Cyber Defense Organization

Spring 2020 - Network Forensics with Wireshark

WORD OF THE WEEK: MALWARE SANDBOX

Malware Sandbox

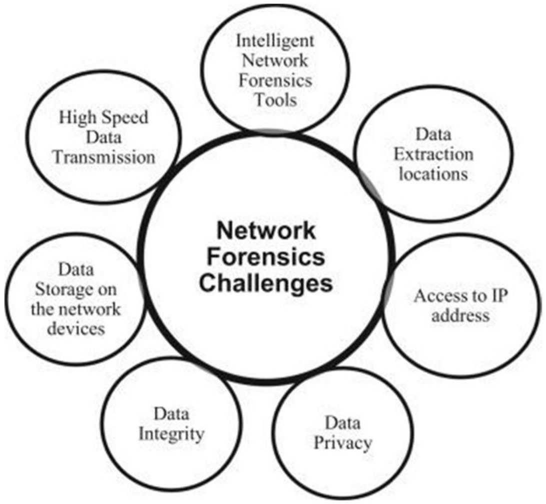
- When testing out malware it is important to isolate it
- That’s what sandboxes are for - to simulate and record all behavior
- Some examples: Joe’s Sandbox & Cuckoo

The End of the Trilogy

- We did Nmap (or would have) & Google Dorking
- Now it is time for Network Forensics to tie it all up!
- Open Up Wireshark
- https://tinyurl.com/CDONetworkForensics

What Is Network Forensics

- Sub branch of Digital Forensics, can be used to support traditional investigations
- Examines one of the most volatile & important artifacts: network traffic
- Can be used in a Cyber Security standpoint to detect lateral movement, C2 communications, etc
- How Marshal busted students cheating last year O.O


Network Forensics Challenges
Intelligent Network Forensics Tools
Data Extraction locations
Access to IP address
Data Privacy
Data Integrity
Data Storage on the network devices
High Speed Data Transmission

What is Wireshark?

- A packet analyzer/sniffer, great way to view in depth info about packets
  - Can detect granular info such as TCP/UDP flags and ethernet data all the way up to HTTP requests, & FTP requests
- Uses pcap files
- Important to have a grasp of networking in order to use it to full potential
  - Remember that networking workshop on protocols from the first semester?

Who Uses Wireshark?

- I’ve used wireshark or some form of it whenever I am stuck on a networking troubleshooting problem
- Cyber security experts use it to look closer at network traffic for malware analysis
- Hackers use it in order to gather info needed to successfully execute networking attacks and sniff out unencrypted credentials

Quick Example of Fun Hacker things

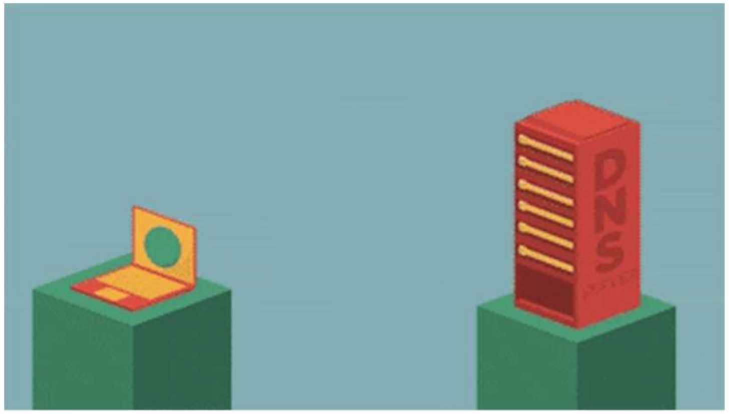
- Telnet sucks, it is unencrypted and unsecure
- Let’s see why (follow along on board)
- https://tinyurl.com/telnetpcap

