LAB MANUAL
for
NETWORK
SECURITY

6th Semester
Diploma in Computer Engineering

Prepared By PINKI
Department of Computer Science
Raja Jait Singh Govt. Polytechnic, Neemka Faridabad

GENERAL INSTRUCTIONS

1) Students are instructed to bring their Lab Record to the Lab.

2) Students should come to the Lab in time.

3) Students should be in a proper Uniform.

4) It is mandatory to enter your name in Log-in-Register.

5) Headphones should not be used for any other purpose except for listening to the software.

6) Students are not allowed into the lab without I.D. Cards.

7) After completion of any experiment/activity the student must record it in Lab record and get it signed by the faculty-in-charge.

8) Use of mobile phones during lab hours is strictly prohibited.

9) All students should actively participate in the lab activities.

10) You will not be allowed to copy any software in any format.

11) Marks will be awarded on the basis of the performance in each experiments

INDEX

ABOUT NETWORK SECURITY :➔ Network security is **any activity designed to protect the usability and integrity of your network and data**. It includes both hardware and software technologies. It targets a variety of threats. It stops them from entering or spreading on your network. Effective network security manages access to the network.

INSTRUCTIONS TO STUDENTS FOR PREPARING A LAB REPORT

This Lab Manual is prepared to help the students with their practical understanding and development of skills, and may be used as a base reference during the lab/practical classes.
Students have to submit Lab Exercise report of previous lab into corresponding next lab, and can be collected back after the instructor/course co-ordinator after it has been checked and signed. At the end of the semester, students should compile all the Lab Exercise reports into a single report and submit during the end semester sessional examination.
The lab report to be submitted during the end semester Sessional Examination should include at least the following topics:-

1. Top Cover page
2. Index
3. Title of the program
8. Output (compilation)

PRACTICAL NO.:-1

AIM: - Installation and comparison of various antivirus software.

INTRODUCTION:-

Software that is created specifically to help detect, prevent and remove malware (malicious software).

Antivirus is a kind of software used to prevent, scan, detect and delete viruses from a computer. Once installed, most antivirus software runs automatically in the background to provide real-time protection against virus attacks.

Comprehensive virus protection programs help protect your files and hardware from malware such as worms, Trojan horses and spyware, and may also offer additional protection such as customizable firewalls and website blocking.

Common types of cyber threats
As the Internet of Things (IoT) grows, so does the risk of cybercrime for mobile phones and other internet-connected devices, not just your personal computer. According to Symantec's Internet Security Threat Report 2018, malware for mobile devices including spyware, ransomware and viruses increased 54% in 2017; and data breaches and identity theft are also on the rise.

How does antivirus work?

Antivirus software begins operating by checking your computer programs and files against a database of known types of malware. Since new viruses are constantly created and distributed by hackers, it will also scan computers for the possibility of new or unknown type of malware threats.

If your computer does not have an antivirus program installed and running, we highly recommend you install one today. Follow the steps below for help on how to install and update an antivirus program on your computer.

Install the antivirus program

To install an antivirus program on your computer, follow the steps below.

1. If you purchased the antivirus program from a retail store, insert the CD or DVD into the computer's disc drive. The installation process should start automatically, with a window opening to help guide you through the install process.

2. If you downloaded the antivirus program on the Internet, find the downloaded file on your computer. If the downloaded file is a zip file, unzip the file to extract and access the installation files. Look for a file named **setup.exe**, **install.exe**, or something similar,

then double-click that file. The installation process should start, with a window opening to help guide you through the install process.

3. In the installation process window, follow the steps provided to install the antivirus program. The install process provides recommended options so the antivirus program will function properly, which in most cases can be accepted as is. The one exception is if the install process recommends to install any toolbars for Internet browsers or other helpful programs for your computer. If prompted to install other software with the antivirus program, uncheck all boxes or decline the install of those extra programs. No additional programs should be needed for the antivirus program to install and run successfully on your computer.

4. When the install process is complete, close out of the install window.

5. If used, remove the CD or DVD from the computer's disc drive.

The antivirus program is now installed and ready to use. While it may not be required, we recommend restarting your computer so that any modified settings in the operating system can take effect correctly.

