



Penetration Testing

Implementation Plan

Azhar Ghafoor

Fall-2024

*Department of Cyber Security,
FCAI, Air University, Islamabad*

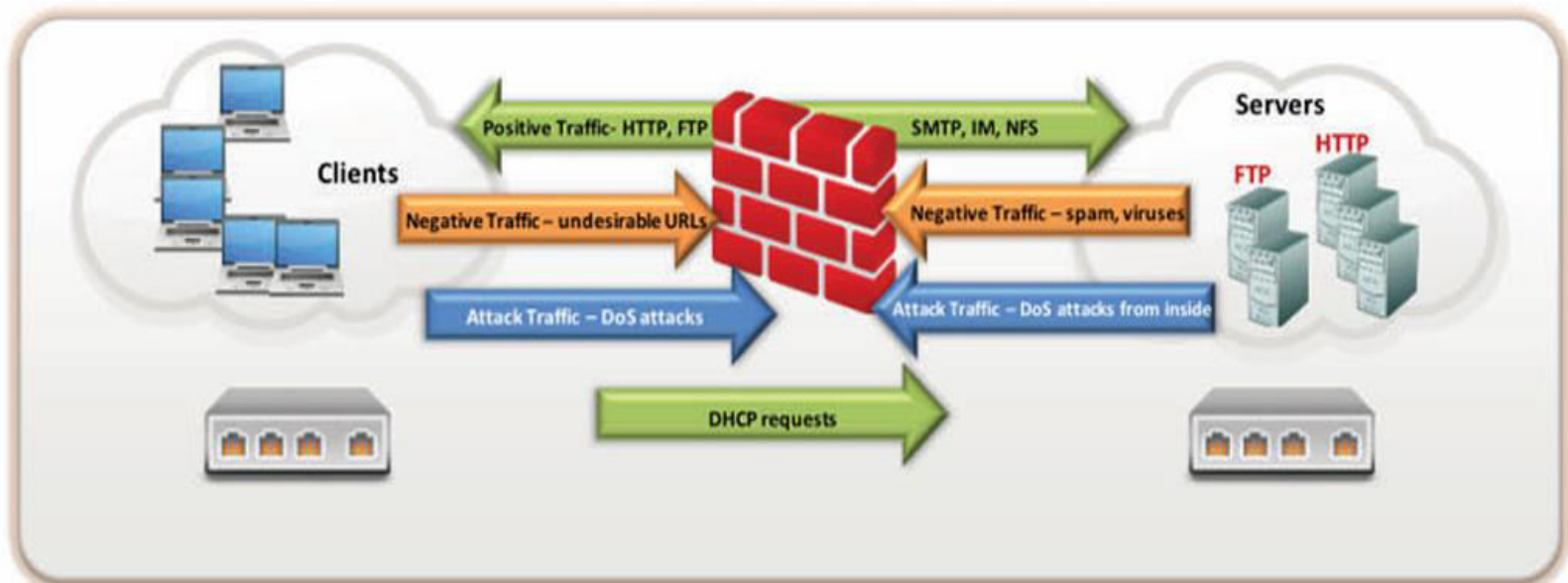
Network Penetration Testing - Perimeter Devices

Assessing Firewall Security Implementation

A firewall is a software- or hardware-based system located at the network gateway that protects the resources of a private network from users on other networks. As a network penetration tester, it is essential for you to assess the security of the installed firewall in the organization.

Testing the Firewall from Both Side

- Examine the firewall by simultaneously testing **both sides of the firewall**
- From **outside**, try to send packets to the firewall and check whether it allows them to pass against the configuration
- From **inside**, analyze the packets coming through the firewall and check whether the firewall allows them to pass against the configuration



Testing the Firewall from Both Side (Cont'd)

The following are some of the activities to be performed for testing the firewall from outside:

- Identify the **firewall rules** by using appropriate **firewall tools** like firewalking
 - Test whether unauthorized connections can be created to the **Internal network from outside**
 - Check for the reaction of the firewall **to fragmented and spoofed packets** that can be generated using a **packet generator**
-

Testing the Firewall from Both Side (Cont'd)

The following are some of the activities to be performed for testing the firewall from **inside**:

1

Test (possibly using tunneled protocols) whether unauthorized connections from the internal network to the **Internet** can be created

2

Execute a **vulnerability scanner** on the hosts of the firewall system (i.e., firewall host, internal router, external router) from inside

3

Identify the **firewall rules** by using appropriate **firewall tools** (like firewalking from both sides)

Find Information about the Firewall

I

Check for information about the company's firewall in the **Engagement Letter/Pen Testing Contract** or search over **Internet** and **publicly available sources** (Newsgroup and blog postings made by employees, job postings, trade publications, etc.)

