Exam 2 Review

Offensive Network Security
Florida State University
Spring 2014

When?

- Friday 02 May 2014
- 15:00 - 17:00
- Test material ~75 Minutes

What to Bring

- Pencil, I will not have any extras
- 8.5x11 Crib sheet
  - Any material (Ensure relevant to Exam)
  - Front & Back

Exam Content

- True / False
  - ~10 Questions
  - 1 point each
- Multiple choice
  - ~10 Questions
  - 2 points each
- Short Answer
  - ~5 Questions
  - Variable points per questions

Exam Content

- Ethernet Frame
- IP Packet
- TCP Packet
- UDP Packet
- Application Layer
  - Know that user protocols can exist in this layer
  - Unknown/known protocols
- Understand when to use network tools
  - Wireshark
  - nmap/nping
  - Scapy

Exam Content

- TCP Three-way Handshake
- TCP Termination Protocol
- What happens when an attacker spoofs an IP source address?
- What values does an attacker need to hijack a TCP session?
- What values does an attacker need to spoof/hijack a UDP session?
- HTTP Keywords, Request, Response
    - GET / HTTP/1.1\r\nhost:www.example.com\r\nuser-agent:....\r\n
    - HTTP/1.1 200 OK\r\nServer: nginx\r\n\r\n<content>
- Create a connection with a client after a DNS requests but server is down
- Big endian notation is only a *convention* for network protocols
    - Bytes on a wire
- How does traceroute work?

Exam Content

- Tracing library/system calls
  - ltrace, strace
  - The network library calls
  - How is a connection made, DNS executed, etc.
- Little endian, Big endian
  - Convert values: 4 bytes to int, 2 shorts, etc.
  - There is a difference between integer value when LE or BE
  - How does someone convert 4 bytes to an integer?
  - Test will deal with unsigned values
  - htons, ntohs, etc.
- Can we always trust payloads of *known* protocols?
  - Can we trust what Wireshark/tcpdump tells us?

Exam Content

- You will be given a series of messages, dissect fields
  - Fields can be little endian or big endian
  - Output will be given to help decode fields
- Given a piece of code, build a packet that takes advantage of the backdoor
  - Build packet in Scapy notation
  - Build packet in Raw Hex notation
- Parse Physical Layer + Network Layer + Transport Layer + App. Layer
  - Ethernet
  - IP
  - UDP/TCP
  - Unknown Protocol in Fields (Other layer fields might help out)
- Explain what is going on if provided a ltrace output

Exam Content

- What is a protocol, network protocol?
- Understand how to perform Needleman-Wunsch.
  - Might be given two strings and asked to perform algorithm
  - Does not have to be two ASCII strings
  - Show final result

Exam Content

- Remember ASCII
  - 0x0A = newline
  - 0x0D = carriage return
  - 0x20 = space
  - 0x2E = period (.)
  - 0x30 - 0x39 = digits
  - 0x41 - 0x5A = Uppercase letters
  - 0x61 - 0x7A = Lowercase letters

0x0d 0x0a

- Thank you for attending and participating in class
- I will set up some IRC remote help times
- I will be in my office all next week
- Best of luck on the exam