Comparison of various antivirus software:-

Company	Software	On-demand scan	On-access scan	Cloud AV	Firewall	IPS	Email Security	Web protection	Price	First release
Avast	Avast Free Antivirus	Yes	Yes	Yes	No	No	Yes	Yes	Free	1988
Avast	Avast Premium Security	Yes	Yes	Yes	Yes	No	Yes	Yes	Trialware	1997

Company	Software	On-demand scan	On-access scan	Cloud AV	Firewall	IPS	Email Security	Web protection	Price	First release
AVG Technologies (avast)	AVG Antivirus FREE	Yes	Yes	No	No	No	No	Yes	Free	1992
AVG Technologies (avast)	AVG Antivirus	Yes	Yes	Yes	No	No	Yes	Yes	Non-free	2006
AVG Technologies (avast)	AVG Internet Security	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Non-free	2008
Avira	Avira Antivirus FREE	Yes	Yes	Yes	No	No	No	No	Free	1988
Avira	Avira Internet Security	Yes	Yes	Yes	No	No	Yes	Yes	Non-free	2002
Cisco (originally Immun	Immunet	Yes	Yes	Yes	No	No	Yes	No	Free	2010

Company	Software	On-demand scan	On-access scan	Cloud AV	Firewall	IPS	Email Security	Web protection	Price	First release
et)										
Dr.Web	Dr.Web Anti-virus	Yes	Yes	Yes	Yes	Yes	No	Yes *	Trialware	1992
Dr.Web	Dr.Web Security Space	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Trialware	2006
McAfee	McAfee Antivirus	Yes	Yes	No	No	No	Yes	No	Non-free	1987
McAfee	McAfee Internet Security	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Non-free	2006
Panda Security	Panda Antivirus Pro	Yes	Yes	Yes	Yes	No	No	No	Non-free	1990

PRACTICAL NO.:-2

Aim:- Installation and study of various parameters of firewall.

Firewall

A firewall is a **network security** device that monitors incoming and outgoing network traffic and permits or blocks data **packets** based on a set of security rules. Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.

How does a firewall work?

Firewalls carefully analyze incoming traffic based on pre-established rules and filter traffic coming from unsecured or suspicious sources to prevent attacks. Firewalls guard traffic at a computer’s entry point, called ports, which is where information is exchanged with external devices.

Think of IP addresses as houses, and port numbers as rooms within the house. Only trusted people (source addresses) are allowed to enter the house (destination address) at all—then it’s further filtered so that people within the house are only allowed to access certain rooms (destination ports), depending on if they're the owner, a child, or a guest. The owner is allowed to any room (any port), while children and guests are allowed into a certain set of rooms (specific ports).

How to install:-

1. Select the **Start** button > **Settings** > **Update & Security** > **Windows Security** and then **Firewall & network protection**. Open Windows Security settings
2. Select a network profile: **Domain network**, **Private network**, or **Public network**.
3. Under **Microsoft Defender Firewall**, switch the setting to **On**. If your device is connected to a network, network policy settings might prevent you from completing these steps. For more info, contact your administrator.
4. To turn it off, switch the setting to **Off**. Turning off Microsoft Defender Firewall could make your device (and network, if you have one) more vulnerable to unauthorized access. If there's an app you need to use that's being blocked, you can allow it through the firewall, instead of turning the firewall off.

PRACTICAL NO.:-3

AIM:- Writing program in C to Encrypt/Decrypt using XOR key.

XOR Encryption is an encryption method used to encrypt data and is hard to crack by brute-force method, i.e generating random encryption keys to match with the correct one.

Below is a simple implementation in C++. The concept of implementation is to first define XOR – encryption key and then to perform XOR operation of the characters in the String with this key which you want to encrypt. To decrypt the encrypted characters we have to perform XOR operation again with the defined key. Here we are encrypting the entire String.

