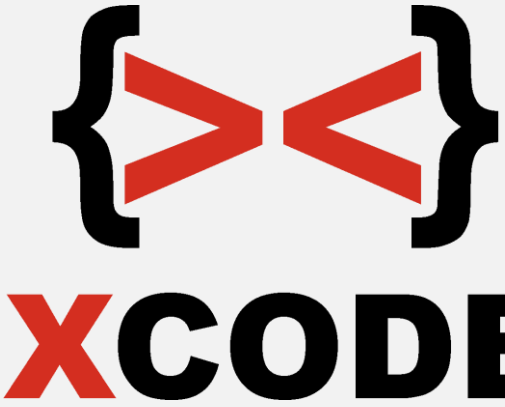
2017



Xcode Intensif Training

Ethical Hacking Advanced

Ethical Hacking – Advanced

Pembelajaran teknik-teknik network hacking, wireless hacking dan web hacking secara ethical. Penambahannya adalah pembahasan exploit development dan shellcode lebih lanjut. 8,

Waktu Training: 8 hari antara 2-5 jam.

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

Ethical Hacking Advanced

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, SMB, POP3, SMTP, MySQL Server, VNC, RDP - Subnetting (CIDR, perhitungan biner ke desimal, perhitungan subnneting, etc) - Routing (NAT) - Port Forwarding - DMZ (Demilitarized Zone) - VPN (Virtual Private Network) - Dasar Kriptopgrafi - Mengenal encode / decode (base64), disertai prakteknya dengan python - Mengenal salah satu enkripsi & dekripsinya pada kriptografi simetris, disertai prakteknya dengan python - Mengenal enkripsi & dekripsinya pada kriptografi asimetris (public key & private key), disertai prakteknya dengan python

		- Mengenal fungsi hash disertai prakteknya untuk membangun hashnya dengan python dan cara crack nya dengan menggunakan wordlist - Firewall - Port Knocking
2	Session 2	- Proxy - TOR Windows - TOR Linux (Advanced) ~ Hacking Server seperti FTP Server, SSH Server, dst dengan koneksi TOR - SSH Tunnel - Command prompt - Managemen user (Command prompt) - Pembelajaran Shell Bash - Repository - Recovery mode di linux - Setting IP Client di linux (Permanen & non permanen) - Menambah ip baru pada interface - Managemen user dan group di linux - File Security : chown, chgrp, chmod (numeric coding, letter coding) - SSH Server (user & admin) - Screen

		- SAMBA (read only, writeable, valid users) - Server APACHE - Firewall ufw - SSH Server (user & admin) - SAMBA (read only, writeable, valid users) - Server APACHE Keamanan - Mematikan recovery pada GRUB - Firewall ufw Pengawasan - Mengenali log-log server dan mengawasi client yang login
3	Session 3	- 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) - 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)
4	Session 4	- 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
5	Session 5	- 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) - 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 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)

6	Session 6	- DNS Spoofing (windows / linux) - Membuat fake login sendiri - Client side Attack ~ Browser IE atau firefox - Bypass login masuk windows (Berbagai versi windows seperti Windows 7, Windows 8.1 dan Windows 10) - Msfvenom untuk backdoor Windows 8.1 & mendapatkan akses administrator (Local Exploit) - 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)
7	Session 7	- 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 pada kasus celah pada plugin wordpress - LFI untuk mendapatkan username pada linux - WPScan - WPScan for brute force (Advanced) ~ Username Enumeration + crack password (Wordlist) - Admin login scanner - Scanning SQL Injection - di Linux dan Windows - Remote File Inclusion - Scanning RFI - di linux dan windows

		- PHP Shell Development (Membuat PHP Shell sendiri dari awal untuk RFI) - Remote shell target dengan celah RFI - Bind Shell & Reverse shell - SQL Injection manual (Dasar) - SQL Injection - bypass login wp - PHP upload & logger Login - Havij di 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
	Session 8	- Dasar Wireless LAN - Mengenal keamanan wireless pada access point - Mac changer - Bypass mac filtering (Deny the stations specified by any enabled entries in the list to access) - Bypass mac filtering (Allow the stations specified by any enabled entries in the list to access)

		- Bypass SSID Hidden (teori) - Analisa dasar paket wireless untuk mengetahui ip address yang ada di jaringan SSID Flooding - Jamming - Hacking WEP - Hacking password WPA-PSK dengan menggunakan 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