

**Ex. No : 10**

## **Study to configure Firewall, VPN**

### **AIM:**

To study and configure firewall and VPN.

### **PROCEDURE FOR CONFIGURING FIREWALL AND VPN:**

#### **Working with Windows Firewall in Windows 7**

##### **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.

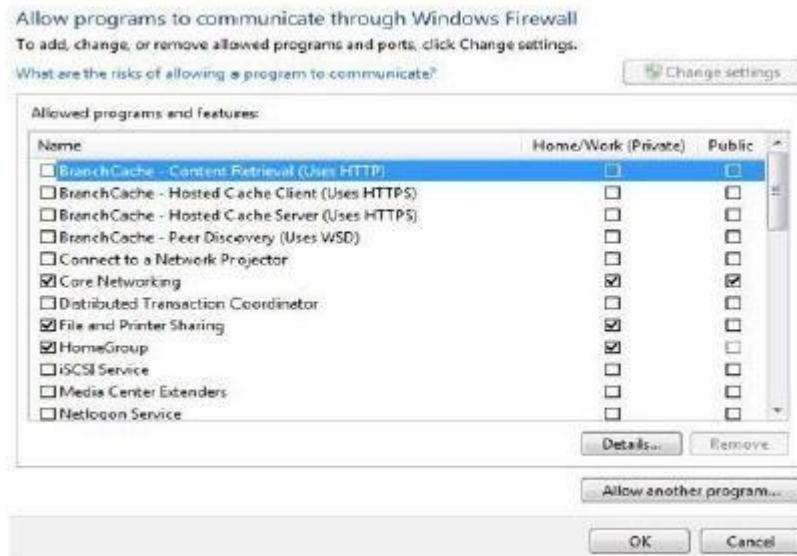
With firewall in Windows 7 we can configure inbound and outbound rules. By default, all outbound traffic is allowed, and inbound responses to that traffic are also allowed. Inbound traffic initiated from external sources is automatically blocked.

#### **Configuring Windows Firewall**

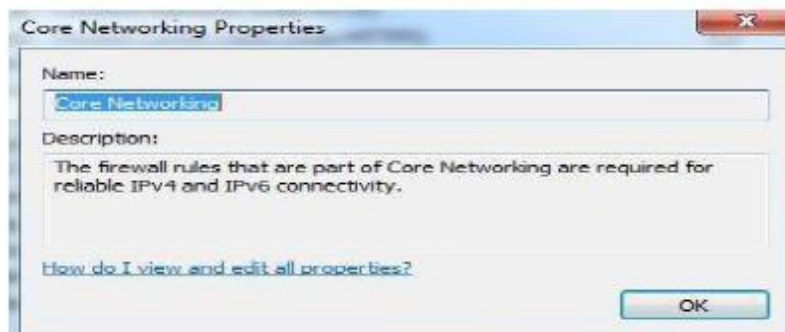
**To open Windows Firewall we can go to Start > Control Panel > Windows Firewall.**



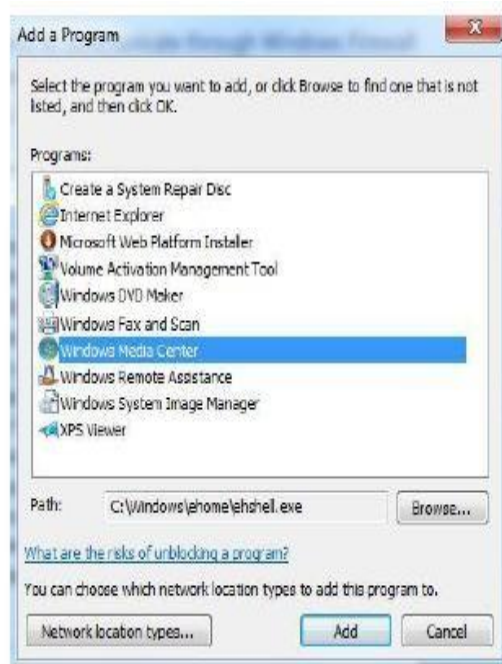
it is also configured to block all connections to programs that are not on the list of allowed programs. To configure exceptions we can go to the menu on the left and select "Allow a program or feature through Windows Firewall" option.



To change settings in this window we have to click the "Change settings" button. the Core Networking feature is allowed on both private and public networks, while the File and Printer Sharing is only allowed on private networks.



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.

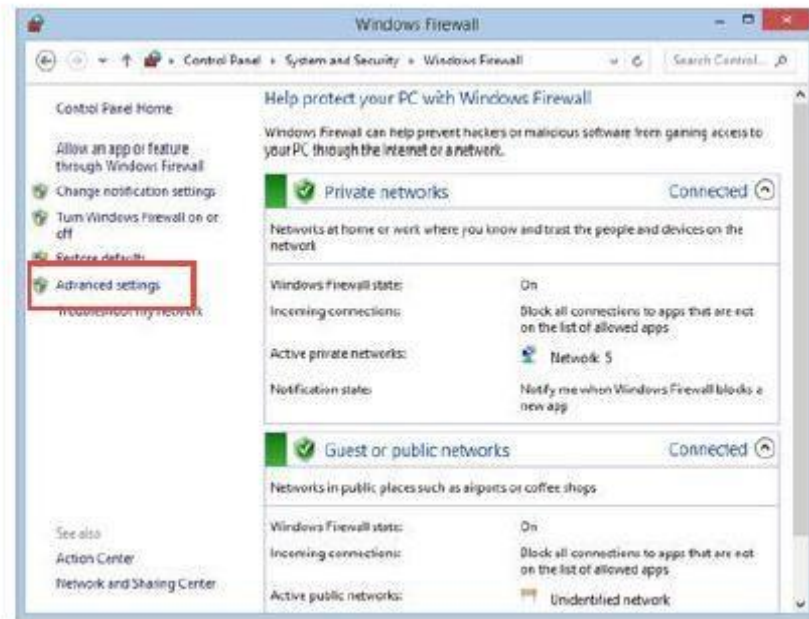


a Program

Program will be allowed to communicate by clicking on the "Network location types" button.



