**The Great Computer Challenge, 2018**

***Cyber Security, Level IV***

# **Background**

Cyber Security is the body of technologies, processes, and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In a computing context, security includes both cybersecurity and physical security.

Ensuring cyber security requires coordinated efforts throughout an information system. One of the most problematic elements of cyber security is the quickly and constantly evolving nature of security risks. The traditional approach has been to focus most resources on the most crucial system components and protect against the biggest known threats, which necessitated leaving some less important system components undefended and some less dangerous risks not protected against. Such an approach is insufficient in the current environment.

In order to understand how to provide cyber security, it is important to also understand how systems can be compromised. These skills are taught and practiced, but they must not be used in an unauthorized or malicious way. Information Security professionals recognize the responsibility to maintain ethical principles that protect the safety and welfare of society and promote the common good; to build public trust and confidence; to protect privacy and property; to act honorably, honestly, justly, responsibly and legally. It is expected that students participating in the GCC Cyber Security Challenge will maintain the same ethical standards. At no time should an attack technique be used via the public wifi or on any target not specified in the challenge. Doing so may constitute an illegal act that can be prosecuted and will disqualify your team from the GCC Cyber Security Challenge.

# **Guidelines & Requirements**

Contestants will solve a selection of cyber security problems using their choice of tools. Contestants will use their laptops on which Virtualbox and an instance of Kali Linux is installed before the competition. They can install any tools they might need before the event. Judges will evaluate the answers to problems without considering the tools used. Answers will be delivered digitally. At the end of the contest time, contestants must leave a completed judging form.

**No printer is needed.  Helpful tools and skills:**Kali Linux, bash scripting, Wireshark, Forensics, file analysis, cryptography, steganography, website analysis, and Googling.

1. Each team member may use one computer during the contest.
2. You may use the internet during the competition. To do so, you will need a computer with wireless capability. Information for connecting to the wireless will be distributed before the contest starts.
3. Internet connection can be used just for accessing information. Any cyber-attack via the Internet is not allowed.
4. Points and durations
	1. Part I (Written Questions): 10 Questions – 30 minutes – 100 Points
	2. Part II (CtF Challenge): 2.5 hours – 500 Points

# **Challenge Part 1**

**Part I**

*Duration: 30 minutes*

*10 Questions - 100**Points available*

*Answers of this challenge will be collected before the 2nd part of the challenge is started. Points from both parts will be added to give final team score.*

1. By viewing the TCP stream via a Wireshark packet capture, what web exploit attack was performed by the malicious actor?



* 1. Cross site scripting (XSS)
	2. Local File Inclusion
	3. SQL injection
	4. Denial of Service Attack

**ANSWER:**

1. What was the malicious actor’s payload to conduct the attack successfully?
	1. ' or 0=0 #
	2. ' or 1=1
	3. <body onload=alert('test1')>
	4. username: <%= password %>

**ANSWER:**

1. Rank the following password schemes from most secure to least secure:
	1. Password 1: 6 characters consisting of uppercase letters, lowercase letters, numbers, and special characters + = ( ) \* & ^ % $ # @ ! with replacement and no repetition allowed
	2. Password 2: 8 characters consisting of uppercase letters, lowercase letters and numbers with replacement and repetition allowed
	3. Password 3: 8 characters consisting of uppercase letters, lowercase letters, numbers, and
	4. Password 4: A 32-bit password

**ANSWER:**

1. For masking your geo-location and increased privacy from internet service providers (ISP) or other interested parties, which option is most applicable?
2. Spoofing
3. Proxy
4. VPN (Virtual Private Network)
5. HTTP (Hyper Text Transfer Protocol)

**ANSWER:**

1. Find out the vendor of an Ethernet which has MAC address 84:3A:4B:C8:A9:99
2. Cisco
3. HP
4. Microsoft
5. Intel

**ANSWER:**

1. Which of these hash algorithms is the oldest?
2. SHA-1
3. SHA-256
4. MD5
5. SHA-512

**ANSWER:**

1. Alice wants to sends a message to Bob, Bob then wants to be sure the message could only have been sent by Alice. This is an example of:
2. Encryption
3. Authentication
4. Confidentiality
5. Digital Signature

**ANSWER:**

1. Which of the following is established when the user is doing a Host isolation?
2. DMZ
3. IDS
4. HIDS
5. IPS

**ANSWER:**

1. Which security property of the target system () is violated when the following code is run on the attacker’s station?

**ping 44.222.83.97 –t -65500**

1. Confidentiality
2. Integrity
3. Availability
4. None of them

**ANSWER:**

1. Which one is the SHA-256 Hash of the GCC2018?
2. D8EAB68FED2B6186457D269C2C799CADF730227A416AD5628A8357EBEB476F5A
3. FE16E629AD72C817833B1D931086EC2EF20EFFA27AC9693F897A7CE2BCA975F6
4. 36283635D031831273E785FB4DE8EE01BAC488FBE544AC175BDD6EC8607E71EF
5. 75A797609C2CC5FCF3B5D7C96B353FE33CF7EAF49ECF29B089D7083EB125E346

**ANSWER:**

# **Challenge Part 2**

**Part II**

*Duration 2.5 hours – Most Points Wins*

The 2nd part of the challenge will be available to you and your team via your favorite web browser. Go to [www.odu.edu/oductf](http://www.odu.edu/oductf)

* This will prompt a login for your team.
* Register your team name and the members of your team.
* Choose an icon or upload one your team likes better.
* As soon as you log on you are ready to play! Good luck!

**Current team scores are available on the Scoreboard! The total score for your team will be added to Part 1 of the challenge to make up your team’s final score.**

TIPS!

* The gameboard allows you to choose any challenge that is available. If you are stuck on a challenge move on to the next one and come back to it later.
* Split up the challenges among your teammates. “Many hands-on-keyboards make light of CTFs”
* Google and YouTube are your greatest ally!
* Always brush your teeth before you go to bed.

# **Judging Criteria**

Judges will evaluate the answers to problems without considering the tools used. Answers will be delivered digitally. At the end of the contest time, contestants must leave a completed judging form.

# **SOL Correlation**

Apply knowledge and skills to generate innovative ideas, products, processes, and solutions.

* Use various creative software, programming environments, or digital tools to convey existing ideas in new and effective ways.
* Use technology to develop innovative and effective solutions for assignments.

Have fun and thanks for participating in the Great Computer Challenge, 2018!