Capture the Flag Write Up

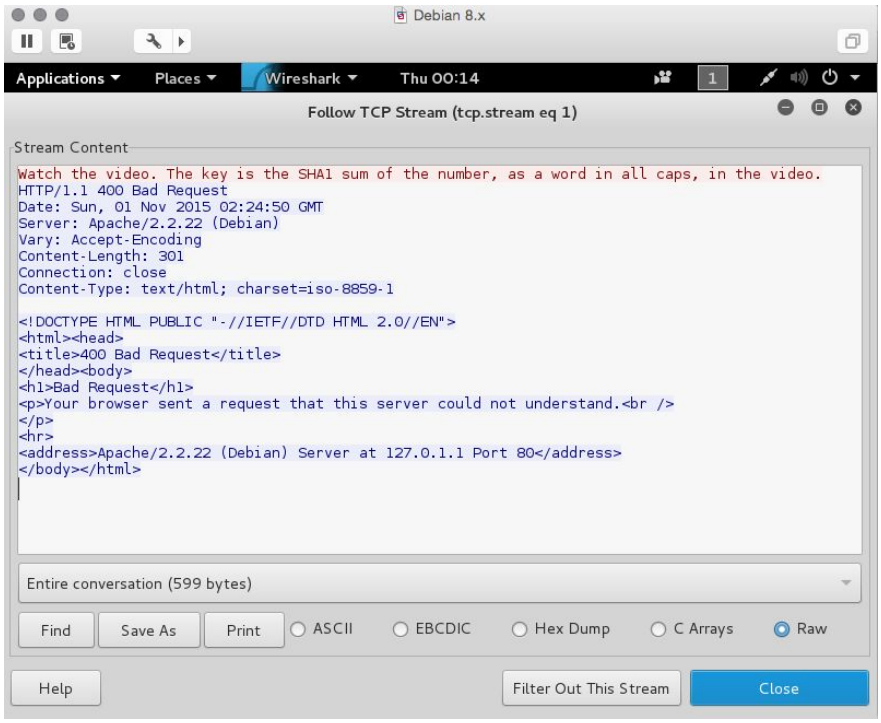
Assignment 3 - 11/5/15

Margaret Feltz, Susie Church, Mathurshan Vimalesvaran, Nik Telkedzhiev (ntelke01)

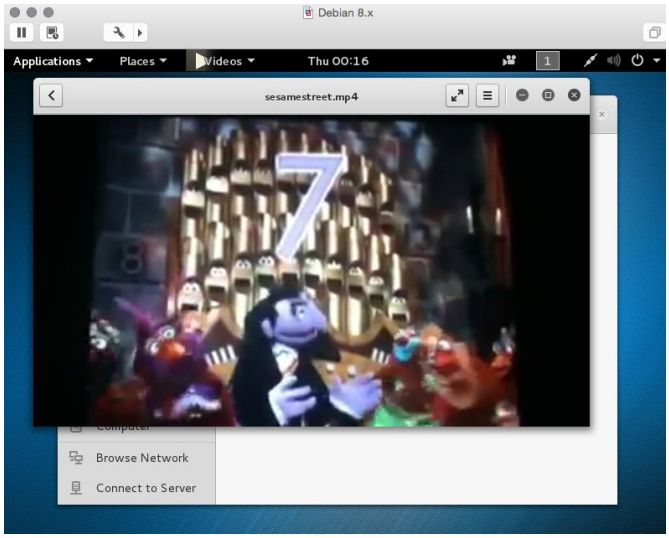
600 pts

Analyze the binary (200):

