Mason Competitive Cyber

If Forensics and Crypto had a baby

Forensics in the real world

- Digital Forensics (branch of Forensic science)
  - Computer Forensics
  - Mobile Device Forensics
    - Diff = integrated communication system + proprietary storage systems
  - Network Forensics
  - Database Forensics
- Gather data, analyze data, investigate devices, recover data found in devices, etc.
- Incident Response / SOC analyst
- Often involved with the criminal justice system
  - Providing evidence for a trial
- Tools often used
  - EnCase - collection, analysis, & reporting
  - FTK (Forensic Toolkit) - file discovery and volume replication
  - Helix - non-destructive forensic analysis
  - Cracking tools - cracking encrypted media
  - Other proprietary tools I don't know about, probably

Forensics in the CTF world

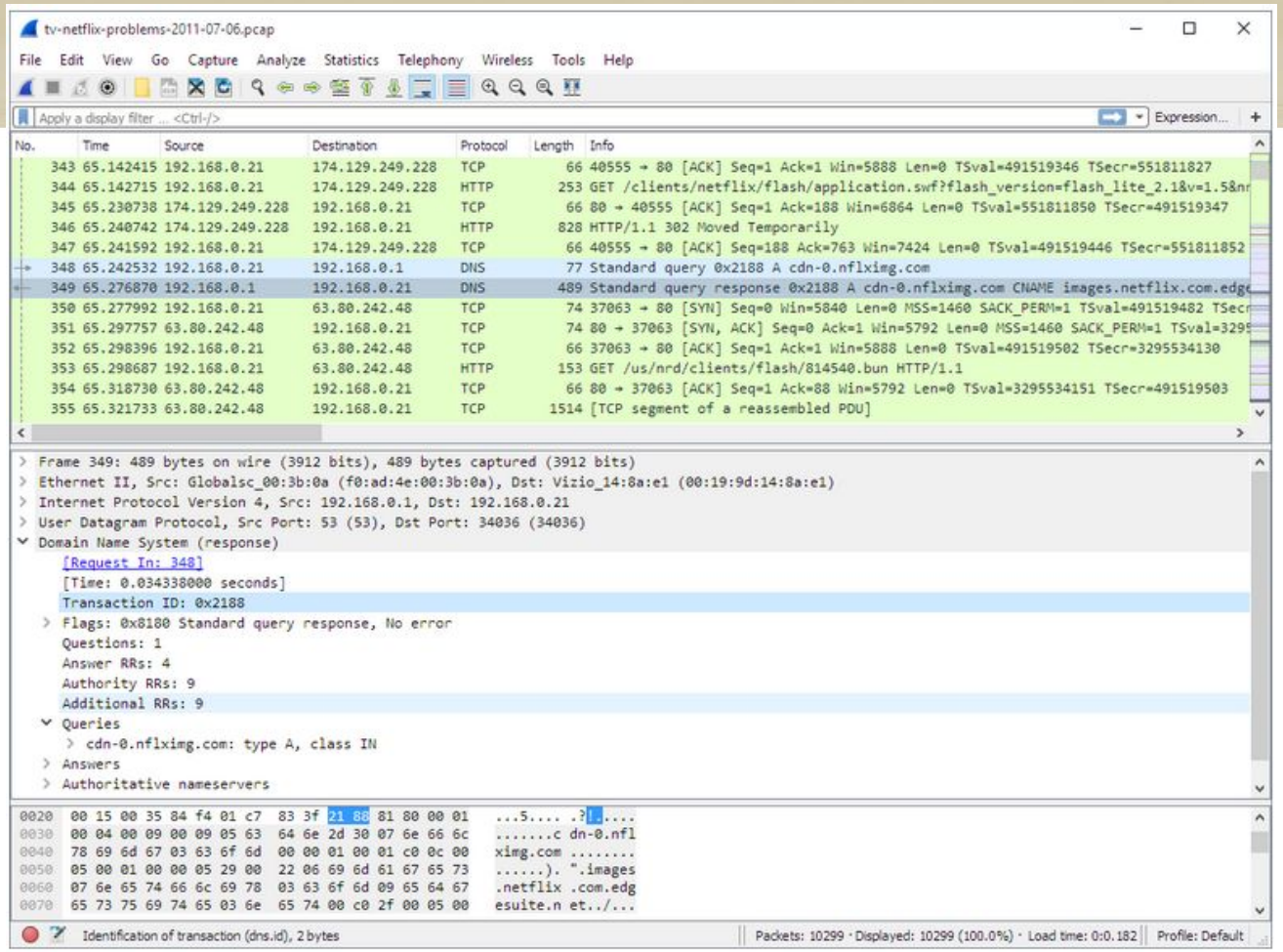
- Imbedded files
  - Extraction of files within other files
  - ***Iterative compression***
- Fixing files
  - Magic bytes, PNG chunking, file formats, etc
- Traffic/Packet analysis
  - PCAPs, PCAPs, PCAPs, and PCAPs
  - Chall could ask you just about anything about PCAPs
- ----------Warning: Baby making area ----------
- Steganography
  - Image or audio
    - LSB, changing color planes
    - spectrogram, mp3->morse
- Cracking
  - Tip: Reduce key space before brute forcing
  - Encrypted pdfs, hashes, plain passwords
  - WPA cracking from PCAPs

