Sızma Testlerinde Armitage Kullanımı

Mesut Türk <mesut.turk@bga.com.tr>

İÇİNDEKİLER

1. ARMITAGE'i TANIYALIM

Armitage, sistemlere sızabilmeye yarayan görsel etkileşimli bir programdır. Sistemlere sızdıktan sonra ele geçirilen bilgisayarlar üzerinden başka bilgisayarlara sızmak için kullanılabilmektedir.

Armitage, aynı zamanda metasploit yazılımının yapabileceklerini görsel olarak kontrol edebilme imkânı sağlayan bir yazılımdır. Armitage programı pentest uygulamaları için kullanıldığından, armitage'i iyi anlamak için önce bazı kavramlara göz atmak gerekmektedir.

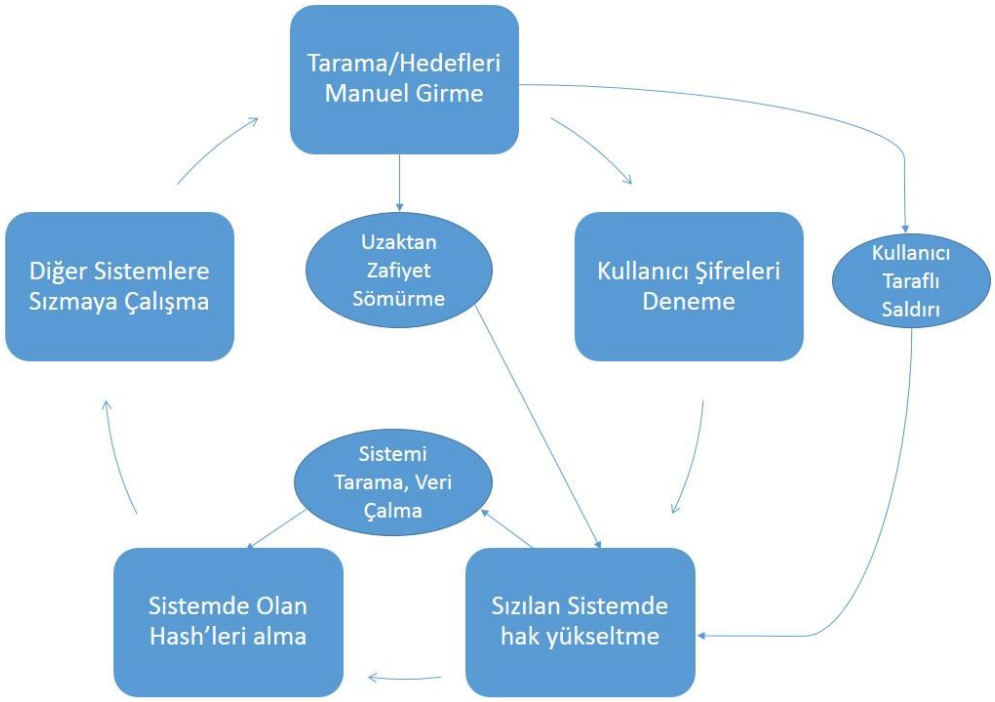
1.1 GENEL KAVRAMLAR

Metasploit: Sistemlerde bulunan açıklıkların test edilmesi ve ispatlanması için yazılmış bir program. Metasploit işletim sistemine benzer bir yapıya sahiptir. Oluşturulmasında ağırlıklı olarak ruby ve python yazılım dilleri kullanılmıştır. Test edilecek açıklıklar sisteme modüller, payload'lar ve auxiliary'ler olarak eklenmiştir.
Exploit: En yalın anlatımı ile avantajlı duruma geçebilmek için karşı tarafa karşı kullanılan şey. Bilgisayar dünyasında bu bir veri yığını, bir program veya kod parçacığı olabilir.
Auxiliary: Açıklıkları tespit etmek için yazılmış kod bloklarıdır.
Post Exploit: Bir bilgisayara sızdıktan sonra sistemde bulunan diğer bilgisayarlara erişim için yapılan çalışmalar.
Payload: Bir sistemde var olan açıklığı değerlendirip sisteme sızdıktan sonra, hedef sisteme yüklenip çalıştırılan ve hedef ile saldırgan arasında kesintisiz iletişim kurmaya yarayan yazılım ya da kod bloğu.
Modül: Her açıklığı sömürmek ya da tespit etmek adına yazılan programcıklar (Payload'lar ve Auixiliary'ler)

Armitage programı, kodlara yabancı olanlar için ve pentest çalışmalarına yeni başlayanlar için tavsiye edilmektedir. Linux dünyasındaki birçok açık kaynak kod yazılımı gibi Armitage programı da açık kaynak bir yazılımdır. Pentest alanında açık kaynak yazılımların üzerinde yapılan değişiklikler sonucu ücretli hale getirilen birçok yazılım gibi Armitage programının da ücretli hali, Cobalt Strike, bulunmaktadır.

1.2 GENEL OLARAK SİBER SALDIRI PLANI

Sonuç olarak bu yazılım sistemlere siber saldırı aracı olarak kullanılacaktır. Siber saldırı olayları çok kapsamlı ve detaylı bir iş öbeği olduğu için belirli bir planı ve metodolojisi olmalıdır.



Basit olarak bir siber saldırı planı bu aşamalardan oluşmaktadır, bu tür bir saldırı daha fazla iç ağlarda yapılan saldırı tipidir.

2. ARMITAGE'İ KULLANMAYA BAŞLAYALIM

2.1 ARMITAGE PROGRAMININ ÇALIŞMASI İÇİN NELER GEREKLİ

Armitage programı bireysel çalışmalara elverişli olduğu gibi takım çalışmalarına da uygundur. Takım olarak çalışabilmek için istemci veya sunucu olarak çalışabilmektedir. Armitage programı Windows, Linux, MacOS üzerinde kullanılabilmektedir.

Hemen belirtmekte fayda var, tüm bileşenleri ile birlikte Windows üzerinde kullanmak mümkün değildir. Windows üzerinde sadece istemci gibi kullanabilir ve takım olarak çalışılabilir.

Armitage programının ihtiyaç duyduğu araçlar;

- Metasploit Framework ve bileşenleri
  - PostgreSQL Veritabanı
  - Nmap
- Oracle Java 1.7

Bu bileşenlerin kusursuz bir şekilde yüklenmesi gerekmektedir. Bu yazılımların hepsinin hazır yüklenmiş bir hali Kali Linux veya Pentoo Linux işletim sistemlerinde bulunmaktadır.

2.2 ARMITAGE KALI LINUX KURULUMU

Normal şartlarda Kali Linux işletim sisteminde Armitage programı yüklü olarak gelmektedir. Programın yüklü olmaması durumunda aşağıdaki komutlar, kurulum esnasında sadece bir kere çalıştırılır.

1. Konsol açılır
2. Veritabanı servisi başlatılır.

```
root@kali:~# service postgresql start
```

3. Metasploit programının veritabanında gerekli tabloları oluşturması sağlanır.

```
root@kali:~# service metasploit start
```

4. Metasploit servisi durdurulur.

```
root@kali:~# service metasploit stop
```

5. Kali Linux işletim sisteminin çevrimiçi olan indirme veritabanı güncellenir.

```
root@kali:~# apt-get update
```

6. Armitage programı kurulur

```
root@kali:~# apt-get install armitage
```

7. Eğer yüklü değilse Java yüklenir (Kali Linux işletim sistemi varsayılan olarak Java 1.7'yi kullanmaktadır)
   32 bit işletim sistemi için;

```
root@kali:~# update-java-alternatives --jre -s java-1.7.0-openjdk-i386
```

   64 bit işletim sistemi için;

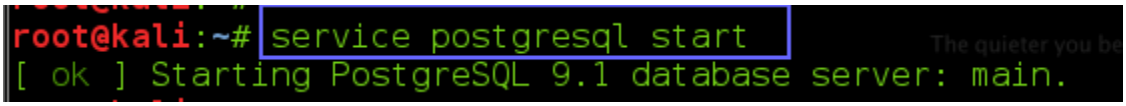
```
root@kali:~# update-java-alternatives --jre -s java-1.7.0-openjdk-amd64
```

Neden sadece Kali Linux'ta kurulum gösterilmiştir?
Sızma testi bir lab ortamına gereksinim duymaktadır. İhtiyaç duyulan tüm araçlar Kali Linux işletim sisteminde mevcuttur. Armitage programından elde edilen bulguları değerlendirmek adına en yararlı işletim sistemi Kali Linux'tur.

2.3 KALI LINUX'TA ARMITAGE KULLANIMI

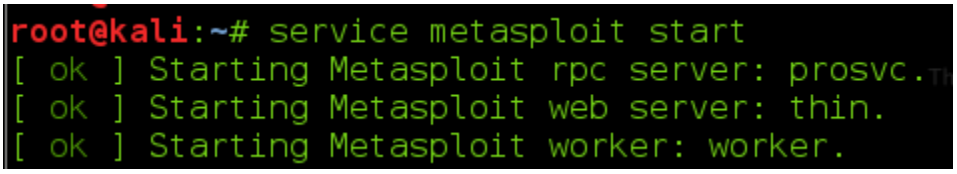
Armitage aracını Kali Linux işletim sisteminde kullanabilmek için postgreSQL ve Metasploit servislerinin aktif edilmesi gerekmektedir.
Kali'de Armitage kullanımı:

1. Konsol açılır.
2. service postgresql start komutu ile postgreSQL veritabanı servisi başlatılır.

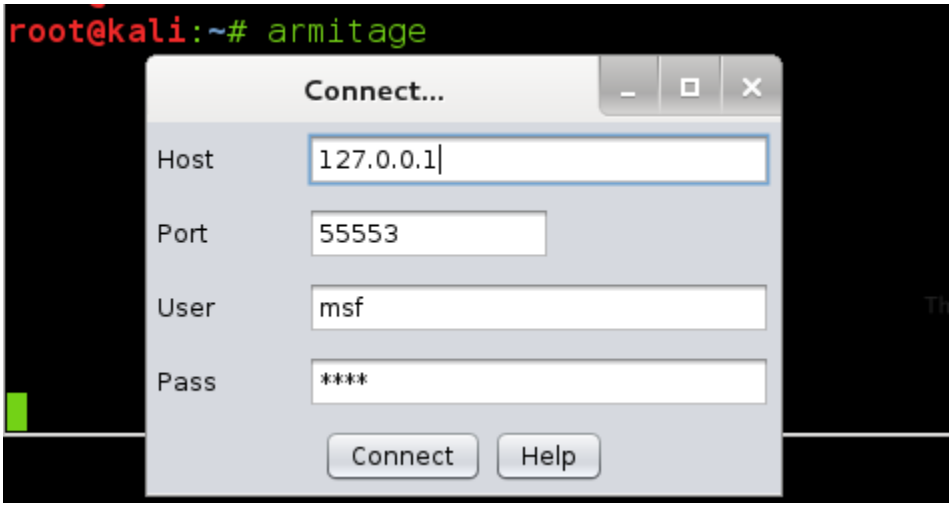


3. Daha önce belirtildiği gibi armitage metasploit programının görsel halidir. Metasploit'in sistemde verileri tuttuğu şekilde verileri tutar. Bundan dolayı metasploit servisinin bir kez çalıştırılıp veritabanında gerekli tabloların oluşturulması gerekir.

service metasploit start komutu ile metasploit servisi başlatılır.



4. armitage komutu girilerek program çalıştırılır. Bu komut sonrası ekran alıntısı;

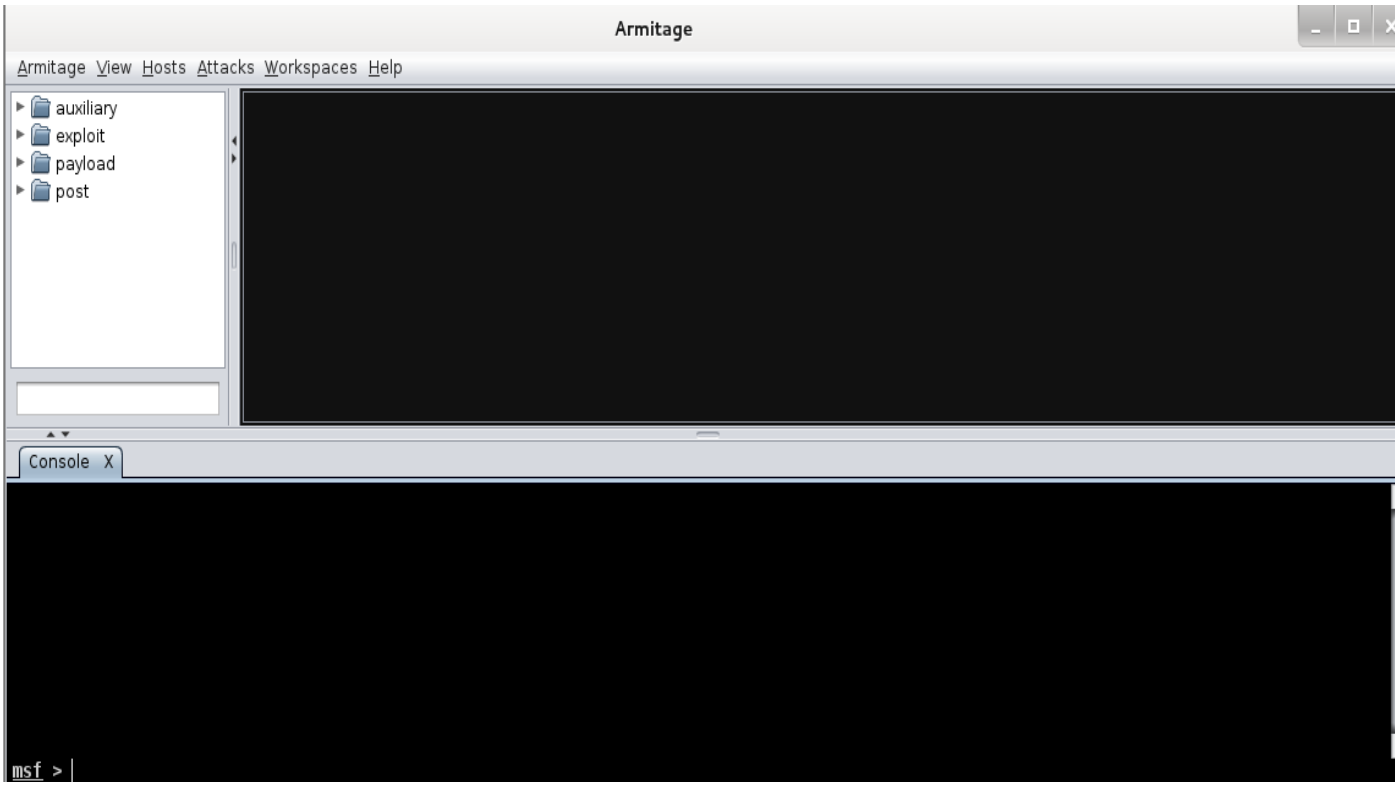


5. Connect seçeneği tıklanır.

Metasploit RPC sunucusunun çalıştırılması gerektiğini belirten bir uyarı gelir, RPC sunucusunun başlatılma önerisi kabul edilir. Daha sonra gerekli java uygulamalarının yüklenmesi beklenir, ilgili ekran alıntısı;

"**Bağlantı reddedildi**" uyarısı endişeye yol açmasın, programın fonksiyonlarının çalışmasını engellememektedir.

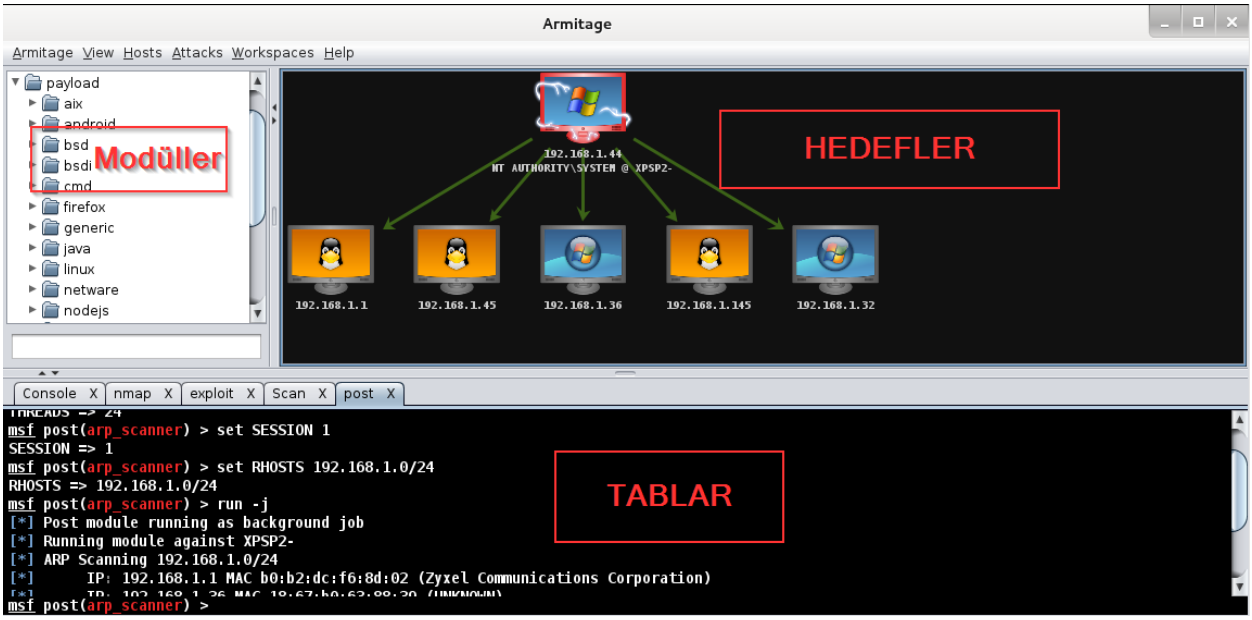
Armitage açıldığında ekrana gelecek olan pencere;



Artık, armitage programı kullanıma hazır.

2.4 ARMITAGE ARAYÜZÜNÜN TANITILMASI

Armitage arayüzü üç ana panelden oluşur. Modüller, Hedefler, Tablar. Bu panellere ek olarak ve hedef sistemlere yönelmek adına "**menü çubuğu**" altında da bazı alt menüler bulunmaktadır.



2.4.1 Modüller

Bu panelde tespit edilmiş ve kullanılabilir hale getirilmiş ve metasploit'e eklenmiş bütün modüller bulunur. Bu kısımı incelemek, siber saldırılarda hangi tür modüllerin ve tekniklerin kullanıldığını anlamak adına da çok faydalı olacaktır. Buradan bir modül kullanmak istenildiğinde üzerine çift tıklanması yeterli olacaktır. Açılan pencerede gerekli olan alanlar doldurulup modül çalıştırılabilir. Daha fazla detay ilerleyen bölümlerde örnekleri ile verilecektir.

2.4.2 Hedefler

Bu panel hedeflerin tutulduğu çalışma alanıdır. Çeşitli tarama teknikleri ile hedeflere ulaşılabileceği gibi manuel olarak da hedef eklenebilmektedir. Bu panel iki farklı şekilde görüntülenebilir; **Grafiksel** olarak ya da **Liste** olarak. Eğer kullanıcısı çok olan bir ağda çalışma yapılacak ise, grafiksel olarak görüntülemek işi çok zorlaştıracaktır.

Kısayollar
Ctrl + : Hedeflerin görünümünü yakınlaştırma.
Ctrl - : Hedefleri daha küçük gösterme
Ctrl 0 : Zoom oranını varsıyan değerine set eder.
Ctrl A : Tüm hedefleri seçer
Esc : Seçimi Temizle
Ctrl C : Hedefleri bir çember halinde göster
Ctrl S : Hedefleri yatay bir sıra halinde göster

Ctrl H: Hedefleri bir hiyerarşi yapısı halinde göster (İlk sızılan sistemden itibaren dallandırılarak gösterir.
Ctrl P: Hedefleri resim olarak kaydeder

2.4.3 Tablar

Armitage programı hedeflerle ilgili tüm işlemleri ayrı ayrı tablarda tutar. Hedef sistemlerde açılan shell oturumları, sistemleri elde etmek için denenen modüller vs her bir işlem ayrı bir pencerede tutulur. Armitage geliştiricileri tarafından bu panelde de kullanılmak üzere bazı kısayollar oluşturulmuştur.
Ctrl +T : Aktif tabta ekran görüntüsü almamızı sağlar.
Ctrl+D : Aktif olan tabı kapatır.
Ctrl+Sol :Tablar arası geçiş sağlar.
Ctrl+Sağ :Tablar arası geçiş sağlar.
Ctrl+W : Etkin olan konsol penceresini panelden bağımsız olarak açar.

