Aalborg University

HAAUKINS

VIRTUALIZED CYBER SECURITY TRAINING

Challenges Guide

Last Update: 10/11/2019

Outline

- Categories and Difficulty levels descriptions
- Challenges Table
- Challenges ordered by category
  - Forensics
  - Web Exploitation
  - Reverse Engineering
  - Binary
  - Cryptography

Challenges - Categories

- **Forensics**: This is a broad category that includes different types of training challenges such as file format analysis, steganography, memory dump analysis, or network packet capture analysis. Any challenge to examine and process a hidden piece of information out of static data files could be considered a Forensics challenge, unless it involves cryptography.

- **Web Exploitation:** This category includes all the challenges that provide a vulnerable website, from the ones that contains a bug to the ones that run over an old version of a framework. All the challenges in this category show up in a kind of challenge in which the user need to exploit a bug to gain some kind of higher level privilege.

- **Reverse Engineering:** It is typically the process of taking a compiled (machine code, bytecode) program and converting it back into a more human readable format.

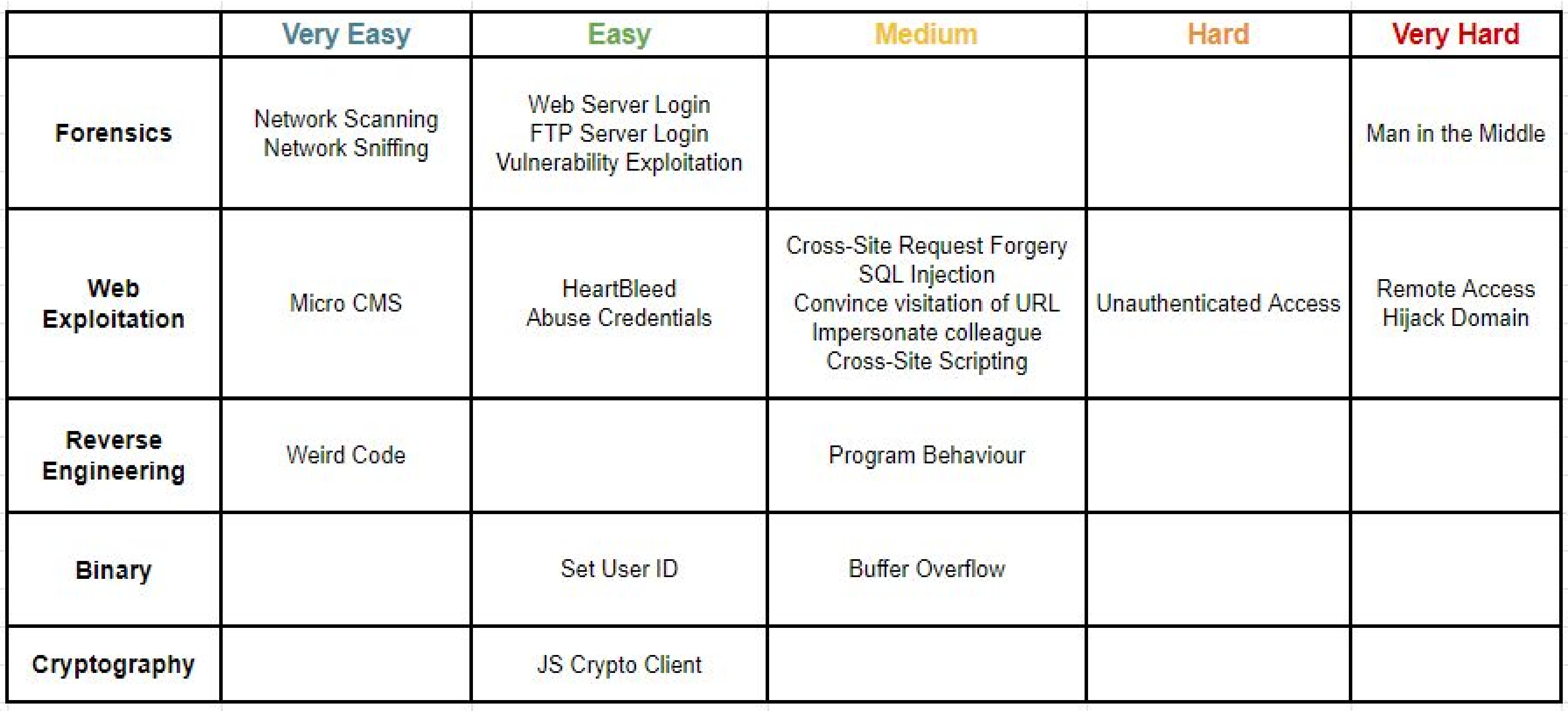
- **Binary (PWN)**: Binary exploitation is the process of subverting a compiled application such that it violates some trust boundary in a way that is advantageous to the attacker. It comes down by abusing vulnerabilities that corrupt memory in software or by finding a vulnerability in the program and exploiting it in order to escalate privileges.

