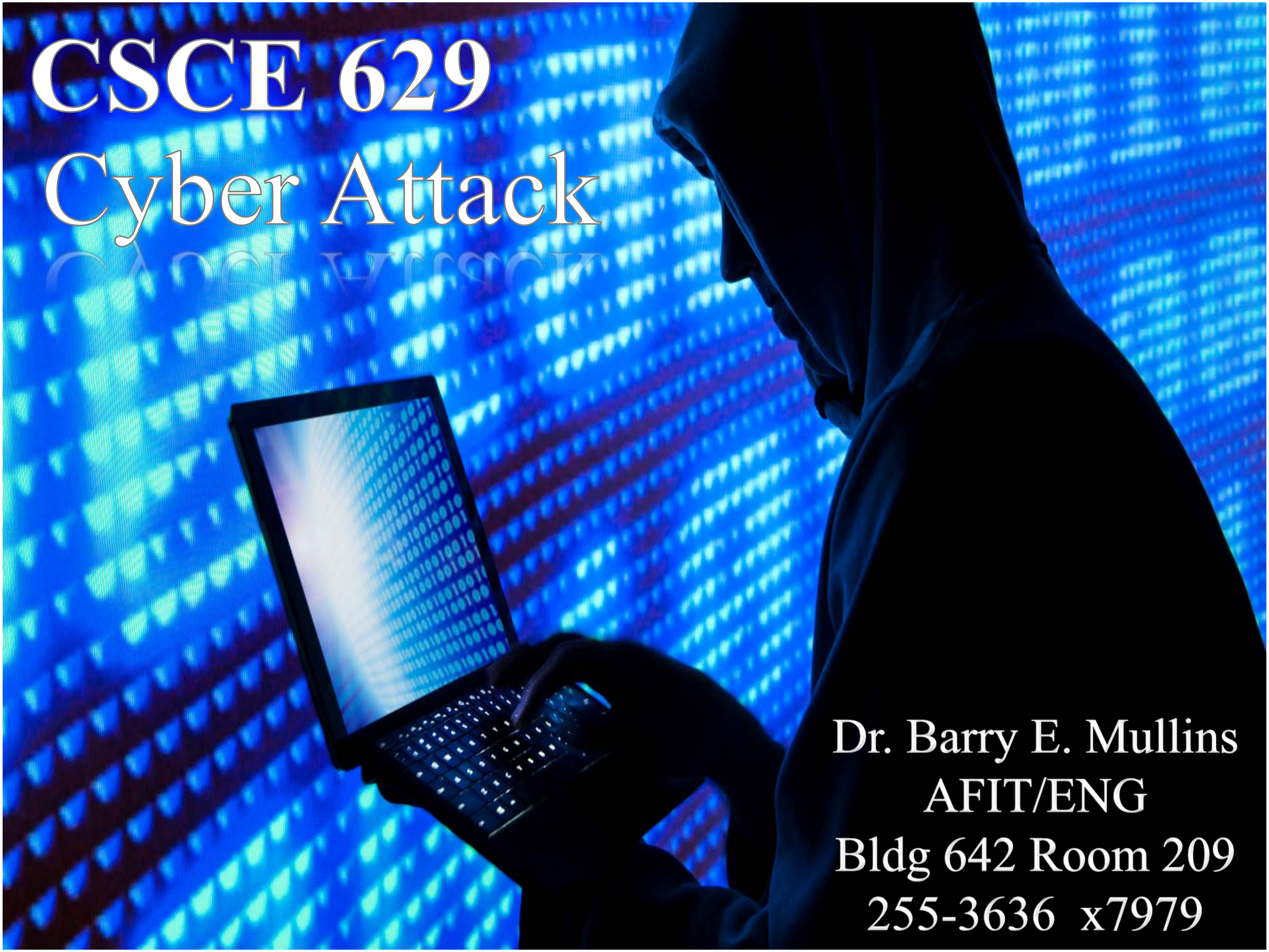


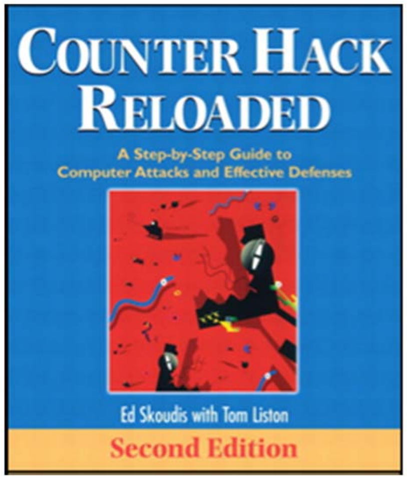
CSCE 629
Cyber Attack

Dr. Barry E. Mullins
AFIT/ENG
Bldg 642 Room 209
255-3636 x7979

root@kali:~# whoami

- 1983 – OTS
- Vandenberg AFB
  - ASAT missile
- AFIT (GCE-87D)
  - MS - AI
- AFRL – Armament Dir - Eglin AFB
  - Expert systems development
- USAFA – EE Dept
- Virginia Tech
  - PhD - Wireless LAN protocols
- AFRL – Information Dir - WPAFB
- USAFA – EE Dept
- Retired on 1 Oct 2004 as Lt Col

Course Materials


COUNTER HACK RELOADED
A Step-by-Step Guide to Computer Attacks and Effective Defenses
Ed Skoudis with Tom Liston
Second Edition

- *Counter Hack Reloaded - A Step-by-Step Guide to Computer Attacks and Effective Defenses*
  - Ed Skoudis, Prentice Hall, 2nd edition, 9th printing

- Class notes
- Select papers

Skoudis @ AFIT 28 Jan 2016

Course Materials
Useful References

- *RTFM: Red Team Field Manual*, Clark 2014
- *BTFM: Blue Team Field Manual*, White 2017
- *Hacking The Art of Exploitation*, 2nd ed, Erickson 2008.
- *BackTrack 5 Wireless Penetration Testing Beginners Guide*, Vivek Ramachandran 2011
- *Metasploit: The Penetration Tester's Guide*, David Kennedy 2011
- *Hacking Exposed*, 7th ed by Stuart McClure 2012
- *Hacking Web Applications Exposed*, Joel Scambray, 3rd ed. 2010.
- *Gray Hat Hacking: The Ethical Hacker's Handbook*, Daniel Regalado 2015