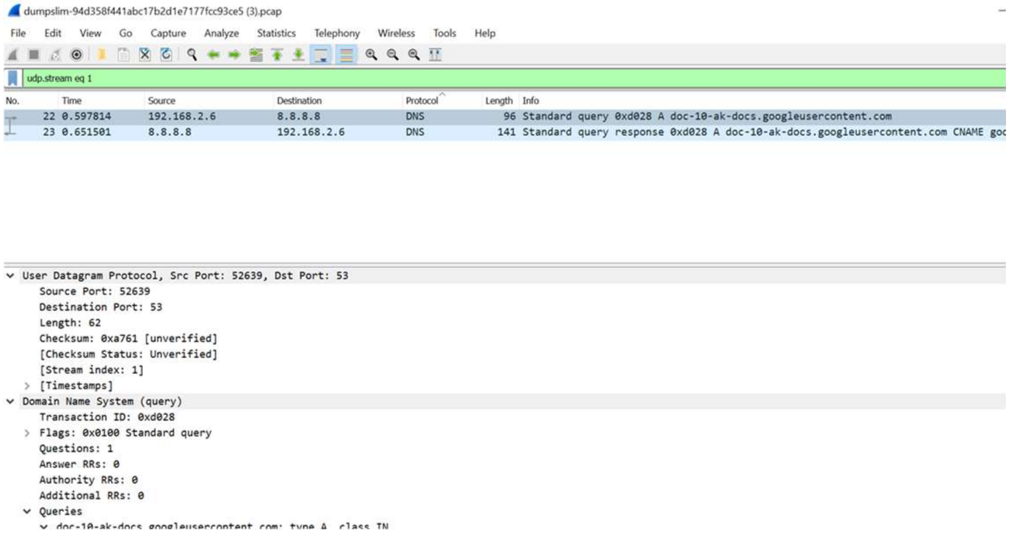
What we will be Doing today?

- I have found a great Pcap file of an actual trojan attack that we will be analyzing
- First though, let's go through some terminology and Wireshark filters

DNS

- DNS is the process of translating URLs to IP addresses
- When you type “google.com” a dns query goes out asking what that is, usually receives an A record back
- That DNS query goes to wherever your DNS servers are, in the case of this file it goes to google’s public DNS





udp.stream eq 1

```
No.   Time        Source         Destination    Protocol   Length  Info
   22 0.597814    192.168.2.6    8.8.8.8        DNS            96  Standard query 0xd028 A doc-10-ak-docs.googleusercontent.com
   23 0.651501    8.8.8.8        192.168.2.6    DNS           141  Standard query response 0xd028 A doc-10-ak-docs.googleusercontent.com CNAME goo
```

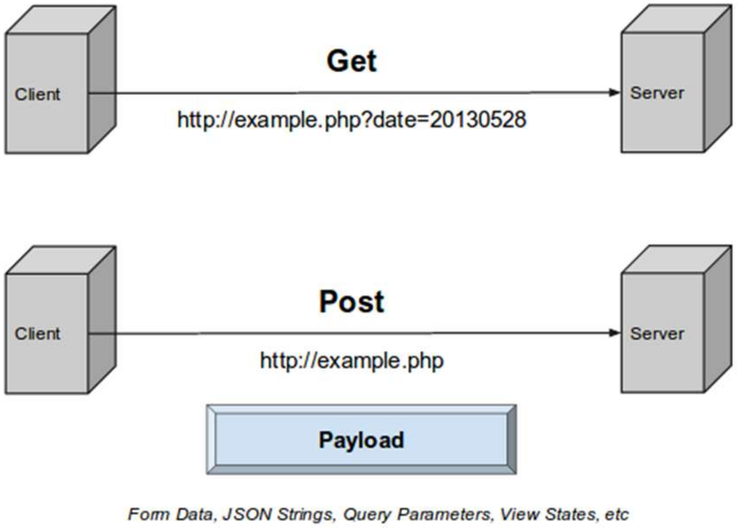
```
v User Datagram Protocol, Src Port: 52639, Dst Port: 53
    Source Port: 52639
    Destination Port: 53
    Length: 62
    Checksum: 0xa761 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  > [Timestamps]
v Domain Name System (query)
    Transaction ID: 0xd028
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v doc-10-ak-docs.googleusercontent.com: type A, class IN
```

