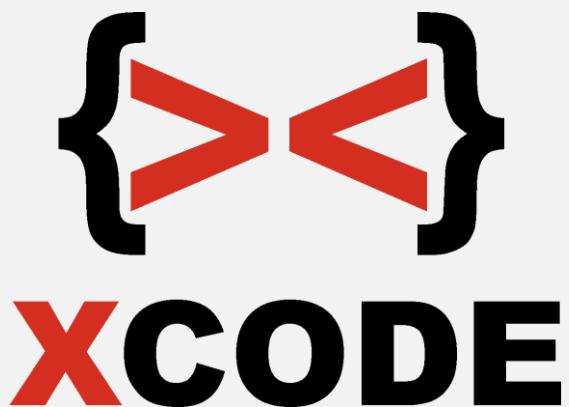
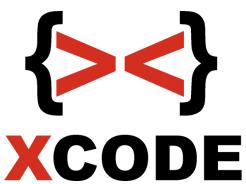


2020



**Xcode Private Training**

**Advanced Network Hacking,  
security & wireless hacking**

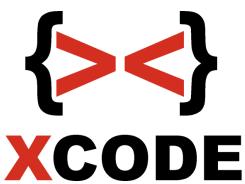


## **Advanced Network hacking, security & wireless hacking**

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

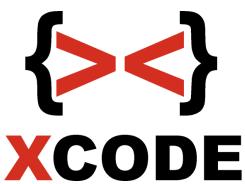
**Jumlah pertemuan :** 7x Pertemuan

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

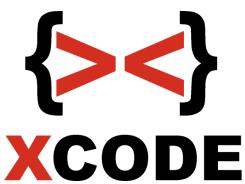


## Advanced Network hacking, security & wireless hacking

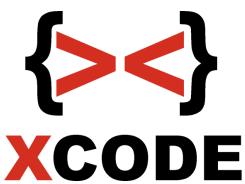
No	Session	Objective
<b>Performing Basic System Management Tasks</b>		
1	Session 1	<ul style="list-style-type: none"><li>- Network Fundamental</li><li>- Dasar IP Address, Mac Address, pengenalan 7 layer osi, etc</li><li>- FTP, SSH, Telnet, DNS, DHCP, Web Server, SMB</li><li>- Subnetting (CIDR, perhitungan biner ke desimal, perhitungan subnetting, etc)</li><li>- Routing (NAT)</li><li>- Port Forwarding</li><li>- Dasar Kriptografi</li><li>- Mengenal encode / decode (base64), disertai prakteknya dengan python</li><li>- Mengenal dasar enkripsi &amp; dekripsi pada kriptografi simetris dan asimetris (public key &amp; private key)</li><li>- Mengenal fungsi hash disertai prakteknya untuk membangun hashnya dengan python dan cara crack nya dengan menggunakan wordlist</li><li>- Firewall</li><li>- TOR Windows</li><li>- Command prompt</li></ul>



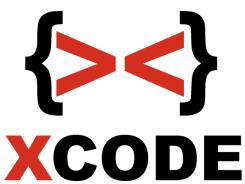
		<ul style="list-style-type: none"><li>- Managemen user (Command prompt)</li><li>- Pembelajaran Shell Bash</li><li>- Repository</li><li>- Setting IP Client di linux (Permanen &amp; non permanen)</li><li>- Managemen user dan group di linux</li><li>- File Security : chown, chgrp, chmod (numeric coding, letter coding)</li><li>- SSH Server (user &amp; admin)</li><li>- Server APACHE</li><li>- Firewall ufw</li><li>- Mengenali log-log server dan mengawasi client yang login</li><li>- IDS (Intrusion detection system) dengan Snort (Linux)</li></ul>
2	Session 2	<ul style="list-style-type: none"><li>- Firewall</li><li>- Port Knocking</li><li>- Forwarding pada managed switch</li><li>- Proxy</li><li>- TOR Windows</li><li>- TOR Linux (Advanced) ~ Hacking Server seperti FTP Server, SSH Server, dst dengan koneksi TOR</li><li>- SSH Tunnel</li><li>- Command prompt</li></ul>