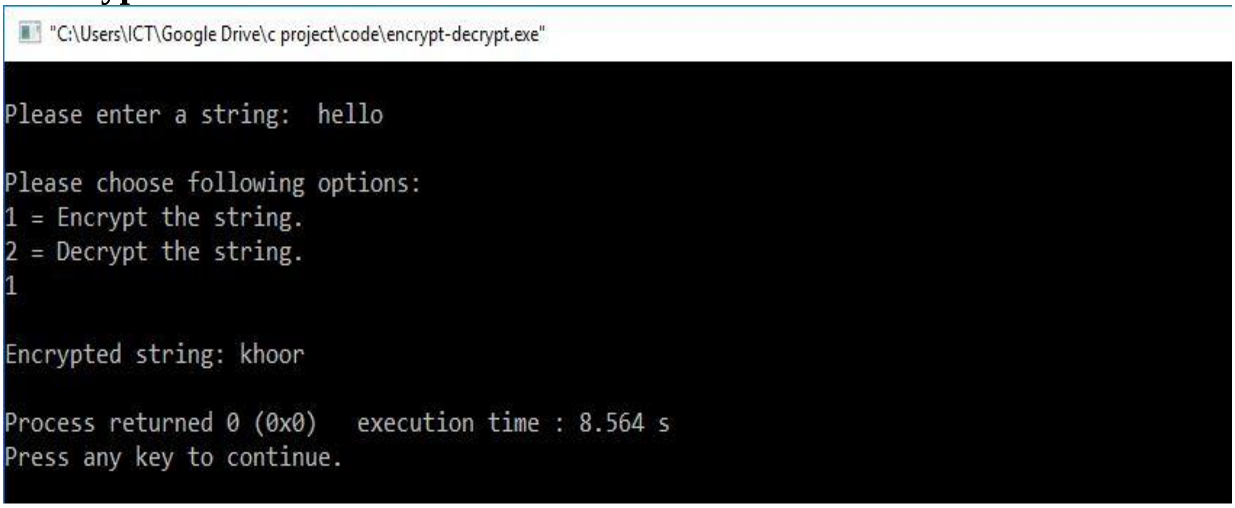
C++

```
// C++ program to implement XOR - Encryption

#include<bits/stdc++.h>

// The same function is used to encrypt and

// decrypt

void encryptDecrypt(char inpString[])

{

    // Define XOR key

    // Any character value will work

    char xorKey = 'P';

    // calculate length of input string

    int len = strlen(inpString);
    // perform XOR operation of key
    // with every character in string
    for (int i = 0; i < len; i++)
    {
        inpString[i] = inpString[i] ^ xorKey;
        printf("%c",inpString[i]);
    }
}
// Driver program to test above function
int main()
{
    char sampleString[] = "GeeksforGeeks";
    // Encrypt the string
    printf("Encrypted String: ");
    encryptDecrypt(sampleString);
    printf("\n");
    // Decrypt the string
    printf("Decrypted String: ");
    encryptDecrypt(sampleString);
    return 0;
```

```
//Simple C program to encrypt and decrypt a string

#include <stdio.h>

int main()

{

  int i, x;

  char str[100];

  printf("\nPlease enter a string:\t");

  gets(str);

  printf("\nPlease choose following options:\n");

  printf("1 = Encrypt the string.\n");

  printf("2 = Decrypt the string.\n");

  scanf("%d", &x);

  //using switch case statements

  switch(x)

  {

  case 1:

    for(i = 0; (i < 100 && str[i] != '\0'); i++)

      str[i] = str[i] + 3; //the key for encryption is 3 that is added to ASCII value
    printf("\nEncrypted string: %s\n", str);

    break;

  case 2:

    for(i = 0; (i < 100 && str[i] != '\0'); i++)

      str[i] = str[i] - 3; //the key for encryption is 3 that is subtracted to ASCII value

    printf("\nDecrypted string: %s\n", str);

    break;

  default:

    printf("\nError\n");

  }

  return 0;

}
```

