

INTRO TO ETHICAL HACKING
MIS 5211.001
Week 8

1

Tonight's Plan

- ❑ Encryption
- ❑ Encoding
- ❑ Malware
- ❑ Next Week

MIS 5212.001 2

2

Encryption (Short Version)

- ❑ Couple of points up front
 - Real "Standards based" encryption is hard to break 😞
 - Proprietary encryption is usually not as hard to break 😊
 - When encryption is broken, it is usually the implementation, not the cypher suite that is broken
 - Example: WEP and RC4
 - Regardless of encryption, the computer must decrypt the data to act on it. Therefore, clear text data is in memory
 - Also true of browsers, browser must decrypt to act

MIS 5211.001 3

3

Encryption (Short Version)

- ❑ One exception to clear text in memory
- ❑ Homomorphic Encryption
 - Computations carried out on ciphertext
 - Result is also encrypted
- ❑ Problem:
 - Very resource intensive
 - Not fast enough for practical use (yet)

MIS 5211.001 4

4



Terms

- ❑ Algorithm - Mathematical rules used to encrypt and decrypt
- ❑ Ciphertext - The encrypted data
- ❑ Encipher - Encrypting
- ❑ Decipher - Decrypting
- ❑ Key - Sequence of bits and instruction that governs encryption and decryption
- ❑ Plaintext - Unencrypted data

MIS 5211.001 5

5

Symmetric vs Asymmetric

- ❑ **Symmetric - Both parties use the same key** 
 - Anyone with a key can encrypt and decrypt
 - Relatively fast, less intensive to use
- ❑ **Asymmetric - Keys linked mathematically, but cannot be derived from each other** 
 - What one key encrypts, the other key decrypts
 - Works both ways
 - Also known as a key pair and associated with PKI or public key encryption
 - Relatively slow, resource intensive

MIS 5211.001 6

6

Stream and Block Ciphers

- ❑ Block Ciphers
 - Data is broken in to blocks
 - Blocks are encrypted/decrypted individually
- ❑ Stream Cipher
 - Message is not broken up
 - Encrypted/decrypted one bit at a time

MIS 5211.001 7

7

Types of Symmetric Systems

- ❑ DES
- ❑ 3DES
- ❑ AES or Advanced Encryption Standard
- ❑ Blowfish

MIS 5211.001 8

8

Types of Asymmetric Ciphers

- ❑ RC4
- ❑ RSA
- ❑ El Gamal
- ❑ ECC or Elliptic Curve Cryptosystems

MIS 5211.001 9

9

Public Key Encryption

- ❑ A “Hybrid” encryption method
- ❑ Symmetric key is used to perform bulk encryption/decryption of data
- ❑ Asymmetric keys are used to pass the symmetric key securely

MIS 5211.001 10

10

Session Keys

- ❑ Basically, just a secret key that is only used for one session between users (or systems) and is then disposed of.

MIS 5211.001 11

11

Public Key Infrastructure (PKI)

- ❑ Comprehensive process including:
 - Programs
 - Data formats
 - Procedures
 - Protocols
 - Policies
 - Mechanisms
- ❑ All working together to secure communications

MIS 5211.001 12

12

Certificate Authority


- ❑ Certificate Authority (CA)
 - Issues public keys
 - Verifies you are who you say you are and provides certificate to prove it that can only come from a secret key you possess
- ❑ Registration Authority (RA)
 - Performs registration activities for a CA

MIS 5211.001 13

13

One Way Function or Hashing

- ❑ Provides for message integrity
- ❑ Mathematical value calculated from data that cannot be reversed
 - Sender and receiver can both calculate the value and verify that the data sent is the data received



MIS 5211.001 14

14

Digital Signature

- ❑ Encrypted hash value
 - Data sent is data received
 - Data can only have come from someone with the appropriate key(s)

Encrypted	Confidentiality
Hashed	Integrity
Digitally signed	Authentication and Integrity
Encrypted and Digitally Signed	Confidentiality, Authentication, and Integrity