List of Helpful Information Security Multimedia

https://github.com/1337list/ephemera-miscellany/blob/master/hackertalkytalk.md

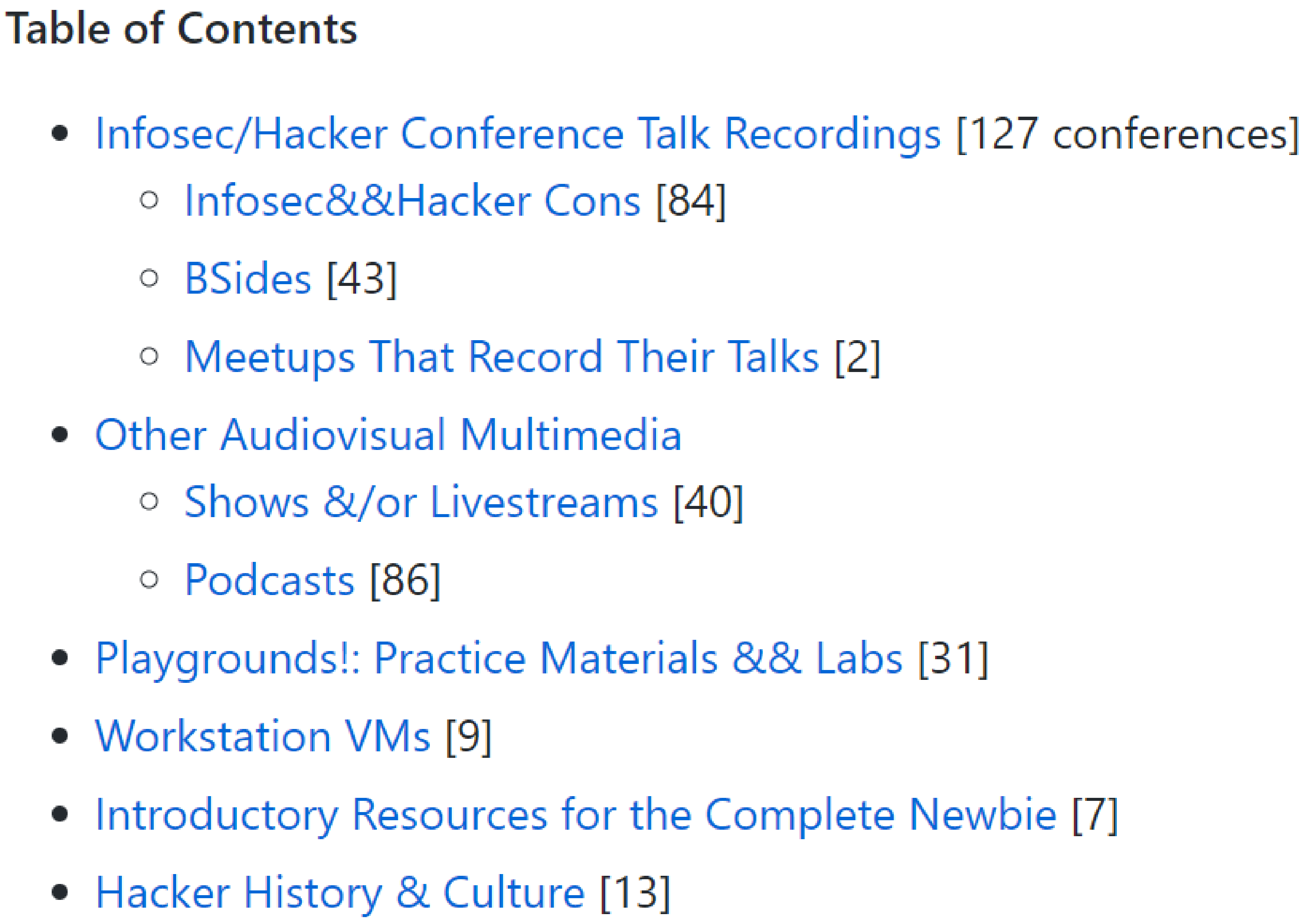
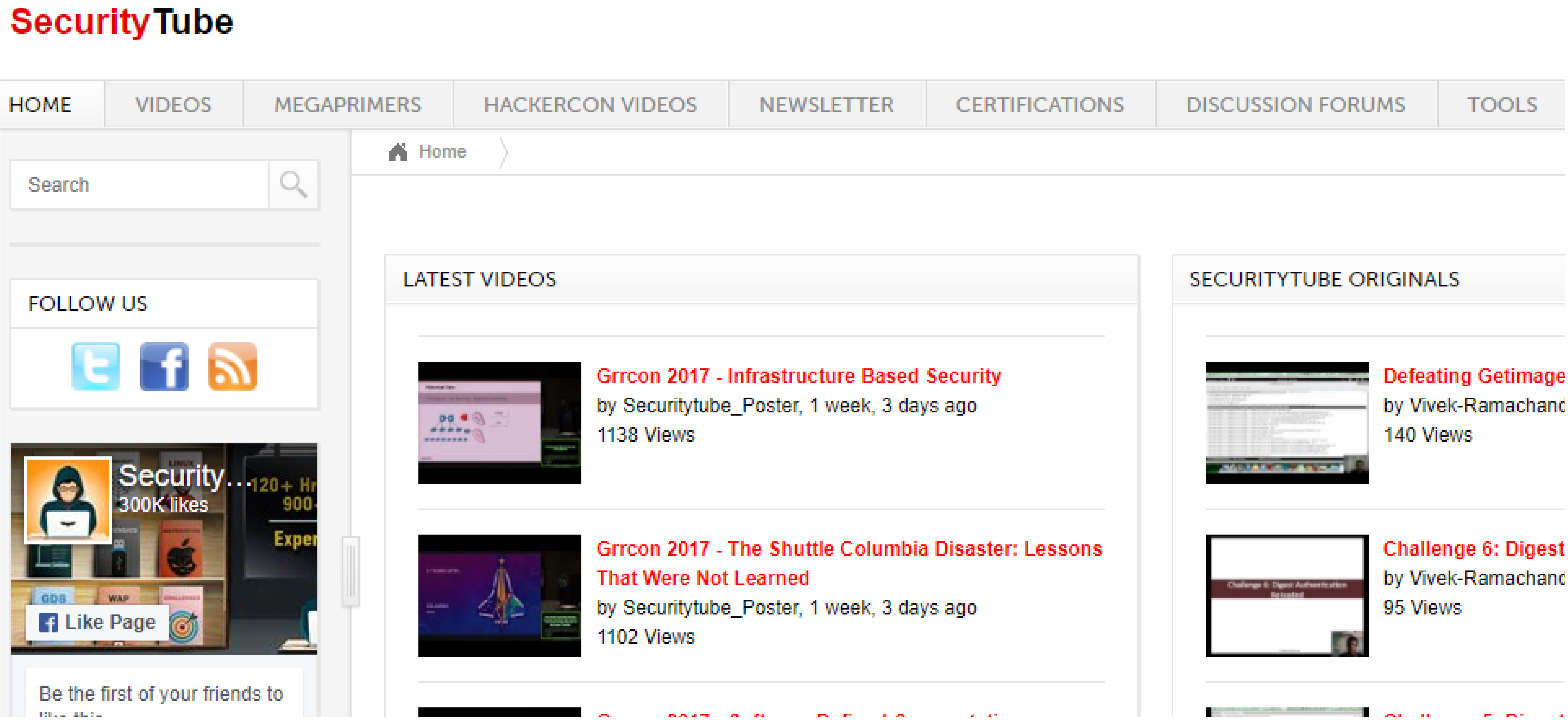


