Ethical Hacking I
Course of Study for HAC2

Description
This course of study is designed to prepare you for the HAC2 objective exam. It outlines the sequence of learning activities you should complete to demonstrate competence in this subject area. The timeline represents the standard number of weeks that you should allow to prepare for this assessment. The average time to complete this course of study is eight weeks. You and your mentor may determine that you require more or less time for preparation.

Introduction
Welcome to the HAC2 – Ethical Hacking Part I Course of Study. My name is Allen Clarkson. I will be the mentor guiding you through this area of study. I hold a B.S. in Philosophy and Classical Studies and an M.S. in Technology Management. I have worked as a system administrator, legal case advisor, forensic researcher, and IT consultant. I am active in Information Security and Digital Forensics research, focusing primarily on the application of legal frameworks to emerging technology and a Systems Science approach to the management of digital forensic labs and investigations.

Course of Study Mentor ..... Allen Clarkson
Email ................................ aclarkson@wgu.edu
Telephone .......................... 1-866-895-9660, x1849
Office Hours .......................... Monday, 11:00am – 7:00pm, Eastern Time
                                 Tuesday, 11:00am – 7:00pm, Eastern Time
                                 Wednesday, 11:00am – 7:00pm, Eastern Time
                                 Thursday, 11:00am – 7:00pm, Eastern Time
                                 Friday, 11:00am – 7:00pm, Eastern Time

Overview
This course of study will help you acquire the skills necessary to protect an organization's information system from unauthorized access and system hacking. You will learn about security threats, penetration testing, vulnerability analysis, risk mitigation, business-related issues, and countermeasures.

Competence is measured by the EC Council Certified Ethical Hacker Exam (ECO-350). The Certified Ethical Hacker exam includes a random selection of 150 questions that must completed within a four-hour time period. To achieve a passing score on the exam, you must score at least 70 percent. Once you have submitted your passing score, you will receive a “PASS” on your AAP for the Hacking I Assessment.

You can do an Internet search for “what is ethical hacking?” and come up with multiple returns. In a nutshell, an “ethical hacker” is someone who purposefully tries to hack a network and computer system with the goal of exposing vulnerabilities. You are probably wondering why anyone might want to do such a thing. A company cannot honestly know if their systems are secure unless they test it. In this course of study, you will not only be introduced to how to expose the vulnerabilities, but you will also be introduced to solutions for eliminating and/or preventing vulnerabilities as well. By now, you should have completed the Network Security Parts I and II and the Wireless Security Parts I and II assessments. In order to understand many of the concepts presented in this course of study, you will need to utilize the skills you acquired in those two courses of study. You will learn how to apply your hacking skills on different types of networks and platforms. The skills you acquire will put you in an excellent place to protect your employer's network and computer systems against potential vulnerabilities.
There are six competencies covered by the Ethical Hacking I Course of Study:

**Competency 426.4.1: Ethics and Legality**
The graduate analyzes ethical and legal issues related to the unauthorized or unwanted access into and of information assets, including types of hacking technologies and related skills.

**Competency 426.4.2: Pre-Attack Planning**
The graduate evaluates techniques used in footprinting and implements industry best practices to protect against this type of information asset vulnerability.

**Competency 426.4.3: System Hacking**
The graduate evaluates various network system hacking counter-techniques.

**Competency 426.4.5: Hacking Web Servers**
The graduate identifies known Web server vulnerabilities and demonstrates industry best practices to protect against this type of threat.

**Competency 426.4.6: Web Application Vulnerabilities**
The graduate identifies common Web application vulnerabilities and uses industry best practices to protect against this type of threat.

**Competency 426.4.7: Wireless Hacking**
The graduate evaluates industry best practices for securing a wireless network, identifies the threats to wireless security, and associates threats with known countermeasures.

**Learning Resources:**

**Textbooks**
- The CEH Prep Guide: The Comprehensive Guide to Certified Ethical Hacking
- CEH Official Certified Ethical Hacker Review Guide: Exam 312-50

**Online Modules**
- LearnKey (“Hacking Revealed”)—12 hours of interactive training
  - Session 1 (7 sections)
  - Session 2 (7 sections)
  - Session 3 (9 sections)
  - Session 4 (7 sections)
  - Session 5 (6 sections)
  - Session 6 (6 sections)

**Week 1**

**Preventing for Success**
To successfully complete HAC2, you will need the appropriate learning resources. You should also prepare a calendar to schedule times devoted to your studies. Share your calendar with family and friends so they are aware of your obligations.

**Acquire Learning Resources**
Arrange to obtain the learning resources listed below so there will be no delays in your studies. These items are essential for you, as this document will guide you week-by-week in the use of
these materials. Some of these items must be shipped to you, so be sure that your mailing address information is current. If you click your name on your AAP, you can check your contact information.

☐ Order Textbooks


*Note: You will reuse this textbook for the FBC2 assessment.*

These three textbooks can be ordered through the WGU Bookstore. You can order through the “Learning Resource” tab of your AAP. *The CEH Prep Guide* (by Krutz and Vines, 2008) is organized into 16 chapters and two appendices. The chapters contain information covering multiple exam categories. On the first page of every chapter, you will see an overview of which exam objectives are covered in the chapter. We recommend that you create sections in your notebook that reflect the specific exam objectives. As you are reading through the text book, take notes and file them accordingly. This will help you go back and review the sections you may have difficulty with as you progress through this assessment.

