LABORATORY MANUAL
FOR
NETWORK SECURITY LAB

6^{TH} Semester

Diploma in Computer Science & Engineering

C. V. Raman Polytechnic

Bidya Nagar, Mahura, Janla, Bhubaneswar

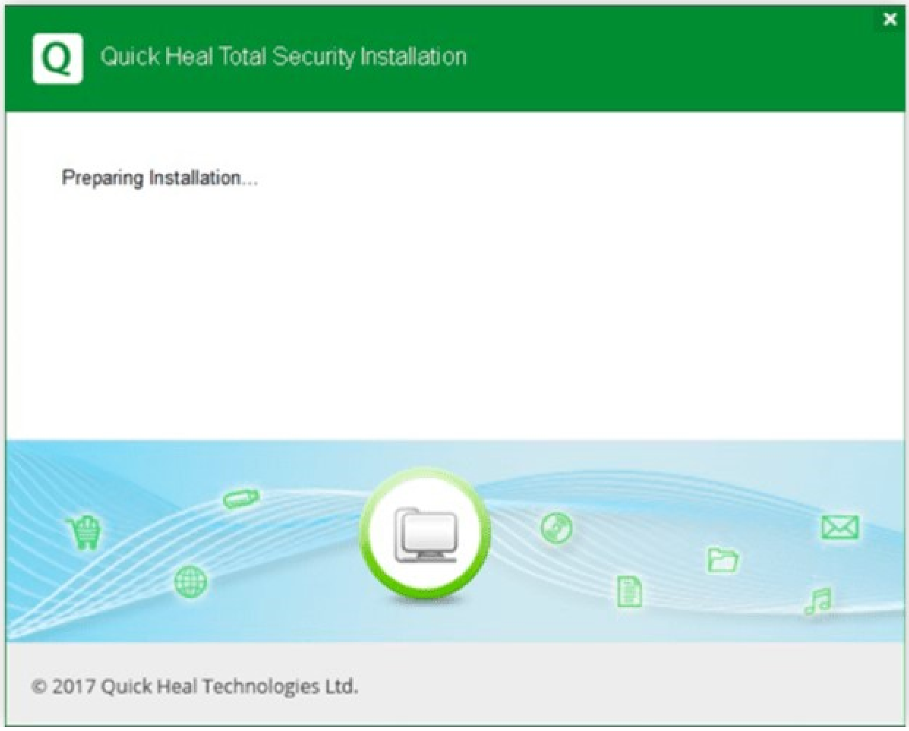
EXPERIMENT-1

Aim: Installation and comparison of various antivirus software.

Procedure and installation antivirus:

Install Quick Heal Total Security Antivirus from CD

- Insert Quick Heal CD in the CD drive of your PC.
- The installer will autorun without any external action.
- Click on Install Quick Heal.

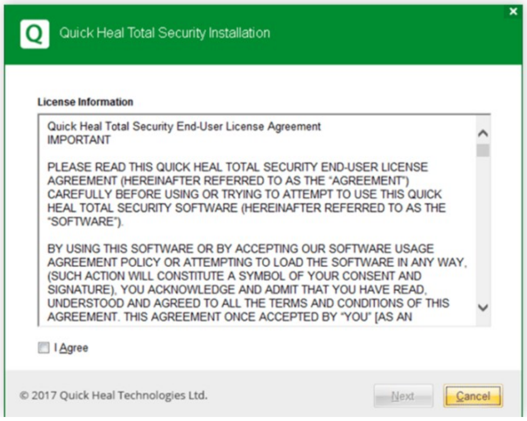


Quick Heal Total Security Installation

Preparing Installation...

© 2017 Quick Heal Technologies Ltd.

- Follow the steps in the setup wizard.
- Read the User and License and Agreement carefully and check the box that says ‘I Agree’



Quick Heal Total Security Installation

License Information

Quick Heal Total Security End-User License Agreement
IMPORTANT

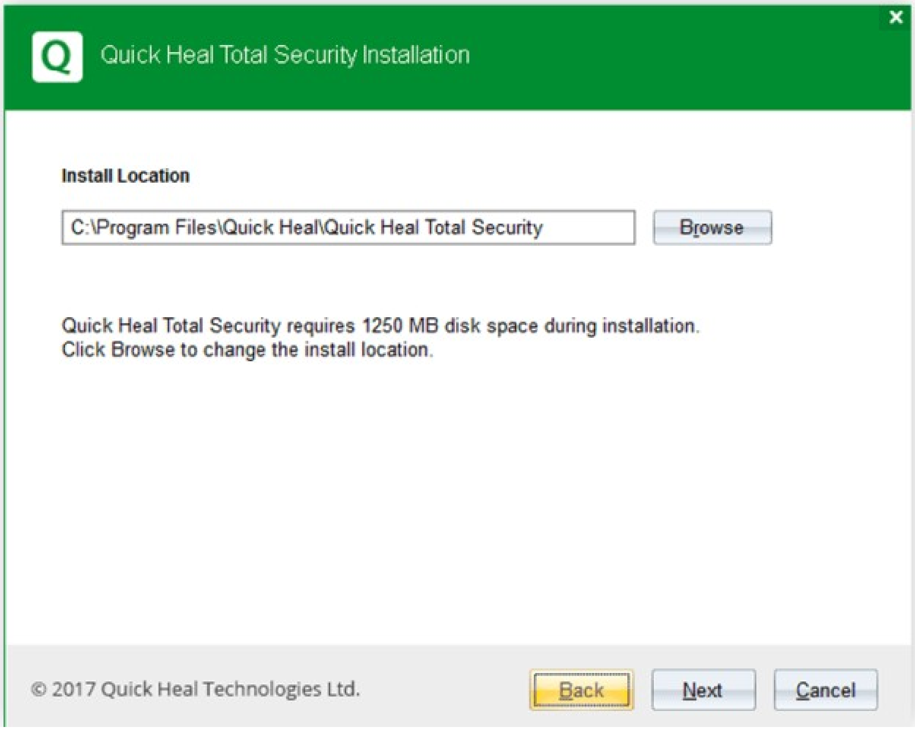
PLEASE READ THIS QUICK HEAL TOTAL SECURITY END-USER LICENSE AGREEMENT (HEREINAFTER REFERRED TO AS THE "AGREEMENT") CAREFULLY BEFORE USING OR TRYING TO ATTEMPT TO USE THIS QUICK HEAL TOTAL SECURITY SOFTWARE (HEREINAFTER REFERRED TO AS THE "SOFTWARE").

BY USING THIS SOFTWARE OR BY ACCEPTING OUR SOFTWARE USAGE AGREEMENT POLICY OR ATTEMPTING TO LOAD THE SOFTWARE IN ANY WAY, (SUCH ACTION WILL CONSTITUTE A SYMBOL OF YOUR CONSENT AND SIGNATURE), YOU ACKNOWLEDGE AND ADMIT THAT YOU HAVE READ, UNDERSTOOD AND AGREED TO ALL THE TERMS AND CONDITIONS OF THIS AGREEMENT. THIS AGREEMENT ONCE ACCEPTED BY "YOU" [AS AN

☐ I Agree

© 2017 Quick Heal Technologies Ltd.