- Reference: CISSP Certification, Shon Harris

MIS 5211.001 15

15

The Unbreakable Code

- ❑ Only one cipher is truly unbreakable
- ❑ One-Time Pad
 - Each pad is only used once
 - Pad is XORd against cleartext data
 - Ciphertext is XORd against pad at receiver
- ❑ Generally, not used due to difficulty in distributing non-recurring pads

MIS 5211.001 16

16

Rules for Key Management

- ❑ Longer keys are better
- ❑ Keys need to be protected
- ❑ Keys should be extremely random and use full spectrum of key space
- ❑ Keys should not be re-used

MIS 5211.001 17

17

Encoding

- ❑ Encoding is **NOT** encrypting
- ❑ Perfect example: Base64 encoding
 - Well known
 - Reversible
 - Provide limited obfuscation
- ❑ Other examples
 - Morse code
 - ASCII
 - UTF-8, 16, 32
 - EBCDIC
 - Unicode

MIS 5211.001 18

18

Why we care about Encoding

- ❑ Often used incorrectly as a substitute for encryption
- ❑ Some "proprietary" encryption systems were nothing more than Base64 or Base64 with character substitution
 - Even if you don't recognize the encoding it is easily "cracked" with frequency analysis

MIS 5211.001 19

19


Encoding and Web Attacks

- ❑ We will see this again when we cover Web applications and intercepting proxies
 - Base64 encoding is often used as an obfuscation technique

MIS 5211.001 20

20

Blockchain



- ❑ Distributed Ledger
 - All parties have a copy
 - Data can be added and is replicated across all copies
 - Data cannot be modified or deleted (so far)
- ❑ Benefits
 - Distributed
 - Lower transaction costs
 - Faster transaction times
 - Transparency & accountability & integrity
 - Usage information and traceability
 - Data security through encryption

MIS 5211.001 21

21

Online Resources

- ❑ Resource for basic hacking
- ❑ <https://tryhackme.com/>

- ❑ Training Environment for Coding
- ❑ <https://www.hackerrank.com/>

- ❑ Online IDE
- ❑ <https://repl.it/~>

MIS 5211.001 22

22

- ❑ Linked In Learning Reference
- ❑ <https://www.linkedin.com/learning/learning-kali-linux-2016/welcome?u=2206009>
- ❑ <https://www.linkedin.com/learning/penetration-testing-advanced-kali-linux/welcome-2?u=2206009>
- ❑ HTB instructions are in the Exercise Files

MIS 5211.001 23

23

Malware

- ❑ Code used to perform malicious action

Or

- ❑ Malware is a set of instructions that run on your computer and make your system do something that an attacker wants it to do.

MIS 5211.001 24

24

What it is used for

- ❑ Steal personal information
 - Credentials
 - Credit Card Numbers
 - Whole Identities
- ❑ Ransom files
- ❑ Delete files
- ❑ Click fraud
- ❑ Use your computer as relay
- ❑ Logic bombs

MIS 5211.001 25

25

Forms

- ❑ Static (My words)
- ❑ Polymorphic : uses a polymorphic engine to mutate while keeping the original algorithm intact (packer)
- ❑ Metamorphic : Change after each infection

MIS 5211.001 26

26

Kaspersky Malware Classification Tree

MIS 5211.001 27

27

Some Definitions

- ❑ Payload - harmful things the malicious program does, after it has had time to spread.
- ❑ Worm - a program that replicates itself across the network (usually riding on email messages or attached documents (e.g., macro viruses).
- ❑ Trojan Horse - instructions in an otherwise good program that cause bad things to happen (sending your data or password to an attacker over the net).
- ❑ Logic Bomb - malicious code that activates on an event (e.g., date).
- ❑ Trap Door (or Back Door) - undocumented entry point written into code for debugging that can allow unwanted users.

