Cybersecurity Attack and Defend, Skill Labs

Course Specifications

Course Number: ACI76-047SL_rev1.0
Lab Length: Approximately 18 hours

Creating and Securing User Accounts

Introduction
Objective

Students will perform user account management from the terminal in Linux and from the command line and the GUI (graphical user interface) in Windows. Students will use various operating system commands and utilities to secure user accounts to learn how to protect a company or organization from the inherent risk associated with local and domain accounts.

Overview

This lab covers account management in Linux and Windows. User account management is an essential skill for anyone working with servers and workstations. It is critical to secure user accounts to prevent users from gaining unauthorized access to systems, applications, or utilities that would put a company or organization at more inherent risk. One of the features of this lab will allow you to compare and contrast the account creation and management process in a Linux and a Windows environment. You will find that in Linux, account management is done at the terminal, whereas in Windows, it is done from either the command line or using the GUI (graphical user interface). Windows Server also has Active Directory which allows streamlined centralized management of users. By the end of this lab, you will become familiar with the commands and operating system utilities for creating and managing users in Linux and Windows.

Outcomes:

In this lab, you will learn to:

1. Managing user accounts in Linux
2. Managing user accounts in Windows

	Key Term	Description
1	Active Directory	Active Directory can be installed on most versions of Windows servers. It allows network administrators to centrally manage a network.
2	Domain	Computers in a domain are managed centrally in a client/server network.
3	Workgroup	Computers in a workgroup are managed in a peer-to-peer network.
4	Administrator	The built-in account that can be used to manage Microsoft operating systems.
5	Local	An account that resides on a single system.

	Key Term	Description
	account	

Network Exploitation

Introduction
Objective

Students will use Metasploit to exploit the eternal blue exploit. The exploit is used against system running certain versions of Windows with file and print sharing enabled. One of the serious ramifications of the exploit is system access on the compromised machine. Patching and updating systems can prevent this type of compromise demonstrated in this lab.

Overview

Network exploitation is the process of using exploits to attack vulnerabilities in remote systems. In this lab, you will attack remote system with vulnerabilities. You will be able to gain system access to these computers' operating system (running Microsoft Windows) and run various commands, wreaking havoc on the victim machines. The best way to prevent network exploitation is to regularly patch and update the systems and to ensure you have anti-virus software installed and all the anti-virus definitions are up-to-date.

Outcomes:

In this lab, you will learn to:

1. Scan a network for vulnerabilities
2. Compromise a system
3. Perform post-installation task

	Key Term	Description
1	Kali Linux	An Advanced Penetration Testing Linux distribution designed for digital forensics and penetration testing, ethical hacking, and network security assessments.
2	zenmap	A GUI front end for nmap; will allow you to scan for open ports and services.
3	Metasploit	A framework that contains exploits for various information systems.
4	nmap	A port scanner which will indicate whether ports are open or closed on a remote system.
5	ARP Scan	An ARP scan will determine which hosts are responding on the network you scan.

Finding Malicious Indicators

Introduction

Objective

Students will examine a network breach and be able to identify the indicators of a compromise using a variety of command line and GUI (graphical user interface) utilities that will provide detailed information about the attacker's foothold into a compromised Windows Server.

Overview

In this lab, you will get an opportunity to examine a system that was and is still actively compromised by an attacker. You have likely read articles in the news or heard from your professors about some of the various high-profile attacks where large companies had systems compromised. It is important to be able to look at a system and know how to examine it in order to determine if the system has been compromised. There are utilities that are built into the operating system as well as third-party utilities that can be utilized to help you determine if a system is compromised. Some of the common tasks that be performed to check for a system compromise include examining network connections, file time stamps, viewing the registry, and dumping and examining the RAM of the system. This lab will help you learn about the possible indications of a compromised system.

Outcomes:

In this lab, you will learn to:

1. Examined a compromised system's connections, processes, and memory.
2. Examine timestamps to find instances of potential breaches.
3. Use Wireshark to capture and examine network traffic.

