

LAB REPORT 5

INTRODUCTION : The Dynamic DDoS Mitigation(DDM) system extends a standard Content Delivery Network(CDN) network with the ability to scale up and down upon the system status. The steps involved is setting up a standard CDN. We then configure several HTTP Reverse Proxy Server to cache the victim's website and then configure DDM DNS server to have 2 domain names pointing to victim and reverse proxy servers. Now we implement DDM with CDN. Passwordless SSH from DDM DNS server to HTTP Reverse Proxy servers(vms) and vm host machines is configured. By setting up the pssh command and modifying ddm.py scripts. We then launch a DDoS attack and add the DDM DNS server's IP to the Bots vms. Next we launch a DDoS attack on the victim's domain and explore the effects of the DDM system.

QUESTIONS :

1. Can this system withstand a DDoS attack? Why or why not?

Ans. The Dynamic DDoS mitigation system can withstand a DDoS attack due to it's multi module architecture. The web server is protected by many web caches. The load is also shared amongst Multiple web caches which are all located in different places. This decreases the blow when there is a sudden DDoS attack. But again there is a limit to how much load the system can take.

2. In what cases would you use a DDM system? Why do you think it's worth it in that case?

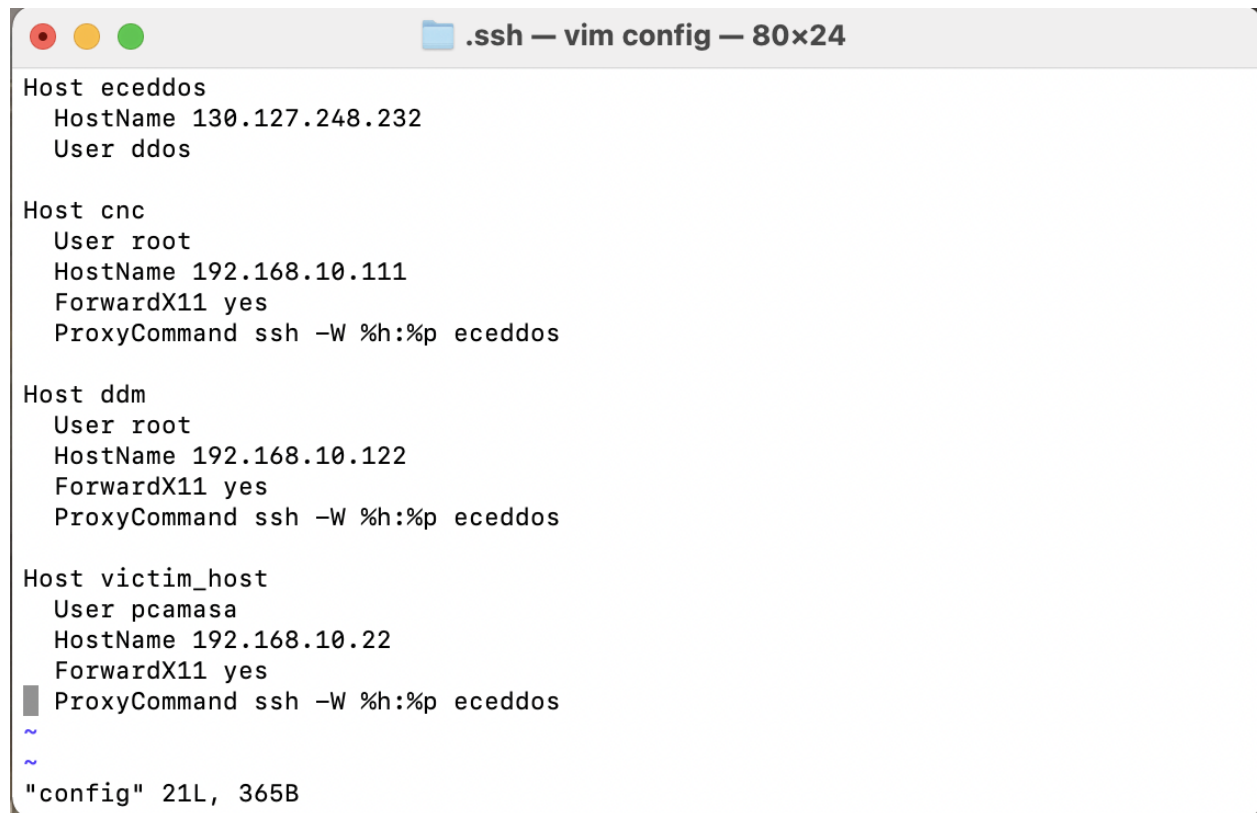
Ans. As the DDM system is really good in distributing its load over multiple servers I would imagine it to be really useful in cloud services as they usually are attacked frequently by adding a lot of traffic. Also client based companies which have access to users information through web services will find this attack system useful.

