MUYSHONDT, ALEXANDER D
3/14/2019

HOMEWORK 3

Due on 3/14, submit in HARDCOPY

1. (15%) Classify each of the following system as an example of a mandatory, discretionary, or originator controlled policy. In each system, state who is the creator, who is the owner of the object, what is the system, who is the admin of the system, and who decides the permission for your selected type of access control.

(a) In a Linux system, a file's permission is set by the owner of the file.

- Classification: Discretionary controlled policy
- Creator: unknown
- Owner of the object: user that owns the file
- The system: Linux system
- Admin of the system: root
- Who decides permission: a user controls the access of the files they own

(b) In a software repository, a software package can be distributed only with author's consent.

- Classification: originator controlled policy
- Creator: author of software
- Owner of the object: author of the software
- The system: a software repository
- Admin of the system: author if the software
- Who decides permission: author of the software

(c) In a classified NSA database, only generals with top secret clearance can search in the database.

- Classification: mandatory controlled policy
- Creator: NSA
- Owner of the object: NSA
- The system: NSA database
- Admin of the system: NSA
- Who decides permission: NSA

2. (15%) In each of the following situations, specify what type of access (read, write, both, or neither) is allowed with Bell-LaPadula model. If the subject cannot read the object, then give one object classification that the subject can read. If the subject cannot write to the object, then give one object classification that the subject can write.

(a) Paul, cleared for (Top secret, {A,C}), wants to access a document classified (secret, {B,C}).

Paul cannot read and cannot write to the document because he does not have dominance over the set.

Paul could read (secret, {A,C}

Paul can write (Top secret, {A,C}) ???

(b) Anna, cleared for (Confidential, {C}), wants to access a document classified (Confidential, {B}).

Anna cannot read and cannot write.

Anna could (Unclassified, {C})
Anna could write (Top Secret, {C})
(c) Jesse, cleared for (Secret, {C}), wants to access a document classified (Confidential, {C}).
Jesse can read document but not write to document
Jesse can write to (Top Secret, {C})
(d) Sammi, cleared for (Top secret, {A,C}), wants to access a document classified (Confidential, {A}).
Sammi can read document, but not write to document.
Sammi could write to (Top secret, {A})
(e) Robin has no clearance, but wants to access a document classified (Confidential, {B}).
Robin cannot read document, but can write to document.
Robin could read (Unclassified, {A})

3. (10%) A system implements both Bell-LaPadula and Biba models to enforce confidentiality and integrity simultaneously. Show the access control matrix achieved in the system.

	Top Secret	Secret	Classified	Unclassified
Top Secret	rw	--	--	--
Secret	--	rw		--
Classified	--	--	rw	--
Unclassified	--	--	--	rw

4. (20%) An integer overflow is the condition that occurs when the result of an arithmetic operation, such as multiplication or addition, exceeds the maximum size of the integer type used to store it. If the integer in question is incremented past the maximum possible value, it may wrap to become a very small, or negative number, therefore providing a very incorrect value. It is often a critical security flaw in software.

For example, in a 16-bit integer system, 19458*37=64586. The result is supposed to be 719946, but has more than 16 bits. Therefore, the result is wrapped, i.e. only the least significant 16 bits of the result remain.

Consider in a 32-bit unsigned integer system,

(1) Let Z = 0xFEDCBA98. What is the result of Z + 0x10000000 ? Note that the result must be a 32-bit integer, because this is a 32-bit integer system.

Result is 0EDCBA98

(2) Let Y = 0xFEDCBA98. What is the result of Y * 0x10? Note that the result must be a 32-bit integer, because this is a 32-bit integer system.

Result is EDCBA980

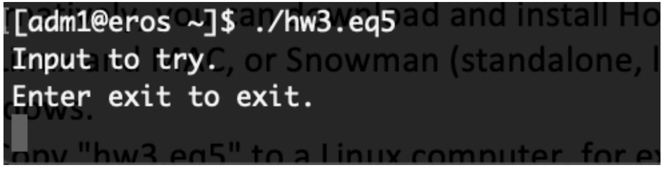
(3) Find "X" that satisfies the following equations.