	Key Term	Description
1	autoruns	A free tool from sysinternals that will alert you to startup registry entries as well as programs that will start automatically with user login or when the system starts up.
2	pslist	A free tool from sysinternals that will show you running processes.
3	netstat	A command to show the active TCP/IP connections.
4	Process Explorer	A free tool from sysinternals that will allow you to view the process running in memory on the system.
5	PID	PID stands for process ID and is a unique number assigned to a running process on a given machine.

Local Operating System Exploitation

Introduction
Objective

CEH Domain:

Domain 1: Background
Domain 4: Tools/Systems/Programs

CEH Objective Mapping:

Objective 1.2 Information Security Threats and Attack Vectors

Objective 4.3 Information Security Tools

Overview

In this lab you, will take advantage of the lack of disk encryption and exploit a local system. When the operating system is not encrypted, an attacker with physical access can leverage this to their advantage and gain access to your system using a number of freely available tools. Various tools such as Live DVDs or even the Windows recovery console can provide ways for the attacker to see the files you have on your system as well as download or upload malware and run it on your system.

Outcomes:

In this lab you will learn to:

1. Exploit a Windows machine.
2. Perform post-exploitation tasks.

	Key Term	Description
1	Kali	A widely used Linux distribution with various security tools installed.
2	md5sum	A Linux command to get the MD5 hash of a file.
3	fgdump.exe	Dumps passwords hashes in Windows.
4	Windows Defender	Built-in antivirus for Windows 10.
5	cp	The command to copy a file in Linux.

Static and Dynamic Malware Analysis

Introduction
Objective

In this lab, students will perform static and dynamic malware analysis. Analyzing malware is important because an analyst will want to know what actions the malware is performing on the system as well as on the network. The hash value of the malware can tell you if the malware has been widely used before. Dynamic analysis involves executing the malware and seeing how it behaves, whereas static analysis just involves examining the information contained within the file

Overview

Analyzing malware is important for many reasons. Malware analysis in general is taking steps to find out more information about things like who crafted a malware payload, where the malware is becoming to, or what types of actions the malware is trying to perform. Static analysis is where you look at the file contents and look at the strings and don't execute the file. With dynamic malware analysis, you run the file (likely in a virtual environment not connected to a real network) to see the types of network and process actions that happen to the system

Outcomes:

In this lab, you will learn to:

1. Perform static malware analysis
2. Perform dynamic malware analysis

	Key Term	Description
1	HxD	A hex editor that allows you to view the data within a file.
2	strings	A tool that will allow you to examine information within a file.
3	VirusTotal.com	A website that helps analyze malware samples.
4	Wireshark	A packet analyzer that will allow you to capture network traffic.
5	Notepad++	A free text editing program with more robust features than regular notepad.

Investigating a Network Compromise

Introduction
Objective

In this lab, you will be exposed to a system that has been compromised by an attacker and learn to look for the signs of compromise, including malicious processes and unauthorized network connections. As the number of network attacks against companies and originations continue to increase, it is paramount that you understand what the indicators of compromise are and how to find them on a system that has been reported for acting suspiciously.

Overview

A network compromise is when your system is attacked and an attacker has a foothold over the operating system and has performed various actions such as installing back doors, modifying the file system, and created log file entries. It is critical for you to be able to know what the indicators of a network compromise are and know how to respond to one.

Outcomes:

in this lab, you will learn to:

1. Collect Volatile Data
2. Capture and Analyze RAM
3. Examine Scheduled Tasks
4. Examine File System Artifacts
5. Examine Services

	Key Term	Description
1	Task Scheduler	This allows an administrator to automatically set programs to run on the system.
2	tasklist	A built-in Windows tool that will show you running processes.

	Key Term	Description
3	msconfig	A built-in Windows tool that allows you to view the System Configuration.
4	find	A Windows command that allows you to parse through output in the command line.
5	dumpit	A free stand-alone executable that can make an image of RAM.

Log Analysis in Linux and Splunk

Introduction
Objective

Log analysis is one of the most widely used skills for an analyst. Logs can give indicators of what might be happening to systems on the network. Logs can indicate precursors to compromise, can contain information about a compromise, and also can contain information relevant to post exploitation activities. There are various tools that can be used to analyze logs. There are commercial tools like Splunk as well as free tools like awk, gawk, and grep. The important thing is to be able to look at the logs and parse the relevant information that you're looking for regardless of the tool used.

