2020

XCODE

X-code Platinum Training

Online

Advanced Ethical Hacking & Security v2

XCODE

X-code Platinum Training (Online)

Advanced Ethical Hacking & Security v2

Pembelajaran teknik-teknik network hacking dan web hacking secara ethical. Penambahannya adalah pembahasan exploit development dan shellcode lebih lanjut. Tambahan dari program materi ini adalah disertai pengamanannya sesuai silabus.

Jumlah pertemuan : 15x pertemuan.

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

X-code Platinum Training (Online)

Advanced Ethical Hacking & Security v2

No	Session	Objective
Performing Basic System Management Tasks		
1	Session 1	- Computer Security & IT Security Awareness - Mengenal data & representasinya, hexdump pada file, ascii table, hexwrite - 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 Kriptografi - Mengenal encode / decode (base64), disertai prakteknya dengan python - Mengenal dasar enkripsi & dekripsi pada kriptografi

		simetris pada caesar (prakteknya dengan python), substitusi (enkripsi dari penyedia layanan di web dan contoh cracknya dari penyedia layanan di web online), enkripsi dan dekripsi dengan XOR (prakteknya dengan python) - Mengenal enkripsi 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 - Mendeteksi jenis hash secara otomatis dan contoh melakukan cracking dari situs cracking hash - Contoh crack hash MD5 / SHA1 dengan Hashcat - Mengenal reverse engineering dengan contoh prakteknya menggunakan program IDA Pro (source code, compile, binary (executable), disassembly & jump to pseudocode)
2	Session 2	- Firewall - Port Knocking - Forwarding pada managed switch - 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) - SMB Client - Server Apache - Server Nginx Keamanan - Mematikan recovery mode pada GRUB - Firewall ufw - Blokir ip ke server dengan firewall ufw - Blokir semua ip client kecuali ip client tertentu pada port service tertentu (Kasusnya misal seperti website hanya bisa dibuka ip tertentu atau juga bisa misal untuk akses ssh hanya bisa diakses ip tertentu, tapi untuk

		web bisa diakses semua ip yang bisa terhubung) Pengawasan - Mengenali log-log server dan mengawasi client yang login - IDS (Intrusion detection system) dengan Snort (Linux)
3	Session 3	- Ethical Hacking - Scanning jaringan - Tips dan trik untuk mengetahui Ip melalui nama komputer di kali linux, mengetahui ip dan mac di jaringan secara cepat di kali linux, dan sebagainya - Scanning IP, port, service, OS yang digunakan, dan sebagainya - CVE dan situs-situs penyedia exploit - Dasar Hacking (Step by step) - Hacking suatu Web Server dengan searchsploit / exploit-db (Step by step) - Shell (eksploitasi di shell seperti copy data) - Mengambil password-password seperti facebook, yahoo mail dan sebagainya yang disimpan pada browser seperti firefox (firefox baru) dan sebagainya, sampai FTP Server filezilla bisa diambil passwordnya melalui shell (post exploitation) - Hacking suatu Web Server yang terinstall di Windows 7 (Step by step) - Hacking suatu router dengan routersploit - Hacking suatu SSH Server dengan memanfaatkan

		situs mesin pencari (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 service SMB Windows XP SP3 ber-firewall (Bypass firewall pada target Windows) (Step by step) untuk mendapatkan akses meterpreter / shell - Hacking pada service SMB Windows 7 SP1 untuk mendapatkan akses shell / meterpreter - Hacking pada service SMB Windows Server 2008 R2 Enterprise untuk mendapatkan akses shell - Hacking pada service SMB Windows 8.1 / 10 / 2012 R2 yang mengijinkan share folder tanpa password untuk mendapatkan akses shell (Bypass Windows Defender) - Hacking Mikrotik Router v6 pada service winbox (Langsung mendapatkan password mikrotik melalui jaringan, bukan brute force)
4	Session 4	- Hacking SAMBA pada suatu target Ubuntu Server untuk mendapatkan akses shell linux (Target Samba dalam kondisi ada yang dishare foldernya tanpa password dengan hak akses writeable) - Hacking pada suatu target FTP server dengan platform linux (Bypass firewall pada target linux)