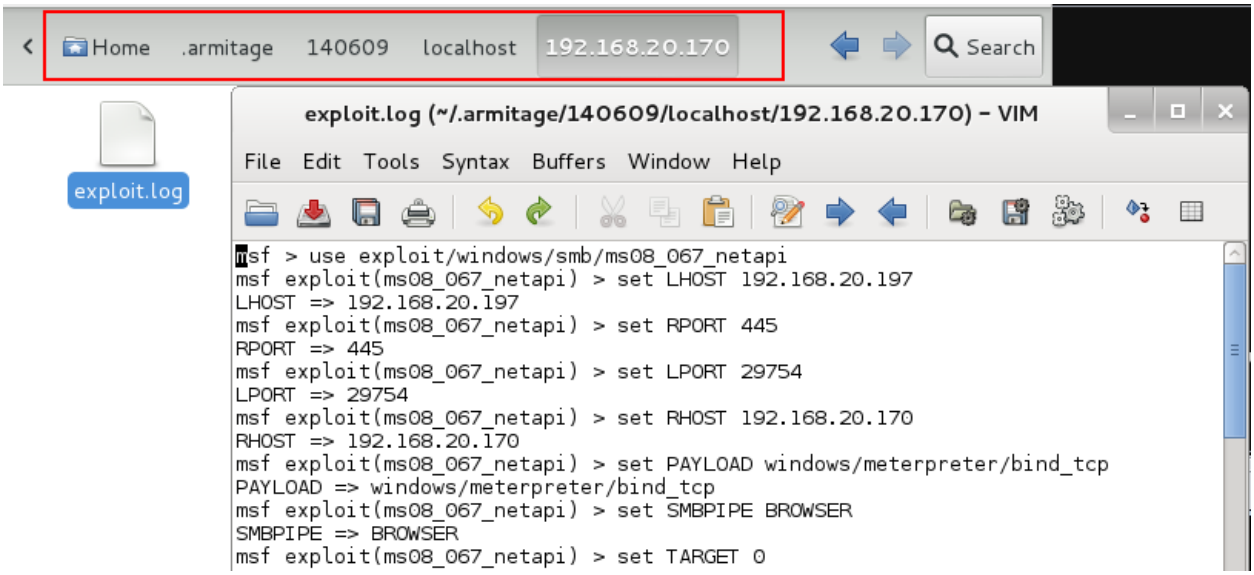
2.4.4 Konsollar

Armitage aracının konsol penceresi kullanım ihtiyacına göre Metaploit, Meterpreter veya Shell konsolları ile etkileşim haline geçer, bu uygulamalar temsilen açılan konsol ekranından yönetilebilir. Yine konsolların daha etkin kullanılabilmesi için bazı kısayollar oluşturulmuştur.
Yukarı Ok: Daha önce girilmiş olan komutlar arası geçiş sağlar.
Aşağı Ok : En son yazılan komutu ekrana basar.
Tab : Yazmaya başlanan komutu tamamlamaya yarar.
Ctrl + : Konsolun font boyutunu büyütür.
Ctrl - : Konsolun font boyutunu küçültür.
Ctrl 0 : Konsolun font boyutunu varsayılan değere atar.
Ctrl F : Konsol içerisinde arama yapar.
Ctrl A : Konsol ekranında bulunan tüm metinleri seçer.
Ctrl N : Yeni bir konsol ekranı açmamızı sağlar.

2.4.5 Üzerinde İşlem Yapılan Cihazlara Dair Kayıtlar (Logging)

Armitage aracının bilgi güvenliğine yönelik testleri gerçeklemek üzere oluşturulduğunu unutulmamalıdır. Bu testler esnasında yapılan tüm işlemlerin bir kaydının tutulması birçok açıdan önemlidir. Armitage bu endişeyi ortadan kaldırmak adına her bir ip adresi için bir klasör oluşturarak kayıtları bu klasör içerindeki log uzantılı bir dosyada tutar.
Bu kayıtlara ulaşmak için

View -> Reporting -> Activity Logs menülerinin takip edilmesi yeterlidir.
Kayıtların nasıl olduğuna dair fikir olması açısından örnek bir ekran görüntüsü;



Bu dosyaların, dosya sisteminde nerede tutulduğunu göstermek adına dizin kırmızı bir çerçeve içerisine alınmıştır. Alıntıda görüldüğü gibi tarih adı ile dosyalandığı için aranılan verilere ulaşmak daha kolay olacaktır.
Bu log dosyaları neler yapıldığının bir kaydını elde tutmaya yaradığı gibi, metasploit kullanmaya yeni başlayanlar için modüllerin, açıklık taramalarının ve açıklığın sömürülmesinin nasıl kodlandığını öğrenmesine yardımcı olur. Yeni başlayanlara iyi bir öğrenme referansı olarak kullanılabilir.
Bu dosyaları dosya sisteminde tutulduğu yere ulaşarak elde edilebileceği gibi, armitage arayüzünden rapor olarak dışa da aktarılabilir.

3. HEDEF YÖNETİMİ

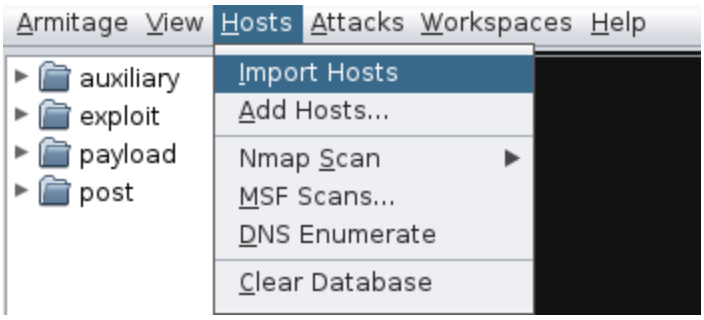
Armitage, hedeflerin daha iyi yönetilebilmesi için çeşitli özelliklere sahiptir. Şimdi bu özellikler incelenecektir.

3.1 HEDEF YÖNETİMİ

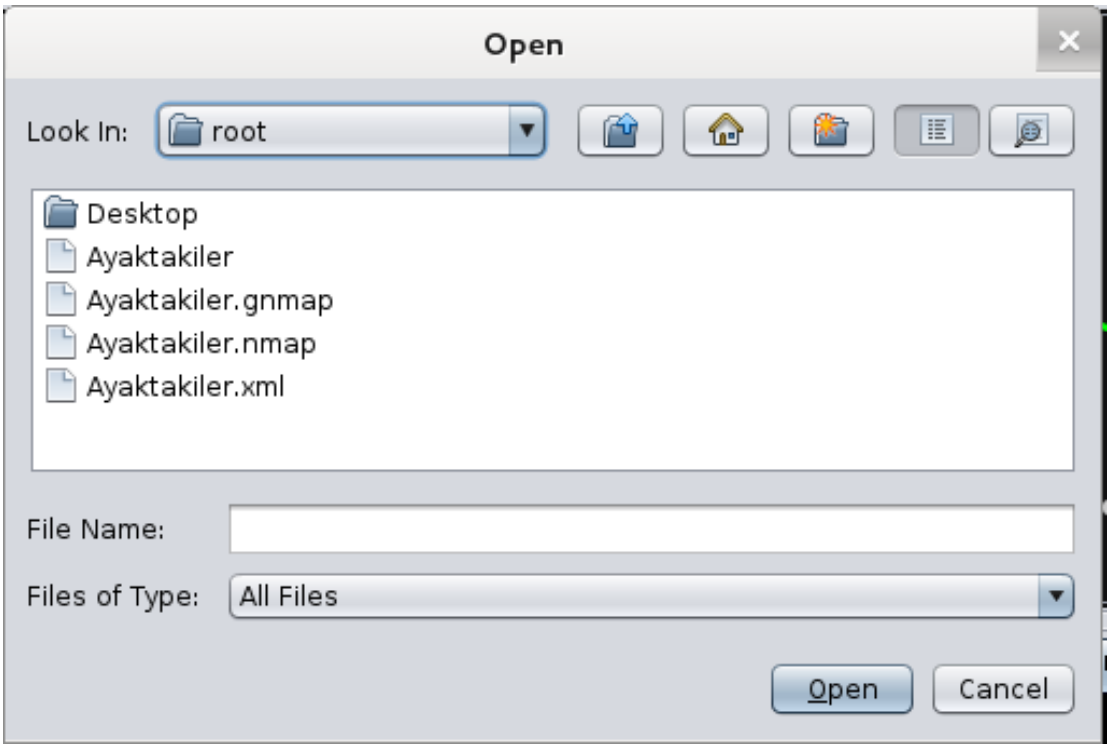
Çalışma alanına yeni bir hedef veya hedefler eklemek istendiğinde, bu işlem iki şekilde yapılabilir.

a. Birinci yöntem

Hosts -> Import Hosts seçenekleri tıklanarak.



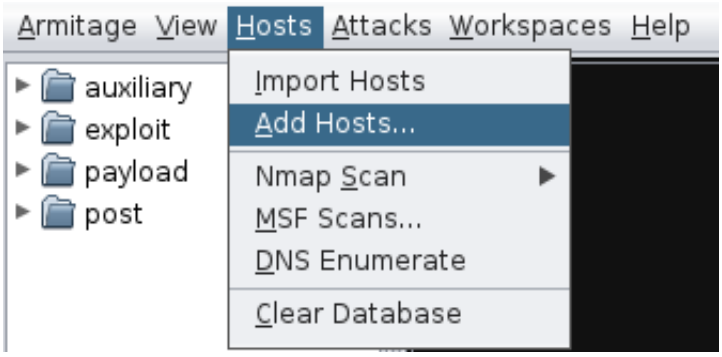
Bu seçenekler tıklandığında, ekrana dizin diyalog penceresi açılacak, sisteme entegre edilecek dosyayı tanıtmak için. İlgili ekran alıntısı;



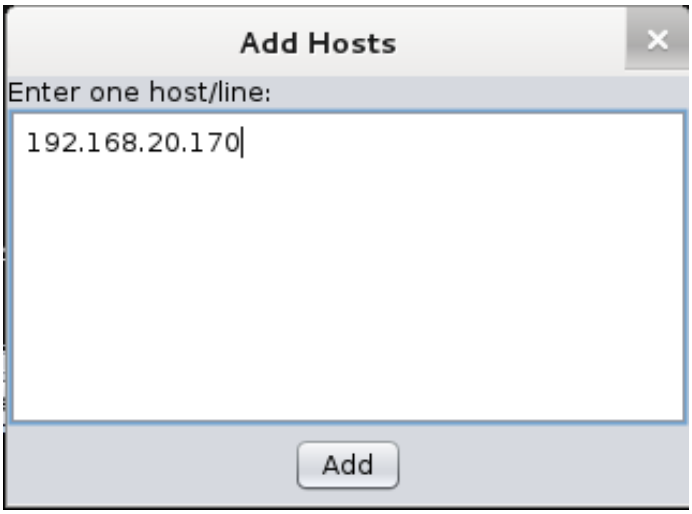
Birçok tarama aracından kayıt alınabilmektedir. Tercih edilecek tarama çıktıları arasında en iyi uyumu sağlayan çıktı **.XML** dosya türüdür.

b. İkinci Yöntem

Hosts -> Add Hosts.. seçeneklerinin izlenmesi gerekmektedir.



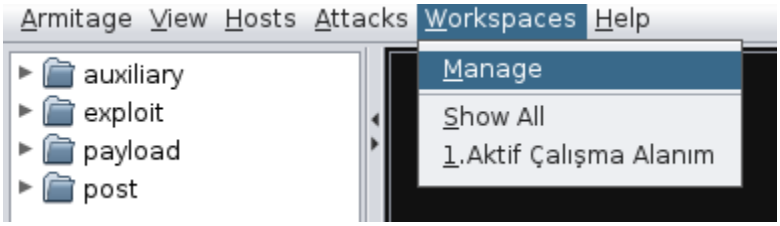
Bu adımda izlenecek yol, hedeflerin manuel olarak girilmesidir. İlgili pencerenin ekran görüntüsü;



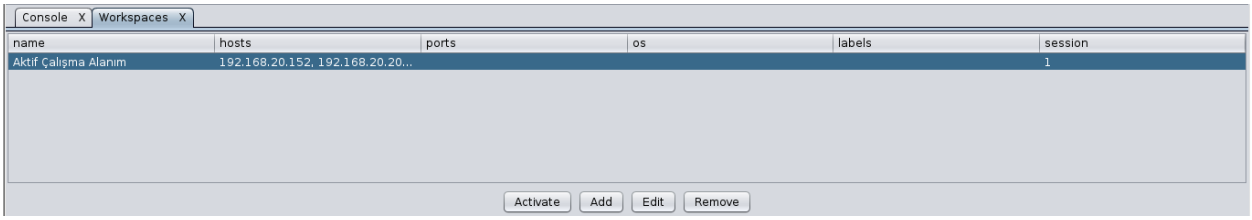
Add butonuna tıklandığında belirlenen adresler çalışma alanına eklenecektir.

3.2 DİNAMİK ÇALIŞMA ALANLARI

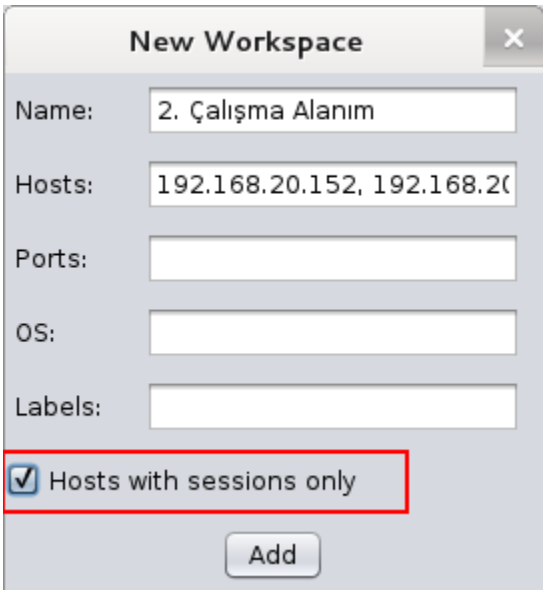
Eğer üzerinde çalışılan ağda aktif olarak bulunan cihaz sayısı fazla ise, hedefleri sadece bir çalışma alanında kontrol etmeye çalışmak işi zorlaştıracaktır.
Üzerinde çalışmak istenilen hedefleri içerisinde barındıran bir çalışma alanı oluşturulabilir.
Bunun için, **Workspace -> Manage**



Bu seçeneklerden sonra açılacak olan pencerenin ekran alıntısı,

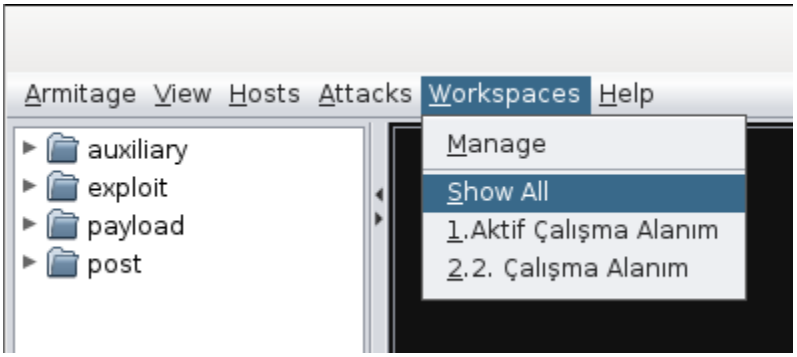


Alıntıda görüldüğü gibi daha önce oluşturulan bir çalışma alanı mevcut. Şimdi yeni bir tane daha eklenebilir. Bunun için **Add** butonuna tıklanılması yeterli, açılacak olan diyalog penceresi;

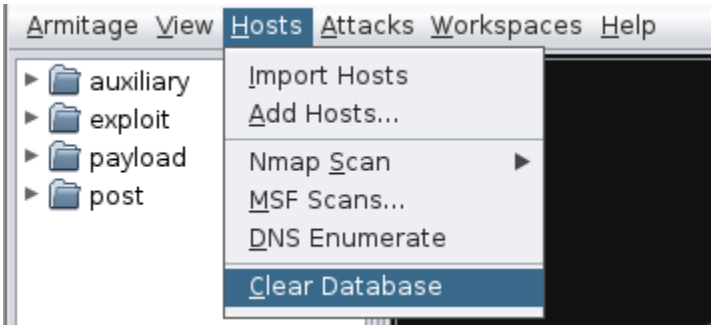


Açılan pencerede çalışma alanının daha etkin bir şekilde oluşturulabilmesi için bazı filtreler belirlenmiştir.
Name: Çalışma alanının ismi (istenilen bir isim verilebilir).
Hosts: Bu kısma çalışmak istenilen cihazların IP adresleri girilir.
Ports: Bir sistemde açıklıklar farklı portlar üzerinde bulunan farklı servisler dolayısı ile meydana gelir, etkin bir filtreleme için bu filtre kullanılabilir.
OS: Bir ağda kullanıcılara bağlı olmak ile birlikte farklı işletim sistemleri bulunabilir. İşletim sistemi tabanlı bir filtre yapılabilir. Fakat tecrübe edildiği oranda, bu filtre kararlı çalışmamaktadır.
Burada en önemli filtrelerden bir tanesi **Hosts with sessions only** seçeneğidir. Otomatik olarak açıklıkların tarandığı ve bazı cihazlar üzerinde açıklıklarından faydalanarak oturum açıldığı düşünüldüğünde, bu seçenek hayat kurtarıcı olacaktır.

Tekrar ana çalışma alanına geçmek istendiğinde, **Workspace -> Show All** seçenekleri ile ilerlenebilir.



Mevcut çalışma bitirilip, raporlar için gerekli veriler alındıktan sonra çalışma veritabanı temizlenebilir. Bunun için yapılması gereken **Hosts -> Clear Database**

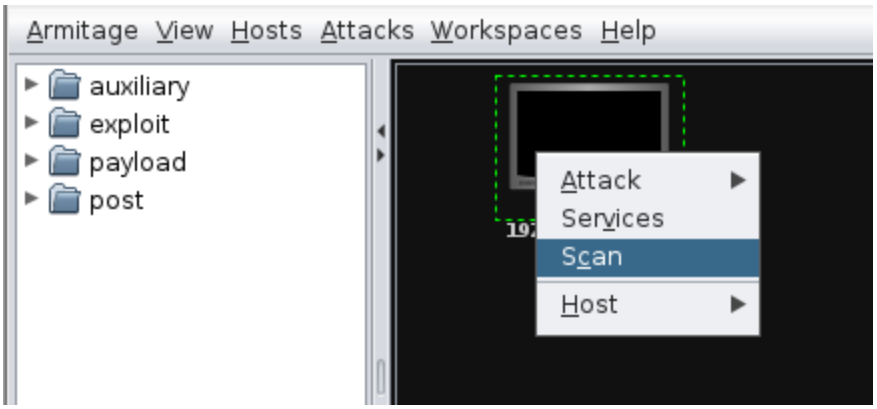


4. AÇIKLIĞIN SÖMÜRÜLMESİ (EXPLOITATION)

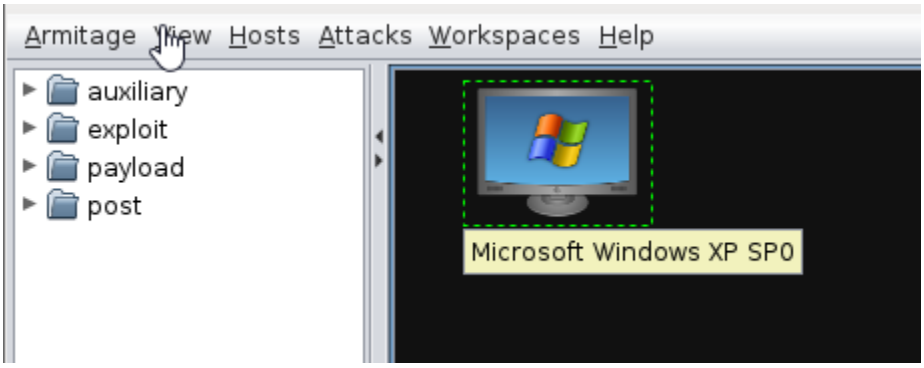
4.1 UZAK SALDIRI YÖNTEMİ

Armitage programı kullanıcılarına hedeflerini uzaktan exploit etme (var olan açıklığı sömürme) imkânı sağlamaktadır.

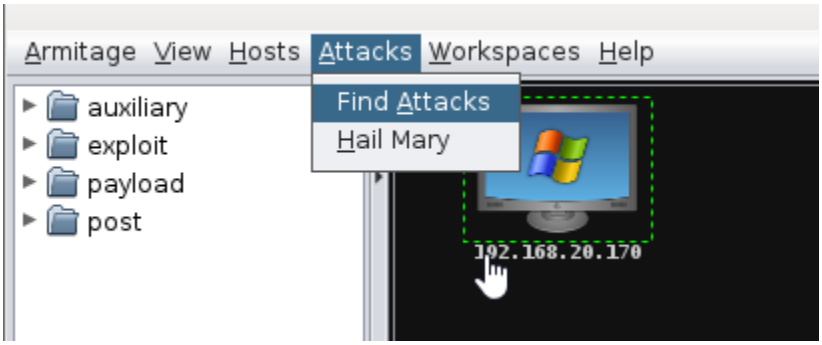
Çalışma alanına hedeflerin girildiği ve işletim sistemlerini tespit edecek şekilde taramaların başlatıldığı varsayılsın (hedef seçilip sağ tıklandıktan sonra **scan** 'a tıklamak yeterli).



