IS-4543: Cyber Attack and Defend

Project Milestone Report for Milestone 1

Name: Delton Robinson

Section: IS-4543-001

Date: 10/4/2024

Milestone Report

This report includes the approved project proposal (included for easy reference), a summary of what was done during this project milestone, a description of what I learned during this milestone, and documentation of the work completed during this milestone.

Project Proposal

Project Idea 3: Honeypot Deployment for Network Intrusion Detection

Description: This project focuses on setting up an internal honeypot within a virtualized environment to lure and log simulated internal attack attempts. Using tools like Cowrie, an SSH honeypot, I will create a fake, "enticing" system for simulated internal attacks. The goal is to analyze common attack vectors in a controlled environment, without exposing the honeypot to external networks.

Milestones:

1. **Virtualized Environment Setup**
    - I'll begin by setting up a completely isolated virtual environment using VMware. This environment will contain multiple virtual machines, including the honeypot (potentially running Cowrie on a Linux VM) and at least one attacker machine (Kali Linux). The network will be fully internal, ensuring no exposure to external traffic, and configured to simulate a typical corporate or home network.
2. **Honeypot Configuration**
    - I'll install and configure a honeypot on a Linux VM, setting it up as an SSH honeypot. The system will be designed to look like a valuable internal server, with fake services, decoy files, and user accounts to entice attackers. I'll configure the system to log all actions in detail, including commands typed and files accessed.
3. **Simulated Attack Scenarios**
    - Using the attacker VM (Kali Linux), I'll simulate multiple types of attacks typically seen in an internal network scenario. This will include brute-force SSH login attempts, privilege escalation attempts, and file exploration. Each attack will be executed in a controlled manner, allowing the honeypot to capture detailed logs of the process.
4. **Analyzing Logs and Attack Patterns**
    - After completing the attack simulations, I'll dive into analyzing the logs captured by Cowrie. I'll look for patterns that could indicate specific attacker behavior, such as

common commands used after gaining access or file manipulation strategies. I'll use these insights to build a report on the attack patterns observed.

5. **Reporting and Future Implementations**
    - Finally, I'll create a detailed report summarizing the findings from the honeypot logs, describing the effectiveness of the honeypot in detecting and logging internal attacks. I'll also propose potential enhancements for internal network security, such as improved monitoring or stricter access control policies to mitigate the risks demonstrated during the simulation.

Summary of Activities

During the completion of this milestone, I created multiple machines within VMWare on my desktop to setup my virtual environment. In this milestone, I prepared my virtual environment with 4 machines; An Ubuntu honeypot that will run cowrie, a Kali Linux attacker, a Windows 10 "Family PC", and an Ubuntu Linux machine I'll use to examine the network traffic using snort.

The first step I took was downloading the Ubuntu iso file from its distributor to serve as my honeypot machine, as well as setting up cowrie on the machine. The process to install an Ubuntu VM within VMWare is simple, as all it took were a few clicks for the machine to be fully up and running. Once the machine was live, I began to use the terminal along with the cowrie documentation to install the packaged honeypot.

- The first step of installing cowrie according to their documentation was to install the necessary requirements, which in this case is Python 3.9+ & python-virtualenv. I installed these requirements using **#sudo apt-get install**
- I then created a user account for cowrie and cloned the GitHub repository within the newly created cowrie user's home directory.
- Next, I used the command **#python -m venv cowrie-env** in order to call python and run the venv module, which will create a virtual environment for me. In this case, a cowrie-env. Immediately after this I used the command **#python -m pip install --upgrade pip** to update my python package manager to the latest version, right before I run almost the same command, **#python -m pip install --upgrade -r requirements.txt**, to install and/or update any existing requirements for cowrie.
- I then started cowrie by running the command **#bin/cowrie start** (from the cowrie directory), which started running the cowrie honeypot on port 2222.

With my honeypot setup and cowrie running, I shifted my attention to my other machines. Beginning with my Kali attacker.

