ÖN BİLGİ

Bu belge

- https://www.bgasecurity.com/makale/sizma-testlerinde-armitage-kullanimi/

resmi adresindeki veya linkin kırık olması ihtimaline karşın alternatif olarak

- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/S%C4%B1zma%20Testlerinde%20Armitage%20Kullan%C4%B1m%C4%B1.pdf

adresindeki makaleye çalışılarak elde edilen notlarımı kapsamaktadır. Bu çıkarılan notlar belgemde alıntılar ve/veya kişisel ilavelerim mevcuttur.

1)

Armitage metasploit yazılımının yapabileceklerini görsel olarak kontrol edebilme imkanı sağlayan bir yazılımdır.

(Page 3)

2)

Post Exploit
Bir bilgisayara sızıldıktan sonra hedef sistemde başka exploitation'larda bulunmaya post-exploit adı verilir. Örneğin hedef sisteme sızıp sonra hak yükseltmek için hedef sistemde başka bir exploit çalıştırmaya veyahut hedef sisteme sızıp hashdump exploit'i ile hedef sistemin credentials'larını çekmeye post-exploit adı verilir.

(Page 3)

3)

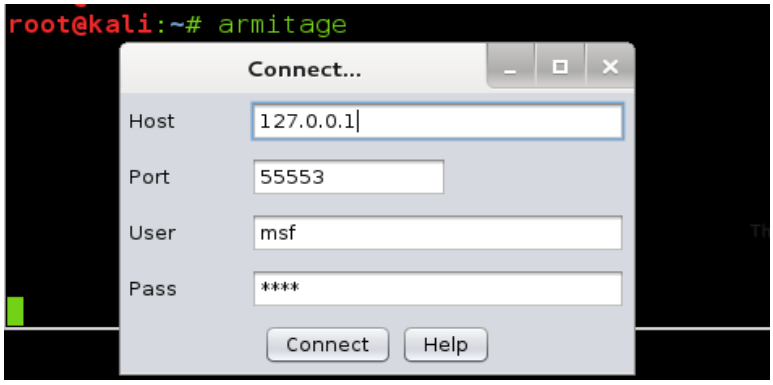
Armitage yazılımı kodlamalara yabancı olanlar için ve pentest çalışmalarına yeni başlayanlar için tavsiye edilen bir yazılımdır. Açık kaynak kodlu bir yazılımdır. Açık kaynak yazılımların üzerinde yapılan değişiklikler sonucu ücretli hale getirilen bir çok yazılım gibi Armitage yazılımının da ücretli hali olan Cobalt Strike bulunmaktadır.

(Page 3)

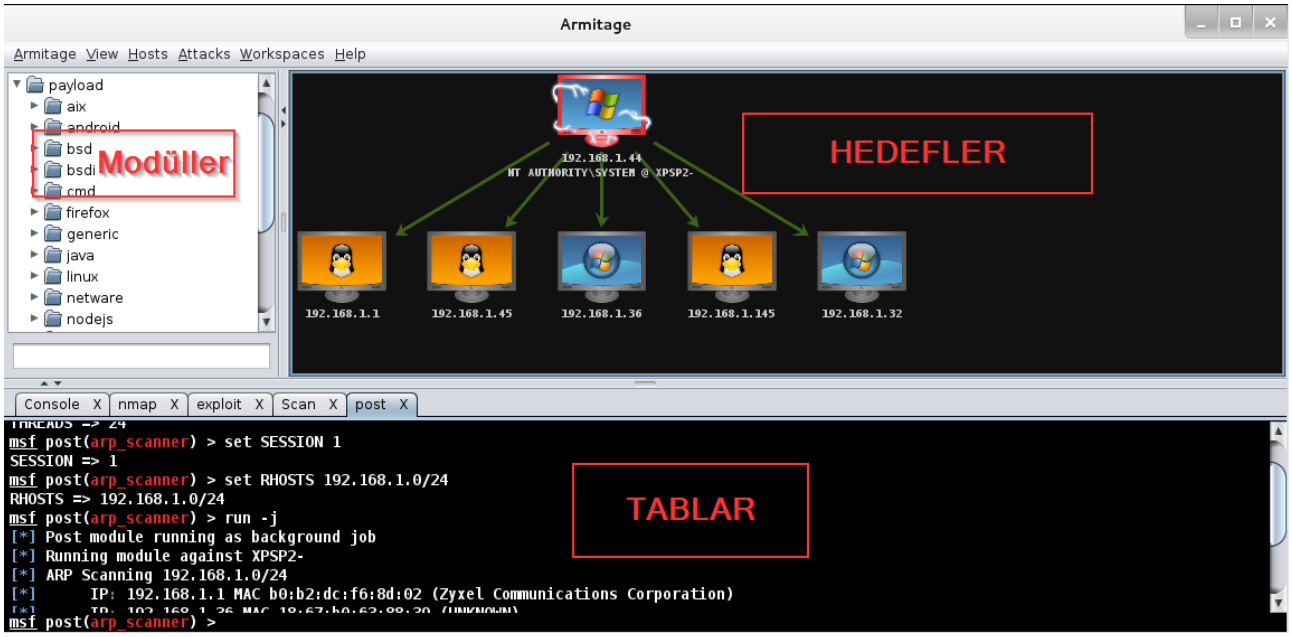
4)

Kali'de Armitage Kullanımı

> service postgresql start
> service metasploit start
> armitage



Açılan popup'daki Connect düğmesine ardından Yes düğmesine basılmasıyla armitage başlatılır.



(Page 6-9)

5)

Modüller Kısmı
Exploit'lerin, payload'ların, auxiliary'lerin sıralandığı kısımdır.

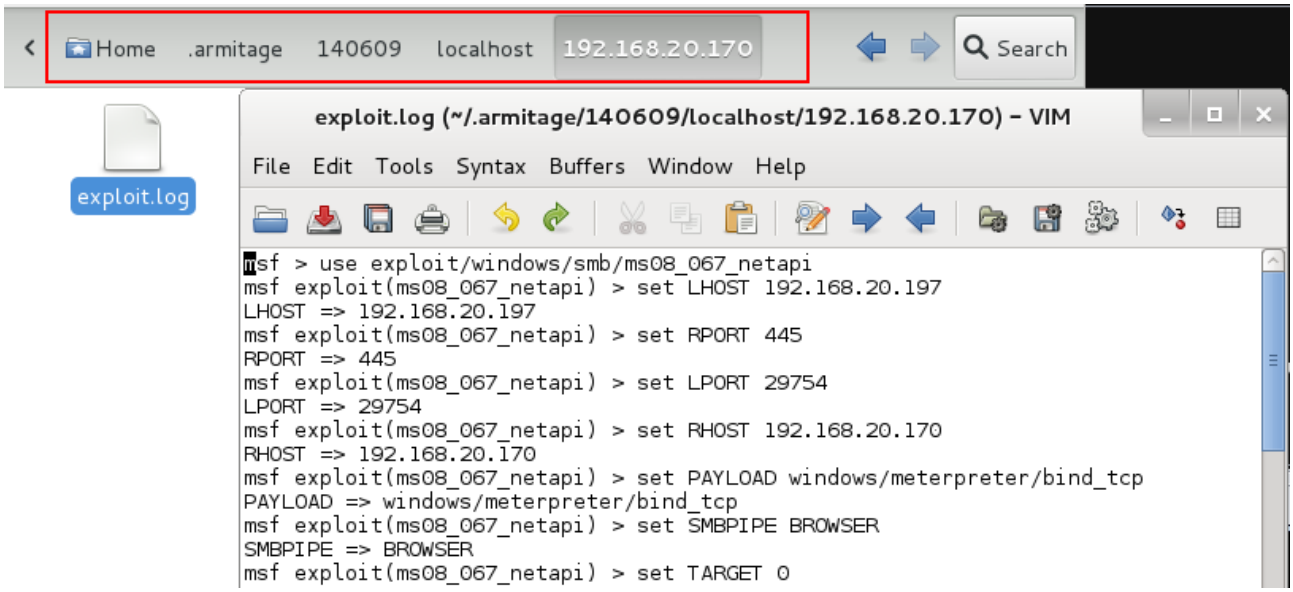
Hedefler Kısmı
Bu panel çeşitli tarama teknikleri ile ya da manuel olarak seçilen hedefleri listeler.

Tablar (Sekmeler) Bölümü
Armitage programı hedeflerle ilgili tüm işlemleri ayrı ayrı sekmeler halinde tutar. Yani örneğin hedef sistemlerde açılan reverse shell oturumları için, sistemleri elde etmede kullanılan modüller için ve bunun gibi her bir eylem için ayrı bir sekme yer alır.

(Page 9-10)

6)

Logging İşlemleri
Armitage ile yapılan testler esnasında yapılan tüm işlemlerin bir kaydının tutulması mühimdir. Armitage herbir ip adresi için bir klasör oluşturarak ilgili kayıtları bu klasör içerisindeki log uzantılı dosyalarda tutar. Bu kayıtlara ulaşmak için Armitage arayüzündeki View->Reporting->Activity Logs menülerine tıklanılması gerekir. Aşağıda örnek bir log dosyası görmektesiniz.



Yukarıda /home/armitage/140609/localhost/192.168.20.170 dizinindeki exploit.log dosyasının içeriğini görmektesiniz. Bu dosyanın içeriğinde görebileceğiniz üzere Metasploit Framework konsoluna girilen kodlamaların dökümü ve çıktıları yer almaktadır.

(Page 10-11)

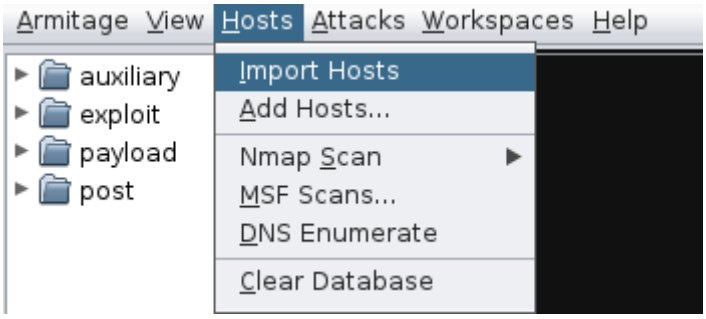
7)

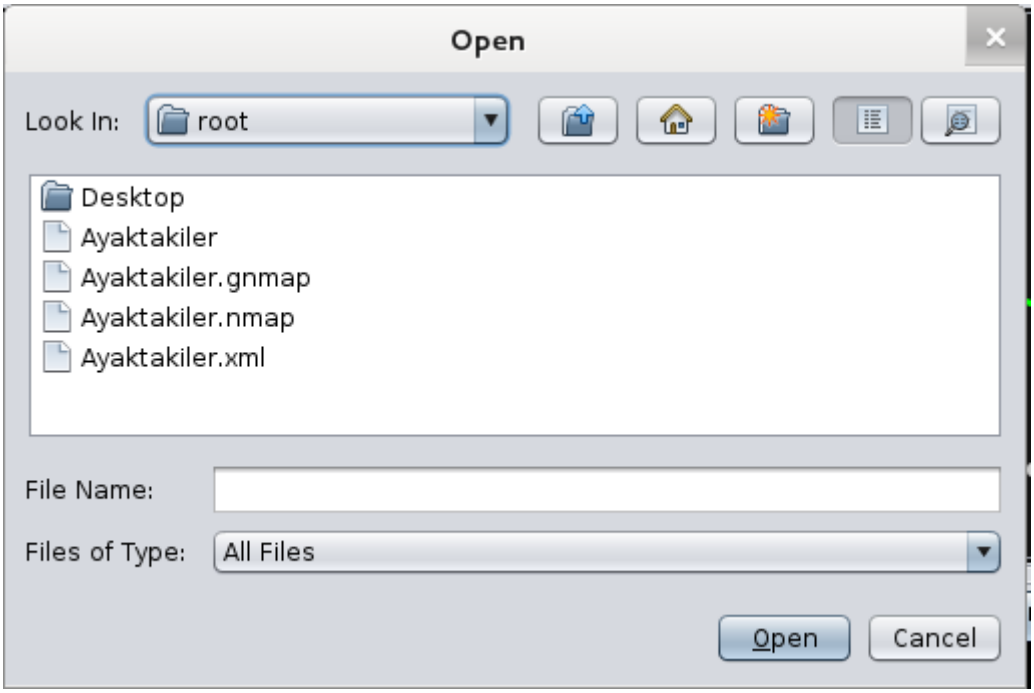
Hedef Tayin Etme
Armitage çalışma alanına hedef eklenmek istendiğinde bu işlem iki şekilde gerçekleştirilebilir:

i) Birinci yöntem

Hosts -> Import Hosts

seçeneklerine gidilmesi ve host IP'lerinin satır satır sıralı olduğu dosyanın seçilmesidir.

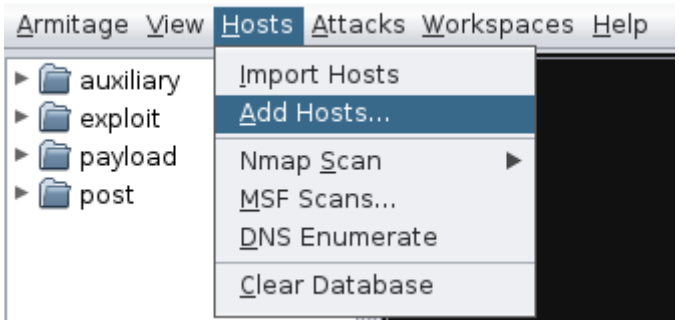


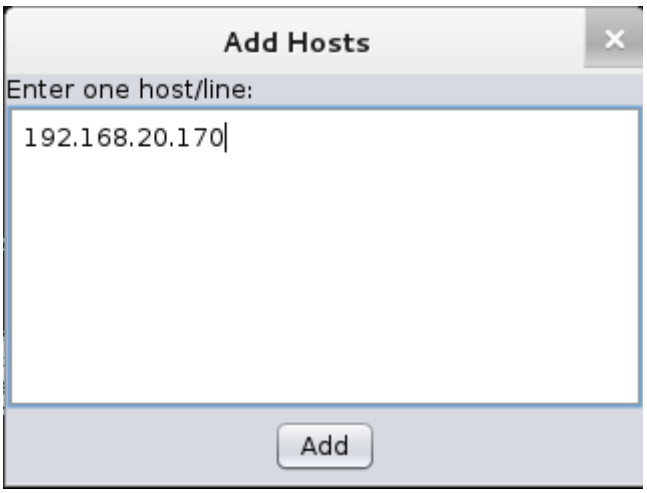


ii) İkinci yöntem

Hosts -> Add Hosts

seçeneklerine gidilmesi ve hedef IP'lerin satır satır elle girilmesidir.

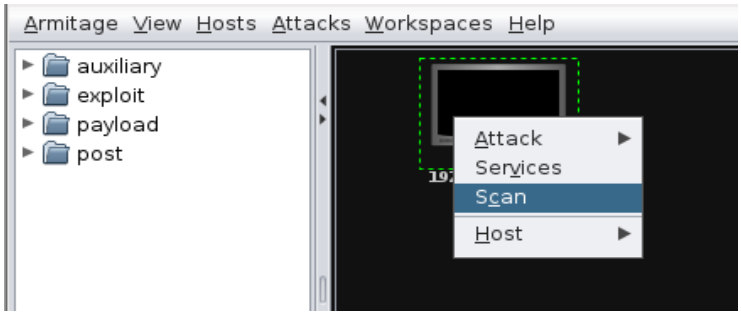


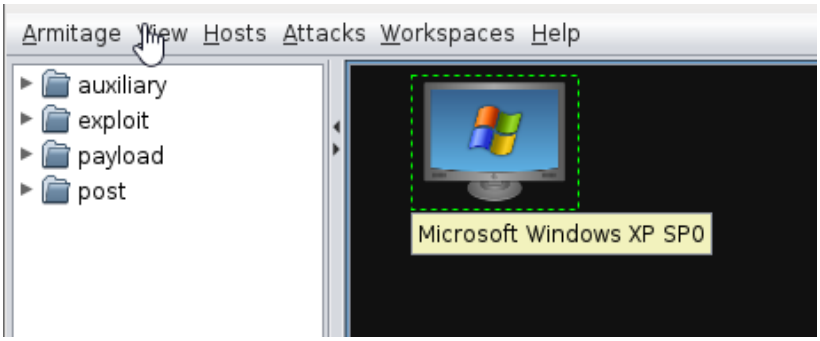


(Page 11-13)

8)

Armitage ile Saldırma Adımları
Host'lar Armitage çalışma alanına eklenildikten sonra hedefin ikonunun üzerine sağ tıklayıp Scan diyerek hedef işletim sistemi ve versiyonunu öğrenelim.

