| Cybersecurity |
| --- |
| Day 2 Activity Guide |

## Attacking Rekall’s Linux 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.
* Today, you will continue to exploit Rekall’s technical infrastructure, but you’ll focus on the organization’s Linux servers and vulnerabilities related to Linux operating systems.
* Like you did on Day 1, 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.
* Once you have logged into the Lab from your Hyper-V, select the “Kali” machine.
* Log in to Kali with the following credentials:
  + User: root
  + Password: kali
* Open a terminal, and cd over to: /root/Documents/day\_2
  + Type: docker-compose pull and press Enter.
  + Type: docker-compose up and press Enter.
  + Leave this window open.
  + From your terminal, open a new tab where you can conduct today’s tasks.
* You can access Nessus by opening a browser and navigating to: <https://kali:8834/>
  + If Nessus does not start automatically, click on the Kali Linux logo in the upper left-hand corner
    - Click 02- Vulnerability Analysis
    - Click nessus start (deleted)
  + Use the following credentials:
  + User: root
  + Password: toor

2. **CTF flag submission page**

* Within your Lab 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.
  + Remember 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 in Rekall’s Linux servers.
* And, as in Day 1’s activity, you are tasked with finding “flags” by exploiting these vulnerabilities.
* The flags are hidden across various Linux hosts within Rekall’s environment.
  + Many flags are hidden within the Linux 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 12 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

* 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.
* To start Nessus on your machine, search for Nessus in your list of applications and select the “Start Nessus” option.
  + Then select the Nessus icon on top of your browser
* 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.

#### 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.

© 2023 edX Boot Camps LLC, a 2U, Inc. brand. All Rights Reserved.