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



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.

## RESULT

Thus the firewall configuration and VPN installations are studied successfully.

Ex.No: 4	<b>Installation of Wireshark, TCPdump and observe the data transferred in client-server communication using UDP/TCP and Identify the UDP/TCP datagram.</b>

**Aim:**

To install wireshark, TCPdump and observe the data transferred in client-server communication using UDP/TCP and Identify the UDP/TCP datagram.

**Wireshark:**

Wireshark is an open-source tool for profiling network traffic and analyzing packets. Such tool is often referred as a network analyzer, network protocol analyzer or sniffer.

It is used to understand how communication takes place across a network and to analyze what went wrong when an issue in communication arises.

It captures network traffic from ethernet, Bluetooth, wireless (IEEE.802.11), token ring, and frame relay connections, among others, and stores that data for offline analysis.

Wireshark allows you to filter the log before the capture starts or during analysis, For example, you can set a filter to see TCP traffic between two IP addresses, or you can set it only to show you the packets sent from one computer. The filters in Wireshark are one of the primary reasons it has become the standard tool for packet analysis.

**Installation of Wireshark:**

**Step 1:** Your first step is to head to the Wireshark download page <https://www.wireshark.org/download.html> and locate the Windows installer.



**Step 2:** You will be presented with the Wireshark wizard to guide you through the installation. Click “Next.”

**Step 3:** Next, you can review, agree to the license agreement, and click “Noted” to continue.

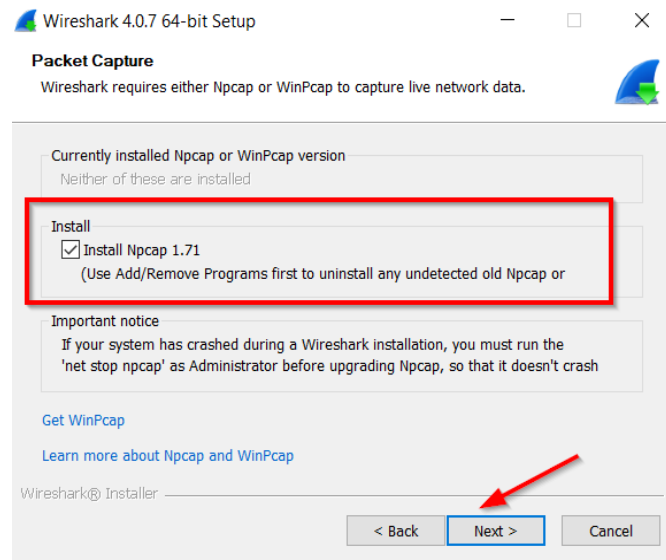
**Step 4:** You will be asked what components you want to install. You can make your

choice and then click “Next.”

**Step 5:** Choose a directory to install Wireshark in, showing you the space required to install it.

**Step 6:** Install Ncap.

Ncap is an open-source library for packet capture and network analysis which allows Wireshark to capture and analyze network traffic effectively. It enhances Wireshark's capabilities by providing optimized packet capture.



**Step 7:** The next screen will ask if you want to install USBPcap, an open-source USB packet capture utility that lets you capture raw USB traffic, helping analyze and troubleshoot USB devices, this is not mandatory.

Click “Install” to begin the installation.

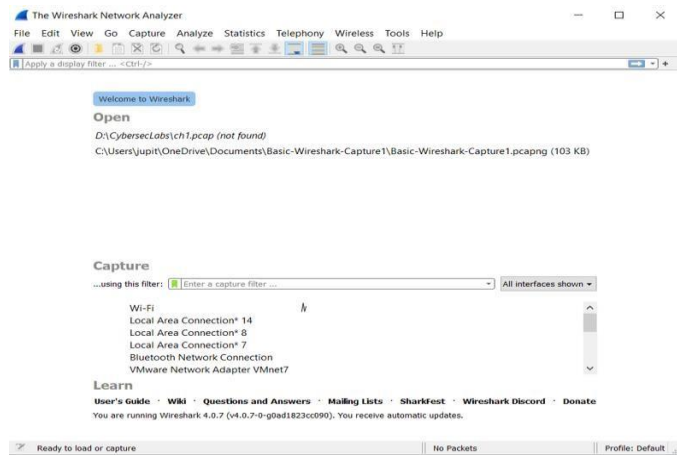
**Step 8:** Wireshark will now begin the installation process. A window will pop up during installation to install cap.

**Step 9:** Ncap will begin the installation; click “Next” once complete.

**Step 10:** Wireshark will now complete its installation. Once complete, you can click “Next.”

**Step 11:** On the last window, click “Finish” to complete the setup.

**Step 12:** Wireshark will now be installed, and you can begin packet capturing.



When you install the wireshark program, the wireshark GUI with no data will be displayed.

Select one of the wireshark interface, eth0, eth1 will be displayed. Click “Start” for interface eth0 to begin the Packet capture.