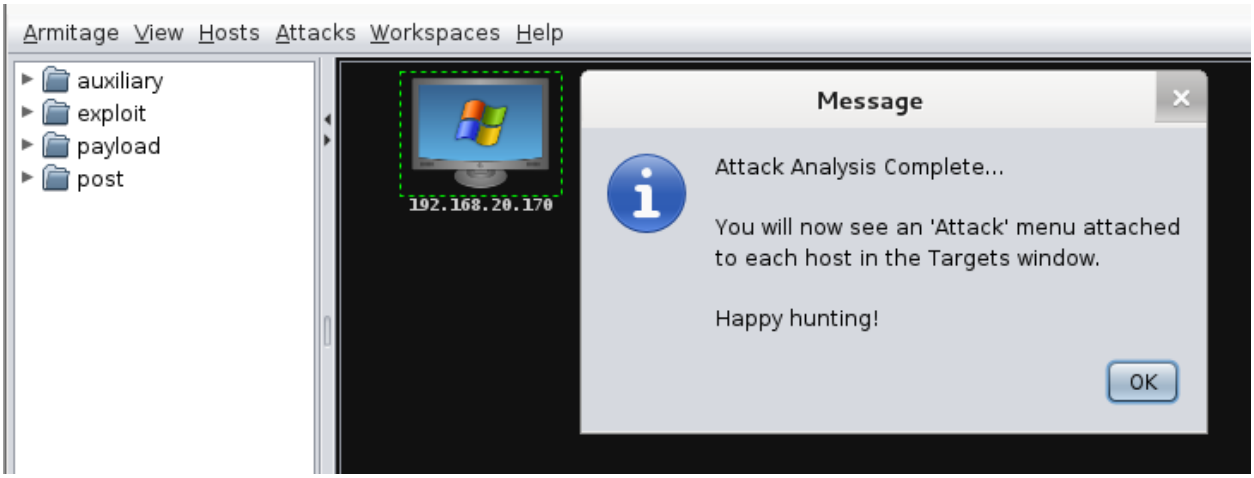
Bu işlem sayesinde hedefin işletim sistemi, hedefte bulunan açık portlar ve üzerinde çalışan servisler tespit edilir. Bu tespit o hedefe uygun açıklıkların belirlenmesi açısından önemlidir.
Bu taramadan sonra işletim sisteminin tespit edilmiş olması gerekli. Örnek olarak ekran görüntüsü alınmıştır.



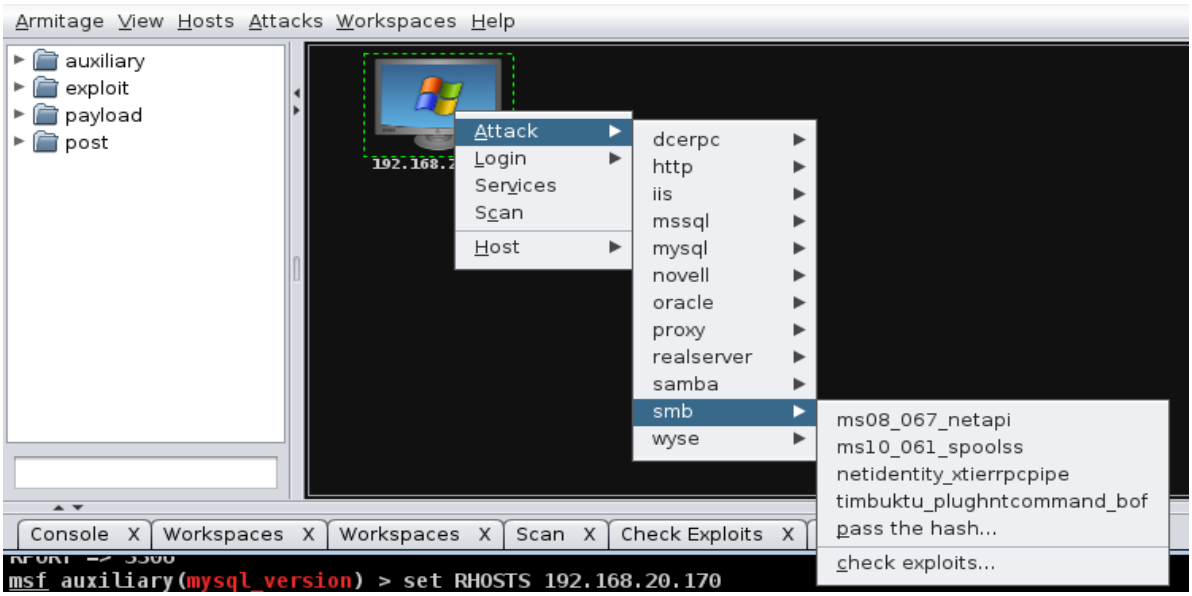
İşletim sisteminin sürümü ile birlikte tespit ettikten sonra şimdi sıra işletim sisteminin barındırabileceği açıklıkları taramaya geldi. Bunun için hazırlan ekran alıntısı takip edilebilir. Taramaya başlamadan önce hedefin seçili olmasına dikkat edilmelidir.



Tarama bittiğinde karşılaşılacak olan ekran.



İlgili açıklıkları görüntüleyebilmek için hedefe sağ tıklanmalıdır.



Not: Burada iki noktaya değinmek gerekiyor;

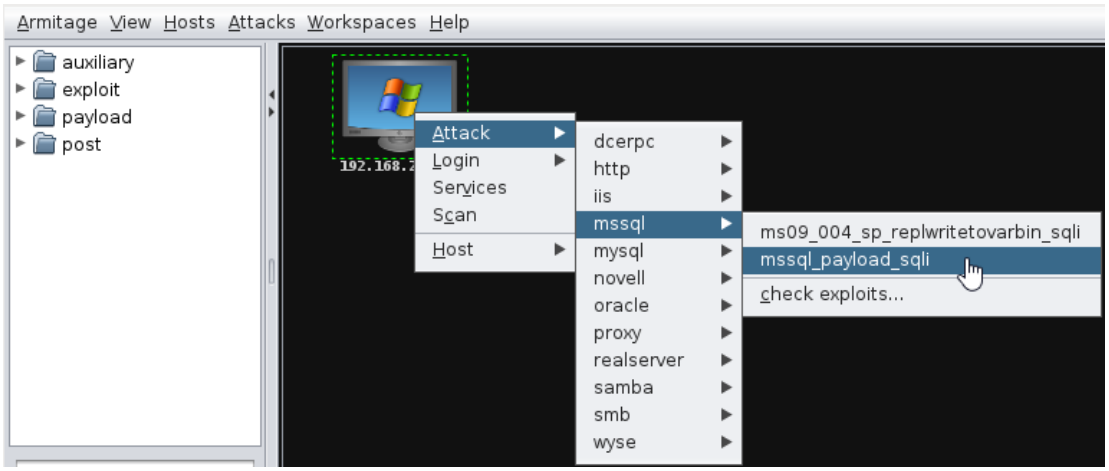
1. İşletim sistemin markası kadar sürümü de önemlidir. Ama maalesef sürümü tespit edebilmek için, sisteme çeşitli şekillerde giriş yapmak gerektiğinden **nmap** ya da **Armitage** araçlarının sürüm bilgisi doğruyu yansıtmayabilir.
2. Hedef için önerilen açıklıklar; ilk maddede değinilen belirsizlik nedeni ile önerilecek açıklıklarda gerçeği yansıtmayabilir. Ama grafiksel ara yüzü sayesinde bu açıklıkları denemek kolay olduğundan ve dahası tüm önerileri deneyebilecek bir modülü olduğundan dolayı, denemekten bir zarar gelmeyecektir (tabi güvenlik

politikası gereği sisteme başarısız giriş sayısının sınırlı tutulmadığı durumlarda, aksi takdirde hedef sistem belirli bir süre erişime kapatılabilir).

A. ÖNERİLEN AÇIKLIĞIN KULLANILMASI

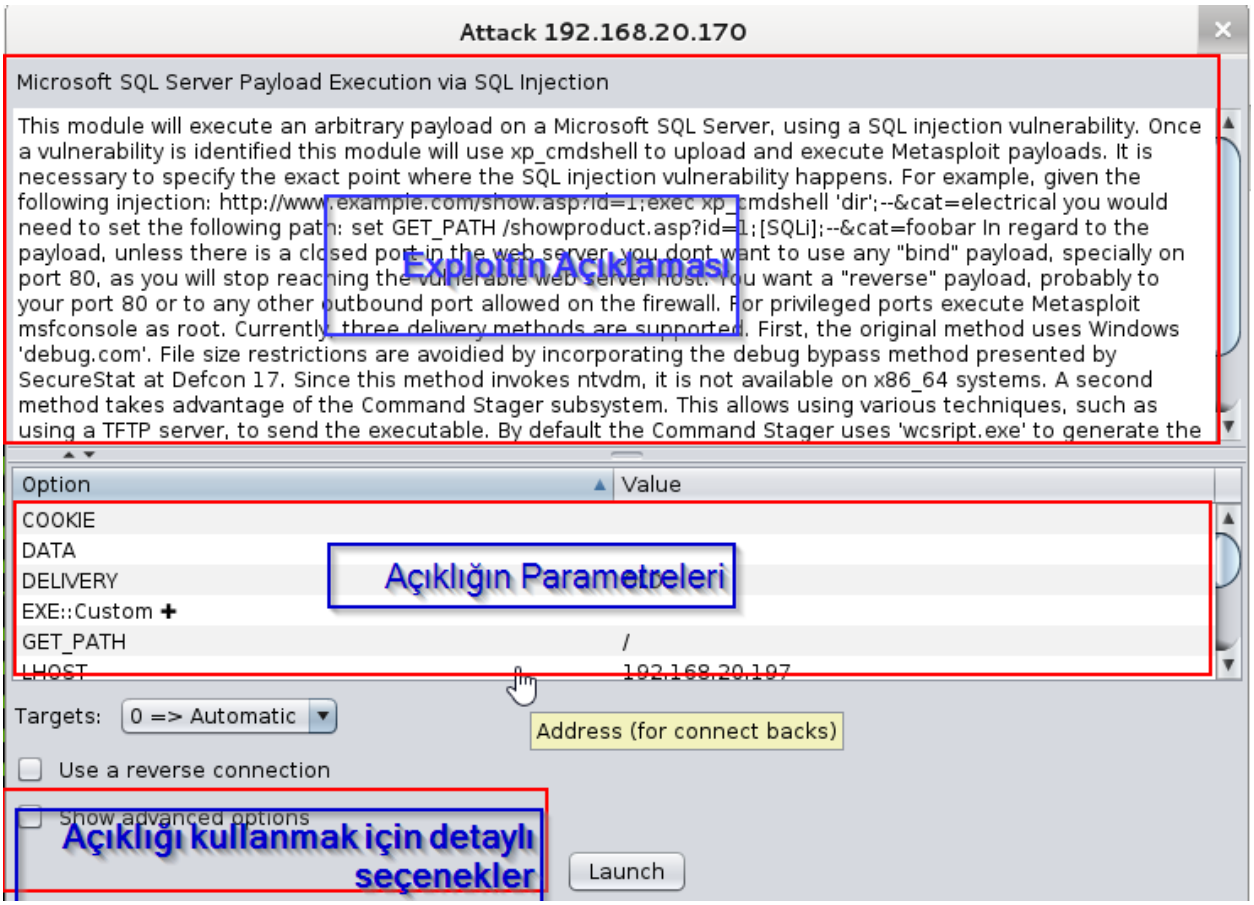
- Başarısız bir exploit girişimi örneği

Önerilen açıklıklardan bir tanesi tıklanarak kullanmaya başlanabilir. Hedefe sağ tıklanıp bir tanesinin seçilmelidir, önce başarısız olunacak bir exploit seçilsin.



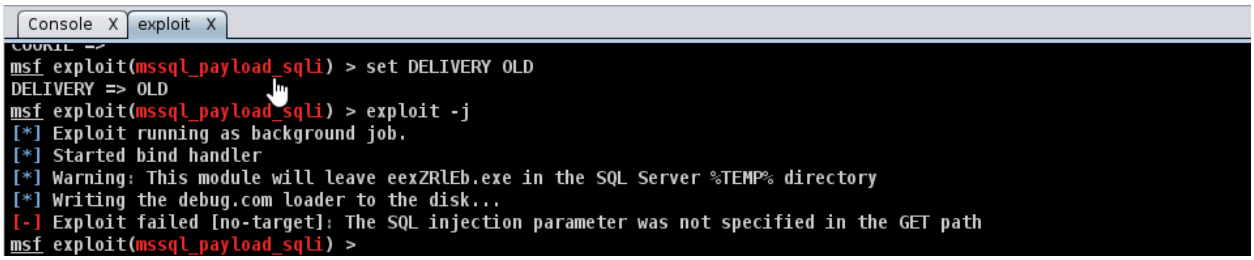
Şunu itiraf etmek gerekir ki, hedef sistemde MSSQL yüklü değil, yukarıda belirtildiği gibi öneriler sizi başarıya götürmeyebilir.

Ama başarısız bir exploit denemesinin çıktılarını görmek için devam ederek exploit seçilsin.



Armitage kullanıcıya metasploitin konsol komutlarından uzak, güzel bir arayüz olanağını sağlar.
Açıklığı daha garantili bir şekilde sömürebilmek için "**Açıklığın Parametreleri**" ve "**Açıklığı kullanmak için detaylı seçenekler**" kısımlarından faydanılmalıdır. Şimdi gerekli ayarlamaların yapıldığı ve çalıştırılmaya hazır olduğu varsayılmaktadır.

Daha önce belirtildiği gibi her exploit girişimi için yeni bir konsol açılır ve hedef ile iletişim o konsol üzerinden devam eder.

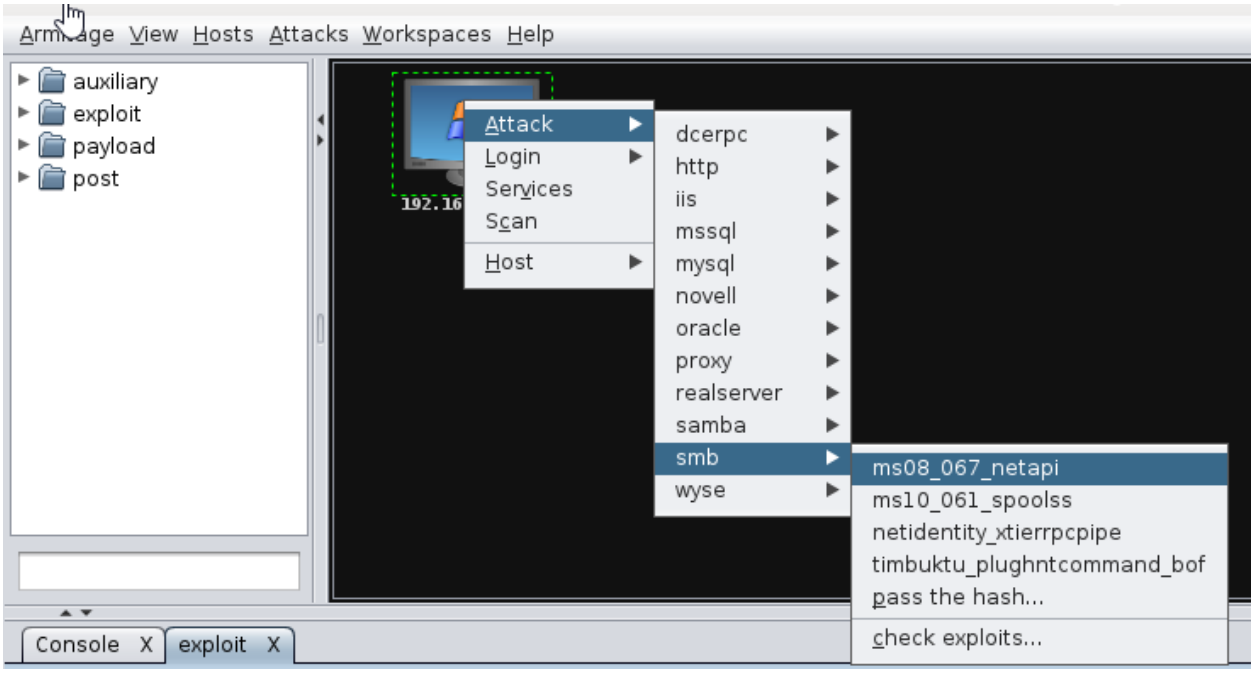


Bu ekran alıntısında da belirtildiği gibi exploit girişimi başarısızlık ile sonuçlandı.

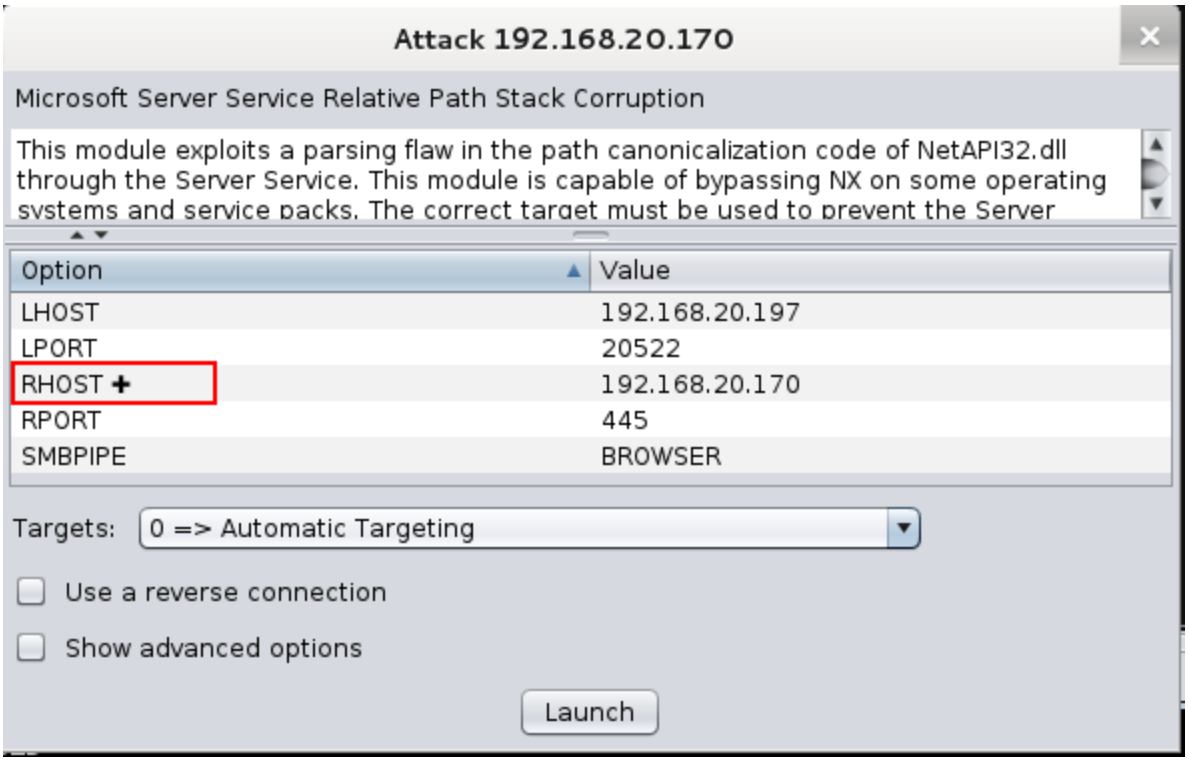
- **Başarılı bir exploit girişimi**

ms08-067 açıklığı çok başarılı ve uzaktan saldırıya olanak verdiği için çok kullanışlı bir exploitttir.

Hedefe sağ tıklayıp ve ms08-067 açıklığı seçilir.

