How I did the Lab:

First I went onto all machines and did:
Systemctl start nftables
Systemctl enable nftables

I then added the nftables.conf file provided for us on canvas to machine A in /etc/sysconfig/

I then created and added these nftables.conf files on the associated machines:

Machine A:

```
#!/usr/sbin/nft -f

flush ruleset

#  Set your DMZ net here
define DMZ = 100.64.12.0/24

#  Machine A
table ip saclass {
   #  Incoming chain
   chain incoming {
      #  Default drop
      type filter hook input priority 0; policy drop;
      #  accept loopback
      iifname lo accept
      #  established connections
      ct state invalid drop
      ct state related,established accept
      #  saclass grader and proxy
      tcp dport {4113,4114} accept
      #  ping
      icmp type {echo-reply,destination-unreachable,echo-request,time-exceeded} accept
      #  ssh from LAN, WAN, DMZ and VPN
      ip saddr {10.21.32.0/24,100.64.0.0/24,$DMZ,198.11.0.0/16} tcp dport 22 accept
      #  Incoming DHCP and NTP
      udp dport {67,123} accept
   }
   #  Outgoing chain
   chain outgoing {
      #  Default accept
      type filter hook output priority 0; policy accept;
      #  Block facebook
      ip daddr 157.240.28.35 drop
   }
   #  Forward chain
   chain forwarding {
```

```
    # Default drop
    type filter hook forward priority 0; policy drop;
    #  established connections
    ct state invalid drop
    ct state related,established accept
    #  interface based chains
    iifname "ens192" oifname "ens224" jump WAN2DMZ
    iifname "ens192" oifname "ens256" jump WAN2LAN
    iifname "ens224" oifname "ens192" jump DMZ2WAN
    iifname "ens224" oifname "ens256" jump DMZ2LAN
    iifname "ens256" oifname "ens192" jump LAN2WAN
    iifname "ens256" oifname "ens224" jump LAN2DMZ
}
#  WAN to DMZ chain
chain WAN2DMZ {
    #  ping
    icmp type {echo-reply,destination-unreachable,echo-request,time-exceeded} accept
    #  DNS
    udp dport 53 accept;
    #  ssh, html, grader
    tcp dport {22,80,4113} accept;
}
#  WAN to LAN chain
chain WAN2LAN {
    # only return traffic
}
#  DMZ to WAN
chain DMZ2WAN {
    #  ping
    icmp type {echo-reply,destination-unreachable,echo-request,time-exceeded} accept
    #  DNS
    udp dport 53 accept;
    #  DNS, http, https
    tcp dport {53,80,443} accept;
}
#  DMZ to LAN
chain DMZ2LAN {
    #  ping
    icmp type {echo-reply,destination-unreachable,echo-request,time-exceeded} accept
    #  ssh and NFS
    tcp dport {22,2049} accept;
}
#  LAN to DMZ
chain LAN2DMZ {
    #  Allow everything
    ip saddr {10.21.32.0/24} accept;
}
#  LAN to WAN
```

```
   chain LAN2WAN {
      #  Block facebook
      ip daddr 157.240.28.35 drop
      #  Allow everything else
      ip saddr {10.21.32.0/24} accept;
   }
}
#  NAT LAN to WAN
table ip nat {
   chain POSTROUTING {
      type nat hook postrouting priority srcnat; policy accept;
      oifname "ens192" ip saddr 10.21.32.0/24 masquerade
   }
}
```

Machines B & F:

```
#!/usr/sbin/nft -f

flush ruleset

#  Set your DMZ net here
define DMZ = 100.64.12.0/24

#  Machine A
table ip saclass {
   #  Incoming chain
   chain incoming {
      #  Default drop
      type filter hook input priority 0; policy drop;
      #  accept loopback
      iifname lo accept
      #  established connections
      ct state invalid drop
      ct state related,established accept
      #  saclass grader and proxy
      tcp dport {4113,4114} accept
      #  ping
      icmp type {echo-reply,destination-unreachable,echo-request,time-exceeded} accept
      #  ssh from LAN, WAN, DMZ and VPN
      ip saddr {10.21.32.0/24,100.64.0.0/24,$DMZ,198.11.0.0/16} tcp dport 22 accept
      #  Incoming DNS
      udp dport 53 accept
      tcp dport 53 accept
   }
   #  Outgoing chain
   chain outgoing {
```

```
      #  Default accept
      type filter hook output priority 0; policy accept;
      #  Block facebook
      ip daddr 157.240.28.35 drop
   }
   #  Forward chain
#   chain forwarding {
#      # Default drop
#      type filter hook forward priority 0; policy drop;
#      #  established connections
#      ct state invalid drop
#      ct state related,established accept
#      # Zone transfers
#      tcp dport 53 accept
#   }
}
```

