



ଓଡ଼ିଶା ରାଜ୍ୟ ମୁକ୍ତ ବିଶ୍ୱବିଦ୍ୟାଳୟ, ସମ୍ବଲପୁର, ଓଡ଼ିଶା  
Odisha State Open University, Sambalpur, Odisha  
Established by an Act of Government of Odisha.

## **DIPLOMA IN CYBER SECURTY**

### **DCS-05 – NETWORK CYBER SECURITY**

#### **BLOCK**

# **4**

#### **LABORATORY MANUAL**



ଓଡ଼ିଶା ରାଜ୍ୟ ମୁକ୍ତ ବିଶ୍ୱବିଦ୍ୟାଳୟ, ସମ୍ବଲପୁର, ଓଡ଼ିଶା  
**Odisha State Open University, Sambalpur, Odisha**  
Established by an Act of Government of Odisha.

**EXPERT COMMITTEE**

**Dr. P.K Behera(Chairman)**  
Reader in Computer Science  
Utkal University, Bhubaneswar, Odisha

**Dr.J.R Mohanty(Member)**  
Professor and HOD  
KIIT University. Bhubaneswar, Odisha

**Sri Pabitranda Pattnaik(Member)**  
Scientist-E, NIC  
Bhubaneswar, Odisha

**Sri Malaya Kumar Das (Member)**  
Scientist-E, NIC  
Bhubaneswar, Odisha

**Dr. Bhagirathi Nayak (Member)**  
Professor and Head (IT & System)  
Sri Sri University  
Bhubaneswar, Odisha

**Dr. Manoranjan Pradhan(Member)**  
Professor and Head (IT & System)  
G.I.T.A, Bhubaneswar, Odisha

**Sri Chandrakant Mallick(Convener)**  
Consultant (Academic)  
School of Computer and Information  
Science., Odisha State Open University  
Sambalpur, Odisha

**DIPLOMA IN CYBER SECURITY**

**Course Writer**

**Chandrakant Mallick**  
**Odisha State Open University, Sambalpur**

# **DCS-05 – NETWORK CYBER SECURITY LABORATORY**

## **LIST OF EXPERIMENTS**

<b>SL. No.</b>	<b>Experiment</b>
1	Study of different wireless network components and features of any one of the Mobile Security Apps.
2	Study of the features of firewall in providing network security and to set Firewall Security in windows.
3	Steps to ensure Security of any one web browser (Mozilla Firefox/Google Chrome)
4	Study of different types of vulnerabilities for hacking a websites / Web Applications.
5	Analysis the Security Vulnerabilities of E-commerce services.
6	Analysis the security vulnerabilities of E-Mail Application

---

## EXPERIMENT-1

---

**Aim: Study of different wireless network components and features of any one of the Mobile Security Apps.**

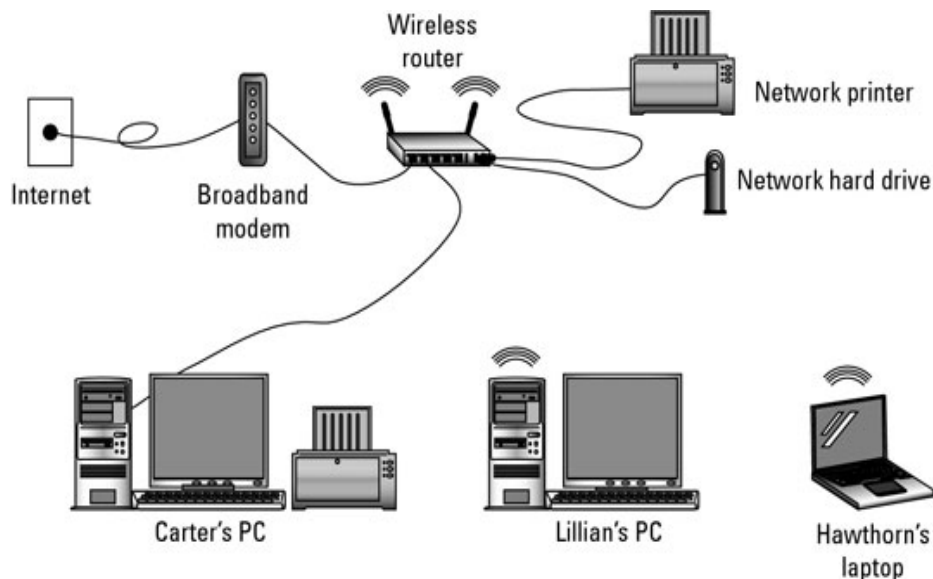
### 1.0 Learning Objectives

At the end of the session you should be able to

- Know about the devices and components in a wireless network.
- Know about the network security **issues in** different types of network devices.
- Identify a mobile security app and how it works for mobile security?

### 1.1 Introduction

As long as you have all the hardware, you can quickly set up any wireless network. Here is everything you need to know about the hardware you need to have in place before you use Windows to configure the wireless network. There are two types of wireless networks: infrastructure and ad hoc. The *infrastructure* network is most likely the type of wireless setup you have in your home or office. It's laid out similarly to a wired network, but without wires.



The basic wireless, peer-to-peer network consists of these components:

#### Wireless Network Adapters

Wireless network adapters (also known as *wireless NICs* or *wireless network cards*) are required for each device on a wireless network. All

newer laptop computers incorporate wireless adapters as a built-in feature of the system.

No wireless hardware other than adapters is required to build a small local network. However, to increase the performance of network connections, accommodate more computers, and increase the network's range, additional types of hardware can be deployed.

### **Wireless Routers**

Wireless routers function comparably to traditional routers for wired Ethernet networks. One generally deploys wireless routers when building an all-wireless network from the ground up.

Similar to routers, access points allow wireless networks to join an existing wired network. One typically deploys access points when growing a network that already has routers installed. In home networking, a single access point (or router) possesses sufficient range to span most residential buildings. Businesses in office buildings often must deploy multiple access points and/or routers.

### **Wireless Antennas**

Access points and routers often utilize a Wi-Fi wireless antenna that significantly increase the communication range of the wireless radio signal. These antennas are optional and removable on most equipment. It's also possible to mount aftermarket add-on antennas on wireless clients to increase the range of wireless adapters.

### **Wireless Repeaters**

A wireless repeater connects to a router or access point. Often called signal boosters or *range expanders*, repeaters serve as a two-way relay station for wireless radio signals, helping clients otherwise unable to receive a network's wireless signal to join.

**Wire-based connections:** Almost every wireless router has one or more standard, wire-based Ethernet port. One port is used to connect the router to a broadband modem. Other Ethernet ports might be also available, allowing you to connect standard wire-based networking to the wireless hub.

**Wireless NIC:** Your computer needs a wireless Network Interface Card, or NIC, to talk with the wireless router. A laptop comes standard with a wireless NIC, but for a desktop PC you have to get a wireless NIC as an option. It's installed internally as an expansion card, or you can use one of the various plug-in USB wireless NICs.

These are the components for infrastructure type of wireless network. The other type of network called the *ad hoc* type of wireless network is basically a group of wireless computers connected with each other. An ad-hoc network has no central hub or router. Instead, all its computers can directly access the other computers' files and shared resources. They may or may not have Internet access, but that's not the point of the ad hoc network.

- One of the beauties of a wireless network is that you can mix in wired components as needed. If you need more Ethernet ports, for example, simply add a switch to the wireless router.
- Despite the wireless nature of wireless networking, you still need an Ethernet cable (a wire) to connect a wireless router to a broadband modem.
- Another advantage of a wireless network is that it's portable. It's far easier to pull up stakes with a wireless network than to pack up all the bits and pieces of a wired network. If you live in an apartment, or just move around a lot, wirelesses setup a good option.
- The term *access point* is often abbreviated AP. Don't be puzzled when you see the words *wireless AP* — it simply refers to the access point, not to the Associated Press.
- A wireless network is often called a *WLAN*, for wireless local-area network.
- A wireless network is also referred to by the term *Wi-Fi*. It stands for *wireless fidelity*.
- Ad hoc networks are often used by computer gamers to gather in a single location to play games with each other.

## 1.2 Mobile App Security

Mobile app security is the extent of protection that mobile device applications (apps) have from malware and the activities of crackers and other criminals. The term can also refer to various technologies and production practices that minimize the risk of exploits to mobile devices through their apps.

A mobile device has numerous components, all of them vulnerable to security weaknesses. The parts are made, distributed, and used by multiple players, each of whom plays a crucial role the security of a device. Each player should incorporate security measures into mobile devices as they are designed and built and into mobile apps as they are conceived and written, but these tasks are not always adequately carried out.

Common vulnerabilities for mobile devices include architectural flaws, device loss or theft, platform weakness, isolation and permission problems and application weaknesses.

When evaluating mobile devices and apps for security, developers should ask themselves the following questions.

