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.) are the target of the crime. Computers – secretly connected through the internet - typically are used to initiate and carry out such crimes.

What is Information Security?

Information security is all about the "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. Furthermore, There are two types of Integrity: a) origin integrity b) data integrity. Altering the data source constitutes an origin integrity breach; however, changing the content constitutes a data integrity breach. For example, if I hear from a friend about highjacking an Afgan plane, but I told you that I heard it on CNN, that's an example of an origin integrity breach. On the other hand, if I see on CNN that people are sitting on top of an Afgan plane, but I tell you that Afgan's bombed a plane, that would be an example of a data integrity breach.
Let's see if you could spot the violations of security in the following scenarios:

a) Jim reads a letter addressed to Sylvia and then burns the letter. (CA)

b) Becky remotely logs onto her school server as a system administrator using a stolen password which modifies a script (program) owned by a system administrator, runs it, and crashes the server. (CI(Data)A)

c) Sonia signs a check as Debbi and then cashes it. (I(Source) A)

d) Cynthia changes the amount from 100 to 1000 on the check she received from Alan and cashes it. (I(Data) A)

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 challenging to carry out – but because people can do it 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.
2. **Quick and easy access from a distance**: Einstein said it correctly - "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 internet interconnects the world, 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 device has some cyber weaknesses.
3. **Uneven distribution of power**: A single person or a small group can gain enormous damaging control over a gigantic enterprise or even a country in a concise amount of time. This is impossible for any other type of crime. Hence, it is exciting and worth pursuing for some people.

4. **Anonymity**: The criminals can do everything without disclosing their identity. All you get is either an IP address or email – at best - sometimes not even that. For example, you can certainly rent a server in Tanzania from anywhere globally, and the IP address you expose is Tanzanian. 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, 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 – maybe $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 enormous. 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 a cyber-attack. These attacks either destroy assets or change them or copy data from them; sometimes, they do it all. Hackers either extort money or interrupt business processes or both. Examples of some significant cyber-attacks:

Log4JShell: Since Dec 2021, a deadly attack surfaced related to logging user information. In this attack, the hacker, instead of valid data, sends a lookup command (back to the hacker's site) to the victim's application that logs this command using Log4J – a logging software. Log4J executes this lookup command and downloads software that connects to the hacker's server. As a result, the hacker now has complete control of the victim's machine. Although the patch for this issue has been published, organizations are still struggling to implement it to everyone needed.

Solarwinds: Solarwinds' Orion software allows information technology departments to look on one screen and check their whole network: servers, printers, firewalls – everything. Hackers -

believed to be directed by the Russian intelligence service, the SVR - hacked into Solarwinds' servers used Orion's routine software update to slip malicious code into Orion's software. Thousands of American organizations – including some government agencies - downloaded and applied the update, and then the hackers were able to carry out a massive cyberattack against these American organizations.

Colonial Pipeline: Colonial Pipeline learned it was in trouble on May 7, 2021, when an employee found a ransom note from hackers on a control-room computer. Joseph Blount, CEO of Colonial Pipeline Co., authorized the ransom payment of $4.4 million because executives were unsure how badly the cyberattack had breached its systems and, consequently, how long it would take to bring the pipeline back.

Turkish Hacktivists: Turkish activists took over the social media accounts of U.S. journalists and used them to post messages praising Turkish President Recep Tayyip Erdogan, according to a prominent cybersecurity intelligence firm, which shared photos of the compromised accounts with CNBC. The attacks targeted Bloomberg, The New York Times, and Fox News journalists.

Who are the hackers?

Well, there are essentially three kinds of hackers:

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

   Demo: Please watch what happened to Colonial Pipeline:

   https://www.youtube.com/watch?v=YRwEjeFv99k

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 do it 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 and networking devices. It involves processes not only to avoid attacks but also to deal with attempted and 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 "not to do." For example, regularly backup data, using strong and lengthy passwords, and not opening email attachments from unknown sources are crucial steps, but it 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 – is efficient, and we must learn how to defend against such attacks.

Here is the general guideline for implementing cyber security:

1. Asset Identification	Get a total inventory of digital assets. Even at home, this is a difficult task.
2. Threat Identification	Classify threats by category. This is a tedious process and requires skills and in-depth knowledge of cyber security
3. Vulnerability appraisal	For each threat identified in step 2, determine which assets are vulnerable to it and how.
4. Risk assessment	All known vulnerabilities are not rated equal. Calculate the likelihood and impact.
5. Risk mitigation	Decide what to do with the risk starting from the highest rating. Then, go down the list one after another.

Cyberattacks

Let's watch the following video and see Kevin Mitnick, a famous hacker, in action with a cyberattack:
https://www.youtube.com/watch?v=NtzZBTjKngw

What is Ethical Hacking?

Ethical hackers are the computer security experts who try to locate weaknesses and vulnerabilities of systems by carrying out a series of actions as malicious hackers with their clients' permission. Parts of 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.

