Introduction to Social Engineering

Social Engineering

First Call to Deer Park Store:

Lisa: "Game City, Deer Park, this is Lisa."

Hacker: "Hi Lisa, this is Mike, Mike Miller. Listen, I bought a Nintendo Switch a few weeks ago; I didn't even open the box. Can I exchange it for a PS4?"

Lisa: "When did you buy it? Within two weeks? Then yes."

Hacker: "Oh no, it's more than a month."

Lisa: "Sorry, I can't help you with that, you have to talk to our manager."

Hacker: "Ok, what's your manager's name?"

Lisa: "Jim Wilson, he comes to work around 10."

Hacker: "Thanks, I will call back after 10. Have a good day."

Lisa: "Thanks. Bye."

Second Call to North Babylon Store, the first call was to Deer Park store, they are nearby:

Becky: "Game City, North Babylon. Becky speaking. How can I help you?"

Hacker: "Hi, Becky. This is Jim Wilson from Deer Park store; I am the new manager here."

Becky: "Hi Jim, what can I do for you?"

Hacker: "Can you please check if you have any used Zelda? I have a customer here who wants it, but I am out; I have three new."

Becky: "Yes, we have two used."

Hacker: "Wonderful, I will send him over to your store."

Third Call to North Babylon Store Again:

Becky: "Game City, North Babylon. Becky here. How can I help you?"

Hacker: "Hey Becky, this is Jim again from Deer Park store."

Becky: "Hi Jim. What's up?"

Hacker: "Is your system working? Mine is down."

Becky: "Let me check. Yeah, mine is working fine."

Hacker: "Listen, I have a senior citizen here, Bill Murphy; he has three grandkids, he buys games for them. He says he has a reward card with us. Can you please look him up?"

Becky: "Sure, What's his name again? Do you have his address?"

Hacker: "Bill Murphy, 78 Cooper Lane, 11703."

Becky: "Got it. Yeah, he has a reward card."

Hacker:" Good, thank you. What's his Mid?"

By the way, MID stands for "Member ID," a term used in Game City, and the hacker knows it.

Becky: "118456".

Hacker: "Thanks. Bill says he has his credit card on file."

Becky: "Yes."

Hacker: "Bill forgot to bring his wallet; he didn't think he would need it. My system is still down. Would you please read the card number to me? I have to write down the transaction on paper for now; what a pain in the neck!"

Becky hesitated for a moment and then said,

"I am not sure if I am allowed to do that."

Hacker: "You are right, generally this is not a good idea, but my system is down, this is how we have to do it for now, trust me, I am the manager, I know how things work."

Becky: "Ok, it is 5272 1434 2323 1102, expiry 10/20, SC 113."

SC stands for security code, another term that Game City uses.

Hacker: "Got it, thanks a lot Becky. I will process his payment as soon as the system comes back up. I called tech support three times already; they are working on it. Ok, thanks again, bye for now."

Becky: "Good luck Jim. Bye".

What went wrong here?

The first call was innocent and was to gather information about the manager. The second call was carefully placed to convince her that he is indeed the manager of the other store and looking out for the company's best interest. At this point, he is bound to receive higher acceptance from a fellow employee, particularly someone of a lower rank. Hacker's last call gained sympathy from Becky since a system malfunction is not uncommon and drives everyone crazy. Moreover, Jim seemed to be looking out for a senior citizen who has the potential of being a loyal customer for years to come.

How should the company protect this from happening in the future?

a) The first problem here is that the company is storing and retrieving credit card information. That should never happen. They should hold the credit card information in a very secure system and receive a token instead. The token and last four digits can be kept in the store's system. The token should be used for future transactions, and the card's last four digits can be displayed and printed but nothing more. This way, even if the token is shared with other stores, no credit card information is leaked.

   This whole process of securing credit card information is known as "PCI (Payment Card Industry) compliance."

b) Employees should be trained not to share customer information with anyone else without proper identity verification of the seeker. Formal verification may include hanging up the phone politely, calling back the other store, and asking for the manager.

PCI Compliance

Companies that deal with credit cards must follow the Payment Card Industry Data Security Standard (PCI DSS). PCI Compliance has the following goals:

1. Building and maintaining a secure network.

2. Protect Cardholder Data.
3. Maintain a Vulnerability Management Program.
4. Implement Strong Access Control Measures.
5. Maintain an Information Security Policy.

PCI Compliance is hard to implement. For this reason, many companies do not store credit card information at all; they only hold the token and use a third-party reliable PCI compliance vendor to keep the actual card information. This way, companies become PCI compliant by simply using an excellent third-party tool – a perfect example of risk transfer.

Social Engineering again!

