Cyber Challenge Range, Skill Labs

Course Specifications

Course Number: ACI76-046SL_rev1.0
Lab Length: Approximately 18 hours

Challenge – Reconnaissance

Introduction
Objective

Reconnaissance - The goal of the lab will be to find the outer firewall and perform a scan on it to find vulnerable services.

Overview

Level – Beginner

Skills Needed – Networking, Vulnerability Assessment, Networking Knowledge.

Goal – To identify the vulnerable machine that will serve as the entrance to the network.

Known Network(s) – None.

Tools used – nmap, curl, linux shell piping and redirection

Challenge - Cracking the Perimeter

Introduction
Objective

Cracking the Perimeter - To find a way to get through the firewall to the DMZ behind it. Once there, find a way to pivot to the DEV network.

Overview

Level – Intermediate

Skills Needed – Enumeration, attention to details, SSH, Base64 encoding

Goal – Compromise the DMZ and pivot to the DEV network.

Known Network(s) – 192.168.1.0/24

Tools used – Metasploit, nmap, meterpreter, sed, unzip, nslookup

Challenge – Infiltration

Introduction
Objective

Infiltration - The object of this next challenge is to gain access to the User network from the DEV network.

Overview
Level – Intermediate

Skills Needed - Network Fundamentals, Password Cracking, Metasploit, Linux

Goal - Gain access to the User network using brute force password cracking and enumeration.

Known Networks – 192.168.1.0/24, 10.10.10.8/29, 10.10.30.16/28

Tools Used – Nmap, Metasploit, Hydra, ProxyChains, net(Windows CLI utility).

Challenge - Situational Awareness

Introduction
Objective

Situational Awareness - The purpose of this lab will be to infiltrate the Admin network with the credentials discovered in the previous lab. To aid in this an implant was set up that will call out every 15 seconds to port 7979 on the attacking machine. Awareness of the Admin network segment will aid in choosing a target quickly.

Overview

Level – Intermediate to Advanced

Skills needed – Basic Networking, Command Line usage, Metasploit, Linux, Situational Awareness, encoding and encryption.

Goal – Pivot from the User network to the admin Network with previously discovered credentials.

Known Network(s) – 192.168.1.0/24, 10.10.10.8/29, 10.10.30.16/28, 10.10.50.16/28, 10.10.70.16/28

Tools used – Metasploit, proxychains, route command, socks4a, msfvenom, rdesktop, nmap, windows command line.

Challenge - Carving Disk Images

Introduction
Objective

Carving disk images - The goal of this lab will be to gain Local Administrative access to the Admin Workstation via information found in a backup image. An implant was set up on the backup server to call out to the attacking machine on port 4321 every 15 seconds. It will allow direct access to it and the admin network.

Overview

Level – intermediate

Skills Needed – nt hash cracking, mounting virtual disks, enumeration of important files, remote desktop

Goal – To gain local admin access to the Admin workstation

Known Network(s) – 192.168.1.0/24, 10.10.10.8/29, 10.10.30.16/28, 10.10.50.16/28, 10.10.70.16/28, 10.10.40.8/29

Tools used – command line, Metasploit, john the ripper, diskpart, remote desktop

Challenge – Kerberoasting

Introduction
Objective

Kerberoasting - The goal of this lab will be to create a golden ticket for the fakecorp.com domain administrator and to prove that it works. An implant was set up to call out to the attacking machine on port 4321 every 15 minutes. It will allow direct access to the admin network.

Overview

Level – intermediate

Skills Needed – creating payloads, evading AV, kerberoasting

Goal – To create a golden ticket for the fakecorp.com domain

Known Network(s) – 192.168.1.0/24, 10.10.10.8/29, 10.10.30.16/28, 10.10.50.16/28, 10.10.70.16/28, 10.10.40.8/29

Tools used – command line, Metasploit, Kiwi, remote desktop

Challenge - Locating the Crown Jewels

Introduction
Objective

Locating the Crown Jewels - The goal of this lab is to locate this organizations 'Crown Jewels'. This is the accounting system that contains sensitive data. An implant was set up to call out to the attacking machine on port 4321 every 15 seconds. It will allow direct access to the admin network.

