TNE30009/TNE80009

Laboratory Session 2

1. Introduction

The purpose of this lab is to learn about port scanning and intrusion detection systems (IDS). We will use a popular port scanner to scan another machine which has been set up with a popular IDS to detect such intrusions.

This work is to be carried out using the virtual machines used in lab 1.

You will use the Snort IDS and nmap port scanning software. You will scan one host from another. The scanned host is to have Snort running to detect intrusions. Both Snort and nmap are already installed on the Virtual Machines you downloaded for lab 1.

You may be asked for a password. All passwords are `user`.

2. Host configuration

The two hosts should have been configured with IP addresses in the previous labs.

Take note of the two IP addresses. (Use `ifconfig`.)

Check connectivity between both hosts with a ping.

3. Test Snort

Once connectivity is established validate that Snort is working on VM1.

Open a command prompt window and type

```
sudo snort -i 3 -c /etc/snort/snort.conf -T
```

You should see a series of messages, the last of which are:

```
Snort successfully validated the configuration!
Snort exiting
```

This may take quite some time.

4. Add a rule to detect pings

At the moment snort has default rules installed that allow it to detect different attacks. We will add an additional rule that will cause it to detect and report pings.

Edit the Snort config file using gedit (or your favourite Linux editor) to add a local rule.

```
sudo gedit /etc/snort/rules/local.rules
```

Add the following line:

```
alert icmp any any -> any any (msg:"ICMP"; sid:1000001;)
```

This will detect messages from any network to any network that is an ICMP. The rule number is 1000001.

Now run snort in intrusion detection mode reporting all exceptions to the console

```
sudo snort -c /etc/snort/snort.conf -A console
```

From VM2 ping this host. You should see a notification of the pings.

TNE30009/TNE80009

Laboratory Session 2

5. Testing the IDS with some common attacks

Nmap

Port scanning is used to identify vulnerable ports on a host.

From VM2 do a port scan of VM1.

```
nmap -system-dns -v -A  ipaddress
```

What information is shown as a result of the nmap output?

What messages did Snort generate as a result of the port scan? Use wireshark to identify some of them.

Tunnelling Attack

Use the hts and htc commands from the previous lab to see if tunnelling of telnet through http using can be detected by Snort.

7. Assessment of this lab

Show the instructor that you have got Snort running and have carried out the attacks listed. The instructor will also ask you the following questions. The last two questions are particularly important.

1. What is port scanning?
2. What is Intrusion Detection?
3. Why is port scanning a threat to an organisation?
4. Did Snort detect the tunnelling of telnet through port 80?
5. How should an organisation deal with port scanning in its security policy?
6. What might be some of the limitations of an Intrusion Detection System such as Snort?