NYU | SCHOOL OF PROFESSIONAL STUDIES

Cyber Defense

HIGH1-CE9074

Session 1

Introduction to Cyber Security

Let’s get ourselves introduced to some of the basic definitions and concepts of cyber defense.

What is Cybercrime?

Cybercrime is where digital assets (like desktops, tablets, cell phones, servers, images, email addresses and contents, credit cards, personal identities etc.) is the target of the crime. Computers – secretly connected through the internet - typically are used to initiate and carry out such crime.

What is Information Security?

Information security is all about “CIA” and no, this CIA does not stand for what you think it does. This CIA is about maintaining 1) **C**onfidentiality, 2) **I**ntegrity, and 3) **A**vailability. Confidentiality is also known as Military Security and Integrity is known as Commercial Security. Integrity can be subdivided into origin integrity vs data integrity. If the source of the data is altered then origin integrity is breached, if the content is altered then data integrity is breached.

Let’s see if you could spot the violations security in the following scenarios:

a) Jim reads a letter addressed to Sylvia and then burns the letter.
b) Becky remotely logs onto her school server as system administrator using stolen password, modifies a script (program) owned by system administrator, runs the script and crashes the server.

c) Sonia signs a check as Debbi and then cashes it.

d) Cynthia changes the amount of 100 to 1000 on the check she received from Alan and cashes it.

Cybercrime includes all of these when committed digitally.

Why is Cybercrime so prevalent?

Every day we hear news about another hacking story. Why is it so prevalent? Cybercrime is not prevalent because it is easy – it is, in fact, quite difficult to carry out – but because it can be done anonymously and often there is no consequence. Here are some of the reasons:

1. **Too many vulnerabilities**: If you leave a bunch of twenties scattered on a table at a shopping mall food court and walk away to refill your soda and take a while to come back, do you expect that some of the bills might disappear? That's pretty much the case with computers. Security holes in your smartphone, tablet, laptop, Wi-Fi, Alexa, smart TV, smart camera, smart alarm, smart toy, smart thermostat etc. are just too many entry points for hackers to explore. Some of them have got to have some security weaknesses, right?
2. **Quick and easy access from a distance**: Einstein said is right - "spooky action at a distance". Ok, I admit, Einstein was not talking about cybercrime, he was questioning "quantum entanglement" – a feature of quantum mechanics. Now, let's get back to cybercrime. The world is interconnected by the internet, and it is as easy for you to access any website thousands of miles away as it is for a hacker to connect to your machine from thousands of miles away if your machine has some cyber weaknesses.
3. **Uneven distribution of power**: A single person or a small group can gain enormous damaging power over a gigantic enterprise or even a country in a very short amount of time. This is impossible for any other types of crime. Hence, it is exciting and worth pursuing for some people.
4. **Anonymity**: The criminal can do everything without disclosing his/her identity. All you get is either an IP address or email – at best - sometimes not even that. You can certainly

rent a server in Tanzania from anywhere in the world and the IP address you expose is a Tanzanian IP address. Similarly, you can open a fake email address and start phishing. You can also buy information or identity on the darknet without the risk of getting caught.

5. **Lack of legal consequences**: If an attack comes from a person initiating from a machine in a foreign country, what legal action is available to go after that person? Not much. Also, to catch a hacker, often you must hack the hacker's computer which is not legal either. So, you don't.
6. **Substantial Reward**: What is the risk-reward ratio of stealing a cell phone? The risk of getting caught is very high but the reward is much less – may be $100. The risk-reward ratio in cybercrime is upside down. If you can hack into some site or some server, the reward you get is huge, meanwhile the risk of getting caught is low. Sometimes the reward is money, other times it is the satisfaction of revenge or even pure evil joy.

Examples of hacking

A "Hack" is basically a cyber-attack. These attacks either destroy assets or change and/or copy them. Hackers either extort for money or interrupt business processes or both. Examples of some big cyber-attacks:

Target: The hackers gained access to Target's network by first stealing credentials from a third-party heating and ventilation company and stole 40 million credit/debit cards and 70 million customer records.