I setup Kali within VMWare through the UI and installed & ran Nmap to verify that the honeypot is configured to my liking. I also went ahead and attempted to connect to the honeypot port, and I was successful in "hacking" (just logging in using the command **#ssh root@[addr] -p 2222**) into the ssh port & guessing the password. (Any password works for the default settings on the cowrie honeypot, due to the login attempt itself being captured, and the attacker being presented with a fake server to snoop around within; However, this setting can be changed, allowing for me to capture brute force attempts.)

Next, I used the VMWare UI to setup an identical Ubuntu machine to the one running the cowrie honeypot; However, I installed snort on this machine to analyze the network traffic between the machines on the network.

Finally, I created a Windows 10 Machine to represent a “Family PC”. This machine only serves the purpose to add more traffic to the network, and potentially make the network seem a bit less artificial.

Description of Learning Completed

I gained hands-on experience setting up Cowrie on an Ubuntu machine within a virtual environment. This deepened my understanding of ports and services on a machine. I also learned that cowrie is heavily configurable, so I learned that I could do much more with this honeypot than I initially thought. I can configure the fake server the attacker is presented with to make it appear as if it’s a personal machine and not a server, or a bank server, or anything else that I may want the attacker to see to log their movements within my system.

I also learned much about Python’s virtual environment management tools. I learned more about the python virtual environment module, and a few of the uses for it. I will be researching this module more, however I think I have the understanding necessary to run cowrie, as much of my time will go into configuring cowrie and making the fake server appear legitimate. This part of this milestone allowed me to gain hands-on experience with Python’s virtual environment management tools, due to it being needed to install cowrie.

Throughout the process of setting up both of my Ubuntu machines (the honeypot and my snort analysis), I’ve learned a fair amount about configuring the same machine for different purposes. It sounds simple, but the process of using the same Ubuntu machine and just using it to run snort did open my eyes a bit more to the reality that I was already aware of, which is that computers really are just blank slates that take instructions.

I also learned the very basics of snort, just so I could install it onto my second Ubuntu machine. I will dive deeper into snort in future milestones, in regard to capturing the traffic between the kali machine and the honeypot.

Finally, the integration of different operating systems like Kali Linux for attacking simulations, Ubuntu for network traffic monitoring, and a Windows 10 machine to simulate a real user environment—helped me understand how different components in a network interact. Setting up this environment solidified my understanding of network traffic flows and how to make the network appear more realistic to potential attackers, which is a critical aspect when simulating real-world cyberattacks.

In summary, this milestone enhanced my practical skills in setting up honeypots, managing virtual environments, performing network traffic analysis, and creating realistic network environments. These experiences are foundational for improving my ability to deploy and analyze security measures in a controlled lab environment.

