**EDR BYPASS NEDİR?**

EDR (Endpoint Detection and Response) sistemleri, kurumların uç nokta cihazlarında (bilgisayar, sunucu vb.) kötü amaçlı yazılımları, şüpheli davranışları ve saldırıları tespit etmek ve yanıt vermek için kullandıkları güvenlik çözümleridir.

EDR Bypass ise bu sistemleri atlatma, kandırma veya etkisiz hale getirme yöntemlerini ifade eder. Genellikle Red Team, sızma testleri veya APT (gelişmiş kalıcı tehdit) saldırılarında kullanılır.

**Amaç:**

✓Güvenlik yazılımlarına yakalanmadan sisteme sızmak

✓Antivirüs/EDR tarafından tespit edilmeden komut çalıştırmak

✓Kalıcılık sağlamak ve iz bırakmamak

**EDR Bypass Teknikleri:**

✓Living Off The Land (LOLBins/LOLBAS) kullanımı

✓PowerShell Obfuscation (karmaşıklaştırma)

✓Process Injection

✓Reflective DLL Injection

✓Shellcode şifreleme (Encryption/Encoding)

✓Signed Binary Misuse (meşru imzalı dosyaların kötüye kullanımı)

**Kullanım Alanları:**

•Red Team ve Blue Team tatbikatlarında

•Gerçek dünya saldırı simülasyonlarında

•Güvenlik yazılımlarının testinde

•Siber savunma farkındalığı oluşturmak

**EDR BYPASS ARAÇLARI:**

**1**. Sharphound

**2**. Rubeus

**3**. Pupy

**4**. LOLBAS

**ARAÇ 1: SHARPHOUND**

**SharpHound Nedir:**

SharpHound, BloodHound aracının bir parçasıdır ve Active Directory (AD) ortamlarında saldırı yüzeyini analiz etmek için kullanılır. Genellikle Red Team'ler tarafından, hedef sistemdeki kullanıcılar, gruplar, izinler ve ilişkileri haritalandırmak için kullanılır.

**Özellikleri:**

**✓**Active Directory ortamındaki ilişki zincirlerini analiz eder

**✓**Kullanıcı, grup, bilgisayar, izin ilişkilerini toplar

**✓**JSON formatında çıktı üretir

**✓**BloodHound aracı ile görselleştirme yapılabilir

**✓**PowerShell ya da EXE olarak çalıştırılabilir

**✓**Sessiz (stealth) veri toplama desteği vardır

**Kullanım Alanları:**

**✓**İç ağ keşfi ve analiz

**✓**Active Directory zaafiyetlerini tespit etme

**✓**Saldırı yollarını görselleştirme

**✓**Kullanıcı ve grup ilişkilerini analiz etme

**Kurulum Aşamaları:**

**1. BloodHound ve Neo4j Yüklenmeli (Görselleştirme için):**

**•**Neo4j Desktop kurulmalı

**•**BloodHound grafik arayüzü indirilip çalıştırılmalı

**2. SharpHound Dosyası Edinilmeli:**

**-**BloodHound GitHub sayfasından ya da özel kaynaklardan edinilir

**-**PowerShell sürümü (SharpHound.ps1) veya binary (SharpHound.exe) kullanılabilir

**3. SharpHound Çalıştırma Örneği: **

**Dikkat Edilmesi Gerekenler:**

**✓**EDR yazılımları bu aracı “şüpheli” olarak işaretleyebilir

**✓“**All” parametresi çok fazla veri toplayacağı için dikkatli kullanılmalı

**✓**JSON çıktılar BloodHound’a doğru şekilde aktarılmalı

**✓**Gelişmiş ağ ortamlarında yavaş çalışabilir

**ARAÇ 2: RUBEUS**

**Rubeus Nedir:**

Rubeus, Kerberos protokolünü hedef alan bir .NET tabanlı post-exploitation aracıdır. Red Team’ler tarafından kimlik doğrulama sürecini manipüle etmek, Kerberos bileti elde etmek veya yeniden kullanmak için kullanılır.

