

LIS 385T.6 – 3.28.00

Information and Network Security

Issues & Questions

- Demo Classes –
 - Trinux Demo – April 4 – meet in IT Lab Annex
 - Network Attack Demo – April 11

Agenda

- Hour One – Final Project
- Hour Two – DDoS and Malware
- Hour Three - Cryptography

Final Project

- Scope – Critical Infrastructure Protection Portal
- Breakout
 - Policy and Background
 - Best Practices and Security Resources
 - Tools, Techniques, and Training
- Teams
 - Structure
 - Members

DoS and DDoS

Denial of Service and Distributed Denial of Service

- What is Denial of Service?
- DoS vs. DDoS
- The effects of DoS/DDoS
 - Bandwidth Consumption – fill the pipe (broadcast attack)
 - Resource Saturation – max out the system (syn floods)
 - System and Application Crash – break the box (Ping of Death)
- DDoS specifics – economies of scale, master/slave relationship

Malware (Viruses and Worms)

Viruses

- Work by attachment to a file or program (or other element such as VBScript in MS Office)
- Infection occurs when the program is executed or transferred
- In many cases the user does not have to activate the program themselves

Worms

- Work without attaching to a program (live in memory)
- Infection through self replication over a network

Malware (Viruses and Worms) cont.

Types of Viruses

- Boot Sector
- Parasitic (file)
- Multipartite
- Macro
- Script (often characterized as worms – take advantage of HTML scripting, but can affect other scripts as well)
- Memetic (virus hoaxes)

Trojans

- What is a Trojan?
 - Program that claims to do one thing (and actually may) but also does something unexpected (and perhaps malicious)
 - Trojans do not self-replicate. They require assistance to activate/propagate (tricking a user into opening a program or email, for instance)
- Types of Trojans:
 - Destructive (take some destructive action upon execution)
 - Privacy-invasive (system information or password stealing)
 - Back Doors (provide an access point to an application)

Trojans cont.

- Remote Access Tools (provides a remote access server to a client elsewhere)
- Droppers (trojan installs a virus into a system)
- Jokes (take some “amusing” action)
- Logic Bombs (malicious programs that function on a timer or according to some preset rules – e.g. the network admin gets fired)
- Rootkits (set of trojanized programs installed by an attacker)
- DDoS agents (programs designed to facilitate DDoS attack)
- Worms (arguable)

Cryptography

- Introduction
- Encryption/Decryption
- Digital Signatures
- Digital Certificates
- Public Key Infrastructures

Cryptography

- Symmetric Key Cryptography
- Public Key Cryptography
 - Secure Symmetric Key Exchange
- Hashing
- Algorithms
 - All about math
 - DES and Triple DES
 - Diffie Helman protocol
 - MD5 (hash algorithm)
- Keys and Key Length

Supplemental Reading

Read:

<http://trinux.sourceforge.net/faq/>

Nmap: http://www.insecure.org/nmap/nmap_manpage.html

Dsniff: <http://www.monkey.org/~dugsong/dsniff/>

Tcpdump : <http://www.rt.com/man/tcpdump.1.html>

<http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/index.shtml>
(PIX 506 doc)

Guidance – Topic Paper 5

Prepare an analysis of one of the following topics:

- Compare and Contrast security between Linux/Unix and Windows operating systems
- Describe and analyze one of the following crypto products/technologies:
 - Public Key Infrastructures
 - PGP
 - The Data Encryption Standard (DES)
- Describe methods and techniques for secure application and code development

Guidance – Topic Paper 6

Prepare an analysis of one of the following topics:

- Computer Security Best Practices and Standards (ISO/BS 17799, NIST SP 800-14, etc.)
- Current privacy regulations (EU Privacy Directive of 1995, Health Information Portability and Accountability Act of 1996 (HIPAA) and associated regulations, Gramm Leach Bliley Act (GLBA), etc.)
- Cryptographic Policies (Export Restrictions, Key Escrow, etc)
- Critical Infrastructure Assurance Policies and Organizations

Preparation for Next Week

Readings:

- Maximum Security*: Chapters 19-24 (high level)
