Comp715 - Problem Set 3

PAVAN KUMAR DONDAPATI

**October 21, 2020.**

**1) *[2 points]* For this question you will do a little online research. Please be detailed.**

1. **Find a Virus attack that hit the US in the last decade and describe it.**
2. **Find a Worm attack that hit the US in the last decade and describe it.**
3. **For each, be sure to answer these questions (please don’t use ones in Hw1)**
   1. **What specifically did it infect?**
   2. **What was the payload?**
   3. **What was the financial toll if any?**

**ANS:-**

**a.)** The past decade has seen rapid growth and evolution of cybercrime with the advent of new technology. Attackers developed malicious programs and techniques to steal data, which increased both the cybercrime rate and the number of cyberattacks per day. People lost trillions of dollars, and it is going to see rapid growth in the years to come.

GameOverZeus is a peer-to-peer botnet based on components from the earlier Zeus trojan. This type of virus secretly steals the login details of monetary transactions. It detects a login page, then proceeds to inject malicious code into the page. The virus creates a sprawling network of virus-infected computers to siphon hundreds of millions of dollars from bank accounts around the world, targeting anyone with enough money worth stealing. The virus has two variants on the internet. One version of them can generate around a thousand domains per day, and the other generates ten thousand per day. The FBI even announced a reward of $3 million in exchange for information regarding the alleged cybercriminal Evgeniy Mikhailovich( who is the actual creator of the virus ). It is the highest amount of money offered by a government agency such as the FBI in exchange for information regarding the cybercriminal Evgeniy. In December 2014, there was a Zeus virus attack on the American National Bank. This lead to the loss of many million dollars of public money.

Once a windows system gets infected with the Zeus malware, an attacker can remotely capture the victim's banking account credentials using malicious software to record keystrokes. After gaining account credentials and other information, the attackers transferred more than $198,200 from Haysite's PNC Bank account to an account under the name of Lynch Enterprises LLC at SunTrust Banks in Atlanta. Only a few hours later, they transferred another $175,750 from Haysite's account to R&R Jewellers, a retailer that maintained an account at Herald National Bank in New York. There were many attacks like this one in the months that came. After a series of attacks, the FBI even announced a hefty amount of $3 million as a reward. In a global law enforcement operation called Tovar, authorities from 10 countries seized the systems serving as the backbone to Gameover Zeus and CryptoLocker ransomware.

**b.)** NGRBot is a worm that uses the IRC network for file transfer, sending and receiving commands between zombie network machines and the IRC server of an attacker, and monitoring and controlling network connectivity and intercept. It employs a user-mode rootkit technique to hide and steal user information. It is a family of bots designed to infect HTML pages with inline frames, causing redirections, blocking victims from getting updates from security/antimalware products, and killing those services.

NGRBot is a worm that propagates through chat messengers, social media, etc. It steals FTP and browser passwords and causes the denial of service by flooding. It employs a user-mode rootkit technique to hide and steal user information. NGRBot downloads other malicious files onto the user's machine. It injects into many running processes, hooks several APIs of various loaded

modules. It injects itself into the explorer browser and connects to the IP address 27.54.193.102 through port 7171. It connects to the IRC server and launches the DDoS attacks.

The risk of the virus is not very high. It just launches itself into tasks and changes configurations. There weren't any noteworthy financial attacks by the worm. The virus had a huge impact in the US, it changed the sensitive information of people.

**2) *[1½ points]* Besides WireShark, what other tools are available to enable packet sniffing?**

1. **Describe at least two that are freely available on your favorite OS. (include URL)**
2. **What features do they offer over WireShark and vice versa?**

**ANS:-** WireShark is a very popular packet sniffer. It is available to install on all the major operating systems. WireShark puts the network card into promiscuous mode so that the computer picks up all network packets. Hackers regularly use Wireshark, and so many network administrators are wary of it. Wireshark system can capture packet traces from wired networks, wireless systems, and also Bluetooth. WireShark doesn’t gather packets itself. Even though Wireshark is not directly responsible for the most powerful part of its operations, the network interface of Wireshark makes it a winner. Some alternatives to WireShark are Savvius Omnipeek, Ettercap, Kismet, SmartSniff, EtherApe.

Ettercap :-A packet sniffer that is widely used by hackers and can give useful information to network defenders. It is available for free just like WireShark and can run on all major operating systems. Ettercap has been designed especially for hackers. Apart from hacking, it is also useful for network administrators. It can detect hacker activities and intrusion.

