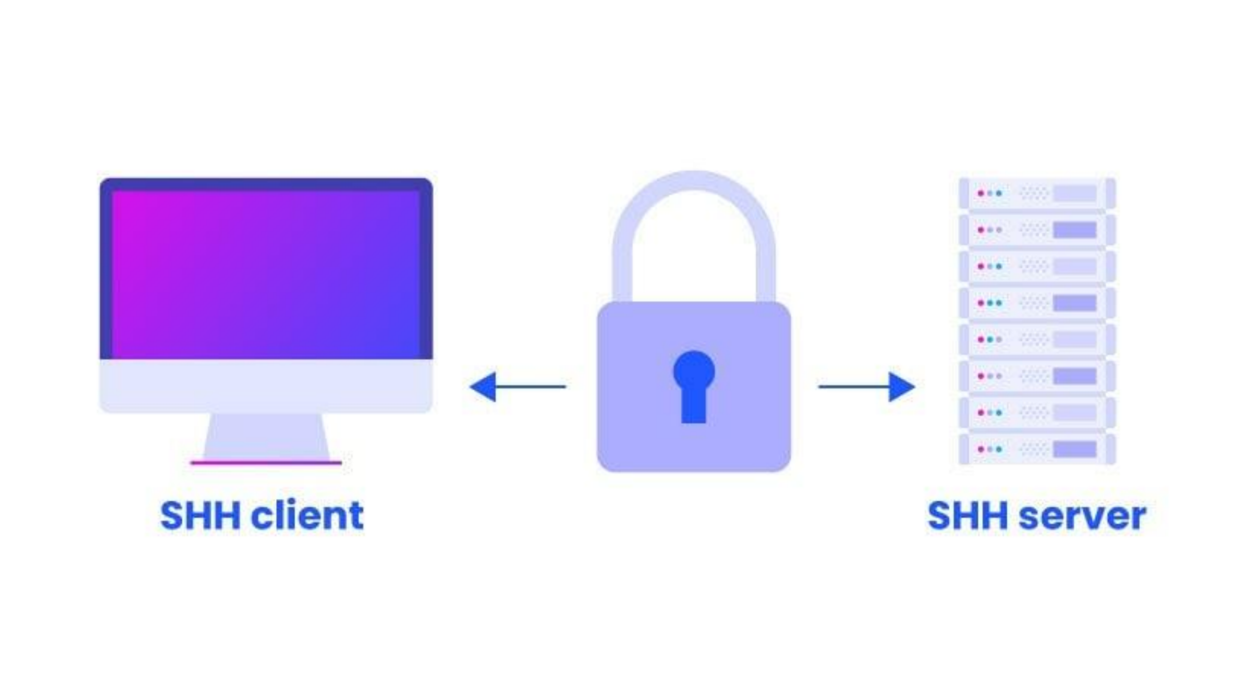
ASSIGNMENT NO 2

NAME: WAJID IQBAL

ASSIGNMENT: SSH, HTTP, HTTPS, SMB, SNMP, VPN

SUBMITTED BY: SIR MOIZUDDIN RAFFAY

SSH

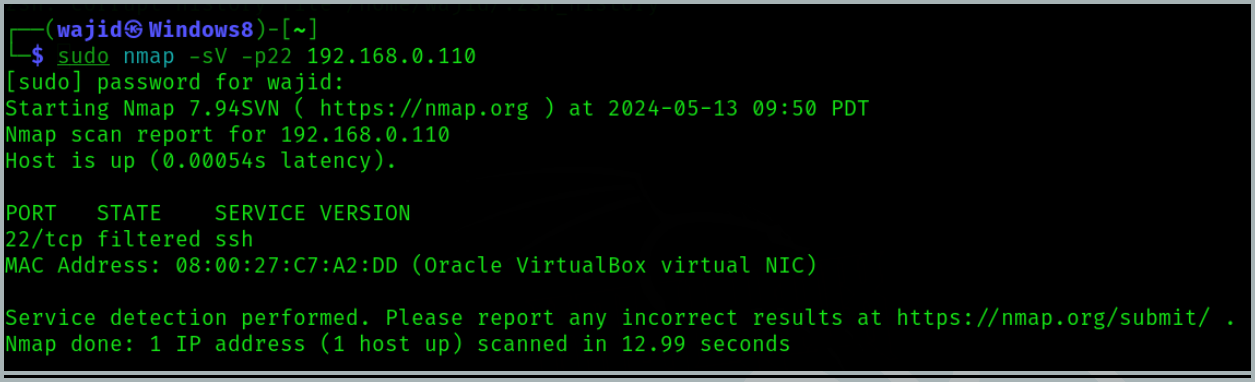


What is SSH?

SSH, or Secure Shell, is a cryptographic network protocol used for secure communication between two computers over an unsecured network. It provides a secure channel over an insecure network by encrypting the data that is exchanged between the two systems. SSH is commonly used for remote login and command execution, allowing users to securely access and manage remote systems. It's widely used in system administration, software development, and other fields where secure remote access is required. SSH operates on port 22 by default, but it can be configured to use different ports for added security.

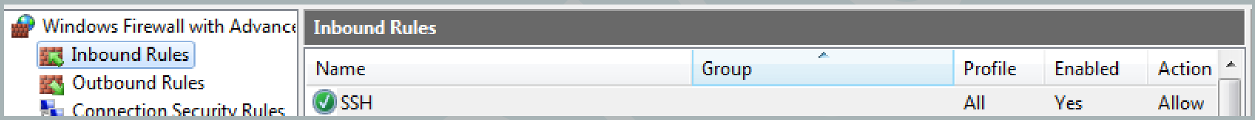
PRACTICAL WORK

FIRST WE WILL CHECK THROUGH TO NMAP SSH PORT OPEN OR CLOSE:

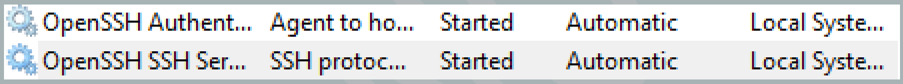


```
┌──(wajid㉿Windows8)-[~]
└─$ sudo nmap -sV -p22 192.168.0.110
[sudo] password for wajid:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-13 09:50 PDT
Nmap scan report for 192.168.0.110
Host is up (0.00054s latency).

PORT   STATE    SERVICE VERSION
22/tcp filtered ssh
MAC Address: 08:00:27:C7:A2:DD (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.99 seconds
```

IF SSH PORT IS NOT OPEN SO WE WILL CHECK FIREWALL AND SERVICES.

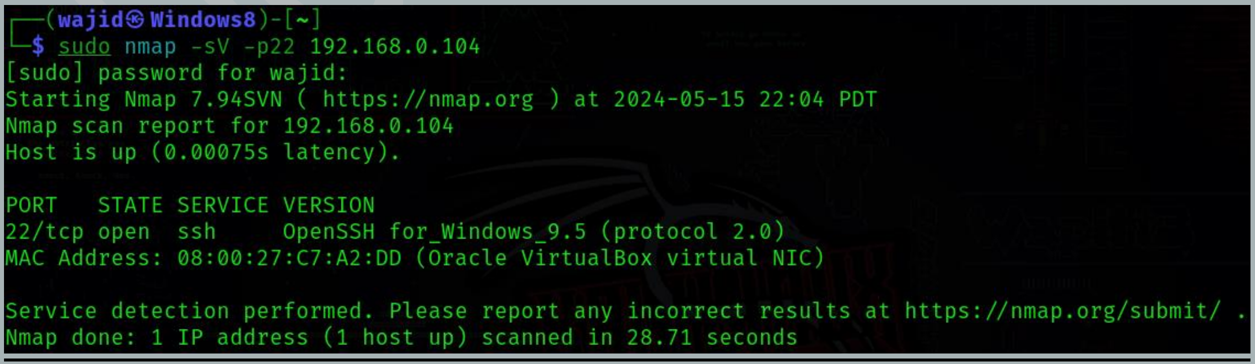


Name	Group	Profile	Enabled	Action
✓ SSH		All	Yes	Allow



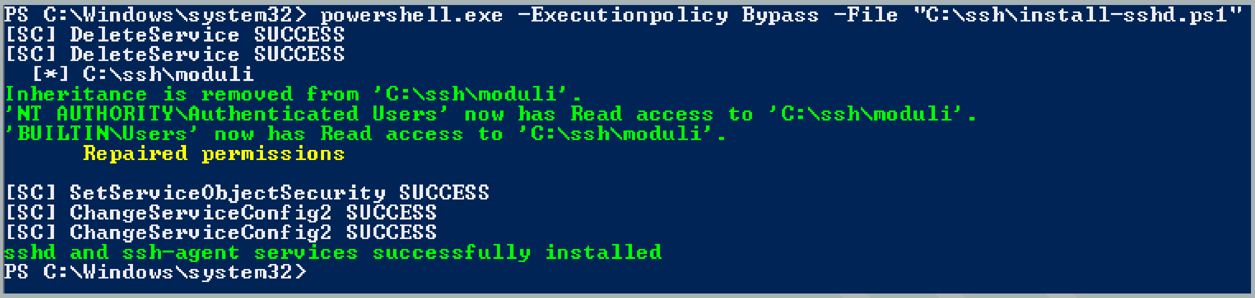
OpenSSH Authent...	Agent to ho...	Started	Automatic	Local Syste...
OpenSSH SSH Ser...	SSH protoc...	Started	Automatic	Local Syste...

CHECK SSH PORT THROUGH TO NMAP:



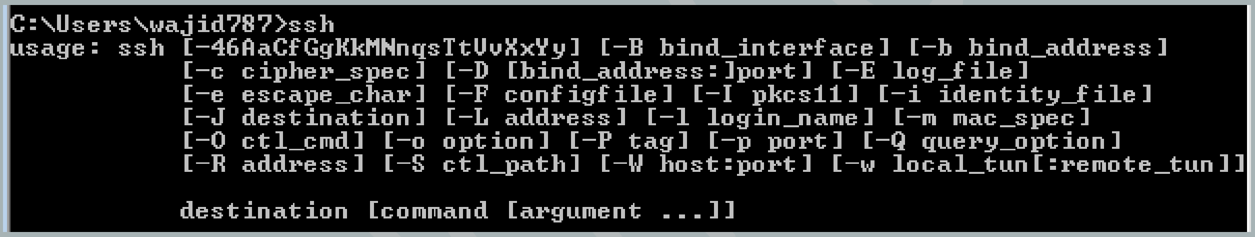
```
┌──(wajid㉿Windows8)-[~]
└─$ sudo nmap -sV -p22 192.168.0.104
[sudo] password for wajid:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-15 22:04 PDT
Nmap scan report for 192.168.0.104
Host is up (0.00075s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH for_Windows_9.5 (protocol 2.0)
MAC Address: 08:00:27:C7:A2:DD (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.71 seconds
```

AFTER WE WILL INSTALL SSHD AND SSH-AGENT SERVICES.