- Select the drive where the software is to be installed.



Quick Heal Total Security Installation

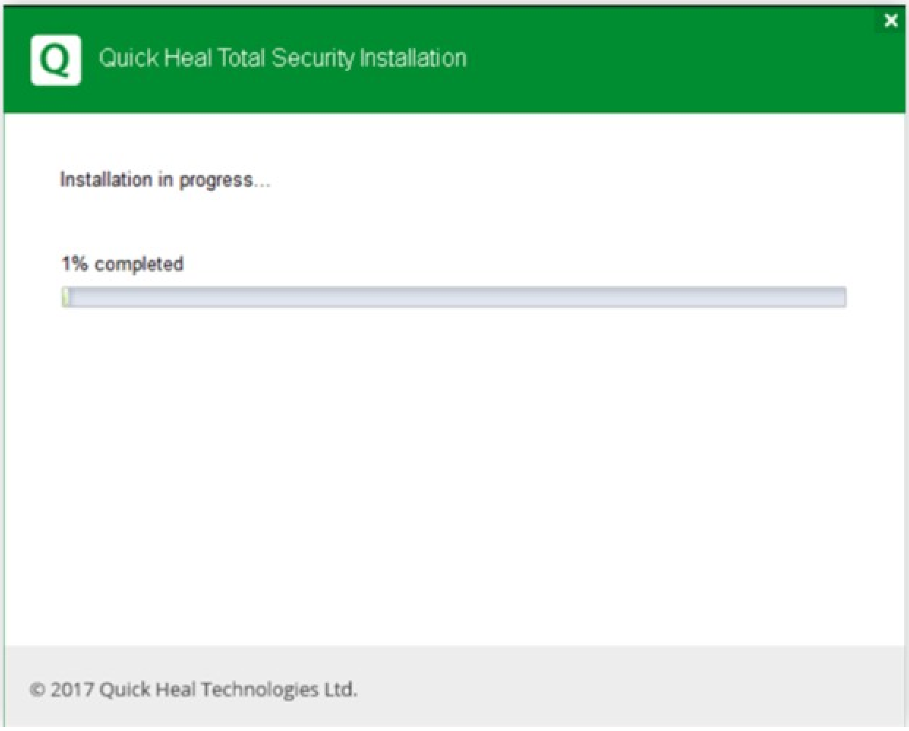
Install Location

C:\Program Files\Quick Heal\Quick Heal Total Security

Quick Heal Total Security requires 1250 MB disk space during installation.
Click Browse to change the install location.

© 2017 Quick Heal Technologies Ltd.

- Let it install files in the selected drive, till it is 100% complete.



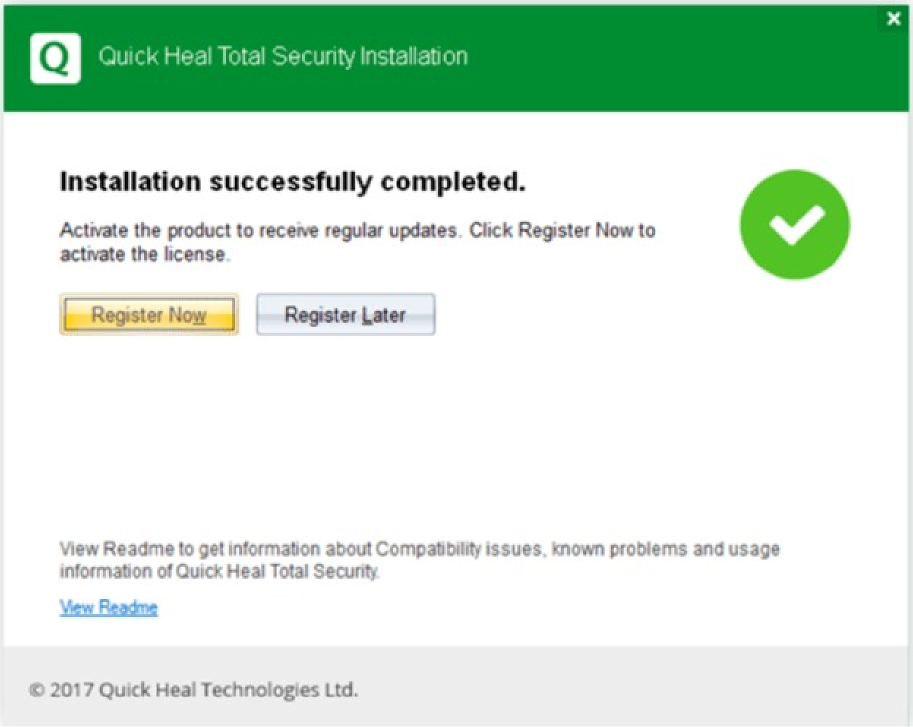
Quick Heal Total Security Installation

Installation in progress...

1% completed

© 2017 Quick Heal Technologies Ltd.

- Once completed, it will ask you to register the product. Click on 'Register Now'.



Installation successfully completed.

Activate the product to receive regular updates. Click Register Now to activate the license.

View Readme to get information about Compatibility issues, known problems and usage information of Quick Heal Total Security.

© 2017 Quick Heal Technologies Ltd.

2. Registering Quick Heal Antivirus License Offline

There are two ways of registering your Quick Heal copy. You can register offline if the system or device isn’t connected to the Internet.

Before visiting the offline activation page, ensure that you have the product key and the installation number with you.