Output

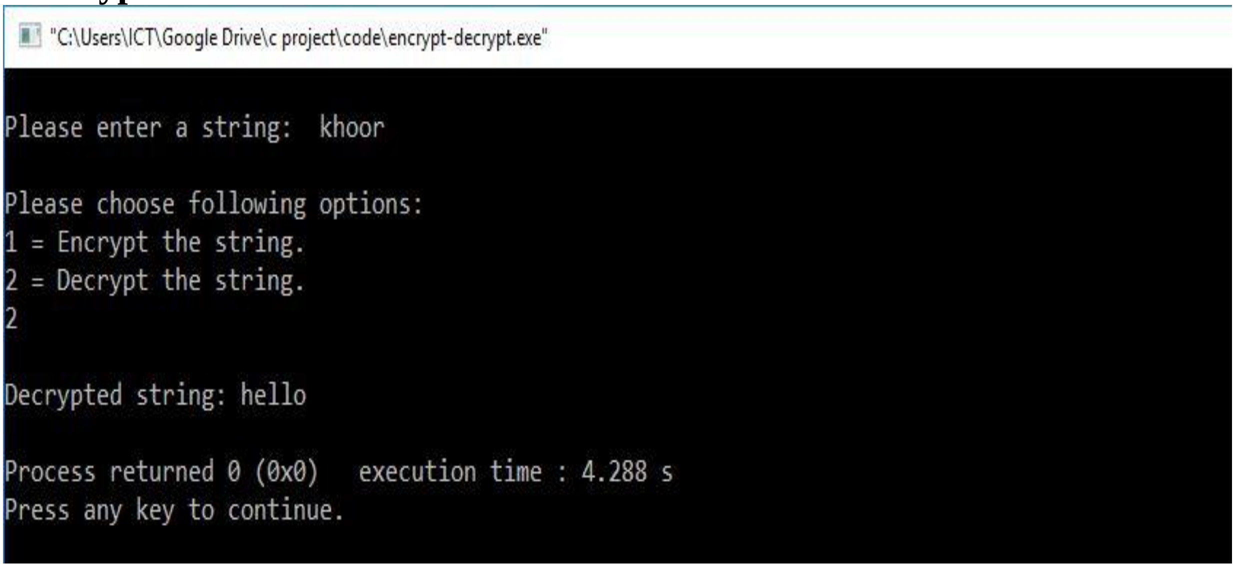
#Encryption



"C:\Users\ICT\Google Drive\c project\code\encrypt-decrypt.exe"

```
Please enter a string:  hello

Please choose following options:
1 = Encrypt the string.
2 = Decrypt the string.
1

Encrypted string: khoor

Process returned 0 (0x0)   execution time : 8.564 s
Press any key to continue.
```

#Decryption



"C:\Users\ICT\Google Drive\c project\code\encrypt-decrypt.exe"

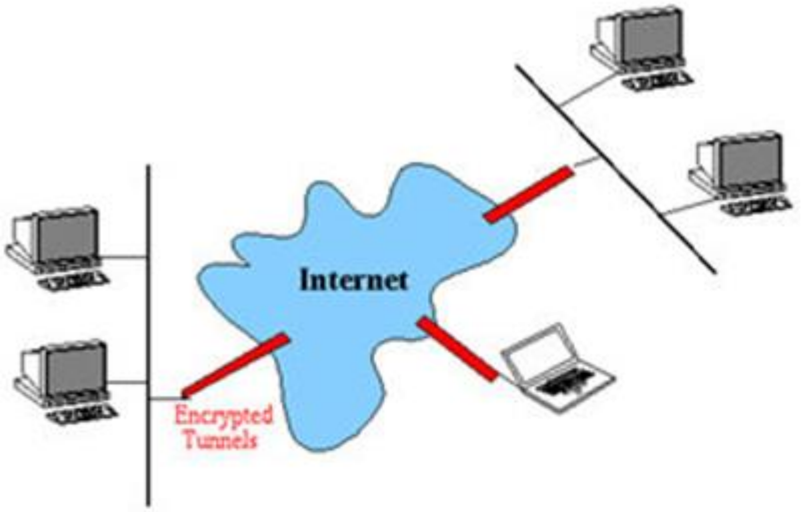
```
Please enter a string:  khoor

Please choose following options:
1 = Encrypt the string.
2 = Decrypt the string.
2

Decrypted string: hello

Process returned 0 (0x0)   execution time : 4.288 s
Press any key to continue.
```

PRACTICAL NO.:-4

AIM:- Study of VPN

VPN: Virtual Private Network

VPN stands for Virtual Private Network. It refers to a safe and encrypted network that allows you to use network resources in a remote manner. Using VPN, you can create a safe connection over a less secure network, e.g. internet. It is a secure network as it is completely isolated from rest of the internet. The government, businesses, military can use this network to use network resources securely.