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, stealing or destroying data, or disrupting websites and networks.

White Hat: Another term for Ethical Hacker.

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

Hacktivists: Blend hacking and activism for a political or social cause. Anonymous is a hacktivist group 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. This malware is often disguised by using steganography techniques.

Bot: A bot, shortened from "robot," is software that performs some automated task. There are many kinds of bots– chatbot, crawler bot, etc. For example, 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. A botnet is typically used with evil intent.

Brute force attack: The hacker tries all possible passwords for a given username to gain access. Brute force attacks often do not work since most sites limit retries.

Denial of Service (DOS) Attack: Websites are meant to serve up pages. However, every website has a limit to handling traffic. If too much traffic hits a website, it will first slow down and 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 a Denial of Service (DOS) Attack.

Distributed Denial of Service (DDOS) Attack: Hackers face a problem with a denial-of-service attack because 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, turning to distributed denial of service attacks (DDOS). They rent or buy many machines with different IPs and different geographical locations and run their BOTs from these machines. It becomes impossible to block them since the website can't distinguish between a legitimate customer and 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 company's CFO got an email from the CEO to transfer funds to an account to acquire 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. Unfortunately, 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 was 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 traveled to the CFO's inbox. This is also known as "CEO fraud" but could happen to anybody. These 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. 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 valuable and harmless but is, in fact, malicious. For example, a site might offer an excellent text editor or image viewer, but it also installs software that enables your microphone when you install this software. So, yes, such malware does exist.

What is Cyber Spying?

Cyber spying is the practice of obtaining personal information without the knowledge of the data holder. Cyber spying is not necessarily a crime, notably if you agreed to it (accepting the contract 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 mainly used for targeted ad placement and search relevancy. However, the data is also available to people who own sites 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 are 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) uses 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/

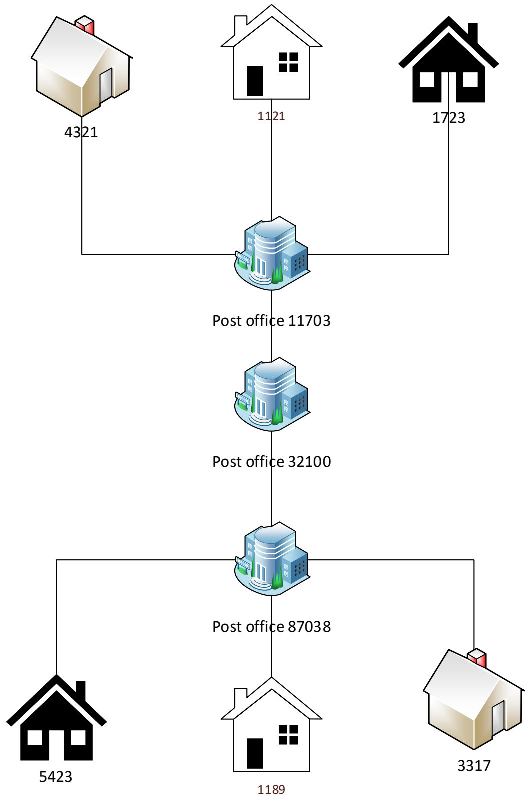
Introduction to Computer Science

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

Every network device has at least one network card with a unique id known as MAC (Media Access Control) Address. A MAC address is an absolute necessity for data communication of any kind.

Every network device is also assigned at least one logical Address known as an IP address. IP addresses are necessary to locate your machine's vicinity and are necessary for inter-network communication.

An analogy of MAC address and IP address is hard to come up with but let's try it. First, let's imagine a dramatic change in the postal system. Every home has been assigned to a PO Box number.



