Scripting for Cybersecurity Assignment 2

Test Environment Setup

This is a companion document for the Assignment 2 brief.

Getting the Files

A zip file, assignment_2.zip is available on Canvas. This zip file contains the following files:

- prep_env.sh
- ip_addresses.txt
- passwords.txt
- assignment_2_cmds.txt
- mininet_launch_command.sh
- index.php
- login.php

Unzip the file in the lab VMs home directory. This can be done by either running the command: unzip assignment_2.zip or right clicking on the file and clicking on “extract”.

Preparing the VM

The prep_env.sh file is used to install the required software and prepare the Virtual Machine for testing the assignment.

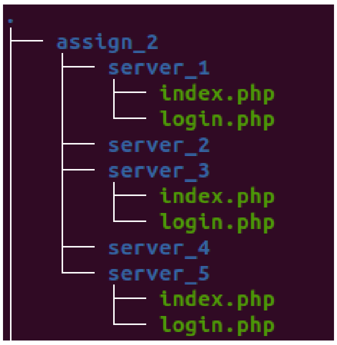
Note: *If you are not using the Scripting for Cybersecurity lab VM then you may need to modify the prep_vm.sh file or perform the operations within the script manually.*

Make sure the file is executable and execute it:

chmod +x prep_vm.sh

./prep_vm.sh

After the script has finished running you should have a new folder in your home directory on the VM called “assign_2” with the following files and folders inside of it:



```
.
├── assign_2
│   ├── server_1
│   │   ├── index.php
│   │   └── login.php
│   ├── server_2
│   ├── server_3
│   │   ├── index.php
│   │   └── login.php
│   ├── server_4
│   └── server_5
│       ├── index.php
│       └── login.php
```

These files will be used by the Mininet hosts.

Running Mininet

The command to run Mininet is in the mininet_launch_command.sh file

The command within the file, which can be used to run Mininet, is the following:

sudo mn --topo single,6 --test pingall --post assignment_2_cmds.txt

This command will run Mininet with 6 hosts (1 attacker and 5 servers).

The Mininet commands used to start services on the Mininet hosts are contained within the assignment_2_cmds.txt

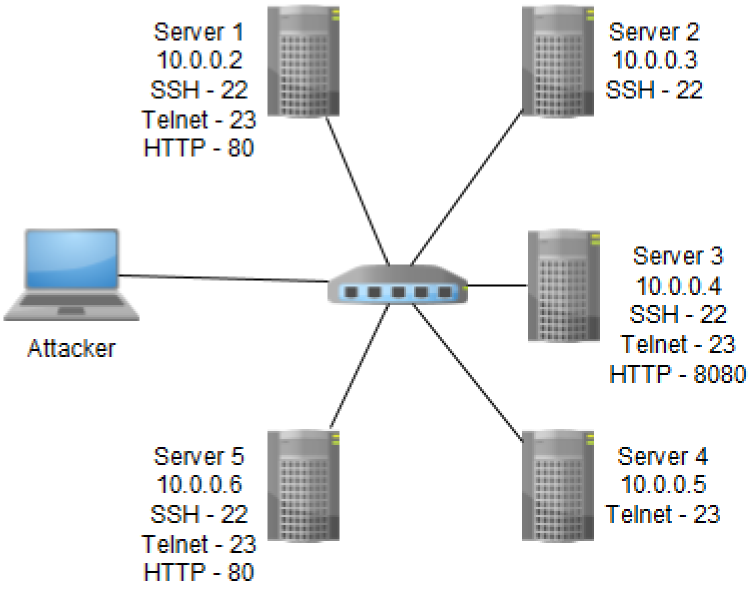
Only two terminal windows will show up when you run the command. If you wish to access the terminal windows for the other hosts you can edit the assignment_2_cmds.txt file.

When you are finished with Mininet and want to stop it, use CTRL+C in the terminal window from which you ran the command to start it up. Use the following command to clean up the Ubuntu host:

sudo mn -c

The Test Network

The Mininet network looks like this:



There is 1 attacker host and 5 server hosts. The servers are running some combination or Telnet, SSH, and a HTTP server on ports 22, 23, 80, or 8080. The IP addresses of each host are shown in the above image, as well as the services running on each of those servers.

You can confirm that your assignment script is working correctly by comparing the reachable IP addresses and open ports your script finds with the content of the above image.

Every server in the above images uses the username “ubuntu”. The password for Telnet and SSH will always be “ubuntu”. The passwords for the web pages will vary depending on the server.

Running your Script

When you launch Mininet the attacker terminal window will open. When you want to test your assignment script you should run it in the attacker terminal window.

The password.txt file contained in the assignment_2.zip file contains a list of passwords to be used for bruteforcing access to the services running on the Mininet hosts.

The ip_addresses.txt file contains a list of IP addresses to target.

You should therefore run your script like this:

```
./net_attack.py -t ip_addresses.txt -p 22,23,80,8080 -u ubuntu -f passwords.txt
```