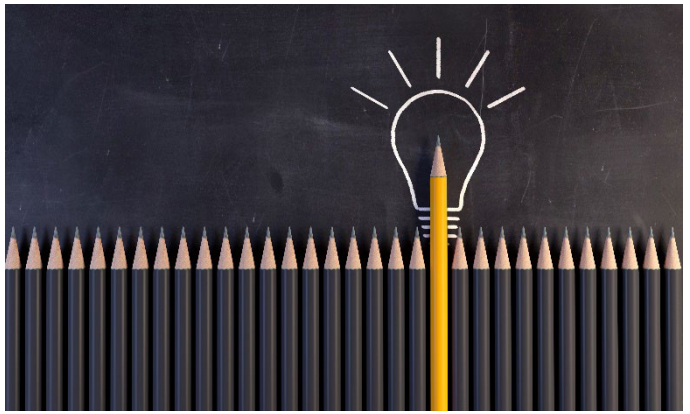
04-Penetration Testing and Malware

Learning Objectives

- Describe what a penetration test is and why it is valuable.
- Identify the rules of engagement and how to perform a pen test.
- Recognize the different types of malware.



Penetration Testing

- Penetration testing (Pen Test) is a simulated cyber attack against an information system to check for exploitable vulnerabilities.
- Unlike vulnerability scanning, pen tests help the organization in finding new deeper vulnerabilities and to understand how they can be exploited.
- In a pen test, the attacks:
  - must be the same as those used by a threat actor
  - and should follow the thinking of threat actors.
- Planning is essential, if a pen test is not well planned:
  - It may result in *creep*, which is expansion beyond the test's limitations.
  - It may lead to unnecessary legal issues.

Rules of Engagement

- The rules of engagement in a pen test define its limitations and parameters.
- To help in planning for the test. The following parameters are often taken into consideration:
  - Timing: when the test will begin and how long it will take.
  - Scope: what should be tested, is it a web app, the internal network, the wireless network, third party services, etc.
  - Authorization: prior written approval to conduct the test.
  - Exploitation Level: what vulnerabilities can be exploited, which ones are off limits.
  - Communication: the tester should notify the organization upon the initiation of the test, discovery of a critical vulnerability, or in case of an emergency.
  - Cleanup: when the test is completed, the tester should remove any installed software, scripts, user accounts created, etc.
  - Reporting: when the test is completed, the tester should provide a full report that includes an executive summary and a detailed part.

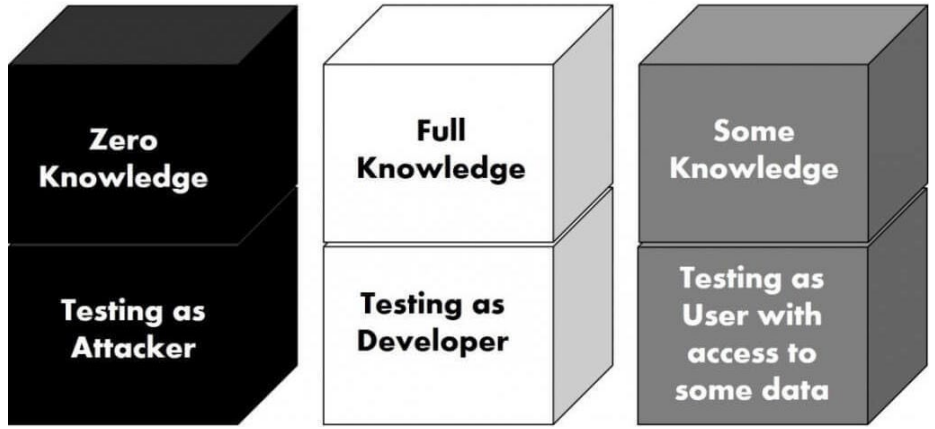
Pen Testing Teams

- A pen test could be conducted by:
  - Internal security employees of the organization.
  - External pen tester consultants.
  - Crowdsourced pen testers.
    - Bug bounty programs such as Hacker one allow the members of the security community to test the security of a client and receive a monetary reward for uncovering a software vulnerability.
- Pen testers are usually divided into teams:
  - Red Team: the attackers.
  - Blue Team: the defenders.
  - White Team: the referees who enforce the rules of engagement.
  - Purple Team: this team provides real-time feedback to attackers and defenders to enhance the overall test.

