Ethical Hacking

A Minor project work report submitted to

Verzeo



in the process of the ongoing internship

on

Cyber Security

Submitted by

Deboleena Bose

e-mail address: [deboleenabose09@gmail.com](mailto:deboleenabose09@gmail.com)

Computer Science and Technology

University of Engineering and Management

Kolkata

**TOPIC: - Ethical Hacking**

1.Foot Printing

2.Vulnerability issues of a system

3.Batch Programming

4.SQL Injection

5.Sniffing data from a website

6.Cryptography and Steganography

1. **Foot Printing**

**INDEX**

|  |
| --- |
| Content |
| 1. Abstract |
| 1. Introduction |
| 1. What is Foot printing? |
| 1. Types of Foot printing |
| 1. Experiment and result |
| 1. Conclusion |

* 1. **Abstract**

Foot printing is one of the ethical hacking tools helps many organizations and companies to analyse and detect their network vulnerabilities and the loopholes for security breach. Footprinting is one of the approachable tools for hackers to reach them close to the target area and get the target information for cyber-attacks. Many different tools are existing to help the hackers in order to alert the organization about the vulnerabilities in the network.

**Keywords: Kali Linux, Microsoft website, Whois**

* 1. **. Introduction**

Foot printing is one of the key stages applied in Ethical hacking. Foot printing is one of the points in investigation phase of ethical hacking, where the attacker gathers system information. Hence, doing the Foot printing the technique provides the system or application information in reconnaissance phase, hence it explores the path in prior to know the attacking techniques and loop hole in the area of attack. It narrows down the possible impact of attacking space.

**1.3. What is Foot printing?**

**Foot printing** (also known as reconnaissance) is the technique used for gathering information about computer systems and the entities they belong to. To get this information, a hacker might use various tools and technologies. This information is very useful to a hacker who is trying to crack a whole system

When used in the computer security lexicon, "Foot printing" generally refers to one of the pre-attack phases; tasks performed before doing the actual attack. Some of the tools used for Foot printing are [Sam Spade](https://en.wikipedia.org/wiki/Sam_Spade_(software)), [nslookup](https://en.wikipedia.org/wiki/Nslookup), [traceroute](https://en.wikipedia.org/wiki/Traceroute), [Nmap](https://en.wikipedia.org/wiki/Nmap) and neotrace.

**Techniques of footprinting:**

* [DNS](https://en.wikipedia.org/wiki/Domain_name_services) queries
* [Network enumeration](https://en.wikipedia.org/wiki/Network_enumerating)
* Network queries
* [Operating system](https://en.wikipedia.org/wiki/Operating_system) identification
* Organizational queries
* [Ping](https://en.wikipedia.org/wiki/Ping_(networking_utility)) sweeps
* Point of contact queries
* [Port Scanning](https://en.wikipedia.org/wiki/Port_scan)
* Registrar queries ([WHOIS](https://en.wikipedia.org/wiki/WHOIS) queries)

**1.4. Types of Foot printing**

There are two types of Foot printing that can be used: Active Foot printing and Passive Foot printing.

* Active Foot printing is the process of using tools and techniques, such as performing a [ping sweep](https://en.wikipedia.org/wiki/Ping_sweep) or using the traceroute command, to gather information on a target. Active Foot printing can trigger a target's [Intrusion Detection System](https://en.wikipedia.org/wiki/Intrusion_Detection_System) (IDS) and may be logged, and thus requires a level of stealth to successfully do.[]](https://en.wikipedia.org/wiki/Footprinting#cite_note-4)
* Passive Foot printing is the process of gathering information on a target by innocuous, or, passive, means. Browsing the target's website, visiting social media profiles of employees, searching for the website on WHOIS, and performing a Google search of the target are all ways of passive Foot printing. Passive Foot printing is the stealthier method since it will not trigger a target's IDS or otherwise alert the target of information being gathered.

**1.5. Experiment and result**

**Objective: To perform Foot Printing on Microsoft Website and gather information about website by using online websites (Whois/net craft/Shodan/dumpster)**

**Procedure:**

### **Ping to find the IP address**

### **Open a browser and go to** Whois tool

* Enter the website name (or IP address) and click “Search “



**1.6. Conclusions**

Foot printing helps to avoid post sensitive and private information on social media. It also alerts about type of vulnerabilities. The help in setting proper configurations and also avoids leak of target system configurations and file sharing information. No software is made with zero vulnerability. So, it is better to understand how a system’s information is gathered before hacking the target system. In this way, various measures can be developed to prevent system attacks. In coming years drastic changes can be seen in the development of Foot printing techniques. If a user is able to understand the different techniques of Foot printing and also follow countermeasures of Foot printing then the user will be able to protect the personal data from getting hacked. A user must update the system security regularly. By improving the system’s security, attacks on the system can be prevented.