All packets being sent/received from/by the computer are now being captured by wireshark. Click”Start”.

## Wireshark User Interface:

The wireshark interface has 5 major components;

- The **Command menus** are the standard pulldown menus located at top.
- The **Packet listing window** displays a one-line summary for each packet captured, it includes Packet number, Packet captured time, Packet’s source & destination address, Protocol type, Protocol specific information.
- The **Packet header details** window provides about packet selected in the packet listing window. It includes details about Ethernet frame and IP datagram of the packet. If the packet has been carried over by TCP/UDP, that details will also be displayed.
- **Packet contents window** display entire contents of the captured frame in both ASCII and hexadecimal format.
- In the **Packet display filter field**, the protocol name or other information can be entered to filter the information displayed in packet listing window.

## Capturing Packets:

After installing and downloading wireshark, Launch it and click the name of an interface under Inyerface List to start capturing packets.



## Test Run:

Start any browser → Start the Wireshark software → Select an interface → Stop Wireshark packet capture once the browser has been displayed.

**Colour coding:** Packets will be highlighted in blue, green, black which helps to identify the types of traffic.

Green → TCP traffic, Dark Blue → DNS traffic, Light Blue → UDP traffic, Black → TCP packets with problems.

## Inspecting Packets:

Click on any packet and go to the bottom pane.

### Inspecting Packet flow:

We have a live packet data that contains all protocol messages exchanged between your computer and other network entities.

To filter the connection and to get a clear data type “http” in the filtering field. Note that directly typing the destination will not work as Wireshark doesn’t have the ability to discern the protocol field.

To get more precise data set

http.host==www.networksecurity.edu Right click on any packet → Select “Follow UDP Stream”.

Close the window, change filter back to

“http.host==www.networksecurity.edu” follow a packet from the list that matches the filter. Use “Contains with other protocols.”

## TCPdump:

**TCP** (Transmission Control Protocol) facilitates the transmission of packets from source to destination.

**Tcpdump** is a command line utility that allows you to capture and analyze network traffic going through your system. It is often used to help troubleshoot network issues, as well as a security tool.

It is a network monitoring and management utility that captures and records TCP/IP data on the run time. Tcpdump is designed to provide statistics about the number of packets received and captured at the operating node for network performance analysis, debugging and diagnosing network bottlenecks and other network-oriented tasks.



**Identifying UDP/TCP datagram:**

IP packets have 8-bit header (Protocol for v4 and Next Header in v6) which determines which transport-layer protocol is used in the payload. For example, if it's 6, the payload is a TCP segment, and if it's 17 then that is an UDP.

TCP is connection-oriented while UDP is connectionless.

TCP sends data in a particular sequence, whereas there is no fixed order for UDP protocol.

**Result:**

Thus, the installation of Wireshark, TCPdump and observing the data transferred in client-server communication using UDP/TCP and Identifying the UDP/TCP datagram has been executed successfully.

Ex.No: 6	Experiment Eavesdropping, Dictionary Attack, MITM Attacks.

**Aim:**

To experiment Eavesdropping, Dictionary Attack, MITM Attacks.

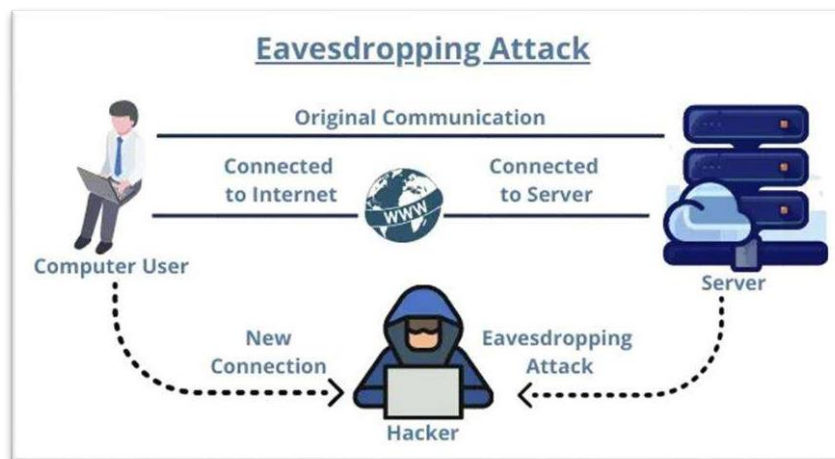
**EAVESDROPPING:**

Eavesdropping refers to the unauthorised and unseen intervention of a private, live conversation.

Sniffing or Eavesdropping pertains to the act of acquiring or intercepting data by capturing the communication flow within a network using a packet sniffer tool.

This technique involves monitoring the packets of information passing through the network, allowing unauthorized access to sensitive data, akin to theft or unauthorized interception of information.

During the transmission of data across networks, if the data packets lack encryption, they become vulnerable to interception, enabling unauthorized parties to read the contents of these network packets with the use of a sniffer.

**Categories of Network Sniffing:**

Active and Passive Sniffing attacks are two distinct categories of network sniffing techniques used by attackers to intercept and analyze data traffic.

**1. Active Sniffing:**

Active Sniffing is performed through a Switch and it is easy to detect.

It involves more direct interaction with the network traffic. Instead of just observing and capturing data, the attacker actively injects or modifies packets within the communication flow.