*Note: The WGU Bookstore has these books available for immediate purchase and delivery. You may shop at other online bookstores, but be sure to order early and use the correct ISBN to get the correct edition.*

☐ Familiarize Yourself With SkillSoft
This resource will be used in conjunction with the hands-on labs and is where you obtain your LearnKey materials. All incoming IT students are automatically enrolled. You should be enrolled in this resource when you have successfully completed EWB. If for some reason, you never received your login credentials, please e-mail our Learning Resources Department (learning@wgu.edu).

☐ Getting Enrolled in SkillSoft
WGU students are batch-loaded into the SkillSoft site.
1. Access the SkillSoft site at [http://wgu.skillport.com](http://wgu.skillport.com)
2. Enter your MyWGU Student Portal username and original WGU password
3. If you cannot remember your original WGU password, you can go to the “Forgot your Password?” link, enter your WGU portal user ID, and the password will be sent to your my.wgu.edu email address.

If you have any trouble, please contact the Learning Resources Department at (learning@wgu.edu). Batch-loads are done at the end of each week. If you have not met AAV, access may be delayed to the next week.
☐ **Enroll in LearnKey**  
**URL:** [http://wgu.onlineexpert.com](http://wgu.onlineexpert.com)

LearnKey is an interactive, video-based learning resource that provides you with engaging video presentations and engaging activities, practice tests, and labs. If you are a visual or auditory learner, you will love this resource. To enroll, click on the learning resource tab in your AAP. Look for the “Hacking Revealed 2008 (6 Sessions)” LearnKey link. Click that link, then click “Enroll Now.” Once you have enrolled, you will receive an email with instructions on how to log in. As you go through this course of study, you will see LearnKey resources listed as “LearnKey course.” Whenever you see that listing, you will know to navigate to [http://wgu.onlineexpert.com](http://wgu.onlineexpert.com).

☐ **MeasureUp Preassessment**  
Your mentor will need to manually enroll in this resource. You will need the technical assessment (what WGU calls a preassessment) to begin with. You will also need the practice materials later in the term. Have your mentor request both for you at the appropriate time. Note that MeasureUp is good as a diagnostic but not as a study tool. It is not a comprehensive question bank—just a “cross section.” You can know every question in the MeasureUp bank and still fail the real exam. So, we will use MeasureUp for benchmarking before and after your studies, but not as a study tool.

☐ **VMWare**  
In this course of study, we strongly encourage you to try any and all hands-on activities you encounter. Many of the activities use multiple different operating systems. If you do not already use VMWare, it is recommended. VMware is an excellent product that will very easily allow you to partition your hard drive and run multiple operating systems on the same machine. There are several product offerings available, depending upon your current OS platform:

1. VMWare Workstation allows you to run Windows, Linux, and more on a PC: [http://www.vmware.com/products/ws/](http://www.vmware.com/products/ws/)
2. VMWare Fusion allows you to run Windows applications on a Mac: [http://www.vmware.com/products/fusion/](http://www.vmware.com/products/fusion/)

As a university student, you can get a discount on either of these products. Use the academic storefront: [http://www.vmware.com/vmwarestore/academicstore.html](http://www.vmware.com/vmwarestore/academicstore.html).

☐ **Create Notebook**  
It is suggested that you create a paper or digital notebook for your studies of database fundamentals. Use organizers or dividers to separate your work. Suggestions divisions include:

- Glossary
- Study notes
- Competency review notes
- Helpful Web sites

☐ **Lab Environment**  
The *Hands-On Information Security Lab Manual* textbook include step-by-step exercises to provide hands-on ethical hacking skills. The included CD-ROM contains all the freeware software used in the exercises.
It is recommended that you invest in certain equipment (Windows XP workstation and Linux Fedora workstation) to get the full effect of the labs. However, much value can be gained by simply reading through the tasks without performing the steps on live equipment.

Many of these labs will have you looking at settings on your home computer, and often time making changes to them. Be sure you are careful to backup your settings before making changes to your system.

You can conduct hands-on practice in the following ways:

1. Acquire two computers—one for Windows XP and one for Linux Fedora. You can obtain a fully licensed version (180-day trial) of Windows Server and Windows XP Professional through the MSDN Academic Alliance. Go to the IT Program Learning Community and search for “MSDN.” There, you will find a how to download your copy. You can download the latest version of Linux Fedora at http://fedoraproject.org/get-fedora. This is recommended.

2. You can consider partitioning your current computer if your current desktop or laptop is running Windows NT/2000 and if you have the software to help you partition your current hard drive on your PC/laptop. This will allow you to install Windows XP Professional and Linux Fedora on one PC, and avoid buying additional hardware (i.e., desktop, laptop, hard drives) in order to conduct hands-on practices for the HAC2.

**Going Forward**

The Ethical Hacking I Course of Study is organized into thirteen main topic areas. Each topic area has multiple activities. Review topics prior to taking your exam, and to ensure you understand the material after reading the book, complete the hands-on labs and the questions at the end of each chapter.

