CMSC388U

Review + Story Time

(Bonus content from poll)

COMPUTER SCIENCE
UNIVERSITY OF MARYLAND

Announcements

- Homeworks #7 - #9 grades released
- Homework #10 due by midnight tonight!
- We changed assignment weights to reflect final breakdown
    - Reminder: Write ups 50%, Midterm + Final 25% each
- Final Exam Details
    - Will be open for 7 days (will ***NOT*** take the whole week to complete)
        - Starting tonight @ 11:59pm, closing 5/14 @ 3:30pm
    - Cheatsheet (similar to midterm) in the near future

CMSC388U

- We made it to week 15!
- This is the first time we've done something like this course
  - Hopefully a lot of things you liked, likely a few things you didn't
    - Please let us know!
      - UMD Course evals, piazza, etc. (We'll post a form too)
- The course (and instructors) have grown a lot over the last semester!
- Feel free to schedule office hours, ask questions over Piazza, etc!
- If you see us around sometime in the future, don't hesitate to say hi!

THANK YOU! <3

Final Exam Basics

- Using CTFd
  - Very popular open platform to make hosting CTFs easy!
- Account credentials will be made for you, and an invite sent
- Will be several multi-part questions
  - Each themed to a different “storyline”
- Will release full rubric

- Write-up will be required for each question
  - Can fit it to the storyline if you want! (e.g. pentest report, spy assignment, etc.)
  - Include the flags you found
    - Directly included, not referred to or theoretical
  - Talk about the overall steps you took
    - Used x tool or x concept in y way because…
    - Make sure to cover the main milestones/checkpoints
  - Explain key concepts
    - *Style* of “I saw x, which made me think of y, so I did z”
  - Write-ups are meant to share knowledge with other people

Welcome to the CMSC388U Final Exam!

