INTERNSHIP PROJECT 2

TOPIC: EXPLOITING SERVER VULNERABILITIES

VIKASH KUMAR | wiryvikash15@gmail.com

1. Check for SMTP open relay

Description:

An open relay is an Simple Mail Transfer Protocol (SMTP) email server that allows anyone on the Internet to send messages through it while hiding or obscuring the source of the messages being sent.

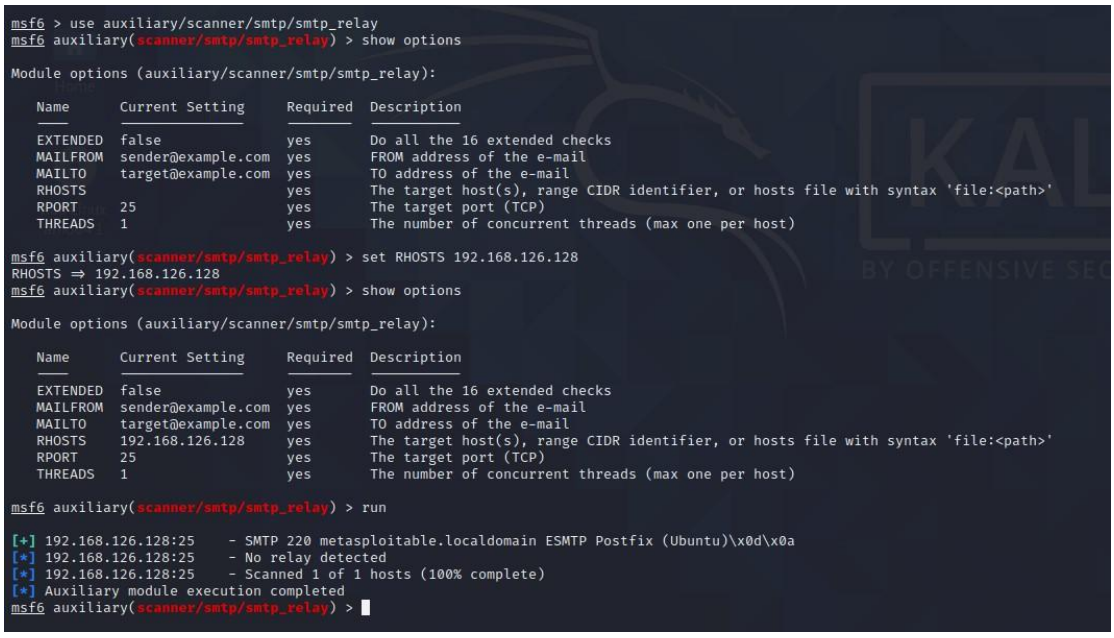
Open relays do nothing to identify the original sender of email messages, making them very vulnerable to address spoofing, a technique that alters email headers to appear as though they originated from a source other than the actual source. Although this is how email was initially set up, this type of system is often exploited by spammers.

Open relay is also known as an open relay server, insecure relay, third-party relay, open mail relay and spam relay.

Screenshots:

Screenshot 1:

Screenshot 2:



2. Check for zone transfers

Description:

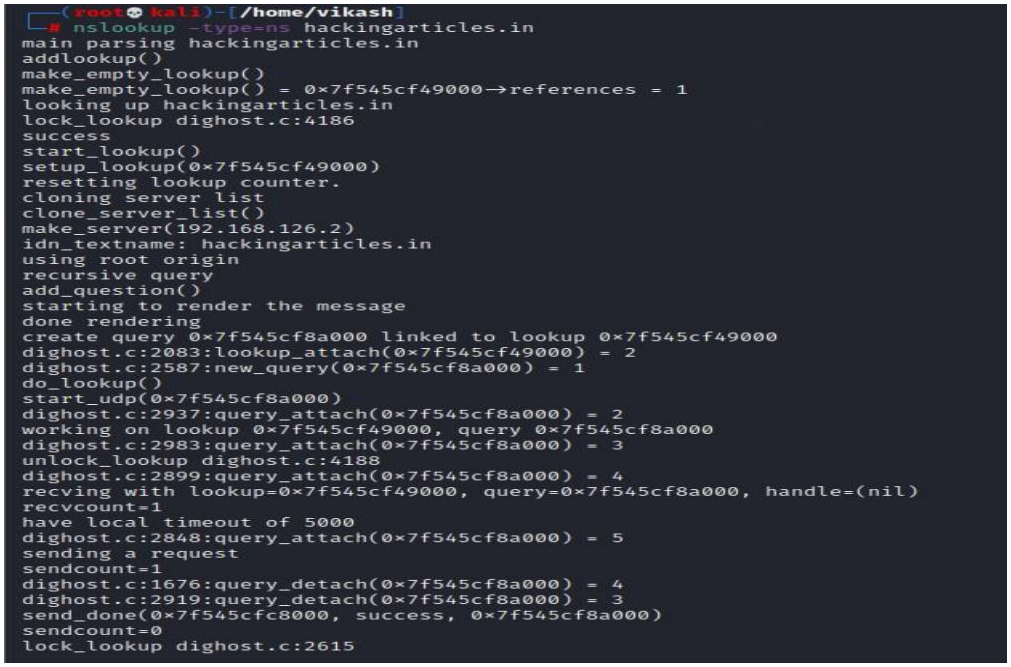
DNS zone transfer, also known as DNS query type AXFR, is a process by which a DNS server passes a copy of part of its database to another DNS server. The portion of the database that is replicated is known as a zone.

