

Student Name:

ISA 656: Network Security

Final Examination

I, _____, hereby certify that I read the following:

University Policy Number 1301: Responsible Use of Computing

<http://www.gmu.edu/facstaff/policy/newpolicy/1301gen.html>

I understand that GMU takes its ethical obligations very seriously and violations will not be tolerated. I fully understand that GMU and its students must conduct the Program's activities in accordance with the highest possible ethical and legal standards. I know that I am responsible for ensuring that my personal conduct is above reproach. As a condition of studying in the ISA Program at GMU, I agree that violations of the standards described in the Code of Conduct shall be made known immediately to my appropriate faculty member(s) and that violations will result in dismissal from the Program and failure to receive the degree. I understand that this is a zero tolerance policy and that no second chances are given.

GENERAL INSTRUCTIONS

The final is worth 110 points (including 10 extra credit points): 50 points of theory and 60 points of Lab exercises. You have 40 minutes for the theory part; a short 10 minutes break and 60 minutes for the Lab part – plan accordingly. The questions are in no particular order of difficulty. Move on to easier ones if you find yourself stuck. You may answer questions in any order as long as they are clearly labeled.

THEORY/WRITTEN QUESTIONS (50 points)

1) [10 points]

How much more secure is the AES block cipher with 128-bit keys compared to AES with 100-bit keys?

2) [20 points]

a) Why do we implement several different forms of encryption when we protect Voice over IP (VoIP) systems and more specifically SIP?

b) Is encryption enough to protect VoIP systems? Justify your answer in detail.

3) [10 points]

How do we protect wireless communications against eavesdropping? Is WEP a good solution?

LABORATORY QUESTIONS (60 points)

1) [50 points] **Snort & Wireshark**

Download final.dmp from the course website:

<http://ise.gmu.edu/~astavrou/isa656final.dmp>

This file contains a tcpdump listing of all the traffic (some interesting, some not so interesting) to and from dsl.gmu.edu.

Your goal is to determine what attacks, if any, this machine made or sustained during the duration of the traffic recording.

After making sure that you have created an appropriate log directory, run Snort on an appropriately defined set of snort.conf files to detect the following:

1. All UDP traffic to dsl.gmu.edu.
2. All TCP traffic to port 443.
3. All traffic from dsl.gmu.edu.
4. A port-scan. What is the range of ports in the scan?
5. Use Wireshark to identify the signature of a worm that attacked dsl.gmu.edu on port 80 (WEB). Based the derived signature write a simple snort rule to detect that Worm.

Use Wireshark to:

- a) Create rules that match the Snort detected traffic for questions 1-5 and verify if Snort is working.
- b) Count the number of packets that match the Snort Rules

2) [10 points] **JAVA**

John Supercoder generated a very simple SSL server:

<http://ise.gmu.edu/~astavrou/isa656server.java>

<http://ise.gmu.edu/~astavrou/isa656client.java>

Unfortunately, his code has some errors both in terms of syntax and in terms of logic. Your task is to help John debug and test his code (prove that it is running).

(Hint: start with the syntax errors and then locate the logical ones).