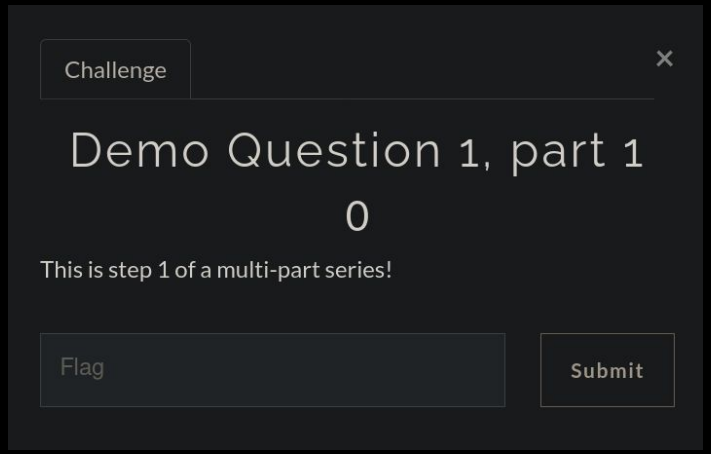
Scoreboard Challenges

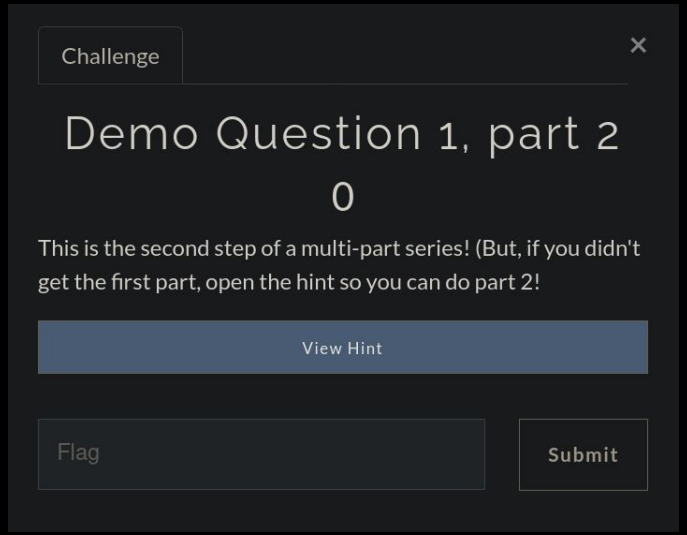
Challenges

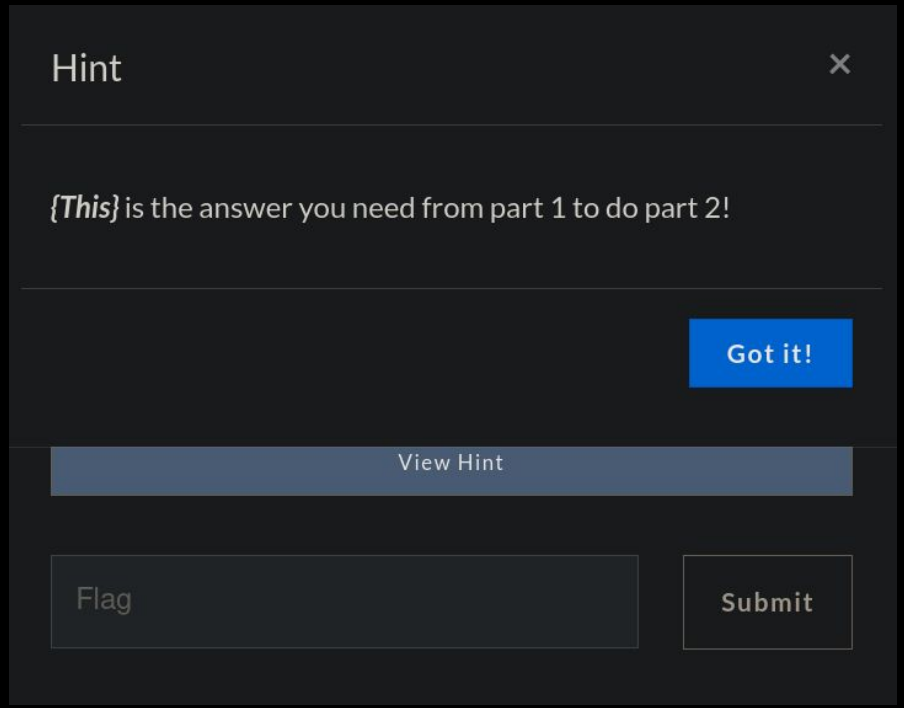
CMSC388U Final Exam has not started yet

Testing

Demo Question 1, part 1	Demo Question 1, part 2
0	0


Challenge
Demo Question 1, part 1
0
This is step 1 of a multi-part series!
Flag
Submit


Challenge
Demo Question 1, part 2
0
This is the second step of a multi-part series! (But, if you didn't get the first part, open the hint so you can do part 2!
View Hint
Flag
Submit


Hint
{This} is the answer you need from part 1 to do part 2!
Got it!
View Hint
Flag
Submit

Week 1: Intros + Ethics

- Initial overview of how the course works
- What is “ethical hacking”
- Basic legal knowledge
- Legality vs Ethics
- Disclosure

- HW: The wonderful ethics question

Week 2: OSINT

- “Open Source Intelligence”
  - Active vs. Passive reconnaissance
  - IP’s & DNS
  - view-source: (Web source)
  - Robots.txt
  - Git commits/source
  - Google “Dorking”
  - Pastebin/”*bin.*”
  - Shodan
  - Ports? Services?
  - Wayback machine

- HW: first look at supersecure.store :)
  - Getting info on the k1tt3ng4ng hackers who broke in

Week 3: OPSEC & Vuln. Scanning

- Vulnerability Scanning:
  - `nmap` (and basic usage)
  - Wordlists
  - Directory bruteforcing
- OPSEC
  - “Operational Security”
  - PGP/ToR/VPNs
  - Threat modeling
  - How to keep yourself reasonably secure
- Basic Social Engineering

- HW: Getting info about the supersecure.store server (nmap & dir bruting)
  - Secret cat pictures

Week 4: Pentesting

- “Penetration Testing”
  - Types of pentesting
  - CVEs
  - Common Exploits & Exploit categories
  - Payloads
  - Basic command injection
  - Privesc
  - Bash tricks

- HW: SETUID privesc, local command injection, finding CVE & exploit based on software version

Week 5: RE

- “Reverse Engineering”
  - Flavors of RE
  - Software RE basics
    - File, strings, hex editors
  - Static vs dynamic analysis
  - Disassembling & decompiling
  - Firmware RE
    - Binwalk

- HW: File info (PDF -> MP4), hidden strings, firmware RE exercise

Week 6: Forensics

- What is digital forensics?
  - Data recovery/extraction
  - Creating/extracting disk images
  - Data analysis guidelines
    - Copy & verify
      - Hashing
  - Analysis techniques & methods
    - Metadata (exiftool)
    - File undeletion
  - Stegonography

- HW: Hidden data in audio, steganography, file integrity, disk recovery

Week 7: Midterm!

- Seems like it went well :)
- 18 page cheatsheet was released :)

Week 8: Spring Break!

Week 9: Binary Exploitation

- Binary Exploitation/pwn basics
  - Brief assembly basics
  - Stack & heap refresher
  - Linking & binary structures
  - Endianess
  - Exploit types
    - Command injection
    - Format string
    - Buffer overflow
  - Basic anti-RE & binary protections

- HW: Binary protections, Code review & exploitation, format string exploitation

Week 10: Forensics II

- Focused on network forensics (PCAPs)
  - Basic network protocols
  - Wireshark UI/basics
    - Filtering syntax
    - UDP/TCP/HTTP Streams
    - Exporting objects
    - Statistics
- Monitor mode overview
- Workflow example

- HW: PCAP analysis! (objects, streams, filtering, statistics)

Week 11: Crypto(graphy)

- Encoding vs. Encrypting
- Encoding
  - Base64, rot13, substitution, vigenere, OTP
    - Frequency analysis
- Encrypting
  - Symmetric vs. asymmetric
  - RSA, AES, EC
  - PGP & GPG
  - OpenSSL
- Hashing
  - (cryptographic) hashing
  - Hash cracking

- HW: Decoding, hash cracking

Week 12: Rescheduled

- Vanya has his 2nd covid dose the day before, turned out to be a good idea to move the live lecture
- Web I and Web II content were combined for Web 2

Week 13: Web II

- Web basics
  - HTTP
    - Response codes
    - Request methods
    - Cookies
  - SSLStrip & HSTS
- Attacks
  - BURP
  - XSS, SQL, LFI
  - IDORs

- HW: Due tonight ;)

Week 14: Car hacking!

- Bonus content chosen by you!
- Cars are hackable?
  - Talked about how modern cars differ from their history
  - ECU overview
  - CAN Bus
    - CAN frames, ARB ID's
  - Car diagnostics
- Hacks
  - Interfacing with CAN
  - Infotainment hacking
    - Links between infotainment and CAN
  - Key fobs

- HW: None!

Week 15: Final review & storytime

- Here we are now :)

<3