VPN is free to use and it uses site-to-site and remote access methods to work. It uses an arrangement of encryption services to establish a secure connection. It is an ideal tool for encryption; it provides you strong AES256 encryption with an 8192bit key.

How VPN Works?

VPN works by creating a secure tunnel using powerful VPN protocols. It hides your IP address behind its own IP address that encrypts all your communication. Thus, your communication passes through a secure tunnel that allows you use network resources freely and secretly.

VPN protocols

There are several different VPN protocols that are used to create secure networks. Some of such protocols are given below;

Skip Ad

- IP security (IPsec)

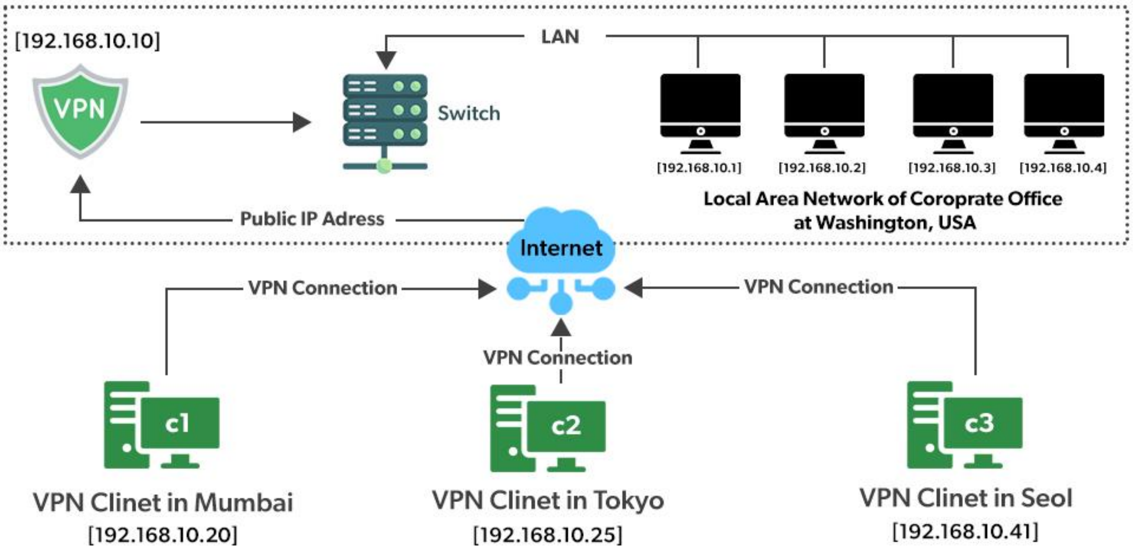
- Point to Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol (L2TP)
- Secure Sockets Layer (SSL) and Transport Layer Security (TLS)

VPN stands for the virtual private network. A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet. A Virtual Private Network is a way to extend a private network using a public network such as the internet. The name only suggests that it is a Virtual “private network” i.e. user can be part of a local network sitting at a remote location. It makes use of tunneling protocols to establish a secure connection.

Lets understand VPN by an example:
Think of a situation where corporate office of a bank is situated in Washington, USA. This office has a local network consisting of say 100 computers. Suppose other branches of the bank are in Mumbai, India, and Tokyo, Japan. The traditional method of establishing a secure connection between head office and branch was to have a leased line between the branches and head office which was a very costly as well as troublesome job. VPN lets us overcome this issue in an effective manner.

