TDC 375 - Network Protocols

Bonus
Stage 1

- Link to http.pcap
- Dissect it with something like Wireshark
- See a HTTP GET for a specific page
- Going to that page would say “Go back one”
- Go to the “referer” in the HTTP GET request
Stage 2

- Enter BGP AS_TRANS value in web form
- Also have to set client source port to that value
- Various ways to do this, one way:
  - `curl --local-port 23456 http:/....`
Stage 3

• Decrypt PGP message
• Password is the number of RFC 1918 addrs
  • \((2^{24}) + (2^{20}) + (2^{16})\)
• Plain text is a SSH key pair
• Use that to login to a system
• Must use IPv6 to login
Stage 4

- DNS server is partially working
- Issue a DNS type TXT query to TCP DNS service
- You'll also need to do this over IPv6
Stage 5

- Say HELO to the SMTP daemon
- You have to impersonate that system in handshake
Stage 6

- Go forward / go back loop
- There is an immediate middle page with refresh
- In that middle page HTML is a clue
Stage 7

• Fill in form with L2 address given IPv6 SLAAC
Stage 8

• Using OSCAR (AOL IM / AIMP), IM tdciorc
Stage 9

- Use one of the tdc?? VM lab boxes
- Issue query for mrulist on ntp1.iorc.depaul.edu
- Find host who was talking using that source port