**HACKING** – One word for online crimes

A person sitting at a desk with several computers

Description automatically generated with low confidence

I Have chosen case 3 for my research. The main reason behind picking this scenario because it’s the most ongoing issue in real world and most of the bigger companies are already victim of such attacks. It doesn’t matter how small or big is the company. System will get hacked anytime unexpected. Main root cause can a breach in the security or by the human interventions. Or both. Now a days, most of the banks are hiring Security analysts with high importance, just to find out the security breaches and how to avoid hacking to their applications.

|  |  |
| --- | --- |
| Part 1 | **[Who will attack the server?](#_Who_will_attack)** |
| Part 2 | [**What kind of harm can attacker cause to the system.**](#_Kinds_of_harm) |
| Part 3 | [**Kinds of vulnerabilities.**](#_Kinds_of_vulnerabilities.) |
| Part 4 | [**Tools Used by Hackers**](#_Tools_Used_by) |
| Part 5 | [**How can you stop them from attacking the system?**](#_How_can_you) |
| Part 6 | **What happened in this** [**scenario**](#_What_happened_in) **?** |
| Part 7 | [**Bibliography**](#_Bibliography) |
| Part 8 | **Appendix** |

# Who will attack the server?

The hands behind this type of hacking can be many. Like, computer hackers mostly called as skilled programmers who focus on the security breaches, infrastructure, and network vulnerabilities. Some of the hackers can be script kiddies. They don’t even need to be skilled in programming.  According to Technopedia black hat is “a person who attempts to find computer security vulnerabilities and exploit them for personal financial gain or other malicious reasons”.

Some organization will **hire black hat hackers** tobring down there competent in market. All these reasons are most common in market and frequently happening for years. Mostly targeted sources are financial sectors who is running the country and some government official websites hacked by the opposite country to make some news globally. Most of the hacks are done intentionally. But there is another category which emerged in last 5 years called grey hat hackers. What they do is that they will pick some victims and tell them anonymously that they are going to be hacked. And challenge them to prevent the hack if they can. Once its hacked, they will ask for money to fix it. Most of the company’s already victim of such grey hackers and paid large amount of money to save the organization.

Another most used method is from **hard copies for printing PII information’s**. Documents having personal details can be used to steal identity of user and hence the details can be hacked any time. These documents can be easily reached in anyone’s hand in the form of garbage. They can sign up to online banking and so on.

Apart from all these widely used methods, simple and easy way is by using **mobile banking app hacking.** Mobile bank applications make life much easier. Users don’t have to struggle with online banking, and this has been manipulated by the hackers by using fake bank applications and fake login page. Hackers will develop application which looks exactly as the bank’s application with same logo and graphical user interface. Users will get these applications from normal app store. Once they login with original username and password, it will directly go to the database and hackers can easily use it. It’s most common hack and still ongoing in real world. Another method is by infecting mobile application by using Trojan virus. The infected application will target mobile application.

# **Kinds of Harms:**

Attackers can do multiple things once they gain the access to the system. E.g.,

* Attackers will Hijack your login credentials.
* They will take your whole money and open a new bank account and credit card on your name and use it for fraudulent activities.
* They will destroy your credit.
* Make online shopping by using your credentials.
* They will add additional user to the account, so that they can control the account in future.
* They will apply for cash advances.
* Miss uses your security number
* Sell your personal information including account no, salary details, payment methods to third party illegally.

# **Kinds of vulnerabilities.**

1. **Finding how weak is the code.**

According to the survey of 300 IT experts by SANS’s institute they found that most easily found breaches by the hackers are outdated software’s, vulnerable configurations. Exposed passwords in the codes instead of using encrypted passwords. Some of the commonly used web applications like WordPress, Joomla and the plugins, themes used by these applications are the most vulnerable things on internet. Users will install third party plugins and these codes can be easily hacked whoever knows the coding. So, use application’s and make sure you have customized everything inside the application and do not install third party plugins and themes which can be malicious in nature.

**2. Server - side vulnerabilities**

Hackers will initially try to get the webserver information like, Tomcat, Apache, or IIS. This can be easily achieved by scanning the server port. Just by sending ‘Telnet’ request to the IP and see if the port is open or not. Once the back-end technology is defined, they will variety of methods to enter the system. First, they will outline of the infrastructure used. Like server OS, Whether the victim’s server is hosted in cloud of other standalone servers. Because intruding in standalone server is very easy as compared to cloud servers. Then they will check what kind of network they use. Is it proxied or the public Ip is exposed to the internet. If the victim is not using any proxy servers, then hacker can easily attack the services like web server, mail server and database server through DDoS attack, Brute force attack and so on. And the result of the attack is slowing down the services or crashing entire website which will cause both financial loss and make whole employees in the company will impact it.