A zone transfer uses the Transmission Control Protocol (TCP) and takes the form of a client-server transaction.

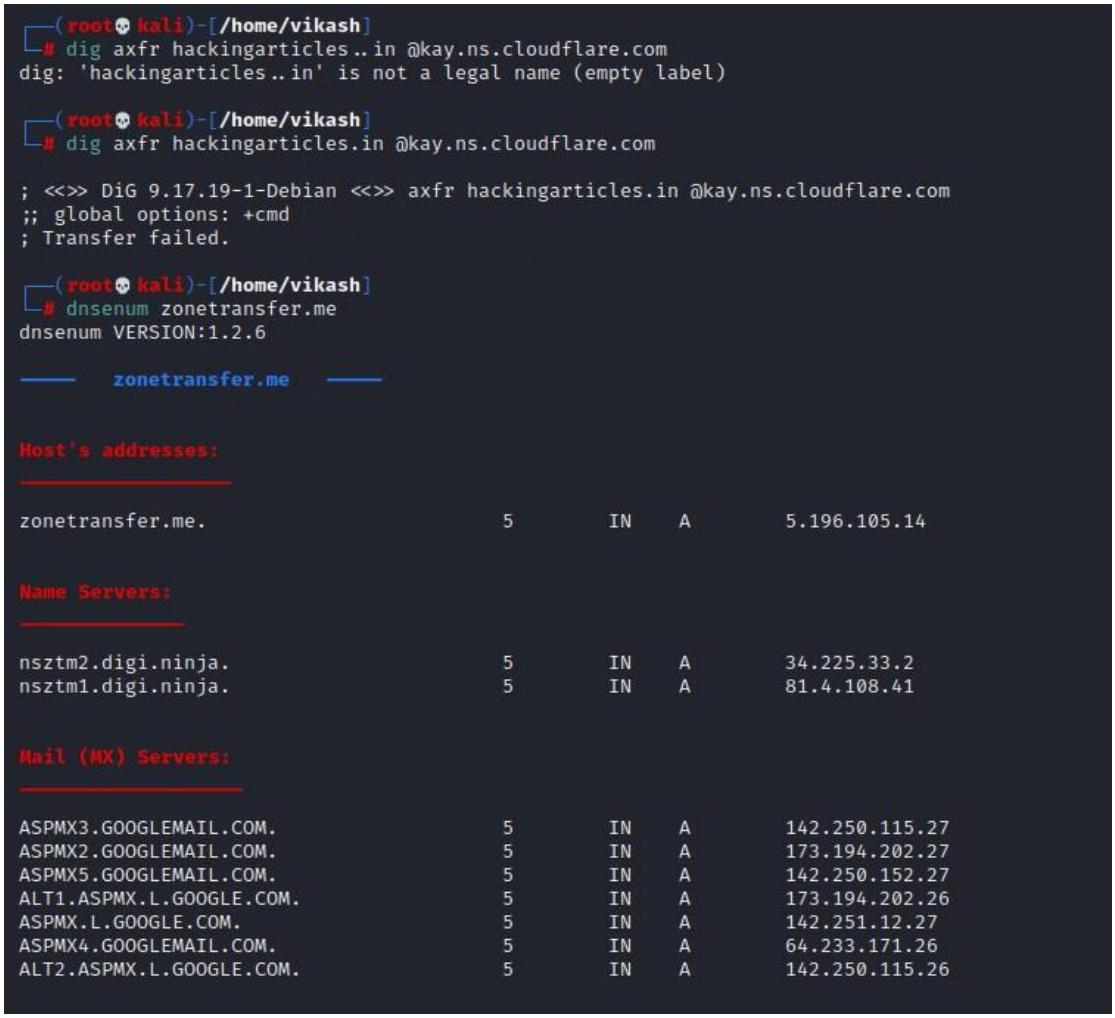
The client requesting a zone transfer may be a slave server or secondary server, requesting data from a master server or a primary server.

