THOMAS NELSON™

The Peninsula's Community College

Course Content Summary
ITN 261 – Network Attacks, Computer Crime and Hacking (4 Credits)

TNCC Cybersecurity Program web page: http://tncc.edu/programs/cyber-security

Course Description:

Encompasses in-depth exploration of various methods for attacking and defending a network. Explores network security concepts from the viewpoint hackers and their attack methodologies. Includes topics about hackers, attacks, Intrusion Detection Systems (IDS) malicious code, computer crime and industrial espionage. Lecture 4 hours per week.

Statement of Purpose:

This course introduces the student to the process and tools, including Nmap and other port scanning tools used to perform ethical hacking. A discussion of different network attacks, computer crime, and hacking is provided. The purpose of this course is to inform the student of common techniques used by attackers in order to increase awareness and assist the student in learning how to effectively counter these attacks. This course also includes content, as indicated below in parenthesis behind each learning objective that directly maps to DHS/NSA's Center of Academic Excellence – 2 Year (CAE2Y) criteria.

Course Prerequisites / Corequisites:

ITN 260.

Required Text:

Hacker Techniques, Tools, and Incident Handling, second edition.
Author: Oriyano, Sean-Philip
Publisher: Jones & Bartlett Learning.

COURSE OBJECTIVES

1.0 Explain the history and current state of hacking and penetration testing, including ethical and legal implications.
2.0 Identify fundamental TCP/IP concepts and technologies related to networking.
3.0 Describe cryptology and its uses in modern computer networking systems.
4.0 Identify basic equipment controls, physical area controls, and facility controls.
5.0 Identify common information gathering tools and techniques.
6.0 Analyze how port scanning and fingerprinting are used by hackers.
7.0 Analyze how enumeration is used in conjunction with system hacking.
8.0 Analyze wireless network vulnerabilities exploited by hackers.
9.0 Describe Web and database attacks.
10.0 Identify and remove common types of malware from infected systems.
11.0 Perform network traffic analysis and sniffing by using appropriate tools.
12.0 Analyze systems using Linux tools.
13.0 Identify common social engineering attacks.
14.0 Perform incident handling by using appropriate methods.
15.0 Compare and contrast defensive technologies.

STUDENT LEARNING OUTCOMES

1.0 The History of Hacking and its Current State of the Art

1.1 Describe and explain the history and evolution of hackers and hacking. (**CT1, CT11**)
1.2 Explain why information systems and people are vulnerable to manipulation.
1.3 Differentiate between hacking, ethical hacking, penetration testing, and auditing.
1.4 Identify the motivations, skill sets, and primary attack tools used by hackers. (**CT2, IA1**)
1.5 Compare the steps and phases of a hacking attack to those of a penetration test.
1.6 Explain the difference in risk between inside and outside threats and attacks.
1.7 Explain the need for ethical hackers and identify the most important steps in ethical hacking.
1.8 Identify important laws related to hacking.

2.0 TCP/IP Review

2.1 Summarize and describe the OSI and TCP/IP reference model functions by layer. (**NC1**)
2.2 List and describe the primary TCP/IP protocols including IP, ICMP, TCP, and UDP. (**NC6**)
2.3 Describe TCP functions and the importance of flags as related to scanning activities.
2.4 Explain the differences between UDP and TCP scanning.
2.5 Explain common ICMP protocol message types and codes.
2.6 Describe the role of IP in networking.
2.7 Describe the operation of Ethernet.
2.8 Explain the structure of Media Access Control (MAC) addresses.
2.9 Explain the operation of CSMA/CD.
2.10 Compare and contrast routable versus routing protocols.

2.11 Compare and contrast Link State versus Distance Vector routing protocols and their vulnerabilities.
2.12 Explain the function and components of protocol analyzer applications.
2.13 Describe common TCP/IP attacks.
2.14 Explain the function of a botnet. (**CT4d**)

3.0 Cryptographic Concepts

3.1 Describe the purpose of cryptography. (**IA6**)
3.2 Explain what a cryptographic algorithm is.
3.3 Describe the usage, advantages, and disadvantages of symmetric encryption. (**IC1**)
3.4 Describe the components of symmetric algorithms such as key size and block size.
3.5 Explain the importance of asymmetric encryption to the goals of integrity and non-repudiation.
3.6 Describe common asymmetric algorithms.
3.7 Explain the purpose and usage of hashing algorithms. (**IC3**)
3.8 Explain the purpose and usage of digital signatures.
3.9 Demonstrate understanding of the basics of Public Key Infrastructure and describe PKI attacks. (**IC2**)
3.10 Demonstrate understanding of cryptanalysis and basic password attack methods. **(CT4a) (IC7)**

4.0 Physical Security

4.1 Explain the role of physical security.
4.2 Describe common physical controls.
4.3 Explain the basic types of locks and describe how they work.
4.4 Describe the purpose and uses of closed circuit TV (CCTV).
4.5 Explain the concept of Defense in Depth. (**CD7**)
4.6 Define physical intrusion detection.
4.7 Explain how to secure the physical environment.
4.8 Define building design best practices.
4.9 Describe alarm systems.

5.0 Footprinting Tools and Techniques

5.1 Describe the purpose of footprinting.
5.2 List the types of information typically found on an organization's website.
5.3 Identify sources on the World Wide Web used for footprinting.
5.4 Demonstrate how attackers map organizations.
5.5 Describe the types of information that can be found about an organization's key employees.
5.6 List examples of unsecured applications used by organizations.
5.7 Demonstrate Google Hacking.

