CMSC389R

Final Lecture!

COMPUTER SCIENCE
UNIVERSITY OF MARYLAND

roadmap

- We did a lot this semester
- We hope you had as much fun taking this class as we did teaching the course :)
- That being said, keep us in the loop where you go after this!

course review

- Ethics
- OSINT
- Pentesting
- Forensics
- Cryptography
- Web
- Binaries

ethics debriefing

- We did a lot of hacking, and *some* ethics.
- Important takeaways:
  - Obey the law, but remember that legality and ethicality are distinct!
  - Think about your actions:
    - Their consequences, the precedent they set, how they affect others...

social engineering

- “Confidence Trick”
  - Trigger and exploit simple human emotions
    - Greed
    - Lust
    - Empathy
    - Curiosity
    - Vanity

social engineering

- In general, (nice) people *want* to help
- People respect authority and want to avoid conflict
- Social bandwagon
  - “Everyone else is doing it, so should you”


OTV

phishing

- Common attack vectors:
  - Email/Phone/Fake websites/Posters/etc
- Spear phishing: direct phishing attack on a particular target of interest
  - 91% of attacks on the Internet
- Clone phishing: previously legit email cloned and replaced with malicious content and resent to victim
- Whaling: phishing that targets execs/higher-ups

root@kali: ~

File Edit View Search Terminal Help

```
root@kali:~# airbase-ng -e HOME-5432 -c 11 wlan0mon
21:32:21  Created tap interface at0
21:32:21  Trying to set MTU on at0 to 1500
21:32:21  Trying to set MTU on wlan0mon to 1800
21:32:21  Access Point with BSSID 9C:EF:D5:FD:33:FF started.
```

how to

- Footprint
  - OSINT
- Trust
  - Develop relationship with victim
- Manipulate
  - “Exploit” trust in victim to extract as much info as possible
- Exit
  - Smooth exit, don’t draw attention/suspicion

attack surfaces

- Dropped USB → “The Good Samaritan”
- Evil twin wifi
- Social media
- Website spoofing
- Any others?

real-life prevention

- Awareness: suspect everything
  - Why is he/she asking me this? Credentials?
- Don’t be socially pressured
  - Take as much time as needed and add delay
- Don’t provide too many details/personal info
- Shred personal documents
- Any others?

technical prevention

- Secure internet connection (HTTPS, VPN, etc)
- Check email headers
  - An email from support@apple.com may not necessarily be from apple
- Disable automatic image loading in email clients
- Any others?

pivoting

- Remember pivoting?
  - Attacker breaches a single machine/service, and uses further exploits/implicit trust to spread across the network
    - Avenues: Exploit chaining, social engineering, backdoors, …
    - Observation: Internal services aren’t always as well secured!

pivoting techniques: exploit chaining

- Shellshock on a customer-facing server yields RCE…
- Which is used to perform SQLi on an employee DB…
- Which is used to inject JS on the payroll site…
- Which is used to exfiltrate bank numbers!

persistence

- Pivoting can take time, and time = discovery risk.
- Attacker’s solution: *persist* their presence by leveraging multiple ingress techniques:
  - Original vulnerability (e.g., RFI)
  - Backdoors (reverse shell, new user)
  - Rootkits, startup/event hooks

persistence techniques: backdooring

- General strategy: create as many surreptitious access channels as possible
  - Reverse shells running as the exploited user
    - Can be as simple as `nc` + `bash`!
  - Additional phony accounts with login/access permissions
  - Replacing binaries (e.g., `ssh`) with versions that steal credentials

persistence techniques: event hooks

- General strategy: make it as hard as possible to scrub the persistence code from the system/network:
  - Add scripts to `cron`, or modify extant scripts
  - Inject commands into startup scripts:
    - .bashrc, .profile, .bash_profile, .xinitrc
  - Observation: attackers will attempt to persist on systems/machines where wiping/resets aren’t an option!

final hack

- Grade server is up - challenges are locked until finals

http://68.183.48.170:4000/

- You have until the last day of finals to finish it (4/18 at 11:59 PM)
- It should take you no more than ~ 1-2 hours
  - If you find yourself taking longer, message us on piazza

final hack

- Three main components:
  1. Hack the Instructor
     a. Reverse engineering
  2. Investigate the Instructor
     a. Forensics
  3. Hack the **(OUR)** Grade Server
     a. Web
     b. DO NOT HACK OR TRY TO HACK THE ACTUAL CS GRADE SERVER

final hack

- Each challenge has exactly 1 flag.
- There are 3 easter egg flags that are separate challenges themselves.
  - They are worth 5 extra points each.
  - Hints for these challenges are available, though they cost 2 points per easter egg.
  - Flags can be found by only hacking **OUR** Grade Server.

parting thoughts

- Tell your friends/family/colleagues/the world about this class!
  - Be sure to include what tools you learned in your resume
- Hack for good, don’t be evil
- Visit ctftime.org to learn more about upcoming CTFs
- Attend UMDCSEC meetings and follow @umdcsec on Twitter