CYBER SECURITY TEAM 2020

SSH (Ubuntu)

SSH is important in network management from a remote location. A network administrator can login to a server, and execute commands on the shell in a secure environment. Even through ssh is secure, there is need to make sure that it has been properly configured and that access to the server via ssh is filtered using a firewall and monitored using logs.

Activity

Install SSH on the server

```
sudo apt install openssh-server
```

```
sudo apt install openssh-client
```

Make sure that SSH is set to start up automatically when the server is powered on sudo

systemctl enable sshd.service

The main configuration file for the OpenSSH server application is /etc/ssh/sshd_config. Make sure you create a backup of the original configuration before making any changes:

```
sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.bak
```

Disable root to login remotely using SSH sudo

nano /etc/ssh/sshd_config

One of the recommended ways to secure your server when using OpenSSH is to disable the Root login. First, (create a new sudo user on your Ubuntu server – later in this lab), and then edit the OpenSSH server configuration file. Locate and uncomment the following line:

`#PermitRootLogin yes` Change

to:

```
PermitRootLogin no
```

To prevent an attacker using brute force attacks to access our system, **limit authentication attempts to**

3 and allow only a maximum of 4 sessions

Set a banner that will display this message " **Welcome to Cyber Ninjas. Unauthorized access is strictly prohibited and will be prosecuted to the full extent of the law**."

Change the default SSH listening port to 70.

Start SSH and make sure that it is running sudo

systemctl start sshd.service

Create a new user called Excellent and assign a user identity of (**750**)

Configure firewall to accept SSH connections only

Login remotely using SSH with the user created

As ROOT, check the Logs to see login information on the system and record the ip address of the computer used by Excellent to access the server

Change the port to **70** (If you are using vmware, otherwise you might close your session)

Login in again as Excellent and try to execute privileged instructions/commands e.g **useradd, userdel, vi /etc/shadow…etc**

Observe what happens?

In Linux, root has unlimited privileges but users can be given permissions to execute all or certain priviledged instructions if they have been added to the /etc/sudoers file

Add Excellent to the file using the command **visudo** and login to execute one of the previous instructions

View the logs as Excellent to see the activity. Check account all account activity for all accounts on the system.

Happy practice cyber ninjas!