Denial of Service Attack with UDP Flood

Jin Minhao

Department of Computer Science and Software Engineering

Xi'an Jiaotong-Liverpool University

Suzhou China

Minhao.Jin17@student.xjtlu.edu.cn

***Abstract*—In recent years, the network security has continuously been a concerned topic with the rapid development of network application and technology. However, with the help of some DDoS (Distributed Denial of Service) tools, the DoS (Denial of Service) attack becomes one of the most popular intrusion methods which breaches the network security and often makes great economic losses and impact [1]. In this paper, one DoS attack method, UDP (User Datagram Protocol) flood will be introduced and a DoS attack experiment with using UDP flood will be designed and discussed.**

***Keywords*— Denial of Service (DOS) attack, UDP.**

I. INTRODUCTION

UDP stands for User Datagram Protocol which is a connectionless protocol to process packets. In the model of OSI (Open System Interconnection), the UDP protocol is located at the transport layer. UDP flood comes under category of DDoS flood attacks [2]. A common method for attacking is to use a large number of UDP packets to impact all kinds of severs, such as streaming media video servers, Radius authentication servers or DNS servers. UDP flood of 100k bps often collapses the devices on the line, such as the firewall, causing the entire network segment to collapse.

In this paper, an FTP server will be established as the victim and a DoS attack with UDP flood to this sever is designed and implemented.

II. THE EXPERIMENTAL PLATFORM FOR DOS ATTACK

A. The Framework of Experimental Platform

The framework of the experiment is shown in Figure 1.

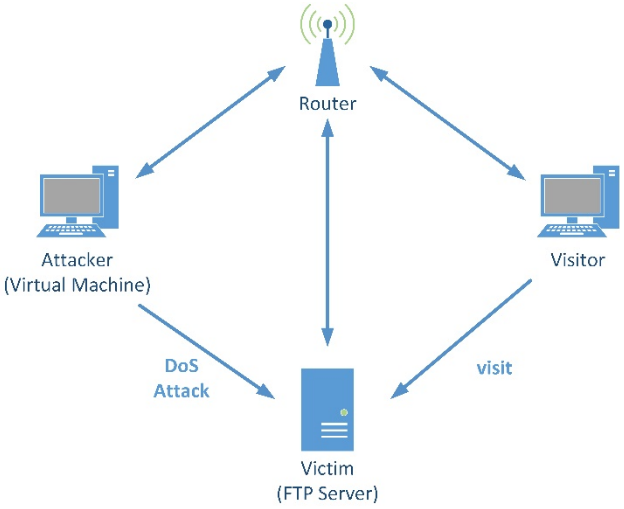


Figure 1: the framework of the experiment

The experiment platform consists of the following components:

- **Router:** The router' s function is to establish links among the virtual machine, visitor PC and the FTP server as a LAN (local area network). The unique IP address of other three devices will be distributed by the router. If there is no attack to the FTP server, in normal case, the connection between visitor and the FTP server is unblocked. In other words, the visitor has the ability to read or write the documents which shared by the FTP server.

- **Attacker (Kali Linux)**: The attacker' s operating system is Kali Linux, which is installed in the virtual machine. More introduction of Kali Linux will be given below.
- **Visitor**: Another PC' s role is a regular visitor who has the access to the FTP server to update the documents saved in the server. The visitor' s operating system is Windows 10. In this experiment, it also monitors and records the response time of the FTP server with the 'Ping command' in the 'command prompt'.
- **Victim (FTP server)**: The third PC' s role is a working FTP server which is vulnerable to the attacker. Steps of setting up an FTP server will also be introduced later. An application called 'Wireshark' (a packet analyzer) is installed on this computer to capture UDP packets from the attack source for further analysis.

In normal cases, the communication between the visitor sever and the FTP server is unrestricted. However, after the attacker launches an UDP flood attack at the FTP server, the connection between the user and sever may be blocked.

B. DoS Attack (UDP Flood)

The connection of network can be effected by a denial-of-service attack. It is realized by flooding the target with huge amount of information to triggers a crash [3]. Since UDP is a connectionless protocol, an attacker can send a large number of small UDP packets with spoofed source IP addresses. Victim will send the acknowledgement to the source IP address after receiving these packets. The victim device keeps waiting for the response if it does not get any feedback in turn. At last when victim gives up responcing, almost all its resources will have been consumed and finally resulting in crash of the system. Also, as long as a UDP port is opened to provide related services, then attacks can be made against these related services.