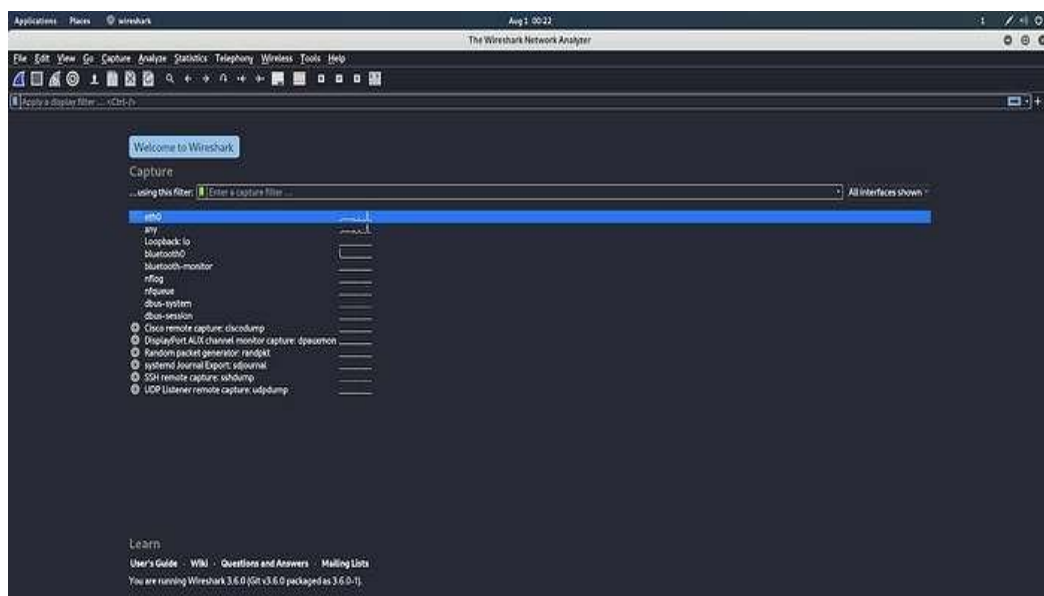
## 2.Passive Sniffing:

Passive Sniffing is performed through a Hub which is difficult to detect.

It involves silently capturing and monitoring network traffic without altering or modifying the data being transmitted. The attacker's presence is relatively discreet, as they do not actively participate in the communication process. They just observe the data that flows through the network, looking for sensitive/crucial information that is not encrypted.

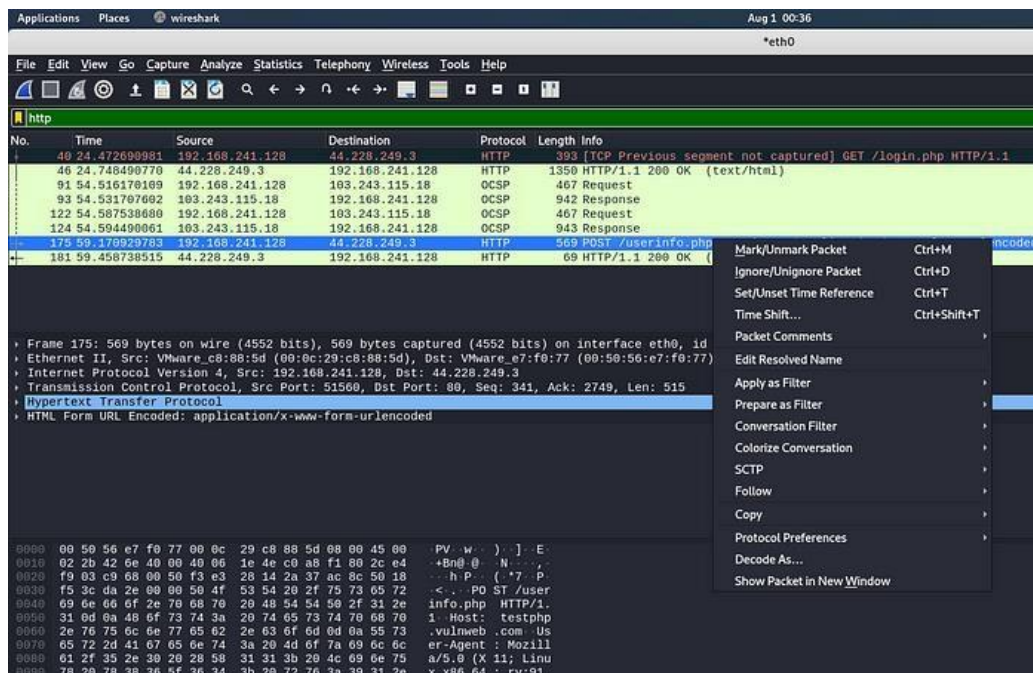
### Experimenting Eavesdropping:

**Step 1:** Launch the Wireshark software on your computer and choose the 'eth0' option, In your web browser, input the URL we want to capture login credentials from.



**Step 2:** Input the login credentials, which are 'test', and then click on the login button.

**Step 3:** Then by entering 'http' in the filter section, the captured packets using the HTTP protocol will be shown. Choose 'Follow' to access additional options, then select 'http stream' from the available choices.



