This course supports the assessments for VUT2. The course covers 4 competencies and represents 2 competency units.

# Introduction

This course is aligned to the VUT2 performance assessment.

## Overview

The Security Planning and Management domain will prepare you to evaluate system and network penetration. Each domain is broken down into sub-domains and competencies. Within the Vulnerability Assessment Course of Study there is one subdomain, which has four competencies. You will evaluate vulnerabilities and analyze security tests and evaluate threats posed by social engineering. Your coursework at WGU is designed to help you to gain a broad overview of the field of vulnerability with a fundamental understanding of key concepts and principles.

Learning these concepts will require that you complete all of the suggested activities contained within this course of study. You are strongly encouraged to work through all activities to give you first-hand experience with many of the concepts.

Watch the following introduction video for this course:

*Note: To download this video, right-click the following link and choose "Save as...": [download video]*

## Competencies

This course provides guidance to help you demonstrate the following 4 competencies:

- **Competency 427.2.1: System and Network Penetration Testing**
  The graduate recognizes common threats, identifies practical and legal issues of system and network penetration testing, and uses best practices to evaluate penetration tests.

- **Competency 427.2.2: Vulnerability Assessment Evaluation**
  The graduate evaluates vulnerability assessments for risks, security threats, and system and network testing.

- **Competency 427.2.3: Penetration Analysis**
  The graduate evaluates security tests and best practices for analyzing the results of penetration testing of a network system.

- **Competency 427.2.4: Advanced Social Engineering**
  The graduate evaluates threats posed by social engineering, and determines common techniques and methods to use when conducting or protecting against social engineering.

## Course Instructor Assistance

As you prepare to successfully demonstrate competency in this subject, remember that course
instructors stand ready to help you reach your educational goals. As subject matter experts, mentors enjoy and take pride in helping students become reflective learners, problem solvers, and critical thinkers. Course instructors are excited to hear from you and eager to work with you.

Successful students report that working with a course instructor is the key to their success. Course instructors are able to share tips on approaches, tools, and skills that can help you apply the content you’re studying. They also provide guidance in assessment preparation strategies and troubleshoot areas of deficiency. Even if things don’t work out on your first try, course instructors act as a support system to guide you through the revision process. You should expect to work with course instructors for the duration of your coursework, so you are welcome to contact them as soon as you begin. Course instructors are fully committed to your success!

Preparing for Success

The information in this section is provided to detail the resources available for you to use as you complete this course.

Watch the following Getting Started video for this course:

Note: To download this video, right-click the following link and choose “Save as...”: download

Learning Resources

The learning resources listed in this section are required to complete the activities in this course. For many resources, WGU has provided automatic access through the course. However, you may need to manually enroll in or independently acquire other resources. Read the full instructions provided to ensure that you have access to all of your resources in a timely manner.

Automatically Enrolled Learning Resources

You can access the learning resources listed in this section by clicking on the links provided throughout the course. You may be prompted to log in to the WGU student portal to access the resources.

SkillSoft and Books 24x7

You will access SkillSoft items at the activity level within this course. For more information on accessing SkillSoft items, please see the "Accessing SkillSoft Learning Resources" page.

The following e-texts are available to you free of charge, but you may purchase hard copies at your own expense through a retailer of your choice. If you choose to do so, please use the ISBN listed to ensure that you receive the correct edition.

The following Books24x7 e-texts will be used in this course:

Pacing Guide
The pacing guide suggests a weekly structure to pace your completion of learning activities. It is provided as a suggestion and does not represent a mandatory schedule. Follow the pacing guide carefully to complete the course in the suggested timeframe.

Note: This pacing guide does not replace the course. Please continue to refer to the course for a comprehensive list of the resources and activities.

Advanced Social Engineering
In this section you will learn about the threats posed by social engineering and the common techniques and methods you can use when conducting tests to protect against social engineering. Identity theft is a rapidly growing social engineering problem for companies and individuals. There are specific techniques that security professionals can use to counteract social engineering.

As you are reviewing the learning material, reflect on these questions:

- What are intruder techniques for physical access to information assets?
- What are intruder techniques for network and information system access?
- How can you overcome resistance to social engineering by employees and stakeholders?
- What are common types of planning documents for social engineering?
- How would you describe techniques to perform and counteract social engineering?
- Why is breaching physical security a social engineering threat?
- How would you explain common methods to protect against social engineering?

Social Engineering Techniques
Social engineering is accomplished by malicious hacker(s) manipulating people into providing confidential information or unconsciously assisting in the attack. This is done one step at a time by asking questions and gathering information. It is an art form that does not require the hacker to be adept at computers, but certainly requires the ability to easily manipulate people and situations.

