1: Setting Up Your Python Environment

- What is Kali Linux (2015(2))
- What is PyCharm and give some characteristics of PyCharm (2016)
- 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 (2015)

2. The Network: Basics

- What is Netcat and how can it be replaced?
- Name all necessary component for making simple TCP Proxy
- What is the “socket/getopt/threading/subprocess/paramiko” modules of Python used for? Name at least 3 methods (functionalities) that we used in our hack scripts in the lab.
- Explain how hash functions works, what is it used for and what is a good hash function?
- Explain encryption algorithms
- Explain public key algorithms: Key generation, encrypt/decrypt and signatures.
- Explain how RSA-keys are generated, why is it important to generate the keys using new prime numbers for each key generated?
- What is “crypto” module of Python used for? Name at least 3 methods (functionalities) that we used in our hack scripts in the lab
- What is Angr, explain its functionalities.
- How can you build a simple SSH client in Python? (2015(2))
- Name all necessary component for making simple TCP client (or server) in python (2016(2), 2015)
- What is “sys” module of Python used for? Name at least 3 methods (functionalities) that we used in our hack scripts in the lab (2015)
- 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? (2015(2))

3. The Network: Raw sockets and Sniffing

- What is “os” module of Python used for? Name at least 3 methods (functionalities) that we used in our hack scripts in the lab. (2016)
- In the lab exercises we have built a simple packet sniffer in Python. Name some of the main commands used for that sniffer. (2016)
- Explain the following Python instruction: sniff(filter="",iface="any",prn=function,count=N) (2015)
- How can you build a simple scanner in python?

4. Owning the Network with Scapy

- How can scapy be used to create a mail sniffer?
- What are pcap files and how can one use scapy to analyse them?
- What is “Scapy” module of Python used for? Name at least 3 methods (functionalities) that we used in our hack scripts in the lab.
- How can we sniff 3 packets with scapy and Python? (2015(2))

5. Web Hackery

- What is “Urllib2” module of Python used for? Name at least 3 methods (functionalities) that we used in our hack scripts in the lab
- What is dojo?
- Explain how the web_app_mapper, content_bruter and joomla_killer works
- What is XSS, explain persistent/DOM based XSS attacks
- Explain the non-persistent XSS attack and its risks. (2016)
- Everything you know about sql injection attacks (2016(2))
- How can you disguise your browsing as “Googlebot” from Python? (2015 / 2016(2))

6. Extending the Burp Proxy

- What is Burp and what functionality does it offer?

7. Github Command and Control

- What is a Trojan Horse?
- Explain the functionality of BOTNETS
- What is JSON?
- In the lab we used the git_trojan.py script to perform some simple Trojan actions on the GitHub.com servers. Name some of the basic actions that we performed working with this script. (2016)

8. Common Trojaning Tasks on Windows

- Explain the main components of creating a simple Python keylogger for linux.
- What is spyware, and what are symptoms?
- How can we start a simple http server that listens the port 8080 with a single command from a terminal invoking the python interpreter? Explain the command (2016)
- What is a keylogger? (2015(2))