Mason Competitive Cyber

Doing the Most with the Least:
CTF Categories with Low Overhead

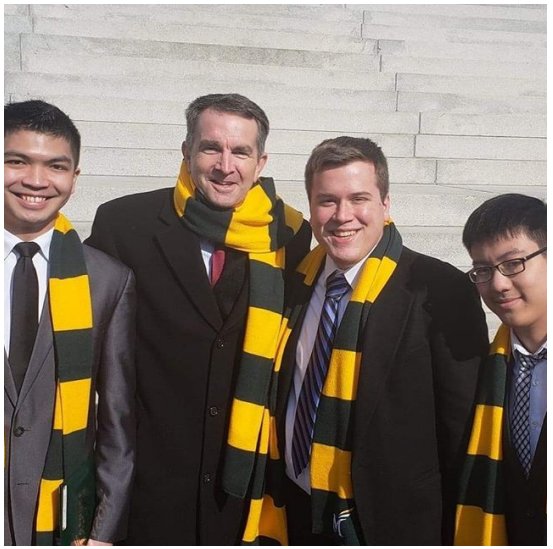
go.gmu.edu/cctraining

Upcoming Competitions & Events

- CCDC
  - Team selected, fee paid, remote site judge selected
  - Feb 11
- VA State Cyber Cup
  - Team selected, seeking observers
  - Feb 22-23
- UMBC CTF
  - March
- **Next week is RSVP**
  - Britton from The Crypsis Group

Club News

- CYSE money movement
  - Officially inquired for transfer
- Cabrera, Jones chatter
- Open third guest spot
- Shitload of Shmoocon attendees
- Reminder: Talk here if you want



Summary

- Breakdown of categories:
  - Linux
  - Cryptography
  - Reversing/Pwn
  - Forensics
  - Web Exploitation
- Breakdown of how to do them with little to no overhead

there is a stain on my shirt let's move on with our lives knowing that

Linux

- What it covers:
  - Common kernel/OS (shh), generally refers to the ability to efficiently navigate the command line
- Why it matters:
  - Linux covers a lot of highly performant systems
  - Fast, high barrier though
- Where you'll need it:
  - Pretty much everywhere - CYSE101, CYSE211, IT342, IT462, IT369, CS110, CS367 (Zeus), CS262 amongst most professional work
- Competitions context:
  - Largely used in "CND" competitions, attack/defense

Linux - Hands-On

- Bandit - Over the Wire
- By far the most upvoted crap

Windows Users: PuTTy
Linux Users: Terminal

http://overthewire.org/wargames/bandit/

Cryptography

- What it covers:
  - Encryption of data, mostly either at rest or in transit
  - Hashing
  - probably other shit
- Why it matters:
  - Keeps data safe?
  - Highly advanced category
- Where you'll need it:
  - A lot of government work
  - A lot of research work
- Competitions context:
  - Dedicated CTF category at most events

Crypto - Hands-On

- Credit Zaine
- Covers mostly mid/low level stuff, not pretty
- Better to learn than Rumkin IMO

http://practicalcryptography.com/

Reverse/Pwning

- What it covers:
  - Reverse Engineering to determine behavior, pwning to develop an exploit
  - Requires a lot of foundation
- Why it matters:
  - Finding vulnerabilities before the bad guys
  - Profit
- Where you'll need it:
  - Malware analysis work
  - Vulnerability research work
- Competitions context:
  - Dedicated CTF category at most events
  - **Probably the most points on the board in most cases**

RE/Pwning Examples

https://wargames.ret2.systems/ - Don’t need an account, limited in nature, we’re on shortlist

https://microcorruption.com/ - Much more expansive, similar concept, minor differences (different instruction set, for instance)

Forensics

- What it covers:
  - Determining details about a certain incident, identifying what happened, why, etc provided artifacts like a disk or pcap or something
- Why it matters:
  - “Who’s W2 was exposed?”, “How do we prevent it in the future?”, (never works, but) “Who did it?”
- Where you’ll need it:
  - ….forensics work
  - “Digital Forensics and Incident Response” - DFIR
- Competitions context:
  - Dedicated CTF category at most events
  - Becoming a trend

Forensics Examples

I have failed you. Forensics is hard to do with low overhead.

Best bet: CloudShark, malicious pcaps

Which malicious pcaps you want depends on what you want

Web App Sec

- What it covers:
  - Security of websites
  - My baby
- Why it matters:
  - Pillaging databases, defacing sites, skimming CC data, etc
- Where you'll need it:
  - Pentesting
  - Any AppSec role
- Competitions context:
  - Dedicated CTF category at most events
  - High value in certain events (e.x. VA Cyber Cup)

Web App Sec Examples

Limit what you do over the network

Consider not running any sort of scanners or automated tools

hack.me - Sandboxes (common one: DVWA)

Questions/Cease to hands on

hack.me - Sandboxes (common one: DVWA)
https://wargames.ret2.systems/ - Don't need an account, limited in nature, we're on shortlist

http://overthewire.org/wargames/bandit/

https://microcorruption.com/ - Much more expansive, similar concept, minor differences (different instruction set, for instance)
http://practicalcryptography.com/

go.gmu.edu/cctraining

Proud Sponsors

Thank you to these organizations who give us their support:

BATTELLE

It can be done™

CRYPSIS™