OWASP
Day 2016
15 - 17 November 2016
" Empowering Knowledge Towards Security Readiness "
HIGHLIGHTS:
1 day Seminar
5 Leading Edge Workshops
VENUE:
Universiti Kuala Lumpur
1016, Jalan Sultan Ismail
50250 Kuala Lumpur
ORGANISED BY:
UniKL UNIVERSITI KUALA LUMPUR
HRDF Claimable
For more details log on to http://www.owasp.unikl.edu.my OR contact 03-21754210

Training Topic

Weaponizing Malware 101

It's time for us to learn how bad guys actually build their bad stuff. Students will learn how we the bad guys actually build /structure their malware and make enchantment along the way. Students will learn how to malware utilize various API gadgets/scripts. By learning the arts of the malware, awareness can be raise to make the future a bit better.
Disclaimer: This is for education purpose only

- **Introduction to Malware History and Cons**
- **Introduction to Windows API**
- **Introduction to Shellcode**
- **Simulating a Malware**
- **Bypassing Antivirus**
- **Introduction to Ransomware**
- **Building a simple Ransomware**
- **Data harvesting technique**
- **Exflitarte Data via Side-Channel Attack**
- **Defence Mechanism Analysis.**
- **Bootkit Attack example.**

About Trainers – Muhammad Shahriman Samsudin

Muhammad Shahriman (GPEN) work as a Senior Security Consultant at Scan Associates Berhad. His hacking knowledge and reputation is known when he won the Uitm International Hacking Competition continuously from 2006 until 2008.His exclusive jobs allow him to experiment with all kinds of hacking tools and techniques during the penetration testing. He has dedicated his life to test out the "security state" of most government agencies, law enforcers and numerous financial institution inside and outside of Malaysia.If
exploits for certain vulnerability is not available off the shelf, he just write his exploit on his own. He also have passion for teaching and have taught on Network Security inside and outside the country the furthest is (King Abdul Aziz University in Saudi).

He also have actively involves in numerous incident response handling cases particularly related to Digital Forensic issues. He capability to understand the structure of a program or a flow of a network aids him a lot in solving a lot of forensics studies issues. He runs his own blog (http://y0nd13.blogspot.com) where he posted up his tools and research such as "Hunnybunny a remote shellcode Launcher", "Twit2bot a SMS twitter basedbotnet", "Bypassing Antivirus using Stealth Meterpreter".In his spare time, he
likes to messed around with Fedora Linux and docodes in Python. He is also an expert in hacking WIMAX/4G Technology.