Forensics in the CTF world

- Imbedded files
  - Binwalk, foremost (scalpel), other tool you find on github, or manually
- Fixing files
  - Hex editors (Bless, Hexedit, HXd, etc)
  - Pngcheck
- Traffic/Packet analysis
  - Wireshark or tcpdump
- ----------Warning: Baby making area ----------
- Steganography
  - Stegsolve, zsteg, steghide, sonic visualizer, morse code audio decoder,
- Cracking
  - John the Ripper
  - Hashcat
  - Airmon-ng

Wireshark

- What is it and what is it used for?
  - Protocol analyzer
  - Analyzing protocols
  - Completely passive tools
    - No injection or packet manipulation
- What can you do with wireshark?
  - Capture live packet data from a network interface
  - Analyze said packet data
  - Gather information on potential attack
- How is it used in a CTF?
  - Often you will be given a .pcap file
  - It’s your job to sift through it efficiently to find various things
    - IOCs
    - Web page content
    - Files transmitted
    - Literally anything else


tv-netflix-problems-2011-07-06.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
343 65.142415 192.168.0.21 174.129.249.228 TCP 66 40555 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519346 TSecr=551811827
344 65.142715 192.168.0.21 174.129.249.228 HTTP 253 GET /clients/netflix/flash/application.swf?flash_version=flash_lite_2.1&v=1.5&nr
345 65.230738 174.129.249.228 192.168.0.21 TCP 66 80 → 40555 [ACK] Seq=1 Ack=188 Win=6864 Len=0 TSval=551811850 TSecr=491519347
346 65.240742 174.129.249.228 192.168.0.21 HTTP 828 HTTP/1.1 302 Moved Temporarily
347 65.241592 192.168.0.21 174.129.249.228 TCP 66 40555 → 80 [ACK] Seq=188 Ack=763 Win=7424 Len=0 TSval=491519446 TSecr=551811852
348 65.242532 192.168.0.21 192.168.0.1 DNS 77 Standard query 0x2188 A cdn-0.nflximg.com
349 65.276870 192.168.0.1 192.168.0.21 DNS 489 Standard query response 0x2188 A cdn-0.nflximg.com CNAME images.netflix.com.edge
350 65.277992 192.168.0.21 63.80.242.48 TCP 74 37063 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491519482 TSecr
351 65.297757 63.80.242.48 192.168.0.21 TCP 74 80 → 37063 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=3295
352 65.298396 192.168.0.21 63.80.242.48 TCP 66 37063 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519502 TSecr=3295534130
353 65.298687 192.168.0.21 63.80.242.48 HTTP 153 GET /us/nrd/clients/flash/814540.bun HTTP/1.1
354 65.318730 63.80.242.48 192.168.0.21 TCP 66 80 → 37063 [ACK] Seq=1 Ack=88 Win=5792 Len=0 TSval=3295534151 TSecr=491519503
355 65.321733 63.80.242.48 192.168.0.21 TCP 1514 [TCP segment of a reassembled PDU]
Frame 349: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)
Ethernet II, Src: Globalsc_00:3b:0a (f0:ad:4e:00:3b:0a), Dst: Vizio_14:8a:e1 (00:19:9d:14:8a:e1)
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.21
User Datagram Protocol, Src Port: 53 (53), Dst Port: 34036 (34036)
Domain Name System (response)
[Request In: 348]
[Time: 0.034338000 seconds]
Transaction ID: 0x2188
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 4
Authority RRs: 9
Additional RRs: 9
Queries
cdn-0.nflximg.com: type A, class IN
Answers
Authoritative nameservers
0020 00 15 00 35 84 f4 01 c7 83 3f 21 88 81 80 00 01 ...5.... .?!.....
0030 00 04 00 09 00 09 05 63 64 6e 2d 30 07 6e 66 6c ....c dn-0.nfl
0040 78 69 6d 67 03 63 6f 6d 00 00 01 00 01 c0 0c 00 ximg.com ....
0050 05 00 01 00 00 05 29 00 22 06 69 6d 61 67 65 73 ......). ".images
0060 07 6e 65 74 66 6c 69 78 03 63 6f 6d 09 65 64 67 .netflix .com.edg
0070 65 73 75 69 74 65 03 6e 65 74 00 c0 2f 00 05 00 esuite.n et../...
Identification of transaction (dns.id), 2 bytes
Packets: 10299 · Displayed: 10299 (100.0%) · Load time: 0:0.182
Profile: Default

