**AĞ VE SİSTEM GÜVENLİĞİ**

**ADI: MERVE**

**SOYADI: ÇELİK**

**KONU: SİBER ATAK ÇEŞİTLERİNİ RAPORLAMA**

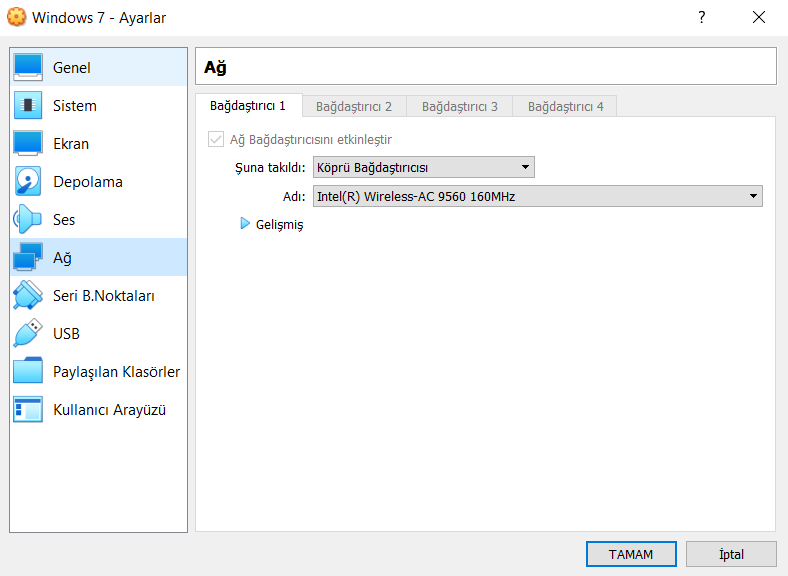
Man in the Middle saldırı için ARP Attack

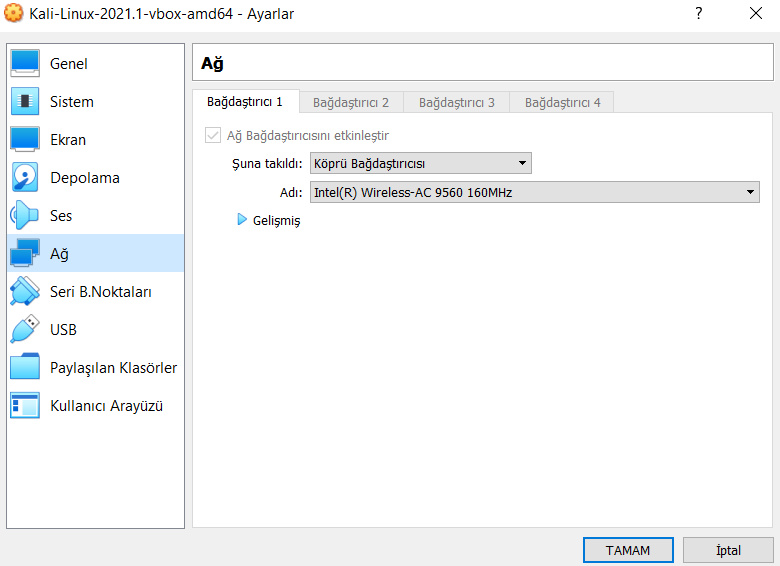
NOT: IP Address spoofing içinde ARP spoofing (ARP Poisoning) bulunmaktadır.Fakat ben videomu ve pdfimi Man in the Middle konumuna geçme amacıyla hazırladığım için başlığın böyle daha iyi durucağını düşündüm.

Bir cihazdan internete bağlanabilmek için access point ve cihazımız arasında bir yetkilendirme yapmamız gerekiyor.Bu yetkilendirmeyi internetin şifresi olarak düşünebiliriz.Bilgisayarımız bu şifreyi girdiği zaman bilgisayarımız ve modemimiz bir token üretir.Ve bu tokenler birbirleriyle yer değiştirir.Böylece modemimiz bilgisayarı,bilgisayarımız modemi tanır.Ve birbirleri üzerinden işlem yapma izni sağlanmış olur.

Biz Man in the Middle saldırısını yapmaya başladığımızda cihaza gidip diyoruz ki ben modemim ben internetim bana bağlan.Modeme de gidip diyoruzki ben bu cihazım , benim üzerimden işlem yap.Böylece bilgisayar bize veri gönderiyor,biz veriyi access pointe gönderiyoruz.Daha sonra dönen paketleri de yine aynı şekilde modem bize gönderiyor biz de bilgisayara cihaza gönderiyoruz.Ve böylece ortadaki adam olarak bütün ağ trafiğini izleyebiliyoruz.Man in the Middle saldırısının kilit noktası ARP saldırısı yapmaktır.Bu protokol ağ katmanı adreslerinin veri bağlantısı katmanı adreslerine çözümlenmesini sağlayan bir protokoldür.Bizi ortadaki adam konumuna getirir.