Ettercap uses the libcap open-source library to capture data packet traces. Ettercap itself can create several network attacks, which include ARP poisoning and MAC address masquerading. It can capture SSL security certificates, alter packet contents in transit, drop connections, and capture passwords. All these functions of Ettercap make it a great alternative to WireShark.

**Kismet :-** Unlike WireShark and Ettercap, kismet cannot capture packets in wired networks. It captures packets only in wireless networks and evades intrusion detection systems. The standard kismet tracks only wifi systems, but it can be modified to detect Bluetooth networks as well. The software is free but available only for Linux, Unix, and Mac OS. It is not available for Windows. Unlike other packet sniffers, kismet doesn't probe networks. Therefore, the detection systems cannot spot their activities. This property of kismet makes it a powerful tool for hackers who have access to a remote desktop with a network connection. Standard network monitoring systems will spot the presence of the device in which the software is up and running, but it won't see that the program is gathering data packets on the network. Kismet can also be used to reap network traffic dumps, which captures all the network packets along with data payloads.

**3) *[1½ points]* Another useful tool is called a port scanner (sniffer). It allows you to see what ports are active on your system (or someone else’s).**

1. **Choose your favorite OS and find one and describe it. (include URL)**

**ANS:-**

Nmap stands for Network Mapper, and it is the most popular network discovery and port scanner in history. It's a free and open-source application used by system administrators, DevOps, and network engineers for security auditing on local and remote networks. Available for Linux, Windows, and Mac OS, you can run it either by using the classic command-line terminal or by using a GUI interface. It is easy to install the Nmap on Ubuntu Linux.

### **Nmap features**

* Active Port scanning allows users to scan and discover open ports on specific networks/hosts.
* Host discovery lets the user identify potential hosts that are responding to network requests.
* OS detection allows users to scan and discover the operating system name and version, along with network details where the host is running.
* Application version detection is possible using Nmap to determine what kind of apps are running and along with the version number.

Installing Nmap on ubuntu is a very process. We have to fire up the terminal and then run the command, sudo apt-get install Nmap.

Nmap is a network mapper that emerged as one of the most popular, free network discovery tools on the market. The number of recent cyberattacks has focused attention on the type of network auditing that Nmap provides. Analysts have pointed out that the most recent Capital One hack, for instance, could have been detected sooner if system administrators had been monitoring connected devices. In this guide, we’ll look at what Nmap is, what it can do, and explain how to use the most common commands.

**4) *[1 point]* In general terms (i.e. don’t talk about JavaScript here) describe in detail what steps you would take to generate the digital signature.**

**ANS:-**

Upload the document into a browser-based wizard. Drag the Signature fields drop them into the document. The system emails a link to the signer(s)and requests their review and signature. The signer must authenticate his identity. It is done by simply logging into his email account to get access to the signed documents, or it could be more involved than that, depending on the level of security. Signers will need to answer detailed questions about themselves or provide a one-time passcode sent to them via a text.

The signer creates a Signing Password and chooses a font or free-hand his signature with a mouse, and digitally sign the document. Behind the scenes, SIGNiX API generates a public/private key pair—two digital keys that are bound together– for the signer, in turn creating a digital certificate, giving an individual a secure digital identity in the SIGNiX system. (This process happens almost instantly behind the scenes of every digital signing process.) At the time of signing, the user is authenticated against their identity, either implicitly or explicitly by typing their Signing Password again, and then a “fingerprint” is taken of the document. This long and unique string of characters is called a hash, and that hash is then mathematically tied to (encrypted by) the SIGNiX private key used for signing documents. The resulting signed hash is permanently embedded into the document alongside the public-facing digital certificate, IP address of the signer, transaction identification, and browser used to sign. That embedded hash of the document becomes the real digital signature because it provides tamper-evidence (or tamper-proofing) and the evidence that proves the document is valid and unique. Throughout the transaction, the audit trail records everything that happens - the creation of the document, sending of the document, emails that are sent, identity authentication, issuing of the digital certificate, the document’s hash, any changes that are made—everything. To the average eye, you’ll know the digital signature is valid when you see a green checkmark in the PDF when opening it in popular, dedicated PDF applications like Acrobat. Once a signer is finished signing, the signer’s digital certificate continues to work alongside the digital signature. Third parties can use it to verify the signature and the identity of the signer. The signature travels with every copy of the document. If someone changes the contents of the document after it’s been signed, the PDF viewer can detect it immediately. If that happens, you’ll see a yellow exclamation or a red “X” mark in the PDF, indicating that the signature isn’t valid, and the document may have been tampered with. Parties that are relying on this document don’t need to rely on a vendor to display that evidence online or even an internet connection!