Overview

Splunk is a widely used commercial log aggregation tool. It is a great tool for ingesting data and then being able to help you analyze network incidents. There are other ways to view log files besides using Splunk. For instance, using grep, gawk, and awk can provide you with similar log parsing results, but those are more arduous methods and those tools are more command line based and require the analyst to remember many various commands and switches.

Outcomes

In this lab, you will learn to:

1. Use Linux commands to search Linux logs.
2. Use Splunk to analyze network traffic and logs.

	Key Term	Description
1	cat	A Linux command used to show the output of data
2	Splunk	A commercial tool with the ability to analyze large log files
3	grep (global regular expressions print)	A Linux tool to parse information
4	Leafpad	A GUI text editor program for Linux (similar to Windows Notepad)
5	tail	The command to show the last few lines of a file in Linux

Network and System Monitoring

Introduction
Objective

Students will set up a sniffer on a Linux box connected to a SPAN port (running in promiscuous mode) and use the command-line utility tcpdump to capture the network traffic. After capturing the network traffic with tcpdump, the student will analyze the network traffic using Wireshark, the most widely used pack analysis tool in the world.

Overview

The tcpdump utility is one of the most widely used free and open-source command-line tools for capturing network traffic on a Linux system. A free tool that is integrated into most Linux operating systems will allow the end user to capture traffic with various parameters, like file size. Wireshark is the most widely used packet analysis tool in the world that can be used to analyze TCP dump files. When networks are attacked, there is valuable information sent to the logs about how the attack happened. In this lab, you will see how long analysis is critical to understanding and dissecting an attack.

Outcomes:

In this lab, you will learn to:

1. Setup a sniffer
2. Use bruter to generate network traffic to monitor
3. Analyze traffic with wireshark
4. Analyze logs

	Key Term	Description
1	Bruter	A brute force tool that will attempt to login to a remote service.
2	auth.log	Keeps track of user activity on a Debian system.
3	tcpdump	A Linux tool to dump network traffic.
4	access.log	Keeps the web traffic on a Linux system.
5	User Agent	Provides information about a browser.

Hardening Windows

Introduction
Objective

Securing an operating system is critical to a company or organization's IT infrastructure. Learning how to secure Windows is extremely important because of the wide use of the operating system within companies, organizations, and homes. Learning the best practices for updating and securing Microsoft Windows is critical to protecting an organization's assets.

Overview

In this lab, you will take a Microsoft Windows system that has security-related issues and patch it. Security-related issues can include items such as default usernames and passwords, clear text protocols like FTP and Telnet, and poorly configured web services. When Windows systems, which are huge

targets of attackers due to their wide use in the industry, are not secured properly, they can be compromised which could lead to data leakage as well as costly remediation. The Windows operating system initially had a very poor reputation for security, but over the years, Microsoft has worked hard to overcome this reputation, and the newer versions of Windows on the market are known for much more robust security.

Outcomes:

In this lab, you will learn to:

1. Exploit a Windows machine
2. Harden a Windows machine

	Key Term	Description
1	Kali Linux	An Advanced Penetration Testing Linux distribution designed for digital forensics and penetration testing, ethical hacking, and network security assessments.
2	Anonymous FTP	Allows a user to connect to an FTP site without an account and upload or download files.
3	Metasploit	A framework that contains exploits for various information systems.
4	nmap	A port scanner which will indicate whether ports are open or closed on a remote system.
5	Vulnerability	A weakness in code that can be exploited.

Hardening Linux

Introduction
Objective

Securing an operating system is critical to a company or organization's IT infrastructure. Learning how to secure Linux is extremely important because of the wide use of the operating system on company and organization's sever infrastructure. Linux is used on a large percentage of servers, and it is widely used in cloud environments. Learning the best practices for securing the configurations and settings on Linux can be critical to protecting an organization's assets.