C. Kali Linux

According to [4], Kali Linux is an advanced penetration testing and security audit Linux distribution. It has over 300 penetration testing tools in categories such as information gathering, vulnerability assessment, password attack and wireless attack, etc. In this experiment, the terminal of Kali Linux is used as a tool to launch the UDP flood attack.

III. The Process Of DoS Attack Experiment

A. The establishment of the FTP server

Firstly, in the Windows Internet information menu, open the FTP services. After the automatic configuration, the FTP function is available in the Internet information service. Then a path in the computer is chosen as the physical address of the FTP server' s storage path. FTP address is set as the same as the third PC' s IP address which is 192.168.0.7 and the port number is set to be 2121. After the FTP service has been launched, we can enter the FTP address in the explorer to check whether the FTP server is accessible for other users under the same network segment.

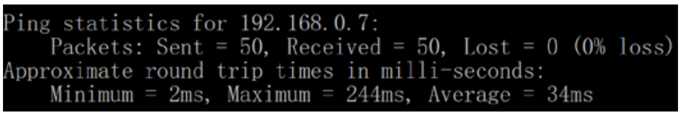
B. The Preparation for The Experiment

Three PCs including attacker, FTP server and visitor are connected to the LAN via router. The router automatically distributes the IP address to different devices. The first step is to figure out the IP address of the different components. All the devices and their IP address are shown in Table I.

TABLE I. THE IP ADDRESS OF DIFFERENT DEVICES

Device	IP Address	MAC Address	Role
Router	192.168.0.1	C4:36:55:76:5F:FB	Local Network Gateway
Virtual Machine on PC1	192.168.0.111	08:00:27:D3:23:2D	Attacker
PC2	192.168.0.14	AC:FD:CE:E0:C7:61	Visitor
PC3	192.168.0.7	F8:DA:0C:4E:58:8D	Attacker

To create a relatively ideal experimental environment, all the firewalls of the devices are closed at the beginning. The group first use ping command to all the other components in the same LAN to check they are connected with each other. The ping command status between the visitor and the FTP server should be concerned because it shows whether the user can successfully get access to the FTP server. For an accurate result, 50 packets are sent each time and each of the packets size is 32 bytes. The sending ping command status between the visitor and the FTP server are displayed in Figure 2, Figure 3 and Table II.



```
Ping statistics for 192.168.0.7:
    Packets: Sent = 50, Received = 50, Lost = 0 (0% loss)
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 244ms, Average = 34ms
```

Figure 2: The sending ping command status

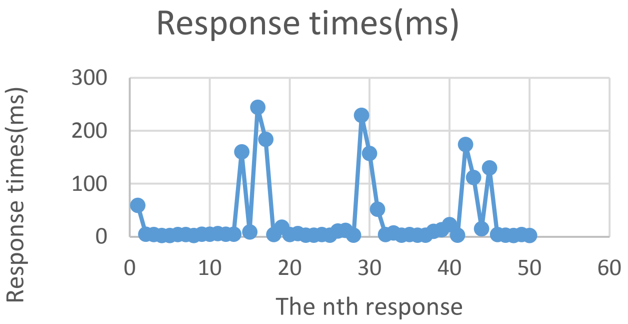


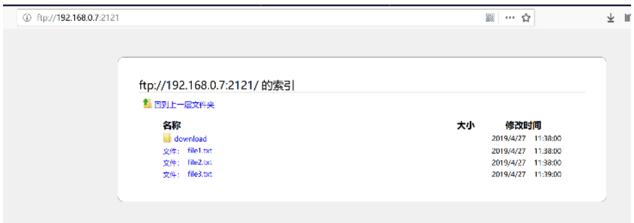
Figure 3: Sending ping command response time

TABLE II. EXPERIMENT RESULTS FOR SENDING PING COMMAND STATUS

Status	response time			packet loss
	Maximum	Minimum	Average	
Sending ping command	244ms	2ms	34ms	0%

Finding. Since the wireless connection is inherently less stable than wired connection, as it is shown in Figure 3, the maximum and minimum response time vary widely. However, the average response time for ping command is very short, only 34ms. Most importantly, there is no packet lost during the transmission, which means the visitor can successfully get the access to the FTP server. The connection is unrestricted at this time.

