Intrusion Detection and Prevention

UNIVERSITY OF MINNESOTA

Packet Capture

The first step in understanding how an IDS works is to understand packet capture. The best way to do this is to grab some packets with TCPdump.

TCPdump is built upon BPF which takes a filter and compiles it into machine code that is used to filter in packet stream for only those packets that you're interested in.

TCPdump

There are a **lot** of command line options for TCPdump. Here's a common way in which it is run:

```
tcpdump -i le0 -n -c 20 -s0
```

-i le0	capture packets from the eth0 interface
-n	do **not** resolve IP addresses
-c 10	stop after capturing 10 packets
-s0	capture packets with "full snap length"

Other commonly use command line options include

`-X`, `-w filename`, `-r filename`

Exercise #1 - Capturing Packets

Use TCPdump to capture some packets on the victim network:

1. Make sure that all VMs are up and running.
2. Start up TCPdump on the Linux Victim host

```
sudo tcpdump -i le0 -n -c 100 -s0
```

3. Scan the internal network from the Linux Attacker

```
nmap -sP 172.16.10.0/24
```

4. Restart TCPdump on the Victim (if necessary)
5. Scan the Victim host from the Attacker

```
nmap -A 172.16.10.10
```

Exercise #1a - Capturing Packets

Use TCPdump to capture more packets on the victim network:

1. Restart TCPdump on the Victim with the -X flag
   ```
   sudo tcpdump -i le0 -n -c 100 -s0 -X
   ```
2. Nmap the victim network from the Attacker
   ```
   nmap -A 172.16.10.1-20
   ```

Snort

Snort is one of the most commonly used Intrusion Detection Systems in use today. It's so popular because it's free, it's very good at what it does and it's well supported.

You can even buy commercial versions from SourceFire.

It's also very well documented.

Snort Rules

Let's look at an example rule and take it apart:

```
alert ip $EXTERNAL_NET $SHELLCODE_PORTS -> $HOME_NET any
(msg:"SHELLCODE Linux shellcode"; content:"|90 90 90 E8
C0 FF FF FF|/bin/sh"; reference:arachnids,343;
classtype:shellcode-detect; sid:652; rev:9;)
```

Snort Rules

Let's make that a little more readable and examine it:

```
alert ip $EXTERNAL_NET $SHELLCODE_PORTS -> $HOME_NET any
  (
    msg:"SHELLCODE Linux shellcode";
    content:"|90 90 90 E8 C0 FF FF FF|/bin/sh";
    reference:arachnids,343;
    classtype:shellcode-detect;
    sid:652; rev:9;
  )
```

Exercise #2: Snort in pfSense

The first step to getting Snort into pfSense is to download and install the snort package for pfSense. This has already been done for you here, but here are the steps.

1. On the Linux Victim, open Firefox and go to http://172.16.10.254
2. Go to **System -> Packages**
3. Snort is already installed, but examine the other available packages

Exercise #3: Installing Snort Rules

Snort isn't much good until it has some rules to work with. By default, the snort package for pfSense comes with no rules at all. To install the standard rules, you have to register for an account at www.snort.org and then generate an oinkmaster code.

Again, this has already been done for you, but here are the steps.

1. Point a browser at www.snort.org
2. Create a new snort.org account (click on Not Registered?)
3. Wait for the email to come back...
4. Log in using your snort.org account and generate an oinkmaster code
5. You'll get a really long hex string for your oinkmaster code
6. Go back to the Linux victim, point a browser at the pfSense console and log in
7. Go to **Packages** -> **Snort** -> and enter your code
8. Go to **Packages** -> **Snort** -> **Update Rules** and wait for snort to update itself
9. You are now running snort with (relatively) up to date rules

Exercise #4: Generate Some Alerts

Now that snort is installed and is running with updated rules let's generate some alerts.

1. Start the nessus client on the Attacker
   ```
   nessus
   ```
2. Login to nessus and start a scan of `172.16.10.10`
3. In the pfSense web console, go to **Services** -> **Snort** -> **Alerts**
4. Refresh a few times if there are no alerts

Exercise #5: Under The Hood

Snort and all of the configuration files that are documented are sitting on pfSense. If you are feeling adventurous and know what you're doing, you edit them directly. This is **not** recommended.

1. On the pfSense VM, enter a command shell (option 8)
2. `cd /usr/local/etc/snort`
3. `snort.conf` contains the primary configuration files for Snort

Questions?

Intrusion Detection and Prevention

UNIVERSITY OF MINNESOTA

Packet Capture

The first step in understanding how an IDS works is to understand packet capture. The best way to do this is to grab some packets with TCPdump.

TCPdump is built upon BPF which takes a filter and compiles it into machine code that is used to filter in packet stream for only those packets that you're interested in.