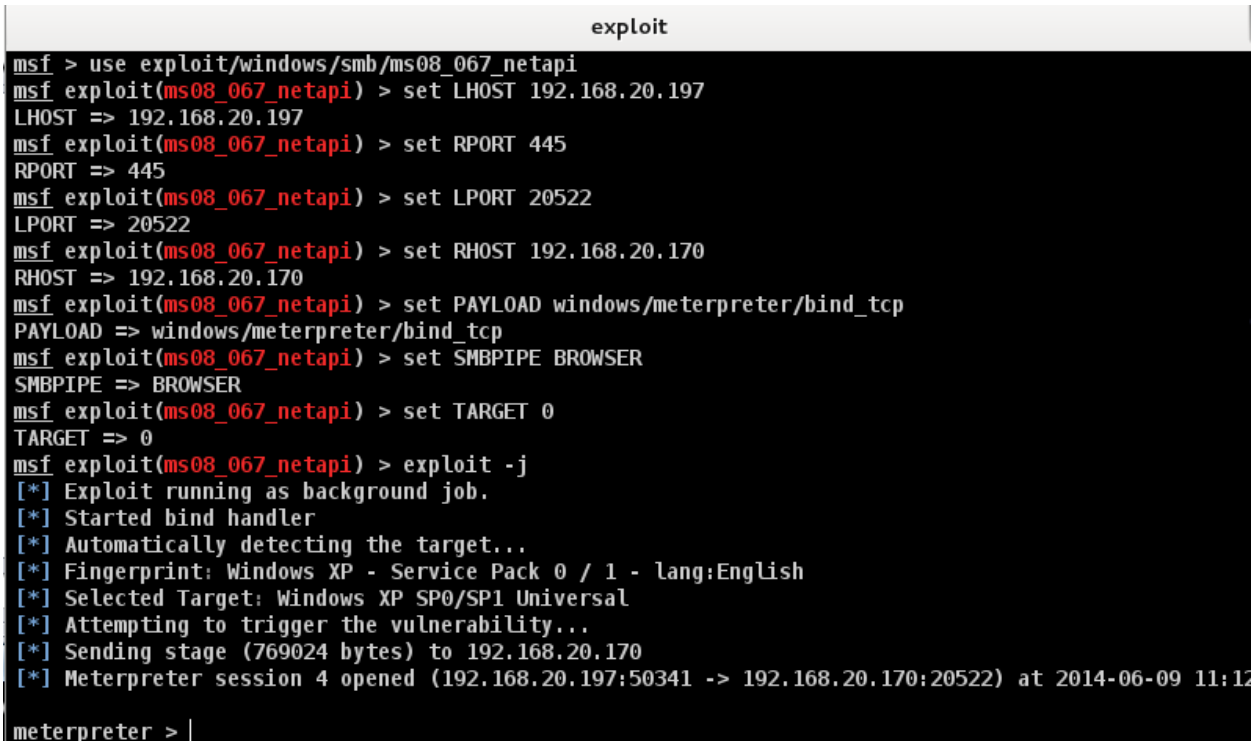


Açıklık tıklandığında ekrana gelecek olan pencereyi görmek adına ekran alıntısını hazırlanımıştır.



Açıklıkların parametrelerine dikkat edilmelidir. Alıntıda görüldüğü üzere bazı değerlerin yanında **+** işareti var, bunun manası o değerin boş olamayacağı. Değiştirmek istediğimiz değer için "**Value**" kolonu altındaki ilgili yere çift tıklamak yeterli. Şimdi exploit çalıştırılabilir.

Exploitin çalışması esnasında ekrana dökülecek olan bildirimler;



Bu Exploitin başarılı olduğu, "Meterpreter session 4 opened" bildirimden anlaşılabilir. Bu arada bir sistemde meterpreter oturumu açıldığında, sistem artık saldırgan kontrolü altında demektir.

4.2 KULLANICI TARAFLI SALDIRI

4.2.1 Payload Oluşturulması

Bu bölümde kullanıcı taraflı saldırının nasıl hazırlanacağı, hedef sistem ile saldırgan aramızda nasıl bağlantı kurulacağı anlatılacaktır.

Her hedef kolayca ve uzaktan sömürülecek kadar zafiyet içermeyebilir. Yayımlanan güncellemeleri zamanında uygulayan bir hedef artık kolay bir hedef değildir. Anti virüs programı kullanan bir hedef kolay bir hedef değildir.

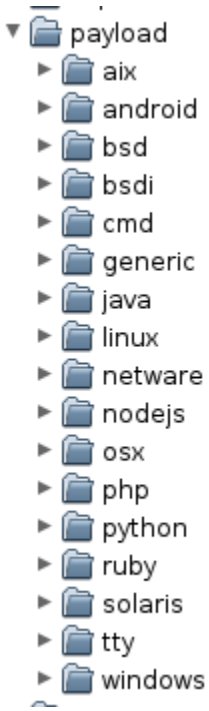
Güncellemeleri takip eden ve güvenlik önlemleri alan bir hedefe sızmak başka teknikler gerektirir. Bu tekniklerden bir tanesi Payload (hedef ile saldırgan arasında bir iletişim kanalı istediğinde bulunacak ve bu trafiği yönetecek olan programcık) oluşturmak gerekir. Hedef, bir şekilde oluşturulan programı çalıştırır ise saldırgan ile direk olarak temasa geçer.

Hedefle saldırgan arasında iletişim kurması amacı ile birçok dosya tipi oluşturulabilir. Bunlardan bazıları;

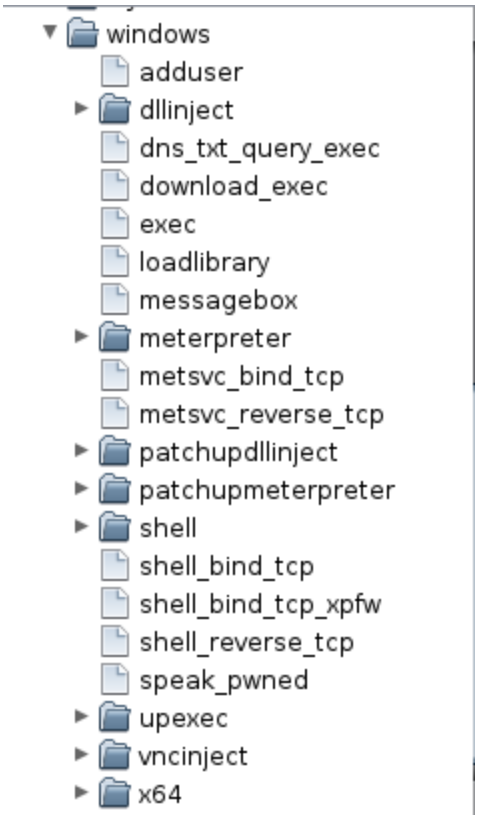
- Exe uzantılı programcıklar
- Word dosyaları
- Excel dosyaları
- PDF dosyaları
- HTML sayfaları…

Görüldüğü gibi saldırı amaçlı kullanılabilecek birçok dosya türü mevcut. Bu dosya türlerini kullanarak sistemlere sızabilmek için farklı payload türleri oluşturmak gerekli.

Metasploit programının zengin bir payload kütüphanesi bulunmakta. Armitage Metasploit programının görsel hali olduğu için aynı kütüphaneye görsel bir şekilde ulaşılabilir. Armitage içerisinde bulunan payload kategorileri;

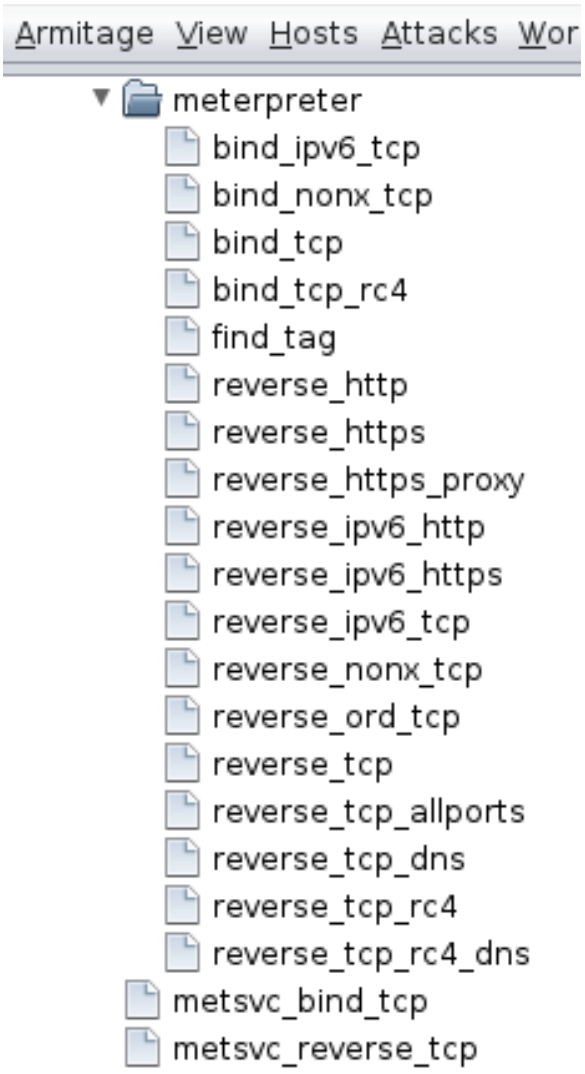


Görüldüğü gibi birçok platform için hazırlanmış payload bulunmakta. Windows klasörünü genişletilip ve çeşitleri görülebilir.

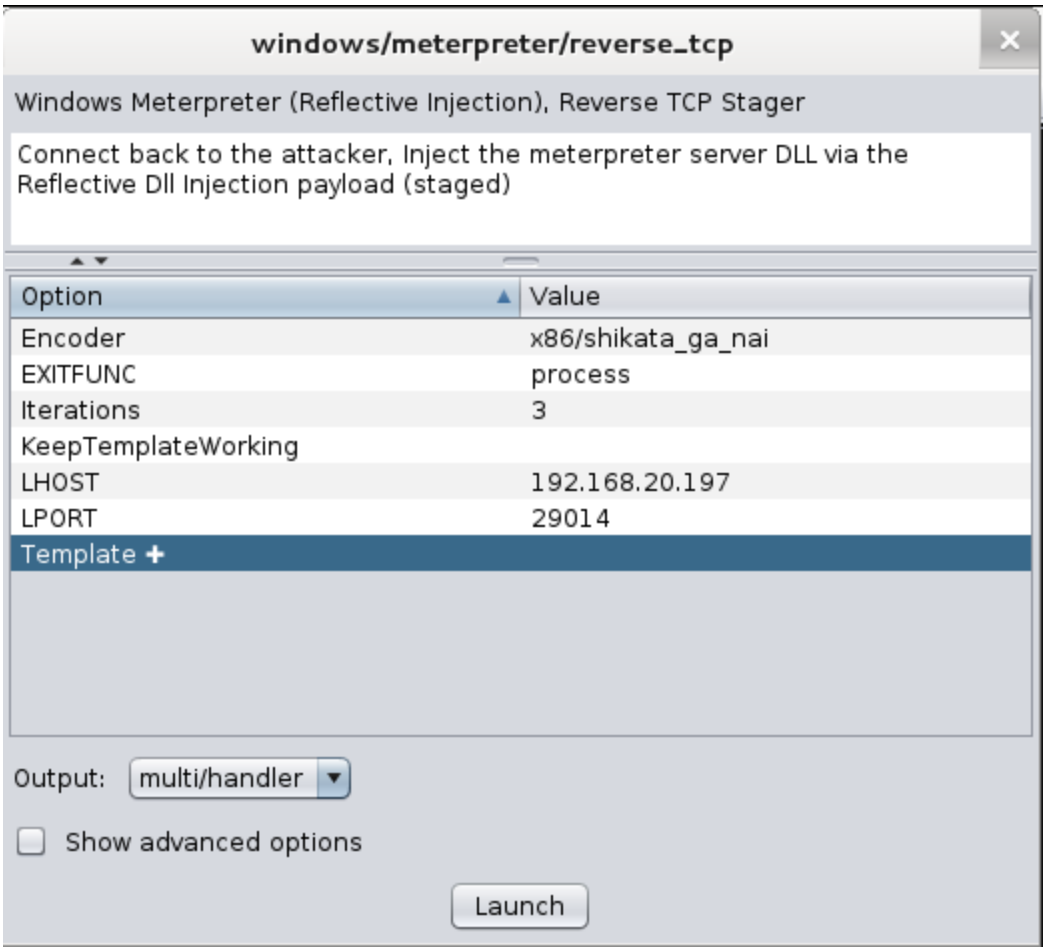


Daha önce belirtildiği gibi meterpreter çok başarılı ve kapsamlı bir oturum yönetme aracı olduğu için bir sistemde bu oturumu açabilmeye çalışmak, istenilen verilere ulaşabilmek açısından önemli olacaktır.

Meterpreter oturumunun elde edilebileceği saldırı çeşitlerini göstermek adına hazırlanan ekran görüntüsü;



Yine bu çeşitler arasında “reverse_tcp”, “reverse_http” ve “reverse_https” en popüler ve kararlı saldırı teknikleridir.
Örnek saldırı “reverse_tcp” tekniği ile yapılacaktır.



reverse_tcp seçildiğinde ekrana gelecek olan pencere.

Bazı parametrelerin özellikleri;

Encoder; derlenecek olan programın derlenme şeklini belirler.

LHOST; Payload çalıştırıldığında uzak bir sisteme bağlantı açmak isteyecektir. Bağlanılacak hedefin adresi LHOST adresidir.

LPORT; bu değer hedefin saldırgana hangi port üzerinden bağlanacağını belirler.

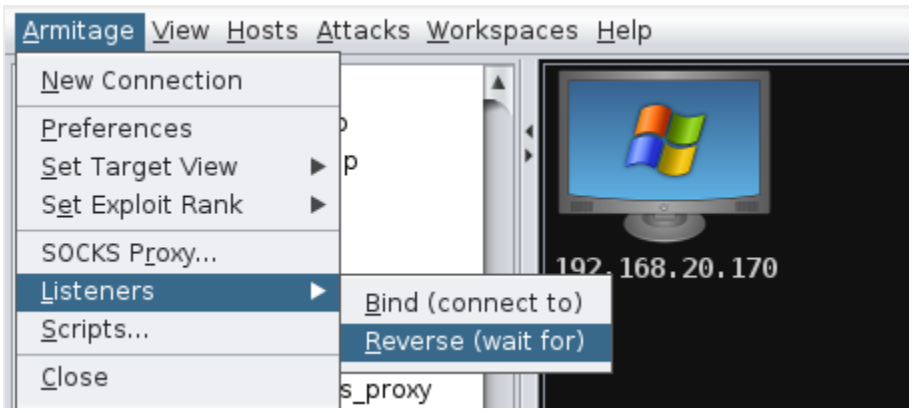
Not: Bazı sistemlerin ulaşabileceği port numaraları kısıtlanmıştır. Bu güvenlik önlemini aşmak için LPORT değerinin 80, 443, 445, 139 gibi tanınmış ve güvenlik duvarları tarafından güvenilen portlara ayarlayabilirsiniz.

Template; Anti virüs programlarını atlatmak için kullanılacak tema.

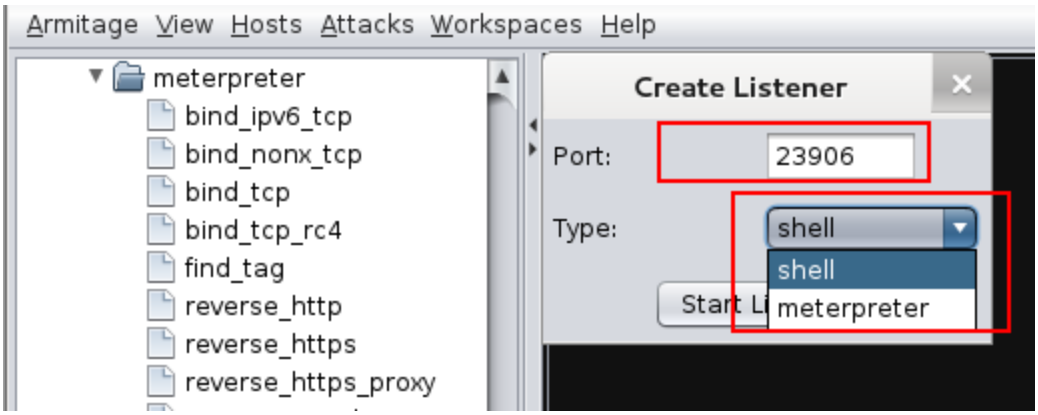
Output; Payload çıktısının türünü belirlemek için kullanılır.

4.2.2 Payload Dinleyicisi

Kullanıcı taraflı saldırı yönteminde çok önemli bir evrede hedeften gelen bağlantı istediğinin ıskalanmadan değerlendirilmesidir. Bunun için Metasploit programı "payload handler" imkânı sunmaktadır. Karşı taraftan gelecek olan istekleri yönetmek için kullanılan bir programdır. Bu programa erişmek için Armitage ara yüzünden Armitage -> Listener -> Reverse (wait for) seçenekleri takip edilir.



Reverse (wait for)' i tıkladığımızda ekranımıza gelecek olan pencere,



Daha önce belirtildiği gibi dinlemenin yapılacağı port numarası ile oturum yönetici program tipinin belirlenmesi önemlidir.

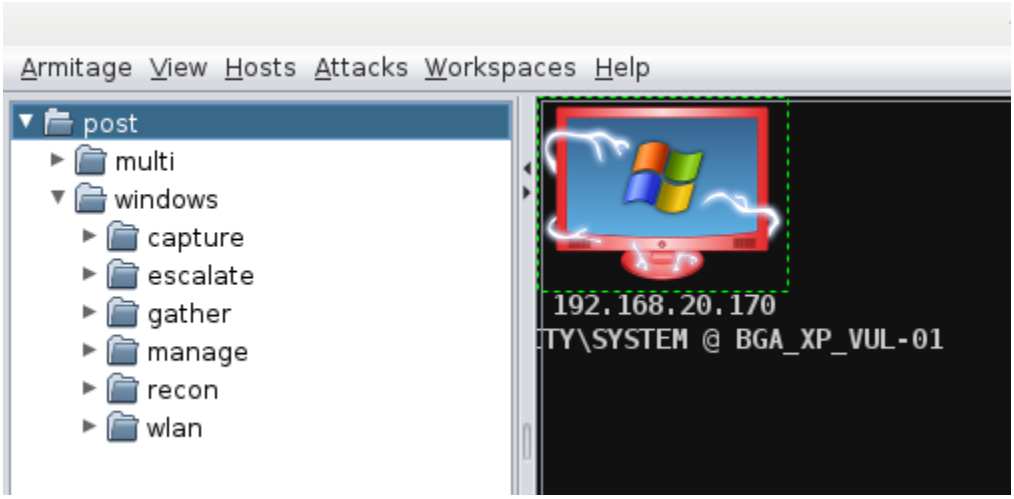
5. POST EXPLOITATION

Bir sisteme, uzaktan veya kullanıcı taraflı bir saldırı düzenleyerek giriş yapıldığı varsayılsın. Peki, şimdi neler yapılabilir;

- **Hak yükseltme**, Bir sisteme belirli bir açıklık üzerinden giderek giriş yapılabilir. Neyin açıklığını kullanarak giriş yapıldı ise o servis veya kullanıcının hakları kullanılabilir. Ama bu servis veya kullanıcının hakları

yapılmak istenenler için yeterli olmayabilir. Bir işletim sisteminde veri yazma veya okuma katmanına gelindiğinde işlemi yapmak isteyen kullanıcı/servise yetkilerini tanıtan bir bilet (token) sorulur. Bu vize gibidir. Başkasına ait olan bir vize sahiplenebilir. İşte, hak yükseltme tam olarak bu manaya gelmektedir. Hak yükseltme olayını başkasının biletini alarak yapmak "**Token Stealing**" diye anılmaktadır.

- **Dosya Görüntüleme (File Browser),** Metasploit yardımı ile bir sisteme sızıldığında dosyaları ve klasörleri kod yardımı ile yönetmek gerekir, fakat Armitage görsel bir yönetim ara yüzü sağlar. Bu ara yüze ulaşmak için hedef panelinden ele geçirilen hedefe sağ tıklanır ve **Meterpreter N -> Explore -> Browse Files** yolu izlenir. Erişim yetkilerine göre dosyalar okunabilir, indirilebilir, silinebilir. Bunun için dosyalama ara yüzünde işlem yapmak istediğimiz dosyaya sağ tıklamak yeterli olacaktır.
- **Komut Satırı;** Bir sisteme sızma gerçekleştirildiğinde, o sistemi komut satırı ile yönetebilmek için hedefe sağ tıklanıp, **Meterpreter -> Interact -> Command Shell** seçenekleri izlenebilir. Aynı şekilde **Meterpreter Shell** penceresi açılabilir.
- **VNC;** Armitage hedef bilgisayarı uzak masaüstü bağlantısı ile yönetebilme olanağı sağlar.
- **Ekran Alıntısı ve Webcam Gözetleme;** Sızılan hedef sistemden ekran alıntısı ve kamerasından görüntüler alınabilir. Bunun **için Meterpreter N -> Explore -> Screenshot** seçeneklerinin takip edilmesi yeterlidir.
  Screenshoot seçeneğinin hemen bir altında "**Webcam Shot**" seçeneği ile kamerasından görüntü alınabilir.
- **Post Exploitation Modülleri;** Armitage sisteme sızıldıktan sonra neler yapılabileceği noktasında yardım etmektedir. İlgili seçenekler post klasörü altında bulunmaktadır.