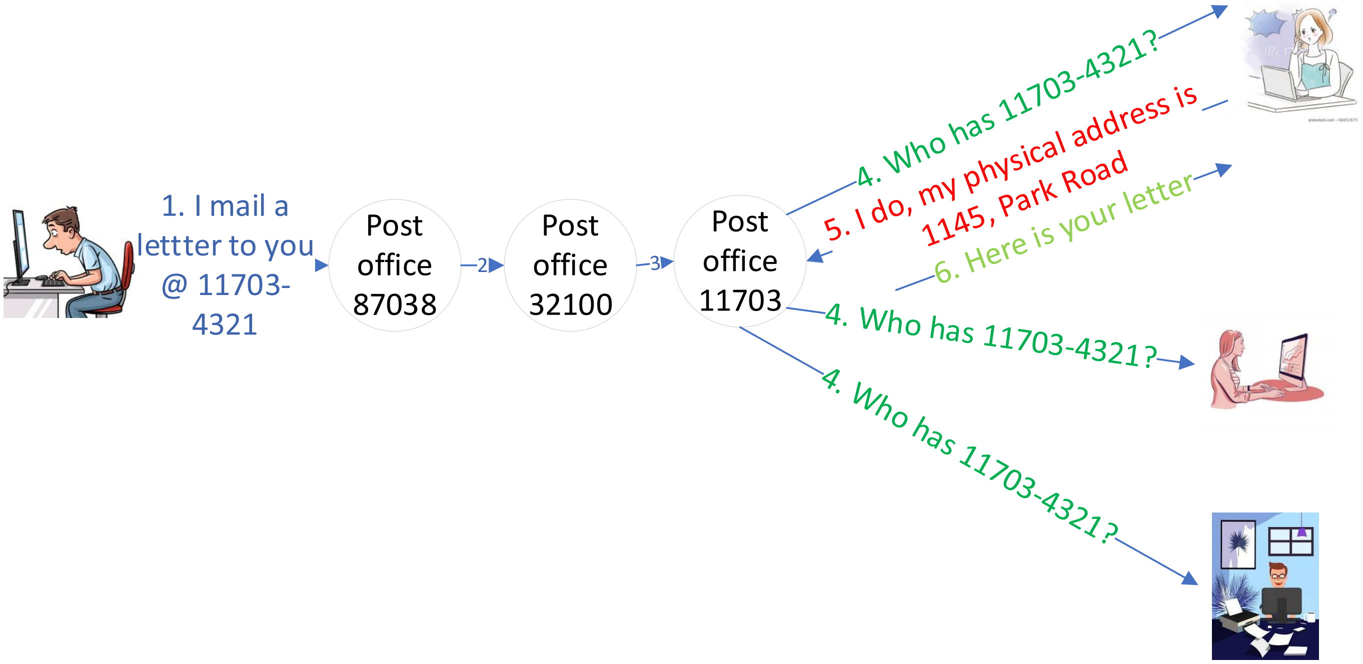
You don't have to write the full address on your mail anymore, simply zip code followed by the recipient's PO Box number.

Here is an example:

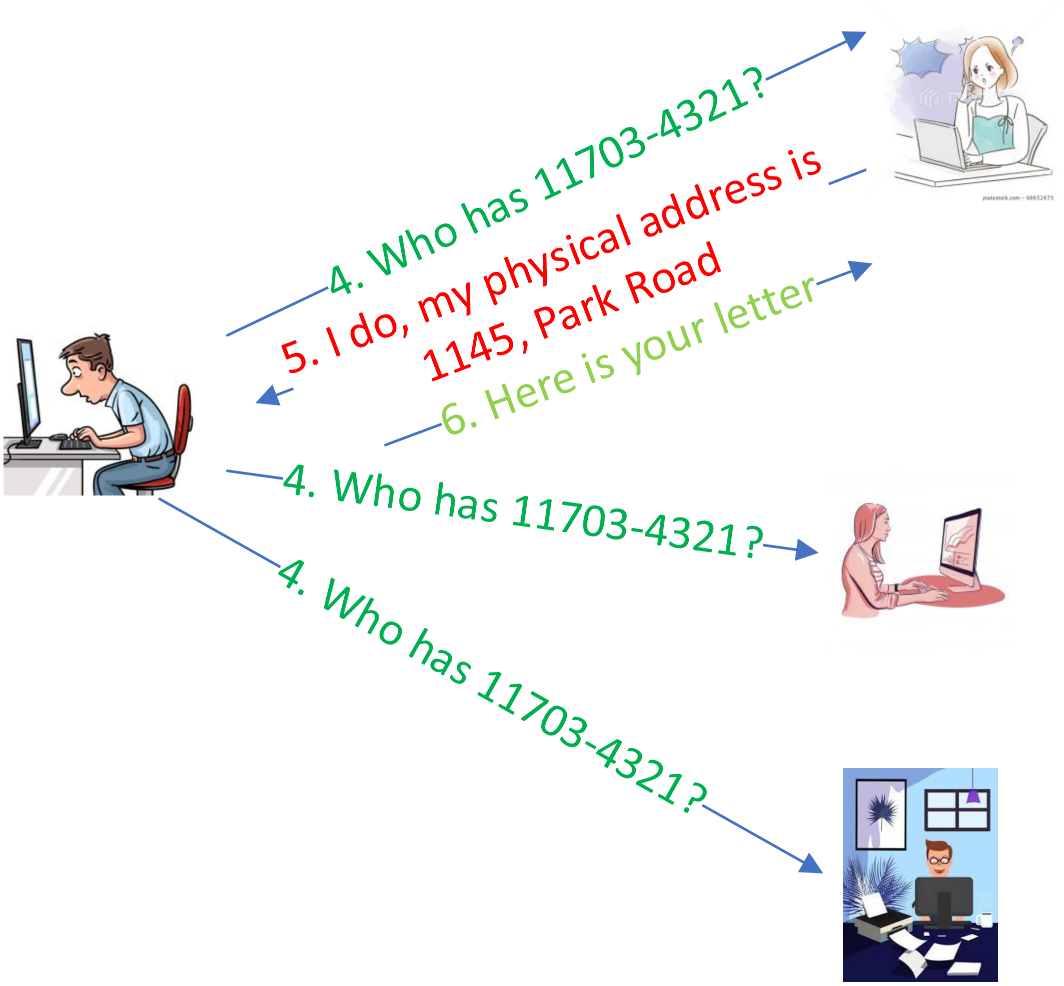
To: John Doe

11703-1143

That's it. When the mail arrives at post office 11703, the post office will email everyone in the neighborhood asking, "Who has PO Box 4321?" Someone will answer: "I do. My physical address is 1145 Park Road." And the post office will gladly deliver the mail to that address.