Lenovo: Using a basic DNS redirect trick, Lizard Squad caused the Lenovo website to redirect to a slideshow of teen hackers nonchalantly posing in front of their webcams, set to the dulcet tunes of Breaking Free from the High School Musical Movie.

Stuxnet: Attack to Iran's uranium purification plant causing significant damage to the plant.

Who are the hackers?

Well, there are essentially 3 kinds of hackers:

1. People who do it for the money. These are criminal minded people.

   Demo: Please watch "Hack" from IBM:

   https://www.youtube.com/watch?v=nG36lKhy7ko

2. People who do it for fun, excitement or some noble cause.

   Demo: Please watch "The Wolf" from HP:

   https://www.youtube.com/watch?v=A0S1j7JGdsc

3. Government or State for political gain or power.

   Demo: Please watch "New Russian Hacking Efforts using SolarWinds"

   https://www.youtube.com/watch?v=3kpaV4FNzc0

How to implement Cybersecurity

Cybersecurity is the practice of protecting digital assets like desktops, networking devices. It involves processes not only to avoid attacks but also to deal with attempted as well as successful attacks. These processes require a substantial amount of people, budget, technology, hardware and software tools. It also involves training people about what “to do” and what “not to do”. For example, backup data regularly, use strong and lengthy passwords, don’t open email attachments coming from unknown sources are crucial steps but it totally depends on people’s cooperation and discipline. After all, a human being is the weakest link in the security chain. “Social Engineering” - the deceptive technique to manipulate individuals into giving away confidential or personal information that may be used for fraudulent purposes – is very effective and we must learn how to defend against such attacks.

Types of Attacks

There are two distinct types of hacking that can destroy your digital assets:

Outside-In Attack: When we think of hacking - this is what we typically think of. The attacker comes from outside, hacks into our machine and steals or damages our property. We will see an example of this attack shortly.

Inside-Out Attack: This is where the attacker's software is in your computer and it is establishing an outgoing connection to the hacker's machine. In recent days, this type of attack is happening more and more. How does the attacker's software make it to your machine? You might have clicked on an attached pdf or inserted an infected thumb drive or installed a software that also installed the hacker's software. In other words, an outside-in attack turned into an inside-out attack.

Let's watch the following video and see Kevin Mitnick, a famous hacker, in action with inside-out-attack:

https://www.youtube.com/watch?v=NtzZBTjKngw

What is Ethical Hacking?

Ethical hackers are the computer security experts who - with the permission of their clients - try to locate weaknesses and vulnerabilities of systems by carrying out a series of actions as if they are the malicious hackers. Parts of the ethical hacking are known as penetration testing, intrusion testing etc. Ethical Hackers are also known as “White Hat” or “Red Team”. Kevin Mitnick has become an ethical hacker. In his early days he hacked without permission but never made money or caused damages to systems he hacked.

Terminologies

Black Hat: Another term for “Real Hacker”. A real hacker breaks into computers with bad intentions. A black hat exploits security vulnerability for financial benefit or to steal or destroy data or to disrupt websites and networks.

White Hat: Another term for Ethical Hacker.

Grey Hat: These people will find venerability without permission (so they are really hacking) but instead of doing something bad they report them expecting monetary benefit.

Hacktivist: These people blend hacking and activism together for a political or social cause. Anonymous is a hacktivist group that is known for its various cyber-attacks against governments and corporations. They even attacked the Church of Scientology.

Malware: Short for malicious software. Malware can be subdivided into two categories:

a) **Virus**: A virus typically attaches itself to a program or file. When the infected application or file runs in the computer, the virus activates and executes in the system. A virus spreads when the infected program migrates through networks.
b) **Worm**: Unlike viruses, worms don’t attach to a file or program. They self-execute and self-replicate to spread from one machine to another.

Steganography: The Greek word “steganos” means “concealed” and “graphein” means “writing”. Steganography is the art of concealing an executable, or message within another image or video or file.

Phishing: A hacking practice of sending emails pretending to be from a reputable company to seduce people to reveal personal information, such as passwords and credit card numbers. Phishing can also be used to deliver Malware to a user’s machine. These malwares are often disguised by using steganography techniques.

