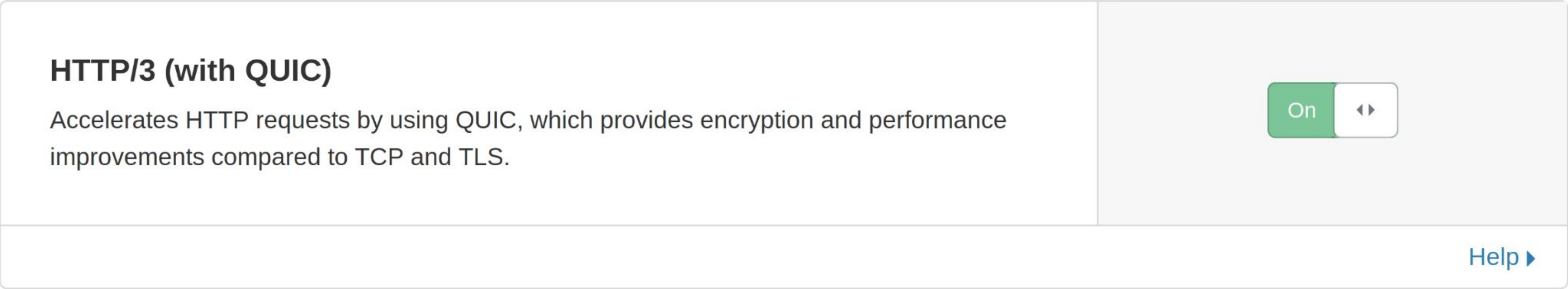
# Mason Competitive Cyber

## OSINT

# News since last meeting

- Yesterday was “Patch Tuesday” for Windows
  - Usual suspects--Flash Player, Remote Desktop Client, Office 365, Internet Explorer
  - Not as bad as it usually is, with only 59 vulnerabilities
  - IMO the most interesting one is a Remote Code Execution vulnerability in Azure
  - Occurs when Azure Stack fails to check the length of a buffer prior to copying memory to it
- HTTP/3 or QUIC is now an option in Cloudflare



**HTTP/3 (with QUIC)**

Accelerates HTTP requests by using QUIC, which provides encryption and performance improvements compared to TCP and TLS.

On

# Upcoming CTFs & Events

- MetaCTF@UVA  (Nov. 2)
- National Cyber League
- Patriot Hacks (Oct. 18-20)
- Scrubs meetup (TBD)

# OSINT - Overview

- OSINT (Open-source Intelligence)
  - Stalking
  - Offensive Recon
  - Determining exposure
  - IOCs
  - CTFs

# OSINT - Stalking

- Goal: Learn what you can about an individual and their whereabouts
  - Twitter, other social media
  - Whitepages
  - Exif data on pictures
  - IP geolocation
- Don’t dox people

# OSINT - Offensive Recon

- Builtwith
  - Lists what websites are built with
  - There are browser plugins which do the same thing
  - Moderately useful for discovering backend information
- Job Postings
  - If a company's job posting for their network administrator says "familiarity with Cisco ASR 1001 routers" then you can probably guess what router that company uses
- Sitemaps
  - XML sitemaps can be useful

# OSINT - Offensive Recon

- Shodan (Sentient Hyper-Optimised Data Access Network)
  - Search engine designed to map and gather information about internet-connected devices and systems
  - Look up IPs for vulnerable devices
- Exploit Database (www.exploit-db.com)
  - Exploit code already out there
- Previous password breaches
  - Pastebin