1. **Vulnerability issues of a system**

**INDEX**

|  |
| --- |
| Content |
| 1. Abstract |
| 1. Introduction |
| 1. What is Vulnerability? |
| 1. Types of Vulnerabilities |
| 1. Most common Vulnerabilities |
| 1. Experiment and result |
| 1. Preventive methods of Vulnerability |
| 1. Conclusions |

* 1. **Abstract**

As the threat landscape changes and advances in time, being able to address most common types of cyber security vulnerabilities gains more importance. In this article, we will discuss types of cyber security vulnerabilities and what you can do about them. As the information becomes the most important asset an organization has, cyber security gains much more importance. In order to be able to successfully conduct your business and preserve the hard-earned reputation of your organization, you need to be able to [protect your data from data breaches](https://www.logsign.com/blog/how-to-prevent-data-breaches-in-2019)**,** malicious attacks, hackers and such. Yet with the recent advancements in technology and rising trend of remote-working, organizations have an increased amount of vulnerabilities such as **end-points.**

**Keywords: PRORAT, Kali Linux, virtual machine**

**2.2.** **Introduction**

System vulnerabilities are weaknesses in the software or hardware on a server or a client that can be exploited by a determined intruder to gain access to or shut down a network. Vulnerabilities exist not only in hardware and software that constitute a computer system but also in policies and procedures, especially security policies and procedures, that are used in a computer network system and in users and employees of the computer network systems. Since vulnerabilities can be found in so many areas in a network system, one can say that a security vulnerability is indeed anything in a computer network that has the potential to cause or be exploited for an advantage.

**2.3. What is Vulnerability?**

A vulnerability is, in broad terms, a weak spot in your defence. Every organization has multiple security measures that keeps intruders out and important data in. We can think of such security measures as the fence that circumvents your yard. Vulnerabilities are cracks and openings in this fence.

Through security vulnerabilities, an attacker can find their way into your systems and network, or extract sensitive information. The term system security vulnerability refers to any kind of exploitable weak spot that threatens the system security of your organization.

**2.4. Types of Vulnerabilities**

**1. Software vulnerabilities-**

Software vulnerabilities are when applications have errors or bugs in them. Attackers look at buggy software as an opportunity to attack the system making use of these flaws.

*Example:* Buffer overflow, race conditions etc.

**2. Firewall Vulnerabilities-**

Firewalls are software and hardware systems that protect intra-network from attacks. A firewall vulnerability is an error, weakness or invalid assumption made during the firewall design, implementation or configuration that can be exploited to attack the trusted network that the firewall is supposed to protect.

**3. TCP/IP Vulnerabilities-**

These vulnerabilities are of the various layers of a network. These protocols may lack features that are desirable on the insecure network.

*Example:* ARP attacks, Fragmentation attacks etc

**4. Wireless Network Vulnerabilities-**

Wireless LANs have similar protocol-based attacks that plague wired LAN. Unsecured wireless access points can be a danger to organizations as they offer the attacker a route around the company’s network. Example: SSID issues, WEP issues etc.

**5. Operating System Vulnerabilities-**

The security of applications running on depends on the security of the operating system. Slightest negligence by the system administrator can make the operating systems vulnerable.

*Example:* Windows vulnerabilities, Linux vulnerabilities.

**6. Web Server Vulnerabilities-**

These vulnerabilities are caused due to design and engineering errors or faulty implementation. Example: sniffing, spoofing etc.

**2.5. Most common Vulnerabilities**

* SQL Injection
* Broken authentication
* Sensitive data exposure
* XML external entities (XXE)
* Broken access control
* Security misconfigurations
* Cross site scripting (XSS)
* Insecure deserialization
* Using components with known vulnerabilities
* Insufficient logging and monitoring

**2.6. Experiment and result**

**Objective: To test the system security by using PRORAT by hacking virtual machine and to observe the change in desktop.**

**Procedures:**

* Download ProRat  
  Open ProRat
* Create ProRat trojan horse
* Click on general setting
* Select bind with file.



* Server extensions
* Choose a server icon



* click on the Create Server button to create the server file which is bound with the file you chose
* Click Yes and continue., simulate the trojan

**2.7. Preventive methods of Vulnerability**

* Need to [find an encryption solution that meets your needs](https://www.esecurityplanet.com/products/top-encryption-products/).
* Never allow OS commands from application-layer code.
* For server products and libraries, diligently stay up to date on the latest bug reports for your systems. For custom apps, ensure that all code from users is reviewed to ensure that it can properly handle arbitrarily large input.
* Double submission of cookies with random tokens assigned can be required that must match before granting access to the application.