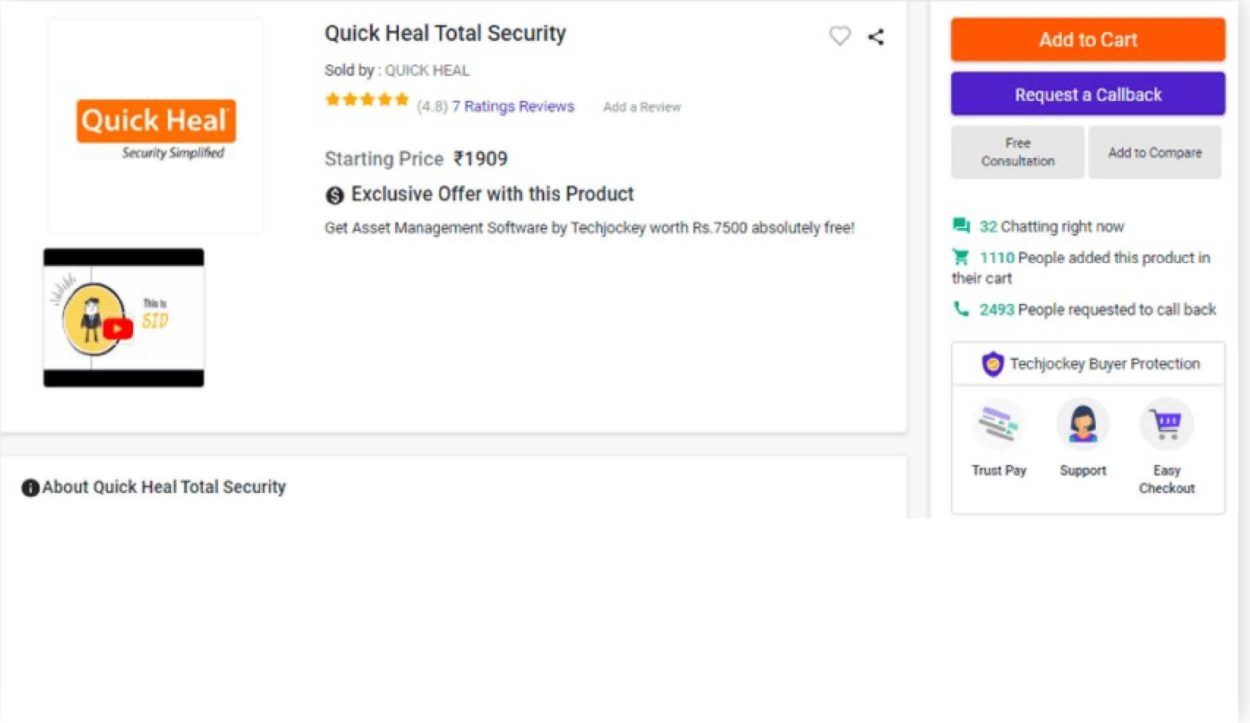
The product key can be found printed either on or inside the product packaging or will be provided when you purchase Quick Heal AntivirusTotal Security online.

With the help of a connected device, visit the offline activation page

Fill the registration form and enter the product key received after buying the product.

3. Installing Quick Heal Antivirus with Product Key Online

Buy Quick Heal Total Security key after installing the free version from the .exe file downloaded from the website. For premium and pro versions, register the product key provided with the product purchase. Here is how to register the Quick Heal Total Security antivirus online:



Quick Heal Total Security

Sold by : QUICK HEAL

★★★★★ (4.8) 7 Ratings Reviews Add a Review

Starting Price ₹1909

Exclusive Offer with this Product

Get Asset Management Software by Techjockey worth Rs.7500 absolutely free!

32 Chatting right now

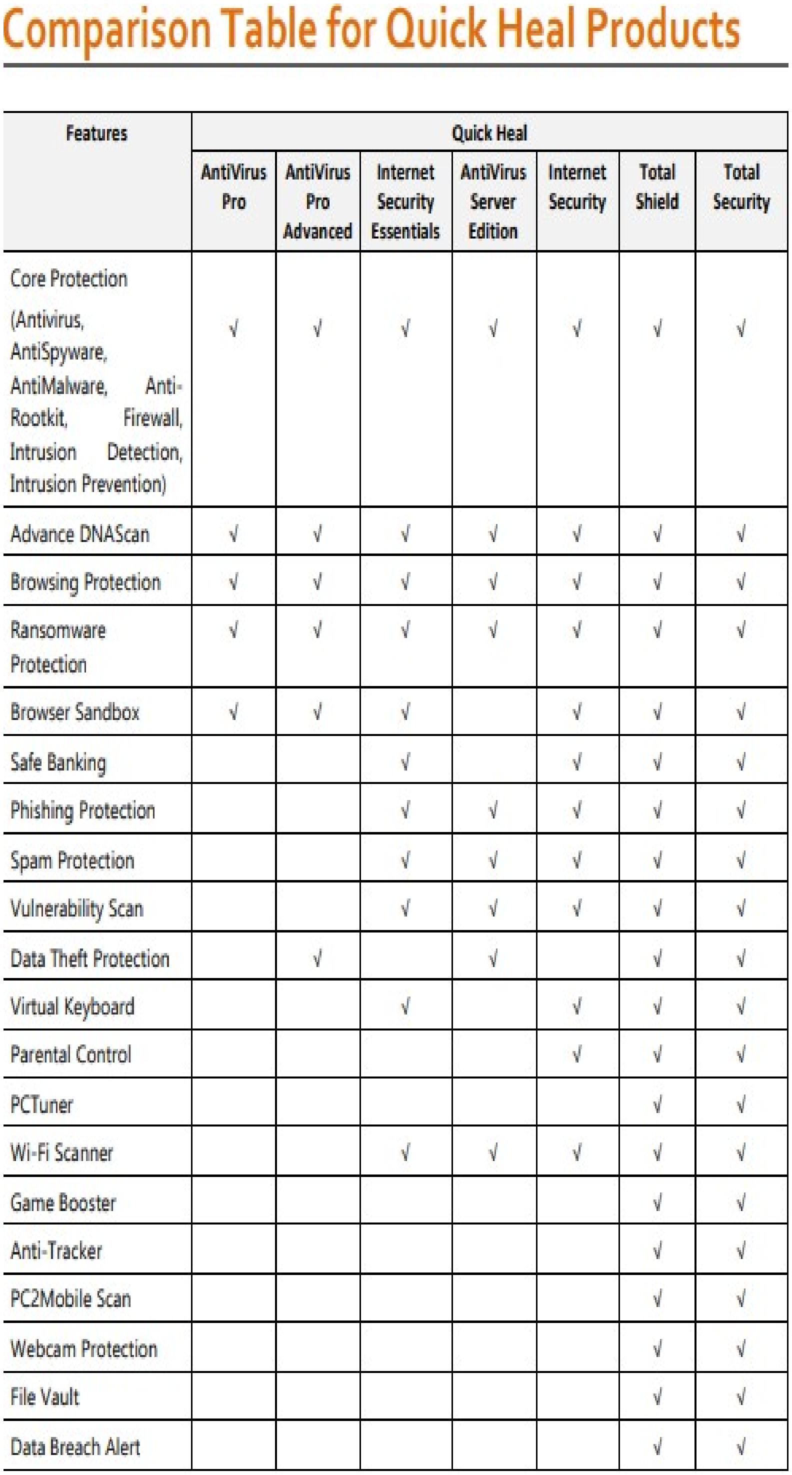
1110 People added this product in their cart

2493 People requested to call back

About Quick Heal Total Security

- Sign-in to Quick Heal from your browser.
- Type in your email id and password for Quick Heal and click ‘Sign In’.
- You can easily create account using the simple signing-up process in case you do not have an account with Quick Heal.
- Click ‘Enter’ a new product key to continue.
- Type the product key and click ‘Next’.
- Follow the instructions to activate the product.

It is crucial for users to register their copy of Quick Heal Antivirus with the product key after installation. A registered user with a license will be given complete access to all the features of Quick Heal Total Security’s features with regular updates and dedicated technical support. They will also receive Quick Heal Total Security antivirus renewal prompt when the renewal is due.