MIS 5211.001 28

28

Shellcode

- ❑ You will see the term Shellcode used intermittently throughout the presentation
- ❑ Shellcode is defined as a set of instructions injected and then executed by an exploit program - The Shellcoder's Handbook 2nd Edition
- ❑ Derived from the original purpose of the software to create a "Shell" at the root level

MIS 5211.001 29

29

What is a Shell

- ❑ **First, a shell is not a terminal**
 - For the mathematically inclined
 - Shell != Terminal
- ❑ What this means
 - Not all terminal commands will work in a shell
 - For instance:
 - ❑ Clear for clear screen
 - ❑ Turn Echo On or Off
 - ❑ CTRL-C
 - ❑ CTRL-D
 - ❑ Etc...

MIS 5211.001 30

30

More on Shell

- ❑ Terminals include code and protection to interpret user input, and ensure everything works
- ❑ A shell is a raw command line to send characters to and receive characters from a system. That is, raw stdin and stdout. That's it. It cannot interpret or catch control codes or screen commands

MIS 5211.001 31

31

Technical Types

- ❑ User Mode Root Kits
- ❑ Kernel Mode Root Kits
- ❑ Keyloggers
- ❑ Sniffers
- ❑ Downloaders
- ❑ HTTP C2 Channels

MIS 5211.001 32

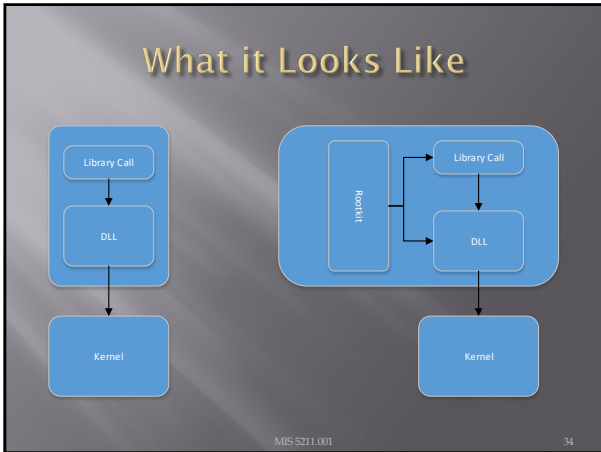
32

User Mode Root Kits

- ❑ Purpose
 - Attain access
 - Maintain access
 - Hide access
- ❑ Operates in user mode
 - That is, gets injected into one or more individual processes

MIS 5211.001 33

33



34

- ### What is Happening
- ❑ Rootkit intercepts data to:
 - Netstat
 - Process Explorer
 - Task Manager
 - ❑ Therefore, when a user or admin looks at these tools everything looks normal
- MIS 5211.001 35

35

- ### Two Key Infection Steps
- ❑ DLL Injection (Dynamic Link Library)
 - Running code within the address space of another process
 - Malware "Injects" itself into a DLL using
 - SetWindowsHookEx
 - CreateRemoteThread/LoadLibrary
 - Note: These are legitimate commands that are used by software for things like patching
 - ❑ API Hooking (Application Programming Interface)
 - Intercepting function calls, messages, or events passed between software components
- MIS 5211.001 36

36

Notes on Rootkits

- ❑ These methods were developed in Windows XP and earlier machines
- ❑ Still possible with Vista, 7, 8, and 10 - Just need to work a little harder

MIS 5211.001 37

37

Kernel Mode Rootkits


- ❑ Injected into the Kernel, below the level of process and DLL
- ❑ Runs at the highest privilege level for software
- ❑ Removal likely requires reinstallation of operating system

MIS 5211.001 38

38

Keyloggers

- ❑ Monitor user key strokes
- ❑ Lots of bots, worms, and assorted other malware does this
 - Sends logs to attacker
- ❑ Common methods
 - Hook for keyboard events
 - Poll keyboard state with GetAsyncKey()



MIS 5211.001 39

39

Sniffers

- ❑ Similar to tcpdump or windump covered earlier, but now its malicious
- ❑ Common method
 - Put interface into promiscuous mode
 - Controller passes all traffic it receives to the CPU
- ❑ Other ways
 - Intercept network related calls
 - Intercept higher level functions
 - We'll see this late with Browser proxies
 - Installing BHOs (Browser Helper Objects)