3. Discuss what would you change if you were to implement this system on the Internet?

Ans. Probably the number of proxys/servers. This is just an implementation on our system which is why such a low number of servers were sufficient. But if the same system is to be implemented on the internet, the incoming traffic would be much more and damaging to the system. In order to withstand this, I would add more number of proxys or servers if possible.

SETUP : The machines used in this lab are the CNC machine: 192.168.10.111, bots machine with IP Addresses 192.168.10.109, 192.168.10.107 and 192.168.10.150, victim machine: 192.168.10.112, DDM DNS machine: 192.168.10.122, HTTP Reverse Proxy machines: 192.168.10.102 hosted at 192.168.10.20, 192.168.10.105 hosted at 192.168.10.21, and 192.168.10.121 hosted at 192.168.10.19.

The first step that I did was to construct the config file in ssh folder as shown below.

A screenshot of a terminal window titled ".ssh — vim config — 80x24". The window displays the contents of an SSH configuration file. The configuration includes four host entries: 'eceddos', 'cnc', 'ddm', and 'victim_host'. Each entry specifies a user, host name, and proxy command. The 'cnc' and 'ddm' entries also specify 'ForwardX11 yes'. The status bar at the bottom indicates the file is 21 lines long and 365 bytes in size.

```
Host eceddos
  HostName 130.127.248.232
  User ddos

Host cnc
  User root
  HostName 192.168.10.111
  ForwardX11 yes
  ProxyCommand ssh -W %h:%p eceddos

Host ddm
  User root
  HostName 192.168.10.122
  ForwardX11 yes
  ProxyCommand ssh -W %h:%p eceddos

Host victim_host
  User pcamasa
  HostName 192.168.10.22
  ForwardX11 yes
  ProxyCommand ssh -W %h:%p eceddos

~
~
"config" 21L, 365B
```

Next I logged into the CNC machine and in the lab 4 folder and started monitoring the webpage response time using the command :

```
# ./ping_web.sh http://edge.ddm.lan
```

This gave me the below response time as a result

```

[root@cnc:~/DDoS_Lab4# ./ping_web.sh http://edge.ddm.lan
Total webpage load time: 0.013
Total webpage load time: 0.013
Total webpage load time: 0.012
Total webpage load time: 0.012
Total webpage load time: 0.012
Total webpage load time: 0.012
Total webpage load time: 0.012
Total webpage load time: 0.012
Total webpage load time: 0.012
Total webpage load time: 0.012
Total webpage load time: 0.013
Total webpage load time: 0.012
Total webpage load time: 0.013
Total webpage load time: 0.012
Total webpage load time: 0.012
Total webpage load time: 0.012
Total webpage load time: 0.012
Total webpage load time: 0.013
Total webpage load time: 0.012
Total webpage load time: 0.012

```

At the same time I started another terminal and logged into the ddm machine in order to run the ddm.py file which has the following changes made.

```

pranitac — root@localhost:~ — ssh < ssh ddm — 80x24

__email__ = "xingsiz@g.clemson.edu"
__license__ = "MIT"
__updated__ = '2018-04-20'

import socket          # Validate IP format
import subprocess      # Execute bash command
import time            # Update DNS zone file serial number
import requests        # Check HTTP request timeout

host_username = 'ddm'      # This is the user name on the host machines with r
everse proxy virtual machine pre-configured
guest_username = 'root'    # This is the user name on the reverse proxy virtual
machine
hosts_file = 'hosts.txt'  # All IPs of the host machines that runs reverse proxy
virtual machines. One IP per line?~Lno punctuations needed.
domain = 'ddm.lan'        # The base domain of the mitigation system. The reso
lved domain will be "edge.ddm.lan"
zone_file = '/etc/named/zones/db.ddm.lan' # Zone file path
minimum_proxies = 1       # If available number of reverse proxy virtual machi
ne is less than this value, start more VMs
@

```

32,1 15%

Now in ddm machine I executed the file using the command # python3.6 ddm.py as below

```
[[root@localhost ~]# python3.6 ddm.py
pssh -l ddm -h temp_hosts -t 15 -P 'vboxmanage guestproperty enumerate CentOS7 |
grep V4/IP' | grep V4/IP | awk '{print substr($5,1, length($5)-1)}'
b'192.168.10.121\n'
1 proxy servers on line.
pssh -l ddm -h temp_hosts -t 15 -P 'vboxmanage guestproperty enumerate CentOS7 |
grep V4/IP' | grep V4/IP | awk '{print substr($5,1, length($5)-1)}'
b'192.168.10.121\n'
1 proxy servers on line.
pssh -l ddm -h temp_hosts -t 15 -P 'vboxmanage guestproperty enumerate CentOS7 |
grep V4/IP' | grep V4/IP | awk '{print substr($5,1, length($5)-1)}'
b'192.168.10.121\n'
1 proxy servers on line.
```

