Network Monitoring and Intrusion Detection

The aim of this laboratory is to appreciate how to setup and configure an intrusion detection system and be able to investigate network traffic.

WARNING!
Be VERY careful about using these tools – they are very powerful tools that can damage the local network, the University network and the Internet. Please only use the tools described in this tutorial. Misuse of these tools is against the law.

WARNING!
The tasks in this lab will require access to software contained on systems within the Cyber Security & Forensics Lab (SMB101).

Please DO NOT attempt these tasks until AFTER the lecturer has provided a demonstration of how to access and use the tools

Laboratory Environment Setup

Task 1: Setup the attacking environment:

- Access the SMB101 lab environment and login
- If not present on the Desktop, copy the Cyber Forensic VM from the V Drive to the Desktop. If present, please use the version already on the desktop.
- Start VMWare Workstation and open and run the Cyber Forensic VM (from the Desktop copy).

Task 2: Setting up the IDS/monitoring environment:

- Copy the Ubuntu160450-base VM from the V drive to the Desktop. If a copy already exists on the Desktop, please replace it with a clean copy from the V drive.
- Start VMware Workstation and click on file open. Point to the desktop copy of the Ubtunto16045 image
- Click on setting and modify the first network interface to NAT.
- Start the Ubuntu VM
- A short demonstration will be provided to help you become familiar with the Linux environment.

Network Analysis

This aspect of the laboratory will introduce Wireshark – an open-source network protocol analyser that permits the analyst to inspect the traffic within the network. It is amongst the most useful tools to debug and investigate issues with networks.

Task 3: Capturing traffic using Wireshark

- Identify the IP address for the Ubuntu VM using:

  `ifconfig` (the ens33 interface IP)

- Within Wireshark on the Ubuntu VM, click on start capturing

- Within the Cyber Forensics VM, using a command prompt, ping the Ubuntu VM

  `ping <id.address>`

- Once the Ping has finished, stop the Wireshark capture and examine the results

Task 4: Analysing local traffic (perhaps to identify misuse against computer use policies!)

- Start Wireshark capturing

- Using Firefox on the Ubuntu machine, browse to a non-encrypted website. Example: http://bitcoinist.com

- Stop the Wireshark capturing and analyse the results.

- Use Follow the TCP Stream

- Repeat the activity but this time use a HTTPS website – which is most websites! What does the resulting traffic show?

Task 5: Analysing a network under attack

- Start Wireshark capturing

- From the Cyber Forensics VM, run an Nmap Intense scan against the Ubuntu machine

- Once Nmap has completed, stop the Wireshark capture. Review the capture – how much traffic was captured? Are you able to identify the port-scan?

Intrusion Detection

Intrusion detection and prevention systems have become critical security countermeasures within a cyber security practitioners toolkit. In this laboratory you will be utilising Snort – a very well-known and widely used open-source network-based IDS. The tasks that follow will give you an appreciate of how to configure, update, run and analyse Snort alerts.

Task 6: Setup and configure Snort

The Ubtuntu image already contains Snort. However, given the IDS rules are constantly updated, it is important that the updated rules are downloaded, and the configuration is checked prior to running Snort.

- Download and update the rules using the following command from a command prompt:

  `sudo-i` (and enter `student` when prompted)

  ```
  wget https://www.snort.org/rules/community -O
  ~/community.tar.gz
  ```

- Unpack the download using:

  ```
  tar xzvf community.tar.gz
  ```

- Copy the new community-rules to the old local.rules location:

  ```
  cp /home/student/community-rules/community.rules
  /etc/snort/rules/local.rules
  ```

- Check that the Snort configuration file compiles successfully:

  ```
  Snort -Tc /etc/snort/snort.conf -i ens33
  ```

- Unpack the download using:

Task 7: Creating a Snort rule and testing the system

- Edit the rules file and add a simple ICMP rule to detect a Ping

  ```
  nano /etc/snort/rules/local.rules
  ```

- Edit the file and add the following rule:

  ```
  Alert icmp any any -> $HOME_NET any (msg: "ICMP Ping
  Alert"; sid: 1000003;)
  ```

- Save and exit the file

- Check the Snort compiles successfully:

```
snort -Tc /etc/snort/snort.conf -i ens33
```

- Lets run Snort and see if it captures the alert. Run Snort using:

```
snort -v -c /etc/snort/snort.conf -i ens33 -l
/home/student/Desktop -A fast
```

- On the Hacking machine (Cyber Forensic VM), use a command prompt and ping the Ubunto machine

```
ping <id address of snort machine>
```

- Once finished, go back to Ubunto machine, click into the terminal window and press Control-C to stop snort – review the statistics

- Open the alert file on the Desktop and confirm the alert.

- View the captured traffic related to the alert. You may need to change permissions:

```
sudo chmod a+rwx /home/student/Desktop/<filename>
```

- Double-click on the file and Wireshark will open. View the captured traffic and confirm the ping.

Task 8: Run Nmap against Snort and analyse the results

- You have been given sufficient information to be able to undertake this task.

- Please note, you will receive different outputs depending upon the nature of the scan you perform.

Task 9: Run captured attack traffic against Snort

- Open the pcap file below using Wireshark. What can you see?

```
/root/Desktop/data/7-nw-forensic-analysis/wiretap.pcap
```

- Run Snort using the following command:

```
snort -v -g snort -u snort -c /etc/snort/snort.conf
-r /home/student/Desktop/data/7-nw-forensic-
analysis/wiretap.pcap -i ens33
```

- Once complete, review the statistics. What do the alerts show?

- Upon completion, please shut down both VMs and **delete the Ubuntu VM folder from the Desktop.**