

LIS 385T.6 – 3.07.00

Information and Network Security

Issues & Questions

- Final Project
- Demo Class

Passive Defenses - Firewalls

- What is it?
- What does/can it do?
- Types of Firewall
 - Packet Filter
 - Stateful Packet Filter
 - Proxy
- Speed and throughput
- Closed vs. open networks
- “fail open vs. fail closed”

Passive Defenses - Firewalls

- Appliance vs. application based FW
- Personal Firewalls
- “Demilitarized Zone” or DMZ concept
 - Packet Filter
 - Stateful Packet Filter
 - Proxy
- Products

Passive Defenses – Intrusion Detection Systems (IDS)

- What is it?
- What does/can it do?
- Types of IDS
 - Network based (NIDS)
 - Host based (HIDS)
 - Anomaly based (AIDS? Ouch.)
- Sensors and consoles, agents and signatures
- IDS monitoring and responses
- Products

Passive Defenses – Logging and Alarms

- What is it?
- What does/can it do?
- Types of logging and alarm solutions
 - Direct
 - Managed
- Syslog and centralized/protected logging
- Products

Topic Paper #3 – Passive Defenses

- This paper will be a review of the technologies and products discussed in Chapters 10, 12, and 13 of *Maximum Security*
- Choose one of the following focus areas:
 - Review one product from each technology group (one Firewall, one IDS system, and one Logging tool) – provide an detailed review of capabilities, limitations, system requirements, pricing, etc. Use established industry reviews as your basis.
 - Same as above, but comparing three products from any one category (only firewall and ids for this paper, no logging tools)
 - Technical paper on a passive technology – *only for the brave (I'll get an engineer to grade it so it better be deep...)*

Topic Paper #4 – Active Defenses

- This paper will be a review of the technologies and products discussed in Chapters 11, 14, and 15 of *Maximum Security*
- Choose one of the following focus areas:
 - Review one product from each technology group (one scanner, one password cracker, and one sniffer) – provide an detailed review of capabilities, limitations, system requirements, pricing, etc. Use established industry reviews as your basis.
 - Same as above, but comparing three products from any one category (scanner, cracker, or sniffer)
 - Technical paper on an active technology – *again graded by an engineer...*

Supplemental Reading

- <http://www.networkcomputing.com>

- <http://www.networkmagazine.com>

<http://www.pcwebopedia.com> (firewall, ids, and log)

- Product Guides in *Maximum Security* (both passive and active)

Preparation for Next Week

Spring Break – No Class

Readings for the following week:

- ***Maximum Security***: Chapters 11,14,15