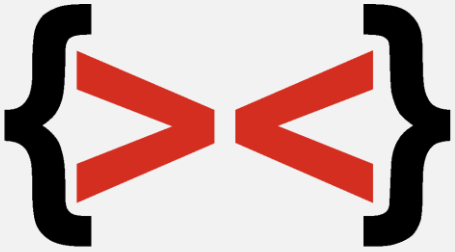
2016



Xcode Private Training

Advanced Vulnerability Development

XCODE

Advanced Vulnerability Development

Pembelajaran teknik-teknik pada pengembangan celah keamanan di Windows akibat dari keberadaan celah pada Stack Overflow.

Waktu Training: 3 hari

Objectives : Dengan Menyelesaikan training ini diharapkan peserta bisa mengembangkan diri untuk pengembangan dasar exploit

XCODE

Advanced Vulnerability Development

No	Session	Objective
Performing Basic System Management Tasks		
1	Session 1	- Buffer Overflow - Fuzzer Development (Membuat fuzzer sendiri dengan Python) - EIP & SEH Handler - Pattern create & pattern offset - Cek proteksi SafeSEH & ASLR dan menghindarinya - Uji coba perbedaan module yang terproteksi dan yang tidak terproteksi - JMP ESP - POP POP RETN (Bypass SEH) - Mengenal Bad Character - Shellcode Development untuk membuat CPU bekerja hingga 100% (Membuat dengan bahasa assembler dari awal) - Tabel kebenaran XOR - Shellcode Development untuk remote (Membuat dengan bahasa assembler dari awal) - Cara penyusunan shellcode secara cepat - Proof of concept pada exploit yang dibuat

		- Shellcode generate dengan encode shikata_ga_nai - Tugas untuk membuat exploit remote buffer overflow pada suatu web server
2	Session 2	- Latihan-latihan
3	Session 3	- Pembahasan tugas pembuatan exploit remote buffer overflow pada web server - Latihan target dengan proteksi SEH & SafeSEH EggHunter - Mengenal Egg Hunter - Implementasi Egg Hunter dengan shellcode DEP - Mengenal proteksi DEP (Data Execution Prevention) - Menghadapi mitigasi DEP dengan hasil generate ROP pada *.DLL - Fuzzing secara advanced (Ultimate) - Contoh exploit development pada suatu kasus FTP Server dan Windows 10 - Porting exploit to Metasploit Contoh Buffer overflow di linux - Membuat aplikasi vuln dan mematikan ASLR pada linux untuk pembelajaran buffer overflow di linux - Gdb & belajar perintah-perintah GDB (list main, disas main, info os, info function, etc)

		- Fuzzing dengan GDB (seg fault) & memeriksa alamat alamat memory - Konfirmasi overwrite pada register ebp & PoC untuk menjalankan shellcode dari menghitung jumlah byte shellcode, nop dan jumlah alamat yang diinject kan - Menjalankan exploit buffer overflow di shell (Terminal bukan di gdb) - Implementasi shellcode bind shell linux