**2.8. Conclusion**

Data collection, storage, analysis, and sharing both enables many cybercrimes and the vast collection, storage, use, and distribution of data without users' informed consent and choice and necessary legal and security protections. Data aggregation, analysis, and transfer occur at scales that organizations are unprepared for, creating a slew of cybersecurity risks. Privacy, data protection, and security of systems, networks, and data are interdependent. In view of that, to protect against cybercrime, security measures are needed that are designed to protect data and user's privacy.

1. **Batch Programming INDEX**

|  |
| --- |
| Content |
| 1. Abstract |
| 1. Introduction |
| 1. What is Batch Programming? |
| 1. Functionality of Batch Programming |
| 1. Experiments and results |
| 1. Advantages and Disadvantages |
| 1. Conclusion |

**3.1. Abstract**

Batch files or scripts are small easy-to-write text files that carry out a series of commands. They can be simple enough that even the average home computer user can take advantage of them. Systems administrators and power users are well aware of the utility of batch files but the average PC user is generally unacquainted with them or is intimidated by the notion of writing or even running a script. This is unfortunate since it means that many are foregoing the use of a powerful tool for carrying out routine or repetitive tasks. Although batch files can be quite sophisticated and used for complicated network and system administration, they can also be of the utmost simplicity and very brief.

**Keywords: Notepad, command prompt, victim machine**

**3.2. Introduction**

Batch programming is a programming paradigm that can execute certain commands automatically at the level of an operating system such as DOS or Windows 7 / XP. A batch file is a stack of such commands. If it is retrieved with the command line, the system will execute each task listed in succession.

Before the implementation of modern GUI’s (Graphical User Interface), in the operating system like MS-DOS, we had to operate every command from command line. Even though we are facilitated with GUI’s, many major core operations can only be achieved through command line instructions.

**3.3. What is Batch Programming?**

A **batch file** is an unformatted text file or script file which contains multiple commands to achieve a certain task. It contains series of command that is executed by [command line interpreter](https://en.wikipedia.org/wiki/Command-line_interface).

**Extensions:**  .bat or .cmd

The instructions in batch files are for automating repetitive command sequences.

**3.4.Commands and Functionality of Batch Programming**

## ****Batch file commands: Windows/DOS****

For the ease of learning, we have listed all the **batch file commands** with relevant examples and explanations below. Please click on the commands to know the details. Batch file commands are not case sensitive.

List of batch file commands

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ASSOC | ATTRIB | CD | CHKDSK | CHOICE |
| CLS | CMD | COMP | CONVERT | COPY |
| DATE | DEL | DIR | DISKART | DRIVERQUERY |
| ECHO | EXIT | EXPAND | FC | FIND |
| FORMAT | HELP | IPCONFIG | LABEL | MD |
| MORE | MOVE | NET | PAUSE | PING |
| RD | FROM | REN | SET | SHUTDOWN |
| SORT | START | SYSTEMINFO | TASKILL | TASKLIST |
| TIME | TITLE | TREE | TYPE | VER |
| VOL | XCOPY |  |  |  |

## Batch File Function Definition

**-Syntax**

**: function\_name**

**Some\_Operational\_Code**

**EXIT /B 0**

As shown in syntax, a function definition in batch file starts with the declaration of a function with a label. Next is the body of function where we write codes to achieve a certain task. At the end EXIT /B 0 to ensure successful termination or proper exit of the functions.

## Batch File Functions Call

Like in every other programming language, to use the defined functions, we need to call it in the main program. For this, CALL command is used.

[Learn more details about all batch file commands here.](http://www.trytoprogram.com/batch-file-commands/#batchfilecommands)

-**Syntax**

:: To call function without parameters

CALL: function\_name

:: To call function with parameters

CALL: function\_name param1, param2, …, paramN

:: To call function with return values

CALL: function\_name return\_value1, return\_value2, …, return\_valueN

So, this is how the function is called in batch files.

**3.5. Experiment and result**

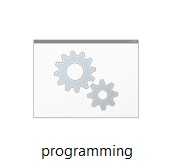
**Objective: To write a small batch program and save as .bat extension. And execute in a victim machine.**

