CIS2390 PRACTICAL

Week 3

Important Warning

Some of the techniques we have discussed in this weeks teaching materials should **not** be used or practiced on **any** University network. To do so could result in instant suspension from the University.

Questions

In order to answer this weeks questions you will need to launch the *Samurai* virtual machine.

1. The student web server (hermes) has the IP address 161.112.232.211.
   a. Ping this address and determine an average time that an ICMP packet takes to travel to this address and back. How many bytes is your packet size?
   b. Assuming that 1 bit travels at the speed of light (ie. 3 x 10^8 m/s), *estimate* how far away the student web server is? If you get a ridiculous answer, this means you have mucked up your arithmetic in some way!
2. Using *scapy*, send[1] a secret message to another student using ICMP.

   If you are the student receiving the secret message, then use the *sniff* command to filter ICMP traffic and then capture and print the payload of the packet sent to you. You might find it useful to modify the *Simplistic ARP Monitor* code[2] in the *scapy* tutorial in order to do this.
3. You are tasked with the job of testing a *snort* IDS (intrusion detection system) sensor. To do this, you will need to craft specially prepared IP packets and then send them past the IDS sensor. If the IDS sensor detects your packet (see the lecture for the *snort* rules used), then it will log this in its event database.

---

[1] **Note:** in order to send the IP packet, *scapy* will need root privileges!

[2] http://www.secdev.org/projects/scapy/doc/usage.html#simplistic-arp-monitor

Use *scapy* to create and send each of the following IP packets:

a. create and send a UDP packet built with the following data:

SOURCE PORT	555
DEST ADDRESS	10.4.76.129
DEST PORT	666

The packets payload should be your student ID. If the destination port were open, what return packets might you expect?

b. create and send a TCP packet built with the following data:

SOURCE PORT	31337
DEST ADDRESS	10.4.76.129
DEST PORT	Any port between 1-1024
TTL	48
ID	242
SEQ	0xa1d96
ACK	0x53
FLAGS	only FIN, RST and PSH should be set

The packets payload should be your student ID. If the destination port were open, what return packets might you expect?

4. Download the *snort* IDS logs (these are in a *tcpdump* format) using the command:

wget http://helios.hud.ac.uk/scomcjp/snort.log

a. Load the snort *tcpdump* logs into *wireshark* and locate all the UDP specific traffic[3]. Can you use *scapy to* craft the same UDP packets, but with the source address set to your NIC MAC and IP addresses and the destination address set to 10.4.76.129?

b. Use snort to replay[4] these packets and thus analyze them looking for alerts. What do you find in doing this?

---

[3] **Hint:** try using `ip.proto == 0x11` (ie. IP datagram protocol is UDP) as your *wireshark* filter. BTW, you can work this value out from a *scapy* prompt with: `(IP()/UDP()).proto`

[4] Use the command `snort -c /etc/snort/snort.conf -r snort.log -l .` to do this.