After the ping command status is checked, the visitor inputs the FTP address which is ftp://192.168.0.7:2121 in the Firefox explorer. As it is shown in Figure 4, the visitor can freely read or write the documents shared by the ftp server.



ftp://192.168.0.7:2121

ftp://192.168.0.7:2121/ 的索引

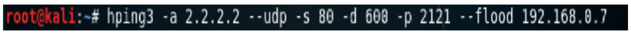
回到上一层文件夹

名称	大小	修改时间
download		2019/4/27 11:38:00
文件: file1.txt		2019/4/27 11:38:00
文件: file2.txt		2019/4/27 11:38:00
文件: file3.txt		2019/4/27 11:39:00

Figure 4: Visiting the FTP server successfully

C. DoS Attack Using Hping3 UDP flood with a spoofed IP address

Open the terminal in the Kali Linux and input the command shown in Figure 5.

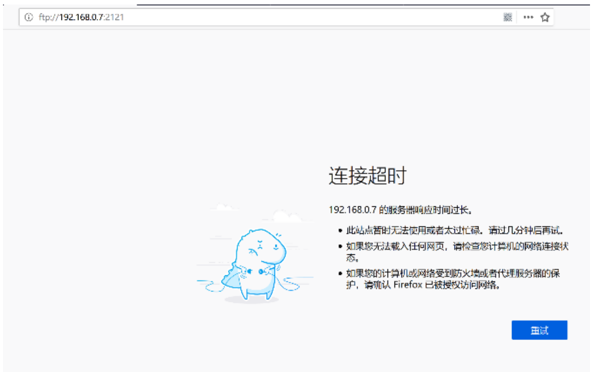


```
root@kali:~# hping3 -a 2.2.2.2 --udp -s 80 -d 600 -p 2121 --flood 192.168.0.7
```

Figure 5: UDP Flood Command

In Figure 5, the command is “hping3 –a 2.2.2.2 --udp –s 80 –d 600 –p 2121 –flood 192.168.0.7”.

“hping3” means the program command. “-a 2.2.2.2” means using the fake IP address “2.2.2.2” to send packets. In other words, the real IP address of the virtual machine which is “192.168.0.111” cannot be detected. “udp” means sending UDP packets only. “-s 80” means the source port. “-d 600” means the data size of each packet is 600 bytes. As mentioned before, the FTP server uses the 2121 port. Thus, “-p 2121” means setting the 2121 port as the destination port. “-flood 192.168.0.7” means sending the packets to the 192.168.0.7, which is the IP address of the FTP server as fast as possible, without taking care to show incoming replies [5].



ftp://192.168.0.7:2121

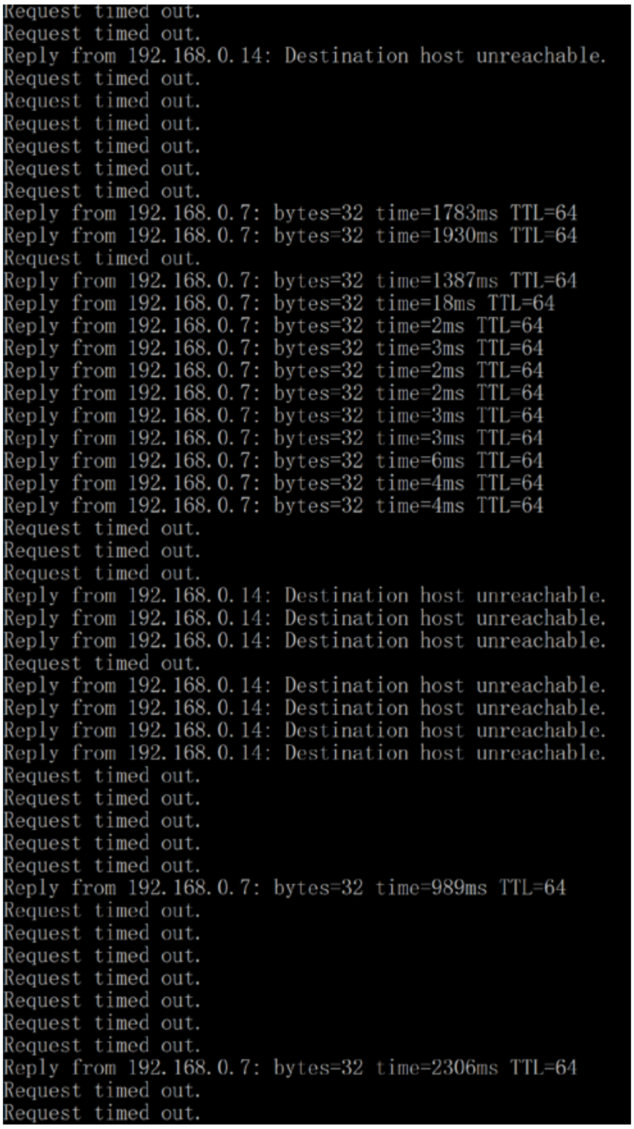
连接超时

192.168.0.7 的服务器响应时间过长。

- 此站点暂时无法使用或者太过忙碌。请过几分钟后再试。
- 如果您无法载入任何网页，请检查您计算机的网络连接状态。
- 如果您的计算机或网络受到防火墙或者代理服务器的保护，请确认 Firefox 已被授权访问网络。

