CYBER RANGE

Active Defense

Course Outline

July 2021

fieldeffect.com

FIELD EFFECT™
Cyber security that keeps business moving.

Active Defense

Course Outline

Course Overview

Active defense is the use of tactics to stop or slow down a hacker and make cyber-based attacks more difficult to carry out. These techniques can be applied to defense strategies and strengthen the Incident Response (IR) to avoid the threat resurfacing. You have been applying active defense tactics already; for example, windows hardening tasks, looking for hidden files, suspicious files or network traffic, and denying traffic with firewall rules. It also introduces some concepts and hands-on, on how to detect, analyze and mitigate/patch vulnerabilities.

Course Prerequisites

Students should have worked with the previous modules in order to complete the tasks, in addition to that some knowledge about kali tools like nmap, dirb and wpscan would be useful.

Workload Expectations

Students should be able to complete the course in an hour. However, the actual time investment will depend on previous knowledge and on time spent on studying the suggested resources and doing optional tasks.

Course Learning Outcomes and objectives

At the end of the course students will be able to:

- Revise previous modules covered
    - Windows Hardening, Suspicious Files, Steganography, Network Analysis, Firewalls, Hashes and Encoding/Decoding
- Detect, Analyze and Mitigate Vulnerabilities
    - Identify, Analyze, Patch and Verify known Vulnerabilities

Course Format

This course recaps the previous modules we worked with, then, introduces active defense tasks which tie up the concepts you have learned. Finally, it discusses Vulnerability Detection , Analysis and Mitigation.

CYBER RANGE

Basic Encoding - Decoding

Course Outline

June 2021

Basic Encoding - Decoding

Course Outline

Course Overview

Encoding is the general technique of replacing characters and symbols with standardized values; this enables different technologies to understand the same meaning, even though they don't necessarily speak the same language. Although encoded data is not readable, encoding does not secure the data (that is encryption). Unfortunately, malicious actors regularly use encoding to minimize the recognition of malware by cyber security tools such as anti-virus scans. Students will learn to identify basic encoding patterns, as well as encode and decode text and files which are important cyber security skills.

Course Prerequisites

A basic understanding of the command line, as presented in the Steganography unit, is required for this course.

Workload Expectations

The student should be able to complete the course in an hour. However, the actual time investment will depend on previous knowledge and on time spent on studying the suggested resources and doing optional tasks.

Course Learning Outcomes and objectives

At the end of the course the student will be able to:

- Recognize common types of encoding: base64, hexadecimal, URL and rot 13
    - Encode and decode simple words using the tool hURL
    - Differentiate encoded values by type
- Encode and decode files
    - Detect combinations of encodings and decode files
    - Apply multiple encoding types

Course Format

The four types of encodings are each introduced in an objective, where the student is guided on how to use the tool hURL. Additional examples are provided as practice. The last objective introduces the common approach of combining encodings, where the student can apply what they have learned.

CYBER RANGE

Linux Command Line Course Outline

v1.0
May, 2023

Linux Command Line

Course Overview

In this course students will learn about the Linux Operating System command line with the goal of getting comfortable with using it and experiencing its superpowers.

Course Prerequisites

Students should be familiar with the file manager to organize their folders and files or have completed the Cyber Range course Linux File Management.

Workload Expectations

The students should be able to complete the course in about 30 minutes. However, the actual time investment will depend on previous knowledge and background.

Course Learning Outcomes and objectives

At the end of the course the students will be able to:

- Describe why one would use the command prompt.
    - Experience some of the superpowers of the command line: convenient and fast
        - Quickly spot a hidden folder
        - Use a wildcard and a pipe
- Use the command prompt comfortably to do some basic tasks:
    - Navigate folders and files using cd

- List folders and files using ls (and arguments)
- View the contents of a file using gedit, eog
- Move, copy and rename files.
- Delete folders and files using rmdir and rm
- Find information about commands using man

Course Format

Each objective briefly explains related concepts and then provides hands-on tasks for the students to practice.

CYBER RANGE

Windows Command Line Course Outline

v1.0
May, 2023

Windows Command Line

Course Overview

In this course students will learn about the Windows Operating System command line (command prompt) with the goal of getting comfortable with using it and experiencing its superpowers.

Course Prerequisites

Students should be familiar with File Explorer to organize their folders and files or have completed the Cyber Range course Windows File Management.

Workload Expectations

The student should be able to complete the course in 30 min. However, the actual time investment will depend on previous knowledge and experience.

Course Learning Outcomes and objectives

At the end of the course the student will be able to:

- Describe why one would use the command prompt.
    - Experience some of the superpowers of the command line: convenient and fast
        - Quickly spot a hidden folder
        - Find the IP address of your computer.
- Use the command prompt comfortably to do some basic tasks:
    - Navigate folders and files using cd

- List folders and files using dir (and arguments)
- View the contents of a file using type
- Move, copy and rename files.
- Delete folders and files using rmdir and del
- Find information about commands using /?

