Cybersecurity

Project Week: Attacking Windows Servers

Project Week Day 3

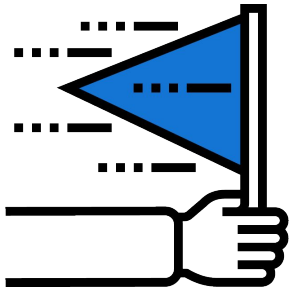
Welcome

This week, you're playing the role of penetration testers hired to conduct a penetration testing engagement by Rekall Corporation.

Project 2

On Days 1 and 2, you found vulnerabilities within Rekall's web application and Linux servers.

Previous lesson | **This lesson**

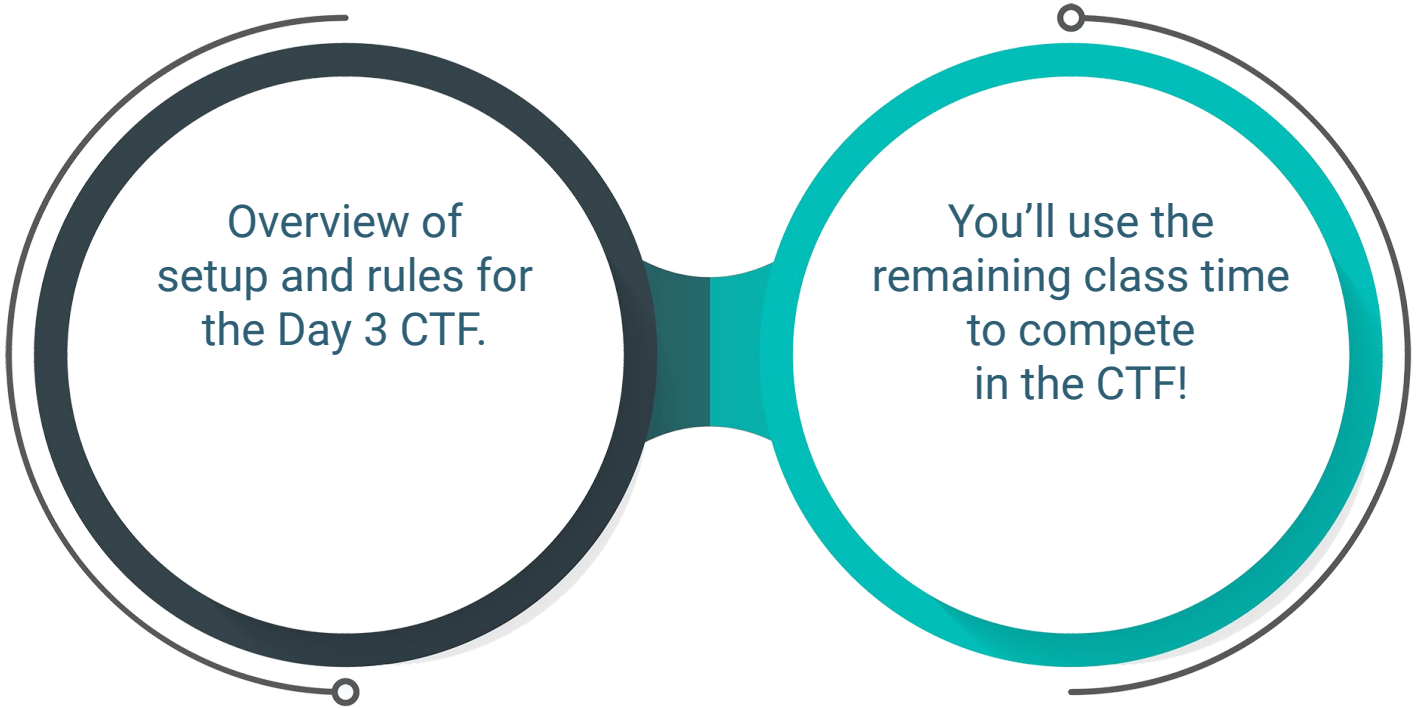


You'll continue finding "flags" during your exploitation.

Today, you'll continue exploiting Rekall's technical infrastructure, but you'll focus on Rekall's Windows servers and vulnerabilities related to Windows operating systems.

Today’s class

Today’s class will proceed as follows:



Day 3 Project Overview

Project Resources and Setup

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.

Project Resources and Setup

CTF Flag Submission Page

- You'll also access your CTF page within your Lab.
- You'll be provided a custom website for your class's CTF when it's time to begin.
- Once you have access to the page, register for an account.

Remember your password in case you need to log back in!

CTF Instructions

You are tasked with finding vulnerabilities within Rekall's Windows servers and 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 web page contains the 10 available flags.Today's flag categories represent challenges associated with 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.

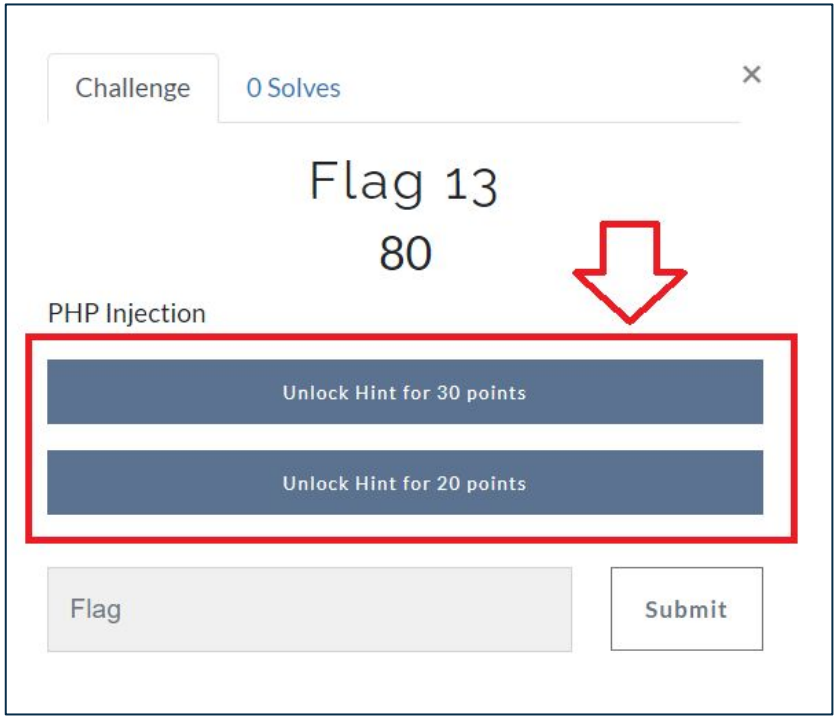
CTF Flag Submission Page

- 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 for guidance on how to acquire that specific flag.
- Once you find a flag, select the box with your 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 already have been awarded the points before you can use them to “pay” for hints.

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.

Hints for Success

- 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.

Hints for Success

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

Rules for today's activity:

- 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 such as Burp Suite, etc.
- If you are able to exploit a vulnerability and a flag does not display, please contact your instructor or TA to receive the flag.
- Your instructor or TA can assist with technical or lab access issues, but will not be able to provide guidance for finding the flags.

Questions?

Activity:

Exploiting Windows Servers

In this activity, you'll work toward completing the project's Day 3 tasks.

Suggested Time:
2 hours 20 minutes

Time’s up!

Let’s review

Questions?

The End