[CRT08]

UNIVERSITY OF BOLTON

CREATIVE TECHNOLOGIES

BSC COMPUTER NETWORKS & SECURITY

SEMESTER TWO EXAMINATION 2018/2019

NETWORK SECURITY

MODULE NO: CPU6004

Date: Tuesday 21st May 2019 **Time: 14:00 – 16:00**

INSTRUCTIONS TO CANDIDATES:

There are SIX questions.

Answer FOUR questions.

All questions carry equal marks.

Individual marks are shown within the question.

Creative Technologies
BSc Computer Networks & Security
Semester Two Examination 2018-2019
Network Security
Module No. CPU6004

QUESTION 1

a) Critically evaluate the phases and concepts of Ethical Hacking, highlight the advantages and disadvantages of hacking and type of hackers.

(8 marks)

b) Evaluate information incident management according to the ISO/IEC 27035, discuss the primary elements and principles.

(7 marks)

c) In the Quantitative Risk Assessment, if the Asset value=£800,000 and the exposure factor=25%, calculate the single and annual loss expectancy?
If you know that, after implementing the safeguard the Annual rate of occurrence reduced from 3 times to 1, and the cost of the safeguard equals £100,000.

Calculate the ROSI (Return On Security Investment)?

(10 marks)

QUESTION 2

a) Discuss the risk management concept in term of Qualitative and semi-quantitative and quantitative impact and risks

(6 marks)

b) Explain the information security goals, missions and objectives using the risk appetite and cost of implementation and the benefit to the business?

(6 marks)

c) According to the ISO-27002 standards, discuss the CIA, DAD concepts needed for information security?

(6 marks)

d) Explain in details the difference between Risk, Threat and Vulnerability, highlights the difference between risk and the residual risk and the secondary risk?

(7 marks)

Creative Technologies
BSc Computer Networks & Security
Semester Two Examination 2018-2019
Network Security
Module No. CPU6004

PLEASE TURN THE PAGE….

QUESTION 3

a) Critically assess Network scanning common techniques, practically focus on a sweeping and port scan.

Support your answer with examples of using hping3, fping, nmap.
(9 marks)

b) Evaluate the vulnerabilities scanning techniques, discuss the Nessus scanner and web-site vulnerabilities scanners, support your answer with examples and diagrams. **(8 marks)**

c) Evaluate the DOS and DDOS in term of Bandwidth/throughput, Protocol and software vulnerabilities attacks?
(8 marks)

QUESTION 4

a) Explain the following: LAND, TEARDROP, SYN flood and SMURF attacks?
(6 marks)

b) Discuss the Enumerations concept, methods and tools?
State the steps and techniques to perform the enumerations.
(9 marks)

c) ABC Company has established Business Continuity (BC) & Disaster Recovery (DR) plan, an Incident happened on Monday at 11.00 am.
The MTD =6 hours.
The RTO took exactly 3.30 hours and the RPO needs 1 Hour.
Evaluate the following terms MTD, RTO, RPO, SDO?

Do you think the company met the MDT in their Business Continuity & Disaster Recovery plan? **(10 marks)**

Creative Technologies
BSc Computer Networks & Security
Semester Two Examination 2018-2019
Network Security
Module No. CPU6004

PLEASE TURN THE PAGE….

QUESTION 5

a) Critically appraise the following Security and Audit frameworks and methodologies (CISO, ITIL, COBIT, ISO-27002)?

(10 marks)

b) Iptables is an end user program that allows network admins to configure and manage a firewall by providing access to the predefined tables in order to allow users to add rules to the appropriate chains. The chains are implemented as a series of Netfilter modules which utilise 'hooks' in order to pass data and call functions from the Linux Kernel. The associated hooks are called to evaluate the packets based upon the rules as defined by the user.

Unstructured attacks come from inexperienced individuals typically using automated attack tools downloaded from the Internet at 193.168.1.20 as shown in Figure-1, create a bash script firewall.sh in order to implement on the Router to avoid and stop the attack. (see Appendix A for iptables help).