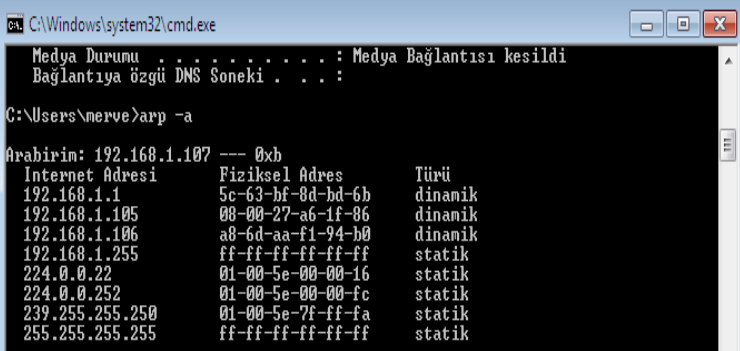
Bu işlem için çift ekran çalışacağız.Sanal makine üzerinde windows 7 ve Kali-Linux var.Bu iki sistem aşağıda gösterildiği gibi aynı ağ üzerinde çalışıyor.





Çoğu yerde ortak internet bulunmaktadır.Aynı zamanda bu saldırı ortak internet kullanımının ne kadar zaralı olduğunun kanıtıdır.

Windows 7 ekranında cmd yi açtıktan sonra arp -a diye komut yazıyoruz.Karşımızı birçok ip ve fiziksel adresleri çıkıyor.



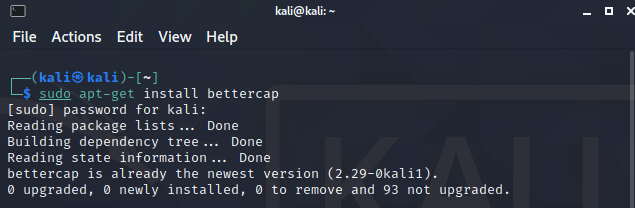
Yukarıda görmüş olduğumuz 192.168.1.1 adresi bağlandığımız internet modem gibi düşünebiliriz burayı gatewayimiz.Ve görmüş olduğumuz gibi kendine ait fiziksel adresi var.192.168.1.105 adresi de aslında Kali-Linuxumuz.

İpconfig yazarak bu bilgisayarın da ip bilgisini görelim.

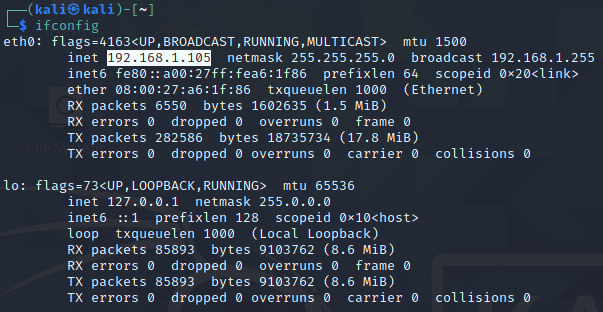


Windows 7nin ip adresi 192.168.1.107 dir.

Saldırı için kullanmamız gereken ismi bettercap olam bir araç var.Bu aracı kurmak için Kali-Linux terminal pencerimizi açıp sudo apt-get install bettercap yazıyoruz.Ardından şifremizi girerek indirme işlemini gerçekleştiriyoruz.Önceden yüklü olduğu için bende yüklü olduğunu söyledi.



Hangi internet arayüzünü kullandığımızı görmek için Kali-Linux terminal pencerimize ifconfig yazıyoruz.



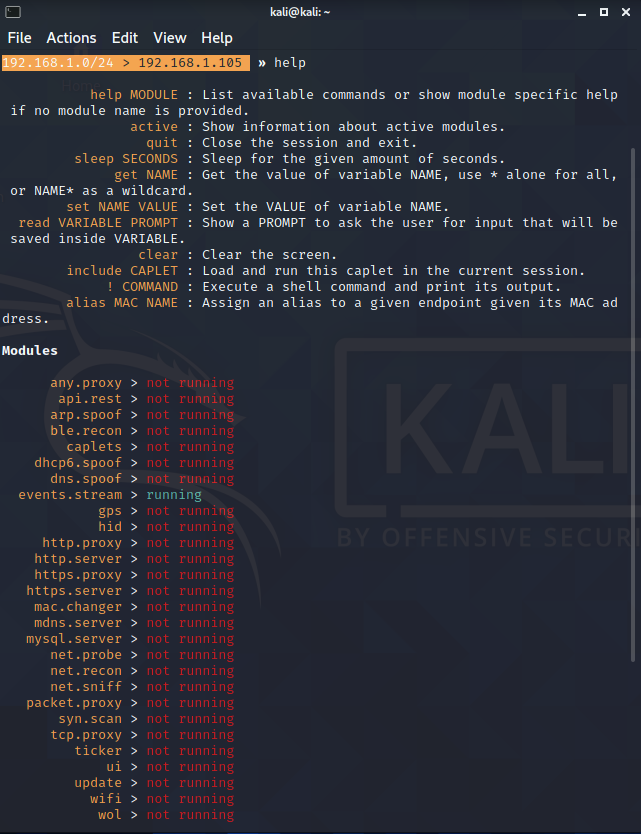
Görmüş olduğumuz gibi eth0 üzerinden internete bağlıyım ve ip adresim 192.168.1.105.