**Step 4:** Explore the provided information, and you will uncover the login credentials.

**Output:**

```
<div id="siteInfo"> <a href="http://www.acunetix.com">About Us</a> | <a href="privacy.php">Privacy Policy</a> | <a href="mailto:wvs@acunetix.com">Contact Us</a> | &copy;2019
Acunetix Ltd
</div>
<br>
<div style="background-color:lightgray;width:100%;text-align:center;font-size:12px;padding:1px">
<p style="padding-left:5%;padding-right:5%"><b>Warning</b>: This is not a real shop. This is an example PHP application, which is
intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and
bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well.
Tip: Look for potential SQL injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.</p>
</div>
</body>
<!-- InstanceEnd --></html>
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 20
Origin: http://testphp.vulnweb.com
Connection: keep-alive
Referer: http://testphp.vulnweb.com/login.php
Upgrade-Insecure-Requests: 1

uname=test&pass=testHTTP/1.1 200 OK
Server: nginx/1.19.6
Date: Tue, 01 Aug 2023 05:34:03 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Set-Cookie: login=test%2Ftest
Content-Encoding: gzip

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLOutsideLocked="false" -->
<head>
```

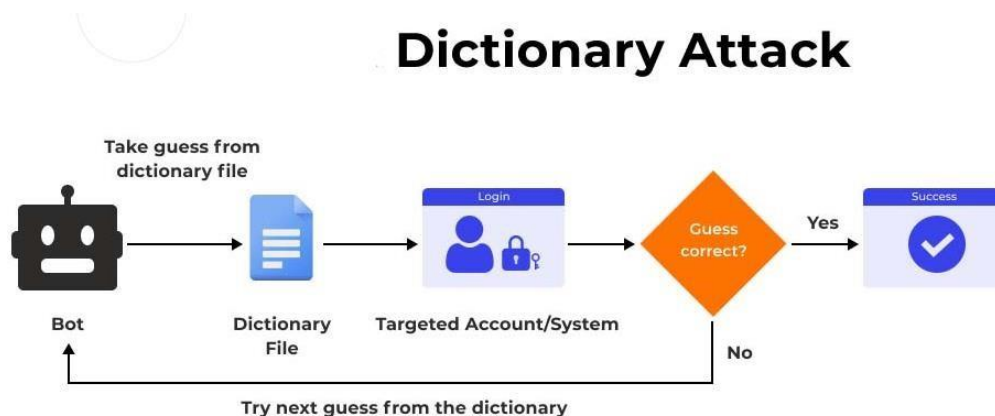
## DICTIONARY ATTACK:

A Dictionary Attack is an attack vector used by the attacker to break in a system, which is password protected, by putting technically every word in a dictionary as a form of password for that system. This attack vector is a form of Brute Force Attack.

Like the brute force attack, the dictionary attack aims to break in by logging in using username and password combinations. It is only inefficient as far as its overall success rate: automated scripts can do this in a matter of seconds.

A hacker will look for applications and websites that don't lock a user out quickly for incorrectusername and password combinations and don't require other forms of authentication when signing in. Sites that allow simple passwords are especially vulnerable.

Suppose the target website or application does not adequately monitor suspicious behavior like this or has lax password rules. In that case, the website runs a high risk of data disclosure resulting from a dictionary attack. Leaked password databases have become a common feature of modern dictionary attacks. Attempting to log in with username and password combinations used multiple times elsewhere makes these dictionary attacks much more successful and potentially harder to detect on the application or website's end.



**Result:**

Thus, Eavesdropping and Dictionary Attack have been implemented successfully.

**Aim:**

To Experiment Sniff Traffic using ARP Poisoning.

**ARP Poisoning:**

Address Resolution Protocol (ARP) poisoning is an attack that involves sending spoofed ARP messages over a local area network. It's also known as ARP spoofing, ARP poison routing and ARPcache poisoning.

ARP poisoning is a type of man-in-the-middle attack that can be used to stop network traffic, change it, or intercept it. The technique is often used to initiate further offensives, such as sessionhijacking or denial-of-service.

The relationship between a given MAC address and its IP address is kept in a table known as the ARP cache. When a packet heading towards a host on a LAN gets to the gateway, the gateway uses ARP to associate the MAC or physical host address with its correlating IP address.

The host then searches through its ARP cache. If it locates the corresponding address, it is used to convert the format and packet length. Otherwise, ARP will send out a request packet that asks other machines on the local network if they know the correct address. When a machine replies with the address, the ARP cache is updated.

**ARP Poisoning Countermeasures:**

We can use several methods to prevent ARP poisoning, each with its own positives and negatives. These include static ARP entries, encryption, VPNs, packet sniffing, Poisoning detection software, OS security, etc.

**Static ARP entries:**

This solution involves a lot of administrative overhead and is only recommended for smaller networks. It involves adding an ARP entry for every machine on a network into each individual computer.

Mapping the machines with sets of static IP and MAC addresses helps to prevent spoofing attacks, because the machines can ignore ARP replies.

**Encryption:**

Protocols such as HTTPS and SSH can also help to reduce the chances of a successful ARP poisoning attack. When traffic is encrypted, the attacker would have to

go to the additional step of tricking the target's browser into accepting an illegitimate certificate.

**VPN:** If it is just a single person making a potentially dangerous connection, such as using public wifi at an airport, then a VPN will encrypt all of the data that travels between the client and the exit server.

### **Operating System Security:**

This measure is dependent on the OS been used. The following are the basic techniques used by various operating systems.

- ❖ Linux: These work by ignoring unsolicited ARP reply packets.

- ❖ Microsoft Windows: The ARP cache behavior can be configured via the registry. The following list includes some of the software that can be used to protect networks against sniffing;

**AntiARP-** provides protection against both passive and active sniffing

**Agnitum Outpost Firewall-** provides protection against passive sniffing

**XArp-** provides protection against both passive and active sniffing

- ❖ Mac OS: ArpGuard can be used to provide protection. It protects against both active and passive sniffing.

