

LIS 385T.6 – 2.14.00

Information and Network Security

Issues & Questions

•Next Week

Hackers and Crackers

- What's the difference?
- Reconnaissance
 - Social Engineering
- Scanners
 - Flags
 - “Noisy” scanning – full connection
 - “Stealth” scanning – FIN scan example

Hackers and Crackers

- OS Identification
 - Uses a sniffer
 - Looks for OS specific attributes
 - TTL example
 - Default packet size example
 - Doesn't connect, so it doesn't get logged

Hackers and Crackers

- Exploits
 - Exploits specific to OS, platform, protocol, and application
 - Bugtraq is the Bible of exploits
- Top Exploits
 - BIND
 - CGI programs
 - RPC, IIS, etc...

Hackers and Crackers

- Cracking
 - Levels of access, control, and damage
 - Threats
 - Crime
 - Espionage
 - Unstructured
 - Structured
 - External
 - Internal

Hackers and Crackers

- Critical Infrastructures
- Cyberwarfare
- Fraud and organized crime
- ID Theft
- Sources and targets

Supplemental Reading

- <http://www.insecure.org> (nmap scanner docs and exploit info)
- <http://www.sans.org/topten.htm> (The SANS Top Ten list)
- The Cuckoo's Egg by Cliff Stohl
(http://www.amazon.com/exec/obidos/ASIN/0743411463/qid=1013715293/sr=1-1/ref=sr_1_1/102-4801063-3432954)
- <http://www.iana.org/assignments/port-numbers> (another list of port numbers and associated services)
- <http://www.sans.org/alerts/SNMP.php> & <http://www.cert.org/advisories/CA-2002-03.html> (SNMP vulnerabilities)

Preparation for Next Week

Readings for the week:

- Maximum Security*: Chapters 7,8,9
