Gabrielle Sudik
IT1025 CRN 12115 – Spring 2017
Professor Tamerlano
Lab 8
May 10, 2017

Executive Summary

The main topic of this week's lab is internet security – preventing system compromises, finding them when they happen, and confirming user identities. This lab also explores some system tools, like Nmap, which can track and manage IT systems of all sizes and designs, and GitHub, which is a web-based tool to share projects with multiple users. Finally, the lab explains how the Fourth and Fifth Amendments to the U.S. Constitution come to bear on searches of electronic devices.

Firewalls, Antivirus Programs and Intrusion Detection Systems

A firewall is a barrier between two computers or computer systems. Firewalls filter incoming packets based on things like packet size, source IP address, protocol and destination port. Its goal is to block traffic that its rules do not allow in. It cannot, however, block everything that might hurt a computer or system.

Antivirus software attempts to prevent viruses from infecting a system by one of two ways. First, it searches the computer or system for all known viruses. Second, the software will scan the computer or system for virus-like behavior, such as a program that searches an entire address book or manipulates the registry.

A firewall is the tool that stops bad things from entering the system in the first place. Antivirus software will stop bad things once they are already in the system.

An intrusion detection system (IDS) is security technology that will check all inbound and outbound activity on a computer or system, looking for patterns that might indicate an attempted break-in. A passive IDS only looks for suspicious activity and logs it, while an active IDS will also shut down suspicious communications.

Internet control message protocol (ICMP) is an error-reporting protocol that devices use to generate error messages when network problems prevent delivery of IP packets. ICMP packets are the IP packets containing information about which packets in the original communication are problematic.

When an IDS discovers that a series of ECPM packets was sent to a computer or system, it is often a sign that the system is being scanned by a program like Cerebus, which is network-scanning software. Such scanning is often a sign that someone is preparing to breach the system's security.

Kerberos is a authentication protocol, which is used by a system to make sure that a user is really who she claims to be. When the user logs in, Kerberos confirms her identify and contacts a “ticket-granting server,” which sends an encrypted ticket to the user's machine. This ticket identifies the user as being logged in, and will later allow her to access resources on the network. Kerberos helps with computer security by using a lot of verification and expiring tickets after a short period of time.

Comparing Norton to McAfee

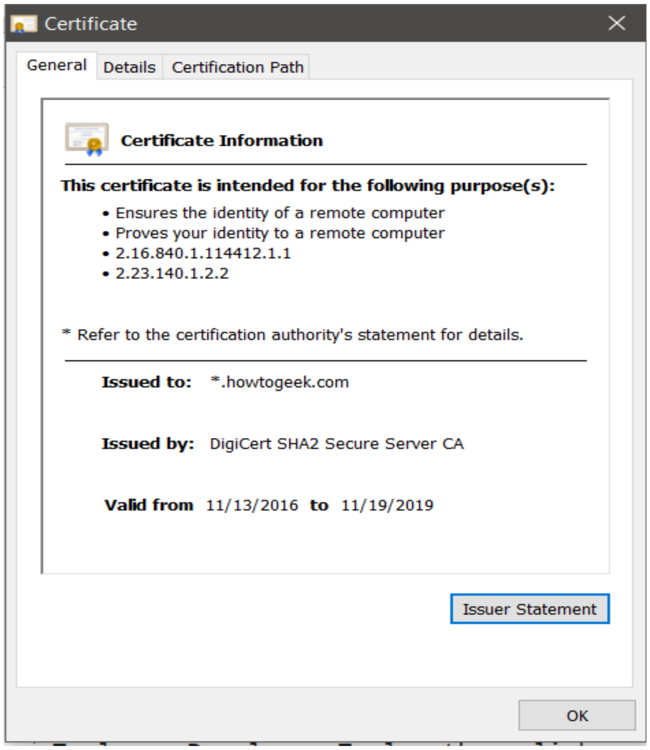
Norton Antivirus takes a few steps to find viruses. First, it will compare a new file to a database of known viruses. If the new file doesn't match a known virus, Norton tries to determine the purpose of the file and understand the actions it will perform. If it expects the file will act like a virus, it will not mark it as safe. If Norton thinks the file is safe, it will allow the user to execute the file, at which point Norton's software will check to make sure that in actuality it does not act like a virus. The software will continue to check the new file at defined intervals.

McAfee starts by scanning the internet for the most up-to-date list of known viruses, as well as how to delete them if discovered on the system. Next, it implements a firewall to keep out most threats. Finally, if any malware makes it past the firewall, McAfee will catch it during a system scan, and will delete it or contain it.

The two systems are similar in always striving to have the most up-to-date list of known viruses. Based on my research, McAfee might be a better job at keeping viruses out of a system in the first place via the firewall. But it might only catch already-present viruses if they are on McAfee's list. Norton, on the other hand, might let a few more viruses into the system, but with its method of analyzing new files and programs for virus-like behavior, it may catch viruses that are not already on a list of known threats.

