Table of Contents

ECE 8930 Lab 7 DDoS Mitigation

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.

For this lab, you will first build a standard CDN and then add the scaling capability to it. By the end of chapter "DNS Server", you should have a working CDN network with 3 HTTP reverse proxy servers with caching enabled. The reverse proxies will take the load and not redirect duplicated queries to the victim. The DNS server distributes the load to all caching nodes with round robin. The DDM controller adds more reverse proxies to the system under heavy load and reduces the number of proxies nodes under light load.

This system needs several machines to run. We have limited number of machines, so the students on each campus need to work as a team.

The code used in lab is a simplified version based on Ilker's research. Here is a link to Ilker's original implementation: https://www.dropbox.com/s/bdxo0fau8nr0073/MitigationSystemInstructions.pdf?dl=0

Lab Setup

Charleston:
Available Hosts: 192.168.10.8~11, 13

Clemson:
Available Hosts: 192.168.10.9~12, 16, 18~22

DoS Bot Virtual Machines:
192.168.10.36, 38~41

DDM Mitigation System Example Setup:

- Hardware:

    - Host Machine x 5
- Victual machines:
    - DDM DNS Server (CentOS) x 1
    - HTTP Reverse Proxy Server (CentOS) x 3
    - Victim HTTP Server (Metasploitable2) x 1

The following IPs and domains are used in this guide.
Please replace them with your settings while implementing.

```
DDM DNS Server VM IP: 192.168.10.130
DDM DNS Server Host IP: 192.168.10.10

HTTP Reverse Proxy Server1 VM IP: 192.168.10.131
HTTP Reverse Proxy Server1 Host IP: 192.168.10.11

HTTP Reverse Proxy Server2 VM IP: 192.168.10.132
HTTP Reverse Proxy Server2 Host IP: 192.168.10.12

HTTP Reverse Proxy Server3 VM IP: 192.168.10.133
HTTP Reverse Proxy Server3 Host IP: 192.168.10.15

Victim HTTP Server VM IP: 192.168.10.88
Victim VM Host IP: 192.168.10.8



HTTP Reverse Proxy Server domain: edge.ddm.lan
Victim HTTP Server domain: www.victim.lan
```

VM Images for Mitigation System:

CentOS VM

CentOS7.ova in VMs/ folder

Credential: root root

Victim website VM:

Metasploitable2.ova in VMs/ folder

Credential: msfadmin msfadmin

CnC VM:

Kali_DDoS_CnC.ova in VMs/ folder

Credential: root private123

Method:

The DDM DNS Server holds a list of available hosts. It checks the availability of the HTTP Reverse Proxy Server. If less than two HTTP Reverse Proxy Server is accessible, the DDM DNS Server send commands to the available hosts, start more HTTP Reverse Proxy Servers and update DNS records and vise versa.

Each team need to:

Step 1. Setup a standard CDN

Import the Metasploitable2.ova and create a victim website.

Import the CentOS7.ova on four of the assigned hosts.

Configure three HTTP Reverse Proxy Servers to cache victim's website.

Configure the DDM DNS server as a regular DNS server with two domains. One for the victim, one for the reverse proxy servers.

Step 2. Implement the DDM with CDN

Setup password-less ssh login from the DDM DNS server to the hosts that will run the HTTP reverse proxy server. (This will be used to start reverse proxy server VM)

Setup password-less ssh login from the DDM DNS server to the HTTP reverse proxy servers. (This will be used to shut down the VMs.)

Setup and test pssh command to start and stop VMs in a batch from the DDM DNS server.

Modify and execute the ddm.py scripts.

Add the DDM DNS server's IP to the bots' /etc/resolve.conf file.

DDoS the reverse proxy servers' domain.