Overview

In this lab, you will take a Linux system that has security-related issues and patch it. Security-related issues can include items such as default usernames and passwords, clear text protocols like FTP and Telnet, and poorly configured web services. When Linux systems are not secured properly, they can be compromised which could lead to data leakage as well as costly remediation. The Linux operating system has a strong reputation for taking security seriously, but it still needs to be updated and maintained on a regular basis to keep it from being compromised.

Outcomes:

In this lab, you will learn to:

1. Exploit a Linux machine
2. Harden a Linux machine

	Key Term	Description
1	Kali Linux	An Advanced Penetration Testing Linux distribution designed for digital forensics and penetration testing, ethical hacking, and network security assessments.
2	Anonymous FTP	Allows a user to connect to an FTP site without an account and upload or download files.
3	Apache	Web server software that predominantly runs on Linux (although it can run on Windows).
4	nmap	A port scanner which will indicate whether ports are open or closed on a remote system.
5	UID of 0	Any user that has a UID of zero has root level privileges.

Windows Registry

Introduction
Objective

In this lab, students will analyze the Windows registry. The Windows registry is a database which holds user and computer settings critical to the operation of the PC. One of the tools used in this lab is the Windows Registry Recovery (WRR), which is able to parse a registry hive into more easily readable values so in analyst can easily discern various registry settings.

Overview

The Windows registry is an extensive database of user and application settings on a Windows system. The Windows registry can be a treasure trove of information which can help an analyst or a forensic examiner determine many things about the user's operating systems. Someone performing malware analysis on a compromised machine is also interested in registry settings because attackers can set things to start at startup by using certain registry keys.

Outcomes:

In this lab, you will learn to:

1. Capture a live Windows registry
2. Analyze the Windows registry with regedit
3. Analyze a FTK image of the Windows registry with Windows Registry Recovery

	Key Term	Description
1	Registry	A database within the Windows operating system that records settings related

	Key Term	Description
		on the machine's users, installed programs, and other system settings.
2	regedit	A tool built into the Windows operating system that will allow you to view the registry hives.
3	SAM	The Security Accounts Manager file of Windows.
4	SYSTEM	A Windows file that has information about computer profile settings, including services.
5	FTK Imager	A free program that can be used to create a forensic image or extract the registry.

Forensic Analysis of Windows Server

Introduction
Objective

Students will use the Autopsy forensic suite, a free and open software tool, to load and then analyze a disk image of a compromised Windows Server. Autopsy will allow you to examine artifacts from the Windows system including the registry files, the scheduled tasks, as well as date and time stamps on files which may give some indication to what was done. This particular server is running IIS, or Internet Information Services, and the IIS logs will provide important clues to the network instruction. After completing this lab, you will be familiar with some of the common locations where forensic artifacts exist on a Windows server.

Overview

In this lab, you will learn how to search through a forensic disk image in dd format to find artifacts related to an intrusion on a Windows Server. A hacker's dream is to compromise a Windows Server, especially a domain controller because they can leverage the Domain administrator account to control most of the other systems within in the network. The relevant forensic artifacts from a Windows Server include log files, event viewer files, and registry entries.

Outcomes:

In this lab, you will learn to:

1. Examine a compromised Windows Server using Autopsy
2. Analyze the common locations of compromised artifacts
3. Analyze a compromised Windows registry using Windows Registry Recovery

	Key Term	Description
1	Registry	A database within the Windows operating system that records settings related on the machine's users, installed programs, and other system settings.
2	WRR	Windows Registry Recovery, automatically parses some of the most pertinent information from the Windows registry files.

	Key Term	Description
3	SAM	The Security Accounts Manager file of Windows.
4	SYSTEM	A Windows file that has information about computer profile settings, including services.
5	Autopsy	A free program that can be used to analyze forensic images.

Forensic Analysis of a Windows 10 Client

Introduction
Objective

In this lab, you will use Autopsy, an open-source forensic suite, to load and then analyze a disk image of a compromised Windows client. After completing this lab, you will be familiar with some of the common locations where forensic artifacts exist on a Windows client machine. Windows client machines include Windows 7, Windows 8.1, and Windows 10. The disk image for this lab was created using the Windows 10 operating system, the latest version of the Windows client operating system at the time this lab was written.