**Özellikleri:**

✓Kerberos bileti (TGT/TGS) elde etme ve yeniden oynatma

✓Pass-the-Ticket, Overpass-the-Hash, Kerberoasting gibi saldırıları destekler

✓Bellekten bilet çıkarma

✓Mevcut bileti listeleme veya dışa aktarma

✓PowerShell uyumlu ve EXE olarak çalıştırılabilir

**Kullanım Alanları:**

✓Active Directory ortamlarında kimlik erişim kontrolünü aşmak

✓Kullanıcı haklarını artırmak

✓Kimlik hırsızlığı simülasyonu

✓Biletleri ele geçirerek başka kullanıcı gibi işlem yapmak

**Kurulum Aşamaları:**

**1. Rubeus’u İndirme:**

-GitHub üzerinden Rubeus.exe veya kaynak kodu indirilir

-Derlenmiş hali doğrudan çalıştırılabilir

**2. EXE Olarak Çalıştırma: **

**3. PowerShell Script Olarak Kullanma: **

**4. Bilet Listeleme Örneği: **

**Dikkat Edilmesi Gerekenler:**

✓EDR sistemleri Rubeus’u yüksek riskli olarak tanıyabilir

✓Bellek içi işlemler şüpheli davranış olarak loglanabilir

✓Domain ortamında yetkili hesapla çalıştırılması gerekir

✓Log’lara yakalanmamak için “stealth” modlar kullanılmalıdır

**ARAÇ 3: PUPY**

**Pupy Nedir:**

Pupy, çok platformlu (multi-platform) bir post-exploitation ve remote administration aracıdır. Python tabanlıdır ve Red Team operasyonlarında hedef sisteme uzaktan erişim, kontrol ve veri toplama işlemleri için kullanılır.

**Özellikleri:**

✓Windows, Linux, macOS, Android desteği

✓Python tabanlı, hafif ve taşınabilir

✓Fileless (dosyasız) çalışma yeteneği

✓Reflective DLL injection, keylogger, ekran görüntüsü alma gibi modüller

✓AES şifreleme ile iletişim

✓Stager destekli (payload zincirleme yapısı)

✓Session yönetimi, çoklu bağlantı desteği

**Kullanım Alanları**:

•Uzaktan erişim ve kontrol

•Kalıcılık sağlamak

•EDR/AV bypass teknikleriyle sessiz kontrol

•Dosya ve bilgi toplama

•Güvenlik sistemlerinin test edilmesi

**Kurulum Aşamaları:**

**1. Sistem Gereksinimleri:**

-Linux sistem (örneğin Kali Linux) önerilir

-Python 2.7 (Pupy, Python 3 ile tam uyumlu değildir)

-Git yüklü olmalı

**2. Pupy’yi İndirme: **

**3. Gereksinimlerin Kurulması: **

**4. Sunucu Başlatma: **

**Dikkat Edilmesi Gerekenler:**

✓Python 2.7 ortamı kullanılmalı, aksi takdirde hata verir

✓AV/EDR sistemleri bazı modülleri engelleyebilir

✓İlk çalıştırmada ek bağımlılık kurulumu gerekebilir

✓Linux üzerinde çalıştırılması daha kararlıdır

**ARAÇ 4: LOLBAS**

**LOLBAS Nedir:**

LOLBAS (Living Off The Land Binaries, Scripts, and Libraries), işletim sistemi içerisinde yer alan ve meşru görünen ama kötüye kullanılabilen dosyaların listesini ve kullanımını ifade eder. Bu yaklaşım, EDR ve antivirüs sistemlerini atlatmak için saldırganlar tarafından kullanılır.

**Özellikleri:**

✓Sistemde zaten var olan dosyalar (örneğin: certutil.exe, mshta.exe) kullanılır

✓Yazılım yüklemeye gerek kalmaz

✓Sistem yöneticileri tarafından sık kullanıldığından dikkat çekmez

✓Dosya indirme, komut çalıştırma, kod inject etme gibi işlevler

✓Güncel ve açık kaynaklı veri tabanı: [https://lolbas-project.github.io]

**Kullanım Alanları:**

•EDR ve antivirüs sistemlerini atlatma

•Post-exploitation işlemleri

•Dosya indirme/yürütme işlemleri

•Gelişmiş kalıcılık teknikleri

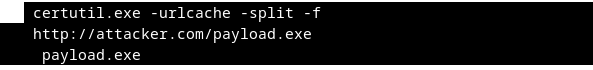
•Script ve DLL yükleme işlemleri

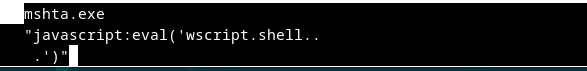
**Kurulum Aşamaları:**

-LOLBAS bir araç değil, bir yöntem ve veri tabanı olduğu için kurulum yapılmaz. Ancak kullanım için GitHub üzerindeki veritabanı veya web sitesi referans alınır:

**1. Veritabanı Erişimi:**

[https://github.com/LOLBAS-Project/LOLBAS]

**2. Meşru Binary Kullanımı Örneği: **

**3. Script ile Kod Yürütme Örneği: **

**Dikkat Edilmesi Gerekenler:**

✓Sistem yöneticileri bu yöntemleri beyaz listeye almış olabilir

✓Log kayıtlarında analiz yapılabilir

✓Davranışsal EDR’ler anormal kullanım tespiti yapabilir