X > 1337

X * 7 + 4 = 1337

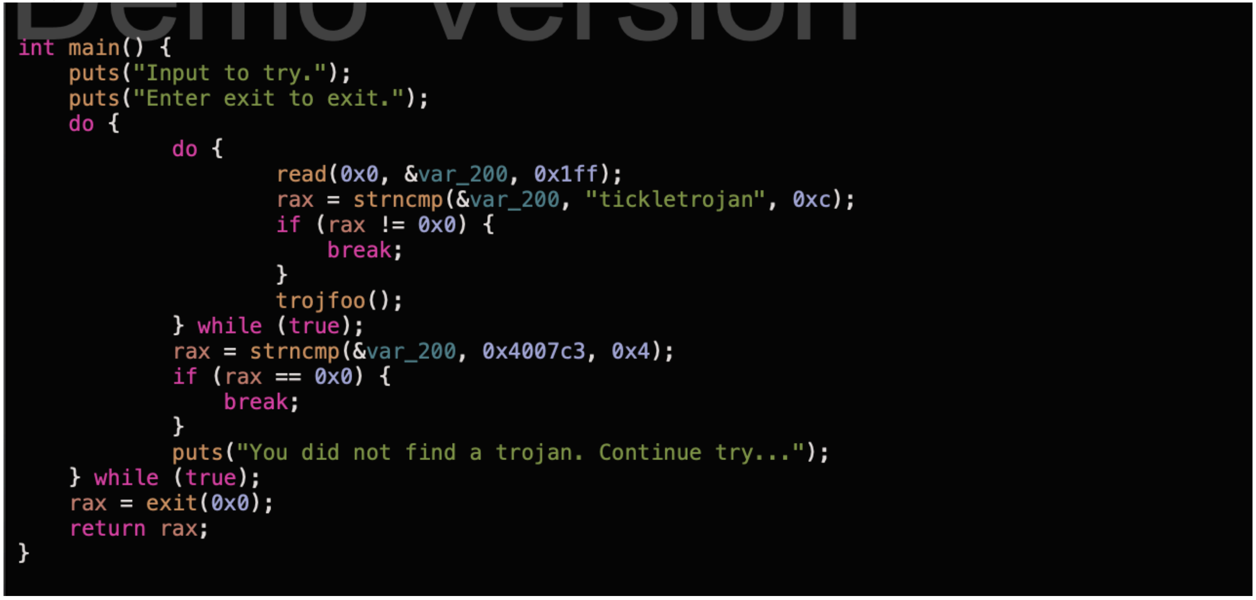
X = 613566947

5. (20%) With a reverse engineering tool, we can identify a Trojan that is normally mixed with the other good code in an executable.
Recommend to use NSA'a Ghidra, download and install from https://ghidra-sre.org/
Alternatively, you can download and install Hopper (latest) from https://www.hopperapp.com/ for Linux and MAC, or Snowman (standalone, latest) from https://derevenets.com/ for Windows.
(1) Copy "hw3.eq5" to a Linux computer, for example, zeus.cs.txstate.edu (tested in this server). Make it executable (chmod +x hw3.eq5) and then run it. Show the screenshot of running "hw3.eq5".
Note, after you copy "hw3.eq5" to zeus, you need to "chmod +x hw3.eq5" and then run "./hw3.eq5" to execute it.



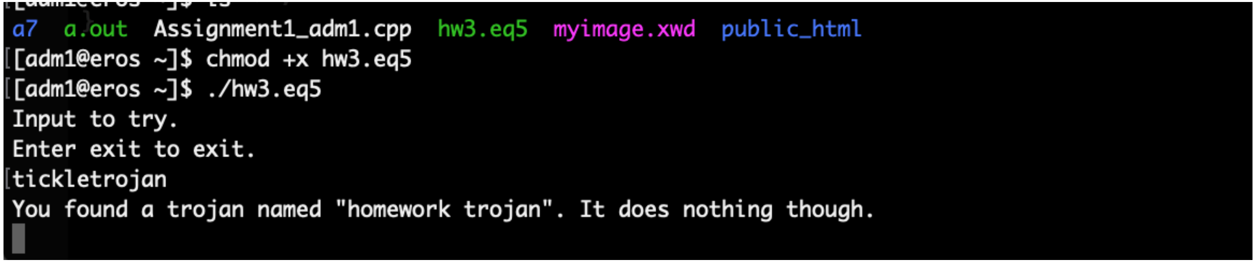
```
[adm1@eros ~]$ ./hw3.eq5
Input to try.
Enter exit to exit.
```

(2) Show the screenshot of decompiling the main() function in your reverse engineering tool (Hopper or Snowman).



