Redback Operations

WAZUH IMPLEMENTATION GUIDE

Redback Operations

Document Owner: Secure Coding Team
Last Modified By: Mehak

Last Modified on: 11 May 2024

Contents

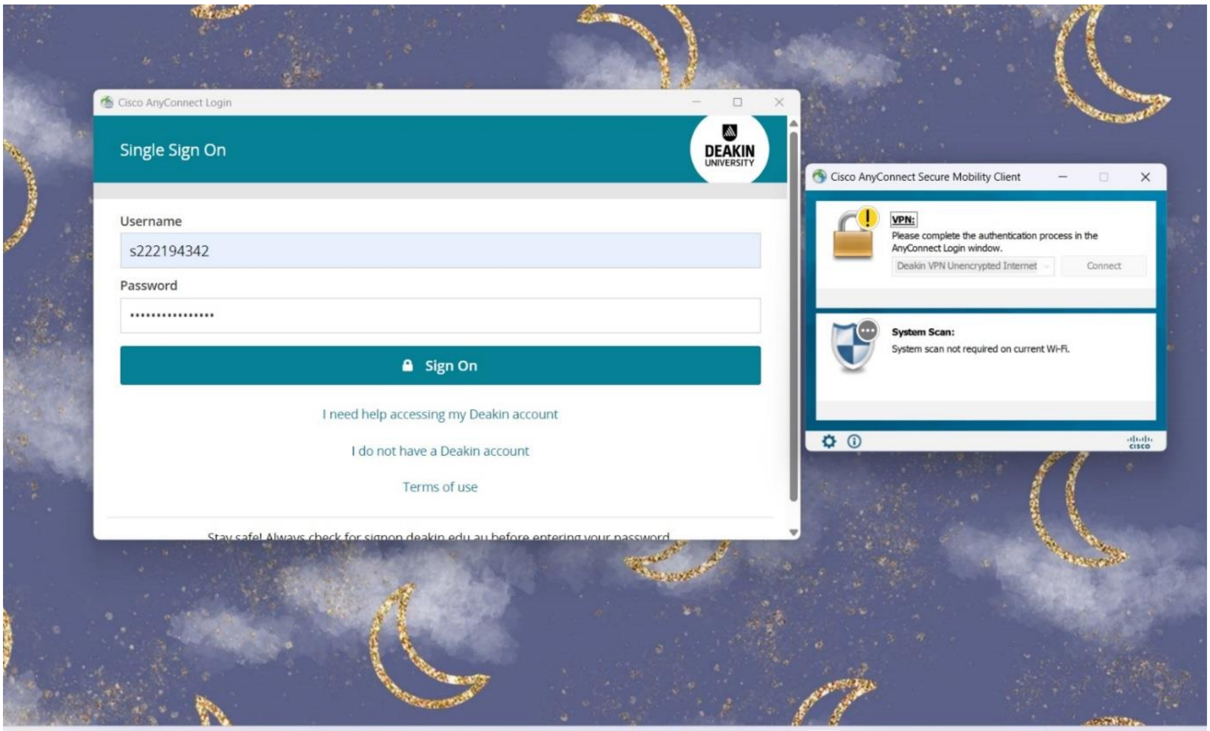
1. Accessing the VM via Terminal: Step-by-Step Guide

1. **Open Terminal**: On your local machine, open the terminal application. This could be Terminal on macOS, Command Prompt on Windows, or any terminal emulator on Linux.

2. **Connect to Deakin VPN (if outside Deakin network)**: If you are accessing the VM from outside the Deakin network, you need to connect to the Deakin VPN. Follow the instructions provided by Deakin University for connecting to the VPN using Cisco AnyConnect.

   https://software.deakin.edu.au/2019/04/16/cisco-anyconnect/

   Once connected to the Deakin VPN, you will be prompted to add your Deakin Credentials.



Cisco AnyConnect Login

Single Sign On

Username: s222194342

Password: ••••••••••••••••

Stay safe! Always check for signon.deakin.edu.au before entering your password.

Cisco AnyConnect Secure Mobility Client

VPN: Please complete the authentication process in the AnyConnect Login window.

