Network Investigation Toolkit (NIT)

From: Decision Group Inc. Taipei Headquarter

2009/12/02, Taipei

Decision Group is pleased to announce the only one in the world, all-in-one portable unit— NIT (Network Investigation Toolkit), with comprehensive network forensics features and can be carried at any location for network-based investigation task.   To intercept on targeted networks or users to collect the necessary evidences and trace out the source of communication, NIT's unique capability can combine LAN, WLAN, HTTPS/SSL MITM real- time interception on both LAN and WLAN networks as well as offline analysis and reconstruction of pre-captured raw data files. The 3.5G/ HSDPA USB Adapter is included in the package for user to remote access and manage the system.

◆ Provides Etherent & Wireless LAN Real-Time Capturing and Reconstruction.

◆ Capture Ethernet LAN traffic (up to about 10-20 Mbps throughput) through the built-in Ethernet LAN Adapter.

◆ Capture Wireless LAN traffic (select from 1-4 Diff. Channels. Stations through external USB Wi-Fi Adapters.

◆ Support cracking of WEP Key.

◆ Intercept HTTPS/SSL traffic on Wireless/ Ethernet LAN user using external USB Wi-Fi Adapter/ internal Ethernet Lan Adapter and connect back to Internet through System internal LAN Ethernet/ Wi-Fi Adapter/ 3/3.5G external USB Modem connection.

◆ Offline raw data import and parsing: available. Up to 100 cases can be created. 100 raw data files to be imported at once. Total raw data files imported cannot be more than 10 GB.

Specification

Features and Functions	
Hardware	1 x Lenovo ThinkPad X200 Laptop with internal Wi-Fi Adapter and Ethernet LAN Adapter. 4 x External USB Wi-Fi Adapters (for up to 4 WLAN Channels Capturing). 1 x 3.5G/HSPDA USB Network Adapter (for Remote Access)
Level and Size of Implementation	Ethernet LAN size (50 users or approximately 10-20 Mbps Throughput). Wireless LAN (up to 4 Channels capturing concurrently.)
Mode of Operation	Ethernet LAN Interception, Wireless LAN (802.11b/g/n) Interception, HTTPS/SSL Interception and Offline Raw Data Reconstruction
System Management	Local Machine or Remote Access - Web GUI (by Firefox), VNC Remote Control.
Storage Size	Single HDD - Size:320GB
Internet Protocols Supported - Decode and Reconstruction	
Email	POP3, SMTP, IMAP

Webmail	Yahoo Mail, Gmail, Windows Live Hotmail, Hinet, Hotmail Standard, PCHome, URL, Giga, Yam, Sina, Seednet, mail.tom.com, mail.163.com, Sohu.com, Gawab
Instant Messaging (IM/Chat)	Yahoo Messenger, Windows Live Messenger (MSN), IRC, ICQ, UT Chat Room, Gtalk, Yahoo Web Chat, MSN Web Chat, Skype Voice Call Duration Log
Skype (4.0) Text & Voice Chat Recording	Skype Agent Implementation for LAN/Organization Networks
HTTP/ HTTPS (HTTPS/ SSL Interception Only)	Link, Content, Upload & Download, Video Streaming (Youtube, Metacafe, Video etc.) HTTPS Decoding and Reconstruction. Username and Password.
File Transfer	FTP Upload/Download P2P File Sharing (BitTorrent, eMule/eDonkey, FastTrack, Gnutella)
Telnet	Support with Play Back
Online Games	Support more than 100 online Games such as Ragnarok Online, Mapple Story, War of World Craft, ZT, FairyLand, Kinf of king, Katrider, BnB, Mabinogi, Nage, etc.
VoIP (IM)	Yahoo Messenger and Gtalk Voice Call (reconstruct back to GIPS format - GIPS Decoder with Codec is required to play back the audio file).
Webcam (IM)	Yahoo Messenger and Windows Live Messenger Webcam session
VoIP (Standard)	SIP, H.323 RTP Voice Sessions (Supported Codecs includes G.711 u-law, G.711 a-law, G.723, G.726, G.729 and iLBC)
Analysis, Forensics, Administrative, Management Functions	
Raw Data (PCAP) Reserving Function	Yes, available.
Search	Free Text Search, Conditional Search.
Data Export Backup - Retention	Yes, export and back up entire system data external storage or burn in CD/DVD.
Information of Targeted User/PC	Account (AD, Username etc.), IP Address, MAC Address, PC Name
Import and Export of Data for Analysis	Import Raw Data for Analysis. Export-Backup Entire System Data.
Reporting	Traffic Report

About Decision

Established in 1986, Decision Group has already devoted in digital forensics technology more than 8 years. As a pioneer of digital forensics software & device provider, Decision offers a total forensics solutions including software, hardware, services and training program to help customers in protecting intellectual property and proactively protecting important information assets from internet threats. Decision's E-Detective series products had been widely applied in Taiwan Police Intelligence Service, Military of Defense, and being used as teaching materials for Taiwan Central Police University.

To know more about Decision and products, please visit

http://www.edecision4u.com   http://www.digi-forensics.com