**Ethics and Legality**

This domain will provide an overview of ethical hacking, ethics and the legalities of ethical hacking. In order to understand ethical hacking, you will need an understanding of legal systems, computer-related laws, and ethical principles. This domain will provide that foundation of knowledge.

**Competency 426.4.1: Ethics and Legality**

The graduate analyzes ethical and legal issues related to the unauthorized or unwanted access into and of information assets, including types of hacking technologies and related skills.

**The Technical Foundations of Hacking**

In this section, you will learn about the history of hacking and why ethical hacking is needed to protect an organization’s information system from unwanted access and cyber attacks.

As you review this material, take notes and attempt to answer the following questions.

- What are the basic tenets of information system security?
- What are the differences between the following: hacker, ethical hacker, cracker, phreaker, whacker, script/kiddie, and cyber-terrorist
- What are the steps in malicious hacking?
LearnKey—Understanding the Network+ Domains

Navigate to “Hacking Revealed 2008 Session 1.” When you arrive, you will notice that the session is broken down into these areas:
- Launch Pre-Assessment
- Launch Network+ 2009 Certification Training
- Launch Labs
- Launch Posttest

For this activity we want you to do two things:
1. Take the preassessment
2. Watch the videos

The preassessment will give you a good idea of which of the lessons you should really focus on. When you have completed the preassessment, you have an option to save and print the study guide. This study guide lists the questions from the preassessment you missed, and the session and lesson you should work from. Print this out and save it. When you run across a “Watch LearnKey Video” activity, you will know to look at your study guide to determine whether or not you think you should watch the lesson.

Watch these three sections from session 1:
- Section A: Introduction to Ethical Hacking
- Section B: Ethics and the Hacker
- Section C: Hacking Legalities

As you are working your way through the sections, be sure to take notes on what to expect on the Ethical Hacking exam and how the domains on that exam are organized.

Read in The CEH Prep Guide

In The CEH Prep Guide: The Comprehensive Guide to Certified Ethical Hacking, read the following chapters.
- Chapter 1 (“Introduction to Ethical Hacking”): This chapter explains the differences between hackers and ethical hackers, and the purpose, scope and steps involved in ethical hacking.
- Chapter 2 (“Legality and Ethics”): This chapter discusses various computer-related laws, ethics and computer crime.

Review Questions

In The CEH Prep Guide: The Comprehensive Guide to Certified Ethical Hacking, complete the section of “Review Questions” in chapters 1 and 2.

The Business Aspects of Penetration Testing

In this section, you will learn about penetration testing. Penetration testing is a component of risk management, and is associated with the protection of an organization’s assets.

As you review this material, take notes and attempt to answer the following questions:
- What are the steps in penetration testing?
- Explain the risk analysis process.

Read in The CEH Prep Guide

In The CEH Prep Guide: The Comprehensive Guide to Certified Ethical Hacking, read chapter 3 (“Penetration Testing for Business”). This chapter discusses the value of
penetration testing and risk analysis in an organization. Penetration testing involves testing an organization’s systems for vulnerabilities.

☐ Review Questions

**Week 2**

**Pre-Attack Planning**
This domain will provide an overview of penetration testing, footprinting, WHOIS, scanning, and enumeration. You will learn the reconnaissance techniques that hackers use to target and exploit networks.

**Competency 426.4.2: Pre-Attack Planning**
The graduate evaluates techniques used in footprinting and implements industry best practices to protect against this type of information asset vulnerability.

**Footprinting and Scanning**
In this section, you will learn about the tools used by hackers to passively (without the organizations knowledge) gain information about an organization – footprinting and scanning.

As you review this material, take notes and attempt to answer the following questions:
- What are the seven steps of reconnaissance?
- What are some utilities used in footprinting?
- What are the common utilities used to identify active machines?

☐ LearnKey—Footprinting
Watch these four sections from session 1:
- Section D: Footprinting Concepts
- Section E: Web Footprinting Tools
- Section F: Local Footprinting Tools
- Section G: Scanning for Gold

This session will give you an excellent overview of the concept of footprinting and how footprinting works locally and on the web. Tom Carpenter does an excellent job of explaining this concept. We strongly encourage you to watch these sections of Session 1 prior to reading the textbook. The introduction to these concepts will prove invaluable as you make your way through the readings.

☐ Read in The CEH Prep Guide
In *The CEH Prep Guide: The Comprehensive Guide to Certified Ethical Hacking*, read the following chapters.
- Chapter 4 (“Footprinting”): This chapter discusses the various types footprinting. Footprinting is the first of phase of attack. Footprinting is gathering information about a network to target networks or systems.
- Chapter 5 (“Scanning”): This chapter discusses scanning—the second phase in an attack. Scanning involves discovering open ports and finding applications vulnerable to hacking.
Review Questions

Hands-On Labs—Footprinting
In *Hands-On Information Security Lab Manual*, do the following modules:
- Module 1A – Footprinting Activities Using Microsoft Windows
- Module 1B – Footprinting Activities Using Linux Systems

These modules will provide you with hands-on knowledge of how to perform footprinting in Microsoft Windows and Linux environments.

Week 3
Pre-Attack Planning
This domain will provide an overview of penetration testing, footprinting, WHOIS, scanning and enumeration. You will learn the reconnaissance techniques that hackers use to target and exploit networks.

