Firewalls

In this homework, you will be applying a variety of Firewall rules on 3 different platforms.

- pfSense
- Linux
- Windows

This homework covers a lot of topics, both broad and specific. If you feel stuck at any point, please reach out to SecDev and we will be there to help.

Anything highlighted in Red should be shown via screenshot in the report. This is for ease of grading purposes.

The report for this should be written cleanly and like you have all been doing for the previous assignments. However, aim to have good notes and structures of the commands. Don't get to caught up in every detail. This assignment is more geared towards being a *cheat sheet* dealing with simple Firewalls.

Possible structure for your assignment report could be like this…

- Intro
- Prerequisites
- pfSense Firewall
- Linux [IP Tables]
- Windows
- Extra Credit
- Resources

pfSense

pfSense is the heart of your network. pfSense is typically your first line of defense in securing your network. pfSense, unlike Windows and Linux, is a network based Firewall, allowing you to both block and allow incoming and outgoing connections unilaterally.

For this part, you could try and use the command line given in pfSense, but us SecDev members would not recommend it. Instead, we will be using the GUI, by simply following these steps:

- Navigate to any one of your clients with a internet connection (hopefully all of them have this by now!)
- Type in your pfSense IP (10.42.**X**.1), where **X** is your Team Number
- You should be presented with the login for pfSense, the default credentials are:
  - Username: **admin**
  - Password: **pfsense**
- If you need to, go through the setup for pfSense (since you have setup pfSense through the CLI, most of this should be clicking 'Next').

Once logged in to pfSense, please screenshot the welcome menu. We will now set up some network based firewall rules:

Block All Ping Traffic to One of Your Windows Clients.

- Show the rule you made to do this
- Briefly explain why you might want to block ping responses in an Infrastructure | Internal Network.

Block All SSH Traffic Coming Into Your LAN Machines

- Attempt to SSH into your Linux machines from one of your DMZ machines (ssh user@ip , where user = client username, ip = client ip)
    - Document how you blocked SSH and show that you are not able to access your LAN from your DMZ (an error message will suffice).
- Assume we turned on logging for SSH.
    - Give a brief summary as to how you could use logging to your advantage in a real world scenario.
    - Is there someway to make logs… nicer, or cleaner? (Hint: look at common SIEMs). Why are these useful?
        - 2-3 sentences is enough

Set up a 1:1 NAT (Network Address Translation) for your Web Server

- https://docs.netgate.com/pfsense/en/latest/book/nat/1-1-nat.html
- Along with screenshots, please give a brief description as to why each step is necessary.
    - If you would like, have another System Security student access your servers through that Public IP! [If you want some extra points do this with another SysSec student, just show each of you connecting etc]

Linux

As we discussed in class, Linux provides us with `iptables` and `ufw`, which are very useful and powerful firewall tools. In this portion, you will set up some firewall rules using these commands.

Log on to either one of your Linux Machines.

- Block all incoming SSH connections from your Linux server (the server that is on your LAN).
    - Show the refused SSH connection from the server.
- Using `iptables`, now block all incoming traffic from your Windows machines ip's.
    - Please take a screenshot of these rules and show that you are not able to ping from your Windows Client to your Linux client.
- Save these rules to a text file, or save them to your `iptables` configuration file.
- Explain the importance of blocking incoming and outgoing traffic. What possible cases would require you to block either?

Windows

For Windows machines, you are able to either use the Windows Defender tool supplied with Windows (arguably easier), or use `netsh` to set up these Firewall rules.

- Using either Windows Firewall or your command line, block all inbound connections from your Linux Machines ip addresses (on your LAN)
  - Screenshot showing that your Linux machines can't ping your Windows client.
  - Give a brief description as to why you think it could be important to block inbound connections between your LAN clients.
- Allow outbound traffic to your pfSense router's ip address.
  - Screenshot your windows defender inbound and outbound rules showing that your custom rules are there (Name them something…unique).
- Block a program of your choice from accessing the internet.
  - You can either choose to block Microsoft edge (You may want it back afterwards), or install a program that accesses the internet and show that it is not able to do so after writing the Firewall rule (Chrome, Firefox, Email, etc.).
  - While you are at it, block Cortana from communicating out, we don't really like her anyways.

EXTRA CREDIT!

This is not a required part of the homework, but could help you during a defense competition. 😎

In pfSense, you are able to install packages and modules to make your life a little simpler. These can help you seek out unwanted traffic or malicious activity on your network. If you decide to do so, you will be installing a couple of these modules on your pfSense box, namely `ntopng` and `snort`.

If you would like more information on either of these, you can click on the **bolded** words to proceed to documentation, or ask your preferred SecDev member.

For this extra credit, please follow these steps…

Step 1: INSTALLATION

- Install both `ntopng` and Snort packages onto your pfSense router. You may have to update and upgrade packages on pfsense using the following command:
  - `pkg update -f`
  - `pkg upgrade -f`
- Please screenshot and show that both of these modules are available on your pfSense router.

Step 2: NTOPNG

- Using `ntopng`:
    - Find the top local host in your domain, screenshot and report on your top host, why does this make sense?
    - Find all operating systems that are connected to your firewall, screenshot the results from ntop.
    - Find one interesting information on your network using ntop and write a summary of what you found.

Step 3: SNORT

- Using Snort:
    - Setup Snort (Yes you must get the `oinkmaster` code by signing up), and attach snort to your LAN and DMZ interface
    - Once Setup, configure rules to detect malicious traffic. For the purposes of this assignment, you can setup port scanning alert rules.
        - To test this you can try port scanning one of your machines and seeing if it pops up as an alert.
    - Write a brief description as to how you could use Snort in a real world scenario, and why products like it are vital for an Infrastructure.

Step 4: CURIOSITY

- Find another package to install on pfSense that you think is especially interesting or useful.
    - Make sure to show the steps you took to install this package, including screenshots with descriptions.
    - Please explain why this particular package is of interest to you, and how you could use it in a real world scenario!

Fin