CSCI4113
LAB6 Notes

Milan Formanek

April 22, 2019

1. Configuring IPtables firewall settings for the DM network

For this lab the DunderMifflin network gets it's firewalls configured. Each of the machines A through F have to have unique IPtables rules based on their uses and running services. To make the deployment easy a .sh script is created, grabbed from github and run with the right parameters for each machine.

2. Configuring Machine B and F - Web Servers

Machines B and F have identical configuration allowing http and https traffic incoming from any ip along with local loopback, icmp traffic and ssh from the local networks. This is done by deploying the LAB6.sh script to the machine with arguments B and F:

```
[root@carriage ~]# wget https://raw.githubusercontent.com/mformanek/Linux-Sys-Admin---LAB6/master/LAB6.sh
                    --2019-04-21 23:20:09--  https://raw.githubusercontent.com/mformanek/Linux-Sys-Admin---LAB6/
     master/LAB6.sh
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 151.101.68.133
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|151.101.68.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 6233 (6.1K) [text/plain]
Saving to: 'LAB6.'sh
100%[=======================================================================================>] 6,233       --.-K/s   in 0s
2019-04-21 23:20:09 (29.4 MB/s) - 'LAB6.'sh saved [6233/6233]
[root@carriage ~]# bash ./LAB6.sh B
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
```

```
[root@saddle ~]# wget https://raw.githubusercontent.com/mformanek/Linux-Sys-Admin---LAB6/master/LAB6.sh
--2019-04-21 23:25:59--  https://raw.githubusercontent.com/mformanek/Linux-Sys-Admin---LAB6/master/LAB6.sh
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 151.101.68.133
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|151.101.68.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 6233 (6.1K) [text/plain]
Saving to: 'LAB6.'sh
100%[=======================================================================================>] 6,233       --.-K/s   in 0s
2019-04-21 23:25:59 (22.9 MB/s) - 'LAB6.'sh saved [6233/6233]
[root@saddle ~]# bash ./LAB6.sh F
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
```

3. Configuring Machine C - FTP Server

Machine C allows FTP connections from the 100.64.0/16 subnet along with local loopback, icmp traffic, DNS requests from Machine D, http and https outbound traffic and ssh from the local networks. This is done by deploying the LAB6.sh script to the machine with argument C:

```
[root@platen ~]# wget https://raw.githubusercontent.com/mformanek/Linux-Sys-Admin---LAB6/master/LAB6.sh
--2019-04-22 00:32:11--  https://raw.githubusercontent.com/mformanek/Linux-Sys-Admin---LAB6/master/LAB6.sh
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 151.101.68.133
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|151.101.68.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 6233 (6.1K) [text/plain]
Saving to: ‘LAB6.’sh
100%[=====================================================================>] 6,233       --.-K/s   in 0s
2019-04-22 00:32:11 (26.6 MB/s) - ‘LAB6.’sh saved [6233/6233]
[root@platen ~]# bash ./LAB6.sh C
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
```

4. Configuring Machine D - DNS Server

Machine D allows DNS queries from any source along with local loopback, icmp traffic and ssh from the local networks. This is done by deploying the LAB6.sh script to the machine with argument D:

```
[root@chase ~]# wget https://raw.githubusercontent.com/mformanek/Linux-Sys-Admin---LAB6/master/LAB6.sh
--2019-04-21 23:32:30--  https://raw.githubusercontent.com/mformanek/Linux-Sys-Admin---LAB6/master/LAB6.sh
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 151.101.68.133
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|151.101.68.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 6233 (6.1K) [text/plain]
Saving to: ‘LAB6.’sh

100%[=====================================================>] 6,233       --.-K/s   in 0s

2019-04-21 23:32:30 (25.0 MB/s) - ‘LAB6.’sh saved [6233/6233]

[root@chase ~]# bash ./LAB6.sh D
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
```

5. Configuring Machine E - File Server

Machine E allows for Samba connections from the 10.21.32.0/24 subnet along with local loopback, icmp traffic and ssh from the same subnet. This is done by deploying the LAB6.sh script to the machine with argument E:

```
[root@roller ~]# wget https://raw.githubusercontent.com/mformanek/Linux-Sys-Admin---LAB6/master/LAB6.sh
--2019-04-21 23:47:44--  https://raw.githubusercontent.com/mformanek/Linux-Sys-Admin---LAB6/master/LAB6.sh
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 151.101.68.133
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|151.101.68.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 6233 (6.1K) [text/plain]
Saving to: ‘LAB6.’sh

100%[=====================================================================>] 6,233       --.-K/s   in 0s
2019-04-21 23:47:44 (22.5 MB/s) - ‘LAB6.’sh saved [6233/6233]
[root@roller ~]# bash ./LAB6.sh E
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
```

