CMSC389R

Vulnerability Scanning, OPSEC and SE

COMPUTER SCIENCE
UNIVERSITY OF MARYLAND

Recap

Homework II

--

Questions?

HW2 bloopers (last semester)

why cant i use grep
let me use grep

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

YouTube

Search

Rick Astley - Never Gonna Give You Up (Video)
475,384,663 views

3.1M   145K   SHARE

vevo

0:00 / 3:32

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
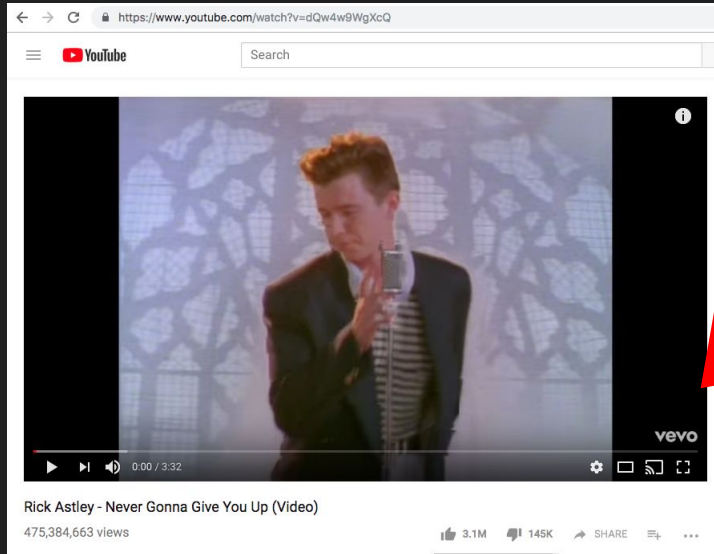
vulnerability scanning

"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
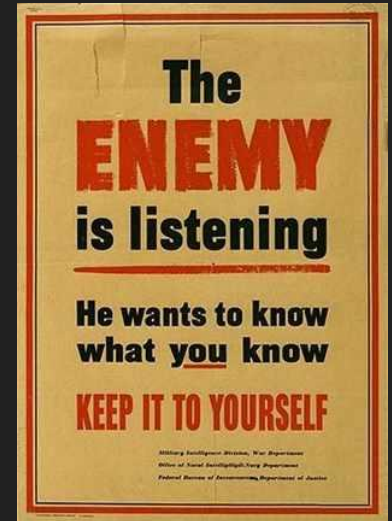 - Can often lead to false positives

SecLists

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

  https://github.com/danielmiessler/SecLists

*Kali wordlists: /usr/share/wordlists

OPSEC

- OPSEC: Operational Security
  - Security practices
  - Covers many fields of security, but we will mostly focus on digital

The **ENEMY** is listening

He wants to know what you know

KEEP IT TO YOURSELF

Military Intelligence Division, War Department
Office of Naval Intelligence, Navy Department
Federal Bureau of Investigation, Department of Justice

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=lc7scxvKQOo
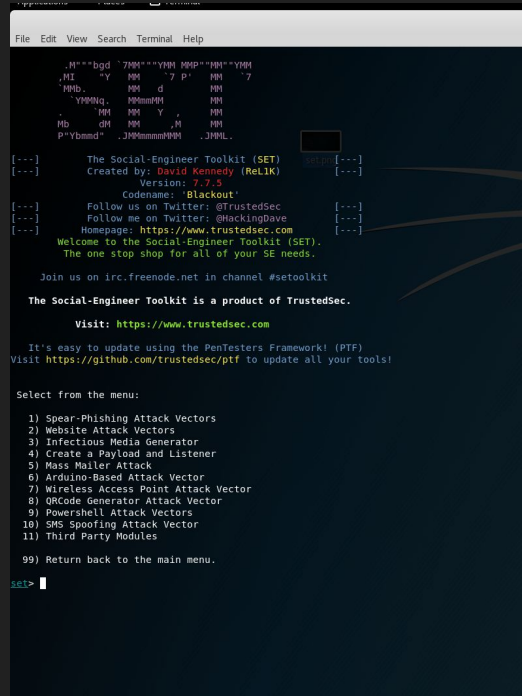
SE - Ethics

- **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

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.