Screenshots:

Screenshot 1:

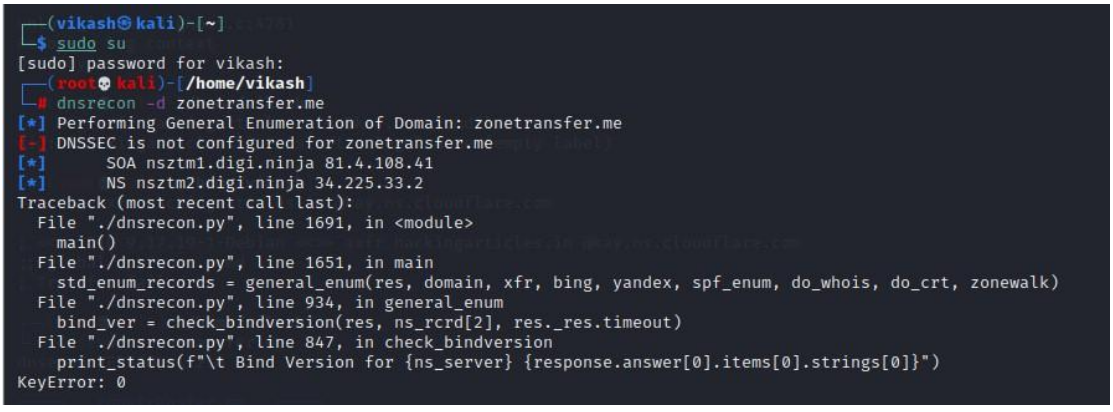


Screenshot 2:



```
┌──(root💀kali)-[/home/vikash]
└─# dig axfr hackingarticles..in @kay.ns.cloudflare.com
dig: 'hackingarticles..in' is not a legal name (empty label)

┌──(root💀kali)-[/home/vikash]
└─# dig axfr hackingarticles.in @kay.ns.cloudflare.com

; <<>> DiG 9.17.19-1-Debian <<>> axfr hackingarticles.in @kay.ns.cloudflare.com
;; global options: +cmd
; Transfer failed.

┌──(root💀kali)-[/home/vikash]
└─# dnsenum zonetransfer.me
dnsenum VERSION:1.2.6

-----   zonetransfer.me   -----


Host's addresses:
__________________

zonetransfer.me.                         5        IN    A        5.196.105.14


Name Servers:
______________

nsztm2.digi.ninja.                       5        IN    A        34.225.33.2
nsztm1.digi.ninja.                       5        IN    A        81.4.108.41


Mail (MX) Servers:
___________________

ASPMX3.GOOGLEMAIL.COM.                   5        IN    A        142.250.115.27
ASPMX2.GOOGLEMAIL.COM.                   5        IN    A        173.194.202.27
ASPMX5.GOOGLEMAIL.COM.                   5        IN    A        142.250.152.27
ALT1.ASPMX.L.GOOGLE.COM.                 5        IN    A        173.194.202.26
ASPMX.L.GOOGLE.COM.                      5        IN    A        142.251.12.27
ASPMX4.GOOGLEMAIL.COM.                   5        IN    A        64.233.171.26
ALT2.ASPMX.L.GOOGLE.COM.                 5        IN    A        142.250.115.26
```

Screenshot 3:



```
┌──(vikash㉿kali)-[~]
└─$ sudo su
[sudo] password for vikash:
┌──(root💀kali)-[/home/vikash]
└─# dnsrecon -d zonetransfer.me
[*] Performing General Enumeration of Domain: zonetransfer.me
[-] DNSSEC is not configured for zonetransfer.me
[*]      SOA nsztm1.digi.ninja 81.4.108.41
[*]      NS nsztm2.digi.ninja 34.225.33.2
Traceback (most recent call last):
  File "./dnsrecon.py", line 1691, in <module>
    main()
  File "./dnsrecon.py", line 1651, in main
    std_enum_records = general_enum(res, domain, xfr, bing, yandex, spf_enum, do_whois, do_crt, zonewalk)
  File "./dnsrecon.py", line 934, in general_enum
    bind_ver = check_bindversion(res, ns_rcrd[2], res._res.timeout)
  File "./dnsrecon.py", line 847, in check_bindversion
    print_status(f"\t Bind Version for {ns_server} {response.answer[0].items[0].strings[0]}")
KeyError: 0
```

3. Perform netbois enumeration

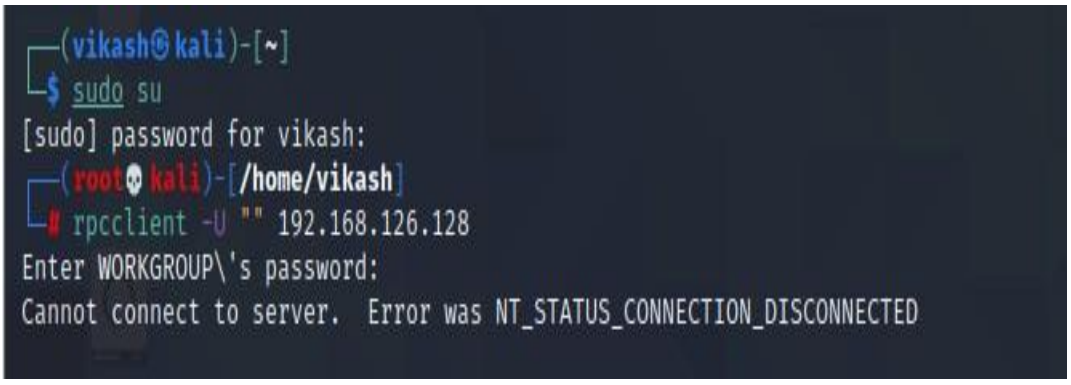
Description:

NetBIOS, which stands for network basic input/output system, is a service that allows computers to communicate over a network . However, NetBIOS is not a networking protocol, it is an API. It runs over TCP/IP via the NBT protocol, allowing it to function on modern networks.