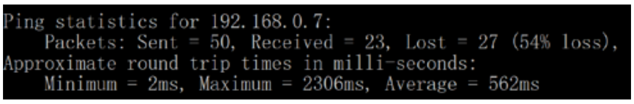
Figure 6: Unable to visit the FTP server

Finding. After the UDP flood attack is launched, as it is shown in the Figure 6, the visitor refreshes the webpage which offered by the FTP server and the webpage shows the connection has already been timed out. This phenomenon shows the communication between visitor and the FTP server may be blocked by the UDP flood. To ensure this, during the attack, the visitor also uses the ping command to verify the connection between the FTP server and itself. The Ping results and statistics are shown below in Figure 7 and 8.



```
Request timed out.
Request timed out.
Reply from 192.168.0.14: Destination host unreachable.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.0.7: bytes=32 time=1783ms TTL=64
Reply from 192.168.0.7: bytes=32 time=1930ms TTL=64
Request timed out.
Reply from 192.168.0.7: bytes=32 time=1387ms TTL=64
Reply from 192.168.0.7: bytes=32 time=18ms TTL=64
Reply from 192.168.0.7: bytes=32 time=2ms TTL=64
Reply from 192.168.0.7: bytes=32 time=3ms TTL=64
Reply from 192.168.0.7: bytes=32 time=2ms TTL=64
Reply from 192.168.0.7: bytes=32 time=2ms TTL=64
Reply from 192.168.0.7: bytes=32 time=3ms TTL=64
Reply from 192.168.0.7: bytes=32 time=3ms TTL=64
Reply from 192.168.0.7: bytes=32 time=6ms TTL=64
Reply from 192.168.0.7: bytes=32 time=4ms TTL=64
Reply from 192.168.0.7: bytes=32 time=4ms TTL=64
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.0.14: Destination host unreachable.
Reply from 192.168.0.14: Destination host unreachable.
Reply from 192.168.0.14: Destination host unreachable.
Request timed out.
Reply from 192.168.0.14: Destination host unreachable.
Reply from 192.168.0.14: Destination host unreachable.
Reply from 192.168.0.14: Destination host unreachable.
Reply from 192.168.0.14: Destination host unreachable.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.0.7: bytes=32 time=989ms TTL=64
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.0.7: bytes=32 time=2306ms TTL=64
Request timed out.
Request timed out.
```

Figure 7: Status of the Ping Command



```
Ping statistics for 192.168.0.7:
    Packets: Sent = 50, Received = 23, Lost = 27 (54% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2306ms, Average = 562ms
```

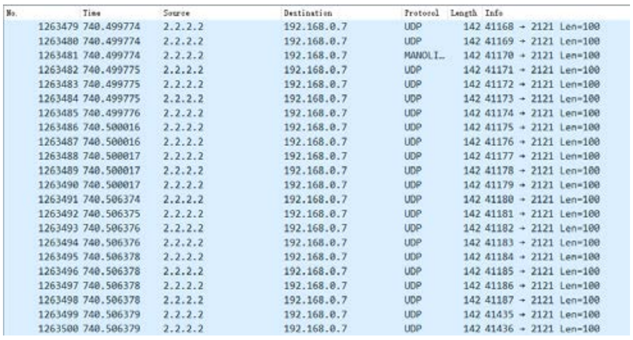
Figure 8: The Ping statistics

Finding. According to Figure 7, in contrast to the initial ping status before UDP flood attack, several different statuses appeared, which includes “Request timed out” and “destination host unreachable”. Figure 8 also reveals that the average response time sharply increases to 562ms rather than 34ms at the beginning. Meanwhile, 54% packets loss happens. These evidence fully proved that the attack is effective and successful. The connection between users and server has been obscured by the attack. In this set of experiments, the size of packets sent by the attacker varies, including 100 bytes, 600 bytes and 1100 bytes. Table III shows the statistics of different packet size according to two criteria: average response time and package loss percentage.

Table III. Experiment Results for DoS Attack Using Hping3 with Different Size of Packets.

