

# CMSC389R

Vulnerability Scanning, OPSEC and SE



**COMPUTER SCIENCE**  
UNIVERSITY OF MARYLAND



# Announcements

Homework II due tonight 11:59 PM

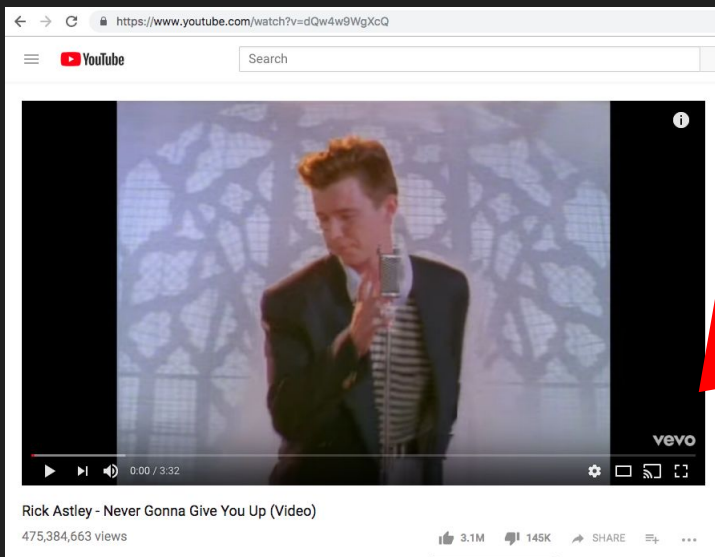
Office hours after class until 4 PM

--

Questions?

## HW2 bloopers

```
why cant i use grep  
let me use grep
```



```
less -n  
less flag  
you guys made this part way too hard  
fr tho like there's no instruction on what to do  
'use osint techniques' oh perfect ez
```

???

```
wget https://www.youtube.com/watch?v=dQw4w9WgXcQ
```

## OSINT - Review

- nmap - Port scanner
- whois - Query for registration info for a domain/IP/etc.
- Poor password reuse is more common than you think.
  - Security practitioners collect wordlists to use in engagements.

## vulnerability scanning

“I’ve identified **systems** belonging to the target (through OSINT or otherwise). Now what?”

Assess those systems for vulnerabilities.

# vulnerability scanning

- Objective: use with OSINT to rank vulnerabilities
- Tools are efficient, but can be noisy
  - Their security or IT team may notice suspicious activity
- Scan results need manual verification
  - Can often lead to false positives

# SecLists

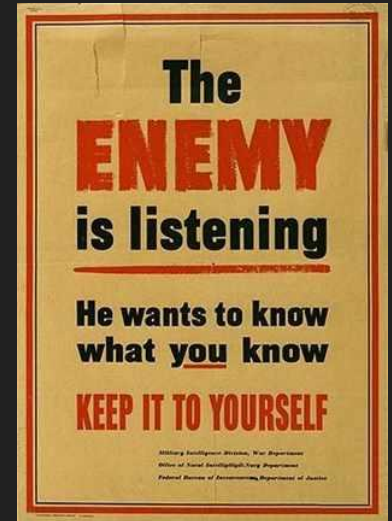
- Categorized repository of security lists containing
  - usernames/passwords
  - URLs
  - Fuzzing
  - ...

<https://github.com/danielmiessler/SecLists>

\*Kali wordlists: /usr/share/wordlists

# OPSEC

- OPSEC: **O**perational **S**ecurity
  - Security practices
  - Covers many fields of security, but we will mostly focus on digital





# OPSEC

- **Controlled** disclosure and use of information
- How much does an organization invest in OPSEC?
  - How do they invest effectively?
- Techniques (ie. PGP, Tor, VPN, throwaway email, burner phones, etc.)
- Don't allow yourself or the organization to be blackmailed

## OPSEC

- Concealing information from public view
  - ie) Coca-cola company secret formula
- Separate work and personal devices
  - BYOD may be prohibited

Competitors/Enemies/etc will do what they can to  
bring you and/or your organization down

Don't let them.

# Social Engineering (SE)

- Social Engineering
  - Deceiving the target into providing you with information or taking an action
  - Humans are *always* security's weakest link
  - Successful SE requires *a lot* of recon (OSINT)
  - Two most important concepts:
    - *Pretext* and *Elicitation*

## SE - Pretexts

- Art of creating an invented scenario to persuade a target to release information/perform an action
- More than just a lie
  - often creating a new identity and impersonating someone, or pretending to have a role you don't
  - Who are you pretending to be? Why are you calling/talking to your target? Why do you need the information you're asking for?

