LOCKHEED MARTIN CYBERQUEST™ COMPETITION

CHALLENGES & SKILLS OVERVIEW

LOCKHEED MARTIN

WHAT MAY YOU ENCOUNTER?

- Challenges may include:
  - Web-based attacks
    - Common vulnerabilities found within websites across the internet
  - Windows & Linux privilege escalation
    - Find vulnerabilities to move from a user to an administrator
  - Packet capture & log analysis
    - A network traffic capture or various application / server logs commonly analyzed by cyber incident responders to retrace an adversary's steps
  - Steganography
    - The practice of concealing a file, message, image, or video within another file, message, image, or video
  - Reverse engineering
    - The processes of extracting knowledge or design information from anything man-made and reproducing it or reproducing anything based on the extracted information
  - Cryptography
    - The construction and analysis of techniques that prevent eavesdroppers from reading private messages

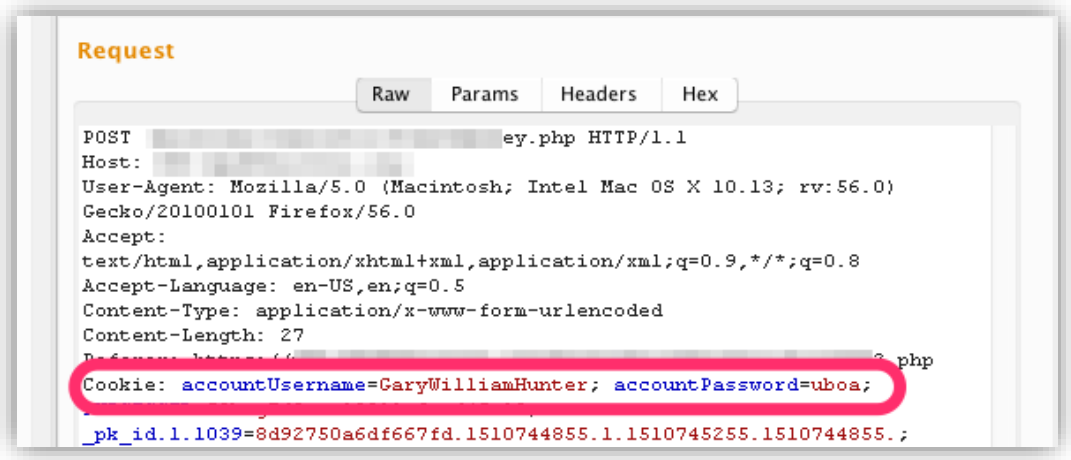
No one will be an expert in everything. This is a chance to expand your skills.

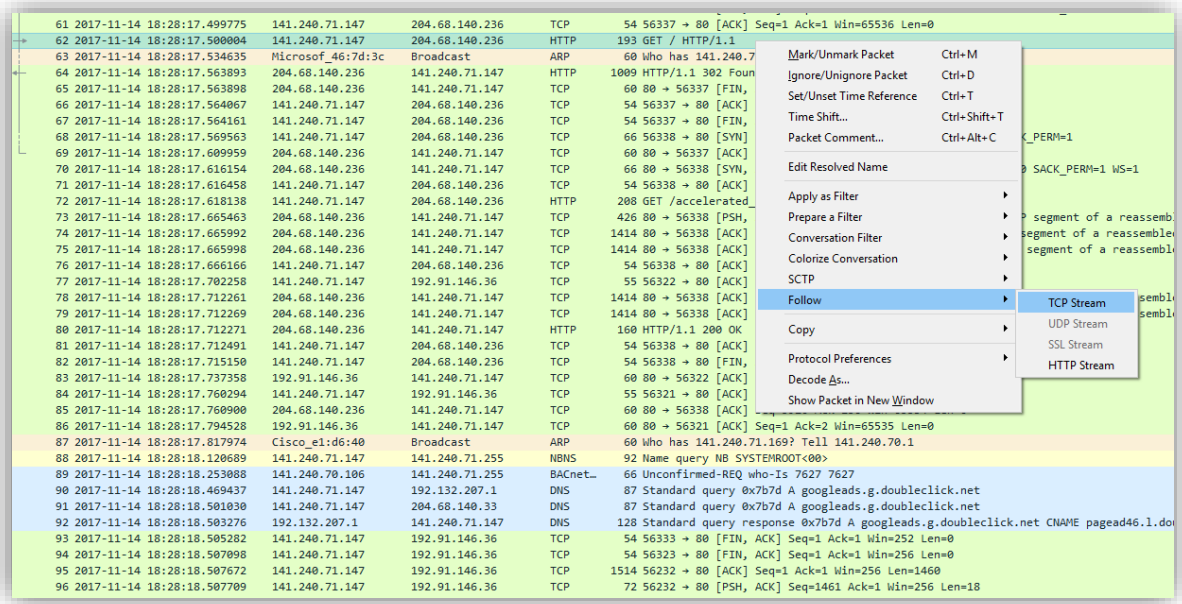
WHAT WOULD BE GOOD TO KNOW?

