


CHAPTER 11

NETWORK RECON & EXPLOIT

[ACADEMY.CYBERKARTA.COM](https://academy.cyberkarta.com)

Praktik

- Setup sistem
 - Setup SSH
 - Shodan API key
- Buat program untuk recon/exploit (lengkap dengan DRIVE framework)
 - a. ping sweep
 - b. port scanning
 - c. SSH brute force (cek chapter sebelumnya)
 - d. Shodan API recon
 - e. Network sniffing
-  **Kode hanya untuk keperluan edukasi. Jangan dijalankan di mesin yang tidak kamu miliki *authorization*-nya.**

Recon: Ping Sweep

- **Definisi:** melakukan ping request ke perangkat lain dalam jaringan untuk cek keaktifan dan potensi target serangan cyber
- **Dampak:** [Low]
 - potensial sebagai target serangan
- **Mitigasi:**
 - ICMP filtering
 - Setup config Firewall
- Library Python terkait:
 - `scapy`
 - `os`
 - `subprocess`

Recon: Port Scanning

- **Definisi:** melakukan ping ke suatu address dan cek apakah port nya terbuka atau tidak
- **Dampak:** [Low]
 - potensial sebagai target serangan
 - pemetaan service
- **Mitigasi:**
 - port knocking
 - config untuk hapus banner
 - rate limiting
- Library Python terkait:
 - **scapy**
 - **nmap**

Exploit: SSH Brute Force

- **Definisi:** serangan kombinasi credential untuk akses server
- **Dampak:** [High]
 - Akses full ke mesin server
- **Mitigasi:**
 - key-based auth
 - rate limiting
 - Fail2ban
- Note: perlu setup SSH untuk praktik
- Library Python terkait:
 - `paramiko`
 - `hydra`
 - `pexpect`

Recon: Shodan API

- **Definisi:** Shodan adalah search engine untuk semua device yang terbuka secara publik, dengan API yang tersedia untuk keperluan cybersecurity
- **Dampak:** [Medium]
 - Service yang terbuka dapat menjadi titik serangan
- **Mitigasi:**
 - security & network config
- Note: perlu setup untuk memperoleh API key Shodan
- Library Python terkait:
 - **shodan**

Exploit: Network Sniffing

- **Definisi:** melakukan intercept pada packet yang melewati network untuk melihat isi datanya (termasuk data sensitif seperti credential, transaksi, dll)
- **Dampak:** [High]
 - Kebocoran data
 - Pencurian akses/credential
- **Mitigasi:**
 - gunakan protocol terenkripsi (SSH, HTTPS)
- Library Python terkait:
 - `scapy`
 - `pyshark`
 - `socket`