II

Send an email message to a non-existing user of the target organization and **check bounced mail header** for company's name server and topographic information

Bounced Mail Header

SMTP <Jhon@abc.com>

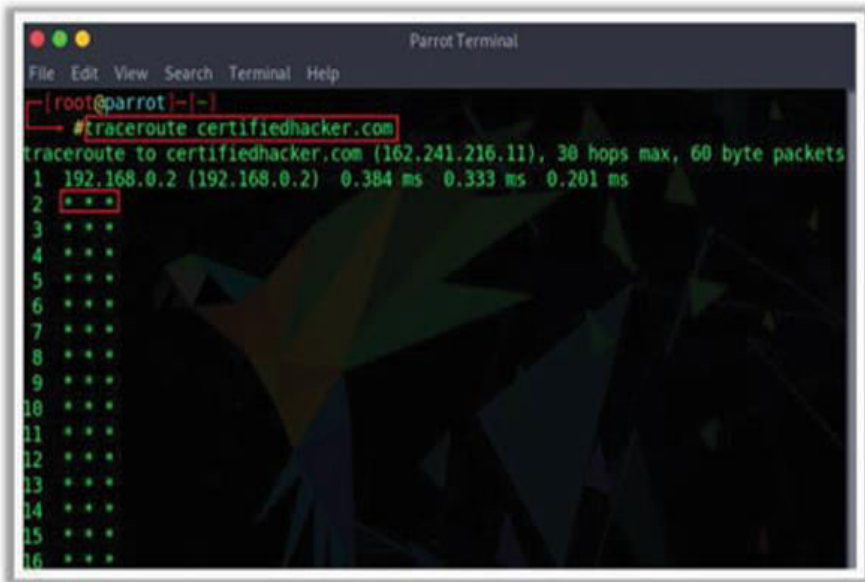
Please reply to **Postmaster@123.abc.com** if you feel this message to be in error.

Received: from **123.abc.com** ([128.105.10.15]) by **123.abc.com**

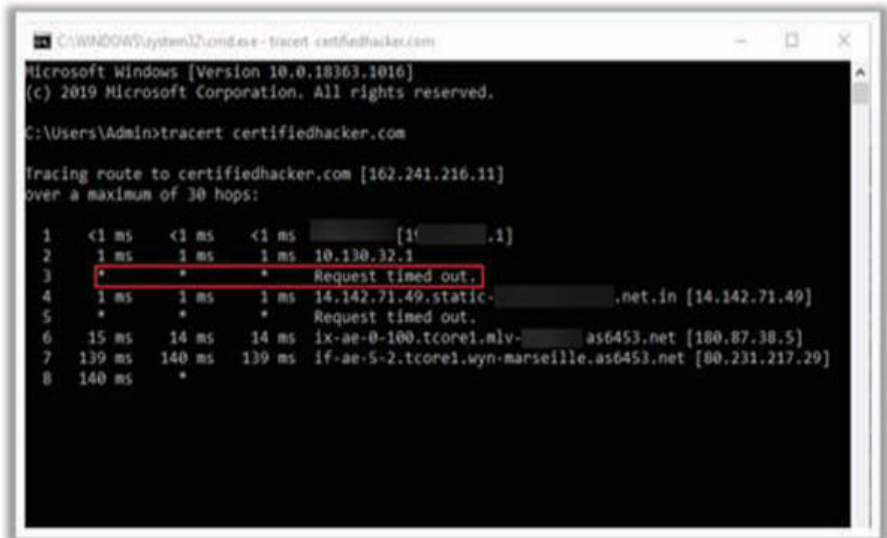
Netscape Mail Server v3.02) with ESMTTP id BBB160 for <Jhon@abc.com >; Sun, 01 March 2015 13:57:40 -0600 Received: from abc.com (root@earth.abc.com [128.164.10.16]) by abc.com (8.7.1/8.7.1) with ESMTTP id CBB29812 for <Jhon@abc.com >; Sun, 01 March 2015 13:57:40 -0600 (EST) Received: from evil.mask.com (lucifer@evil [128.105.10.16]) by abc.com (8.7.1/8.7.1) with SMTP id CBB29804 for <Jhon@abc.com >; Sun, 01 March 2015 13:57:40 -0600 (EST)