**Procedures:**

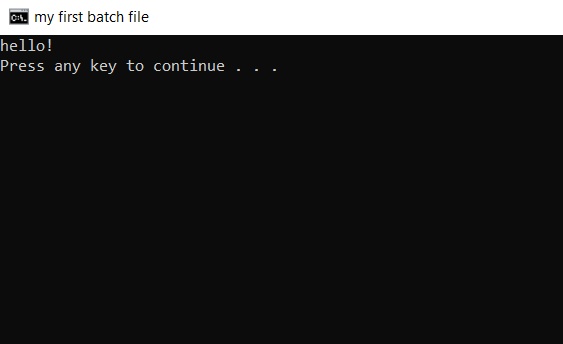
* Write a batch program in notepad

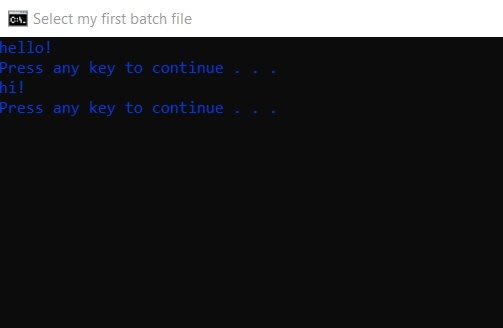


* Save the program with .bat extension



* Open the batch program, command prompt will be displayed.





Then we will create a folder bomb which creates random malicious files in the victim machine

**3.6. Advantages and**

**Disadvantages**

**Advantages:**

* It is very difficult to guess or know the time required for any job to complete. Processors of the batch systems know how long the job would be when it is in queue
* Multiple users can share the batch systems
* The idle time for the batch system is very less
* It is easy to manage large work repeatedly in batch systems

**Disadvantages:**

* The computer operators should be well known with batch systems
* Batch systems are hard to debug
* It is sometimes costly
* The other jobs will have to wait for an unknown time if any job fails

**3.7. Conclusion**

DOS can also enable us to do automated sequencing of different DOS commands by using “batch files” which are named this since you batch together a sequence of DOS commands and store them in a file with an extension of “.bat”. This saves time by doing a bunch of commands all at once as opposed to one by one. To make a batch file, you can use the programs notepad, MS Word (save it as plain text) or the DOS “copy” command and save it with a “.bat” file extension. When DOS initially comes onto your screen, type in the batch file’s name without the extension “.bat”.

**4.SQL Injection**

**INDEX**

|  |
| --- |
| Content |
| 1. Abstract |
| 1. Introduction |
| 1. What is SQL injection? |
| 1. Subclasses of SQL injection |
| 1. Experiment and result |
| 1. Preventive measures to avoid SQL injection |
| 1. Conclusion |

**4.1. Abstract**

SQL injection is one of the major threats to the security of the web applications. Attackers try to gain unauthorized access to the database, which has vital and private information of the users. Many researchers have provided various techniques and practices to protect the web applications from attackers. There is a plethora of techniques available to perform SQL injection and usually not everyone is familiar with every attack. Hence, this kind of attack is still the most prevalent. In this paper, we have presented the types of SQL injections attacks and most dominant ways to prevent them.

**Keywords: Kali Linux, Havij tool, SQL cheat codes, http://testphp.vulnweb.com**

**4.2. Introduction**

**SQL injection** is an attack technique that exploits a security vulnerability occurring in the database layer of an application. Hackers use injections to obtain unauthorized access to the underlying data, structure, and DBMS. By an SQL injection attacker can embed a malicious code in a poorly-designed application and then passed to the back-end database. The malicious data then produces database query results or actions that should never have been executed. It can also be used to add, modify and delete records in a database, affecting data integrity. To such an extent, SQL Injection can provide an attacker with unauthorized access to sensitive data.

**4.3. What is SQL Injection?**

SQL injection, also known as SQLI, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed. This information may include any number of items, including sensitive company data, user lists or private customer details.

**4.4. Subclasses of SQL Injection**

SQL Injection can be classified into three major categories – In-band SQLi, Inferential SQLi and Out-of-band SQLi.

## 1.In-band SQLi (Classic SQLi)

In-band SQL Injection is the most common and easy-to-exploit of SQL Injection attacks. In-band SQL Injection occurs when an attacker is able to use the same communication channel to both launch the attack and gather results.

The two most common types of in-band SQL Injection are Error-based SQLi and Union-based SQLi.

### Error-based SQLi

Error-based SQLi is an in-band SQL Injection technique that relies on error messages thrown by the database server to obtain information about the structure of the database. In some cases, error-based SQL injection alone is enough for an attacker to enumerate an entire database. While errors are very useful during the development phase of a web application, they should be disabled on a live site, or logged to a file with restricted access instead.

### Union-based SQLi

Union-based SQLi is an in-band SQL injection technique that leverages the UNION SQL operator to combine the results of two or more SELECT statements into a single result which is then returned as part of the HTTP response.