Documentation of Work Completed

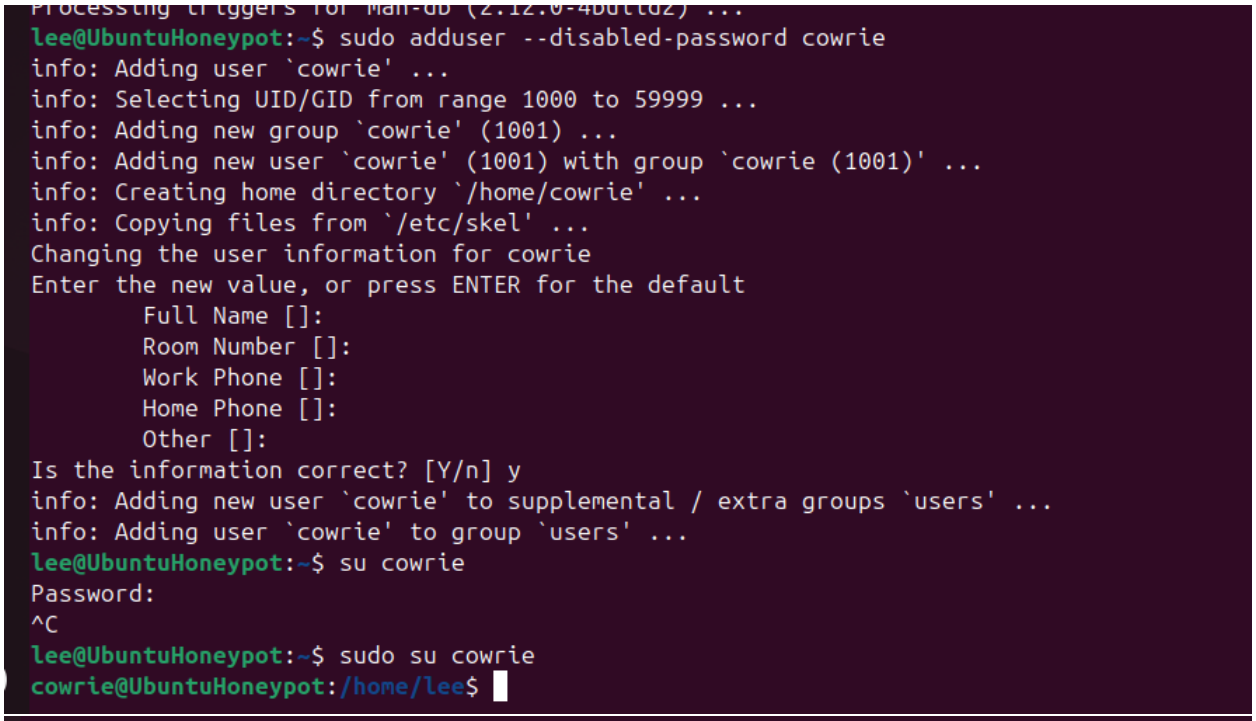
Setting up my Honeypot.

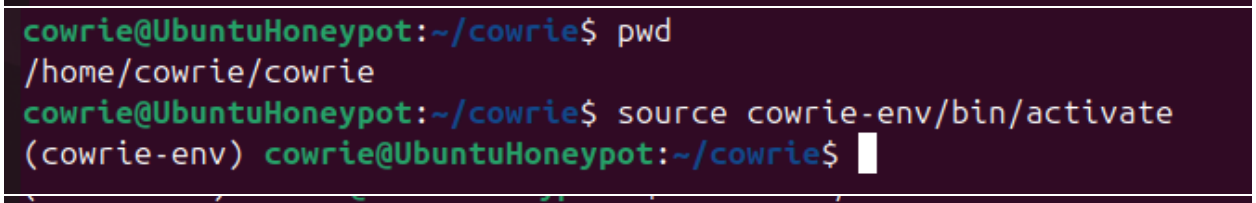
1.

