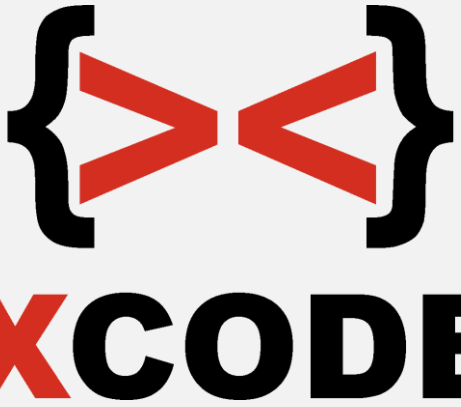
2018



Xcode Private Training

Advanced Network Hacking &

Wireless Hacking

XCODE

Advanced Network hacking & Wireless hacking

Pembelajaran teknik-teknik network hacking secara ethical. Penambahannya adalah materi wireless hacking.

Waktu Training: 6 hari antara 2-5 jam.

Objectives : Dengan Menyelesaikan training ini diharapkan peserta bisa melakukan teknik-teknik network hacking & Wireless hacking.

XCODE

Basic Network hacking & Wireless 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 dan contoh encode pada payload saat eksploitasi

		- Backdoor pada target Windows (Tiap target masuk windows, attacker langsung mendapatkan akses) - Scanning bug dengan Nessus dan contoh eksploitasinya dengan metasploit - Hacking pada SMB Windows XP SP3 ber-firewall (Bypass firewall pada target Windows) (Step by step) untuk mendapatkan akses shell - Perintah-perintah meterpreter dasar - Hacking pada service SMB Windows Vista / Windows Server 2008 untuk mendapatkan akses shell - Hacking pada service SMB Windows 7 Full Version /Windows 7 SP1 untuk mendapatkan akses shell / meterpreter - Hacking pada service SMB Windows Server 2008 R2 Enterprise untuk mendapatkan akses shell - Hacking Mikrotik Router v6 pada service winbox (Langsung mendapatkan password mikrotik melalui jaringan, bukan brute force)
3	Session 3	- Hacking pada service SMB Windows 8.1/10 yang mengijinkan share folder tanpa password untuk mendapatkan akses shell (Bypass Windows Defender) - Hacking pada service SMB Windows Server 2012 R2/2016 yang mengijinkan share folder tanpa password untuk mendapatkan akses shell (Bypass Windows Defender) - Hacking pada target samba server linux ubuntu server untuk mendapatkan akses shell - 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 - 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) - 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) (Blue Screen) - Denial of Service SMBv2 - (SMB Windows Vista, SMB Windows Server 2008) (Blue Screen) - Denial of Service RDP (RDP Windows 7) (Blue Screen) - Denial of Service SMB Windows 7 SP1 (Blue Screen) - Denial of Service SMB Windows 8.1 / 10 / 2012 R2 / 2016 dengan sharing folder tanpa password (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 - Eksploitasi heartbleed untuk membaca memory dari server yang diproteksi oleh OpenSSL (Bisa mengambil password pengguna pada web dan sebagainya) - Sniffing password dengan SSLStrip - Cookies stealing (MITM + Wireshark) dengan tujuan bypass login web tanpa memasukkan password

		(Wireshark cookie dump) ~ Session Hijacking (Cookie Hijacking)
5	Session 5	- DNS Spoofing (windows / linux) - Membuat fake login sendiri - Client side Attack ~ Browser IE atau firefox - Eksploitasi celah remote pada Microsoft Word 2010 / 2013 / 2016) - Bypass login masuk windows (Berbagai versi windows seperti Windows 7, Windows 8.1 dan Windows 10) - Msfvenom untuk backdoor Windows (Backdoor diinject kan ke file exe lain) - Membuat backdoor Android (Backdoor di injek kan ke file apk lain) - Meterpreter (Download, upload, keylogger, VNC, etc) - Privilege escalation pada Windows Server 2008 / Windows 8.1 / Windows 10 / Windows Server 2012 R2 / 2016 - Mendapatkan password logon / admin windows secara langsung di desktop windows dengan akses administrator pada Windows 7 / Windows 8 - 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)

6	Session 6	- 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 (teori) SSID Flooding (teori) - Jamming - Hacking WEP - Hacking password WPA-PSK dengan menggunakan wordlist - Cracking password WPA-PSK dengan semua kemungkinan pada kriteria tertentu di linux (bukan daftar kata yang ada pada file text) - 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

XCODE