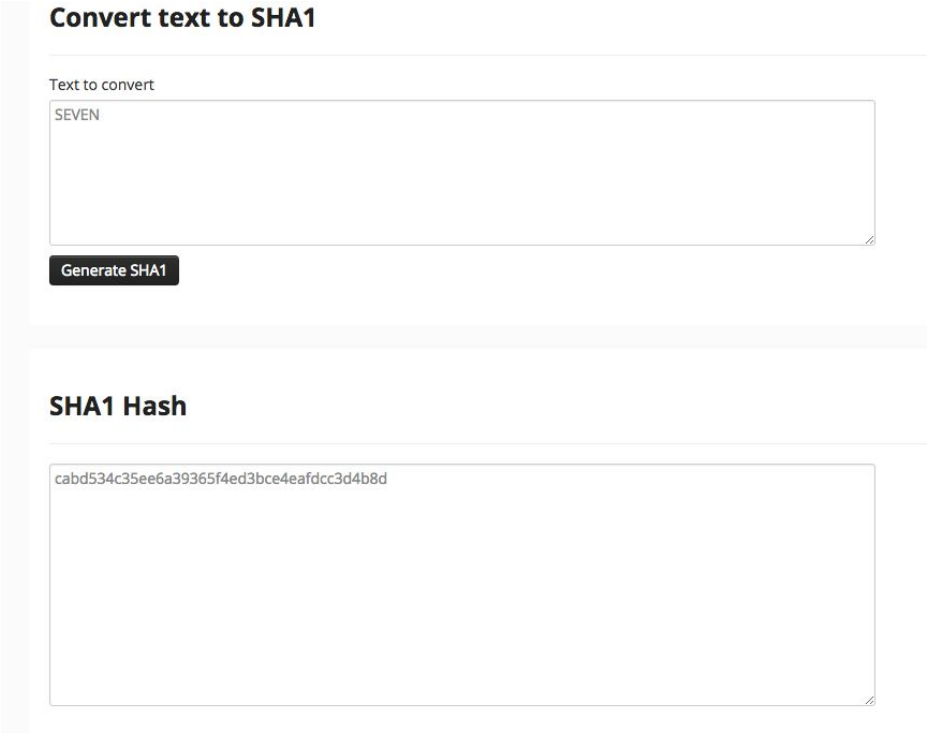
1) We clicked on runme.exe and nothing executed, so we ran *file runme.exe* in the terminal and found that it was a tcpdump capture file.
2) Opened the file in Wireshark and filtered using “tcp contains key”.
3) Found 2 packets: one which contained the instructions found by following the TCP stream and one that was the video file that we exported. The first packet instructions said:



4) We extracted the mp4 file from the stream.

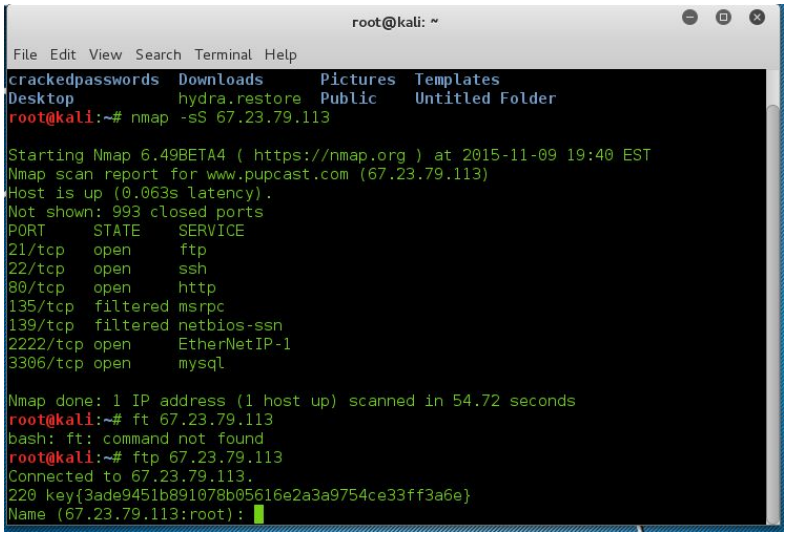


5) Put the string “SEVEN” into a SHA1 hash generator and found the flag was the generated hash. (www.timestampgenerator.com/tools/sha1-generator/)