Locate the Firewall by Conducting Traceroute

- Run a normal traceroute command to **find out the access control device, such as a firewall**
- "Request timed out" means the packet could not make it there and back. It is due to firewall or other security measures at the target system



```
Parrot Terminal
File Edit View Search Terminal Help
root@parrot:~# traceroute certifiedhacker.com
traceroute to certifiedhacker.com (162.241.216.11), 30 hops max, 60 byte packets
 1  192.168.0.2 (192.168.0.2)  0.384 ms  0.333 ms  0.201 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
```



```
C:\WINDOWS\system32\cmd.exe - tracert certifiedhacker.com
Microsoft Windows [Version 10.0.18363.1016]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Admin>tracert certifiedhacker.com

Tracing route to certifiedhacker.com [162.241.216.11]
over a maximum of 30 hops:
  0  <1 ms  <1 ms  <1 ms  [192.168.0.1]
  1  1 ms  1 ms  1 ms  10.130.32.1
  2  * * * Request timed out.
  3  * * * Request timed out.
  4  1 ms  1 ms  1 ms  14.142.71.49.static-.net.in [14.142.71.49]
  5  * * * Request timed out.
  6  15 ms  14 ms  14 ms  ix-ae-0-100.tcore1.mlv-.as6453.net [180.87.38.5]
  7  139 ms  140 ms  139 ms  if-ae-5-2.tcore1.vyn-marseille.as6453.net [80.231.217.29]
  8  140 ms  *  *
```

Note: By default Windows tracert uses ICMP and both Mac OS X and Linux traceroute use UDP

Try to Pass through the Firewall Using Hping

- Hping is tcp ping utility that allows you to pass through firewall even if they are blocked
- With the help of Hping, create **custom packets** to send towards the firewall. It will elicit unique responses from the **firewall**
- T

- 10.10.1.7: Target IP address.
- -c2: Sends 2 packets.
- -S: Sends SYN packets (used in TCP handshakes).
- -p21: Targets port 21 (FTP).
- -n: Prevents DNS resolution for faster results.

Example 1:

```
[root@localhost]# hping 10.10.1.7 -c2 -S -p21 -n
# HPING 10.10.1.7 (eth0 10.10.1.1) : S set, 40 data bytes
60 bytes from 10.10.1.1: flags=SA seq=0 ttl=242 id=65121
win=64240
time=144.4 ms
```

Try to Pass through the Firewall Using Hping (Example 2)

- ❏ Craft a **SYN packet** using **Hping** or any other packet crafter and send it to the firewall
- ❏ Look for ICMP messages coming back from the firewall
- ❏ If you get an ICMP unreachable type 13 message (which is an admin prohibited packet) with a source IP address of the access control device, you will know that the packet filter is blocking the connection.

- 10.10.1.10: Target IP address.
- c2: Sends 2 packets.
- S: SYN packets.
- p80: Targets port 80 (HTTP).
- n: Disables DNS resolution.

Example 2:

```
[root@localhost]# hping 10.10.1.10 -c2 -S -p80 -n
#HPING 10.10.1.10 (eth0 10.10.1.1) : S set, 40 data bytes
ICMP Unreachable type 13 from 10.10.1.8
```

Enumerate Firewall Access Control List Using Nmap



Most firewall **implementations** have default ports in use for **remote** management purposes, for example, user authentication, management, VPN connections, etc.



Nmap can be helpful to find out loopholes in firewall implementation



With Nmap, you can find state of ports open, filtered, unfiltered and closed on the firewall

Nmap shows three states of ports:



Open – Port is **listening**



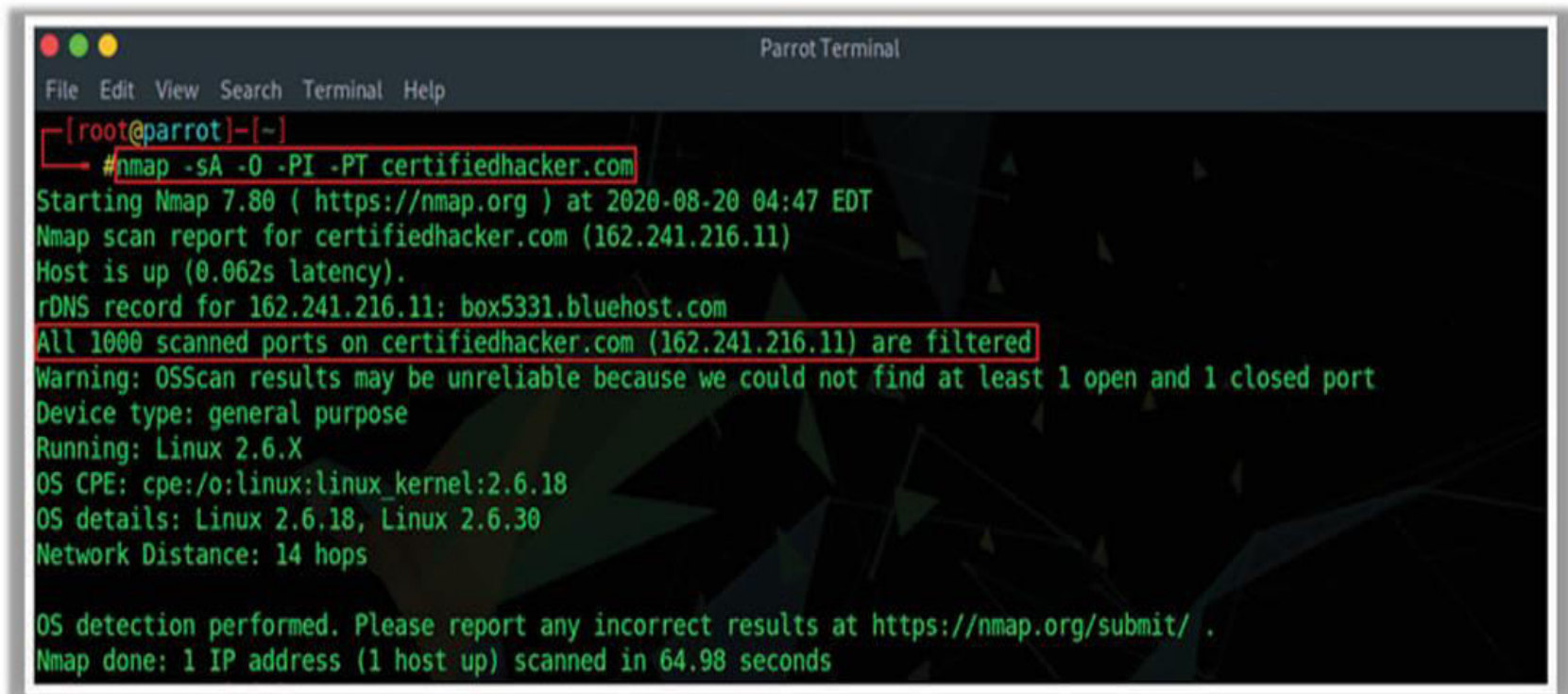
Filtered – Port is blocked by an **access control device** (router/firewall)



Unfiltered – Traffic is passing from access control devices (firewall/router), but the port is not open

Example: Enumerate Firewall Access Control List Using Nmap

ACK scan for enumeration of Access Control list



```
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~# nmap -sA -O -PI -PT certifiedhacker.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-20 04:47 EDT
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.062s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com
All 1000 scanned ports on certifiedhacker.com (162.241.216.11) are filtered
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.18
OS details: Linux 2.6.18, Linux 2.6.30
Network Distance: 14 hops

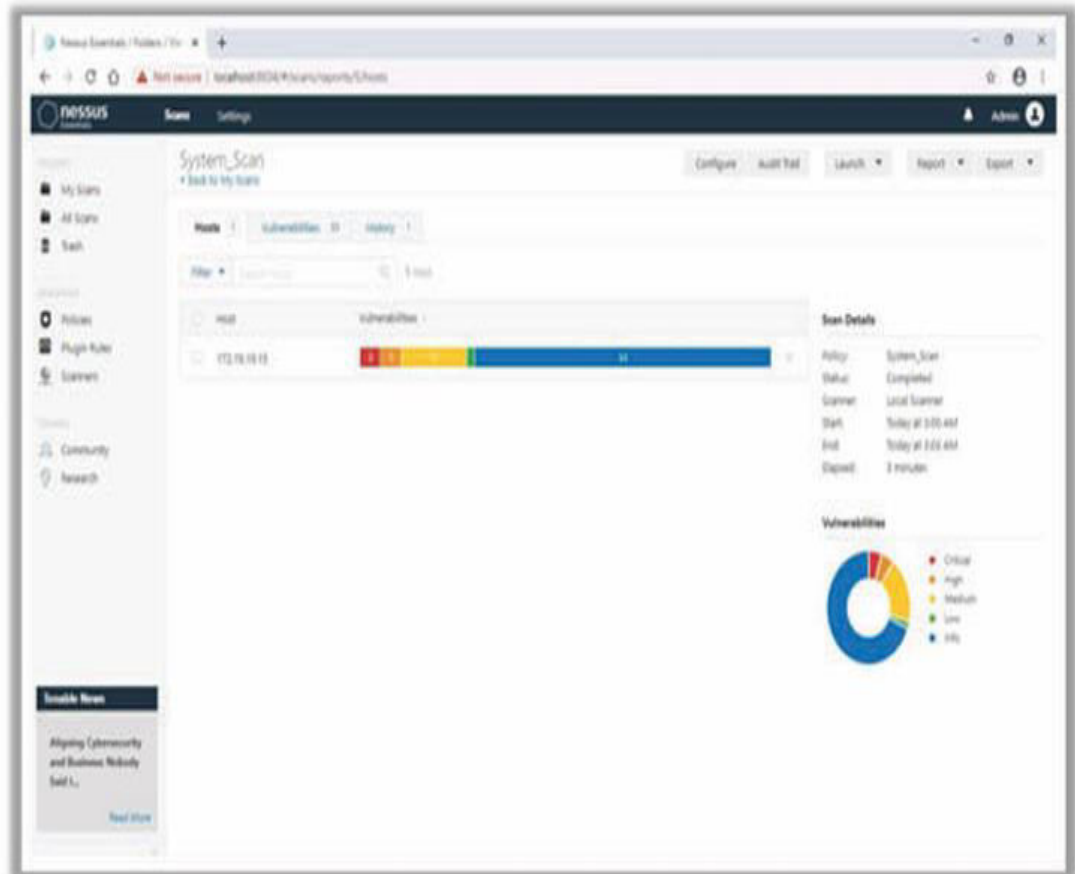
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 64.98 seconds
```