- How do users obtain a particular app?
- Should a firm create its own app store?
- How is an app vetted before it is offered for sale?
- How is an app protected against malware?
- How can users tell the difference between a legitimate app and a fake?
- How easily can automatic update features get hijacked?
- What measures exist to control the risk of device jail breaking?
- What kind of permissions should a particular app ask for?
- Can any other apps keep track of when, where, and how a certain app is used?

Let us now discuss the features of a popular mobile security app called CM Security.

### 1.2.1 CM Security

CM security (Clean Master) is an all-singing, all-dancing option made by Cheetah Mobile that brings you a whole host of anti-virus and security features for free - as long as you don't mind a few ads.

#### Features of CM security

Feature-wise it tries to offer everything - anti-virus, browsing protection, battery saving, privacy protection of apps, the whole lot. It takes pretty much the same simplified approach to each of those things too. CM security identifies what it describes as threats and then asks what you want to do about them in a straightforward way.

That might disappoint people who love spending time in settings menus, but you're not going to be doing that with CM Security. One potential drawback, however, is that it's relentless in nagging you about other aspects of your device and other apps made by Cheetah that can help you out. But again, it's free, so it's hard to complain too much.



---

## EXPERIMENT-2

---

**AIM: Study of the features of firewall in providing network security and to set Firewall Security in windows.**

### 2.0 Learning Objectives

At the end of the session you should be able to

- Know how to setup a firewall on Operating System.
- Know about the Windows Firewall with Advanced Security.
- Know the Connection Security Rules

### 2.1 Working with Windows Firewall in Windows 7

#### 2.1.1 Firewall in Windows 7

Windows 7 comes with two firewalls that work together. One is the **Windows Firewall**, and the other is **Windows Firewall with Advanced Security (WFAS)**. The main difference between them is the complexity of the rules configuration. Windows Firewall uses simple rules that directly relate to a program or a service. The rules in WFAS can be configured based on protocols, ports, addresses and authentication. By default, both firewalls come with predefined set of rules that allow us to utilize network resources. This includes things like browsing the web, receiving e-mails, etc. Other standard firewall exceptions are File and Printer Sharing, Network Discovery, Performance Logs and Alerts, Remote Administration, Windows Remote Management, Remote Assistance, Remote Desktop, Windows Media Player, Windows Media Player Network Sharing Service

With firewall in Windows 7 we can configure inbound and outbound rules. By default, all outbound traffic is allowed, and inbound responses to that traffic are also allowed. Inbound traffic initiated from external sources is automatically blocked.

Sometimes we will see a notification about a blocked program which is trying to access network resources. In that case we will be able to add an exception to our firewall in order to allow traffic from the program in the future.

Windows 7 comes with some new features when it comes to firewall. For example, "full-stealth" feature blocks other computers from performing operating system fingerprinting. OS fingerprinting is a malicious technique



used to determine the operating system running on the host machine. Another feature is "boot-time filtering". This feature ensures that the firewall is working at the same time when the network interface becomes active, which was not the case in previous versions of Windows.

When we first connect to some network, we are prompted to select a network location. This feature is known as Network Location Awareness (NLA). This feature enables us to assign a network profile to the connection based on the location. Different network profiles contain different collections of firewall rules. In Windows 7, different network profiles can be configured on different interfaces. For example, our wired interface can have different profile than our wireless interface. There are three different network profiles available:

- Public
- Home/Work - private network
- Domain - used within a domain

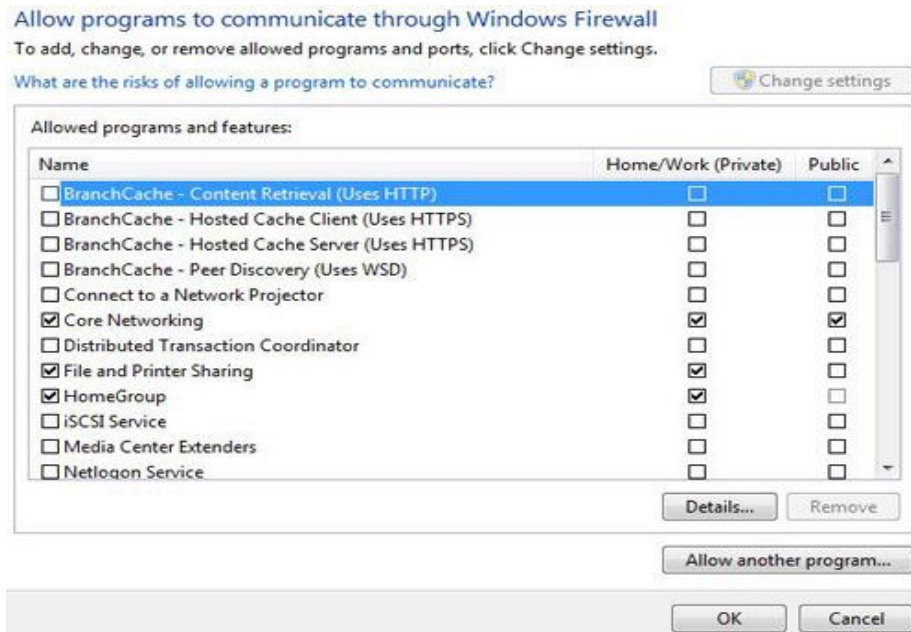
We choose those locations when we connect to a network. We can always change the location in the Network and Sharing Center, in Control Panel. The Domain profile can be automatically assigned by the NLA service when we log on to an Active Directory domain. Note that we must have administrative rights in order to configure firewall in Windows 7.

### 2.1.2 Configuring Windows Firewall

To open Windows Firewall we can go to **Start > Control Panel > Windows Firewall**.

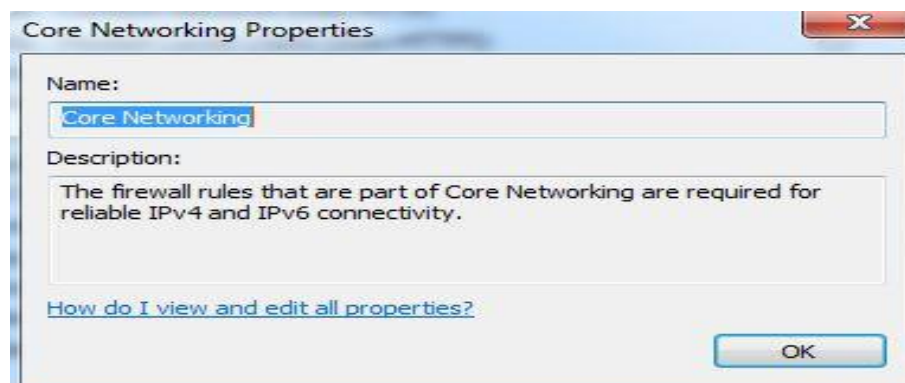


By default, Windows Firewall is enabled for both private (home or work) and public networks. It is also configured to block all connections to programs that are not on the list of allowed programs. To configure exceptions we can go to the menu on the left and select "Allow a program or feature through Windows Firewall" option.



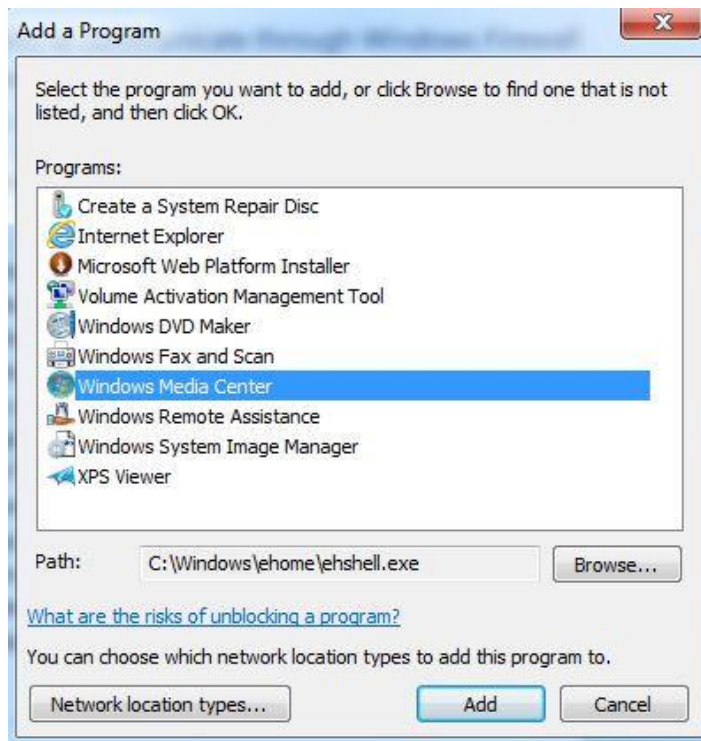
## Exceptions

To change settings in this window we have to click the "Change settings" button. As you can see, here we have a list of predefined programs and features that can be allowed to communicate on private or public networks. For example, notice that the Core Networking feature is allowed on both private and public networks, while the File and Printer Sharing is only allowed on private networks. We can also see the details of the items in the list by selecting it and then clicking the Details button.