- **Cryptography:** the main goal is usually to crack or clone cryptographic objects or algorithms to reach the flag.

Challenges - Difficulty Levels

The levels of difficulty scale is based on the number of steps required in order to solve the Training Challenge

- Very Easy: It requires just one step in order to get the flag
- Easy: It requires one-two steps, it is based on the challenge category
- Medium: It requires two-three steps, it is based on the challenge category
- Hard: It requires three-four steps based on the challenge category
- Very Hard: It requires several steps in order to get the flag



	Very Easy	Easy	Medium	Hard	Very Hard
Forensics	Network Scanning Network Sniffing	Web Server Login FTP Server Login Vulnerability Exploitation			Man in the Middle
Web Exploitation	Micro CMS	HeartBleed Abuse Credentials	Cross-Site Request Forgery SQL Injection Convince visitation of URL Impersonate colleague Cross-Site Scripting	Unauthenticated Access	Remote Access Hijack Domain
Reverse Engineering	Weird Code		Program Behaviour		
Binary		Set User ID	Buffer Overflow		
Cryptography		JS Crypto Client			

1. Forensics

1.1 Network sniffing

Points: 5 **Difficulty:** Very Easy

Learning Objectives:
- Working with Kali Linux
- Network packets, protocols and software (Wireshark) dedicated to monitor and analyse network traffic

Description: The network sniffing challenge, encourages the HAAUKINS user to utilize basic knowledge about network communication to execute a simple cyber attack of network eavesdropping. The user is expected to make use of Wireshark, to complete a basic passive network scan of the local network. By sorting the traffic captured over a short period of time and analysing the result, the user should be able to successfully locate an unencrypted login request to a HTTP server. Inspecting this POST request packet, will lead to the flag.

Prerequisite:
- Basic knowledge in Linux OS and its terminal
- Wireshark

1.2 Network scanning

Points: 5 **Difficulty:** Very easy

Learning Objectives:
- Introduction to NMAP and network scanning
- Knowledge in fingerprinting, ports and specific protocols such as HTTP

Description: The network scanning challenge is indented as an introduction to vulnerabilities associated with unencrypted network traffic, HTTP. The HAAUKINS user, is expected to perform a simple active network scanning procedure of a local subnet using NMAP. Through analysing the outcome of the scan, it should be possible to locate a completely open unencrypted webserver, that subsequently can be accessed directly by ip-address and provide the flag.

Prerequisite:
- Basic knowledge in Linux OS and its terminal
- Know what software to use when scanning a network

1.3 Web server login

Points: 5 **Difficulty:** Easy

Learning Objectives:
- Knowledge of HTTP POST requests and why encrypted traffic is so important

Description: In this challenge, the HAAUKINS user is expected to utilise a combination of knowledge from the network sniffing and network scanning exercises. By further inspecting the HTTP POST request packet, the user will be able to find login credentials. This is a simulation of wiretapping into a network and monitoring the traffic, while someone else connected to the same network completed a login procedure to an unencrypted website. The flag is presented to the user, when they access the website connected to the destination ip-address of the HTTP POST request packet, and successfully logs in using the login credentials they have just sniffed.

Prerequisite:
- 1.2 Network scanning

1.4 FTP server login

Points: 7 **Difficulty:** Easy

Learning Objectives:
- Introduction to File Transfer Protocol, FTP, and its vulnerabilities such as missing encryption
- Fingerprinting with NMAP
- Brute force attacks on a live system and why a powerful wordlist can do this easy
- Characteristics of encoding schemes

Description: FTP servers are used to keep files and deliver it through FT protocol, however some FTP servers use weak or default passwords which make them vulnerable to brute force attacks and gain access to files. This challenge requires to brute force FTP server using default dictionaries on Kali machine in order to achieve flag file.

Prerequisite:
- Knowhow to scan a network (challenge 1.2)
- Basic knowledge of Hydra (Kali Tool) or different techniques to make a brute force attack on a live system

1.5 Vulnerability exploitation

Points: 10 **Difficulty:** Easy

Learning Objectives:
- Introduction to the Metasploit framework

- Confidence navigating Kali Linux terminal
- Acquire knowledge about vulnerability search and exploits

Description: In this challenge, the HAAUKINS user is expected to utilise an operating system specific active network scan, to locate a host connected to the network running an outdated and extremely vulnerable operating system. By deeper inspection, the user will be able to retrieve specific information about this host, that will allow them to Google their way to an exploit using the Metasploit framework for exactly this target. By navigating through Metasploit and setting up the configuration, the user will be able to gain root access to the Windows computer. In the final step of the challenge, the user has to navigate through the filesystem and find a file containing sensitive information.