Bettercapi başlatmak için Kali-Linux terminal pencerisine sudo bettercap -iface eth0 yazıyoruz.eh0 yazılan yere kullanmış olduğumuz arayüz yazılır.

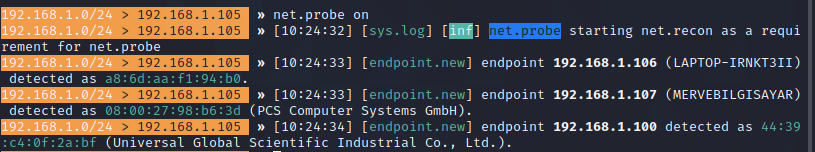


Ve interaktif bir kullanım sağlıyor burada.

Yanına help yazıp ne var ne yok diye bakıyoruz.



Görmüş olduğumuz gibi birçok modül var burada.Bizim şuanda bulunduğumuz ağda bir keşif yapmamız lazım.Bu yüzden net.probe modülünü çalıştırmamız gerekiyor.Bu modül ağdaki tüm cihazları dürtecek ve cevap verenleri bize şuanda aktif olarak gösterecek.Bunun için terminal penceresine net.probe on yazıyoruz ve çalıştırdıktan sonra net.probe çalışır hale geliyor.



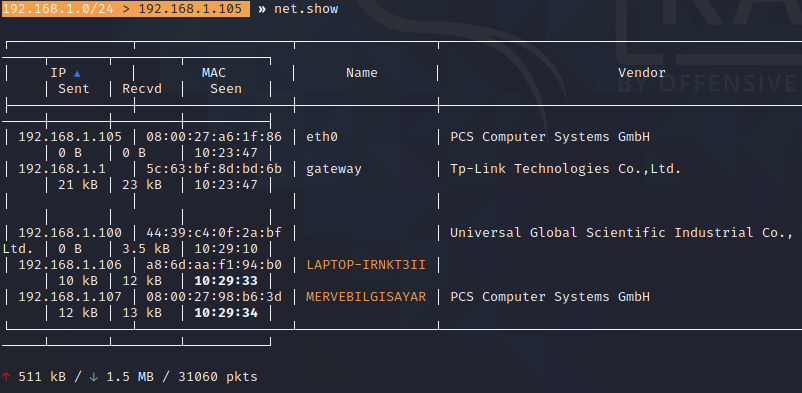
İki tane bilgisayar ipsini tespit etti biz MERVEBILGISAYAR a saldırı yapacağız.Windows 7 nin ipsini 192.168.1.107 diye tespit etmiş oldu.

Tekrar help yazarak aktif modülleri görüyoruz.



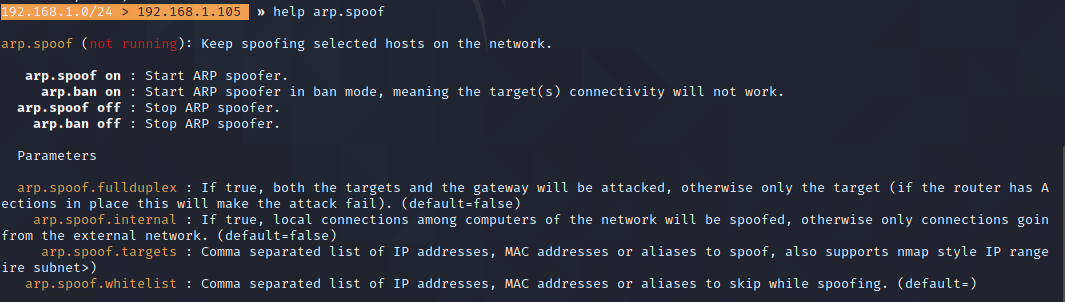
net.probe ile birlikte net.recon da çalışmaya başladı.

Ağda kimlerle etkileşime girebileceğimizi görmek için terminale net.show yazıyoruz.



192.168.1.105 Kali-Linux un ip adresi.192.168.1.106 aynı ağdaki başka bir bilgisayarın ip adresi.192.168.1.107 aynı ağdaki saldırı yapacağımız windows 7 nin ip adresi.

Arp saldırısı yapmak için arp.spoof modülünü çalıştırmamız gerekir.Bu modülün birkaç paremetresi var ayarlanması gereken o yüzden terminale help arp.spoof yazıyoruz.Modülün içeriğini böylelikle görebiliyoruz.



Değiştirmemiz gereken iki tane paremetre var.Birtanesi arp.spoof.fullduplex parametresi diğeri arp.spoof.targets paremetresi.