Course Format

Each objective briefly explains related concepts and then provides hands-on tasks for the students to practice.

CYBER RANGE

Linux File Management Course Outline

v1.0
April, 2023

Linux File Management

Course Overview

Students will learn about and practice file management techniques to organize and manage files such as copying, moving, deleting, and searching for files using a Linux Operating System.

Course Prerequisites

Students should be familiar with using a computer and would benefit from having completed the Cyber Range course Introduction to Operating Systems.

Workload Expectations

The students should be able to complete the course in about 30 minutes. However, the actual time investment will depend on previous knowledge and background.

Course Learning Outcomes and objectives

At the end of the course the students will be able to:

- View and search for a file or folder using a file manager.
- Create, copy, move, delete, restore from Trash, and rename files and folders.

Course Format

Each objective briefly explains related concepts and then provides hands-on tasks for the students to practice.

CYBER RANGE

Windows File Management Course Outline

v1.0
April 27, 2023

Windows File Management

Course Overview

Students will learn about and practice file management techniques to organize and manage files such as copying, moving, deleting, and searching for files using a Windows Operating System.

Course Prerequisites

Students should be familiar with using a computer and would benefit from having completed the Cyber Range course Introduction to Operating Systems.

Workload Expectations

The students should be able to complete the course in about 30 minutes. However, the actual time investment will depend on previous knowledge and background.

Course Learning Outcomes and objectives

At the end of the course the student will be able to:

- View and search for a file or folder using File Explorer
- Create, copy, move, delete, restore from Recycle Bin, and rename files and folders.

Course Format

Each objective briefly explains related concepts and then provides hands-on tasks for the students to practice.

CYBER RANGE

Hashes

Course Outline

v1.0
July 09, 2021

Hashes

Course Overview

A hash is like a fingerprint of data: it uniquely identifies a set of data. Any change in the data results in a different hash value (fingerprint). For example, a difference between the original hash value and a freshly recalculated one, immediately indicates that a file had been tampered with. Hashes are an important component of a security strategy, though they are not encodings nor encryption. In this course, students will learn to create hashes and identify common security scenarios where they are used.

Course Prerequisites

Students should have a basic working familiarity with a computer and files, and a basic understanding of the Linux command line, as presented in the Steganography unit.

Workload Expectations

The student should be able to complete the course in an hour. However, the actual time investment will depend on previous knowledge and on time spent on studying the suggested resources and doing optional tasks.

Course Learning Outcomes and objectives

At the end of the course the student will be able to:

- Identify the purpose of a hash
    - Identify its characteristics: fixed-length, not reversible, uniqueness

- Identify common use cases
    - Detect if a file has been modified
    - Add a security layer for storing passwords
- Create hashes
    - Create hashes (md5, SHA)
    - Detect weak passwords with the hashcat tool

Course Format

The student is introduced to the characteristics of hashes by creating hash values using common algorithms, available as tools on the Linux command line. Then, they generate and compare hashes as part of security measures involving files and passwords.

CYBER RANGE

Introduction to Operating Systems Course Outline

v1.0
April, 2023

Introduction to Operating Systems

Course Overview

Students learn about the role of an Operating Systems (OS) in a computer. They will get some background information and hands-on experience with two families of OS: Windows and Linux.

Course Prerequisites

Students should be familiar with using a computer.

Workload Expectations

The student should be able to complete the course in 30 minutes. However, the actual time investment will depend on previous knowledge.

Course Learning Outcomes and objectives

At the end of the course the student will be able to:

- Describe what an OS is
- Name different OS
- Experience the look and feel of different OS

Course Format

In the first objective, students are given a simple analogy for an OS and immediately access two of them to engage them before providing a more robust definition in the second objective. In the

third objective, they are given tasks to do in both OS to appreciate similarities and differences. Finally, in the last objective they are encouraged to see that OS are more than just for general purpose computers.

CYBER RANGE

Malware Awareness Course Outline

v1.0
June, 2023

Malware Awareness

Course Overview

This course raises awareness about malware manifestations students might encounter and security measures they should strive to adopt.

Course Prerequisites

Students should be familiar with a computer and ideally have taken the Windows File Management course.

Workload Expectations

The students should be able to complete the course in about 30 minutes. However, the actual time investment will depend on previous knowledge and background.

Course Learning Outcomes and objectives

At the end of the course the students will be able to:

- Describe how to protect themselves regardless of knowledge of malware.
- Describe adware and ransomware and their symptoms.
- Use the Task Manager to:
    - monitor apps running on their computer;
    - find some apps that get started after the computer powers up;
    - find unexpected apps and terminate them.

