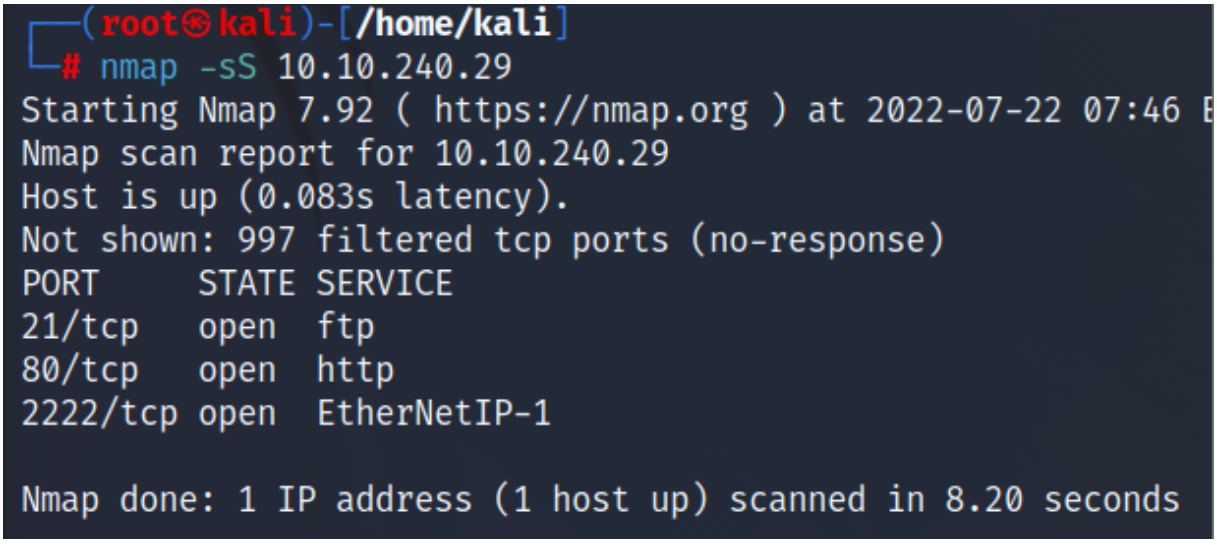
SIMPLE CTF WRİTEUP

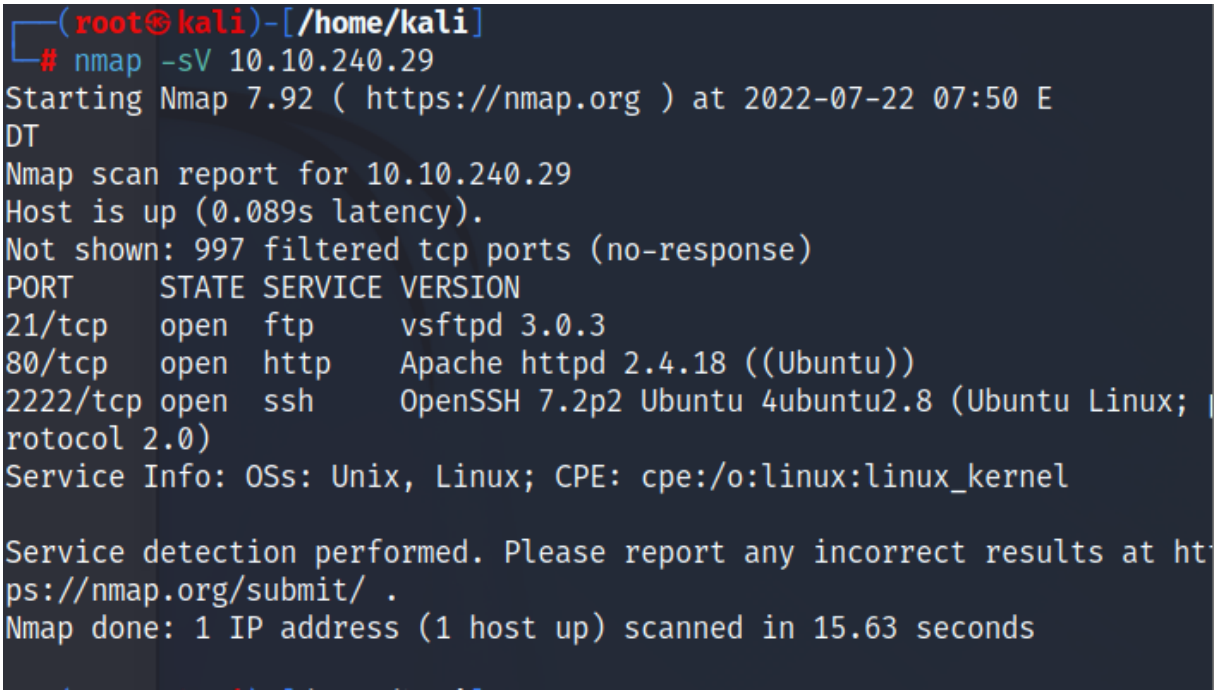
Odaya ilk girildiğinde sorulara kısaca baktığımızda NMAP, Gobuster gibi toolları çalıştırmakta fayda olduğunu görüyoruz. Nmap açık portları ve portların numaralarını görmede, işletim sistemi ve versiyonlarını ve kullanılan servisleri görmekte yardımcı olan bir tooldur.