6. Configuring Machine A - Router

Finally the most complicated one, Machine A. It has to forward packets to the other computers in the DM network. It also mirrors the firewall settings on the individual machines in order to provide an extra layer of security on the network. Rules to block Facebook.com,icanhas.cheezburger.com and cheezburger.com are also implemented here. Icanhas.cheezburger.com and cheezburger.com have the same IP making life a little easier.

```
[root@router ~]# wget https://raw.githubusercontent.com/mformanek/Linux-Sys-Admin---LAB6/master/LAB6.sh
--2019-04-22 18:36:56--  https://raw.githubusercontent.com/mformanek/Linux-Sys-Admin---LAB6/master/LAB6.sh
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 151.101.68.133
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|151.101.68.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 6136 (6.0K) [text/plain]
Saving to: ‘LAB6.’sh
100%[=============================================================================================================>]
      6,136       --.-K/s   in 0s
2019-04-22 18:36:56 (19.2 MB/s) - ‘LAB6.’sh saved [6136/6136]
[root@router ~]# bash ./LAB6.sh A
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
```

7. LAB6.sh - Deployment Script

```
#!/bin/bash
# ------------------------------------------------------------------
# By Milan Formanek   LAB6 Deployment Script
# ------------------------------------------------------------------
VERSION=0.1.0
SUBJECT=some-unique-id
USAGE="Run on the individual DM machines with the letter name of the machine as the parameter."

if [ $# == 0 ] ; then
    echo $USAGE
    exit 1;
fi

if [ $1 == "OFF" ] ; then #ENABLE EVERITHING IN IPTABLES for testing
    iptables -P INPUT ACCEPT
    iptables -P FORWARD ACCEPT
    iptables -P OUTPUT ACCEPT
    iptables -F #reset IPTABLES
    service iptables save # make sure to save rules!!!
    exit 1;
fi

iptables -F #reset IPTABLES

iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT #Allow return packets for ESTABLISHED and
     RELATED packets

iptables -P INPUT DROP # set default DROP policy
iptables -P OUTPUT ACCEPT

iptables -A INPUT -i lo -j ACCEPT  #Allow loopback traffic
iptables -A OUTPUT -o lo -j ACCEPT

iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT
iptables -A INPUT -p icmp --icmp-type time-exceeded -j ACCEPT
iptables -A INPUT -p icmp --icmp-type destination-unreachable -j ACCEPT #ACCEPT ICMP packets.

if [ $1 != "E" ] ; then
  iptables -A INPUT -p tcp -s  100.64.0.0/16 --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT
  iptables -A INPUT -p tcp -s  10.21.32.0/24 --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT
  iptables -A INPUT -p tcp -s  198.18.0.0/16 --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT
  iptables -A OUTPUT -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT
  #On all machines exlcuding E allow inbound ssh connections from the 100.64.0.0/16, 10.21.32.0/24, and 198.18.0.0/
      16 subnets
fi

if [ $1 != "A" ] ; then
```

```
47    iptables -P FORWARD DROP #disble forwarding on non routers
48  else #RULES FOR ROUTER/MACHINE A
49        iptables -P FORWARD DROP #enable forwarding on routers
50        iptables -A FORWARD -s 157.240.28.35 -j DROP
51        iptables -A FORWARD -d 157.240.28.35 -j DROP #block FACEBOOK
52        iptables -A FORWARD -s 216.176.177.74 -j DROP
53        iptables -A FORWARD -d 216.176.177.74 -j DROP #block CHEESEBURGER.com
54
55        iptables -A FORWARD -p tcp -s  100.64.0.0/16 --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT
56    iptables -A FORWARD -p tcp -s  10.21.32.0/24 --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT
57    iptables -A FORWARD -p tcp -s  198.18.0.0/16 --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT
58        iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT #FORWARD SSH
59
60    iptables -A FORWARD -p tcp --dport 80   -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
61    iptables -A FORWARD -p tcp --dport 443  -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
62
63    iptables -A FORWARD -p icmp --icmp-type echo-request -j ACCEPT
64    iptables -A FORWARD -p icmp --icmp-type echo-reply -j ACCEPT
65    iptables -A FORWARD -p icmp --icmp-type time-exceeded -j ACCEPT
