Strathmore UNIVERSITY

SCHOOL OF COMPUTING AND ENGINEERING SCIENCES

BACHELOR OF SCIENCE IN COMPUTER NETWORKS AND CYBER SECURITY

CNS 3202: ETHICAL HACKING I

END OF SEMESTER EXAM

Date: 1st December 2022 **Time:** 2 Hours

Instructions:

This Examination consists of **FIVE** questions

Answer **Question ONE (COMPULSORY)** and any other **TWO** questions.

QUESTION ONE (20 MARKS)

a) What is hacking? What does hacking involve (4 marks)

b) Scanning is the process of gathering additional detailed information about the target using highly complex and aggressive reconnaissance techniques.

Required

What would be the objectives for scanning a network? (5 marks)

c) With suitable examples, write short notes on the following hacker classes and clearly show their differences. **Black hats, White hats and hacktivists** (6 marks)

d) Explain five reasons why organizations recruit ethical hackers (5 marks)

QUESTION TWO (20 MARKS)

e) You receive a RST-ACK from a port during a SYN scan. What is the state of the port? (4 marks)

a) Explain six techniques for enumeration (6 marks)

b) Identify and describe the four key steps commonly termed as risk management phases (4 marks)

c) Briefly describe below services and TCP/UDP ports that can be enumerated

Describe TCP/UDP 53: DNS zone transfer,

TCP 139: NetBIOS Session service (SMB over NetBIOS) (6 marks)

QUESTION THREE (20 MARKS)

a) A team member issues the **nbtstat.exe –c** command. Briefly discuss the intention of the command? (5 marks)

b) Foot printing countermeasures, entail the measures or actions taken to prevent or offset information disclosure. Discuss any four foot-printing countermeasures (4 marks)

c) What is vulnerability assessment? What is it used for and what information is obtained from vulnerability scanner? (6 marks)

d) Describe the following HOSTS file that an ethical hacker pulled during an incident response: how would a user avoid this incident (5 marks)

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host
220.181.0.16      mybank.com
220.181.0.16      amazon.com
220.181.0.16      google.com
220.181.0.16      gmail.com
220.181.0.16      facebook.com
# localhost name resolution is handled within DNS itself.
#      127.0.0.1       localhost
#      ::1             localhost
```

QUESTION FOUR (20 MARKS)

The cybersecurity analyst and ethical hackers inevitably uncover evidence of criminal activity. In order to protect the organization and to prevent cybercrime, it is necessary to identify threat actors, report them to the appropriate authorities, and provide evidence to support prosecution.

Required

a) Outline and explain the role of digital forensics processes (8 marks)

b) Write short notes explaining the steps in the Cyber kill chain (7 marks)

c) A pen tester is performing banner grabbing and executes the following command:

$ nmap -sV host.domain.com -p 80 Briefly explain the following output: (5 marks)

```
Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-08 19:10 EST
Nmap scan report for host.domain.com (108.61.158.211)
Host is up (0.032s latency).
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd
Service detection performed. Please report any incorrect results at
http://nmap.org/submit/.
VCEConvert.com
Nmap done: 1 IP address (1 host up) scanned in 6.42 seconds
```

QUESTION FIVE (20 MARKS)

a) Consider the following incident:

An employee reports that his computer is acting abnormally. A host scan by the security technician indicates that the computer is infected with malware. An analysis of the malware reveals that the malware contains a list of CnC domain names that resolve to a list of IP addresses. These IP addresses are used to identify the adversary and investigate logs to determine if other victims in the organization are using the CnC channel.

Required

Use the Diamond Model Characterization of an Exploit, to illustrate how the adversary pivots from one event to the next (8 marks)

b) You are examining test logs from the day's pen test activities and note the following entries on a Windows 10 machine:

```
C:\> net user
User accounts for \\ANYPC
-------------------------------------------------------------------------------
Administrator            Backup                   DefaultAccount
Guest                    USER1
The command completed successfully.
C:\> net user USER1 user2
```

Required

Briefly analyze the test log (6 marks)

c) A Certified Ethical Hacker (CEH) follows a specific methodology for testing a system. List and briefly describe the first five steps in the CEH methodology? (6 marks)