Types of Attacks and Malicious Software

Chapter 6

News

- https://www.ic3.gov/ - Industry Alerts
- https://www.welivesecurity.com/en/eset-research/lazarus-luring-employees-trojanized-coding-challenges-case-spanish-aerospace-company/

Module 5 Labs Review

- Pass-Crack lab
  - The longer the password, the longer cracking takes
  - Salts don't typically add much to cracking time
    - If the cracking program knows that salts are added to the beginning of the password, it will do the same before hashing and looking for a match. It may take a few iterations to add at beginning, end middle, etc.
    - It does increase the size of the input to the hash algorithm, making it more difficult to match
- ACL lab
  - Default ACLs – some did multiple attempts and ended up with something that seemed to work.
  - Script – Alice does not have default access to bob directory. If your default ACL works, you could write to Alice directory for Bob access
    - No ACL required in the script

Classification of Malware

Classified into two broad categories:

- Based first on how it spreads or propagates to reach the desired targets
- Then on the actions or payloads it performs once a target is reached

Also classified by:

- Those that need a host program (parasitic code such as viruses)
- Those that are independent, self-contained programs (worms, trojans, and bots)
- Malware that does not replicate (trojans and spam e-mail)
- Malware that does replicate (viruses and worms)

Propagation Mechanisms

- Infection of existing content by viruses that is subsequently spread to other systems
- Exploit of software vulnerabilities by worms or drive-by-downloads to allow the malware to replicate
- Social engineering attacks that convince users to bypass security mechanisms to install Trojans or to respond to phishing attacks

Payloads

- Corruption of system or data files
- Theft of service/make the system a zombie agent of attack as part of a botnet
- Theft of information from the system/keylogging
- Data Encryption for ransom
- Stealthing/hiding its presence on the system

Advanced Persistent Threats (APTs)

- Well-resourced, persistent application of a wide variety of intrusion technologies and malware to selected targets (usually business or political)
- Typically attributed to state-sponsored organizations and criminal enterprises
- Differ from other types of attack by their careful target selection and stealthy intrusion efforts over extended periods
- High profile attacks include Aurora, RSA, APT1, and Stuxnet

Attack or Exploit Kits

- Initially the development and deployment of malware required considerable technical skill by software authors
- Toolkits are often known as “crimeware”
- Examples are:
    - Zeus
    - Angler
    - Magnitude
    - Nuclear
- https://www.privacyaffairs.com/dark-web-price-index-2023/

Classification by Propagation Technique

Poll 1 – Questionpro.io

Viruses

- Piece of software that infects programs
  - Modifies them to include a copy of the virus
  - Replicates and goes on to infect other content
  - Easily spread through network environments
- When attached to an executable program a virus can do anything that the program is permitted to do
  - Executes secretly when the host program is run
- Specific to operating system and hardware
  - Takes advantage of their details and weaknesses

Detecting Malware Lab 1

- Virus Total Lab
- Go to NCR Kali Machine
  - Download VirusTotalLab files from Web Campus

Virus Components

Infection mechanism

- Means by which a virus spreads or propagates
- Also referred to as the *infection vector*

Trigger

- Event or condition that determines when the payload is activated or delivered
- Sometimes known as a ***logic bomb***

Payload

- What the virus does (besides spreading)
- May involve damage or benign but noticeable activity

Macro and Scripting Viruses

NISTIR 7298 defines a macro virus as:

"a virus that attaches itself to documents and uses the macro programming capabilities of the document's application to execute and propagate"

- Macro viruses infect scripting code used to support active content in a variety of user document types
- Are threatening for several reasons:
  - Is platform independent
  - Infect documents, not executable portions of code
  - Are easily spread because they infect user documents rather than system programs, traditional file system access controls are of limited use in preventing their spread, since users are expected to modify them
  - Are much easier to write or to modify than traditional executable viruses

Virus Classifications

Classification by target

- Boot sector infector
  - Infects a master boot record or boot record and spreads when a system is booted from the disk containing the virus
- File infector
  - Infects files that the operating system or shell considers to be executable
- Macro virus
  - Infects files with macro or scripting code that is interpreted by an application
- Multipartite virus
  - Infects files in multiple ways

Classification by concealment strategy

- Encrypted virus
- Stealth virus
- Polymorphic virus
- Metamorphic virus

Worms

- Program that actively seeks out more machines to infect and each infected machine serves as an automated launching pad for attacks on other machines
- Exploits software vulnerabilities in client or server programs
- Can use network connections to spread from system to system
- Spreads through shared media (USB drives, CD, DVD data disks)
- E-mail worms spread in macro or script code included in attachments and instant messenger file transfers
- Upon activation the worm may replicate and propagate again
- Usually carries some form of payload
- First known implementation was done in Xerox Palo Alto Labs in the early 1980s