Types of Pen Testing

Based on the level of information and access provided to the attacker, pen tests can be classified into:

- Black Box: the tester is given no information and no special privileges.
- White Box: the tester is given full knowledge of the network and the source code of applications.
- Gray Box: the tester is given limited knowledge and access level.



Phases of a Pen Test 1/2

Once the test is planned and the rules of engagement are defined, the test starts and often includes several stages that threat actors often use to attack a system:

- Reconnaissance: also called *footprinting*, is the process of gathering information about the organization. It could be:
  - Active: by directly probing the system for vulnerabilities and useful information. For example, perform a war driving/fly driving to find unprotected wireless networks that can be used to gather information or circumvent security.
  - Passive: by searching online for publicly accessible information called Open-Source Intelligence (OSINT) that can reveal valuable insight about the system.
- Scanning: threat actors often use various tools to check network traffic on the target system and identify open ports as they are potential entry points for attacks.
- Initial Exploit: threat actors then use a discovered exploitable vulnerability to gain access to the system.

Phases of a Pen Test 2/2

- Establishing Persistence: attackers may install a backdoor that allows them easier, repeated, and long-term access to the system in the future without having to use the initial vulnerability.
- Moving Laterally: the initial exploit most often does not contain the data that is the goal of the attack. Threat actors usually attempt to escalate to more advanced resources that are usually protected from users and applications (privilege escalation).
- Accessing Data: threat actors continue to probe until they find their ultimate target and perform their intended malicious action, such as stealing R&D information, password files, or customer credit card numbers.

(Video 15:50, Watch hackers break into the US power grid).

Malware

Malware (Malicious Software) is software that enters a computer system without the user's knowledge or consent and then performs an unwanted and harmful action.

- Malware is continually evolving to avoid detection.
- Based on the primary action that the malware performs, malware can be classified into:
  - Imprison.
  - Launch.
  - Snoop.
  - Deceive.
  - Evade.

  (Video 2:45, Malware: Difference Between Computer Viruses, Worms and Trojans)

Imprison (1-Ransomware)

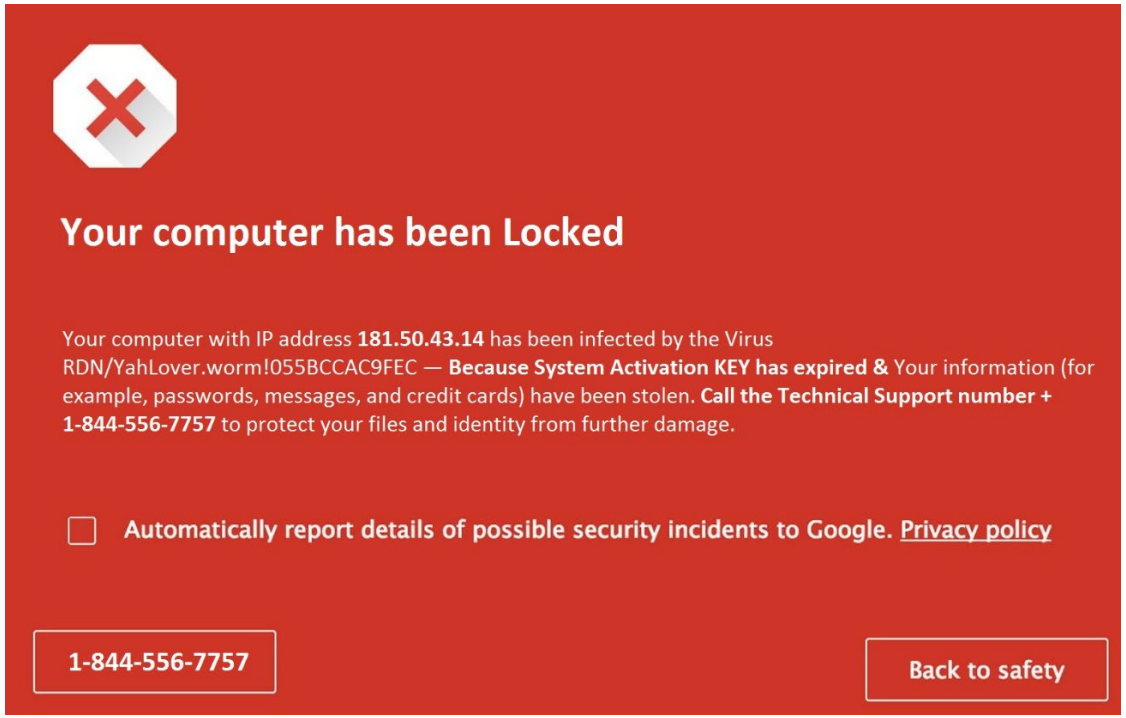
Imprison:

The malware attempts to take away the freedom of the users to do what they want on their computer by blocking it.