### **Sniff Traffic:**

Network sniffing is the process of intercepting data packets sent over a network. This can be done by the specialized software program or hardware equipment. Sniffing can be used to;

- Capture sensitive data such as login credentials
- Eavesdrop on chat messages
- Capture files have been transmitted over a network.

### **Types of Sniffing:**

**Passive sniffing** is intercepting packages transmitted over a network that uses a hub. It is called passive sniffing because it is difficult to detect. It is also easy to perform as the hub sends broadcast messages to all the computers on the network.

**Active sniffing** is intercepting packages transmitted over a network that uses a switch. There are two main methods used to sniff switch linked networks, ARP Poisoning, and MAC flooding.



## Sniff Traffic using ARP Poisoning:

**Step 1:** Open the command prompt and Enter the command.

```
ipconfig /all
```

Detailed information about all the network connections available on your computer will be displayed. The results shown below are for a broadband modem to show the MAC address and IPv4 format and wireless network to show IPv6 format.

```
C:\Users\robst>ipconfig /all

Windows IP Configuration

Host Name . . . . . : DESKTOP-VHG8MCG
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . . :
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address. . . . . : 08-00-27-D5-F7-25
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2402:d000:811c:3acc:840c:fb0e:cdbc:fc8(Preferred)
Temporary IPv6 Address. . . . . : 2402:d000:811c:3acc:58e7:5077:5e19:dcec(Preferred)
Link-local IPv6 Address . . . . . : fe80::840c:fb0e:cdbc:fc8%5(Preferred)
IPv4 Address. . . . . : 192.168.1.240(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Tuesday, July 5      10:39:12 PM
Lease Expires . . . . . : Friday, July 8       10:39:13 PM
Default Gateway . . . . . : fe80::1%5
                          192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 101187623
DHCPv6 Client DUID. . . . . : 00-01-00-01-2A-57-88-1C-08-00-27-D5-F7-25
DNS Servers . . . . . : fe80::1%5
                          192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled
```

**Step 2:** **arp** command calls the ARP configure program located in Windows/System32 directory

**-a** is the parameter to display to contents of the ARP cache.

```
arp -a
```

```
C:\Users\DAEMON>arp -a

Interface: 192.168.1.38 --- 0xc
Internet Address      Physical Address      Type
192.168.1.1           00-23-f8-ce-fd-96    dynamic
192.168.1.33          64-27-37-1a-6a-05    dynamic
192.168.1.34          24-b6-fd-0f-49-e3    dynamic
192.168.1.255         ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.252           01-00-5e-00-00-fc    static
224.0.0.253           01-00-5e-00-00-fd    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static

C:\Users\DAEMON>
```

**Step 3:** Static entries are added manually and are deleted when the computer is restarted.

**Step 4:** After getting the IP/MAC address, enter the following command.

```
arp -s 192.168.1.38 60-36-DD-A6-C5-43
```

**Step 5:** To view the ARP cache

```
arp -a
```

```
C:\Users\DAEMON>arp -a
Interface: 192.168.1.38 --- 0xc
Internet Address      Physical Address      Type
192.168.1.1           00-23-f8-ce-fd-96    dynamic
192.168.1.33          64-27-37-1a-6a-05    dynamic
192.168.1.34          24-b6-fd-0f-49-e3    dynamic
192.168.1.36          64-27-37-1a-39-15    dynamic
192.168.1.37          24-b6-fd-0e-e2-e9    dynamic
192.168.1.38          60-36-dd-a6-c5-43    static
192.168.1.255         ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.252           01-00-5e-00-00-fc    static
224.0.0.253           01-00-5e-00-00-fd    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static
```

The IP address has been resolved to the MAC address we provided and it is of a static type.

**Step 6:** Command to remove an entry.

```
arp -d 192.168.1.38
```

```
C:\Users\DAEMON>arp -d 192.168.1.38
C:\Users\DAEMON>_
```

ARP poisoning works by sending fake MAC addresses to the switch.

## Result:

Thus, the Sniff Traffic using ARP Poisoning have been executed successfully.

**AIM:**

To install a rootkit hunter and find the malwares in a computer.

**ROOTKIT HUNTER:**

- rkhunter (Rootkit Hunter) is a Unix-based tool that scans for rootkits, backdoors and possible local exploits.
- It does this by comparing SHA-1 hashes of important files with known good ones in online databases, searching for default directories (of rootkits), wrong permissions, hidden files, suspicious strings in kernel modules, and special tests for Linux and FreeBSD.
- rkhunter is notable due to its inclusion in popular operating systems (Fedora, Debian, etc.)
- The tool has been written in Bourne shell, to allow for portability. It can run on almost all UNIX-derived systems.

**GMER ROOTKIT TOOL:**

- GMER is a software tool written by a Polish researcher Przemysław Gmerek, for detecting and removing rootkits.
- It runs on Microsoft Windows and has support for Windows NT, 2000, XP, Vista, 7, 8 and 10. With version 2.0.18327 full support for Windows x64 is added.

**Step 1**

**GMER** <http://www.gmer.net>  
all your rootkits are belong to us [\*]

Start  
Files  
News  
Rootkits  
FAQ  
Contact

**Start**

GMER is an application that detects and removes rootkits .