Overview

In this lab, you will learn how to search through a forensic disk image in dd format to find artifacts related to an intrusion on a Windows client machine. Windows' client machines tend to be a large target for hackers because end users, who may lack knowledge of computer security, can download malicious files or open malicious attachments. Some of the relevant forensic artifacts from a Windows server include Windows event log files, event viewer files, and registry entries.

Outcomes:

In this lab, you will learn to:

1. Examine a compromised Windows 10 client using Autopsy
2. Analyze the common locations of compromised artifacts
3. Analyze a compromised Windows registry using Windows Registry Recovery

	Key Term	Description
1	Autopsy	A free program that can be used to analyze forensic images.
2	Event Viewer files	The most commonly viewed Event Viewer files are the Application, Security, and System logs. The files are stored in modern versions of Windows in C:\Windows\winevt.
3	Scheduled tasks	These are programs that are set to run automatically, normally stored in the C:\Windows\System32\Tasks folder.
4	Registry files	Some of the registry files with a large amount of information about Windows configurations, including SYSTEM, SOFTWARE, and SAM, are stored in

	Key Term	Description
		C:\Windows\System32\Config.
5	Creation date	A timestamp in Windows that can be used to track when a file was placed on a system.

Forensic Analysis of a Linux System

Introduction
Objective

Students will use the Autopsy forensic suite, a free and open software tool, to load and then analyze a disk image of a compromised Linux system. Some people have the misconception that malware does not work on or affect Linux systems when using malware against Linux systems is common. After completing this lab, you will be familiar with some of the common locations where forensic artifacts exist on a Linux system, which are very different from analysis of Windows systems.

Overview

In this lab, you will learn how to search through a forensic disk image in dd format to find artifacts related to an intrusion on a Linux Server. Some of the relevant forensic artifacts from a Linux system include apache log files, the history file, and the secure or auth.log file, which includes valuable information such as SSH connections or user account activity. You will find that forensic analysis of a Linux system is far different than forensics in Windows.

Outcomes:

In this lab, you will learn to:

1. Create an image of a compromised Linux machine using FTK imager
2. Examine a compromised Linux machine using Autopsy
3. Analyze the common locations of compromised artifacts

	Key Term	Description
1	FTK Imager	A free program that can be used to create forensic images.
2	auth.log	A file that tracks security-related events on the system.
3	/etc/shadow	A file that contains the password hashes for the users.
4	history file	This file contains commands that the user typed during a session.
5	/etc/passwd	This file contains the names of the users on the system as well as their user IDs (UID).

Using EFS

Introduction

Objective

Students will use EFS to protect files and folders on the system. Students will grant other user's on their Windows system access to the EFS files. Users who are not granted access to the EFS files and folders will receive an error message when they try to access and read the files.

Overview

Data integrity is one of the three pillars of the CIA triad (confidentiality, integrity, and availability). The encrypted file system first came into use on NTFS volumes starting with Windows 2000 and since then has been a very good way to keep files and folders secure on Windows server and client systems. If the user's password is changed, the user might need to use a recovery key to recover the file. In this lab, you will see how it is possible to provide access to other users to the files or folders that were encrypted using EFS.

Outcomes:

In this lab, you will learn to:

1. Encrypt a folder
2. Backup a user's key
3. Give access to files to Windows users
4. Access encrypted files

	Key Term	Description
1	EFS	The Encrypted File System is a Microsoft Technology that allows a user to encrypt a file.
2	Encryption	The process of making data unreadable through a process of encoding. Data that is encrypted and cannot be read without the decryption keys is known as ciphertext.
3	Ciphertext	When plaintext data is encrypted by using mathematical algorithms, it becomes known as ciphertext. Ciphertext is encoded, encrypted data.
4	Plaintext	Data that is not encoded or encrypted; data that anyone can read without a decryption key.
5	Decryption	The process of using keys or ciphers to decode ciphertext. When the data is decoded or decrypted with the decryption keys, it is known as plaintext.

Using Disk Encryption

Introduction
Objective

In this lab, you will exploit a Windows operating system using the Windows recovery console to view files and folders on the system without any type of password to the system. After using a disk encryption

utility, you will no longer be able to view the files or folders on the system, thus securing the data from compromise when a user gets physical access to it.