## 2.Inferential SQLi (Blind SQLi)

Inferential SQL Injection, unlike in-band SQLi, may take longer for an attacker to exploit, however, it is just as dangerous as any other form of SQL Injection. In an inferential SQLi attack, no data is actually transferred via the web application and the attacker would not be able to see the result of an attack in-band (which is why such attacks are commonly referred to as “[blind SQL Injection attacks](https://www.acunetix.com/websitesecurity/blind-sql-injection/)”). Instead, an attacker is able to reconstruct the database structure by sending payloads, observing the web application’s response and the resulting behavior of the database server.

The two types of inferential SQL Injection are Blind-boolean-based SQLi and Blind-time-based SQLi.

### Boolean-based (content-based) Blind SQLi

Boolean-based SQL Injection is an inferential SQL Injection technique that relies on sending an SQL query to the database which forces the application to return a different result depending on whether the query returns a TRUE or FALSE result.

### Time-based Blind SQLi

Time-based SQL Injection is an inferential SQL Injection technique that relies on sending an SQL query to the database which forces the database to wait for a specified amount of time (in seconds) before responding. The response time will indicate to the attacker whether the result of the query is TRUE or FALSE.

## 3.Out-of-band SQLi

[Out-of-band SQL Injection](https://www.acunetix.com/blog/articles/blind-out-of-band-sql-injection-vulnerability-testing-added-acumonitor/) is not very common, mostly because it depends on features being enabled on the database server being used by the web application. Out-of-band SQL Injection occurs when an attacker is unable to use the same channel to launch the attack and gather results.

Out-of-band techniques, offer an attacker an alternative to inferential time-based techniques, especially if the server responses are not very stable (making an inferential time-based attack unreliable).

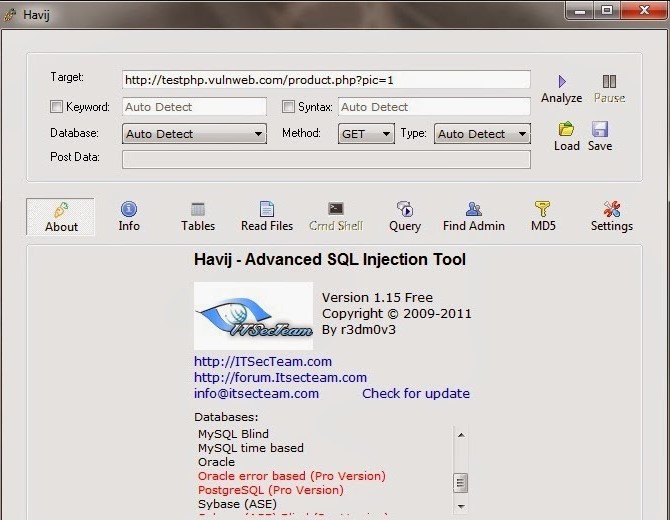
Out-of-band SQLi techniques would rely on the database server’s ability to make DNS or HTTP requests to deliver data to an attacker. Such is the case with Microsoft SQL Server’s xp\_dirtree command, which can be used to make DNS requests to a server an attacker controls; as well as Oracle Database’s UTL\_HTTP package, which can be used to send HTTP requests from SQL and PL/SQL to a server an attacker control.

**4.5. Experiment and result**

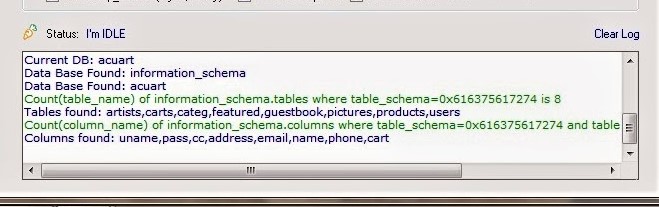
**Objective: To perform SQL injection on by using Havij tool on** [**http://testphp.vulnweb.com**](http://testphp.vulnweb.com)

**Procedure:**

* Find [**SQL injection Vulnerability**](http://silentethical-hacker.blogspot.in/2013/11/sql-injection-is-not-cup-of-cake-2.html) in tour site and insert the string (like http://testphp.vulnweb.com) of it in Havij**.** Now click on the Analyze button
* Now click on the Tables button and then click Get Tables button from below column



* Now select any one Table and then click Get columns button
* Now select desired columns and click on get data to get the result



**4.6. Preventive steps to avoid SQL Injection**

* 1. [Install a security plugin](https://www.malcare.com/blog/preventing-sql-injections/#easy1)
  2. [Only use trusted themes and plugins](https://www.malcare.com/blog/preventing-sql-injections/#easy2)
  3. [Delete any pirated software on your site](https://www.malcare.com/blog/preventing-sql-injections/#easy3)
  4. [Delete inactive themes and plugins](https://www.malcare.com/blog/preventing-sql-injections/#easy4)
  5. [Update your website regularly](https://www.malcare.com/blog/preventing-sql-injections/#easy5)

6.[Change the default database name](https://www.malcare.com/blog/preventing-sql-injections/#tech1)

7.[Control field entries and data submissions](https://www.malcare.com/blog/preventing-sql-injections/#tech2)

8.[Harden your WordPress website](https://www.malcare.com/blog/preventing-sql-injections/#tech3)

**4.7. Conclusions**

SQL injection is one of the more common and more effective forms of attack on a system. Controlling the malicious SQL code/script on the web application and maintaining the end privacy is still a key challenge for the web developer. These issues must be considered seriously by the web developers involved in developing websites using databases.

