JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

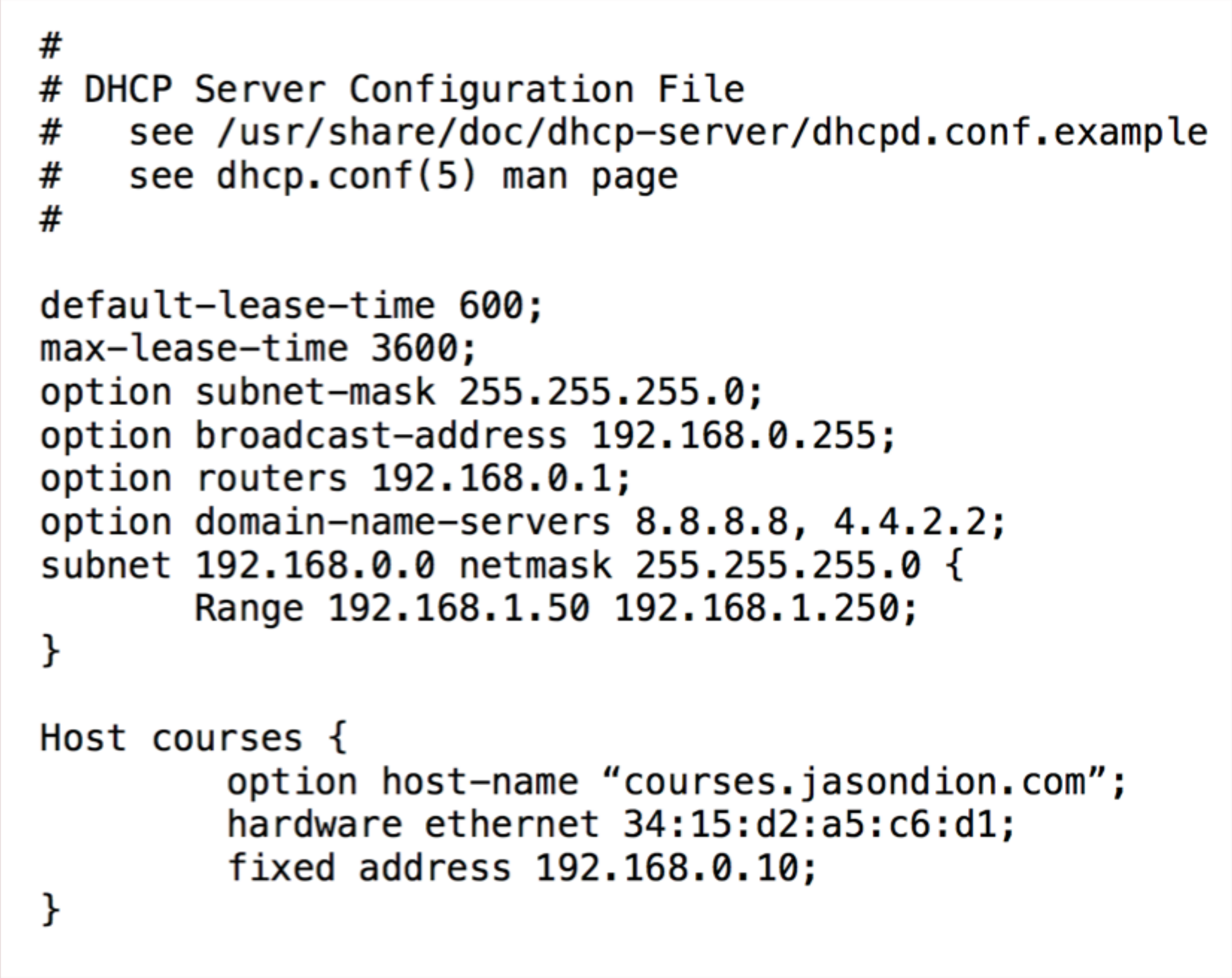
DHCP Logs and Configs

THREAT MANAGEMENT

What is DHCP?