It is 8:15 on a Tuesday morning.

A young lady called the front desk, posing as a vendor, asked if anyone in accounts payable was in yet. It turns out "Carl Davis" is in, and his extension is "15-1023".

First Call:

Carl: "Accounts payable, Carl speaking."

Hacker: "Good morning Carl, this is Ruby Brown from the helpdesk. We are getting reports of some network problems on your floor, is anybody in your department impacted?"

Carl: "No one else in my department is in yet, but I am logged in to my computer, and I don't see any problem."

Hacker: "Good, good, glad to hear that. Listen, while I have you on the phone, can you please quickly check what port you're connected to?"

Carl: "I have no idea what you are talking about."

Hacker: "Ok, no problem. Check the back of your computer. Do you see a network cable connected to your computer?"

Carl: "Hold on, let me see…..yes, I see it."

Hacker: "Good, now trace it back to where It's plugged in on the wall. Is there a label on the jack?"

Carl: "Oh boy, I have major back pain, hang in, let me squat down slowly."

A few moments later, he returned to the phone and said,

"It says LTP 35".

Hacker: "Good, that's what I have here too. Thank you. Listen, if you have any computer problem call me back, please. I will give you my cell number it is 631 812 1020. You got it?"

Carl: "Yeah, I wrote it down, thanks. What's your name again?"

Hacker: "Ruby Brown."

Carl: "Ok, thanks, Ruby."

Hacker: "Bye Carl, thanks for your help again."

Friday, three days later, 10:30 AM.

Second Call:

Chris: "NOC, Chris speaking."

Hacker: "Hi Chris, this is Cindy Wilson from PC support. I'm in Carl Davis's office in Accounts Payable. We are troubleshooting a cabling problem. Can you please disable his network port LTP 35? I will be done in a few minutes and will call you back to enable it."

Chris: "Who is your manager?"

Hacker: "Denis Bradley."

Chris: "Ok, can I have your phone number?"

Hacker: "Sure, I am never at my desk, call me on my cell, 631 812 1020."

Chris: "Thanks. It's done."

Hacker: "Thanks, Chris. Bye."

Third Call:

A few minutes later, the hacker's phone rings. She was expecting this call. She picked up and said:

"Ruby Brown, helpdesk."

Carl: "Hi, Ruby. This is Carl from Accounts Payable. Remember you called me about some network problem a few days ago?"

Hacker: "Yeah, I know, we've got a problem going on right now. Are you impacted?"

Carl: "Yes, I can't connect to anything. I have so much work to do here. It's Friday; I have plans this evening."

Hacker: "I understand; things are crazy here; let me see what I could do. Can I call you back?"

Carl: "Thank you, Ruby."

Hacker: "You are welcome, bye."

Hacker hangs up, calls NOC, asks for Chris, and tells him to re-enable port LTP 35.

Forth Call:

Hacker calls Carl.

Hacker: "Carl, this is Ruby again. Try now; your connection should be fine."

Carl: "Wow! thank you. Let me try. Yes, it's working."

Hacker: "Good, let me make sure your connection is solid. Do me a favor, go to your browser and type: www.diagnoseconnection.com and download the "test connection" tool.

Carl takes a few minutes and downloads the tool.

Carl: "It's downloaded on my browser. Should I open it?"

Hacker: "Yes, go ahead and open it."

Carl: "It's asking for administrative permission. Should I say Yes?"

Hacker: "Yes, please."

Carl: "It says you have no connectivity issues."

Hacker: "Good, good, you can close your browser now."

Carl: "Thanks, Ruby."

Hacker: "You are welcome, Carl. Call me back if you have any other problem, bye".

Carl: "I will, thanks, Ruby. Bye."

The hacker takes the battery out of her burner phone, tosses the phone in the nearby trash can, and grins from ear to ear.

About 20 seconds later, Carl's machine connects back to the hacker's machine creating a "Remote Command Shell," The hacker has complete control over his machine, including his microphone and camera.

What went wrong here? How should this be prevented?

This is a hard one. Multiple things went wrong here, and they are all not that easy to mitigate.

1. Carl should not have given out his port number. But that would only make sense if he was trained not to give out such information.
2. Carl should not have called Ruby's cell number. Instead, he should have contacted the help desk and asked for Ruby. But it looks like using cell phones to contact each other is a norm in this company, so culture has to change for sensitive communication.
3. NOC should not have disabled the port without the proper identification and authorization process in place.
4. Carl should not have the administrative privilege to install and execute an unnotarized app on his machine. Instead, the machine should have been locked down. This is called the "Principle of least privilege." Every person, every program should be given the least privilege needed to operate.