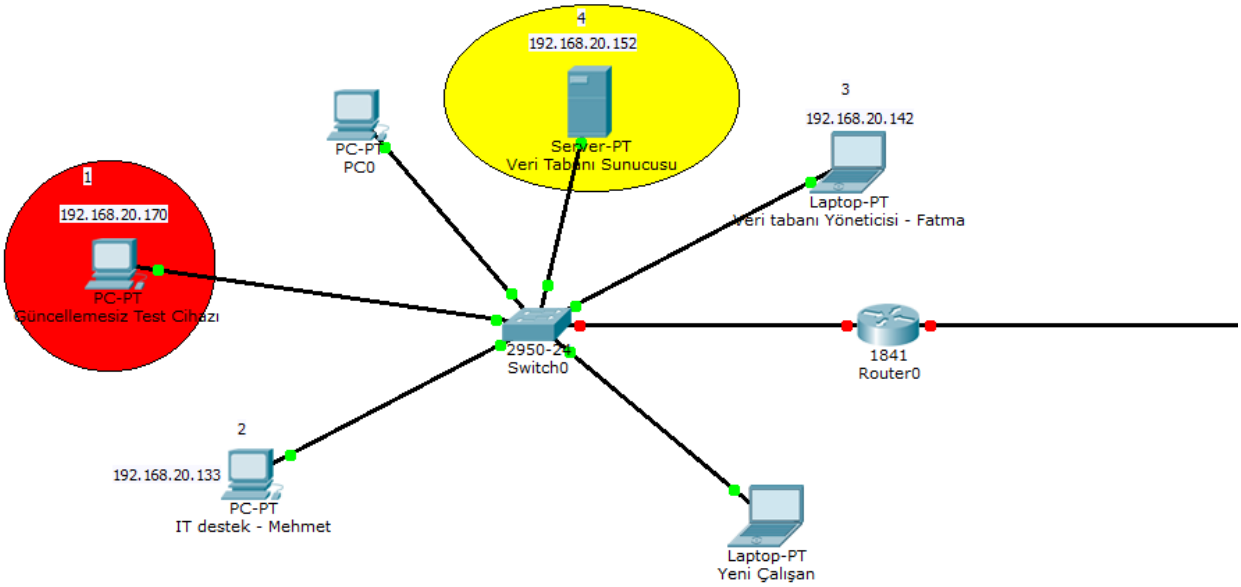
Bu kısımdaki ilgili modüllerin kullanımı forumlardan ve offensive security sitesinden öğrenilebilir.

6. SALDIRI SENARYOLARI

Armitage aracı tanıtılmış oldu. Şimdi senaryolar ile armitage aktif olarak nasıl kullanılabilir sistemlere nasıl sızılabilir ve en önemlisi Post Exploitation olarak neler yapılabilir bunlar incelenecektir.

Senaryo: Bilgi Güvenliği Akademisi Bankasının Veritabanı Erişim Bilgilerinin Elde Edilmesi

Senaryonun uygulanacağı internet ağının topolojisi;



Senaryonun Açıklaması;

BT destekçisi Mehmet şirketinde yapacağı denetlemeleri ve düzenlemeleri, şirketin ağına uygulamadan önce kendisi için hazırladığı laboratuvar ortamında (1 numaralı, Test Cihazı) test etmektedir. Mehmet'in test cihazı güncellemelerden uzak nasıl olsa üzerinde şirkete dair bir program çalışmadığı için güvenlik önlemleri ihmal edilmiştir. Mehmet'in test için kullandığı bilgisayar üzerinde bulunan kullanıcı hesaplarından bir tanesini aynı zamanda kendi bilgisayarında kullanmaktadır. Mehmet işlerin yoğunluğundan dolayı hızlı bir şekilde ulaşabilme amacıyla şirket ağındaki bilgisayarlara ait varsayılan (başlangıç) değerlerini masaüstünde tutmaktadır.

Geçen hafta bilgisayarı yenilenen Fatma (şirketin veri tabanı yöneticisi) önem vermediği giriş bilgilerini değiştirmemiştir. Fatma veri tabanı sunucusuna erişim bilgilerini, bilgisayarının masa üstünde tutmaktadır.

Şirkete yeni alınan çalışanın kötü niyetli olduğu varsayılsın (ki o sizsiniz ☺), Yeni çalışanın sisteme ne kadar zarar verebileceği incelenecektir.
Not: Bu senaryoda amaç Armitage programının kullanımına yönelik pratik bir uygulama gerçekleştirmektir.

Amaç; Veri tabanı sunucusu bilgilerine erişmek, dolayısı ile veri tabanında bulunan verilere erişmek, fakat önce sunucu erişim bilgilerinin edinilmesi gerekmektedir.
İzlenecek Adımlar;

1- Ağı taranacak, hangi cihazların ayakta olduğu ve hangi işletim sistemlerinin kullanıldığı tespit edilecek.
2- Bazı işletim sistemlerinin bilinen açıklıkları bulunabilir, bu açıklıklar denenecek.
3- Sızılan bilgisayarlardan kullanıcılara ait hesap özetleri (hash) alınacak
4- Alınan hash'ler diğer sistemlerde denenecek.
5- Başarılı girişlere, oturum açma denenecek ve bilgi toplanmaya çalışılacak.

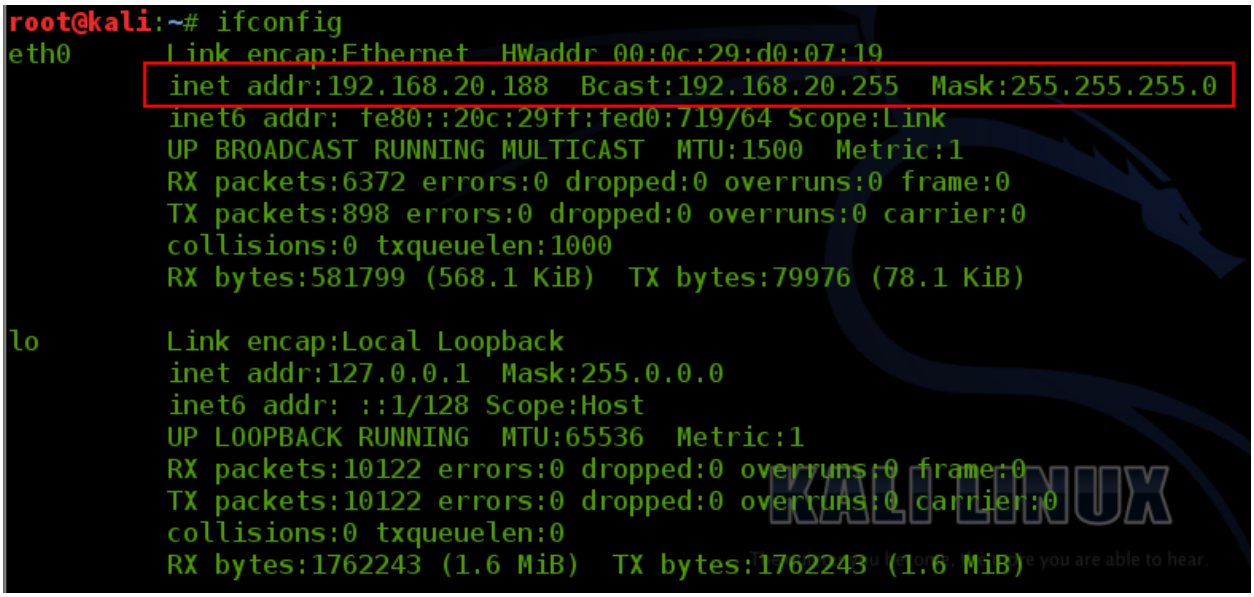
Senaryonun Uygulanması

Şirkette işe başlandığında verilen bilgisayar Kali Linux işletim sistemi ile başlatılır (işletim sisteminin live-usb sürümleri mevcuttur)

Gerekli olan servisler başlatılır;

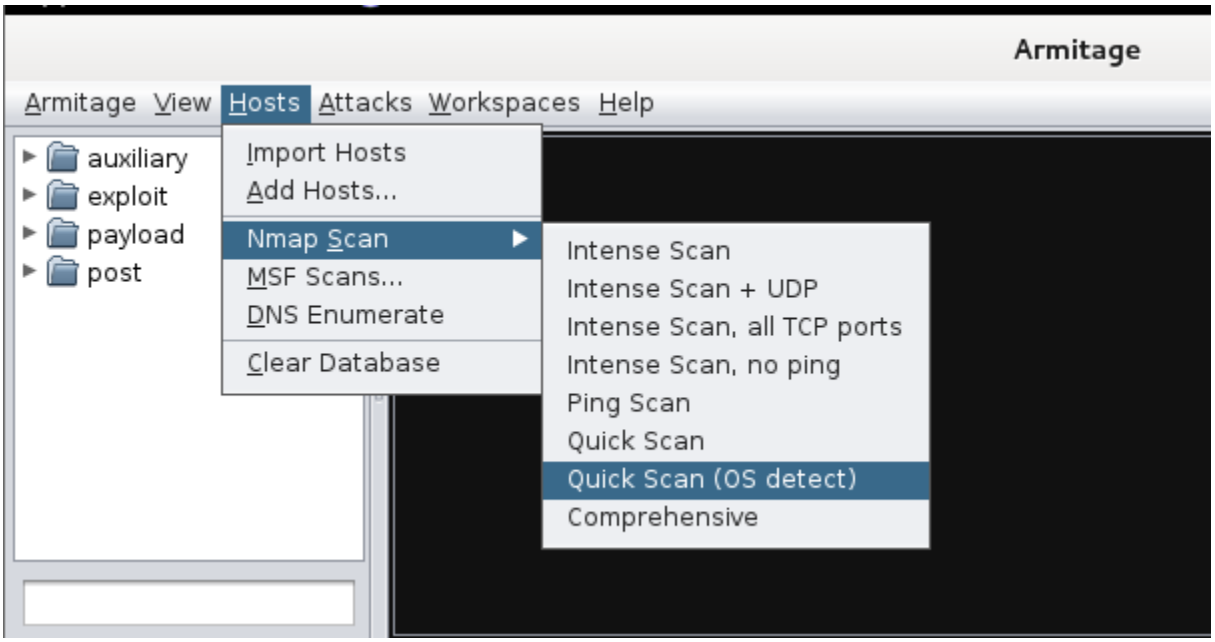
- **service postgresql start**
- **service metasploit start**
- **armitage**

2- Hangi ağda bulunulduğu tespit edilir, IP adresine bakılarak bu bilgi edinilebilir.

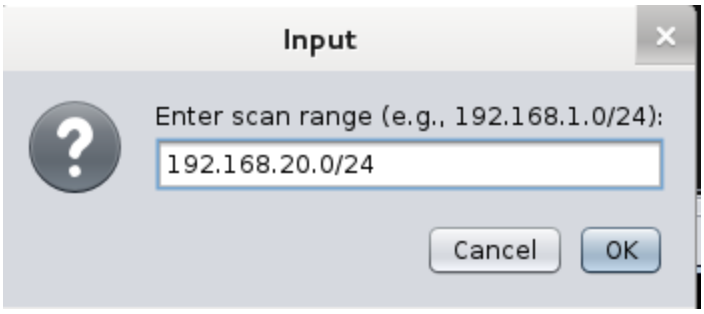


IP adresi 192.168.20.188, o zaman taranması gereken ağ 192.168.20.0/24 olacaktır.

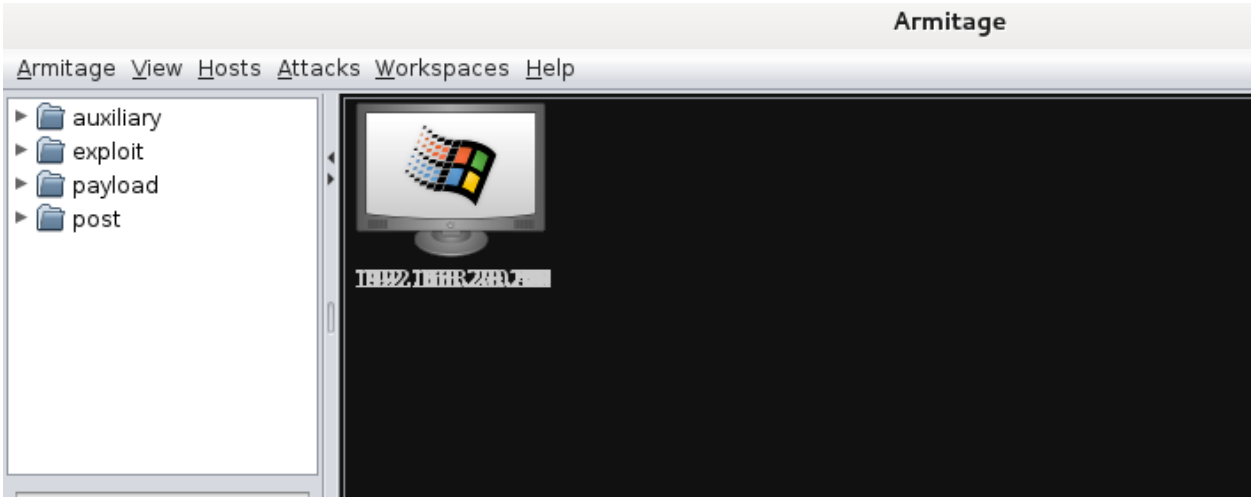
3- Armitage ara yüzünden faydalanarak ağda hangi IP'lerin ayakta olduğu ve hangi işletim sistemi ile çalıştığı tespit edilir.



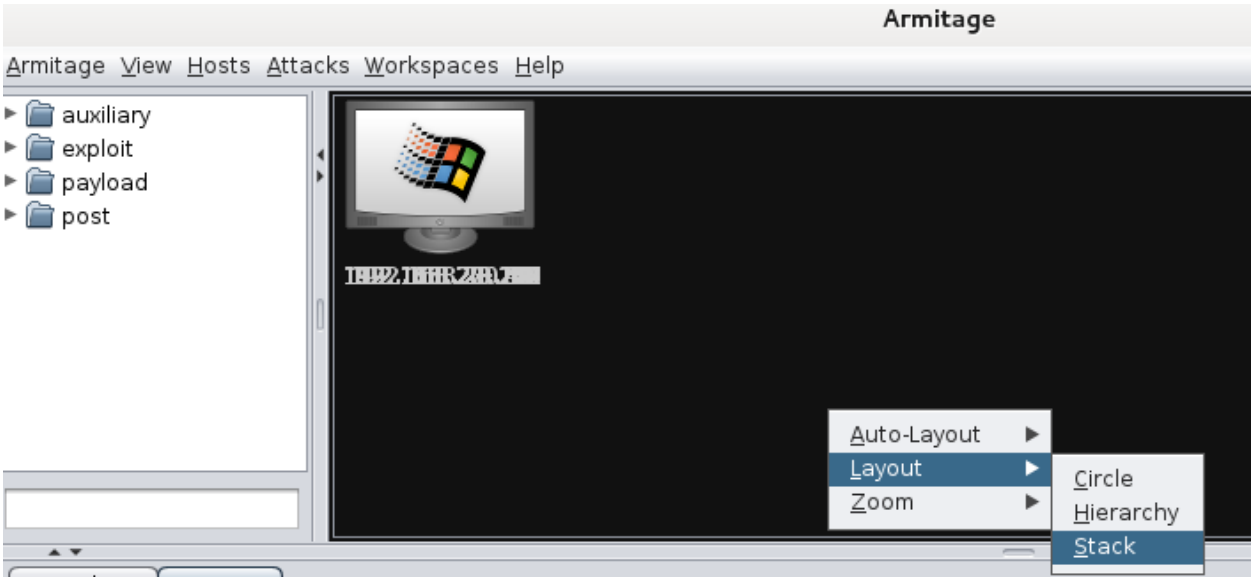
Quick Scan (OS detect) seçildiğinde, ekrana gelecek olan pencerede taranmak istenilen ağ bilgisi girilir.



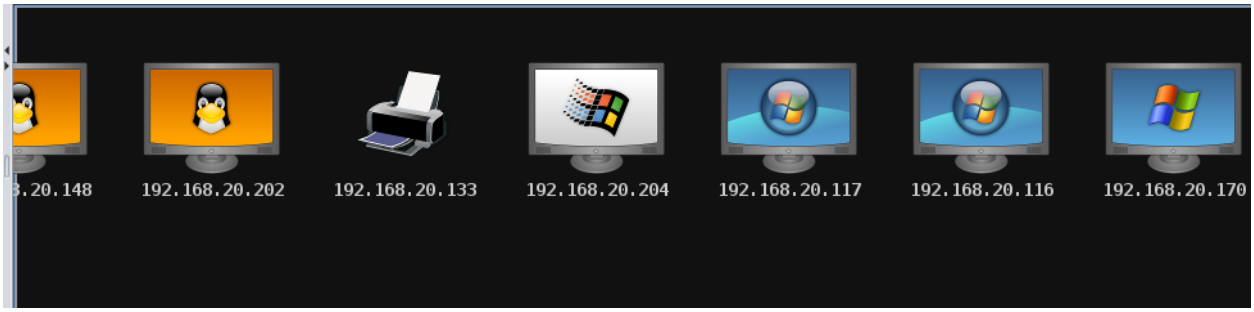
Ve sonucunun ekran alıntısı;



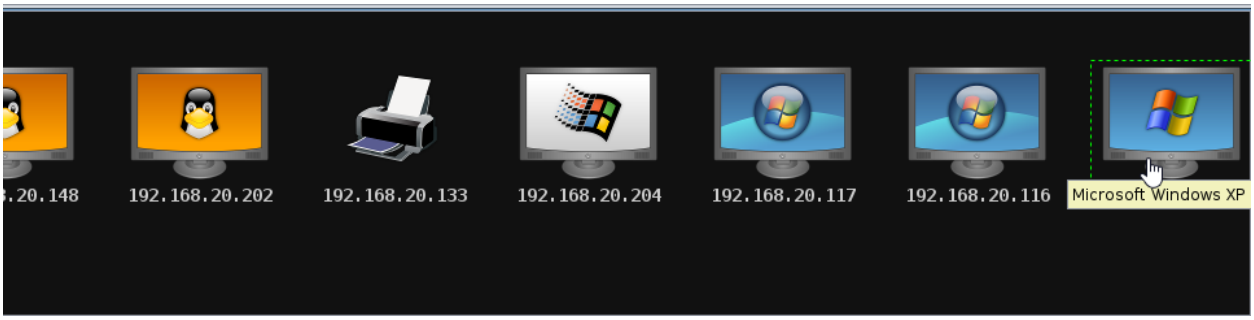
Tarama sonucu elde edilen hedefler böyle üst üste görünür ise, hedef panelinde sağ tıklanıp **Layout -> Stack** seçeneği tıklanır.



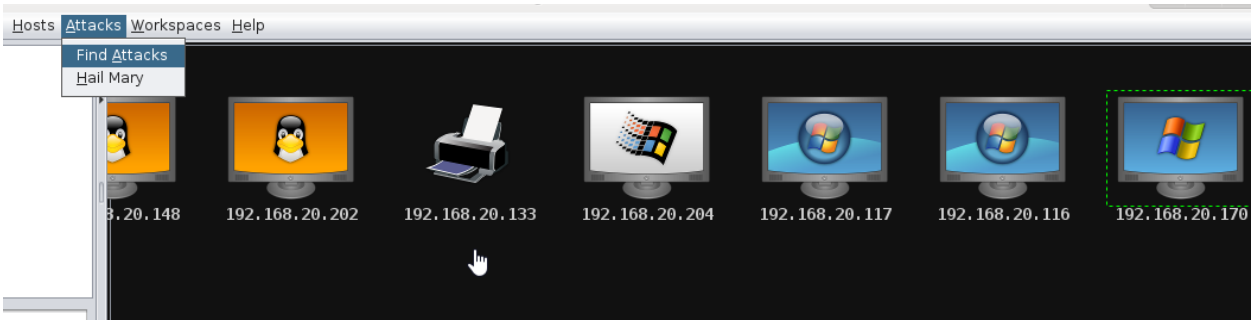
Artık hedefler bir dizi halinde görünecektir.



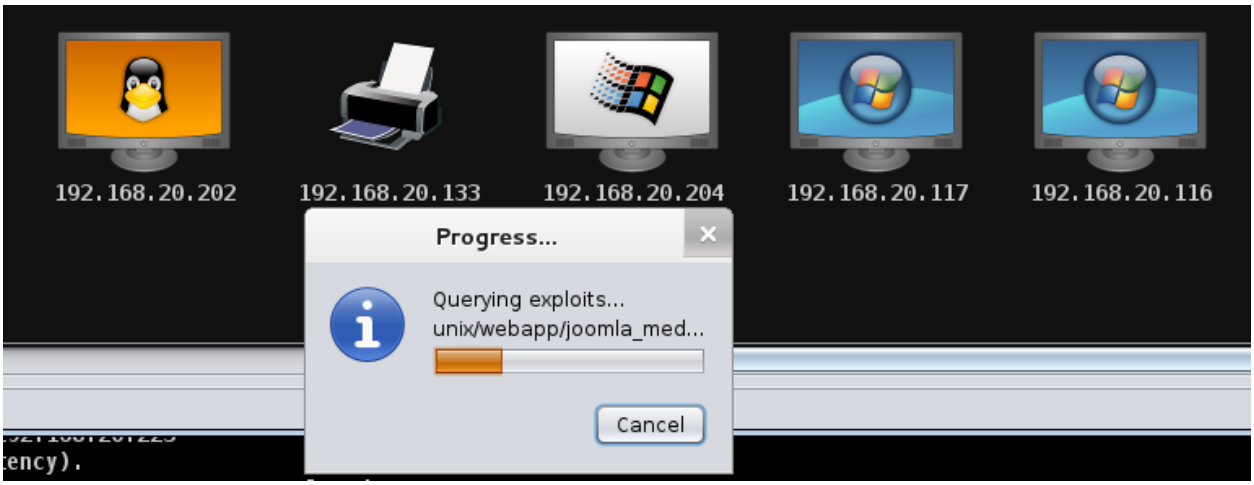
4- Hedeflerin üzerlerine gelerek işletim sistemlerini belirten bildirim yazısını görülmeye çalışılır, aranılan şey eski bir işletim sistemi. Mesela XP.



