Mahmud Ab Rahman (M.Sc.Comp., GPEN (GOLD),GREM)
Certification:

- CISCO CCNP and CCNA
- GIAC SANS GPEN (GOLD)
- GIAC SANS GREM

Publications

1) Analyzing Malicious PDF - E-Security Megazine for CyberSAFE Malaysia
2) Getting Owned by Malicious PDF - SANS GPEN (GOLD)
3) Reversing Android Malware: Geinimi

Contributing into few information security reports such as:

1) ENISA's Botnets: 10 Tough Questions
http://www.fkie.fraunhofer.de/content/dam/fkie/de/documents/forschungsbereiche/botnets-10-toughquestions.pdf
2) ENISA's Botnets: Detection, Measurement, Disinfection & Defence
www.enisa.europa.eu/act/res/botnets/botnets-measurement-detection-disinfection-anddefence/at_download/fullReport

Work Experience

02/2008 – 12/2012 CyberSecurity Malaysia (MyCERT)., MY
Manager (Specialist) Emergency Readiness for Malware Research Center (MRC)

1) Manage and responsible for the new unit (MRC) in handling information security threats such as malware, intrusion, hacking, exploits, apt and many more.
2) Designed and implemented a drill for APCERT (Asia Pacific Computer Emergency Repsonse Team) in corresponding to Beijing 2008 Olympic.
3) Manage and architect the National Cyber Drill (XMAYA) to support National Cyber Security Policy for almost 5 years.
4) Researched and implemented on honeynet technologies to be better suit with enterprise environment.
5) Researched and implemented technique to detect and analyze malicious pdf file. This technique allowed to help analyst on detecting and analyzing malicious pdf. The end result is to speed up the detection and analysis report related to malicious pdf.
6) Research on detection and analyzing malicious flash file. The result this research is a tool to analyze malicious flash file. It is able to disassemble and decompile flash bytecode.
7) Research on Android malware. This research is to provide a technical landscape view on Android mobile platform. The result is discussed at national level of the threat associated with Android malware.
8) Mentored and enriched new analysts in achieving quality security researcher and analyst.
9) Monitor requirements, design and implementation phase for any security project development.
10) CyberSecurity Malaysia Honeynet Chapter Lead

11/2006 – 01/2008 **CyberSecurity Malaysia (MyCERT).**, MY
Intrusion Analyst

1) Handle incident handling and response on security incidents reported to MyCERT in area of malware, intrusion/hacking and malicious code.
2) Perform penetration testing and vulnerability assessment for high-profile system for critical national information infrastructures (CNII).
3) Established cyber early warning system (CEWS) for sampling monitoring of Malaysian traffic by implementing network security monitoring approach. Many components involved in this project such as Snort, Sguil framework, Netflow suite(cflowd, nfsen) and honeyport technologies.
4) Implement honeynet technologies in MyCERT research networks which consisted of 8 different ISPs.
5) Established honeynet project for CyberSecurity Malaysia chapter for Honeynet Project
6) Involved in high profile cyber security investigation related to Malaysian Government.
7) Researched and implemented best practices, standards, processes and tools that allow to integrate and customize MyCERT operation on time and on budget.
8) Equipped with good skill in these area honeynet, malware analysis, reverse engineering, exploitation and network security monitoring.
9) Involved with National IT Security Roadmap Research and Development Task Force

Training

1) Incident Handling Training for National CERT (Cambodia, Laos, Myanmar) - FEB 2007
2) Honeynet Training for FIRST-TC, Doha, Qatar - APRIL 2007
3) Network Security Monitoring for APCERT, Hong Kong - MARCH 2008
4) Network Security Monitoring for FIRST TC, Tokyo, Japan - APRIL 2008
5) Honeypotting with Dionaea, OIC-CERT Conference, Kuala Lumpur, Malaysia - June 2009
6) Analyzing Malicious PDF file, Honeynet Project, Mexico City, Mexico - March 2010
7) Analyzing Malicious PDF File, Asia Pacific Hi-Tech Crime unit, Semarang, Indonesia (Training) - December 2010
8) Reversing Android Malware, Honeynet Project, Paris, French - March 2011
9) Reversing Android Malware Training, ISSUMMIT 2011, Hong Kong - November, 2011
10) Reversing Malicious Flash, Honeynet Project, USA - March, 2012
11) Reversing Android Malware Training, Honeynet Project, USA - March, 2012
12) Analyzing Malicious PDF v 2.0 Training, Taiwan - June 2012

Security conferences

I had presented at numerous **security conferences** for information security related presentation. Below are list of my presentations:

1) Analyzing Malicious PDF, FIRST Technical Colloquium, Kuala Lumpur, Malaysia
2) Portable Destructive File (PDF), FIRST Conference, Miami, United State (Presentation)

3) Threats Landscape on Malware (Panelist), CSM-ACE Conference, Kuala Lumpur, Malaysia
4) Reversing Android Malware, Honeynet Project, Paris, France. March 2011
5) Reversing Android Malware, HITCON, Taiwan. July 2011
6) Sneaky PDF, DEFCON, USA. July 2011
7) Reversing Android Malware 2.0, Hack In The Box, Malaysia. October, 2011
8) Reversing Encryption Routine Inside Android Malware, Taiwan. June 2012
9) Mobile Malware on The Rise: CSM-ACE 2012, Malaysia. October 2012.