		Pengamanan - Teknik untuk meminimalisir serangan ke server dan pengamanannya secara umum - Teknik melakukan banned otomatis di linux pada ip target yang melakukan scanning menggunakan NMAP dengan option seperti misal -sV dan -A (Linux) - Scanning dan pembangunan komputer lab untuk fuzzing hingga pengembangan expoit - Mengenal Memory layout - Buffer Overflow - Fuzzer Development (Membuat fuzzer sendiri dengan Python) - EIP & SEH Handler - Pattern create & pattern offset - JMP ESP - 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 - 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
5	Session 5	- Pembahasan tugas pembuatan exploit remote buffer overflow pada web server - SEH (Structured Exception Handling) - Latihan target program yang memiliki proteksi SEH - Cek proteksi SafeSEH / ASLR dan menghindarinya - POP POP RETN (Bypass SEH) - Mengenal Jump Short - Uji coba perbedaan module yang terproteksi dan yang tidak terproteksi 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 - Membangun exploit untuk metasploit berdasarkan exploit python yang dibuat sebelumnya.

		Contoh Buffer overflow di linux - Gdb & belajar perintah-perintah GDB (list main, disas main) - Fuzzing dengan GDB (seg fault) & memeriksa alamat eip - PoC untuk menjalankan shellcode dari menghitung jumlah byte shellcode, nop dan jumlah alamat yang diinjeksikan - Menjalankan exploit buffer overflow di shell (Terminal bukan di gdb) - Implementasi shellcode bind shell linux
6	Session 6	- Scanning IP, port, service, OS dll - Denial of Service - Web Server. Contoh pada apache server, web dari OS mikrotik dan access point tp-link - 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) - Denial of Service SMB Windows 7 (Blue Screen) - Denial of Service Windows 8.1 / 10 / 2012 R2 pada SMB Service yang mengijinkan share folder tanpa password (Blue Screen) - Denial of Service SMB Windows 10 pada celah CVE-2020-0796 (Blue screen) - Netcut

		- ARP Spoofing - Wireshark - Sniffing password dengan SSLStrip - Eksploitasi heartbleed untuk membaca memory dari server yang diproteksi oleh OpenSSL (Bisa mengambil password pengguna pada web dan sebagainya) Pengamanan - Mengatasi serangan Netcut di Windows (Pengujian sebelum diamankan dan setelah diamankan) - Pengamanan di linux dari serangan netcut dan serangan sniffing password dengan ARP Spoofing (Pengujian sebelum diamankan dan setelah diamankan)
7	Session 7	- DNS Spoofing - Membuat fake login sendiri - Client side Attack ~ Browser IE (Windows XP/Windows 7) / Client side Attack ~ Browser Firefox (Windows XP) / Client side Attack ~ Browser ~ Adobe Flash (Pengujian di IE 11 & Windows 8.1) - Eksploitasi celah remote pada Microsoft Word 2013 / 2016) - Msfvenom untuk backdoor Windows (Backdoor di inject kan ke file exe lain) - Meterpreter (Download, upload, keylogger, VNC, etc) - Privilege escalation (Menaikkan hak akses dari user biasa menjadi akses admin pada Windows Server 2008 / Windows 7 SP1 / Windows 8.1 / Windows 10 /