Course Format

The first three objective briefly explains related concepts and then provides hands-on tasks for the students to practice. The last objective provides the best practices to follow.

CYBER RANGE

Networking Concepts Course Outline

v1.0
July, 2023

Networking Concepts

Course Overview

In this course students will learn how computers communicate on a network by introducing concepts like IP and MAC address, ARP, ping and hostname and by doing hands-on tasks to gain experience.

Course Prerequisites

Students should be familiar with Windows command prompt and a web browser or have completed the Cyber Range course Windows Command Line.

Workload Expectations

The student should be able to complete the course in 30 min. However, the actual time investment will depend on previous knowledge and experience.

Course Learning Outcomes and objectives

At the end of the course the student will be able to:

- Recognize the architecture and the usage of IP addresses.
    - Differentiate Public and Private IP addresses.
    - Describe different classes of IP addresses.
    - Describe subnet mask and default gateway.
    - Use the command prompt to get the IP address of a device.
- Recognize the architecture and the usage of MAC addresses.
    - Use the command prompt to get the MAC address of a device.
- Differentiate between IP and MAC addresses.

    - Recognize the ARP (Address Resolution Protocol) table.
- Comprehend how two machines in the same network communicate.
    - Identify the ping command and its response.
    - Access a remote website using its IP address.
- Recognize a hostname/domain name.
    - Access remote websites using their hostname/domain name.

Course Format

Each objective briefly explains related concepts and then provides hands-on tasks for the students to practice.

CYBER RANGE

Steganography

Course Outline

June 2021

Steganography

Course Outline

Course Overview

Steganography is the technique of hiding secret data within a file or image. This technique predates the modern era and continues to be used today by individuals and organizations who wish to exchange sensitive information without drawing attention to it. Unfortunately, it is also used by malicious actors to hide malware; therefore, steganalysis is an important skill for cyber security analysts. Students will learn about and apply steganalysis to five types of files and steganography to two file types.

Course Prerequisites

A basic understanding of using a computer is required for this course. A cheat sheet is provided to guide students who have not used a command line.

Workload Expectations

The student should be able to complete the course in an hour. However, the actual time investment will depend on previous knowledge and on time spent on studying the suggested resources and doing optional tasks.

Course Learning Outcomes and objectives

At the end of the course the student will be able to:

- Detect files with hidden data using Notepad, Strings, 7-Zip and Steghide

    - Apply Steganalysis to image, audio, video and executable and zip files
- Hide data in files with 7-zip and Steghide
    - Apply Steganography to an image file using two different methods

Course Format

The topics of steganography and steganalysis for beginners revolve around hiding and extracting data. Students are guided through examples to demonstrate fundamental concepts of applying steganalysis to different types of files, in both a Windows and a Kali virtual machine. The guidance also includes initiating students to the command line with Kali. Additional examples are provided to enable students to put into practice what they have learned.

CYBER RANGE

Suspicious Files and Hidden Folders

Course Outline

June 2021

Suspicious files and Hidden Folders

Course Outline

Course Overview

After this course, the student should be able to search for and identify suspicious files, including files within hidden folders. They should also be able to distinguish between regular hidden files and malicious hidden files.

Course Prerequisites

Basic use of the Windows GUI.

Workload Expectations

The student should be able to complete the course in an hour. However, the actual time investment will depend on previous knowledge and on time spent on studying the suggested resources and doing optional tasks.

Course Learning Outcomes and objectives

At the end of the course the student will be able to:

- View all the folders and files within a folder, including hidden directories/files
- Identify suspicious files from:
    - Location
    - Scheduled tasks
    - High CPU usage

    - File extensions
- Gather information on files and folders to determine the purpose of hidden directories and files.
- Gather information on files and folders to determine the purpose of executable files.

Course Format

The student is given a Windows 10 VM, and the instructions will use the GUI where possible as the audience for this course includes casual PC users. The students are presented with a scenario in which they are given a Windows 10 machine that was used by uncle Joe who is a little too trustworthy of download links. Students are guided through tasks to search, identify, and, if needed, remove suspicious files and hidden folders on a Windows virtual machine while at the same time cyber security concepts are explained. They will use Windows File Explorer, Windows Task Scheduler and Task Manager. Additional non-guided tasks are provided to enable students to put into practice what they have learned.

CYBER RANGE

Windows Hardening

Course Outline

June 2021

Windows Hardening

Course Outline

Course Overview

In this course, students will learn how to better protect a Windows computer system against basic threats and vulnerabilities by identifying security risks and applying standard hardening techniques to mitigate (reduce) those risks.

The course is set up as a hands-on learning experience focused on students who are first introduced to cyber security.

Course Prerequisites

Students should have a basic working familiarity with a Windows computer.

Workload Expectations

The student should be able to complete Lab 1 of the course in an hour. However, the actual time investment will depend on previous knowledge and on time spent on studying the suggested resources and doing optional tasks. Lab 2 is optional.