**5.Sniffing Data**

**INDEX**

|  |
| --- |
| Content |
| 1. Abstract |
| 1. Introduction |
| 1. What is Sniffing? |
| 1. Types of Sniffing |
| 1. Protocols which are affected |
| 1. Hardware protocol analyzer |
| 1. Experiment and result |
| 1. Conclusion |

**5.1. Abstract**

The number of network user is rapidly increasing day by day which reflects the growth of Network Traffic also. For a large network, it’s a very complicated task to monitor the network because a large number of packets are available. For this purpose, Sniffing is used. Sniffing is important in Network Monitoring to Network activities which help network administrators to find out the weakness of network. By working with network sniffing tool Wireshark, we can capture Traffic as well as capture analysed traffic.

**Keywords: Wireshark tool, Kali Linux, http://demotestfire.net/**

**5.2.**  **Introduction**

Sniffers are used by network administrators to keep track of data traffic passing through their network. Data packets captured from a network are used to extract and steal sensitive information such as passwords, usernames, credit card information, etc. Attackers install these sniffers in the system in the form of software or hardware. There are different types of [sniffing tools](https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_sniffing_tools.htm) used and they include:

Wireshark,

Ettercap,

BetterCAP,

Tcpdump,

WinDump, etc.

**5.3. What is Sniffing?**

[Sniffing](https://www.greycampus.com/blog/information-security/what-is-a-sniffing-attack-and-how-can-you-defend-it) is a process of monitoring and capturing all data packets passing through given network. Sniffers are used by network/system administrator to monitor and troubleshoot network traffic. Attackers use sniffers to capture data packets containing sensitive information such as password, account information etc.

**5.4. Types of Sniffing**

## There are two types:

### Active Sniffing:

### Sniffing in the switch is active sniffing. A switch is a point to point network device. The switch regulates the flow of data between its ports by actively monitoring the MAC address on each port, which helps it pass data only to its intended target. In order to capture the traffic between target sniffers has to actively inject traffic into the LAN to enable sniffing of the traffic.  This can be done in various ways.

### Passive Sniffing:

This is the process of sniffing through the hub. Any traffic that is passing through the non-switched or unbridged network segment can be seen by all machines on that segment. Sniffers operate at the data link layer of the network. Any data sent across the LAN is actually sent to each and every machine connected to the LAN. This is called passive since sniffers placed by the attackers passively wait for the data to be sent and capture them.

**5.5. Protocols which are affected**

* **HTTP** − It is used to send information in the clear text without any encryption and thus a real target.
* **SMTP** (Simple Mail Transfer Protocol) − SMTP is basically utilized in the transfer of emails. This protocol is efficient, but it does not include any protection against sniffing.
* **NNTP** (Network News Transfer Protocol) − It is used for all types of communications, but its main drawback is that data and even passwords are sent over the network as clear text.
* **POP** (Post Office Protocol) − POP is strictly used to receive emails from the servers. This protocol does not include protection against sniffing because it can be trapped.
* **FTP** (File Transfer Protocol) − FTP is used to send and receive files, but it does not offer any security features. All the data is sent as clear text that can be easily sniffed.
* **IMAP** (Internet Message Access Protocol) − IMAP is same as SMTP in its functions, but it is highly vulnerable to sniffing.
* **Telnet** − Telnet sends everything (usernames, passwords, keystrokes) over the network as clear text and hence, it can be easily sniffed.

**5.6. Hardware Protocol Analyzer**

**Hardware protocol analyzers** plug into the network at the hardware level and can monitor traffic without manipulating it.

* Hardware protocol analyzers are used to monitor and identify malicious network traffic generated by hacking software installed in the system.
* They capture a data packet, decode it, and analyze its content according to certain rules.
* Hardware protocol analyzers allow attackers to see individual data bytes of each packet passing through the cable.

