Lab 7

1. **All Machines**
    a. **All incoming traffic is allowed for established or related connections**
        i. iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
        ii. service iptables save
        iii. COMPLETED
    b. **and traffic originating from the local loopback adapter lo.**
        i. iptables -I INPUT 1 -i lo -j ACCEPT
        ii. service iptables save
        iii. COMPLETED
    c. **All incoming ICMP traffic should only be allowed if it is an echo request, echo reply (ping), time exceeded (traceroute), or destination unreachable type of message.**
        i. iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
        ii. iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT
        iii. iptables -A INPUT -p icmp --icmp-type time-exceeded -j ACCEPT
        iv. iptables -A INPUT -p icmp --icmp-type destination-unreachable -j ACCEPT
        v. service iptables save
        vi. COMPLETED AND TESTED WITH PING

d. **On all machines except Machine E, new incoming SSH connections are ONLY allowed from 100.64.0.0/24, 100.64.N.0/24 100.64.254.0/24, and 10.21.32.0/24.**
    i. iptables -A INPUT -p tcp -s 100.64.0.0/24 --dport 22 -j ACCEPT
    ii. iptables -A INPUT -p tcp -s 100.64.24.0/24 --dport 22 -j ACCEPT
    iii. iptables -A INPUT -p tcp -s 100.64.254.0/24 --dport 22 -j ACCEPT
    iv. iptables -A INPUT -p tcp -s 10.21.32.0/24 --dport 22 -j ACCEPT
    v. service iptables save
    vi. COMPLETED
e. **On all machines except Machine A / Router and Machine C / Platen, the default policies should be such incoming and forwarded traffic are set to dropped, and outgoing traffic is set to accept.**
    i. iptables -P INPUT DROP
    ii. iptables -P OUTPUT ACCEPT
    iii. iptables -P FORWARD DROP
    iv. service iptables save
    v. COMPLETED AND TESTED

2. **Machine A / Router**
    a. **Forwarded traffic going out to, or coming in from Facebook should be dropped. You don't need to block all IP addresses in use by Facebook, just the one you receive after completing a one time resolve of facebook.com.**
        i. iptables -A FORWARD -s 173.252.110.27 -j DROP

ii. iptables -A FORWARD -d 173.252.110.27 -j DROP

iii. service iptables save

iv. COMPLETED AND TESTED WITH PING

b. Forwarded traffic going out to, or coming in from icanhas.cheezburger.com, and cheezburger.com should be dropped. Again, you don't need to block all possible IP addresses, just the ones you receive after completing a one time resolve.

i. iptables -A FORWARD -d 208.115.96.72 -j DROP (icanhas.cheezburger.com)

ii. iptables -A FORWARD -s 208.115.96.72 -j DROP (icanhas.cheezburger.com)

iii. iptables -A FORWARD -s 157.56.163.21 -j DROP (cheezburger.com)

iv. iptables -A FORWARD -d 157.56.163.21 -j DROP (cheezburger.com)

v. service iptables save

vi. COMPLETED AND TESTED WITH PING

c. Traffic coming in should be allowed if it is established, or related, and new connections to the given machines should be allowed based on the rules for each specific machine, but all other forwarded traffic coming inward should be dropped (e.g. in the input interface is eth0).

i. iptables -A FORWARD -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

ii. Machine B rules

1. iptables -A FORWARD -p tcp -d 100.64.24.2 --dport 80 -j ACCEPT (HTTP)
2. iptables -A FORWARD -p tcp -d 100.64.24.2 --dport 443 -j ACCEPT (HTTPS)

iii. Machine F rules

1. iptables -A FORWARD -p tcp -d 100.64.24.5 --dport 80 -j ACCEPT (HTTP)
2. iptables -A FORWARD -p tcp -d 100.64.24.5 --dport 443 -j ACCEPT (HTTPS)

iv. Machine C rules

1. iptables -A FORWARD -p tcp -d 100.64.24.3 --dport 21 -s 100.64.24.0/24 -j ACCEPT
2. iptables -A FORWARD -p tcp -d 100.64.24.3 --dport 21 -s 100.64.0.27 -j ACCEPT
3. iptables -A FORWARD -p tcp -s 100.64.24.3 --sport 80 -j ACCEPT (HTTP)
4. iptables -A FORWARD -p tcp -s 100.64.24.3 --sport 443 -j ACCEPT (HTTPS)
5. iptables -A FORWARD -p tcp -s 100.64.24.3 --sport 21 -j ACCEPT (FTP)

6. iptables -A FORWARD -p udp -s 100.64.24.3 --sport 53 -j ACCEPT (DNS)

v. Machine D rules

1. iptables -A FORWARD -p udp -d 100.64.24.4 --dport 53 -j ACCEPT (DNS)

vi. Machine E rules

1. iptables -A FORWARD -p tcp -s 10.21.32.0/24 -d 10.21.32.2 --dport 135 -j ACCEPT
2. iptables -A FORWARD -p udp -s 10.21.32.0/24 -d 10.21.32.2 --dport 137 -j ACCEPT
3. iptables -A FORWARD -p udp -s 10.21.32.0/24 -d 10.21.32.2 --dport 138 -j ACCEPT
4. iptables -A FORWARD -p udp -s 10.21.32.0/24 -d 10.21.32.2 --dport 139 -j ACCEPT
5. iptables -A FORWARD -p tcp -s 10.21.32.0/24 -d 10.21.32.2 --dport 445 -j ACCEPT
6. iptables -A FORWARD -p tcp -s 10.21.32.0/24 -d 10.21.32.2 --dport 22 -j ACCEPT

