Asia Masters Center

Hacker Tools, Techniques, Exploits and Incident Handling

Asia Masters Centre (AMC), Suite 2 B, level 6, Office Block, Grand Millennium Hotel, Bukit Bintang Street, 55100 Kuala Lumpur, Malaysia. | Tel: +60327326992|Mobile: +601 8909 0379 | Fax: +60327326992
Website: http://www.asiamasters.org/ | Email: info@asia-masters.com

Asia Masters Center

Hacker Tools, Techniques, Exploits and Incident Handling

Course Objective

- Apply incident handling processes-including preparation, identification, containment, eradication, and recovery-to protect enterprise environments
- Analyze the structure of common attack techniques in order to evaluate an attacker's spread through a system and network, anticipating and thwarting further attacker activity
- Utilize tools and evidence to determine the kind of malware used in an attack, including rootkits, backdoors, and Trojan horses, choosing appropriate defenses and response tactics for each
- Use built-in command-line tools such as Windows tasklist, wmic, and reg, as well as Linux netstat, ps, and lsof to detect an attacker's presence on a machine
- Analyze router and system ARP tables along with switch CAM tables to track an attacker's activity through a network and identify a suspect
- Use memory dumps and memory analysis tools to determine an attacker's activities on a machine, the malware installed, and other machines the attacker used as pivot points across the network
- Gain access to a target machine using Metasploit, and then detecting the artifacts and impact of exploitation through process, file, memory, and log analysis

- Analyze a system to see how attackers use the malware to move files, create backdoors, and build relays through a target environment
- Run the Nmap port scanner and Nessus vulnerability scanner to find openings on target systems, and apply tools such as tcpdump and netstat to detect and analyze the impact of the scanning activity
- Apply the tcpdump sniffer to analyze network traffic generated by a covert backdoor to determine an attacker's tactics
- Employ the netstat and Isof tools to diagnose specific types of traffic-flooding denial-of-service techniques, and choose appropriate response actions based on each attacker's flood technique
- Analyze shell history files to find compromised machines, attacker-controlled accounts, sniffers, and backdoors

Target Audience

- Incident handlers
- Leaders of incident handling teams
- System administrators who are on the front lines defending their systems and responding to attacks
- Other security personnel who are first responders when systems come under attack

Asia Masters Center

Course Outline

- **Day 1**
- Incident Handling Step-by-Step and Computer Crime Investigation
- Topics
- Preparation
- Building an incident response kit
- Identifying your core incident response team
- Instrumentation of the site and system
- Identification
- Signs of an incident
- First steps
- Chain of custody
- Detecting and reacting to Insider Threats
- Containment
- Documentation strategies: video and audio
- Containment and quarantine
- Pull the network cable, switch and site
- Identifying and isolating the trust model
- Eradication
- Evaluating whether a backup is compromised
- Total rebuild of the Operating System
- Moving to a new architecture
- Recovery
- Who makes the determination to return to production?
- Monitoring to system
- Expect an increase in attacks
- Special Actions for Responding to Different Types of Incidents
- Espionage
- Inappropriate use

- Incident Record-keeping
- Pre-built forms
- Legal acceptability
- Incident Follow-up
- Lessons learned meeting
- Changes in process for the future

- **Day 2**
- Computer and Network Hacker Exploits – Part 1
- Topics
- Reconnaissance
- What does your network reveal?
- Are you leaking too much information?
- Using Whois lookups, ARIN, RIPE and APNIC
- Domain Name System harvesting
- Data gathering from job postings, websites, and government databases
- Recon-ng
- Pushpin
- Identifying publicly compromised accounts
- Maltego
- FOCA for metadata analysis
- Scanning
- Locating and attacking unsecure wireless LANs
- War dialing with War-VOX for renegade modems and unsecure phones
- Port scanning: Traditional, stealth, and blind scanning
- Active and passive Operating System fingerprinting
- Determining firewall filtering rules
- Vulnerability scanning using Nessus and other tools

- CGI scanning with Nikto
- Powershell Empire
- Bloodhound
- Rubber Duckie attacks to steal wireless profiles
- User Behavioral Analytics
- Intrusion Detection System (IDS) Evasion
- Foiling IDS at the network level
- Foiling IDS at the application level: Exploiting the rich syntax of computer languages
- Web Attack IDS evasion tactics
- Bypassing IDS/IPS with TCP obfuscation techniques