Let's now imagine that I live in your neighborhood and wish to send you a letter but only know your PO Box number. Do I need to go to a post office to find you? Instead, I can send an email to everyone in the neighborhood "who has the PO Box number 4321?". You will come back with a response containing your physical address, and I will give you the letter to you.



In the case of computers, the Zip Code & PO Box number combination, like 11703-4321, is your IP address, and your physical address, like 1145 Park Road, is the MAC address. The IP address is required to route the message to the correct network (post office), and the MAC address is necessary for the last hop (destination computer).

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

getmac and ipconfig (or "ifconfig" for Linux/MacOS)

a) getmac is a program (windows only) that shows your MAC addresses:

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

```
getmac /v
```

How many physical addresses (MAC addresses) does your machine have? What are they used for?

b) 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 device 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 see on your device?

b) What is your Default Gateway (router)? Note down the Default Gateway information.

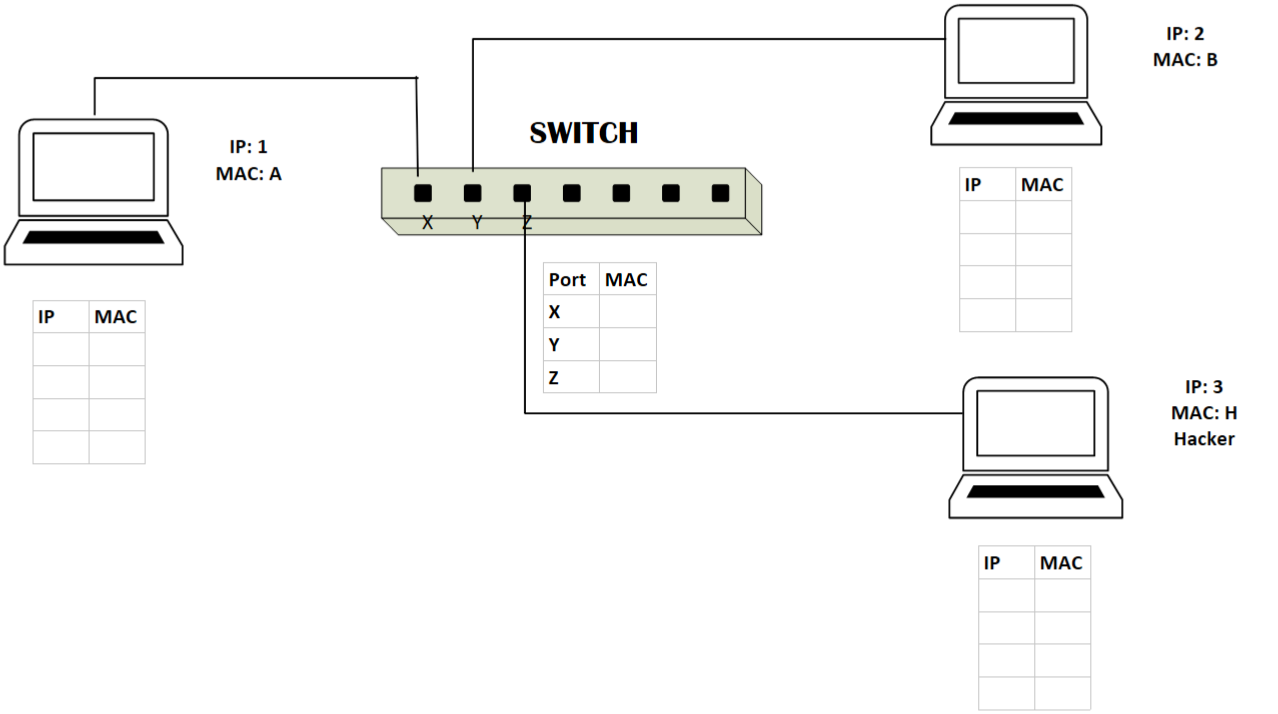
On a MacOS, search for Terminal and select it. You will see a small new window. Type:

```
Ifconfig
```

You will see your IP addresses and MAC addresses. Of course, on MacOS, you can go to system preferences and the network and find all the information.

