MACQUARIE University

Offensive Security (COMP6320)

CTF-1 Report

Team 55

Team Members	Email
Samip Pant	samip.pant@students.edu.mq.au
Ayush Lal Bajracharya	ayushlal.bajracharya@studnets.edu.mq.au
Chisthia Kahn	chisthia.khan@students.edu.mq.au
Yousra Mehrin	yousra.mehrin@students.edu.mq.au
Aavishkar Bhattarai	aavishkar.bhattarai@students.edu.mq.au

Report By: Samip Pant (48599506)

Date: 31/08/24

Table of Contents

1. REPORT SUMMARY

1.1 Introduction

The Capture the Flag-1 (CTF-1) was an event held toward the completion of Offensive Security (COMP6320) course in the first semester of Masters of Information Technology in Cybersecurity at Macquarie University. The event was held on Week 5 (18 August-24 August) of the course.

Our team named Team 55 participated in the event. The team consisted of me and four other members listed on the front page. This report is the individual technical report on the findings of the CTF-1 challenge.

The Capture the Flag-1 (CTF-1) event provided an opportunity to apply the knowledge and skills acquired throughout the first 4 weeks of Offensive Security (COMP6320) course. Each member of Team 55 contributed to solving the challenges, and this report details the individual technical approach I took to tackle the problems encountered during the event.

The CTF-1 experience was both challenging and rewarding, providing valuable insights into real-world cybersecurity scenarios. Through this report, I aim to demonstrate my understanding of the offensive security concepts taught in the week 1-4 and the practical application of these concepts in a simulated environment.

1.2 Objective

CTF-1 consisted of 5 flags each worth 10 points each. The objective of the event was to find the 5 different flags in a simulated environment. The simulated environment in this case was a vulnerable Kali Linux system. Each flag had its own system which was accessed through telnet. Our team was able to solve 2 flags worth 20 points in total.

1.3 Ethics

In participating in the Capture the Flag-1 (CTF-1) event, it was imperative to adhere to strict ethical standards, as written on the University policy, and the “Acceptable usage of hacking tools agreement”. The CTF-1 event was conducted within a controlled environment provided by the course instructors, ensuring that all activities were confined to the designated simulated systems.

2. FLAGS

2.1 Flag 1

Challenge Details

Challenge Name: RTFM

Hint: “This is a based one”

Points: 10

Difficulty: Easy

Objective: Retrieve the hidden flag located somewhere in the system.

Date: 18/08/24

Methodology

1. Accessing the Challenge

- **Actions Taken:**
  - Logged in to the CTF Scoreboard at https://offsec.site/ctf1/ to gain access to the challenge.
  - Accessed the virtual Kali Linux environment via the web portal at https://offsec.site/kali/ using the provided credentials.
- **Outcome:** Successfully gained access to the Linux server environment for the challenge.

2. Connecting to the Challenge Server

- **Actions Taken:**
  - Installed telnet using `sudo apt install telnet`.
  - Logged in to the server hosting the "RTFM" challenge using the command `telnet 10.55.1.10`.
  - Logged in to the server as a guest user.
- **Outcome:** Successfully connected to the server where the "RTFM" challenge was located.

3. Initial Exploration and Understanding the Challenge

- **Actions Taken:**
  - Listed directory contents using `ls -la`.
  - Searched online for the meaning of "RTFM" and learned that it stands for "Read The Fucking Manual."
- **Outcome:** Understood that the challenge likely involved using Linux manual pages (man) to find the flag.

4. Searching the Linux Manual

- **Actions Taken:**
  - Explored Linux manual commands (“man”, “man man”) to learn about accessing various manuals.
  - Tried different man commands related to potential keywords such as ls, flag, pages, etc.
- **Outcome:** Discovered a custom man page for flag, which contained filler text but suggested progress.

5. Analyzing the Custom man Pages

- **Actions Taken:**
  - Analyzed the `man flag` page, finding an encoded string: `MZQWY43FEBTGYYLH`.
  - Attempted to enter the string as the flag, but it was incorrect.
  - Found a clue to check the `man offsec` and `man rtfm` pages.
- **Outcome:** Found another encoded string in the `man rtfm` page, which seemed more promising.

6. Decoding and Retrieving the Flag

- **Actions Taken:**
  - Decoded the string `MZWGCZ33GVTGEZRVMUZTQNTGG44DMNJRMQYTAZRRHFSTINJWGEZTSYJWGQZX2===` using base32 with the command echo `"MZWGCZ33GVTGEZRVMUZTQNTGG44DMNJRMQYTAZRRHFSTINJWGEZTSYJWGQZX2===" | base32 –decode`.
- **Outcome:** Successfully retrieved the flag “`flag{5fbf5e386f78651d10f19e456139a643}`” and completed the challenge.