Packet size	**Average response time**	**Package loss percentage**
100 bytes	506ms	48%
600 bytes	562ms	54%
1100 bytes	1539ms	48%

Finding. In Table III, although the Package loss Percentage almost remains the same when the packet size increases, the average response time also increase along with the packet size. Thus, the response time is proportional to the packet size, which implies that the attack with lager packet size will be more effective.



```
No.      Time       Source    Destination   Protocol Length Info
 1263479 740.499774 2.2.2.2   192.168.0.7   UDP         142 41168 → 2121 Len=100
 1263480 740.499774 2.2.2.2   192.168.0.7   UDP         142 41169 → 2121 Len=100
 1263481 740.499774 2.2.2.2   192.168.0.7   MANOLI…     142 41170 → 2121 Len=100
 1263482 740.499775 2.2.2.2   192.168.0.7   UDP         142 41171 → 2121 Len=100
 1263483 740.499775 2.2.2.2   192.168.0.7   UDP         142 41172 → 2121 Len=100
 1263484 740.499775 2.2.2.2   192.168.0.7   UDP         142 41173 → 2121 Len=100
 1263485 740.499776 2.2.2.2   192.168.0.7   UDP         142 41174 → 2121 Len=100
 1263486 740.500016 2.2.2.2   192.168.0.7   UDP         142 41175 → 2121 Len=100
 1263487 740.500016 2.2.2.2   192.168.0.7   UDP         142 41176 → 2121 Len=100
 1263488 740.500017 2.2.2.2   192.168.0.7   UDP         142 41177 → 2121 Len=100
 1263489 740.500017 2.2.2.2   192.168.0.7   UDP         142 41178 → 2121 Len=100
 1263490 740.500017 2.2.2.2   192.168.0.7   UDP         142 41179 → 2121 Len=100
 1263491 740.506374 2.2.2.2   192.168.0.7   UDP         142 41180 → 2121 Len=100
 1263492 740.506375 2.2.2.2   192.168.0.7   UDP         142 41181 → 2121 Len=100
 1263493 740.506376 2.2.2.2   192.168.0.7   UDP         142 41182 → 2121 Len=100
 1263494 740.506376 2.2.2.2   192.168.0.7   UDP         142 41183 → 2121 Len=100
 1263495 740.506378 2.2.2.2   192.168.0.7   UDP         142 41184 → 2121 Len=100
 1263496 740.506378 2.2.2.2   192.168.0.7   UDP         142 41185 → 2121 Len=100
 1263497 740.506378 2.2.2.2   192.168.0.7   UDP         142 41186 → 2121 Len=100
 1263498 740.506378 2.2.2.2   192.168.0.7   UDP         142 41187 → 2121 Len=100
 1263499 740.506379 2.2.2.2   192.168.0.7   UDP         142 41435 → 2121 Len=100
 1263500 740.506379 2.2.2.2   192.168.0.7   UDP         142 41436 → 2121 Len=100
```

Figure 9: The experiment in Wireshark

In figure 9, it is easy to find that the source IP address is 2.2.2.2 which is spoofed. Thus, it can be concluded that the attacker successfully camouflage itself through a fake IP address to launch an UPD flood attack.

IV. CONCLUSION

In this paper, a FTP server is set up as a target under attack. A DoS attack with UDP flood is launched by using Kali Linux. The connection states between the visitor and FTP server before and during the attack are shown in the experiment results. Moreover, the results imply that the attack with larger packet size is more effective.

In further study, the method for defending such DoS attack will be discussed and the and the defense effect will also be analyzed.

V. REFERENCES

[1] W. Liu, "Research on DoS Attack and Detection Programming," *2009 Third International Symposium on Intelligent Information Technology Application*, Shanghai, 2009, pp. 207-210.

[2] A. Singh, D Junefa, "Agent Based Preventive Measure for UDP Flood Attack in DDoS Attacks", *IJEST*, vol. 2, no. 8, pp. 3405-3411, 2010.

[3] S. Alanazi, J. Al-Muhtadi, A. Derhab, and K. Saleem, "On resilience of Wireless Mesh routing protocol against DoS attacks in IoT-based ambient assisted living applications," in International Conference on EHealth Networking, Application & Services, 2015.

[4] L. Allen et al., Kali Linux- Assuring Security by Penetration Testing. Mumbai,Birmingham: Packt Publishing, 2014.

[5] L. Liang, K. Zheng, Q. Sheng and X. Huang, "A Denial of Service Attack Method for an IoT System," *2016 8th International Conference on Information Technology in Medicine and Education (ITME)*, Fuzhou, 2016, pp. 360-364.