Bot: A bot, shortened from “robot”, is a software that performs some automated task. There are many kinds of bots out there – chat bot, crawler bot etc. A google bot will crawl a website and discover all the urls. Websites have a file called robot.txt that indicates which urls are ok to crawl and which ones are prohibited but only good bots honor these restrictions.

Botnet: Several computers working together as bots. Botnet is typically used with evil intent.

Brute force attack: An attack where the hacker tries all possible passwords for a given username. to get access. Brute force attacks often do not work since most sites have limits on retries.

Denial of Service (DOS) Attack: Websites are meant to serve up pages. However, every website has a limit of handling traffic. If too much traffic hits a website, it will first slow down and finally will stop working. Hackers know this, and they attack a website with hundreds of thousands even millions of hits per second using BOTs until the site is down. This is called Denial of Service (DOS) Attack.

Distributed Denial of Service (DDOS) Attack: One problem that hackers face with denial-of-service attack is that they all come from the same IP or a handful of similar IPs. So, DOS attacks can easily be stopped by blocking those IPs. Hackers know this, so they turn to distributed denial of service attacks (DDOS). Where they rent or buy a big number of machines with different IP and different geographical location and run their BOTs from these machines. Now, it becomes impossible to block them since the website can’t distinguish which is a legitimate customer and which one is a BOT. One simple technique that works if block any IP that sends more than “x” number of hits per second knowing that a real user can’t possibly send many hits in a second – that’s humanly impossible.

Spoofing: Consider the following scenario. The CFO of the company got an email from the CEO to transfer funds to an account for the acquisition of another company. Acquisitions are top secret in a company, so it is not surprising that the CEO didn’t mention the specifics of the acquisition and the CFO is aware of an upcoming acquisition, expect the money transfer request to come, and he/she does the money transfer. The hackers got the money. How did this happen?

Well, using email software, hackers changed the sender's name, address, and source IP to make it look like the email is from a company's CEO. Alternatively, they gained access to the CEO's email account. Regardless of how they managed to send the email, the email passed through all the email filters and travelled to the CFO's inbox. This is also known as "CEO fraud" but could happen to anybody. These types of attacks are also known as "spear phishing" or "whale phishing".

Spyware: Spyware is software that gathers information about a person or organization without their knowledge. A spyware can turn on your microphone or record your keystrokes and send them over to the hackers.

Trojan Horse: A Trojan horse is a program that appears useful and harmless, but is, in fact, malicious. For example, a site might offer a nice text editor or image viewer but when you install this software it also installs a software that enables your microphone. Yes, such malware does exist.

What is Cyber Spying?

Cyber spying is the practice of obtaining personal information without the knowledge of the holder of the information. Cyber spying is not necessarily a crime, particularly if you agreed to it (by accepting the contract that you never read).

Not just the government, Google, Apple, Amazon, Microsoft, Facebook, Twitter, even your employer (assuming you are working somewhere) are spying on you. They know what websites you go to, what link you click on, what video you watch, what machine/phone you are using, what you like, what you don't like, what you buy, what you research on, what your email contains, your phone number, your address and many more.

All this information is mostly used for targeted ad placement and search relevancy. The data is also made available to people who own sites that are tracking data via their analytical tool. The data can also be sold for a fair price. More importantly, this data could be hacked (and has been hacked) putting you in danger.

So, how much effort did you put in to protect yourself from tracking? Let's find out, from your home computer open your browser and type the following url:

Click on Test Me. How exposed is your browser? What's your options to protect yourself?

Also, go to:

https://www.ghostery.com/

If you download their plug-in. It will tell you what tracking mechanism each site (or even your own company) is using as you move from one site to another.

Safe Searching

What search engines can you use if you don't like to be tracked as you search the internet?

Try:

https://duckduckgo.com/

What is the difference between MAC Address (Physical) and IP Address (Logical)?

Every network device has at least one network card, therefore, one unique physical address that is given to your network card during manufacturing. This is known as MAC (Media Access Control) Address. A MAC address is an absolute necessity for data communication of any kind.