Comparison Table for Quick Heal Products

Features	Quick Heal						
	AntiVirus Pro	AntiVirus Pro Advanced	Internet Security Essentials	AntiVirus Server Edition	Internet Security	Total Shield	Total Security
Core Protection (Antivirus, AntiSpyware, AntiMalware, Anti-Rootkit, Firewall, Intrusion Detection, Intrusion Prevention)	√	√	√	√	√	√	√
Advance DNAScan	√	√	√	√	√	√	√
Browsing Protection	√	√	√	√	√	√	√
Ransomware Protection	√	√	√	√	√	√	√
Browser Sandbox	√	√	√		√	√	√
Safe Banking			√		√	√	√
Phishing Protection			√	√	√	√	√
Spam Protection			√	√	√	√	√
Vulnerability Scan			√	√	√	√	√
Data Theft Protection		√		√		√	√
Virtual Keyboard			√		√	√	√
Parental Control					√	√	√
PCTuner						√	√
Wi-Fi Scanner			√	√	√	√	√
Game Booster						√	√
Anti-Tracker						√	√
PC2Mobile Scan						√	√
Webcam Protection						√	√
File Vault						√	√
Data Breach Alert						√	√

Comparison of antivirus software:

Norton:

Pros: Strong malware detection, low system impact, comprehensive features (firewall, VPN, etc.), user-friendly interface.

Cons: Can be relatively pricey compared to some other options.

Bitdefender:

Pros: Excellent malware detection, minimal impact on system performance, comprehensive features, user-friendly interface.

Cons: May have occasional false positives, might lack some advanced customization options.

Kaspersky:

Pros: Great malware detection, low system impact, diverse feature set, strong anti-phishing capabilities.

Cons: Concerns over data collection practices (though disputed by the company), occasional privacy controversies.

McAfee:

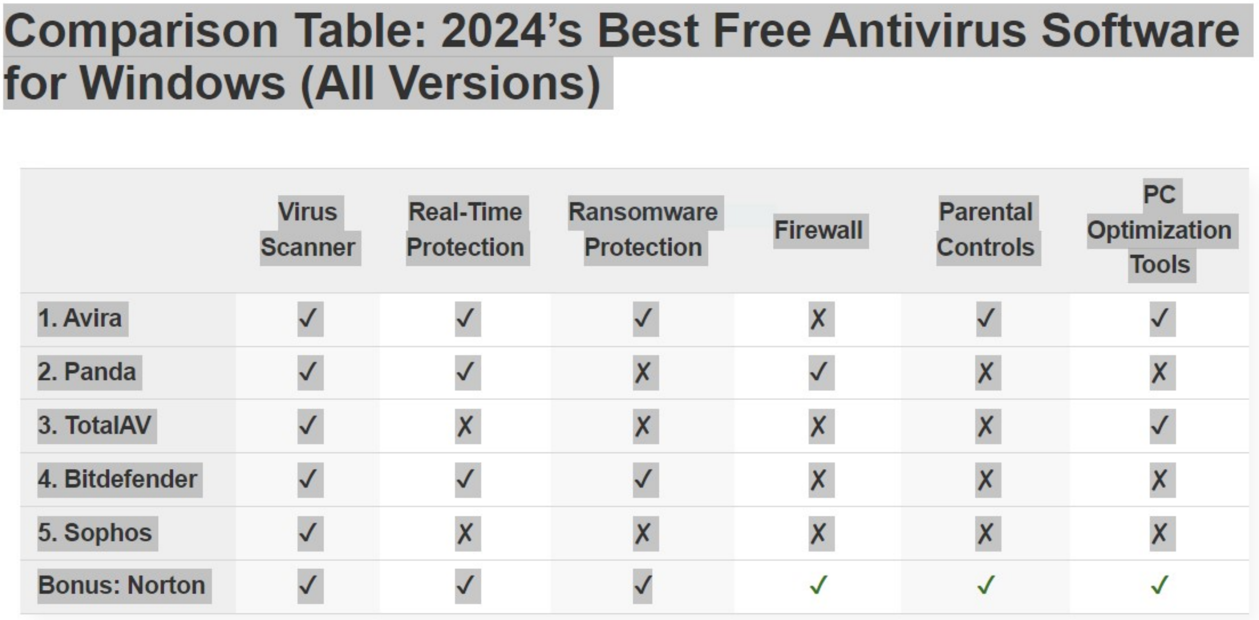
Pros: Offers a wide range of features, decent malware detection, user-friendly interface.

Cons: Can be resource-heavy, might impact system performance, occasionally intrusive with notifications.

Avast:

Pros: Free version available, decent malware detection, a wide array of features.Cons: The free version is ad-supported, some privacy concerns in the past, occasional pop-ups for upgrades.

When choosing an antivirus, consider factors like your usage habits, system specifications, desired features (firewall, VPN, etc.), and budget. Also, keep in mind that the effectiveness of antivirus software can change over time due to updates and evolving threats.



Comparison Table: 2024’s Best Free Antivirus Software for Windows (All Versions)

	Virus Scanner	Real-Time Protection	Ransomware Protection	Firewall	Parental Controls	PC Optimization Tools
1. Avira	✓	✓	✓	✗	✓	✓
2. Panda	✓	✓	✗	✓	✗	✗
3. TotalAV	✓	✗	✗	✗	✗	✓
4. Bitdefender	✓	✓	✓	✗	✗	✗
5. Sophos	✓	✗	✗	✗	✗	✗
Bonus: Norton	✓	✓	✓	✓	✓	✓

EXPERIMENT-2

Aim: Installation and study of various parameters of firewall.

Firewalls are essential security tools used to monitor and control incoming and outgoing network traffic based on predetermined security rules. Installing and understanding various parameters of a firewall involves several steps:

Installation:

Choose a Firewall: There are different types like software-based (e.g., Windows Firewall) and hardware-based (e.g., Cisco ASA). Choose based on your needs.

Installation Process: Follow the vendor's instructions for installation, which may involve downloading software, configuring hardware, or setting up virtual machines.

Understanding Parameters:

Rule Configuration: Learn how to create rules defining what traffic is allowed or denied based on criteria like IP addresses, ports, protocols, and applications.

Logging and Monitoring: Understand how to enable logging to track traffic, analyze logs, and identify potential security issues or breaches.

Intrusion Detection/Prevention: Familiarize yourself with features that detect and prevent unauthorized access or malicious activities.

Network Zones: Learn how to set up different security zones within your network and define rules for communication between these zones.

User Authentication: Explore options for user-based access control, like integrating with LDAP, Active Directory, or other authentication systems.

Update and Maintenance: Understand how to keep the firewall updated with the latest security patches and firmware updates.

INSTALLATION PROCEDURE

Installing a Cisco ASA (Adaptive Security Appliance) involves several steps. Here's a general outline:

Hardware Installation:

Physical Setup: Unpack the Cisco ASA device and place it in a secure location. Connect power and necessary cables (Ethernet, console, etc.).

Console Connection: Use a console cable to connect a computer to the ASA's console port. Use terminal emulation software like PuTTY or SecureCRT to access the ASA's command-line interface (CLI).

Initial Configuration:

Power On: Power up the ASA.

