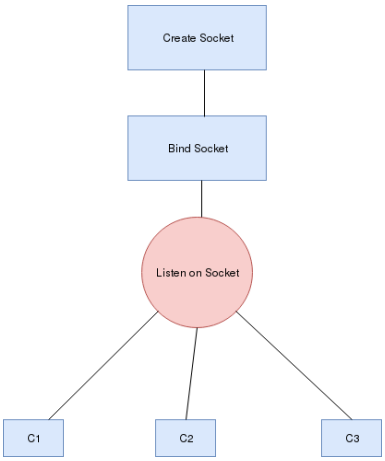
CS4480-Networking Programming Asgmt-1

Salvador Gutierrez

February 2019

1 Introduction

My multi-client proxy is non-sophisticated and bulky by design constrainst(we couldn't use 'request' libraries, so we are re-inventing the wheel). It only uses sockets, I run an event-loop that is constantly listening for connections. Upon a connection happening I spin up a thread that will handle the rest of the logic.



Each thread has a function called "conn" which gets the request, checks if it is correctly formatted (Allowing for both relative and absolute URI's). If it is correctly formatted it proceeds to send the request to the end-point and intercepts the response. Upon intercepting the response I check the content type, the 2 outputs I care about are "text/html" and "application". If it is text/html I send it to a function which parses it scanning for the word "Simple" or "simple", upon finding an instance I change it to "Silly" or "silly" accordingly and then send the response back to the client. If the response from the end-point is an application I extract the byte-code and use python's hashlib.md5 to get a hex-digest of the byte-code. I then establish a connection to VirusTotal and make a request for a scan with my api-key and the md5 digest produced. The response from VirusTotal will be JSON. I can then check if there are any positive scans that indicate if it is malware. If it is malware I respond with an

HTML web-page containing the info and permalink of the scan. Otherwise I simply send an OK response with the byte-code.

2 Testing

In order to test my proxy I opted in using Firefox and pointing it to my proxy running on my localhost:6666. At every step I made sure I could access:

- http://www.cs.utah.edu/ germain/CS4480/index.html
- http://www.cs.utah.edu/ kobus/simple.html

Which was true. However when I got to the final part I had issues obtaining the correct checksums of binary files. I realized this when I decided to download the *hello_world.exe* file and get an md5 checksum from my terminal. The solution to this turned out to be that I had to keep working in bytes instead of encoding to a string (I lost some information that way).

- I tested being able to load/download 'http://www.cs.utah.edu/ germain/CS4480/hello_world.exe' from my browser.
- I also tested using telnet to access relative URI's (results will be in the 'Output' part of this report).
- I also tested using different ports in the URI for both relative and absolute URI's.

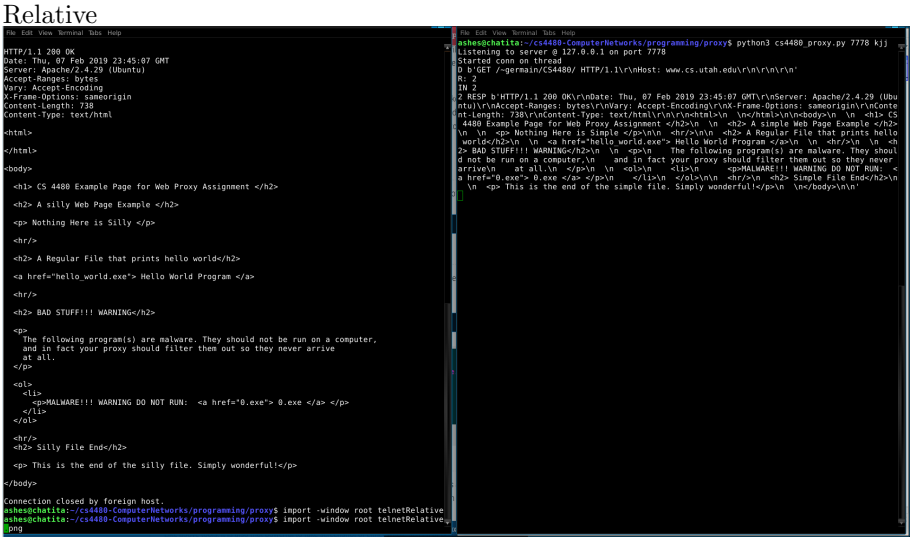
Other tests I did included using a service like http://httpvshttps.com/ to see if I could load pages with more content than just the simple cases above. This also worked successfully.