Overview

Level – Advanced

Skills Needed – Networking, port scanning, leveraging privilege, 3270 terminal emulators.

Goal – To gain access to the mainframe and log in.

Known Network(s) – 192.168.1.0/24, 10.10.10.8/29, 10.10.30.16/28, 10.10.50.16/28, 10.10.70.16/28, 10.10.40.8/29

Tools used – Metasploit, proxychains, meterpreter, powershell, nmap, x3270

Challenge - Exfiltrating Data

Introduction
Objective

Exfiltrating data - The purpose of this lab is to pull the data for the bank accounts from the mainframe server. An implant was set up to call out to the attacking machine on port 4321 every 15 minutes. It will allow direct access to the admin network.

Overview

Level – Advanced

Skills Needed – 3270 terminal, taking screenshots

Goal – To exfiltrate the bank account data from the mainframe.

Known Network(s) – 192.168.1.0/24, 10.10.10.8/29, 10.10.30.16/28, 10.10.50.16/28, 10.10.70.16/28, 10.10.40.8/29, 10.10.80.16/28

Tools used – Metasploit, proxychains, meterpreter, powershell, nmap, x3270

Challenge - Covering your Tracks

Introduction
Objective

Covering your tracks - During a pentest or red team exercise, it is often necessary to erase traces of your presence, to throw the opposition off. The easiest way is to erase the logs outright. Also, as a scenario wraps up you want to leave a way back in with the creation of new accounts on several systems and/or the domain. An implant was set up to call out to the attacking machine on port 4321 every 15 seconds. It will allow direct access to the admin network. This will aid in accessing the main Active Directory server.

Overview

Level – Intermediate

Skills Needed – Using Metasploit, anti-detection.

Goal – To eliminate traces of malicious activity on the corporate network.

Known Network(s) – 192.168.1.0/24, 10.10.10.8/29, 10.10.30.16/28, 10.10.50.16/28, 10.10.70.16/28, 10.10.40.8/29, 10.10.80.16/28

Tools used – meterpreter, Metasploit, windows and linux command line.

Challenge - Maintaining Persistence

Introduction
Objective

Maintaining persistence - The goal of the final lab is to leave a back door into the network. The choice of a print server or printer is a wise choice since they are often overlooked. We established a temporary

backdoor that is installed on the multi-function to allow for ready access. this calls out to port 3943 on the 192.168.1.34 machine. Metasploit is not needed for this lab.

Overview

Level – Advanced

Skills Needed – knowledge of linux startup procedures, bash scripting, netcat.

Goal – To install a persistent connection on one of the printer servers.

Known Network(s) – 192.168.1.0/24, 10.10.10.8/29, 10.10.30.16/28, 10.10.50.16/28, 10.10.70.16/28, 10.10.40.8/29, 10.10.80.16/28

Tools used – vi, systemctl, netcat

Challenge - Host Based Forensics

Introduction

Objective

You are tasked with conducting a computer forensic analysis and answer the challenge questions.

Challenge - Mobile Forensics

Introduction
Objective

Mobile Cell Phone Forensic Analysis - The objective of this lab is to become familar with conducting a simple forensic analysis on a cell phone.

Overview

Scenario - Suspect Josh Hickman is suspected is stalking an individual during the month of February 2020. You are taken with examining the Pixel 3 image and seeing if photographs of scouted locations exist on the image and determining when and where these images were taken and verify the identity of the suspect and that there is reasonable suspicion that this individual was scouting the locations during this period. All times are in Pacific Standard Time (PST)

Level – Basic

Skills Needed – Basic understanding of the use and purpose of forensic tools.

Goal – To perform a basic forensic analysis and fullfill the request stated in the objectives.

Known Network(s) – None.