## Details

If we have a program on our computer that is not in this list, we can manually add it by clicking on the "Allow another program" button.



## Add a Program

Here we have to browse to the executable of our program and then click the Add button. Notice that we can also choose location types on which this program will be allowed to communicate by clicking on the "Network location types" button.



## Network Locations

Many applications will automatically configure proper exceptions in Windows Firewall when we run them. For example, if we enable streaming from Media Player, it will automatically configure firewall settings to allow streaming. The same thing is if we enable Remote Desktop feature from the system properties window. By enabling Remote Desktop feature we actually create an exception in Windows Firewall.

Windows Firewall can be turned off completely. To do that we can select the "Turn Windows Firewall on or off" option from the menu on the left.

### Customize settings for each type of network

You can modify the firewall settings for each type of network location that you use.

[What are network locations?](#)

#### Home or work (private) network location settings



☒ Turn on Windows Firewall

☐ Block all incoming connections, including those in the list of allowed programs

☒ Notify me when Windows Firewall blocks a new program



☐ Turn off Windows Firewall (not recommended)

#### Public network location settings



☒ Turn on Windows Firewall

☐ Block all incoming connections, including those in the list of allowed programs

☒ Notify me when Windows Firewall blocks a new program



☐ Turn off Windows Firewall (not recommended)

## Firewall Customization

Note that we can modify settings for each type of network location (private or public). Interesting thing here is that we can block all incoming connections, including those in the list of allowed programs.

Windows Firewall is actually a Windows service. As you know, services can be stopped and started. If the Windows Firewall service is stopped, the Windows Firewall will not work.

Windows Event Collector	This service ...	Started	Automatic
Windows Event Log	This service ...	Started	Automatic
Windows Firewall	Windows Fi...	Started	Automatic
Windows Font Cache S...	Optimizes p...	Started	Automatic (D...
Windows Image Acqui	Provides im		Manual

## Firewall Service

In our case the service is running. If we stop it, we will get a warning that we should turn on our Windows Firewall.



## Warning

Remember that with Windows Firewall we can only configure basic firewall settings, and this is enough for most day-to-day users. However, we can't configure exceptions based on ports in Windows Firewall any more. For that we have to use Windows Firewall with Advanced Security.

### 2.1.3 How to Start & Use the Windows Firewall with Advanced Security

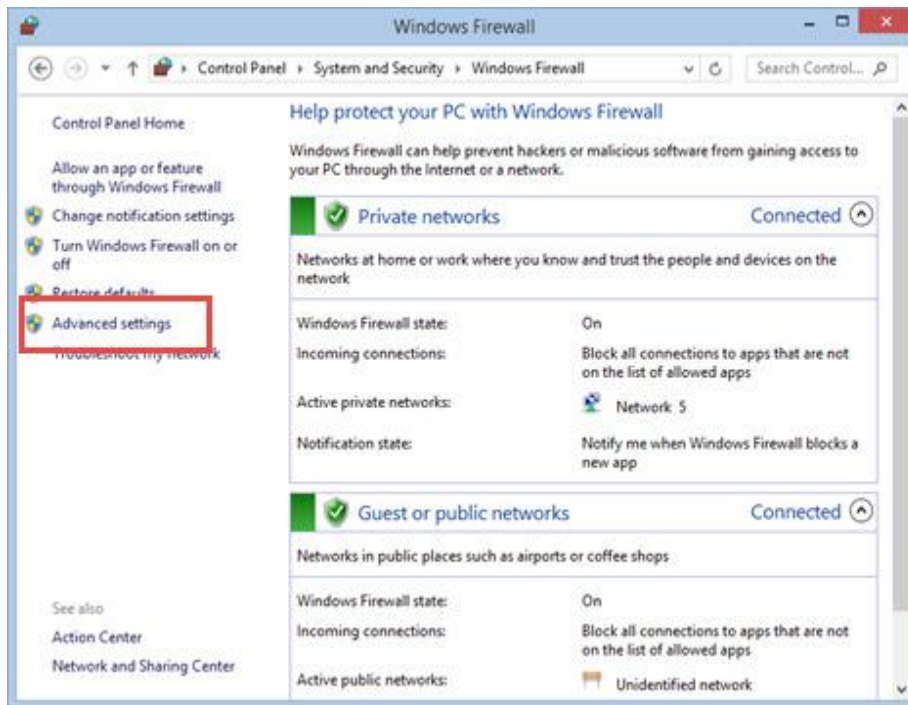
The *Windows Firewall with Advanced Security* is a tool which gives you detailed control over the rules that are applied by the *Windows Firewall*. You can view all the rules that are used by the *Windows Firewall*, change their properties, create new rules or disable existing ones. In this tutorial we will share how to open the *Windows Firewall with Advanced Security*, how to find your way around it and talk about the types of rules that are available and what kind of traffic they filter.

#### 2.1.3.1 How to Access the Windows Firewall with Advanced Security

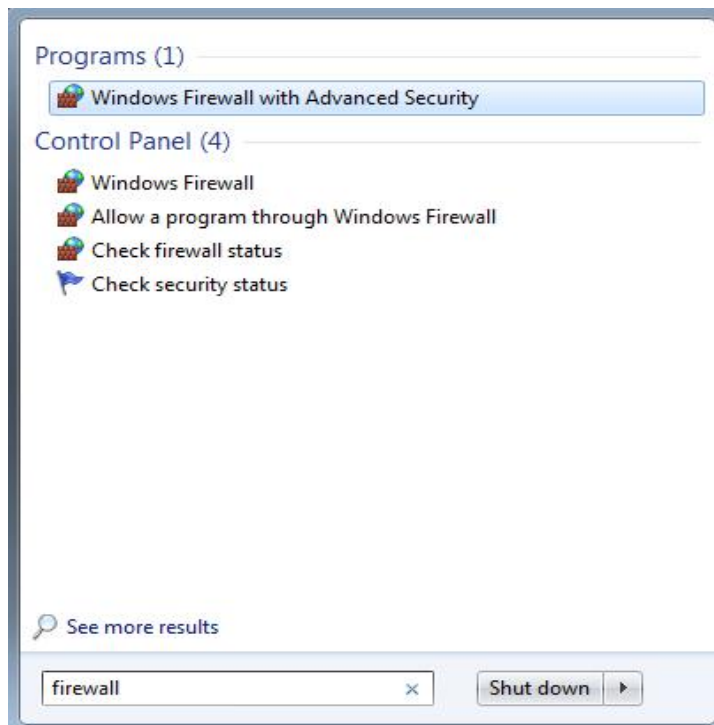
You have several alternatives to opening the *Windows Firewall with Advanced Security*:

One is to open the standard Windows Firewall window, by going to "*Control Panel -> System and Security -> Windows Firewall*". Then, click or tap *Advanced settings*.



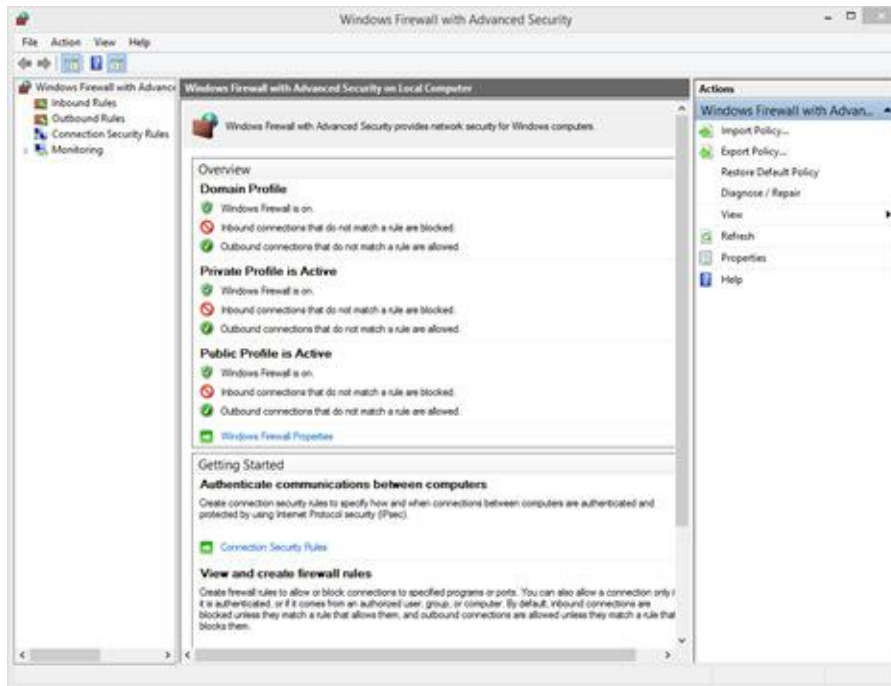


In Windows 7, another method is to search for the word *firewall* in the *Start Menu* search box and click the "*Windows Firewall with Advanced Security*" result.