## SE - Pretexts

- OSINT and Target Recon is *extremely* important!
- More research = better chance of success
- Don't claim to know things you know nothing about
- Simpler pretexts are better
  - Pretext should appear spontaneous and legitimate
  - Follow through to a logical conclusion to evade any suspicion
  - Be confident!
  - Use background noise (if over phone) to improve how real it sounds

## SE - Elicitation

- **Elicitation:** “to bring to draw out; a stimulation that calls up a particular class of behaviors; subtle extraction of information during an apparently normal and innocent conversation”
- Effective social engineers elicit from targets without them knowing they’re giving away information

## SE - Elicitation

- The goal of SE is to elicit information that the target thinks is innocuous, or harmless
- A lot of information learned through SE often seems innocuous for reasons other than building trust
  - Getting innocuous details can help sell that you're someone else to a target

Example: <https://www.youtube.com/watch?v=1c7scxvKQ0o>

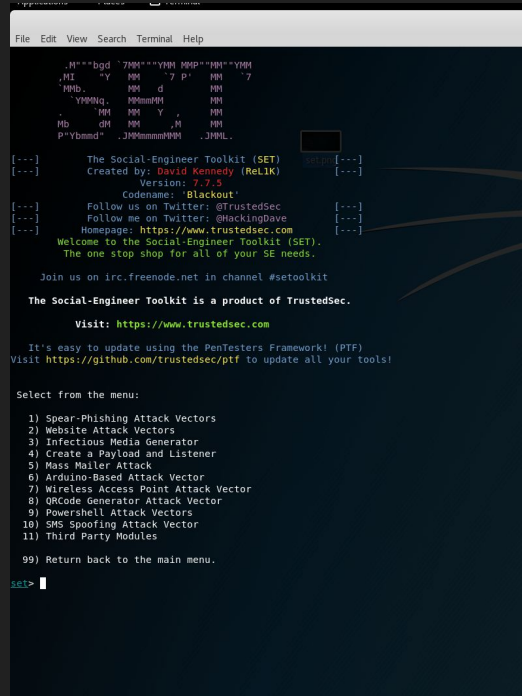
## SE - Ethics

- Fact: It is extremely easy to elicit personal information from most people
  - Everyone's ignorance and trust is arguably their biggest weakness
  - Anything done with SE should be *strictly* within the bounds of your engagement
    - Say you were asked to run a phishing campaign against employees to test a company's OPSEC awareness
  - Pretexting using fraud, deception, or misleading questions is illegal according to the FCC
  - Specifically illegal to use pretexting to retrieve customer info from financial documents or telephone (HP, 2006)



# Example: Social Engineer Toolkit (SET)

- <https://github.com/trustedsec/social-engineer-toolkit>

A screenshot of a terminal window displaying the Social-Engineer Toolkit (SET) interface. The terminal has a dark background with light green text. At the top, there's a header with ASCII art and version information. Below that, a menu of options is listed, including Spear-Phishing Attack Vectors, Website Attack Vectors, Infectious Media Generator, and others. The prompt 'set>' is visible at the bottom left.

```
File Edit View Search Terminal Help

.N''''bgd `7MM''''YMM MMp''MM''YMM
.MI  "Y MM  "7 P' MM  "7
MMb.  MM  G  MM
YMMNg. MMmmMM MM
.  "MM MM Y .  MM
Mb  GM MM  ,M  MM
P"Ybmd" .JMMmmmmMM .JMM.

[---] The Social-Engineer Toolkit (SET) set>[---]
[---] Created by: David Kennedy (ReLIX) [---]
[---] Version: 7.7.5 [---]
[---] Codename: 'Blackout' [---]
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]
[---] Welcome to the Social-Engineer Toolkit (SET).
[---] The one stop shop for all of your SE needs.

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) SMS Spoofing Attack Vector
11) Third Party Modules

99) Return back to the main menu.

set>
```

## Example: SECTF @ DefCon

- <https://youtu.be/yhE372sqURU?t=3m8s>



## homework #3

will be posted tonight.

Let us know if you have any questions!

It is due by 9/20 at 11:59 PM.