Information Security and Cyber Security

Two Close Related Twins

By: Michael Lassiter Jr. (@EthicalMJPen)
Abstract

This document is only a brief synopsis of the ever-expanding and demanding field of information security. It contains explanations, screenshots or visual cues, and tips on multiple subjects such as system defenses, reducing vulnerabilities, and the presence of malicious threats. Smaller areas, such as vulnerability assessment and penetration testing, are also covered because they are very significant in the security of information. While vulnerability assessment is a necessity, penetration testing is purely an option to the security engineer.

Table of Contents

What is Information Security? ................................................................. 1
Threats ................................................................................................. 2-3
Strategies to Reduce Vulnerabilities .................................................... 3-4
What is Cyber Security? ........................................................................ 4-5
TOOLS ................................................................................................. 5
    Nmap ............................................................................................. 5-6
    Zenmap ......................................................................................... 7
    Metasploit ..................................................................................... 7-10
CONCLUSION ........................................................................................ 10
**What is Information Security?**

Information security is often defined as the security or assurance of information and it requires the ability to maintain the authenticity of the information. The three common components of information security are **confidentiality**, **integrity**, and **availability** and they form an essential base for the overall picture of information security.

Confidentiality is perhaps one of the most common aspects of information security because any information that is withheld from the public within the intentions to only allow access to authorized individuals is confidential. Encryption is often used to maintain the confidentiality of information as encryption is one of multiple methods of access control and Microsoft BitLocker is an example of access control-encryption feature. Although TrueCrypt is no longer a secure method of protecting data, I will discuss it further in the Cyber Security portion of the paper.

In addition to confidentiality, integrity is an important aspect because the original format or content of the information should not change under any circumstances except by permission from authorized individuals. The hashing method is commonly used to ensure integrity and hash of the source must match the hash of the destination to ensure that the data is void of any modification. Finally, the information should be available to all authorized individuals and this component is usually targeted by denial-of-service attacks or DOS. Availability is essential to the continuity of a company in the times of disaster, extreme emergency or data breach so it is heavily dependent on the ability of a company or agency to provide services and consistently back up all data. During the case of a breach or a “hack”, availability is a top priority as security engineers strive to seal the access to confidential data while permitting those that are authorized to access the data. The inter-relationship between confidentiality, integrity, and availability is critical to establishing policies and procedures in information technology. Therefore, it creates one of the main reasons why a narrow distinction exists between the fields of information security and cyber security. The issues of policies and procedures are also extensive in information security and they are often set or advised by the Chief Information Security Officer (CISO) or the Information Security Director. The policies are critical because they are not only for regulating the activities of the personnel but they are establish to protect the network from negligent practices. Also, the standards of procedures are used to create a redundancy plan in case of a data breach and start a recovery plan from the victimization of a threat.
Threats Against Information Security

The threats against information security include dangers such as malware, social engineering, and negligence on the staff but I will give a brief overview of malware. Malware is often known as software that contains malicious code and its main focus is to damage a system by gaining access without authorization from the owner. Malware can further be classified into four different types which include viruses, worms, trojans, and rootkits.

A virus is an actual set of malicious code and it can only penetrate a system by attaching itself to a host application. Therefore, the execution of the host application is necessary for the sequential execution of the virus and it may seek to attach itself to additional applications within the system. One of the most dangerous types of viruses is polymorphic viruses because they have the ability to mutate the code so they create a hardship in identification of signatures of the virus. Similar to the operation of a virus, a trojan requires execution but it is actually a malicious program that masquerades as a harmless application.

They are usually, yet unfortunately, acquired through a variety of ways from downloads from the internet to web applications and peer-to-peer applications. The execution of trojans and the use for exploitation is later covered in the Tools section of this paper. An example of a trojan is a file named FREEITTRAINING.DO CX.EXE. If you look at the file name closely, it should be apparent that there are some irregularities or things that should raise some concerns. Although it appears to be a Microsoft Word document, it is actually a program with an executable extension due to the “exe” at the end of the file. The recommended option to reduce the possibility of executing this particular type of trojan is to “check” the show file extensions in Windows Explorer. Since this option is not automatically checked in older versions of Windows, I advise for this option to be checked for future navigation in Windows Explorer.

Unlike the execution requirement of viruses and trojans, worms are also dangerous because they can damage a system without attaching to an internal application or program. After infection of one computer, a worm searches for the next vulnerable system to infect and it can leave a payload which could cause further damage to a system. One of the first worms to infect systems on an enormous scale was created over twenty five years ago. It exploited a vulnerability in a program that enabled commands from a remote system to be executed and approximately six thousand computers were affected by the worm.