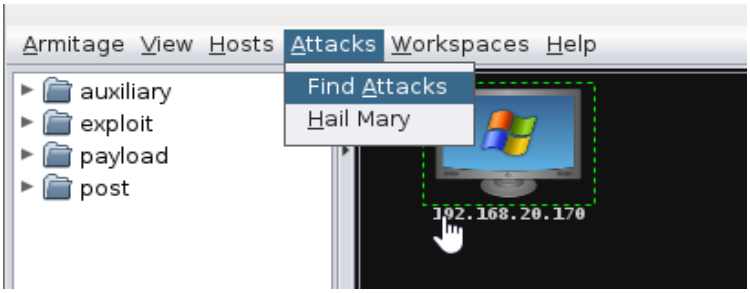


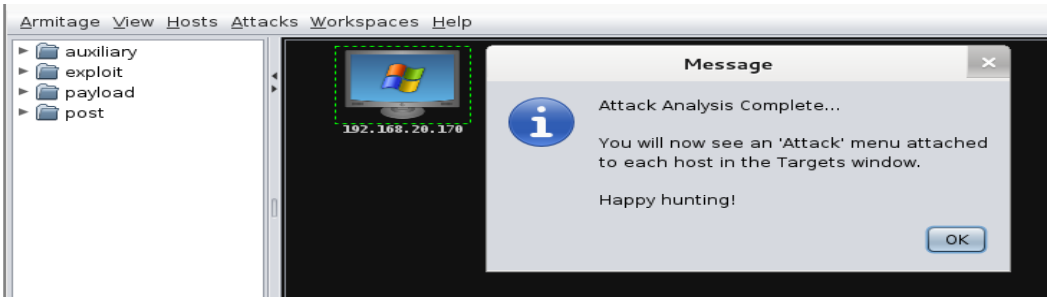


Hedefin işletim sistemi ve versiyonu tespit edildikten sonra ilgili açıklıkları bulmak için

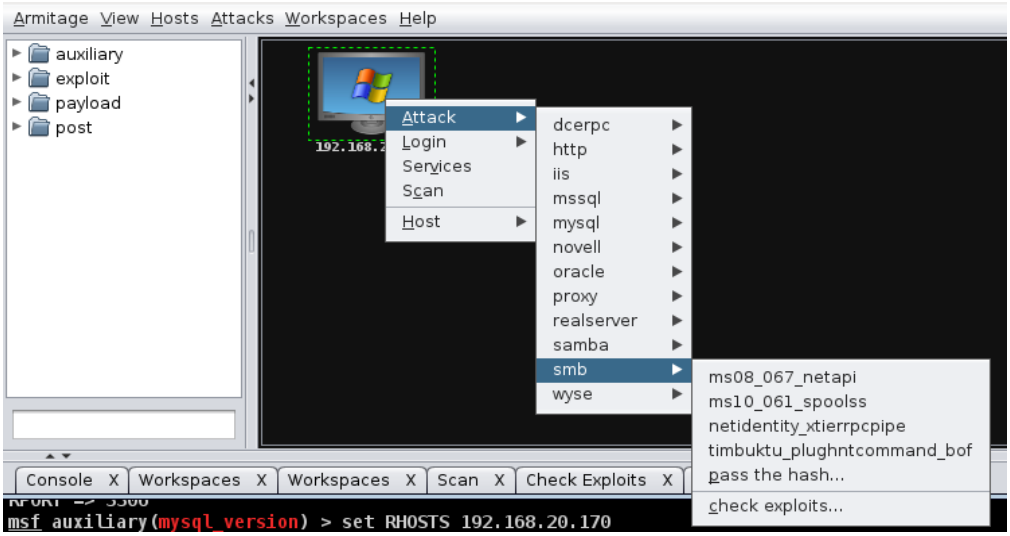
Attacks -> FindAttacks

sekmesine tıklayalım.

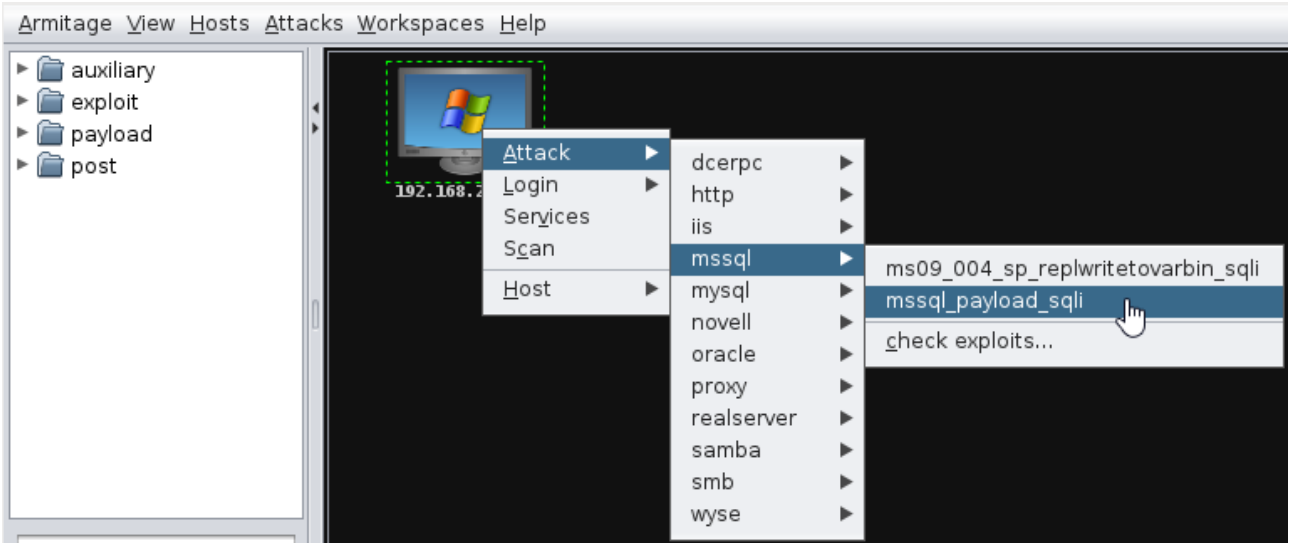


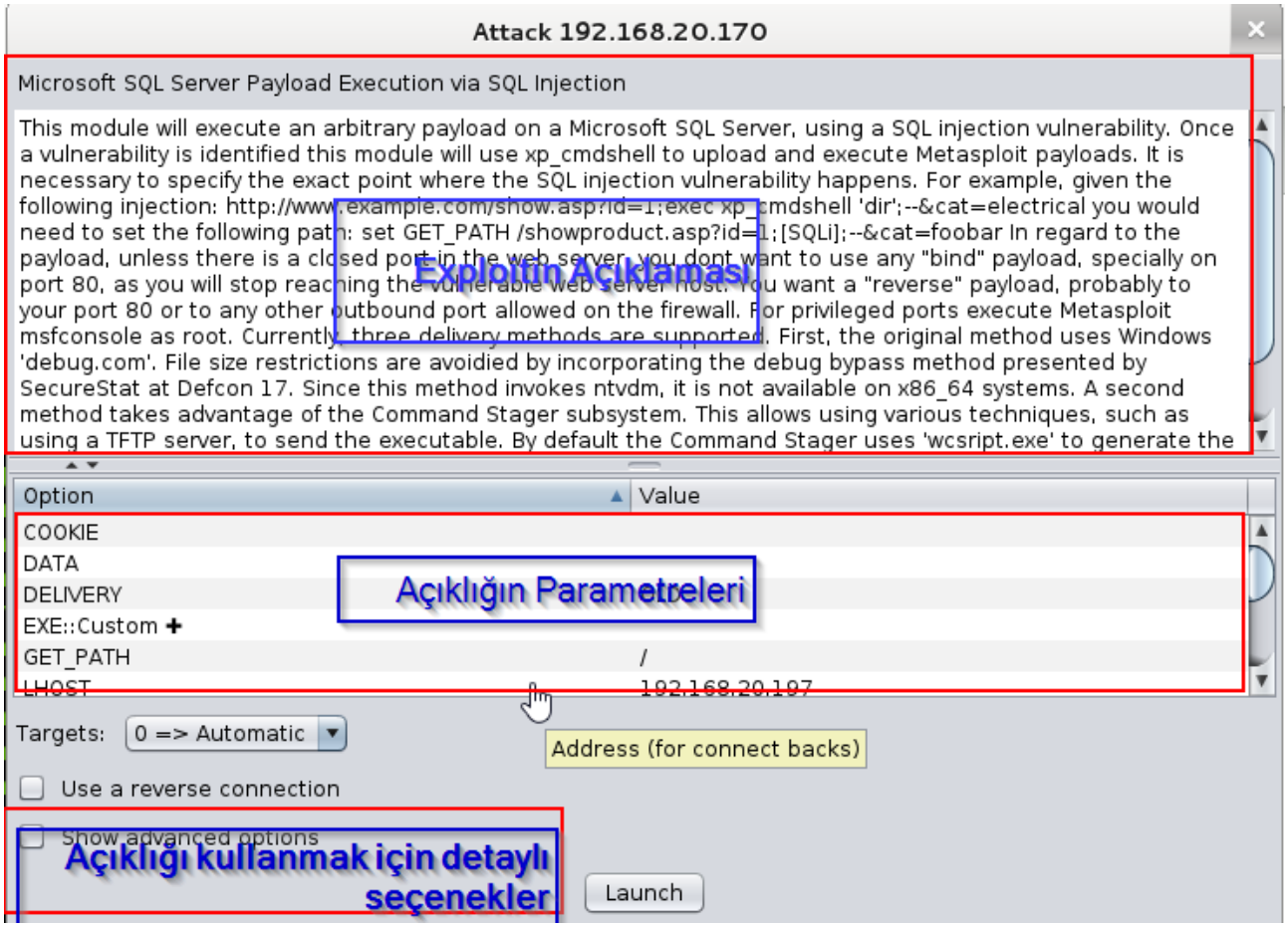


Ardından ilgili açıklıkları görüntüleyebilmek için hedefin ekrandaki simgesine sağ tıklayıp Attack seçeneğine tıklayalım.

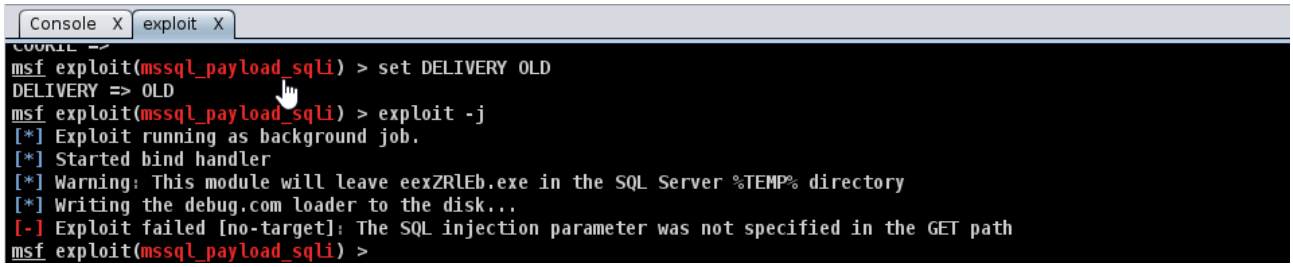


Önerilen açıklıklardan bir tanesi tıklanarak kullanılmaya başlanabilir. Öncelikle başarısız bir exploit çıktısını görmek için başarısız olunacak bir exploit'i seçelim.

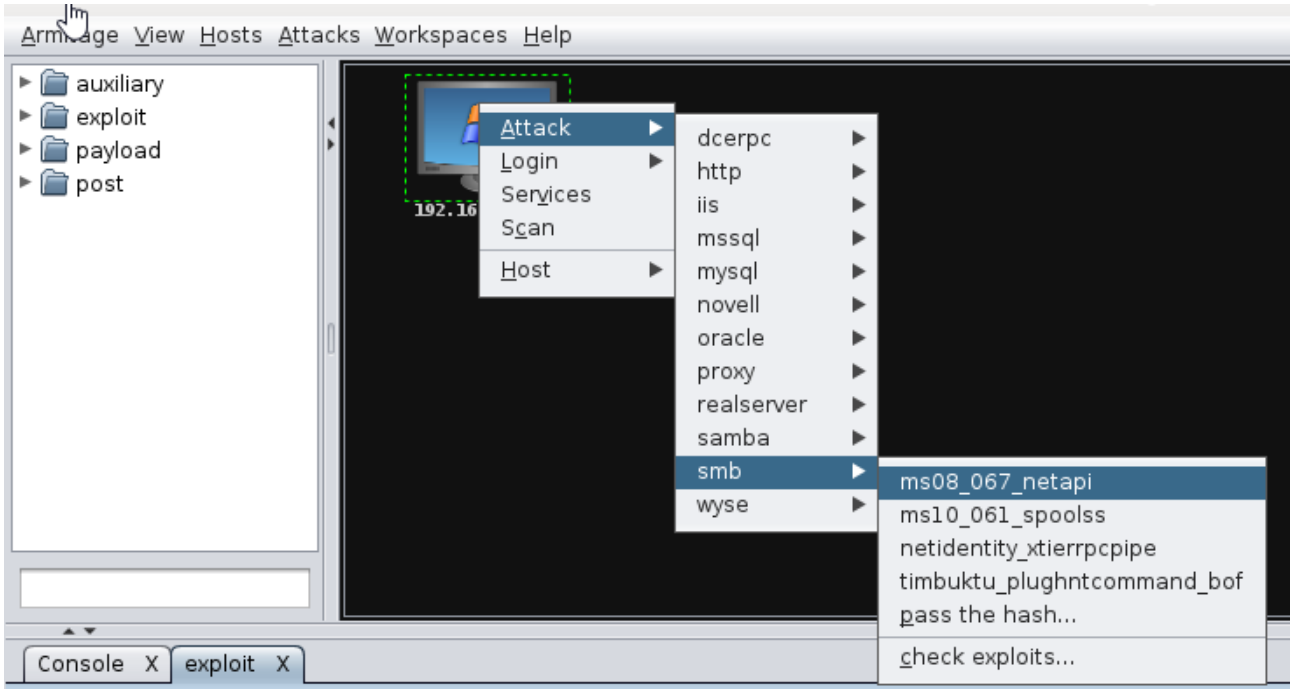


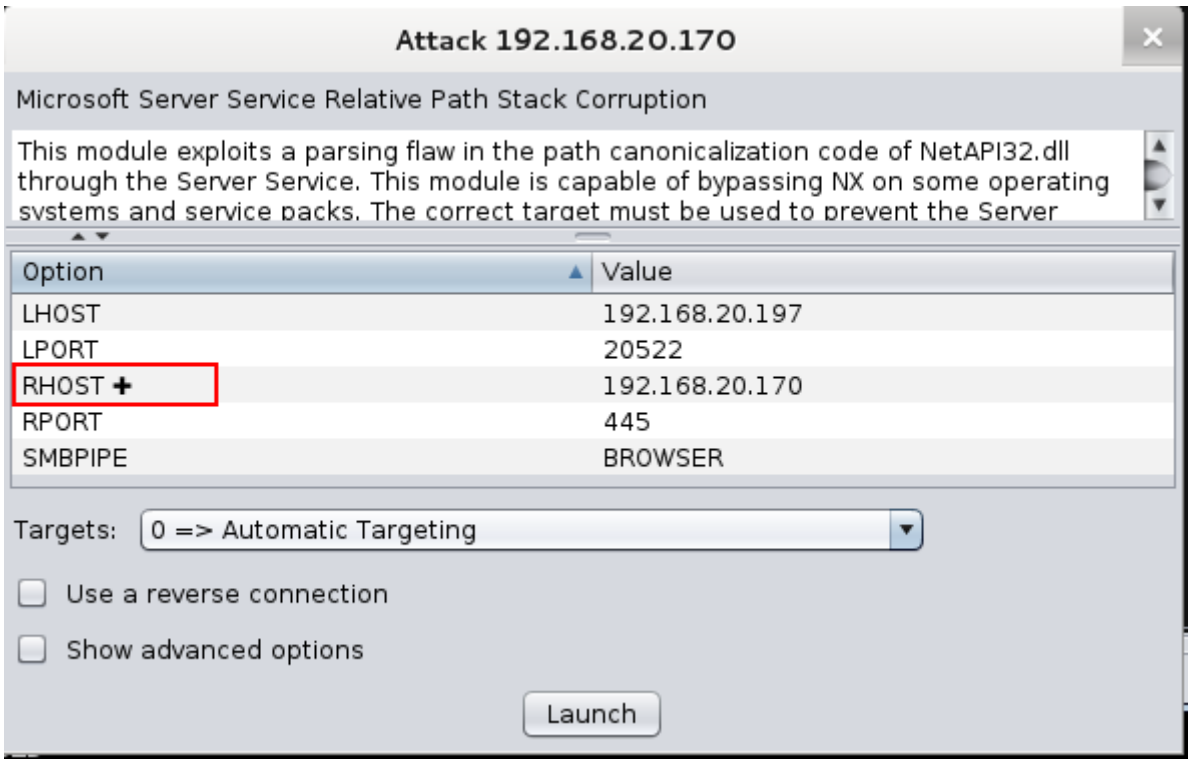


Açıklığın parametrelerini doldurduğumuzu varsayalım ve Launch ile exploit işlemini tetikleyelim. Daha önceden de belirtildiği gibi her exploit teşebbüsü için yeni bir tab (sekme) açılır ve hedef ile iletişim bu tab'ın konsolu üzerinden devam eder.