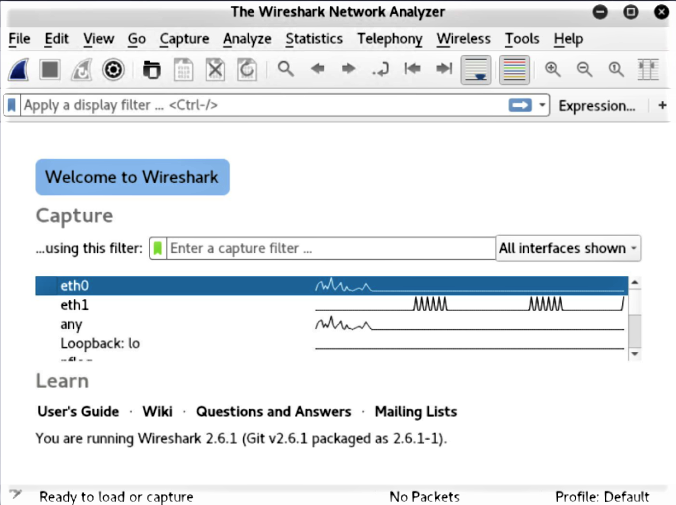
These hardware devices are not readily available to most ethical hackers due to their enormous cost in many cases.

**5.7. Experiment and result**

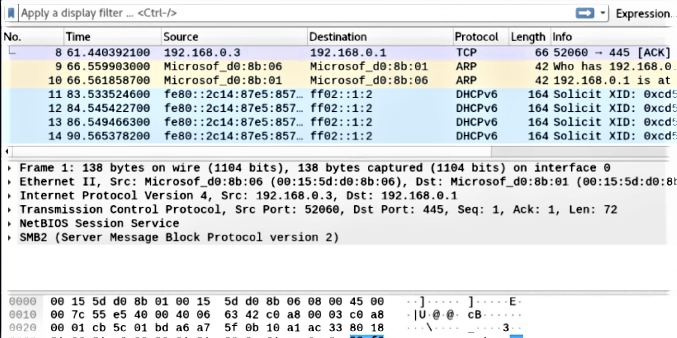
**Objective: Use Wireshark tool to sniff the data and try to get the username and password of** [**http://demotestfire.net/**](http://demotestfire.net/)

**Procedure:**

* Open Wireshark, you see a screen that shows you a list of all of the network connections you can monitor.
* One or more of the network interfaces can be selected using “shift left-click.” Once you have the network interface selected, you can start the capture, and there are several ways to do that.
* Click the first button on the toolbar, titled “Start Capturing Packets.”



* You can select the menu item Capture -> Start.
* During the capture, Wireshark will show you the packets that it captures in real-time.
* Then click on stop the capture



**5.8. Conclusion**

Sniffing can be used for either good or evil depending on the intentions of the person using the program. It can help with analyzing network problems and detect misuses in the network for good purposes. Meanwhile, it can also help hackers and other cyber-criminals steal data from insecure networks and commit crimes, as in the case of Dave & Buster’s. The best way to protect data from being “sniffed” is to encrypt it. Necessary policies and training also help with the protection.

**6.Encryption of data**

**INDEX**

|  |
| --- |
| Content |
| 1. Abstract |
| 1. Introduction |
| 1. What is encryption of data |
| 1. What is cryptography? |
| 1. Types of Cryptography |
| 1. Cryptography Techniques |
| 1. What is Steganography? |
| 1. Types of Steganography |
| 1. Advantages |
| 1. Experiment and result |
| 1. Conclusion |

**6.1. Abstract**

The security of data transmitted across a global network has turned into a key factor on the network performance measures. So, the confidentiality and the integrity of data are needed to prevent eavesdroppers from accessing and using transmitted data. Steganography and Cryptography are two important techniques that are used to provide network security. In this paper, we survey a number of methods combining cryptography and steganography techniques in one system. Moreover, we present some differences between cryptography and steganography.

**Keywords: Stego tool or Stegosuite, Kali Linux, an image, notepad, command prompt**

**6.2. Introduction**

The development of new transmission technologies forces a specific strategy of security mechanisms especially in state of the data communication. The significance of network security is increased day by day as the size of data being transferred across the Internet. Cryptography and steganography provide most significant techniques for information security. The most important motive for the attacker to benefit from intrusion is the value of the confidential data he or she can obtain by attacking the system. Hackers may expose the data, alter it, distort it, or employ it for more difficult attacks. A solution for this issue is using the advantage of cryptography and steganography combined in one system

**6.3. What is Encryption of data?**

In the computing world, encryption is the conversion of data from a readable format into an encoded format that can only be read or processed after it's been decrypted.

Encryption is the basic building block of data security and is the simplest and most important way to ensure a computer system's information can't be stolen and read by someone who wants to use it for nefarious means.

Utilized by both individual users and large corporations, encryption is widely used on the internet to ensure the sanctity of user information that's sent between a browser and a server.