Prerequisite:
- Knowhow to scan a network and what to look after (challenge 1.2)

1.6 Man in the Middle

Points: 15 **Difficulty:** Very hard

Learning Objectives:
- ARP spoofing a network

Description: Man-in-the-middle is an attack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other. To get the flag the participant will need to act as man-in-the-middle between a server and a client.

Prerequisite:
- Know what a man-in-the-middle attack is
- Know the vulnerabilities attached by only running https on part of the website

2. Web Exploitation

2.1 Micro CMS XXS and URL

Points: 5-5 **Difficulty:** Very easy

Learning Objectives:
- Lean how much is it important to sanitize the data submitted through a form
- Manage and Modify the URL

Description: The users will be faced with a basic Content Management System in which they can create and edit web pages. The main goal of this challenge is to let the user understand how an XSS works and also how is possible to retrieve data managing the url. On this challenge the user has to find 2 flag.

Prerequisite:
- Know how an Cross-Site Scripting (XSS) works

2.2 Heartbleed

Points: 8 **Difficulty:** Easy

Learning Objectives:
- Achieve confidence using the Metasploit framework
- Understand that also encrypted web traffic (HTTPS) can be exploited

Description: In this challenge, the HAAUKINS user is expected to complete an attack abusing the famous Heartbleed Bug, that is a serious vulnerability in the popular OpenSSL cryptographic software library. This bug allows an attacker to access information otherwise protected by SSL/TLS encryption. The user is expected to gather information about conducting a Heartbleed attack from Google, and subsequently configure a Metasploit session to complete the exploit. The target host should be determined through an active network scan.

Prerequisite:
- Fundamentals in Linux terminal
- Knowing what Metasploit is and its capabilities

2.3 Cross-Site Request Forgery

Points: 12 **Difficulty:** Medium

Learning Objectives:

- Gain a basic understanding of web APIs

Description: In this challenge the user is expected to utilise knowledge about web service communication. After registering on the website the user should figure out that the people in the chat is clicking on all links send. After realising this the user should use knowledge about web APIs to create a link that will get the other users to send money in order to buy the flag.

2.4 SQL Injection

Points: 15 **Difficulty:** Medium

Learning Objectives:
- Understand how an SQL attack is performed
- SQL language and its syntax

Description: In this challenge, the HAAUKINS user is expected to utilise knowledge about web service communication. When accessing and logging into the website in challenge “1.3: Web server login”, it should be noticed that the presented home screen includes a comments field. When posting a comment this is shown on the website page, which illustrates that database communication is active. After this realisation the user is expected to form an abusive SQL query and exploit the comments field to access passwords from the database users table.

Prerequisite:
- Understand the fundamentals of database communication (SQL)

2.5 Convince visitation of URL

Points: 15 **Difficulty:** Medium

Learning Objectives:
- Introduction to mail servers and protocols as ‘Simple Mail Transfer Protocol’, SMTP.
- Mail clients and how to forward emails through a STMP server in a terminal.
- Capturing POST requests

Description: Social Engineering including spear phishing emails is very popular in the hacking community, because it’s a lot easier to hack a person than a computer. In this challenge the HAAUKINS user shall try to trick a person into visiting a website of his choice. In order to do that the user needs to know who to target; the first goal is to do some recon on the network and websites. The next step is to send the target an email with an URL. Haaukins is a closed environment and the user will need to use a mail server running on the network. The participants can see various flags (through traffic analysis) being exposed as they conduct phishing against an email listed on the web server.

Prerequisite:
- It’s necessary to know how an SMTP server works and how to find services on a network like web server and SMTP server (challenge 1.2).

2.6 Impersonate colleague

Points: 15 **Difficulty:** Medium

Learning Objectives:
- Learn how to send a phishing email

Description: This is phishing challenge in which the user shall try to trick a person into visiting a website of his choice. In order to do that the user has to find the destination email by looking the network and the website. The user should let the destination email understand that the email is from the same domain in order to get the flag.

Prerequisite:
- 2.5 Convince visitation of URL

2.7 Abuse Credentials

Points: 10 **Difficulty:** Easy

Learning Objectives:
- Introduction to mail servers and protocols as Simple Mail Transfer Protocol
- Setup a simple web server with a custom HTML script

Description: If a you can get a person to visit your website, maybe you can get him to input credentials and hand it over to you? In this challenge the user will continue working on phishing, but he will learn that it's a lot more than just sending some emails to important people. He will need to trick them into passing confidential information without suspicion. He can do this by cloning a website the victim is trusting and trick him visit it.

