

HW4

April 5, 2020

Contents

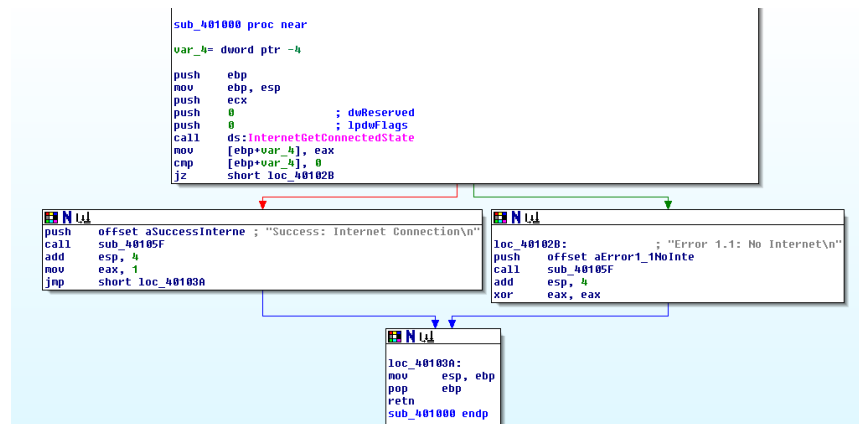
1	Lab 6-1	2
1.1	Question 1	2
1.2	Question 2	2
1.3	Question 3	2
2	Lab 6-2	2
2.1	Question 1	2
2.2	Question 2	3
2.3	Question 3	3
2.4	Question 4	3
2.5	Question 5	4
2.6	Question 6	4
3	Lab 6-3	4
3.1	Question 1	4
3.2	Question 2	5
3.3	Question 3	5
3.4	Question 4	5
3.5	Question 5	6
3.6	Question 6	6
4	Lab 6-4	6
4.1	Question 1	6
4.2	Question 2	6
4.3	Question 3	7
4.4	Question 4	7
4.5	Question 5	7
4.6	Question 6	7

Questions

1 Lab 6-1

1.1 Question 1

Checks to see if there is an internet connection present, and printing a message accordingly.



1.2 Question 2

It appears to be some sort of printing function.

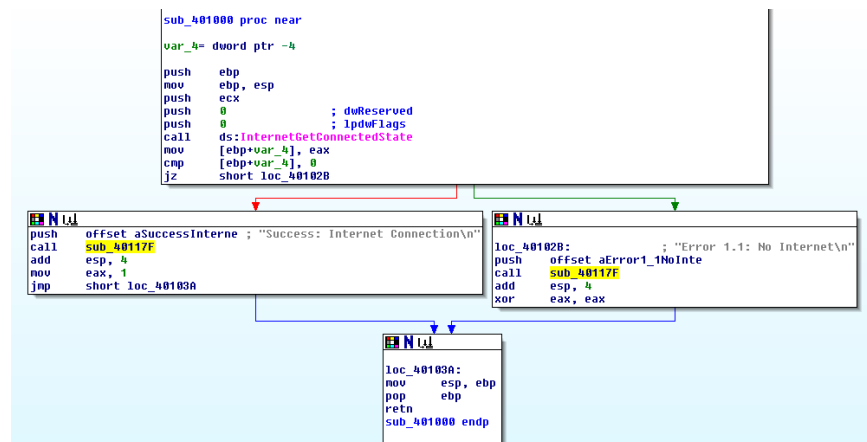
1.3 Question 3

It returns with exit code 1 if there is no internet connection, else 0.

2 Lab 6-2

2.1 Question 1

Same as Lab 6-1.



2.2 Question 2

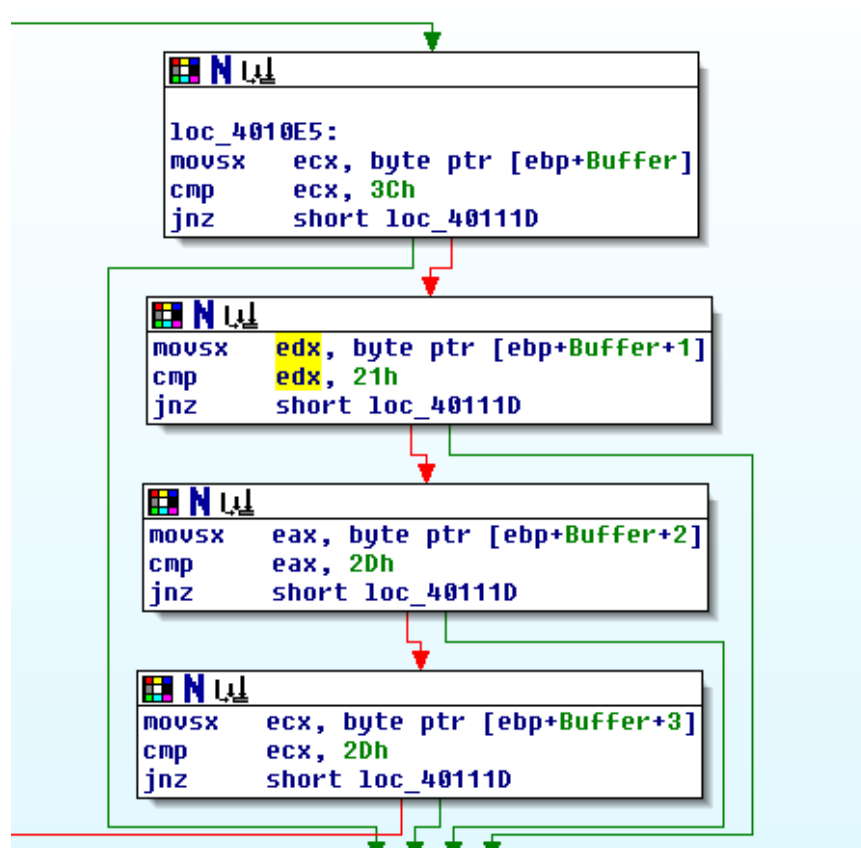
Same as Lab 6-1.