MIS 5211.001 40

40

Downloaders

- ❑ Used by attackers to deliver malware in stages
- ❑ Initial malware can be very small, only needs to fetch the next piece of software
 - Easier to obfuscate
 - May escape detection
 - Action is not malicious in and by itself
- ❑ Droppers are similar, but embedded the downloaded functionality in their own code

MIS 5211.001 41

41

Example Commands

- ❑ URLDownloadToFile()
 - Download and save file to disk
- ❑ ShellExecute()
 - Execute file
- ❑ WinExec()
 - Execute file

MIS 5211.001 42

42

Command and Control Channels

- ❑ AKA HTTP C2 Channels
 - Ubiquitous
 - Port 80 almost always open
 - Use port 443 and your coms are encrypted
- ❑ Alternatives
 - IRC (Internet Relay Chat)
 - P2P (File Sharing)
 - DNS (Tunnel data over DNS)

MIS 5211.001 43

43

Approaches

- ❑ Reverse shell over HTTP (Port 80)
- ❑ Embedded in regular HTTP traffic
 - Disguised like normal user traffic

MIS 5211.001 44

44

Infection Channels

- ❑ MS Office Files
- ❑ PDF Files
- ❑ Flash
- ❑ JavaScript

- ❑ Lots more, but these are the ones we will talk about

MIS 5211.001 45

45

MS Office Files

- Why Office
 - Everybody is using it
 - File freely passed around and not unexpected
 - Parsing binary office format is difficult
 - Robust embedded scripting language (VBA)
 - You can even hook Apple products



Source for Graphic:
<https://www.microsoft.com/en-us/office/officeapps.aspx>
<https://www.microsoft.com/en-us/office/officeapps.aspx>
<https://www.microsoft.com/en-us/office/officeapps.aspx>

MIS 5211.001 46

46

Techniques

- Embedded Shellcode
 - Exploits vulnerability in office software
 - No user interaction required
- Embedded VBA Script
 - Executes on document open
 - May require user to click OK or "Enable Content"

Note about VBA – Term Macro is misleading. Implies it is for basic scripting. Today, VBA is a full fledged language.

MIS 5211.001 47

47

Adobe PDF

- Why PDF
 - Everybody is using it
 - Files freely passed around and not unexpected
 - PDF Format
 - Proprietary (ish)
 - Used to be proprietary, published by ISO as ISO/IEC 32000-1:2008
 - Feature rich
 - Can include active content
 - JavaScript
 - ActionScript via Flash Objects
 - And finally
 - New vulnerabilities found regularly

MIS 5211.001 48

48

More Adobe PDF

- ❑ High profile attack target
 - <http://www.darkreading.com/vulnerabilities--threats/report-sixty-percent-of-users-are-running-unpatched-versions-of-adobe/d/d-id/1136022>
 - 6 in 10 installs of Adobe Reader are out of date
- ❑ Complex structure
 - Easily obfuscated
 - Need software tools to open and understand
 - Even AV vendors have problems keeping an eye on this

MIS 5211.001 49

49


Where are the Vulnerabilities

- ❑ Parser components
- ❑ JavaScript and ActionScript
- ❑ Embedded Shellcode executes by exploiting these vulnerabilities

MIS 5211.001 50

50

Flash



- ❑ (was) Ubiquitous on websites
- ❑ Frequent (weekly) new vulnerabilities
- ❑ So bad Apple and now Kindle will not allow flash to be installed without jail breaking the devices
- ❑ Adobe took action:
 - End of Support, No Updates, as of December 31, '20.
 - Activated "kill" switch in recent updates on January 12, '21.