NetBIOS provides two primary communication methods. The datagram service allows for connectionless communication over a network, ideal for situations where fast transmission is preferred, such as error generation. The session service, on the other hand, allows two computers to establish a connection for reliable communication. NetBIOS also provides name services which allow for name resolution and registration over the network.

Screenshots:

Screenshot 1:



4. Sniff the data of any application using wire-shark

Description:

Computers communicate by broadcasting messages on a network using IP addresses. Once a message has been sent on a network, the recipient computer with the matching IP address responds with its MAC address.

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;

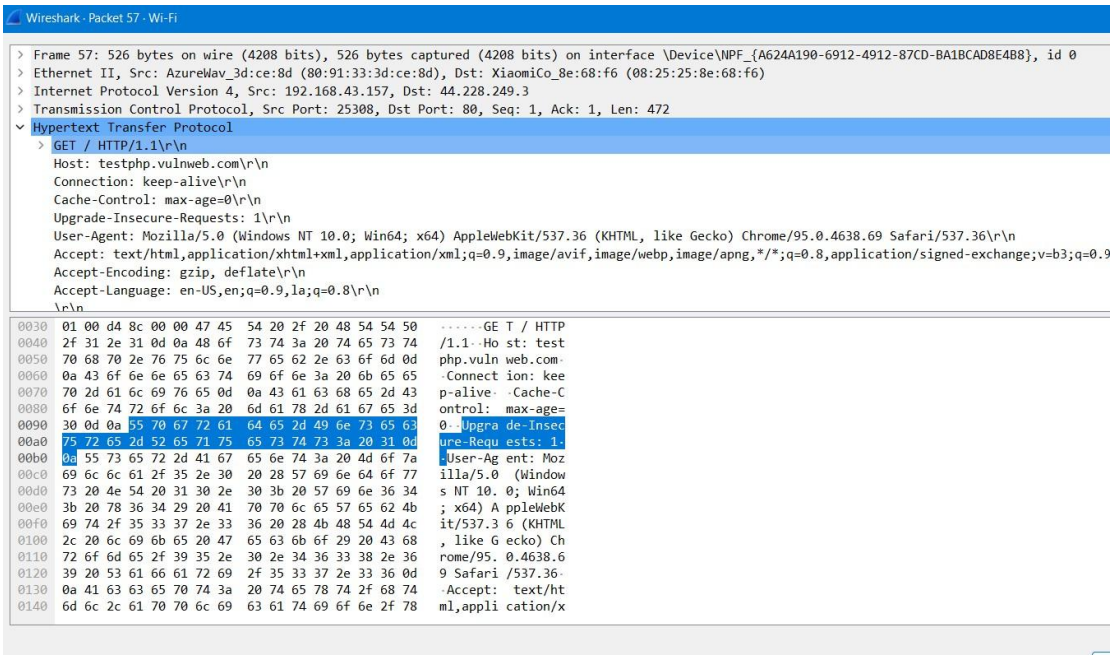
Capture sensitive data such as login credentials
Eavesdrop on chat messages
Capture files have been transmitted over a network

The following are protocols that are vulnerable to sniffing

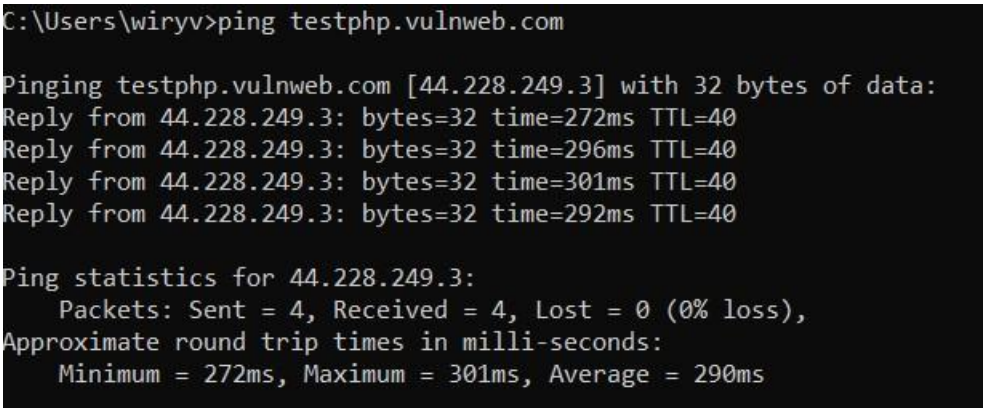
- Telnet
- Rlogin
- HTTP
- SMTP
- NNTP
- POP
- FTP
- IMAP