Table of Contents

- Infosec/Hacker Conference Talk Recordings [127 conferences]
  - Infosec&&Hacker Cons [84]
  - BSides [43]
  - Meetups That Record Their Talks [2]
- Other Audiovisual Multimedia
  - Shows &/or Livestreams [40]
  - Podcasts [86]
- Playgrounds!: Practice Materials && Labs [31]
- Workstation VMs [9]
- Introductory Resources for the Complete Newbie [7]
- Hacker History & Culture [13]

Course Materials
Useful References-www.securitytube.net



SecurityTube

HOME | VIDEOS | MEGAPRIMERS | HACKERCON VIDEOS | NEWSLETTER | CERTIFICATIONS | DISCUSSION FORUMS | TOOLS

Home

Search

FOLLOW US

Security... 300K likes

Like Page

Be the first of your friends to

LATEST VIDEOS

Grrcon 2017 - Infrastructure Based Security
by Securitytube_Poster, 1 week, 3 days ago
1138 Views

Grrcon 2017 - The Shuttle Columbia Disaster: Lessons That Were Not Learned
by Securitytube_Poster, 1 week, 3 days ago
1102 Views

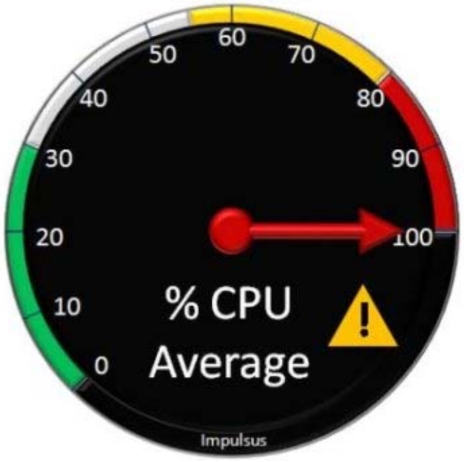
SECURITYTUBE ORIGINALS

Defeating Getimage
by Vivek-Ramachand
140 Views

Challenge 6: Digest
by Vivek-Ramachand
95 Views

Course Workload

Coursework	Weight
Exam (week 8)	25%
Final Project (weeks 7-10)	35%
6 Labs	30%
Project (Python tools)	10%



- Late penalties apply to work not submitted on time

1 business day	-10%
2 business days	-30%
3 business days	-60%
4 business days	-100%

- Submit a hardcopy during class unless told otherwise
  - Please do not email your work
  - Please do not “drop off” your work at my office

Grades

Grade	Grade Point Equivalent	Percent Equivalent
A	4.0	93.0-100.0
A-	3.7	90.0-92.9
B+	3.3	87.1-89.9
B	3.0	83.0-87.0
B-	2.7	80.0-82.9
C+	2.3	77.1-79.9
C	2.0	73.0-77.0
C-	1.7	70.0-72.9
D+	1.3	67.1-69.9
D	1.0	60.0-67.0
F	0.0	below 60.0

You’ll Get Your Hands Dirty

- Build a man a fire, and he'll be warm for a day.
  Set a man on fire, and he'll be warm for the rest of his life.”
  - Terry Pratchett, Jingo

- This is a VERY hands-on course
- After lab 1, you will work in teams of two
- Complete the skills survey
  - https://www.afit.edu/en/Surveys/ACE_CSCE_Survey/
- Select your partner
  - 1700, 3 Jan: Send me an email with
    - Partner request
    - Top three desk assignment preferences in 204
      - Seating chart is in course folder
  - 4 Jan: Dr. Lacey and I will assign partners and seats

Cyber Defense Network (CDN)

- You will need an account on the CDN

- CCR Workflow will ask (via email) for you to complete the appropriate forms

- You MAY use USB thumb drives on the CDN network
  - Do NOT use it on any EDU computer

Course Odds and Ends…

- Prerequisites: CSCE 560

- Office hours: appointment or walk-in

- In-class style: interaction, questions (please!)

