**Evil-WinRM**, Windows makineler üzerinde uzaktan komut çalıştırmak için kullanılan popüler bir **Windows Remote Management (WinRM)** istemcisidir. Kırmızı takım (Red Team) ve CTF senaryolarında, özellikle bir makineye **Administrator** veya **SYSTEM** haklarıyla erişim sağlandıysa bu erişimi kullanışlı ve hızlı bir şekilde yönetmek için tercih edilir.

Evil-WinRM, PowerShell komutlarını uzaktan yürütme, dosya yükleme/indirme ve script çalıştırma gibi yetenekleri ile **post-exploitation** (sömürü sonrası) aşamasının vazgeçilmez araçlarından biridir.

Ancak unutulmamalıdır ki bu araç yalnızca **izinli testler** ve **etik hackerlık faaliyetleri** kapsamında kullanılmalıdır.

**Bu aracın özellikleri nelerdir?**

**WinRM Üzerinden Bağlantı:** Windows Remote Management hizmetini kullanarak hedef sisteme bağlanır.

**Uzaktan PowerShell:** PowerShell komutlarını doğrudan uzaktan çalıştırma imkanı tanır.

**Dosya Transferi:** Hedef sisteme dosya yükleyebilir veya hedeften dosya çekebilir.

**Etkin Script Kullanımı:** Yerel veya uzaktaki PowerShell script’lerini çalıştırabilir.

**SSL/TLS Desteği:** Güvenli bağlantılar için SSL desteği sunar.

**Açık Kaynak:** GitHub üzerinde topluluk katkılarına açıktır ve geliştirilmeye devam etmektedir.

**Hızlı ve Kullanıcı Dostu:** Terminal arayüzü üzerinden hızlı ve esnek kullanım sağlar.

**Bu aracı Kali Linux'a kurma ve kullanma adımları:**

**Adım 1: Gerekli Ruby Paketlerinin Kurulması**

Evil-WinRM Ruby ile yazılmıştır. Bu nedenle Ruby’nin sistemde kurulu olması gerekir:

“sudo apt update

sudo apt install ruby”

**Adım 2: Evil-WinRM Kurulumu**

Evil-WinRM aracı Ruby’nin gem yöneticisi üzerinden kolayca kurulabilir:

“sudo gem install evil-winrm”

**Adım 3: Evil-WinRM ile Uzak Sisteme Bağlanma**

Bağlantı kurmak için aşağıdaki komut yapısını kullanabilirsiniz:

“evil-winrm -i 10.10.10.100 -u administrator -p 'P@ssw0rd'”

Burada:

* -i: Hedef sistemin IP adresi
* -u: Kullanıcı adı (örneğin administrator)
* -p: Parola

**Adım 4: Komut Kullanımı Örnekleri**

Bağlantı kurulduktan sonra Evil-WinRM terminali üzerinden aşağıdaki işlemler yapılabilir:

* **PowerShell komutu çalıştırma:**

“PS> whoami

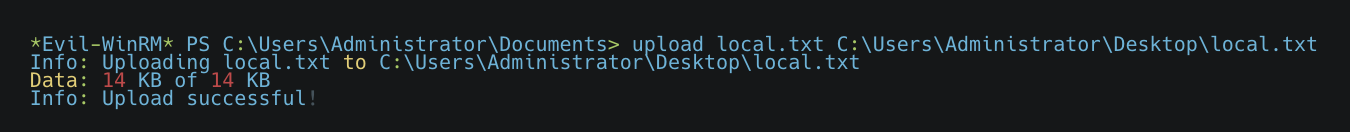
PS> ipconfig /all”

metin, ekran görüntüsü, yazı tipi içeren bir resim

Açıklama otomatik olarak oluşturuldu

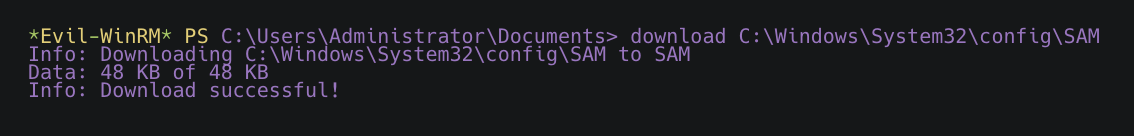
* **Dosya yükleme:**

“upload local.txt C:\Users\Administrator\Desktop\local.txt”



* **Dosya indirme:**

“download C:\Windows\System32\config\SAM”



* **Script çalıştırma:**

“script myscript.ps1”

metin, ekran görüntüsü, yazı tipi içeren bir resim

Açıklama otomatik olarak oluşturuldu