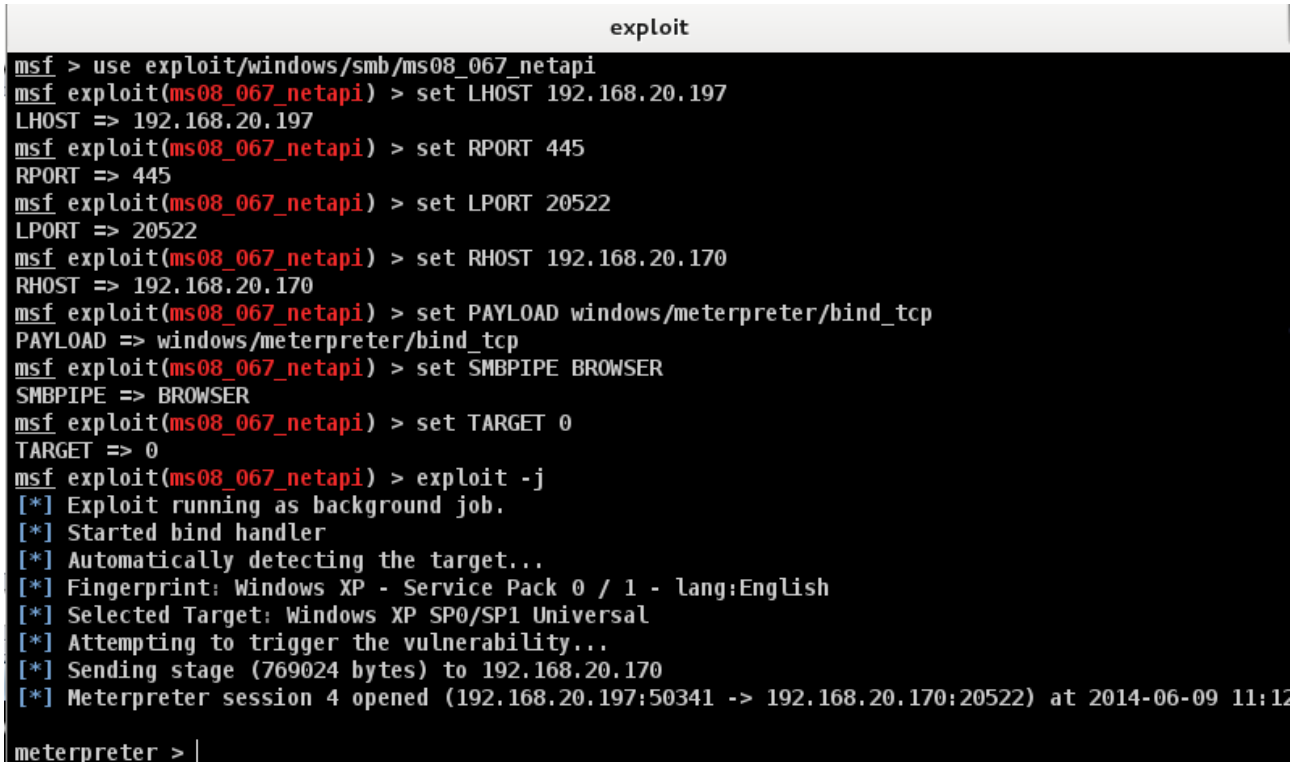


Tab'ın sunduğu konsol ekranından da görülebileceği gibi exploit girişimi başarısız olmuştur. Şimdi işe yarayacak bir exploit seçelim.





Açıklıkların parametrelerine dikkat edilmelidir. Resimde görüldüğü üzere bazı değerlerin yanında + işareti var, bunun manası o değerin boş olamayacağıdır. Launch'a basıldığı takdirde ilgili TAB'a aşağıdakiler yansıyacaktır:



Böylece hedef sistemde meterpreter oturumu açılmış olacaktır.

(Page 15-22)

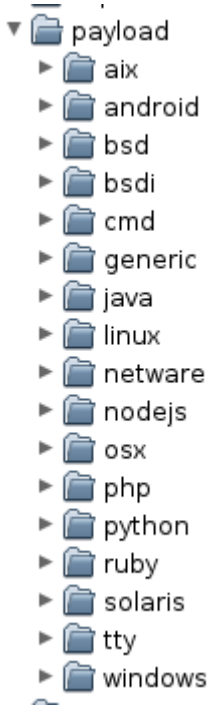
9)

Her hedef kolayca ve uzaktan sömürülecek kadar zafiyet içermeyebilir. Yayımlanan güncellemeleri zamanında uygulayan bir hedef artık kolay bir hedef değildir. Antivirüs 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.

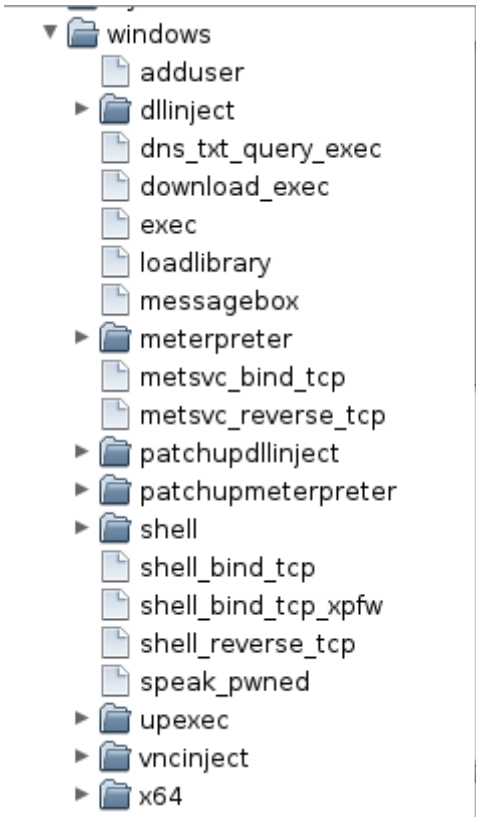
Hedefle saldırgan arasında iletişim kurması amacı ile birçok dosya tipi oluşturulabilir. Bunlardan bazıları;

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

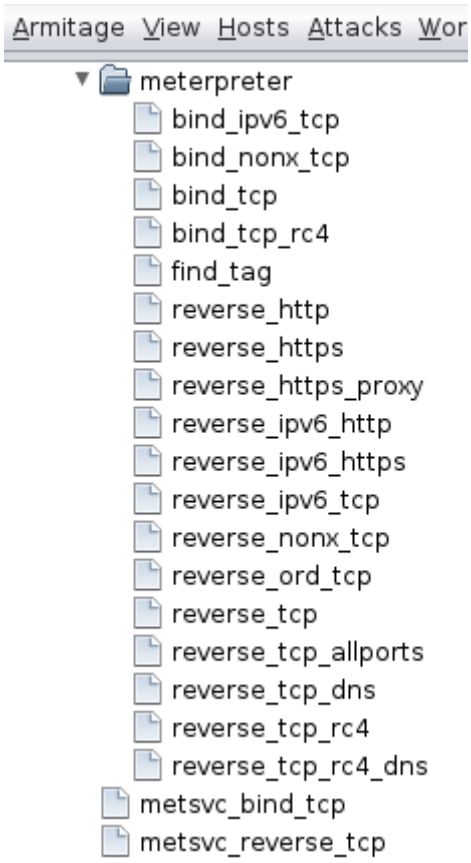
Görüldüğü gibi saldırı amaçlı kullanılabilecek birçok dosya türü mevcut. Bu dosya türlerini kullanarak payload oluşturulabilir. Metasploit programının zengin bir payload kütüphanesi bulunmakta. Armitage Metasploit programının görsel hali olduğu için aynı kütüphaneye görsel bir şekilde ulaşılabilir. Armitage içerisinde bulunan payload kategorileri şunlardır:



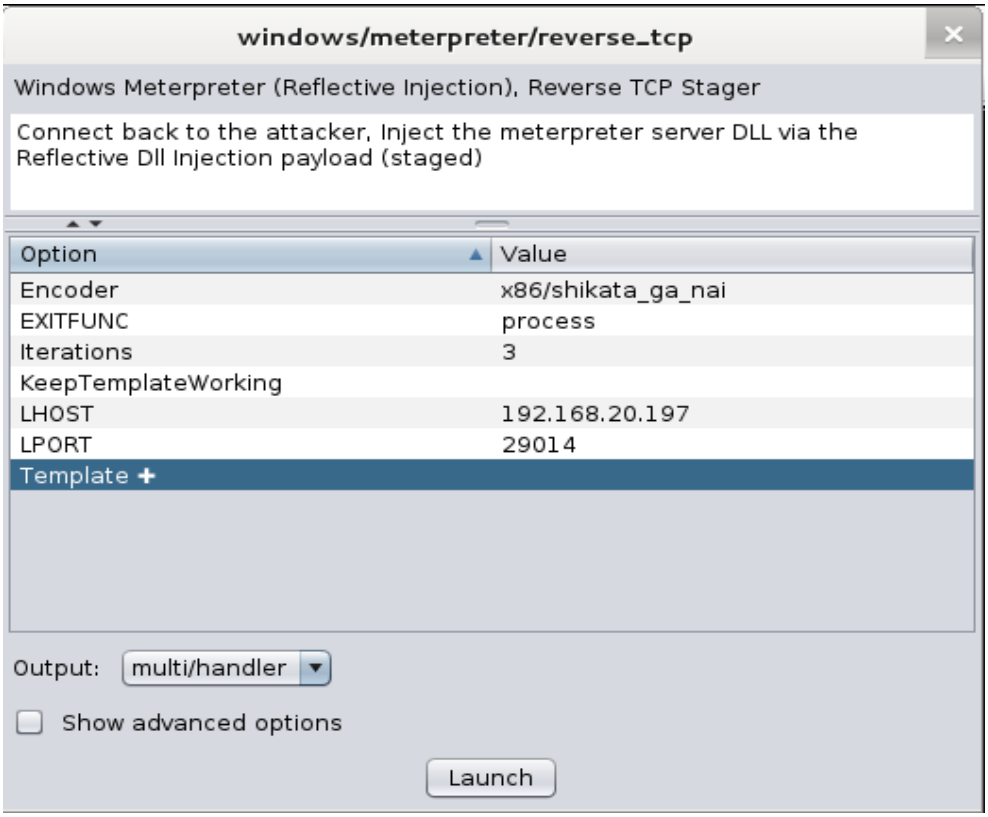
Görüldüğü gibi birçok platform için hazırlanmış payload bulunmaktadır. Windows klasörünü genişletelim ve çeşitleri görelim.



Resimde sıralı payload'lardan meterpreter'e odaklanalım:



Meterpreter çeşitleri arasında “reverse_tcp”, “reverse_http” ve “reverse_https” en popüler olanlarıdır. Bu belgede reverse_tcp ele alınacaktır. reverse_tcp yi seçelim. Bu takdirde ekrana aşağıdaki pencere yansır:



Ekranda gözüken parametreler ve anlamları şunlardır:

Encoder
: Derlenecek olan programın derlenme şeklini belirler.

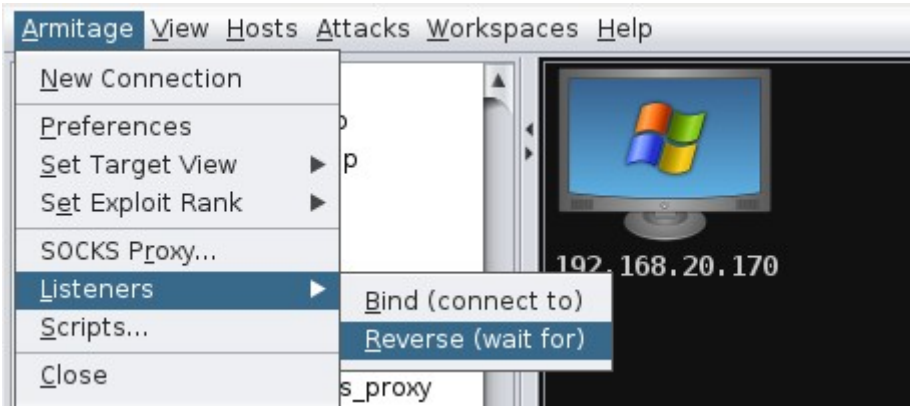
LHOST
: Payload çalıştırıldığında kurban uzak bir sisteme bağlantı açmak isteyecektir. LHOST kurbanın bağlanacağı adrestir. Yani saldırganın adresidir.

LPORT
: Bu değer kurbanın saldırgana hangi port üzerinden bağlanacağını belirler. Yani kurbanın bilgisayarındaki çıkış portunu değil, saldırganın makinasına giriş portunu belirler.

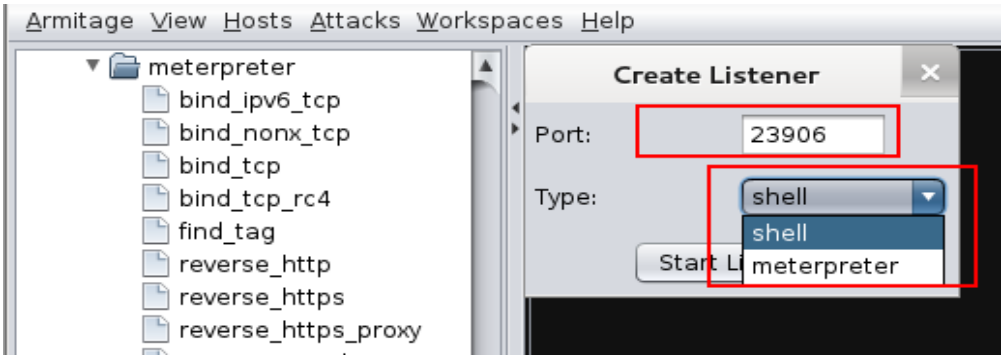
Output
: Payload çıktısının ismini belirlemek için kullanılır.

Template
: Anti virüs programlarını atlatmak için kullanılan bir opsiyondur.

Oluşturulan zararlı belge (payload) kurbana gönderildikten sonra kurbandan gelecek isteğin ıskalanmadan değerlendirilebilmesi için payload handler kullanmak gerekir. Bu modulü kullanmak için Armitage -> Listeners -> Reverse (wait for) seçeneklerine tıklanmalı,



ekrana gelecek olan popup penceresindeki dinlenilecek port numarasına gönderilen payload'un geleceği port numarası yazılmalıdır. Tip olarak da dinlenilecek payload'un tipi seçilir.



(Page 22-27)

10)

Post Exploitation
Varsayalım ki hedef sisteme bir exploit ile giriş yapılabildi. Bu işlemden sonra yapılabilecek şeyler şunlardır:

Hak Yükseltme

Neyin açıklığı kullanılarak sisteme sızılmış ise o servisin ya da o kullanıcının hakları kadar şey uzak sistemde yapılabilir. Hedef işletim sistemindeki veri yazma ya da veri okuma katmanına gelindiğinde kullandığımız servis ya da kullanıcının yetkisine dair bir token istenir. Bu token ötelere gidebilmek için bir tür vize gibidir. Başkasının pasaportunu kullanarak vize kontrolünden geçmeye ise hak yükseltme denir.

Dosya Görüntüleme

Hedefi temsilen gösterilen arayüzdeki monitöre sağ tıklanır ve Meterpreter N -> Explore -> Browse Files sekmelerine tıklanır. Yetki ölçüsünde dosyalar görüntülenebilecektir.

Screenshot ve Webcam Görüntüsü Alma

Hedefi temsilen gösterilen arayüzdeki monitöre sağ tıklanır ve Meterpreter N -> Explore -> Screenshot sekmeleriyle ekran görüntüsü Meterpreter N -> Explore -> Webcam Shot ile webcam'den görüntü alınabilir.