Ransomware and cryptomalware fall in this category.

Ransomware: prevents a user's endpoint device from properly and fully functioning until a fee is paid.

- The fee could be small for individuals (200-500$) but could go up to millions of dollars for organizations.
- Ransomware usually cannot be avoided, even if the computer is restarted.



Imprison (2-Cryptomalware)

- Cryptomalware: encrypts all files on the device so that none of them can be opened.
  - The cost to unlock may increase by time.
  - New variants of cryptomalware encrypt all files on any server, NAS, or DAS device connected to that computer.

Launch (1-Virus)

Launch:

The malware infects a computer to launch attacks on the same computer or other computers. This includes viruses, worms, and bots.

A Virus could be file-based or fileless.

- File-based virus is malicious code that is attached to a file.
  - The virus reproduces itself on the same computer without intervention by inserting its code into another file.
  - Doesn't transfer to another computer unless the infected file is copied or sent in an email by human.
  - Malicious actions may include deleting files, preventing programs from launching, causing a computer to freeze or crash repeatedly, or turning off the computer's security settings.

Launch (1-Virus)

- Fileless virus does not attach itself to a file.
  - Instead, it takes advantage of native services and processes that are part of the OS to avoid detection and carry out its attacks.
  - The code is loaded directly in the computer's Random Access Memory (RAM).
  - Fileless viruses are more powerful since:
    - They are easy to infect as there is no need for a file, the code can be downloaded from the web as part of a script.
    - They have extensive control as they use the OS processes.
    - They are persistent as they write to the *Windows Registry* so that they launch again when the computer restarts.
    - Difficult to detect as they reside in the memory. Tools that scan files cannot find them.
    - Difficult to defend against as they need to terminate the process running them which may cripple the whole system.

Launch (2-Worm)

A worm is a malicious program that uses a computer network to replicate and spread itself (Network Viruses).

- A worm enters the computer through the network and exploits a vulnerability on that computer.
- It then searches the network for another computer with that vulnerability.
- Early worms used to affect the network by increasing the traffic due to their self replication and spreading.
- Newer worms leave a payload behind them that causes damage to the computer as well.
  - They may delete files on the computer.
  - They may also make the computer susceptible to be controlled remotely.

Launch (3-Bots)

A bot allows the infected computer to be placed under the remote control of an attacker for the purpose of launching attacks.

- The affected computer is called a bot or zombie.
- When millions of computers are infected, they are called a botnet.
- They receive instructions from a remote computer called the bot herder through a command and control (C&C) structure.
- Botnets could be used in:
  - Sending spam emails.
  - Spreading other malware by downloading and executing a file sent by the attacker.
  - Ad fraud by making the bots mimic the click of an ad on a targeted website. Attackers earn money by the increased number of clicks.
  - Mining cryptocurrencies.

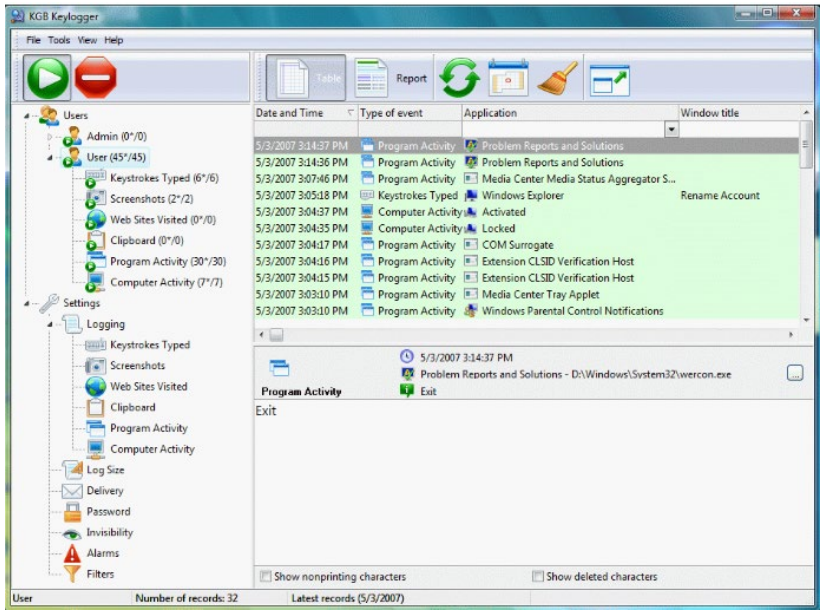
Snoop (1-Keylogger)