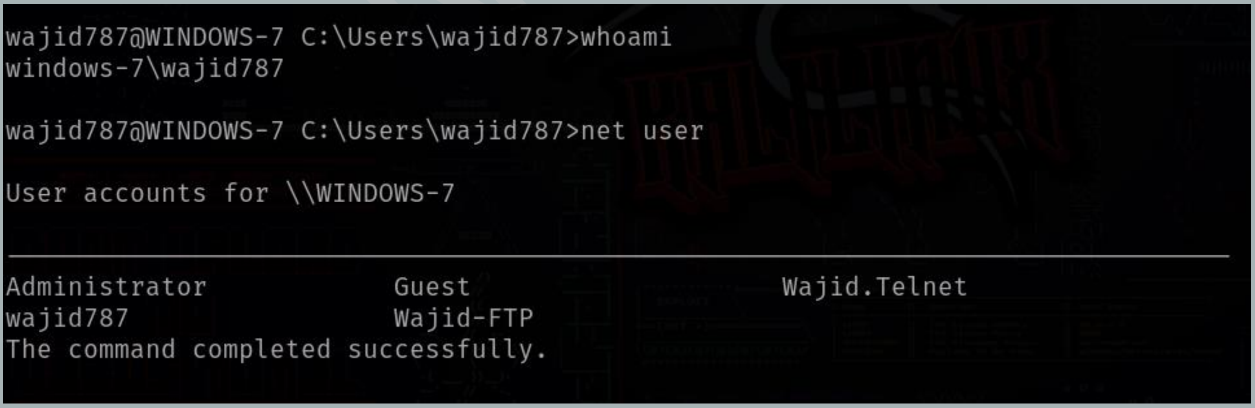


```
PS C:\Windows\system32> powershell.exe -Executionpolicy Bypass -File "C:\ssh\install-sshd.ps1"
[SC] DeleteService SUCCESS
[SC] DeleteService SUCCESS
  [*] C:\ssh\moduli
Inheritance is removed from 'C:\ssh\moduli'.
'NT AUTHORITY\Authenticated Users' now has Read access to 'C:\ssh\moduli'.
'BUILTIN\Users' now has Read access to 'C:\ssh\moduli'.
      Repaired permissions

[SC] SetServiceObjectSecurity SUCCESS
[SC] ChangeServiceConfig2 SUCCESS
[SC] ChangeServiceConfig2 SUCCESS
sshd and ssh-agent services successfully installed
PS C:\Windows\system32>
```

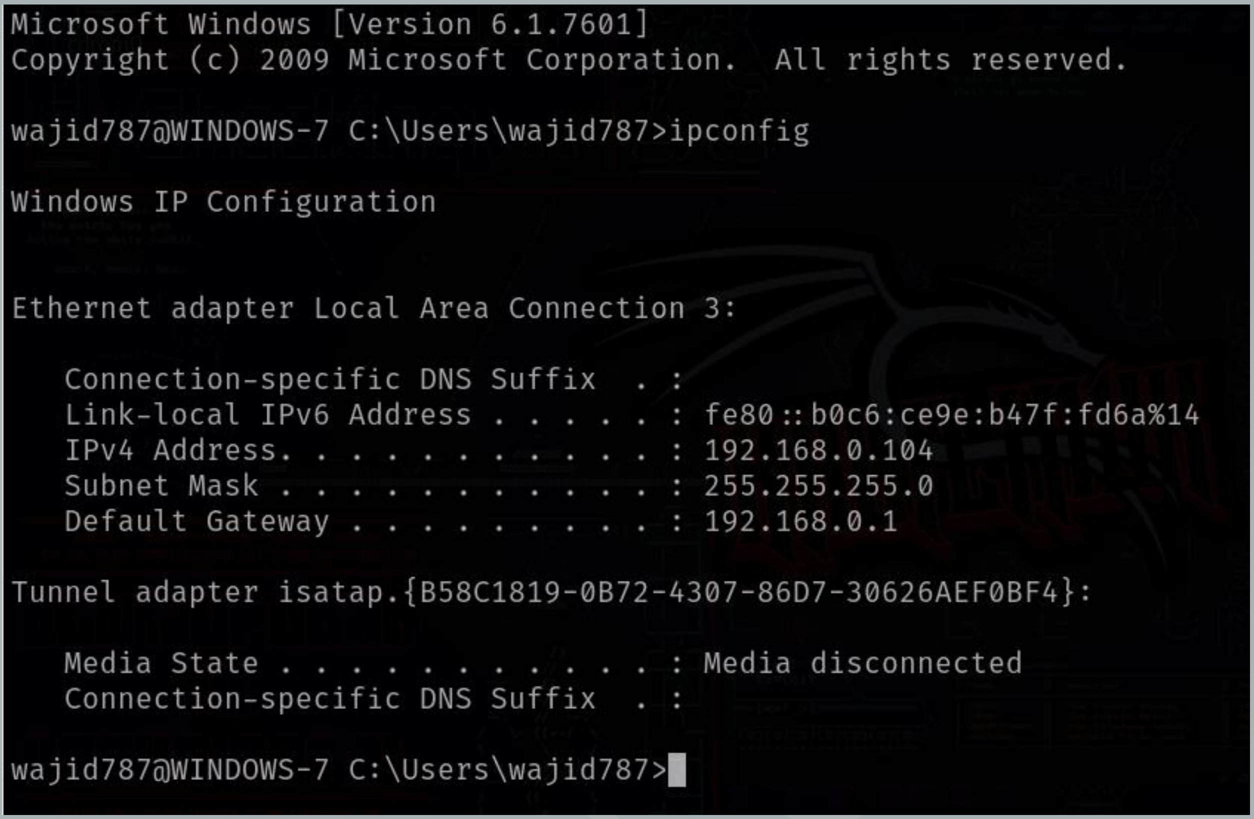
THEN WE WILL CHECK SSH IN CMD:



```
C:\Users\wajid787>ssh
usage: ssh [-46AaCfGgKkMNnqsTtVvXxYy] [-B bind_interface] [-b bind_address]
           [-c cipher_spec] [-D [bind_address:]port] [-E log_file]
           [-e escape_char] [-F configfile] [-I pkcs11] [-i identity_file]
           [-J destination] [-L address] [-l login_name] [-m mac_spec]
           [-O ctl_cmd] [-o option] [-P tag] [-p port] [-Q query_option]
           [-R address] [-S ctl_path] [-W host:port] [-w local_tun[:remote_tun]]

           destination [command [argument ...]]
```



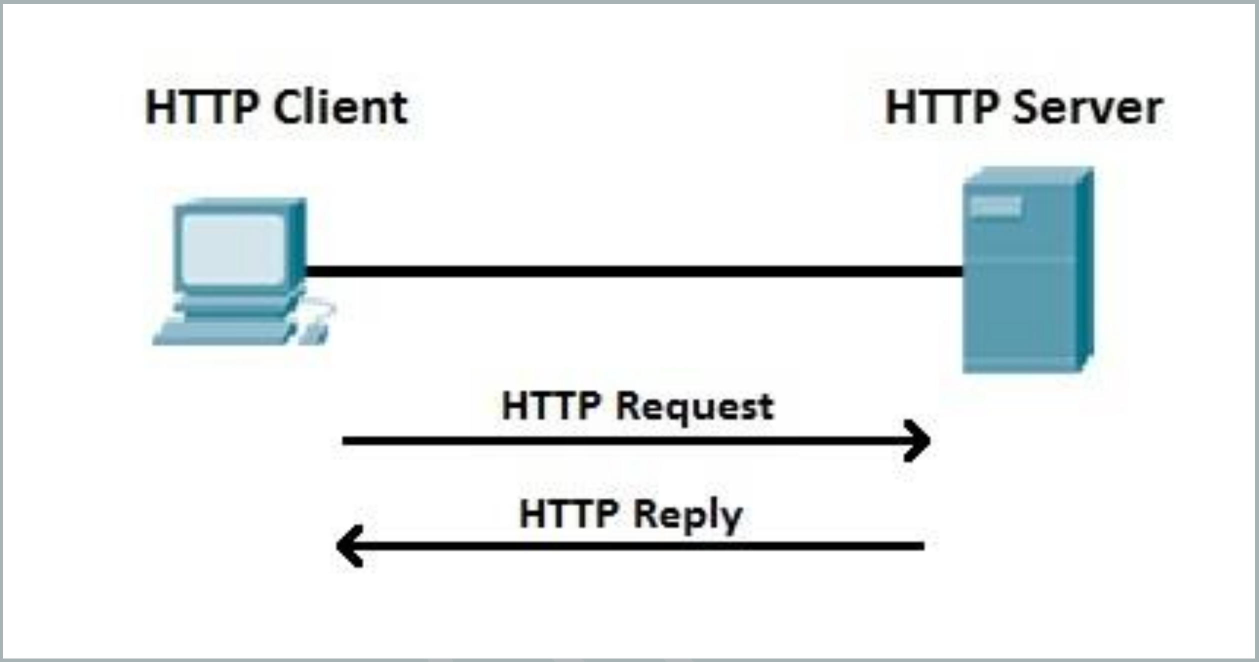
```
wajid787@WINDOWS-7 C:\Users\wajid787>whoami
windows-7\wajid787

wajid787@WINDOWS-7 C:\Users\wajid787>net user

User accounts for \\WINDOWS-7

-------------------------------------------------------------------------------
Administrator            Guest                    Wajid.Telnet
wajid787                 Wajid-FTP
The command completed successfully.
```