Introduction to Cyber Defense

Phases of Attack

Assume you are an ethical hacker hired by Yahoo to penetrate their infrastructure. How would you go about crafting an attack? First, would you spend some time exploring what systems/services Yahoo is running and what kind of known variabilities exist for such systems/services? Would you then try to gain access to Yahoo's systems/services using those vulnerabilities? If successful, would you either steal some documents/passwords to prove that you can? Next, would you try to become a superuser on their systems/services? Finally, before leaving, would you try to delete the log files and other footprints to conceal what you did and how you did it before handing off a detailed report to Yahoo?

In general, there are five Ps of attack:

1. Probe: Find vulnerabilities
2. Penetrate: Find the right tool and attack
3. Persist: Create backdoor
4. Propagate: Attack other machines on the system
5. Paralyze: Steal data, destroy data or even bring down the systems

Steps of Defense

Let's now imagine that Yahoo didn't hire you to hack into their systems/services as an ethical hacker. Instead, they hired you in their cyber defense team to protect their assets. How would you go about doing that? Would you try to identify Yahoo's vulnerabilities and rank them as Critical, High, Medium, Low, etc.? Would you then install software/hardware to protect Yahoo from these exposures? Would you also install monitoring/detecting software just in case Yahoo still got hacked?

Let's assume you did all that, but Yahoo still got hacked because someone discovered a zero-day vulnerability and used it to attack. What is a zero-day vulnerability? A Zero-day is a flaw in the software, hardware, or firmware that is either 1) unknown to the party or parties responsible for patching or 2) is known to them but have not been able to come up with a fix yet. Let's imagine you got alerted by the monitoring software that some intruder is in your system.

What would you do? Will you kick the intruder out of the system? Would you shut down the infected machines? Would you notify the police and or FBI? Would you notify Yahoo's legal team?

What next? Would you quarantine the machines and patch/reinstall software on them? Would you conduct a post-mortem on the event? Would you have a lesson learned meeting with your team?

The National Institute of Standards and Technology (NIST) developed a Cybersecurity Framework that provides private sector organizations with a structure for assessing and improving their ability to prevent, detect and respond to cyber incidents. It defines five core functions of Cybersecurity:

The first two steps identify and protect are preventative steps to avoid the attack. The next three steps, detect, respond and recover, are reactive steps after an attack occurs.

1. **Identify**: Using various software tools available in the market, companies should scan their network, run penetration tests and other measures to identify vulnerabilities and risks. Then, they should define roles and responsibilities for risk mitigation and develop policies and procedures.

2. **Protect**: Using cyber defense software tools available in the market and other social engineering prevention mechanisms, companies must develop and implement the appropriate safeguards to limit or contain the impact of a potential cybersecurity event. For example, servers should be patched and upgraded, awareness training, particularly in social engineering, should be provided to all employees, data must be secured, and all entry points to the IT infrastructure should be firmly guarded. Entry points include physical access as well as logical access.

3. **Detect**: Even after all the protections are in place, new vulnerabilities will be found, hackers would develop new exploits, and a successful attack may still take place. In such unfortunate instances, companies must quickly identify cybersecurity breaches. Continuous monitoring and threat hunting using various hardware and software are effective ways to detect a cyber-attack incident.

4. **Respond**: If a cyber-attack is detected, companies must have the workforce and tools to respond to the attack and minimize the impact. There must be a response plan, communication plan, and forensic analysis plan. In addition, the legal team should always be ready to work with the FBI and other law enforcement agents to go after the hackers.

5. **Recover**: After a cyber-attack has been responded to, companies must restore all the impaired services due to a cybersecurity event. In addition, companies must have a disaster recovery plan in place, coordinate restoration activities with external parties, and incorporate lessons learned into the updated recovery strategy.

Risk Management

You all probably carry a cell phone with you. It is a beautiful device to have with you, but several risks are associated with maintaining a phone. For example, you may lose your phone; you may damage it. In addition, someone might steal it and get hold of your confidential information or, worse, use it to impersonate you.

How do you manage these risks?

A cyber-attack is a risk that every company must account for. Risk management is the process of identification, assessment, and prioritization of risks followed by coordinated application of resources to minimize, monitor, and control the probability and(or) impact of unfortunate events. So, how does a company manage any risk?