Every network device also has at least one logical address that is assigned to it. This is called an IP address. IP addresses are necessary to locate your machine's vicinity and are necessary for inter-network communication.

So, it looks like both MAC addresses and IP addresses both are must haves, why? Which one is used when?

Let me give an analogy. Let's say, you want to talk to your classmate Jim who is in the same classroom as you are. All you need to know is his name (MAC Address) and you can start a conversation with him. You don't need to know Jim's home address (IP Address) to reach out to him. However, if Jim moved out to another city with his parents and you want to write him a letter, you must know his mailing address.

Like a mailing address, your machine's IP address can change from time to time as you move from one network to another, but you will still be reachable, and your MAC address will remain the same. IP addresses are used to locate where your machine is in the vast interconnected network systems, but a MAC address is used to physically identify your machine and deliver messages. Therefore, data communication starts with an IP address but there comes a point when it needs to be mapped to a MAC address for the data to reach the destination.

Let's imagine a message arrives to your home router with your machine's IP address. By looking at the IP address, your router knows this message does not need to go to any other network, there is a local machine that has this IP address, but it does not know exactly which machine has that. It sends a broadcast message (known as ARP message) asking all the machines to acknowledge if they have this IP address. Your machine, and only your machine, will reply to this message with its MAC address. Your router then, using the provided MAC address can send you the message.

Let’s now imagine that you reply to a message that came from the outside world. Your message contains the destination IP address and reaches your router. Your router, by looking at the IP address pattern, knows this message is for a remote machine and forwards it to the next router and this process goes on until the message arrives to the router of the destination machine. That destination router finds the MAC address of the destination machine using the same ARP technique described above and delivers your message.

MAC addresses and IP addresses together make all network communications (like email, web surfing, chatting) possible.

ipconfig (or simply “ifconfig” for Linux/MacOS)

ipconfig is a program that will show you your IP address and various network card’s that you have and their physical MAC addresses.

Windows Machine:

```
ipconfig /all
```

The above command will show your IP addresses and MAC addresses on a windows machine. The MAC address will be of xx-xx-xx-xx-xx-xx format.

Linux/MacOS:

```
ifconfig
```

The above command will show your IP addresses and MAC addresses on a Linux/MacOS machine. The MAC address will be shown in xx:xx:xx:xx:xx:xx format.

Demo:

Assuming you are running a windows machine, click the search icon on your machine and type: cmd

You will now be on the black command prompt.

Please run the following command on your computer:

```
ipconfig /all
```

a) How many IP addresses did you find on your machine? How many MAC addresses did you find on your machine?
b) What is your Default Gateway (router)? Note down the Default Gateway information.

On a MacOS, search for Terminal and select it. You will see a small new window. Type:

```
Ifconfig
```

You will see your IP addresses and MAC addresses.

What is ARP Cache?

Address Resolution Protocol (ARP) Cache is simply a map of IP addresses to MAC addresses in the memory of a machine. Instead of asking for the MAC address of the same IP address over and over, a machine simply caches the information.

Please run the following command on your machine’s command prompt (windows only):

```
getmac /v /fo list
```

How many MAC addresses does your machine have? What are they for?

Now, please run the following command prompt/terminal) :

```
arp -a
```

How many entries did you find?

What is ARP Spoofing/Poisoning?

In ARP spoofing, first, the hacker is already on a computer in your local area network (LAN). Then the hacker sends a falsified ARP message to the router that links the hacker's MAC address to your IP address. The hacker now starts receiving all incoming messages meant for you (like email messages, software updates) from the router. He then forwards these messages to your machine after keeping a copy.

Similarly, the hacker can also send falsified ARP messages to your machine that links hacker's MAC address to the router's IP address. Therefore, all outgoing messages from your machine will reach the hacker's machine and then the hacker forwards these messages to the router after keeping a copy.

This is known as a man-in-the-middle attack. Below is a link showing a man-in-the-middle attack using ARP spoofing:

https://www.youtube.com/watch?v=hI9J_tnNDCc

What is a Domain Name?