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

wajid787@WINDOWS-7 C:\Users\wajid787>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 3:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b0c6:ce9e:b47f:fd6a%14
   IPv4 Address. . . . . . . . . . . : 192.168.0.104
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Tunnel adapter isatap.{B58C1819-0B72-4307-86D7-30626AEF0BF4}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

wajid787@WINDOWS-7 C:\Users\wajid787>
```

NOW IT'S COMPLETED.

HTTP



What is HTTP?

HTTP, or Hypertext Transfer Protocol, is the foundational protocol used on the World Wide Web for transferring web pages and other resources from servers to clients (typically web browsers). It defines how messages are formatted and transmitted, and how web servers and browsers should respond to various commands.

Key points about HTTP:

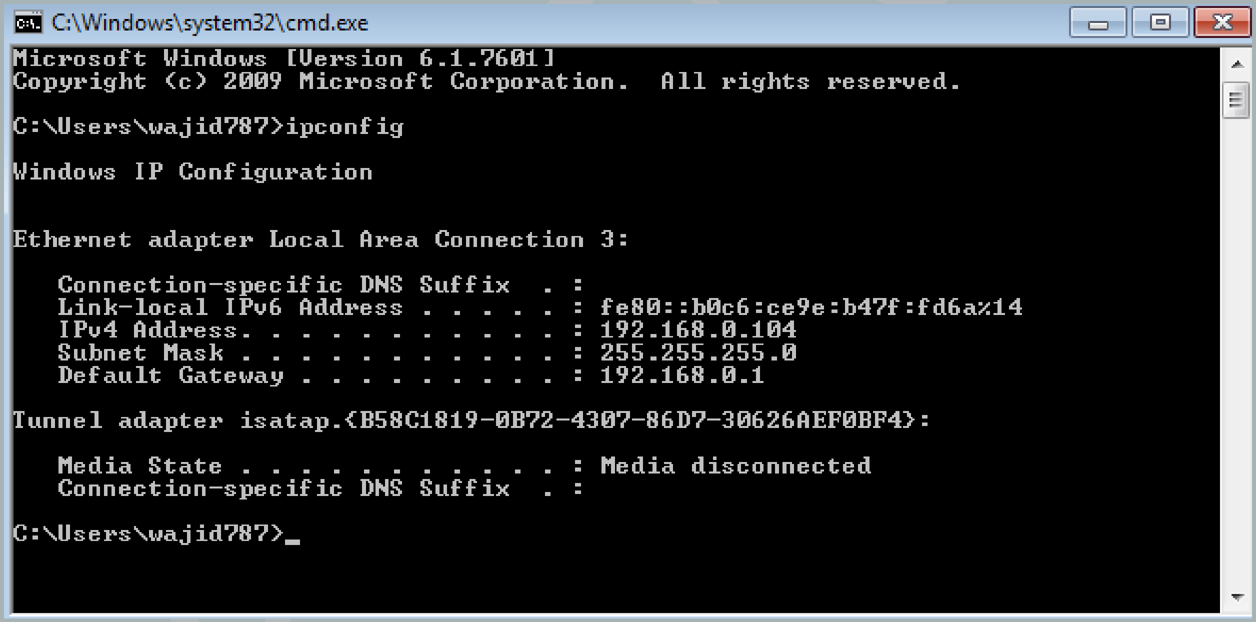
1. **Stateless Protocol**: Each request from a client to a server is independent; the server does not retain any state between requests.
2. **Methods**: HTTP uses methods (also known as verbs) to perform different actions. Common methods include:
   - **GET**: Requests a resource from the server.
   - **POST**: Submits data to the server (e.g., form data).
   - **PUT**: Updates a resource on the server.
   - **DELETE**: Deletes a resource on the server.
3. **URL**: Resources are identified and located using Uniform Resource Locators (URLs).

4. **Headers and Body**: HTTP messages consist of a header and an optional body. The header contains metadata about the request or response, and the body contains the actual data being transferred.
5. **HTTP/HTTPS**: HTTP operates over plain text, while HTTPS (HTTP Secure) encrypts the data using SSL/TLS to provide a secure communication channel.

HTTP is essential for the functioning of the web, enabling the retrieval and display of web pages and the interaction with web services.

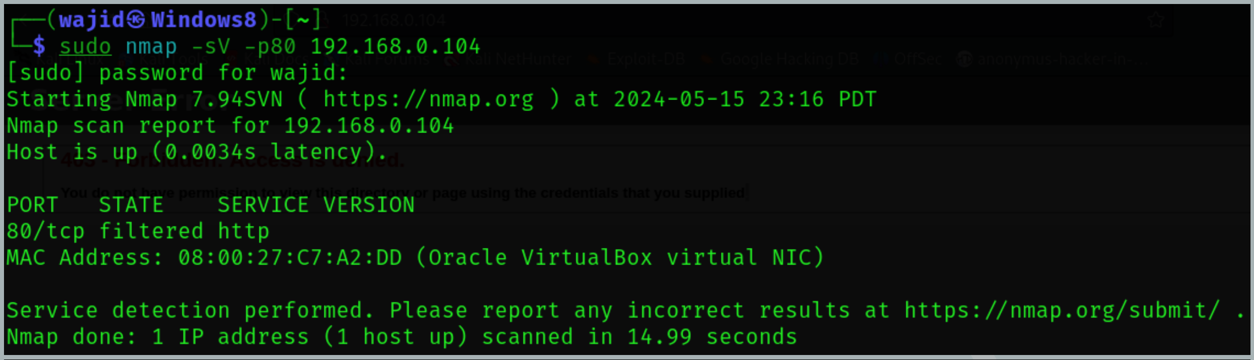
PRACTICAL WORK

FIRST WE WILL CHECK IP:



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\wajid787>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 3:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b0c6:ce9e:b47f:fd6a%14
   IPv4 Address. . . . . . . . . . . : 192.168.0.104
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Tunnel adapter isatap.{B58C1819-0B72-4307-86D7-30626AEF0BF4}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\wajid787>_
```

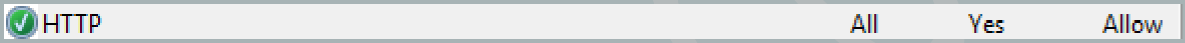
THEN WE WILL CHECK THROUGH TO NMAP, HTTP PORT IS OPEN OR NOT:



```
┌──(wajid㉿Windows8)-[~]
└─$ sudo nmap -sV -p80 192.168.0.104
[sudo] password for wajid:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-15 23:16 PDT
Nmap scan report for 192.168.0.104
Host is up (0.0034s latency).

PORT   STATE    SERVICE VERSION
80/tcp filtered http
MAC Address: 08:00:27:C7:A2:DD (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.99 seconds
```

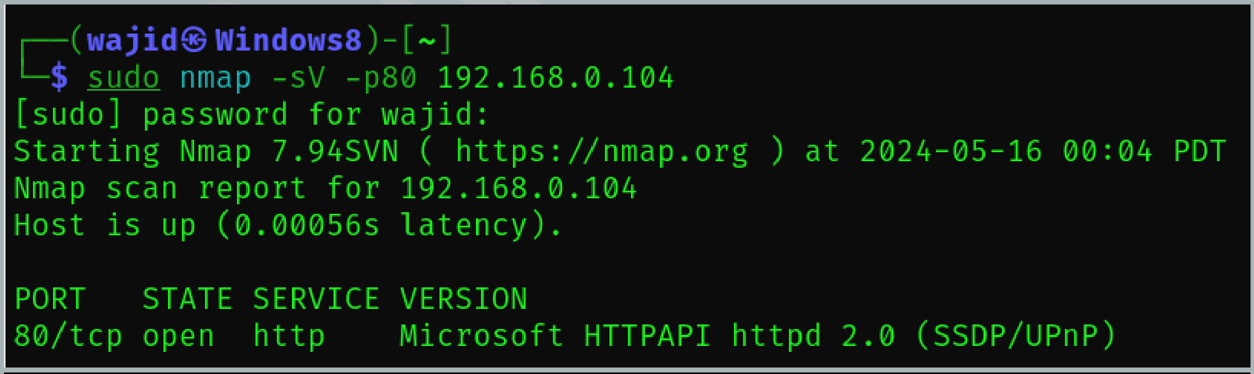
HTTP Port Is Filtered so,

WE WILL ALLOW HTTP PORT ON FIREWALL:



✓ HTTP All Yes Allow

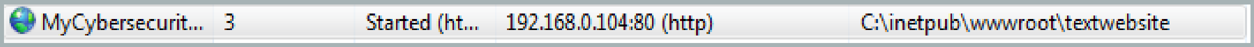
THEN WE WILL CHECK THROUGH TO NMAP, HTTP PORT IS OPEN OR NOT:



```
┌──(wajid㉿Windows8)-[~]
└─$ sudo nmap -sV -p80 192.168.0.104
[sudo] password for wajid:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-16 00:04 PDT
Nmap scan report for 192.168.0.104
Host is up (0.00056s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
```

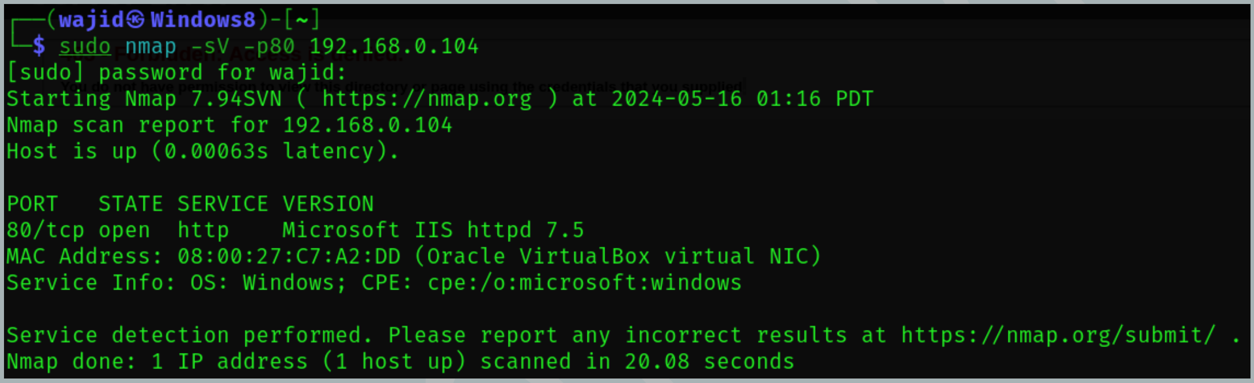
Now HTTP Port Is Up.

THEN WE WILL ADD WEBSITE IN INTERNET INFORMATION SERVICES MANAGER (IIS):



MyCybersecurit... 3 Started (ht... 192.168.0.104:80 (http) C:\inetpub\wwwroot\textwebsite

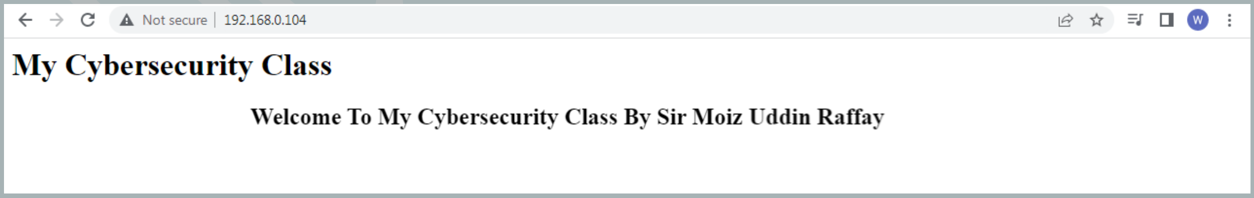
AFTER WE WILL CHECK THROUGH TO NMAP, HTTP PORT IS OPEN OR NOT:



```
┌──(wajid㉿Windows8)-[~]
└─$ sudo nmap -sV -p80 192.168.0.104
[sudo] password for wajid:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-16 01:16 PDT
Nmap scan report for 192.168.0.104
Host is up (0.00063s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 7.5
MAC Address: 08:00:27:C7:A2:DD (Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.08 seconds
```

Now HTTP Port Is Open.

