| Cybersecurity |
| --- |
| Day 3 Activity Guide |

## Attacking Rekall’s Windows Servers CTF

### Project Scenario

For this week’s project, you’re playing the role of penetration testers hired to conduct a penetration testing engagement by **Rekall Corporation**.

* On Day 1, you found vulnerabilities within Rekall Corporation’s web application.
* On Day 2, you found vulnerabilities within Rekall Corporation’s Linux Servers.
* Today, you will continue to exploit Rekall's technical infrastructure, but you’ll focus on the organization’s Windows servers and vulnerabilities related to Windows operating systems.
* Like you did on Days 1 and 2, you will also find “flags” during your exploitation.

As you work through the project, remember to continue completing your required deliverable, the **penetration testing summary report**, and to take screenshots of your exploits that you’ll include in this report.

### Project Resources and Setup

You'll use the following resources to complete today’s project:

1. **Rekall’s environment**

* You will access today’s activity within your Project 2 Lab.
* We recommend that you use the Kali Linux server as your attacking server.
* Rekall’s Windows servers will be accessible from the Kali Linux machine.

2. **CTF flag submission page**

* Within your Kali Linux browser, open a second tab and access your CTF page.
  + Your instructor will provide the custom website for your CTF when you are ready to begin.
* Once you have accessed this page, select “Register” on the top right to register your account
  + Don’t forget your password in case you need to log back in!

### CTF Instructions and Rules

#### Instructions

* As penetration testers, you are tasked with finding all vulnerabilities within Rekall’s Windows servers.
* As in Day 1 and 2’s activities, you are also tasked with finding “flags” by exploiting these vulnerabilities.
* The flags are hidden across various Windows hosts within Rekall’s environment.
  + Many flags are hidden within the Windows hosts and titled Flag 1, Flag 2, etc.
  + Some flags are the answer to a specific challenge, such as: What is the IP of your machine?
  + Flags labeled Flag 1, Flag 2, etc. consist of a mix of letters and numbers: e.g., “Flag 1: d8sksydasksdy”.
* Once you have found your flag or answered your question, enter the flag on the CTF flag submission page.
* Don't forget to take screenshots of the exploits you discover, as you will submit them in your summary!

#### CTF Flag Submission Page

* This webpage contains the 10 available flags.
* Today’s flag categories represent the phases of a penetration test engagement. For example:
  + **Reconnaissance**: This category contains challenges that use open source intelligence tools.
  + **Scanning**: This category contains challenges that use scanning tools, such as Nmap and Nessus.
  + **Exploitation**: This category contains challenges that use exploitation tools, such as Metasploit.
  + **Post Exploitation**: This category contains challenges that use post-exploitation tools, such as Meterpreter.
* The points awarded for each flag are indicated in its respective flag box.
  + The more challenging the flag, the more points will be awarded.
* Be sure to read the details in each flag box for important guidance on how to acquire that specific flag.
* Once you find a flag, select the box with the corresponding flag number, and enter the flag.
* You can view your point total by selecting the “Scoreboard” option at the top of the page.

#### CTF Hints

* This CTF provides you an option to “pay” for hints with points.
* Clicking on a flag will also display any available hints for that flag and the points it costs to unlock those hints.
  + **Note**: You must have already been awarded the points before you can use them to “pay” for hints.

#### Additional Hints for Success

* Rekall’s CISO, Jessica Smith, has several concerns about Rekall’s Windows security. Specifically, she mentioned concerns about the following:
  + Developers hosting private company data on Rekall’s official GitHub account.
  + The security of file sharing services.
  + Old versions of software.
  + Poor password policies.
  + Unnecessary scheduled tasks.
* Use the internet to help you figure out methods for exploiting these vulnerabilities.
* Refer to your class notes and slides to help find several of the flags.
* Certain exploits can be used to find information that will help you find other flags.
* Most of the exploits that you’ll use were covered in class, but there are some new exploits which will require additional research.
* Trying and failing is often part of a penetration tester’s work, so don’t be afraid to attempt multiple exploits until one is successful.
* The 10 available flags are discoverable at different locations:
  + One flag is outside of the network and requires OSINT.
  + Six flags are on the Windows 10 machine.
  + Three flags are located on the Server 2019 machine.
    - One of these, the final flag, is the Administrator user’s password hash on Server2019. This hash does not need to be cracked.

#### CTF Rules

* Each group will start at the same time, once the URL for the CTF has been provided.
* The team with the most points at the end of the allotted time will win.
* You can use all available resources to assist you: class notes, slides, internet resources, tools, etc.
* Your instructor or TA can assist with technical or lab access issues, but will not be able to provide guidance for finding the flags.

### Conclude and Submit Your Project

Congratulations on completing your second project! Complete the following important instructions to submit and conclude your project.

* **Project Deliverables**
  + Complete your penetration testing summary report, and submit it through Canvas.
* **Interview and Resume Guidance**
  + When networking and talking to potential employers, you should be able to reference the work done on this project to answer specific interview questions or to demonstrate your skills within a specific domain.
  + Refer to the following document for guidance on how to add your project to your resume, discuss your project, and answer potential interview questions regarding your project activities: [Interview and Resume Guidance](https://docs.google.com/document/d/1BshXKvp_OI8YHRSYT8SzvRQhN6hmPSt266dUFehqK7U/edit?usp=sharing).

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.