The situation is described below:

- All 100 hundred computers of the corporate office at Washington are connected to the VPN server(which is a well-configured server containing a public IP address and a switch to connect all computers present in the local network i.e. in US head office).
- The person sitting in the Mumbai office connects to The VPN server using a dial-up window and the VPN server returns an IP address that belongs to the series of IP addresses belonging to a local network of the corporate office.
- Thus person from the Mumbai branch becomes local to the head office and information can be shared securely over the public internet.
- So this is the intuitive way of extending the local network even across the geographical borders of the country.



VPN is well exploited all across the globe

We will explain to you with an example. Suppose we are using smartphones regularly. Spotify-a Swedish music app which is not active in India But we are making full use of it sitting in India. So how ?? VPN can be used to camouflage our geolocation.

- Suppose the Ip address is 101.22.23.3 which belongs to India. That’s why our device is not able to access the Spotify music app.
- But the magic begins when we used the Psiphon app which is an android app and is used to change the device IP address to the IP address of the location we want(say US where Spotify works in a seamless manner).
- The IP address is changed using VPN technology. Basically what happens is that your device will connect to a VPN server of the respective country that you have entered in your location textbox of the Psiphon app and now you will inherit a new IP from this server.

Now we typed “what is my IP address”? Amazingly the IP address changed to 45.79.66.125 which belongs to the USA And since Spotify works well in the US, so we can use it now being in India (virtually in the USA). Is not that good? obviously, it is very useful.

PRACTICAL NO.:-5

AIM: Study of various hacking tools

Hacking tools:-

In this chapter, we will discuss in brief some of famous tools that are widely used to prevent hacking and getting unauthorized access to a computer or network system.

NMAP

Nmap stands for Network Mapper. It is an open source tool that is used widely for network discovery and security auditing. Nmap was originally designed to scan large networks, but it can work equally well for single hosts. Network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

Nmap uses raw IP packets to determine −

- what hosts are available on the network,
- what services those hosts are offering,
- what operating systems they are running on,
- what type of firewalls are in use, and other such characteristics.

Nmap runs on all major computer operating systems such as Windows, Mac OS X, and Linux.

Metasploit

Metasploit is one of the most powerful exploit tools. It's a product of Rapid7 and most of its resources can be found at: www.metasploit.com. It comes in two versions − **commercial** and **free edition**. Matasploit can be used with command prompt or with Web UI.

With Metasploit, you can perform the following operations −

- Conduct basic penetration tests on small networks
- Run spot checks on the exploitability of vulnerabilities
- Discover the network or import scan data
- Browse exploit modules and run individual exploits on hosts

Burp Suit

Burp Suite is a popular platform that is widely used for performing security testing of web applications. It has various tools that work in collaboration to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.

Burp is easy to use and provides the administrators full control to combine advanced manual techniques with automation for efficient testing. Burp can be easily configured and it contains features to assist even the most experienced testers with their work.

Angry IP Scanner

Angry IP scanner is a lightweight, cross-platform IP address and port scanner. It can scan IP addresses in any range. It can be freely copied and used anywhere. In order to increase the scanning speed, it uses multithreaded approach, wherein a separate scanning thread is created for each scanned IP address.

Angry IP Scanner simply pings each IP address to check if it’s alive, and then, it resolves its hostname, determines the MAC address, scans ports, etc. The amount of gathered data about each host can be saved to TXT, XML, CSV, or IP-Port list files. With help of plugins, Angry IP Scanner can gather any information about scanned IPs.

Cain & Abel

Cain & Abel is a password recovery tool for Microsoft Operating Systems. It helps in easy recovery of various kinds of passwords by employing any of the following methods −

- sniffing the network,
- cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks,
- recording VoIP conversations,
- decoding scrambled passwords,
- recovering wireless network keys,
- revealing password boxes,
- uncovering cached passwords and analyzing routing protocols.

Cain & Abel is a useful tool for security consultants, professional penetration testers and everyone else who plans to use it for ethical reasons.

Ettercap

Ettercap stands for Ethernet Capture. It is a network security tool for Man-in-the-Middle attacks. It features sniffing of live connections, content filtering on the fly and many other interesting tricks. Ettercap has inbuilt features for network and host analysis. It supports active and passive dissection of many protocols.

You can run Ettercap on all the popular operating systems such as Windows, Linux, and Mac OS X.