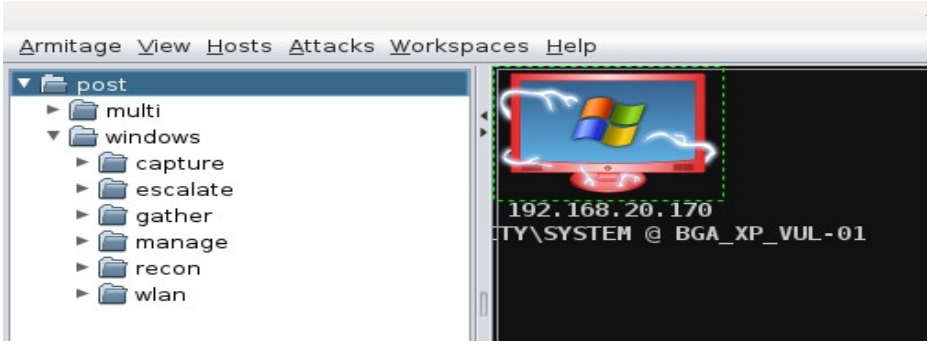
Komut Satırını Çekme

Hedefi temsilen gösterilen arayüzdeki monitöre sağ tıklanır ve Meterpreter -> Interact -> Command Shell sekmeleri tıklanarak hedef sistemin komut satırını komut satırımıza getirebiliriz.

(Page 27-28)

11)

Post Exploitation Modülleri
Armitage sisteme sızıldıktan sonra neler yapılabileceği konusunda seçenekler sunmaktadır. Bu ilgili seçenekler aşağıdaki resmin solunda yer alan post klasörü altında sunulmuştur:



Bu seçeneklerin (modüllerin) kullanımı offensive security'nin sitesinden veyahut forumlardan öğrenilebilir.

(Page 28)

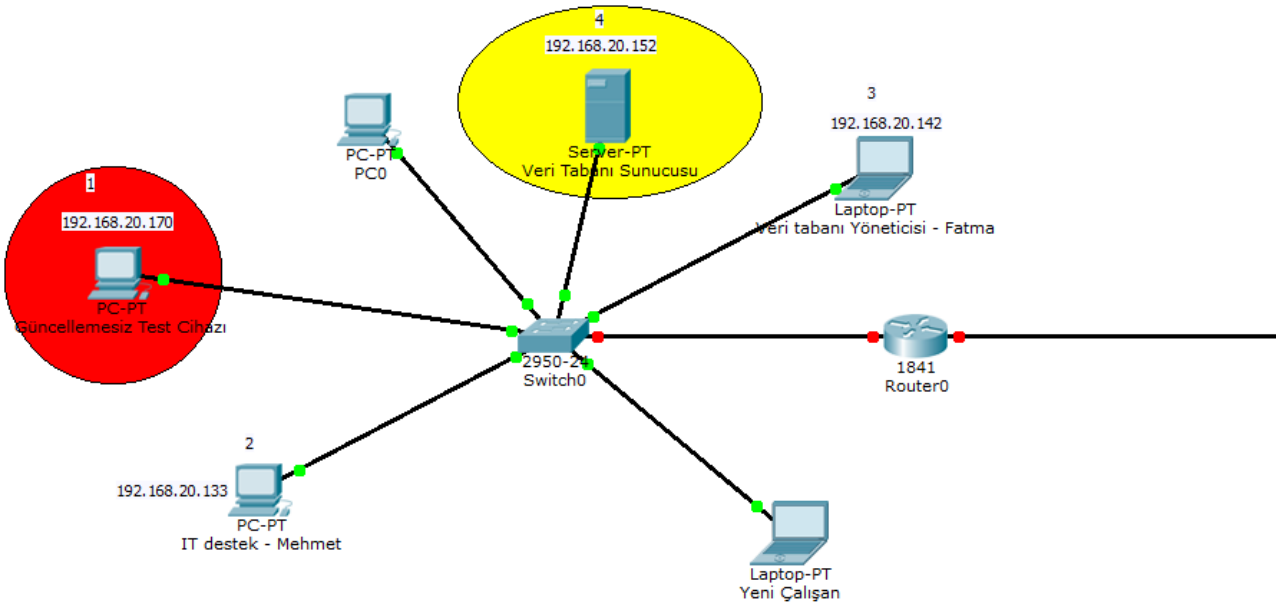
12)

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

(Page 29)

13)

BGA Veritabanı Erişim Bilgilerinin Elde Edilmesi Senaryosu
Senaryoyu açıklamadan önce senaryonun uygulanacağı hedef ağ topolojisini bir inceleyelim.



Bilgi İşlem personeli Mehmet şirketinde yapacağı denetlemeleri şirketin ağına uygulamadan önce test maksadıyla bir köşede duran kırmızı renkli makinaya uygulayacaktır. Mehmetin bu test makinası şirkette aktif iş yapan makinalardan biri olmadığı için güncellemelerden yoksundur. Varsayalım ki Mehmet bu test edilecek makinada kendi makinasındaki oturum bilgilerini kullanmaktadır. Şirketin veritabanı yöneticisi Fatma ise veritabanı giriş bilgilerini masaüstünde tutuyor olsun. Bu iki şahıs dışında bir de bizi temsil edecek kötü niyetli bir personelin bu ağ topolojisine sahip şirkette işe alındığını varsayalım. Bu senaryoya göre kötü niyetli işe yeni alınmış personel olarak amacımız veritabanında bulunan verilere erişmektir. Bunun için veritabanının

erişim bilgilerine erişmemiz gerekmektedir. Dolayısıyla izlenecek adımlar şunlardan oluşur:

1. Ağ taranacak ve hangi cihazların ayakta olduğu ve hangi işletim sistemlerinin kullanıldığı tespit edilecek.

2. Tespit edilen işletim sistemlerinin bildirilmiş mevcut açıklıkları olabilir. Bu açıklıklar varsa denenecektir.

3. Bilgisayara bu bilinen açıklıklardan sızıldığı takdirde hedef makinanının kullanıcılarına ait hesap özetleri (hash'ler) alınacaktır.

4. Alınan hash'ler ile diğer sistemlere login olunmaya çalışılacaktır.

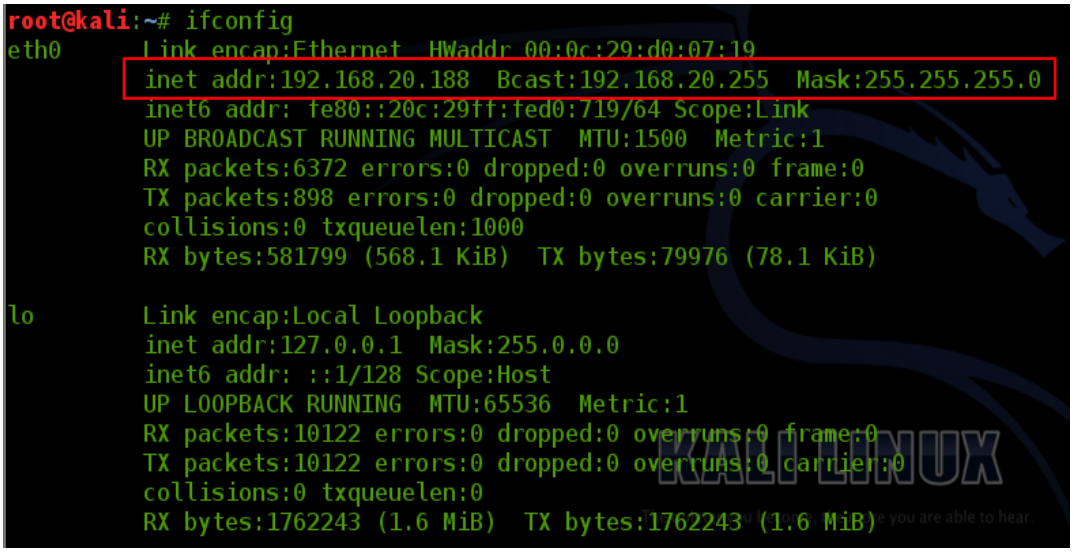
5. Başarılı girişler sonucu oturum yapılan makinelerden bilgi toplanmaya çalışılacaktır.

Senaryonun Uygulanması
a)
Şirkette kötü niyetli bir personel olarak işe başlanır. Verilen bilgisayarda Kali Linux USB'den başlatılır ve gerekli servisler aşağıdaki gibi başlatılır:

> service postgresql start
> service metasploit start
> armitage

b)
Ardından verilen bilgisayarın hangi ağda olduğu tespiti yapılmalıdır. Bu işlem IP adrese bakarak gerçekleştirilebilir:

> ifconfig

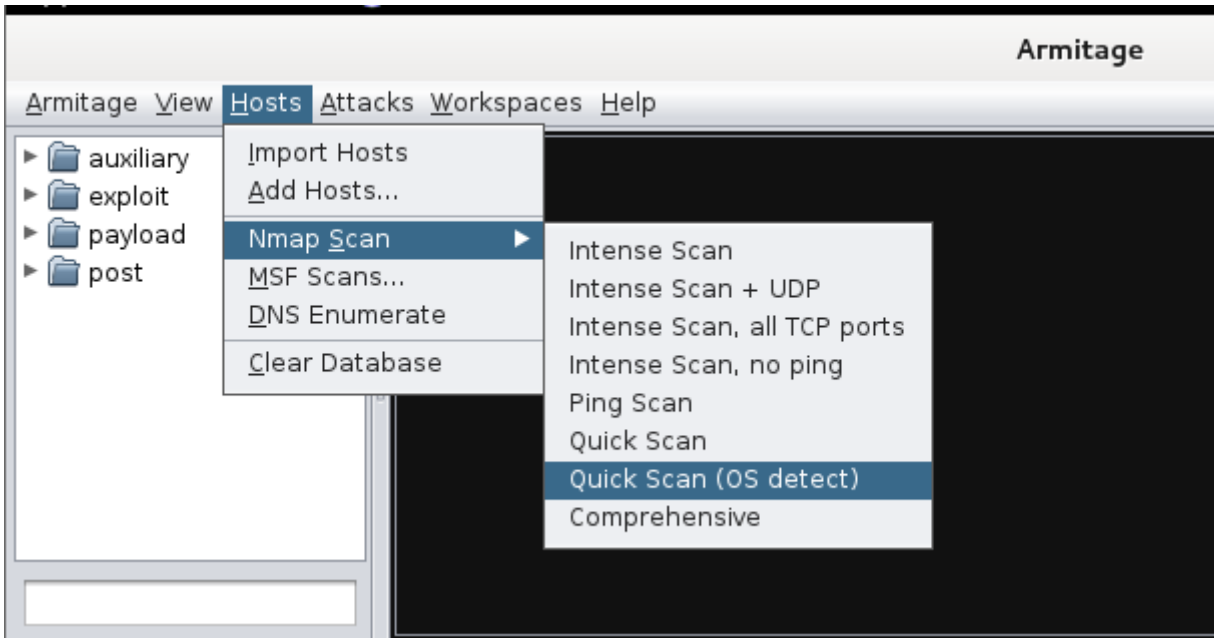


IP'miz 192.168.20.188'miş. Subnet Mask değeri 255.255.255.0 olduğuna göre ait olduğumuz network address'imiz 192.168.20.0 olmalıdır. Mask'ta 24 tane 1 olduğuna göre bu durumda

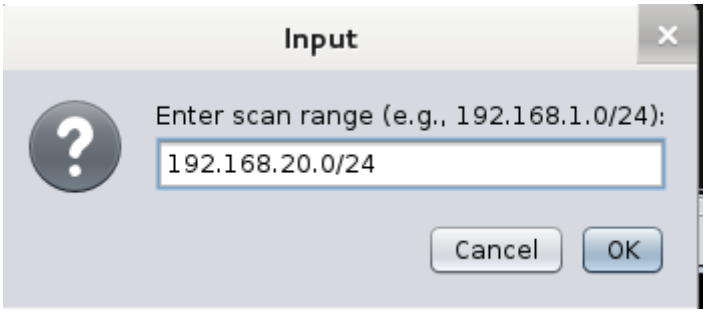
192.168.20.0/24

şeklinde ifade elde edilir. Bu ifade Armitage'dan ayaktaki sistemleri tespit etmek maksadıyla kullanılacaktır.

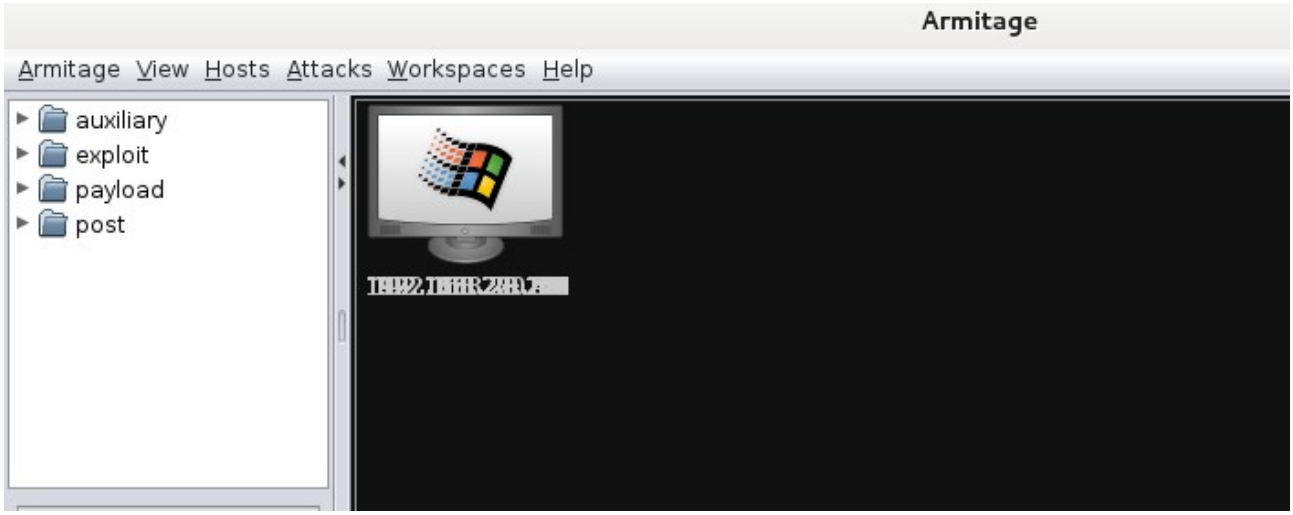
c)
Armitage arayüzünden faydalanarak ağda hangi IP'lerin ayakta olduğunu ve hangi işletim sistemlerini çalıştırdığını tespit edelim:



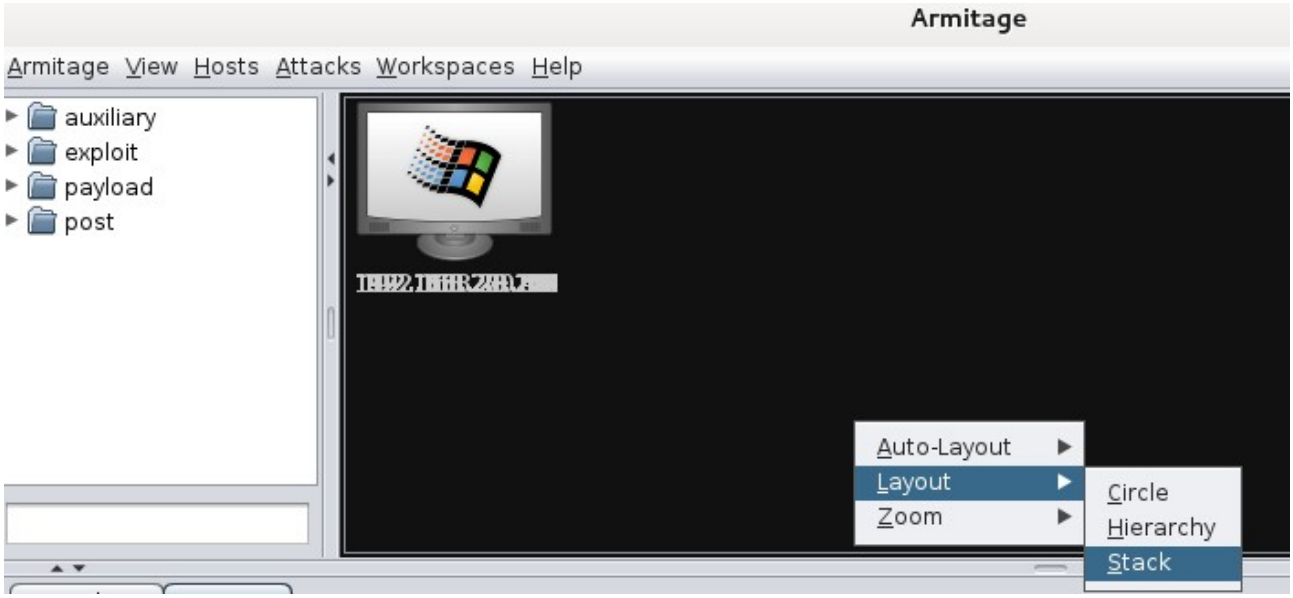
Quick Scan (OS detect) seçildiğinde, ekrana gelecek olan pencereye taranmak istenilen ağ adresi girilir.

