TTM4536 ETISK HACKING, HØST 2016
Department of Telematics, NTNU

A Sample of Exam for December 2016

The student has 15 minutes to write down a sketch of the answers. Then in the next 15 minutes the student will orally explain the answers in front of the examination committee.

1. When setting up a virtual machine in VirtualBox, explain in brief as many system components as you can, that should be defined for the machine. (max 10p)
   Possible answers (each brings 2 points, but max points are 10):
   a. Define which operating system is running in the virtual machine. (2p)
   b. Define how big is the base RAM memory. (2p)
   c. Define how many CPUs has the virtual machine. (2p)
   d. Define how big is the video memory. (2p)
   e. Define how big is the hard disk of the machine. (2p)
   f. Define what is the type of the network adapter. (2p)
   g. Define the shared folders between host and the guest operating system. (2p)

2. Name all necessary components for making a simple TCP client in Python (10p)
   Answers:
   a. The module socket should be imported with "import socket" instruction. (2p)
   b. An object (for example named client) should be created by the instruction:
      client = socket.socket(socket.AF_INET, socket.SOCK_STREAM)   (2p)
   c. Connect the client with the instruction
      client.connect((target_host,target_port))
      where target_host and target_port are predefined with some previous instructions. (2p)
   d. Send some data to the target host with the instruction
      client.send("GET / HTTP/1.1\r\nHost: yyyyyy.com \r\n\r\n")
      where yyyyyy.com is the same name as predefined target_host (2p)
   e. Receive some data from the target host with the instruction
      response = client.recv(4096) (2p)

3. What is "sys" module of Python used for (4p)? Name at least 3 methods (functionalities) that we used in our hack scripts in the lab (Each functionality brings 2 points, in total max 10p)
   Answers:
   a. "sys" module provides access to some variables used or maintained by the interpreter and to functions that interact strongly with the interpreter. It is always available. (4p)
   b. sys.exit(some number) (2p)
   c. sys.argv( ) (2p)
   d. sys.stdin.read() (2p)

4. Explain the following Python instruction:
   sniff(filter="",iface="any",prn=function,count=N) (10p)

   Answers:

   a. This instruction is from the Python interactive packet manipulation program “Scapy”. (2p)
   b. The filter parameter allows us to specify a BPF (Wireshark-style) filter to the packets that Scapy sniffs. (2p)
   c. The iface parameter tells the sniffer which network interface to sniff on. (2p)
   d. The prn parameter specifies a callback function to be called for every packet that matches the filter. (2p)
   e. The count parameter specifies how many packets you want to sniff. (2p)

5. How can you disguise your browsing as “Googlebot” from Python? (10p)

   Answers:

   a. use “urllib2” module with the command:
      import urllib2 (2p)
   b. define the target url address with the command:
      url = "http://10.0.2.15" (2p)
   c. construct an indexed set headers with the instruction:
      headers['User-Agent'] = "Googlebot” (2p)
   d. construct a concrete url request form that will be sent to some url address with:
      request = urllib2.Request(url, headers=headers) (2p)
   e. contact the defined url with:
      response = urllib2.urlopen(request) (2p)

6. Everything you know about SQL Injection Attacks? (10p)

   Answer can include:

Explanation that a SQL injection attack involves placing SQL statements in the user input in web pages, discussion about some specific SQL commands (like SELECT), mentioning some specific SQL injection queries (like 'OR 1=1--), use of some tools like sqlmap, what are the possible defenses, …