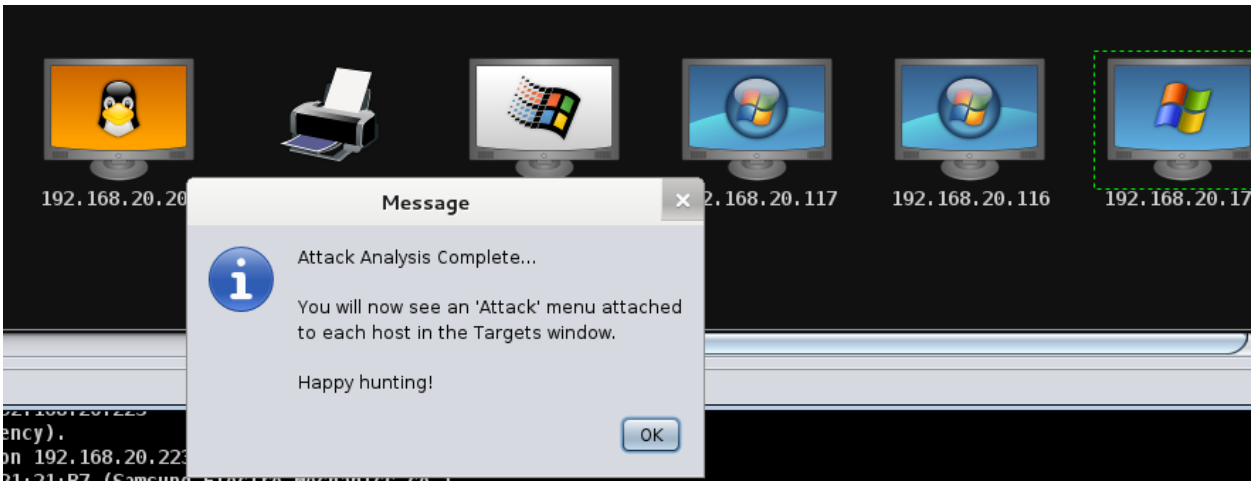
5- Bu işletim sisteminin IP değeri; 192.168.20.172
şimdi bu hedef tıklanıp, Armitage menüsünden **Attacks -> Find Attacks** seçenekleri takip edilir.



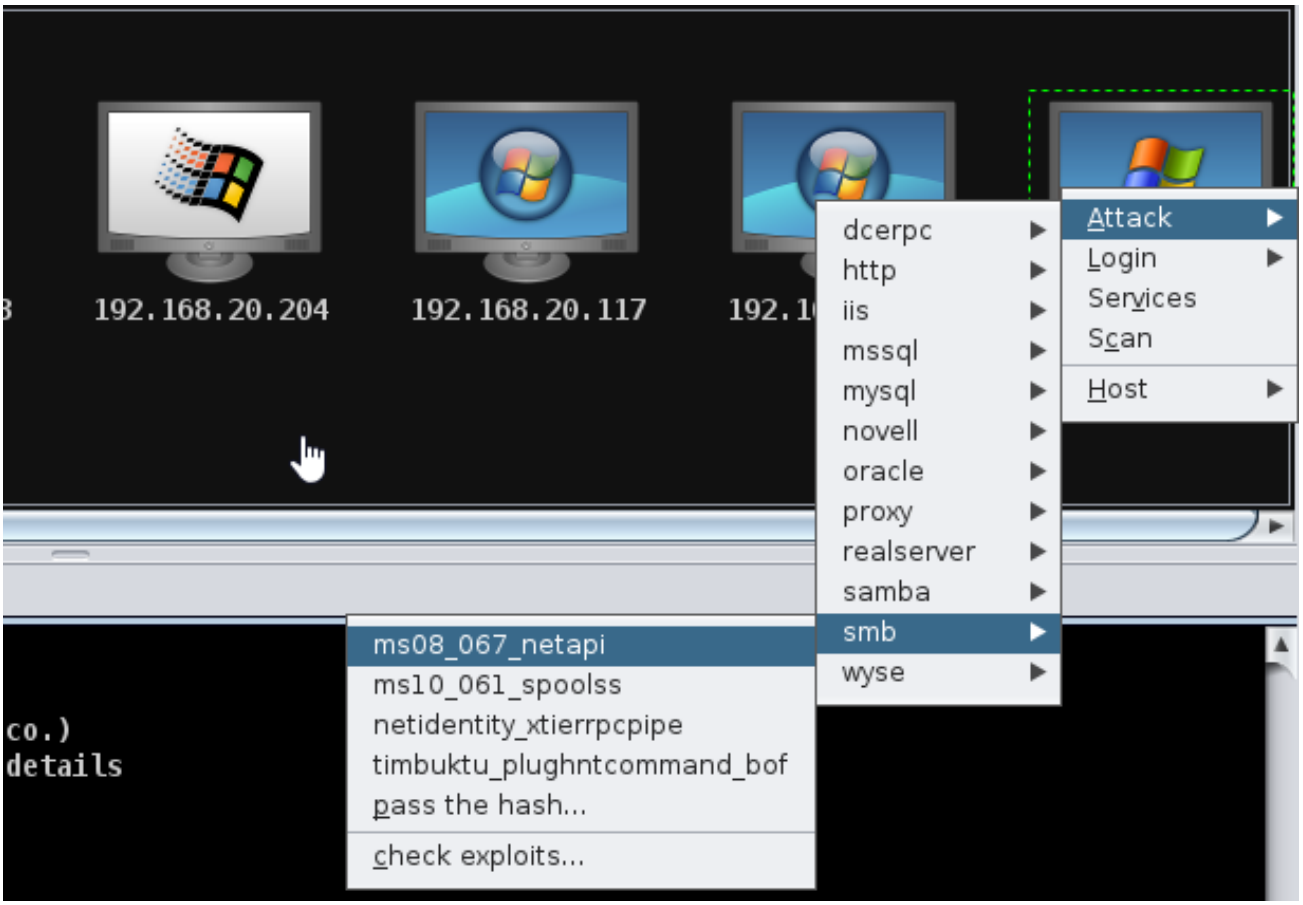
Hedefin işletim sistemi ve Service Pack değeri göz önüne alınarak bir takım exploitler önerilecektir. Bu arama işlemi devam ederken ki ekran görüntüsü.



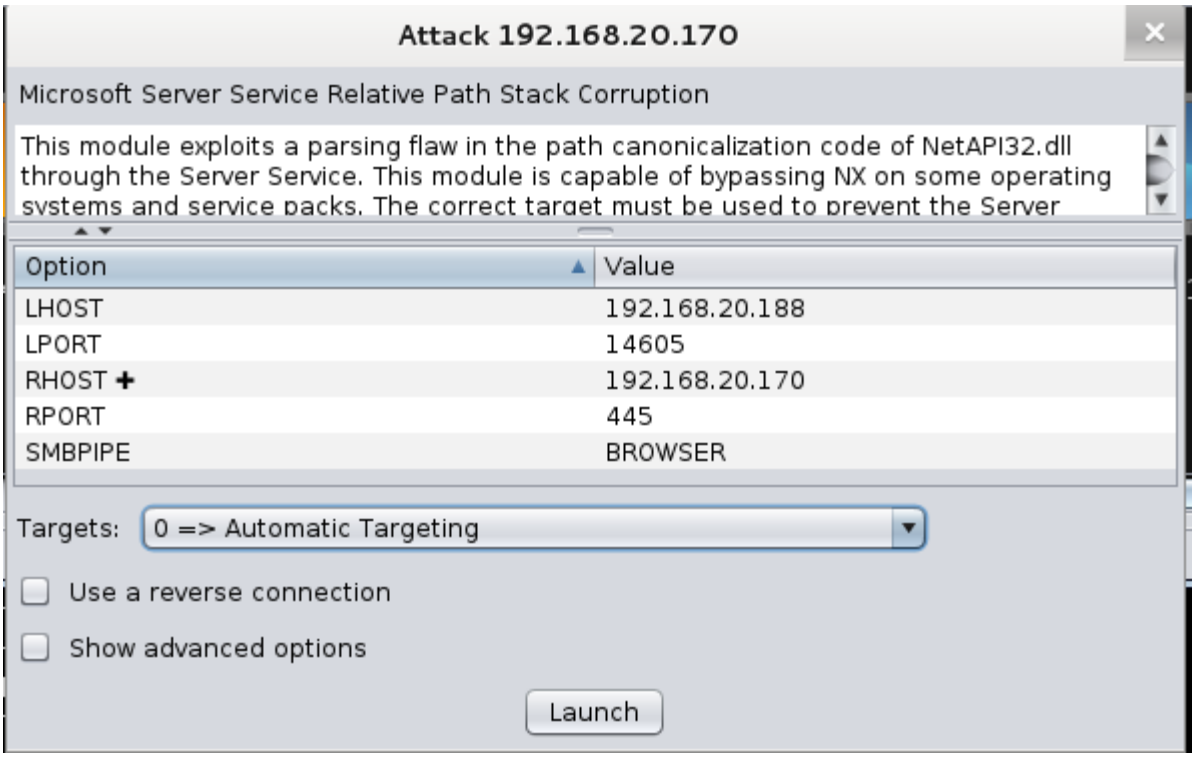
Ve tarama bittiğinde ekrana bastırılacak olan bildirim penceresi.



6- Şimdi hedefe sağ tıklanıp, Attack menüsünden başarı oranı yüksek bir expoit seçilir.



Bu exploit seçildiğinde ekrana bastırılacak olan pencere.

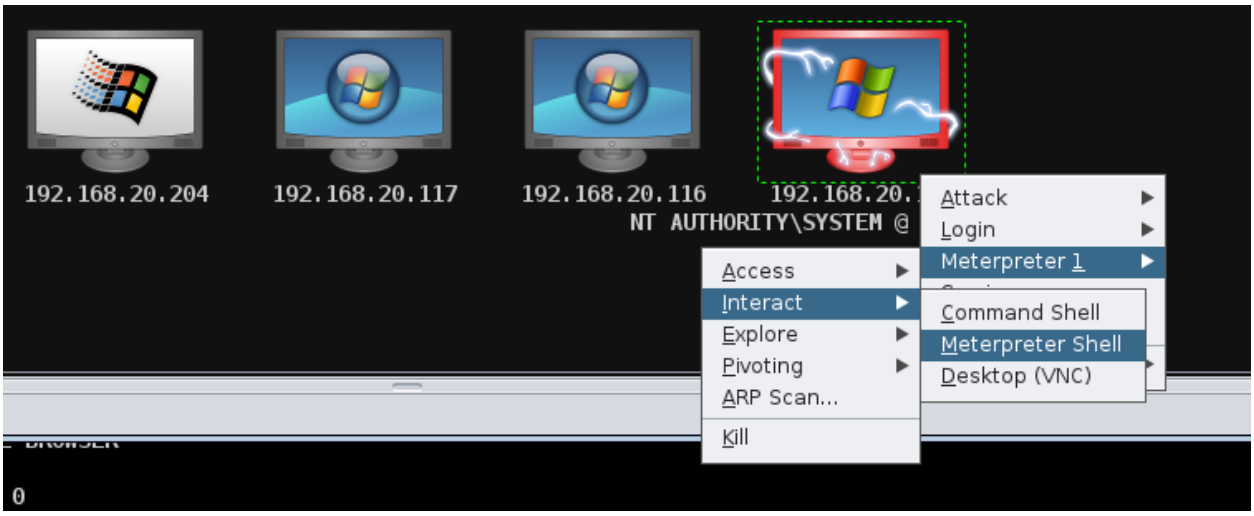


Bu exploit için genelde bir ayarlama yapmak zorunda kalınmaz, çünkü başarılı bir exploit olarak tanınmaktadır. Ama her expoit için aynı şey geçerli değildir. Bazen dinleme portunun, bazen kullanılan payload'ın değiştirilmesi gerekir.
Exploit çalıştırılır.
Başarılı bir exploit sonrası exploit için açılan konsolda görülmesi gerekenler ve hedefin simgesindeki değişiklik.

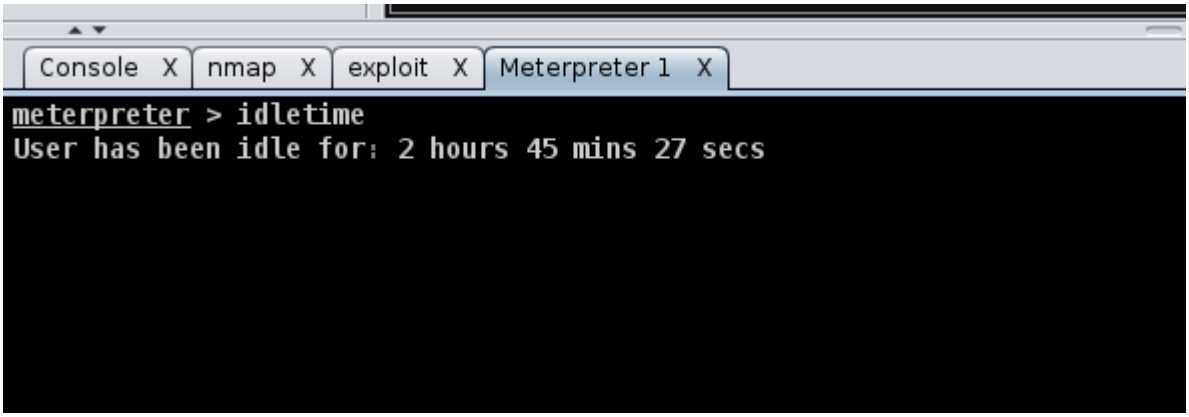
7- Artık hedefe sızılmış, meterpreter oturumu açılmıştır. Şimdi sızılan sistemden veri toplamaya çalışılacaktır.

Hedefle daha iyi etkileşim için meterpreter oturumu etkinleştirilir.

Sağ tık -> Meterpreter 1 -> Interact -> Meterpreter Shell



Sistem ne zamandır boşta bunu gözlenir.

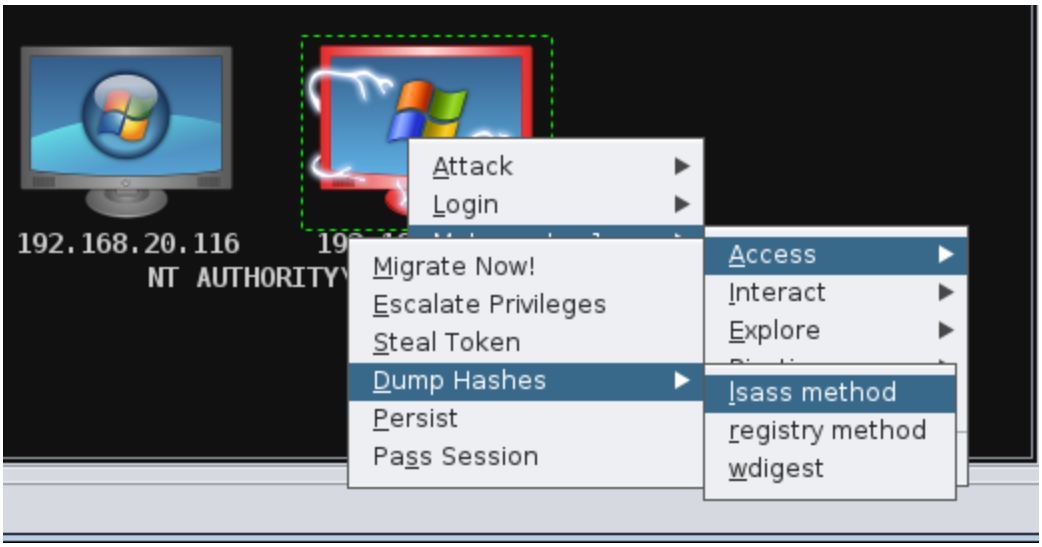


Güzel, yaklaşık üç saattir bir etkinlik söz konusu değil (system kullanıcısı için)

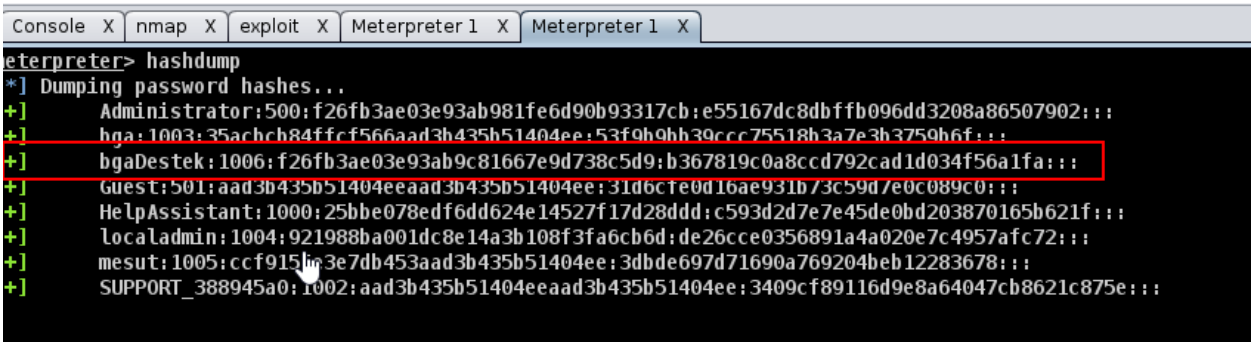
Sistemde var olan kullanıcıların hesap bilgileri alınır.

Hedefe sağ tık -> Meterpreter 1 -> Access -> Dump Hashes Isass method

(Her işletim sistemi için Dump Hashes Isass method başarı ile sonuçlanmayabilir)



Ve kullanıcı hesaplarına ait özetlerin görüntüsü

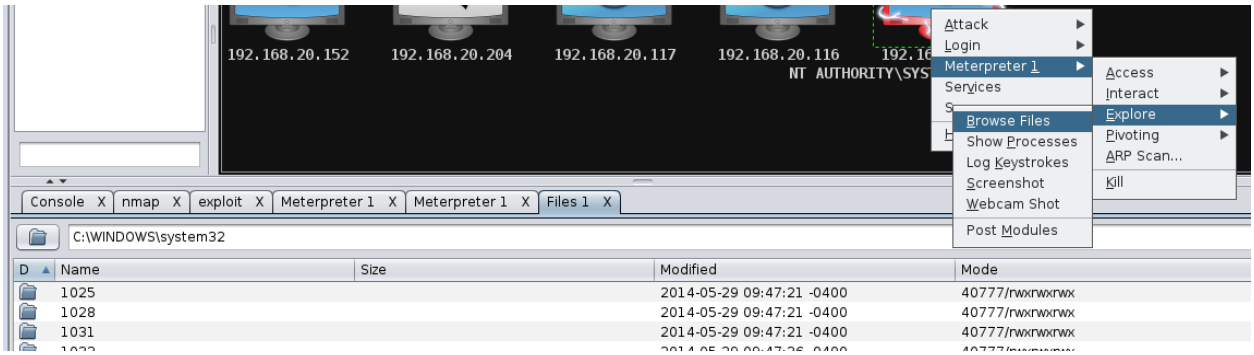


Burada kırmızı çerçeve içerisine alınan kullanıcı bilgileri lazım olabilir, çünkü daha kurumsal ve genel bir kullanıcıya benziyor.

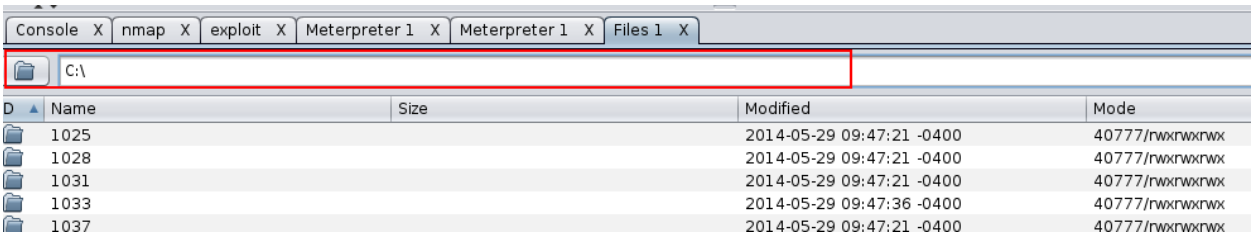
Not: Buradan sonra kullanıcı hesapları üzerinden ilerlemek adına birbirinden farklı yollar mevcut,

1- Şifreleri kırılmaya çalışılabilir
2- Elde edilen bilgiler, tüm ağdaki bilgisayarlara girmek için kullanılabilir.