Risk Treatments: A risk can be treater in one of the following five different ways:

a) **Avoidance**: Avoidance is the easiest option. For example, running websites on "HTTP" mode is risky, so companies avoid it by only allowing "HTTPS" mode. However, risk avoidance is always an option. For example, you can take down your company's eCommerce site to avoid any risk of hacking, but that's not practical.

b) **Mitigation**: Not all risks can be mitigated, but some can be. For example, the risk of losing a data center due to a cyberattack can be avoided by mirroring data in another data center and periodically practicing a Disaster Recovery Plan.

c) **Deter**: Most of the time, we deter a risk. For example, by periodically patching/upgrading servers, workstations, operating systems, and applications, a company can prevent cyberattack risk by a significant margin.

d) **Transfer**: Buying car insurance is an excellent example of risk transfer. In case of an accident, you want the insurance company to pay for the damage. So, the risk of damage is now

transferred from you to the insurance company. Cyber insurance can be similarly purchased to transfer the loss of attack to an insurance company.

e) **Accept:** Something you can do nothing about risk but accept. For example, suppose a vulnerability is detected in your system, but no patch/upgrade is available to fix it (zero-day vulnerability). In that case, you accept the risk and hope and pray no hacker will find out and attack you.

By the way, you don't have to pick one of the above options; you can choose multiple simultaneously. So, for example, You can patch/upgrade your server, buy the insurance and have a disaster recovery plan all at the same time.

Introduction to Networking

Internet Protocol (IP)

Computer Networking is all about transferring data from point A to point B. Raw data is put into packets with "to" and "from" addresses and then propagates through several hubs and finally to the destination. This is, in a nutshell, the Internet Protocol or IP. IP is like the process that the post office follows to route and deliver mail.

Transmission Control Protocol (TCP)

When you send several packets to the same address using the regular postal service, the packets might arrive in any order, some of them might be delayed, or even get lost. Uncertain delivery is equally undesirable for postal mail as well as for electronic data. In the case of postal mails, we deal with this problem by sending registered mail with acknowledgment. A similar protocol is used for networking to guarantee reliable delivery in the order in which packets are sent. This additional protocol is known as Transmission Control Protocol (TCP).

Together, they make TCP/IP protocol.

Client-Server Model

When two machines try to communicate with each other, one obviously must initiate the communication. This machine would be tagged as a client for the entire duration of the communication. The machine responding to the client is classified as the server for the whole period of the communication.

IP Address and Port Number

The communication between two endpoints is based on the IP address and port number. You already know the IP Address is the unique number for a machine; the port number is like the unique identifier of an app running on that machine. So together, they make a unique endpoint.

To give you an analogy, assume for a moment that everyone lives in apartment buildings. The street address of each apartment complex would be the IP address, and the apartment number would be the port number. Every machine connected to the internet should have a unique IP address. A single server may (and indeed does) provide many different services simultaneously using many port numbers. Examples of these services are website, email server, chat server, etc.

If a machine wants to initiate a conversation (client) with another machine (server) four things must happen:

a) The server must acquire the IP address and port number and patiently listen for the client connection.
b) The client must acquire an IP address and port number.
c) The client must also know the IP address and port number of the server. On the other hand, the server does NOT need to know the client's IP or port.
d) The client must initiate the connection.

To initiate a conversation, the client must know the server's IP address and the port number for the server's service. Port numbers under 1024 are reserved for system software use. For example, Port # 23 is the telnet service; Port #80 is the HTTP service, etc.

Sockets

TCP/IP connections between clients and servers use a software concept called "Socket." Think of sockets as telephone sets; you need to make a phone conversation to give you an analogy.

Initially, the server keeps listening for incoming requests at a specific port number using Socket. Then, the client initiates a connection using another Socket. Then using the two sockets on two ends, they exchange data with each other.

Risks with Sockets

Socket connections are cool. What are some of the risks associated with socket connections? Well, hackers often remotely hack using a Socket connection. So, open ports on a machine are inherently risky. Some of the known services run on known ports; therefore, they are well known to hackers. For example, FTP service runs on port 21; Telnet service runs on port 23; HTTP service runs on port 80.

Therefore, if you run any of these services on your machine, a hacker already knows your open ports. Open ports themselves are not risky; the risk comes from the known vulnerability of the services you are running. For example, someone might have misconfigured a service, or the service may have known security holes. There are many more factors that determine whether a port and the underlying service are safe.

The problem with ports is that there are too many of them. For example, there are a total of 65,535 TCP ports and another 65,535 UDP ports. However, most of these ports will be closed in any system, even if a handful open could be very risky. For example, FTP servers, as useful for file transfer, carry numerous vulnerabilities such as anonymous authentication capabilities and directory access, making port 21 an ideal target. Therefore, protocols like FTP, Telnet, HTTP that sends data in the clear text should be avoided at all cost to stop **man-in-the-middle** attack. Instead, their secured counterparts like SFTP, SSL, HTTPS, etc., should be used.