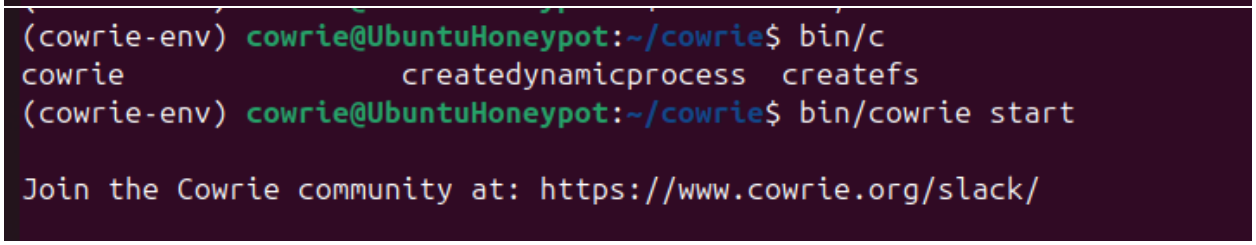
```
lee@UbuntuHoneypot:~$ sudo apt-ghet install git python3-venv libssl-dev libffi-dev build-essential libpython3-dev python3-minimal authbind
[sudo] password for lee:
sudo: apt-ghet: command not found
lee@UbuntuHoneypot:~$ sudo apt-get install git python3-venv libssl-dev libffi-dev build-essential libpython3-dev python3-minimal authbind
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
libssl-dev is already the newest version (3.0.13-0ubuntu3.4).
libffi-dev is already the newest version (3.4.6-1build1).
build-essential is already the newest version (12.10ubuntu1).
libpython3-dev is already the newest version (3.12.3-0ubuntu2).
python3-minimal is already the newest version (3.12.3-0ubuntu2).
authbind is already the newest version (2.1.3build2).
The following additional packages will be installed:
  git-man liberror-perl python3.12-venv
Suggested packages:
  git-daemon-run | git-daemon-sysvinit git-doc git-email git-gui gitk gitweb git-cvs git-mediawiki git-svn
The following NEW packages will be installed:
  git git-man liberror-perl python3-venv python3.12-venv
0 upgraded, 5 newly installed, 0 to remove and 10 not upgraded.
Need to get 4,811 kB of archives.
After this operation, 24.5 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu noble/main amd64 liberror-perl all 0.17029-2 [25.6 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu noble-updates/main amd64 git-man all 1:2.43.0-1ubuntu7.1 [1,100 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu noble-updates/main amd64 git amd64 1:2.43.0-1ubuntu7.1 [3,679 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu noble-updates/universe amd64 python3.12-venv amd64 3.12.3-1ubuntu0.2 [5,678 B]
Get:5 http://us.archive.ubuntu.com/ubuntu noble-updates/universe amd64 python3-venv amd64 3.12.3-0ubuntu2 [1,034 B]
```

2.

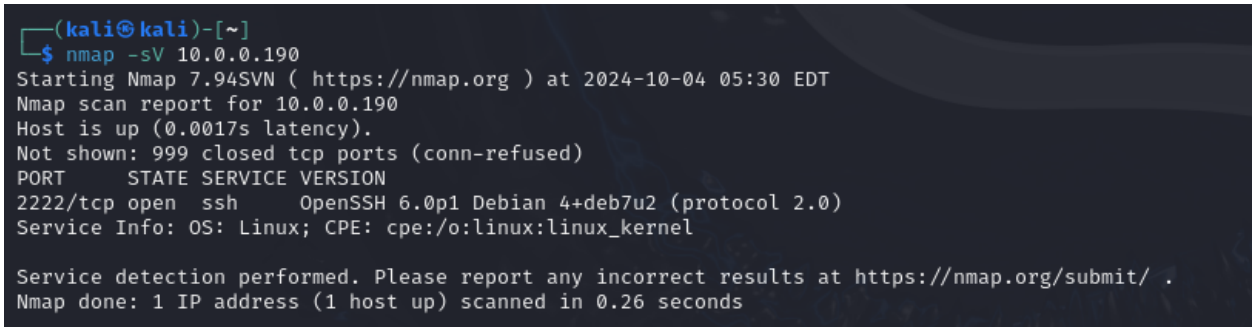
```
Processing triggers for man-db (2.12.0-4build2) ...
lee@UbuntuHoneypot:~$ sudo adduser --disabled-password cowrie
info: Adding user `cowrie' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `cowrie' (1001) ...
info: Adding new user `cowrie' (1001) with group `cowrie (1001)' ...
info: Creating home directory `/home/cowrie' ...
info: Copying files from `/etc/skel' ...
Changing the user information for cowrie
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
info: Adding new user `cowrie' to supplemental / extra groups `users' ...
info: Adding user `cowrie' to group `users' ...
lee@UbuntuHoneypot:~$ su cowrie
Password:
^C
lee@UbuntuHoneypot:~$ sudo su cowrie
cowrie@UbuntuHoneypot:/home/lee$
```

3. 

4. 

5. 