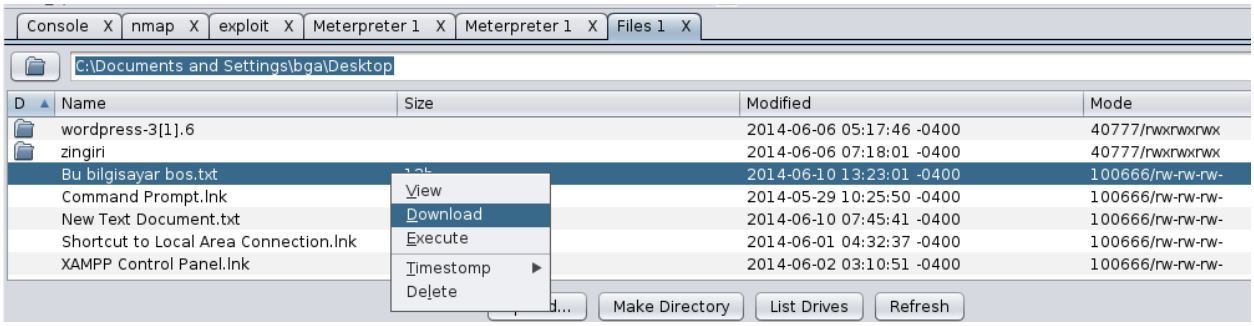
Sızılan bilgisayarda bulunan dosyalar incelenmeye başlanır.
Bunun için izlenilecek yol
Hedefe sağ tık -> Meterpreter 1->Explore -> Browse Files
Sonrasındaki ekran çıktısı ile birlikteki alıntı.



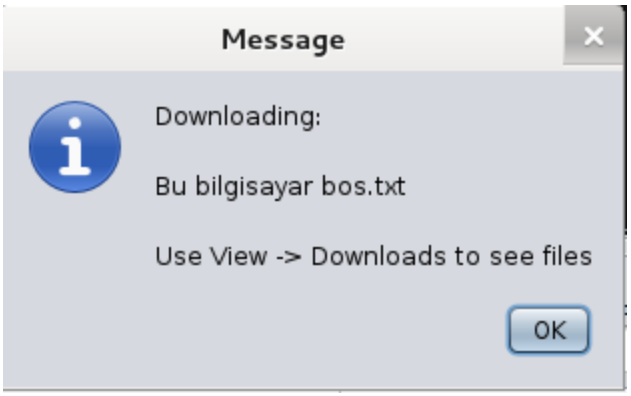
Kullanıcının masaüstüne gidilir (genelde sisteme ait yapılandırma dosyaları masaüstünde tutulur)
Önce adres çubuğundan C:\ gidilir. (C:\ yazdıktan sonra Enter tuşuna basalım)



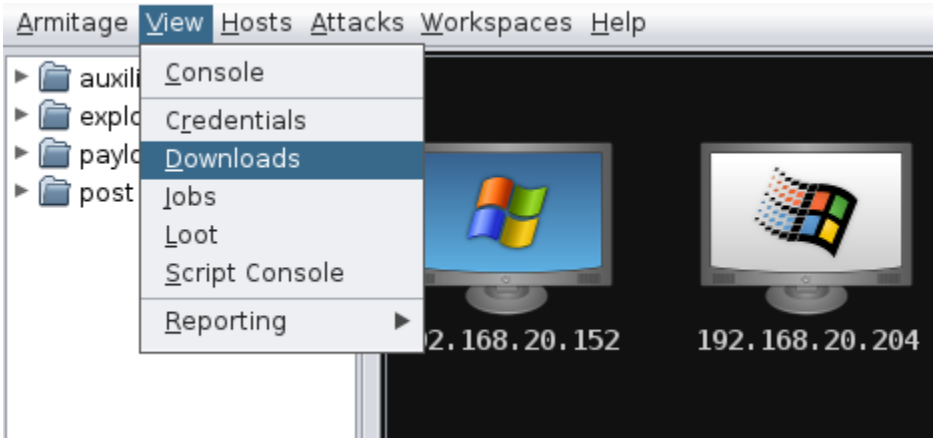
Daha sonra “C:\Documents and Settings\bga\Desktop” dizinine geçilir.
İlgi çeken bir dosya olursa sağ tıklanıp indirilir.



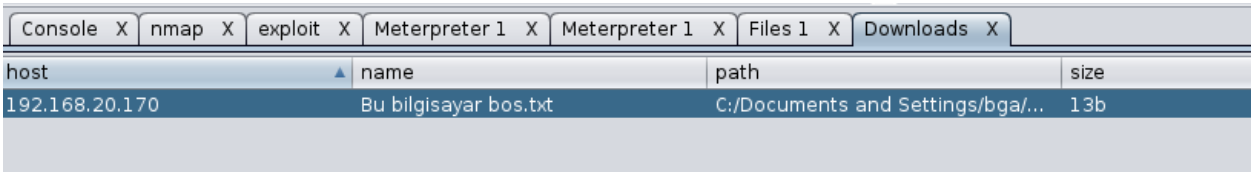
İndirme tamamlandığındaki ekran alıntısı

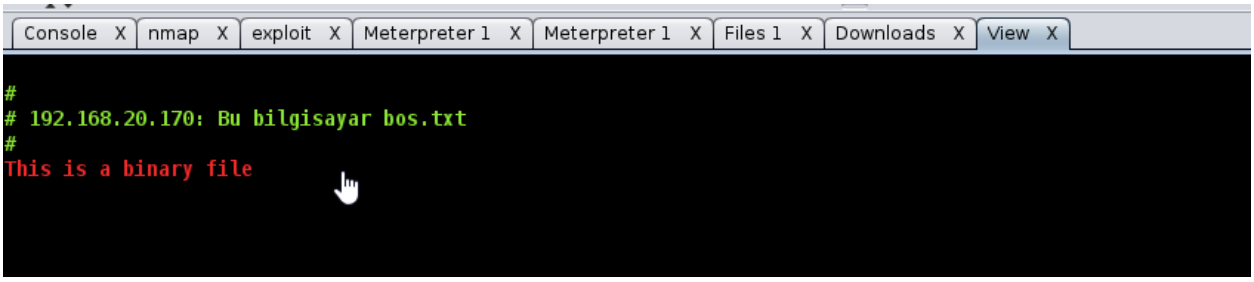


İndirilenlere ulaşmak için;



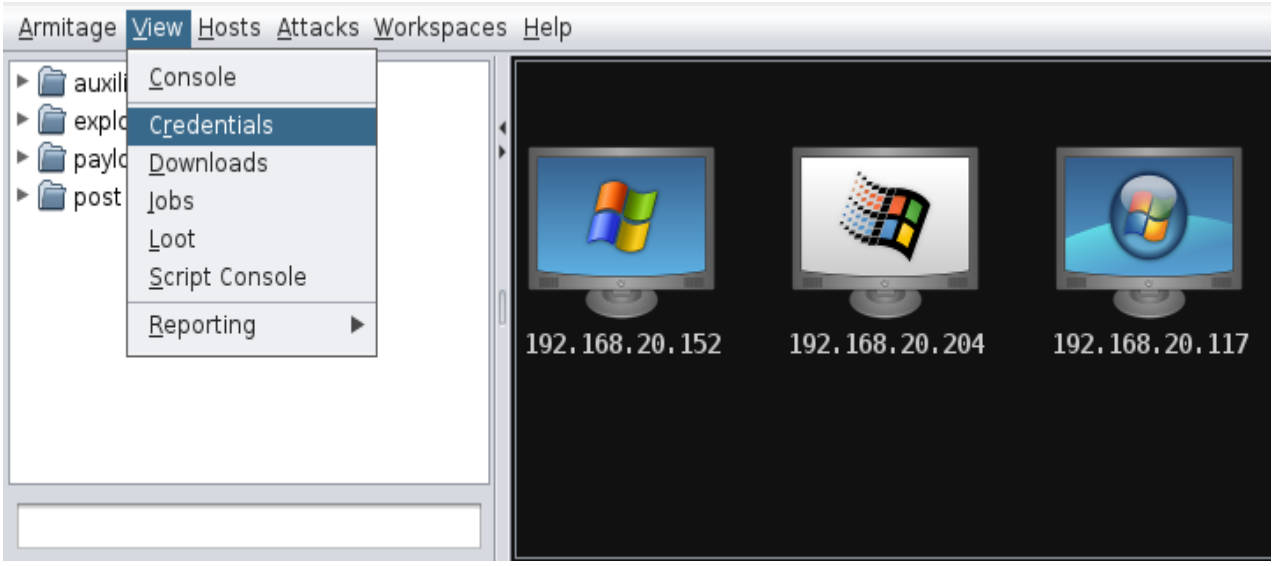
Dosyayı okumak için dosyayı çift tıklamak yeterli.



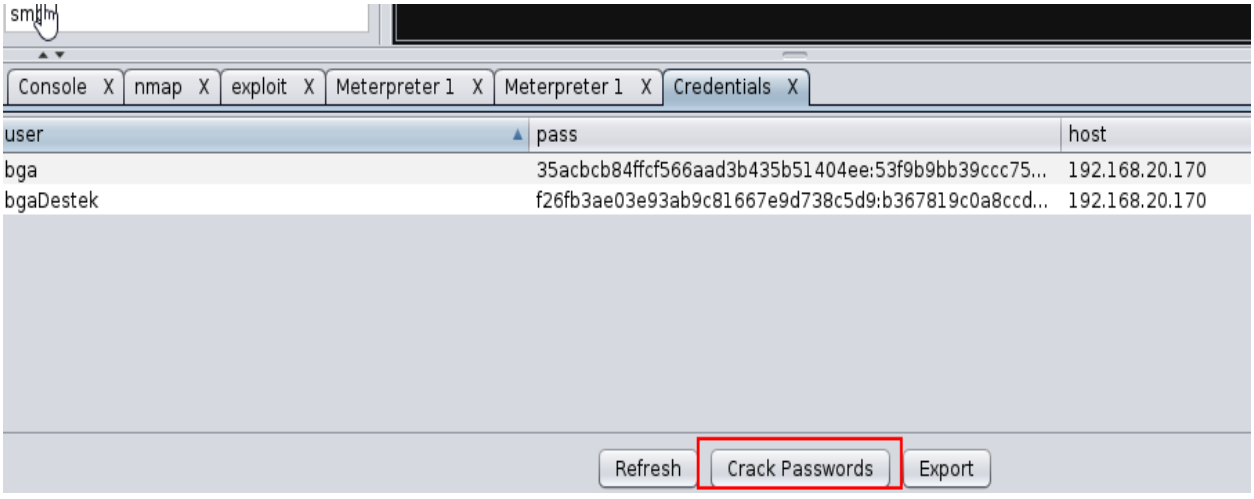


Evet, dosya gerçekten boşmuş ☺.

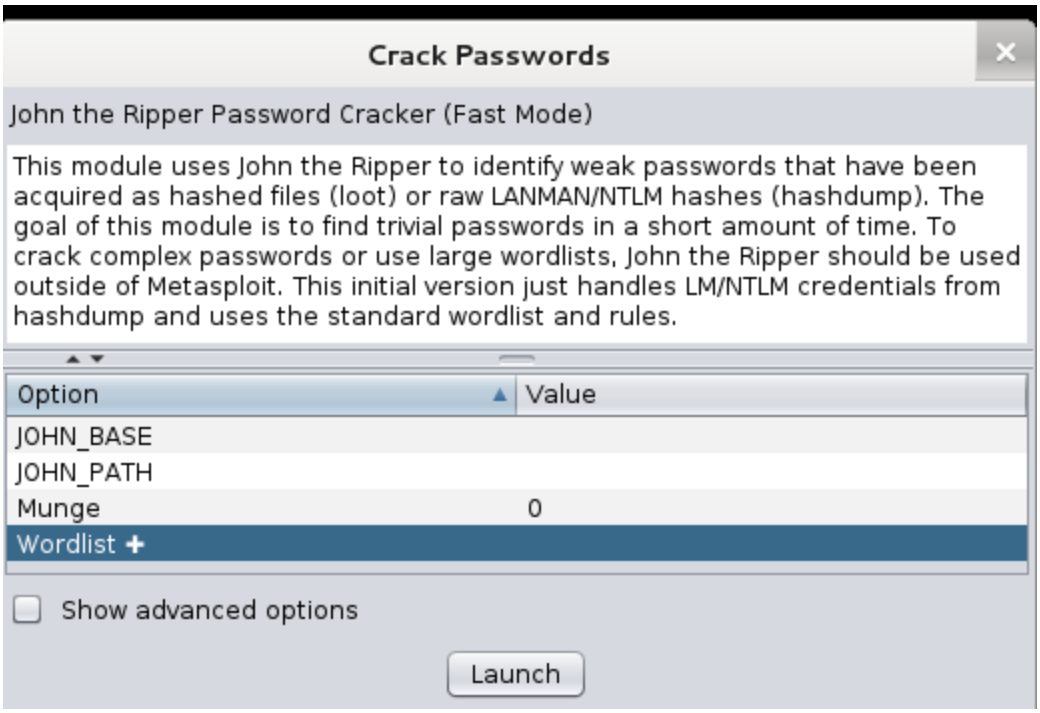
8- Maalesef bu bilgisayardan kullanıcı hesap özetlerinden başka bir şey çıkmadı. Şifreler kırılmaya çalışılır. Toplanılan kullanıcı bilgilerinin özetlerini görüntülemek için,



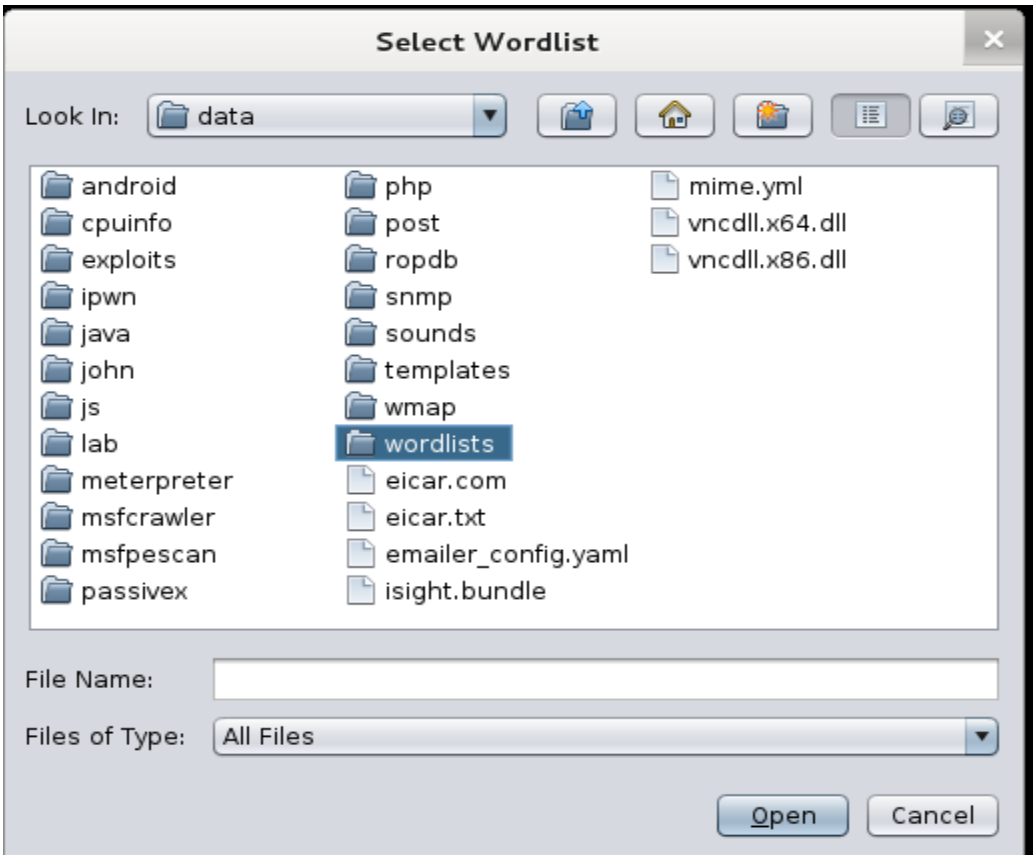
Ekrana dökülen hesaplardan işe yaramayacak hesaplar kaldırılır (Sağ tık -> Delete).
Aksi takdirde kırma işlemi daha da uzun sürecektir. Burada iki hesap bırakılmıştır (bga, bgaDesktek).



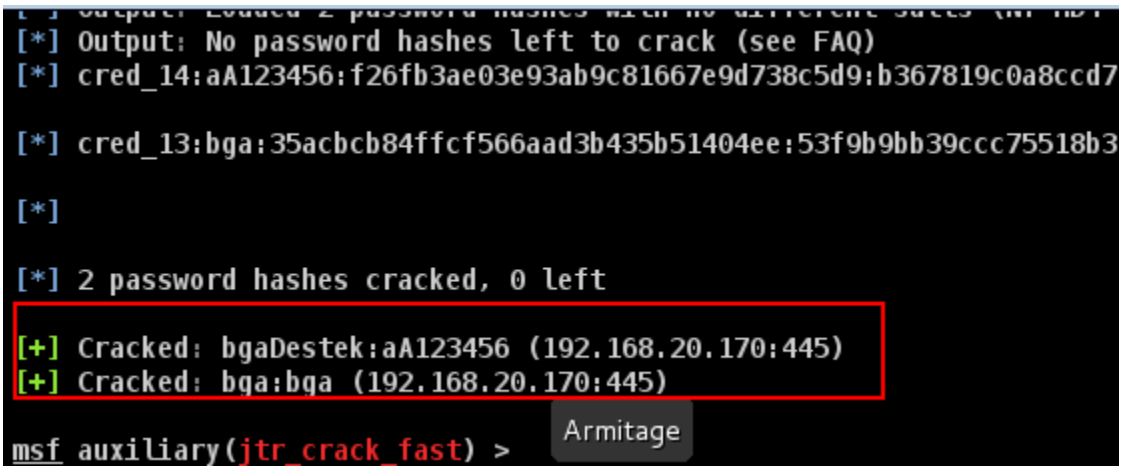
Evet şimdi kırma işlemine başlanabilir, kırma işlemi için bir şifre sözlüğü hedef olarak verilebilir, eğer verilmez ise tüm sözlükler denenecektir. Bu dizin dışındaki başka sözlüklerde kaynak olarak verilebilir.



Wordlist + ifadesine çift tıklanır.
Metasploit programının kendine özel bir wordlist'i bulunmaktatır.



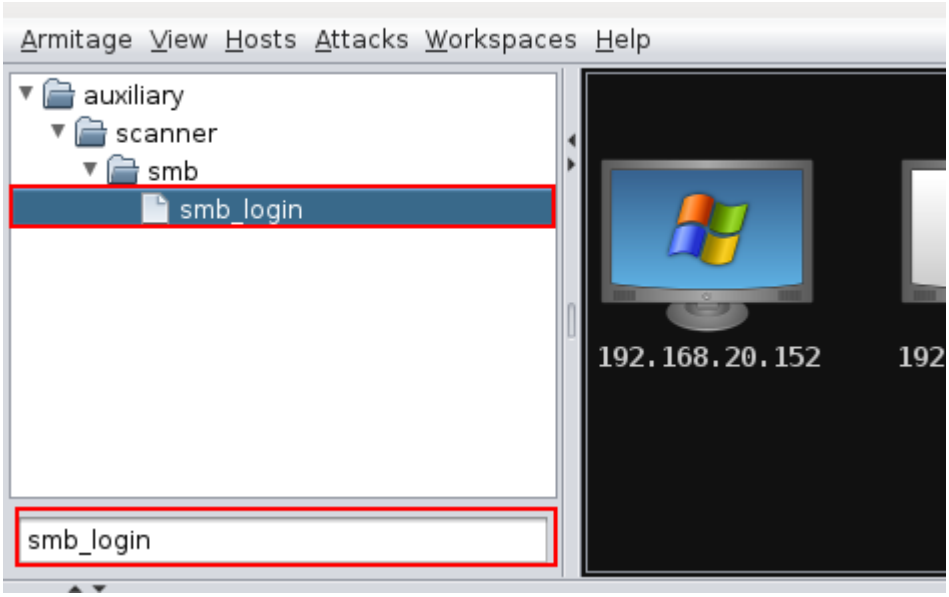
Hangi şifre listesini seçeceğime karar verilemediğinde boş geçilip, modülü çalıştırılabilir.
Başarılı bir şifre kırma işleminden sonra alınmış ekran çıktısı.



