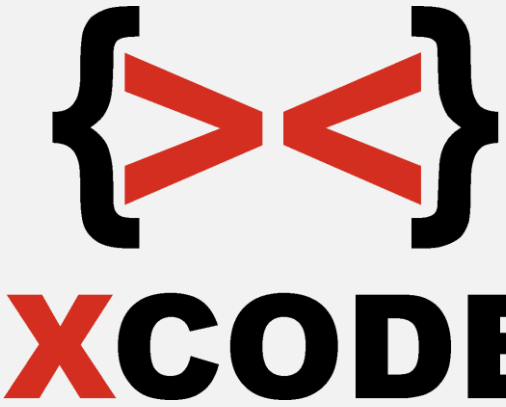
2017



Xcode Intensif Training

Ethical Hacking

Ethical Hacking

Pembelajaran teknik-teknik network hacking, wireless hacking dan web hacking secara ethical. Penambahannya adalah pembahasan exploit development dan shellcode lebih lanjut.

Waktu Training: 7 hari antara 2-5 jam.

Objectives : Dengan Menyelesaikan training ini diharapkan peserta bisa melakukan teknik-teknik network hacking, web hacking dan wireless hacking. Selain itu peserta diharapkan dapat mengembangkan diri untuk pengembangan exploit.

XCODE

Ethical Hacking

No	Session	Objective
Performing Basic System Management Tasks		
1	Session 1	- Network Fundamental - Dasar IP Address, Mac Address, pengenalan 7 layer osi, etc - FTP, SSH, Telnet, DNS, DHCP, Web Server, MySQL Server, VNC, RDP - Routing (NAT) & Port Forwarding - Dasar Kriptopgrafi - Mengenal encode / decode (base64) - Mengenal salah satu enkripsi & dekripsinya pada kriptografi simetris - Mengenal enkripsi & dekripsinya pada kriptografi asimetris (public key & private key) - Mengenal fungsi hash - Firewall - TOR Windows - Command prompt - Managemen user (Command prompt) - Shell bash

		- Repository - Setting ip address di linux - Managemen user dan group di linux - SSH & Screen - Apache Server - Firewall UFW
2	Session 2	- Ethical Hacking - Strategi, metode & langkah dasar - Scanning jaringan - Scanning IP, port, service, OS yang digunakan, dll - Dasar Hacking (Step by step) - Hacking suatu Web Server dengan searchsploit / exploit-db (Step by step) - Shell (eksploitasi di shell seperti copy data) - Hacking suatu Web Server yang terinstall di Windows 7 (Step by step) - Hacking suatu FTP Server yang terinstall di Windows 10 (Step by step) - Hacking suatu FTP Server dengan metasploit framework (Step by step) - Perintah-perintah metasploit dasar - Backdoor pada target Windows (Tiap target masuk windows, attacker langsung mendapatkan akses)

		- Scanning bug dengan Nexus dan contoh eksploitasinya dengan metasploit - Hacking pada SMB Windows XP SP3 ber-firewall (Bypass firewall pada target Windows) (Step by step) - Perintah-perintah meterpreter dasar - Hacking pada service SMB Windows Vista / Windows Server 2008 - Hacking pada service SMB Windows 7 Full Version / Windows 7 SP1 - Hacking pada service SMB Windows Server 2008 R2 Enterprise - Hacking pada target server dengan platform linux (Bypass firewall pada target linux)
3	Session 3	- 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 - SEH & SafeSEH - POP POP RETN (Bypass SEH)

		- Mengenal Bad Character - Mengenal bahasa mesin, heksadesimal dan x86 assembler instruction set opcode table - Tabel kebenaran XOR - Shellcode Development untuk membuat CPU bekerja hingga 100% (Membuat dengan bahasa assembler dari awal) - Shellcode Development untuk remote (Membuat dengan bahasa assembler dari awal) - Penggunaan nasm dan objdump untuk shellcode yang dibuat - Cara penyusunan shellcode secara cepat - Shellcode generate dengan encode shikata_ga_nai - Proof of concept pada exploit yang dibuat
4	Session 4	- Scanning IP, port, service, OS dll - Denial of Service - Web Server (intranet & internet) - Denial of Service - IP Publik (Koneksi internet target down) - Denial of Service SMBv1 - (SMB Windows XP, SMB Windows Server 2003) - Denial of Service SMBv2 - (SMB Windows Vista, SMB Windows Server 2008) - Denial of Service RDP (Rdp Windows 7) - Serangan meningkatkan proses CPU melalui SMB secara cepat di Windows 8