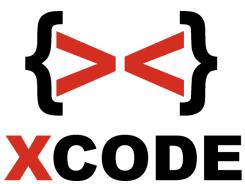
- Managemen user (Command prompt)
- Pembelajaran Shell Bash
- Repository
- Recovery mode di linux
- Setting IP Client di linux (Permanen & non permanen)
- Menambah ip baru pada interface
- Managemen user dan group di linux
- File Security : chown, chgrp, chmod (numeric coding, letter coding)
- SSH Server (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



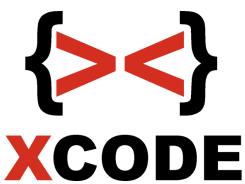
		- IDS (Intrusion detection system) dengan Snort (Linux)
3	Session 3	<ul style="list-style-type: none"><li>- Ethical Hacking</li><li>- Strategi, metode &amp; langkah dasar</li><li>- Scanning jaringan</li><li>- Scanning IP, port, service, OS yang digunakan, dll</li><li>- Dasar Hacking (Step by step)</li><li>- Hacking suatu Web Server dengan searchsploit / exploit-db (Step by step)</li><li>- Shell (eksplorasi di shell seperti copy data)</li><li>- Hacking suatu Web Server yang terinstall di Windows 7 (Step by step)</li><li>- Hacking suatu FTP Server yang terinstall di Windows 10 (Step by step)</li><li>- Hacking suatu FTP Server dengan metasploit framework (Step by step)</li><li>- Perintah-perintah metasploit dasar dan contoh encode pada payload saat eksplorasi</li><li>- Backdoor pada target Windows (Tiap target masuk windows, attacker langsung mendapatkan akses)</li><li>- Scanning bug dengan Nessus dan contoh eksplorasinya dengan metasploit</li><li>- Hacking pada SMB Windows XP SP3 ber-firewall (Bypass firewall pada target Windows) (Step by step) untuk mendapatkan akses shell</li><li>- Perintah-perintah meterpreter dasar</li></ul>



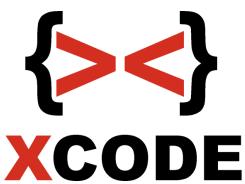
		<ul style="list-style-type: none"><li>- Hacking pada service SMB Windows Vista / Windows Server 2008 untuk mendapatkan akses shell</li><li>- Hacking pada service SMB Windows 7 Full Version / Windows 7 SP1 untuk mendapatkan akses shell</li><li>- Hacking pada service SMB Windows Server 2008 R2 Enterprise untuk mendapatkan akses shell</li><li>- Hacking pada service SMB Windows 8.1 / 10 / Server 2012 R2 yang mengijinkan share folder tanpa password untuk mendapatkan akses shell (Bypass Windows Defender)</li><li>- Hacking Mikrotik Router v6 pada service winbox (Langsung mendapatkan password mikrotik melalui jaringan, bukan brute force)</li></ul>
4	Session 4	<ul style="list-style-type: none"><li>- 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)</li><li>- Hacking pada suatu target FTP server dengan platform linux (Bypass firewall pada target linux)</li></ul> <p>Pengamanan</p> <ul style="list-style-type: none"><li>- Teknik untuk meminimalisir serangan ke server dan pengamanannya secara umum</li><li>- Teknik melakukan banned otomatis pada ip target yang melakukan scanning menggunakan NMAP dengan option seperti misal -sV dan -A (Linux)</li><li>- Buffer Overflow</li><li>- Fuzzer Development (Membuat fuzzer sendiri dengan Python)</li></ul>