THESE TOPICS WILL HELP YOU PREPARE FOR THE COMPETITION

GENERAL SKILLS & ABILITIES

- Familiarity with…
  - Linux & bash (including common CLI tools)
  - Common inter-computer communications
  - Kali & Metasploit
  - Network / Host recon (nmap / wireshark)
  - Intercepting proxies (Burp Suite)
  - Scripting (python)



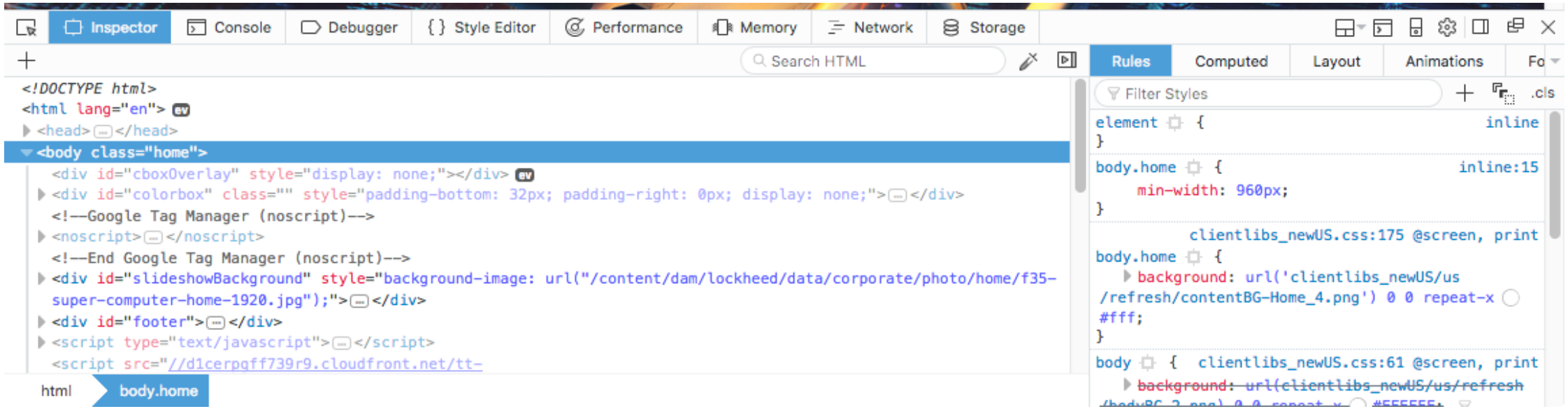


OFFENSIVE AREAS TO STUDY