Worm Replication

Electronic mail or instant messenger facility	• Worm e-mails a copy of itself to other systems • Sends itself as an attachment via an instant message service
File sharing	• Creates a copy of itself or infects a file as a virus on removable media
Remote execution capability	• Worm executes a copy of itself on another system
Remote file access or transfer capability	• Worm uses a remote file access or transfer service to copy itself from one system to the other
Remote login capability	• Worm logs onto a remote system as a user and then uses commands to copy itself from one system to the other

Target Discovery

- Scanning (or fingerprinting)
- Random
  - Each compromised host probes random addresses in the IP address space using a different seed
- Hit-list
  - The attacker first compiles a long list of potential vulnerable machines
- Topological
  - This method uses information contained on an infected victim machine to find more hosts to scan
- Local subnet
  - If a host can be infected behind a firewall that host then looks for targets in its own local network

WannaCry – Based on NSA's Eternal Blue

- Ransomware attack in May 2017 that spread extremely fast over a period of hours to days, infecting hundreds of thousands of systems belonging to both public and private organizations in more than 150 countries
- It spread as a worm by aggressively scanning both local and random remote networks, attempting to exploit a vulnerability in the SMB file sharing service on unpatched Windows systems.
- This rapid spread was only slowed by the accidental activation of a "kill-switch" domain by a UK security researcher
- Once installed on infected systems, it also encrypted files, demanding a ransom payment to recover them

Mobile Code as Infection Vector

NIST SP 800-28 defines mobile code as

> "programs that can be shipped unchanged to a heterogeneous collection of platforms and executed with identical semantics"

- Transmitted from a remote system to a local system and then executed on the local system
- Often acts as a mechanism for a virus, worm, or Trojan horse
- Takes advantage of vulnerabilities to perform its own exploits

- Popular vehicles include:
  - Java applets
  - ActiveX
  - JavaScript
  - VBScript
- Most common ways of using mobile code for malicious operations on local system are:
  - Cross-site scripting
  - Interactive and dynamic Web sites
  - E-mail attachments
  - Downloads from untrusted sites or of untrusted software

Mobile Phone Worms

- First discovery was Cabir worm in 2004
- Then Lasco and CommWarrior in 2005
- Communicate through Bluetooth wireless connections or MMS
- Can completely disable the phone, delete data on the phone, or force the device to send costly messages
- CommWarrior replicates by means of Bluetooth to other phones, sends itself as an MMS file to contacts and as an auto reply to incoming text messages

Poll 2

Drive-By-Downloads

Exploits browser and plugin vulnerabilities so when the user views a webpage controlled by the attacker, it contains code that exploits the bug to download and install malware on the system without the user's knowledge or consent

In most cases the malware does not actively propagate as a worm does

Spreads when users visit the malicious Web page

Watering-Hole Attacks

- A variant of drive-by-download used in highly targeted attacks
- The attacker researches their intended victims to identify websites they are likely to visit, then scans these sites to identify those with vulnerabilities that allow their compromise
- They then wait for one of their intended victims to visit one of the compromised sites
- Attack code may even be written so that it will only infect systems belonging to the target organization and take no action for other visitors to the site
- This greatly increases the likelihood of the site compromise remaining undetected

Malvertising or Madware

- Places malware on websites without compromising them
- The attacker pays for advertisements that are highly likely to be placed on their intended target websites and incorporate malware in them
- Using these malicious ads, attackers can infect visitors to sites displaying them
- The malware code may be dynamically generated to either reduce the chance of detection or to only infect specific systems
- Has grown rapidly in recent years because they are easy to place on desired websites with few questions asked and are hard to track
- Attackers can place these ads for as little as a few hours, when they expect their intended victims could be browsing the targeted websites, greatly reducing their visibility

Clickjacking

- Also known as a user-interface (UI) redress attack
- A typical attack uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the top-level page
- Using a similar technique, keystrokes can also be hijacked as a user could be typing into an invisible frame controlled by the attacker

Mitigation:

https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html

BankofAmerica.com example

- Use developer tools to view Response Header
  - Script-scr 'self' limits loading of scripts to this site
  - Unsafe-inline and unsafe-eval blow that up
  - https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy/script-src

Social Engineering

Spam

- Unsolicited bulk e-mail
- Significant carrier of malware
- Used for phishing attacks