Once the file starts running I opened another cnc terminal and implemented a Flood DDoS attack using the below command. Before doing this I made sure that the newbot.txt has the bot machine IP address.

```
# pssh -h newbot.txt -t30 'sleep 1; hping3 --udp -d 10000 -p 80 --flood edge.ddm.lan
& sleep 10; pkill hping3'
```

This gave me the result as SUCCESS for all the three machines.

```
[root@cnc:~/LAB4# pssh -h newbot.txt -P -t30 'sleep 1; hping3 --udp -d 10000 -p 80
--flood edge.ddm.lan & sleep 10; pkill hping3'
192.168.10.109: HPING edge.ddm.lan (eth0 192.168.10.121): udp mode set, 28 heade
rs + 10000 data bytes
[1] 15:13:26 [SUCCESS] 192.168.10.109
[2] 15:13:26 [SUCCESS] 192.168.10.107
[3] 15:13:26 [SUCCESS] 192.168.10.150
root@cnc:~/LAB4#
```

As the attack was launched I could see the response time suddenly jumping to 1.482 and then gradually coming down back.

```
Total webpage load time: 0.014
Total webpage load time: 0.020
Total webpage load time: 0.015
Total webpage load time: 0.015
Total webpage load time: 0.013
Total webpage load time: 1.482
Total webpage load time: 0.284
Total webpage load time: 0.345
Total webpage load time: 0.076
Total webpage load time: 0.103
Total webpage load time: 0.076
Total webpage load time: 0.066
Total webpage load time: 0.067
Total webpage load time: 0.065
Total webpage load time: 0.068
Total webpage load time: 0.067
Total webpage load time: 0.065
Total webpage load time: 0.065
Total webpage load time: 0.067
Total webpage load time: 0.067
Total webpage load time: 0.065
Total webpage load time: 0.070
Total webpage load time: 0.068
```

Now I went on to check if the proxy machines were running appropriately with the command

```
# pssh -l ddm -h hosts.txt -P 'hostname'
```

I got the result as success which means all the proxy servers are up and running.

```
[[root@localhost ~]# pssh -l ddm -h hosts.txt -P 'hostname'
192.168.10.20: clemson20.seclab.lan
[1] 15:44:18 [SUCCESS] 192.168.10.20
192.168.10.21: clemson21.seclab.lan
192.168.10.19: clemson19.seclab.lan
[2] 15:44:18 [SUCCESS] 192.168.10.21
[3] 15:44:18 [SUCCESS] 192.168.10.19
[root@localhost ~]#
```

The next step is to turn the machine on and turn it off. In order to turn the machine on, I used the command

```
# pssh -l username -h hosts.txt -P 'vboxmanage startvm CentOS --type headless'
```

And to turn them off, I used the command

```
# pssh -l username -h hosts.txt -P 'vboxmanage controlvm CentOS poweroff'
```


Once that is done, I implemented the ddos attack on the victim machine, I went to the cnc machine and launched the command

```
# pssh -h newbot.txt -t30 'sleep 1; hping3 --udp -d 10000 -p 80 --flood www.victim.lan & sleep 10; pkill hping3'
```

```
root@cnc:~/LAB4# pssh -h newbot.txt -P -t30 'sleep 1; hping3 --udp -d 10000 -p 80 --flood www.victim.lan & sleep 10; pkill hping3'
[1] 15:46:33 [SUCCESS] 192.168.10.109
[2] 15:46:33 [SUCCESS] 192.168.10.107
192.168.10.150: HPING www.victim.lan (eth0 192.168.10.112): udp mode set, 28 headers + 10000 data bytes
[3] 15:46:33 [SUCCESS] 192.168.10.150
root@cnc:~/LAB4#
```

When I looked at the response time one thing I observed was as compared to the other attack where the time jumped suddenly by a large value, I saw that the time started to gradually increase slowly. This is because in my opinion when the reverse proxy takes on the load and the victim is not overwhelmed with traffic.

```
^Z
[2]+  Stopped                  ./ping_web.sh http://edge.ddm.lan
root@cnc:~/LAB4# ./ping_web.sh http://www.victim.lan
Total webpage load time: 0.090
Total webpage load time: 0.062
Total webpage load time: 0.085
Total webpage load time: 0.075
Total webpage load time: 0.079
Total webpage load time: 0.083
Total webpage load time: 0.105
Total webpage load time: 0.130
Total webpage load time: 0.164
Total webpage load time: 0.113
Total webpage load time: 0.101
Total webpage load time: 0.129
Total webpage load time: 0.075
Total webpage load time: 0.087
Total webpage load time: 0.067
Total webpage load time: 0.078
Total webpage load time: 0.073
Total webpage load time: 0.067
Total webpage load time: 0.091
Total webpage load time: 0.084
Total webpage load time: 0.071
```