Competency 426.4.2: Pre-Attack Planning
The graduate evaluates techniques used in footprinting and implements industry best practices to protect against this type of information asset vulnerability.

Enumeration and System Hacking
In this section, you will learn about enumeration. Enumeration involves looking for user account information, system groups and roles, passwords and unprotected shares. You will learn about the kinds of attacks that hackers use to compromise an organization’s information system.

As you review this material, take notes and attempt to answer the following questions:
- What are some common enumeration tools?

You should be familiar with the following hacking techniques/tools:
- Password guessing
- Password cracking
- Keystroke loggers
- Keyloggers
- Rootkits
- File hiding

LearnKey—Enumeration and Password Cracking
Watch these three sections from session 2:
- Section B: Enumeration
- Section D: Password Cracking
- Section E: Ownership Privileges

This section will introduce you to some pretty interesting concepts. You will learn what enumeration is, what some basic NET commands are, how to use DumpSEC, and how to perform SuperScans. In the “Password Cracking” section, you will learn about authentication, predictable passwords, cracking methods, securing passwords and cracking passwords. After you finish viewing these sections, you will be able to visualize
many of the concepts you are reading about. Be sure you do the labs located within the session, as well as the hands-on labs at the end of this topic area.

☐ **Read in The CEH Prep Guide**

In *The CEH Prep Guide: The Comprehensive Guide to Certified Ethical Hacking*, read the following chapters:

- Chapter 6 ("Enumerating"): This chapter discusses enumerating—the third phase in an attack. Enumerating involves looking for user account information, system groups and roles, passwords, and unprotected shares.
- Chapter 7 ("System Hacking Techniques"): This chapter discusses system hacking techniques—password cracking, keyloggers and rootkits.

☐ **Review Questions**


☐ **Hands-On Labs—Scanning and Enumeration**

In *Hands-On Information Security Lab Manual*, do the following modules:

- Module 2A – Scanning and Enumeration on Microsoft Windows Systems
- Module 2B – Scanning and Enumeration on Linux Systems

These modules will provide you with hands-on knowledge of how to perform scanning and enumeration on Microsoft Windows and Linux Systems.

---

**Week 4**

**System Hacking**

This domain provides an overview of password cracking hacking techniques, sniffing, Trojans, worms, viruses, and other exploits. You will learn the various attack techniques and tools that hackers use to exploit networks; and techniques on how to counter the attacks.

As you are working through the activities in this section look for answers to these questions:

- What is a Trojan horse and how is it distributed?
- What is a RAT, how is it related to a backdoor, or is it even related?
- What types of tools and commands are out there to help you find Trojans, back doors, and sniffers?

**Competency 426.4.3: System Hacking**

The graduate evaluates various network system hacking counter-techniques.

**Trojans, Backdoors, and Sniffers**

In this section, you will learn about the various techniques hackers use to hack into systems.

You should be able to differentiate between the following:

- Trojans and backdoors
- Viruses
- Worms
- Sniffers
LearnKey—Trojans and Sniffers
Watch these two sections from session 2:
- Section F: Trojan Horses
- Section G: Sniffers

In these sections, you will learn about Trojan horses—not the same Trojan horses you remember from history class, but in theory it is a similar concept. You will also learn about sniffers, vulnerability protocols, sharing, FTP logon packets, and e-mail authentication packets. Watching the lessons will shed some light on what all of this stuff means and why it is so important to be familiar with these concepts in hacking scenarios. These lessons will give you a great foundation for the readings that follow this activity.

Read in The CEH Prep Guide
In The CEH Prep Guide: The Comprehensive Guide to Certified Ethical Hacking, read chapter 8 (“Trojans, Backdoors, and Sniffers”). This chapter discusses various Trojans, backdoors, and sniffers, and how they aid hackers in gaining access to systems.

Review Questions

Hands-On Labs—Operating System Vulnerabilities and Resolutions
In Hands-On Information Security Lab Manual, do the following modules:
- Module 3A – Microsoft Windows Server Vulnerabilities
- Module 3B – Linux Systems Vulnerabilities

These modules will provide you with hands-on knowledge on how to identify vulnerabilities in Windows and Linux Systems.

Sniffers, Denial-of-Service Attacks, and Session Hijacking
In this section, you will learn about the various techniques hackers use to hack into a system, "own" a system completely, and cover their tracks. Denial–of-service (DoS) attacks are very real. Ever been to a website that seems to take forever to load? What do you suppose causes that delay? Could it be a DoS attack? Could it be session hacking? These are the types of questions you should be able to answer as an ethical hacker.

You should be familiar with the following hacking techniques:
- Denial of service (DoS)
- Distributed denial of service
- Session hijacking

You should be able to answer the following questions:
- What are some of the measures that can be taken to prevent DoS attacks?
- What are the names of some session hijacking tools?

LearnKey—Poisoning and DoS Attacks
Watch these two sections from session 3:
- Section A: ARP, MAC, and DNS
- Section B: DoS Attacks
When you are done with these two sections you should know the difference between ARP spoofing, ARP poisoning, intranet poisoning, DNS poisoning, proxy server poisoning, and DNS cache server poisoning. You will also learn what a DoS attack is, what the different types and methods of these attacks are, and what the difference between a Smurf and SYN attack is.

