CCDC Homework #5

Resources

Remember to always use safe Internet practices.

Link to ISOs if you want to work on your local computer:

1. **Ubuntu 20.04:**
    a. **https://da.gd/g0MwDe**
2. **CentOS 8 Stream**
    a. **CentOS 8 Stream Download Mirrors**
3. **Windows 2022:**
    a. **Windows Server 2022**
4. **Activation Keys can be found here:**
    a. **https://docs.microsoft.com/en-us/windows-server/get-started/kms-client-activation-keys**

Questions

1. Why would a business want their Linux machines joined to an Active Directory domain?
2. What is Windows Subsystem for Linux? Why does it exist?
3. What's the difference between passwd and chpasswd?
4. Is it generally better to use a root session when hardening a Linux machine as opposed to prefixing every command with `sudo`? Why or why not?
5. How would you implement a secure password policy on Ubuntu? How does this differ from the implementation on CentOS? Include your configuration for both.
6. Learn the commands and syntax for `iptables` and `ufw`. What are the primary differences between the two? Then, create the following rules using equivalent `ufw` and `iptables` commands:
    a. Set a default deny rule on incoming connections.
    b. Allow port 22 over tcp only.
    c. Allow your mysql port over tcp only (find out what port that is).
    d. Deny port 80 over both tcp and udp.
    e. Allow only 10.10.10.4 to access port 3306.
7. What is a `netstat` command you can use to view your current connections to detect reverse shells?

Lab (Part A)

1. On your CentOS machine create a new user named “centosadmin” and give them a password of your choosing. Add them to the group for CentOS administrators (Google what that group is if you need to).
2. Set up an SSH server on CentOS.
3. Connect to it by signing in as “centosadmin” from another VM (such as Ubuntu).

Lab (Part B)

1. Ensure your Ubuntu image has an SSH server
2. Create an SSH key pair using the Ed25519 algorithm and name them “ccdckeys” and give them a password of your choosing. Transfer your public key to another VM (such as CentOS) running an SSH server.
3. After password authentication on your SSH server is disallowed, use Ubuntu to connect over SSH to the other VM using the key.

Lab (Part C)

1. Connect your Ubuntu 20.04 VM to the Active Directory domain. If you are working on your local computer, you may reuse your domain from last week if you want, or you can make a new one for additional practice.
    a. Make sure you can login using AD credentials over SSH

Lab (Part D)

1. On CentOS 8 create a mail server using Postfix and Dovecot, with MySQL as a backend and RoundCube as a web mail client.
    b. Make sure you send emails from one AD user and receive as another AD user
        i. This implies you must connect CentOS to your domain!

Deliverables

1. **Submit a PDF with all of the following:**
    a. **answers to all the questions**
    b. **a screenshot of successfully SSHing into "centosadmin"**
    c. **a screenshot of successfully SSHing into CentOS with an SSH key**
    d. **a write-up on how you accomplished Part C that includes:**
        i. **a screenshot showing your Ubuntu VM being a part of the domain**
        ii. **a screenshot of you using SSH on Ubuntu to log into an AD user via your Ubuntu's SSH server**

    e. **a write-up on the steps you took to complete Part D that includes:**
        i. **a screenshot showing the MySQL database tables**
        ii. **a screenshot of mail being sent successfully**
        iii. **a screenshot of mail being received successfully**
2. **Make sure all sections and images are readable and labeled.**
3. **Name the file with the following format: FirstLast_CCDCHomework5.pdf**

If you are trying out for the team, make sure you submit your PDF in Canvas.

Otherwise, please use this form if you want to be graded:

https://forms.gle/at2XhAXSptio2i527.