vii. All Machines

1. iptables -A FORWARD -p icmp --icmp-type echo-request -j ACCEPT

2. iptables -A FORWARD -p icmp --icmp-type echo-reply -j ACCEPT
3. iptables -A FORWARD -p icmp --icmp-type time-exceeded -j ACCEPT
4. iptables -A FORWARD -p icmp --icmp-type destination-unreachable -j ACCEPT

viii. All machines except machine E

1. iptables -A FORWARD -p tcp -s 100.64.0.0/24 --dport 22 -j ACCEPT
2. iptables -A FORWARD -p tcp -s 100.64.24.0/24 --dport 22 -j ACCEPT
3. iptables -A FORWARD -p tcp -s 100.64.254.0/24 --dport 22 -j ACCEPT
4. iptables -A FORWARD -p tcp -s 10.21.32.0/24 --dport 22 -j ACCEPT

ix. Other Drop Rules

1. iptables -A FORWARD -i eth0 -j DROP

x. COMPLETED

d. The default policies on Machine A should be such that incoming traffic is set to dropped, and both outgoing and forwarded traffic is set to accept.

i. iptables -P INPUT DROP

ii. iptables -P OUTPUT ACCEPT

iii. iptables -P FORWARD ACCEPT

iv. service iptables save

v. COMPLETED

3. **Machines B & F / Carriage, & Saddle**
   a. **New HTTP and HTTPS connections are allowed regardless of the source address.**
      i. iptables -A INPUT -p tcp --dport 80 -j ACCEPT (HTTP)
      ii. iptables -A INPUT -p tcp --dport 443 -j ACCEPT (HTTPS)
      iii. service iptables save
      iv. COMPLETED AND TESTED WITH NMAP
4. **Machine C / Platen**
   a. **All outgoing traffic is on the local loopback is allowed, and so are existing established or related connections any any adapter.**
      i. iptables -A OUTPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
      ii. iptables -I OUTPUT 1 -o lo -j ACCEPT
      iii. service iptables save
      iv. COMPLETED
   b. **New incoming FTP connections are allowed only from 100.64.N.0/24 and 100.64.0.27.**
      i. iptables -A INPUT -p tcp --dport 21 -s 100.64.24.0/24 -j ACCEPT
      ii. iptables -A INPUT -p tcp --dport 21 -s 100.64.0.27 -j ACCEPT

iii. service iptables save

iv. COMPLETED AND TESTED WITH NMAP

c. Outgoing DNS requests should be allowed to 100.64.N.4 (Chase).

i. iptables -A OUTPUT -p udp -d 100.64.24.4 --dport 53 -j ACCEPT

ii. service iptables save

iii. COMPLETED AND TESTED WITH PING

d. Outgoing FTP, HTTP and HTTPS connections to any hosts should be allowed.

i. iptables -A OUTPUT -p tcp --sport 80 -j ACCEPT (HTTP)

ii. iptables -A OUTPUT -p tcp --sport 443 -j ACCEPT (HTTPS)

iii. iptables -A OUTPUT -p tcp --sport 21 -j ACCEPT (FTP)

iv. service iptables save

v. COMPLETED

e. Outgoing ICMP traffic should be allowed if it is an echo request, echo reply (ping), time exceeded (traceroute), or destination unreachable type of message.

i. iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT

ii. iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT

iii. iptables -A OUTPUT -p icmp --icmp-type time-exceeded -j ACCEPT

iv. iptables -A OUTPUT -p icmp --icmp-type destination-unreachable -j ACCEPT

v. service iptables save

vi. COMPLETED AND TESTED WITH PING

f. The default policy for output and input should be set to dropped.

i. iptables -P OUTPUT DROP

ii. iptables -P INPUT DROP

iii. service iptables save

iv. COMPLETED AND TESTED

5. **Machine D / Chase**

a. New DNS queries should be allowed from any source.

i. iptables -A INPUT -p udp --dport 53 -j ACCEPT

ii. service iptables save

iii. COMPLETED AND TESTED WITH PING

6. **Machine E / Roller**

a. **New connections to the file sharing services (CIFS and SMB) should be restricted to the 10.21.32.0/24 network only. The port numbers used by CIFS and SMB are: 135/tcp, 137-139/udp, and 445/tcp.**

i. iptables -A INPUT -p tcp -s 10.21.32.0/24 --dport 135 -j ACCEPT

ii. iptables -A INPUT -p udp -s 10.21.32.0/24 --dport 137 -j ACCEPT

iii. iptables -A INPUT -p udp -s 10.21.32.0/24 --dport 138 -j ACCEPT

iv. iptables -A INPUT -p udp -s 10.21.32.0/24 --dport 139 -j ACCEPT

v. iptables -A INPUT -p tcp -s 10.21.32.0/24 --dport 445 -j ACCEPT

vi. service iptables save

vii. COMPLETED AND TESTED WITH PING

b. New SSH connections should only be allowed from hosts within the 10.21.32.0/24 network, and no others.

i. iptables -A INPUT -p tcp -s 10.21.32.0/24 --dport 22 -j ACCEPT

ii. service iptables save

iii. COMPLETED AND TESTED WITH SSH