THEN WE WILL CHECK HTTP WEBSITE ON BROWSER:

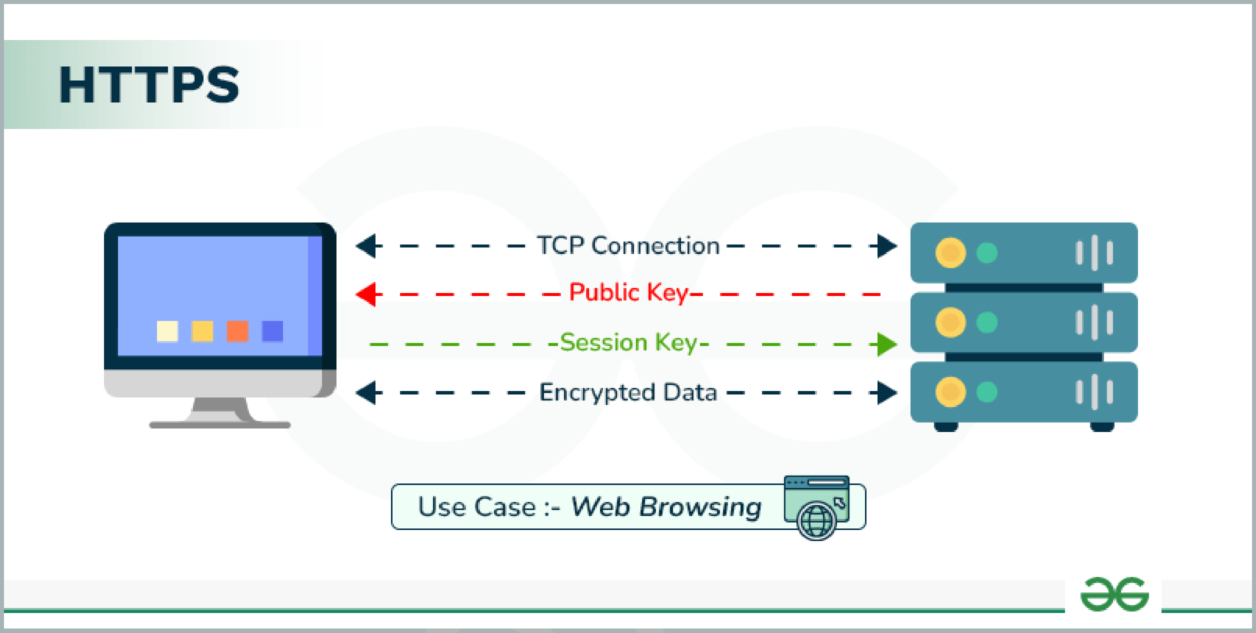


My Cybersecurity Class

Welcome To My Cybersecurity Class By Sir Moiz Uddin Raffay

NOW IT'S COMPLETED.

HTTPS



What is HTTPS?

HTTPS, or Hypertext Transfer Protocol Secure, is an extension of HTTP used for secure communication over a computer network. It combines HTTP with SSL/TLS (Secure Sockets Layer/Transport Layer Security) to provide encryption, authentication, and data integrity. This ensures that data transmitted between a client (such as a web browser) and a server is encrypted and secure from eavesdropping, tampering, and man-in-the-middle attacks.

Key features of HTTPS:

1. **Encryption**: HTTPS encrypts data transmitted between the client and server, protecting it from being intercepted or read by unauthorized parties.
2. **Authentication**: HTTPS uses SSL/TLS certificates to authenticate the server's identity, ensuring that the client is communicating with the intended server.
3. **Data Integrity**: HTTPS ensures that data is not altered during transmission, providing assurance that the data received is the same as the data sent.

Benefits of HTTPS:

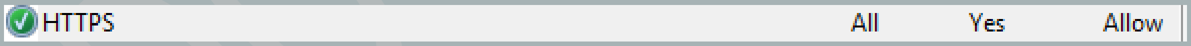
- **Security**: Encrypts sensitive data such as login credentials, payment information, and personal details.
- **Privacy**: Prevents eavesdropping on communication between the client and server.
- **Trust**: Browsers indicate a secure connection with a padlock icon, enhancing user trust.

To use HTTPS, a website must have an SSL/TLS certificate issued by a trusted certificate authority (CA). This certificate verifies the website's authenticity and establishes a secure connection.

In summary, HTTPS is essential for ensuring secure and private communication on the web, particularly for sensitive transactions and personal information.

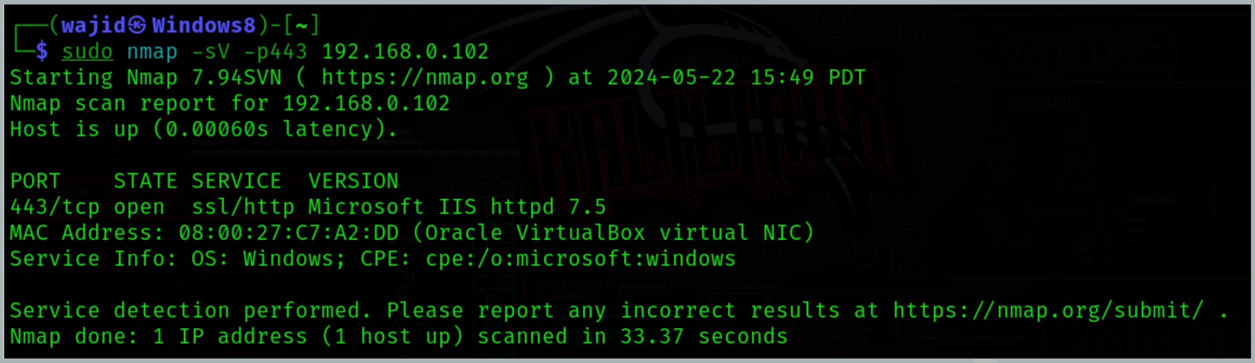
PRACTICAL WORK

FIRST WE WILL ALLOW HTTPS PORT ON FIREWALL:



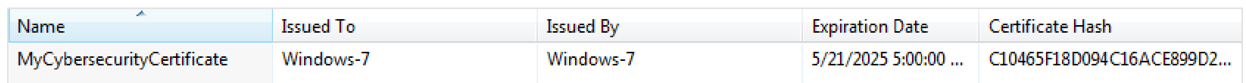
✓ HTTPS	All	Yes	Allow

THEN WE WILL CHECK THROUGH TO NMAP, HTTPS PORT IS OPEN OR NOT:



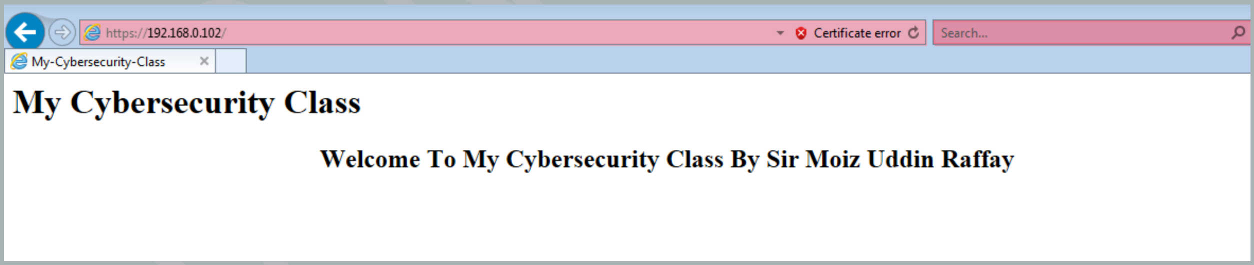
```
┌──(wajid㉿Windows8)-[~]
└─$ sudo nmap -sV -p443 192.168.0.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-22 15:49 PDT
Nmap scan report for 192.168.0.102
Host is up (0.00060s latency).

PORT    STATE SERVICE  VERSION
443/tcp open  ssl/http Microsoft IIS httpd 7.5
MAC Address: 08:00:27:C7:A2:DD (Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.37 seconds
```

THEN WE WILL CREATE HTTPS CERTIFICATE:



Name	Issued To	Issued By	Expiration Date	Certificate Hash
MyCybersecurityCertificate	Windows-7	Windows-7	5/21/2025 5:00:00 ...	C10465F18D094C16ACE899D2...

THEN WE WILL CHECK HTTPS WEBSITE ON BROWSER:

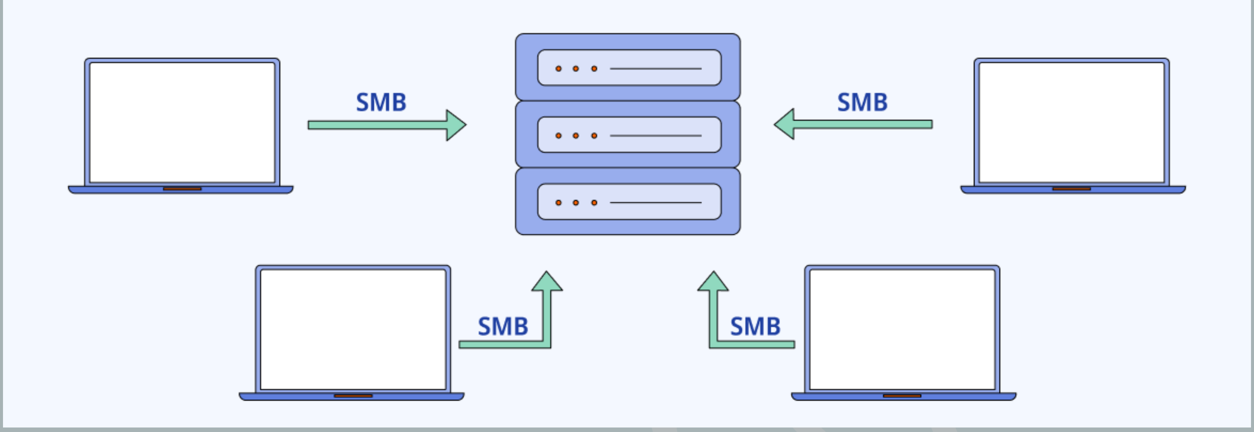


My Cybersecurity Class

Welcome To My Cybersecurity Class By Sir Moiz Uddin Raffay

NOW IT'S COMPLETED.

SMB



What is SMB?

SMB, or Server Message Block, is a network protocol used for providing shared access to files, printers, and serial ports between nodes on a network. It allows applications and users to read and write to files on a remote server and interact with server programs in a client-server model.

Key features of SMB:

1. **File Sharing**: SMB allows users to access and manage files on remote servers as if they were on their local machines. This includes opening, reading, writing, and managing files.
2. **Printer Sharing**: SMB enables networked printers to be shared and accessed by multiple users.
3. **Network Browsing**: SMB supports network discovery, allowing users to browse and locate shared resources within the network.
4. **Inter-process Communication**: SMB facilitates communication between different processes on a network, supporting various client-server interactions.

SMB has evolved over time, with several versions providing enhanced features and security:

- **SMB 1.0**: The original version, introduced in the 1980s, had basic file sharing capabilities.
- **SMB 2.0**: Introduced with Windows Vista, it improved performance, scalability, and security.

