2024

XCODE

Ethical Hacking & Security Excellence

XCODE

X-code Platinum Training

Ethical Hacking & Security Excellence

Pembelajaran teknik-teknik yang berhubungan cyber security, network hacking, web hacking, exploit development & penetration testing.

Waktu Training: 6x pertemuan.

X-code Platinum Training

Ethical Hacking & Security Excellence

No	Session	Objective
Performing Basic System Management Tasks		
1	Sesi 1	Sesi 1 Cyber Security Fundamental Dasar jaringan komputer Keamanan protokol jaringan - FTP - SSH - Telnet - SMTP - HTTP - POP3 - SMB - MySQL Dasar kriptografi - Encode & Decode - Encrypt & Decrypt (Simeteris & Asimetris) - Fungsi hash Dasar Reverse Engineering - Target file binary Linux - Target file binary Windows TOR & TSOCKS

		Dasar terminal linux Firewall Snort
2	Sesi 2	Sesi 2 Ethical Hacking Contoh langkah-langkah hacking pada aplikasi vulnerable di windows 10 untuk mendapatkan akses shell - Scanning target di jaringan - Scanning target pada target - Pencarian informasi celah keamanan dan exploit - Eksploitasi celah service target Nessus Langkah-langkah Hacking SMB Windows 7 64 bit (Firewall aktif & Windows Defender aktif) Meterpreter - Keylogger - VNC - Upload & download Langkah-langkah Hacking SMB Windows 10 32 bit dengan sharing folder tanpa password Langkah-langkah pasang backdoor di Windows 10 – Otomatis aktif saat komputer target menjalankan Windows 10 Contoh langkah-langkah hacking FTP Server di target linux - Identifikasi aplikasi FTP Server

		- Pencarian exploit yang sesuai - Eksploitasi Contoh langkah-langkah hacking SAMBA di target linux - Scanning - Identifikasi service samba dan versinya - Pencarian exploit yang sesuai - Eksploitasi Pengamanan dengan firewall dan update
3	Sesi 3	Sesi 4 Exploit Development pada target Windows 10 Buffer Overflow Membuat program Fuzzer dengan python Pattern create & pattern offset Extended Instruction Pointer (EIP) Extended Stack Pointer (ESP) NOPSleed Mengenal Bad Character Bypass SEH Bypass SafeSEH Bypass ASLR (Address Space Layout Handling) Generate shell reverse shell dengan msfvenom Jumpshort

		PoC
4	Sesi 4	Sesi 4 Hacking Website secara beretika Information Gathering - Mencari berbagai informasi tentang web target - Mencari file-file sensitif - Mendeteksi WAF pada target - Scanning keberadaan subdomain pada web target Contoh Teknik Bypass Cloudflare untuk mendapatkan ip address web target Denial of Service pada web server Apache & Nginx Pengamanan dari serangan Denial of Server pada Apache & Nginx XSS (Cross Site Scripting) – Non Persistent Pengamanan dari serangan XSS XSS (Cross Site Scripting) – Persistent Mengambil Cookie dengan memanfaat XSS untuk login tanpa password RFI (Remote File Inclusion) Pengamanan dari serangan RFI dari sisi pemrograman dan PHP.INI Privilege Escalation pada target linux Backdoor akun pada target linux

		Rootkit Incident handling - Analisa log - Mencari backdoor dengan cepat - Deteksi PHP Shell otomatis dengan cepat - Menghapus backdoor - Perbaikan celah keamanan pada aplikasi
5	Session 5	Sesi 5 LFI (Local File Inclusion) Contoh cara mendapatkan akses shell dari celah Local File Inclusion Pengamanan dari serangan LFI dari sisi pemrograman dan PHP.INI Brute force login pada web Brute force login pada CMS Wordpress & Joomla Contoh langkah-langkah Hacking CMS (Wordpress dan Joomla) Insecure Direct Object References (IDOR) SQL Injection (GET dan POST) Pengamanan dari serangan SQL Injection Bypass Web Application Firewall (WAF) – SQL Injection Bypass Web Application Firewall (WAF) – XSS Pengamanan maksimal dengan WAF Pengamanan dari sisi serangan PHP Shell dan

		serangan disable function
6	Sesi 6	Sesi 6 The Penetration Testing Execution Standard Dasar Pentest Pre-engagement Interactions General Questions Penetration testing offers Intelligence Gathering OSINT Threat Modeling Vulnerability Analysis Testing Exploitation CVSS Score Post Exploitation Vulnerability Impact and risks Recommendation Reporting