Old exam from 2015. Note that in 2015 max points from the oral exam were 50, while in 2016 max points earned on oral exam will be 60.

TTM4536 ETISK HACKING, HØST 2015
Department of Telematics, NTNU

Exam 2 December 2015

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. Explain in as much details as you can what is Kali Linux? (10p)

2. How can you build a simple SSH client in Python (10p)

Old exam from 2015. Note that in 2015 max points from the oral exam were 50, while in 2016 max points earned on oral exam will be 60.

3. In order to speed up the hacking that a function “do_some_hack” is doing we want to run 10 instances of that function in parallel. How can we achieve that in Python? (10p)

4. How can you sniff 3 packets with scapy and Python?

5. Keyloggers (10p)
    a. What is a keylogger? (2p)
    b. How can you detect a keylogger from a command line in Linux? (2p)
    c. List several keyloggers that we worked with (or mentioned) in the lab (each 2p)

Old exam from 2015. Note that in 2015 max points from the oral exam were 50, while in 2016 max points earned on oral exam will be 60.

TTM4536 ETISK HACKING, HØST 2015
Department of Telematics, NTNU

Exam 2 December 2015

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. Explain in as much details as you can what is Kali Linux? (10p)
   Possible answers up to max 10 points:
   a. Kali is a penetration testing operating system. (4p)
   b. It is based on Debian Linux. (2p)
   c. It is designed by Offensive Security. (2p)
   d. It comes with a number of hacking tools preinstalled. (2p)

2. How can you build a simple SSH client in Python (10p)
   Possible answers that each brings 2 points (up to max 10p):
   a. We need the Python module paramiko installed in the system with the instruction: pip install paramiko (2p)
   b. The module paramiko should be imported with "import paramiko" instruction. (2p)
   c. We should define a function
      ssh_command(ip, user, passwd, command)
      where "ip" is the ip address of the ssh server, "user" is the user name, "passwd" is the password, and "command" is the command that will be executed upon successful connection. (2p)
   d. An object (for example named client) should be created by the instruction:
      client = paramiko.SSHClient() (2p)
   e. Connect the client with the instruction
      client.connect(ip, username=user, password=passwd) (2p)
   f. Open a ssh session with
      ssh_session = client.get_transport().open_session() (2p)
   g. Execute a command with:
      ssh_session.exec_command(command) (2p)

Old exam from 2015. Note that in 2015 max points from the oral exam were 50, while in 2016 max points earned on oral exam will be 60.

3. In order to speed up the hacking that a function “do_some_hack” is doing we want to run 10 instances of that function in parallel. How can we achieve that in Python? (10p)

   Answers:

   a. We need to import “threading” module. (2p)
   b. We define a variable threads = 10 (2p)
   c. We define the function “do_some_hack” (2p)
   d. We run a for loop to spawn 10 threads of the function with
      for i in range(threads):
          t = threading.Thread(target= do_some_hack)
          t.start()
      (4p)

4. How can you sniff 3 packets with scapy and Python?
   a. We need to import scapy with the instruction
      from scapy.all import * (2p)
   b. We need to define a callback function that will be invoked after the sniffing:
      def packet_callback(packet):
          print packet.show() (4p)
   c. We call the sniff function of scapy by
      sniff(prn=packet_callback, count=3) (4p)

5. Keyloggers (10p)
   a. What is a keylogger? (2p)
   b. How can you detect a keylogger from a command line in Linux? (2p)
   c. List several keyloggers that we worked with (or mentioned) in the lab (each 2p)

   Possible answers:

   a. A computer program that records every keystroke made by a computer user (2p)
   b. With a command “top” or the command “ps –aux” (2p)
   c. PyKeylogger (2p)
   d. simple-key-logger or SKeylogger (2p)
   e. logkeys (2p)
   f. LKL Linux KeyLogger (2p)