Machines C & D:

```
#!/usr/sbin/nft -f

flush ruleset

#  Set your DMZ net here
define DMZ = 100.64.12.0/24

#  Machine A
table ip saclass {
   #  Incoming chain
   chain incoming {
      #  Default drop
      type filter hook input priority 0; policy drop;
      #  accept loopback
      iifname lo accept
      #  established connections
      ct state invalid drop
      ct state related,established accept
      #  saclass grader and proxy
      tcp dport {4113,4114} accept
      #  ping
      icmp type {echo-reply,destination-unreachable,echo-request,time-exceeded} accept
      #  ssh from LAN, WAN, DMZ and VPN
      ip saddr {10.21.32.0/24,100.64.0.0/24,$DMZ,198.11.0.0/16} tcp dport 22 accept
      # Allow incoming HTTP & HTTPS
      tcp dport {80, 443} accept
   }
   #  Outgoing chain
   chain outgoing {
```

```
      #  Default drop
      type filter hook output priority 0; policy drop;
      # accept loopback
      oifname lo accept
      # established connections
      ct state invalid drop
      ct state related,established accept
      #  Block facebook
      ip daddr 157.240.28.35 drop
      # Allow DHCP
      ip daddr 100.64.12.1 udp dport 67 accept
      # Allow NTP
      ip daddr 100.64.12.1 udp dport 123 accept
      # Allow DNS to B and F
      ip daddr 100.64.12.2 udp dport 53 accept
      ip daddr 100.64.12.6 udp dport 53 accept
      # Allow NFS to E
      ip daddr 10.21.32.2 tcp dport 2049 accept
      # Allow SSH to DMZ
      ip daddr 100.64.12.0/24 tcp dport 22 accept
      # Allow ping except LAN
      icmp type {echo-reply,destination-unreachable,echo-request,time-exceeded} ip
daddr !=10.21.32.0/24 accept
      # Allow http/https to anywhere
      tcp dport {80, 443} accept
   }
   #  Forward chain
#   chain forwarding {
#      # Default drop
#      type filter hook forward priority 0; policy drop;
#      #  established connections
#      ct state invalid drop
#      ct state related,established accept
#      # Zone transfers
#      tcp dport 53 accept
#   }
}
```

Machine E:

```
#!/usr/sbin/nft -f

flush ruleset

#  Set your DMZ net here
define DMZ = 100.64.12.0/24

#  Machine A
```

```
table ip saclass {
   #  Incoming chain
   chain incoming {
      #  Default drop
      type filter hook input priority 0; policy drop;
      #  accept loopback
      iifname lo accept
      #  established connections
      ct state invalid drop
      ct state related,established accept
      #  saclass grader and proxy
      tcp dport {4113,4114} accept
      #  ping
      icmp type {echo-reply,destination-unreachable,echo-request,time-exceeded} accept
      #  ssh from LAN, WAN, DMZ and VPN
      ip saddr {10.21.32.0/24,100.64.0.0/24,$DMZ,198.11.0.0/16} tcp dport 22 accept
      # Allow NFS from DMZ
      ip saddr 100.64.12.0/24 tcp dport 2049 accept
   }
   #  Outgoing chain
   chain outgoing {
      #  Default accept
      type filter hook output priority 0; policy accept;
      #  Block facebook
      ip daddr 157.240.28.35 drop
   }
   #  Forward chain
#   chain forwarding {
#      # Default drop
#      type filter hook forward priority 0; policy drop;
#      #  established connections
#      ct state invalid drop
#      ct state related,established accept
#      # Zone transfers
#      tcp dport 53 accept
#   }
}
```