Digital Certificates

In encryption, a digital certificate can be used to provide a public security key, as well as a means to authenticate that the holder of the certificate is who he claims to be. Digital certificates are “signed” by trusted third parties known as certificate authorities, and they contain information such as who has issued the certificate, how long it is good for, the version, etc. Here is an example of a digital certificate, from howtogeek.com, which is where I learned to find it in Chrome:



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- 2.16.840.1.114412.1.1
- 2.23.140.1.2.2

* Refer to the certification authority's statement for details.

Issued to: *.howtogeek.com

Issued by: DigiCert SHA2 Secure Server CA

Valid from 11/13/2016 to 11/19/2019

Virtual Private Networks

A virtual private network (VPN) is a way to use the Internet to create a virtual connection between a remote computer and a central location. A packet is a little bundle of information that is routed from one source to another on the Internet. In a VPN, all packets are encrypted, and thus private. There are three different ways to create a VPN. The most recent of these (Ipsec) provides extra protection by encrypting not only the packet but its header information. It prevents the re-transmission of packets, which prevents a hacker from grabbing the first packet in a transmission, and putting his own information through behind it.

Algorithms and Wifi Security

An algorithm is a self-contained set of rules that dictate what actions are to be performed. An encryption algorithm is the set of rules that will convert text into a “secret code” and then back into text again. WEP, WPA and WPA2 are the three wifi security protocols, all of which are encryption algorithms, but which vary in effectiveness.

WEP (wired equivalent privacy) is the oldest and least secure wifi security, using either a 64- or 128-bit key. Its weakness is that uses the same initiation vector for every encryption, leaving messages encrypted with WEP very vulnerable to hacking. The next oldest system is WPA (wifi protected access), which creates a new encryption key for each packet sent. So even if one packet is cracked, remaining packets all have their own, different keys. The most recent wifi security is WPA2 provides packet-specific encryption like WPA, and also ensures that packets were not altered during transit (either accidentally or on purpose) by authenticating data origin, confidentiality and integrity.

Nmap

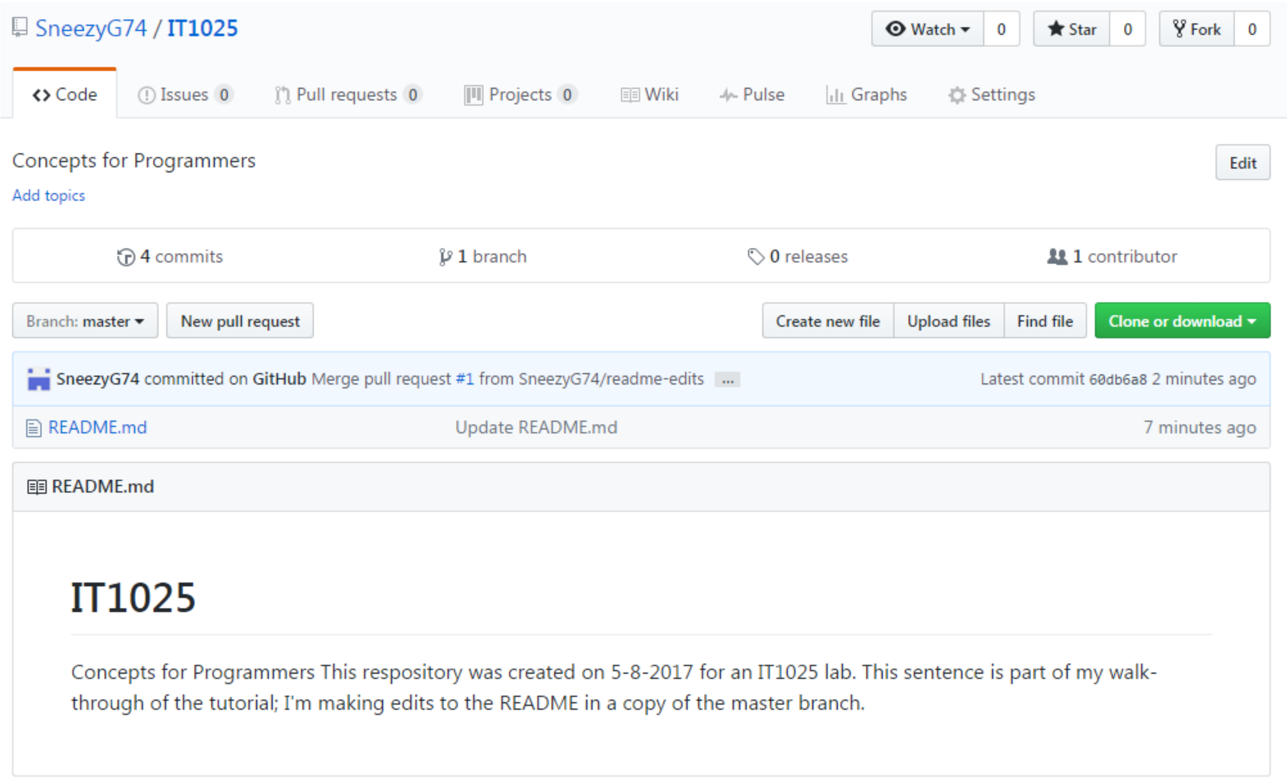
Nmap is a utility for network discovery and security auditing. It can map a system, counting hosts, routers, firewalls, and IP filters. It can detect operating systems and manage upgrades. It can work on a system as small as one host or as large as hundreds of thousands of machines. Nmap is free, well documented and well supported by many engaged volunteers.