Findings

- **Flag Retrieved:** `5fbf5e386f78651d10f19e456139a643`
- **Location:** The flag was hidden in a custom man page (`man rtfm`), encoded in base32 format.
- **Challenges:** The primary challenge was identifying and decoding the custom man pages and the use of encoding/decoding techniques.

Reflection

- **Learning Outcomes:** This challenge highlighted the importance of needing to pay attention to hints and analyze custom system files critically and the application of encoding/decoding techniques.
- **Tools & Techniques:** The challenge was solved using basic Linux command-line tools (`man, base32, telnet`), demonstrating the practical application of these utilities in a real-world scenario.

2.2 Flag 2

Challenge details

Challenge Name: Spartan

Hint: “Collect the three sea shells”

Points: 10

Difficulty: Easy

Objective: Retrieve the hidden flag located somewhere in the system.

Date: 21/08/24

Methodology

1. Installing and Connecting via Telnet

- **Actions Taken:**
  - Logged in to the server hosting the "Spartan" challenge using the command “telnet 10.55.1.20”.
  - Logged in to the server as a guest user.
- **Outcome:** Successfully connected to the server where the "Spartan" challenge was located.

2. Initial Exploration and Understanding the Challenge

- **Actions Taken:**
  - Searched the name of the challenge and the hint. Could not find anything of significance.
  - Typed “Linux Sea shells” in Linux. Finally came across different Linux shells such as bash shell, zsh shell, bourne shells, c shells etc.
  - Realized “sea shell” could mean c shell
  - Searched how to access c shell and found the `csh command.`
- **Outcome:** Successfully decoded the hint and `csh` command.

3. Executing Commands in Shell

- **Actions Taken:**
  - Entered the command `csh` to switch to the C shell, followed by `bash`, and observed the terminal response: `1% Reset tty pgrp from 1077 to 1074.`
  - Repeated the command sequence `csh` followed by `bash`, and then `csh` again, leading to a sequence of outputs: `1%`, `2%`, `3%`.
  - At the `3%` prompt (as denoted in the hint “3 sea shell”), typed `flag` and received the encoded flag text: `ZmxhZ3tmNTA1MmVhYjg5MjRiZmY1NGIxYTFiODJkY2QyOGNiNH0K`.
- **Outcome:** Successfully retrieved an encoded flag after executing a series of shell commands.

4. Decoding the Flag

- **Actions Taken:**
  - Used the base64 decoding command to decode the retrieved flag text: `echo ZmxhZ3tmNTA1MmVhYjg5MjRiZmY1NGIxYTFiODJkY2QyOGNiNH0K | base64 -d`.
- **Outcome:** Successfully decoded the flag, revealing the flag: `flag{f5052eab8924bff54b1a1b82dcd28cb4}`.

Findings

- **Flag Retrieved:** `f5052eab8924bff54b1a1b82dcd28cb4`
- **Location:** The flag was hidden in the shell environment and was revealed after following a specific sequence of commands as denoted in the hint section.
- **Challenges:** The main challenge was decoding the hint and from the hint identifying the correct sequence of commands to execute in the shell.

Reflection

- **Learning Outcomes:** This challenge emphasized the importance of understanding shell environments and the use of command sequences to trigger hidden outputs. Additionally, it reinforced the need for proficiency with encoding/decoding techniques such as base64.
- **Tools & Techniques:** The combination of telnet, shell commands (`csh`, `bash`), and base64 decoding was critical in successfully solving the challenge.

3. CONCLUSION

The Capture the Flag-1 (CTF-1) event provided a practical and challenging opportunity to apply the concepts learned during the first four weeks of the Offensive Security (COMP6320) course. By participating in this event, our team, Team 55, was able to engage directly with real-world cybersecurity scenarios in a controlled environment, allowing us to test our skills and knowledge.

Throughout the CTF-1 event, we successfully captured two of the five flags, demonstrating our ability to analyze problems, utilize appropriate tools, and apply systematic methodologies to achieve our objectives. The challenges we encountered required us to navigate Linux environments, decode encoded data, and interpret hints, all of which are fundamental skills in the field of cybersecurity.

The event also highlighted areas for improvement, particularly in terms of enhancing our proficiency with advanced tools and refining our teamwork under time constraints. Despite these challenges, the experience was both rewarding and educational, providing valuable insights into the practical application of offensive security techniques.

In conclusion, the CTF-1 event was an essential part of our learning process in the Offensive Security course. It allowed us to translate theoretical knowledge into practice and provided a clear understanding of the areas where further development is needed. The skills and insights gained from this experience will be crucial as we continue to advance in our studies and careers in cybersecurity.