☐ Read in The CEH Prep Guide

In *The CEH Prep Guide: The Comprehensive Guide to Certified Ethical Hacking*, read chapter 9 (“Denial-of-Service Attacks and Session Hijacking”). This chapter discusses DoS and session hijacking attacks. A DoS attack is an assault on an information system in which damage can occur to system operations without the attacker gaining access to the system. Session hijacking is a powerful intrusion into a communication session between hosts where an attacker takes over one end of the transmission and replaces a valid, authorized user.

☐ Review Questions


Week 5

System Hacking

This domain provides an overview of password cracking hacking techniques, sniffing, Trojans, worms, viruses, and other exploits. You will learn the various attack techniques and tools that hackers use to exploit networks, as well as techniques on how to counter the attacks. As you are working your way through this section, we encourage you to take notes in your notebook. You may want to create a chart of sorts. The chart would have columns for the operating system, the scanning tool used, a description of what the tool does, and a description of how to use the tool. This handy reference will allow you to find what you need for a particular hacking scenario quickly.

Competency 426.4.3: System Hacking

The graduate evaluates various network system hacking counter-techniques.

**Linux and Automated Security Assessment Tools**

In this section, you will learn about various Linux hacking tools used to compromise an organization’s information system.

You should be familiar with the following tools:

- Linux network scanning tools
- Linux hacking tools
- Linux security tools

☐ LearnKey—Scanning Tools

This section will introduce you to some Windows-based scanning tools. You will be shown the ping command, what an Angry IP scanner is, what Nmap is, IP spoofing, and MBSA. Be sure to take notes on how to do each of the things presented in the lessons. Make sure you try what is demonstrated to ensure you have a feel for how it works, rather than just the theory. If you practice, you will remember it better!
Watch this section from session 2:
- Section A: Mastering Scanning Tools

- □ Read in The CEH Prep Guide
  In *The CEH Prep Guide: The Comprehensive Guide to Certified Ethical Hacking*, read chapter 11 ("Linux Hacking Tools"). This chapter discusses some popular Linux hacking tools.

- □ Review Questions

  Use your notebook to record your answers for use in reviewing later on.

- □ Hands-On Labs—Network Security Tools and Technologies
  In *Hands-On Information Security Lab Manual*, do the following modules:
  - Module 4A – Microsoft Windows Network Security Tools and Technology
  - Module 4B – Linux Network Security Tools and Technology

  These modules will provide hands-on knowledge on how to use various Microsoft Windows and Linux tools to monitor and detect system-level and network attacks.

**Physical Security and Social Engineering**
In this section, you will learn about the non-technical techniques that hackers use to gain unauthorized access to information systems—social engineering and threats to physical security.

You should be familiar with the following social engineering concepts:
- Reverse social engineering
- Phishing
- Identity theft

As you review this material, take notes and attempt to answer the following questions:
- What are some typical threats to physical security?
- How can you defend against social engineering attacks?

- □ LearnKey—Social Engineering
  Social engineering includes concepts such as dumpster diving, shoulder surfing (aka. looking over someone’s shoulder), eavesdropping, phishing, identity theft, and other problematic access issues. The sections in this session will provide you a fantastic overview and insight into these concepts prior to your readings. We strongly encourage you to take notes as you watch.

  Watch these two sections from session 3:
  - Section C: Social Engineering
  - Section D: Advanced Social Engineering

- □ Read in The CEH Prep Guide
  In *The CEH Prep Guide: The Comprehensive Guide to Certified Ethical Hacking*, read chapter 12 ("Social Engineering and Physical Security"). This chapter discusses the social and physical approaches to compromising networks, and ways to mitigate these kinds of attacks.
Review Questions

Use your notebook to record your answers for use in reviewing later on.

Hands-On Lab—Information Security Management

This module will provide hands-on experience on how to examine information security policies for correctness, completeness, and appropriateness.

LearnKey—Session 5
This session covers six sections. The sections range from implementing physical security to buffer overflows. As always, we recommend you take the pretest to determine which sections are where you may be a bit weaker in your competence. Watch the appropriate sections, do the labs, and then do the posttest at the end.

Week 6
Hacking Web Servers
This domain focuses on how to identify known web server vulnerabilities, manage web server patch/upgrade policies, and learn best practices and techniques for hardening a web server.

Competency 426.4.5: Hacking Web Servers
The graduate identifies known Web server vulnerabilities and demonstrates industry best practices to protect against this type of threat.

Web Server Hacking, Web Application, and Database Attacks
In this section, you will learn about web infrastructure, the basic function of web servers, and common web server vulnerabilities. You will also learn about common vulnerabilities of web applications, including SQL injection testing, attacks, prevention, remediation and tools.

As you review this material, take notes and attempt to answer the following questions:

- What are some common web server and web application vulnerabilities?
- What are some countermeasures than can be used to mitigate web server and web application vulnerabilities?
- What are some common SQL injection attacks?
- What are some ways to prevent SQL injection attacks?