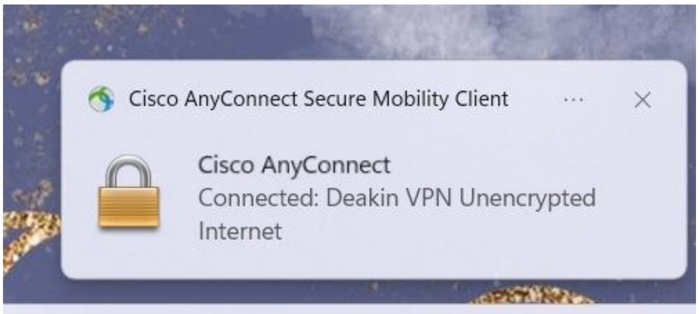
Deakin VPN Unencrypted Internet

System Scan: System scan not required on current Wi-Fi.

DEAKIN UNIVERSITY
Sign On
I need help accessing my Deakin account
I do not have a Deakin account
Terms of use
Connect
cisco

Figure 1 connecting to Deakin VPN

After entering your Deakin username and password and approving the DUO Push notification, you should encounter the following pop-up message.



Cisco AnyConnect Secure Mobility Client

Cisco AnyConnect
Connected: Deakin VPN Unencrypted Internet

Figure 2 connected to Deakin VPN

3. **SSH into the VM**: Once connected to the VPN (if required), you will need SSH access to connect to the VM. However, if the credentials for accessing the VM are unknown, please contact the appropriate administrator or team member who has access to the credentials. They will provide you with the necessary username and password to log in to the VM.

4. **Obtain Credentials**: Request the username and password required to access the VM from your supervisor, or the designated person responsible for managing the VM.

5. **Use SSH**: Once you have obtained the credentials, return to the terminal, and use the SSH protocol to connect to the VM. Type the following command:

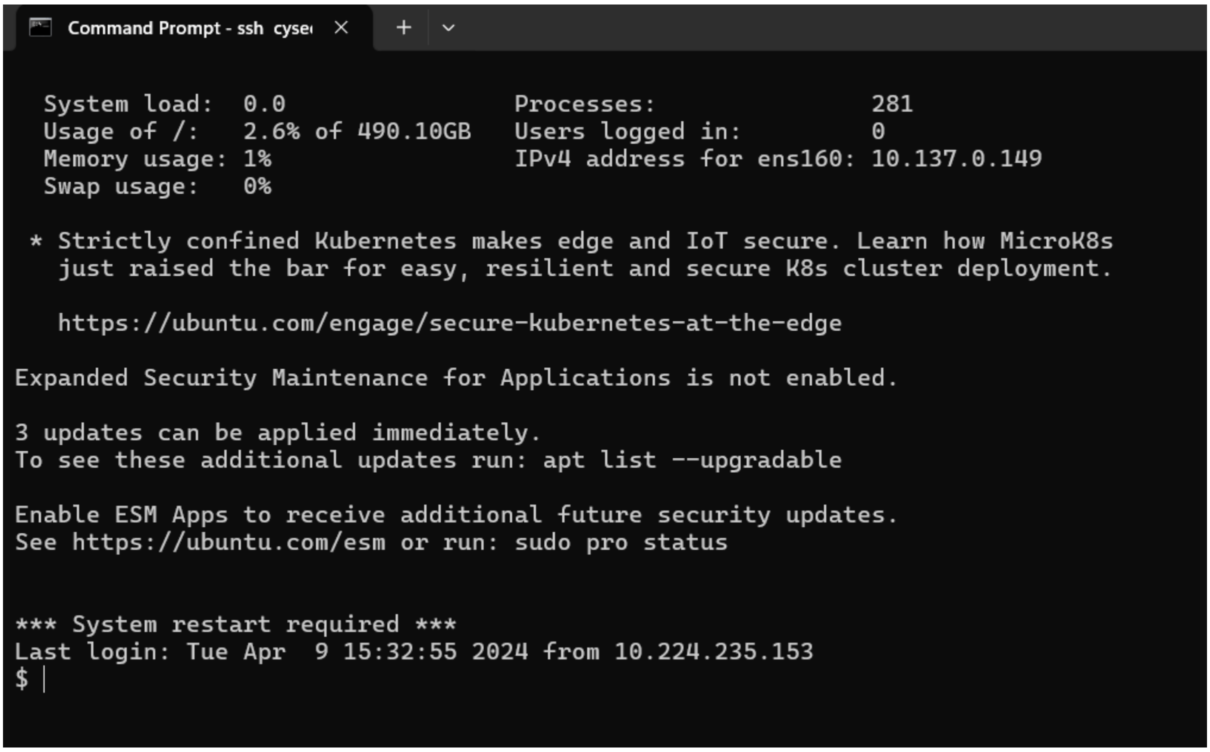
   ```
   ssh [username]@redback.it.deakin.edu.au
   ```

   Replace [username] with the provided username. Press Enter.

