X-code Training Online ~ Network hacking & Security
Jumlah pertemuan : 5x pertemuan

Materi

Sesi 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
- Dasar firewall
- TOR Windows
- Command prompt
- Managemen user (Command prompt)

Sesi 2
- Mengenal linux
- Shell bash (Perintah-perintah di linux)
- Repository
- Setting ip address di linux
- Managemen user dan group di linux
- SSH
- Apache Server
- Firewall UFW
- IDS (Intrusion detection system) dengan Snort

Sesi 3
- Ethical Hacking
- 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 router dengan routersploit
- 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

Sesi 4
- Hacking pada service SMB Windows 8.1 / 10 yang mengijinkan share folder tanpa password untuk mendapatkan akses shell (Bypass Windows Defender)
- Hacking pada service Samba Linux Ubuntu Server untuk mendapatkan akses shell
- Teknik untuk meminimalisir serangan ke server
- Teknik melakukan banned otomatis pada ip target yang melakukan scanning menggunakan NMAP dengan option seperti misal -sV dan -A
- Buffer Overflow
- Fuzzer Development (Membuat fuzzer sendiri dengan Python)
- EIP & SEH Handler
- Pattern create & pattern offset
- Cek proteksi SafeSEH & ASLR dan menghindarinya
- JMP ESP
- SEH & SafeSEH
- POP POP RETN (Bypass SEH)
- Mengenal Bad Character
- Eksploitasi

Sesi 5
- Denial of Service - Web Server (intranet & internet). Contoh pada apache server, web dari OS mikrotik x86 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) (Blue Screen)
- Denial of Service SMB Windows 8.1 / 10 dengan sharing folder tanpa password (Blue Screen)
- DHCP Flooding
- 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
- Mengamankan Web Server dari serangan DoS tertentu (Pengujian sebelum diamankan pada serangan sebelumnya dan setelah diamankan) (Linux)

Sesi 6
- DNS Spoofing (windows / linux)
- Membuat fake login sendiri
- Client side Attack ~ Browser IE atau firefox
- Eksploitasi celah remote pada Microsoft Word
- Msfvenom untuk backdoor Windows (Backdoor diinject kan ke file exe lain)
- Privilege escalation pada Windows Server 2008 / Windows 8.1 / Windows 10
- John the ripper pada Windows / linux
- Brute force attack
- Membangun wordlist dengan berbagai kriteria sendiri secara cepat (generate)

Pengamanan
- Teknik melakukan banned pada ip attacker secara otomatis yang melakukan serangan brute force pada SSH

Informasi jadwal training :
Jadwal training adalah kesepakatan dengan pengajar

Metode pembelajaran
- Tampilan layar interaktif menggunakan VNC (https://www.realvnc.com/en/connect/download/viewer/)
- Komunikasi menggunakan whatsapp

Fasilitas
- Modul elektronik dan sertifikat X-code Training Online