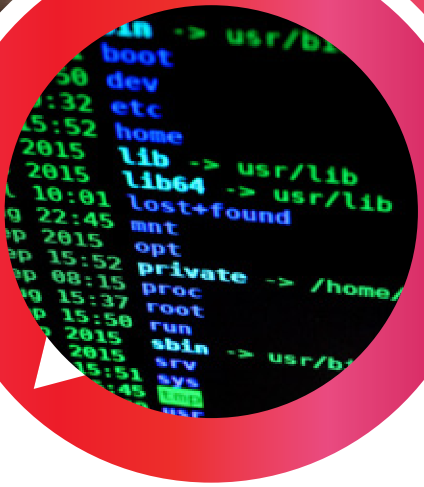

```
in -> usr/bi
   boot
50 dev
:32 etc
5:52 home
2015 lib -> usr/lib
2015 lib64 -> usr/lib
 10:01 lost+found
g 22:45 mnt
ep 2015 opt
ep 15:52 private -> /home/
ep 08:15 proc
g 15:37 root
p 15:50 run
p 2015 sbin -> usr/b
2015 srv
15:51 sys
:45 tmp
```

COURSE CATEGORY: : CYBER DEFENCE

COURSE LEVEL: ADVANCED

COURSE CODE: IFIS CDE/03

COURSE NAME: : INTRUSION DETECTION TRAINING

0101
010
IFIS

Institute of Forensics & ICT Security
Forensics. Security. Training

About this Course

This course delivers the technical knowledge, insight, and hands-on training you need to defend your network with confidence. You will learn about the underlying theory of TCP/IP and the most used application protocols, such as DNS and HTTP, so that you can intelligently examine network traffic for signs of an intrusion. You will get plenty of practice learning to master different open source tools like tcpdump, Wireshark, Snort, Bro, tshark, and SiLK.

Learning Outcomes

- Configure and run open source Snort and write Snort signatures
- Configure and run open source Bro to provide a hybrid traffic analysis framework
- Understand TCP/IP component layers to identify normal and abnormal traffic
- Use open source traffic analysis tools to identify signs of an intrusion
- Comprehend the need to employ network forensics to investigate traffic to identify a possible intrusion
- Use Wireshark to carve out suspicious file attachments
- Write tcpdump filters to selectively examine a particular traffic trait
- Craft packets with Scapy
- Use the open source network flow tool SiLK to find network behavior anomalies
- Use your knowledge of network architecture and hardware to customize placement of IDS sensors and sniff traffic off the wire

Prerequisites

This course covers all of the core areas of security and assumes a basic understanding of technology, networks, and security

Course Outline

Topic 1: Traffic Analysis Fundamentals

a) TCP/IP concepts
b) Introduction to wireshark
c) Network access
d) IP Layers
e) Wireshark display filters

f) Writing tcpdump filters
g) TCP
h) UDP
i) ICMP

Topic 2: Traffic Analysis and application controls

a) Scapy
b) Advanced wireshark
c) Detection methods for application controls
d) DNS
e) Microsoft protocols
f) HTTP (2)
g) SMTP
h) IDS/IPS Evasion Theory

Topic 3: Network monitoring

a) Network Architecture
b) Introduction to IDS/IPS
c) Snort
d) Bro

Topic 4: Network traffic forensics

a) Introduction to network forensics analysis
b) Using network flow records
c) Examining command and control traffic
d) Analysis of pcaps

Requirements

- x86- or x64-compatible 1.5 GHz CPU minimum or higher
- USB Port
- 4GB RAM or higher
- 60 GB free hard drive space
- Windows XP/Vista/7/8/10, Mac OS X, or Linux - any type

Target Audience

- Intrusion detection, systems and security analysts
- Network engineers/ administrators
- Hands-on security managers

Duration and Fees

Duration: 2 days

Pricing: $250

For Inquiries, booking and more information,

Call Admissions on 0393517236/0784270586 orEmail: admissions@forensicsinstitute.org