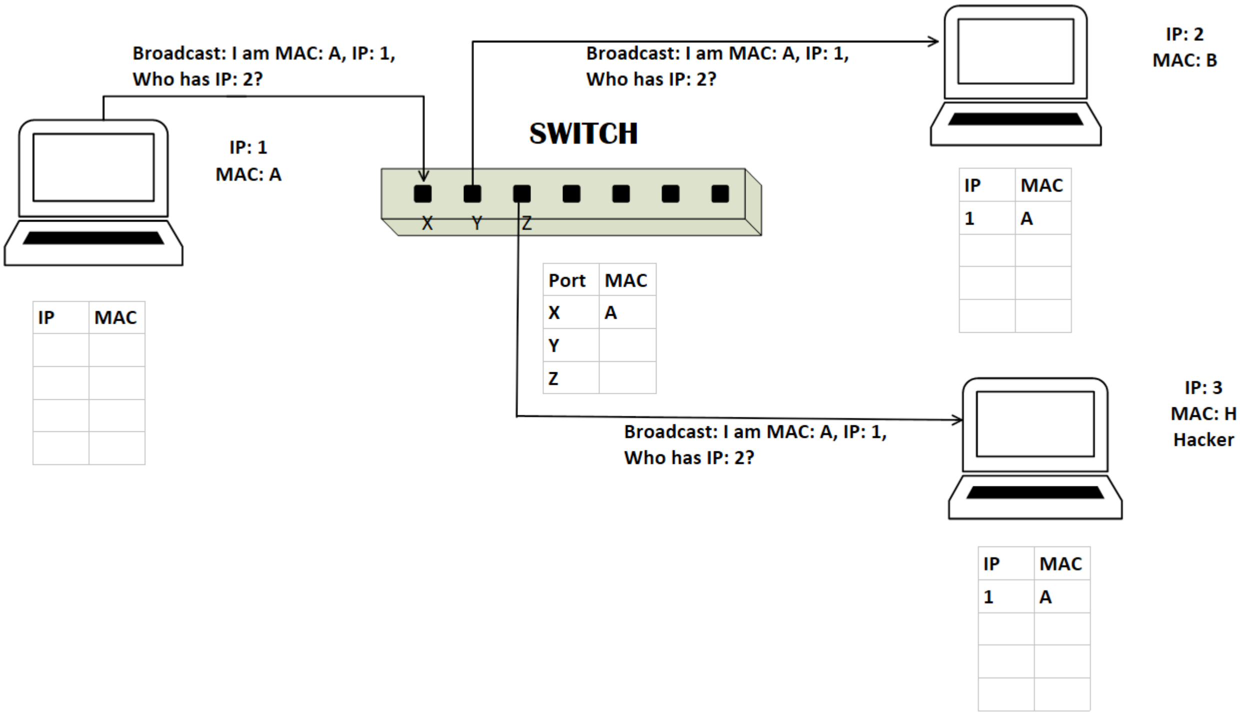
What is ARP Cache?

In our previous example, in the second case, I, being in your neighborhood, asked, "Who has PO Box 1143?" Computers become neighbors when they are connected via a switch as follows:



Computers in the same neighborhood (network) get to know each other's physical address (MAC Address) by using a protocol. That's called Address Resolution Protocol (ARP). In this protocol, an ARP request is sent to everyone in the neighborhood asking for the MAC Address of an IP address, and an ARP reply is received from the machine that has that IP Address.

Here is an ARP request:


Broadcast: I am MAC: A, IP: 1,
Who has IP: 2?
Broadcast: I am MAC: A, IP: 1,
Who has IP: 2?
IP: 2
MAC: B
IP: 1
MAC: A
SWITCH
X
Y
Z
Broadcast: I am MAC: A, IP: 1,
Who has IP: 2?
IP: 3
MAC: H
Hacker