(15 marks)

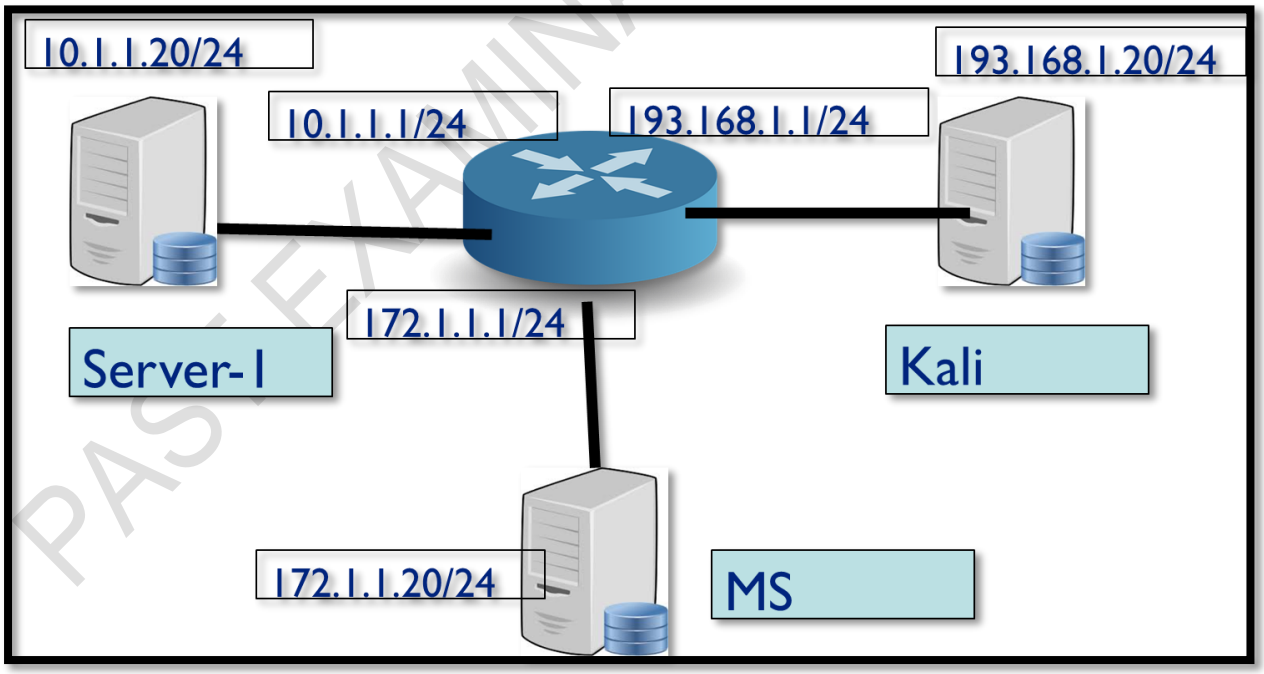

Figure-1: The Network infrastructure related to Q5:b)

Creative Technologies
BSc Computer Networks & Security
Semester Two Examination 2018-2019
Network Security
Module No. CPU6004

PLEASE TURN THE PAGE….

QUESTION 6

a) Critically appraise Spoofing Attack, expanding on ARP and RARP, IP, DNS Spoofing? Highlight on Spoofing Defenses to secure and protect the network. **(10 marks)**

b) Discuss in details using examples and diagrams the Session Hijacking Concepts and Tools, in term of Typical Session, Attack Methods, Session Sniffing, Man in the Middle Attack.

How to Prevent Session Hijacking? **(15 marks)**

END OF QUESTIONS

Appendix A – Iptables bash script over the page….

PLEASE TURN THE PAGE….

Creative Technologies
BSc Computer Networks & Security
Semester Two Examination 2018-2019
Network Security
Module No. CPU6004

Appendix A – Iptables bash script

#!/bin/bash

Default Policy iptables -P FORWARD DROP iptables -P INPUT DROP iptables -P OUTPUT DROP

iptables -A PREROUTING -i enp0s9 -p tcp -d 123.123.123.254 --dport 80 -j DNAT --to-destination 172.16.66.80 iptables -A FORWARD -i enp0s3 -o enp0s9 -p tcp --syn --dport 80 -m conntrack -ctstate NEW -j ACCEPT iptables -A FORWARD -i enp0s3 -o enp0s9 -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT iptables -A FORWARD -i enp0s9 -o enp0s3 -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

iptables -t nat -A POSTROUTING -o enp0s9 -p tcp --sport 80 -s 172.16.19.66 -j SNAT --to-source 123.123.123.254 iptables -A FORWARD -i enp0s9 -o enp0s8 -p tcp --syn --dport 80 -m conntrack --ctstate NEW -j ACCEPT iptables -A FORWARD -i enp0s8 -o enp0s9 -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT iptables -A FORWARD -i enp0s9 -o enp0s8 -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

iptables -A INPUT -i enp0s3 -p tcp -s 193.63.10.0/24 --dport 22 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT iptables -A OUTPUT -o enp0s3 -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEP

Scrpit1: **Use the above script as a guide to create your own rules.**

END OF PAPER