In Windows 8.1, *Windows Firewall with Advanced Security* is not returned in search results and you need to use the first method shared above for opening it.

The *Windows Firewall with Advanced Security* looks and works the same both in Windows 7 and Windows 8.1. To continue our tutorial, we will use screenshots that were made in Windows 8.1.



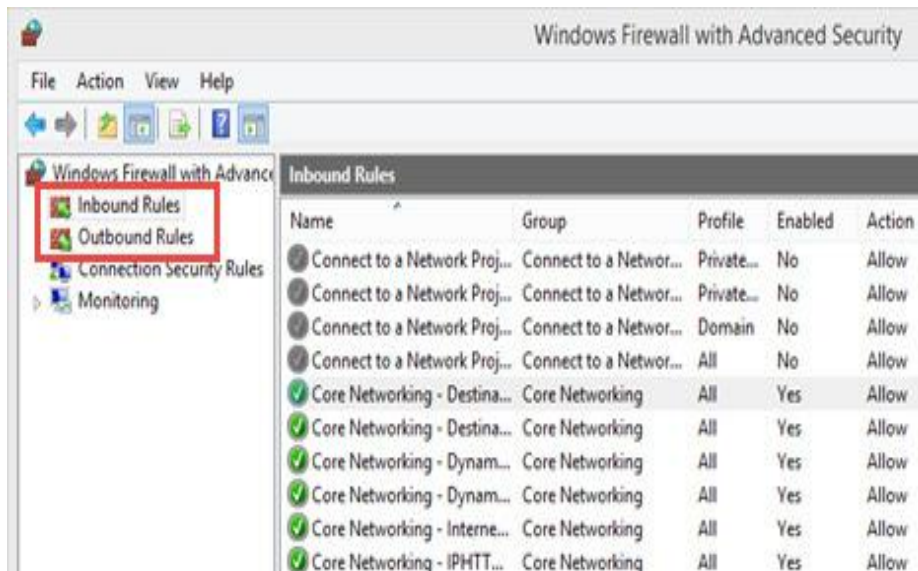
### 2.1.3.2 What Are The Inbound & Outbound Rules?

In order to provide the security you need, the *Windows Firewall* has a standard set of inbound and outbound rules, which are enabled depending on the location of the network you are connected to.

Inbound rules are applied to the traffic that is coming from the network and the Internet to your computer or device. Outbound rules apply to the traffic from your computer to the network or the Internet.

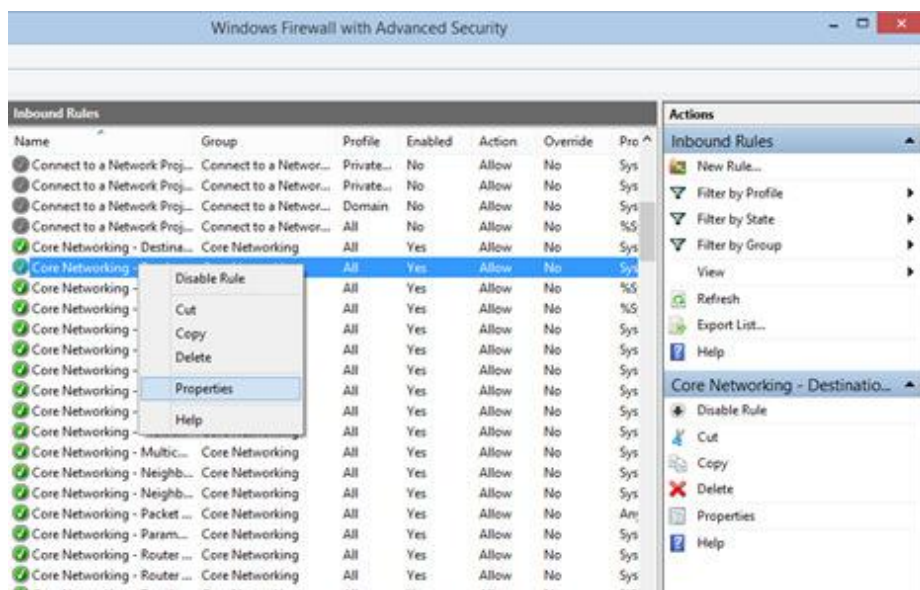
These rules can be configured so that they are specific to: computers, users, programs, services, ports or protocols. You can also specify to which type of network adapter (e.g. wireless, cable, virtual private network) or user profile it is applied to.

In the *Windows Firewall with Advanced Security*, you can access all rules and edit their properties. All you have to do is click or tap the appropriate unit in the left-side panel.



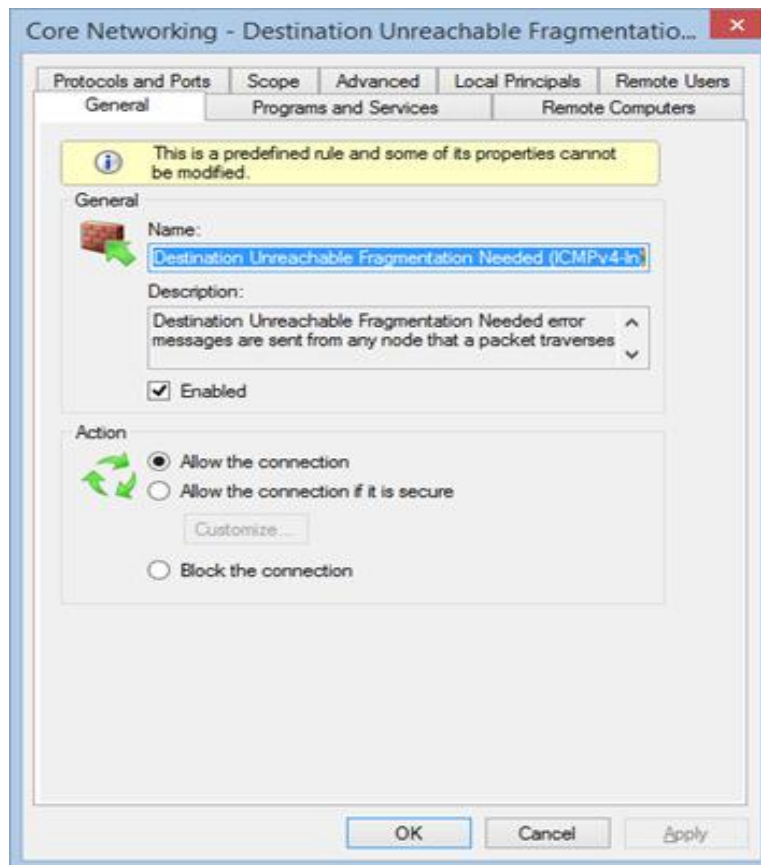
The rules used by the *Windows Firewall* can be enabled or disabled. The ones which are enabled or active are marked with a green check-box in the *Name* column. The ones that are disabled are marked with a gray check-box.

If you want to know more about a specific rule and learn its properties, right click on it and select *Properties* or select it and press *Properties* in the column on right, which lists the actions that are available for your selection.



In the *Properties* window, you will find complete information about the selected rule, what it does and in when it is applied. You will also be able to edit its properties and change any of the available parameters.





### 2.1.3.3 What Are The Connection Security Rules?

Connection security rules are used to secure traffic between two computers while it crosses the network. One example would be a rule which defines that connections between two specific computers must be encrypted.

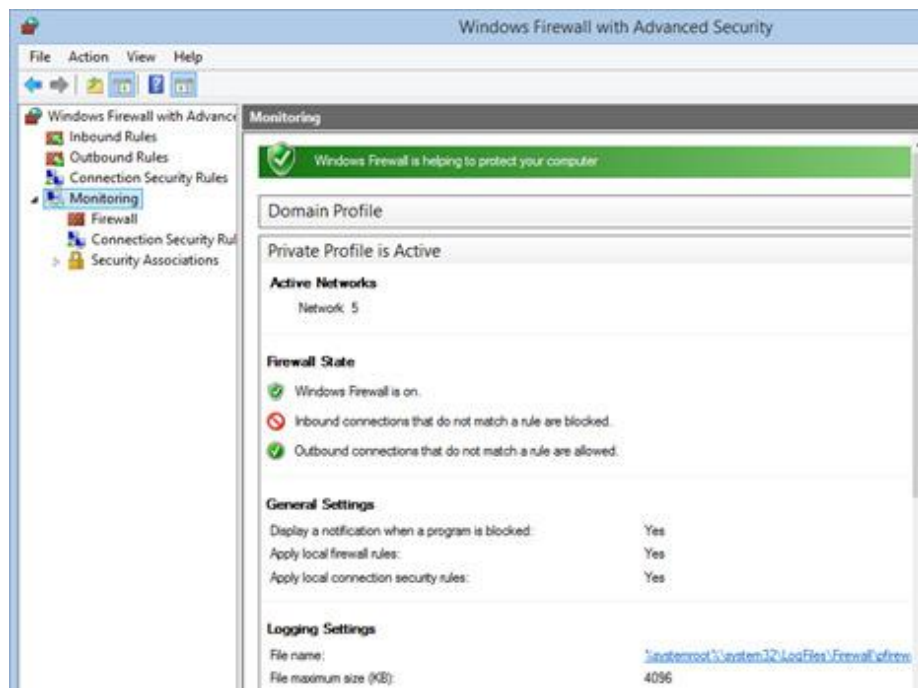
Unlike the inbound or outbound rules, which are applied only to one computer, connection security rules require that both computers have the same rules defined and enabled.