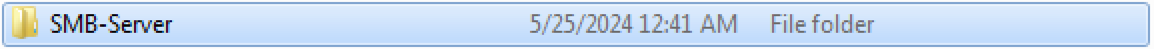
- **SMB 3.0**: Introduced with Windows 8 and Windows Server 2012, it added features like end-to-end encryption, improved performance, and support for modern data center features.

SMB is predominantly used in Windows environments, although other operating systems like Linux and macOS also support it. Samba, for example, is an open-source implementation of SMB/CIFS (Common Internet File System) used to provide SMB services on Unix-like systems.

In summary, SMB is a crucial protocol for networked file and printer sharing, allowing seamless access to resources across a network, and has been a fundamental component in both enterprise and home networks for many years.

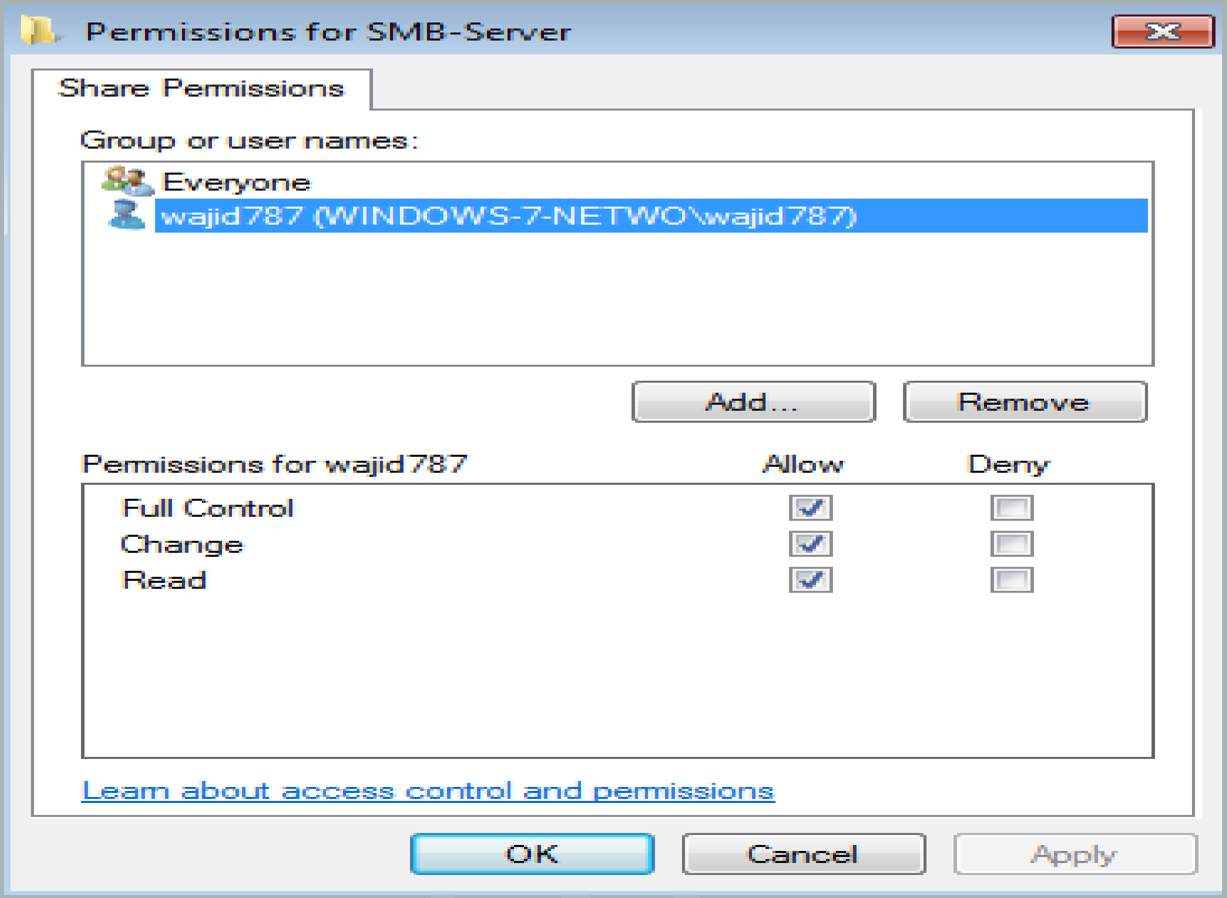
PRACTICAL WORK

FIRST WE WILL CREATE SMB FOLDER:



```
SMB-Server                5/25/2024 12:41 AM      File folder
```

AFTER CREATE FOLDER ALLOW PERMISSION FOR SMB-SERVER:

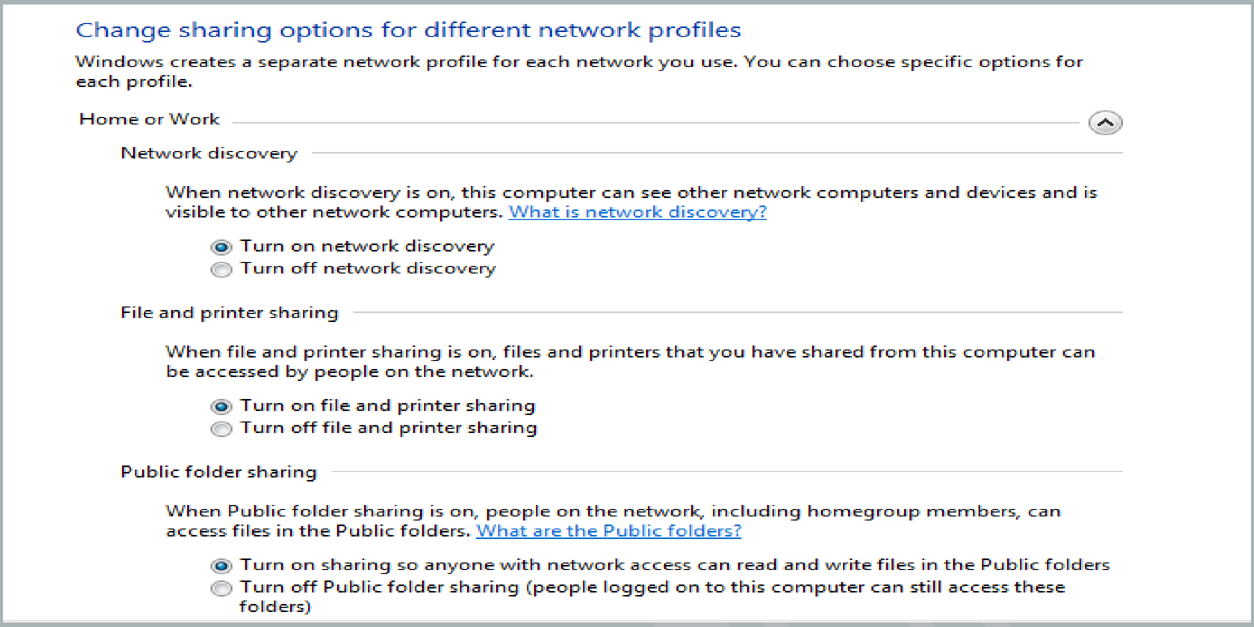

Permissions for SMB-Server
Share Permissions
Add...
Remove
Learn about access control and permissions
OK
Cancel
Apply

Group or user names:

- Everyone
- wajid787 (WINDOWS-7-NETWO\wajid787)

Permissions for wajid787	Allow	Deny
Full Control	☑	□
Change	☑	□
Read	☑	□

THEN WE WILL TURN ON PRIVATE NETWORK PERMISSION FOR SMB:



Change sharing options for different network profiles

Windows creates a separate network profile for each network you use. You can choose specific options for each profile.

Home or Work

Network discovery

When network discovery is on, this computer can see other network computers and devices and is visible to other network computers. What is network discovery?

● Turn on network discovery
○ Turn off network discovery

File and printer sharing

When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network.

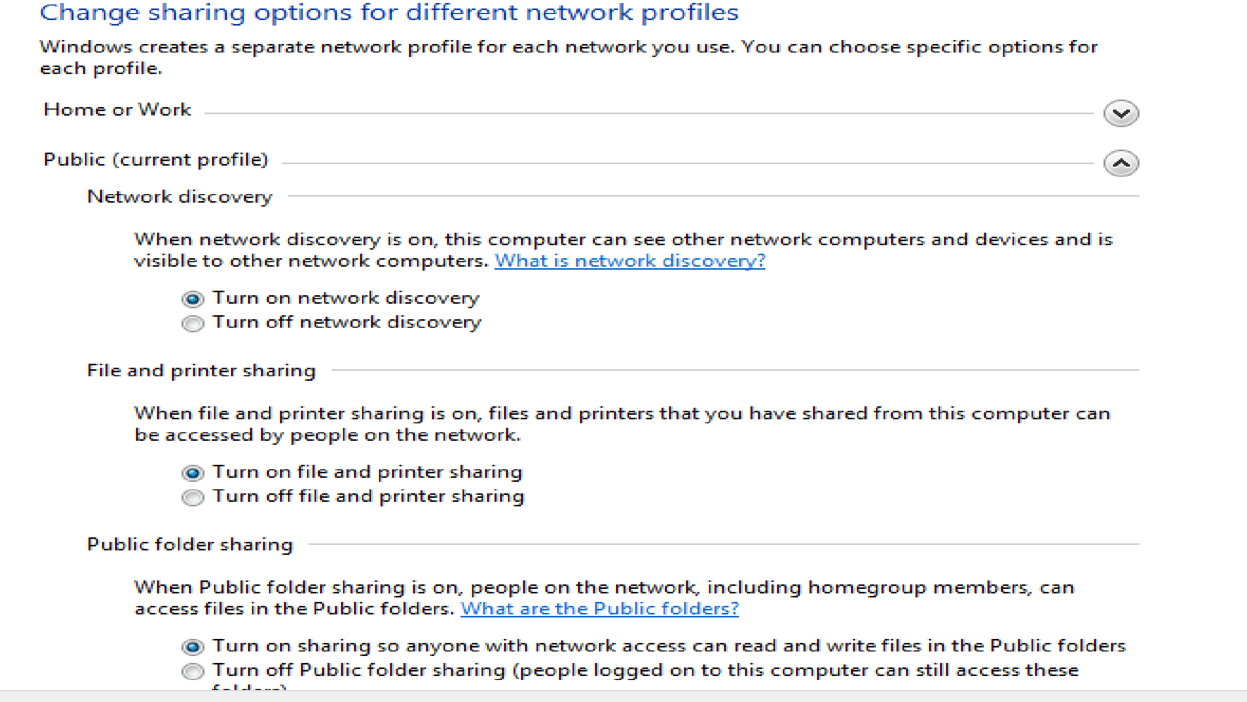
● Turn on file and printer sharing
○ Turn off file and printer sharing

Public folder sharing

When Public folder sharing is on, people on the network, including homegroup members, can access files in the Public folders. What are the Public folders?