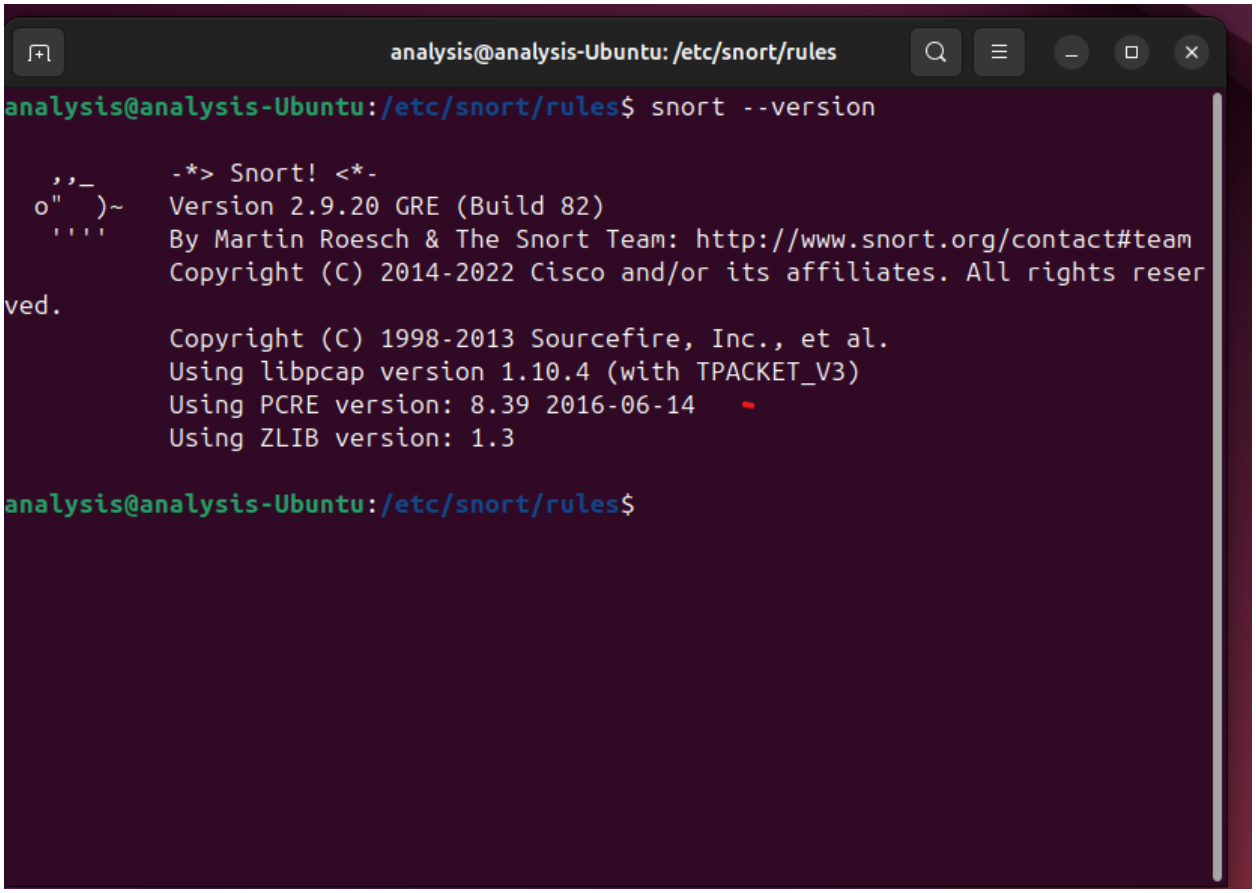
Running Nmap on my Kali Machine & connecting to confirm my honeypot setup.

1. 