Scan the Firewall for Vulnerabilities

Run network vulnerability scanner, such as Nessus against your firewall to determine if there are any problems with it

Nessus includes a **whole category of vulnerability checks** just for firewalls

It can check the **firewall of a host** and **applications** vulnerabilities



Source: <https://www.tenable.com>

Map Firewall Make and Version with Associated Vulnerabilities

- Firewalls have specific **vulnerabilities**
- If a firewall is not patched up, then it is **vulnerable to attacks**
- Search the security vulnerabilities associated with specific version, make, model of firewall on the Internet and find out related exploits in Google hacking databases
- Send product-specific exploits against **firewall vulnerabilities** and test for responses

Try to Bypass the Firewall by IP Address Spoofing

- When the firewall allows all the traffic based on the IP address, you can exploit this firewall configuration by spoofing IP address

- Use `nmap -S <spoofed ip> -e [interface]` option to spoof IP address to go undetected

For Example,

```
nmap -e eth0 -S 192.168.1.100  
192.168.1.109
```

`-e` = interface

`-S` = Specify source (+ address)

- It will use the eth0 interface and spoof a source IP of 192.168.1.100 while scanning 192.168.1.109

```
C:\Users\Administrator>nmap -e eth0 -S 192.168.0.20 192.168.0.7  
WARNING: If -S is being used to fake your source address, you may  
using it to specify your real source address, you can ignore this  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-20 03:40 Pacific  
Nmap scan report for 192.168.0.7  
Host is up (0.0000010s latency).  
Not shown: 988 closed ports  
PORT      STATE SERVICE  
21/tcp    open  ftp  
80/tcp    open  http  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn
```

Try to Bypass the Firewall by Varying Packet Size

Many firewalls are configured to **detect port** scan attempts by **inspecting** size of packets as the ports scanners, generally, send packets that have a specific size

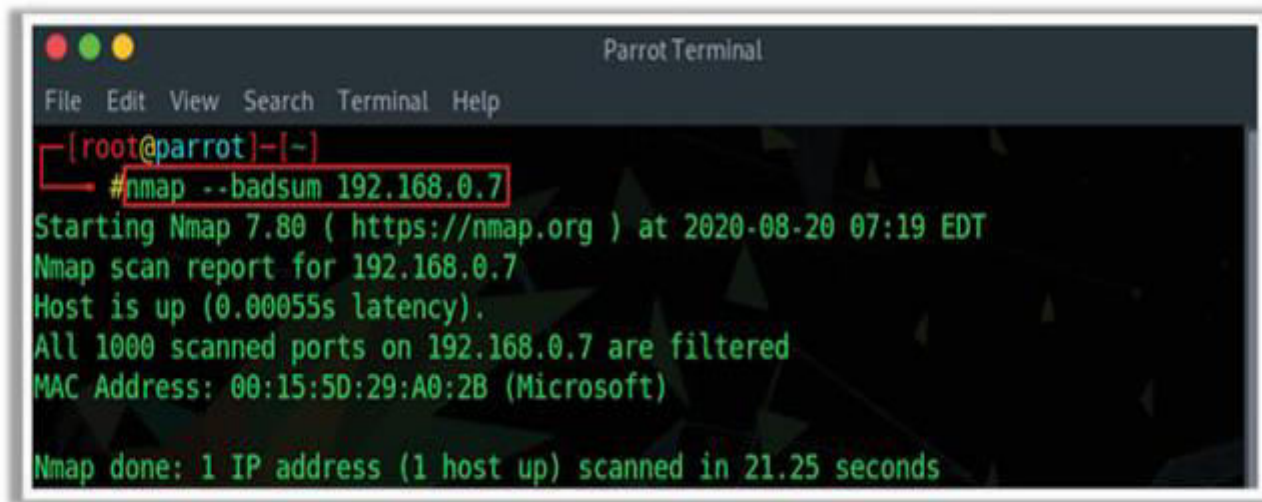
To avoid detection of your port scan attempt, use **nmap --data-length** option to send the packets with different size than the default value

```
File Edit View Search Terminal Help
[root@parrot]-[~]
#nmap --data-length 25 192.168.0.7
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-20 06:45 EDT
Nmap scan report for 192.168.0.7
Host is up (0.0015s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
```