● Turn on sharing so anyone with network access can read and write files in the Public folders
○ Turn off Public folder sharing (people logged on to this computer can still access these folders)

AFTER WE WILL TURN ON PUBLIC NETWORK PERMISSION FOR SMB:



Change sharing options for different network profiles

Windows creates a separate network profile for each network you use. You can choose specific options for each profile.

Home or Work

Public (current profile)

Network discovery

When network discovery is on, this computer can see other network computers and devices and is visible to other network computers. What is network discovery?

● Turn on network discovery
○ Turn off network discovery

File and printer sharing

When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network.

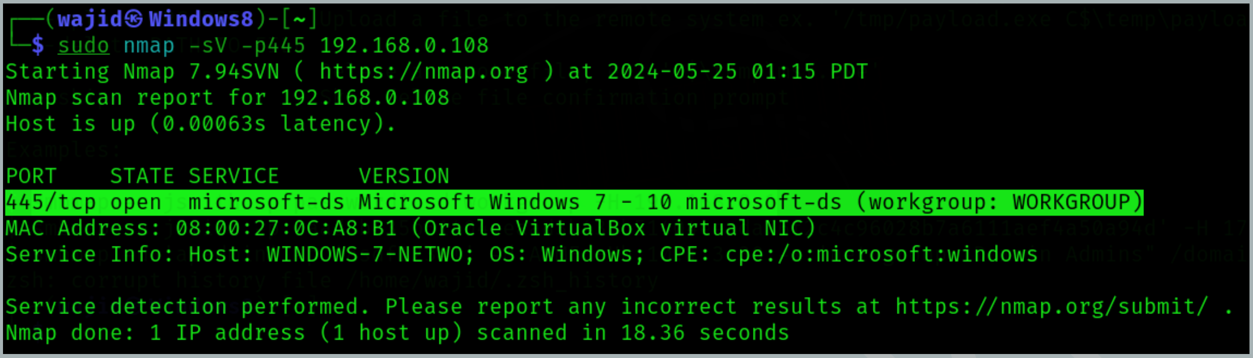
● Turn on file and printer sharing
○ Turn off file and printer sharing

Public folder sharing

When Public folder sharing is on, people on the network, including homegroup members, can access files in the Public folders. What are the Public folders?

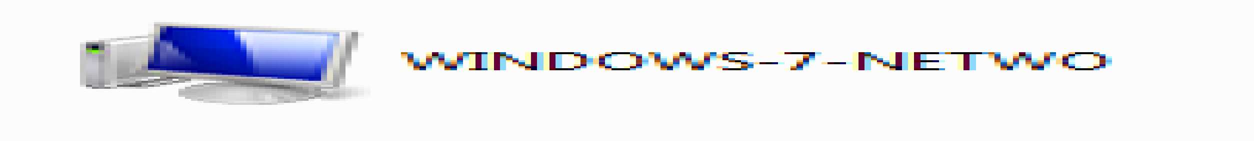
● Turn on sharing so anyone with network access can read and write files in the Public folders
○ Turn off Public folder sharing (people logged on to this computer can still access these folders)

THEN WE WILL CHECK THROUGH TO NMAP, SMB PORT IS OPEN OR NOT:



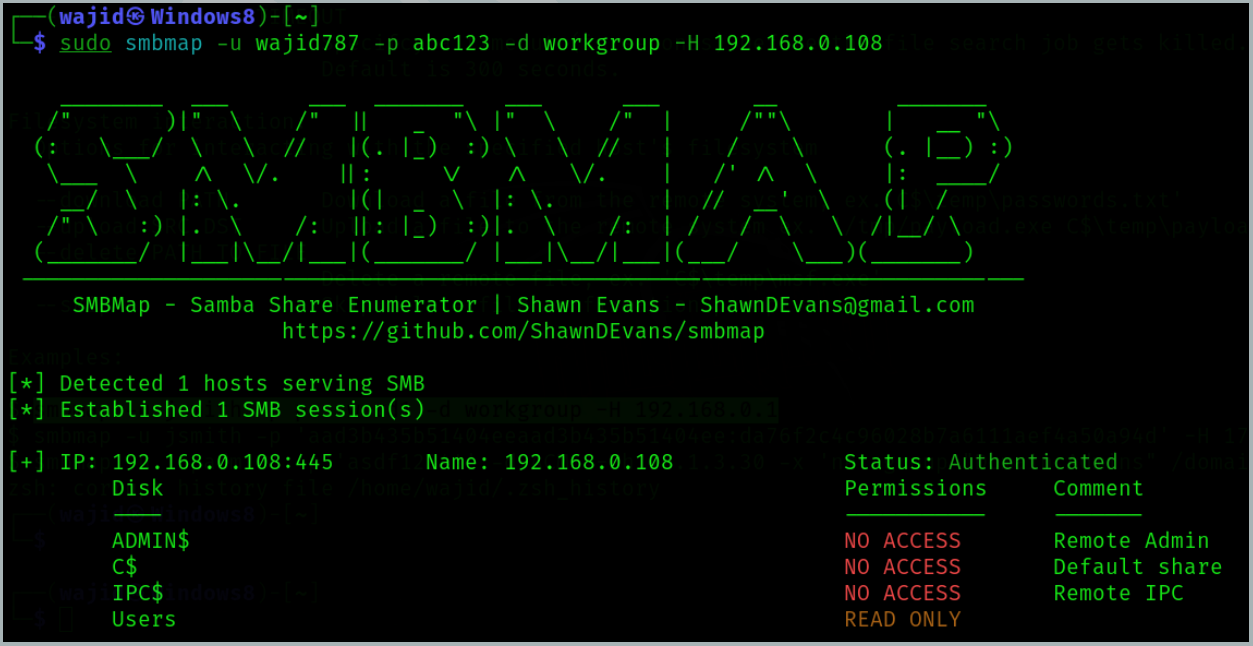
```
┌──(wajid㉿Windows8)-[~]
└─$ sudo nmap -sV -p445 192.168.0.108
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-25 01:15 PDT
Nmap scan report for 192.168.0.108
Host is up (0.00063s latency).

PORT    STATE SERVICE      VERSION
445/tcp open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
MAC Address: 08:00:27:0C:A8:B1 (Oracle VirtualBox virtual NIC)
Service Info: Host: WINDOWS-7-NETWO; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.36 seconds
```

SMB WINDOWS 7 OPTION:



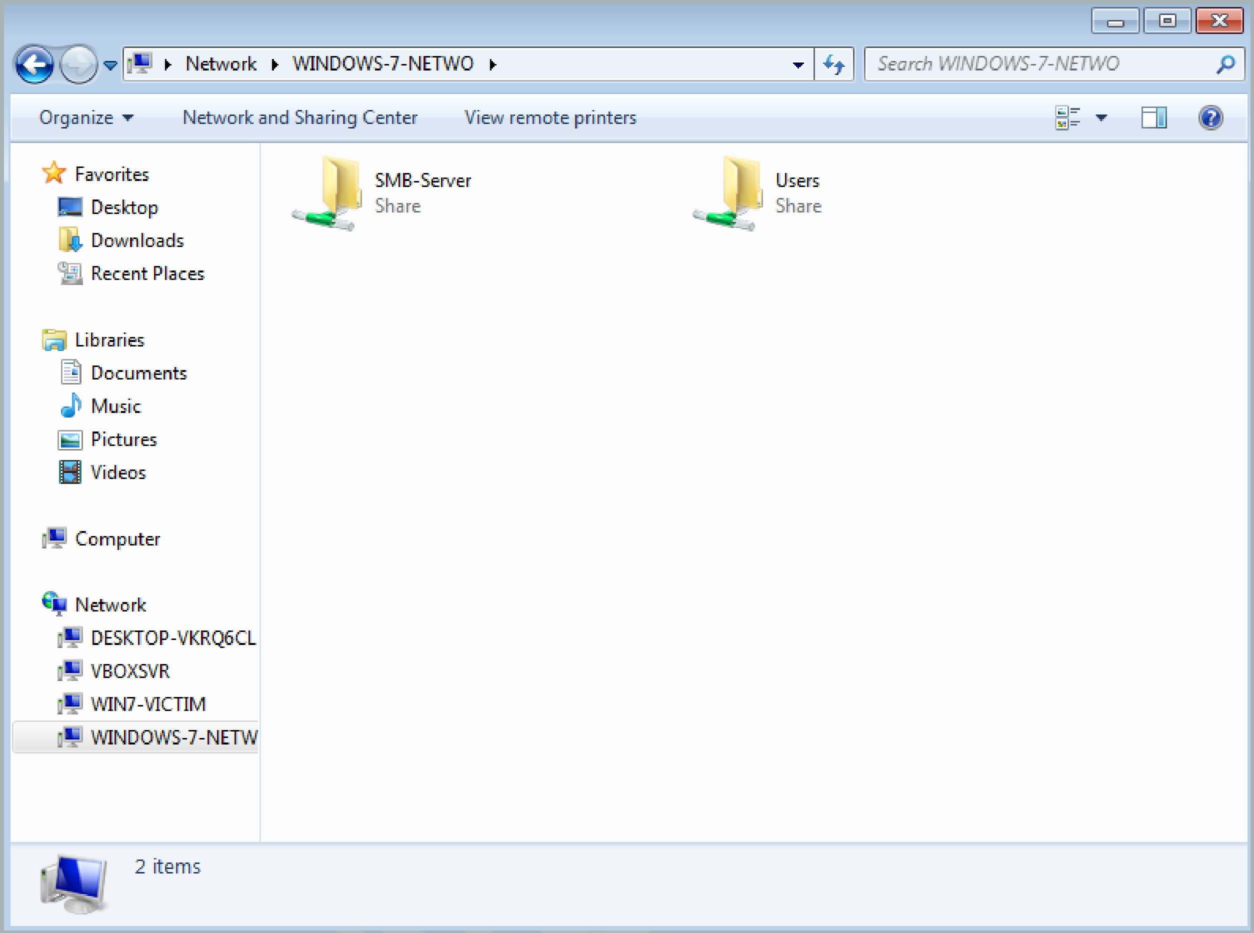
WINDOWS-7-NETWO

AFTER WE WILL CHECK SMB SERVER DETECTION:



```
┌──(wajid㉿Windows8)-[~]
└─$ sudo smbmap -u wajid787 -p abc123 -d workgroup -H 192.168.0.108

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
 -----------------------------------------------------------------------------
     SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB session(s)

[+] IP: 192.168.0.108:445       Name: 192.168.0.108             Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    NO ACCESS       Remote IPC
        Users                                                   READ ONLY
```

SMB WINDOWS 7 FOLDER ACCESS:



NOW IT'S COMPLETED.

SNMP

SNMP, or Simple Network Management Protocol, is an Internet Standard protocol used for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior. It is widely used in network management for monitoring network-attached devices such as routers, switches, servers, printers, and other devices that support SNMP.

