Clear Layout

It is vitally important that your assignment is clearly laid out with questions and parts of questions clearly defined. It must be a straight forward matter for the examiner to determine that you have completed each exercise satisfactorily. We want quality not quantity. Poorly organised submissions will be rejected or receive a poor mark.

A text file or PDF/A document typeset using vanilla LaTeX are preferred over a document produced by a word-processor. If you must use Microsoft Word please export your document as PDF/A[1] not PDF.

Command Output

When answering these questions you will have to run commands under Linux—whenever a command is run you will need to:

a. explain in your own words the purpose of the command in the context of the assignment question. (Please do not just copy the "Description" section from the man page!) Also, you need to explain in your own words all terminology used—as if you were explaining to an average user! (Please show you understand what you are doing!)

b. show that the command worked—either from its output or the output from another command. For example

```
prompt> dd if=/dev/zero of=Crypt.fs bs=1M count=32
32+0 records in
32+0 records out
33554432 bytes (34 MB) copied, 0.109063 s, 308 MB/s
prompt> ls -l Crypt.fs
-rw-r--r--1useruser335544322010-02-2510:18Crypt.fs
```

c. To capture text output from programs you will have to redirect the output to a file or use the command script. If you are using the command script turn off the tty escape sequences that change the colour of console text—the escape sequences will appear in output file and make it impossible to read.

[1] PDF/A is an archival format of PDF that embeds all fonts used in the document within the PDF file. To ensure PDF/A format in Word check "ISO-19005-compliant (PDF/A)" under "Options" when saving a file as PDF.

(marks 20)

Question 1

The following "firewall" script is run on a "gateway" machine—

```
1echo 1 > /proc/sys/net/ipv4/ip_forward
2
3iptables -F
4iptables -X
5
6iptables -P INPUT DROP
7iptables -P OUTPUT ACCEPT
8iptables -P FORWARD DROP
9
10iptables -A INPUT -i lo -j ACCEPT
11iptables -A INPUT -i eth1 -s 192.168.37.0/24 -j ACCEPT
12iptables -A INPUT -i eth0 \
13-m state --state RELATED,ESTABLISHED -j ACCEPT
14
15iptables -A FORWARD -i eth1 -s 192.168.37.0/24 \
16-m state --state NEW -j ACCEPT
17iptables -A FORWARD -m state \
18--state RELATED,ESTABLISHED -j ACCEPT
19
20iptables -t nat -F
21iptables -t nat -X
22
23iptables -t nat -A POSTROUTING -o eth0 -s 192.168.37.0/24 \
24-j SNAT --to-source 147.63.112.42
```

Using the script above answer the following questions:

a. (4 marks) Explain, in your own words what a "gateway" machine is and what it is used for.

b. (4 marks) Explain the general purpose of the firewall above. Your explanation should include a description of the networks the gateway machine is connected to and how it is connected. Note: this is a "general description" do not make any explicit reference to the commands above.

c. (6 marks) Explain the purpose of each filter rule of this script. That is, for each filter rule—what packets are being filtered and why? Note: some rules are not filter rules.

d. (3 marks) There are two rules for the FORWARD chain in the above script. Explain how iptables knows a packet is to be forwarded and must apply these rules.

e. (3 marks) The last rule in the script modifies the POSTROUTING chain of the NAT table. What is the POSTROUTING chain and why are SNAT rules applied to this chain?

Notes:

(marks 20)

a. The backslash character \ is a line continuation character in scripts.

Question 2

As the system administrator you would like to SSH to a gateway machine (see Exercise 1) from off-site. Unfortunately that would mean opening the SSH port to the world—and you would rather not do that.

A friend tells you of the dæmon knockd that can temporarily open a port for quick access.

Install knockd and configure it to open a timed temporary hole in a firewall using a "single" timed knock.

Your write-up will need to include the following:

a. (3 marks) A couple of paragraphs in your own words describing how knockd works.

b. (3 marks) Explain why a single timed knock is better than a knock to open and a knock to close. Also explain why the connection is not broken when knockd closes the temporary hole in the firewall.

c. (3 marks) A couple of paragraphs in you own words describing the security flaws in the knockd approach to opening a temporary hole in a firewall.
Hint: Read about Single Packet Authorisation methods.

d. (3 marks) The configuration file or files you needed to modify to open a temporary hole in a firewall using a "single" timed knock. Include an explanation in your own words of the purpose of every line in the configuration file or files.

e. (3 marks) The firewall on the machine. Use the output from the command iptables -L -v to show that the machine has been firewalled.

f. (5 marks) Output showing that knockd worked. A successful SSH session and the output from the command iptables -L -v to show the hole that knockd has created in the firewall.

Notes:

a. The firewall of Exercise 1 may be used as a starting point for a firewall for this question. It will have to be simplified for this question (One interface—so no NAT or FORWARD rules).

b. Do not explain how you installed the knockd package.

c. The knockd man page has a number of examples of configuring knockd—copying an example exactly without explanation and attribution will receive zero marks. Also note using examples in a

(marks 20)

published document foolishly creates a security breach - wich will loose marks.

Question 3

One way to protect any communication on the Internet is to use a VPN. A VPN can be useful for individuals and companies. One of the most popular VPN technologies is OpenVPN (see www.openvpn.net)

In about a page, explain in your own words what a VPN is, what it is used for and how it works.

Your explanation should include:

- (5 marks) In general terms what a VPN is,
- (4 marks) examples of where a VPN may be useful,
- (7 marks) the technologies used in SSL/TLS VPNs such as OpenVPN, and
- (4 marks) how the technologies are used to ensure a secure connection between two networks or a remote machine and a network.
  Hint: One way to answer this question is to describe the steps the software goes through to establish and maintain a connection.

Notes:

a. We are not discussing here web browser SSL connections (though the technology is the same) this is a discussion of a VPN with all that implies.

b. This is an extremely technical topic and I do not expect you to cover all aspects of it. But you should explain all terms used in your answer (not covered in the study book), for example, VPN, SSL/TLS, certificates, HMAC, key authentication, session keys, … c. You do not have to implement an OpenVPN connection — though it may be helpful in understanding the underlying technologies.

d. List all resources used in answering the question.