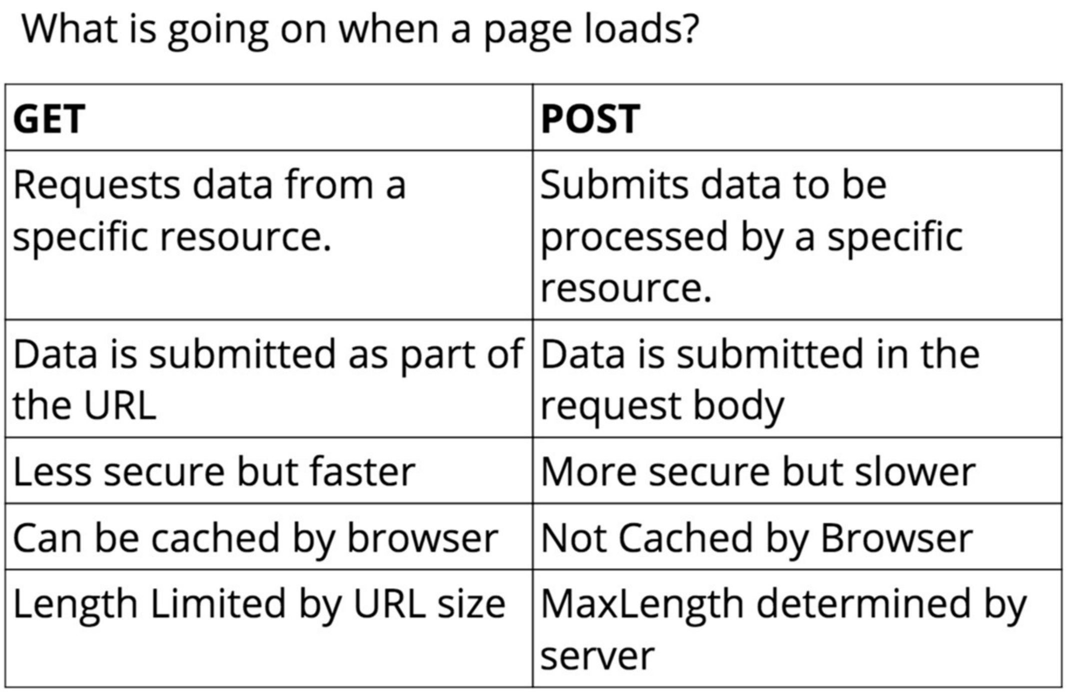
Dynamic DNS

- Dynamic DNS is pretty much DNS but constantly updating when the IP address updates
- It is designed to be the solution to home networks or businesses who's external ip is assigned through DHCP
- Can be used for bad: large scale attacks can use DDNS for flexibility purposes
    - A larger share of network attacks is using this method, and state actors use it a lot

HTTP Methods

- Common ones are GET requests but there are a whole list of operations
- What is GET & POST


Client
Get
Server
http://example.php?date=20130528
Client
Post
Server
http://example.php
Payload
Form Data, JSON Strings, Query Parameters, View States, etc


What is going on when a page loads?

GET	POST
Requests data from a specific resource.	Submits data to be processed by a specific resource.
Data is submitted as part of the URL	Data is submitted in the request body
Less secure but faster	More secure but slower
Can be cached by browser	Not Cached by Browser
Length Limited by URL size	MaxLength determined by server

Snort Signatures

- IDS uses signatures to detect potentially malicious network traffic
- Today, that is exactly what we will be doing: picture that an IDS set off an alarm and you have been called to investigate

Important Wireshark Features

- Can filter based on protocol (type in DNS or http)
- Can filter based on http method (http.request.method ==)
- Can filter based on ip addresses (ip.addr ==)
- Can filter based on port (tcp.port == udp.port==)
- Uses same Boolean logic as other programs (|| is or and is and)
- Can follow an entire network conversation in one view by right clicking on a packet and saying “follow tcp stream” or “follow HTTP stream”

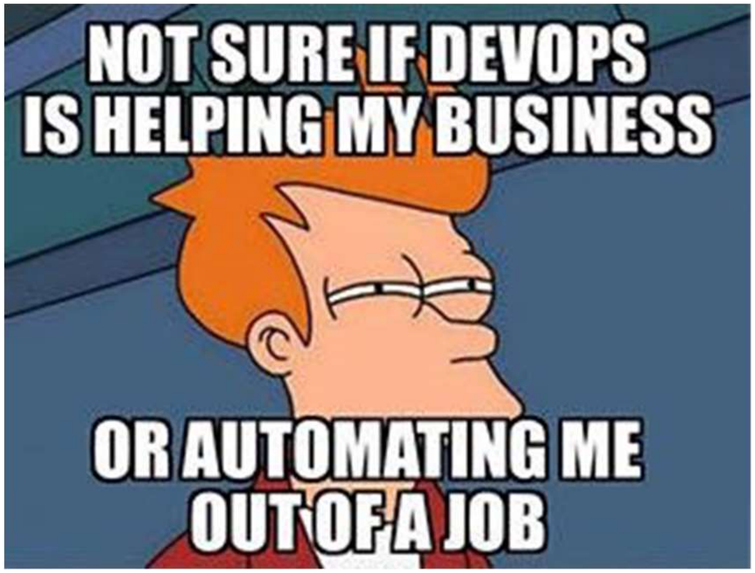
Hands On Time

- Boot up Wireshark and go to this link for hands on section:

https://tinyurl.com/CDONetworkForensics

Next Time... Terraform!

HashiCorp
Terraform



Add us on Social Media!

Twitter: **@ualbanyCDO**

Instagram: **ualbany_cdo**

Website: **uacyber.org**

Myinvolvement: **Cyber Defense Org**

We have a discord!