MIS 5211.001 51

51

More Flash

- ❑ Uses the SWF file format
- ❑ See:
<https://www.adobe.com/content/dam/acom/en/devnet/pdf/swf-file-format-spec.pdf>
- ❑ Supports ActionScript language for scripting, including legacy support for older versions of ActionScript

MIS 5211.001 52

52

Flash Vulnerabilities

- ❑ Client Side
 - Flash Parameter Injection
 - Inject parameters when Flash object is embedded in an HTML page
 - Cross Domain Privilege Escalation
 - Access and modify DOM
 - Cross Site Scripting
 - Access and modify DOM
 - Cross Site Flashing
 - Call another flash object from flash

MIS 5211.001 53

53

JavaScript

- ❑ Just a teaser at this point
- ❑ JavaScript is a primary infection path with web site based attacks
 - Used for:
 - Cross Site Scripting (XSS)
 - Cross Site Request Forgery (CSRF)
 - Direct Delivery
 - Downloaders
 - Droppers
 - Keyloggers
 - And anything else you want

MIS 5211.001 54

54

More JavaScript

- ❑ JavaScript based attacks are frequently heavily obfuscated with multiple layers of encryption, obfuscation, encoding, and false flags
- ❑ Attackers will “buy” ad space and put up legitimate looking ads on legitimate sites
 - Since adds are rotated, infection is inconsistent and difficult to pin down

MIS 5211.001 55

55

Testing AV

- ❑ During Penetration Tests a tester may be asked to verify that the AV suite is working
- ❑ You don't want to send malware
- ❑ What do you do?
- ❑ Answer
 - EICAR
 - <http://www.eicar.org/86-0-Intended-use.html>

MIS 5211.001 56

56

EICAR

- ❑ EICAR is a Anti-Malware Test File
- ❑ Originally developed by Paul Ducklin
- ❑ All major AV vendors will flag this file if properly installed and configure
- ❑ Tester can simply send the file in via normal channel being tested and then confirm that AV suites correctly identified and blocked file.
- ❑ X5O!P%@AP[4\PZX54(P^7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H*

MIS 5211.001 57

57

Odds and Ends

- ❑ I'm malware, where do I hide
 - Inside other executables
 - Inside data files
 - In Alternate Data Streams (ADS)
 - On the hard drive, but outside of the file system
 - In BIOS

MIS 5211.001 58

58

Detection

- ❑ Malware in executables and data files can be detected if you know what good is supposed to look like
- ❑ Malware also leaves markers in the file system that can be detected
- ❑ Commercial tools like Mandiant, FireEye, and others can pick these up
 - Worth noting: FireEye bought Mandiant

MIS 5211.001 59

59

Alternate Data Stream (ADS)

- ❑ Compatibility feature of NTFS
 - Part of file system, but not part of file system
 - Originally created to allow NTFS to handle Apple file attributes that were stored outside of the file structure
 - Creates an "Off Book" location to store data and/or executables that will not be seen via file commands or through GUI folder tools
 - http://www.windowsecurity.com/articles-tutorials/windows_os_security/Alternate_Data_Streams.html

MIS 5211.001 60

60

Hard Drive

- ❑ Not all space on the drive is consumed by the file system
- ❑ Vendors sometime use this space to keep configuration information or recovery files
- ❑ Attackers can use the space as well
- ❑ Caution: While tools exist to read and write to raw space, writing is extremely dangerous as you can render the file system useless.

MIS 5211.001 61

61

BIOS

- ❑ Firmware installed on motherboard that instructs CPU how to turn on
 - What drive to boot from
 - Is there a password to just turn on
- ❑ Other hardware has similar Firmware
 - Graphics Cards
 - Network Cards
 - Other specialty boards

MIS 5211.001 62

62

What is Firmware

- ❑ Firmware is rewritable code in a chip or other piece of hardware that retains it's coding even without power
- ❑ It only changes when specific external commands are given to update or overwrite

MIS 5211.001 63

63

Impact of BIOS Malware

- ❑ Malware can withstand a complete re-image of the file system
- ❑ Replacing the hard drive will not mitigate
- ❑ Since it is in place a boot time, before the kernel ever starts, it can re-infect

MIS 5211.001 64

64

Next Week

- ❑ We will be covering
 - OWASP top 10
 - Web Application Hacking
 - Intercepting Proxies
 - URL Editing

MIS 5211.001 65

65

Questions

?

MIS 5211.001 66

66
