Matric No:_____

NAPIER UNIVERSITY

SCHOOL OF COMPUTING

CO32034

SERVER ADMINISTRATION

ACADEMIC SESSION: 2004-2005

EXAMINATION DIET: AUGUST

TRIMESTER: ONE

EXAM DURATION: 2 HOURS

READING TIME: NONE

EXAM PAPER INFORMATION

Answer any THREE questions

Number of questions – FIVE

Number of pages – SIX

Number of sections – ONE

OPEN BOOK EXAMINATION

EXAMINERS: UTA PRISS & GORDON RUSSELL

PLEASE READ THE FULL INSTRUCTIONS BEFORE COMMENCING WRITING

1. Network Configuration

In answering this question, the following information may prove useful:

```
Usage: iptables -[AD] chain rule-specification [options]
       iptables -[RI] chain rulenum rule-specification [options]
       iptables -D chain rulenum [options]
       iptables -[LFZ] [chain] [options]
       iptables -[NX] chain
       iptables -E old-chain-name new-chain-name
       iptables -P chain target [options]
       iptables -h (print this help information)

Commands:
Either long or short options are allowed.
  --append  -A chain            Append to chain

  --replace -R chain rulenum
                                Replace rule rulenum in chain
  --list    -L [chain]          List rules in a chain or all chains
  --flush   -F [chain]          Delete rules in  chain or all chains
  --zero    -Z [chain]          Zero counters in chain or all chains
  --new     -N chain            Create a new user-defined chain
  --delete-chain
            -X [chain]          Delete a user-defined chain
  --policy  -P chain target     Change policy on chain to target

Options:
  --proto       -p [!] proto    protocol: by name, eg. `tcp'
  --source      -s [!] address[/mask]
                                source specification
  --destination -d [!] address[/mask]
                                destination specification
  --in-interface -i [!] input name[+]
                                network interface name ([+] for wildcard)
  --jump        -j target
                                target for rule (may load target extension)
  --match       -m match
                                extended match (may load extension)
  --numeric     -n              numeric output of addresses and ports
  --out-interface -o [!] output name[+]
                                network interface name ([+] for wildcard)
  --table       -t table        table to use (default: `filter')
  --verbose     -v              verbose mode
  --line-numbers                print line numbers when listing
  --exact       -x              expand numbers (display exact values)
```

(a) Firewall configuration in Linux 2.4 and beyond used “iptables”. “iptables” makes use of a number of “tables”, each of which can have a number of chains.

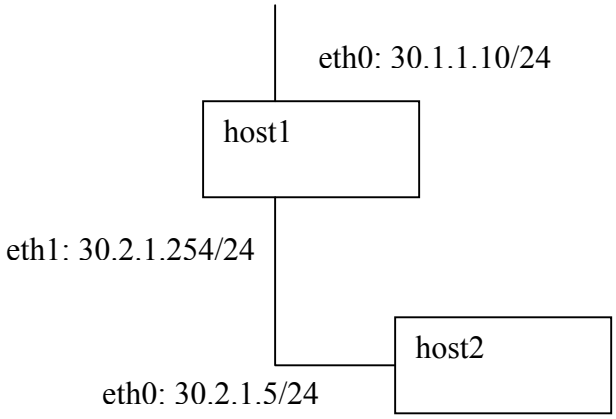
(i) One table is “filter”. What are the other two tables?

(2)

(ii) What are the chains defined by default in the filter table. Discuss which packets will be processed by each chain.

(6)

(b) Consider the following network architecture:



(i) Write a set of routing and network configuration commands for host1 that can support this architecture, given that eth0 on host1 is the gateway connection.

(5)

(ii) Given that host1 is running http, and host2 is running http and sshd, provide iptable commands (using reasonable syntax) to implement a firewall on host1. All services should be accessible from any network point. Document your commands. In answering the question you should also consider adding in reasonable additional requirements to the specification to improve security.

(6)

(c) host2, as discussed in (b), has started to suffer significant network degradation. List 4 possible reasons and an action which could be performed to investigate each possible reason.

(6)

Total Marks [25]

2. Processes, Services, and Disks

(a) (i) telnetd is not started in init.d, yet you can still log onto the machine using telnet. Explain why this is possible, and the philosophy behind this approach to services.

(4)

(ii) You have noticed a process using ps with a state Z. What does this mean and what does it signify to a system administrator?

(2)

(iii) You have run the pstree command, and see the following:

init—sshd—sshd—bash—pstree

What does this mean and why is this the case?

(3)

(iv) In the example shown in (iii), what would happen if you sent "kill –9" to the "sshd" process listed immediately after "init"?

(2)

(b) "The linux kernel insulates the user from hardware dependencies, and as such makes running linux on different hardware platforms simple to manage".

Discuss this statement and give detailed examples of this in practice, paying particular reference to device files, major and minor numbers, and kernel internal device names.

(6)

(c) You have a single 10 GB SCSI disk to partition to hold a linux server installation. Users need 3GB. Propose and discuss a partitioning strategy for this disk, and include the mountfile information.

(8)

Total Marks [25]

3. Web Server Configuration

(a) Discuss simple authentication in http, with reference to how it can be implemented in Apache from a web publisher perspective. Include examples, and any security implications that may exist.

(6)

(b) A virtual host configuration has to be set up in apache.

(i) Write a virtual host configuration which includes “hia.com” as the main hostname, with “hoho.org” and “www.hia.com” as aliases. Include as many basic options as may be relevant, suggesting values for the unknown information.

(6)

(ii) Add the following to the definition as mod_rewrite rules:

- www.hia.com get rewritten to hia.com
- hoho.org rewritten to hia.com, unless it is hoho.org/~andrew, in which case do nothing.
- hia.com/~gordon gets rewritten to hia.com/root1

(8)

(c) Discuss the tuning parameters of apache, such as MinSpareServers, and issues to be considered when setting their values.

(5)

Total Marks [25]

4. Database Configuration and System Security

(a) (i) A web server utilising MySQL in the backend is suffering from significant performance issues. Discuss three things which may be the cause, and how you would proceed to investigate those things.

(6)

(ii) You have been authorised to spend money on more hardware in an attempt to solve this problem. However, have slightly less money available to spend than was original spent on buying the machine. On what can the money be best spent? Include a discussion of the options.

(4)

(b) You have been asked to visit a company as a security advisor. Make a list of ten security aspects which could be investigated, and a short reason why each should be considered.

(10)

(c) Your own company’s web server has been defaced, so that all your web pages now direct visitors to your competitors. Discuss how you can begin to investigate this incident to understand what happened.

(5)

Total Marks [25]

5. Non-Linux Administration

(a) (i) Describe how user and group password authentication is handled by traditional Unix systems.

(3)

(ii) Discuss how Directory Services in Mac OS X (10.2 and later) handles authentication. Consider Netinfo in your answer and name several other services that are available through directory services.

(4)

(iii) Discuss the role of Directory Services with respect to application programming.

(4)

(b) List some possible design strategies which may have been important to Apple when they designed Directory Services. In your answer consider Apple's market share, history and user group and their differences to Microsoft and traditional Unix.

(7)

(c) Critically analyse the broader impact that differences between flavours of Unix have on system administration using the example of authentication. Discuss the areas of system administration that are most affected. Also discuss your prediction for future Unix development in this area.

(7)

Total Marks [25]

END OF PAPER