Tools Used – Autopsy, Sleauthkit, Assoicated Plugin(s)

Challenge - Malware Analysis in Windows

Introduction
Objective

Malware Analysis - The objective of this lab is to perform a quick analysis on some basic malware samples and determine program flow and the components, calls and libraries it accesses in its operation. This will allow the student to help determine the purpose and motivation behind these samples and locate indicators of compromise (IOCs) that can be used for later detections.

Overview

Level – Intermediate

Skills Needed – Basic Static Malware Analysis.

Goal – To perform a basic analysis on some suspected malware.

Known Network(s) – None.

Tools used – DiE, Universal Extractor

Challenge - Reverse Engineering in Linux

Introduction
Objective

To reverse engineer and disassemble two Linux binaries

Overview

Having the skill to disassemble suspect binaries is an essential task in cyber security. This lab will challenge the students' ability to dissect a Linux binary using the built-in GNU Debugger (GDB).

Scenario – As a member of an IR team, you are tasked with reverse engineering 2 pieces of software. Determine the characteristics, and the passwords of each piece of software using the tools available on the Remnux VM.

Level – Advanced

Skills Needed – Knowledge of assembly language and how to read it, general understanding of the GNU Debugger

Goal – Solve the two binaries

Known Network(s) – None

Tools Used – file command, strings command, GDB

Challenge - Binary Exploitation

Introduction
Objective

Binary Exploitation – Gain ssh access to the remote VM. Create an exploit that takes advantage of a race condition and allows the reading of a root-only access file.

Overview

Scenario – You are contracted to work as a penetration tester and have been given have gained user access to a client system. Your objective is to compromise this system by exploitation access code left on the system. This access code will grant simulated access and contain a flag.

Level – Advanced

Skills Needed – Reading and understanding disassembly, shell scripting, knowledge of race conditions, enumeration techniques

Goal – To create an exploit that makes use of a race condition for the binary on the remote VM

Known Network(s) – 192.168.1.0/24

Tools Used – arp-scan, ssh, nano, sudo, nmap, ln

Challenge - Searching Through Evidence

Introduction
Objective

Find Hidden Data – Uncover the flags found in the evidence files using the forensics tools found on Kali Linux.

Scenario – A system was seized in a ransomware case. It is believed that the suspect has hidden bitcoin wallet addresses inside text files and has used encoding methods to hide these addresses. There is believed to be five accounts hidden in these files. Please search for these addresses. This data is needed to recover victim funds.

Overview

Level – Intermediate

Skills Needed – Knowledge of forensic techniques and tools and encoding methods

Goal – Uncover the flags hidden in the evidence files

Known Network(s) – N/A

Tools Used – Kali forensic tools

Challenge - File Recovery

Introduction
Objective

File Recovery – The objective of the labs is to recover an unknown file type into a working file.

Scenario – An unknown file was found on a suspect's cell phone. As part of the forensics team, it is your responsibility to recover the file to a useful state. Use the tools available in the Flare VM to identify the file and then recover it.

Overview

Level – Advanced

Skills Needed – File identification, Hex Editing

Goal – Reconstruct a file

Known Network(s) – N/A

Tools Used – HxD, Internet search

Challenge - Recreating an Attack

Introduction
Objective

To discover a vulnerability and recreate an attack.

Scenario – As a forensic examiner, you have recreated an exploited box and want to determine what kind of exploit was used to compromise it.

Overview

Level – Easy/intermediate

Skills Needed – Enumeration, Linux command line, reading and understanding source code

Goal – To successfully recreate the exploit performed on the vulnerable machine.

Known Network(s) – N/A

Tools Used – ss, ls, less

Challenge - Debugging Existing Python Code

Introduction
Objective

To take existing Python code and get it to run properly.

Scenario – As a penetration tester, you may have to take someone's proof of concept code and get it to run properly on your system.

The goal of this challenge is to take existing code, debug it, and get it working.

Overview

Level – Intermediate

Skills Needed – Knowledge of the Python programming language

Goal – To get the code to run properly

Known Network(s) – N/A

Tools Used – Idle Python Editor