eJPT Certification

Section: Introduction

08/7/2020

Learning Objectives:

* The Infosec culture
* Basics of cryptography
* Wireshark usage
* Numeric Systems

Notes

* HTTP- Hyper Text Protocol is enables clear text protocol and creates an environment for an attacker to easily eavesdrop.
* HTTPS- Hyper Text Protocol Secure is encrypted and cannot be read.

Information Security Terms

* White hat hacker- professional pen tester or ethical hacker who performs authorized attacks against a system helping the client solve their security issues.
* Black hat hacker- hacker who performs unauthorized attacks against a system with the purpose of causing damage or gaining profit.
  + Sub category of black hat hackers called crackers.
* User- is a computer system user. Can be an employee of your client or an external user.
* Malicious user- a user who misuses or attacks computer systems and applications
* Root/administrator- users who manage IT networks or single systems.
  + Have max privileges over a system.
    - In a computer system, privileges identify the action that a user is allowed to do.
* Security through obscurity- the use of secrecy of design, implementation or configuration in order to provide security.
  + This cannot stop a skilled and motivated attacker.
* Attack- any kind of action aimed at misusing or taking control over a computer system or application. Examples:
  + Getting unauthorized access to an administration area
  + Stealing a user’s password
  + Causing denial of service
  + Eavesdropping on communications
* Privilege escalation- an attack where a malicious user gains elevated privileges over a system.
* Denial of service (DoS)- is an attack that a malicious user makes to make a system or service unavailable.
  + Can be done by making the service crash or by saturating the service resources, thus making it unresponsive for legitimate users.
* Remote code execution- an attack that a malicious user makes that manages to execute some attacker-controlled code on a victim remote machine.
  + These types of attacks are very dangerous because they can be exploited over the network by a remote attacker.
* Shellcode- custom code which provides the attacker a shell on the victim machine.
  + Shellcodes are generally used during remote code execution attacks.

Cryptography and VPNs

* Clear-text Protocols transmit data over the network without any kind of transformation (encryption).
  + This allows an attacker to eavesdrop on the communication, as well as perform other malicious actions.
  + Clear-text protocols are easy to intercept, eavesdrop and mangle. Should NOT be used to transmit critical or private information.
  + There are no alternatives to clear text protocols and therefore should only be used on trusted networks.
* Cryptographic Protocols
  + If traffic is intercepted by an attacker, they will not be able to understand it.
  + Should be used to transmit private and sensitive data over a network.
  + You can use a cryptographic Tunnel to “wrap” a clear-text protocol
    - An example of a Cryptographic Tunnel or Tunneling protocol is a VPN
* Virtual Private Network (VPN)
  + Uses cryptography to extend a private network over a public one, like the internet.
  + The extension is made by performing a protected connection to a private network
    - Such as your office or home network
  + From the client’s perspective being in the VPN is the same as being directly connected to the private network.
  + When running a VPN, you are running the same protocols of the private network.

Wireshark Introduction

* Wireshark is a network sniffer tool.
  + A sniffer allows you to see the data transmitted over the network to and from your computer.

Binary Arithmetic Basics

* Bitwise operations- Computers can directly manipulate bits by performing bitwise operations, which are use a lot in network programming and assembly programming.
* NOT- simple operation that flips the bits: zeroes become ones and ones become zeroes.
* AND- Performs a logical AND between the bits of its operands if both bits in the comparing position are ones, the result is one; otherwise, it is zero.
* OR performs a Logical OR between the bits of its operands.
  + If at least one of the bits in the comparing position is one, the result is one.