LearnKey—Web Servers: Hacking, Applications, and Passwords
Watch these four sections from session 3:
- Section F: Web Servers
- Section G: Hacking Web Servers
- Section H: Web Applications
- Section I: Cracking Web Passwords
These four sections will give you an excellent introduction and emersion into web vulnerabilities, functionality, password cracking, and applications. There is quite a bit of information presented in these lessons, so take notes. Some of the things you should be looking for include types of attacks, how to manage patches, countermeasures and server hardening, attack prevention, and different types of authentication. We strongly encourage you to watch these lessons. After you finish the lessons, do the labs and posttest when you have completed all of session 3.

☐ **Read in The CEH Prep Guide**

☐ **Review Questions**

Use your notebook to record your answers for use in reviewing later on.

☐ **Hands-On Lab—Security Maintenance**
In *Hands-On Information Security Lab Manual*, do the following modules:
- Module 5A – Windows Security Maintenance
- Module 5B – Linux Security Maintenance

These modules will provide hands-on knowledge on how to configure and monitor event logs, and how to capture and analyze network traffic on Microsoft Windows and Linux systems.

**Hacking Web Application Vulnerabilities**
This domain focuses on web application vulnerabilities, penetration testing and SQL injection vulnerabilities.

**Competency 426.4.6: Web Application Vulnerabilities**
The graduate identifies common web application vulnerabilities and uses industry best practices to protect against this type of threat.

**Web Server Hacking, Web Application, and Database Attacks**
In this topic area you will be learning about SQL injections and attacks. You will also be learning about different types of web application vulnerabilities. If you have not had prior database experience, some of the concepts may not make much sense. We strongly encourage you to visit the learning community to get suggestions for some database exercises to bring you up to snuff.

☐ **LearnKey—SQL**
Watch these two sections from session 4:
- Section A: SQL Injections
- Section B: SQL Attacks

SQL attacks, be it injections or attacks that retrieve records, are a little scary. It is amazing what hackers can do with a little SQL knowledge. This lesson will give you a firsthand look
at the types of attacks that are possible. You will read more about these in the activities that follow. We strongly encourage you to take the time to view these lessons. It will bring the concept of SQL attacks into context.

☐ Read in The CEH Prep Guide
In *The CEH Prep Guide: The Comprehensive Guide to Certified Ethical Hacking*, read the following chapters.
- Chapter 14 (“SQL Injection Vulnerabilities”): This chapter discusses popular and effective attacks against database applications on web servers—SQL injection. This type of attack takes advantage of SQL server vulnerabilities.
- Chapter 10 (“Penetration Testing Steps”): This chapter provides a high-level review of the steps in penetration testing, and discusses various penetration methodologies.

☐ Review Questions

Use your notebook to record your answers for use in reviewing later on.

**Week 7**

**Wireless Hacking**

This domain provides an overview of cryptography, wireless hacking, evading IDSs, honeypots, firewalls, wireless network attacks, DoS, and session hijacking. You will learn how hackers exploit wireless networks and how to mitigate wireless vulnerabilities.

**Competency 426.4.7: Wireless Hacking**
The graduate evaluates industry best practices for securing a wireless network, identifies the threats to wireless security, and associates threats with known countermeasures.

**Cryptographic Attacks and Defenses**
In this section, you will learn about cryptography—the art and science of hiding the meaning of a communication from unintended recipients.

As you review this material, you should become familiar with the following concepts:
- Symmetric Key Cryptography
- Public Key Cryptography
- Public Key Certificates
- Password Cracking Tools and Countermeasures

☐ LearnKey—Hijacking and Wireless Attacks
Watch this section from session 3:
- Section E: Session Hijacking

Watch these five sections from session 4:
- Section C: Wireless Vulnerabilities
- Section D: WEP Attacks
- Section E: WPA and EAP
- Section F: Viruses and Worms
• Section G: Physical Security Policies

One of the things that makes this particular section great is the description of the difference between hijacking and spoofing. People often times confuse these two concepts.

☐ Read in The CEH Prep Guide
In The CEH Prep Guide: The Comprehensive Guide to Certified Ethical Hacking, read the following chapters.
• Chapter 15 (“Cryptography”): This chapter discusses symmetric key cryptography (private key) and public key cryptosystems.
• Chapter 16 (“Cracking Web Passwords”): This chapter discusses various techniques for cracking web passwords.

☐ Review Questions
• In The CEH Prep Guide: The Comprehensive Guide to Certified Ethical Hacking, complete the section of “Review Questions” in chapters 15 and 16.
• Use your notebook to record your answers for use in reviewing later on.

☐ Hands-On Labs—File System Security and Cryptography
In Hands-On Information Security Lab Manual, do the following modules:
• Module 7A – Microsoft Windows File System Security
• Module 7B – Linux File System Security

These modules will provide hands-on knowledge on how to apply various cryptographic techniques (e.g., digital certificates using Microsoft Windows and Linux systems).

☐ LearnKey—Session 6
Watch these six sections from session 6:
• Section A: Cryptography
• Section B: Symmetric Cryptography
• Section C:Multi-Hat Hacking
• Section D: Computer Forensics
• Section E: Hack Prevention
• Section F: Security Policies

This will take you some time to get through. The concepts presented in some cases will be review in other cases; you may not have seen them before. We recommend you take the pretest to see what you already know. The pretest will recommend sections to watch. After watching the sections you choose, be sure to complete the labs and the posttest at the end. If are not feeling 100% comfortable with some of the content, go back and review the textbook, hands-on labs, and exercises within those topic areas to better solidify your competence. If you get stuck or have questions, post a question in the learning community or ask the course of study mentor (aclarkson@wgu.edu) directly.

