1ST Class – Tuesday morning, January 6, 2015

Instructor: Bill Reed (First Two-Weeks)

Instructor: Andre Martinez – [amartinez@coleman.edu](mailto:amartinez@coleman.edu)

Midterm – 4th week not the 5th week.

Chapter 1

Some intruders are smarter than you.

Many intruders are unpredictable.

Prevention will eventually fail.

97% of companies are hacked. 48, 229,

Popeyedsws – you can buy stolen credit card info

All passwords can be guessed, eventually.

You can buy or lease botnets

Patches to software will fix or enhance the product

– Typically, there are 15-50 software bugs/1000 lines of code. 5-15 bugs are exploitable.

Cyber Threat Map – [www.fireeye.com/cyber-map/threat-map.html](http://www.fireeye.com/cyber-map/threat-map.html)

Metasploit (<http://download.cnet.com/Metasploit/3000-2653_4-75289381.html>) – Armorage – Hail Mary

Script Kiddie is most dangerous.

“Anonymous” – Hacktivists

Steps of a network attack:

1. Reconnaissance – Gather information

2. Scanning, enumeration (probing) OS detection.

3. Vulnerability assessment/scanning

4. Penetration (Testing)

5. Create a Backdoor to get back in.

6. Harden your system (patch known vulnerabilities) so no one else can get in.

‘Banner Grabbing’ accesses using Telnet, which tells too much info about your CPU brand, OS, etc.

Chapter 2

Malicious Software:

Viruses – Spreads by a vector (human) Appender,

Worms – Travels on its own

Trojans – Disguised payload

Spyware

Rootkits – Most evil of all, others you can defend against or get rid of, but not rootkits. You can only reformat the drive.

There are kernel rootkits and application rootkits. They intercept system calls and do something else with them.

Products to detect a Rootkit, e.g. CheckRootkit, RootkitRevealer.

Adware

Bots – Computers are used as ‘Botnets’ zombies, which are deployed by a worm, to inflict a DoS from saturation of many PCs.

I.e. Lizard Squad affected Xbox and PlayStation on Christmas.

You can lease a botnet.

TOR – Technology to allow browsing anonymously, e.g. In Firefox and IE you can select the option browse privately.

Logic Bomb – Code lies dormant waiting for something to trigger it, i.e. a date.

Backdoor – Typically deployed by Trojans. To get into your systems.

Keyloggers – Records keystrokes.

Microsoft Office products can be exploited by VB script for macros.

PDF and RTF products can be exploited by JavaScript in forms.

BluffMyCall – To change your CallerID, to bypass call-waiting and go to voicemail, to disguise your voice; about $1/minute.

Google – Dell Phishing Quiz

Scraped websites – you enter your username and password.

Buy the domain name that is similar. There is a paragraph that contains misspelled words.

Homework: From the Syllabus, not Webclass.

- Writing assignment: Small Business

- End of chapter review questions,

- Lab manual exercise (no points-not mandatory).

Quiz (handed out) next week on Chapters 1 and 2.

2ND Class – Tuesday morning, January 13, 2015

Instructor: Bill Reed (First Two-Weeks)