**3. API’s and Cyber threats.**

Most of the Systems including bank websites are composed of two parts. One is API and another is databases. Front end will connect to the back end through API calls. If the attacker can hack the API calls, then he can enter the system easily. Hacker will get the internet architecture through API’s. In this scenario, attacker used social engineering to get the sensitive information about the website and about the customers information.

Another reason behind API attack is unencrypted information passed from front end to back-end server. Back-end server mostly composed of information about their customers including their name, PII, Contact no and so on. These information’s should pass to the front end to complete several operation’s including user login and making financial transactions. Most of these API’s use SSL encryption technology to encrypt the data passed between front end and back end. If it’s failing, then all the information’s can be easily hacked.

# Tools Used by Hackers

Chart

Description automatically generated

From this figure, we can see there is lots of ways to hack. Even though, through social engineering attacker can get some information. But it’s not enough to hack an entire system and get some profit of hacking.

1. Social Engineering:

Social engineering can be applied anywhere, where human interaction is involved. Attackers use Human as medium for getting the things smoother. Below are the most used digital engineering methods in market,

Baiting: As the name implies, baiting is concentrated on victim’s who are greedy or curious. Hackers will leave the bait which can be pen drives or any hardware devices as data storage device and leave anywhere it get public attention. Victims pick up these items and insert into their office space or their personal system.

Scareware: Sometimes, users can see the legitimate popups in their system such as ‘Your computer has been infected with viruses. Scan immediately to make your computer safe from viruses’. Victims found this vry legit and they click on such pop ups and system get infected by the malware.

Social engineering road map followed by attacker looks like: -

Diagram

Description automatically generated

1. Web Based Attacks:

Criminals explore the coding vulnerabilities they will use below techniques for attacking.

* Cross-site scripting
* DDoS Attack.
* Local file Inclusion
* SQL Injection

Through Cross site scripting, attacker try to inject malicious codes into the victim’s website/application. Attacker even try to send malicious contents to the end user and ask them to click on it.

Another frequently used attack is DDoS attack. They will try to put down any service in the server by scanning the ports of the server first. Then attacker will check for the open ports which are open to internet, and they could find if it’s used for any applications, web server, mail server etc. Once found, using hacking medium such as Kali Linux and Windows tools they will target the victims Ip address and do millions of attacks which will slow down the server and leads to website crashing.

1. Compromised Accounts:

Attackers normally won’t try get the passwords manually. They will use automation tool to generate most used passwords and password combinations known us brute force techniques. There are lots of techniques to check the username and password combination which is highly used by peoples to hack the credentials. Also, they will loop the username password combination without any human intervention. Only matter is time. How long they are spending time on hacking the password. If the user is not using any multi factor authentication for login, then simply by using the login user and password any one can login. Sometimes, users will write there password somewhere secure. But this is the main fault anyone can do. Also using password which have username on it and using date of birth, place of birth is the root cause of compromised accounts. Be wise on creating passwords and storing them safely and do not share personal information’s in social medias. Which can lead to assume your details and anyone who don’t have technical background can assume your credentials.

1. Command and Control Servers:

C&C is also called command and control is used by hackers to control the slave machines which are infected by malware. C&C servers issues commands against infected/compromised systems. They make simple communication by sending heartbeat requests to the target machine and the system will respond normally to the master until and unless the compromised systems are detected against the attack and took proper actions against them.

One of the most used mails is phishing mails received to the user by mimicking as an original bank website or another legit website and the machine becomes under control of master machine.

1. Key-logger hacking:

Key-logger is a type of malware or hardware which records your keystrokes while you are typing. And send this information to the hacker by using command and control server(C&C). There are types of key-loggers. Software key logger and hardware key logger,

1. **Software keylogger:** This consists of programs and applications installed in the user’s computer to steal information’s. These programs can act as monitor and send the information’s directly.
2. **Hardware keylogger**: Main feature is, use of a hardware which should be physically connected to the target machine. Due to this reason, the organisation should monitor and restrict each system to use external hardware devices allocated to the users and show which devices connected to which system if any suspicious activity found. If any unauthorized person gets a chance to use any devices used by the organization, they can install the hardware key logger and it won’t get easily detected and the hacker will make the key logger device accessible via Wi-Fi. Even hacker leave the area, he doesn’t have to physically in the system to collect the information’s. Attacker can fetch all the stored data anywhere around the Wi-Fi connectivity. This can be intentionally by the employees in the bank. If anyone approach the employee to connect a device and offer them money this is the easy way to get data.

Depending upon the environment used by the user, hacker can decide which one is suitable. Also, most common approach is **video surveillance.** This is to see the connection between the keyboard and the user. A camera with view of keyboard can give good visual of your personal details. Once it is recorded, if the user is not frequently changing passwords once it looks suspicious or used in wrong place. Hacker can use the video and play it slowly to get all information’s.