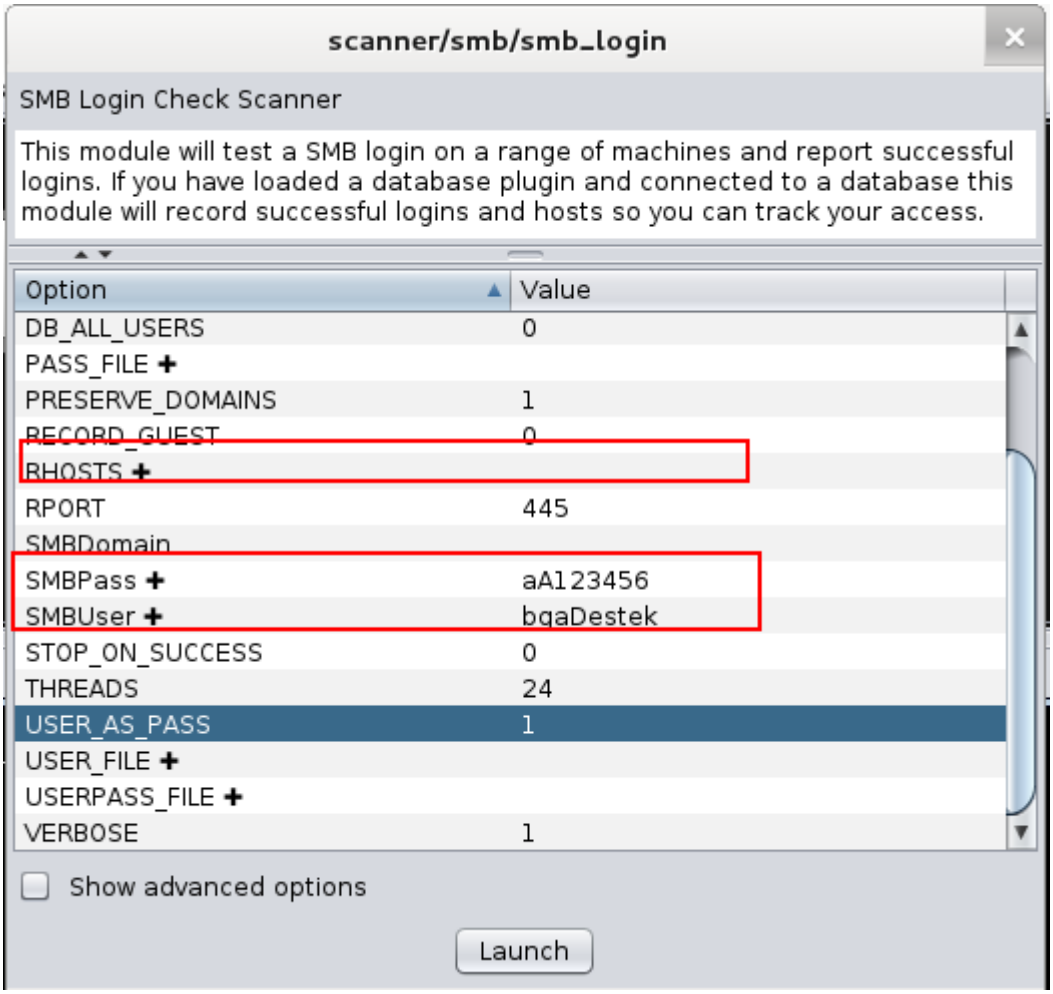
bgaDesktek:aA123456
bga:bga şifreler alınmıştır.

Bundan sonra yapılacak iş bu şifreler ve hesaplar ile tüm ağa **smb_login** çekip, bu kullanıcı ve parolaları başka kimler kullanıyormuş tespit etmek.

9- Modül arama kısmına gelip **smb_login** modülünü bulunur.

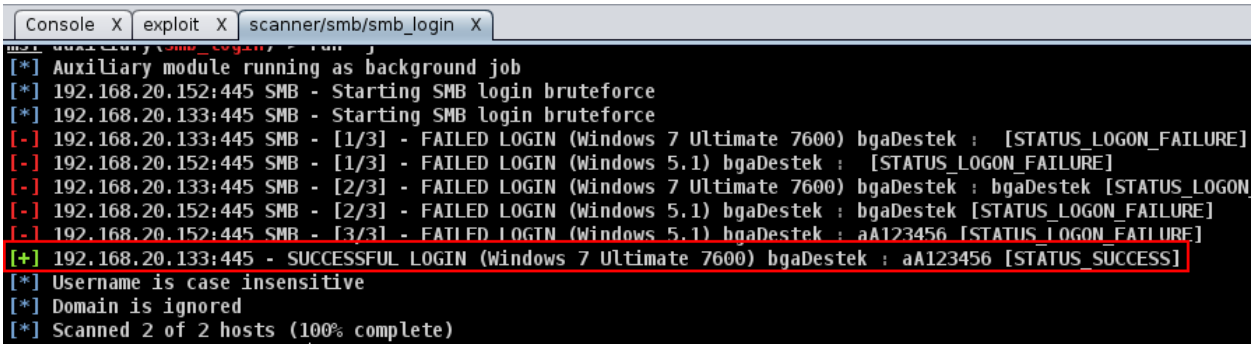


Modüle çift tıklanır, açılacak olan pencere,



Kırmızı çerçeve içerisine alınan değerler atanmak zorundadır. Eğer başka bir kullanıcı listesi denenmek istenirse **USER_FILE**, başka bir şifre dosyası denenmek istenirse **USERPASS_FILE** değerlerine dosya yolunu tanıtmak gerekiyor. Burada kullanıcı adı ve şifreler için dosya verilmeyecektir.

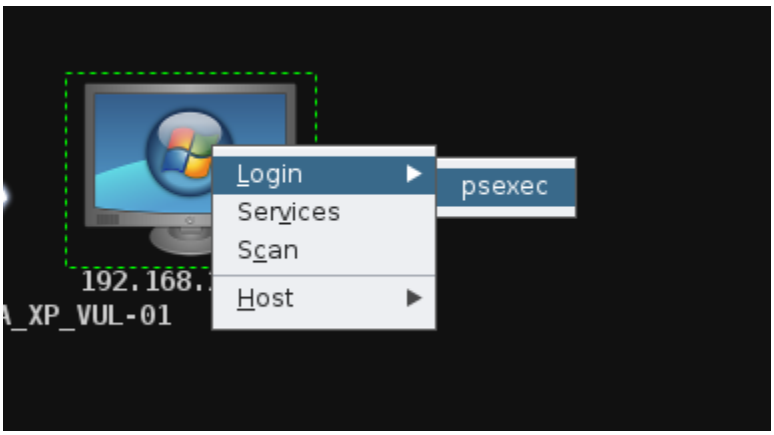
Daha sonra RHOSTS değeri düzenlenir. Taramak için verilecek IP değerleri;
192.168.20.133,192.168.20.152,192.168.20.142,192.168.20.204.
Bu değerleri de girdikten sonra modül çalıştırılır. Sonucun ekran alıntısı,

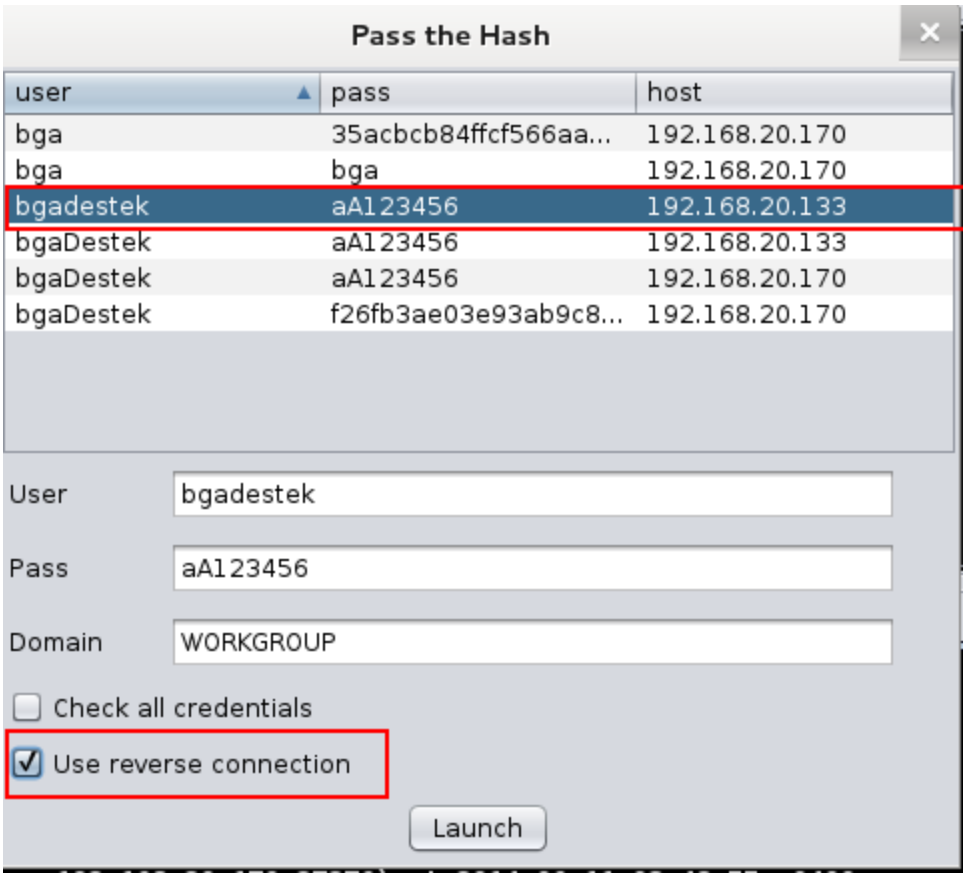


Satır başında **+** işareti olan taramalar olumlu sonuçlandı, yani bu sistemlere giriş yapmak mümkün.

10- Şimdi 192.168.20.133 sistemine metasploit **psexec** oturumu açmayı deneyip, başarılı olunduğunda meterpreter oturumu açılmaya çalışılacak. Hedefe sağ tıklayıp

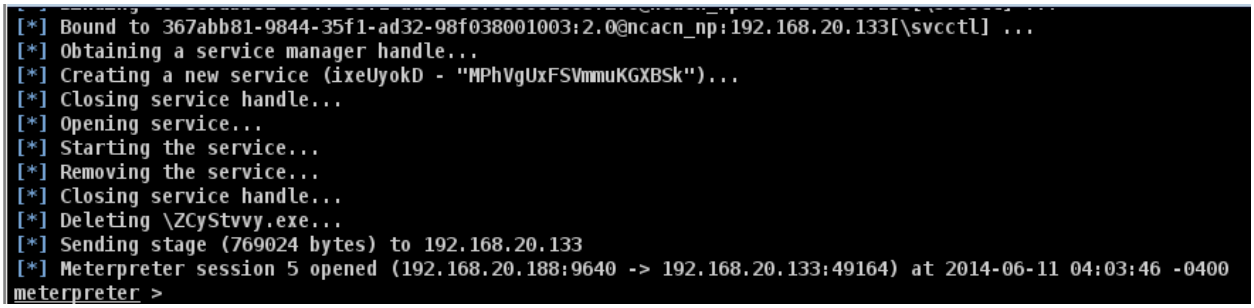
Login -> psexec modülü seçilir.



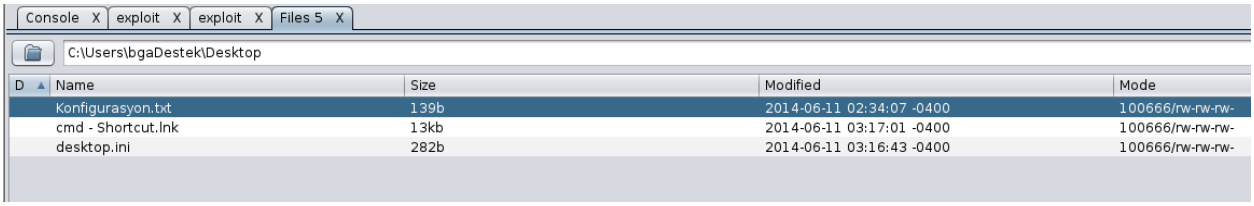


Kırmızı çerçeve içerisine alınan değerlerin seçili olduğuna dikkat edilirmelidir.
Uyarı: "**User everse connection"** seçeneğini tıklanmaz ise payload oluşturulur ve karşıya gönderilir, sizin için çalıştırılır. Fakat, gelen bağlantı isteğini dinleyip yorumlayacak bir modül çalışmadığı için bu istek paketleri düşürülür.

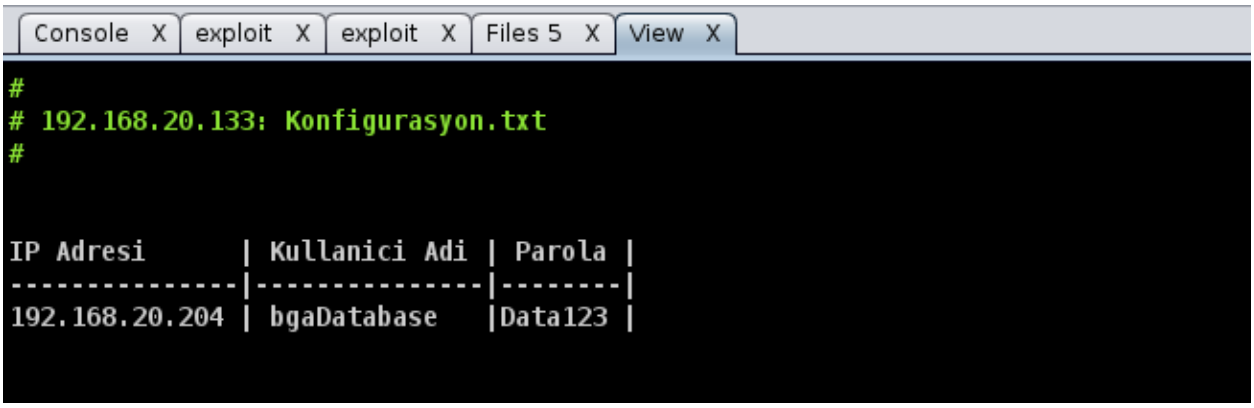
Şimdi modül çalıştırılır.
Girişim başarılı olduğunda modül konsoluna dökülecek bildirim.



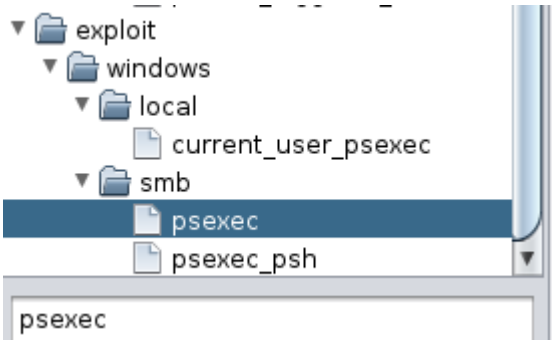
Şimdi sızılan bilgisayar incelenmeye başlanır. Direk olarak masa üstüne gidip dosyalarına bakılabilir.



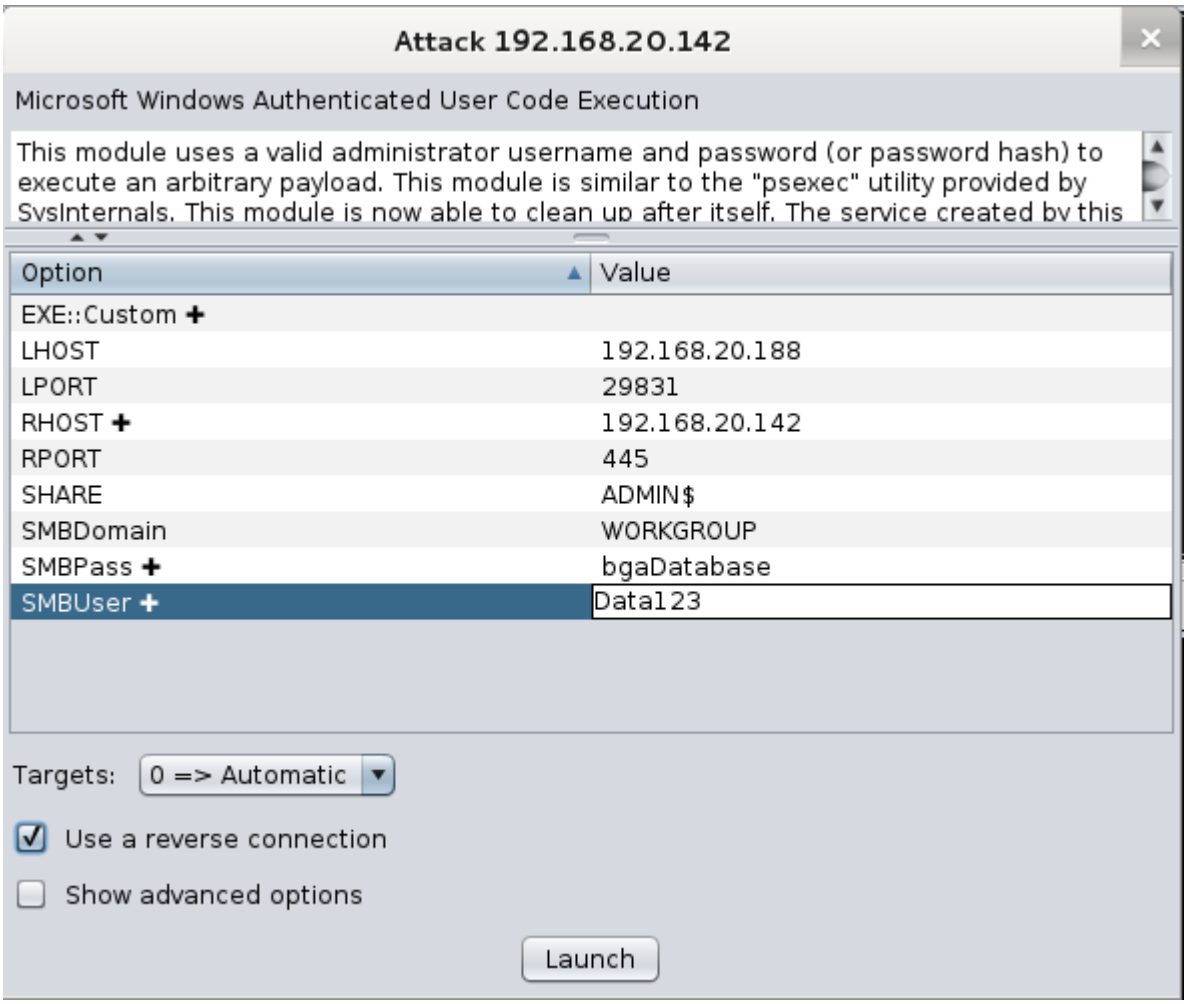
Konfigürasyon dosyası indirilip incelenir.



11-Artık son hamleyi yapmanın zamanı geldi. Eğer veri tabanı yöneticisinin bilgisayarına sızıp veri tabanına erişim bilgilerini elde edilebilirse. Senaryo tamamlanmış olacak.
Hedefe tıklayıp menüden saldırılar aranır.
Daha sonra hedefe sağ tıklayıp,
Login ->psexec seçenekleri takip edilir.
Eğer bu menüde görünmez ise saldırı tipinin **smb** protokolü üzerinden psexec tekniği ile olacağı bilindiğinden, modül arama kısmından **psexec** yazarak aranabilir.

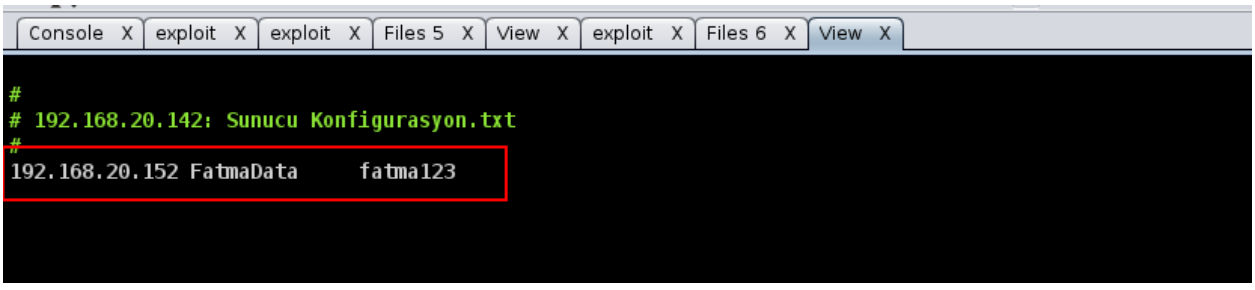


Modüle çift tıklayıp gerekli ayarlamalar yapılır.



Artık modül başlatılabilir. Sisteme meterpreter oturumu açıldığında masaüstüne gidip kayda değer veri olup olmadığı incelenir.

Masaüstünde bulunan sunucu yapılandırma dosyasının içeriği görüntüllendiğinde,



İstenilen veriye ulaşılmış oldu.

Not: Buradaki senaryo basit olarak kurgulanmış, programın yapabilecekleri tanıtılmaya çalışılmıştır. Daha iyi deneyim kazanmak için diğer modüllerde kullanılmalıdır.