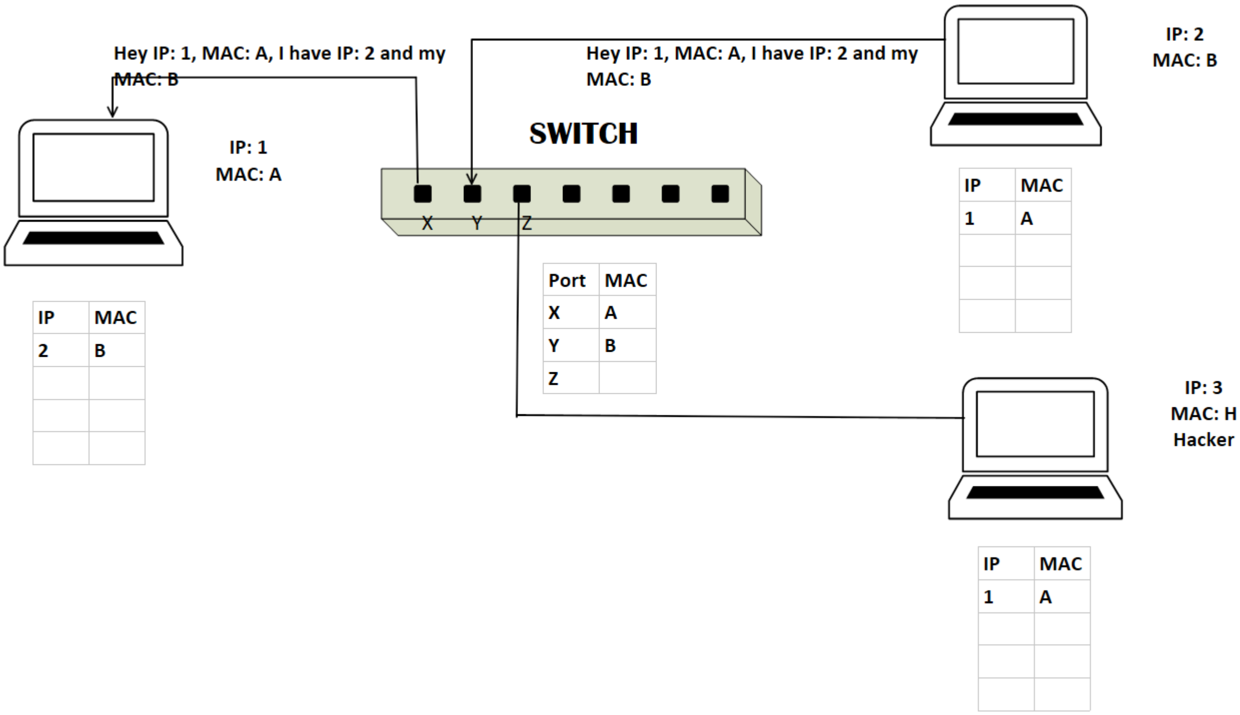
IP	MAC

Port	MAC
X	A
Y	
Z	

IP	MAC
1	A

IP	MAC
1	A

Here is an ARP reply:


Hey IP: 1, MAC: A, I have IP: 2 and my
MAC: B
Hey IP: 1, MAC: A, I have IP: 2 and my
MAC: B
IP: 2
MAC: B
IP: 1
MAC: A
SWITCH
X
Y
Z
IP: 3
MAC: H
Hacker

IP	MAC
2	B

Port	MAC
X	A
Y	B
Z	

IP	MAC
1	A

IP	MAC
1	A

Once a reply is obtained, the switch and other machines can cache this information for future use. This is called ARP Cache.

ARP Cache is simply a map of IP addresses to MAC addresses in the memory of a machine. Instead of repeatedly asking for the MAC address of the same IP address, a device caches the information.

Please run the following command prompt/terminal) :

```
arp -a
```

How many entries did you find?

Ping: The ping command tests the ability of the computer to reach a specified destination computer. The ping command sends Internet Control Message Protocol (ICMP) Echo Request messages, by default, to the destination computer and waits for responses. If Ping is used to locate another machine on the same network, Ping will use the ARP protocol to find the MAC address of another machine on the network. To ping anther machine on your network, type the following:

```
ping <the other machines IP Address>
```

You will get a response from the machine.

In my case, my machine’s IP is 192.168.1.113, and I am looking for another machine with IP: 192.168.1.51 on the same network. I will type:

```
Ping 192.168.1.51
```

Now type:

```
apr -a
```

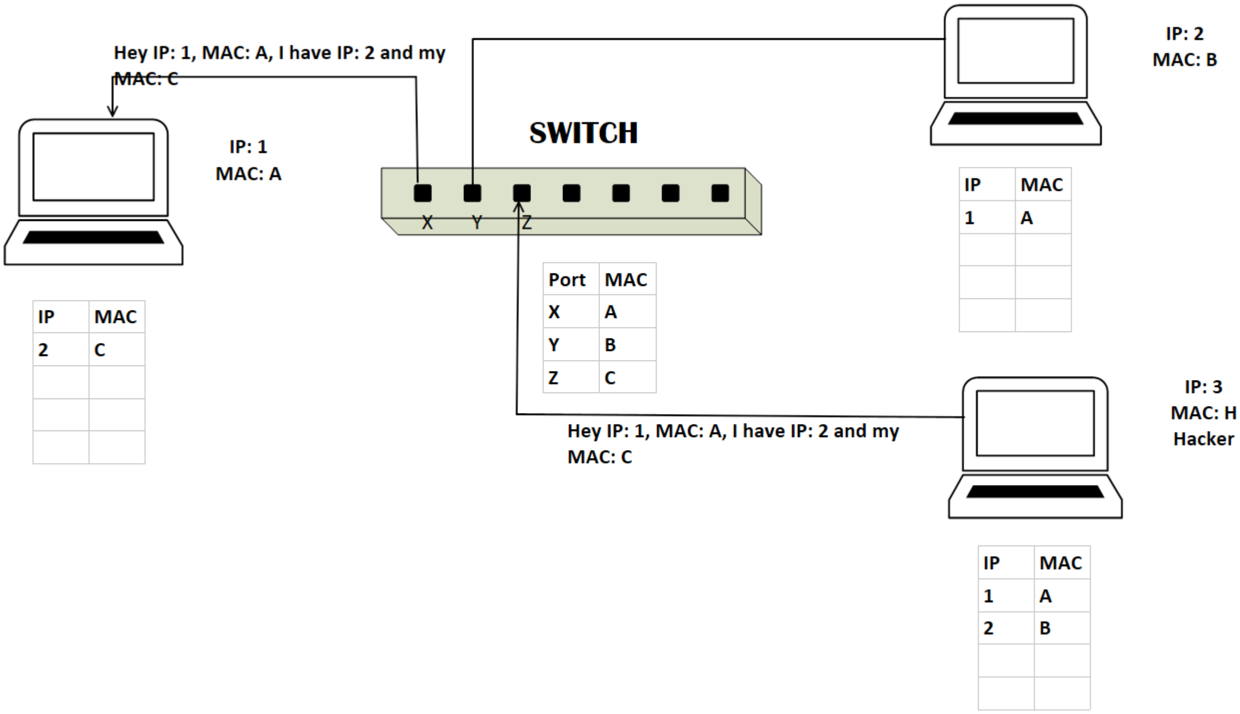
Do you see the MAC Address of the other machine listed? In my case, I do see the MAC Address of 192.168.1.51 cached in my APR cache.