2.3 Question 3

It reads the contents of the page <http://www.practicalmalwareanalysis.com/cc.htm> into a buffer.

2.4 Question 4

Looks like an unrolled loop, looking for a string beginning with <!--, which is the start of an HTML comment.



2.5 Question 5

The program checks the internet connection, and if connected makes a request to <http://www.practicalmalwareanalysis.com/cc.htm>.

2.6 Question 6

It checks the internet connection, and if so prints out a byte as a "command" from an HTML comment on a webpage, then sleeps and exits.

3 Lab 6-3

3.1 Question 1

There's a new subroutine that does something with the command instead of just exiting.



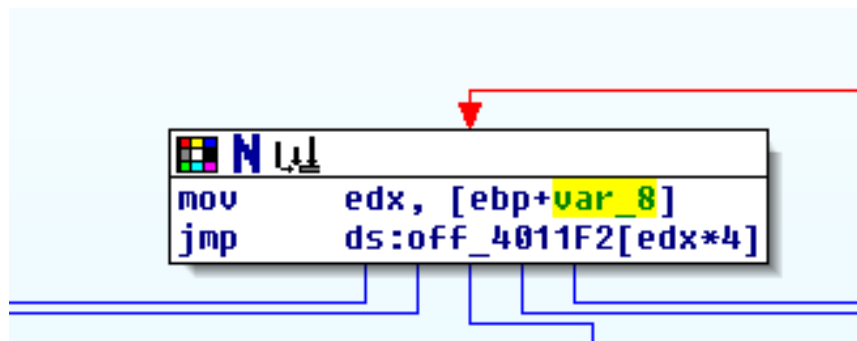
```
loc_40123C:
movsx ecx, [ebp+var_8]
push ecx
push offset aSuccessParsedC ; "Success: Parsed command is %c\n"
call sub_401271
add esp, 8
mov edx, [ebp+argv]
mov eax, [edx]
push eax ; lpExistingFileName
mov cl, [ebp+var_8]
push ecx ; char
call sub_401130
add esp, 8
push 0EA60h ; dwMilliseconds
call ds:Sleep
xor eax, eax
```

3.2 Question 2

A filename and a buffer. In this case it's called with the path of the running program, and the command.

3.3 Question 3

Looks like a jump table based on the command.



3.4 Question 4

It can do 5 different things depending on the command, either create a directory C:\Temp, copy itself to C:\Temp\cc.exe, delete C:\Temp\cc.exe, add C:\Temp\cc.exe to the startup registry key, or sleep and exit.

3.5 Question 5

It can create the file C:\Temp\cc.exe or the registry key Software\Microsoft\Windows\CurrentVersion

3.6 Question 6

The program makes sure there is an internet connection, then reads a command from a command and control server, then does some various things based on the command.

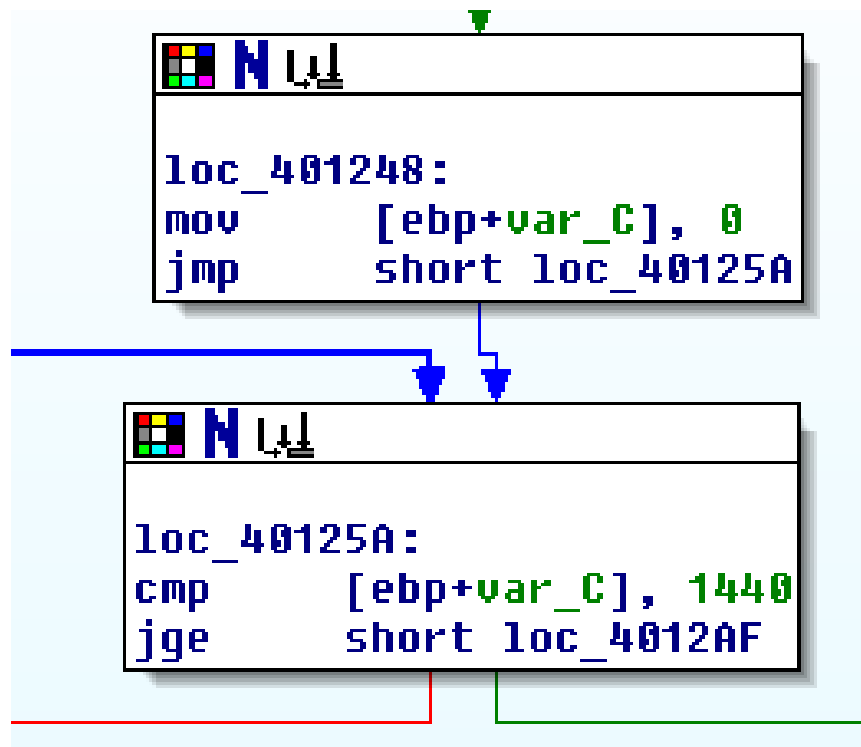
4 Lab 6-4

4.1 Question 1

The command parsing function has a new argument.

4.2 Question 2

A loop has been added around the main body.



4.3 Question 3

It now uses the loop counter in the user agent used to make the request to the webpage.

4.4 Question 4

The main loop runs 1440 times, each loop sleeping 60 seconds plus any network request time, so for around 1 day.

4.5 Question 5

The user agent is different this time.

4.6 Question 6

Same as the last one, except it now executes commands repeatedly instead of just once.