As you review the learning materials, reflect on the following questions:

- What methods can be used to prevent social engineering?
- How can social engineering be counteracted?
- What are intruder techniques for network social engineering?
- Why are planning documents important in defending against social engineering?
- How can threats from social engineering be evaluated?
Social Engineering

Read the following:

- chapter 34 ("Social Engineering") in Defeating the Hacker
- chapter 219 ("Social Engineering the Human Factor in Information Assurance") in Information Security Management Handbook
- "Social Engineering: Manipulating the Source"
- "Understanding and Auditing"
- "War Dialing"

Pay particular attention to the threats posed by social engineering and the methods for protecting against social engineering, such as physical access techniques, intruder technique for network access, planning documents addressing social engineering, and counteracting social engineering.

Share Your Thoughts: Social Engineering

You have probably heard that knowledge is power. In social engineering, perpetrators are aware of the great value that knowledge (i.e., information) can have. Since humans are typically the weakest link in an information security context, many perpetrators use various tactics to gain confidential information from unsuspecting people.

Take a moment to think about some of the different social engineering techniques you have learned about. What are some ways to combat these threats? Share your thoughts on the message board with your peers.

RVUT Task 1 Performance Task

Complete the following in Taskstream.

- VUT2: RVUT Task 1

For details about this performance assessment, see the "Assessment" tab in this course.

Vulnerability Assessment

In this section you will learn about common threats and the practical and legal issues of system and network penetration testing. The best way to protect your organization's IT (information technology) security is to try to break into it. Penetration testing is the best way to verify good security.

Generally, penetration testing is done by a third-party company that specializes in penetration testing, and it involves a complete review of legal and procedural issues prior to penetration testing.

System Penetration and Analysis Testing

System penetration testing is somewhat controversial in that you become a white hat (ethical hacker) and test a system as if you were a black hat hacker (i.e., a bad guy). There are some
managers and executives that object to penetration testing. Well-structured penetration testing exposes the vulnerable, weak areas of a system so that after an analysis is complete, issues can be addressed, and countermeasures applied to ensure the system cannot be successfully penetrated.

As you review the learning materials, reflect on the following questions:

- What are common automated network penetration tools?
- How would you explain a legal framework for a penetration test?
- What are web application threats?
- Why are penetration test plans important?
- How would you describe best practices for penetration testing?

**Protecting Your Website and Penetration Testing**

Read the following chapters in *Defeating the Hacker*:

- chapter 12 (“Protecting Your Web Site”)
- chapter 14 (“Penetration Testing”)

Read the following chapter in *The Best Damn IT Security Management Book Period*:

- chapter 16 (“Legal Principles for Information Security Evaluators”)

Pay particular attention to identifying practical and legal issues of penetration testing, such as common automated network penetration testing tools, penetration test legal framework, web application threats, penetration test plans, and industry-best practices for penetration testing. **Collecting Current and Relevant Information**

Find out more about system and network penetration testing. Visit the following websites to build a reference library about this topic:

- [Information Assurance Support Environment](#)
  This website has federal agencies’ security practices, links to the National Security Agency configuration guides, and common criteria evaluation and validation schemes.
- [Security Technical Implementation Guides](#)
  This website provides penetration test policies, security reviews, and security checklists from the federal government.
- [Security Standards: "Standards for Information Security Management”](#)
  This website has CISCO security standards and ISO objectives.
- ["Management Planning Guide for Information Systems Security Auditing”](#)
  This document is a planning guide developed by The National State Auditors Association and the U.S. General Accounting Office.

Using the websites, create your own vulnerability “cheat sheet.” For each of the five items listed, identify at least two important items to keep in mind when conducting a vulnerability assessment. Then post a response to the message board and indicate which of these five items...
you feel is most helpful when performing a vulnerability assessment.

Share Your Thoughts: Vulnerability Assessment

A vulnerability assessment is an important tool that organizations can use to identify potential exploits or opportunities for intrusion. Every system and network environment is different. As such, the results from a vulnerability assessment will vary from organization to organization.

You have had the opportunity to learn what vulnerability assessments are and why it is important to perform them periodically. What are some of the steps involved in conducting a vulnerability assessment? Are there any automated tools that can assist with the process? Share your thoughts on the message board with your peers.

