

CMSC389R

Vulnerability Scanning, OPSEC and SE



COMPUTER SCIENCE
UNIVERSITY OF MARYLAND



Recap

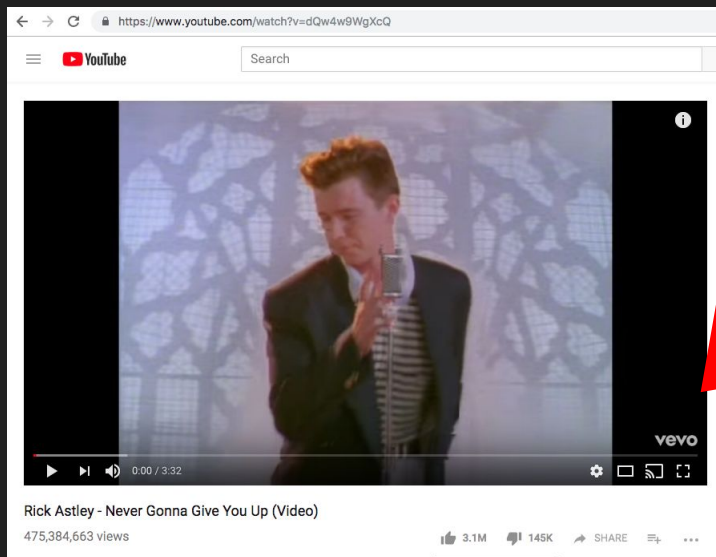
Homework II

--

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
```

2,301 variations of f\$%# were
issued on our server

???

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

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

Demo: SecLists

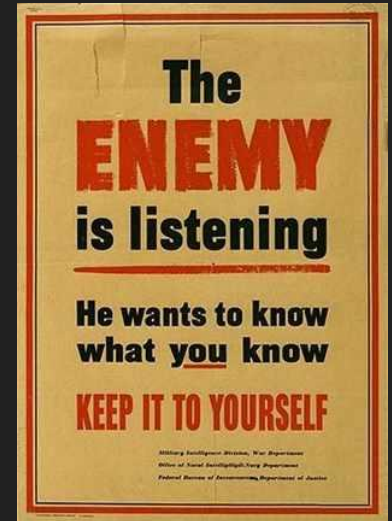
- Categorized repository of security lists containing
 - usernames/passwords
 - URLs
 - Fuzzing
 - ...

<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

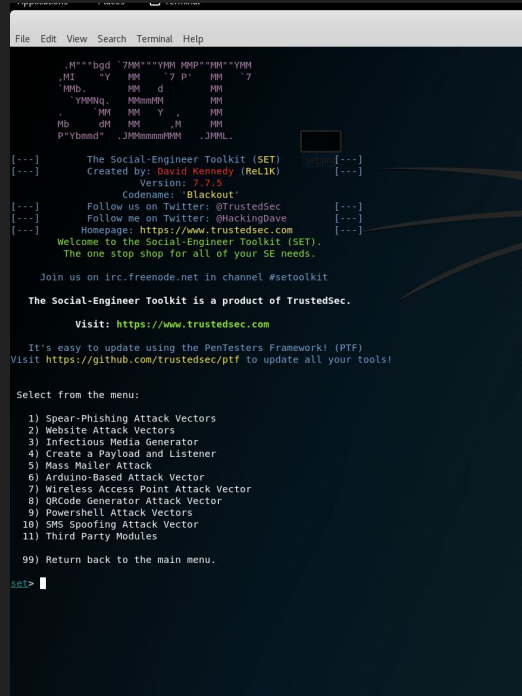
Don't let them.

Social Engineering

- **Social Engineering:** deceive the target into providing you with information or taking an action
 - Email/Phone/URL/Wifi...
 - Useful for OSINT as well as going for low-hanging fruit
 - Effective, inexpensive, little left-over evidence

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 menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. Below this, a ASCII art logo for 'The Social-Engineer Toolkit (SET)' is shown. The main text in the terminal reads: 'The Social-Engineer Toolkit (SET) Created by: David Kennedy (ReL1K) Version: 7.7.5 Codename: 'Blackout''. It then lists social media links: 'Follow us on Twitter: @TrustedSec', 'Follow me on Twitter: @hackingdave', and 'Homepage: https://www.trustedsec.com'. A welcome message follows: 'Welcome to the Social-Engineer Toolkit (SET). The one stop shop for all of your SE needs.' Below this, it says 'Join us on irc.freenode.net in channel #setoolkit' and 'The Social-Engineer Toolkit is a product of TrustedSec.' with a visit link 'Visit: https://www.trustedsec.com'. It then mentions 'It's easy to update using the PenTesters Framework! (PTF)' and provides a GitHub link 'Visit https://github.com/trustedsec/ptf to update all your tools!'. Finally, it presents a menu titled 'Select from the menu:' with 11 numbered options: 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, and 99) Return back to the main menu. The prompt 'set>' is visible at the bottom left.

Example: SECTF @ DefCon

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



homework #3

will be posted soon.

Let us know if you have any questions!

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