Finally, I tested that unsupported methods returned a '501 Not Implemented' and non-well formed requests return a '400 Bad Request'.

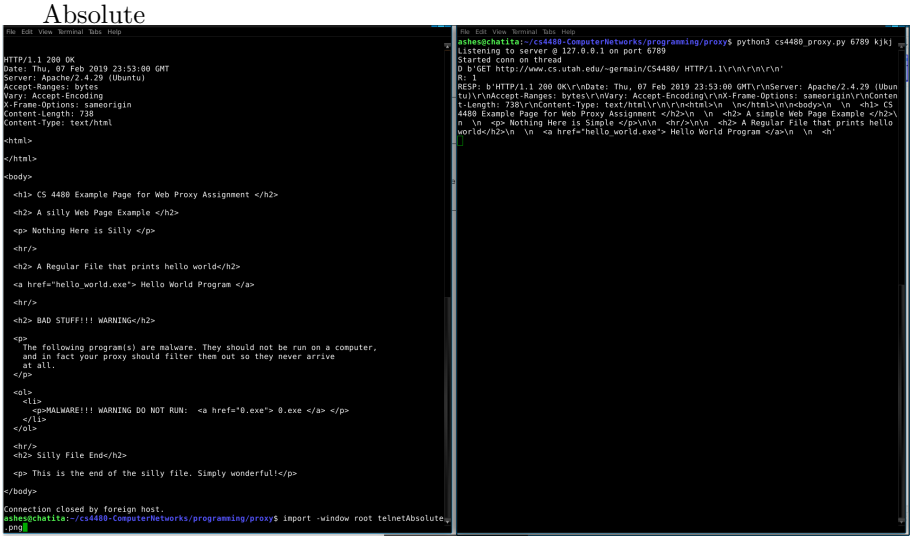
UNDEFINED BEHAVIOR: It was not specified in the instructions for this assignment what we should do if a response does not include the 'Content-Type' so my function that detects whether something is an application or just text/html will not work if this header line is not specified.