It looks like Nmap has starred in a lot of terrible movies! And it's typecast too, usually being cast as a computer hacker. But I see that Nmap broke out of the mold by also starring in a porn flick. It's unclear what its role was, but he probably taught the movie's heroine how to use the ones and zeros. (/sorry)

Zenmap is the graphical user interface that helps new users navigate Nmap. It works on most operating systems, and is also useful for more advanced users. I downloaded Nmap/Zenmap, but for some reason it won't run on my computer. I do not expect any extra credit for this, but I thought you'd enjoy this amusing snip from my desktop:

GitHub

As with most exercises we've done in this class, my experience learning the first steps of GitHub was pretty simple. In large part that was due to well-written instructions. While doing this, I was thinking of the numerous times I was the primary author of some legal document, that needed input from and changes by several other people. It was always a laborious process, getting their hand-written or red-lined edits, and both incorporating them or (sometimes) reconciling conflicting edits. Although I didn't get another person to try GitHub with me, I imagine that it would work well for several authors to collaborate, with one main author editing all of the work. I assume the scope of GitHub goes well beyond mere document editing, however.



Concepts for Programmers

SneezyG74 committed on GitHub Merge pull request #1 from SneezyG74/readme-edits … Latest commit 60db6a8 2 minutes ago

README.md Update README.md 7 minutes ago

README.md

IT1025

Concepts for Programmers This respository was created on 5-8-2017 for an IT1025 lab. This sentence is part of my walk-through of the tutorial; I'm making edits to the README in a copy of the master branch.

The Constitution, Digital Searches and Digital Testimony

The Fourth Amendment to the U.S. Constitution protects individuals from unreasonable searches and seizures. There is a lot of case law that defines both what constitutes a search and what constitutes “unreasonable.” But basically, the rules about when the government can search a person or place vary by circumstances that include where the person is, what the police are looking for, and the likelihood that a person might be dangerous and/or might destroy evidence. For example, a person has more protection inside her own home and when she is clearly not a danger to others, than she does in a public place when she is behaving in a threatening manner.

When it comes to computing and technology, courts treat electronic devices similarly to closed containers, and have repeatedly ruled that people have a high expectation of privacy over these devices. Therefore, police need search warrants before searching the content of devices, and warrants are obtainable only when the government can show a court it has probable cause to think the item being searched is relevant to a crime or will reveal evidence of a crime. In some cases, the police might not need a warrant to *seize* a device, if the circumstances make the police think a suspect will destroy evidence on it. But they will still need a warrant to *search* the device.

In a recent case, *Riley v. California*, 2014, the U.S. Supreme Court unanimously concluded that police need search warrants to search a cell phone, even if the phone is legally seized without a warrant. The Justices, understanding that today’s cell phones store an enormous amount of personal data about their owners and others, compared these devices to carrying around filing cabinets containing everything about a person: Her health history, her phone and mail history, her finances, her personal writings, etc. Since police would need a search warrant to look for any one of those things, they need it for a cell phone.

Drones are aircraft that do not carry human operators but are controlled remotely. They can do everything from take photographs and videos, to scan faces in a crowd, to carry packages, to drop bombs. The FAA Modernization and Reform Act (2012) called on the FAA to “integrate” drones into the national air space system and to write rules governing their use. There have been only a few court cases involving drones and the extent to which they fall under the constraints of traditional search and seizure law. Among these cases is *New Mexico v. Davis*, 2014, in which a state court in New Mexico concluded that a drone used to photograph a man’s backyard without a warrant (and which found marijuana) was unreasonable. That case was based on the state constitution, however, and other states or federal courts might conclude that aerial photography without a warrant is a reasonable search.

The Fifth Amendment to the U.S. Constitution provides that no one can be compelled to testify against himself. Encryption is related to the Fifth Amendment when police have legally seized an electronic device that is protected by a password, and the question of whether a suspect providing a password constitutes testifying against himself. Basically, courts have concluded that when the police know exactly what information is on the device (say, a specific document) but are unable to read it, a defendant can be compelled to give up their password to the police can view the information. However, when police seize a device without knowing what is on it, and need a password so they can find out, courts have generally held that people cannot be compelled to share their password. Because in this case, it's not just a matter of turning over documents the police already know exist, but is opening up an entire system for inspection, and in doing so force the device's owner to “speak” on matters that are private. (As a general matter, courts also don't allow search warrants that allow police to look for just anything... aka, a “fishing expedition.” Police have to have something specific in mind, and can only look in places they might reasonably find it. This is more of a Fourth Amendment issue than a Fifth.)

Conclusion

This lab studied internet security, including the prevention of system compromises, finding them when they happen, and confirming user identities. This lab also examined Nmap, a program to track and manage IT systems, and GitHub, a program that allows multiple people to work on the same project at once. Finally, the lab spelled out rules of police searches and seizures when it comes to electronic devices.