That information could include everything from payment data to personal information. Firms of all sizes typically use [encryption to protect sensitive data](https://www.kaspersky.com/blog/encryption-kes10/15123/) on their servers and databases.

**6.4. What is Cryptography?**

Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it.

In computer science, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher. These deterministic algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on the internet, and confidential communications such as credit card transactions and email.

**6.5. Types of Cryptography**

There are three types of cryptography:

1.Symmetric Key Cryptography:  
It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system is Data Encryption System (DES).

2.Asymmetric Key Cryptography:  
Under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows the private key.

3.Hash Functions:  
There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.

**6.6. Cryptography techniques**

Cryptography is closely related to the disciplines of [cryptology](https://searchsecurity.techtarget.com/definition/cryptology) and [cryptanalysis](https://searchsecurity.techtarget.com/definition/cryptanalysis). It includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling [plaintext](https://searchsecurity.techtarget.com/definition/plaintext) (ordinary text, sometimes referred to as cleartext) into [ciphertext](https://whatis.techtarget.com/definition/ciphertext) (a process called [encryption](https://searchsecurity.techtarget.com/definition/encryption)), then back again (known as decryption).

**6.7. What is Steganography?**

Steganography is the practice of hiding a secret message inside of (or even on top of) something that is not secret. That something can be just about anything you want. These days, many examples of steganography involve embedding a secret piece of text inside of a picture. Or hiding a secret message or script inside of a Word or Excel document.

The purpose of steganography is to conceal and deceive. It is a form of covert communication and can involve the use of any medium to hide messages.

**6.8. Types of Steganography**

There are five types of Steganography

1. Text Steganography
2. Image Steganography
3. Audio Steganography
4. Video Steganography
5. Network Steganography

**6.9.** **Advantages**

Steganography and cryptography alone are insufficient for the security of information, therefore If we combine these systems, we can generate more reliable and strong approach. The combination these two strategies will improve the security of the information secret. This combined will fulfil the prerequisites, for example, memory space, security, and strength for important information transmission across an open channel. Also, it will be a powerful mechanism which enables people to communicate without interferes of eavesdroppers even knowing there is a style of communication in the first place.

**6.10. Experiment and result**

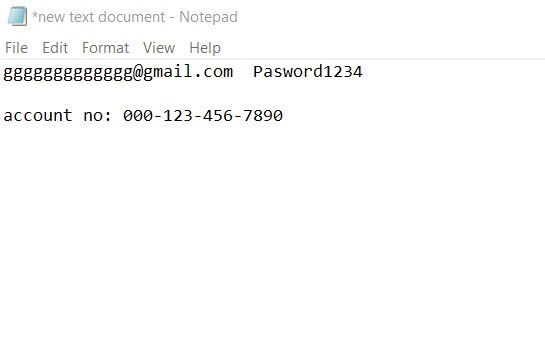
**Objective: Try to Encrypt the data in an image file using quick stego tool and command prompt also and show them how to decrypt also**.

**Procedures:**

To form the stego- image we require two files, first cover image file and second message file. Before embedding process, the system must know the size of the cover image file. image will be combined with message to produce the stego-image, In the LSB technique, the LSB of the pixels is replaced by the message to be sent. The message bits are permuted before embedding, this has the effect of distributing the bits evenly, thus on average only half of the LSB's will be modified. Popular steganographic tools based on LSB embedding, vary in their approach for hiding information. Some algorithms change LSB of pixels visited in a random walk, others modify pixels in certain areas of images, or instead of just changing the last bit they increment or decrement the pixel value

**Hiding texts in the image file**

Find an image and a document that you want to conceal and place them in a folder.





Now, open the CMD (Command Prompt) and navigate to the folder where you keep your original image and a secret document.

**Ex:** (cd C:\Users\hp\Downloads\New folder).

Next, type the following command to combine the image and a secret document into a stego image, and then specify a name to output the result as a “JPG” file. In our example, we named the stego image as “secret-image.jpg.”

**Ex**: (copy/b “C:\Users\hp\Download\New folder\the-road-815297\_\_340.jpg” +C:\Users\hp\Downloads\New folder\New Text Document.txt” secter-image.jpg).

To read the secret message from the stego image file, you need to open it up with a notepad or similar application and scroll down to the bottom of the page. There you’ll be able to view and read the document you’ve embedded into the image

**6.11. Conclusion**

Cryptography is the study of hiding information, while Steganography deals with composing hidden messages so that only the sender and the receiver know that the message even exists. In Steganography, only the sender and the receiver know the existence of the message, whereas in cryptography the existence of the encrypted message is visible to the world. Due to this, Steganography removes the unwanted attention coming to the hidden message. Cryptographic methods try to protect the content of a message, while Steganography uses methods that would hide both the message as well as the content.