Trojan horse

- Program or utility containing harmful hidden code
- Used to accomplish functions that the attacker could not accomplish directly

Mobile Trojans

- First appeared in 2004 (Skuller)
- Target is the smartphone

Poll 3

Detecting Malware Lab 2

- Hashing-Yara Lab on NCR

Classification by Propagation Payload

Payload - System Corruption

- Real-world damage
  - Causes damage to physical equipment
    - Chernobyl virus rewrites BIOS code
  - Stuxnet worm
    - Targets specific industrial control system software
  - There are concerns about using sophisticated targeted malware for industrial sabotage
- Logic bomb
  - Code embedded in the malware that is set to "explode" when certain conditions are met

Ransomware

- WannaCry
  - Infected a large number of systems in many countries in May 2017
  - When installed on infected systems, it encrypted a large number of files and then demanded a ransom payment in Bitcoin to recover them
  - Recovery of this information was generally only possible if the organization had good backups and an appropriate incident response and disaster recovery plan
  - Targets widened beyond personal computer systems to include mobile devices and Linux servers
  - Tactics such as threatening to publish sensitive personal information, or to permanently destroy the encryption key after a short period of time, are sometimes used to increase the pressure on the victim to pay up

Poll 4

Payload – Attack Agents: Bots

- Takes over another Internet attached computer and uses that computer to launch or manage attacks
- *Botnet* - collection of bots capable of acting in a coordinated manner
- Uses:
  - Distributed denial-of-service (DDoS) attacks
  - Spamming
  - Sniffing traffic
  - Keylogging
  - Spreading new malware
  - Installing advertisement add-ons and browser helper objects (BHOs)
  - Attacking IRC chat networks
  - Manipulating online polls/games

Remote Control Facility

- Also called command and control or C&C
- Distinguishes a bot from a worm
  - Worm propagates itself and activates itself
  - Bot is initially controlled from some central facility
- Typical means of implementing the remote-control facility is on an IRC server
  - Bots join a specific channel on this server and treat incoming messages as commands
  - More recent botnets use covert communication channels via protocols such as HTTP
  - Distributed control mechanisms use peer-to-peer protocols to avoid a single point of failure

Poll 5

Payload – Information Theft

- Keylogger
  - Captures keystrokes to allow attacker to monitor sensitive information
  - Typically uses some form of filtering mechanism that only returns information close to keywords (“login”, “password”)
- Spyware
  - Subverts the compromised machine to allow monitoring of a wide range of activity on the system
    - Monitoring history and content of browsing activity
    - Redirecting certain Web page requests to fake sites
    - Dynamically modifying data exchanged between the browser and certain Web sites of interest

Malware Analysis Lab - Keylogger

- Analyze with strings command using – n 20
- Analyze with grep
- Analyze with ghidra and search strings
  - Other options include:
    - Radare2 on Kali
    - Ida or Ida Pro – commercial software

Payload – Information Theft - Phishing

- Exploits social engineering to leverage the user's trust by masquerading as communication from a trusted source
- Include a URL in a spam e-mail that links to a fake Web site that mimics the login page of a banking, gaming, or similar site
- Suggests that urgent action is required by the user to authenticate their account
- Attacker exploits the account using the captured credentials

- Spear-phishing
  - Recipients are carefully researched by the attacker
  - E-mail is crafted to specifically suit its
    recipient, often quoting a range of information to convince them of its authenticity

Poll 6

Payload – Backdoor

- Also known as a ***trapdoor***
- Secret entry point into a program allowing the attacker to gain access and bypass the security access procedures
- ***Maintenance hook*** is a backdoor used by Programmers to debug and test programs
- Difficult to implement operating system controls for backdoors in applications
- Mostly an insider threat

Poll 7

Malware Analysis Lab - GREP/Strings Lab

Payload – Rootkit

- Set of hidden programs installed on a system to maintain covert access to that system
- Hides by subverting the mechanisms that monitor and report on the processes, files, and registries on a computer
- Gives administrator (or root) privileges to attacker
  - Can add or change programs and files, monitor processes, send and receive network traffic, and get backdoor access on demand

Rootkit Classification Characteristics

- **Persistent**
  - Activates each time the system boots. The rootkit must store code in a persistent store, such as the registry or file system, and configure a method by which the code executes without user intervention. This means it is easier to detect, as the copy in persistent storage can potentially be scanned.
- **Memory based**
  - Has no persistent code and therefore cannot survive a reboot. However, because it is only in memory, it can be harder to detect.
- **User mode**
  - Intercepts calls to APIs (application program interfaces) and modifies returned results. For example, when an application performs a directory listing, the return results don't include entries identifying the files associated with the rootkit.