Zenmap/Nmap Tool

To protect our computing devices from unattended open ports, we need to scan our machines using port scanning tools periodically. Nmap is an excellent tool for this. It even comes with a graphical interface which is known as Zenmap.

Let's download Zenmap/Nmap and start it.

A) My machine’s IP address is: 192.168.1.51 and I want to check if it up and running. So, on the command textbox of Zenmap, I type:

nmap -sn 192.168.1.51

It shows that the machine is up and running.

B) In my network, I could have 254 machines starting from IP: 192.168.1.1 all the way to 192.168.1.254. How do I check how many of them are up and running? I type:

nmap -sn 192.168.1.1-254

It shows which IPs are being used and what MAC Address are they currently using.

C) Let's find out which ports are open on my machine:

nmap -sT 192.168.1.51

D) Let's try to find out what operating system in running on my machine:

nmap -A 192.168.1.51

It say's I am running Windows

E) I have a machine 192.168.1.11 running macOS, let's try that one:

nmap -A 192.168.1.11

nmap actually fails to figure out my macOS but tell me that my network card (MAC Address) is issued by Apple.

Watch the following video to learn more:

https://www.youtube.com/watch?v=4t4kBkMsDbQ&t=113s

Netstat command

Nmap will only show open ports on a machine listening for incoming connections. In other words, it helps you to protect yourself from an attack. But what about attacks from inside? How do you know if your machine is connecting to an external device or not? Well, we have a tool for that – Netstat.

Netstat Stands for Network Statistics. It shows the connections to and from your computer and ports used by your computer to make these connections.

Go to your command/terminal prompt and type:

netstat -a

You should see all the connections made by your computer and the ports used for these connections.

If you have administrative privileges on your machine, search for "cmd" again and right-click on "Command Prompt," and select the "run as administrator" option. It will probably ask for your confirmation, so confirm.

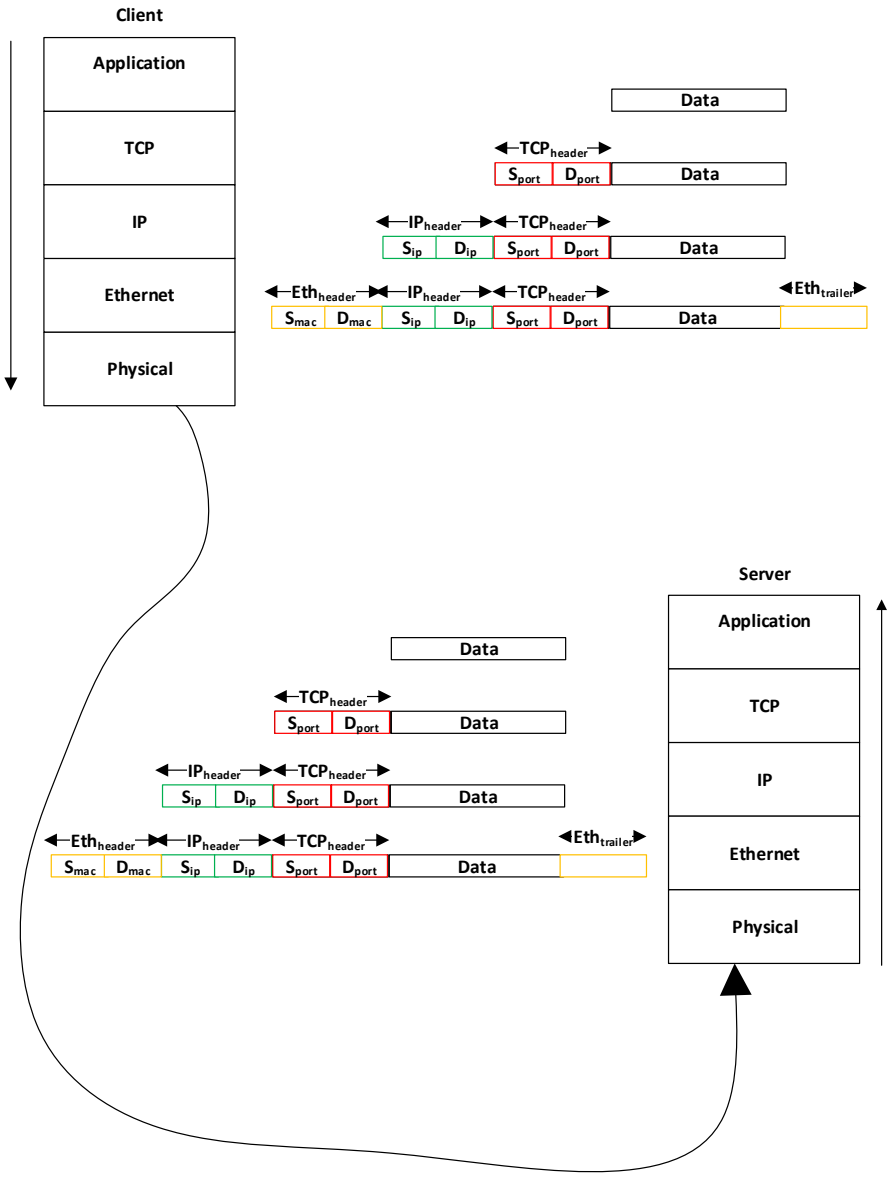
Now on this command prompt, type:

netstat -b

It will show you the executables that made these connections. This is much more informative than netstat – a.

Data Flow

Let's take a look at the data flow from a client application to a server application using TCP/IP protocol:



The client application starts with raw data and sends it down to the TCP layer. Next, the TCP layer adds source and destination port numbers and sends it down to the IP layer. Next, the IP layer adds source and destination IP addresses and hands it off to the Ethernet (or Wireless)

layer. Next, the Ethernet layer adds an ethernet header and footer and finally hands it off to the physical layer. The physical layer then sends the data to the server's physical layer.

On the server-side, the opposite happens. Each layer strips off its header (and trailer, if any) and sends it up to the next layer until the raw data appears on the server's application layer.

Networking Devices and Security

Switches, routers, and firewalls are electronic devices used to build data networks. They serve as essential components of the internet, moving information rapidly from one computer to the next. In many commercial networks, a separate piece of hardware handles each of these functions. However, for small office/home office use, the switch, router, and firewall are typically combined into one convenient, low-cost unit.

Switch: A switch, which can handle dozens of simultaneous connections, serves as a central point through which computers on a local network communicate with each other.

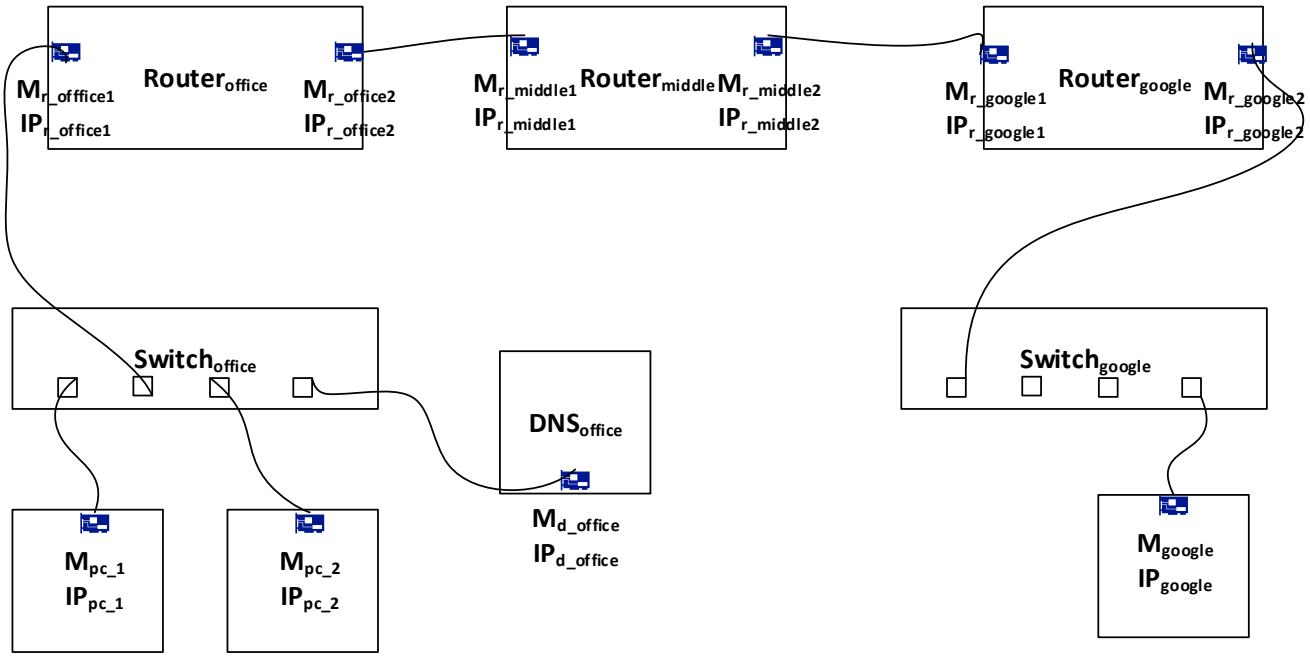
However, a switch cannot connect one network to another. For example, it cannot connect your office computers to the internet.

