Mason Competitive Cyber

Meeting 2: Wireshark, Metropolis, and Pico

Upcoming Events

- Metropolis
  - In-person beginner CTF and conference
  - Tomorrow 9AM-4PM at UMD
  - Need Kali VM
- Boston Key Party
  - Online CTF
  - Friday 2/24 8PM - Sunday 2/26 8PM
- Cryptoparty
  - In-person cryptography workshop at GMU
  - 2/25 9:30am-3:30pm in SUB I 3B
  - go.gmu.edu/cryptoparty

AlexCTF Easiest Forensics Problem

- **fore1.core** ← core dump = usually used for debugging of process that terminated unexpectedly
- strings fore1.core
- `cvqAeqacLtqazEigwiXobxrCrtuiTzahfFreqc{bnjrKwgk83kgd43j85ePgb_e_rwqr7fvbmHjklo3tews_hmkogooyf0vbnk0ii87Drfgh_nkiwutfb0ghk9ro987k5tfb_hjiouo087ptfcv}
- Flag format = ALEXCTF{}

AlexCTF Easiest Forensics Problem

- `cvqAeqacLtqazEigwiXobxrCrtuiTzahfFreqc{bnjrKwgk83kgd43j85ePgb_e_rwqr7fvbmHjklo3tews_hmkogooyf0vbnk0ii87Drfgh_n kiwutfb0ghk9ro987k5tfb_hjiouo087ptfcv}
- Flag format = ALEXCTF{}
- ALEXCTF{K33P_7H3_g00D_w0rk_up}

PicoCTF 2013

- If you haven’t competed in any CTF before, do PicoCTF 2013 during the meeting
- go.gmu.edu/pico

Wireshark

- Tool to capture and analyze network traffic
- Download it at wireshark.org
- Cloudshark, Tshark

- In real life-
  - Capture network traffic
  - Analyze network traffic

- In CTFs-
  - Given .pcap file
  - Analyze file

BSidesSF 2017

- go.gmu.edu/wireshark
- easycap.pcap

BSidesSF 2017

- go.gmu.edu/wireshark
- easycap.pcap

- Solution:
  - All TCP
  - Right click on a packet
  - Follow
  - TCP Stream

SecconCTF 2016

- go.gmu.edu/wireshark
- voip.pcap

SecconCTF 2016

- go.gmu.edu/wireshark
- voip.pcap

- Solution:
  - Telephony
  - VoIP calls
  - Play streams
  - Listen and write down flag

PoliCTF 2015

- go.gmu.edu/wireshark
- john-in-the-middle.pcap

- john-in-the-middle.tar.gz.gpg
- ^GPG key in folder, optional

PoliCTF 2015

- go.gmu.edu/wireshark
- john-in-the-middle.pcap

- Solution:
  - See many HTTP GET requests
  - File, Export Objects, HTTP
  - logo.png → steganography
  - Manipulate colors/brightness

AlexCTF 2017

- go.gmu.edu/wireshark
- fore2.pcap

AlexCTF 2017

- go.gmu.edu/wireshark
- fore2.pcap

- Solution:
  - It’s USB traffic, not network traffic
  - Sort packets by length
  - Recognize largest packet as containing PNG
  - File, Export Packet Bytes

Insomni’Hack 2017 - advanced problem

- go.gmu.edu/wireshark
- TheGreatEscape- *md5*.pcap

Insomni'Hack 2017 - advanced problem

- go.gmu.edu/wireshark
- TheGreatEscape- *md5*.pcap

- Solution:
  - Traffic: HTTP (web), FTP (files), SMTP (email), TLS (encrypted), OSCP (certificates)
  - Filter by FTP
  - See Bob logging in and sending ssc.key
  - Filter by FTP-data
  - Copy key to txt file
  - Filter by SSL, which HTTP server has flag?
  - Filter by SMTP, read email, realize that flag on 52.214.142.175

Insomni’Hack 2017 - advanced problem

- go.gmu.edu/wireshark
- TheGreatEscape- *md5*.pcap

- Solution:
  - Filter by SMTP, read email, realize that flag on 52.214.142.175
  - Wireshark, preferences, protocols, SSL, add the txt file with the private key as the RSA key
  - Now traffic is decrypted, filter by HTTP
  - Flag in header