If you want to see if there are any such rules on your computer, click or tap "*Connection Security Rules*" on the panel on the left. By default, there are no such rules defined on Windows computers and devices. They are generally used in business environments and such rules are set by the network administrator.



#### 2.1.3.4 What Does the Windows Firewall with Advanced Security Monitor?

The *Windows Firewall with Advanced Security* includes some monitoring features as well. In the *Monitoring* section you can find the following information: the firewall rules that are active (both inbound and outbound), the connection security rules that are active and whether there are any active security associations.



You should note that the *Monitoring* section shows only the active rules for the current network location.

---

## EXPERIMENT-3

---

**AIM: Steps to ensure Security of any one web browser (Mozilla Firefox/Google Chrome).**

### 3.0 Learning Objectives

At the end of the session you will be able to

- Understand the security and privacy features and operation of browsers.
- Know the security vulnerabilities of browsers.
- Explore, how to browsers hacks and there steps for better security.
- Learn, how to stop advertisers from tracking you
- Learn to stop your browser from automatically downloading malware.
- Learn to block pop-ups and ads
- Know , how to avoid unsafe websites
- Learn how to manage cookies

### 3.1 Browser security is an important part in keeping your information safe.

**Your browser is the window to the internet** and also the first line of defence against malware threats. Some small tweaks to your browser security settings are all that you need to make your time online that much safer.

### 3.2 Browser features and their security vulnerabilities

Browsers use many tools for various tasks, such as Java, Flash Player, ActiveX, etc. But these often come with security flaws, which cybercriminals exploit to get access to your PC. A quick rundown of these tools will help you figure out if you need them or not.

**Deactivate ActiveX.** A browser add-on that comes preinstalled on Internet Explorer or Microsoft Edge and only works with these browsers. ActiveX acts as a middle man between your PC and Java/Flash based interactions in certain sites.

This creates security problems by giving malicious websites a window into your PC. What's more, ActiveX is rarely used nowadays, so be on your guard if a site asks you to install it and accept the installation only if you are 150% sure that site is trustworthy.

**Try to disable JavaScript.** JavaScript is a programming language used by websites to run various programs and features. Sites such as YouTube or Google Docs need it to function, but so do advertising, pop-up software and a whole host of other spammy elements from the internet.

Cybercriminals use JavaScript in **malicious ways in order to infect your device** with malware and other harmful software.

If you disable JavaScript altogether you will get a much quicker and simplified browser experience, with little to no ads, pop-ups, greatly improved page load times and generally a cleaner Internet experience at the cost of specialized tools such as Google Docs or YouTube.

This doesn't need to be as drastic as it sounds, since browsers do allow you to white list certain sites which can run JavaScript.

**Delete Cookies.** These are small data files stored on your browser. Websites use cookies in order to remember your accounts and passwords, **browsing history and to track user behaviour on their site.**

Because of the information they contain, **cookies are prime targets for cybercriminals**, especially the ones that contain emails, account names and passwords.

When you disable and clear cookies you cut down on the personal data cybercriminals can obtain.

One thing you will want to keep in mind is that **there are two types of cookies:**

First party and third party cookies. First party cookies are placed by the site you visit, for instance you get a first party cookie by cnn.com while visiting cnn.com.

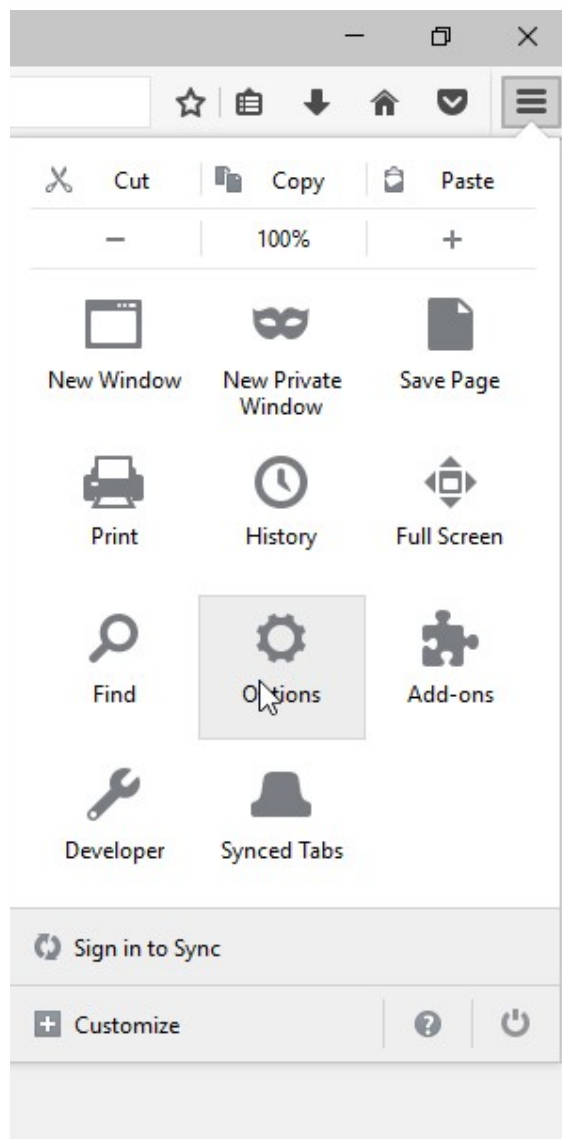
Third party cookies are placed by other sites, for example you get a cookie from amazon.com while visiting cnn.com.

First party cookies are frequently used to remember your login information so you don't have to enter it every time you visit a site. But we can't stress this enough, **don't allow your browser to save passwords!** Third party cookies are almost always placed on your computer by advertisers or marketers interested in tracking your movement online, so nothing bad will happen if you block them.

**Browser extensions and add-ons** add extra functionality to your browser such as ad blocking or search bars. However, these add-ons pose a security risk, since they can open up windows into your PC which can be exploited to inject malware.

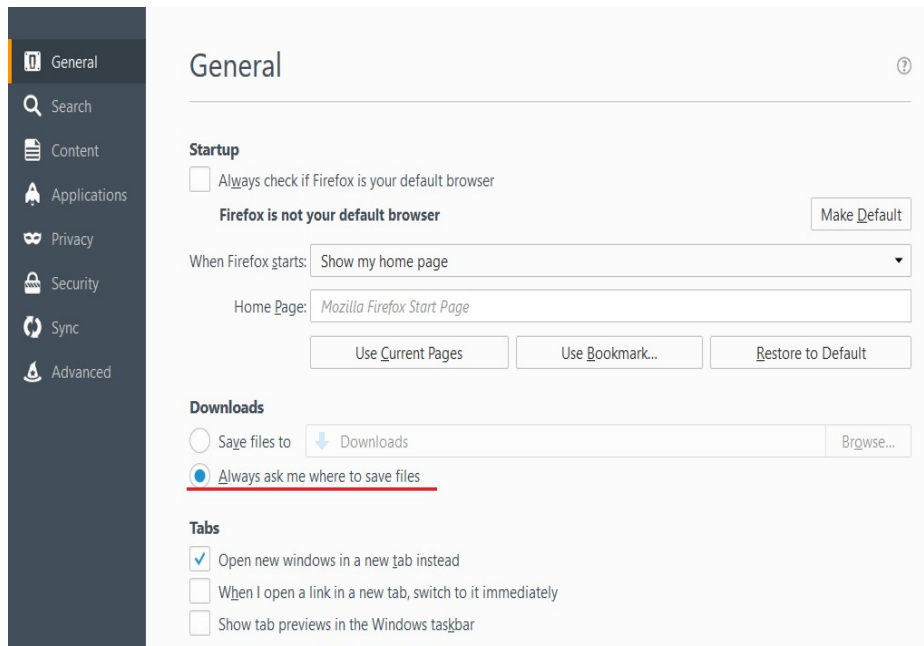
### 3.3 Firefox hacks and tips for better security

If you use Mozilla Firefox and want to improve your browser security settings, press the hamburger menu in the top right corner and go to “Options”.