		Windows Server 2012 R2 / Windows server 2016 - Cara mendapatkan password login windows 7 / 8 secara langsung dengan akses administrator (Mengambil dari memory, bukan brute force) - Cara mendapatkan password login pada Linux Ubuntu Desktop secara langsung dengan akses root (Mengambil dari memory, bukan brute force) - Cara mendapatkan NTLM hash windows 10 dengan akses administrator (Mengambil dari memory), lalu crack NTLM hashnya dengan hashcat (brute force)
8	Session 8	- Crack password Windows dengan John the ripper - Crack password Linux dengan John the ripper - Brute force attack dengan wordlist (VNC / telnet / ftp / pop3 / http / mysql / rdp / ssh / vnc / samba linux) - Membangun wordlist dengan berbagai kriteria sendiri secara cepat (generate) Pengamanan - Pengamanan umum - SSH Honeypot (Linux) - Membatasi jumlah login SSH yang salah (Linux) - Port Knocking pada SSH (Linux) Tambahan - Cara mendeteksi SSH Honeypot - Pengenalan web dan database (HTML, PHP, MySQL) - Form, action, metode post, input type text dan submit,

		koneksi database, mysqli_connect, mysqli_query, pengkondisian & mysql_num_rows, create database, use, create table, insert, select, alter, update, drop. - Managemen user pada MySQL - Mengenal web hacking - Scan untuk mendeteksi nama web server yang digunakan serta versinya, sistem operasi apa yang digunakan, jika menggunakan PHP maka menggunakan PHP versi berapa, jika menggunakan CMS maka apa nama CMS yang digunakan, jika CMS wordpress maka versi berapa wordpressnya dan sebagainya - Whois - Reverse domain - Teknik-teknik bypass cloudflare - Scanning sub domain
9	Session 9	- Google hacking - Google hacking untuk kasus-kasus khusus (mendapatkan file-file dari folder yang terbuka,dst) - Mencari situs sesuai kriteria dengan cepat pada bing (Menampilkan semua yang dicari dalam 1 halaman) - Mencari halaman login admin (Secara otomatis mencari halaman web login admin berdasarkan dengan mencoba-coba nama-nama file halaman login admin yang umum) - Dirbuster - Dirsearch

		- Dirhunt - Scan lebih dalam untuk mendapatkan versi pada suatu CMS, untuk kasus jika tidak terdeteksi menggunakan salah satu tool dari bawaan kali linux - Mendeteksi Web Application Firewall pada website - Memahami Get Method & post method - Cross-site scripting (XSS) - Pengamanan XSS dari sisi pemrograman - Scanning celah XSS di linux - Variasi teknik-teknik injeksi pada target dengan celah XSS - Eksploitasi XSS persistent untuk menggunakan akun target tanpa password login (Mengambil cookie dari target), masukkan ke browser lalu akses akun target - Memahami keamanan cookie dengan mengenal session cookie httponly dan session cookie secure - Bypass filter upload image dengan burp suite - Pengamanan upload dengan .htaccess - Variasi teknik-teknik bypass filter upload - Cross-Site Request Forgery (CSRF)
10	Session 10	- Remote File Inclusion - WPScan - Scanning celah RFI di linux Contoh alur mendapatkan akses root dari hasil

		eksploitasi web yang vulnerable Crack password dengan john the ripper Menambah user dan menjadikan user menjadi admin Mengambil username dan password linux dari memory (Target : Ubuntu Desktop) Menyisipkan backdoor upload ke file php dan memasang backdoor php shell - Remote shell target dengan celah RFI - Bind Shell & Reverse shell - Ngeroot Linux - Contoh pengamanan terhadap serangan Remote File Inclusion dari sisi pemrograman - Contoh pengamanan terhadap serangan Remote File Inclusion dari sisi konfigurasi PHP.INI - Local File Inclusion - LFI untuk mendapatkan akses PHPMyadmin pada kasus celah pada plugin wordpress - Scanning celah LFI di linux - LFI untuk mendapatkan username pada linux - Contoh pengamanan LFI dari sisi programming - Contoh pengamanan LFI dari sisi konfigurasi PHP.INI - Variasi teknik-teknik injeksi pada target dengan celah LFI - Cara mendapatkan akses shell dari LFI dengan

