**UMass Lowell 2021 GenCyber Summer Camp Competition**

1. **INSTRUCTIONS**

Please read all the instructions of this competition carefully.

* The competition will start at 10:30AM and end at 11:40AM on Jul. 23, 2021. Hard deadline!!!
* This is an open book competition and students can refer to anything including our slides and videos.
* The competition can be completed by one student or two students as a team. A team cannot have more than 2 students.
* After the competition is done, students will be ranked first based on the total score and then based on who submits earlier if students have the same score.
* The top 3 finishers (or teams) will be announced before noon 12:00PM on Jul. 23, 2021.
* Underlined blue text points to a web link.

1. **PROBLEMS (4 problems in total)**

**Problem 1: Password security (1 point)**

In the folder named **competition** in your home folder at the Kali server in Cyber Range, there is a password hash file named **passwdhash**.

**Question**: What is the original password corresponding to the password hash of the one account in **passwdhash**?

**Problem 2: Hash-based message authentication code (HMAC) (2 points)**

In the folder named **competition** in your home folder at the Kali server in Cyber Range, it is supposed that **msg-hmac.txt** stores the HMAC of **msg.txt** using the following command.

*openssl* [*dgst*](https://www.openssl.org/docs/man1.1.1/man1/openssl-dgst.html) *-sha256 -hmac "GenCyber21@UML" -out* ***msg-hmac.txt******msg.txt***

**Question**: Does **msg-hmac.txt** indeed store the HMAC of **msg.txt**?

**Problem 3: Secure email (3 points)**

Suppose a person called **Alice** wants to send an email message ***M*** to another person called **Bob**. Alice does not want anyone except Bob to see M. She knows that in general public key crypto is slow because of its heavy math computation. Therefore, Alice plans to use public key crypto and symmetric key crypto together to encrypt M for efficiency. She encrypts a symmetric key such as an AES key named ***K*** using Bob’s public key ***eB***, and then encrypts ***M*** with ***K***. Therefore, the final message Alice sends to Bob has two parts as follows: (i) encrypted AES key ***K*** by Bob’s public key ***eB*** and (ii) encrypted message ***M*** by ***K***

eB(K), K(M)

In the folder named **competition** in your home folder at the Kali server in Cyber Range, the file named **KM** stores K(M) and the file named **eBK** stores eB(K). The file **privkeyB.pem** contains Bob’s private key (and public key too)..

* **eBK** is created with the following command, where **eB.pem** is Bob’s public key.

*echo* ***K*** *| openssl* [*rsautl*](https://linux.die.net/man/1/rsautl) *-encrypt -inkey* ***eB.pem*** *-pubin -out* ***eBK***

* **KM** is created with the following command

*echo* ***M*** *| openssl* [*enc*](https://wiki.openssl.org/index.php/Enc) *-iter 1000 -aes-256-cbc -a -k* ***K*** *-out* ***KM***

**Question**: What is the message M?

**Problem 4: Remote hack of Windows 10 VM (4 points)**

Our vulnerable chat server *vulnserver.exe* runs on the following Windows VMs at port **9998**.

192.168.7.62

192.168.7.56

192.168.7.117

192.168.7.60

192.168.7.66

192.168.7.63

192.168.7.113

192.168.7.81

192.168.7.101

192.168.7.90

192.168.7.123

192.168.7.113

192.168.7.92

Find a way to hack into any of these Windows VMs. Note: the Windows VMs are configured and run as it is. Students cannot ask for help from TAs or instructors if they feel these systems do not work or cannot hack into these Windows VMs.

There is a secret in the file C:\Tools\secret.txt.

**Question**: What is the secret message in C:\Tools\secret.txt?