Initial Setup Wizard (ASDM or CLI):

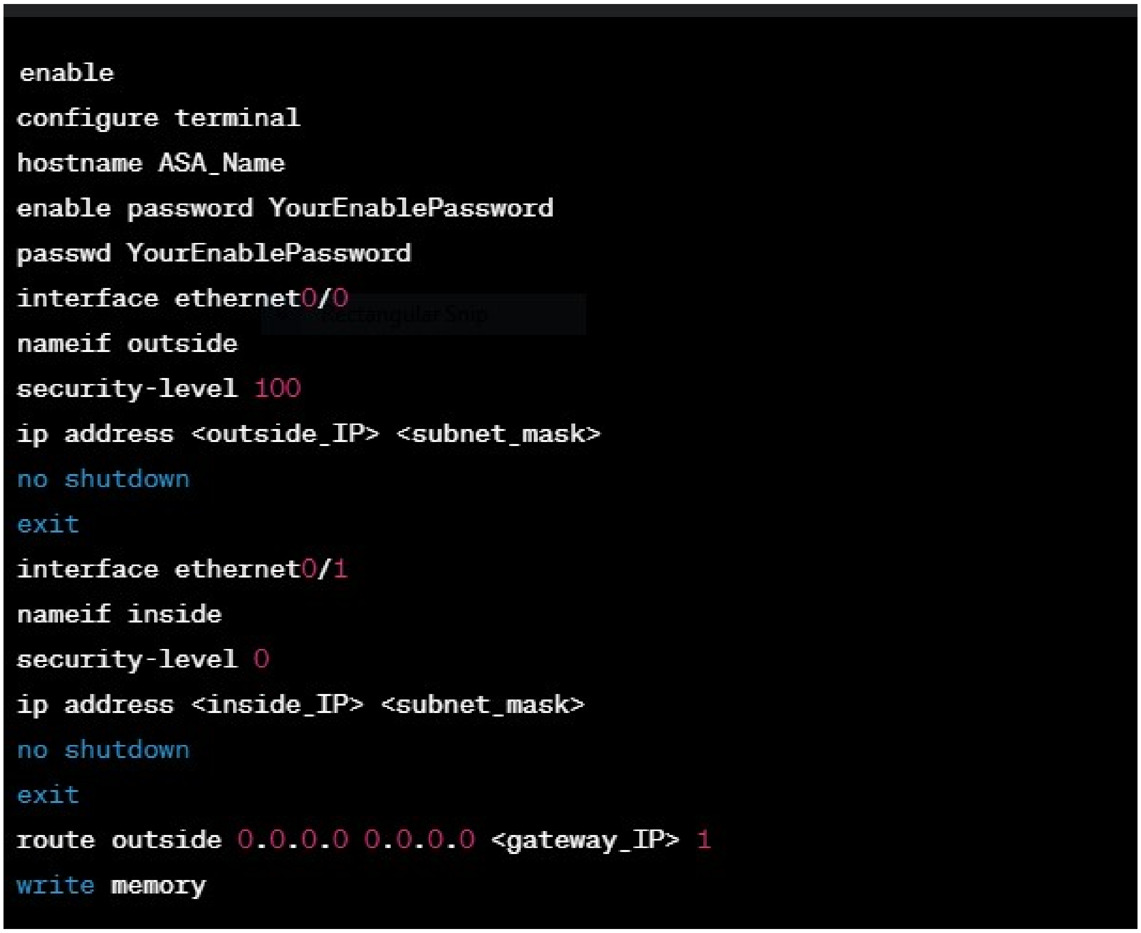
CLI: If using the Command Line Interface, you'll be prompted with a setup wizard for basic configuration (setting hostname, passwords, management interfaces, etc.).

ASDM (Adaptive Security Device Manager): Alternatively, you can use the graphical ASDM interface for initial setup and configuration. ASDM offers a more user-friendly interface compared to the CLI.

Basic Configuration via CLI:

Here's a simplified example of configuring a basic setup via CLI:

Perl



```
enable
configure terminal
hostname ASA_Name
enable password YourEnablePassword
passwd YourEnablePassword
interface ethernet0/0
nameif outside
security-level 100
ip address <outside_IP> <subnet_mask>
no shutdown
exit
interface ethernet0/1
nameif inside
security-level 0
ip address <inside_IP> <subnet_mask>
no shutdown
exit
route outside 0.0.0.0 0.0.0.0 <gateway_IP> 1
write memory
```

Additional Configuration:

Access Control: Create access control rules to permit/deny traffic between interfaces.

NAT (Network Address Translation): Configure NAT rules for translating private IPs to public IPs.

VPN Configuration: Set up VPNs for remote access or site-to-site connectivity.

Logging and Monitoring: Configure logging to track events and monitor the ASA's performance.

Testing and Verification:

Ping Tests: Test connectivity between interfaces.

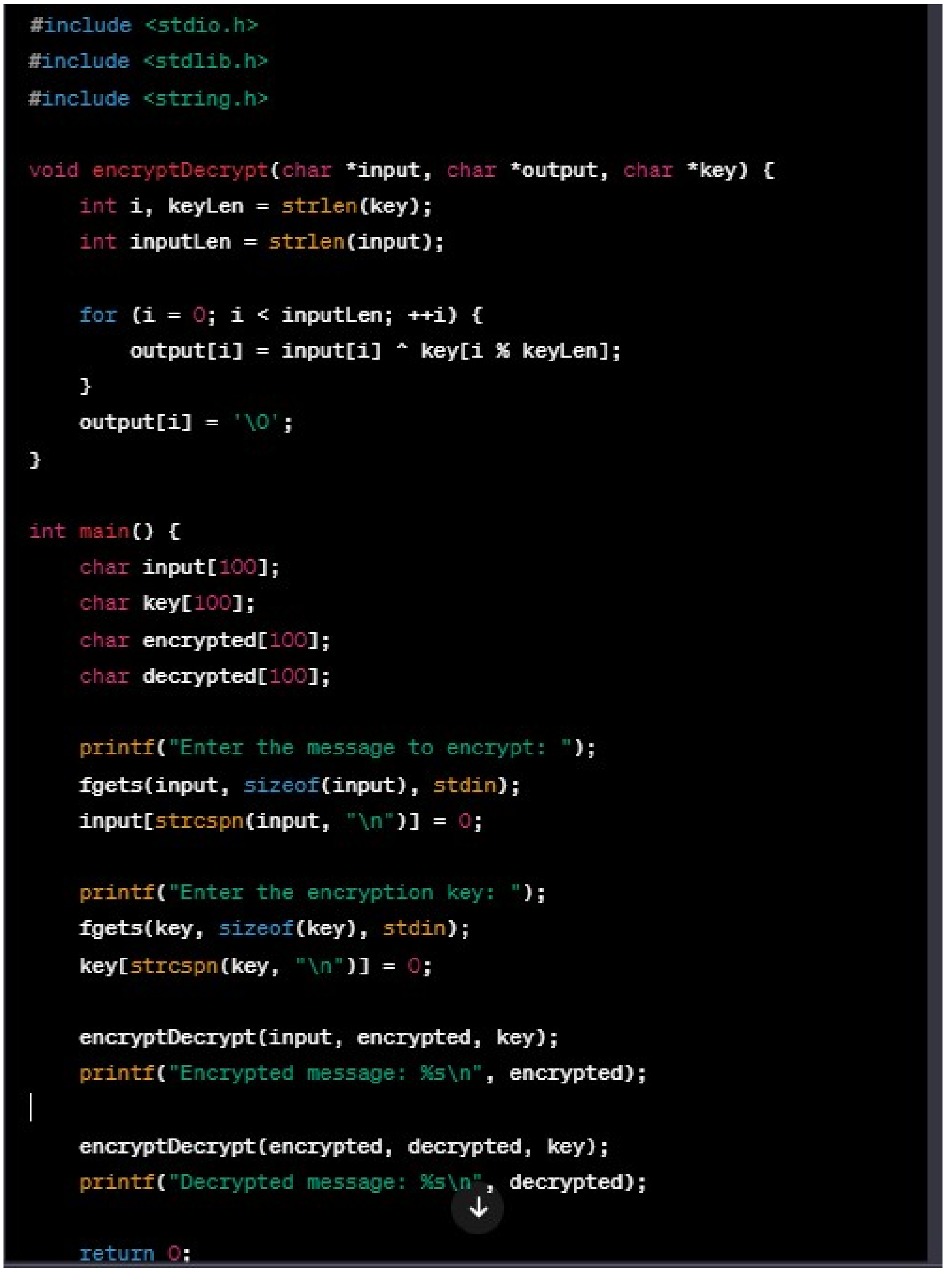
Access Tests: Verify that access rules are correctly permitting/denying traffic as intended.

