COSC130 Fundamentals of Cybersecurity and Privacy

Tutorial Week 7 Solutions

1. [Stalling, 2017] The following a code of a simple virus that we considered in the lecture.

```
Program V :=
{
goto main;
      1234567;
      subroutine infect-executable :=
            {
            loop;
            file := get-random-executable-file;
            if (first-line-of-code = 1234567)
                  goto loop
            else prepend V to file;
            }
      subroutine do-damage :=
            {
            whatever damage is to be done
            }
      subroutine trigger-pulled :=
            {
            return TRUE if some condition is met
            }
main:       main-program :=
      {
      infect-executable;
      if  (trigger-pulled)
            do-damage;
      goto next;
      }
next:
}
```

What will happen when all the executable files on the computer are infected, and program V is executed?

Solution:

If all executable files on the computer are already infected, they will all have '1234567' in the first line (after goto main). Then the condition in the 'if' statement in line 10 will always be satisfied, and the program will always go back to 'loop' in line 8. Therefore, the program will get stuck in the infinite loop in lines 8 - 11, trying to find an uninfected executable file.

2. There is an island in the middle of an ocean where an isolated community lives. There is only one cook on the island, and he cooks for all those islanders and only those islanders who do not cook for themselves. The question is, who cooks for the cook? Explain your answer.

   Solution:

   Cook is one of the islanders, so he cooks for himself if and only if he does not cook for himself!!!

   If cook cooks for the himself, that implies that he does not cook for himself – a contradiction.

   If cook does not cook for himself, then he cooks for himself – again a contradiction.

   We conclude that an island with such a rule (that cook cooks for all those islanders and only those islanders who do not cook for themselves) cannot exist.

3. Although nowadays we have very powerful computers and technologies (for example, AI), there are computational problems that cannot be solved by computers.

   A famous example of such a problem is the so-called halting problem. In general, if an execution of a program on particular input is not affected by any outside influence (e.g., computer crash, power outage), one of the following two things will happen: either the program will halt (finish execution), or it will run forever.

   Halting problem is asking the following question: Is it possible to write a program H, such that H takes any program P and any input I to that P, and outputs YES, if P halts on I, and NO if P does not halt on I.

   We can use reasoning similar to the one in the previous question (Who cooks for the cook?) and show that it is not possible to write such program H.

   In this exercise we focus on a similar question: Is it possible to write a program VIRUS, such that VIRUS takes any program V as its input and outputs YES is V contains a virus

(will infect other programs), and NO is V does not contain a virus. Use reasoning similar to the one in "Who cooks for the cook?" problem.

Solution:

$$VIRUS(V) = \begin{cases} YES\ is\ v\ contains\ a\ virus \\ NO\ is\ V\ does\ not\ contain\ a\ virus \end{cases}$$

We modify the Program V, so that it contains a virus if and only if VIRUS(V) is NO. That is a contradiction, similarly to what we had in the previous exercise.

The new/modified lines are red and the deleted lines are ~~strikethrough~~.

```
Program V :=
{
goto main;
        1234567;
        subroutine infect-executable :=
                {
                loop;
                file := get-random-executable-file;
                if (first-line-of-code = 1234567)
                        goto loop
                else prepend V to file;
                }
        subroutine do-damage :=
                {
                whatever damage is to be done
                }
        subroutine trigger-pulled :=
                {
                return TRUE if some condition is met
                }
main:   main-program :=
                {
                If (VIRUS(V) = YES)
                        goto next;
                else
                        infect-executable;
                ~~if (trigger-pulled)~~
                        ~~do-damage;~~
                goto next;
                }
next:
```

```
}
```

4. [Stallings, 2017] Consider the following fragment:

```
legitimate code
if date is Friday the 13th;
        crash_computer();
legitimate code
```

What type of malicious software is this?

Solution:

This is a logic bomb, as it will lie dormant unless the date is Friday the 13th.

5. [Stallings, 2017] Consider the following fragment in an authentication program:

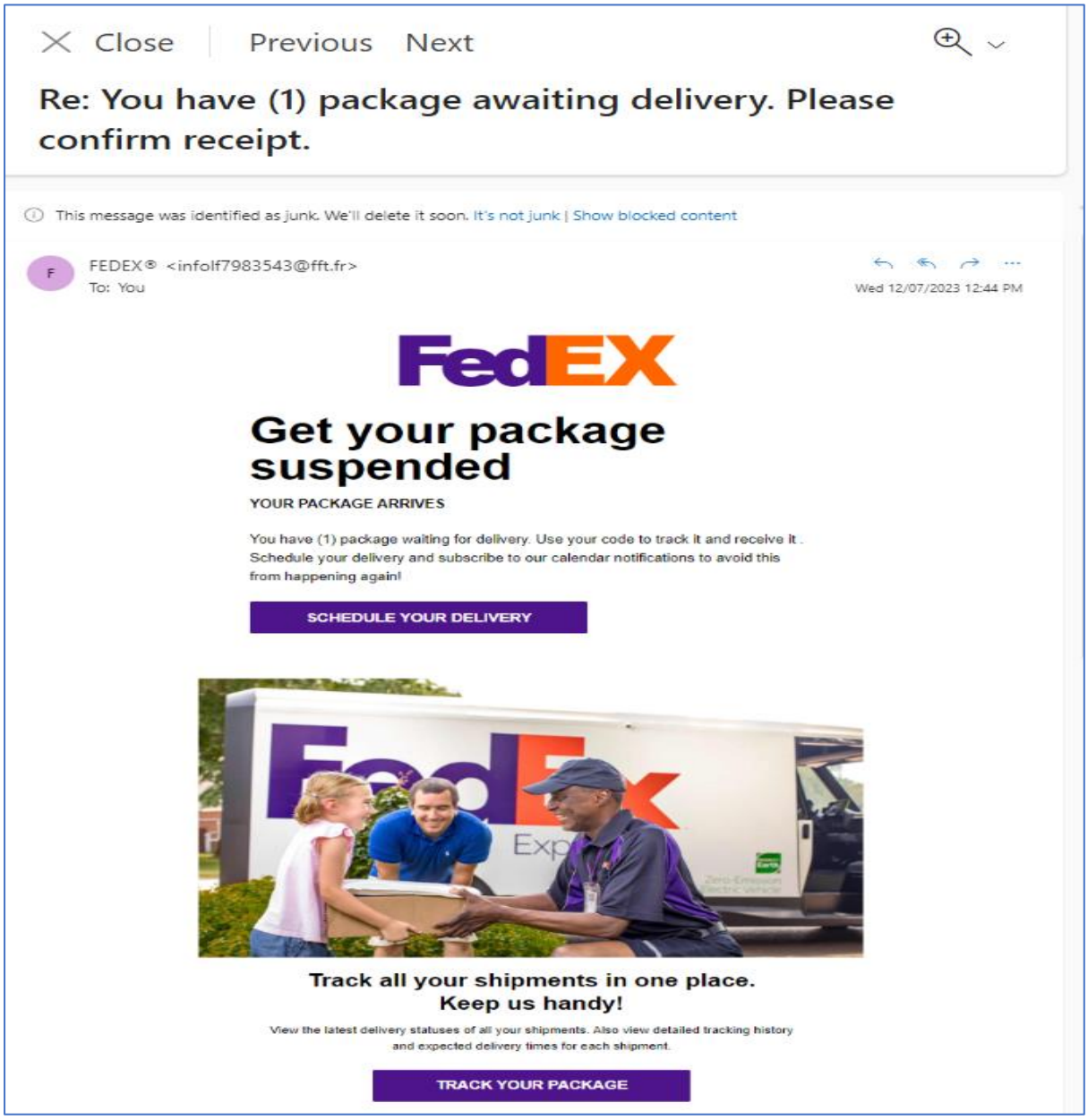
```
username = read_username();
password = read_password();
if username is "133t h4ck0r"
        return ALLOW_LOGIN;
if username and password are valid
        return ALLOW_LOGIN
else return DENY_LOGIN
```

What type of malicious software is this?

Solution:

This is a backdoor, as it allows an attacker to access the system while bypassing the authentication.

6. You have received the following email:



What is the most likely purpose of this email? Justify your answer.

a. To let you know that your package is on its way
b. To check with you when is the best time to deliver your package
c. This is most likely a scam designed to trick you into taking some action detrimental for you, or revealing some information.
d. All of the above
e. None of the above

Solution:

There are several signs that this is a scam: the sender's email does not correspond to FedEX, there is no information specific to the customer and/or shipment, English is akward (Keep us

handy! etc), the message is not logical (you can get your package 'suspended', tracked, or schedule delivery), the email contains an image instead of text and is trying to entice the recipient to reply or go to a particular webpage.

What is the sender of this email most likely trying to achieve? Justify your answer.

f. Get you to reply to this email
g. Get you to visit a webpage where you will be exposed to malware
h. Get you to visit a webpage where you will be tricked into providing some personal information
i. All/any of the above
j. None of the above

Solution: The recipient is invited both to reply to the email, and click on links and be taken to a particular webpage.

7. Personal information such as names, addresses, driver's license and passport details, are usually stolen to enable
    a. hacking
    b. identity theft
    c. house break-ins
    d. all of the above
    e. none of the above

Solution: Some personal information can facilitate hacking (e.g., login details) or house break-in (address), all this information together and more is needed for identity theft.

8. Research antimalware software available in 2024. Identify features that are commonly supported. Create a table to compare at least 5 antimalware software packages in respect to price and identified features.