**PEASS-ng Nedir?**

PEASS-ng, sistemlerdeki zayıflıkları inceleyerek bir kullanıcı hesabının yetkilerini yükseltebileceği (privilege escalation) yolları tespit etmek için kullanılan açık kaynaklı bir araç setidir.

PEASS-ng, bilgisayardaki "dikkatsizlikleri" ya da "zayıf yapılandırmaları" kontrol ederek, bir kullanıcının nasıl yönetici (admin/root) olabileceğini gösteren bir analiz aracıdır.

**Ne İşe Yarar?**

Sızma testi (penetration testing) sırasında bir sisteme erişim sağlandıysa, sıradaki adım genellikle yetki yükseltme (Privilege Escalation) olur. PEASS-ng bu aşamada şu işlevleri görür:

Sistemdeki zayıf yapılandırmaları tespit eder

Yanlış izinler, bozuk servisler, çalışan programlar, açık portlar, zayıf dosya izinleri gibi alanları tarar

Kullanıcıdan yöneticiliğe geçiş fırsatlarını listeler

Hem Windows hem de Linux sistemlerde çalışabilir

**Kurulum ve Kullanım (Windows & Linux)**

PEASS-ng indirildikten sonra doğrudan çalıştırılabilir. Herhangi bir kurulum işlemi gerekmez.

**winPEAS (Windows) Kullanımı**

winPEAS.exe dosyasını hedef sisteme aktar

GitHub’dan indir: ***https://github.com/carlospolop/PEASS-ng/releases***

Windows’ta komut satırını aç ve çalıştır

***winPEAS.exe***

veya sessiz modda:

***winPEAS.exe quiet***

linPEAS (Linux) Kullanımı

Script’i indir

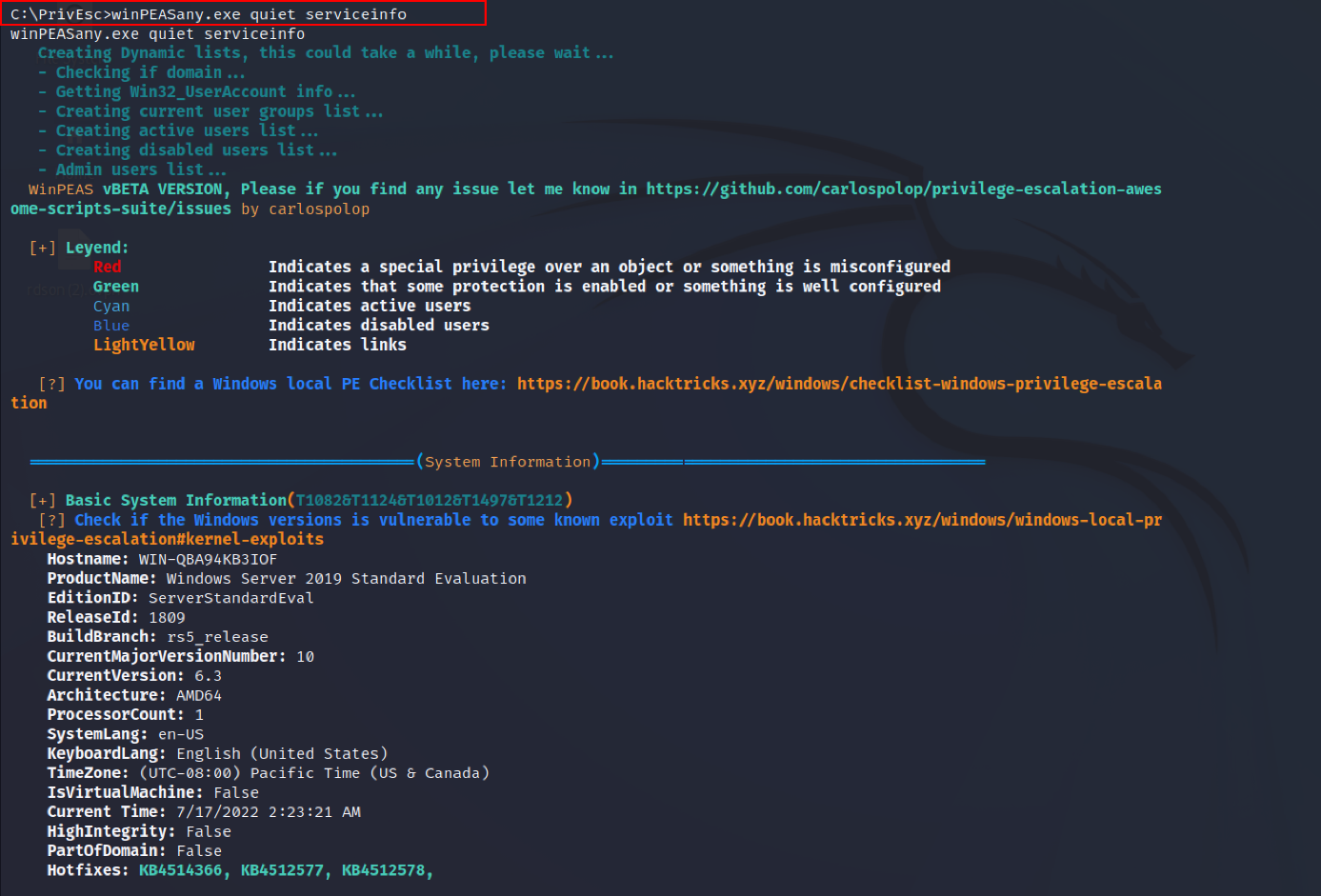
***curl -sL https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh -o linpeas.sh***

***chmod +x linpeas.sh***

Script’i çalıştır

***./linpeas.sh***

Alternatif: ***bash linpeas.sh***



linPEAS script’i, Linux sistemlerde sistem bilgisi, zayıf dosya izinleri, halen çalışan servisler gibi verileri toplar; kırmızı/scarlet renkler potansiyel yetki yükseltme yollarını belirtir.

**Avantajları ve Dikkat Edilmesi Gerekenler**

**Avantajları:**

* Açık kaynak ve ücretsizdir
* Hem Windows hem Linux için çalışır
* Otomatik analiz yapar, sonuçları okunabilir şekilde sunar
* Gerçek dünyadaki güvenlik açıklarını simüle eder

**Dikkat Edilmesi Gerekenler:**

* Yalnızca test veya izinli sistemlerde kullanılmalıdır
* Bazı antivirüs yazılımları PEASS-ng dosyalarını zararlı olarak algılayabilir
* Her zaman sanal makine ortamında çalıştırılması tavsiye edilir

PEASS-ng, bir sistemde “yetki yükseltme” yollarını tespit etmek için kullanılan, hem eğitim hem de sızma testi amaçlı mükemmel bir araçtır. Özellikle linPEAS ve winPEAS bileşenleri sayesinde, Linux ve Windows sistemlerde hangi açıklardan root ya da admin hakları alınabileceği anlaşılır.