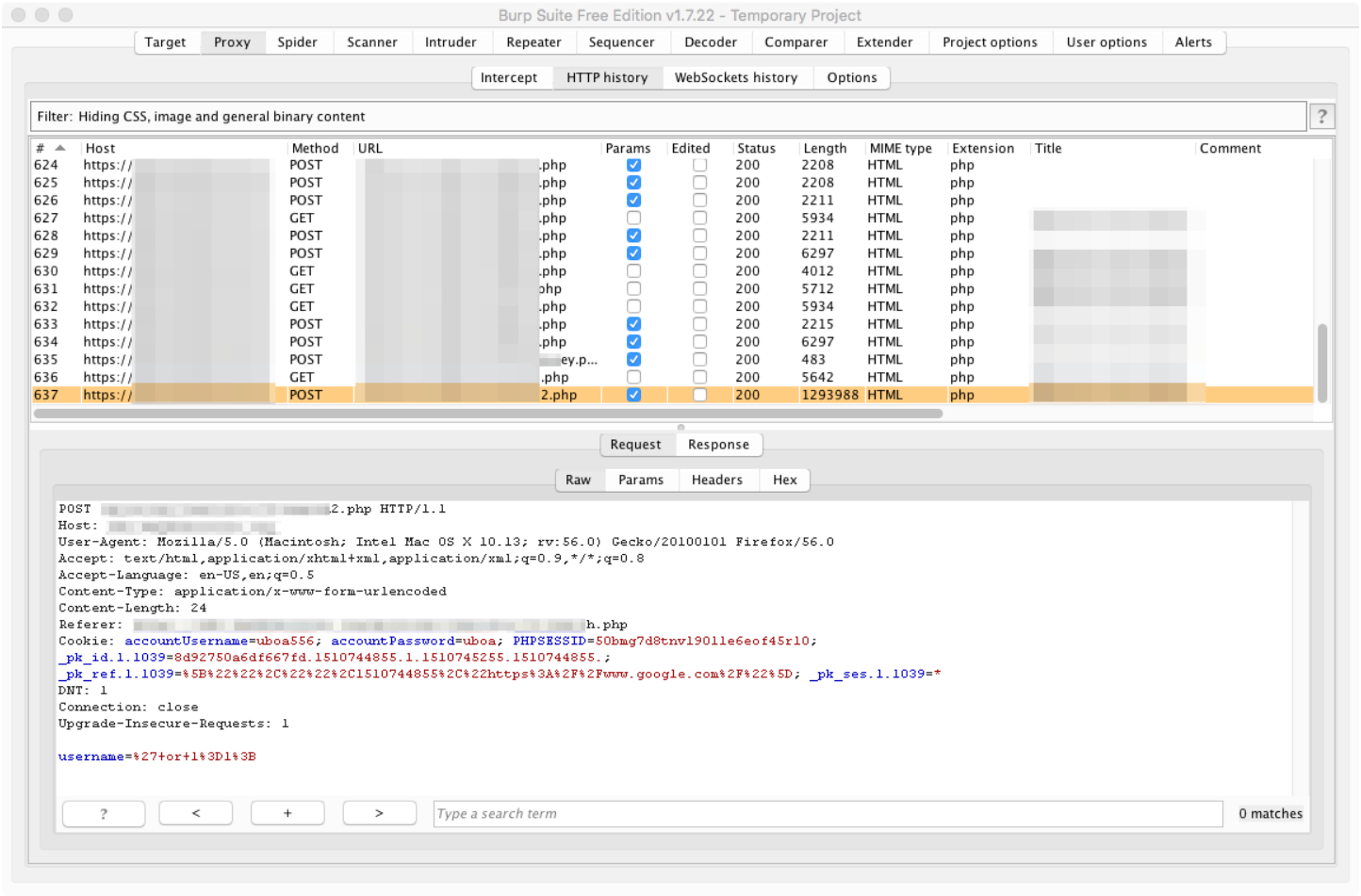
- Common web application security vulnerabilities
  - OWASP Top 10
- Configuring a browser to use an intercepting proxy such as Burp Suite (and how to use that proxy)
- Port scanning tools such as nmap
- How to use ssh
- Read / write basic bash & html
- Common tools in Kali Linux

A SOLID UNDERSTANDING OF THE GENERAL PRINCIPLES / ABILITIES WILL DO YOU WELL.

