2.2 The three stages employed by the OS are identification and authentication, access control, and logging and auditing. For identification and authentication, the system conducts authentication by comparing the input credential with the stored one and only allow entry when the credential matches. For Access control, the principle of least privilege is used where users only have access to the resources needed to perform the desired tasks. Privilege separation is also used where the system is split into different components and each component is assigned with the least privilege needed for its tasks. Limiting privilege prevents attack from taking over the entire system. For logging and auditing, an audit trail records all protection oriented activities to understand what happened and why, and also spot things that should not happen

SC3010 Computer Security

Tutorial 4 – Operating System Security

Identification and Authentication: authenticate if a user attempting to enter the system is correct or not.
Access Control: when a subject(process, user,...) wants to access an object (file, network socket,...), check if such access is allowed

1. Circle the correct answers in the following questions.

 1) Which statement is false about UNIX security model?

 [✓ A.] Real User ID of a process determines the permissions for this process.
 B. Files, directories and I/O devices are managed in a unified manner.
 C. Even a superuser cannot write to a read-only file.
 D. In controlled invocation, the users have the extra privilege of the SUID program's owner only when the program is being executed.

 2) In the privileged ring of OS, which component is the most privileged?

 Hardware not part of the privileged ring

 A. Application
 B. Device driver
 [✓ C.] OS kernel
 D. Hardware

2.1 A rootkit can compromise different kernel structures to achieve malicious behaviours. For example, It can change a function pointer in the system call table to make it point to a malicious function. It can directly change the system call function, making it jump to a malicious function. It can change a function pointer in the interrupt descriptor table to make it point to a malicious function.

 3) Modern operating systems provide logging and auditing services. Which security property do those services support?

 A. Integrity
 B. Availability
 [✓ C.] Accountability
 D. Non-repudiation

2.1 The rootkit inserts and execute arbitrary malicious code in the system's code path. It also hides its existence in malicious process and not be detected.

2.3 Controlled Invocation is where superuser privilege is required to execute certain OS functions. SUID flag is employed so that the user who executes the program will inherit the permissions of the program owner. The potential dangers are that a SUID program owned by the root can be tricked to do unintended things, allowing an attacker to act as the root.

As the user has the program owner's privileges when running a SUID program, the program should only do what the owner intended.

2. Answer the following questions.

 1) Give an example of how a rootkit can compromise the system after obtaining the root privilege.

 2) Briefly describe three stages employed by the OS.

 3) What is the controlled invocation? What is its potential danger?

3. Consider a computer system with three users: Alice, Bob, and Cindy. Alice owns the file *alicerc*, and Bob and Cindy can read it. Cindy can read and write the file *bobrc*, which Bob owns, but Alice can only read it. Only Cindy can read and write the file *cindyrc*, which she owns. Assume that the owner of each of these files can execute it.

 1) Create the corresponding access control matrix.

 2) Cindy gives Alice permission to read *cindyrc*, and Bob removes Alice's ability to read *bobrc*. Show the new access control matrix.

 3) Show the capabilities associated with Alice.

3.1,3.2,3.3

	alicerc	bobrc	cindyrc
Alice	~~rws~~ --x	r-- ---	--- r--
Bob	r--	~~rws~~ --x	---
Cindy	r--	rw-	~~rws~~ rwx

4.1

alicerc: ~~rwsr~~--r-- --x---r-- 104
bobrc: r--rwsrw- --xrw-r-- 164
cindyrc: ------rws rwx------ 700

owner, group , other

4.2 delete r from M(Alice,bobrc)
enter r into M(Alice,cindyrc)

o means others

chmod 160 bobrc
chmod 704 cindyrc

chmod o-r bobrc
chmod o+r cindyrc

4. Let's consider the scenario in Q3 again. Assume this is the Unix system. The users Bob and Cindy are in the same group, while Alice is in a different group.

   1) For the original access control matrix in Q3(a), please write the permission for the files *alicerc*, *bobrc* and *cindyrc*.

   2) To adjust the permissions in Q3(b), please write the corresponding commands for *cindyc* and *bobrc*, respectively.

5. A group of researchers is working on analyzing web search results from a major Internet search provider. At the Internet company, a group of search engineers collects and updates databases of: search queries, IP (internet protocol) addresses where the queries came from and timestamps for the queries made by online users. A search manager is in charge of the group of engineers, and can read the query and timestamps database, but not the IP address database -- due to privacy concerns. The researchers are able to access the databases with read-only privileges. The general public should not have access to the database for privacy reasons.

   a. Complete the access control matrix by filling in the access permissions for the different objects shown. Each entry can be either read, write, read/write, or '-' (for no access).

   b. List the ACLs for each object (or class of objects)

   c. List the capabilities for each subject (or class of subjects).

5.1

	search queries	IP of queries	Timestamp of queries
Search manager	read	None	read
Engineers	read,write	read,write	read,write
General Public	None	None	None
Researchers	read	read	read

but write in letters eg. r,w,-

5.2

For search queries, only engineers can write. Search manager, engineers and researchers can read.
For IP of queries, only engineers can write. Only researchers can read
For timestamp of queries, only engineers can write. Search manager, engineers and researchers can read

but follow format

5.3

Search manager can read search queries and timestamp of queries
Engineers can read and write search queries, IP of queries and timestamp of queries
General cannot access search queries, IP of queries and timestamp of queries
Researchers can read search queries, IP of queries and timestamp of queries

but also follow format

Query: {SE:{rw}; SM: {r}; R:{r}; P:{-}}
IP: {SE:{rw}; SM:{-}; R: {r}; P:{-}}
TimeStamp: {SE:{rw}; SM:{r}; R:{r}; P:{-}}

Search Engineers: {Query:{rw}; IP: {rw}; TimeStamp: {rw}}
Search Manager: {Query:{r}; IP:{-}; TimeStamp:{r}}
Research: {Query:{r}; IP:{r}; TimeStamp:{r}}
Public: {Query:{-}; IP:{-}; TimeStamp: {-}}