CentOS VM

Import VM

- Execute the following commands on the **host machine**:

```
$ vboxmanage import CentOS7.ova
$ vboxmanage startvm CentOS --type headless
```

Check VM's IP

- Execute the following commands on the **host machine**:

It takes about one to two minutes since boot until the VM gets an IP with DHCP:

```
$ vboxmanage guestproperty enumerate CentOS | grep V4/IP
```

SSH Password-less Login to Other Hosts

- Execute the following commands on the **virtual machine**:

You will need ssh passwordless login from the CentOS DNS server to all other host machines. This will save a lot time in the following setup. Also, you will need pssh to execute ssh command on multiple machines at once. It will be a lot easier to use pssh with ssh passwordless login.

```
# ssh-keygen
# ssh-copy-id -i ~/.ssh/id_rsa.pub username@192.168.10.X
# ssh username@192.168.10.X
```

Metasploitable2 VM

Import VM

- Execute the following commands on a **host machine**:

```
$ vboxmanage import Metasploitable2.ova
$ vboxmanage startvm Metasploitable2 --type headless
```

To get the IP of Metasploitable2, you could ssh -X to the host machine and run virtualbox. Or nmap the network and find new HTTP servers. **It would be better to setup static IP after login.**

Test Website

- Execute the following commands on any machine:

```
$ curl http://192.168.10.88
```

And you will get:

```
<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>


                _                  _       _ _        _     _
   ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | _
__|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/
_ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |
__// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\_
__|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></li>
<li><a href="/dav/">WebDAV</a></li>
</ul>
</body>
</html>
```

Configure HTTP Reverse Proxy Server with Caching Using CentOS VM.

Install http on CentOS VM

```
#yum install httpd
```

Enable http/https on firewall

- Execute the following commands on the **virtual machine**:

```
# firewall-cmd --permanent --zone=public --add-service=http
# firewall-cmd --permanent --zone=public --add-service=https
# firewall-cmd --reload
# firewall-cmd --list-all
```

Add reverse http proxy with caching

- Execute the following commands on the **virtual machine**:

Creat and edit file /etc/httpd/conf.d/default-site.conf

```
<VirtualHost *:80>
    ProxyPreserveHost On

    ProxyPass / http://192.168.10.88/
    ProxyPassReverse / http://192.168.10.88/

    CacheQuickHandler off

    CacheLock on
    CacheLockPath /tmp/mod_cache-lock
    CacheLockMaxAge 5

    CacheIgnoreHeaders Set-Cookie

    <Location />
        CacheEnable disk
        CacheHeader on

        CacheDefaultExpire 600
        CacheMaxExpire 86400
        CacheLastModifiedFactor 0.5

        ExpiresActive on
        ExpiresDefault "access plus 5 minutes"

        Header merge Cache-Control public
        FileETag All
    </Location>
</VirtualHost>
```

Enable Cache:

```
# mkdir -p /etc/systemd/system/httpd.service.requires
# ln -s /usr/lib/systemd/system/htcacheclean.service /etc/system
d/system/httpd.service.requires
```

Edit and add the following lines to file /etc/httpd/conf/httpd.conf

```
CacheRoot /var/cache/httpd/proxy
CacheDirLevels 2
CacheDirLength 1
```

Check Apache config:

Run the following command to test the cache server:

```
# apachectl configtest
AH00558: httpd: Could not reliably determine the server's fully
qualified domain name, using localhost.localdomain. Set the 'Ser
verName' directive globally to suppress this message
Syntax OK
```

Restart server:

```
# systemctl restart httpd
```

Test the reverse http proxy

```
$ curl http://192.168.10.131
```

You should get the same output:

```
<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>


                _                  _       _ _        _     _
   ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | _
__|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/
_ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |
__// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\_
__|_____|
                           |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></li>
<li><a href="/dav/">WebDAV</a></li>
</ul>
</body>
</html>
```

At the same time, run tshark on the host of the victim machine, you will see that the reverse proxy are not redirect every query to the victim's website.

Configure DNS Server Using CentOS VM.

