**EXPLOIT TOOLS NEDİR?**

Exploit tools, sistemlerdeki açıkları (vulnerability) kullanarak yetkisiz erişim, ayrıcalık yükseltme, veri sızdırma gibi amaçlarla kullanılan araçlardır. Bu araçlar, belirli bir zafiyeti hedef alır ve sisteme sızma ya da kontrol sağlama imkânı verir.

**Amaç:**

•Güvenlik açıklarını test etmek

•Sızma testleri gerçekleştirmek

•Yetki yükseltme (privilege escalation)

•Zafiyet istismarı ile sistem kontrolü

•Post-exploitation hazırlığı yapmak

**Kullanım Alanları:**

✓Red Team ve sızma testleri

✓Sistem yöneticilerinin zafiyet kontrolü

✓Eğitim ve simülasyon ortamları

✓Gerçek dünya saldırı analizi

**EXPLOIT TOOLS ARAÇLARI:**

-Bu bölümde aşağıdaki araçları sırayla anlatacağız:

**1**. NoPac

**2**. Chisel

**3**. Responder

**4**. CrackMapExec

**ARAÇ 1: NOPAC**

**NoPac Nedir:**

NoPac, Windows sistemlerinde Active Directory ortamındaki ciddi bir güvenlik açığını (CVE-2021–42278 & CVE-2021–42287) istismar ederek domain controller yetkisi kazanmayı mümkün kılan bir saldırı zinciridir. Bu açıklar, kullanıcı nesnelerinin taklit edilmesi ve ticket (bilet) sisteminin manipülasyonu yoluyla sistemin ele geçirilmesini sağlar.

**Özellikleri:**

✓Domain admin haklarına yükselme sağlar

✓CVE-2021–42278 ve CVE-2021–42287 zafiyetlerini kullanır

✓Active Directory ortamına özel bir saldırıdır

✓Sistem yeniden başlatılmadan çalışabilir

✓Sızma testlerinde yüksek etki sağlar

**Kullanım Alanları:**

•Active Directory içeren kurum içi ağ testleri

•Privilege escalation (yetki yükseltme)

•Red Team saldırılarında etkiyi büyütme

•Zafiyet kontrol testleri

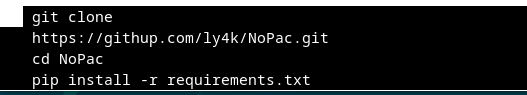
**Kurulum Aşamaları:**

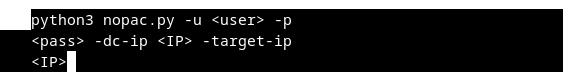
**1. Sistem Gereksinimleri:**

-Hedef sistem Active Directory ortamında olmalı

-Windows 10/Server sistemlerde zafiyet bulunmalı

-Python 3 kurulu bir Linux ya da Windows ortamı

**2. PoC Kodunun Edinilmesi (Örnek): **

**3. Saldırının Çalıştırılması: **

**Dikkat Edilmesi Gerekenler:**

✓Bu zafiyetin çalışması için sistemlerin yamalanmamış olması gerekir

✓Saldırı yalnızca Active Directory sistemlerinde geçerlidir

✓Loglama açık ise sistem yöneticileri tarafından tespit edilebilir

✓Test amaçlı kullanımlarda hedef ortamdan izin alınmalıdır.

**ARAÇ 2: CHISEL**

**Chisel Nedir:**

Chisel, bir TCP/UDP tünelleme aracıdır. Genellikle güvenlik duvarı (firewall) veya NAT arkasında bulunan sistemlere erişmek için kullanılır. Saldırganın, hedef sistemle gizli bir bağlantı kurarak veri akışı sağlamasına olanak tanır. Go diliyle yazılmıştır ve taşınabilir bir yapıdadır.

**Özellikleri:**

✓TCP ve UDP tünelleme desteği

✓Reverse proxy işlevi

✓Port yönlendirme

✓Hafif ve bağımsız çalışabilir (standalone)

✓Şifreli bağlantı (TLS destekli)

✓Linux, Windows, macOS uyumlu

**Kullanım Alanları:**

•Güvenlik duvarı/NAT arkasındaki sistemlere sızma

•Red Team operasyonlarında gizli bağlantı oluşturma

•Ağ dışına veri aktarımı (exfiltration)

•SOCKS proxy kurma

•Reverse shell tünelleme

**Kurulum Aşamaları:**

**1. Chisel Dosyasını İndirme:**

-https://github.com/jpillora/chisel/releases üzerinden işletim sistemine uygun binary indirilir

**2. Sunucu Tarafını Başlatma (Saldırgan Tarafı): **

**3. İstemci Tarafını Çalıştırma (Hedef Sistem): **

-Bu örnek, hedef sistemdeki port 4444'ü saldırgan sistemine yönlendirecektir.

**Dikkat Edilmesi Gerekenler:**

✓Bağlantılar şifreli olsa da ağ üzerinde tespit edilebilir

✓Antivirus yazılımları .exe dosyasını zararlı olarak algılayabilir

✓Bağlantı stabilitesi için portlar açık olmalıdır

**ARAÇ 3: RESPONDER**

**Responder Nedir:**

Responder, iç ağda bulunan makinelerin kimlik doğrulama trafiğini dinleyerek kimlik bilgilerini (hash’leri) ele geçirmeye yarayan güçlü bir network sniffer ve spoofing aracıdır. Özellikle Windows ortamlarında, zayıf yapılandırılmış ağlarda etkili sonuçlar verir.

**Özellikleri:**

✓LLMNR, NBT-NS ve MDNS isteklerini ele geçirir

✓SMB, HTTP, FTP gibi servisleri taklit ederek kimlik bilgisi toplar

✓NTLM hash’lerini yakalayabilir

✓Otomatik şekilde spoofing (aldatma) yapar.

✓Python tabanlı ve Linux üzerinde çalışır

**Kullanım Alanları:**

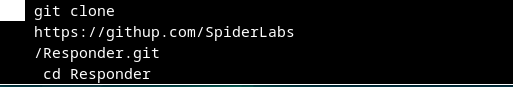
•İç ağda kimlik bilgisi toplama

•Red Team operasyonlarında ilk erişim sağlama

•Pass-the-Hash gibi saldırılar için hazırlık

•Kullanıcı oturumlarının manipülasyonu

**Kurulum Aşamaları:**

**1. Responder’ın İndirilmesi: **

**2. Gereksinimlerin Kurulması:**

•Genelde pip install -r requirements.txt gerekmez çünkü bağımlılık azdır

•Python 3.x kurulu olm

**3. Responder’ı Başlatma: **

-eth0 ,dinlemek istediğin ağ arayüzüdür.Sisteme göre değişebilir.(ip a komutu ile kontrol edebilirsin)

**Dikkat Edilmesi Gerekenler:**

✓Aynı ağda başka güvenlik araçları varsa çakışma olabilir

✓Windows Defender bazı davranışları tespit edebilir

✓Sadece yerel ağda çalışır (WAN desteklemez)

✓Ağ trafiği fazla olan ortamlarda log dosyaları hızlı şişebilir.

**ARAÇ 4: CRACKMAPEXEC (CME)**

**CrackMapExec Nedir**:

CrackMapExec, ağ güvenlik testlerinde yaygın olarak kullanılan bir post-exploitation aracıdır. SMB, RDP, WinRM gibi protokoller üzerinden hedef sistemlere bağlantı kurup zafiyetleri kontrol edebilir, hash ile oturum açabilir ve komut çalıştırabilir. Özellikle Active Directory ortamlarında çok güçlüdür.

**Özellikleri:**

✓SMB, RDP, MSSQL, WinRM protokollerini destekler

✓NTLM hash ve password ile kimlik doğrulama yapılabilir

✓Komut çalıştırma, servis yükleme, credential dump gibi işlemler

✓Otomasyon dostu ve hızlıdır

✓Parola politikası testi yapılabilir

✓BloodHound gibi araçlarla entegre olabilir

**Kullanım Alanları:**

•Active Directory zafiyet taramaları

•Parola denemeleri (brute-force değil, kontrol amaçlı)

•Lateral movement

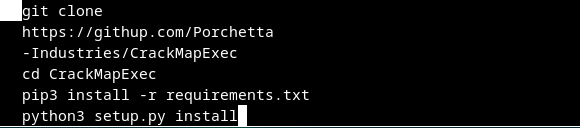
•Yetki testleri

•Kimlik bilgisi doğrulama (valid creds)

•Red Team sonrası erişim değerlendirmesi

**Kurulum Aşamaları:**

**1. Gerekli Paketlerin Yüklenmesi: **

**2. Kaynaktan Kurulum (Güncel Versiyon için): **

**3. Kullanım Örneği: **

**Dikkat Edilmesi Gerekenler:**

✓Aşırı sorgu göndermek ağda fark edilme riskini artırır

✓Hedef sistemlerde güvenlik duvarı varsa bağlantı engellenebilir

✓Bazı güvenlik sistemleri aracın imzasını tanıyabilir

✓Karmaşık AD ortamlarında doğru yapılandırma önemlidir