# **How can you stop them from attacking the system?**

### 1.**Train your Staffs**

This is the most powerful technique you can use to prevent 80% of the attacks can be prevented if the staffs are well trained for dos and don’ts when they are dealing with customers sensitive information. Nobody wants their information exposed in public or getting hacked. Most of these incidents are happened due to ignorance and simple mistakes while handling data in internet. So, it is important to train the staffs and test them frequently to know if they really following the security aspects which they should follow while working under an organization.

### **2. Alert on the Email attachments**

90% of the online hacking is done through malicious contents sent through email and Victims open with curiosity in mind. Most of the mails will contain subjects which are sometimes about the unexpected incidents such as ‘Dead Body’s falling down ‘which sometimes cause curiosity to the users who are educated or sometimes educated ones also falls under these scams. So better to know the internet reality, educate yourself and do verify all the details in internet before clicking on any links.

### **3. Update your Software and Scan your Hardware frequently.**

Outdated software’s will bring vulnerabilities in entire system, and this can be a loophole to enter the infrastructure front end or back end. Doesn’t matter how strong the infrastructure is, updating all software’s frequently and monitor them is one of the key factors when it comes to security.

### **4. Use of anti-phishing toolbar**

Most of the companies want some sort of anti-software/Toolbar to protect their employees from attack. For that, they adjust employee’s browser which support anti-phishing toolbar. Main purpose of this tools is to detect the malicious contents used on the website by there algorithms used and block them automatically before user click on any links inside the website. These techniques are highly usable, when the peoples using the system don’t have any knowledge about internet and cybersecurity.

### **5. Encrypt Customer Data**

If the customers data is compromised, that will lead to big legal issues. Customers can make complaints and legal actions against the bank, and it will cause huge loss for company. So Better way to encrypt the customer data so that even though the system got hacked, the hacker won’t be able to decrypt the contents.

## What happened in the in this scenario?

Firstly, the root cause behind attack is due to 3 reasons. One is **making a system which is easily breakable**. Two is authenticating staffs to see the company architecture and the payment systems they are handling. Even though, the staffs are under the same organisation, we cannot give most of the access to them due to high confidentiality of the information. It should be restricted among layers. Means, no one in the organization, except main head should not be able to view the financial reports and payment gateway used. Backend or Database servers should be built on internal network. That means, IP should not be public one. And use IPv6 for public domains including proxy servers to hide the network from outer world is also a plus when it comes to security of the infrastructure. Means, only few people including the owner should have access to the root server. And others should have restricted access with proper alerting system. If she/He is attempted any restricted things, then it should be properly logged or monitored. Hiring more skilled persons to monitor these activities can prevent happening such type of human interventions to the system.

Second breach happened is **unavailability of technical persons** during bank holidays. Hackers will look for such time and they will intrude into the system without anyone knowing. If they DDoS into the system and there is no one to monitor the traffic, then how will the company know if the system is compromised/hacked? So, do not leave the system unattended in bank holidays. Keep the system monitored for 24 hours.

Summary is no systems are fault tolerant. It should be frequently changed according to the new trends in market, and it should be tested against vulnerabilities. You can **hire one white hat hacker** to find the loopholes and then by using security analyst and programmers you can close those incidents. Most important thing is this should not be done at once. It should be checked frequently, and the monitoring systems should be capable enough to read the millions of data and suspicious attacks into the system and block them and report them right away if anything happened.

Also, company infrastructure should be re structured in such a way that all the employees working should not be able to send any mails outer the organisation and do not allow to copy any files from the system provided by the organisation. Do not take any photos inside the company so that some information’s including ID of employee which can be duplicated through photograph can be leaked in internet. They should be trained enough to do not do such practices even when they are inside the organization and when they left the organization. If they failed to do so, company can take legal actions against them. If these protocols are followed strictly, then human interventions will be handled safely.

Another efficient way is to **hire security analyst** to scan entire infrastructure and check for system and code vulnerabilities.

## Bibliography

## Ross Anderson and Tyler Moore, [*Information security: where computer science, economics, and psychology meet*](http://rsta.royalsocietypublishing.org/content/367/1898/2717.abstract), Phil Trans Roy Soc A v 367 no 1898 pp 2717–2727 (2009). Study Guide for the Professional exam - CEH  [CEH v11 certified ethical hacker study guide - University of East London (exlibrisgroup.com)](https://uel.primo.exlibrisgroup.com/discovery/fulldisplay?docid=alma9921400858601121&context=L&vid=44UEL_INST:UEL_VU1&lang=en&search_scope=MyInstitution&adaptor=Local%20Search%20Engine&tab=LibraryCatalog&query=any,contains,CEH%20ethical%20hacker&sortby=date_d)

**Appendix**

Modern world is converting every possible way into online. So, it is obvious that these information’s/data can reach wrong hands if it is not secured properly. There is huge role for network security in internet.