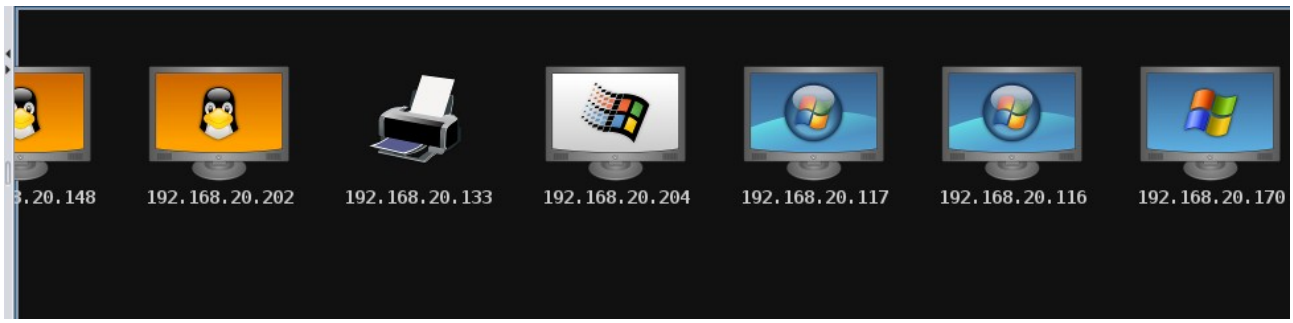


Böylece bulunduğumuz ağdaki tüm olası IP adresleri taranacaktır ve yanıt dönen makinaların ayakta olduğu tespit edilir Armitage ekranına monitor simgesi şeklinde yansıyacaktır.



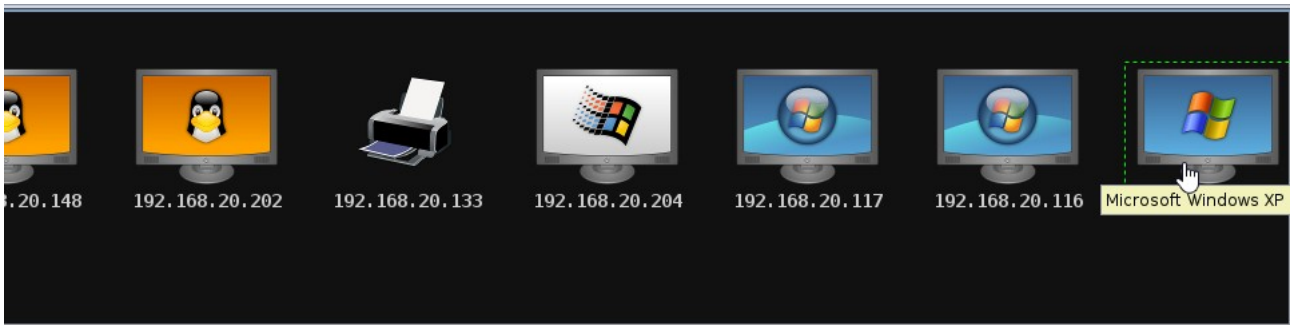
Tarama sonucu elde edilen hedefler yukarıdaki gibi üst üste binmiş şekilde ekrana yansırsa siyah ekrana sağ tıklayıp Layout -> Stack seçeneği tıklanmalıdır.





Böylece tarama sonucu ayakta olduğu tespit edilen sistemler ekrana sıralı bir şekilde yerleşmiş olur.

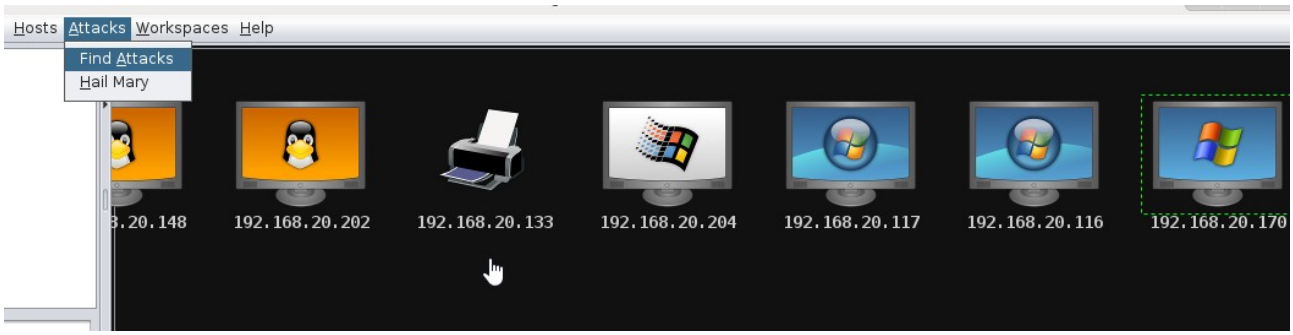
d)
Monitör simgelerin üzerlerine gelinerek hedeflerin işletim sistemlerini belirten bildirim yazıları görüntülenir ve eski bir işletim sistemi aranır. Mesela XP.



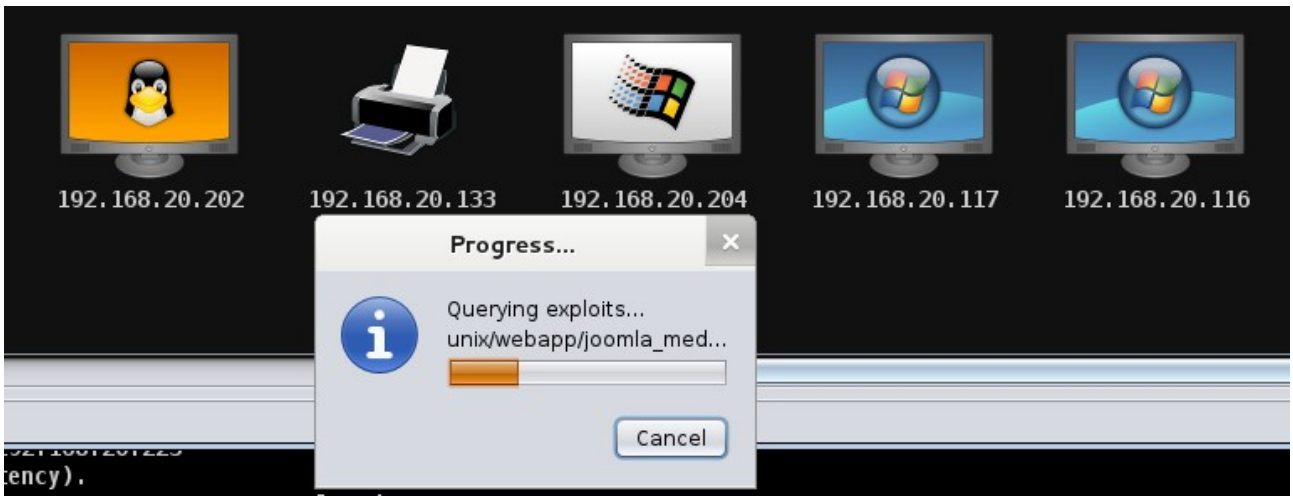
e)
Seçilen XP sisteminin IP değeri ekrandaki fare imlecini monitör üzerinden çekerek öğrenilebilir: 192.168.20.172 . Şimdi bu hedefin monitörüne bir kez tıklayalım ve Armitage menüsünden

Attacks->Find Attacks

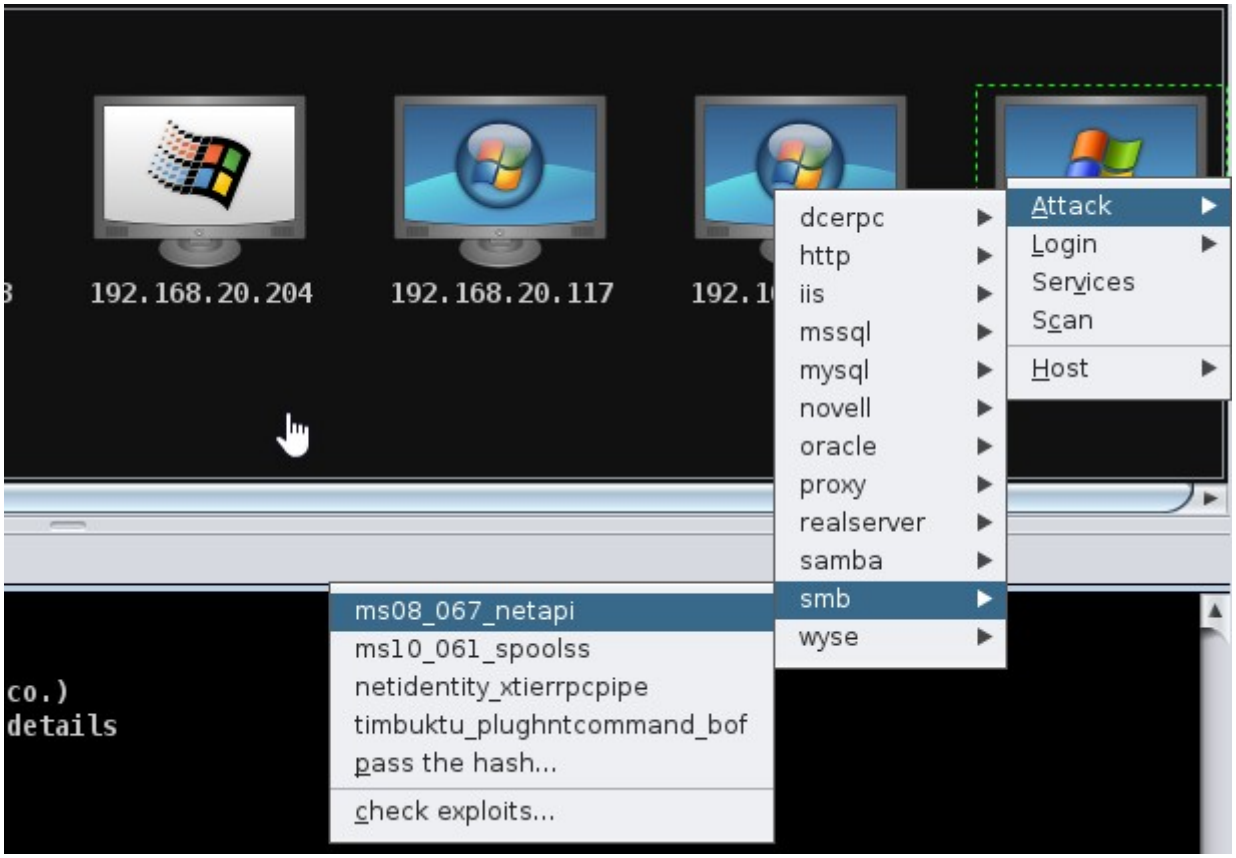
seçeneklerine sırasıyla tıklayalım.



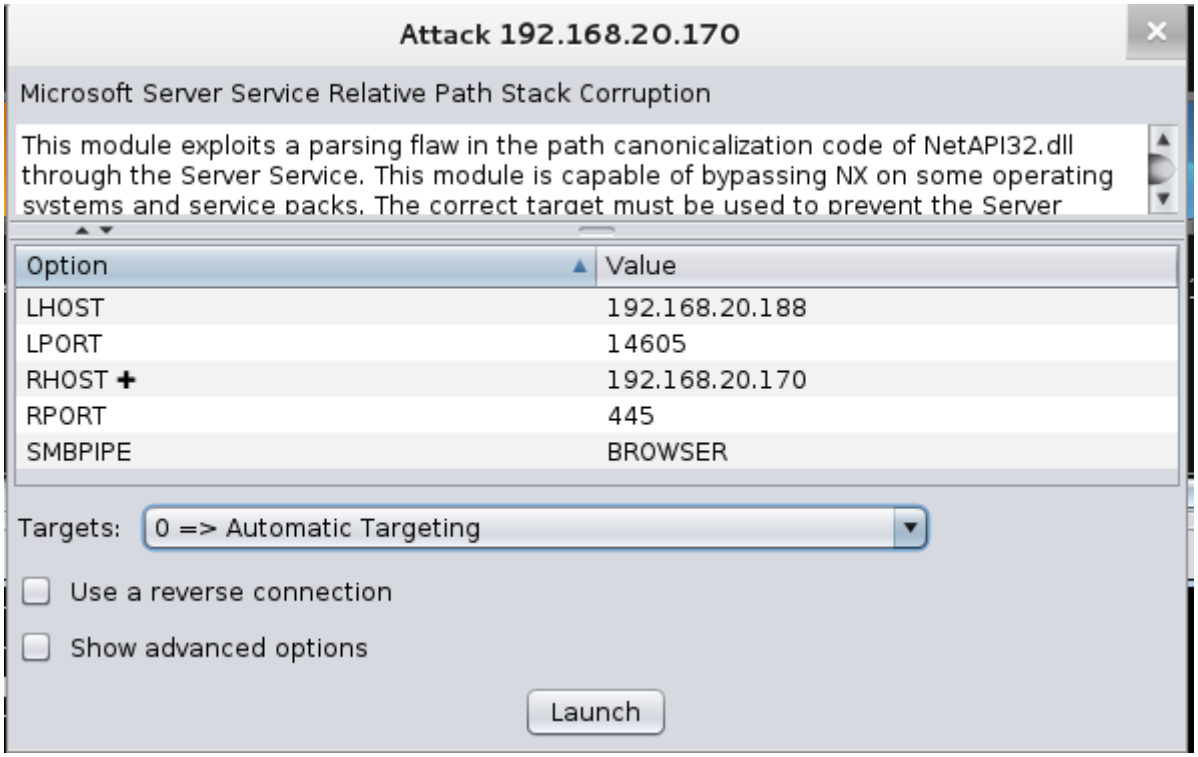
Armitage seçtiğimiz hedefin işletim sistemi ve Service Pack değerini göz önüne alarak bir takım exploitler önerecektir. Bu arama işlemi devam ederken aşağıdaki gibi bir pencere görüntülencektir.



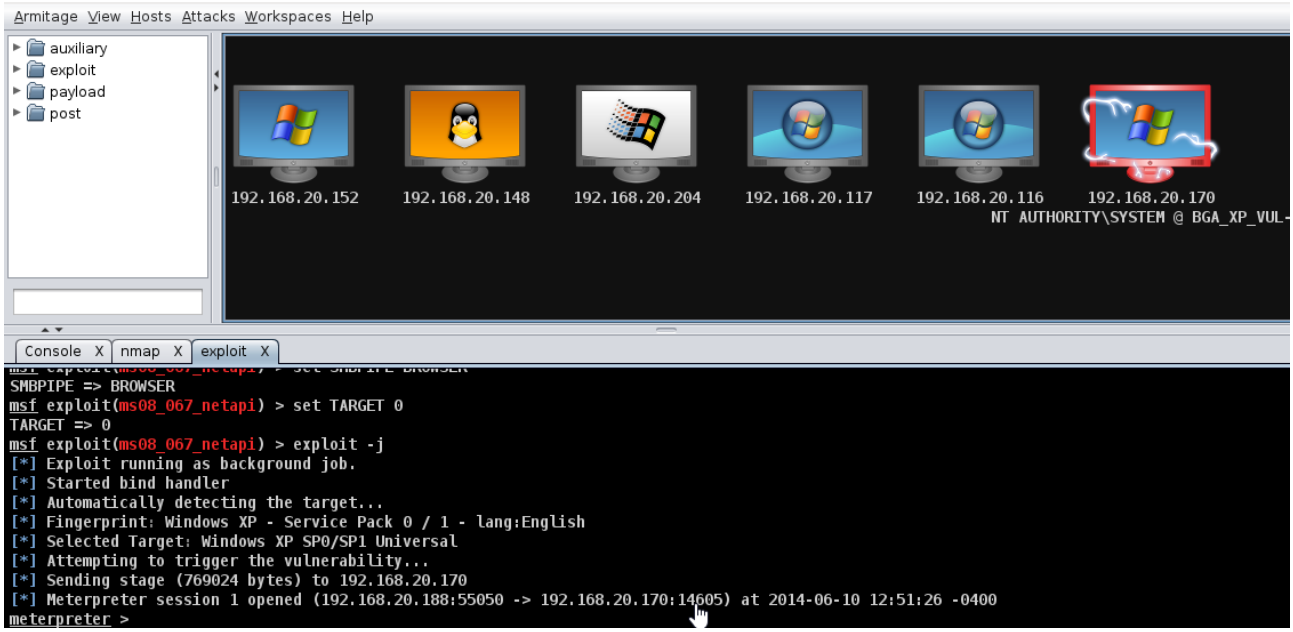
f)
Tarama bittikten sonra hedefin monitör simgesine sağ tıklayıp Attack seçeneğinde bizim hedefe uygun sunulmuş exploit'ler arasından dilediğimizi seçebiliriz. Diyelim ki ms08_067_netapi exploit'ini seçtik.



Exploit seçildikten sonra ekrana parametreler ve değerlerini gösteren pencere yansır.