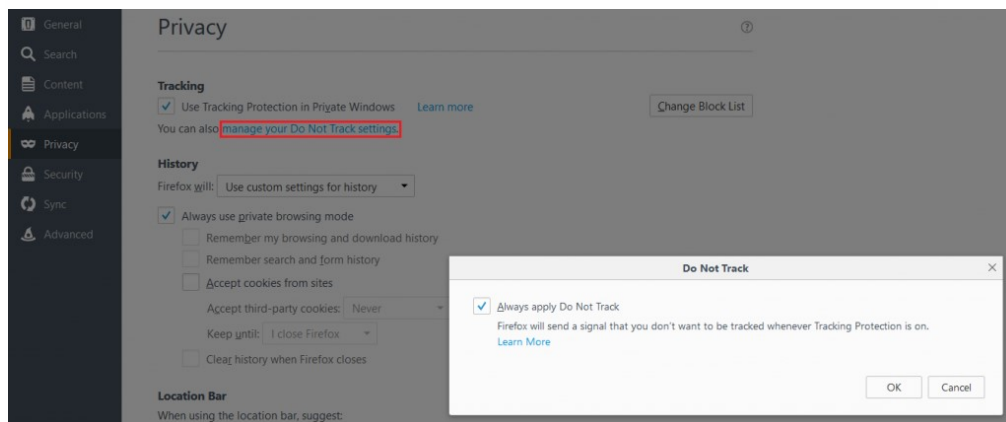
In the “General” tab, at the Downloads section, press “Always asks me where to save files”. This way, you won’t have a web location try to automatically save dangerous content to your computer. At the same time,

this gives you the option to place suspicious content in a safe location where you can analyze it afterwards.

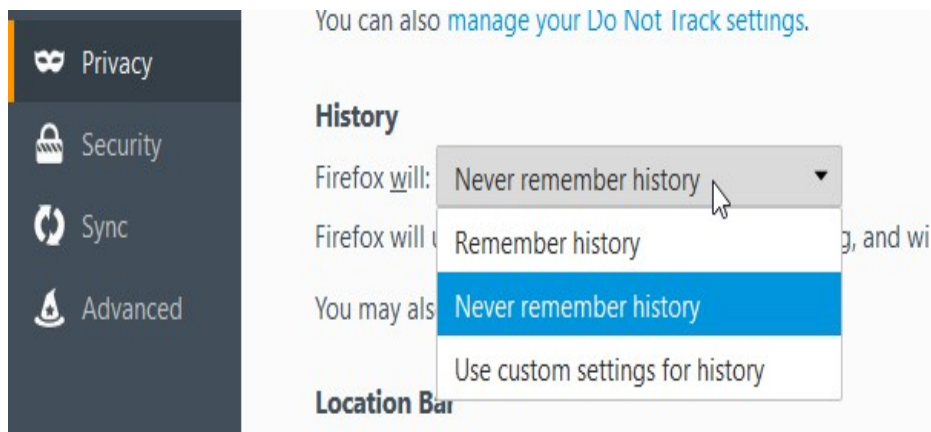


Next, go to the **Privacy** tab.

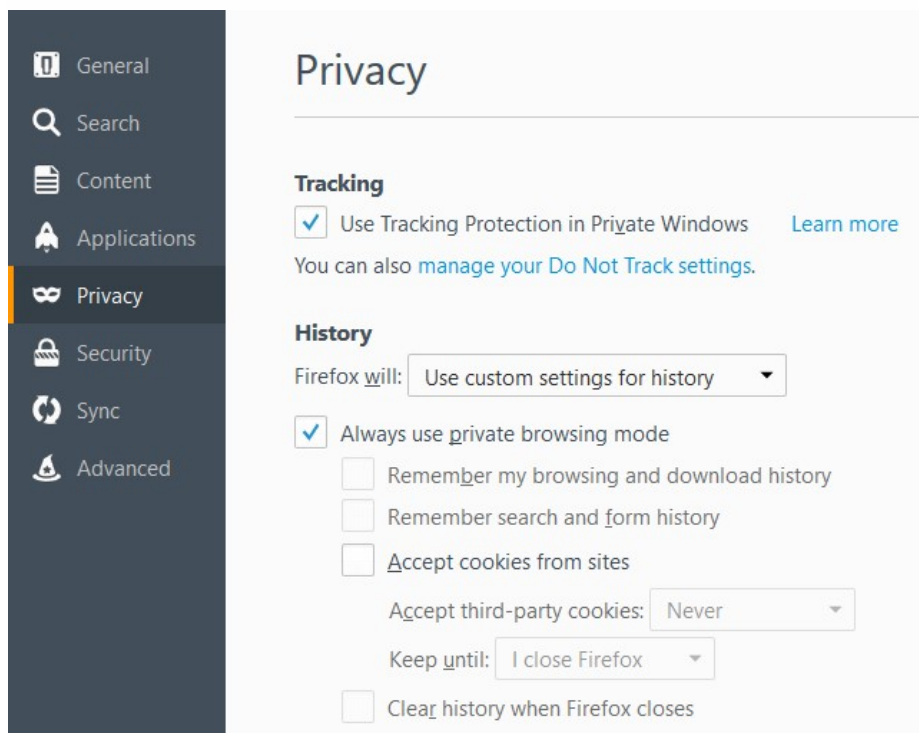
At the “Tracking” section press the blue text with “manage your Do Not Track settings” and check “Always apply do not track”. After you do this advertising, commerce and various other sites shouldn’t be able to track you across the web.



While in the Privacy tab, at the “History” section, choose “Firefox will never remember history”. This is especially important if you know your device may be used by other people.

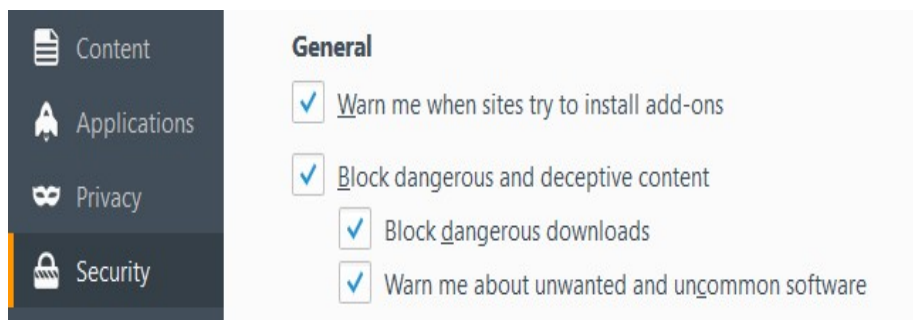


For a more detailed control of your history section, select “Use custom settings for history”.



Check “Always use private browsing mode” so every time you close your Firefox browser it will clear browsing history, search results, cookies and download history.

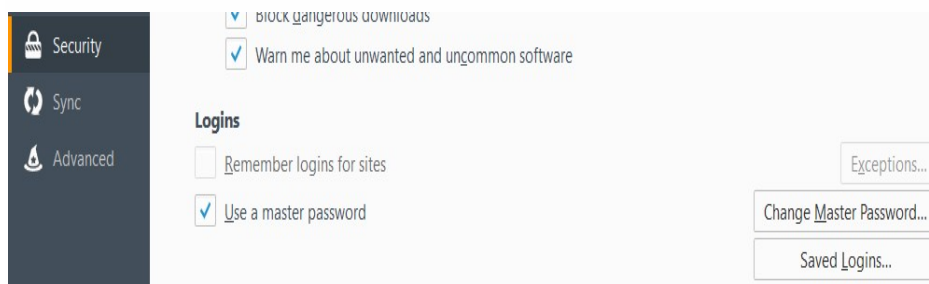
The last changes you should make in Firefox can be found in the “**Security**” category.



First, make sure all of the four check boxes in the General section are checked in. This ensures that your browser will inform you whenever websites try to install malicious add-ons and other content.

In the “Logins” section you can set up a Master Password. Doing this is especially useful when multiple people have access to the computer, since it asks you introduce a master password before you can access logins.

This way, other people won’t be able to access your important accounts such as email. Once more, we cannot recommend this enough, but don’t let your browser remember your passwords.





---

## EXPERIMENT-4

---

**AIM: Study of different types of vulnerabilities for hacking a websites / Web Applications.**

### 4.0 Learning Objectives

After going through this session, you should be able to:

- Know the reasons for attacking web applications
- Identify different types of Web Application Vulnerability

### 4.1 Reasons for Attacking Web Applications

Currently there are many privacy risks in web applications. Today too many websites are hacked by anonymous. They target website because of different types of reasons. They are mentioned in table 1.