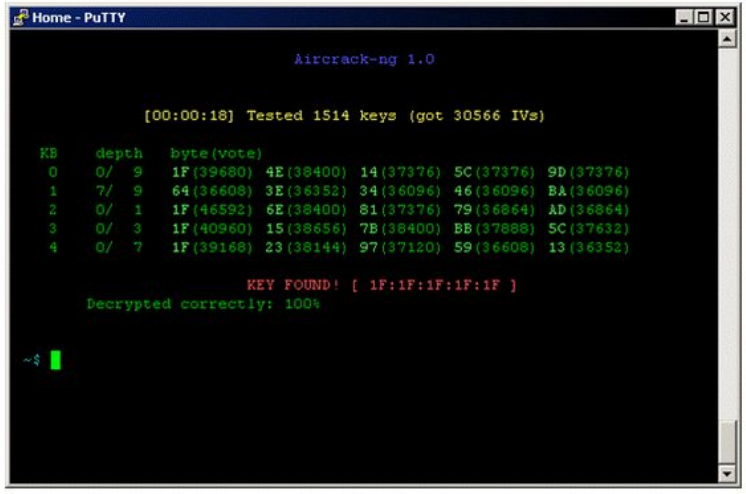
Cracking

- Scale is the only difference between real world cracking and CTF cracking
  - Single cpu vs a cluster of high-performing-specifically-built GPUs
- Identification
- Check other sources first
- Decrease key space is best as possible
- Compute how
- Sit back and hope

MD2 128 bits
MD4 128 bits
MD5 128 bits
MD6 Up to 512 bits
RIPEMD-128 128 bits
RIPEMD-160 160 bits
RIPEMD-320 320 bits
SHA-1 160 bits
SHA-224 224 bits
SHA-256 256 bits
SHA-384 384 bits
SHA-512 512 bits
SHA-3 (originally known as Keccak) arbitrary
Tiger 192 bits
Whirlpool 512 bits

HASHCAT

osophcrack



Proud Sponsors

Thank you to these organizations who give us their support:

BATTELLE

It can be done™

CACI

EVER VIGILANT

```
CH  9 ][ Elapsed: 4 s ][ 2007-03-24 16:58 ][ WPA handshake: 00:14:6C:7E:40:80

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID

00:14:6C:7E:40:80   39 100       51      116   14   9  54  WPA2 CCMP   PSK  teddy

BSSID              STATION            PWR  Lost  Packets  Probes

00:14:6C:7E:40:80  00:0F:B5:FD:FB:C2   35     0      116
```