Bu exploit için bir ayarlamaya lüzum yoktur. Ama her exploit için aynı şey geçerli değildir. Bazen dinleme portunun, bazen kullanılan payload'ın değiştirilmesi icab edebilir. Şimdi pencereyi olduğu gibi bırakalım ve Launch düğmesine tıklayarak exploit'i çalıştıralım. Çalışma sonrası eğer exploit başarılı olursa hedefin monitörünün ekranını kaplayan eller aşağıdaki gibi görülecektir.

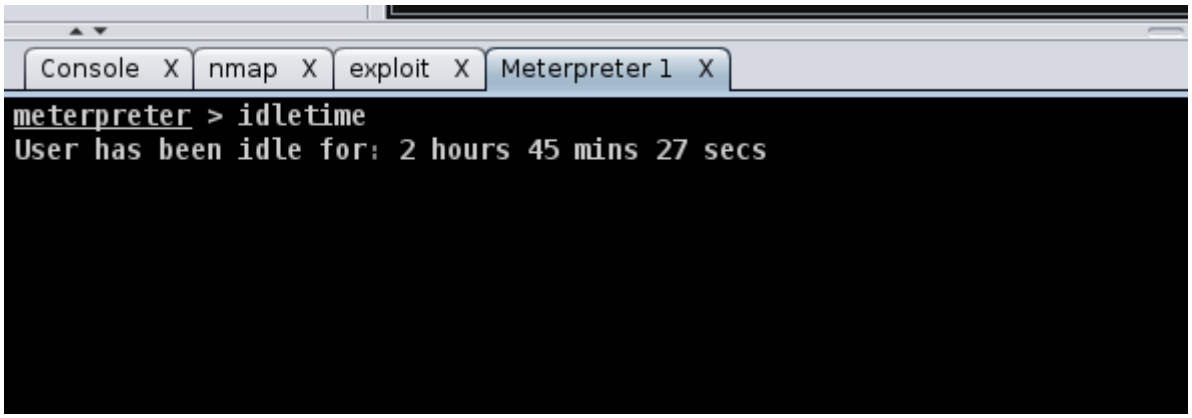


g)

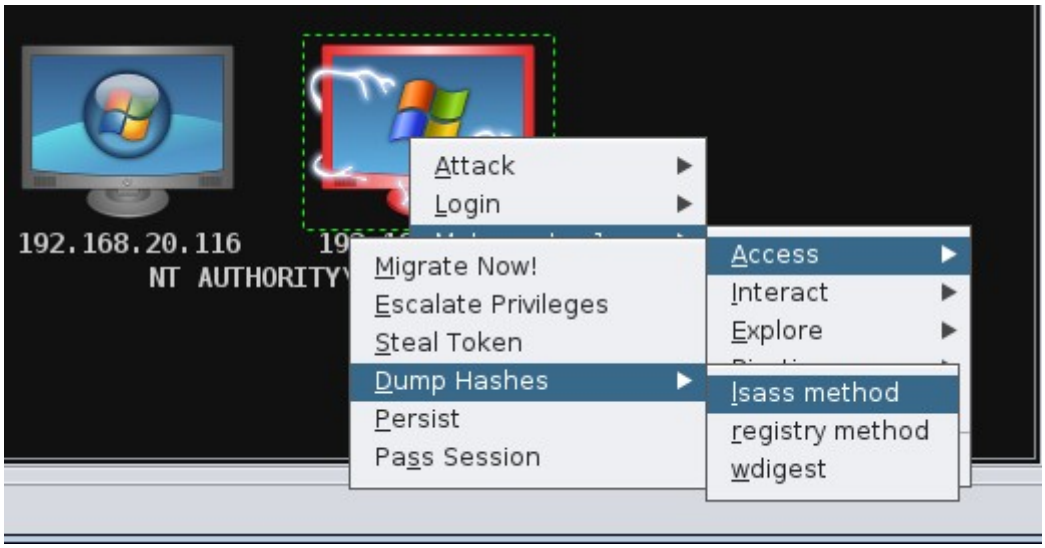
Artık hedefe ms08_067_netapi exploit'i ile sızılmış ve parametrelerde belirtilen meterpreter payload'u ile oturum açılmış vaziyettedir. Bu oturumu Armitage'ın altındaki konsol tab'ının arayüzünde de görebiliriz.

meterpreter >

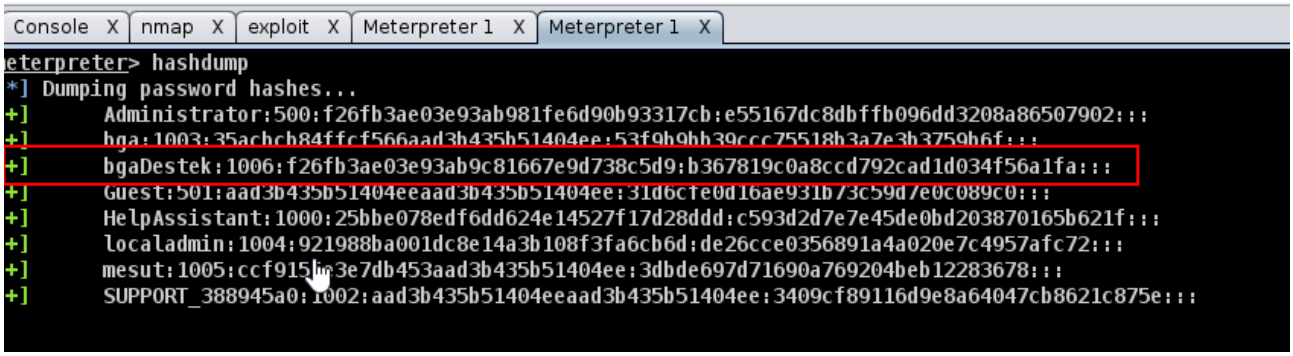
Arayüzden meterpreter komutları girebilmek için ayrıyetten bir meterpreter tab'ına ihtiyaç vardır. Bu nedenle sızılan sistemin monitörüne sağ tıklayıp Meterpreter 1 -> Interact -> Meterpreter Shell seçeneklerine sırasıyla tıklanılmalıdır. Böylece aşağıdaki gibi Meterpreter 1 tab'ı açılır.



idletime komutu hedef sistemin ne kadar süredir boşta beklediğini gösterir. Komutun çıktısına göre yaklaşık 3 saattir hedef, makinasını kullanmıyor ve öylece açık bırakmış vaziyette. Şimdi kötü niyetli personel olarak işe koyulalım ve hedef sistemin kullanıcılarının hesap bilgilerini çekelim. Bunun için hedef monitöre sağ tıklayıp Meterpreter 1 -> Access -> Dump Hashes -> Isass method seçeneklerine sırasıyla tıklayalım.

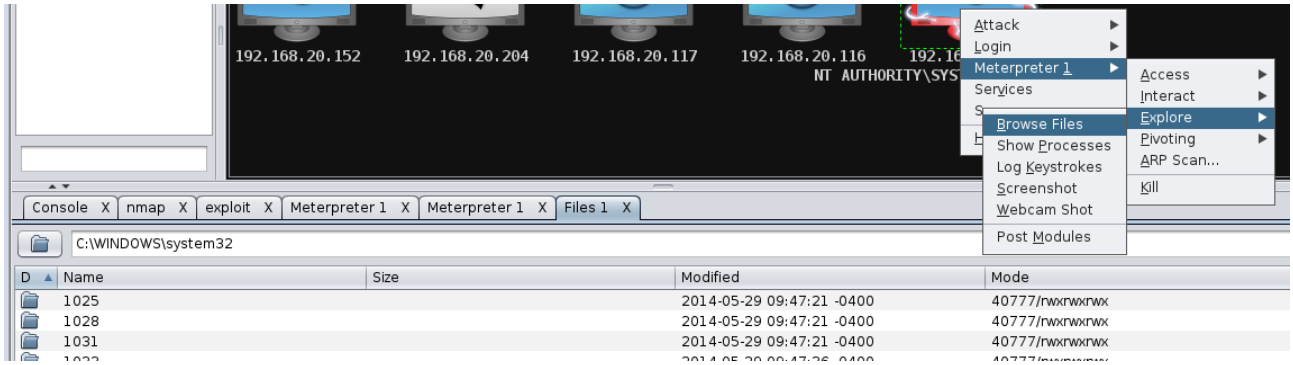


Tıklamalar sonucu Meterpreter 1 tab ekranına kullanıcı adları ve şifreler (hash'ler) yansır:



Yukarıdaki resimde kırmızı çerçeve içerisine alınan kullanıcı bilgileri daha kurumsal göründüğünden ona odaklanmayı seçebiliriz.

Şimdi sızılan bilgisayarın dosya ve klasörlerini meterpreter payload'u ile görelim. Bunun için hedef sistemi temsil eden monitöre sağ tık yapıp Meterpreter 1 -> Explore -> Browse Files seçeneklerine tıklayalım.



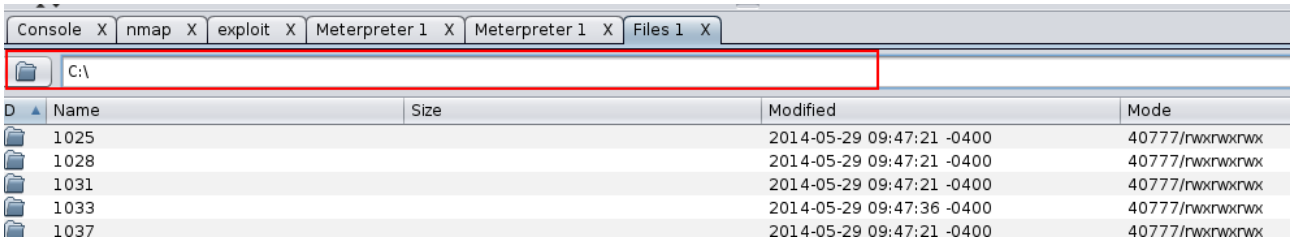
Yukarıdaki resmin altında görebileceğiniz gibi Files 1 adlı bir tab açılmıştır. Bu tab'ın içeriğinde hedef sistemin dizinleri listelenmiştir. Dizinlerin hemen üstünde ise bulunulan dizini ifade eden

C:\Windows\system32

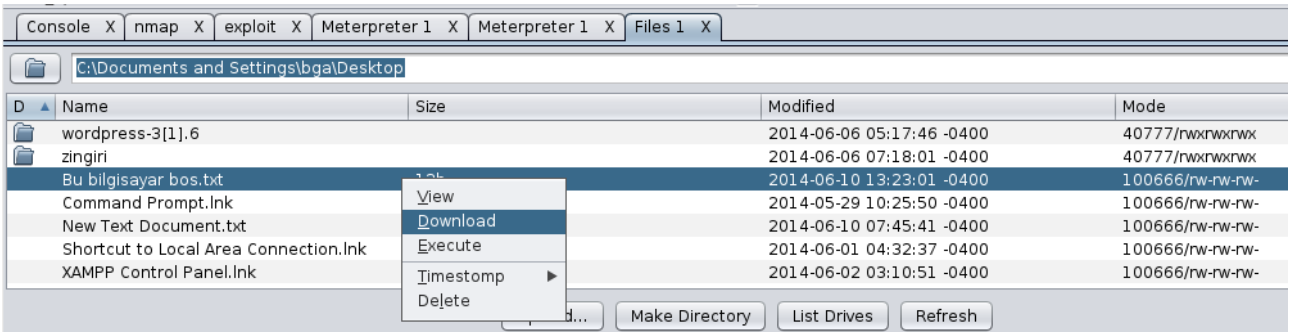
ibaresi vardır. Şimdi hedef sistemin masaüstü dizinine geçiş yapalım. Çünkü kritik bilgiler genellikle ulaşımı kolay olsun diye masaüstüne konuyor. Bu nedenle

C:\Documents and Settings\bga\Desktop

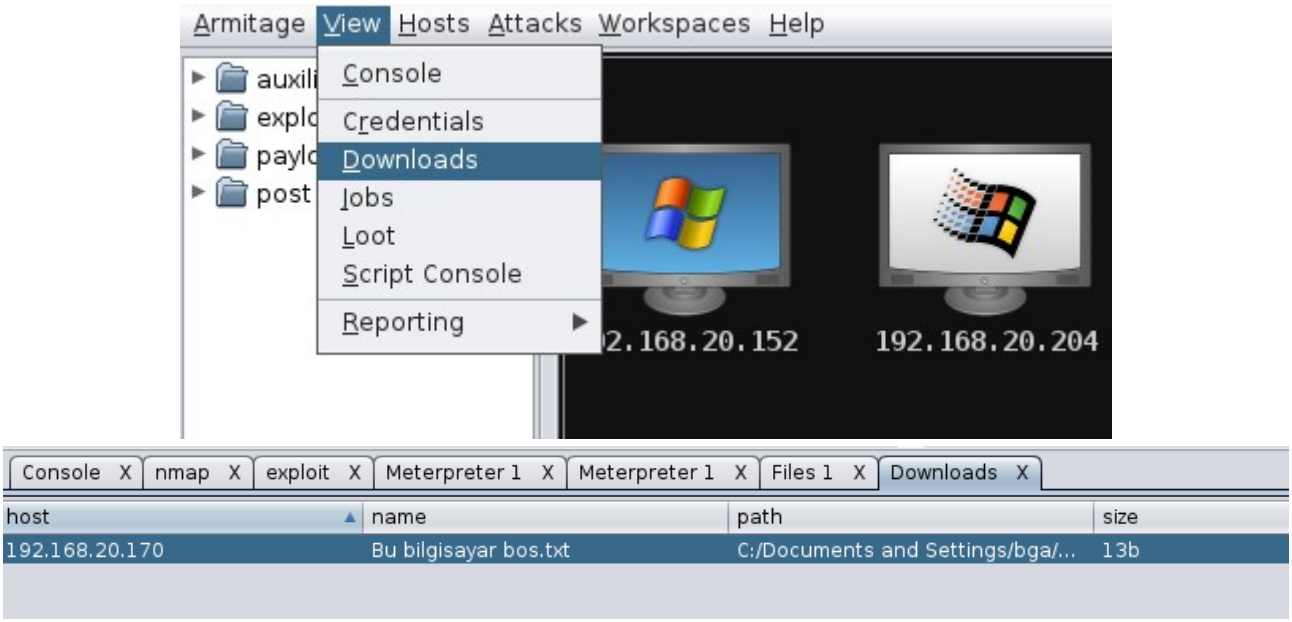
path'ini aşağıda kırmızı ile vurgulanmış kutucuğa girelim.



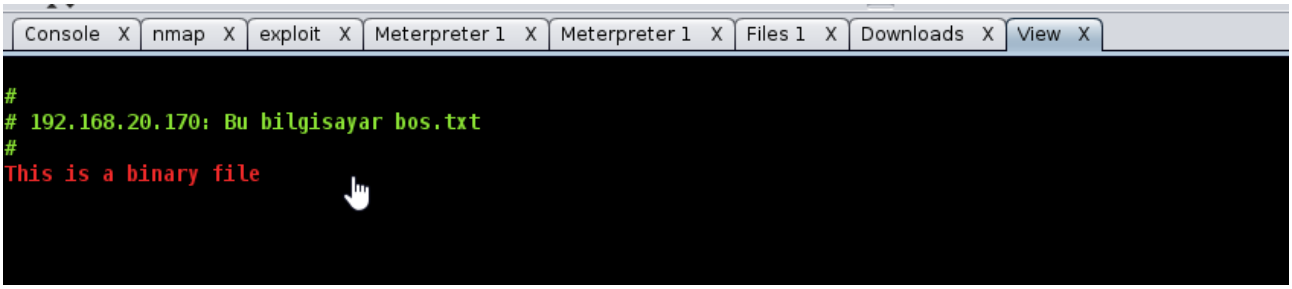
Yeni listelenen dosyalardan birine sağ tıklayıp Download diyerek uzak sistemdeki dosyayı Meterpreter aracılığıyla indirmiş oluruz.



Bu şekilde uzak sistemden bilgisayarımıza inen dosyalara ulaşmak için View -> Downloads sekmesine gidilebilir.



