FSCT 8560 Assignment 1 - Firewall
Due: Tuesday, May 24th, 2022

Your goal is to secure a computer with iptables.

Provide three shell scripts:

- one to set up the default firewall rules
- one to add new firewall rules
- one to reset the firewall rules back to the defaults (all chains ACCEPT)
- (bonus) one to remove a firewall rule

Create a set of rules that will implement the firewall requirements. Specifically, the firewall will control:

- Set the default policies to DROP.
- Do not accept any packets with a source address from the outside matching your internal network.
- You must ensure the firewall rejects those connections that are coming the “wrong” way (i.e., inbound SYN packets to high ports).
- Drop all TCP packets with the SYN and FIN bit set.
- Do not allow Telnet packets at all.
- Accept all TCP packets that belong to an existing connection (on allowed ports).
- Inbound/Outbound TCP packets on allowed ports (configurable).
- Inbound/Outbound UDP packets on allowed ports (configurable).

It is required that:

- You design a test procedure that will test all of your firewall rules.
- The firewall/packet filter must be designed and implemented using Netfilter (iptables)

By default your firewall must:

- Permit inbound/outbound ssh packets.
- Permit outbound http packets.
- Permit outbound https packets.
- Only allow NEW and ESTABLISHED traffic to go through the firewall. In other words, you are doing stateful filtering.
- You must ensure that you reject those connections that are coming the "wrong" way, meaning inbound connection requests (unless of course, it is to a permitted service).
- Users should be able to add new rules for outgoing connections that can be restricted based on:
    - Destination port(s);
    - Destination ip address.
    - The port(s) and address are optional (eg. you can say this ip address and port or just this ip address which implies all ports, or just port which implies all ip addresses)

You must provide a video demonstration of your firewall that shows:

- The original setup (all ACCEPT)
- Run your setup script and show the rules (iptables -L)
- Show that the setup script properly handles the cases above

- Add a new service (port/ip address)
- Show that the new rule is properly handled
- Run the reset script and show that the firewall is reset

There will be an additional video with the details to be provided in class. This video will be created after the assignment has been handed in.

Submission

- Hand in complete and well-documented design work and the firewall script
- A formal and detailed test plan as well as the test results for each rule.
- Provide your test and firewall scripts and all supporting documentation.
- Include a set of instructions on how to use your script. Essentially a small "HOW-TO".
- Submit a zip file (not RAR, or any other format) containing all the code and documents as described below in the learning hub folder for this course under “Assignment 1”.
- Your report must follow the standard technical format.
- All documentation must be submitted in PDF format.
- The zip package must also contain all the materials outlined in the demo section above.
- Your zipped package MUST follow the following naming scheme: FirstName_LastName-StudentID.zip
- The zipped package must use the following subdirectory structure:
    - Documents: The report files in PDF format.
    - Scripts: Will contain the firewall scripts.
    - Packet Captures: All the packet captures for each test.
    - Videos: All of the demo videos for each task or test.