Key components of SNMP:

1. **Managed Devices**: These are network nodes containing an SNMP agent and reside on a managed network. These devices can include routers, switches, servers, workstations, printers, and more.
2. **SNMP Agents**: Software modules that reside on the managed devices. An agent has local knowledge of management information and translates that information into a form compatible with SNMP.
3. **Network Management Systems (NMS)**: These are applications that monitor and control managed devices. They provide the bulk of the processing and memory resources required for network management.
4. **Management Information Base (MIB)**: A virtual database used for managing the entities in a computer network. It comprises a collection of information organized hierarchically. MIBs are accessed using SNMP.

Key operations in SNMP:

- **GET**: Retrieves one or more values from the managed devices.
- **SET**: Modifies or sets the value of one or more parameters on the managed devices.
- **GETNEXT**: Retrieves the value of the next OID in the MIB tree.
- **GETBULK**: Efficiently retrieves large blocks of data, particularly in large tables.
- **TRAP**: Asynchronous notifications from agents to the NMS indicating events or issues.
- **INFORM**: Similar to TRAP, but includes an acknowledgment from the NMS back to the agent.

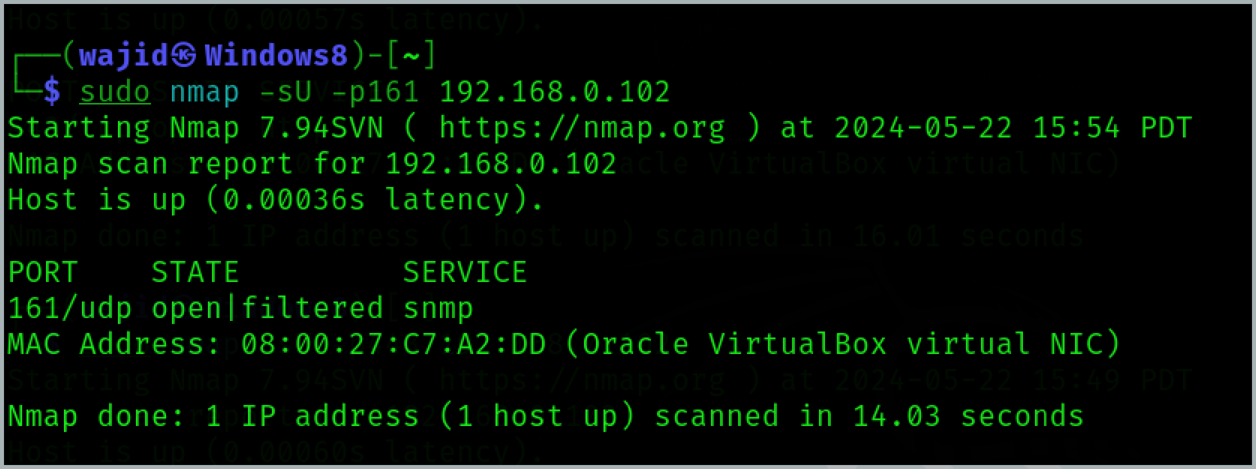
Versions of SNMP:

- **SNMPv1**: The original version with basic features and security.
- **SNMPv2**: Enhanced performance and additional protocol operations, but still with limited security.
- **SNMPv3**: Improved security, including authentication and encryption, making it the preferred version for modern networks.

SNMP is crucial for network administrators as it provides the tools needed to monitor the health and performance of the network, troubleshoot issues, and ensure the smooth operation of networked devices.

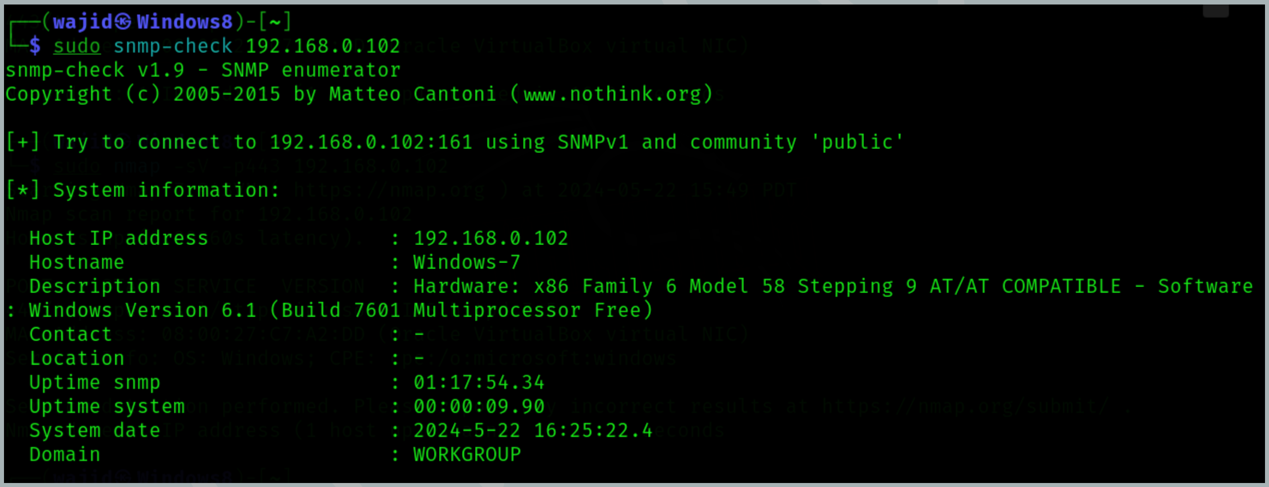
PRACTICAL WORK

FIRST WE WILL CHECK THROUGH TO NMAP, SNMP PORT IS OPEN OR NOT:



```
┌──(wajid㉿Windows8)-[~]
└─$ sudo nmap -sU -p161 192.168.0.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-22 15:54 PDT
Nmap scan report for 192.168.0.102
Host is up (0.00036s latency).

PORT    STATE         SERVICE
161/udp open|filtered snmp
MAC Address: 08:00:27:C7:A2:DD (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.03 seconds
```

GET SYSTEM DETAILS THROUGH TO SNMP:



```
┌──(wajid㉿Windows8)-[~]
└─$ sudo snmp-check 192.168.0.102
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

[+] Try to connect to 192.168.0.102:161 using SNMPv1 and community 'public'

[*] System information:

  Host IP address               : 192.168.0.102
  Hostname                      : Windows-7
  Description                   : Hardware: x86 Family 6 Model 58 Stepping 9 AT/AT COMPATIBLE - Software
: Windows Version 6.1 (Build 7601 Multiprocessor Free)
  Contact                       : -
  Location                      : -
  Uptime snmp                   : 01:17:54.34
  Uptime system                 : 00:00:09.90
  System date                   : 2024-5-22 16:25:22.4
  Domain                        : WORKGROUP
```

NOW IT'S COMPLETED.

VPN

A VPN, or Virtual Private Network, is a technology that creates a secure and encrypted connection over a less secure network, such as the internet. It allows users to send and receive data as if their devices were directly connected to a private network, thereby benefiting from the functionality, security, and management policies of the private network.

Key Features and Benefits of VPN:

1. **Security**: VPNs encrypt data transmitted between your device and the VPN server, protecting it from interception and unauthorized access.
2. **Privacy**: By masking your IP address and routing your internet traffic through the VPN server, VPNs help maintain your online privacy and anonymity.
3. **Remote Access**: VPNs allow remote workers to securely connect to their organization's internal network, accessing resources such as files, applications, and printers as if they were on-site.
4. **Bypassing Geo-Restrictions**: VPNs can allow users to access content that is restricted based on geographic location by making it appear as if they are accessing the internet from a different location.

5. **Enhanced Anonymity**: By hiding your real IP address and mixing your traffic with other users on the VPN server, VPNs make it harder for websites and services to track your online activities.

How VPN Works:

1. **Client and Server**: A VPN client installed on the user's device connects to a VPN server located in a different location.
2. **Tunneling Protocols**: VPNs use tunneling protocols to create a secure connection. Common protocols include OpenVPN, L2TP/IPsec, PPTP, and IKEv2/IPsec.
3. **Encryption**: Data sent through the VPN tunnel is encrypted, ensuring that even if it is intercepted, it cannot be read by unauthorized parties.
4. **IP Address Masking**: The user's real IP address is hidden, and they are assigned an IP address from the VPN server's location, which helps in maintaining privacy and accessing region-locked content.

Types of VPN:

1. **Remote Access VPN**: Commonly used by individual users to connect to a private network from a remote location. Examples include employees accessing a corporate network from home.
2. **Site-to-Site VPN**: Used to connect entire networks to each other, often used in businesses to connect different office locations securely over the internet.
3. **Personal VPN**: Used by individuals primarily for privacy, security, and bypassing geo-restrictions.

VPN Providers and Services:

There are numerous VPN providers available, offering various features and levels of service. Some popular VPN services include:

- **ExpressVPN**
- **NordVPN**
- **CyberGhost**
- **Surfshark**
- **Private Internet Access (PIA)**

Using a VPN:

To use a VPN, you generally need to:

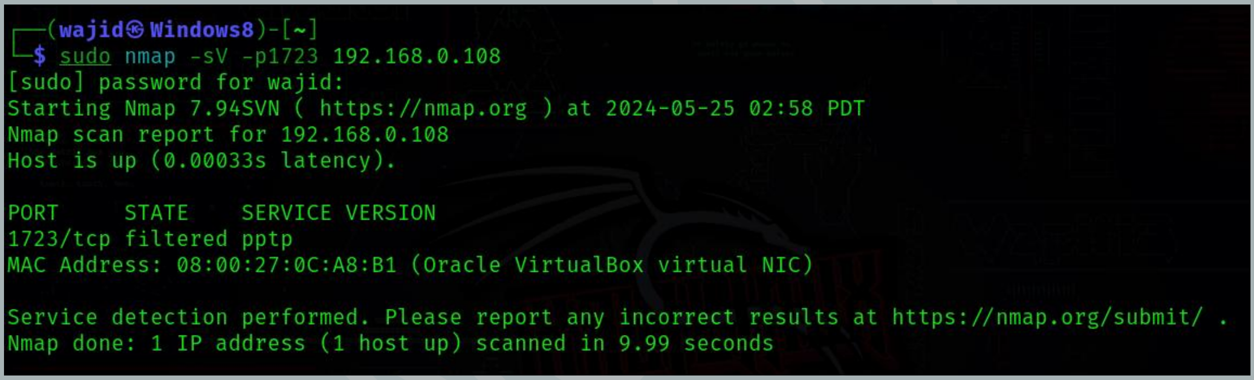
1. **Choose a VPN Provider**: Select a reputable VPN service based on your needs (privacy, security, speed, etc.).
2. **Install the VPN Client**: Download and install the VPN software or app on your device.
3. **Connect to a Server**: Open the VPN client, log in, and connect to a server of your choice.

4. **Browse Securely**: Once connected, your internet traffic will be encrypted and routed through the VPN server.

In summary, a VPN is a powerful tool for enhancing online security, privacy, and accessibility, making it a valuable resource for both individual users and organizations.