HTML & AN INSPECTOR SHOULD BE FAMILIAR



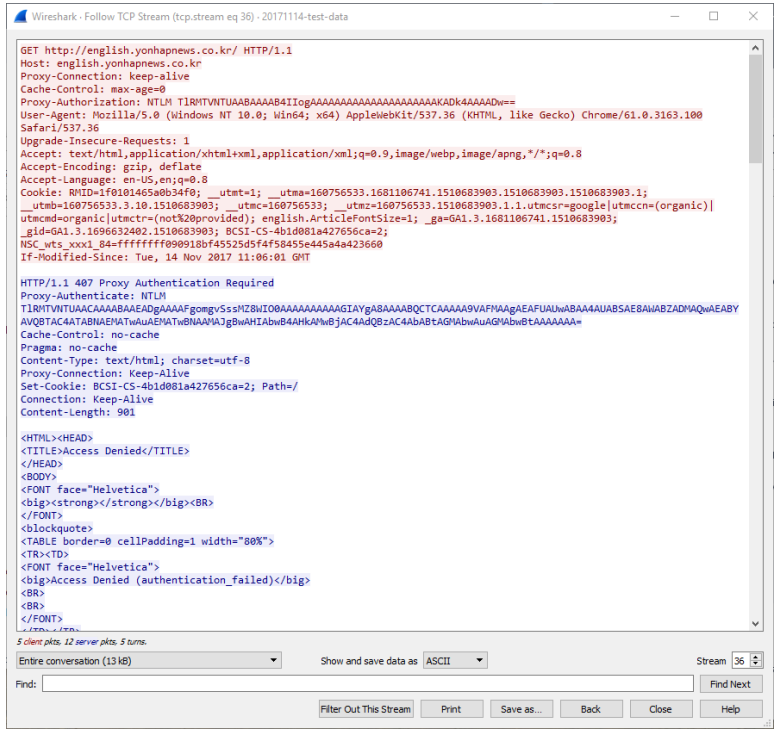
... AS SHOULD BURP SUITE



…LOGS & WIRESHARK TOO

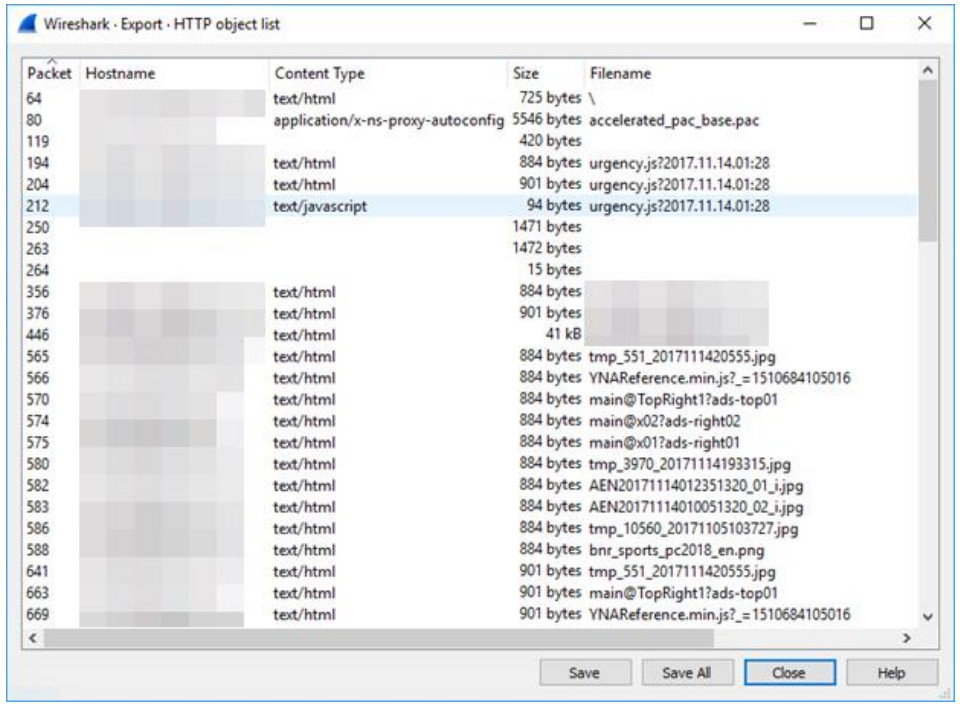
```
$ cat /cygdrive/c/Users        'Desktop/Working/Projects/Code\ Quest\ Cyber/Test-Data/u_ex171115.log | head -5
14.139.187.130 - - [01/Jan/2017:02:16:51 -0800] "GET / HTTP/1.1" 200 10267 "https://www.google.co.in/" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.87 Safari/537.36"
14.139.187.130 - - [01/Jan/2017:02:16:55 -0800] "GET /GitHub-Mark.png HTTP/1.1" 200 7428 "http://www.secrepo.com/" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.87 Safari/537.36"
14.139.187.130 - - [01/Jan/2017:02:16:56 -0800] "GET /twitter-icon.png HTTP/1.1" 200 27788 "http://www.secrepo.com/" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.87 Safari/537.36"
68.180.228.229 - - [01/Jan/2017:02:17:59 -0800] "GET /robots.txt HTTP/1.1" 200 233 "-" "Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)"
68.180.228.229 - - [01/Jan/2017:02:17:59 -0800] "GET /self.logs/access.log.2015-11-01.gz HTTP/1.1" 200 6465 "-" "Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)"
```