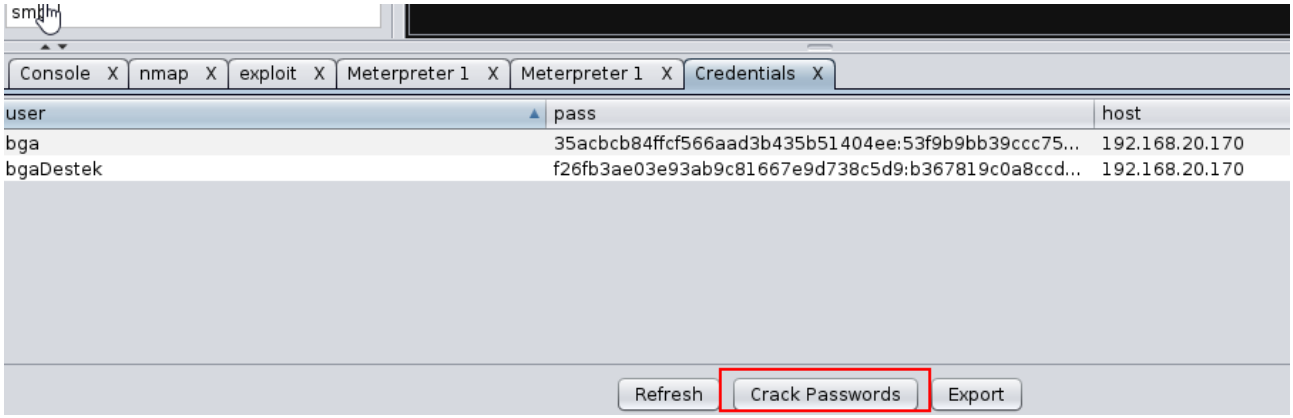
Listelenen inmiş dosyalardan birine çift tıklayarak içeriğini Armitage'da açılan yeni bir tab içerisinde aşağıdaki gibi okuyabiliriz.



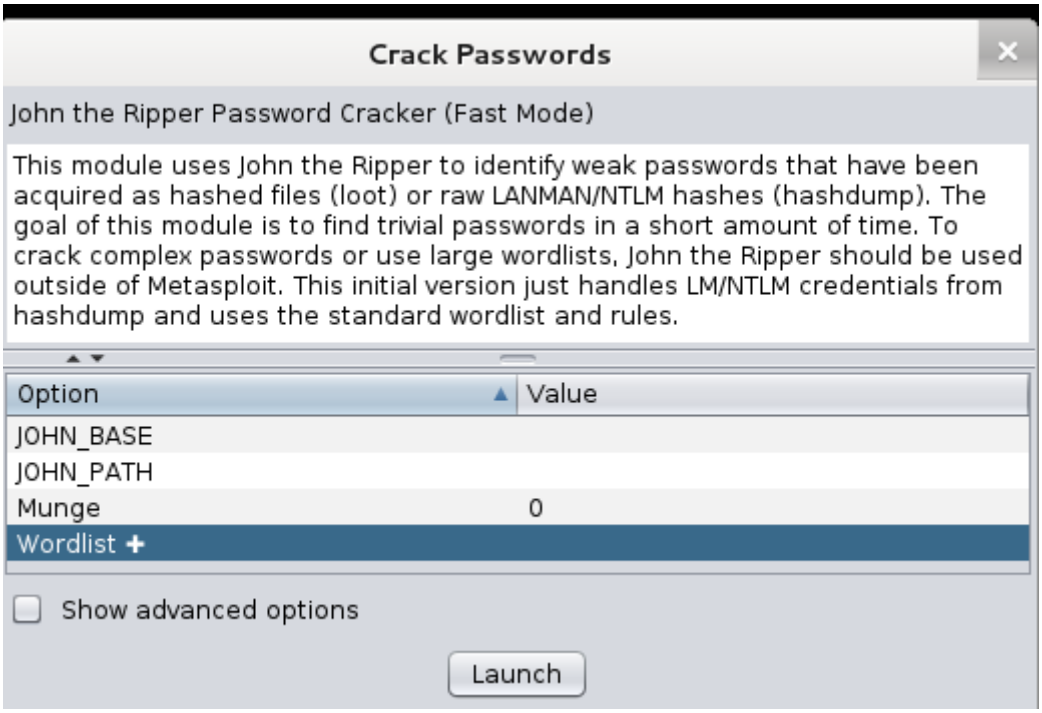
h)

Maalesef sızdığımız hedef sistemden kullanıcı hesap özetleri dışında değerli bir bilgi alamadık.

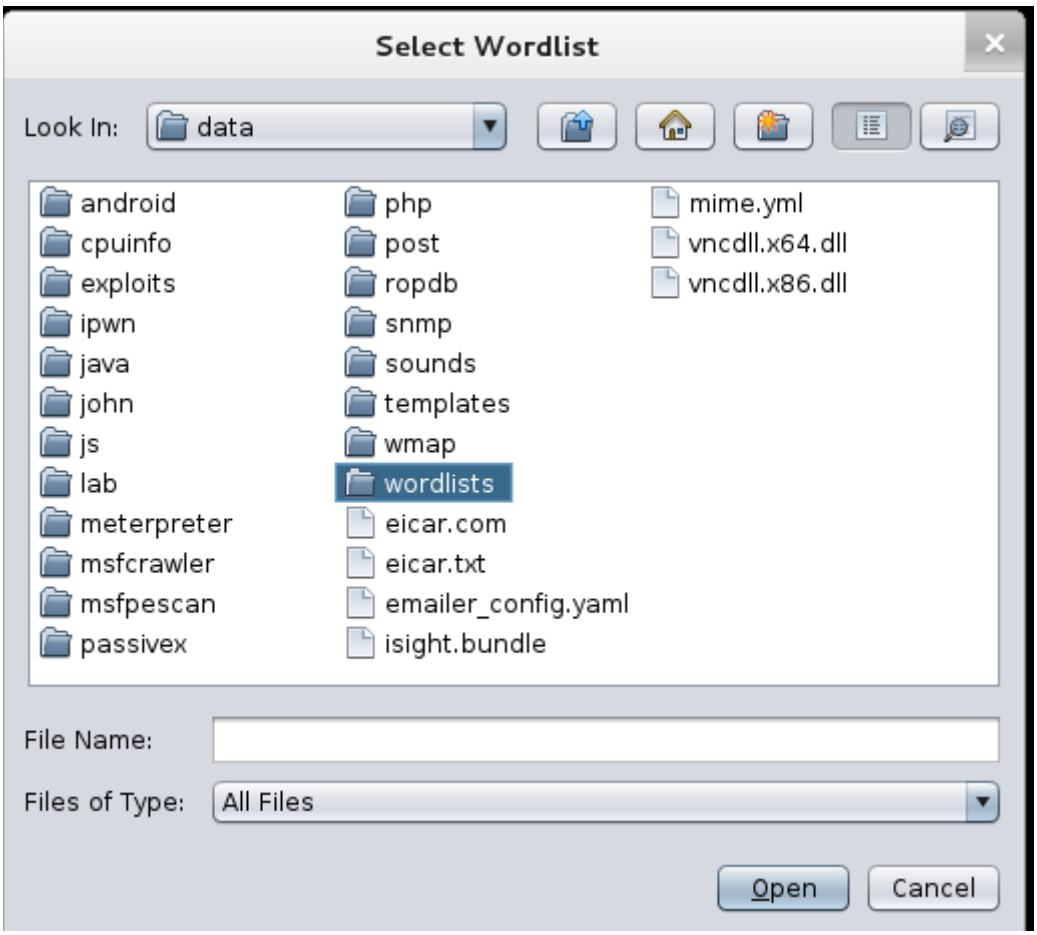
Elde ettiğimiz bu özetleri kıracak olursak Armitage menüsünden View -> Credentials seçeneklerine geçeriz ve alt tarafta belirecek Credentials tab'ındaki gereksiz account satırlarını DELETE tuşu ile sileriz. Böylece Crack Passwords butonuna basarak tab ekranında bıraktığımız satırlardaki hash'leri kırma sürecini başlatabiliriz.



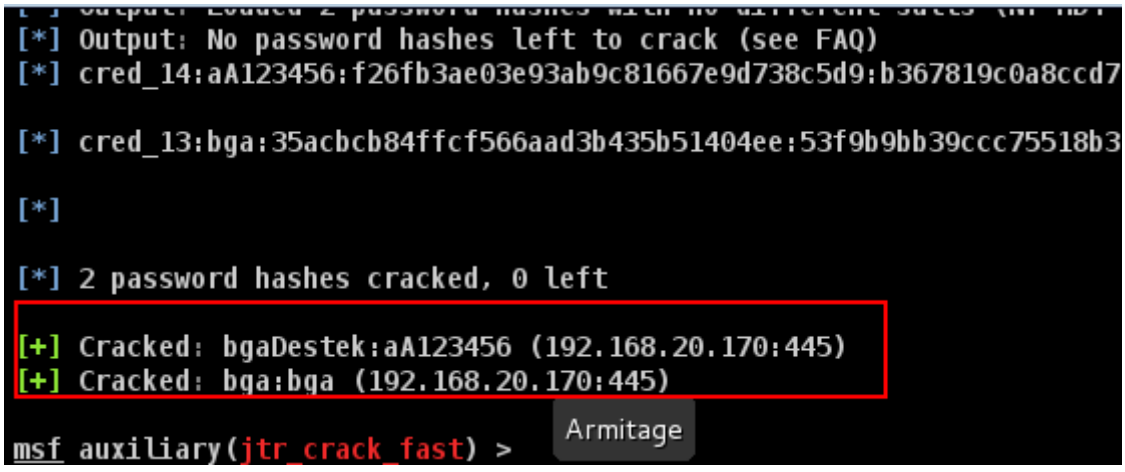
Crack Password butonuna basıldıktan sonra ilgili auxiliary'nin (JTR'nin) parametreleri ekrana yansıyacaktır.



Görüldüğü üzere Wordlist mandatory olarak verilmiş. Dolayısıyla Wordlist + ifadesine çift tıklanır. Bir wordlist seçilir.

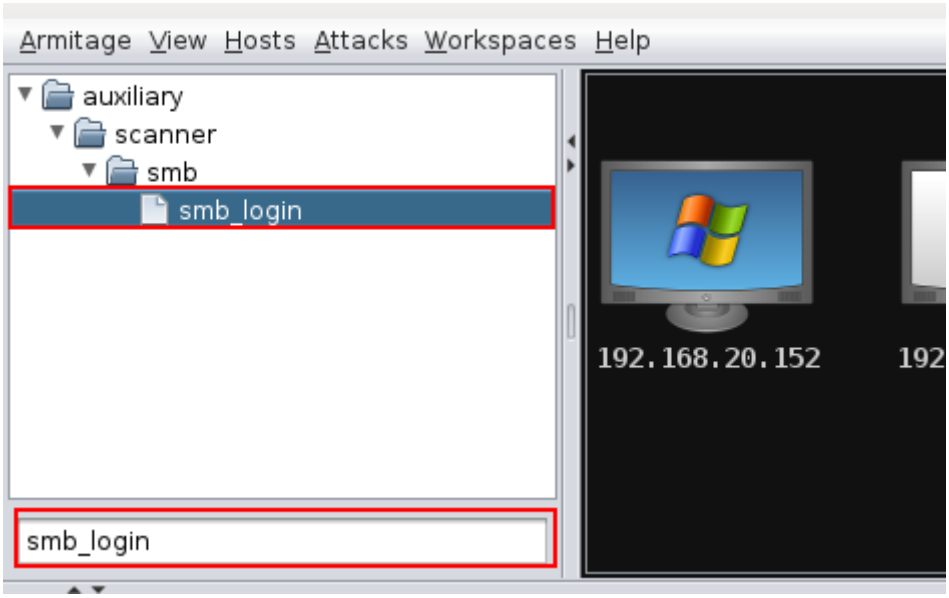


Ardından modül Launch butonuna basılarak başlatılır.

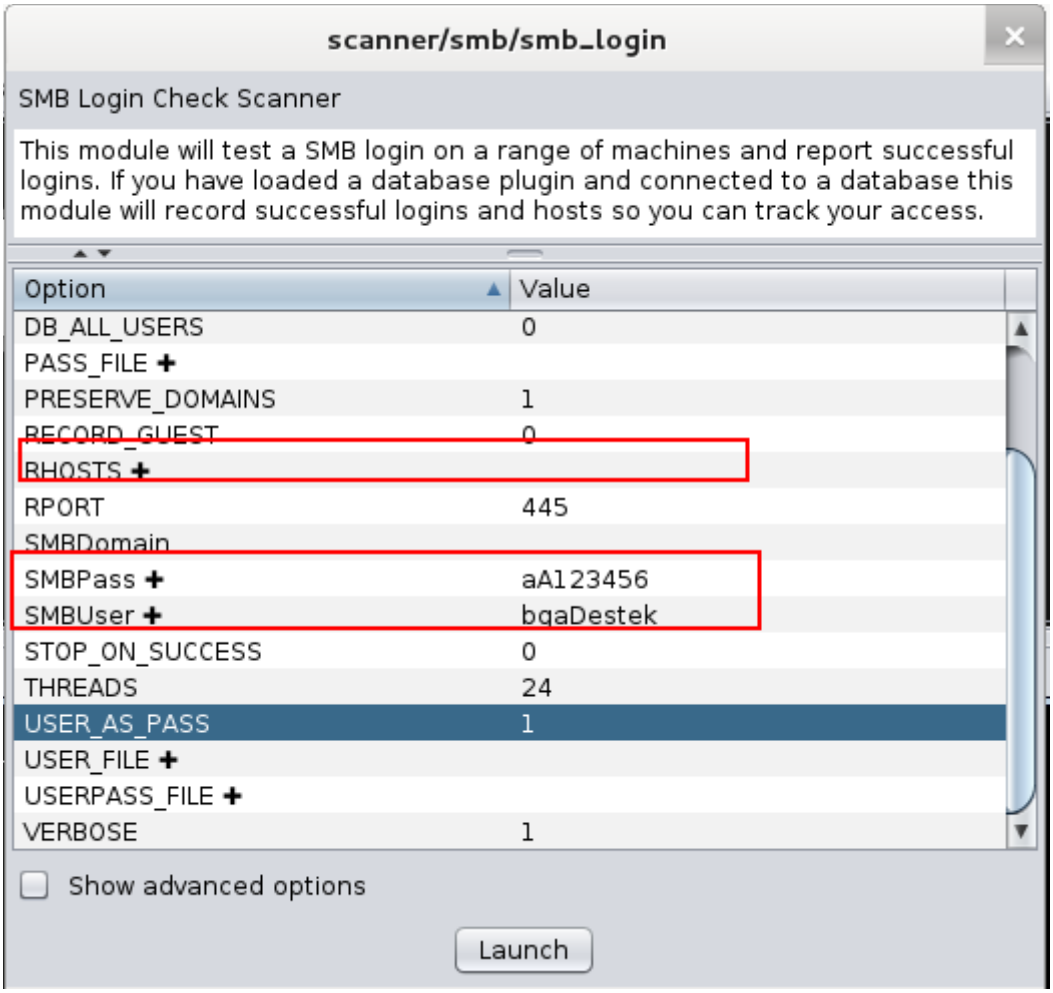


Modülün açtığı tab ekranındaki kırmızı kutucuktan görülebileceği üzere bgaDestek kullanıcısının şifresi aA123456 imiş ve bga kullanıcısının şifresi bga imiş.

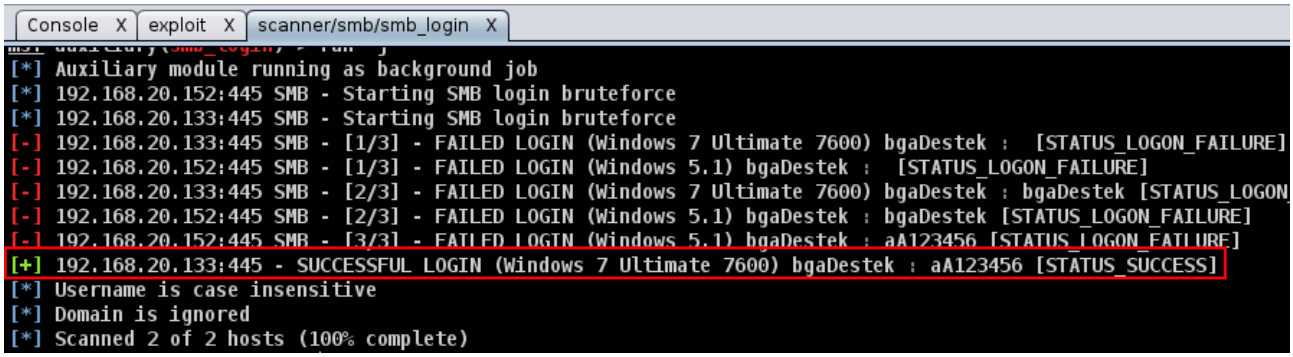
Bu elde edilen şifreler sonrası yapılacak iş network'teki tüm ayakta olan cihazlara elde edilen hesap bilgileriyle smb_login çekmektir. Böylelikle bu hesaplar başka bilgisayarlarda da kullanılıyor muyu öğrenmiş oluruz. Şimdi bu işlemi gerçekleştirelim.