Try to Bypass the Firewall by Sending Bad Checksums

Send the packets with **bad checksum** in an attempt to avoid firewall detection. This will **reveal** information from systems when it is not properly configured

If you don't get any information, it indicates that the **system** is well **configured**



```
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[~]
#nmap --badsum 192.168.0.7
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-20 07:19 EDT
Nmap scan report for 192.168.0.7
Host is up (0.00055s latency).
All 1000 scanned ports on 192.168.0.7 are filtered
MAC Address: 00:15:5D:29:A0:2B (Microsoft)
Nmap done: 1 IP address (1 host up) scanned in 21.25 seconds
```

Try to Bypass the Firewall Using Port Redirection

■ If you cannot get direct access to a port, then use **port redirection**

■ It is used to **bypass** port filtering

■ Install a **port redirector** and make it listen on a selected port number

■ Packets received on the **listening port number** are forwarded to the desired port on the remote host

■ **Tools:**

```
• fpipe -l 80 -r 139 192.168.10.40
• datapipe 80 139 192.168.10.40
```

The command is setting up a local port forwarding from port 80 to the remote port 139 on the IP address 192.168.10.40.

Try to Bypass the Firewall Using IP Address in Place of URL

- Use online services, such as **Host2ip**, that convert host/domain names to an IP address to find the IP address of the blocked website
- In order to bypass the firewall, type the **IP address directly into the browser's address bar** in place of typing the blocked website's domain name
 - For example, to access Facebook, type its **IP address** (173.252.120.6) instead of typing domain name



Note: This method fails if the blocking software tracks the IP address sent to the web server

Try to Bypass the Firewall Using Anonymous Website Surfing Sites

- Search over the Internet for anonymous website surfing sites that provide options to **encrypt the URLs** of the websites
- These websites **hide the actual IP address** and show another IP address, which could prevent the website from being blocked, thus allowing access to them

Anonymous Website Surfing Sites

1

<http://anonymouse.org>

2

<http://www.anonymizer.com>

3

<http://www.webproxyserver.net>

4

<http://kproxy.com>

5

<http://proxify.com>

6

<http://www.spysurfing.com>

7

<http://zendproxy.com>

8

<http://anype.com>

Try to Bypass the Firewall Using a Proxy Server

Find an **appropriate** proxy server

In the Port box, type the **port number** that is used by the proxy server for client connections (by default, 8080)

On the Tools menu of any Internet browser, go to LAN of Network Connections tab, and then click **LAN/Network Settings**

Click to select the bypass proxy server for local addresses check box, if you do not want the proxy server computer to be used when connected to a computer on the **local network**