Screenshots:

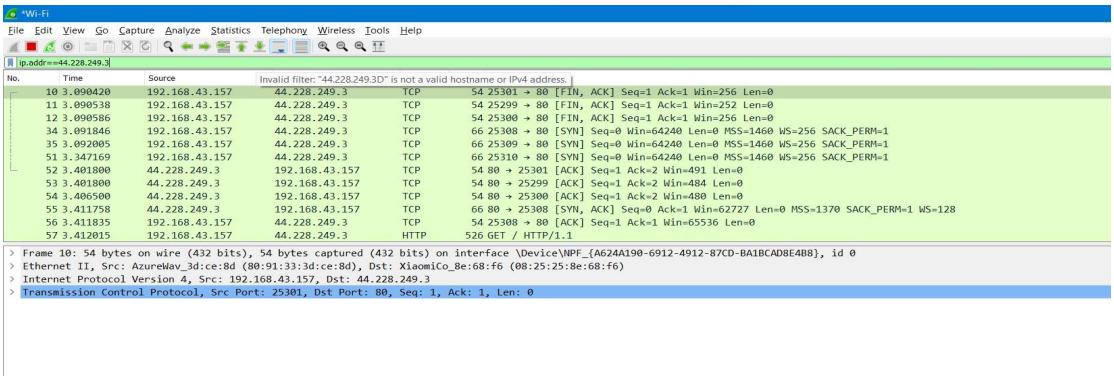
Screenshot 1:



Screenshot 2:



Screenshot 3:



5. Perform DOs Attack using metasploit framework

Description:

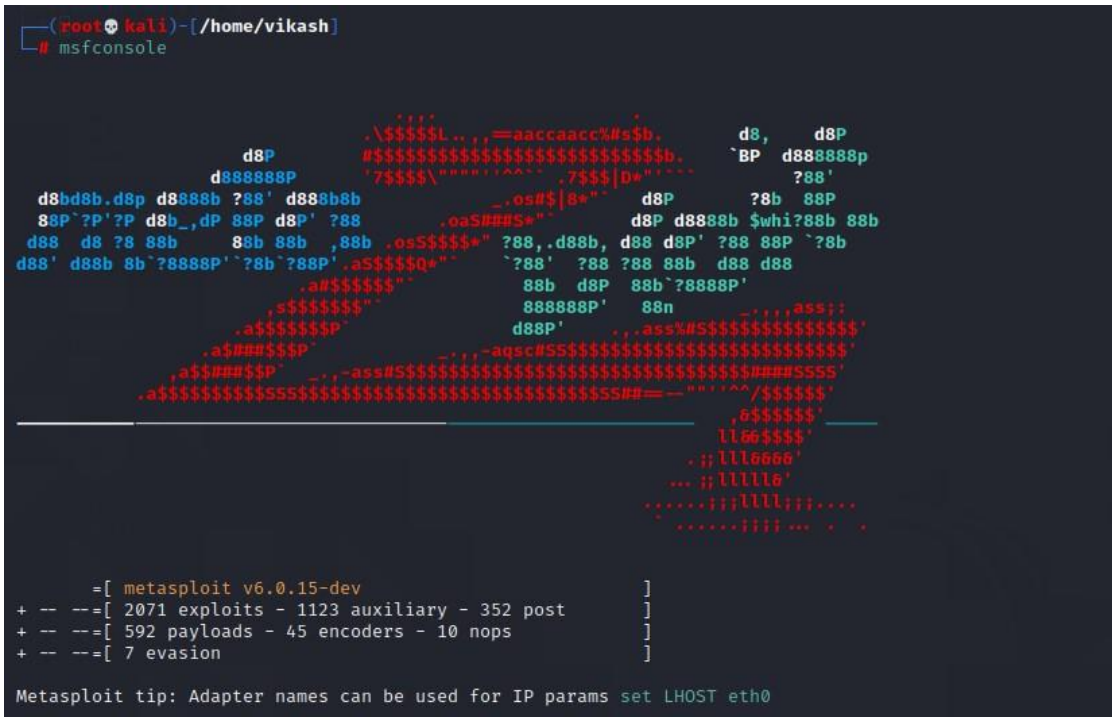
Typically, a Penetration Testing exercise is focused on identifying the gaps in security rather than harming a system. This is a key feature that separates a real attacker from an authorized Penetration Tester. Real hackers don't follow the rules and are not concerned about interrupting business if it can improve their situation.