Attack Goal	%
Stealing Sensitive Information	42%
Defacement	23%
Planning Malware	15%
Unknown	08%
Deceit	03%
Blackmail	03%
Link Spam	03%
Worm	01%
Phishing	01%
Information Warfare	01%

**Table 1: Reasons for Attacks**

### 4.2 Web Application Vulnerability

There are several different types of attacks used by hackers. These types of attacks and its usage are mentioned in following Table 2.

Attack/Vulnerability Used	% of use
SQL Injection	20 %
Unintentional Information Disclosure	17 %
Known Vulnerability	15 %
Cross Site Scripting (XSS)	12 %
Insufficient Access Control	10 %
Credential/Session Prediction	08 %

OS Commanding	03 %
Security Misconfiguration	03 %
Insufficient Ant automation	03 %
Denial Of Service	03 %
Redirection	02 %
Insufficient Session Expiration	02 %
Cross Site Request Forgery(CSRF)	02 %

**Table 2: Types of Attacks**

This all are the Vulnerability types and how much it's usage. The SQL Injection and Cross Site Scripting are the most famous vulnerabilities in web application. Generally web servers, application servers, and web application environment are affected to following types of vulnerabilities. The OWASP (Open Web Application Security Project) listed all security vulnerability at .There are two types of attacks which are frequently used by hackers namely SQL Injection attack and XSS (Cross Site Scripting) Attack. The following are the brief explanation of each type of attack.

#### **4.2.1 SQL Injection Attack**

Injection means tricking an application into including unintended commands in the data sent to an interpreter. Here what interpreters do? They take strings and interpret them as command. (SQL, OS Shell, XPath, LDAP etc.) Any web application which accepts the user input as a basis of performing database query may be vulnerable to SQL Injection. It uses loopholes in the web application that interact with database. In this attacker exploits input vulnerability and attempt to send incorrect command or SQL query to the web application. These queries can fraud the interpreter to display unauthorized data to hacker. By this attack hacker can Read the important information related to user (user name, password, email) from database. Access admin account and perform all the operation which is done by only admin. Hacker can also modify data by passing query. He run operating systems command on database server. There are also some parts in SQL Injection;

- Union Based SQL Injection
- String Based SQL Injection
- Error Based SQL Injection

#### **4.2.2 Cross Site Scripting (XSS)**

XSS is also one of the danger attacks. In this attack hacker simply inject script in WebPages. These pages are returned to client and malicious code will be executed in the browser of client with alert popup. And by simply

responding the web application hacks. (Ex. Attacker sets the trap – update my profile then victim views page – see Attacker profile and script silently sends attacker victim's session cookie). Hacker can Access cookies, session tokens, do remote code execution and get sensitive data. We can classify XSS into two classes' server XSS and client XSS. There are three types of XSS;

- Stored XSS
- Reflected XSS
- Dom based XSS

Stored XSS also known as persistent XSS .This occurs when hacker stored malicious script permanently in target server like database, visitor log, and comment field or in URL. Reflected XSS occur when hacker insert inject script into some input field.

#### **4.2.3 Broken Authentication / Session Management**

This attack also like bypass authentication. Authentication is method utilized by web application to verify that whether the user is authorize or not. Valid user's password and username stored in to database. This is a most frequent system for web application. Various actions can break the authentication no matter its strong. If the user authentication system of website is weak then Hacker can take full advantage he can change the password, modify account information, and get sensitive information.

#### **4.2.4 Cross site request forgery (CSRF)**

This attack also like a XSS but there is one difference that is here attacker create forged http request (e.g. Update account, login – logout, purchase process) and forced victim in to submitting malicious action via image tags, XSS, or other techniques. In which he is authenticated such as submitting http request through alert box or with other techniques. If the user is authenticated the attack succeeds. By this attack attacker can steal all the information or get the password or username.

#### **4.2.5 Insecure Direct Object References**

When developer expose references to initial implementation object like file, dictionary, database key. Without access control check or other protection attacker can manipulate these references to access an authorized data hacker who is unauthorized simply changes a parameter value that directly refers to the system object to another object the user isn't authorized for .

#### **4.2.6 Security Misconfiguration**

Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server and platform. In these types of attack hacker accesses default accounts, unused pages, un-patched flaws, unprotected files and dictionaries to gain unauthorized access or for the knowledge of the system.

#### **4.2.7 Sensitive Data Exposure**

Many applications do not properly protect important information like credit card; tax ID's, authentication Ids. Hacker may steal or change such weekly protected data to conduct credit card fraud, id theft or other crimes. Hacker generally does not break cryptography. They break something else such as steal keys, do man in middle attacks or steal clear text data of the server while transit or from user's browser.

#### **4.2.8 Using Components with Known Vulnerability**

Components like frameworks or software module always run with full privileges. If vulnerable component exploited then attack can facilitate important data loss. In this hacker search a weak component by scanning. He customizes the exploit as need and executes the attack.

#### **4.2.9 Invalidated Redirects and Forwards**

Generally web application redirects users to another page or website and use un-trusted data to consider designation pages without proper validation. Hacker can redirect victim to phishing site. Hacker links to redirect and forced victim to click. Since the link is to a valid site. Attacker targets unsafe forward to bypass authentication.

#### **4.2.10 Missing Function Level Access Control**

Mostly web applications verify function level rights before making that visible in the UI. Application need to perform the same access control checks on the server when each function is accessed. If request are not verified hacker, it will be able to forge requests in order to access functionality without proper authorization. Hacker who is authorized user simply changes the URL or a parameter to privileged system. He can also access private functions that aren't protected.

---

## EXPERIMENT-5

---

**Aim-: Analysis the Security Vulnerabilities of E-commerce services.**

### 5.0 Learning Objectives

After going through this session, you should be able to:

- Know about Security Vulnerabilities of E-commerce services.
- Identify the vulnerabilities input validations and database servers.
- Point out the vulnerabilities in TCP/IP Protocols used for communications.

### 5.1 Security Vulnerabilities of E-commerce services

Vulnerability is a weakness which allows an attacker to reduce a system's information assurance. Vulnerability is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw. To exploit vulnerability, an attacker must have at least one applicable tool or technique that can connect to a system weakness

#### 5.1.1 Software life cycle not secure.

Over the years, efforts to enhance software development life cycle (SDLC) practices have been shown to improve software quality, reliability, and fault-tolerance. Now-a-days strategies to improve the security of software in organizations such as Microsoft, Oracle, and Motorola have resulted in software products with less vulnerabilities and greater dependability, trustworthiness, and robustness.

As per the SANS Institute's Top 20 list of security vulnerabilities, the MITRE Common Vulnerabilities and Exposures (CVE) site, the US-CERT Technical Cyber Security Alerts site, and the Microsoft Security Advisory site show that common software defects are the leading cause of security vulnerabilities (buffer overflows have been the most common software defect leading to security vulnerabilities).

Some of the things that can be incorporated in SDLC are:

1. Software should be installed using security defaults
2. A software patch management process should be there.

#### 5.1.2 Vulnerabilities due to input validations

**Buffer Overflow:** A buffer overflow condition occurs when a program attempts to copy more data in a buffer than it can hold. Buffer overflow is

probably the best known form of software security vulnerability. At the code level, buffer overflow vulnerabilities usually involve the violation of a programmer's assumptions. Hackers use buffer overflows to corrupt the execution stack of a web application. Buffer overflow flaws can be present in both the web server or application server products that serve the static and dynamic aspects of the site. Buffer overflows generally resulted in to crashes. Other type of attacks will create the situation like lack of availability are possible, including putting the program into an infinite loop.

**5.1.3 Log Forging:** Writing invalidated user input to log files can give access to attacker for forging log entries or injecting malicious content into the logs. Log forging vulnerabilities occur in following conditions:

- i) Data copied to an application from an unreliable source.
- ii) The data is copied to an application or system log file.

Applications uses log file to store a history of events for later review and record, statistics gathering, or debugging. Analysis of the log files may be misdirected if an attacker can supply inappropriate data to the application. In the most common case, an attacker may be able to insert false entries into the log file by providing the application with input that includes appropriate characters. If the log file is processed automatically, the attacker can render the file unusable by corrupting the format of the file or injecting unexpected characters. A more dangerous attack might involve changing the log file statistics.

**5.1.4 Missing XML Validation:** Failure to implement validation when parsing XML gives an attacker the way to supply malicious input. By accepting an XML document without validating it against a DTD or XML schema, the programme gives chance to attackers to copy unexpected, unreasonable, or malicious input. It is not possible for an XML parser to validate all aspects of a document's content; a parser cannot understand the complete semantics of the data. However, a parser can do a complete and thorough job of checking the document's structure and therefore guarantee to the code that processes the document that the content is well-formed.

**5.1.5 Validation checks in client:** Performing validation check in client side code, mostly JavaScript, provides no protection for server-side code. An attacker can simply disable JavaScript, use telnet, or use a security testing proxy to bypass the client side validation. Client-side validation is widely used, but is not security relevant.