Wireless Technologies, Security, and Attacks
In this section, you will learn about wireless threats, wireless hacking tools, and securing wireless LANs.
As you review this material, you should be familiar with the following concepts:
- IEEE 802.11 family
- WAN operational modes
- Wireless application protocol (WAP)
- Wired equivalent privacy (WEP)
- Firewall architectures
- Intrusion detection and protection systems
- Honeypots

You should be able to answer the following questions:
- What are some WLAN threats?
- What are some common wireless hacking tools?
- What are some strategies used to secure wireless LANs?

☐ Read in The CEH Prep Guide
In The CEH Prep Guide: The Comprehensive Guide to Certified Ethical Hacking, read chapter 17 (“Wireless Network Attacks and Countermeasures”). This chapter discusses various wireless network attacks and the countermeasures that can be implemented to mitigate these kinds of attacks.

☐ Review Questions

Week 8
Wireless Hacking
This domain provides an overview of cryptography, wireless hacking, evading IDSs, honeypots, firewalls, wireless network attacks, DoS, and session hijacking. You will learn how hackers exploit wireless networks and how to mitigate wireless vulnerabilities.

Competency 426.4.7: Wireless Hacking
The graduate evaluates industry best practices for securing a wireless network, identifies the threats to wireless security, and associates threats with known countermeasures.

IDS, Honeypots, and Firewalls
In this section, you will learn about different approaches to protecting a network and associated computing resources—firewalls, intrusion detection systems, and honeypots.

As you read through this material, you should become familiar with the following concepts:
- Proxy firewall
- Packet level filtering firewall
- Stateful inspection firewall
- Host-based IDS
- Network-based IDS

You should be able to answer the following questions:
- What techniques are used to breach and bypass firewalls?
- What are the three principal approaches to IDS detection and analysis?
Read in The CEH Prep Guide
In *The CEH Prep Guide: The Comprehensive Guide to Certified Ethical Hacking*, read chapter 18 (“Firewalls, Intrusion Detection Systems, and Honeypots”). This chapter discusses three popular network defenses: firewalls (perimeter guard), intrusion detection system (analyzes network traffic), and honeypots (used as decoys once an intruder has breached the network).

Review Questions

Hands-On Labs—Computer Forensics
In *Hands-On Information Security Lab Manual*, do the following modules:
- Module 8A – Forensics Data Collection
- Module 8B – Forensics Data Analysis and Reporting

These labs will provide hands-on knowledge of computer forensics. You will gain experience preparing and collecting forensics, as well as analyzing and reporting forensics information.

Buffer Overflow, Viruses, and Worms
In this section, you will learn various kinds of malware, viruses, worms and buffer overflow exploits, and how they are used for hacking purposes.

As you read through this material, you should become familiar with the following concepts:
- Differences between viruses and worms
- Virus Life Cycle
- Buffer Overflows

Read in The CEH Prep Guide
In *The CEH Prep Guide: The Comprehensive Guide to Certified Ethical Hacking*, read chapter 19 (“Viruses, Worms and Buffer Overflows”). This chapter defines the various types of viruses, worms buffer overflow exploits, and how they are used for hacking purposes.

Review Questions

Conclusion
Congratulations! Upon completion of the activities in this course of study, you have already successfully accomplished the goals of mastering the competencies set forth by WGU. While the term “hacking” does have negative connotations, “ethical hacking,” as you have discovered, is substantially different. Ethical hackers typically try to uncover three key areas of vulnerability: first, information that an unethical hacker might be able to get to; second, what an unethical hacker can do with that information; and finally, what might be done to alert stakeholders about a break-in. By studying the chapters, lesson reviews, and the hands-on practice associated with each competency, you have acquired the knowledge and skills necessary for passing the HAC2.
One of the key difficulties some find with this course of study is their lack of exposure to multiple different types of operating systems. If you have only worked with Windows machines, trying to understand the different Linux distributions and Macintosh operating systems can often be a challenge. At the beginning of this course of study, there is a description of VMWare with a recommendation to purchase a copy and try installing multiple operating systems simultaneously. You can read about how to do all these things on different operating systems, but, if you do not actually try it, it will not “stick,” and when the time comes to complete a task on one of these operating systems while on the job, you might not be able to.

**Review of Major Points**
As demonstrated above, this course of study covers six competencies within the Hacking subdomain area. The competencies and their associated chapters and modules are:

**Competency 426.4.1: Ethics and Legality**
The graduate analyzes ethical and legal issues related to the unauthorized or unwanted access into and of information assets, including types of hacking technologies and related skills.

*The CEH Prep Guide: The Comprehensive Guide to Certified Ethical Hacking*
- Chapter 1 (“Introduction to Ethical Hacking”)
- Chapter 2 (“Legality and Ethics”)
- Chapter 3 (“Penetration Testing for Business”)

**Competency 426.4.2: “Pre-Attack” Planning**
The graduate evaluates techniques used in footprinting and implements industry best practices to protect against this type of information asset vulnerability.