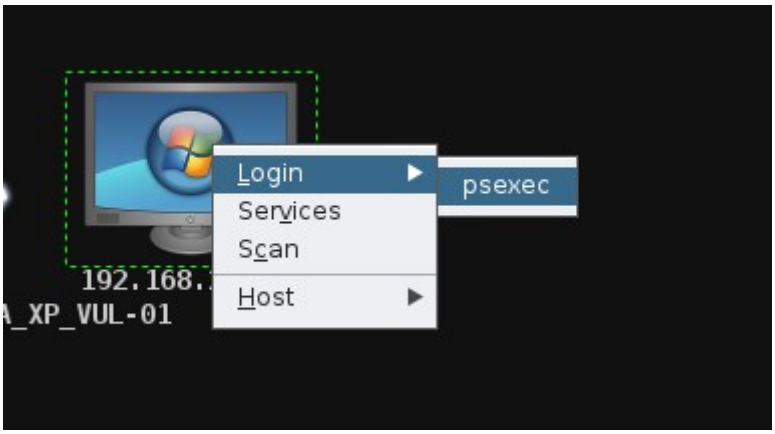
Armitage'ın sol sütunundaki smb_login modülüne çift tıklayalım.



SMBUser parametresine elde ettiğimiz hesaplardan birinin kullanıcı adını, SMBPass parametresine ise elde ettiğimiz bu hesabın şifresini koyalım. RHOSTS parametresine ise daha önce yerel network'teki taramalarımızda tespit ettiğimiz ve Armitage ekranına monitör olarak gelen ayaktaki bilgisayarların IP'lerini virgülle ayırarak girelim. Ardından Launch diyerek bir dosya paylaşım servisi olan smb_login hizmetine uzak sistemlerde oturum açma denemelerini başlatalım.



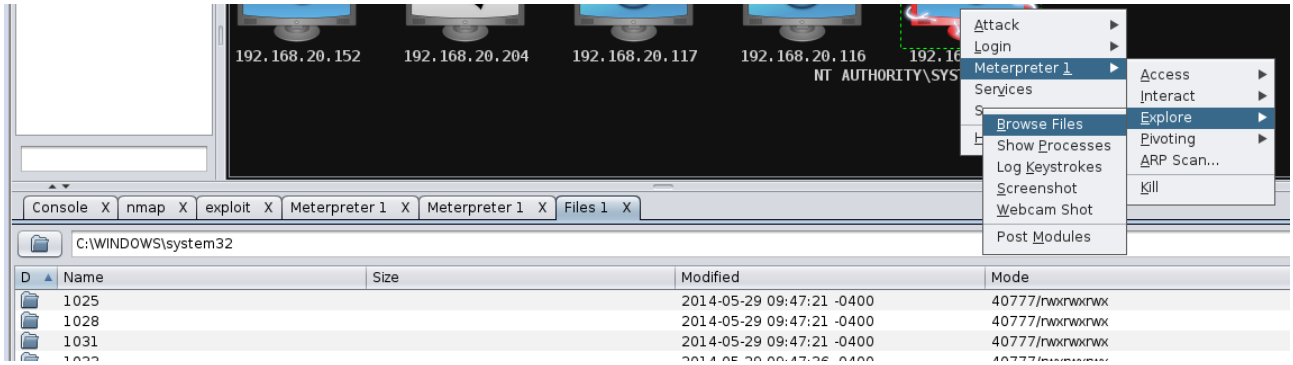
Yeşil renkli satır bize smb servisine login olabildiğimizi söylemektedir. Bu noktadan sonra yapılabilecek şey bu yeşil renkli smb login ile giriş yapılabilen 192.168.20.133 nolu bilgisayara psexec modülü ile sızmaktır (Monitör simgesine sağ tıklayıp Login -> psexec seçeneklerine tıklanarak çalıştırılır).



Modül çalıştıktan sonra bir meterpreter session'ı elde edilecektir.

```
[*] Bound to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:192.168.20.133[\svcctl] ...
[*] Obtaining a service manager handle...
[*] Creating a new service (ixeUyokD - "MPhVgUxFSVmmuKGXBSk")...
[*] Closing service handle...
[*] Opening service...
[*] Starting the service...
[*] Removing the service...
[*] Closing service handle...
[*] Deleting \ZCyStvvy.exe...
[*] Sending stage (769024 bytes) to 192.168.20.133
[*] Meterpreter session 5 opened (192.168.20.188:9640 -> 192.168.20.133:49164) at 2014-06-11 04:03:46 -0400
meterpreter >
```

Session elde edildiğine göre hedef sistemin dizinlerini görelim. Bunun için hedef sistemi temsil eden monitöre sağ tık yapıp Meterpreter 1 -> Explore -> Browse Files seçeneklerine tıklayalım.



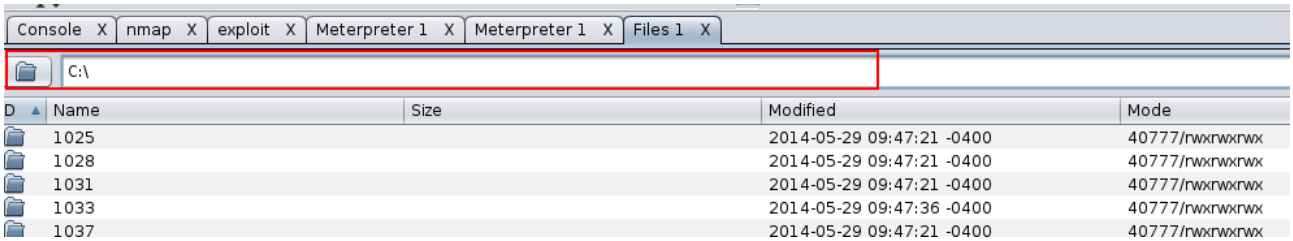
Yukarıdaki resmin altında görebileceği gibi Files 1 adlı bir tab açılmıştır. Bu tab'ın içeriğinde hedef sistemin dizinleri listelenmiştir. Dizinlerin hemen üstünde ise bulunulan dizini ifade eden

C:\Windows\system32

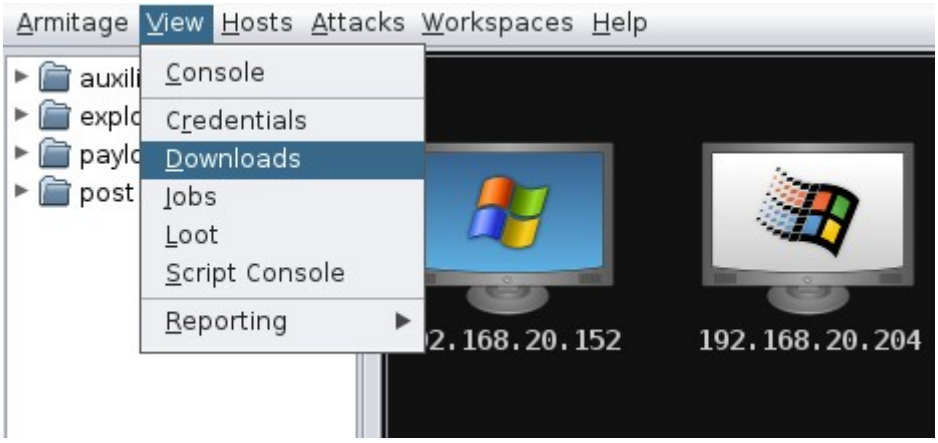
ibaresi vardır. Şimdi hedef sistemin masaüstü dizinine geçiş yapalım. Çünkü kritik bilgiler genellikle ulaşımı kolay olsun diye masaüstüne konuyor. Bu nedenle

C:\Documents and Settings\bga\Desktop

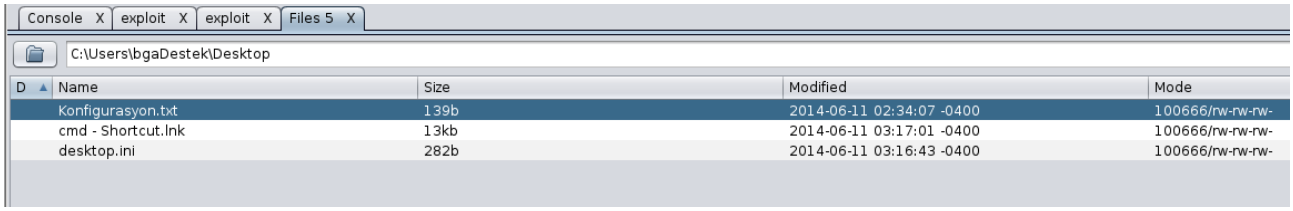
path'ini aşağıda kırmızı ile vurgulanmış kutucuğa girelim.



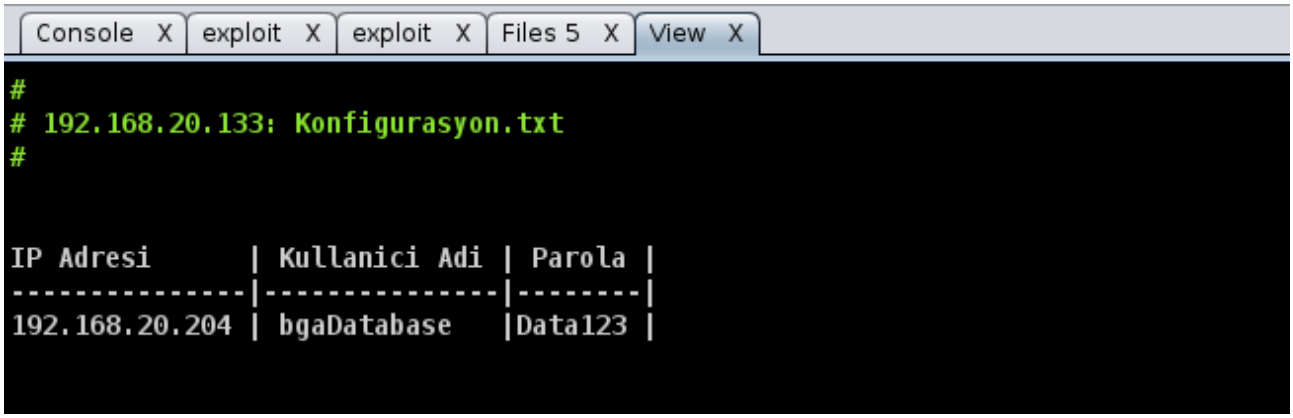
Yeni listelenen dosyalardan birine sağ tıklayıp Download diyerek uzak sistemdeki dosyayı Meterpreter aracılığıyla indirmiş oluruz. İnen dosyayı görüntülemek için View -> Downloads sekmesine gidilebilir.



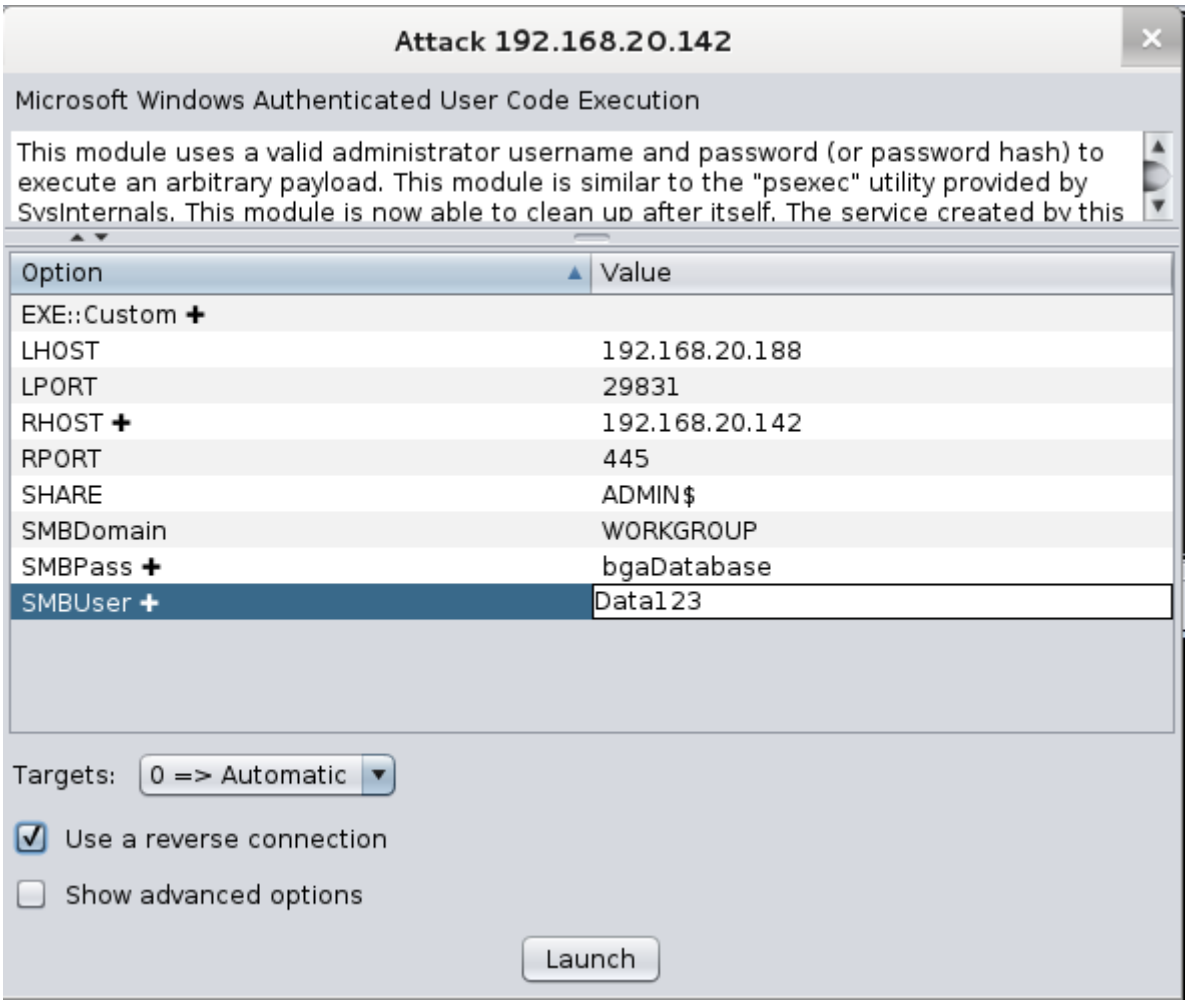
İndirilmiş dosyaları listeleyen aşağıdaki tab ekrana gelir.



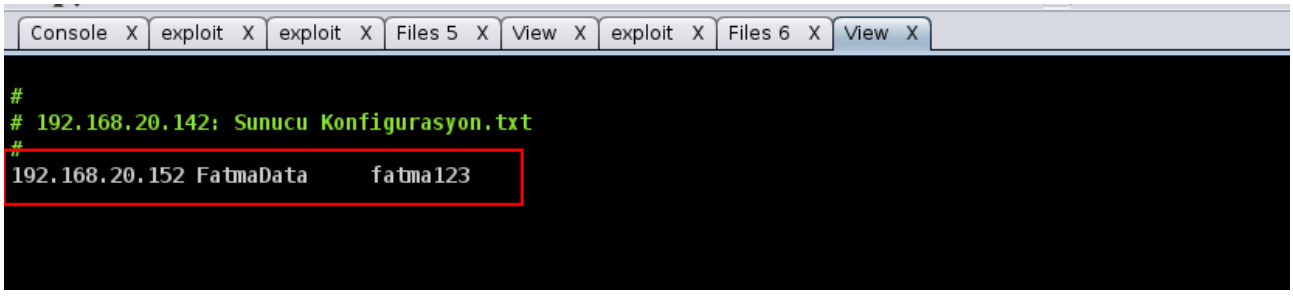
Konfigurasyon.txt dosyasına çift tıkladığımızda ise aşağıdaki tab ekrana gelir.



Böylece hedef sistemin masaüstünde duran konfigurasyon dosyasından hedef veritabanının yüklü olduğu sunucunun hesap bilgisini elde etmiş olduk. Şimdi hedef veritabanı sunucusunun kullanıcı adı ve şifresini öğrendiğimize göre bu hesap bilgisiyle veritabanı sunucusuna sızalım. Bunun için konfigurasyon.txt dosyasından elde ettiğimiz veritabanı sunucusunun IP'sine göre armitage arayüzündeki ilgili monitörü seçelim, sağ tık Login -> psexec diyelim ve yine konfigurasyon.txt dosyasından elde ettiğimiz credentials'ları (bgaDatabase kullanıcı adını ve Data123 şifresini) parametrelere girelim.



Session elde edildikten sonra masaüstü dizinine gidelim ve veritabanı sunucusundaki konfigurasyon dosyasını indirelim. İnen dosya görüntülendiğinde aşağıdaki içerik ekrana yansıyacaktır.



Böylece veritabanı sunucusundaki veritabanı uygulamasının kullanıcı adı ve şifresini elde etmiş olduk. Yani senaryoyu tamamlamış olduk. Artık veritabanına uzaktan bağlanıp dilediğimiz kritik bilgileri çekebiliriz.

(Page 30-49)