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 2 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, 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 3 new.”

Becky: “Yes, we have 2 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 3 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. Can 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 3 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 that he is indeed the manager of the other store and looking out for the best interest of the company. At this point, he is bound to receive higher acceptance from a fellow employee, particularly someone of a lower rank. The last call gained sympathy from Becky since a system malfunction is not that uncommon and it 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 future?

a) The first problem here is that the company is storing and retrieving credit card information. That should never happen. They should store the credit card information in a very secured system and receive a token instead. The token and last 4 digits can be kept in the store's system. The token should be used for transactions going forward and the last 4 digits of the card can be displayed and printed but nothing more. This way, even if the token is shared with some 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. Proper verification may include hanging up the phone politely, calling back the other store and then 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 store the token and use a third-party reliable PCI compliance vendor to store the actual card information. This way, companies become PCI compliant by simply using a good third-party tool – perfect example of risk transfer.

Social Engineering again!

It is 8:15 on a Tuesday morning.

A young lady called the front desk, posing to be a vendor and asked if anyone in accounts payable is in yet. 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 in 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 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, 3 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:

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 Hacker’s machine creating a “Remote Command Shell” and the Hacker has full control over his machine including his microphone and camera.

What went wrong here? How should this be prevented?

This is a hard one. There are multiple things that 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 to not give out such information.
2. Carl should not have called Ruby’s cell number. 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 that culture has to change for sensitive communication.
3. NOC should not have disabled the port without proper identification and authorization process in place.
4. Carl should not have the administrative privilege to install and execute unnotarized app on his machine. 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 perform the operation.

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? Would you spend some time exploring what systems/services Yahoo is running and what kind of known variabilities are out there 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? Would you try to become a super user 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 as an ethical hacker to hacker into their systems/services. 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 all the vulnerablities Yahoo has 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 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 shutdown 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) came up with 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 5 core functions of Cybersecurity:

The first 2 steps identify and protect are preventative steps to avoid attack. The next 3 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. Servers should be patched and upgraded, awareness training, particularly in the area of social engineering, should be provided to all employees, data must be secured and all entry points to the IT infrastructure should be strongly guarded. Entry points include physical access as well as logical access.

3. **Detect**: Even after all the protections in place, new vulnerabilities will be found, new exploits would be developed by hackers 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 very effective ways to detect a cyber-attack incident.

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

5. **Recover**: After a cyber-attack has been responded, companies must be able to restore all the services that were impaired due to a cybersecurity event. Companies must have a disaster recovery plan in place, be able to 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 wonderful device to have with you but there are several risks associated with carrying a phone. For example, you may lose your phone, you may damage it, 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 5 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 as 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 by practicing a Disaster Recovery Plan on a periodic basis.

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

d) **Transfer**: Buying car insurance is a great 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 a risk but accept it. If there is a vulnerability detected in your system, but no patch/upgrade is available to fix it (zero day vulnerability) then 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 pick multiple at the same time. For example, You can patch/upgrade your server, buy 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 on it and then propagates through a number of 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 acknowledgement. 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 between each other, one obviously must initiate the communication. This machine would be tagged at Client for the entire duration of the communication. The machine that is responding to the Client is tagged as Server for the entire duration of the Communication.

IP Address and Port Number

The communication between two end points 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. Together, they make a unique end point.

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 certainly does) provide many different services at the same time using many port numbers. Examples of these services are like 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. The server, on the other hand, 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 IP address of the server and the port number for the service that the server is running. Port numbers under 1024 are reserved for system software use. For example, Port # 23 is the telnet service, Port #80 is HTTP service etc.

Sockets

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

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

Demo:

A live socket connection between two machines.

Risks with Sockets

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

Therefore, if you are running 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. 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 is safe.

The problem with ports is that there are too many of them. There are a total of 65,535 TCP ports and another 65,535 UDP ports. Although 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 as they are for file transfer, carry numerous vulnerabilities such as anonymous authentication capabilities, directory access making port 21 an ideal target. Protocols like FTP, Telnet, HTTP that sends data in 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.

Nmap/Zenmap Tool

To protect our computing devices from unattended open ports, we need to scan our machines using some sort of port scanning tool on a periodic basis. Nmap is a wonderful tool for this. It even comes with a graphical interface which is known as Zenmap.