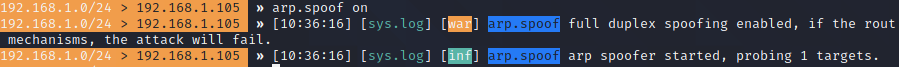
arp.spoof.fullduplex i falseden trueya çevirmemiz gerek.Çevirmezsek bizim üzerimizden cihaza internet gitmeyecektir.Aşağıda görüldüğü gibi trueya çevrilir:



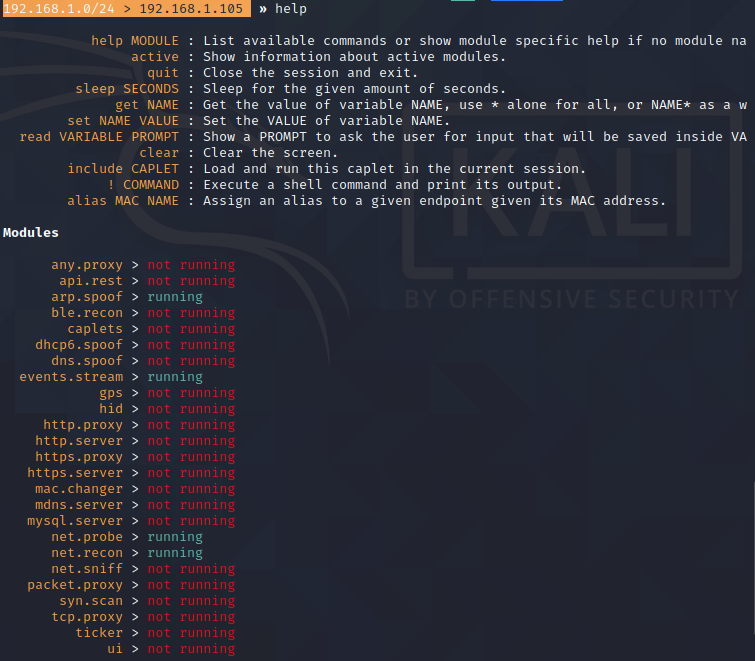
Aşağıdaki şekilde saldırı yapacağımız hedefin ip adresini yazıyoruz:



Aşağıdaki gibi arp.spoof on yazarak arp saldırımızı başlatıyoruz.



Tekrardan help yazarak arp.spoof modülünün de aktif olduğunu görüyoruz.

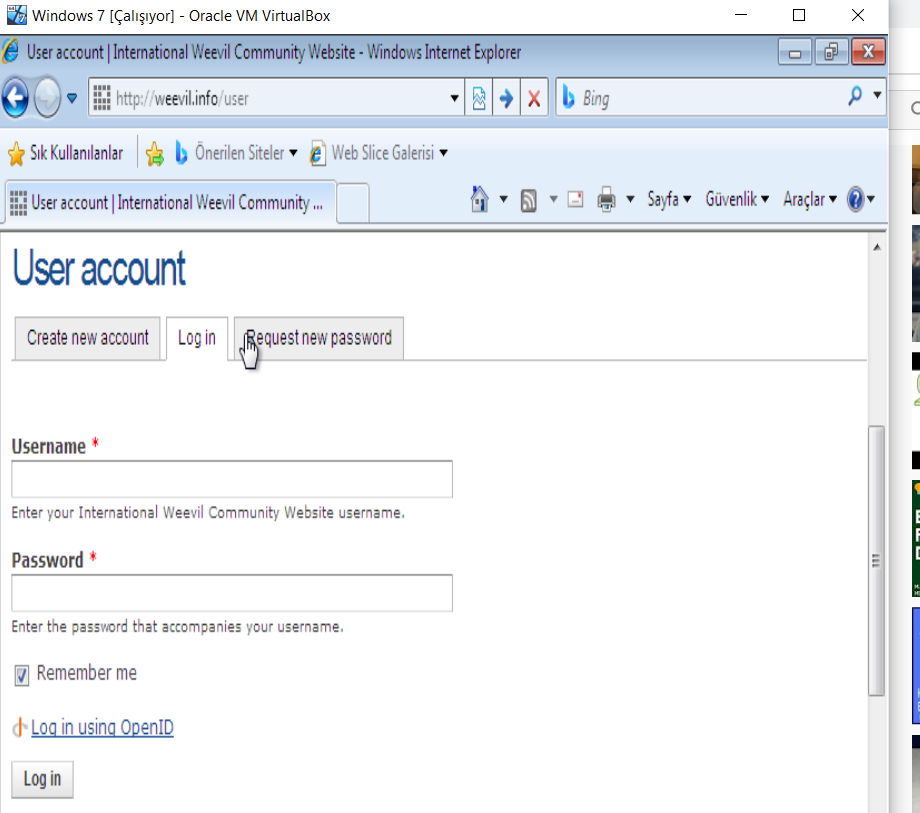


Son olarak net.sniff modülünü aktif ederek ağda olanları izleyebileceğiz.Aktif etmek için terminale net.sniff on yazıyoruz.



Artık tüm gelen giden bağlantıları görebileceğiz.

Windows 7 den internete giriyoruz.Browserı açar açmaz paketler gelmeye başlar.Örnek olarak bir siteye girdik ve username ile password kısmını dolduracağız.



Username kısmına merve,password kısmına 123456 yazdım ve logine bastım.

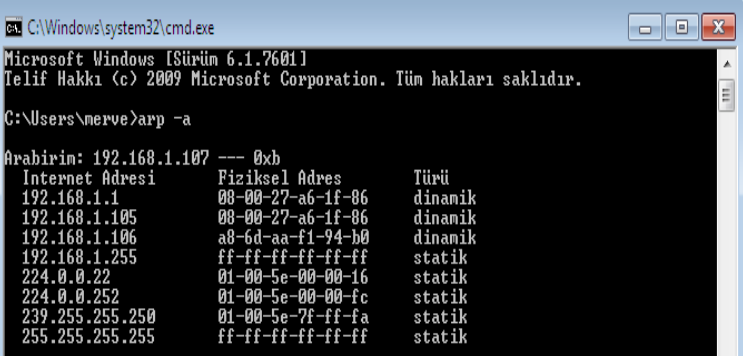
Kali-Linux terminalinde bir çok paketle karşılaşıyoruz.Aşağıda giriş için yazdığımız bilgilerin aynısı da görüldüğü gözükmektedir.