- Execute the following commands on the **virtual machine**:

In this example we run the DNS server on 192.168.10.130. We create two domains "ddm.lan" and "victim.lan", and subdomains "edge.ddm.lan" and "www.victim.lan"

Install name on DNS Server VM

```
# yum install bind bind-utils -y
```

Configure firewall:

```
# firewall-cmd --zone=public --permanent --add-service=dns
# firewall-cmd --reload
# firewall-cmd --list-all
```

Config DNS query permission

Edit /etc/named.conf
Modify the following three lines in the option{}

```
listen-on port 53 { any; };
listen-on-v6 port 53 { any; };
allow-query { any; };
```

Enable DNS:

```
# systemctl enable named
# systemctl start named
```

Add zone

Edit /etc/named.conf, and add the following line at the end of the file:

```
include "/etc/named/named.conf.local";
```

Create and edit /etc/named/named.conf.local
Here we use ddm.lan and victim.lan as examples. You need to modify the domains to something else

```
zone "ddm.lan" {
        type master;
        file "/etc/named/zones/db.ddm.lan";
};

zone "victim.lan" {
        type master;
        file "/etc/named/zones/db.victim.lan";
};
```

Create the following directory and files and check the configuration

```
# mkdir /etc/named/zones/
# touch /etc/named/zones/db.ddm.lan
# touch /etc/named/zones/db.victim.lan
# named-checkconf
```

If "named-checkconf" returns nothing you should be good.

Edit zone file

Edit file /etc/named/zones/db.ddm.lan

```
$TTL    1200
@   IN  SOA ns.ddm.lan.    admin.ddm.lan. (
        1523759211   ; Serial
        120         ; Refresh
        180         ; Retry
        7200        ; Expire
        300         ; Negative Cache TTL
)

        IN  NS  ns.ddm.lan.     ; define name server - NS record
        IN  A   192.168.10.130  ; define name server's IP addres
s - A record
ns      IN  A   192.168.10.130  ; define IP address of a hostnam
e - A record

edge    IN  A   192.168.10.131  ; IP of reverse proxy server1
        IN  A   192.168.10.132  ; IP of reverse proxy server2
```

Check the file by:

```
named-checkzone ddm.lan /etc/named/zones/db.ddm.lan
```

Edit file /etc/named/zones/db.victim.lan

```
$TTL    1200
@   IN  SOA ns.victim.lan.    admin.victim.lan. (
        1523759211   ; Serial
        120         ; Refresh
        180         ; Retry
        7200        ; Expire
        300         ; Negative Cache TTL
)

        IN  NS  ns.victim.lan.  ; define name server - NS record
        IN  A   192.168.10.130  ; define name server's IP addres
s - A record
ns      IN  A   192.168.10.130  ; define IP address of a hostnam
e - A record

www     IN  A   192.168.10.88   ; IP of the victim website www.v
ictim.lan
```

Check the file by:

```
named-checkzone victim.lan /etc/named/zones/db.victim.lan
```

If no error returned, reload the named:

```
systemctl reload named
```

Test DNS

Add the DNS server IP to /etc/resolv.conf on your DDoS cnc VM so that you can visit both domains.

```
nameserver 192.168.10.130
```

Now you should be able to visit both the www.victim.lan and the edge.ddm.lan:

```
# curl http://edge.ddm.lan
```

And you should get:

```
<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>


                _                  _       _ _        _     _
   ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | _
__|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/
_ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |
__// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\_
__|_____|
                           |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></li>
<li><a href="/dav/">WebDAV</a></li>
</ul>
</body>
</html>
```

Setup DDM System

First, make sure you have a working CDN and ssh password-less from the DNS server to all the hosts and VMs in the CDN.

pssh/pscp

- Execute the following commands on the DNS server **virtual machine**:

pssh will be used by the DDM system to control the start and stop of the VMs on the host machines.

pssh executes ssh commands in parallel. pscp executes scp in paralle.