Rootkit Classification Characteristics

- **Kernel mode**
- Can intercept calls to native APIs in kernel mode. The rootkit can also hide the presence of a malware process by removing it from the kernel's list of active processes.

- **Virtual machine based**
- This type of rootkit installs a lightweight virtual machine monitor, and then runs the operating system in a virtual machine above it. The rootkit can then transparently intercept and modify states and events occurring in the virtualized system.

- **External mode**
- The malware is located outside the normal operation mode of the targeted system, in BIOS or system management mode, where it can directly access hardware
- https://otx.alienvault.com/pulse/615da17a17aebe726ae818f1

Kali Rootkit Lab

Check Root Kit from Kali terminal:

- git clone https://github.com/Magentron/chkrootkit.git
- cd chkrootkit
- ./chkrootkit

RK-hunter from Kali terminal:

- wget http://downloads.sourceforge.net/project/rkhunter/rkhunter/1.4.6/rkhunter-1.4.6.tar.gz
- cd Downloads
- tar -xvf rkhunter-1.4.6.tar.gz
- rkhunter --check

Fileless Malware

- Link to malicious website
- Website loads Flash or other plugin that launches PowerShell commands
- https://www.crowdstrike.com/cybersecurity-101/malware/fileless-malware/

Malware Counter Measures

Malware Countermeasure Approaches

- Ideal solution to the threat of malware is prevention
- If prevention fails, technical mechanisms can be used to support the following threat mitigation options:
  - Detection
  - Identification
  - Removal

Four main elements of prevention:

- Policy
- Awareness
- Vulnerability mitigation
- Threat mitigation

Counter Measure Discussion

- What Policies?
- What Vulnerability Mitigation?
- What Threat Mitigation?

Generations of Anti-Virus Software

- First generation: simple scanners
  - Requires a malware signature to identify the malware
  - Limited to the detection of known malware
- Second generation: heuristic scanners
  - Uses heuristic rules to search for probable malware instances
  - Another approach is integrity checking
- Third generation: activity traps
  - Memory-resident programs that identify malware by its actions rather than its structure in an infected program
- Fourth generation: full-featured protection
  - Packages consisting of a variety of anti-virus techniques used in conjunction
  - Include scanning and activity trap components and access control capability

Host-Based Behavior-Blocking Software

- Integrates with the operating system of a host computer and monitors program behavior in real time for malicious action
  - Blocks potentially malicious actions before they have a chance to affect the system
  - Blocks software in real time so it has an advantage over anti-virus detection techniques such as fingerprinting or heuristics

Limitations
• Because malicious code must run on the target machine before all its behaviors can be identified, it can cause harm before it has been detected and blocked

Perimeter Scanning Approaches

- Anti-virus software typically included in e-mail and Web proxy services running on an organization's firewall and IDS
- May also be included in the traffic analysis component of an IDS
- May include intrusion prevention measures, blocking the flow of any suspicious traffic

Ingress monitors

Located at the border between the enterprise network and the Internet

One technique is to look for incoming traffic to unused local IP addresses

Egress monitors

Located at the egress point of individual LANs as well as at the border between the enterprise network and the Internet

Monitors outgoing traffic for signs of scanning or other suspicious behavior

Two types of monitoring software

Researching Malware

- Simple consumer tools
  - https://www.virustotal.com
  - https://www.hybrid-analysis.com/
- Research
  - https://malpedia.caad.fkie.fraunhofer.de/
    - Look at Process Injection in BugSleep Loader
  - https://virusshare.com/about.4n6
- Advanced tools
  - https://otx.alienvault.com/preview

Malware Hunting - Sandbox Analysis

- Running potentially malicious code in an emulated sandbox or on a virtual machine
- Allows the code to execute in a controlled environment where its behavior can be closely monitored without threatening the security of a real system
- Running potentially malicious software in such environments enables the detection of complex encrypted, polymorphic, or metamorphic malware
- The most difficult design issue with sandbox analysis is to determine how long to run each interpretation

Malware Monitoring Lab - Windows

In-class Malware Challenge

Important Tips for NICE Challenge

- Update the virus definitions
- DO NOT scan the entire machine. You have a good clue of where the problem is, so start with user files
- Beware of processes that re-install files
- If you can move the quarantine files to the security desk and still not get a check, take a screen shot

Module 6 Assignment

- Labtainer lab using Metasploit
  - A bit repetitive, but do all of them
  - You may need to enter a “y” or CTL-C to end some processes