Demo: show ARP requests and responses in Wireshark.

What is ARP Spoofing/Poisoning?

Did you notice a flaw in the ARP protocol? You don't have to prove that you own the IP address. Instead, you have to claim that you do. Hackers take advantage of this flaw, and it is called ARP spoofing.

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 my machine via the switch that links the hacker's MAC address to your IP address.


Hey IP: 1, MAC: A, I have IP: 2 and my MAC: C
IP: 1
MAC: A
SWITCH
X
Y
Z
IP: 2
MAC: B
Hey IP: 1, MAC: A, I have IP: 2 and my MAC: C
IP: 3
MAC: H
Hacker

IP	MAC
2	C

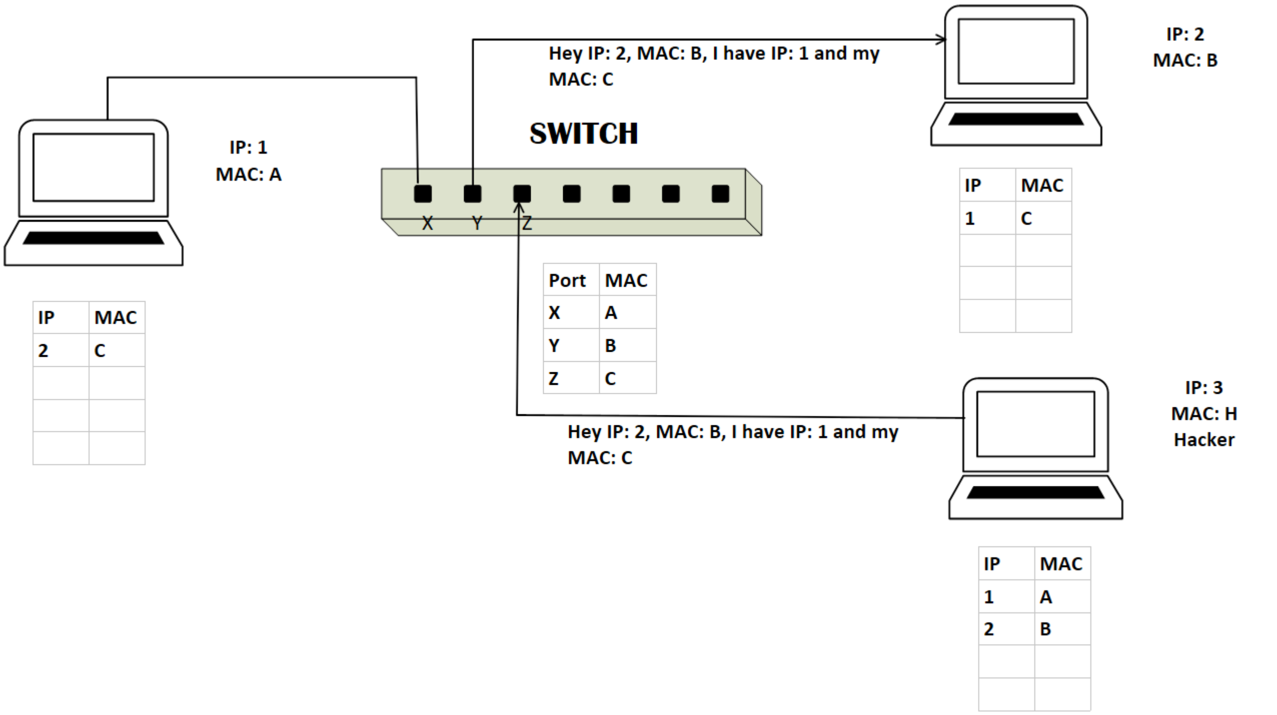
Port	MAC
X	A
Y	B
Z	C

IP	MAC
1	A

IP	MAC
1	A
2	B

The hacker now starts receiving all incoming messages meant for you (like email messages software updates) from me. He then forwards these messages to your machine after keeping a copy.