Let’s download Nmap and run it. Let’s enter ‘localhost’ (means ‘this machine’, also IP Address: 127.0.0.1 also means ‘this machine’) as target and hit scan.

How many ports are open?

By the way, Nmap and ZenMap can be used to find open ports on any machine if you know the IP address of the machine.

Netstat command

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

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

Go to your command/terminal prompt and type:

netstat -a

You should see all the connections in and out made by your computer and 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.

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. For small office/home office use, the switch, router, and firewall are typically combined into one convenient, low-cost unit.

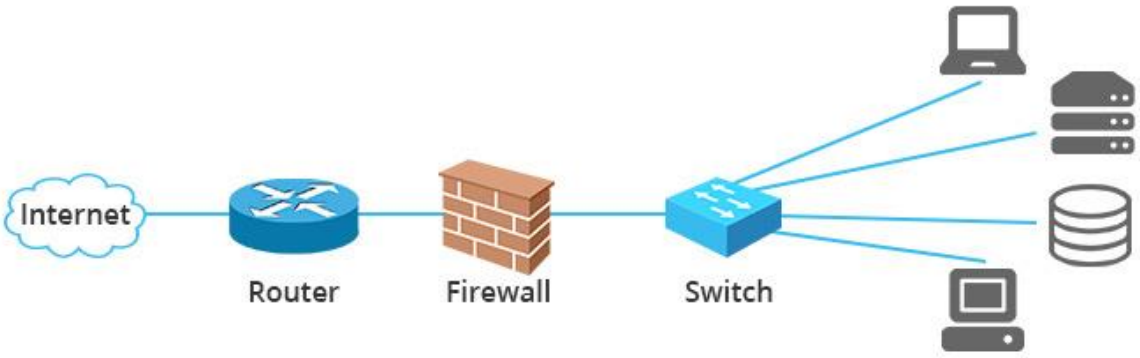
Switch: A switch, which can handle dozens of simultaneous connections, serves as a central point through which computers on a local network communicate with each other.

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.

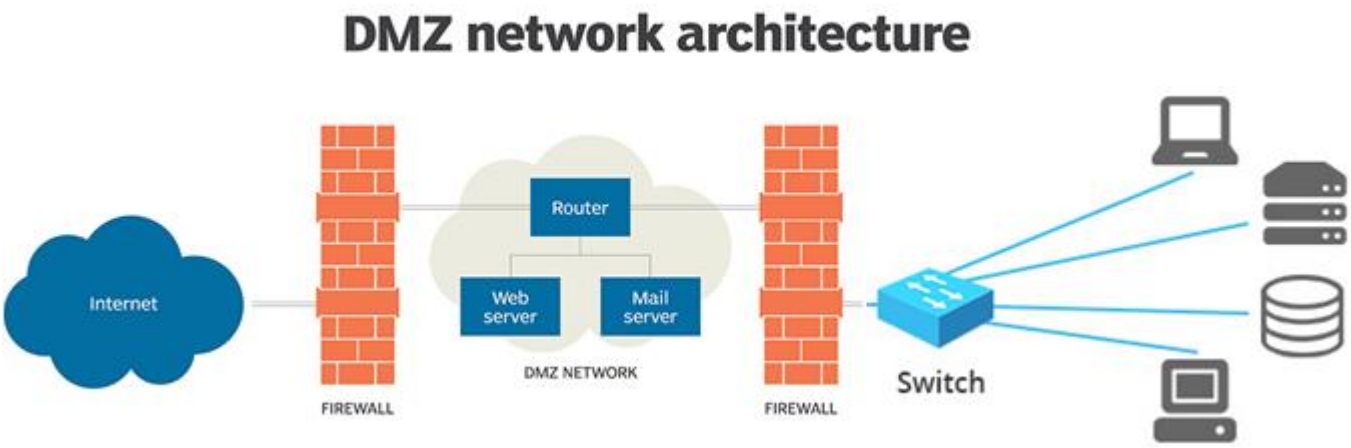
We are all familiar with Wi-Fi routers that connect our home computers with the internet. By the way, your home router also works as your switch.

Firewall: A network firewall is a security device that puts up 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 allow 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 web server to 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 server is 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 web server and mail server above. But only, the web server and mail server can get to the internal computers. This approach discourages hackers since they have to pass through two layers of protections 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 in 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?