It scans for:

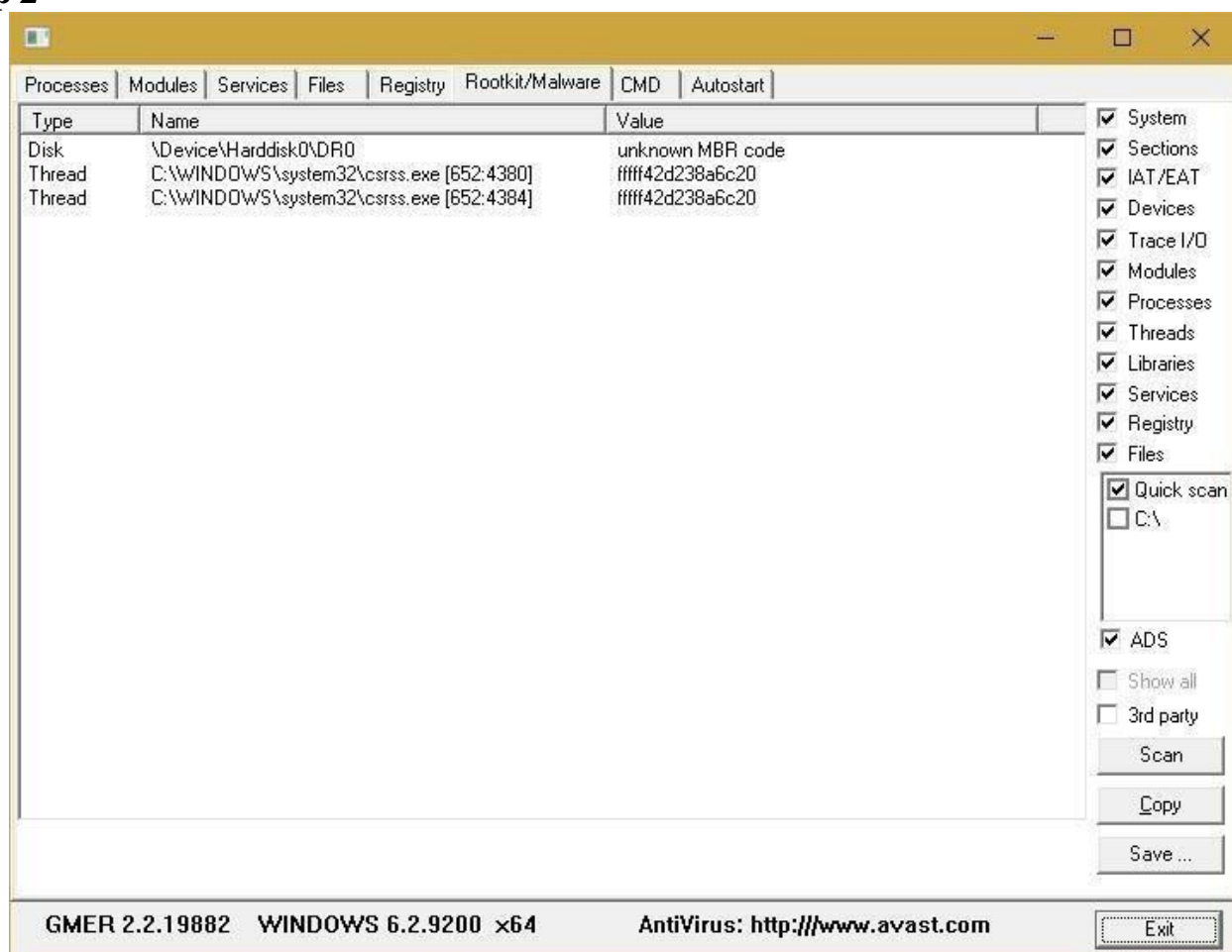
- hidden processes
- hidden threads
- hidden modules
- hidden services
- hidden files
- hidden disk sectors (MBR)
- hidden Alternate Data Streams
- hidden registry keys
- drivers hooking SSDT
- drivers hooking IDT
- drivers hooking IRP calls
- inline hooks

Type	Name	Value
IAT	C:\Windows\system32\ntoskrnl.exe[KDCCOM.dllKdD3Transition]	[#####80000b9b840] \SystemRoot\system32\kdcom.dll [text]
IAT	C:\Windows\system32\ntoskrnl.exe[KDCCOM.dllKdD0Transition]	[#####80000b9b834] \SystemRoot\system32\kdcom.dll [text]
IAT	C:\Windows\system32\ntoskrnl.exe[KDCCOM.dllKdReceivePacket]	[#####80000b9b820] \SystemRoot\system32\kdcom.dll [text]
IAT	C:\Windows\system32\ntoskrnl.exe[KDCCOM.dllKdSendPacket]	[#####80000b9b818] \SystemRoot\system32\kdcom.dll [text]
IAT	C:\Windows\system32\ntoskrnl.exe[KDCCOM.dllKdRestore]	[#####80000b9b80c] \SystemRoot\system32\kdcom.dll [text]
IAT	C:\Windows\system32\ntoskrnl.exe[KDCCOM.dllKdSave]	[#####80000b9b800] \SystemRoot\system32\kdcom.dll [text]
IAT	C:\Windows\system32\ntoskrnl.exe[KDCCOM.dllKdDebuggerInitialize0]	[#####80000b9b8e4] \SystemRoot\system32\kdcom.dll [text]
IAT	C:\Windows\system32\ntoskrnl.exe[KDCCOM.dllKdDebuggerInitialize1]	[#####80000b9b8f0] \SystemRoot\system32\kdcom.dll [text]
IAT	C:\Windows\system32\hal.dll[KdRestore]	[#####80000b9b80c] \SystemRoot\system32\kdcom.dll [text]
IAT	C:\Windows\system32\kdcom.dll[ntoskrnl.exeHalPrivateDis...	
IAT	C:\Windows\system32\kdcom.dll[ntoskrnl.exeHalAtol]	
IAT	C:\Windows\system32\kdcom.dll[ntoskrnl.exeKeFindConfig...	
IAT	C:\Windows\system32\kdcom.dll[ntoskrnl.exeMmMapIoSp...	
IAT	C:\Windows\system32\kdcom.dll[ntoskrnl.exe_strupr]	
IAT	C:\Windows\system32\kdcom.dll[ntoskrnl.exeInbvDisplayS...	
IAT	C:\Windows\system32\kdcom.dll[ntoskrnl.exeKdDebugger...	
IAT	C:\Windows\system32\kdcom.dll[ntoskrnl.exeKdStrt]	
IAT	C:\Windows\system32\kdcom.dll[ntoskrnl.exeKeBugCheck...	
IAT	C:\Windows\system32\kdcom.dll[HAL.dllHalQueryRealTime...	

