filename:comptia-secplussy0601-9-2-1-packet-capture-and-replay
Showname: Security+ (SY0-601)
Topic: Operational Security and Incident Response
Episode: Packet Capture and Replay
Learner Objectives:

Given a scenario, use the appropriate tool to assess organizational security

Description:In this episode, the viewer will identify how to use *tcpdump* to capture network packets as well as viewing and extracting data from a capture file with file manipulation. The viewer will also identify how to create a capture file to be viewed in WireShark. Finally the viewer will see how to replay the capture packets using *tcpreplay*.

- Determine the machine that you will work from
  - I am using my laptop
- Identify the interface used to capture files

```
ifconfig
```

- Start the packet capture

```
sudo tcpdump -i eth1
```

- Make FTP connection (simulate plain-text protocol)

```
ftp 10.10.128.4
msfadmin/P@
```

- Generate FTP-Data

```
ls
cd ../../
ls
```

- Saving the capture to a file

```
sudo tcpdump -i eth1 > test-cap.txt
```

- Generate FTP-Data

```
ls
cd ../../
ls
get tradesecrets
```

- Stop capture and view file output

```
cat -n test-cap.txt
grep ftp-data test-cap.txt
grep ftp-data test-cap.txt |head -n 5
grep ftp-data test-cap.txt |tail -n 5
```

- Create a script to review capture file

```
vi capsearch.sh
grep ftp-data test-cap.txt |tail -n 5
```

- Make script executable

```
sudo chmod +x capsearch.sh
```

- Make capture file exportable

```
sudo tcpdump -i eth1 -w test-cap.pcap
```

- Generate FTP Data

```
ls
cd ../../
ls
get tradesecrets
```

- Stop capture and open PCAP file in Wireshark

```
CRTL+C
sudo wireshark
```

- Replaying packets to the network

```
tcpreplay -i eth1 test-cap.pcap
```