Course Learning Outcomes and objectives

Upon completion of the course, the students will be able to

- Assess and configure basic Windows Security Settings on a Windows 10 pro machine according to best practices.
    - Auto login (disable) and screensaver settings (set screensaver password)
    - Account Policy Security settings (Password Policy and Account Lockout Policy Settings) based on resources and/ or scenario requirements.
    - Windows Update (automatic update)
    - Windows Defender Firewall settings (default)
    - Virus and Threat Detection (default)
    - Remote access (disable)
- Assess and configure appropriate user accounts and privileges on a Windows 10 computer.
    - Set up user and guest accounts with appropriate user rights to reduce cyber security risks.
    - Disable, delete, or rename user, guest, and administrator accounts to reduce cyber security risks.
- Detect basic security risks and threats and apply the appropriate hardening strategies to mitigate the risks.

Course Format

Students will be presented with two scenarios in which they have to better secure a Windows10 computer based on the information given in the scenario. Each scenario is presented in a lab which contains a Windows10 Virtual Machine (VM). This VM has no access to internet.

In the first lab, the scenario will guide students through basic Windows 10 hardening steps by having the students perform several tasks per step. Resources are provided. If the resource is a link, students are expected to use the internet browser of their own system to access it.

In the second lab students are presented with a new scenario and accompanying VM. The challenges in this lab will be like the first lab. However, the big difference is that there is no guidance; the student must rely on his newly acquired knowledge and skills as well on his research skills to complete the challenge. Students are expected to read the scenario and assess the

security risks. Based on their assessment they determine what strategies they will apply to mitigate these security risks.

CYBER RANGE

Basic Firewalls Course Outline

v1.0
July 14, 2021

Basic Firewalls

Course Outline

Course Overview

Although a basic tool, firewalls can be very effective at defending your computers from attackers when setup correctly. Firewalls are basic network security tools, used to filter incoming and outgoing packets based on pre-set rules. In other words, a rule decides if a packet is blocked or allowed to reach your computer. Firewalls can have default actions for packets that do not match a rule, and the rules can also specify their own unique actions. Students will learn how to create rules, and how to determine the parameters of firewall rules.

Course Prerequisites

Students should have a basic understanding of command line usage, at a similar level to the Steganography unit. Students should also understand packets from the Network Analysis course.

Workload Expectations

The student should be able to complete the course in an hour. However, the actual time investment will depend on previous knowledge and on time spent on studying the suggested resources and doing optional tasks.

Course Learning Outcomes and objectives

At the end of the course, the student will be able to:

- Create firewall rules based off of intended use of a server
    - Set a default behavior for packets that do not match a rule
    - Analyze the services on the server to determine which ports are in use
    - Allow ports for services that should be allowed to receive requests from the network
    - Use source IP and destination ports to write more specific firewall rules

Course Format

The student is asked to secure a web server that hosts a website to track the number of visitors at the local community center every day. They have followed all the password policies; however, the server has been left completely open to the Internet. Someone seems to be altering the database on the server, and despite changing the password, they still have access. The website is simple, just pulling database records from a local MySQL database.

CYBER RANGE

Basic Network Analysis Course Outline

v1.0
July 14, 2021

FIELD EFFECT™
Cyber security that keeps business moving.

Basic Network Analysis

Course Outline

Course Overview

Every day people access the Internet without being aware of the information coming in and out of their phones and computers to enable this access. Also hidden from view are the numerous devices linking every computer to everyone else's, in other words, a network of links and data joining everything. The goal of this course is to initiate students to network data at the core of network analysis. It introduces some fundamental concepts, and how to view, create and analyze network data with the tool Wireshark.

Course Prerequisites

Students should have a basic working familiarity with a computer and files, and a basic understanding of the command line, as presented in the Steganography unit.

Workload Expectations

Students should be able to complete the course in an hour. However, the actual time investment will depend on previous knowledge and on time spent on studying the suggested resources and doing optional tasks.

Course Learning Outcomes and objectives

At the end of the course students will be able to:

- Discover fundamental characteristics of network data using Wireshark

    - Identify IP addresses and protocols
    - Use the tool ping to confirm two devices share a network
- Create and capture network data in files using Wireshark
    - Create network data through a browser, pings and SSH session
- Analyze network data to identify certain protocols
    - Detect characteristics about protocols such as HTTP, SSH, ICMP

Course Format

The course consists of three objectives. In the first one, students are initiated to some key fundamental concepts such as IP addresses, protocols and packets. They are also introduced to the packet analyzer tool Wireshark. In the second objective, they use Wireshark to create network traffic; then, they are guided on how to discover specific details. Finally, in the last objective, they are guided on how to analyze a given file of network data, by using the filtering features of Wireshark.