Institution: SecureSet Academy.

Program: Bootcamp Prep.

Course: Introduction to Network Security.

Course Description: This three-session course is meant to be an introduction to Network Security. We will cover the first four layers of the OSI model in depth (physical, data link, network, transport). We will also cover basic network security issues and countermeasures. We will have exercises given as homework at the end of each session, to be collected for corrections and feedback. Besides the homework, there will not be a formal assessment, as the Bootcamp Prep program already has an exam.

Course Objectives:

At the completion of this course, students will be able to:

1. Describe network traffic in terms of the OSI model
2. Understand the basics of the physical layer
3. Understand the basics of the data link layer
4. Understand the basics of the network layer
5. Understand the basics of the transport layer
6. Understand classic network security vulnerabilities
7. Use wireshark, minimally
8. Use netcat, minimally

Course Policies:

- **General**
  - While the instructor is demonstrating code/commands you should feel free to try it for yourself, but pay attention during lecture.
- **Homework**
  - Homework is assigned at the end of each class, and collected at the beginning of the next.
- **Attendance**
  - Attendance is expected each class.
  - Since final Bootcamp Prep evaluations cover all the material (not just Network Security), it is the student's responsibility to attend each session.

Course Schedule:

Day	Content
Day 1	• Introduction to the OSI model • The Physical layer – Ethernet – WiFi – Fiber optics • The Data link layer – Routers – Switches (managed vs unmanaged) • The Network layer – IPv4 addresses – Private IP addresses – Public IP addresses – Subnetting – CIDR notation – IPv6 addresses • Frames and encapsulation • **Homework.** Install wireshark and dsniff on your Linux VM.

Course Schedule:

Day	Content
Day 2	• MAC addresses • MAC addresses vs IP addresses • ARP • ARP tables • Man-in-the-middle attacks • ARP spoofing • ARP spoof demonstration (using dsniff that they installed as part of their homework) • The Transport layer – Ports – Privileged ports – Port forwarding – NAT tables • Wireshark • **Homework.** Make a table of ten of the most commonly used ports and the services that usually use them.

Course Schedule:

Day	Content
Day 3	• The Transport layer – TCP vs UDP – TCP three-way handshake – TCP flags – Sequence numbers • netcat – What is netcat? – netcat chat – netcat HTTP GET – netcat port scanning – netcat bind shells and reverse shells (time allowing) • DNS • DoS/DDoS attacks • Firewalls • **Homework.** Capture a TCP three-way handshake in wireshark. Make a table listing the following items: – Source and destination IP address – Source and destination port – Beginning sequence numbers (for both parties)