		reverse shell - WPScan for brute force (Advanced) ~ Username Enumeration + crack password (Wordlist) - PHP Shell Development (Membuat PHP Shell sendiri dari awal untuk RFI) - Command Injection dan teknik-teknik variasinya
11	Session 11	- IDOR (Insecure Direct Object References) - Scanning celah SQL Injection di linux - SQL Injection union (MANUAL) - BLIND SQL Injection (MANUAL) - TIME BASED SQL Injection (MANUAL) - Havij di Windows - SQLMAP di Linux hingga crack hash password login dengan brute force - SQLMAP di Linux untuk masuk ke akses phpmyadmin - Contoh pengamanan SQL Injection dari sisi pemrograman - SQL Injection - bypass login wp - PHP upload & logger Login - SQL Injection pada web halaman login - Tabel kebenaran gerbang AND dan OR - Contoh pengamanan pada web login dari SQL Injection dari sisi pemrograman (Filter pada input

		variablel) - Contoh pengamanan pada web login dari SQL Injection dari sisi pemrograman (pengecekan dengan input password)
12	Session 12	- Instalasi dan konfigurasi WAF (A web application firewall) - SQL Injection untuk BYPASS WAF (ADVANCED) - Brute force dengan Burp Suite - Hacking untuk mendapatkan akses shell dengan memanfaatkan celah shellsock - Hacking wordpress secara default pada versi tertentu, bukan pada celah dari plugin atau themes (Mengganti isi content) - Hacking Joomla secara default pada versi-versi tertentu, bukan pada celah component atau tambahan lainnya (Mengakses shell linux) - Websploit untuk scan PMA - PhpMyAdmin Exploitation (Advanced) Covering tracks - Menghapus log server dan menghapus history.
13	Session 13	Pengamanan - Pengamanan web server dari PHP Shell (Pengujian sebelum diamankan dan setelah diamankan) (Linux) - Eksploitasi PHP 7 (bypass disable_function & open_basedir) serta pengamanannya)

		- Periksa celah kernel linux dan update kernel (Mengamankan kernel dari rooting exploit yang sebelum berhasil di rooting) - Deteksi PHP Shell di web server secara otomatis (Linux) - Menonaktifkan Directory Listing (Linux) - Mengganti url default URL pada PHPMyadmin (Linux) - Instalasi dan konfigurasi WAF (A web application firewall) (Linux) - Cara agar teknik SQL Injection khusus bypass WAF tidak mampu bypass WAF (Linux) - Pengujian pengamanan maksimal pada WAF untuk serangan XSS, RFI & SQL Injection (Termasuk serangan SQL Injection untuk bypass WAF) - Teknik melakukan banned pada ip attacker secara otomatis yang melakukan serangan brute force pada SSH (Linux) - Teknik melakukan banned secara otomatis pada ip target yang melakukan scanning otomatis atau cek celah pada variabel secara manual pada web yang diamankan (Linux)
14	Session 14	- Pertahanan dengan cloudflare - Setting name servers di domain dengan name server dari cloudflare - Set SSL / TLS encryption mode is Full (Strict) - pengamanan dengan cloudflare origin CA certificate on the server - Under Attack Mode di cloudflare

		- Setting virtualhost di web server - 2 Teknik bypass ip cloudflare disertai pengamanannya - Teknik agar web tidak bisa diakses lewat ip - Log pada web server jika diakses lewat domain / subdomain
15	Session 15	- Dasar Wireless LAN - Mengenal keamanan wireless pada access point - Macchanger - 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) - Hacking WEP - Hacking password WPA-PSK dengan menggunakan wordlist di linux - Cracking password WPA-PSK dengan semua kemungkinan pada kriteria tertentu di linux (bukan daftar kata yang ada pada file text / wordlist) - Hacking password WPA-PSK melalui WPS (tidak sampai 1 menit - tidak semua AP bisa) - Hacking password WPA-PSK dengan LINSET