Unnecessary Service (100):

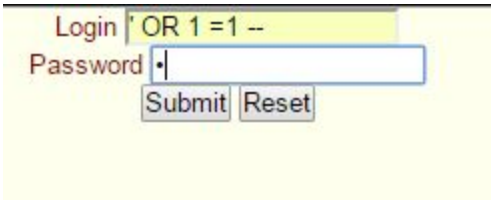
1) Ran *nmap -sS 67.23.79.113* to see what ports were open.
2) Looked for unnecessary services on open ports, found FTP on port 21.
3) FTPed to the server ip.
4) Got the key as a response.



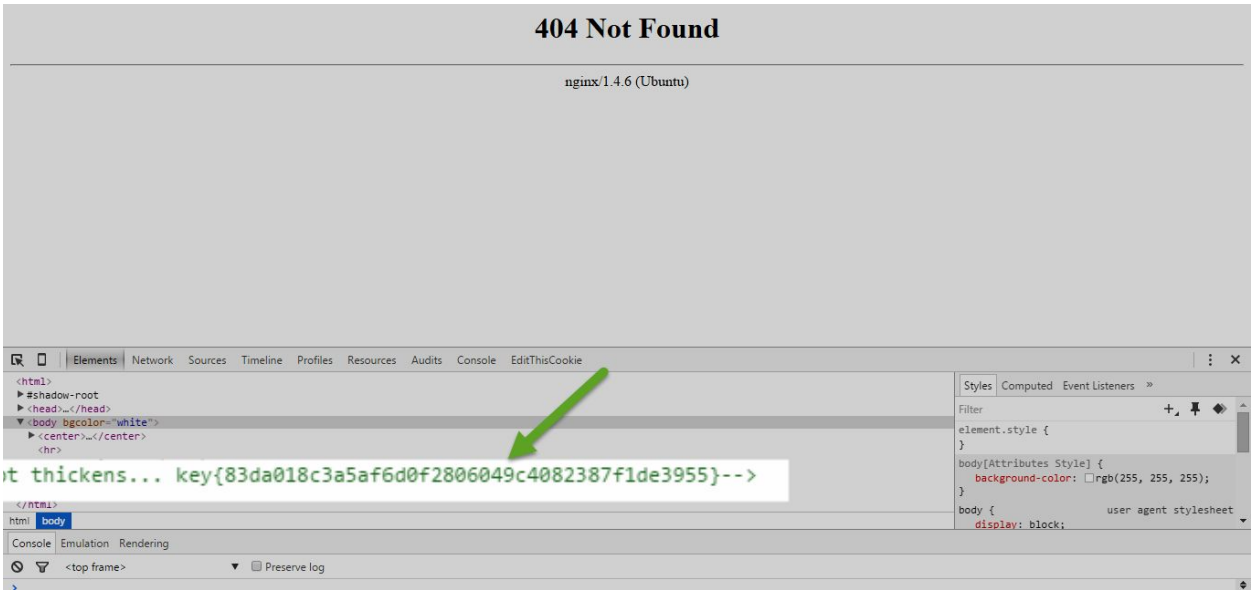
Login SQL Injection (200 points)

1) Went to 67.23.79.113/ctf/board.php with JS disabled
2) Navigated to bottom of page and clicked “Administration” link
3) Arrived at http://67.23.79.113/ctf/admin.php (as seen below)

4) Injected SQL to bypass login with any password (as seen below)



5) Successful login took us to http://67.23.79.113/ctf/main.php with flag in HTML source as a comment (as seen below)



Logout.php (100):

1. Navigated to http://67.23.79.113/ctf/logout.php after successfully logging into main.php to cover your tracks. Logout success message was displayed on page (as seen below)

2. Flag was at bottom of page (as seen below)