# OSINT - Defenders Intel

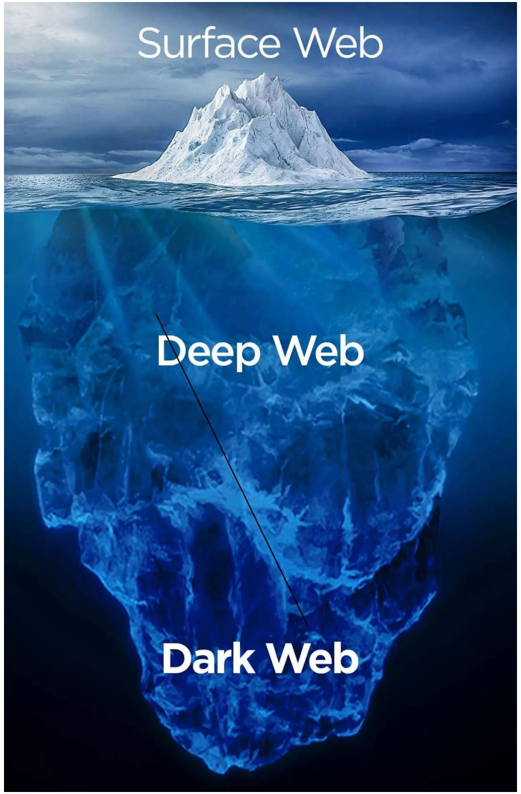
- VirusTotal
  - Search for malware in documents/websites
  - Find new/similar malware
  - Find other documents
- Haveibeenpwned
  - Made for defenders, but can be used offensively
  - Don’t reuse passwords!
- Google Dorks
  - Find sensitive documents that may have been exposed
  - Good for research in general

# OSINT - Defenders Intel

- Maltego
  - Massive library for visualizing OSINT and forensics
    - Comes with most Kali Linux downloads
    - Very powerful paid version
  - Network fingerprinting
    - Identify DNS servers, Mail servers, Name servers, etc
  - Find and analyzed emails
    - Search google, public gpg server, etc for emails
    - Identify emails that have been part of a breach (HIBP or Pastebin)

# OSINT - Defenders Intel

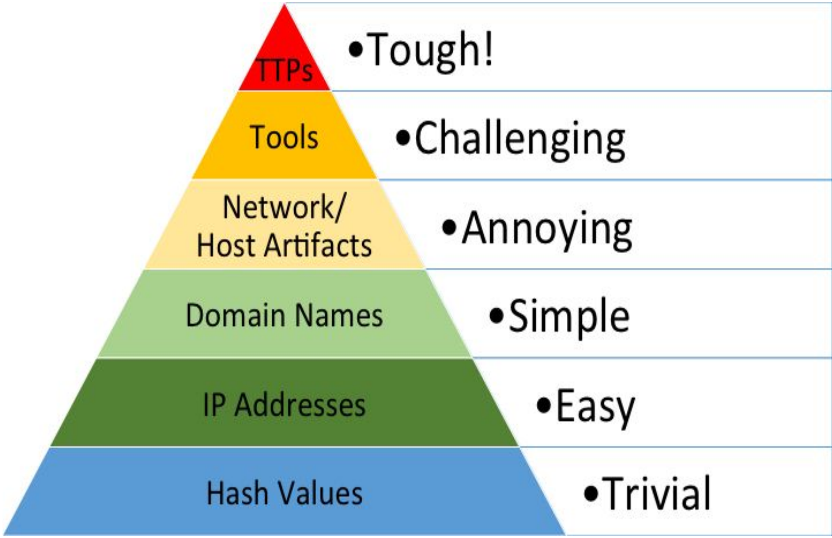
- Deep and dark web forums
  - Hackers have tutorials on the DDW
  - Popular RaaS offerings



# OSINT

- Data is not intelligence
  - Good intelligence is generally actionable
  - IOCs can be better or worse (see pyramid of pain)
- Tools
  - MISP
  - MITRE ATT&CK
  - Flashpoint Intelligence Platform

FLASHPOINT



TTPs •Tough!

Tools •Challenging

Network/ Host Artifacts •Annoying

Domain Names •Simple

IP Addresses •Easy

Hash Values •Trivial

# OSINT - Misc. CTF

- Github - API keys, pages, old commits, etc.
- The Wayback Machine (archive.org)
- Robots.txt
- Lots of Googling
- But mostly just twitter
  - I’ve found at least 3 flags on MetaCTF’s twitter

# Proud Sponsors

CACI

EVER VIGILANT

BATTELLE

It can be done™

CRYPSIS™