Ethical Hacking 200

Assignment 5-2: Building Signatures and Packet Analysis

Contents

Ethical Hacking 200 1
Assignment 5-2: Building Signatures and Packet Analysis 1
Recap 1
Your Assignment: 1
What to turn in: 2
Im having a really hard time! 2

Recap

In class we covered what signatures are and built upon your fundamental networking knowledge. It's important to have a firm understanding of topics, a firm grasp of concepts, and not just recite/replay theoretical facts. Put the knowledge you have learned to practical use.

This will help you to answer questions that may pop up in your career such as

- Taking network traffic or protocols as an example – how would you make a signature?
- TCP is everywhere, but would you recognize it if you saw it?
- If you needed to build a protocol fuzzer, where would you even start?
- What is the purpose of bit flipping?
- Could you describe to someone what it is?
- Back to signatures…
    - Can you recognize what a signature is doing?
    - How would you describe what malicious traffic looks like at the packet/protocol level?

Your Assignment:

- **Practice reading RFCs**, https://tools.ietf.org/html/rfc793 will be needed here.
- **Part 1 – Scenario:**
  You have received a section of data pulled from the code of malware. It appears to be a list of hex strings? You know the surrounding code was creating sockets and there was other network related activity. Determine what, if any, potentially malicious activity might be going on in this section of data. (***hint:*** *there are 2 behaviors to be found, pay attention to patterns, once you identify a pattern it is easier to research what it is*)

```
(1) \x20\x01\x03\x28\xcb\xcd\x00\x00\x50\x06\xa7\xec\x22\x08\x0b\x03\x0c\x0a\x0a\x02
(2) \x40\x03\x00\x28\xcb\xcd\x03\x00\x50\x05\xa6\xec\x22\x08\x0b\x03\x1c\x0a\x0a\x02
```

(3) \x00\x50\x0D\x3D\xcb\xcd\x01\x00\x50\x01\xa1\xec\x22\x08\x0b\x03\x2c\x0a\x0a\x02
(4) \x00\x50\x0D\x3D\xcb\xcd\x01\x01\x50\x01\xa7\xec\x22\x08\x0b\x03\x3c\x0a\x0a\x02
(5) \x00\x50\x0D\x3D\xcb\xcd\x01\x02\x50\x03\xa4\xec\x22\x08\x0b\x03\x1c\x0a\x0a\x02
(6) \x00\x50\x0D\x3D\xcb\xcd\x01\x03\x50\x07\xa1\xec\x22\x08\x0b\x03\x5c\x0a\x0a\x02
(7) \x00\x50\x0D\x3D\xcb\xcd\x01\x04\x50\x08\xa3\xec\x22\x08\x0b\x03\x8c\x0a\x0a\x02
(8) \x00\x50\x0D\x3D\xcb\xcd\x01\x05\x50\x02\xa4\xec\x22\x08\x0b\x03\x1c\x0a\x0a\x02
(9) \x40\x02\x00\x28\xcb\xcd\x04\x00\x50\x04\xa2\xec\x22\x08\x0b\x03\x7c\x0a\x0a\x02
(10)\x40\x01\x01\x28\xcb\xcd\x08\x00\x50\x01\xa2\xec\x22\x08\x0b\x03\x5c\x0a\x0a\x02

- **Part 2 – Code:**
  In the code provided "send.py" what is line #37 doing?
  tcp_header += b'\x0b\x0d\x0a\x02'
  You must be able to describe what the purpose of hex/bit string is, in relation to the TCP header. What purpose, in relation to the TCP header structure, does each section play? (***hint:*** *as a example look at the comments of the lines before and after line #37, read the rfc and pay attention to sizes, if your comfortable play/experiment with the python scripts*)

What to turn in:

- Two answers
  - A description answering the questions in "part 1 – scenario". This should include what the observations/pattern is (what you noticed), and it should also include what the "attack" might be. This will take some work, but the answer does not have to be elaborate, a couple sentences will suffice.
  - A description, similar in format to the comments in the code, for what the hex/bytes/bits in line #37 do such as "#[source port (1-2) 16 bits][destination port (3-4) 16 bits]". This will take some thought, but naturally will be a short answer.

- Any reasonable text format is acceptable

Im having a really hard time!

As always, the best thing you can do is reach out as early as possible to the instructor.

Feel free to discuss in group chat, but please do not give out examples or answers. An appropriate level of information in group chat would be sharing information sources discovered (e.g: hey I found this nice explanation on what "bits" vs "bytes" are). However, you should NOT directly address answer in group chat (e.g: hey did you know "x0b" on line 37 means…). It should be up to each student to read, absorb information, and build up then apply their own practical skills to be able to do this on their own.