However, rootkits are entirely different from the previous types of malware as they can actually conceal the presence of other malware in a system. A rootkit is defined as a combination of tools used by an attacker to penetrate a computer with the intentions...
to obtain administrator privileges and perform an assortment of non-permitted actions. The ability of a rootkit to replace the operating system commands with modified versions is a dangerous characteristic of a rootkit. The operating system would be less likely to identify the presence of malware in the system. Due to the current availability of anti-virus tools, it is becoming a bit easier to detect the presence of rootkits but the removal of them can be arduous at times. Although detection is the first step to defending against rootkits, some anti-virus products are incapable of removing rootkits. Therefore, the only option may consist of reformatting a hard drive and re-installing the operating system. Since we have discussed several types of malware, we can take a look at some strategies to reduce the risk of infection by malware and other vulnerabilities.

**Strategies to Reduce Vulnerabilities**

It is evident that the origin of many data breaches is not located outside a network but actually within the internal borders of the network. Although there is one hundred percent impossible for a system to be invulnerable, there are some methods that can be used to mitigate some risks. **Patches** are critical to maintaining productivity, protection and eliminating any weaknesses that could lead to a breach. For example, a virtual environment simulation product such as VmWare is excellent for creating virtual machines, yet VmWare should be patched whenever a bug or vulnerability is discovered because some malware can actually exploit a weakness in the VmWare. In addition to VmWare, many people are familiar with patches in reference to anti-virus and it is a formidable defense against malware.

Similar to the process of patching, **anti-virus software** will require updates and it is due to the use of signature or definition files. I can recall from personal experiences that not all anti-virus products are created equal. Individuals should consider every necessity before purchasing a specific anti-virus product. Despite the differences among vendors, a capability that should not be ignored under any circumstances is the ability to actually remove a threat from the system. Some anti-virus products are only capable of scanning a system for threats so the user is unable to use the product to actually remove the threat from the system. Therefore, it is important to pay attention to the features and choose the best option for the system. Patches and anti-virus software are only two pieces of a defensive framework and cyber defense will hardly exist without the use of a firewall.

A **firewall** is used as a prevention tool against the entering or departure of malicious packets from computers. Due to current technology, it can be based on either software or hardware components. A personal software firewall is a program that protects a local host against attacks. A firewall is typically
placed on the outside of a network security perimeter as a first line of defense so the firewall is the “infantry” of network defense. Also, a firewall has a set of three rules and they consist of “allow, “block”, and “prompt”. The ‘allow’ rule permits a packet to go through the firewall while ‘block’ prohibits a packet from passing - it drops the packet as a result of the dismissal. Finally, the prompt rule requests additional input from the user so this is the basic rule set of a firewall. In addition, a firewall can filter the traffic that leaves a network by preventing users from viewing pages that contain offensive or crude material.

Firewalls also have two types of filtering and they consist of stateful packet filtering and stateless packet filtering. Stateless packet filtering utilizes the rule base to determine if an incoming packet will be either accepted or denied access to the system. Unfortunately, an attacker can bypass the stateless packet filtering by exploiting an internal IP address and altering the packet to resemble a document that is destined for port 80. Stateful packet filtering, however, makes decisions in reference to packets by comparing the traffic to current records of connections between an internal computer and an external server. Stateful packet filtering will not accept an incoming packet if an internal computer did not previously request the information from the external server, so stateful packet filtering offers greater protection than stateless.

The difference between personal and hardware firewalls is rooted in the strength of the host system. A personal software firewall pulls its effectiveness from the specifications of the host operating system, so a weakness within the OS creates a weakness within the firewall. A Hardware-based firewall runs its own operating system but can be costly. So, hardware firewalls are typically used in commercial environments.

**What is Cyber Security?**

As mentioned earlier, information security is the assurance of information and it may seem to be the same as cyber security but there is a narrow distinction. Cyber security mostly involves or requires the skills to be “hands-on” with the protection of data. Although information security includes duties such as drafting of procedures, enforcement of policies, and creation of regulations that govern computer use in a commercial or government environment; cyber security has a “front-line” approach to data protection. If an individual takes a brief period of time to research the expectations of available jobs within information and cyber security, the individual could see the difference between the two closely related fields.