- Course materials are located at:
  - CDN file share → \\fs-cdn-01\Public\CSCE 629
  - CDN file share → \\10.1.2.7\Public\CSCE 629
  - No material is on the EDU L: drive
  - Protect the information on the slides
  - Do not disseminate material to anyone!!
  - Team folders will be locked down to partners only

Resources

- ❒ Verify Windows Defender virus protection is turned off on your computer or it deletes some of our tools (e.g., fgdump)
  - ❖ Click on Defender icon in tray → shouldn't see a check mark
- ❒ Also turn off all firewalls

- ❒ Download Public\CSCE 629\Resources
  - ❖ Install 7-Zip on your computer
  - ❖ Unzip Files.7z using 7-Zip
  - ❖ Includes
    - Kali 2017.4 32-bit VM
    - Windows 7 VM with some tools installed
    - Windows XP VM with some tools installed
    - Videos, applications, documents, VMWare Workstation
- ❒ You may install VMware Workstation on your personal computers

Schedule

- Class – 1400-1600 TR
- Lab – 1600-1700 TR

- Very good chance we'll miss at least one day due to snow

- Cannot afford to forfeit class time
  - May use lab time as lecture

Random sign
I'm thinking the fine is
the least of your worries

Academic Honesty

- Plagiarism and cheating will not be tolerated
  - "[A] piece of writing that has been copied from someone else and is presented as being your own work" is an example of plagiarism [WordNet ® 1.6, © 1997 Princeton University]. Similarly "...taking someone's words or ideas as if they were your own" is also plagiarism [WordNet ® 1.6, © 1997 Princeton University].
- The AFIT Honor Code will be strictly enforced
  - IAW ENOI 36-107, "Willful violations of academic misconduct will likely result in disciplinary action including but not limited to:
    - failure of the assignment;
    - failure of the course;
    - administrative disciplinary action;
    - dismissal from the graduate school;
    - disenrollment from AFIT; or
    - prosecution under the UCMJ, as appropriate."

Collaboration and Information Sharing

Assignment	Work with	Consult
Lab 1-6	Partner	Any current 629 student
Project	Partner	Any current 629 student
Exam	Self	None
Final Project	Partner	None

Current students may be consulted for approaches to solving problems but all work must be your own.

Select problems restrict collaboration to just your team.

Be Careful Out There!

- ❒ Do **NOT** try what you are about to see at home… EVER!
- ❒ We discuss vulnerabilities and attacks
  - ❖ Although most vulnerabilities have been fixed, some attacks may still cause harm
- ❒ Appropriate Use Policies for CSCE 629 Course Materials
  - ❖ Sign the form or drop the course
- ❒ List of legal sites to practice
  - ❖ https://www.checkmarx.com/2016/12/04/15-vulnerable-sites-legally-practice-hacking-skills-2016-update/

⚠ WARNING

AFIT and/or Dr. Mullins are not responsible for your actions outside CDN lab.