Prerequisite:
- 2.5 Convince visitation of URL
- 2.6 Impersonate colleague

2.8 Cross-Site Scripting

Points: 15 **Difficulty:** Medium

Learning Objectives:
- Learn how to gain unauthorized access on a website

Description: The challenge consists of two machines a server and a client. The server hosts a website with a comment section which is vulnerable to injecting JavaScript. The users has to use the section in order to steal the session cookie from the client, which visits the site from time to time. When they have stolen the cookie, then they can use it to gain authorized access and find the flag.

Prerequisite:
- 2.1 Micro CMS

- Know how the cookies work

2.9 Unauthenticated Access

Points: 20 **Difficulty:** Hard

Learning Objectives:
- Understanding of how HTTP headers works and how to manipulate them in order to get remote code execution access.

Description: The challenge provides to the user a website in which is installed an old version of Joomla. This CMS suffers from an unauthenticated remote code execution that affects all versions from 1.5.0 to 3.4.5. It means any file on server can be accessible by sending commands, so in order to get flag from the server, users should be able to search for it and then read it.

Prerequisite:
- Knowledge about HTTP requests and headers
- Familiarity to metasploit modules

2.10 Remote Access

Points: 20 **Difficulty:** Very hard

Learning Objectives:
- Know how to use cURL

Description: The challenge provides to the user a website in which is installed an old version of Webmin. Webmin is a web-based interface for system administration for Unix. Using any modern web browser, it is possible to setup user accounts, Apache, DNS, file sharing and much more. This web-based interface suffers from an unauthenticated remote code execution that affect the version 1.920. The main goal of the challenge is to get the flag contained into a txt file making request through either command line i.e. curl or some Kali Linux tools

Prerequisite:
- Analyse Wireshark traffic
- Know how to make an HTTP request from command line
- 2.5 Convince visitation of URL

2.11 Hijack Domain

Points: 20 **Difficulty:** Very hard

Learning Objectives:
- Learn how spoofing works
- ARP Protocol

Description: This is a phishing challenge in which the user has to hijack the challenge domain. The user should redirect the traffic of the legitimate website to the kali machine in order to get the flag.

Prerequisite:
- 2.5 Convince visitation of URL
- 2.6 Impersonate colleague
- 2.7 Abuse Credentials

3. Reverse Engineering

3.1 Weird Code

Points: 5 **Difficulty:** Very Easy

Learning Objectives:
- Learn the basic syntax of Go Programming language

Description: This is a Code-base challenge in which the user will have access to an FTP server in order to download a source code file. The user have to gather the piece of flag spreaded over the tricky source code in order to solve the challenge.

Prerequisite:
- Basic concepts of a programming language

3.2 Program Behaviour

Points: 10 **Difficulty:** Medium

Learning Objectives:
- Learn how to crack a program

Description: This is a simple reverse engineering challenge in which the users will have access to an FTP server in order to download a binary file containing the flag. The main goal of the challenge is to let understand the user how to crack a program in order to change its behaviour. It will be necessary to use a debugger tool to analyse and understand the workflow on the program.

Prerequisite:
- Know how to use a debugger tool
- Basic knowledge of Assembly and CPU registers

4. Binary

4.1 Set User ID

Points: 10 **Difficulty:** Easy

Learning Objectives:
- Learn how to escalate the privilege and get root access
- Scanning a system to check if programs have specific privileges

Description: In this challenge the users will have access to an SSH session in which there are a file containing the flag. That file is only readable by user with root privileges. In order to solve the challenge the user will have to find the command for which is set the SUID bit and then escalate privileges in order to open the file containing the flag.

Prerequisite:
- Basic usage of linux from command line
- Know linux user permissions

4.2 Buffer Overflow

Points: 20 **Difficulty:** Medium

Learning Objectives:
- Learn how the processes are held in the memory
- Learn how to exploit a buffer overflow through shellcode
- Learn how to manipulate memory and it's registers to execute malicious code

Description: In this challenge the users will have access to an SSH session in which there are a file containing the flag. That file is only readable by user with root privileges. The challenge will require the user to find a program which has SUID bit set and is vulnerable to buffer overflow. The main goal is to debug the program in order to find how many bytes are necessary for the buffer to overwrite the instruction pointer and then write some assembly code to get root privileges.

Prerequisite:
- Know what is a buffer overflow
- Know how to debug a binary file
- Basic knowledge of Assembly

5. Cryptography

5.1 JS Crypto Client

Points: 5 **Difficulty:** Easy

Learning Objectives:
- Understanding of cryptography algorithms

Description: The challenge is based on a rotation of the Caesar’s cipher encryption. Challenge includes only index.html file which contains the encrypted flag through some JS code.

Prerequisite:
- Know how Caesar’s cipher encryption techniques works