I can draw from personal experiences as I’ve been questioned by human resource managers and recruiters if I preferred the “policy and procedure
side” or the “cyber side.” As a result, many companies are recognizing that some candidates are more focused on the policy side while others have a preference for the technical side. I personally suggest for those that are interested in the field of information security to have a technical background that consists of cyber operations because it would greatly influence the creation of any policy. Since cyber security includes a base knowledge of common tools and software, we will take a closer look at some tools. Similar to the method of a mechanic, there are a variety of tools that are available to the cyber security engineer, which can seem to be virtually endless, but I will emphasize some of the most common tools and include screenshots as well.

**TOOLS**

It would be an injustice to attempt to discuss every available tool or even most because it would take a document with at least three times the length of this paper to discuss them. I will; however, discuss some of the main tools that are not only commonly used by security professionals worldwide but are often used by criminal hackers to unethically hack into a network. A great way to have an overall base knowledge in the use of cyber tools is to approach a system or think in a method that would resemble a black hat hacker. The available tools are classified into two types of categories: open-source software and commercial products.

**Open-source software** has existed for decades and a prime example is the Linux operating system and numerous types of distributions that have sprouted from its initial creation. In addition to open-source operating systems, cyber security professionals should be aware of open-source tools that vary from forensics, port scanning, penetration testing, and vulnerability assessments. An example of an excellent open-source tool is Nmap and I strongly encourage those that are interested in cyber security to become familiar with this tool.

**Nmap**

Nmap is perhaps the most widely used tool in the focus of scanning and enumeration and one of its main features is the wide assortment of scans or often called switches. The switches can be used to target specific ports and each switch has a certain level of speed. Therefore, the speed of the scan can create varying amounts of noise and it can cause an alert on the intrusion detection system of the targeted machine. As mentioned earlier, some tools are used by both criminal hackers and security professionals. This tool is absolutely no exception to the statement. Also, nmap has both a GUI-based version and a command-line version for use and I strongly suggest security professionals to become familiar with both versions. The command-line version of nmap is fairly easy to use and it requires an understanding of the syntax structure.
Figure 1.1
If you take a look at the above screenshot, there are a few key details that I will point out. I started up my Kali-Linux virtual machine which includes Nmap and its GUI-counterpart, Zenmap. After opening Nmap, it displays multiple options by default yet I chose to use a scan that searches for the name of the operating system and any open ports. The command line syntax for Nmap is the following: `nmap [type of scan] [IP address of targeted system]`. The command that I chose was of the following: `nmap -O -sS (the IP address)`. I want to emphasize that the targeted IP address belonged to one of my virtual machines so this document lacks any black hat or gray hat influence. I mentioned earlier that the scans can cause varying levels of noise on a system and the scan, `-sS`, is a SYN scan. This particular scan is also noted for stealth, but be mindful that it can trigger the radar of some intrusion detection systems.

Figure 1.2
The above screenshot shows the results of the nmap scan on the targeted system. There are a few things that I want to point out in the screenshot. The open ports are listed in the scan results and the very first port is port 80 which is used for http. It lists ports that are related to netbios and msrpc and the MAC address which was assigned through VmWare. Note: The msrpc port is critical because it can be exploited in older versions of Microsoft Windows that are not patched such as Microsoft Windows XP. Prior to the patch that was released in July 2003, Microsoft Windows was vulnerable to attacks against the Distributed Component Object Model (DCOM) and Remote Procedure Call. The scan included the `-O` option. The `-O` is used to fingerprint for the type of operating system that is functioning in the targeted system. The scan yielded successful results as the targeted system was Windows 7 so this is a great combination to use for fingerprinting a system.
Zenmap

Zenmap is the GUI-based version of nmap so it is preferred by those that are more familiar with the GUI-based version of software than the command-line tools. The scans are entered the same because the “nmap” is the first part of the command in both versions. Take a look at the screenshot below.

![Figure 1.3 Zenmap Screenshot]

The screenshot above is basically a GUI version of the screenshot that was taken from the nmap command version. The scans are the same and they produced the same results. One of the key differences consists of the options that are listed as tabs on the screen. The topology, for example, provides a picture of the network setup of the targeted machine so Zenmap is very useful in concentrations such as penetration testing and vulnerability assessment. In addition to Nmap, I will briefly cover a tool that has virtually become synonymous with both penetration testing and cybersecurity – Metasploit.