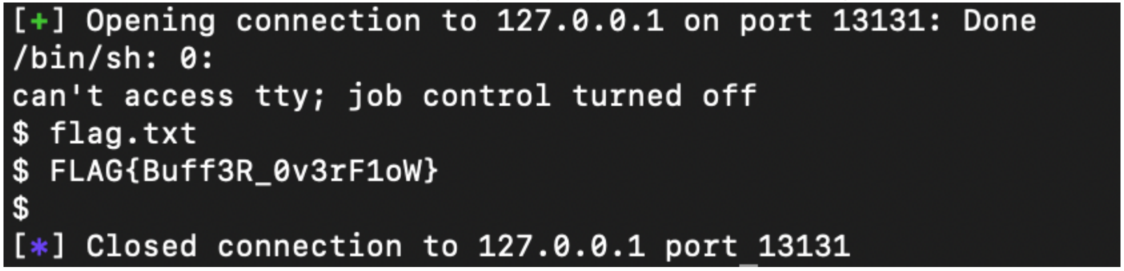
```
int main() {
    puts("Input to try.");
    puts("Enter exit to exit.");
    do {
            do {
                    read(0x0, &var_200, 0x1ff);
                    rax = strncmp(&var_200, "tickletrojan", 0xc);
                    if (rax != 0x0) {
                        break;
                    }
                    trojfoo();
            } while (true);
            rax = strncmp(&var_200, 0x4007c3, 0x4);
            if (rax == 0x0) {
                break;
            }
            puts("You did not find a trojan. Continue try...");
    } while (true);
    rax = exit(0x0);
    return rax;
}
```

(3) Identify the secret input to trigger the Trojan in "hw3.eq5" and show the screenshot of the output of the Trojan.



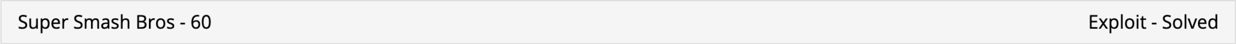
```
[adm1@eros ~]$ ls
a7  a.out  Assignment1_adm1.cpp  hw3.eq5  myimage.xwd  public_html
[adm1@eros ~]$ chmod +x hw3.eq5
[adm1@eros ~]$ ./hw3.eq5
Input to try.
Enter exit to exit.
[tickletrojan
You found a trojan named "homework trojan". It does nothing though.
```

6. (10%) Run the CTF virtual box, read the partial solution of "Super Smash Bros".
(1) Show the screenshot of executing "ls" command after hacking into the server.



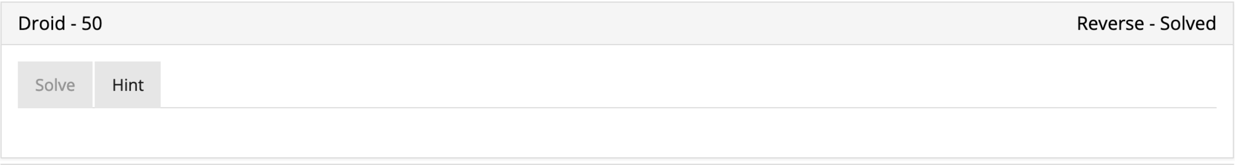
```
[+] Opening connection to 127.0.0.1 on port 13131: Done
/bin/sh: 0:
can't access tty; job control turned off
$ flag.txt
$ FLAG{Buff3R_0v3rF1oW}
$
[*] Closed connection to 127.0.0.1 port 13131
```

(2) Solve the problem and show the screenshot of getting the flag.



Super Smash Bros - 60 Exploit - Solved

7. (10%) Run the CTF virtual box, read the partial solution of "Droid". Solve the problem and show the screenshot of getting the flag.



Droid - 50 Reverse - Solved