Vulnerability Assessment Evaluation

In this section you will learn about vulnerability assessments for risk, such as security threats and system and network testing. Vulnerability assessments help organizations identify security risks and liabilities in systems, networks, and applications. There are specific steps involved in conducting a vulnerability assessment. Organizations must exercise due diligence to protect information security assets, and vulnerability assessments are an accepted method to assess risk and protect information assets.

Vulnerability Assessment Evaluation

Vulnerability assessments analyze a network system to identify possible areas of exposure for the network. A vulnerability assessment may include the operating system, firewalls, routers and switches, connectivity, wireless and remote access, security policies, and network architecture. The goal is to mitigate risk and identify countermeasures.

As you are reviewing this learning material, reflect on these questions:

- How would you describe vulnerability assessment and penetration testing?
- How would you evaluate a vulnerability assessment for issues related to system and network testing?
- What are the steps for conducting a vulnerability assessment?
- What risks are involved in an internal vulnerability assessment?
- What types of threats would be identified in a vulnerability assessment?
- Why would an organization outsource vulnerability assessments?
- What are the steps in developing a vulnerability assessment with a third-party vendor?

Tying It All Together

Read the following chapters and article in *The Best Damn IT Security Management Book Period*:

- chapter 1 ("Windows of Vulnerability")
- chapter 6 ("Going Further")
- chapter 2 ("Vulnerability Assessment 101")
- chapter 11 ("Tying it All Together")
Pay particular attention to evaluating assessments for risks and threats, such as

- system and network testing,
- the steps in a vulnerability assessment,
- the risks in conducting a vulnerability assessment,
- the types of threats a vulnerability assessment identifies, and
- a third-party vulnerability assessment.

RVUT Task 2 in Taskstream

Complete the following in Taskstream:

- RVUT task 2

For task instructions, evaluation procedures, and scoring rubrics, please go to Taskstream.

Penetration Testing and Analysis

In this section you will learn about evaluating security tests and best practices for penetration testing for network systems. Different types of analyses are used in the industry to prevent breaches due to attacks such as denial of service (DoS) or password cracking. Evaluating physical security is important in preventing social engineering. Utilizing a wide range of security analyses represents best practices in information security assurance. As you are reviewing this learning material, reflect on these questions:

- How would you describe a denial of service security analysis?
- Why is a password-cracking security analysis important?
- Why is an internal penetration security analysis considered to be an industry best practice?
- What are the elements of an external penetration security analysis?
- How would you conduct a router analysis?
- How would you evaluate a test agreement for external and internal penetration testing?

Penetration Analysis

Penetration testing simulates real-life attacks on a network in order to discover and exploit system vulnerabilities. It is better for the organization to discover its weak areas and correct them before a hacker discovers the weakness and compromises the network system or is able to steal sensitive information.

As you review the learning material, reflect on the following questions:

- What are best practices for analyzing penetration testing?
- What are the components of a password-cracking analysis?
- What are the elements of an external penetration security analysis?
- How would a physical security penetration test be evaluated?
- What tools could be used to conduct a penetration analysis?

Practice simulating real-world attacks by discovering and exploiting system vulnerabilities
Penetration Analysis

Read the following chapters in *Information Security Management Handbook*:

- chapter 73 ("A New Breed of Hacker Tools and Defenses")
- chapter 74 ("Hacker Attacks and Defenses")
- chapter 76 ("Insight Into Intrusion Prevention Systems")
- chapter 77 ("Penetration Testing")

Read the following articles:

- "NIST Incident Handling Guide"
- "Information Security Management SANS Audit Checklist"
- "DNS Amplification Attacks"
- "Network Analysis and Optimization Techniques"

Pay particular attention to the evaluation of security tests and best practices, such as

- denial of service security analyses,
- components of password-cracking security analyses,
- elements of external penetration security analyses,
- router analyses,
- firewall analyses,
- intrusion detection system (IDS) security analyses,
- wireless analyses, and
- physical security analyses.

**Share Your Thoughts: Penetration Testing**

A penetration test offers an organization the ability to see how well its security systems live up to a realistic attack. Many security consulting firms provide penetration testing, and such a test can provide a wealth of information to an organization looking to harden its security.

What are some reasons to perform a penetration test? How can this information be used to further secure a network environment? Share your thoughts on the message board with your peers.

**VUT2 Task 3 in Taskstream**

Complete the following in Taskstream:

- VUT2 Task 3

For task instructions, evaluation procedures, and scoring rubrics, please go to Taskstream.

**Final Steps**

Congratulations on completing the activities in this course! This course has prepared you to
complete the assessments associated with this course. If you have not already been directed to complete the assessments, schedule and complete your assessments now.