

CHAPTER 12

REVERSE SHELL USING PYTHON

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

Checkpoint

- *Done*
 - Recon & exploit sistem target menggunakan program Python
- *What's next?*
 - Membuat reverse shell script untuk di-deliver ke sistem target

Tentang Reverse Shell

- **Definisi**

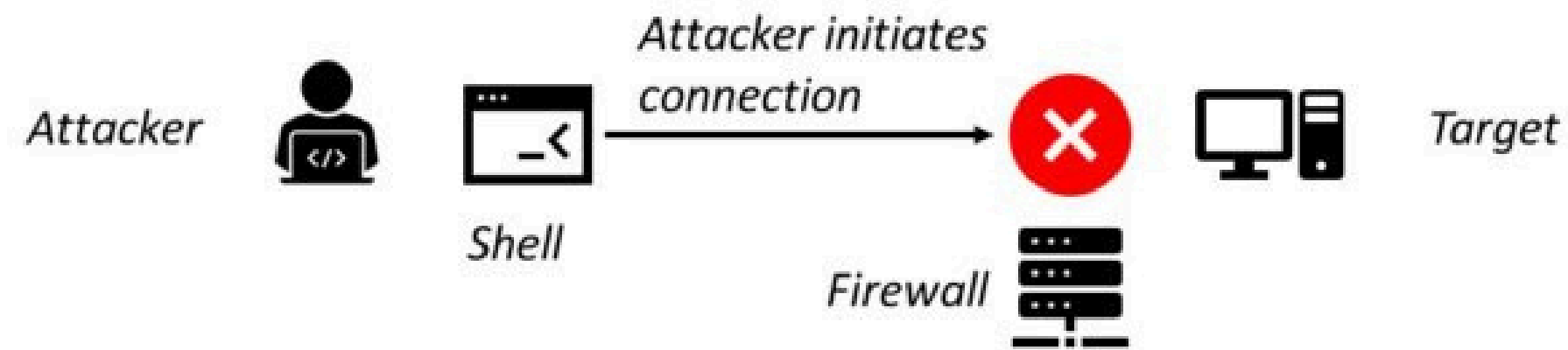
- Sederhananya, reverse shell adalah kebalikan dari akses shell via SSH
- SSH → membuka gerbang sistem dari luar dengan credential (akses ketat)
- Reverse shell → membuka gerbang sistem dari dalam dengan establish connection (lebih tersembunyi)

- **Syarat**

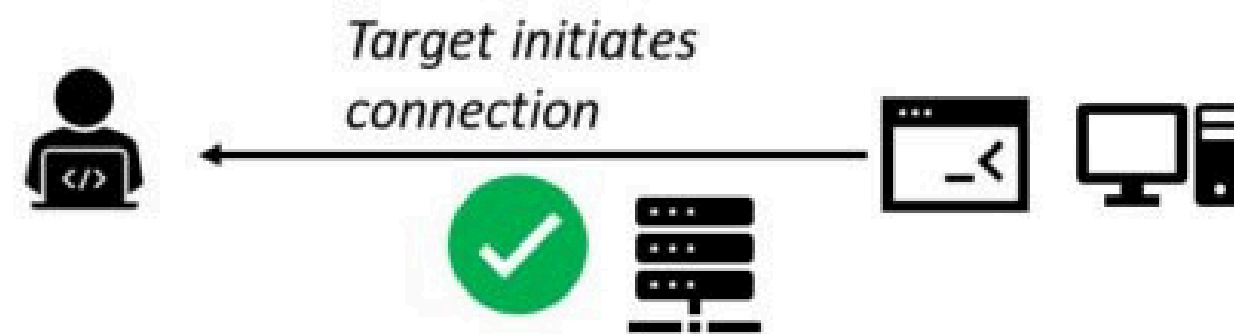
- Syarat terpenting untuk menjalankan reverse shell adalah attacker harus menaruh program di sistem target, lalu mengeksekusinya.
- Cara menaruh program? Gunakan tools recon & exploit (Chapter 10 & 11)

Tentang Reverse Shell

Without Reverse Shell



With Reverse Shell



Praktik

- Setup sistem attacker & victim
- Buat program untuk memasang reverse shell
- Eksekusi reverse shell agar attacker punya akses ke victim
- **⚠ Kode hanya untuk keperluan edukasi. Jangan dijalankan di mesin yang tidak kamu miliki *authorization*-nya.**