Similarly, the hacker can also send a falsified ARP message to your machine that links the hacker's MAC address to my IP address.


Hey IP: 2, MAC: B, I have IP: 1 and my MAC: C
IP: 2
MAC: B
IP: 1
MAC: A
SWITCH
X
Y
Z
Hey IP: 2, MAC: B, I have IP: 1 and my MAC: C
IP: 3
MAC: H
Hacker

IP	MAC
2	C

Port	MAC
X	A
Y	B
Z	C

IP	MAC
1	C

IP	MAC
1	A
2	B

Therefore, all messages from your machine to my machine will reach the hacker's machine, and then the hacker forwards these messages to me 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

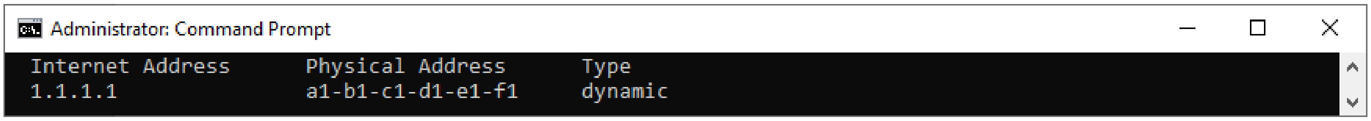
Demo:

Using a python tool called scapy, I ran the following python code from another machine (IP: 192.168.1.113):

```
a=ARP()
a.show()
a.psrc='1.1.1.1'
a.hwsrc='a1:b1:c1:d1:e1:f1'
a.pdst= '192.168.1.51'
a.hwdst='ff:ff:ff:ff:ff:ff'
send(a)
```

By the way, my current machine's IP address is: 192.168.1.51

And, "ff:ff:ff:ff:ff:ff" MAC address means it is a broadcast
message to all machines in my network.
On my machine, I then ran:
arp -a
Sure enough, my arp cache is poisoned, and the entry is now
on my arp cache:



```
Internet Address      Physical Address      Type
1.1.1.1               a1-b1-c1-d1-e1-f1     dynamic
```

What is a Domain Name?

Humans are not good at remembering numbers, particularly long numbers like IP addresses. But people are excellent at remembering names. So, www.yahoo.com and www.nike.com are assigned to publicly available IP addresses of companies and government agencies. These are domain names. Domain names have to be purchased and registered.

What is DNS?

Domain Name System (DNS) is a lookup process for converting domain names into numeric IP addresses. So, for example, www.google.com may mean an IP address: 142.250.81.228.

DNS related tools:

Ping: Ping can also be used to find a public domain’s IP address. Most public domains will not respond to ping for security reasons, but you will find the IP address of the domain regardless.

Demo1:

Type: ping www.nyu.edu

nslookup: nslookup helps lookup DNS records.

Demo:

Type:

Nslookup www.google.com

The IP address for www.google.com is given by my DNS server and shows up in the non-authoritative section since my DNS server is not the authority that maintains this record.

Let's do another example this time; I am trying to figure out the “authority” (-type=ns) for google’s domain.

nslookup -type=ns www.google.com

Turns out it is ns1.google.com

Finally, let’s do another lookup for www.google.com:

nslookup www.google.com ns1.google.com

We will get the same IP as before, but the reply will be authoritative(does not say that the answer is non-authoritative) since the authority which maintains this record is ns1.google.com, and we reached out to the authority this time.

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

Demo:

Type:

tracert www.bing.com

Now, tracert the default gateway that you noted from 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. However, it will look and feel precisely 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.

Demo: show DNS spoofing of www.facebook.com by modifying /etc/hosts file (seed class demo in private mode)

Steganography Demo

At this point, we will learn how steganography can be done at a fundamental level. First, we will learn how to hide an executable inside an image and 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 an unzipping program like 7-zip or WinZip. You will see the executable inside the image. You can click on the executable, and it will pop up. You can also extract it out. Putty is a harmless executable used to connect with other machines. So, we have 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 the title would be "hidden data." Right-click on it, select "Save as.." and name 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 the passphrase that you entered before and verify it. A popup will show putty.exe. On your hard disk, you can right-click on it and select "Save as…" putty.exe.

Homework 1

1. Run IPConfig /all on your home machine (it is "ifconfig" and no "/all" on Mac and Linux). How many physical(MAC) addresses do you have? What are they used for? How many of them have IPv4 Addresses? 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 address does it return?
4. nslookup www.google.com. Check the Non-authoritative answer section. What IP addresses does it return? Two? One is IPv6 (alphanumeric), and the other is IPv4(numeric)? Does IPv4(numeric) one match with the IP returned by ping? It should.
5. Google search for "Metasploit project was hacked" and find out what kind of attack the Metasploit project suffered from. Does it sound familiar? Explain.
6. What is DNSpionage? How to stop it? Watch the following video before you answer it in your own words:
   https://www.youtube.com/watch?v=H1mwVTmFlNk&t=57s