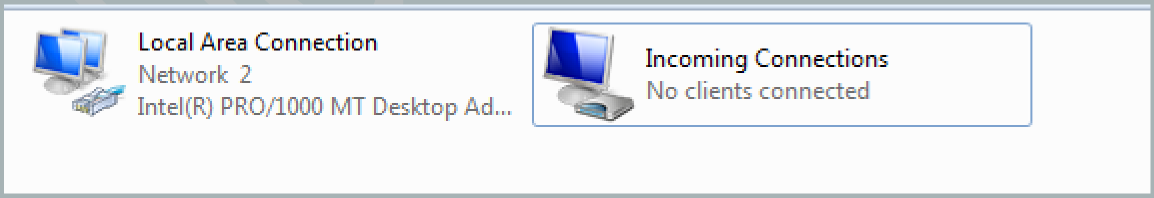
PRACTICAL WORK

FIRST WE CHECK THROUGH TO NMAP, VPN PORT:



```
┌──(wajid㉿Windows8)-[~]
└─$ sudo nmap -sV -p1723 192.168.0.108
[sudo] password for wajid:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-25 02:58 PDT
Nmap scan report for 192.168.0.108
Host is up (0.00033s latency).

PORT     STATE    SERVICE VERSION
1723/tcp filtered pptp
MAC Address: 08:00:27:0C:A8:B1 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.99 seconds
```

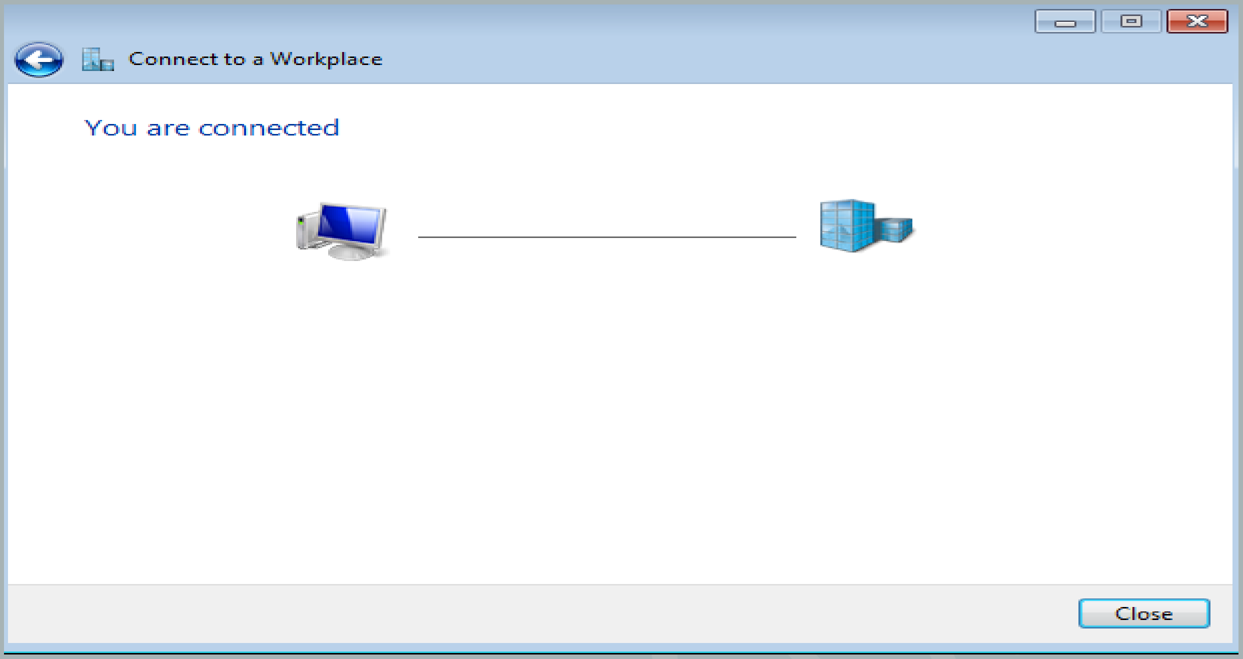
AFTER WE WILL MAKE VPN, VPN IS DISCONNECTED NOW:



Local Area Connection
Network 2
Intel(R) PRO/1000 MT Desktop Ad...

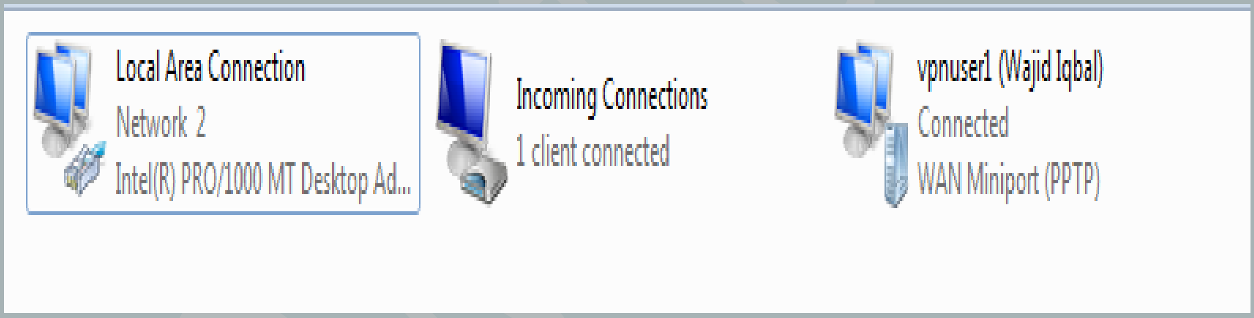
Incoming Connections
No clients connected

THEN WE WILL CONNECT VPN:



Connect to a Workplace

You are connected

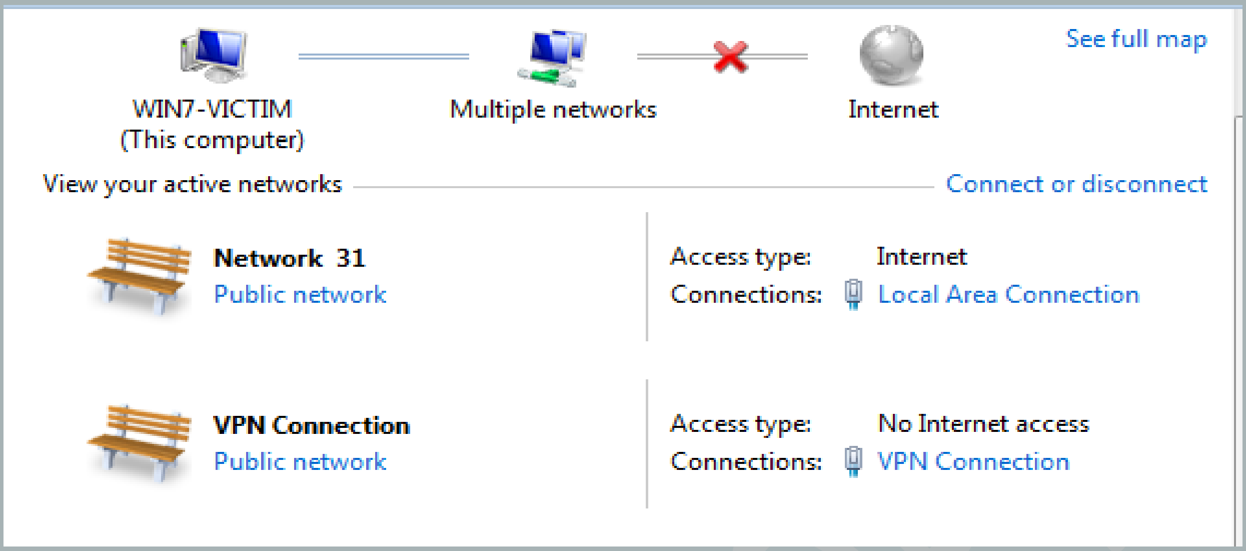


Local Area Connection
Network 2
Intel(R) PRO/1000 MT Desktop Ad...

Incoming Connections
1 client connected

vpnuser1 (Wajid Iqbal)
Connected
WAN Miniport (PPTP)

VPN IS CONNECTED TO INTERNET:



View your active networks — Connect or disconnect

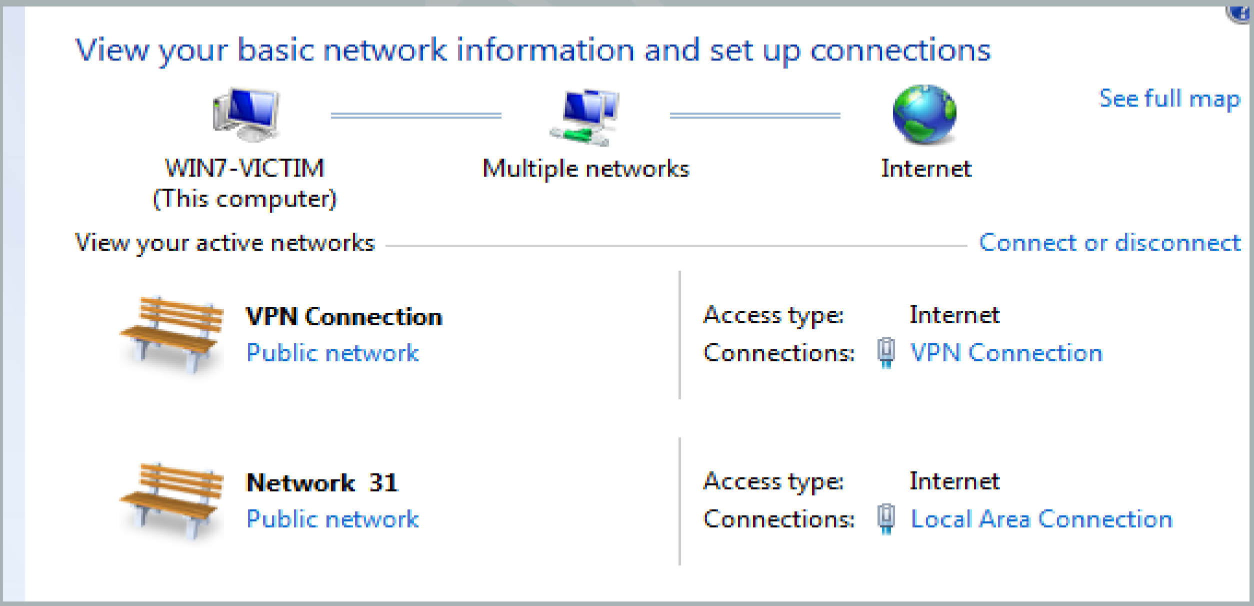
Network 31
Public network

Access type: Internet
Connections: Local Area Connection

VPN Connection
Public network

Access type: No Internet access
Connections: VPN Connection

VPN IS CONNECTED TO MULTIPLE CONNECTIONS:



View your basic network information and set up connections

View your active networks — Connect or disconnect

VPN Connection
Public network

Access type: Internet
Connections: VPN Connection

Network 31
Public network

Access type: Internet
Connections: Local Area Connection

NOW IT'S COMPLETED