In some cases, a hacker is looking to create any form of negative impact on a target, including taking down critical systems. For this reason, it makes sense in some cases to test systems for the risk Denial of Service(DoS) type attacks. This is commonly termed as stress testing your Internet facing services.

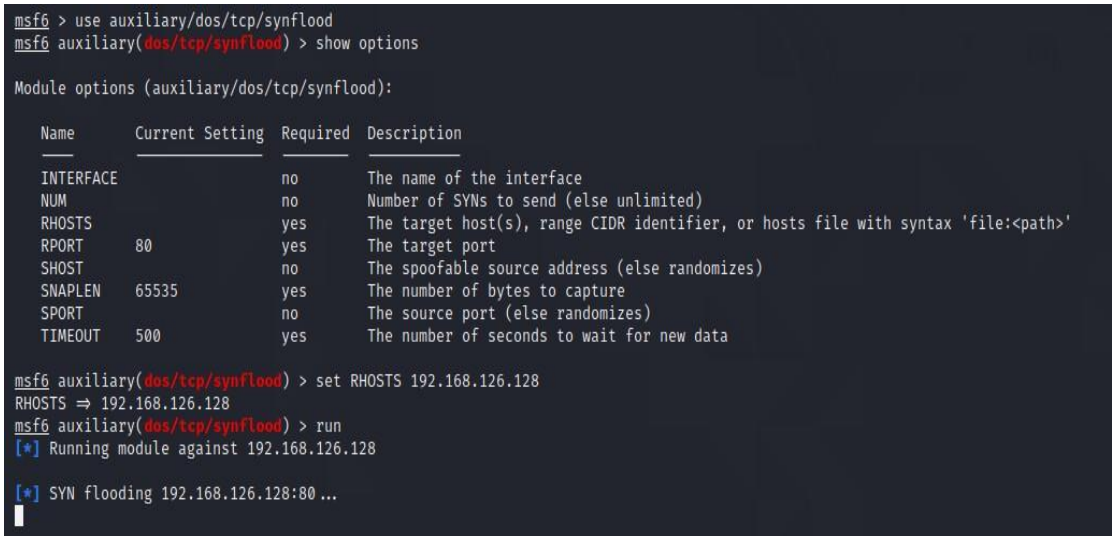
The most common DoS attack involves flooding a target with external communication requests. This overload prevents the resource from responding to legitimate traffic, or slows its response so significantly that it is rendered unavailable. DoS attacks can target system resources (IE disk space, bandwidth, and so on), configuration information (IE remove route tables), state information (TCP session resetting), or anything that can harm system operation.

Screenshots:

Screenshot 1:



Screenshot 2:



Screenshot 3: