Exam 1 Review

Offensive Network Security
Florida State University
Spring 2014

When

- Thursday, 27 March 2014
- 15:35-16:50
- Can begin early iff everyone is in class
- Can go until 17:05

What to Bring

- Pencil, I will not have any extras
- 8.5x11 Crib (note) sheet
  - Allowed to have any material on it
  - Front and Back

Exam Content

- True / False
  - Normally around 10 questions
  - 1 point each
- Multiple choice
  - Normally around 10 questions
  - 2 points each
- Short answer
  - Normally around 5 questions
  - Points vary per question

Exam Content

- Ethernet frame
  - destination
  - source
  - type
- IP Packet
  - IP addresses
  - TTL
- TCP Packet
  - Ports
  - Flags
- UDP Packet
  - Ports
  - IP Addresses

Exam Content

- How are packets routed through a LAN?
  - Ethernet switches
  - End-nodes
- How can TCP be used to determine open ports?
  - How are the TCP flags used
  - How are the responses used to determine connected status
- TCP Three-way handshake
- ARP
- DNS Protocol
  - A Record
  - PTR Record
  - AAAA Record
  - NS Record

Exam Content

- Tools
  - tcpdump / Wireshark / tshark
  - nmap, nping, ncat
  - Scapy
  - Questions related to “how” to use a tool
- OSI Model or Hybrid Model: Physical, Link-Layer, Network, Transport, Application
- Think how ARP, TCP, ICMP protocols are used and abused
- Final question will be to dissect an Ethernet frame with payload.

Sample Questions

- What is the SYN flag?
- What protocol is used to determine domain-name mapping to IP mapping
- How can TTL be used to determine the path of routers?
- Bytes given for one protocol, convert to another protocol (IP -> ARP)
  - Use the bytes provided for fields in one protocol and use them in another protocol's fields