Monitoring: Ensure that the ASA is properly logging events.

EXPERIMENT-3

Aim :Writing program in C to Encrypt/Decrypt using FXOR key.

C program to perform XOR encryption and decryption using a key:



```c
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

void encryptDecrypt(char *input, char *output, char *key) {
    int i, keyLen = strlen(key);
    int inputLen = strlen(input);

    for (i = 0; i < inputLen; ++i) {
        output[i] = input[i] ^ key[i % keyLen];
    }
    output[i] = '\0';
}

int main() {
    char input[100];
    char key[100];
    char encrypted[100];
    char decrypted[100];

    printf("Enter the message to encrypt: ");
    fgets(input, sizeof(input), stdin);
    input[strcspn(input, "\n")] = 0;

    printf("Enter the encryption key: ");
    fgets(key, sizeof(key), stdin);
    key[strcspn(key, "\n")] = 0;

    encryptDecrypt(input, encrypted, key);
    printf("Encrypted message: %s\n", encrypted);

    encryptDecrypt(encrypted, decrypted, key);
    printf("Decrypted message: %s\n", decrypted);

    return 0;
```

EXPERIMENT-4

Aim: study of VPN

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 tunnelling protocols to establish a secure connection.

1. Remote Access VPN

Remote Access VPN permits a user to connect to a private network and access all its services and resources remotely. The connection between the user and the private network occurs through the Internet and the connection is secure and private. Remote Access VPN is useful for home users and business users both. An employee of a company, while he/she is out of station, uses a VPN to connect to his/her company’s private network and remotely access files and resources on the private network. Private users or home users of VPN, primarily use VPN services to bypass regional restrictions on the Internet and access blocked websites. Users aware of Internet security also use VPN services to enhance their Internet security and privacy.

2. Site to Site VPN

A Site-to-Site VPN is also called as Router-to-Router VPN and is commonly used in the large companies. Companies or organizations, with branch offices in different locations, use Site-to-site VPN to connect the network of one office location to the network at another office location.

Intranet based VPN: When several offices of the same company are connected using Site-to-Site VPN type, it is called as Intranet based VPN.

Extranet based VPN: When companies use Site-to-site VPN type to connect to the office of another company, it is called as Extranet based VPN.

3. Cloud VPN

A Cloud VPN is a virtual private network that allows users to securely connect to a cloud-based infrastructure or service. It uses the internet as the primary transport medium to connect the remote users to the cloud-based resources. Cloud VPNs are typically offered as a service by cloud providers such as Amazon Web Services (AWS) and Microsoft Azure. It uses the same encryption and security protocols as traditional VPNs, such as IPsec or SSL, to ensure that the data transmitted over the VPN is secure. Cloud VPNs are often used by organizations to securely connect their on-premises resources to cloud-based resources, such as cloud-based storage or software-as-a-service (SaaS) applications

4. Mobile VPN

Mobile VPN is a virtual private network that allows mobile users to securely connect to a private network, typically through a cellular network. It creates a secure and encrypted connection between the mobile device and the VPN server, protecting the data transmitted over the connection. Mobile VPNs can be used to access corporate resources, such as email or internal websites, while the user is away from the office. They can also be used to securely access public Wi-Fi networks, protecting the user’s personal information from being intercepted. Mobile VPNs are available as standalone apps or can be integrated into mobile device management (MDM) solutions. These solutions are commonly used by organisations to secure their mobile workforce.

5. SSL VPN

SSL VPN (Secure Sockets Layer Virtual Private Network) is a type of VPN that uses the SSL protocol to secure the connection between the user and the VPN server. It allows remote users to securely access a private network by establishing an encrypted tunnel between the user’s device and the VPN server. SSL VPNs are typically accessed through a web browser, rather than through a standalone client. This makes them easier to use and deploy, as they don’t require additional software to be installed on the user’s device. It can be used to access internal resources such as email, file servers, or databases. SSL VPNs are considered more secure than traditional IPsec VPNs because they use the same encryption protocols as HTTPS, the secure version of HTTP used for online transactions.

6. PPTP (Point-to-Point Tunneling Protocol) VPN

PPTP (Point-to-Point Tunneling Protocol) is a type of VPN that uses a simple and fast method for implementing VPNs. It creates a secure connection between two computers by encapsulating the data packets being sent between them. PPTP is relatively easy to set up and doesn’t require any additional software to be installed on the client’s device. It can be used to access internal resources such as email, file servers, or databases. PPTP is one of the oldest VPN protocols and is supported on a wide range of operating systems. However, it is considered less secure than other VPN protocols such as L2TP or OpenVPN, as it uses a weaker encryption algorithm and has been known to have security vulnerabilities.

7. L2TP (Layer 2 Tunneling Protocol) VPN

L2TP (Layer 2 Tunneling Protocol) is a type of VPN that creates a secure connection by encapsulating data packets being sent between two computers. L2TP is an extension of PPTP, it adds more security to the VPN connection by using a combination of PPTP and L2F (Layer 2 Forwarding Protocol) and it uses stronger encryption algorithm than PPTP. L2TP is relatively easy to set up and doesn’t require additional software to be installed on the client’s device. It can be used to access internal resources such as email, file servers, or databases. It is supported on a wide range of operating systems, but it is considered less secure than other VPN protocols such as OpenVPN, as it still has some vulnerabilities that can be exploited.