- **Day 3**
- Computer and Network Hacker Exploits – Part 2
- Topics
- Network-Level Attacks
- Session hijacking: From Telnet to SSL and SSH
- Monkey-in-the-middle attacks
- Passive sniffing
- Gathering and Parsing Packets
- Active sniffing: ARP cache poisoning and DNS injection
- Bettercap
- Responder
- LLMNR poisoning
- WPAD Attacks
- MITMf
- DNS cache poisoning: Redirecting traffic on the Internet
- Using and abusing Netcat, including backdoors and nasty relays
- IP address spoofing variations
- Operating System and Application-level Attacks

- Buffer overflows in-depth
- The Metasploit exploitation framework
- Format string attacks
- AV and application whitelisting bypass techniques
- Netcat: The Attacker's Best Friend
- Transferring files, creating backdoors, and shoveling shell
- Netcat relays to obscure the source of an attack
- Replay attacks

- **Day 4**
- Computer and Network Hacker Exploits – Part 3
- Topics
- Password Cracking
- Analysis of worm trends
- Password cracking with John the Ripper
- Hashcat
- Rainbow Tables
- Password spraying
- Web Application Attacks
- Account harvesting
- SQL Injection: Manipulating back-end databases
- Session Cloning: Grabbing other users' web sessions
- Cross-Site Scripting
- Denial-of-Service Attacks
- Distributed Denial of Service: Pulsing zombies and reflected attacks
- Local Denial of Service

- **Day 5**
- Computer and Network Hacker Exploits – Part 4
- Topics
- Maintaining Access
- Backdoors: Using Poison Ivy, VNC, Ghost RAT, and other popular beasts
- Trojan horse backdoors: A nasty combo
- Rootkits: Substituting binary executables with nasty variations
- Kernel-level Rootkits: Attacking the heart of the Operating System (Rooty, Avatar, and Alureon)
- Covering the Tracks
- File and directory camouflage and hiding
- Log file editing on Windows and Unix
- Accounting entry editing: UTMP, WTMP, shell histories, etc.
- Covert channels over HTTP, ICMP, TCP, and other protocols
- Sniffing backdoors and how they can really mess up your investigations unless you are aware of them
- Steganography: Hiding data in images, music, binaries, or any other file type
- Memory analysis of an attack
- Putting It All Together
- Specific scenarios showing how attackers use a variety of tools together
- Analyzing scenarios based on real-world attacks
- Learning from the mistakes of other organizations
- Where to go for the latest attack info and trends

Asia Masters Center

➢ The Feature Of Asia Master Training And Development Center

- we pick up the customer from the airport to the hotel.
- we give the participant training bag includes all the necessary tools for the course.
- Working within groups to achieve the best results.
- All our courses are confirmed and we do not postpone or cancel the courses regardless of the number of participants in the course.
- We can assist you in booking hotels at discounted prices if you wish to book through us.
- We offer the certificate from Asia Masters Center for Training and Administrative Development.

➡ The Cost Of The Training Program Includes The Following:

1) Scientific article on flash memory.
2) Training Room.
3) Training.
4) Coffee break.
5) The training bag includes all the tools for the course.

Asia Masters Centre (AMC), Suite 2 B, level 6, Office Block, Grand Millennium Hotel, Bukit Bintang Street, 55100 Kuala Lumpur, Malaysia. | Tel: +60327326992|Mobile: +601 8909 0379 | Fax: +60327326992
Website: http://www.asiamasters.org/ | Email: info@asia-masters.com

Asia Masters Center

Price (USD)
Communicate with the training department to know the participation fees ➢ There are offers and discounts for groups
The details of the bank account
Bank name: CIMB Bank Berhad Account name: Asia Masters Center SDN. BHD Bank account number: 80-0733590-5 Swift code: CIBBMYKL IBAN: Null

Asia Masters Centre (AMC), Suite 2 B, level 6, Office Block, Grand Millennium Hotel, Bukit Bintang Street, 55100 Kuala Lumpur, Malaysia. | Tel: +60327326992|Mobile: +601 8909 0379 | Fax: +60327326992
Website: http://www.asiamasters.org/ | Email: info@asia-masters.com