		- Windows 7 SMB ATTACK (Target Windows 7 FULL VERSION restart) - Windows 8.1 / 10 SMB CLIENT DoS (Blue screen) - DHCP Flooding - Netcut - ARP Spoofing (Sniffing http / telnet / pop3 / mysql & crack with wordlist / smb & crack with wordlist / ftp / Sniffing isi email (client ke smtp server) - Wireshark - Sniffing password dengan sertifikat SSL palsu pada koneksi HTTPS - Sniffing password dengan SSLStrip - Eksploitasi heartbleed untuk membaca memory dari server yang diproteksi oleh OpenSSL (Bisa mengambil password pengguna pada web dan sebagainya) - Cookies stealing (MITM + Wireshark) - Bypass login web tanpa memasukkan password (Wireshark cookie dump) ~ Session Hijacking (Cookie Hijacking)
5	Session 5	- DNS Spoofing (windows / linux) - Membuat fakelogin sendiri - Client side Attack ~ Browser IE atau firefox - Bypass login masuk windows (Berbagai versi windows seperti Windows 7 dan Windows 8.1)

		- Msfvenom untuk backdoor Windows (Backdoor di inject kan ke file exe lain) - Membuat backdoor Android (Backdoor di injek kan ke file apk lain) - Meterpreter (Download, upload, keylogger, VNC, etc) - Privilege escalation - John the ripper pada Windows / linux - Brute force attack (VNC / telnet / ftp / pop3 / http / mysql / ssh / vnc / samba linux) - Membangun wordlist dengan berbagai kriteria sendiri secara cepat (generate) - Covering Track (Menghapus jejak)
6	Session 6	- Pengenalan web dan database (HTML, PHP, MySQL) - Mengenal web hacking - Reverse domain - Google hacking - Mendeteksi jenis hash secara otomatis dan contoh melakukan cracking dari situs-situs cracking hash - Mendeteksi Web Application Firewall pada website - Cross-site scripting (XSS) - Scanning XSS - di linux dan windows - Eksploitasi XSS non persistent untuk remote target melalui client side attack (browser ~ metasploit framework)

		- Eksploitasi XSS persistent untuk menggunakan account target tanpa password login (Mengambil cookie dari target), masukkan ke browser lalu akses account target - Cross-Site Request Forgery (CSRF) - Local File Inclusion - LFI untuk mendapatkan akses PHPMyadmin - Remote File Inclusion - Remote shell target dengan celah RFI - Reverse shell - Bind shell - Scanning RFI - di linux dan windows - WPScan - WPScan for brute force (Advanced) ~ Username Enumeration + crack password (Wordlist) - Admin login scanner - Scanning SQL Injection - di Linux dan Windows - SQLMAP di Linux - SQL Injection pada web halaman login - Tabel kebenaran gerbang “AND” dan “OR” - Variasi SQL Injection pada login - Websploit untuk scan PMA - PhpMyAdmin Exploitation Advanced

		- Ngeroot Linux (Linux Privilege escalation)
7	Session 7	- Dasar wireless - Mac changer - Bypass mac filtering - Bypass SSID Hidden (teori) - Analisa dasar paket wireless untuk mengetahui ip address yang ada di jaringan (teori) SSID Flooding - Jamming - Hacking password WEP - Hacking password WPA-PSK dengan wordlist - Cracking dengan paket WPA-PSK dengan VGA Card (CUDA) - Hacking password WPA-PSK melalui WPS (tidak sampai 1 menit - tidak semua AP bisa) - Hacking passsword WPA-PSK pada router ADSL melalui eksploitasi Wifi.id - Hacking password WPA-PSK dengan LINSET