

VE482 HW8

Wu Jiayao 517370910257

EX.1

1.

Yes, scanner is doing the input job while the network is doing the output job.

2.

The OS use a table of function pointers to interface device driver with the rest of the OS. When a new device is installed, the table needs to be updated. The drivers are modules which can be loaded and unloaded dynamically.

3.

- Device driver
- Device driver
- Device Independent OS Software
- User-level software

4.

$$\frac{32bit}{100ns \times 4 \div 2} = 2 \times 10^7 B/s \approx 20MB/s \quad (1)$$

5.

A thin client is a lightweight computer that has been optimized for establishing a remote connection with a server-based computing environment. The server does most of the work, which can include launching software programs, performing calculations, and storing data.

Reference: https://en.wikipedia.org/wiki/Thin_client

6.

A modern HDD records data by magnetizing a thin film of ferromagnetic material on both sides of a disk. Sequential changes in the direction of magnetization represent binary data bits. The data is read from the disk by detecting the transitions in magnetization. User data is encoded using an encoding scheme, such as run-length limited encoding, which determines how the data is represented by the magnetic transitions.

A typical HDD design consists of a spindle that holds flat circular disks, called platters, which hold the recorded data. Information is written to and read from a platter as it rotates past devices called read-and-write heads that are positioned to operate very close to the magnetic surface, with their flying height often in the range of tens of nanometers. The read-and-write head is used to detect and modify the magnetization of the material passing immediately under it.

Reference: https://en.wikipedia.org/wiki/Hard_disk_drive

7.

RAID 0: striping, without mirroring or parity

RAID 1: data mirroring, no parity, striping or spanning of disk space

RAID 5: block-level striping with distributed parity

RAID 6: block-level striping with two parity blocks distributed across all member disks

RAID 10: mirroring and striping

EX.3

1.

/usr/lib/mutt

2.

$$\frac{1KB}{4B} = 256 \quad (2)$$

One block of address can store $256 * 1$ KB data.

$$13 + 256 + 256^2 + 256^3 = 16843021KB \quad (3)$$

3.

$$8 + 2 + \frac{1024}{262144} = 10.003ms \quad (4)$$

$$8 + 2 + \frac{2048}{262144} = 10.008ms \quad (5)$$

$$8 + 2 + \frac{4096}{262144} = 10.016ms \quad (6)$$

delay time reference from https://en.wikipedia.org/wiki/Hard_disk_drive_performance_characteristics#Command_processing_time

EX.4

1.

$$\binom{26}{8} = 1562275 \quad (7)$$

It's easy and of low cost to apply a bruce-force attack on such a small range of password

2.

When a computer is booted, all of its memory are 0. When a process terminated, the memory it used is not necessary to be freed. On the other hand, if the memory is freed, we have no idea where the freed memory is. As processes may require different ranges of memory, have different running time, the order of memory for malloc is sure to be random, rather than fixed.

3.

The lowest level of security among all components.

4.

No, as an operating system is always interfered by outcome issues. New problem may arise somewhere else, conditions never considered of may also occur when issues interfere in.

Ex.5

Iptable

iptables is a user-space utility program that allows a system administrator to configure the tables provided by the Linux kernel firewall (implemented as different Netfilter modules) and the chains and rules it stores. Different kernel modules and programs are currently used for different protocols; iptables applies to IPv4, ip6tables to IPv6, arptables to ARP, and ebtables to Ethernet frames.

iptables requires elevated privileges to operate and must be executed by user root, otherwise it fails to function. On most Linux systems, iptables is installed as /usr/sbin/iptables and documented in its man pages, which can be opened using `man iptables` when installed. It may also be found in /sbin/iptables, but since iptables is more like a service rather than an "essential binary", the preferred location remains /usr/sbin.

The term iptables is also commonly used to inclusively refer to the kernel-level components. x_tables is the name of the kernel module carrying the shared code portion used by all four modules that also provides the API used for extensions; subsequently, Xtables is more or less used to refer to the entire firewall (v4, v6, arp, and eb) architecture.

Reference: <https://en.wikipedia.org/wiki/Iptables>

Ebtable

Ebtables is an application program used to set up and maintain the tables of rules (inside the Linux kernel) that inspect Ethernet frames. It is analogous to the iptables application, but less complicated, due to the fact that the Ethernet protocol is much simpler than the IP protocol.

There are three ebtables tables with built-in chains in the Linux kernel. These tables are used to divide functionality into different sets of rules. Each set of rules is called a chain. Each chain is an ordered list of rules that can match Ethernet frames. If a rule matches an Ethernet frame, then a processing specification tells what to do with that matching frame. The processing specification is called a 'target'. However, if the frame does not match the current rule in the chain, then the next rule in the chain is examined and so forth. The user can create new (user-defined) chains that can be used as the 'target' of a rule. User-defined chains are very useful to get better performance over the linear traversal of the rules and are also essential for structuring the filtering rules into well-organized and maintainable sets of rules.

Reference: <https://linux.die.net/man/8/ebtables>

Arptable

Arptables is a user space tool, it is used to set up and maintain the tables of ARP rules in the Linux kernel. These rules inspect the ARP frames which they see. arptables is analogous to the iptables user space tool, but arptables is less complicated.

The kernel table is used to divide functionality into different sets of rules. Each set of rules is called a chain. Each chain is an ordered list of rules that can match ARP frames. If a rule matches an ARP frame, then a processing specification tells what to do with that matching frame. The processing specification is called a 'target'. However, if the frame does not match the current rule in the chain, then the next rule in the chain is examined and so forth. The user can create new (user-defined) chains which can be used as the 'target' of a rule.

Reference: <http://ebtables.netfilter.org/misc/arptables-man.html>

Ex.6

A kernel panic is a safety measure taken by an operating system's kernel upon detecting an internal fatal error in which it either is unable to safely recover or cannot have the system continue to run without having a much higher risk of major data loss.

`:() { :|:& } ;:`

Reboot your computer.