2020

XCODE

Xcode Private Training

Advanced Network Hacking,

security & wireless hacking

XCODE

Advanced Network hacking, security & wireless hacking

Pembelajaran teknik-teknik network hacking secara ethical disertai keamanan, penambahannya adalah materi wireless hacking.

Jumlah pertemuan : 7x Pertemuan

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

XCODE

Advanced Network hacking, security & 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, SMB - Subnetting (CIDR, perhitungan biner ke desimal, perhitungan subnneting, etc) - Routing (NAT) - Port Forwarding - Dasar Kriptografi - Mengenal encode / decode (base64), disertai prakteknya dengan python - Mengenal dasar enkripsi & dekripsi pada kriptografi simetris dan asimetris (public key & private key) - Mengenal fungsi hash disertai prakteknya untuk membangun hashnya dengan python dan cara crack nya dengan menggunakan wordlist - Firewall - TOR Windows - Command prompt

		- Managemen user (Command prompt) - Pembelajaran Shell Bash - Repository - Setting IP Client di linux (Permanen & non permanen) - Managemen user dan group di linux - File Security : chown, chgrp, chmod (numeric coding, letter coding) - SSH Server (user & admin) - Server APACHE - Firewall ufw - Mengenali log-log server dan mengawasi client yang login - IDS (Intrusion detection system) dengan Snort (Linux)
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 Pengawasan - Mengenali log-log server dan mengawasi client yang login

		- IDS (Intrusion detection system) dengan Snort (Linux)
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) - 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 - Hacking pada service SMB Windows Server 2008 R2 Enterprise untuk mendapatkan akses shell - Hacking pada service SMB Windows 8.1 / 10 / Server 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 pada ip target yang melakukan scanning menggunakan NMAP dengan option seperti misal -sV dan -A (Linux) - 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). 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) (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 / Server 2012 R2 pada SMB Service yang mengijinkan share 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 SSLStrip - Eksploitasi heartbleed untuk membaca memory dari server yang diproteksi oleh OpenSSL (Bisa mengambil password pengguna pada web dan sebagainya) - Cookie stealing dengan MITM (Cain + Wireshark) untuk bypass login web tanpa memasukkan password (Session Hijacking)

		Pengamanan - Mengamankan Web Server dari serangan DoS tertentu (Pengujian sebelum diamankan dan setelah diamankan) (Linux) - 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)
6	Session 6	- DNS Spoofing - Membuat fake login sendiri - Client side Attack ~ Browser IE atau firefox - Eksploitasi celah remote pada Microsoft Word 2010 / 2013 / 2016 - Bypass login masuk windows 7 dan 8.1 - Msfvenom untuk backdoor Windows (Backdoor di inject kan ke file exe lain) - Meterpreter (Download, upload, keylogger, VNC, etc) - Membangun backdoor untuk remote Windows 10 dan bypass antivirus internal Windows 10 (Windows Defender) - Privilege escalation pada Windows Server 2008 / Windows 8.1 / Windows 10 / Windows Server 2012 R2 / 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) - 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 - Teknik melakukan banned pada ip attacker secara otomatis yang melakukan serangan brute force pada SSH (Linux) - Port Knocking pada SSH (Linux) - SSH Honeypot (Linux) Tambahan : - Cara mendeteksi SSH Honeypot (Linux)
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) - Analisa dasar paket wireless untuk mengetahui ip address yang ada di jaringan (teori) - Bypass SSID Hidden - SSID Flooding - 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 password WPA-PSK dengan LINSET