Humans are not good at remembering numbers, particularly long numbers like IP addresses. So, an easy to remember name like www.google.com is assigned to publicly available IP addresses of companies, government agencies and all entities interested. Domain names have to be purchased and registered.

What is DNS?

Domain Name System is a lookup process for converting alphabetic domain names into numeric IP addresses. For example: www.google.com may really mean an IP address: 172.217.7.4.

Some, DNS related tools:

Ping: The ping command is used to test the ability of the computer to reach a specified destination computer. The ping command sends four Internet Control Message Protocol (ICMP) Echo Request messages, by default, to the destination computer and waits for a response. Most public domains will not respond to ping but at least, you will resolve the domain name to an IP address.

Demo:

Type: ping www.nyu.edu

Now, ping your default gateway that you noted down from ipconfig /all

nslookup: nslookup is useful for looking up DNS record. Type:

Demo:

Type: nslookup www.nyu.edu

Now, nslookup your default gateway that you noted form ipconfig /all

Tracert (or traceroute for MacOS/Linux): Shows all the hops that your connection goes through to get to the destination. It tries each hop 3 times and shows the response time in 3 columns.

Demo:

Type: tracert www.bing.com

Now, tracert your default gateway that you noted form ipconfig /all

What is DNS Spoofing/Poisoning?

DNS Spoofing, also known as DNS Cache Poisoning, will map legitimate domain names to false IPs. For example, www.citibank.com will send you to a fake Citibank site. It will look and feel exactly like Citibank's site. You will type in your user id and password and it will probably say something like "we are experiencing technical difficulty…..blah blah blah". The hacker, meanwhile, will use your user id and password to transfer all your money to some offshore account and you will probably never see that money.

DNS spoofing is easy to accomplish when you have already done a man-in-the-middle attack using ARP spoofing. The following demo shows how they work together:

https://www.youtube.com/watch?v=Y3j-rlA0CbE

Introduction to Cyber Attack

Steganography Demo

At this point, we are going to learn how steganography can be done at a very basic level. We will learn how to hide an executable inside an image and then how to extract the executable from the image.

a) Assuming we have an image named cat.jpg and an executable putty.exe in the same folder. We will first zip up the image in putty.zip. Then from the command prompt we will run:

```
copy /b cat.jpg + putty.zip
```

This will copy the zip inside the image. You can still view the image without any problem.

Now, Open cat.jpg with a unzipping program like 7-zip or WinZip. You will see the executable inside the image. You can click on the executable and it will popup. You can also extract it out.

Putty is a harmless executable used to connect with other machines. So, nothing to worry about.

b) Assuming, you have an image named marbles.bmp, run s-Tools.exe. Drag and drop marbles.bmp inside s-Tools. Now, drag and drop putty.exe inside the image of marbles. A popup will ask for a "passphrase" and verify it. Enter any passphrase you like. A new frame will popup with the same image and title would be "hidden data". Right click on it, select "Save as.." and name it marbles_danger.bmp. Close s-Tools. Open marbles_danger.bmp and it will appear harmless but it has putty.exe embedded in it that you can't see.
Open s-Tools again and drag and drop marbles_danger.bmp in it. Right click and select reveal. Enter your passphrase that you entered before and verify it. A pop-up will show putty.exe. You can right-click on it and select "Save as…" putty.exe on your hard-disk.

Shellshock Attack Demo

Shellshock, also known as Bashdoor, is a security bug that allows the attacker to remotely issue commands on the server, also known as remote code execution.

If time permits, we will see a demo of a Shellshock attack.

Congratulations!! You have done your first couple of ethical hacks.

Homework 1

1. Run IPConfig /all on your home machine and take a screenshot (it is ifconfig on Mac and Linux). How many MAC addresses do you have? What are they for? What is your default gateway (router)?
2. Can you get to your router (default gateway) using your browser and router's IP address? If so, is your router password protected? If yes, is it using a default password (google search default password for your type of router and try it)? Speak to your parents if you see no password or default password.
3. ping www.google.com? If it never stops, press control+C to stop it. Does it respond? What IP do you get?
4. nslookup www.google.com. What IP address does it return? Does it match with the IP returned by ping?