6.0 Port Scanning

6.1 Define and explain the purpose of port scanning.
6.2 Demonstrate common port scanning techniques.
6.3 Explain why scanning UDP is harder than scanning TCP.
6.4 Demonstrate understanding and usage of the Nmap application. (**CD1**)

6.5 Describe OS fingerprinting.
6.6 Explain the difference between active and passive scanning.
6.7 Describe various network mapping tools.

7.0 Enumeration and Computer System Hacking

7.1 Explain the process of enumeration. (**CD1**)
7.2 Explain the process of system hacking.
7.3 Explain the process of password cracking. (**CT4a**)
7.4 Identify and explain common tools used to perform enumeration.
7.5 Describe the significance of privilege escalation.
7.6 Explain how to perform privilege escalation.
7.7 Explain the importance of covering tracks.
7.8 Describe the concept of backdoors. (**CT4b**)
7.9 Explain how to create backdoors. (**CT4b**)

8.0 Wireless Vulnerabilities

8.1 Define and explain the purpose of wireless security.
8.2 Describe the history of wireless communications.
8.3 Explain the security issues associated with wireless applications such as satellite TV and cell phones.
8.4 Define and explain the functionality of Bluetooth.
8.5 Explain the security issues associated with Bluetooth based communications. **(CT1)**
8.6 Describe wireless LANs and explain how they function.
8.7 Identify threats to wireless LANs. **(CT1)**
8.8 Describe types of wireless hacking tools.
8.9 Demonstrate how to defend wireless networks.

9.0 Web and Database Attacks

9.1 Explain the issues facing web servers and the applications that run on them. **(CT1)**
9.2 Identify vulnerabilities of web servers and the applications that run on them. (**CT4f**)
9.3 Describe the challenges faced by a web master. **(CT1)**
9.4 Explain how to deface a website.
9.5 Describe how to enumerate web services.
9.6 Describe how to attack web applications. (**CT4e**)
9.7 Describe the nature of buffer overflows.
9.8 Explain input validation and its usage.
9.9 Describe how DoS attacks are carried out against websites.
9.10 Describe SQL injection and its usage.
9.11 Identify security issues associated with cloud computing.

10.0 Malware

10.1 List the common types of malware found in the wild.
10.2 Describe the nature of and the threats posed by malware. (**CD4**)
10.3 Describe the threats posed by viruses. (**CT4b**)
10.4 Identify removal and mitigation techniques for malware.
10.5 Explain the common behaviors and goals of Trojans. (**CT4b**)
10.6 Explain how to detect Trojans.
10.7 Describe the tools used to create Trojans.
10.8 Explain the purposes of backdoors. (**CT4a**)
10.9 Explain the significance of covert channels. (**CT12**)

11.0 Sniffers, Session Hijacking, and Denial of Service Attacks

11.1 Describe the value of sniffer applications. (**CT4c**)
11.2 Explain the purpose of session hijacking. (**CT4c**)
11.3 Describe the process of DoS attacks. (**CT4d**)
11.4 Describe botnets. (**CT4d**)
11.5 Identify the capabilities of sniffer applications. (**CT4c**)
11.6 Describe the process of session hijacking. (**CT4c**)
11.7 Describe the features of a DoS attack. (**CT4d**)

12.0 Linux and Penetration Testing

12.1 Describe the Linux OS and identify some of its features.
12.2 Explain what Kali Linux is.
12.3 Explain some of the basics of working with Linux.
12.4 Describe the benefits of live CDs.

13.0 Social Engineering

13.1 Explain how social engineering differs from other kinds of attacks. (**CT6**)
13.2 Describe several common types of social engineering attacks. (**CT6**)
13.3 Explain how your web browser can protect you as you surf the WWW.
13.4 Identify several best practices for safe computing.
13.5 Explain the creation of good password policy.
13.6 Explain how social engineering is a particular threat in the world of social networking. (**CT6**)
13.7 Describe the challenges of social media in the corporate setting.

14.0 Incident Response

14.1 Describe the components of incident response.
14.2 Explain the goals of incident response.

15.0 Defensive Technologies

15.1 Explain two forms of Intrusion Detection Systems (IDS). (**CD2**) **(IT6)**
15.2 Describe the goals of an IDS. **(IT6)**
15.3 Describe the detection methods of IDS. **(IT6)**
15.4 List the different types of firewalls. **(CD2, NC4) (IT6)**
15.5 Explain the purpose of firewalls. **(CD2, NC4) (IT6)**
15.6 Explain the purpose of honeypots.
15.7 Explain the purpose of honeynets.
15.8 Describe the purpose of administrative controls.

CAE2Y Knowledge Unit Domain Index

Course Content KU Indicator	CAE2Y KU Full Domain Name
BD	**Basic Data Analysis**
BS	**Basic Scripting**
CD	**Cyber Defense**
CT	**Cyber Threats**
FS	**Fundamental Security Design Principles**
IA	**Information Assurance Fundamentals**
IC	**Introduction to Cryptography**
IT	**Information Technology System Components**
NC	**Networking Concepts**
PL	**Policy legal Ethics and Compliance**
SA	**Systems Administration**

NOTE: the number following the KU Indicator represents the KU Domain topic as shown in the KU mapping matrix (Excel file).