Note: This homework assignment is worth 115 points.

1 Worms \{20 points\}

(a) \{5 points\} You are the network administrator of an enterprise network, and you can view all network \textit{flows} on your network, where a flow is defined as a four-tuple of \((\text{srcIP}, \text{srcPort}, \text{destIP}, \text{destPort})\). (You can think of a flow as a connection.) Due to privacy requirements, you cannot inspect the payloads of packets. Given this vantage point, how might you detect the presence of a worm in your network?

(b) \{5 points\} Suppose each instance of a worm launched at time \(t_0\) finds and infects 5 vulnerable nodes per hour. How many nodes will be infected at time \(t_0 + 12\) hours?

(c) \{5 points\} You are a firewall administrator at a large organization. You are responsible for protecting the corporate network from malicious traffic. One method of securing your network is to use whitelisting (i.e., allowing only whitelisted IPs to send information into your network). What is a \textbf{major} disadvantage of IP whitelisting as a technique to thwart attacks from worms and botnets? (Limit your answer to one sentence.)

(d) \{5 points\} What is a \textbf{major} disadvantage of IP blacklisting as a technique to thwart attacks from worms and botnets? (Limit your answer to one sentence.)
2 Attacking the LAN \{35 points\}

(a) \{10 points\} Prof. Pedantic connects his laptop to the Internet using his department’s switch. His archenemy, Prof. Adroit, also connects to the Internet through the same switch. Figure 1 shows the architectural layout of their department network. Briefly explain (1-3 sentences) how Prof. Adroit can intercept Prof. Pedantic’s Internet-bound traffic.

(b) \{10 points\} Suppose the two profs use a different network in which Prof. Adroit is outside of Prof. Pedantic’s local network, but can observe all traffic that enters and leaves Prof. Pedantic’s router. (See Figure 2.) Briefly explain (1-3 sentences) how Prof. Adroit can cause Prof. Pedantic to resolve any hostname (incorrectly) as 1.2.3.4.

(c) \{10 points\} Briefly explain (1-3 sentences) how DNSSEC mitigates the attack described in the previous question.

(d) \{5 points\} Assume that the DNSSEC root key has been compromised by Prof. Adroit. Explain how he can re-enable the attack (i.e., cause Prof. Pedantic to resolve all hostnames to 1.2.3.4).

---

Figure 1: Network diagram for question 2(a).

Figure 2: Network diagram for question 2(b).
3 A Port Scanner \{30 points\}

In this programming assignment, you will be building a port scanner. A port scanner is a software program that probes a target computer for open ports—i.e., ports that have services listening on them. They are often used for network diagnostics, but also as a precursor to launching an attack, since they identify potentially vulnerable services.

Your port scanner, PortScan, will probe all $2^{16}$ TCP ports on a targeted host, and report the ports that accept connections. Your scanner should not require superuser (root) privileges, and can attempt to establish full TCP connections to the tested ports.

Your scanner should scan the ports in random order as quickly as possible. That is, you should not pause or sleep between probes.

For each open port, PortScan should report both the port number and the service that normally runs on that port. The latter can be found by using the `socket.getservbyport()` function.

PortScan should also report how long it took to probe all ports, the number of ports that were found to be open, and the scan rate (ports scanned per second).

The command-line usage for PortScan should be:

```python
python PortScan.py target
```

where target is the hostname or IP address of the machine that is to be scanned.

**IMPORTANT NOTICE REGARDING COMPUTER ETHICS.** It is not cool to scan hosts on the Internet when you do not have permission to do so. Since port scanners are sometimes used to prepare for an attack, network administrators build tools to detect their use (see the next part of this assignment). Hence, by scanning a host, you may cause an alarm to be raised. Even if the target machine is not being monitored for probes, routers along the path from the scanner to the target may detect the “attack”. You are strictly forbidden to run PortScan against any machine except for netid-alice-HW1, netid-bob-HW1, or any machines announced by the teaching staff as being an appropriate target. Nor should you run PortScan from any machine other than netid-alice-HW1 and netid-bob-HW1.
A Port Scanner Detector {30 points}

For the second part of the homework, you will build PSDetect, a port scanner detector. PSDetect will use pycapy\(^1\) to listen to incoming connections, and report the presence of a scanner if a single machine (identified by a single source IP address) attempted to connect to 30 or more ports within a 5 second window. PSDetect should therefore be able to detect when PortScan is used.

PSDetect should not produce any output until a scanner is detected. When a scanner is detected, it should print out the message\(^2\):

Scanner detected. The scanner originated from host A.B.C.D.

where A.B.C.D should be replaced with either the IP address or the hostname of the machine that attempted to connect to 15 or more consecutive ports within a 5 second window.

PSDetect should only terminate when the user presses CTRL-C.

The difficult part of this assignment is obtaining the IP header of captured packets. pcap functions at the data link layer and will return to you Ethernet frames. You’ll need to access the part of those frames that correspond to the IP headers. You can use the dpkt library that is installed on your machines; the page for pycapy has an example that will help you greatly.

PSDetect will require superuser (root) privileges. You will need to run it via either “sudo PSDetect” or “sudo python PSDetect.py”.

Submission Instructions

Include the source code to all three programs in a single compress tarball (.tar.gz file), and upload that file to Blackboard. Include compilation instructions, if your code requires it.

To upload your assignment, navigate to the COSC535 course, click the “Assignments” link on the left hand side, and select “hw2”. Look for the “Attach File” section and upload your submission. Be sure to hit the “Submit” button when done. Upload your assignment before 11:59pm on March 6th.

Please post questions (especially requests for clarification) about this homework to Piazza.

---

\(^1\)see [https://code.google.com/p/pypcap/](https://code.google.com/p/pypcap/)

\(^2\)It does not have to print this message in red.