8. OpenVPN

OpenVPN is an open-source software application that uses SSL and is highly configurable and secure. It creates a secure and encrypted connection between two computers by encapsulating the data packets being sent between them. OpenVPN can be used to access internal resources such as email, file servers, or databases. It is supported on a wide range of operating systems and devices, and can be easily configured to work with various network configurations and security settings. It is considered one of the most secure VPN protocols as it uses the industry standard SSL/TLS encryption protocols and it offers advanced features such as two-factor authentication and kill switch.

Types of Virtual Private Network (VPN) Protocols:

Internet Protocol Security (IPSec): Internet Protocol Security, known as IPSec, is used to secure Internet communication across an IP network. IPSec secures Internet Protocol communication by verifying the session and encrypts each data packet during the connection. IPSec runs in 2 modes:

(i) Transport mode

(ii) Tunneling mode

Layer 2 Tunneling Protocol (L2TP): L2TP or Layer 2 Tunneling Protocol is a tunneling protocol that is often combined with another VPN security protocol like IPSec to establish a highly secure VPN connection. L2TP generates a tunnel between two L2TP connection points and IPSec protocol encrypts the data and maintains secure communication between the tunnel.

Point–to–Point Tunneling Protocol (PPTP): PPTP or Point-to-Point Tunneling Protocol generates a tunnel and confines the data packet. Point-to-Point Protocol (PPP) is used to encrypt the data between the connection. PPTP is one of the most widely used VPN protocol and has been in use since the early release of Windows. PPTP is also used on Mac and Linux apart from Windows.

SSL and TLS: SSL (Secure Sockets Layer) and TLS (Transport Layer Security) generate a VPN connection where the web browser acts as the client and user access is prohibited to specific applications instead of entire network. Online shopping websites commonly uses SSL and TLS protocol. It is easy to switch to SSL by web browsers and with almost no action required from the user as web browsers come integrated with SSL and TLS. SSL connections have “https” in the initial of the URL instead of “http”.

Secure Shell (SSH): Secure Shell or SSH generates the VPN tunnel through which the data transfer occurs and also ensures that the tunnel is encrypted. SSH connections are generated by a SSH client and data is transferred from a local port on to the remote server through the encrypted tunnel.

SSTP (Secure Socket Tunneling Protocol): A VPN protocol developed by Microsoft that uses SSL to secure the connection, but only available for Windows.

IKEv2 (Internet Key Exchange version 2): A VPN protocol that provides fast and secure connections, but not widely supported by VPN providers.

OpenVPN: An open-source VPN protocol that is highly configurable and secure, widely supported by VPN providers and considered one of the most secure VPN protocols.

WireGuard: A relatively new and lightweight VPN protocol that aims to be faster, simpler and more secure than existing VPN protocols.

EXPERIMENT-5

Aim: Study of various hacking tools.

Hacking tools are software or programs designed to identify vulnerabilities in computer systems, networks, or software. They can range from simple scripts to sophisticated software with various functionalities. Here are some categories of hacking tools:

Vulnerability Scanners: Tools like Nessus, OpenVAS, and Qualys scan networks and systems for potential vulnerabilities. They identify weaknesses that attackers could exploit.

Exploitation Frameworks: Metasploit is a popular framework that helps in developing, testing, and executing exploit code against a remote target. It allows ethical hackers to simulate real-world attacks.

Packet Sniffers: Tools like Wireshark capture and analyze network traffic. They can be used to inspect data packets, identify potential security issues, and troubleshoot network problems.

Password Crackers: Programs such as John the Ripper and Hashcat attempt to crack passwords by using various methods like dictionary attacks, brute force, or rainbow tables.

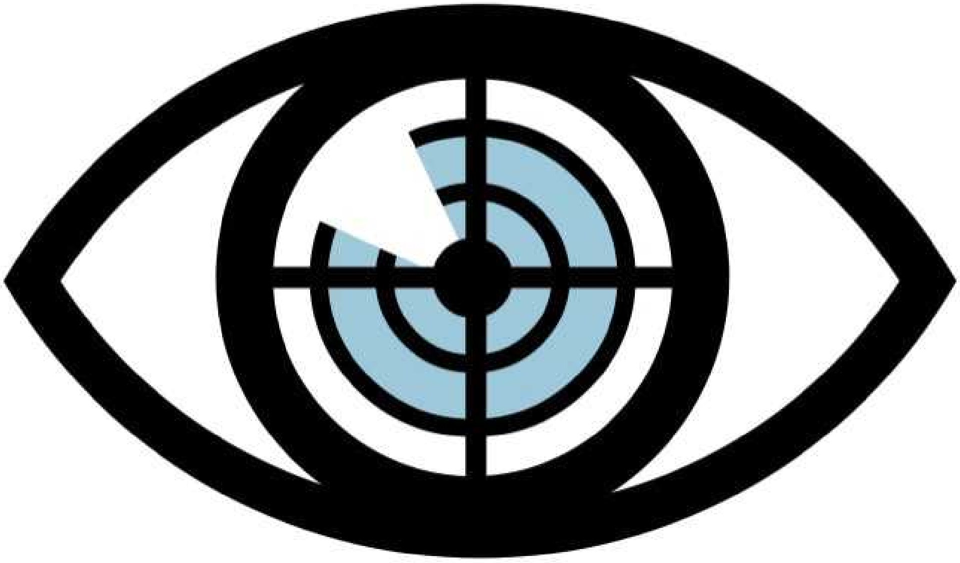
Network Scanners: Nmap is a widely used tool for network discovery and security auditing. It detects hosts, services, open ports, and their vulnerabilities.

Steganography Tools: These tools hide information within other files (images, audio, etc.) to facilitate covert communication or data hiding. Examples include OpenStego and Steghide.

Web Application Scanners: Tools like OWASP ZAP and Burp Suite help in assessing web applications for vulnerabilities like SQL injection, cross-site scripting (XSS), etc.

some of the necessary hacking tools

1.) Nmap:



It is a free and open-source tool that's used for network discovery and security auditing. Nmap is a powerful tool because it is often used to scan vast networks having thousands of machines. It's a command-line tool. Nmap suite additionally includes a complicated GUI that's referred to as "ZenMap". It supports a large variety of OS that is:

Linux

Microsoft Windows

Mac OS X

FreeBSD

OpenBSD

Solaris

IRIX

It uses raw IP packets to determine

Hosts that are accessible on the specific networks.

Services that are offered by hosts, i.e., Application name together with its versions.

Operating system and its version running on the target system, type of firewall on the target system.

Scans for the exploitation of the open port, both TCP and UDP protocols.

Nmap download link: https://nmap.org/download.html

2.) Metasploit

metasploit logo

It is essentially a Security Assessment and Penetration Testing tool. Metasploit is often used to launch an attack on alternative systems with it. It uses a vulnerable system on that security testing may be conducted to use the failings within the system.

Metasploit may enforce as follows:

Initially, protocol port scanning is complete to get data concerning the target

system.

Host lists and services running on them may be read and analyzed within the project view.

Now, the vulnerability scan runs on the target system's information that enlists the failings inside the system.