**WARNING !!!**  
GMER has found system modification caused by ROOTKIT activity.

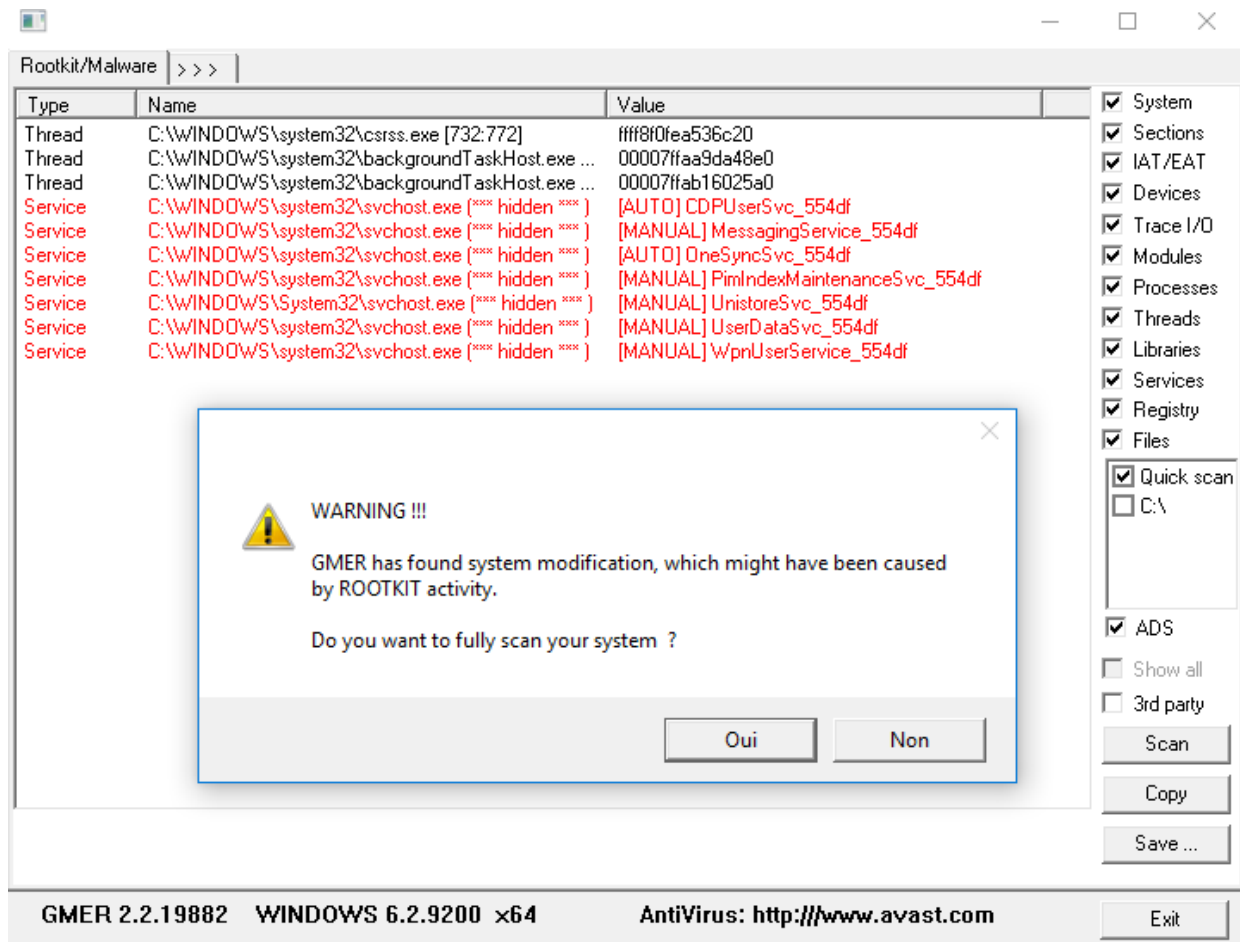
Visit GMER's website (see Resources) and download the GMER executable. Click the "Download EXE" button to download the program with a random file name, assume rootkits will close "gmer.exe" before you can open it.

## Step 2



Double-click the icon for the program.  
Click the "Scan" button in the lower-right corner of the dialog box. Allow the program to scan your entire hard drive.

### Step 3



When the program completes its scan, select any program or file listed in red. Right-click it and select "Delete." If the red item is a service, it may be protected. Right-click the service and select "Disable." Reboot your computer and run the scan again, this time selecting "Delete" when that service is detected. When your computer is free of Rootkits, close the program and restart your PC.

### RESULT:

A rootkit hunter software tool *gmer* has been installed and the rootkits have been detected.