Router: A router connects two separate networks, allowing information to route from one to the other. For example, it connects your local area network to the internet.

We are all familiar with Wi-Fi routers that connect our home computers with the internet. By the way, your home router also works as your switch.

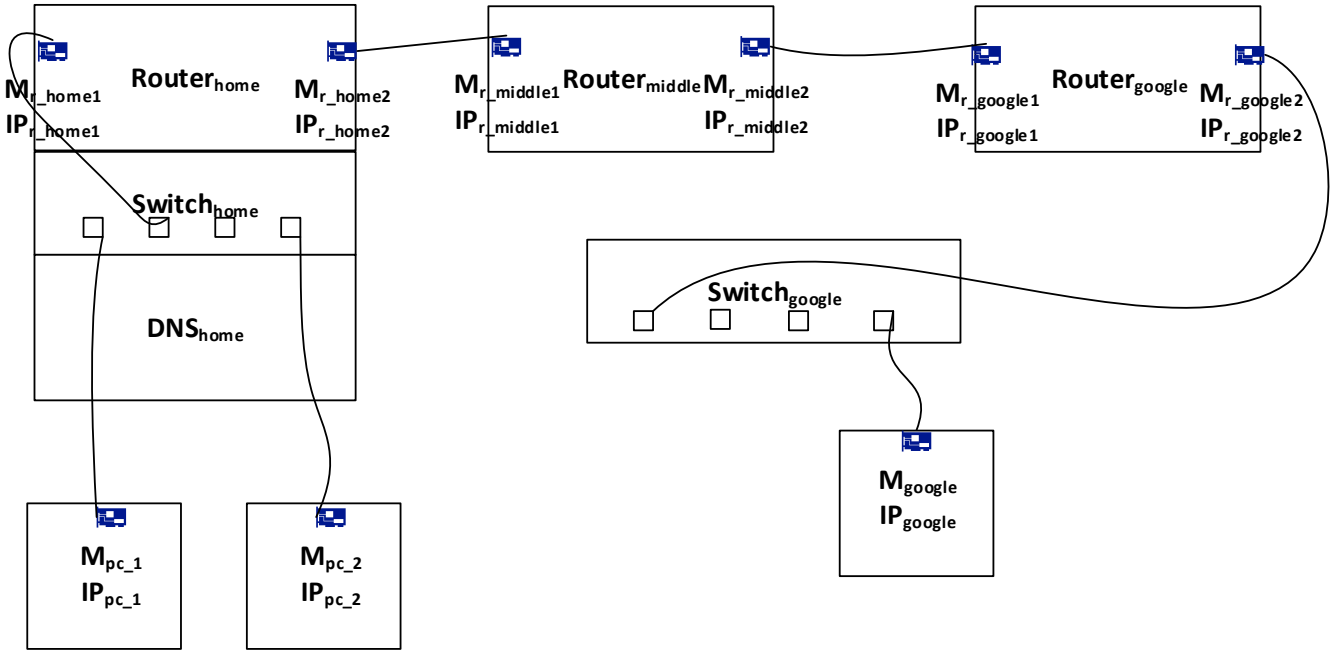
Data Flow

Let's imagine I am in my office, and I decided to do a Google search on my browser. How would the data flow from my machine to Google's server? Here is a picture of such flow:



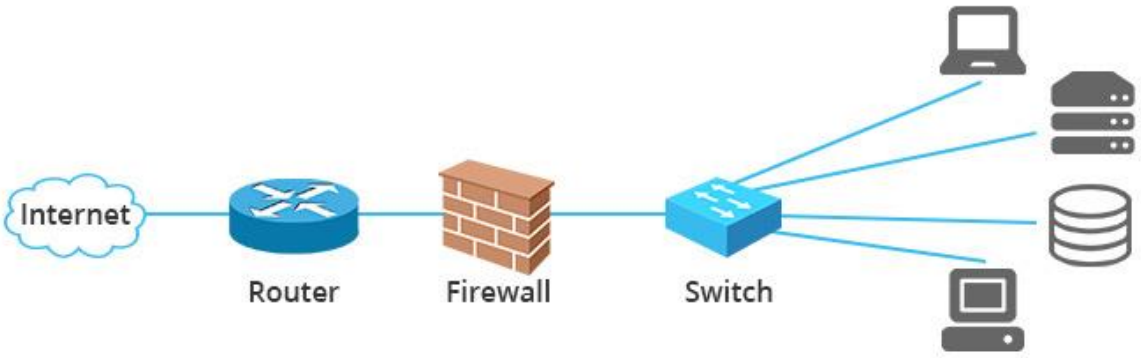
My machine M_{pc_1} is connected to my office's switch, which, in turn, is connected to a DNS and a router. First, my machine will look up Google's IP using DNS. Then my machine will send packets to the switch. Then, the switch will forward these packets to my office's router. These routers are interconnected, and finally, the packets will arrive at Google's router. Google's router will then forward the packets to the switch that delivers the packets to the server.