General usage:

First create a file contains target IPs. In the example setup, the hosts.txt should be:

```
192.168.10.11
192.168.10.12
192.168.10.15
```

Then test the pssh command:

```
[root@localhost ~]# pssh -l username -h hosts.txt -P 'hostname'
192.168.10.12: fulla.seclab.lan
[1] 16:08:22 [SUCCESS] 192.168.10.12
192.168.10.11: balour.seclab.lan
[2] 16:08:22 [SUCCESS] 192.168.10.11
192.168.10.15: fenrir.seclab.lan
[3] 16:08:22 [SUCCESS] 192.168.10.15
```

At this moment, you should have all reverse proxy servers setup. If you haven't turn them off, run the following command to turn them off:

```
[root@localhost ~]# pssh -l username -h hosts.txt -P 'vboxmanage
 controlvm CentOS poweroff'
[1] 16:15:50 [SUCCESS] 192.168.10.11
[2] 16:15:50 [SUCCESS] 192.168.10.12
[3] 16:15:51 [SUCCESS] 192.168.10.15
```

Now turn them on with:

```
[root@localhost ~]# pssh -l username -h hosts.txt -P 'vboxmanage
 startvm CentOS --type headless'
192.168.10.12: Waiting for VM "CentOS" to power on...
VM "CentOS" has been successfully started.
[1] 16:12:45 [SUCCESS] 192.168.10.12
192.168.10.15: Waiting for VM "CentOS" to power on...
VM "CentOS" has been successfully started.
[2] 16:12:45 [SUCCESS] 192.168.10.15
192.168.10.11: Waiting for VM "CentOS" to power on...
VM "CentOS" has been successfully started.
[3] 16:12:46 [SUCCESS] 192.168.10.11
```

Wait few minutes and run the following command to get the gust IP and its relative host IP:

```
[root@localhost ~]# pssh -l username -h hosts.txt  -t30 -P 'vbox
manage guestproperty enumerate CentOS | grep V4/IP' | grep V4/IP
 | awk '{print substr($5,1, length($5)-1),substr($1,1, length($1
)-1)}'
192.168.10.131 192.168.10.11
192.168.10.132 192.168.10.12
192.168.10.133 192.168.10.15
```

Create another file guests.txt and save the IPs of the guest and execute:

```
[root@localhost ~]# pssh -h guests.txt -P 'hostname'
192.168.10.131: localhost.localdomain
[1] 16:18:31 [SUCCESS] 192.168.10.131
192.168.10.132: localhost.localdomain
[2] 16:18:31 [SUCCESS] 192.168.10.132
192.168.10.133: localhost.localdomain
[3] 16:18:31 [SUCCESS] 192.168.10.133
```

With all above test successful, you can move on to next step. You can leave the VMs on or off that does not matter, the script can start from any status.

ddm.py

Before running the script, make sure the DNS server and the above pssh commands are tested and running properly.

Download the ddm.py script to the DNS server from the following link: https://github.com/sonusz/dynamic-cdn/blob/master/ddm.py

Edit the ddm.py script and modify the following lines according to your need:

```
host_username = 't1'        # This is the user name on the host machines with reverse 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，no punctuations needed.
domain = 'ddm.lan'          # The base domain of the mitigation system. The resolved domain will be "edge.ddm.lan"
zone_file = '/etc/named/zones/db.ddm.lan'   # Zone file path
minimum_proxies = 2         # If available number of reverse proxy virtual machine is less than this value, start more VMs
maximum_proxies = 2         # If available number of reverse proxy virtual machine is more than this value, stop one VM
```

The ddm.py automates the above tested pssh commands and controls the CDN you previously built. It checks the overall availability using "curl get" to each of the running reverse proxy nodes and decide whether to add more reverse proxy node or turn off some nodes.

To run the script:

```
[root@localhost ~]# python3.6 ddm.py
```

To stop the script: Hit Ctr + C

There will be some of the edge VMs still running and some turned off when stopped the script. You can restart the script if needed and no need to start or stop all edge nodes before restart.

At the end of your expireemnt, it is better to turn all edge VMs off.

Questions:

1, Can your system withstand a DDoS? Why or why not?

2, There is at least one security flaw in the DNS set up in this tutorial, what is it?

3, What do you need to change if you need to implement this system on the Internet?