EtherPeek

EtherPeek is a wonderful tool that simplifies network analysis in a multiprotocol heterogeneous network environment. EtherPeek is a small tool (less than 2 MB) that can be easily installed in a matter of few minutes.

EtherPeek proactively sniffs traffic packets on a network. By default, EtherPeek supports protocols such as AppleTalk, IP, IP Address Resolution Protocol (ARP), NetWare, TCP, UDP, NetBEUI, and NBT packets.

SuperScan

SuperScan is a powerful tool for network administrators to scan TCP ports and resolve hostnames. It has a user friendly interface that you can use to −

- Perform ping scans and port scans using any IP range.
- Scan any port range from a built-in list or any given range.
- View responses from connected hosts.
- Modify the port list and port descriptions using the built in editor.
- Merge port lists to build new ones.
- Connect to any discovered open port.
- Assign a custom helper application to any port.

QualysGuard

QualysGuard is an integrated suite of tools that can be utilized to simplify security operations and lower the cost of compliance. It delivers critical security intelligence on demand and automates the full spectrum of auditing, compliance and protection for IT systems and web applications.

QualysGuard includes a set of tools that can monitor, detect, and protect your global network.

WebInspect

WebInspect is a web application security assessment tool that helps identify known and unknown vulnerabilities within the Web application layer.

It can also help check that a Web server is configured properly, and attempts common web attacks such as parameter injection, cross-site scripting, directory traversal, and more.

LC4

LC4 was formerly known as **L0phtCrack**. It is a password auditing and recovery application. It is used to test password strength and sometimes to recover lost Microsoft Windows passwords, by using dictionary, brute-force, and hybrid attacks.

LC4 recovers Windows user account passwords to streamline migration of users to another authentication system or to access accounts whose passwords are lost.

LANguard Network Security Scanner

LANguard Network Scanner monitors a network by scanning connected machines and providing information about each node. You can obtain information about each individual operating system.

It can also detect registry issues and have a report set up in HTML format. For each computer, you can list the **netbios** name table, current logged-on user, and Mac address.

Network Stumbler

Network stumbler is a WiFi scanner and monitoring tool for Windows. It allows network professionals to detect WLANs. It is widely used by networking enthusiasts and hackers because it helps you find non-broadcasting wireless networks.

Network Stumbler can be used to verify if a network is well configured, its signal strength or coverage, and detect interference between one or more wireless networks. It can also be used to non-authorized connections.

ToneLoc

ToneLoc stands for Tone Locator. It was a popular war dialling computer program written for MS-DOS in the early 90’s. War dialling is a technique of using a modem to automatically scan a list of telephone numbers, usually dialling every number in a local area code.

Malicious hackers use the resulting lists in breaching computer security - for guessing user accounts, or locating modems that might provide an entry-point into computer or other electronic systems.

It can be used by security personnel to detect unauthorized devices on a company’s telephone network.

PRACTICAL NO.:-6

AIM:- Practical applications of digital signature

Introduction to Digital Signature

A digital signature is an electronic signature form used for authentication of the identity of the communicator or an authority signing the document. It ensures authenticity and originality of the content of the communication or the document. Digital Signatures remain unchanged throughout the communication or documentation, they are easily transportable and it cannot be imitated by anyone else. It also makes sure that the sender cannot deny the content sent via that signed document.

Understanding Digital Signature Certificate

Digital signature certificate can be better understood as the electronic alternative to physical or paper certificates such as driving license, PAN Card, passport, etc. Digital Certificates are proof of the identity of a person having a specified purpose. For example, a passport identifies a citizen’s identity with relation to a nationality and that citizen is eligible to legally travel to any country on a grant of permission. Under these identity requirements, the digital certificate is used to electronically prove a citizen’s identity and helps access to information or services via the internet or other electronic mediums or to sign documents digitally.

Applications of Digital Signature

- To send and receive encrypted emails, that are digitally signed and secured
- To carry out secure online transactions
- To identify participants of an online transaction
- To apply for tenders, efiling with Registrar of Companies (MCA), efiling of income tax returns and other relevant applications
- To sign and validate Word, Excel and PDF document formats