Metasploit

Metasploit is one of my favorite tools because it can be used to conduct advanced scans and execute an assortment of functions such as payloads, modules, and exploits. Although it has an open-source version that is free, it also has a pro version that costs a fair amount, but it is not expensive in comparison to other penetration testing tools. Despite the differences between the free and pro version, both versions have common features and provide the capability to conduct penetration tests.

An exploit is a function which enables an attacker to take advantage of a flaw in an application, service or system. A payload; however, is a type of code that is executed by the system and it is widely used to gain access to a system through a command shell. Scanning and enumeration was covered earlier in the screenshots that involved Nmap, yet Metasploit
contains auxiliary modules that are great for scanning and they can yield some extensive results. **Shellcode** is a unique feature as it is written in assembly code and has a similar operation to a payload because it can be used after a successful exploitation has taken place in a system. I will now cover Metasploit in the next series of screenshots by demonstrating some of its capabilities.

![FIGURE 1.5](http://metasploit.pro)

The above screenshot is the opening of the Metasploit framework and it also has a GUI version yet the command line version will increase the hands on knowledge of commands and syntax that is similar to Unix/Linux. Although it is not the current version of Metasploit, it shows that I have 1302 available exploits, 700 auxiliary and 335 payloads.

![FIGURE 1.6](image)

A simple command of “show exploits” will display a list of available exploits; however, I must warn you that the list is enormous so I recommend using the search option to shorten the time. For example, the command `search ftp` will generate a list of options that only pertain to File transfer protocol (FTP).

This is an example of the use of an auxiliary in Metasploit. The command for using an auxiliary in the screenshot is of the following: use auxiliary /scanner/http/ntlm_info Enumeration and the following line was a show options command. The options within the auxiliary are displayed on the screen.
**FIGURE 1.7**

```
msf auxiliary(ntlm_info Enumeration) > show options

Module options (auxiliary/scanner/http/ntlm_infoEnumeration):

<table>
<thead>
<tr>
<th>Name</th>
<th>Current Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxies</td>
<td>no</td>
<td>Use a proxy chain</td>
</tr>
<tr>
<td>RHOSTS</td>
<td>yes</td>
<td>The target address range or CIDR identifier</td>
</tr>
<tr>
<td>RPRT</td>
<td>80</td>
<td>The target port</td>
</tr>
<tr>
<td>TARGET_URI</td>
<td>no</td>
<td>Single target URI</td>
</tr>
<tr>
<td>TARGET_URI_FILE</td>
<td>/opt/metasploit/apps/proc/msf/data/wordlist/http_common.txt</td>
<td>Path to list of URLs to request</td>
</tr>
<tr>
<td>THREADS</td>
<td>1</td>
<td>The number of concurrent threads</td>
</tr>
<tr>
<td>VHOST</td>
<td>no</td>
<td>HTTP server virtual host</td>
</tr>
</tbody>
</table>

msf auxiliary(ntlm_info Enumeration) >
```

**FIGURE 1.8**

```
msf > use auxiliary/scanner/netbios/nbname
msf auxiliary(nickname) > set RHOSTS 192.168.35.131
RHOSTS => 192.168.35.131
msf auxiliary(nickname) > set THREADS 2
THREADS => 2
msf auxiliary(nickname) > run

[*] Sending NetBIOS requests to 192.168.35.131->192.168.35.131 (1 hosts)
[*] 192.168.35.131 [LH-XY6PDXB9A0T9] OS:Windows Name:(LH-XY6PDXB9A0T9, WORKGROUP P) Addresses:(192.168.35.131) Mac:00:c2:2f:8f:4e Virtual Machine:VMWare
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(nickname) >
```
The results of the auxiliary provide some interesting details. The auxiliary scanner has a focus on netbios and the end of the option states “nbname”. The option informs Metasploit that I am searching for the name of the netbios in the targeted machine. The Remote Host (RHOST) was set to the IP address of the target system and the threads were set to two (2). I chose to run it and it sent NetBios requests to the target system and the target system responded with the name of the Netbios. It is important to understand how to use the auxiliaries, exploits, and payloads because the command line syntax is the same; however, make sure that you are targeting the right system.

**CONCLUSION**

I sincerely hope that this document has been helpful to you as an introduction to Information Security, or sparked an interest to continue your desires and/or training in the field. It is a field that is expanding rapidly so maintain your passion in the field. Also, be mindful of the laws and regulations that govern each state and country because the only acceptable form of hacking, vulnerability assessment, or penetration testing lies within the boundaries of permission and authorization.