3 Output

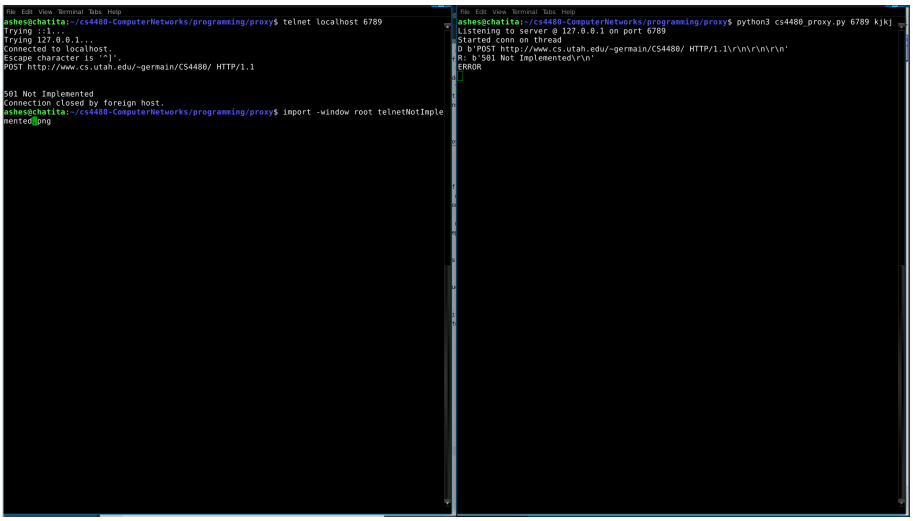
Basic Cases Telnet:
Relative



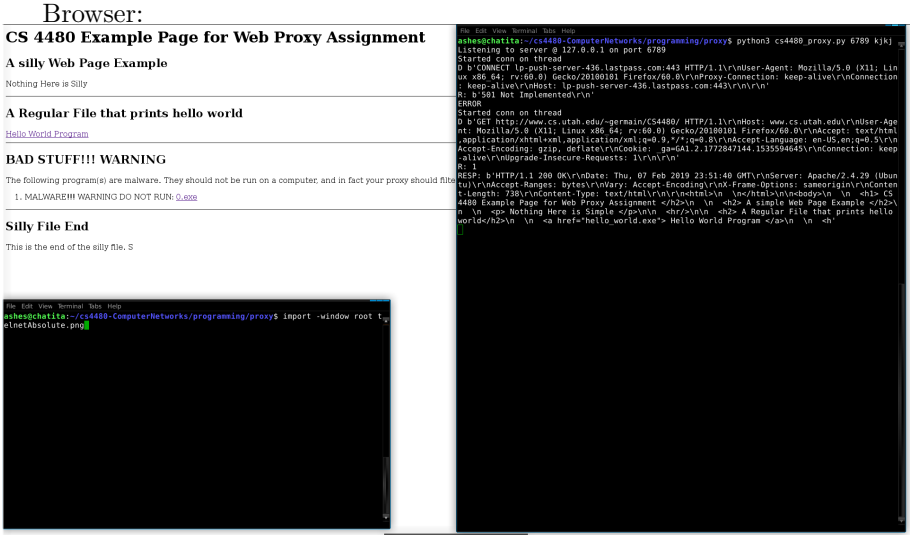
Absolute



Not Implemented and Bad Request

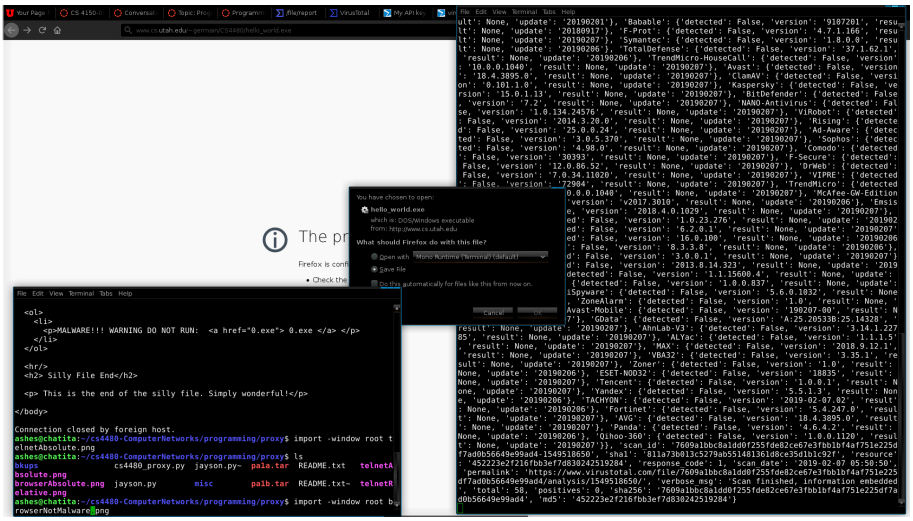

ashes@chatita:~/cs4480-ComputerNetworks/programming/proxy$ telnet localhost 6789
Trying ::1...
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
POST http://www.cs.utah.edu/~germain/CS4480/ HTTP/1.1
501 Not Implemented
Connection closed by foreign host.
ashes@chatita:~/cs4480-ComputerNetworks/programming/proxy$ import -window root telnetNotImplemented.png
ashes@chatita:~/cs4480-ComputerNetworks/programming/proxy$ python3 cs4480_proxy.py 6789 kjkj
Listening to server @ 127.0.0.1 on port 6789
Started conn on thread
D b'POST http://www.cs.utah.edu/~germain/CS4480/ HTTP/1.1\r\n\r\n\r\n'
R: b'501 Not Implemented\r\n'
ERROR
ashes@chatita:~/cs4480-ComputerNetworks/programming/proxy$ telnet localhost 6789
Trying ::1...
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
GET /~germain/CS4480/ HTTP5.1
Host: www.cs.utah.edu
400 Bad Request
Connection closed by foreign host.
ashes@chatita:~/cs4480-ComputerNetworks/programming/proxy$ import -window root telnetBadRequest.png

Browser:


CS 4480 Example Page for Web Proxy Assignment
A silly Web Page Example
Nothing Here is Silly
A Regular File that prints hello world
Hello World Program
BAD STUFF!!! WARNING
The following program(s) are malware. They should not be run on a computer, and in fact your proxy should filte
1. MALWARE!!! WARNING DO NOT RUN: 0.exe
Silly File End
This is the end of the silly file. S
ashes@chatita:~/cs4480-ComputerNetworks/programming/proxy$ python3 cs4480_proxy.py 6789 kjkj
Listening to server @ 127.0.0.1 on port 6789
Started conn on thread
D b'CONNECT lp-push-server-436.lastpass.com:443 HTTP/1.1\r\nUser-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0\r\nProxy-Connection: keep-alive\r\nConnection: keep-alive\r\nHost: lp-push-server-436.lastpass.com:443\r\n\r\n'
R: b'501 Not Implemented\r\n'
ERROR
Started conn on thread
D b'GET http://www.cs.utah.edu/~germain/CS4480/ HTTP/1.1\r\nHost: www.cs.utah.edu\r\nUser-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\nAccept-Language: en-US,en;q=0.5\r\nAccept-Encoding: gzip, deflate\r\nCookie: _ga=GA1.2.1772847144.1535594645\r\nConnection: keep-alive\r\nUpgrade-Insecure-Requests: 1\r\n\r\n'
R: b
RESP: b'HTTP/1.1 200 OK\r\nDate: Thu, 07 Feb 2019 23:51:40 GMT\r\nServer: Apache/2.4.29 (Ubuntu)\r\nAccept-Ranges: bytes\r\nVary: Accept-Encoding\r\nX-Frame-Options: sameorigin\r\nContent-Length: 730\r\nContent-Type: text/html\r\n\r\n<html>\n \n</html>\n\n<body>\n \n <h1> CS 4480 Example Page for Web Proxy Assignment </h2>\n \n <h2> A simple Web Page Example </h2>\n \n   Nothing Here is Simple \n\n <hr/>\n\n <h2> A Regular File that prints hello world</h2>\n \n Hello World Program \n \n <h'
The File you requested appears to contain
Information:
MD5 Hash: 2d75cc1bf8e57872781f9cd04a529256
Positives: 27
Scan Date: 2019-01-25 07:01:21
First Scan ID: Bkav
Thanks to VirusTotal for this information.
For more information see Virus Total Permanent Link
ashes@chatita:~/cs4480-ComputerNetworks/programming/proxy$ import -window root telnetAbsolute.png

MALWARE!!! WARNING DO NOT RUN: 0.exe

<hr/>
<h2> Silly File End</h2>
 This is the end of the silly file. Simply wonderful!
</body>
Connection closed by foreign host.
ashes@chatita:~/cs4480-ComputerNetworks/programming/proxy$ import -window root telnetAbsolute.png
ashes@chatita:~/cs4480-ComputerNetworks/programming/proxy$ ls
bkups cs4480_proxy.py jayson.py~ pala.tar README.txt
bsolute.png
browserAbsolute.png jayson.py misc palb.tar README.txt~
elative.png
ashes@chatita:~/cs4480-ComputerNetworks/programming/proxy$ import -window root telnetBrowserNotMalware.png
ashes@chatita:~/cs4480-ComputerNetworks/programming/proxy$ import -window root telnetBrowserMalware.png


hello_world.exe
What should Firefox do with this file?
Open file
Save file
Cancel

MALWARE!!! WARNING DO NOT RUN: 0.exe

<hr/>
<h2> Silly File End</h2>
 This is the end of the silly file. Simply wonderful!
</body>
Connection closed by foreign host.
ashes@chatita:~/cs4480-ComputerNetworks/programming/proxy$ import -window root telnetAbsolute.png
ashes@chatita:~/cs4480-ComputerNetworks/programming/proxy$ ls
bkups cs4480_proxy.py jayson.py~ pa1a.tar README.txt telnetAbsolute.png
browserAbsolute.png jayson.py misc pa1b.tar README.txt~ telnetRelative.png
ashes@chatita:~/cs4480-ComputerNetworks/programming/proxy$ import -window root browserNotMalware.png