In the World of Security *Hackers Rule*

Presenter – Aditya K. Sood

Date: November 10th 2011 | Time: 7 PM – 8 PM | 1279 Anthony Hall

The talk sheds light on the new trends of web attacks that are used by attackers to serve malware. A variety of vulnerabilities in operating systems and websites are exploited to serve malware for diversified infections. Attackers spread malware elegantly by exploiting the vulnerabilities through drive-by downloads. Third generation banking malware such as SpyEye and Zeus have been devastating. Can we turn the tables on them? This is possible only when we think like hackers. This presentation covers the artifacts of being a real hacker and the thought process required to trace down the hidden elements. In this talk I will emphasize live hacks that cover

1.) Website vulnerabilities like Cross Site Scripting (XSS), SQL Injection (SQLI), Local File Inclusion (LFI), Remote File Inclusion (RFI) and other web attacks.
2.) There is a complete demonstration of an IRC-based bot to show how the IRC channels are used to infect machines and extracting sensitive information.

Note: The talk covers 90% demos and very few slides. We are talking about hacking; let's show the attacks in the real world. This is all for educational purposes only.

Most of the work has been done under the guidance of Dr. Richard J Enbody.

Biography:

Aditya K Sood is a senior security researcher and PhD candidate at Michigan State University. He has already worked in the security domain for Armorize, COSEINC and KPMG. He is also a founder of SecNiche Security Labs, an independent security research arena for cutting edge computer security research. At SecNiche, he also acts as an independent researcher and security practitioner for providing services including software security and malware analysis. He has been an active speaker at industry conferences and already spoken at RSA, Virus Bulletin, HackInTheBox, ToorCon, HackerHalted, Source, TRISC, AAVAR, EuSecwest, XCON, Troopers, OWASP AppSec USA, FOSS, CERT-IN, etc. He has written content for HITB Ezine, Hakin9, ISSA, ISACA, CrossTalk, Usenix Login, and Elsevier Journals such as NESE and CFS. Email: adi.zerok@gmail.com | soodadit@cse.msu.edu