- Dynamic Host Configuration Protocol
- Provides an IP address, default gateway, subnet mask, and DNS server to a host
- DHCP server logs and configurations are useful during passive reconnaissance
- Combined with firewall logs, you can determine which hosts use dynamic or static IPs

Example DHCP Configuration

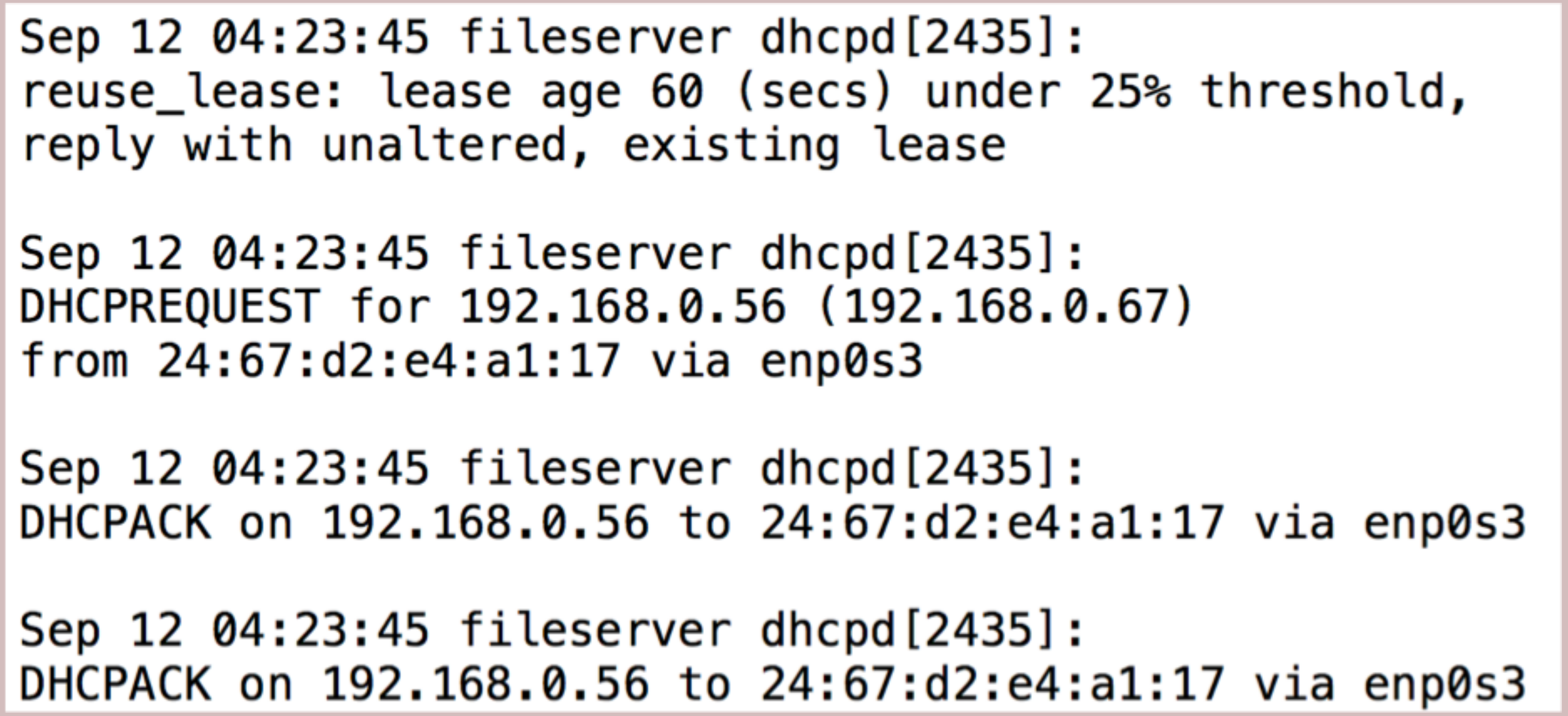


```
#
# DHCP Server Configuration File
#   see /usr/share/doc/dhcp-server/dhcpd.conf.example
#   see dhcp.conf(5) man page
#

default-lease-time 600;
max-lease-time 3600;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.0.255;
option routers 192.168.0.1;
option domain-name-servers 8.8.8.8, 4.4.2.2;
subnet 192.168.0.0 netmask 255.255.255.0 {
       Range 192.168.1.50 192.168.1.250;
}

Host courses {
        option host-name “courses.jasondion.com”;
        hardware ethernet 34:15:d2:a5:c6:d1;
        fixed address 192.168.0.10;
}
```

Example DHCP Logs



```
Sep 12 04:23:45 fileserver dhcpd[2435]:
reuse_lease: lease age 60 (secs) under 25% threshold,
reply with unaltered, existing lease

Sep 12 04:23:45 fileserver dhcpd[2435]:
DHCPREQUEST for 192.168.0.56 (192.168.0.67)
from 24:67:d2:e4:a1:17 via enp0s3

Sep 12 04:23:45 fileserver dhcpd[2435]:
DHCPACK on 192.168.0.56 to 24:67:d2:e4:a1:17 via enp0s3

Sep 12 04:23:45 fileserver dhcpd[2435]:
DHCPACK on 192.168.0.56 to 24:67:d2:e4:a1:17 via enp0s3
```