Strathmore UNIVERSITY

Faculty of Information Technology
MSC in Information Systems Security
End of Semester Examination
MST 8506 Special Topics in Digital Forensics

DATE: 16 October, 2017 Time: 1 Hour

Instructions

- This examination consists of **FIVE** questions.
- Maximal points for the examination is **50**.

QUESTION ONE

Flow-based analysis techniques.

a. Define flow record and its typical properties. Specify when and how the flow records are created. [**5 Marks**]

b. Describe the difference between Netflow version 5 and Netflow version 9. Explain the templating mechanisms used in Netflow version 9. [**5 Marks**]

QUESTION TWO

Network Intrusion Detection and Analysis:

a. Outline the typical NIDS functionality. Briefly explain the issue of data normalization. [**4 Marks**]

b. Describe the detection engine. Discuss detection methods. [**2 Marks**]

c. Define the structure of SNORT rule. Explain the following SNORT rule:

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP PING"; icode:0; itype:8; classtype:misc-activity; sid:384; rev:5;) [**4 Marks**]

QUESTION THREE

Analysis of network devices:

a. List at least 5 volatile evidence and 3 persistent evidence that can be gathered from network devices (switch, router, firewall). [**2 Marks**]

b. Explain caching mechanism supported by HTTP/1.1. protocol (RFC 2616). Define expiration and validation models. What mechanism are used for validation? [**4 Marks**]

c. List different types of evidence you can get from web proxy server. For each evidence shortly discuss its value for investigation. [**4 marks**]

QUESTION FOUR

Consider wireless network forensics:

a. Briefly compare traffic capturing in wireless environment and in wired environment: [**2 marks**]

b. List and explain the different 802.11 Frame Types. Discuss the importance of different types of frames for forensics investigation. What kind of information may be get from different types of frames? [**3 Marks**]

c. Explain why WEP is considered unsecure. being a secure. Shortly describe the principle of WEP attack. [**5 Marks**]

QUESTION FIVE

Threat Analysis:

a. Explain the following system security properties: [**3 Marks**]
   Confidentiality
   Integrity
   Assurance
b. Provide the specification of the AAA framework: [**6 Marks**]
c. Explain the basic principle of risk management: [**1 Marks**]