Overview

Data integrity is one of the three pillars of the CIA triad (confidentiality, integrity, and availability). Using disk encryption will help to protect and secure data. A perfect example of this is the stolen laptop scenario. When a laptop is stolen, the data on the hard drive can be accessible to attackers under certain conditions. In this lab, you will see what the differences are for an "attacker" when data is not encrypted and when the data on the disk is encrypted.

Outcomes:

In this lab, you will learn to:

1. Examine a hard drive without encryption
2. Encrypt a Windows partition
3. Verify encryption

	Key Term	Description
1	Encryption	The process of making data unreadable through a process of encoding. Data that is encrypted and cannot be read without the decryption keys is known as ciphertext.
2	Ciphertext	When plaintext data is encrypted by using mathematical algorithms, it becomes known as ciphertext. Ciphertext is encoded, encrypted data.
3	Plaintext	Data that is not encoded or encrypted; data that anyone can read without a decryption key.
4	Decryption	The process of using keys or ciphers to decode ciphertext. When the data is decoded or decrypted with the decryption keys, it is known as plaintext.
5	VeraCrypt	A free and open source tool for Windows, Linux, and Mac OS that encrypts volumes and disks. The tool can be downloaded free by using this link: https://www.veracrypt.fr/en/Downloads.html

Using SSH and SCP

Introduction
Objective

Students will use the secure shell protocol to transfer files using encryption. Other methods such as FTP do not provide encryption and put the security of an organization or a user's credentials at risk. SSH is the standard, and SSH and SCP are widely used throughout the industry because of the security offered that was often lacking in older file transfer protocols.

Overview

Secure communion and secure authentication are critical to keeping a company or organization's network resources protected. An SSH server uses a pair of asymmetrical keys which allows the session

between the client and the server to be fully encrypted. This results in better security, and SSH has for the most part replaced FTP and telnet because of its use of encryption as opposed to the clear text transmission methods used by Telnet and FTP.

Outcomes:

In this lab you will learn:

1. Setup an SSH Server
2. Connect to a SSH Server
3. Use SCP

	Key Term	Description
1	SCP	Secure Copy can be used to securely copy files between systems. SCP is a preferable method over FTP which is a clear text protocol.
2	SSH	Uses TCP port 22 and is a protocol that will allow you to securely administer a remote machine from the terminal.
3	Kali Linux	An Advanced Penetration Testing Linux distribution designed for digital forensics and penetration testing, ethical hacking, and network security assessments.
4	nmap	A port scanner which will indicate whether ports are open or closed on a remote system.
5	ssh-keygen	A Linux command that will generate the public and private keys needed for an SSH server to operate securely.

Using Hash Functions to Validate Data Integrity

Introduction
Objective

In this lab, students will use various hashing function such as md5, sha1, and sha512 to verify that files are the same after they are transferred. Hashing algorithms will help determine that the data has integrity and is the same on the source drive as it is on the destination drive.

Overview

Data integrity is one of the three pillars of the CIA triad (confidentiality, integrity, and availability). There are many different types of hashing functions. For example, md5, sha1, sha256, sha384, and sha512. Different mathematical calculations result in stronger hash values. The strongest of these hash values listed is the sha512, and the weakest is the md5. Although weaker than the others, the md5 hash is still accepted in court for testimony. As the number of files continues to increase, larger hash values ensure even more reliability than older ones that were used

Outcomes:

In this lab, you will learn to:

1. Verify integrity in Windows

2. Verify integrity on a Linux System after File transfer
3. Verify integrity after downloading files from a Web Site

	Key Term	Description
1	MD5 Hash	The Message Digest 5 hashing algorithm, a 128-bit hexadecimal value.
2	SHA-1 Hash	The Secure Hashing Algorithm which is a 160-bit hexadecimal value.
3	SHA-256 Hash	A version of the Secure Hashing Algorithm which is a 256-bit hexadecimal value.
4	SHA-384 Hash	A version of the Secure Hashing Algorithm which is a 384-bit hexadecimal value.
5	SHA-512 Hash	A version of the Secure Hashing Algorithm which is a 512-bit hexadecimal value.