eJPT Certification

Section: System Attacks

09/23/2020

Learning Objectives

* Malware
* Password Attacks
* Buffer Overflow Attacks

Malware

* Why is malware important?
  + Enable us to use right malware during penetration testing engagement.
  + Knowledgeable of how to use malware while keeping your test under the rules of an engagement.
  + Ability to maintain access to a compromised machine.
* Malware = Malicious software
  + Any software used to misuse computer systems with the intent to:
    - Cause denial of service
    - Spy on user’s activity
    - Get unauthorized control over one or more computer systems.
    - Cause other malicious activities.
* Types of malware:
  + Virus
    - Small piece of code that spreads from computer to computer, without any direct action or authorization by the owners of the infected machine.
    - Viruses usually copy themselves to special sections of the hard disk, inside legitimate programs or documents. The virus typically will only run anytime the infected program or file is opened or running.
  + Trojan Horse
    - Malware that comes embedded in a seemingly harmless file such as an executable, an MS word document, PDF file, ect.
    - When the malicious file is opened by the victim then the malware starts compromising the machine.
    - The most common type of Trojan horse is backdoor. This type of trojan horse allows a hacker to get a shell on the infected system.
  + Backdoors
    - Backdoors are software made by two components: a server and a backdoor client.
    - The backdoor server runs on the victim machine listening on the network and accepting connections. The client usually runs on the attacker machine, and it is used to connect to the backdoor to control it.
      * Old school backdoors such as: NetBus and SubSeven are very famous backdoors; they enable the attacker to browse the victim’s hard drive, upload and download files, execute programs and perform a number of other activities.
      * Once installed the attacker can get full control over the remote host
    - Firewalls, if configured correctly can block attackers from established backdoor connection.
    - **Firewalls vs. connect-back backdoors**
      * Instead of the victim machine acting as a server and listening to the client commands, it acts as a client and connects back to the attackers machine.
      * The attacker machine would listen on a port that is well known and common allowed on most of the firewalls, such as port 80 (the web server port).
        + The reason this can be so effective is because the firewall can’t tell the difference between a user surfing the web and a backdoor connecting back to the attackers machine.
  + Rootkit
    - Rootkit is malware designed to hide itself from users and antivirus programs in order to completely subvert the OS functioning.
    - Enables the attacker to maintain privileged access to the victim machine without being noticed.
  + Bootkit
    - Bootkits are rootkits which circumvent OS protection mechanisms by executing during the bootstrap phase. Bootkits start before the OS, so they get complete control over the machine the OS.
  + Adware
    - Annoying software that shows ads to computer users.
  + Spyware
    - Used to collet info about users’ activity. Spyware collects info such as:
      * The OS installed on a machine
      * Visited websites
      * Passwords
    - The information is sent back to a log collection server controlled by the attacker.
  + Greyware
    - Malware that does not fall under anyone one category. For example, the greyware could be a combination of adware and spyware.
  + Dialer
    - Software that tries to dial numbers on dial-up connections in order to collect money from the victim’s phone bill.
    - More recently, smartphones have been more of a central focus for obvious reasons.
  + Key-logger
    - Records every keystroke on the remote victim machine.
    - Keyloggers perform the following:
      * Recording keystrokes
      * Recording the window name where the victim user was typing
      * Saving the keystrokes in a log file on the victim machine
      * Sending the logs to a server controlled by the attacker.
    - Keyloggers can be stopped by firewalls if the firewall is configured correctly.
    - Keyloggers can get login information, emails sent, documents typed, and chats.
    - Information can be used to exploit the system or email info can be used to create a target social engineering attack.
    - Other types of Keyloggers:
      * Hardware keyloggers
      * Rootkit keyloggers, which are stealthy and more invisible to the victim user than software keyloggers.
    - **Hardware Keyloggers**
      * Small devices that can be installed between a keyboard and a computer.
        + Log keystrokes into internal memory. An attacker needs to two trips to the victim machine to exploit a hardware keylogger: one to install it and one to retrieve it.
        + Are not as common as software keyloggers.
    - **Rootkit keyloggers**
      * Rootkit keyloggers is a piece of software working at the kernel level by hijacking the OS APIs to record keystrokes.
      * Every time a key is pressed on a keyboard, a particular function of the OS kernel is call through a mechanism call an interrupt.
        + There are many different interrupts, each handling a specific function in the system: reading/writing to disk, call device drivers, and so on.
        + Every time the key on the keyboard is pressed, the keyboard interrupt is called.
        + The interrupt calls a specific function of the OS that actually performs the operation intended for the key.

By taking control of this function, the rootkit manages to know which key has been pressed and records it for later use.

* + A screenshot of a cell phone

    Description automatically generatedBotnet
    - Bots are small pieces of software that get installed on millions of internet-connected machines to perform Distributed Denial of Service or serving as spamming sources.
    - These bots are commanded remotely by a so-called command and control server. The c&c server can instruct thousands or even millions of bots to perform a given operation simultaneously.
  + Ransomware
    - Software that encrypts a computer or smartphone content with a secret key.
    - Then it asks the victims for a ransom to give them the content back.
  + Data-Stealing malware
    - Steals important data on the victim’s hard disk and send it back to the attacker. Most of the time the attack is target to a specific company and tailored to work on the target environment.
    - Alternatively, the attacker could use a backdoor to perform data stealing.
  + Worm
    - Worms spread over the network by exploiting OS systems and software vulnerabilities. Worms can also exploit default credentials or misconfigurations to attack a service or a machine.
      * Typically worms are part of other malware, and offer an entry point into the target system.

**Password Attacks**

* One-way encryption algorithm is a way of storing a password. There is no way to know the password starting from its encrypted form.
* Cryptographic hashing functions- used to transform a password from its clear -text form to an encrypted and safe to store form.
* There are two main types of password cracking strategies:
  + Brute force attacks
  + Dictionary attacks
* **Brute Force Attacks**
  + An automated password attack that generates every possible password.
  + Passwords start at one-character and increments the password size until a valid password is found.

**A screenshot of a cell phone

Description automatically generated**

**It will text every possible lowercase character and then every single uppercase character. After the algorithm is done cycling through uppercase characters it will start testing numbers, and then finally symbols.**

**A screenshot of a cell phone

Description automatically generated**

* **Given enough time, a brute force attack is always successful.**

**Brute Force Weaknesses**

* The major issue with brute force cracking is the time constraint. A poor user password can possible be cracked in a few minutes to a few hours. However, a strong password consisting of upper and lowercase characters and symbols could take days and even years.

**John the Ripper**

* Very popular password cracking tool written for Unix-based OS. Sources and binaries for Linux, Mac OSX and Windows can be found to run John the Ripper.
* John the Ripper can run both brute force and dictionary-based attacks against a password database.
* Can be used on nearly 100 encryption formats. To check what type of encryption it can handle execute the command john –list=formats in your terminal.
* Username and password hashes from the compromised machine need to be in the same file in order to use john the ripper.

**A screenshot of a cell phone

Description automatically generated**