Windows 7deki kullanıcının bilgilerini böylece ele geçirmiş olduk.

Httplerde bu şekilde bilgileri çekebiliriz.Httpste ise https açılan siteyi httpye düşürüp kullanıcıya öyle sunuyoruz ve http üzerinden bir bağlantı sağlandığı için yine aynı bilgileri çekiyoruz.

Bu saldırıya uğradığımızı programsız anlayabilmek için cmdye arp -a yazıyoruz.Örneğin aşağıdaki gibi Windows 7 de yazdık.



192.168.1.1(Gateway) ile 192.168.1.105 ipli bir cihazın(Kali-Linuxun) mac adresleri aynı.Bu da demek oluyorki benim cihazım 192.168.1.105 ipli cihazı modem olarak görüyor,veriyi sürekli olarak oraya gönderiyor.Ve 192.168.1.105 ipli cihaz bu verileri asıl modeme gönderiyor.Ve ortadaki adam olunduğu bu şekilde anlaşılıyor.

Bu saldırıdan korunma yolları:

* Zehirlenmeyi algılayan ve önleyen yazılımlar kullanılmalıdır.
* Güçlü bir güvenlik duvarı kullanılmalıdır.

Password Attack

Parolalar, kullanıcıları bir bilgi sistemine doğrulamak için en sık kullanılan mekanizma olduğundan, parola almak yaygın ve etkili bir saldırı yaklaşımıdır.

Bir kişinin şifresine erişim, kişinin masasının etrafına bakarak, şifrelenmemiş şifreleri elde etmek için ağ bağlantısını "koklayarak", sosyal mühendisliği kullanarak, bir şifre veritabanına erişerek veya doğrudan tahmin ederek elde edilebilir.

Password atağın Brute Force türünden bahsedeceğiz.

BRUTE-FORCE

Müşteriler tarafından e-ticaret siteleri üzerinden alışveriş gerçekleştirilmek istendiğinde genelde kullanıcı girişi yapılması gerekiyor. Bir kullanıcı adı ve şifreyle sağlanan girişlerde önceden tanımlı adres, isim-soy isim, e-posta adresi, bazen de önceden tanımlı kredi kartı bilgilerini içeren kullanıcı hesabı ile hızlıca alışveriş gerçekleştirilebiliyor. Kritik önem taşıyan kritik önem taşıyan bu verilere brute force saldırısı ile ulaşılabilir.

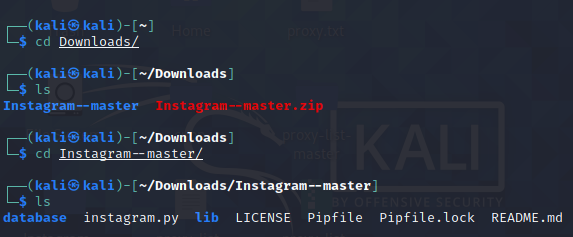
Bir brute-force (kaba kuvvet) saldırısı,bir hesaba erişebilmek için deneme-yanılma yöntemi kullanılmasına denir. Bu, duruma bağlı olarak şifre kırılmasını içerebilir.

Brute-force(kaba kuvvet) şifre tahmini, farklı şifreler deneyerek rastgele bir yaklaşım kullanmak ve bir işin umuduyla çalışmak anlamına gelir.Kişinin adı, iş unvanı, hobileri veya benzer öğeleriyle ilgili şifreler denenerek uygulanabilir.

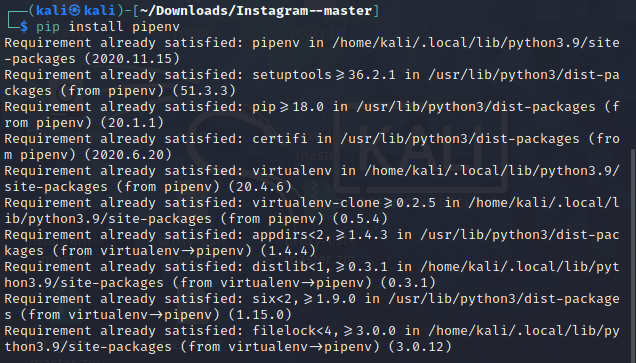
Aşağıda BRUTE-FORCE saldırısının nasıl yapıldığı adım adım anlatılmıştır:

İlk olarak İnstagram Bruter indiriyoruz.İnstagram Bruter sayesinde şifreler teker teker denenecek ve şifreler eşleşirse saldırımız başarılı olacak eşleşmezse saldırımız başarısız olacak.Bu programın dezavantajı bayağı uzun sürmesidir.