Under the proxy server settings; select the use a **proxy server for LAN**

Click **OK** to close the **LAN Settings** dialog box

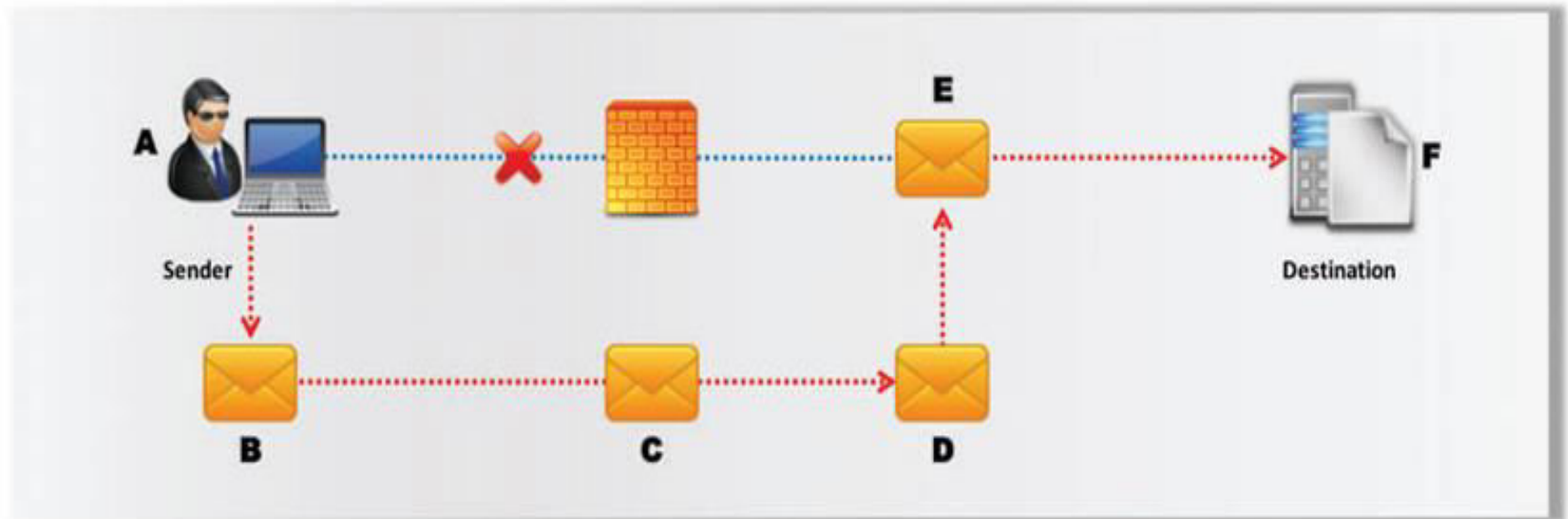
In the Address box, type the **IP address** of the proxy server

Click **OK** again to close the **Internet Options** dialog box

Try to Bypass the Firewall Using Source Routing

Source routing is a technique in which the sender of a packet partially or completely **specifies the route** the packet takes through the network

Modify the **addressing information** in the IP packet header and the source address bits field in order to bypass the firewall



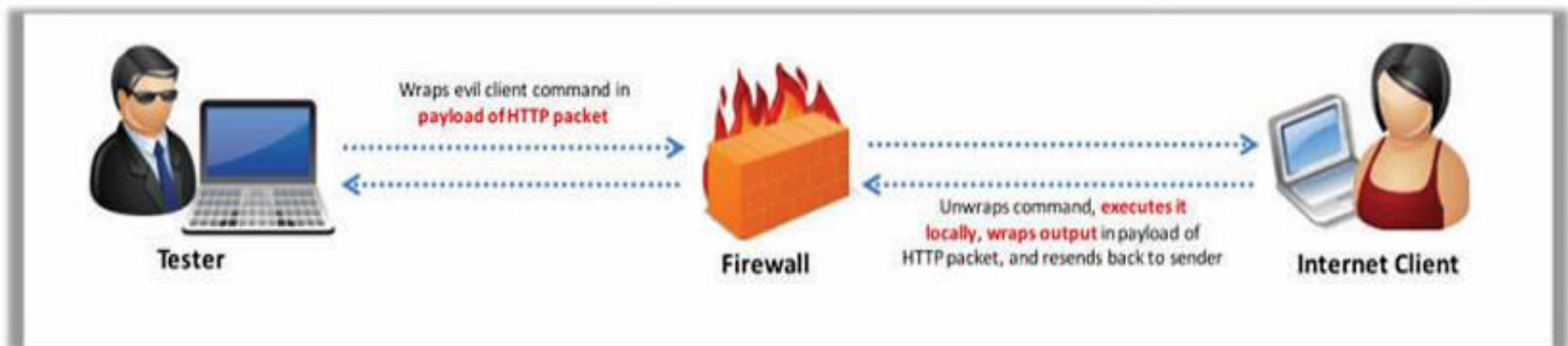
Try to Bypass the Firewall Using HTTP Tunneling Method

This method can be implemented if the target company has a **public web server** with **port 80 used for HTTP traffic**, that is unfiltered on its firewall

Many firewalls **do not examine the payload of an HTTP packet** to confirm that it is legitimate HTTP traffic; thus, it is possible to tunnel traffic inside TCP port 80 because it is already allowed

Tools, such as **Super Network Tunnel**, **HTTPTunnel**, **HTTPORT**, and **HTTHOST** use this technique of tunneling traffic across **TCP port 80**

Upload the **server onto the target system** and tell it which port is to be redirected through **TCP port 80**



HTTP-Tunnel

Source: *<http://www.httptunnelclient.com>*

HTTP-Tunnel technology allows users to perform various internet tasks despite the restrictions imposed by firewalls. This is made possible by sending data through HTTP (port 80). Additionally, HTTP-Tunnel technology is very secure, making it indispensable for both average and business communications.