Let's now imagine I am at home doing the same thing. I don't have a separate router, switch, and DNS. They are all bundled in one unit. Here is what the picture looks like:



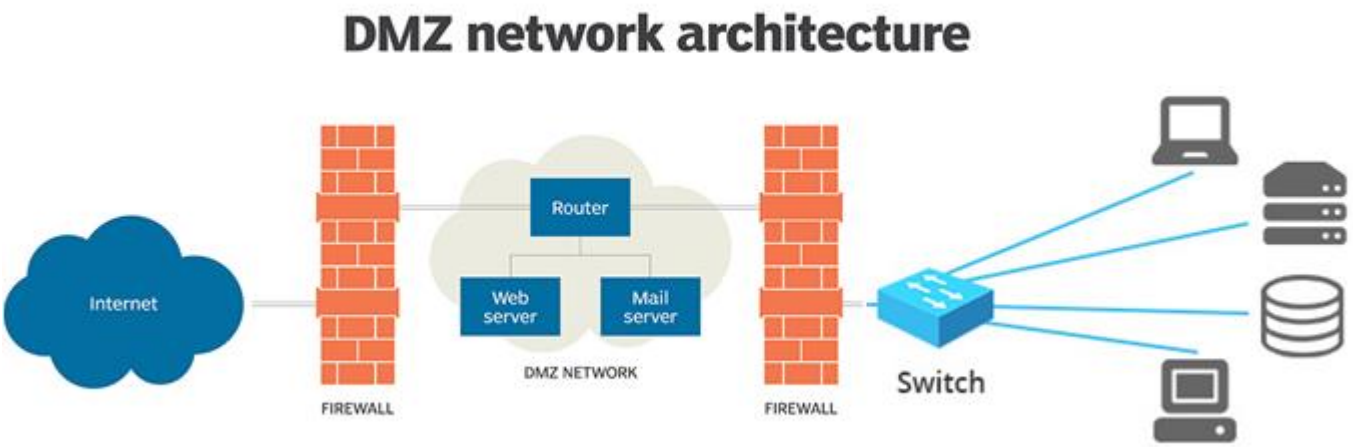
Network Security

Firewall: A network firewall is a security device that creates a barrier between a local network and the internet. The firewall acts as a filter, allowing or restricting data traffic between the network it protects and other networks. Firewalls will enable you to deploy blocking rules, such as by IP addresses, by protocols (TCP, UDP, ICMP), by ports, or for software applications and services.



For example, your firewall might have a rule that allows all connections to port 443 (HTTPS port) but no connection to port 80 (HTTP port). Another example of a firewall rule might be it allows connections from the webserver to the app server, but no other machine can connect to the app server.

Demilitarized Zone (DMZ): In Computer networks, a DMZ (demilitarized zone) is an area that separates the internet (outside world) from valuable and confidential computers (inside world). Public-facing servers like web servers and mail servers are placed in the DMZ for public access. All other computers are protected by putting them behind the DMZ. A DMZ is typically created using two firewalls as follows:



The first firewall allows all traffic from the internet to specific ports on specific servers (web servers, mail servers). The second firewall only allows traffic from the DMZ to the internal computers on various ports. In other words, anybody can get to the webserver and mail server above. But only the webserver and mail server can get to the internal computers. This approach discourages hackers since they have to pass through two layers of protection, and it is typically much harder to do. It is not unusual that a hacker will hack into the DMZ and access boring machines like web servers but cannot pass through the second firewall into the internal computers like app servers or database servers where valuable information is stored.

Homework 2

1) Run the following command on your machine:

   netstat -p TCP -n > connections.csv

   This will put netstat's output in connections.csv.

   You can now open the CSV file in Excel or any text editor (like notepad).

   For some of the destination IP addresses, find out who they belong to. To do so, go to:

   https://www.shodan.io

   and type the IP address on the search text box and search for it.

   What do you get? Report some of your findings.

2) Is your machine listening to any ports? What are they? What tool did you use to discover the open ports? What tool did you use to validate that those ports are open?

   Show outputs of discovered open ports. Show screenshots of validating open ports.

3) Is Social Engineering a powerful tool? Is it hard to protect from? What approaches could be taken to stop people from being a victim of social engineering?