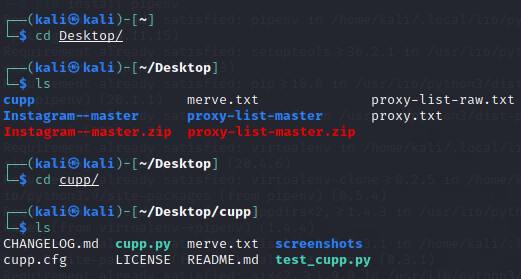
İnstagram Bruter Downloads klasörünün içinde olduğu için ilk başta Downloads klasörüne gitmemiz gerekiyor.Bunun için cd Downloads/ yazıyoruz.ls yazarak Downloads klasörünün içindeki dosyaları görebiliyoruz.Bu dosyalardan Instagram- -master dosyasının içine girmek istiyoruz.Bunun için terminale cd Instagram- -master yazıyoruz.İçindekileri görmek için ls yazıyoruz.



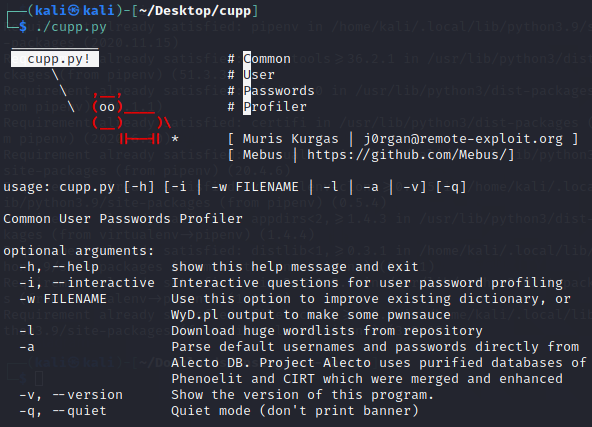
İçinde instagram.py denilen bir dosya var fakat bu çalışır durumda değil.İnstagram Bruterı indirdiğimiz yerde kurulum gereksinimleri yazan yerdeki yazıyı kopyalayıp terminale yazarak indiriyoruz..Bu yazı pythonu kullanaraktan gerekli kurulum dosyalarının kurulmasını sağlıyor.



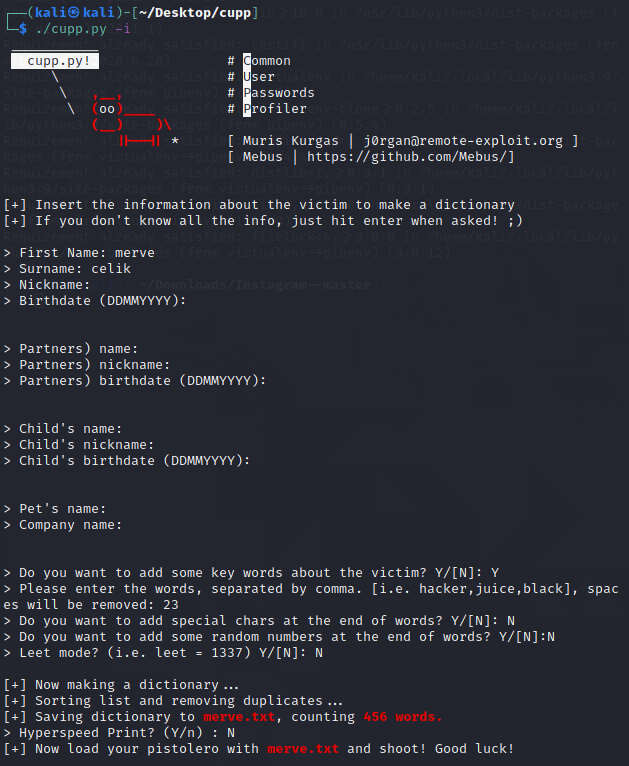
Saldırı yapabilmemiz için bir wordlist oluşturmaya ihtiyacımız var.Bunun için cupp-masterı indirdik.Yeni bir terminal açıyoruz.Masaüstüne gitmek için cd /Desktop yazıyoruz.Ardından ls yazarak masaüstünün içini görüyoruz.cupp dosyasının içine girebilmek için cd cupp/ yazıyoruz.ls yazarak bu dosyanın içindekileri görüyoruz.



./cupp.py yazarak cupp.py dosyasını çalıştırıyoruz.

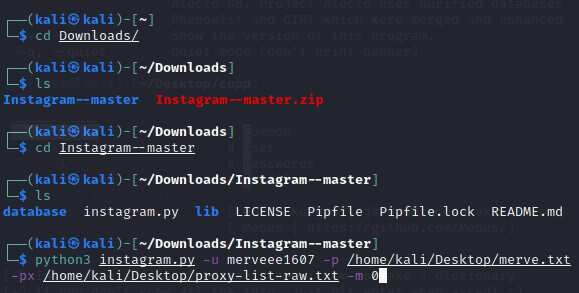


İnteractive modunu kullanacağız.Bunun için ./cupp.py -i yazıyoruz.Denenecek şifrelerin oluşturulması için aşağıdaki sorulardan istediklerimizi yanıtlıyoruz.Özel karakter istemediğim için N yazıyorum.Random numaralarda istemediğim için N yazıyorum.