66    iptables -A FORWARD -p icmp --icmp-type destination-unreachable -j ACCEPT #ACCEPT ICMP packets
67
68
69    iptables -A FORWARD -p udp --sport 1024:65535 --dport 53 -m state --state NEW,ESTABLISHED -j ACCEPT
70    iptables -A FORWARD -p udp --sport 53 --dport 1024:65535 -m state --state ESTABLISHED -j ACCEPT
71    iptables -A FORWARD -p udp --sport 53 --dport 53 -m state --state NEW,ESTABLISHED -j ACCEPT
72    iptables -A FORWARD -p udp --sport 53 --dport 53 -m state --state ESTABLISHED -j ACCEPT
73    #allow inbound DNS lookup on chase
74
75
76
77    iptables -A FORWARD -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT #Allow return packets for ESTABLISHED and
          RELATED packets
78
79
80  fi
81
82  if [ $1 == "B" ] || [ $1 == "F" ] ; then #RULES FOR MACHINE B AND F
83    iptables -A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
84    iptables -A INPUT -p tcp -m tcp --dport 443 -j ACCEPT #allow http and https inbound traffic
85  fi
86
87  if [ $1 == "C" ] ; then #RULES FOR MACHINE C
88    iptables -P OUTPUT DROP #defaul output drop
89
90    iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
91    iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT #allow related connections
92
93    iptables -A OUTPUT -p udp -d 100.64.21.4 --dport 53 -m state --state NEW,ESTABLISHED -j ACCEPT
94    iptables -A INPUT  -p udp -s 100.64.21.4 --sport 53 -m state --state ESTABLISHED     -j ACCEPT
95    iptables -A OUTPUT -p tcp -d 100.64.21.4 --dport 53 -m state --state NEW,ESTABLISHED -j ACCEPT
96    iptables -A INPUT  -p tcp -s 100.64.21.4 --sport 53 -m state --state ESTABLISHED     -j ACCEPT #allow DNS lookup
          on chase
97
98    iptables -A OUTPUT -p tcp -m tcp --dport 80 -j ACCEPT
99    iptables -A OUTPUT -p tcp -m tcp --dport 443 -j ACCEPT #allow outbound http and https traffic
100
101   iptables -A OUTPUT -p tcp --dport 22 -j ACCEPT #allow outgoing ssh
102
103   iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT
104   iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT
105   iptables -A OUTPUT -p icmp --icmp-type time-exceeded -j ACCEPT
106   iptables -A OUTPUT -p icmp --icmp-type destination-unreachable -j ACCEPT #ACCEPT outbound ICMP packets #allow
          outgoing ICMP
107
108   iptables -A OUTPUT -p tcp --sport 21 -m state --state ESTABLISHED -j ACCEPT
109   iptables -A OUTPUT -p tcp --sport 20 -m state --state ESTABLISHED,RELATED -j ACCEPT
110   iptables -A OUTPUT -p tcp --sport 1024: --dport 1024: -m state --state ESTABLISHED -j ACCEPT
111   iptables -A INPUT -p tcp --dport 21 -m state --state NEW,ESTABLISHED -j ACCEPT
112   iptables -A INPUT -p tcp --dport 20 -m state --state ESTABLISHED -j ACCEPT
113   iptables -A INPUT -p tcp --sport 1024: --dport 1024: -m state --state ESTABLISHED,RELATED,NEW -j ACCEPT
114   #FTP Rules
115 fi
116
117 if [ $1 == "D" ] ; then #RULES FOR MACHINE D - DNS SERVER
118   SERVER_IP="100.64.21.4"
119   iptables -A INPUT -p udp -s 0/0 --sport 1024:65535 -d $SERVER_IP --dport 53 -m state --state NEW,ESTABLISHED -j
          ACCEPT
120   iptables -A OUTPUT -p udp -s $SERVER_IP --sport 53 -d 0/0 --dport 1024:65535 -m state --state ESTABLISHED -j
          ACCEPT
121   iptables -A INPUT -p udp -s 0/0 --sport 53 -d $SERVER_IP --dport 53 -m state --state NEW,ESTABLISHED -j ACCEPT
122   iptables -A OUTPUT -p udp -s $SERVER_IP --sport 53 -d 0/0 --dport 53 -m state --state ESTABLISHED -j ACCEPT
123   #allow inbound DNS lookup on chase.
124 fi
```

```
125
126 if [ $1 == "E" ] ; then #RULES FOR MACHINE E - FILE SERVER
127   iptables -A INPUT -p tcp -s 10.21.32.0/24 --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT
128   iptables -A OUTPUT -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT #enable SSH connections only from
          10.21.32.0/24 net
129
130   iptables -A INPUT -m state --state NEW -p udp --dport 137 -j ACCEPT
131   iptables -A INPUT -m state --state NEW -p udp --dport 138 -j ACCEPT
132   iptables -A INPUT -m state --state NEW -p tcp --dport 139 -j ACCEPT
133   iptables -A INPUT -m state --state NEW -p tcp --dport 445 -j ACCEPT
134   #allow incoming connections for CIFS and SMB
135 fi
136
137 service iptables save # make sure to save rules!!!
```