HTTP-Tunnel Applications

Following are various applications utilized to implement HTTP-Tunnel technology:

HTTP-Tunnel Client: An application that runs in the system tray acting as a SOCKS server, managing all data transmissions between the computer and the network.

HTTP-Tunnel Server: A customizable server software solution for both personal and corporate networks.

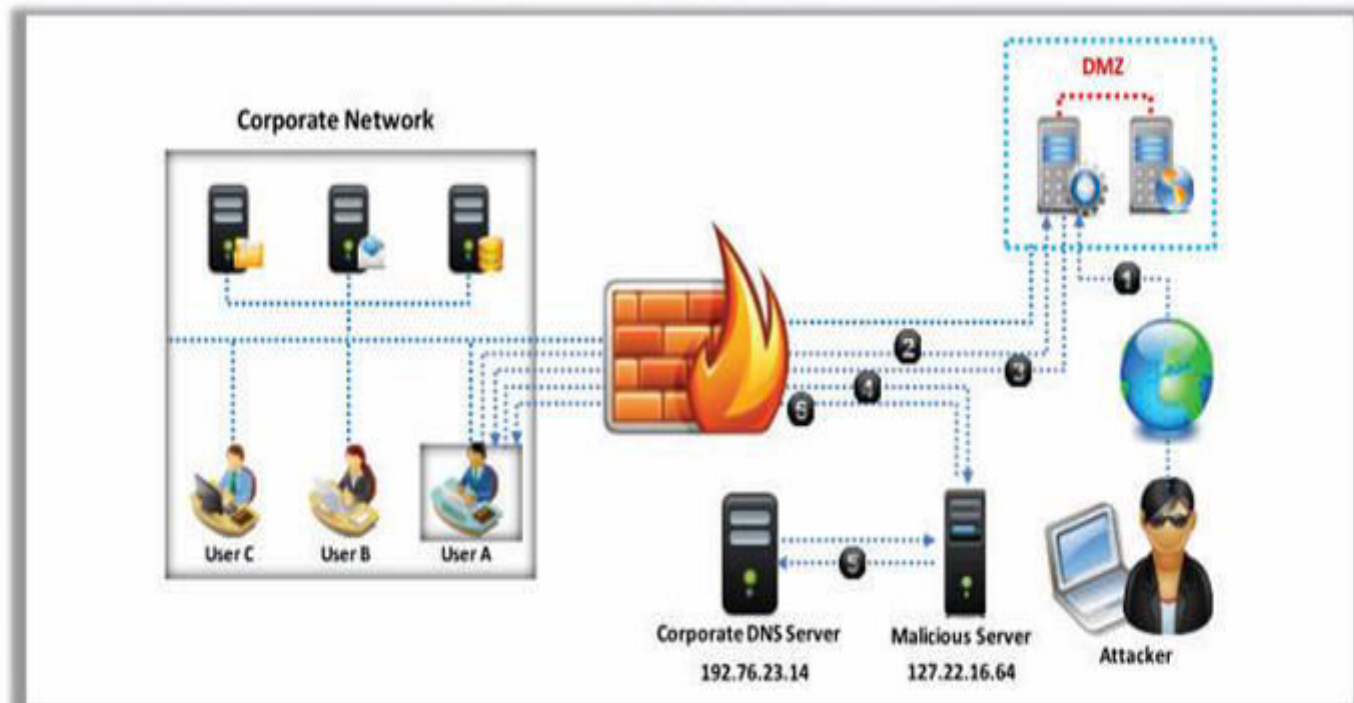
HTTP-Tunnel ActiveX Control: It allows developers to incorporate HTTP-Tunnel technology into their software applications.

Corporate Messenger (VCM): It is a secure and serverless instant messaging application, suitable for corporate intranets.

Try to Bypass the Firewall Through MITM Attack

DNS Server Poisoning Process

1. User A requests WWW.example.com from the **corporate DNS server**
2. Corporate DNS server sends the **IP address (127.22.16.64) of the attacker**
3. User A accesses the **attacker's malicious server**
4. Attacker connects with the real host and **tunnels the user's HTTP traffic**
5. The malicious codes embedded in the attacker's web page are **downloaded and executed** on the user's machine



Try to Bypass the Firewall Using Malicious Contents

■ Create a malicious file using **Trojan Horse** Construction Kit

■ Embed a **malicious file** in software installation files, mobile phone software, or text, multimedia, and graphics files to carry malicious content

■ Send the contents containing **malicious code** to the user and trick him/her to open it so that the malicious code can be executed



Q&A



Thankyou