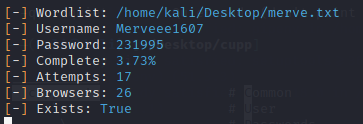


cupp içindeki merve.txt dosyasına 406 kelimeden oluşan bir wordlist oluşturdu.merve.txtye masa üstünden erişebilmek için masaüstüne kopyalıyoruz.

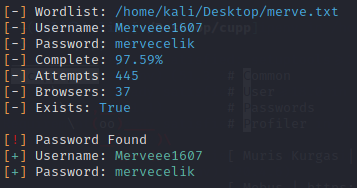
Terminali açıp cd Downloads/ yazıyoruz masaüstüne gitmek için.ls yazarak içini görüyoruz.cd Instagram- -master yazarak buraya gidiyoruz.ls yazarak Instagram- -masterın içindekileri görüyoruz.instagram.py yi çalıştırmak için python3 instagram.py merveee1607 /root/Desktop/merve.txt -m 0 yazıyoruz.Aşağıdaki gibi wordlistler okunmaya başlıyor ve saldırı başlıyor.



Aşağıda saldırı başladıktan kısa bir süre sonraki görüntü bulunmaktadır:



Aşağıda saldırı bittikten sonraki görüntü bulunmaktadır.



Görüldüğü gibi saldırımız başarıyla sonuçlanmıştır.Merveee1607 isimli kullanıcının şifresi mervecelik olarak bulundu. Ve siteye bu şifreyle giriş yapabiliyoruz.

Bu yöntemle şifremizin bulunamaması için aşağıda yazılanlara dikkat etmeliyiz.

* Web sitelerinde güvenlik eklenti/yazılımları yüklü ve aktif durumda olmalıdır.
* İki faktörlü kimlik doğrulama sistemi kullanılabilir.
* Daha uzun şifre tercihi.
* Sizinle ilgili olmayan (doğum yılınızı ya da tuttuğunuz takımı içermesi gibi) şifreler kullanılmalıdır.
* Kişisel bilgilerimizi içermeyen şifreler kullanılmalıdır.
* Sosyal medya ve çeşitli platformlarda (forumlar, vb) gerektiğinden fazla bilgi paylaşılmaması gerekir.
* Sosyal medyadaki gizlilik ayarlarında tanınmayan kimselerin kişisel bilgileri görmesini bloke etmek.
* Şifreler ardışık sayılardan ve harflerden oluşmamalıdır.
* Büyük-küçük harf, özel karakter, alfanümerik şifre kombinasyonları kullanılmalıdır.
* Belirli sayıda hatalı giriş yapıldığı taktirde sonraki denemeyi bloklayıcı özellikler kullanılabilir.

Phishing Attacks

-Social Phishing Attack

Phishing saldırılarıyla kullanıcı hesap numaraları,kullanıcı şifreleri ve parolaları,kredi kartı numaraları,internet bankacılığında kullanılan kullanıcı kodu ve şifreleri gibi bilgilerin çalınması amaçlanıyor.

Oltalama alan adları, bankalar, e-ticaret siteleri vb. gibi şirketlerin gerçek sitelerinin kopyalarıdır. Kurban giriş bilgilerini (kullanıcı adı ve şifre) veya diğer önemli bilgileri girdiğinde, bu kopya siteden gerçek siteye yönlendirilir.

E-posta yöntemini kullanan dolandırıcılar burada da kullanıcıları farklı şekillerde aldatma yoluna giderler:

**a)** E-postanıza devamlı temas halinde olduğunuz kuruluşlardan gönderiliyormuş izlenimi verilen sahte bir e-posta gönderiliyor. Bu e-postalarda kullanıcıya kurumun web sitesine gitmesinin gerektiği, şifresinin süresinin dolduğu söylenir ve altta o sayfaya yönlendirileceği bir link (bağlantı) verilir. Dolandırıcı daha önceden hazırladığı ve kuruluşun sitesinin aynısı veya benzeri olan bu siteye kullanıcıyı getirdikten sonra, ondan şifreyi girmesini ister. Dolandırıcı bu şifreyi kullanarak internet aracılığı ile para transferi, e-ticaret, sizin adınıza bağış toplama, reklam gönderme, çok sayıda spam mesaj gönderme vb. işler yapabilir.

**b)** Bazı e-postalarda ise; bir yarışma düzenlendiği ve bu yarışmaya katılması teklif edilen kullanıcılara ödül olarak bir ürün kazandıkları ancak gerekli kişisel bilgileri vermeleri gerektiği söylenir. Bu gibi durumlarda bilgilerini veren kullanıcının tüm bilgileri dolandırıcının eline geçer.

**c)** Bir başka kullanılan teknikte ise; gelen e-postada müşteriye kişisel bilgilerini güncellemesi gerektiği, tüm bilgileri tekrar girmesi bunun kendileri açısından daha iyi hizmet verebilmeleri için gerekli olduğu söylenir.

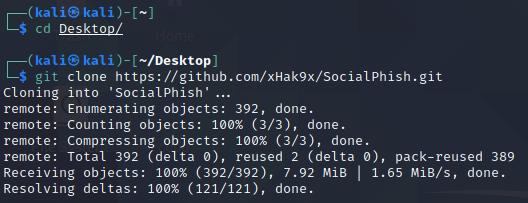
**d)** Bir başka teknikte ise; gelen e-postada kullanıcının e-posta kotasının dolduğu, eğer bilgilerini güncellemezse hesabının kapatılacağı söylenir.

