Mason Competitive Cyber

CCDC Prep - Windows System Hardening

Interview Questions

- If you have to compress and encrypt a file, which order would you do it in? Why?
  - A) Compress and then encrypt
  - B) Encrypt and then compress

Interview Questions

- If you have to compress and encrypt a file, which order would you do it in? Why?
  A) Compress and then encrypt
  B) Encrypt and then compress

Answer: A

1) compressing first = smaller file to encrypt = faster encryption
2) compression algorithms rely on repetition. Encryption decreases the repetition in files
   Lossless vs. Lossy

Interview Questions

- Difference between Encrypting, Encoding, Hashing, and Obfuscation

Interview Questions

- Difference between Encrypting, Encoding, Hashing, and Obfuscation

Encrypting - changing data so it is only available to be read by the intended parties and can't be tampered with

Encoding - changing data from one form to another.

Encoding standards

Hashing - one way function that transforms data into a value

Integrity Verification

Obfuscation - making something unclear

Making code hard to read

What is MasonCC?

- Cybersecurity club focused on competition
- Sponsored by Battelle and The Crypsis Group
- competitivecyber.club
  - sign up for our Slack

- Capture the Flag competitions (CTFs)
  - Online or In-Person
  - Jeopardy style: Technical Challenges
    - Cryptography
    - Web Exploitation
    - Reverse Engineering
    - Forensics
- Computer Network Defense competitions
  - Secure VMs

Requirements to join MasonCC

- You are a current or past GMU student
- ANY MAJOR

- Don’t have a skill base in cyber security?
  - We have links to help you build one
    go.gmu.edu/ccbeginners
  - Some of our talks are more basic than others

- Never competed in a CTF before?
  - TCTF.competitivecyber.club

Upcoming Competitions & Events

- CCDC
  - Feb 11
  - Online at GMU
  - CND
- VA Cyber Fusion
  - Feb 22-23
  - In person at VMI? Need 2 “observers”
  - Jeopardy CTF
- NeverlanCTF
  - Beginner focused
  - Jan 31 - Feb 3
  - Online
  - Jeopardy CTF

Upcoming Competitions & Events

MASON COMPETITIVE CYBER

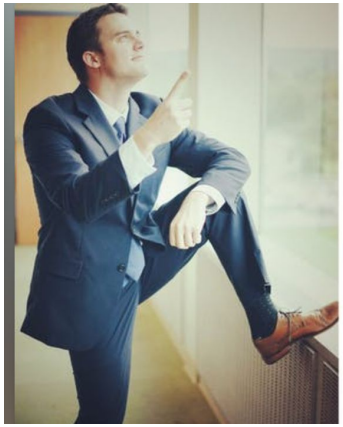
GMU'S CYBERSECURITY ORGANIZATION

Home Videos Calendar

Meeting Info

February 6

On Wednesday, February 6 Gold Track will be going over **Britton Manahan from The Crypsis Group - Power of the Shell** in **JC Meeting Room A**, whereas Green Track will be going over **Britton Manahan from The Crypsis Group - Power of the Shell** at **JC Meeting Room F** from 7:00pm til 8:00pm. **In addition, there is a mandatory signup enforced for this meeting: here**



Britton Manahan

The Power of the Shell

Johnson Center Room A
February 6th, 7:00pm
George Mason University
RSVPs Recommended

An event run in cooperation with
The Crypsis Group and
Mason Competitive Cyber

Future Competitions

Name: **CCDC Virtual Q**
Starts: **February 16**
Ends: **February 16**
Location: **George Mason**
More info
NOTE: This competition is
Please note you are not promi
if you'd like to participate, you should

CCDC & Windows System Hardening

- Collegiate Cyber Defense Competition
- Computer Network Defense
  - Protect VMs from Red Team

- Windows System Hardening
  - Reducing attack surface (harder to hack)

Users

- Change all passwords
- Rename default accounts
- Backdoors not always complicated fileless malware
- Create own user to log back in
- Periodically run net user
- Check permissions and which groups a user belongs to
  - Should the default “Administrator” account have a weak password and be part of RDP users?

Firewall

- Check inbound and outbound rules
- Lock down what's unneeded
- Don't be too restrictive
  - stop critical services
  - lock yourself out (if RDP'd in)

Services and Processes

- Process Explorer
- Services snap-in
  - run, mmc

- Should X be running? Does it need to be?

Group Policy

- Audit Policy
  - audit everything
- Security Options
  - Anything that looks important
  - Restrict CD-ROM access to locally logged on user only
  - Do not allow anonymous enumeration of SAM accounts
  - UAC: only elevate executables that are signed and validated

Finding Backdoors

- netstat -anb
- Startup
  - Use Autoruns
  - Run key
  - Startup folder
- Sticky Keys

File Tricks

- In Explorer, view hidden files and don’t hide extensions
- Know how to manipulate permissions and ownership of files/folders

Updates

- Automatic Updates
- Most recent version by the end of competition
  - Strategy
  - Win XP SP0 = bad time

Common Mistakes

- Enabling firewall blocking everything
  - Or otherwise locking yourself out
- Not rechecking common backdoors
- Not periodically checking critical services
- Not writing your super secure password down

Technical Challenge

- Scored Win7 Image
  - Hacker:letmein
- CCDC style
- System harden it for points
- Score report

    C:/CyberPatriot Score Report/Score Report.html

go.gmu.edu/ccdc

Proud Sponsors

Thank you to these organizations who give us their support:

BATTELLE

It can be done™

CRYPSIS™