6. **Enter Password**: You will be prompted to enter the password for the user. Type the password provided by your administrator and press Enter. Note that when typing the password, characters will not be displayed on the screen for security reasons.

7. **Successful Connection**: If the credentials are correct, you will be logged into the VM via SSH and presented with the command prompt. You are now ready to execute commands on the remote VM.

8. **Perform Operations**: You can now perform various operations on the VM. The presence of the terminal prompt ($) indicates that you have successfully established a shell session on the VM. You can execute commands and interact with the system through the terminal interface.



```
  System load:  0.0                Processes:             281
  Usage of /:   2.6% of 490.10GB   Users logged in:       0
  Memory usage: 1%                 IPv4 address for ens160: 10.137.0.149
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

3 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


*** System restart required ***
Last login: Tue Apr  9 15:32:55 2024 from 10.224.235.153
$ 
```

Figure 3 VM access granted

9. **Logout**: When you are done with your tasks, you can log out of the remote VM by typing **exit** and pressing Enter. This will terminate the SSH session and return you to your local machine's terminal prompt.

2. Introduction to Wazuh and Implementation Guide

2.1 Introduction to Wazuh:

Wazuh is an open-source security monitoring platform designed to detect and respond to security threats in real-time. It offers capabilities for log analysis, intrusion detection, vulnerability detection, and more. By centralizing security event monitoring and analysis, Wazuh enhances an organization's ability to identify and mitigate security incidents, protecting critical assets and data.

2.2 Why Implementing Wazuh:

The implementation of Wazuh on our company VM is crucial for bolstering our cybersecurity posture. By deploying Wazuh, we aim to achieve the following objectives:

1. **Enhanced Threat Detection:** Wazuh provides advanced threat detection capabilities, allowing us to identify and respond to security threats promptly.
2. **Improved Incident Response:** With real-time monitoring and alerting, Wazuh enables us to respond swiftly to security incidents, minimizing their impact on our systems and data.
3. **Compliance Requirements:** Wazuh helps us meet regulatory compliance requirements by providing comprehensive security monitoring and reporting capabilities.
4. **Centralized Security Monitoring:** By centralizing security event monitoring on a single platform, Wazuh streamlines our security operations and improves visibility into potential threats.

2.3 Implementation Guide:

Step 1: Log in via SSH

- Use SSH to connect to the VM. If you are unsure how to do this, refer to the earlier instructions provided.

Step 2: Preparing the System

- Switch to the root user:

```
sudo su
```

- Update the system and install necessary upgrades:

```
apt update && apt upgrade -y
```

  Note: This process may take a few minutes.

- Configure required system parameter for Docker:

```
echo "vm.max_map_count=262144" | sudo tee -a /etc/sysctl.conf
```

Step 3: Installing Docker and Docker Compose

- Install Docker and Docker Compose

  ```
  curl -sSL https://get.docker.com/ | sh
  curl -L "https://github.com/docker/compose/releases/download/v2.20.3/docker-compose-$(uname -s)-$(uname -m)" -o /usr/local/bin/docker-compose
  chmod +x /usr/local/bin/docker-compose
  ```

Step 4: Deploying Wazuh

- Change to the deployment directory and clone the Wazuh Docker repository:

  ```
  cd /opt/ && mkdir deploy && cd deploy
  git clone https://github.com/wazuh/wazuh-docker.git -b v4.5.0
  cd wazuh-docker/single-node/
  ```
- Generate indexer certificates

  ```
  docker-compose -f generate-indexer-certs.yml run --rm generator
  ```
- Start Wazuh using Docker Compose:

  ```
  docker-compose up -d
  ```

Step 5: Accessing Wazuh Web Interface

- Access the Wazuh web interface using the external IP address of the VM from your browser:
  http://VM_External_IP:5601
  Make sure to replace **VM_External_IP** with the actual external IP address of the VM.
  Use the following default credentials to log in:
  - Username: kibanaserver
  - Password: kibanaserver

3. Conclusion:

Conclusion: Following these steps, you will successfully deploy Wazuh on the company VM, enhancing our cybersecurity monitoring capabilities. While the company does not currently have an external IP address set up, once established in the future, it can be utilized to access the Wazuh dashboard remotely. Regular monitoring and maintenance of the Wazuh deployment are essential to ensure effective threat detection and incident response capabilities.