

LIS 385T.6 – 3.14.00

Information and Network Security

Issues & Questions

- Final Project – I'll decide by next week
- Crypt lecture deferred until next week
- Demo Classes –
 - Trinux Demo – April 4
 - Network Attack Demo – April 11

Active Defenses - Scanners

- What is it?
- What does/can it do?
- Types of Scanner
 - Host
 - Network
 - Web/Application
- Completeness (nothing catches everything)
- Timeliness (signature updates)
- Accuracy (false positives and false negatives)

Active Defenses – Password Crackers

- What is it?
- What does/can it do?
- Cracking versus guessing
 - Encrypting/decrypting passwords
 - Hashing/matching passwords
 - Collecting vs. storing passwords (out-of-band vs. real-time)
- Dictionary files
- The Randall Schwartz reference
- Commercial crackers

Active Defenses – Sniffers

- What is it?
- What does/can it do?
- Types
 - Keystroke
 - Packet
 - Protocols
- Dictionary files
- The Randall Schwartz reference

Active Defenses – Sniffers

- Detecting sniffers
 - Resource usage
 - MD5 Checksums
 - Sniffer “ sniffers”
- Defending against sniffer attacks
 - Compartmentalization
 - Encryption (SSH)

Supplemental Reading

- Review Chapters 6,7,9 in *Secrets and Lies*
- <http://www.rsasecurity.com/rsalabs/faq/> (RSA Crypto FAQ)
- <http://www.pcwebopedia.com> (cryptography & associated links)
- <http://www.avp.ch/avpve/> (AVP Virus Encyclopedia)
- <http://www.avp.ch/avpve/classes/malware.stm> (AVP entry for Trojan Horses)
- <http://www.attrition.org/security/denial/> (DoS Database)

Preparation for Next Week

Readings:

- Maximum Security*: Chapters 16,17,18
