Teradici Corporation

4601 Canada Way, Suite 301,
Burnaby, BC, V5G 4X7 CANADA
www.teradici.com

SRE/DevOps - Take Home Test

Overview

This document is a take-home assignment for assessing your technical ability as well as your analytical skills. You may use the internet to help with these questions. If a question is ambiguous, feel free to make assumptions. Please provide us with your assumptions, working code and any instructions on running your code. Please provide a link to a publicly accessible code repository (e.g., GitHub, Bitbucket, etc.) containing your work.

Finally, we would like to know how much time you spend on each question. This information will not be used to determine you as a candidate but will be used to help us refine the questions as needed.

Bash

1. Write a script that accepts a remote host and a series of ports or port ranges (e.g., 5000 or 5000-5200). Use **`netcat`** to scan for connectivity to each port or port range and report the results.
2. Write a script that accepts a filename, a regular expression, and a replacement string. This script will replace all regular expression occurrences with the replacement string inside the file and return the modified content as a string.
3. Write a script with a function that accepts a string to insert, a line number and a filename. The function should open the file and insert the string at the first occurrence of the line number and all increments of the line number until the end of the file is reached. e.g., if **`line_number`** is **`5`**, lines 5, 10, 15, etc. should be modified until EOF is reached.

Teradici Corporation

4601 Canada Way, Suite 301,
Burnaby, BC, V5G 4X7 CANADA
www.teradici.com

Python

For questions in this section, you may wish to use Google's Colaboratory service for interactive Python notebooks (https://colab.research.google.com/) and share links to the resulting notebook(s) with us.

1. Write a script that uses GitHub's REST API to retrieve the following information from https://github.com/teradici/deploy:
    a. Display the "Author Name" and the total number of commits for the user who has made the most commits for all time.
    b. Count the number of commits which occurred during the period from July 1, 2018 – Aug. 30, 2018 and print the total.

Please note that these APIs can be accessed anonymously and do not require authentication. The following resources will be helpful:

- GitHub commits API: https://developer.github.com/v3/repos/commits/
- general GitHub API documentation: https://developer.github.com/v3/
- Python requests library to help with making HTTP requests: http://docs.pythonrequests.org/en/master/ (if you are using Colaboratory, this library is already available to be imported; otherwise, you will need to install it locally in some fashion)

Terraform

1. Create a terraform script that creates the following on AWS or GCP:
    a. One VPC
    b. One subnet
    c. Two virtual machines with:
        i. Public IPs
        ii. The latest Ubuntu 20.04 image released by Canonical.
2. Using the previous Terraform script as a basis, extend to ensure only a selected IP address provided when performing a **`terraform apply`** can access the VMs via SSH.
3. Extend the same Terraform script to output both the value of the internal and external IP of each VM on the completion of a successful **`terraform apply`**.

Teradici Corporation

4601 Canada Way, Suite 301,
Burnaby, BC, V5G 4X7 CANADA
www.teradici.com

Chef

Create a Chef cookbook that automates the following three tasks on Ubuntu 20.04 and include unit tests using the Spec of your choice.

1. Place an XML file in **`/home/demo.xml`** (depending on Windows/Linux) so that the file is owned by a non-root user, and only that user can read the file. Make it so the values inside the **`<test>`** tag are easily configurable without modifying the cookbook or recipe.

demo.xml:

```
<demo-xml>

      <test>hello world</test>

</demo-xml>
```

2. Configure the **`sshd`** service in Linux to automatically start on reboot.
3. Mount **`tmpfs`** at **`/tmp`**, and ensure it has **`nodev`** option without using **`/etc/fstab`**

Security

For this section please be sure to document the tools and process you used.

1. Clone, build and run the following docker image: https://github.com/marko999/metasploit2-docker
2. Scan the container and try to determine what service/versions are running on them, include the output or screenshot of your results.
3. List 2 CVEs this container may be vulnerable to based on your results.
4. Document any mitigation for these CVEs.