**e)**Son zamanlarda bazı bankaların başlatmış oldukları ve cep telefonları ile para transferine imkân veren sistem kullanılarak banka müşterilerine sanki kendi hesaplarına para gönderilmiş veya alınmış gibi gösterilip sahte banka sitesi linki (bağlantı yolu) verilerek bu paranın tahsil edilebilmesi için bilgi güncelleştirmesi istendiği bilinmektedir.

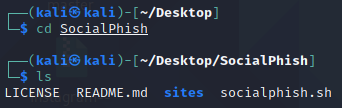
Bir bilgisayar korsanı sahte bir uygulama giriş sayfası oluşturduğunda uygulamaya yapılan kimlik avı saldırısı başlar. Kullanıcıları kandırmak için, bu sahte sayfalar olabildiğince gerçek siteye benzeyecek şekilde tasarlanmıştır. Bir kullanıcı uygulama kullanıcı kimliğini ve şifresini sahte sayfaya verdiğinde, bu kimlik bilgileri saldırgan tarafından ele geçirilir. Kullanıcı, gerçek kimlik doğrulaması için genellikle gerçek uygulama oturum açma sayfasına yeniden yönlendirilecektir. Ancak hasar çoktan verilmiştir. Kullanıcıların uygulama kimlik bilgileriyle saldırgan, hesaba tam erişime sahiptir. (Kullanıcı aynı kimlik bilgilerini diğer sosyal medya siteleri için veya daha kötüsü banka hesabı için de kullanıyorsa, saldırgan potansiyel olarak bunlara da erişebilir. )

Aşağıda SPEAR PHİSİNG saldırısının nasıl yapıldığı adım adım anlatılmıştır:

Masaüstüne gitmek için cd /Desktop yazıyoruz.Ardından terminalimize git clone yazıp yanına <https://github.com/xHak9x/SocialPhish.git> linkini kopyalayıp yapıştırıyoruz.Masaüstümüze dosya iniyor.



Terminale cd SocialPhish yazarak dosyanın içine giriyoruz.ls yazıp dosyanın içindekileri görüyoruz.

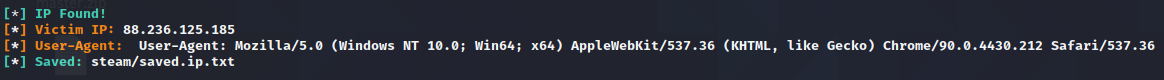


Socialphish.sh yi başlatmamız gerekiyor.Bunun için terminale bash socialphish.sh yazıyoruz.Karşımıza çıkan site isimlerinden hangisini kopyalamak istiyorsak onun numarasını yazıyoruz.Ben steam istediğim için 11 yazıyorum.Ardından iki hizmet çıkıyor karşımıza.Ngrok hizmetini yüklemek istediğim için 2 yazıyorum.



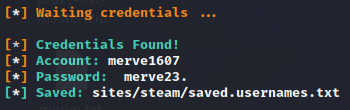
Karşımıza çıkan iki linkide kullanabiliyoruz.

Linki kopyalayıp internette açtığımızda steam sayfası gibi görünen sayfa açılıyor.Bu sayfayı kim açtıysa terminalimizde o kişinin hem ip adresini hem de işlettiği sistemin özelliklerini gösterir.Bilgiler steam/saved.ip.txt dosyasına yazılır.



Giren kişi username ve password kısmını doldurdup sign in butonuna bastıktan sonra o kişi steam sitesinin anasayfasına yönlendirilir.

Bizim terminalimize giriş tuşuna basan kişinin bilgileri account ve password şeklinde gelir.



Böylelikle merve1607 adlı kullanıcının şifresini öğrenmiş olduk ve saldırımız başarıyla gerçekleşti.

Bu saldırıdan korunma yolları:

* Kişisel bilgilerinizi isteyen e-postalara yanıt vermeyin.
* Gelen e-postanın kimden geldiğinden emin değilseniz dikkate almayınız. Unutmayın hiç bir kurum veya kuruluş e-posta yoluyla sizden kişisel bilgilerinizi istemez.
* Şüpheli gördüğünüz e-postalardaki URL linklerini tıklamayın.
* E-posta mesajlarındaki kısaltılmış URL linklerine ( bit.ly,ow.ly, tinyurl.com, is.gd, goo.gl, tiny.cc, cli.gs vb.) kesinlikle tıklamayın.
* Şüpheli veya bilmediğiniz web sitelerine kişisel bilgilerinizi vermeyin.
* Kişisel bilgilerinizi girmek için banka, kredi kartı ve servis sağlayıcılarının web sitelerini ziyaret ettiğinizde, web sitesinin URL’sini internet tarayıcınıza doğrudan yazın.
* Güvenli olan sitelerde bile çevrimiçi olarak bir formu doldurmadan önce, sitenin üçüncü kişilerle bu bilgileri paylaşıp paylaşmadığını belirten gizlilik anlaşmasının olup olmadığını kontrol edin.