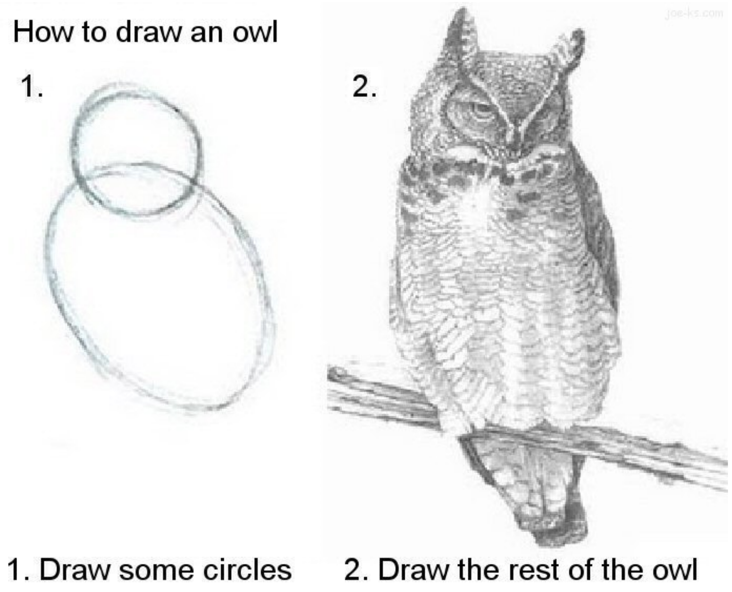
Warnings

- Hacking is as much art as science…
- Three rules to always remember
  1. Patience and persistence are a must!!!
  2. Patience and persistence are a must!!!
  3. See rules 1 and 2
- "The final project was the best. Time consuming, challenging, frustrating, but truly a rewarding experience that will be remembered. I enjoyed every head banging minute of it!"
  -- Quote from 2014 student on course survey

Warnings

You'll be graded on your
documentation of the process
as well as the results themselves

You cannot just provide the answer



You will take A LOT of screenshots

Warnings

- Tools are not "production quality"
- May not work 100% of the time
- Not all targets are configured exactly the same
  - An exploit may work on your partner's machine but not your machine

- What do you do?

Remember patience?

Warnings

You may not record the lectures

Non-Attribution – What you say in class will not be attributed to you if and when your thoughts or ideas are repeated outside of class

AFIT Faculty Handbook 2014

AU Instruction 36-2305

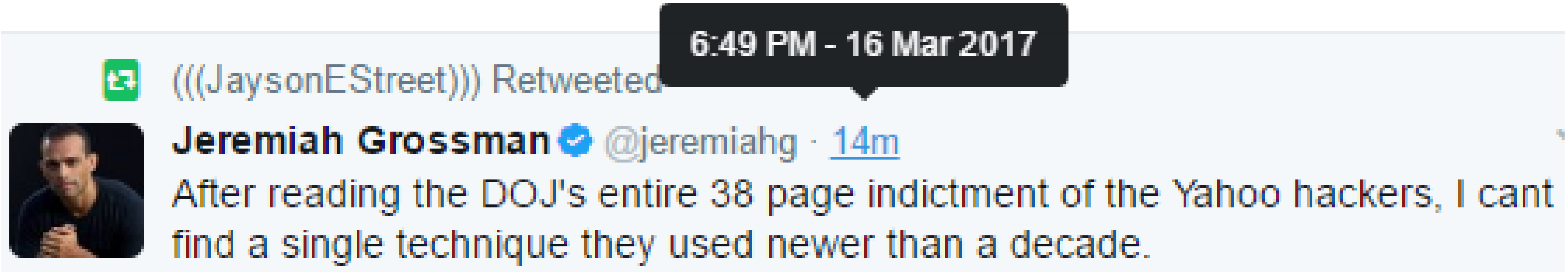
Not everything in the hacking world is politically correct

R RESTRICTED

UNDER 17 REQUIRES ACCOMPANYING PARENT OR ADULT GUARDIAN

What is this Course About?

- Introductory course in cyber attack



6:49 PM - 16 Mar 2017

(((JaysonEStreet))) Retweeted

Jeremiah Grossman @jeremiahg · 14m

After reading the DOJ's entire 38 page indictment of the Yahoo hackers, I cant find a single technique they used newer than a decade.

- Learn principles and practice of cyber attack → It isn't magic …

What is this Course About?

- This is NOT a course on how to simply use various tools
  - We will understand the underlying principles that make various attacks possible

- Goals:
  - Learn a lot (you tend to learn as you break stuff)
  - Have fun (I KNOW I have a BLAST every year!)

Course Objectives

1. Understand the basic concepts, terminology and resources used in information security.
2. Understand cyber attack methodologies based on stated policies, requirements and threats.
3. Apply structured exploitation and attack methods to design a viable attack strategy.
4. Demonstrate the ability to identify target computer systems.
5. Demonstrate the ability to perform basic enumeration and scanning of computer systems.
6. Demonstrate the ability to gain unauthorized access to a computer system.
7. Demonstrate the ability to attack confidentiality (cracking, sniffing), authenticity (spoofing), availability (denial-of-service) and integrity (buffer-overflows/Trojan-horse).
8. Demonstrate the ability to gather information from a target computer system.
9. Demonstrate the ability to hide attack occurrence and assess attack success.

Acknowledgements and Way Forward

- Slides are adapted from SANS Institute and Prentice Hall

- You will learn A LOT
- In fact, by the end of the course, you'll be like …

End of course overview

/* */ || ??