Snoop:

The malware snoops or spies on its victims.

Keyloggers and spyware are classified in this category.

A Keylogger silently captures and stores each keystroke that a user types on the computer's keyboard.



- The threat actor can then search the captured text for useful information such as passwords, credit card numbers, or other PII.
- A keylogger can be a software program or a small hardware device plugged like a USB.
- Software keyloggers can also capture the user's screen and silently turn on the camera to record images of the user.
- Hardware keyloggers go undetected by antimalware programs but must be installed on the computer and then removed manually.

Snoop (2-Spyware)

A Spyware is a tracking software that is deployed without the consent or control of the user.

- They could be used to monitor the user's activities (e.g., web pages browsed, or apps launched) or collect personal information.
- They often use technologies embedded in the device itself without the need for additional software.

Deceive (1-PUP)

Deceive:

The malware attempts to deceive the user and hide its true intentions. Software in this category includes Potentially Unwanted Programs (PUPs), Trojans, and Remote Access Trojans (RATs).

A PUP is a software that the user does not want on their computer.

- PUPs often become installed along with other programs as a result of the user overlooking the default installation options.
- Examples of PUPs are:
  - Adware or advertising that obstructs content or interferes with web browsing.
  - Pop-up/Pop-under Windows.
  - Search engine hijacking.
  - Home page hijacking, etc.

Deceive (2-Trojan & RAT)

A Trojan is an executable program that disguises as performing a benign activity but also does something malicious.

- Often associated with free downloadable apps. For example:
- The user installs a disk cleaner app, but the app is associated with a malware that scans the system for stored credit card numbers and passwords, connects through the network to a remote system, and then transmits that information to the attacker.

A Remote Access Trojan is similar to the regular trojan but allows the attacker unrestricted access to the victim's computer. The attacker can:

- Monitor what the user is doing.
- Change computer settings.
- Browse and copy files.
- Use the victim's computer to access other computers connected on the network.

Evade (Backdoor, Logic Bomb, and Rootkit)

Evade:

The malware attempts to hide another malware or help attacks to evade detection. This includes Backdoors, Logic Bombs, and Rootkits.

A Backdoor gives access to a computer, program, or service that circumvents normal security protections.

- A backdoor installed on a computer allows the attacker to return later and bypass security settings.
- Some software developers create a legitimate backdoor to be removed when the app is finalized. If forgotten, attackers can use it to access illegally.

A Logic Bomb is computer code that is typically added to a legitimate program but lies dormant and evades detection until a specific event triggers it. It then performs its malicious activity (e.g., delete files).

- Could be implanted by a mad employee.

A Rootkit can hide its presence and the presence of other malware on the computer.

- It does this by accessing "lower layers" of the OS to make alterations.

Common File Types

File Type	Extension	Explanation
Plain text	txt	Plain text files are the safest (Only 1 known exploit)
comma separated Value (spreadsheet)	csv	Text files with commas separating fields can be used to save spreadsheet files, but without formatting
web page	html	Text files with HTML metatags can embed other files including scripts
rich text file	rtf	Rich text files allow formatting Microsoft rtf files have contained malware!
image, video or audio file types	jpg gif tiff bmp png svg mp4 mpeg	Any binary file can host executable code and activate on user actions. E.g., change the file extension or extract
Microsoft Office	docx xlsx pptx	MS Office documents can have macros. Macros are Visual Basic (VB) executable code. Even fonts in MS Office files are exploited by malware
portable document	pdf	Adobe pdf writer, and some pdf readers execute files embedded in the pdf file
executable or script files	exe dll scr com bat ps1	Any executable or script file can be malware
compressed file	zip, rar	Can contain a collection of any other files

The End

End of Slide Set