social media icons for Facebook, Twitter, Google+, LinkedIn, and Email.

Hacker News

The screenshot shows the Hacker News website interface. At the top, there is a navigation bar with links for Home, Hacking, Tech, Cyber Attacks, Vulnerabilities, Malware, and Spying. The main header features the site's logo, "The Hacker News™ Security in a serious way", and social media statistics for Google+, Twitter, and Facebook. Below the header, there are three product advertisements: a Supermicro SuperServer 5038D-I, a 2FA Endpoint Protection solution, and an HP 813874-B21 10Gbase-T Sfp+ Transceiver. The main content area displays two articles. The first article, titled "End of SMS-based 2-Factor Authentication; Yes, It's Insecure!", is dated Wednesday, July 27, 2016, and is by Mohit Kumar. It includes a red banner with the text "SMS two-factor is Dead!" and a hand holding a smartphone. The article text states that SMS-based Two-Factor Authentication (2FA) has been declared insecure and might be a thing of the past. The second article, titled "KeySniffer Lets Hackers Steal Keystrokes from Wireless Keyboards", is also dated Wednesday, July 27, 2016, and is by Mohit Kumar. It features a graphic showing a keyboard and a person with a keyhole over their mouth. The article text explains that radio-based wireless keyboards and mice can expose all secrets, including passwords and credit card numbers. On the right side of the page, there is a green advertisement for "Beginner's Guide to Open Source Intrusion Detection Tools" with a "DOWNLOAD FREE GUIDE" button. Below this is another advertisement for a Supermicro SuperServer 5038D-I - 4x... with an image of the server hardware.



MS08-067 CVE-2008-4250 Hack

Live demo

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



VLab Pod Setup

Live demo

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

Assignment



Assignments and Due Dates

Lesson	Date	Topics	Chapter	Due*
1	8/30	<p>Ethical Hacking Overview</p> <ul style="list-style-type: none"> How the course works Presentation slides (download) <p>Supplemental</p> <ul style="list-style-type: none"> How to become an Ethical Hacker (link) Ethical Hacking Code of Ethics (link) VLab Pod Setup (link) <p>Assignment</p> <ul style="list-style-type: none"> Student Survey & Agreement Lab 1 <p>CCC Confer</p> <ul style="list-style-type: none"> Enter virtual classroom Class archives 	1	
2	9/6	<p>Quiz 1</p> <p>TCP/IP Review</p> <ul style="list-style-type: none"> TBD TBD TBD <p>Materials</p> <ul style="list-style-type: none"> Presentation slides (download) <p>Supplemental</p> <ul style="list-style-type: none"> TBD (download) <p>Assignment</p> <ul style="list-style-type: none"> Lab 2 <p>CCC Confer</p> <ul style="list-style-type: none"> Enter virtual classroom Class archives 	2	<p>Lab 1</p> <p>Student Survey & Agreement</p>

Assigned on 8/30

Survey & Agreement

Lab 1

Both due by 11:59PM (Opus Time) on Tuesday 9/6

Lab Assignments

Pearls of Wisdom:

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



Wrap up



Next Class

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

*Lab 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