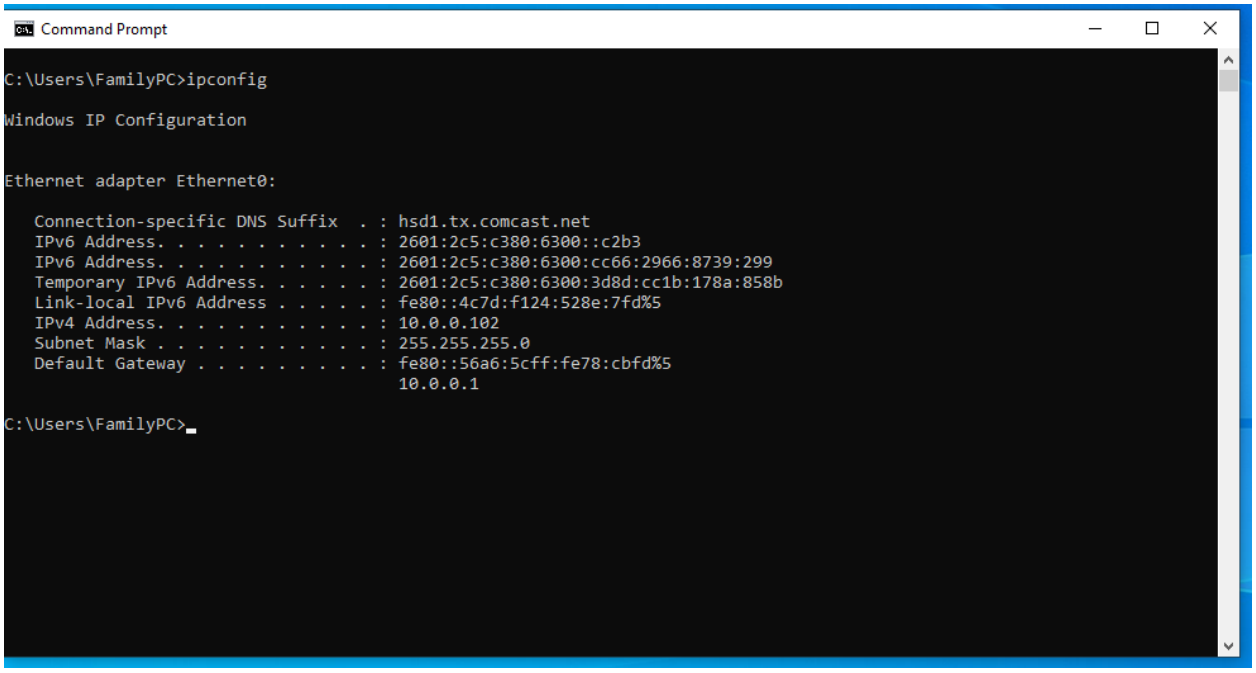
2.

After configuring my snort machine, I viewed the version to confirm the installation.

1.



Running ipconfig on my windows machine just to note the address.

1. 
Command Prompt
C:\Users\FamilyPC>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet0:
Connection-specific DNS Suffix . : hsd1.tx.comcast.net
IPv6 Address. . . . . : 2601:2c5:c380:6300::c2b3
IPv6 Address. . . . . : 2601:2c5:c380:6300:cc66:2966:8739:299
Temporary IPv6 Address. . . . . : 2601:2c5:c380:6300:3d8d:cc1b:178a:858b
Link-local IPv6 Address . . . . . : fe80::4c7d:f124:528e:7fd%5
IPv4 Address. . . . . : 10.0.0.102
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::56a6:5cff:fe78:cbfd%5
10.0.0.1
C:\Users\FamilyPC>

References

Reference for Cowrie Documentation: Cowrie Project. (n.d.). *Cowrie Honeypot Installation Guide*. Read the Docs. https://cowrie.readthedocs.io/en/latest/INSTALL.html

Reference for Snort on Ubuntu Guide: Vasanthabalaji. (2019, June 5). *Snort on Ubuntu*. Medium. https://medium.com/@vasanthabalaji/snort-on-ubuntu-3d865834c768

Reference for Python Virtual Environments: Python Software Foundation. (n.d.). *venv — Creation of virtual environments*. Python Documentation. https://docs.python.org/3/library/venv.html