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:

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
#   }
}
```