**5.1.6 Vulnerabilities in database servers:** There are various techniques to attack a database. External attacks may exploit configuration weaknesses that expose the database server. Also weak and insecure Web application

can be used to exploit the database. An application with excess privilege in the database can put database at risk. The main threats to a database server are:

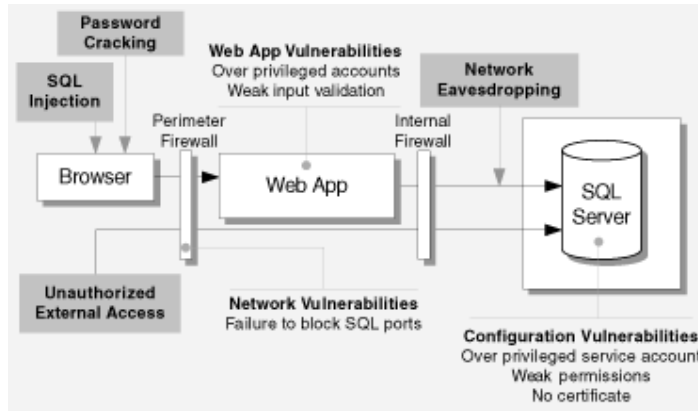


Fig 1: Main threats to a database server

- **SQL injection**: Technique used to attack database through website entry fields.
- **Network eavesdropping**: It is a network level attack consisting of capturing packets from the networked computers.
- **Unauthorized server access**: Attacked made unauthorised access through various loopholes in the system such as O/S, non availability of firewall etc.
- **Password cracking**: Technique of recovering password from data stored in computer.

### 5.1.7 Vulnerabilities in TCP/IP Protocols used for communications

TCP/IP is very popular and known to everyone, IP – (Internet Protocol) that handles routing packets of data from one computer to another or from one router to another. TCP, (Transmission Control Protocol) , deals with ensuring that the data packets are delivered in a reliable manner from one computer to another.

## 5.2 Major causes of vulnerabilities

- Dependency on IP source address for authentication
- Minimal/no authentication in network control mechanisms, e.g. routing protocol, congestion control, flow control, ICMP messages, etc.

### 5.2.1 Vulnerabilities in firewall

Firewall vulnerability is defined as an error made during firewall design, implementation, or configuration that can be exploited to attack the trusted network that the firewall is supposed to protect. For example, common firewall vulnerabilities and improper configurations include:

- (1) ICMP allowed, e.g., the firewall can be ping-ed;

- (2) Provides the attacker with additional information, or improves the speed of the attacker's port scan by doing Denial rather than drop of traffic to ports by the firewall suppose to block;
- (3) Misconfiguration that allows a TCP ping of internal hosts with Internet-routable IP addresses (e.g., in-bound TCP 80 is not restricted to the web server);
- (4) Trust or unrestricted access to certain IP addresses;
- (5) Availability of extra/ non required services on the firewall;
- (6) Unnecessarily open TCP and UDP ports;

**5.2.2 Vulnerability in IPS:** The main function of intrusion prevention systems is to identify malicious activity, log information about malicious activity, attempt to block/stop activity, and report activity. Some of the IPS Vulnerabilities are as follows:

- (1) Under estimation of security capabilities, including information gathering, logging, detection, and prevention.
- (2) Focus on Performance rather than security, including maximum capacity and performance features.
- (3) Non-defined Management policies, including design and implementation (e.g., reliability, interoperability, scalability, product security), operation and maintenance (including software updates), and training, documentation, and technical support.

### 5.2.3 Vulnerability loopholes of the users

- (1) **Tolerating weak passwords:** weak passwords are arguably the most nonsensical, yet simplest security flaws to fix.
- (2) **Connecting to unsecured Wi-Fi hotspots:** Many people don't think twice about logging onto a random (and unprotected) wireless network just to get some work done. That's all it takes for someone with ill intent to capture a user's login credentials and work his way onto your wireless network.
- (3) **Ignorance in encrypting hard drives and USB storage disks:** Simply encrypting computer hard drives can eliminate a huge portion of information risks.
- (4) **Assuming that patches are under control:** There are typically hundreds of missing patches on both workstations and servers. In many situations, admins are unaware of specific patches to be installed.
- (5) **Not balancing security with convenience:** Unintended acts, security controls often get in the way of users, who then find ways around it. General habit of writing passwords on sticky notes is just the beginning.



---

## EXPERIMENT-6

---

**AIM:** Analysis the security vulnerabilities of E-Mail Applications

### 6.0 Learning Objectives

At the end of the session you should be able to

- Understand the security issues and vulnerability in Email system.
- Identify the threats in Email Communication
- Point out the limitations exists in currently used protocols.

### 6.1 Security Issues and vulnerability in Email System

E-mail is one of the main modes of communication today but in the following section it can be seen how insecure it is. The importance of email is for corporate and private communication can be estimated by the summary presented by Radicati Group's report titled "E-Mail Market, 2012-2016" that the world wide each day total emails sent in 2012 was 144.8 billion, which is increased steadily with each passing year and in 2016 approximately 192.2 billion emails will sent each day. The report also states that corporate webmail clients grow from 629 million in 2012 to over one billion by the end of 2016.

### 6.2 Threats in Email Communication

**Eavesdropping:** E-mail messages pass through networks which are part of big picture i.e. Internet with a lot of people on it. So it is very easy for someone to track or capture your message and read it.

**Identity Theft:** Means someone pretend to be you on the network. It may be possible if not proper security protocols are followed that someone may steal or capture your username/password and used to read your email messages. Further also send email messages from your account without your knowledge.

**Message Modification:** Anyone who captures your message can also alter your message contents if it is not encrypted. Further anyone having administrative rights on any of SMTP server your message visit can not only read your message but can also modifies it.

**False Messages:** Sender's name can easily be fabricated so it is very easy to send message that pretends to be send by someone else.

**Unprotected Backups:** Messages generally stored in plain Text on SMTP server and also backups can be created. Even if you delete the message they can be residing on the severs/backup-servers for years. So anyone who accesses these servers can also access or read your message.

**Repudiation:** As it is known that email messages can easily be forged so anyone sending you some message can later on deny regarding sending of message and it is very difficult to prove it. This has implications corresponding to emails use as contracts in business communications.

**Email spoofing:** Sometime email that pretends to be received from an authentic source but in actual it is send from somewhere else.

**Email Spamming:** Spam or junk mail refers to sending of email to no. of persons for any advertisement purpose or for some malicious intent. To send spam often lists are created by searching data from Internet, or by stealing mailing list from the internet.

**Email bombing:** E-mail "bombing" is refers to sending identical mail repeatedly by abusers to a particular address/user.

**Sending threats:** Threatening mails are sending to users which disturb their state of mind or to provoke them to take some wrong step. Sometimes false statements are also forwarded to third parties or users to injure the reputation of some particular person. It is called as Defamation, a communication is not considered defamatory unless it is forwarded to someone other than the target.

**Email frauds:** Email Fraud is the intentional deception made for some personal or monetary gain.

**Emails used as tools to spread malicious software:** Emails are also used as tools to spread viruses, worms and other malicious software. They are attached to your emails as attachment, when you click on them they attack your computer or browser.

**Phishing:** It is also most common attack through email. It is originally defined as an attack to steal your confidential information like passwords, ATM pin and other bank credentials. It works as some email coming to you that pretends to be from some trusted source you know like your bank. These emails entice you to click on some link present in email or to open

some attachment or respond to some message and that click directed to you their site in actual but it appears like your trusted website of bank and ask to fill some confidential information like passwords which is actually stolen from you and use for any malicious intent later on.

### **6.3 Limitations exist in currently used protocols**

Any Network service like email system must provide following five services for security reasons

**Message Confidentiality:** It promotes privacy that is the message transfer between sender and receiver is secure and no one can read or track the message while transferring.

**Message Integrity:** It says that the same message/data should arrive at receiver end as it can be send by sender. No alteration intentionally or accidentally takes place during transfer.

**Message Authentication:** It ensures that message can be received from the sender only or from the trusted source. In this receiver must be sure about the identity of sender.

**Message Non-repudiation:** It ensures that anytime sender should not be able to deny sending of message which originally sends by him/her.

**Entity Authentication:** It ensures identification of user; the user must be verified before accessing the resources and services. This is done by asking login-id and password.

**SMTP:** SMTP does not encrypt messages. So the communication between SMTP servers is in plain text so eavesdropping takes place. If you are login to SMTP server using your username and password that is also pass in plain text so again anyone stole your information during transfer. Messages sent through SMTP also contains information about sending computer and software used which when capture can be used for malicious intent. So SMTP lacks privacy concern.

**POP and IMAP:** POP and IMAP are pull protocols, Request is send to mail server to access the mailbox and for that login using username and password is required. These details are not encrypted before sending unless SSL is used. So our confidential information is at stake.