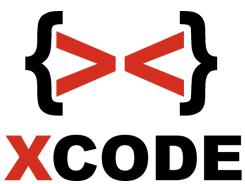
		<ul style="list-style-type: none"><li>- EIP &amp; SEH Handler</li><li>- Pattern create &amp; pattern offset</li><li>- Cek proteksi SafeSEH &amp; ASLR dan menghindarinya</li><li>- Uji coba perbedaan module yang terproteksi dan yang tidak terproteksi</li><li>- JMP ESP</li><li>- SEH &amp; SafeSEH</li><li>- POP POP RETN (Bypass SEH)</li><li>- Mengenal Bad Character</li><li>- Mengenal bahasa mesin, heksadesimal dan x86 assembler instruction set opcode table</li><li>- Tabel kebenaran XOR</li><li>- Shellcode Development untuk membuat CPU bekerja hingga 100% (Membuat dengan bahasa assembler dari awal)</li><li>- Shellcode Development untuk remote (Membuat dengan bahasa assembler dari awal)</li><li>- Penggunaan nasm dan objdump untuk shellcode yang dibuat</li><li>- Cara penyusunan shellcode secara cepat</li><li>- Shellcode generate dengan encode shikata_ga_nai</li><li>- Proof of concept pada exploit yang dibuat</li></ul>
5	Session 5	<ul style="list-style-type: none"><li>- Scanning IP, port, service, OS dll</li></ul>



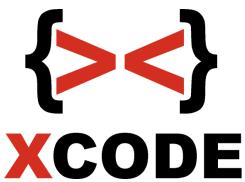
- Denial of Service - Web Server (intranet & internet). Contoh pada apache server, web dari OS mikrotik dan access point tp-link
- Denial of Service - IP Publik (Koneksi internet target down)
- Denial of Service SMBv1 - (SMB Windows XP, SMB Windows Server 2003) (Blue Screen)
- Denial of Service SMBv2 - (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
- Eksloitasi 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
6	Session 6	<ul style="list-style-type: none"><li>- Mengamankan Web Server dari serangan DoS tertentu (Pengujian sebelum diamankan dan setelah diamankan) (Linux)</li><li>- Mengatasi serangan Netcut di Windows (Pengujian sebelum diamankan dan setelah diamankan)</li><li>- Pengamanan di linux dari serangan netcut dan serangan sniffing password dengan ARP Spoofing (Pengujian sebelum diamankan dan setelah diamankan)</li><li>- DNS Spoofing</li><li>- Membuat fake login sendiri</li><li>- Client side Attack ~ Browser IE atau firefox</li><li>- Eksloitasi celah remote pada Microsoft Word 2010 / 2013 / 2016</li><li>- Bypass login masuk windows 7 dan 8.1</li><li>- Msfvenom untuk backdoor Windows (Backdoor di inject kan ke file exe lain)</li><li>- Meterpreter (Download, upload, keylogger, VNC, etc)</li><li>- Membangun backdoor untuk remote Windows 10 dan bypass antivirus internal Windows 10 (Windows Defender)</li><li>- Privilege escalation pada Windows Server 2008 / Windows 8.1 / Windows 10 / Windows Server 2012 R2 / 2016</li></ul>



		<ul style="list-style-type: none"><li>- Cara mendapatkan password login windows 7 / 8 secara langsung dengan akses administrator (Mengambil dari memory, bukan brute force)</li><li>- Cara mendapatkan password login pada Linux Ubuntu Desktop secara langsung dengan akses root (Mengambil dari memory, bukan brute force)</li><li>- Cara mendapatkan NTLM hash Windows 10 dengan akses administrator (Mengambil dari memory), lalu crack NTLM hashnya dengan hashcat (brute force)</li><li>- John the ripper pada Windows / linux</li><li>- Brute force attack (VNC / telnet / ftp / pop3 / http / mysql / ssh / vnc / samba linux)</li><li>- Membangun wordlist dengan berbagai kriteria sendiri secara cepat (generate)</li></ul> <p>Pengamanan</p> <ul style="list-style-type: none"><li>- Pengamanan umum</li><li>- Teknik melakukan banned pada ip attacker secara otomatis yang melakukan serangan brute force pada SSH (Linux)</li><li>- Port Knocking pada SSH (Linux)</li><li>- SSH Honeypot (Linux)</li></ul> <p>Tambahan :</p> <ul style="list-style-type: none"><li>- Cara mendeteksi SSH Honeypot (Linux)</li></ul>
6	Session 6	<ul style="list-style-type: none"><li>- Dasar Wireless LAN</li><li>- Mengenal keamanan wireless pada access point</li></ul>



- 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