Training Topic
Malware Forensic

This class will immerse the students into an interactive environment where they will be shown how to scan, test, hack and secure their own systems. The lab intensive environment gives each student in-depth knowledge and practical experience with the current essential security systems. Students will begin by understanding how perimeter defences work and then be lead into scanning and attacking their own networks, no real network is harmed. Students then learn how intruders escalate privileges and what steps can be taken to secure a system. Students will also learn about Malware Dynamic Analysis, Honeynet, Windows Malware, Hardware Malware (Bad USB), Android Malware, Botnet, and Virus Creation. When a student leaves this intensive 2 day class they will have hands on understanding and experience in Malware Forensics Basic. This course will significantly benefit security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure

Training Modules

- Introduction to Malware
  - Introduction
  - Malware Terminology
  - Isolated Lab Setting
  - Virtualbox
  - VM's Network Setting (1)
  - VM's Network Setting (2)
  - Change IP on Windows
  - Countermeasures for Spyware
  - Countermeasures for Rootkit Detection
  - Countermeasures for Adware
  - Anonymous Web Browsing With T0R
  - Web Based Anonymizers
  - Virtual Private Network
- Introduction Malware Tools
  - Behavioural Analysis Tools
    - File system and registry monitoring : Process Monitor with ProcDOT
    - Process monitoring : Process Explorer and Process Hacker
    - Network monitoring : Wireshark
    - Change detection : Regshot
- Code Analysis Tools
    - Disassembler and debugger : OllyDbg and IDA Pro Freeware
    - Memory dumper : Scylla and OllyDumpEx

- Online Analysis Tools
    - MALWR
    - ThreatExpert
    - Virustotal
    - Syrianmalware
    - hybrid-analysis

- Introduction Honeynet, Honeypot and online tools
  - Introduction Parrot Security Operating System
    - Ntop
    - Ntopng
    - Splunk
    - Email Header Analysis
    - Whois
    - Nslookup
    - Mxtoolbox
    - ARIN
    - Kartoo Search Engine
    - Baidu search engine
    - Yandex Search engine
    - Malware Domain list

- Honeypot for Windows
  - Kfsensor Professional
  - Honeybot
  - Simulation attack with nmap
- Malware Analysis
  - Classification with ClamAV
  - RAT Exploration- Poison IVY
  - Behavioral Analysis
- Persistence Technique
    - Using Registry Files
    - Using File Systems
    - Using Windows Services
    - Analyze malicious JS and shellcode from PDFs and Office documents
    - Extract malware from pcap (wireshark)
    - Scanning Malware with Virustotal.com
    - Scanning File with Jotti Malware scan
    - Scanning File with NOVIRUSTHANKS
    - Malware Reporting with Network Miner
    - Malware Reporting with Cap Analysis
- Android Malware
    - Introduction Android Malware Operating System
    - Droidjack
    - Spynote
    - Androrat
- Windows Malware
    - Njrat
    - Spyeye
    - PoisonIVY
    - Hacker Defender
    - Conficker
    - Conficker scanner

- Linux Malware
    - Botnet SSH Client manager

- Hardware Malware / Bad USB for Beginner
    - Introduction Bad USB
    - Hello World
    - Wifi Password Grabber with Bad Usb
    - Chrome Password Stealer with Bad Usb

About Trainers – Ade Yoseman Putra

Ade Yoseman Putra was an information security addict.bug researcher in some vulnerability website (0day, packetstormsecurity; security focus, exploit db, etc). Have a small business and working under government too as cyber security at ID-SIRTII equivalent to MyCERT,CSM Love to doing research and development especially in malware forensics. Co-founder securityjustillusion.org (non-profit organization information security).5 years' experience in information security as security engineer, security analyst, penetration tester, trainer and speaker in information security, experience in cert (computer emergency response team) as malware analysis.