Auditing and Digital Forensics. Verificare la compliance con lo stato dell'arte

Dario Forte, CFE

Information Security Analyst

Agenda

- La digital forensics come disciplina trasversale
- *Computer Forensic*
- *Network Forensic*
- Legal Compliance
- Il ruolo degli Edp Auditor

La Digital Forensic come disciplina trasversale

- Furto di informazioni, frodi interne, attacchi coordinati, stepping stones sono riconoscibili tramite un’azione DF Based
- L’interazione con le Forze di Polizia è sempre maggiore
- Ergo c’è bisogno di complance con le best practices

Computer Forensic

- È la disciplina che si occupa dell'analisi delle workstation/server
- Consiste nell' analisi di tutto ciò che è all'interno del "green circle"
- è alla base delle azioni di correlazione
- gli accertamenti devono essere ripetibili

Network Forensic

- Utile per ricostruire lo scenario di attacco subìto;
- necessaria per le certificazioni di infedeltà aziendale
- presume un’ampia compliance legale dal punto di vista organizzativo e di policy.

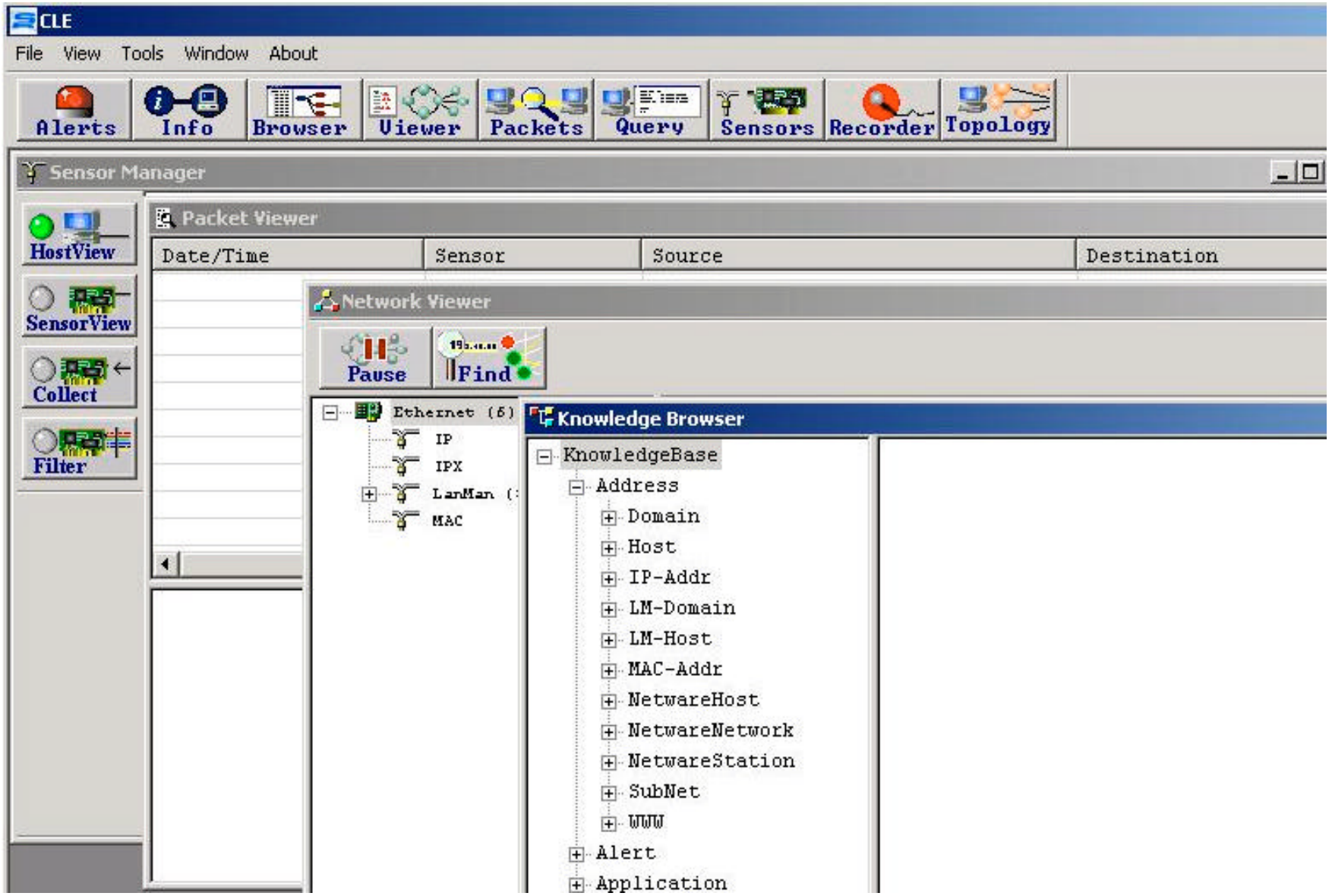
Computer Forensic: Stato dell'arte

- Un tool deve essere in grado di gestire:
  - Slack Space
  - metodiche di cancellazione avanzata
  - Anti Forensic Tools
  - *Real* Bitstream imaging
  - ripetibilità degli atti effettuati

Network Forensic: Stato dell’arte

- Deve essere in grado di normalizzare i dati di input
- Deve aderire al principio della Cross Technology Correlation
- Deve consentire l’analisi off line
- punto di management centralizzato

Network Forensic: un esempio


CLE
File View Tools Window About
Alerts
Info
Browser
Viewer
Packets
Query
Sensors
Recorder
Topology
Sensor Manager
HostView
SensorView
Collect
Filter
Packet Viewer
Date/Time
Sensor
Source
Destination
Network Viewer
Pause
Find
Ethernet (6)
IP
IPX
LanMan (
MAC
Knowledge Browser
KnowledgeBase
Address
Domain
Host
IP-Addr
LM-Domain
LM-Host
MAC-Addr
NetwareHost
NetwareNetwork
NetwareStation
SubNet
WWW
Alert
Application

Legal Compliance

- Generalmente la LC è correlata a due settori:
  - Penale e procedurale: Log, Acquisizioni dischi, eventuali procedure di intercettazione interne devono seguire la legge del paese in cui si sta svolgendo l'indagine
  - Policy/lg privacy e statuto dei lavoratori: l'acquisizione delle fonti di prova deve presumere un impegno di questo genere.

Il ruolo degli Edp Auditor

- Gli EDP Auditor dovrebbero intervenire:
  - verifica della compliance con lo stato dell'arte tecnologico
  - verifica della compliance tra le tecnologie e lo scenario legale.

Verifica della compliance con lo stato dell'arte tecnologico

- Per la Computer Forensics
  - utilizzo di software di acquisizione che consentano sia il formato DD sia quello proprietario
  - "possibilmente" devono consentire l'esaminabilità anche da un tool opensource
  - cross platform in file system analysis
  - cross platform in operating systems

Verifica della compliance con lo stato dell'arte tecnologico

- Per la Network Forensics:
  - gestire i log provenienti da più fonti
  - time stamping e protezione da scrittura (anti tampering)
  - gestione della log rotation
  - interazione con gli IDS multi architettura.

Conclusioni

- Gli EDP Auditor estenderanno, per forza di cose, la loro competenza verso il legal;
- è consigliabile, quindi, avere visibilità sugli scenari di basso livello, sia sugli OS sia sulla parte network
- negli Usa gli Edp Auditor iniziano ad avere, per conoscenza, alcuni report di incidente informatico.

Thanks

www.dflabs.com

dario.forte@acm.org