This data used for designing the attack on the target system.

Metasploit download link: https://github.com/rapid7/metasploit-framework/wiki/Nightly-Installers

3.) Wireshark

Wireshark Logo

It is an open-source tool that's used to capture traffic on the network. It's essentially a network protocol analyzer tool.

Wireshark helps in:

Sniffing for the passwords.

Identifying the destination and source IP address of the traffic.

Capturing all the packets over the network.

Next, we tend to enter the valid John the Ripper command that is used to extract the password from the hash password given as an input.

It additionally captures HTTP packet transmission over the network. Click on "Follow protocol connection" within the HTTP packet. Currently, you'll be able to see the username and passwords that are captures over the network.

Wireshark download link: https://www.wireshark.org/#download

4.) John the Ripper

John The Ripper

JTR is free and open-source software that's wide employed by hackers for password cracking. It uses the varied cryptanalytics attacks like "Dictionary Attack" and "Brute-Force Attack". It additionally comes with the business version moreover, i.e., "John the Ripper Professional." It's a lot of accessible versions providing a lot of practicality in password cracking at the enterprise level.

John the Ripper working:

Initially get the hashed password that needs to be crack.

We need to possess a wordlist of expected passwords in our system because it makes the password cracking job easier.

Next, we tend to enter the valid John the ripper command that is used in extracting the password from the hash password given as an input.

The rate at which the password is going to be cracked depends utterly on the password's strength and offered wordlist. It keeps attempting to break the password continuously till the termination command isn't given.

John the ripper download link: https://www.openwall.com/john/

5.) Burp Suite

Burpsuite

It is an integrated platform that's used for activity a check on net application security. It provides a large variety of tools that are used from initial mapping to exploiting the

applications' vulnerabilities. Once the issues are detected, hackers will use it to break into the security of the system.

Burp Suite comes in 3 editions:

Community Edition: It is available free of charge for downloading.

Professional Edition: Penetration testers and bug bounty hunters utilize it.

Enterprise Edition: An organization utilizes it.

Burp Suite features:

It may be used to launch attacks on internet Applications. It will check and detect Cross-site scripting (XSS) and SQL injection.

It operates as an internet proxy server that helps permit interception, inspection, and modification of network traffic.

Burp Suite download link: https://portswigger.net/burp

6.) Angry IP Scanner

angryipscanner

It is one of the quickest IP addresses and port scanner. By exploitation, this hacker will gather data concerning open ports within the target system. It pings every IP address within the target system to see whether it's active or not. Further, it resolves the hostnames and determines the MAC address.

Features:

It additionally extracts the NetBIOS data, which has services associated with the session layer within the OSI model that are workgroup names and current active users.

Scanned results may be saved in CSV, TXT, XML, or IP-Port list files.

It will gather any data concerning scanned IP's because it uses plugins.

If anyone writes plugins, he will efficiently extend the practicality of Angry IP Scanner.

Angry IP Scanner download link: https://angryip.org/download/#windows

7.) Nikto

NIKTO Scanner

It is a web-server assessment tool. It is an open-source platform that performs tests against web servers to seek multiple vulnerable files, misconfigurations, out-of-date servers, and programs on its web server. It depends on HTTP response to seeing whether or not a page or script exists on the target.

Features:

Provides HTTP proxy support.

Checks for the out-of-date server parts.

It will scan multiple ports on the server.

Guesses credentials for authorization with attempting many alternative ID and password combos.

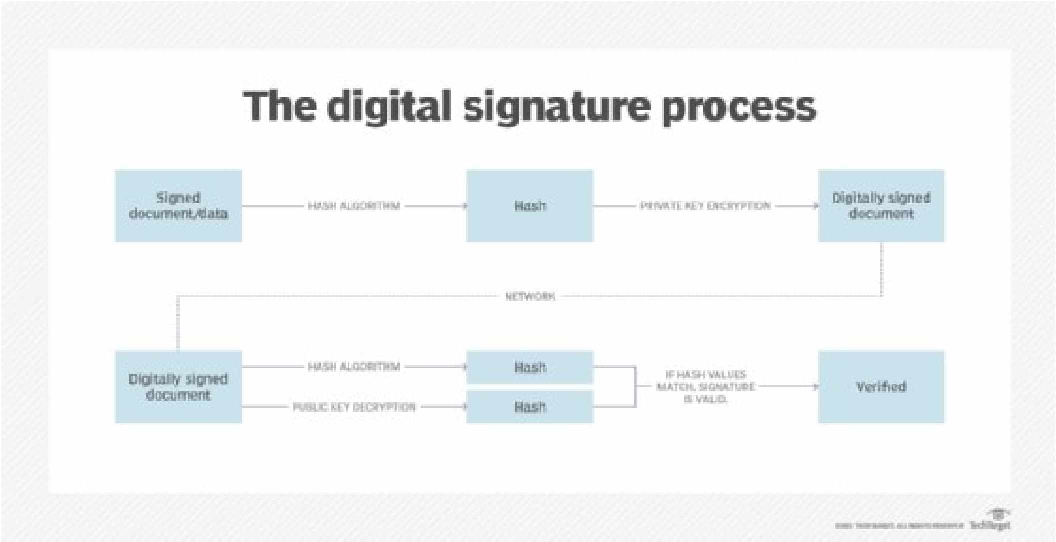
EXPERIMENT-6

Aim: Practical applications of digital signature

digital signature:

A digital signature is a mathematical technique used to validate the authenticity and integrity of a digital document, message or software. It's the digital equivalent of a handwritten signature or stamped seal, but it offers far more inherent security. A digital signature is intended to solve the problem of tampering and impersonation in digital communications.

Digital signatures can provide evidence of origin, identity and status of electronic documents, transactions or digital messages. Signers can also use them to acknowledge informed consent. In many countries, including the U.S., digital signatures are considered legally binding in the same way as traditional handwritten document signatures.



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

Digital Signature Web Application Process

A digital signature certificate links the identity of a person with a pair of electronic keys, i.e. public and private keys, endorsed by a CA. The certificate consists of information related to the user's identity (Like: name, pin code, country, email address, certificate issue date, and the Certifying Authority Name).

The keys are complementary to each other and one cannot work without the presence of another. The browsers and servers to encrypt and decrypt the information of the certificate user during the complete process. The private key can be stored on the user's hard disk, computer or any external device. The user controls the access and it only works with the assigned password. In case of mismatch of the two, the authentication process fails. This ensures that only authorized personnel can use the Digital signatures whereas the unauthorized ones cannot access the data.

Digital Signature Web Application allows a faster, convenient and secure way to create your digital signatures that are authentic and can be used for almost every documentation process. Also, the digital signature web application is equally useful for personal and business use. It can be stored safely and can be used for applications of digital signatures to avail various services.

We at Sigplex are constantly building efficient and effective technological solutions for businesses. Our Digital Signature web application is made for safe, secure and convenient transactions. Feel free to write to us at contact@sigplex.com on how your personal and business transactions can be secured via digital signature.