Examining a flat text file that is delimited with a space



Following a TCP Stream

...MORE WIRESHARK & SOME PYTHON



Exporting HTTP Objects

```
>>> encoded = '1b37373331363f78151b7f2b783431333d78397828372d363c78373e783a393b3736'
>>> import binascii
>>> nums = binascii.unhexlify(encoded)
>>> strings = (''.join(chr(num ^ key) for num in nums) for key in range(256))
>>> max(strings, key=lambda s: s.count(' '))
```

Simple Python Encryption Algorithm

A FEW HANDY TOOLS

- ImageMagick
  - https://www.imagemagick.org/download/binaries/ImageMagick-7.0.8-8-portable-Q16-x86.zip
- OllyDbg 1.10
  - http://www.ollydbg.de/download.htm
- x64dbg (snapshot_2018-07-15_19-25)
  - https://sourceforge.net/projects/x64dbg/files/snapshots/

BEING FAMILIAR WITH WHAT EACH OF THESE CAN DO WILL BE HELPFUL.

A FEW MORE HANDY TOOLS

- Portable App Platform
  - https://portableapps.duckduckgo.com/pacplatform/PortableApps.com_Platform_Setup_15.0.2.paf.exe

- For Windows, these portable apps may be useful
  - 7-ZipPortable
  - DiffImgPortable
  - DiffpdfPortable
  - FileAlyzerPortable
  - FirefoxPortable
  - FrhedPortable
  - GIMPPortable
  - gVimPortable
  - InkscapePortable
  - JPEGViewPortable
  - KeepNotePortable
  - Notepad++Portable
  - PortableApps.com
  - winMd5SumPortable

MANY OF THESE ARE AVAILABLE NATIVELY ON LINUX.

ADDITIONAL RESOURCES

- Common web vulnerabilities
  - https://www.owasp.org Top 10 for 2017, 2013, 2010

- Tools included in Kali Linux like webshells
  - https://tools.kali.org/maintaining-access/webshells

- Bash
  - Search for “intro to bash programming” and read the first few pages of pretty much any result that you find interesting

- Burp Suite
  - https://portswigger.net/burp

ADDITIONAL RESOURCES

- Nmap
  - Search for common scan syntax – know how to scan common ports, perform a service scan
- Common Linux commands
  - Your favorite search engine will answer all your questions
    - awk, cut, sed, wc, less, grep
- Wireshark
  - Search for how to filter on IP addres, port, HTTP request method
  - Search for how to follow streams, inspect packet fields
  - Search for how to carve files from:
    - Pcap, stream, specific packet


LOCKHEED MARTIN