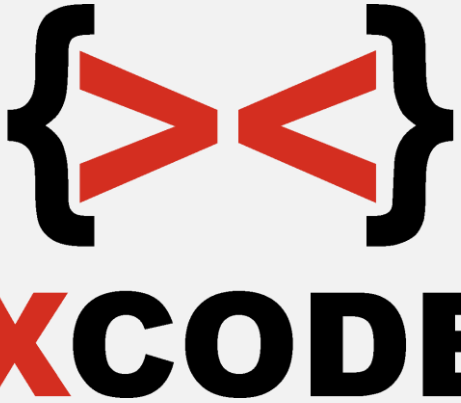
2017



Xcode Private Training

Network hacking & Security

XCODE

Network hacking & Security

Pembelajaran teknik-teknik network hacking secara ethical, pengembangan exploit dan security.

Waktu Training: 5 hari antara 2-5 jam.

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

XCODE

Network hacking & Security

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 - IDS (Intrusion detection system) dengan Snort
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 Nexus dan contoh eksploitasinya dengan metasploit - Scanning bug dengan OpenVas 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) Pengamanan - Teknik untuk meminimalisir serangan ke server dan pengamanannya secara umum - Teknik melakukan banned otomatis pada ip target yang melakukan scanning menggunakan NMAP dengan option seperti misal -sV dan -A
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 - Jump Short - 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). Contoh pada apache server, web dari OS mikrotik dan access point tp-link - 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

		- Cookies stealing (MITM + Wireshark) - Eksploitasi heartbleed untuk membaca memory dari server yang diproteksi oleh OpenSSL (Bisa mengambil password pengguna pada web dan sebagainya) - Bypass login web tanpa memasukkan password (Wireshark cookie dump) ~ Session Hijacking (Cookie Hijacking) Pengamanan - Mengamankan Web Server dari serangan DoS tertentu (Pengujian sebelum diamankan pada serangan sebelumnya dan setelah diamankan) (Linux) - Pengamanan dari serangan ARP Spoofing dan pengamanan lainnya (Linux) - Membangun komunikasi data pada Web Server dengan membuat SSL Certificate (HTTPS) (Linux)
5	Session 5	- DNS Spoofing (windows / linux) - Membuat fake login sendiri - Client side Attack ~ Memanfaatkan celah browser - Client side Attack ~ Memanfaatkan celah adobe Acrobat - 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) – Tersembunyi / tidak terlihat - Membuat backdoor Android (Backdoor di injek kan ke file apk lain) – Tersembunyi / tidak terlihat

		- 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) Pengamanan - Pengamanan umum - Membatasi jumlah login SSH yang salah - Teknik melakukan banned pada ip attacker secara otomatis yang melakukan serangan brute force pada SSH - SSH Honeypot