*The CEH Prep Guide: The Comprehensive Guide to Certified Ethical Hacking*
- Chapter 4 (“Foot Printing”)
- Chapter 5 (“Scanning”)
- Chapter 6 (“Enumerating”)
- Chapter 7 (“System Hacking Techniques”)

*Hands-On Information Security Lab Manual*
- Module 1A and 1B – Footprinting
- Module 2A and 2B – Scanning and Enumeration

**Competency 426.4.3: System Hacking**
The graduate evaluates various network system hacking counter-techniques.

*The CEH Prep Guide: The Comprehensive Guide to Certified Ethical Hacking*
- Chapter 8 (“Trojans, Backdoors and Sniffers”)
- Chapter 9 (“Denial-of-Service Attacks and Session Hijacking”)
- Chapter 11 (“Linux Hacking Tools”)
- Chapter 12 (“Social Engineering and Physical Security”)

*Hands-On Information Security Lab Manual*
- Module 3A and 3B – Operating System Vulnerabilities and Resolutions
- Module 4A and 4B – Network Security Tools and Techniques
- Module 6A – Information Security Management

**Competency 426.4.5: Hacking Web Servers**
The graduate identifies known web server vulnerabilities and demonstrates industry best practices to protect against this type of threat.

*The CEH Prep Guide: The Comprehensive Guide to Certified Ethical Hacking*
- Chapter 13 (“Web Server Hacking and Web Application Vulnerabilities”)

19
**Hands-On Information Security Lab Manual**
- Module 5A and 5B – Security Maintenance

**Competency 426.4.6: Web Application Vulnerabilities**
The graduate identifies common web application vulnerabilities and uses industry best practices to protect against this type of threat.

*The CEH Prep Guide: The Comprehensive Guide to Certified Ethical Hacking*
- Chapter 14 (“SQL Injection Vulnerabilities”)
- Chapter 10 (“Penetration Testing”)

**Competency 426.4.7: Wireless Hacking**
The graduate evaluates industry best practices for securing a wireless network, identifies the threats to wireless security, and associates threats with known countermeasures.

*The CEH Prep Guide: The Comprehensive Guide to Certified Ethical Hacking*
- Chapter 15 (“Cryptography”)
- Chapter 16 (“Cracking Web Passwords”)
- Chapter 17 (“Wireless Network Attacks and Countermeasures”)
- Chapter 18 (“Firewalls, Intrusion Detection Systems, and Honeypots”)
- Chapter 19 (“Viruses, Worms, and Buffer Overflows”)

**Hands-On Information Security Lab Manual**
- Module 7A and 7B – File System Security and Cryptography
- Module 8A and 8B – Computer Forensics

**Transfer and Application**
Acquiring knowledge from textbooks is only part of the learning process. There are some pretty cool concepts in this course of study, many of which you will most likely use on the job. Skills you may have learned should include hardening systems, collecting data evidence, setting up honeypots, preventing DoS attacks, etc. Completing this course of study means you have acquired offensive and defensive hacking skills—skills that are invaluable to an employer looking to secure their networks and systems. New vulnerabilities are exposed all the time; this means you will need to keep your knowledge of hacking, networking systems, and security current and up-to-date.

They say once you ride a bike, you can always ride a bike. The same is not necessarily true of being an ethical hacker. Keep current, keep up-to-date, and keep malicious hackers out of your networks and systems.

The ultimate goal of learning is to turn knowledge into skills that can be readily applied in the practical field. The following are some recommendations for transferring knowledge acquired through textbooks into practical skills real work environment:

**Emphasize course of study activities**
Practice makes perfect. Hands-on practices help turn short-term memory into long-term memory. Finally, personal experiences also help reinforce learning outcomes.

**Research solutions through various channels**
There are many ways to research solutions on issues associated with wireless security, including the use of Internet to look for solutions that are not addressed in textbooks. Since new issues may appear in the real work environment, textbooks are not good enough to cover all of them. Learning through research helps you explore new solutions to new problems.
Collaborate and cooperate with peers or other students
There are different ways of learning, including the use of cooperation and collaboration to facilitate learning processes. Working with your coworkers, fellow classmates, and even with other students in the learning community will definitely exert positive impact on your learning outcomes.

Participate and contribute to online learning community
Finally, it is a good practice to participate and/or contribute to the discussion threads in the Systems Security Learning Community. Many students, besides the learning community facilitator, are good partners for your mastering ethical hacking competencies.

Next Steps: Request a Referral for the Assessment
Once you have completed all the tasks associated with the competencies, preassessments, readings, activities, hands-on practices, and practice exams, you should prepare to schedule the HAC2 assessment at a Prometric testing center.

The following are the steps necessary for making arrangements to take the actual assessment:
1. Request a referral for the HAC2 assessment through your AAP.
2. Once your mentor has approved the referral, you will receive a voucher number by e-mail from the Assessment Department.
3. Using the voucher number, you will need to schedule the actual date for the assessment through your nearest Prometric Testing Center.
4. After the exam, scan your test results, and submit to the Assessment Department via vendorassessments@wgu.edu, and copy (CC) your mentor.

Feedback
If you wish to provide feedback on this Course of Study, please contact Gwendolyn Britton at gbritton@wgu.edu.