Nmap -h ile parametreleri görmek için kullanabilirz. Burada 1000 in altında kaç port var göreceğiz

-sS tcp syn ile 1000'in altında iki tane port olduğunu gördük 22 ve 80. Portlar.



-sV hem açıkları hem servisleri gösteriyor artı versiyonlar işletim sistemleri de var. -v kullanırsak detaylandıracaktır.



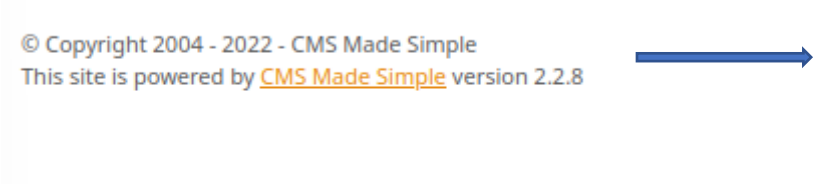
-sV ikisini de Verdi hem açık portlar hem servisler -sS sadece açık portları verdi . Root privilege istiyor. Çünkü NULL, Stealth SYN Scan ve diğerleri gibi bazı gelişmiş port tarama özellikleri, Nmap'in size kullanılabilir sonuçlar vermesi için ham paket verilerine erişmesi gerektiğinden yalnızca kök ayrıcalıklarıyla çalışabilir.8

CVE nin kodları var cve-2019-9053 gibi bunlar zafiyetlerin system versiyonlarına bağlı id leri. Ben şimdi gobuster ile sitenin alt sayfalarına girebilmem lazım . gobuster bir tane txt kullanıyo common txt ile bana alt sayfaları Verdi birinde versiyonunu veren bir sayfa buldum 2.2.8 cmd yazınca cve de aratınca id ler çıktı cve-2019-9053 kodu bu zafiyet ile uyuşuyor. SQL İnjection zafiyeti olduğunu görüyorum.

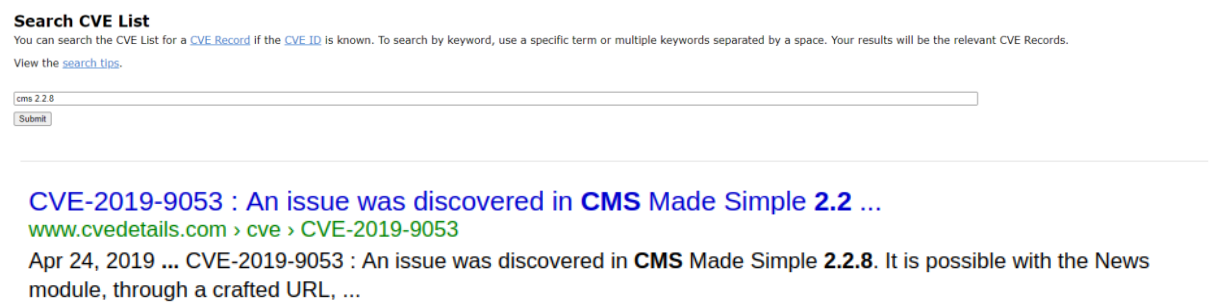
```
┌──(root㉿kali)-[/]
└─# gobuster dir -u http://10.10.240.29 -w ./usr/share/dirb/wordlists/common.txt

===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.240.29
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                ./usr/share/dirb/wordlists/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/07/22 08:31:54 Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 291]
/.htpasswd            (Status: 403) [Size: 296]
/.htaccess            (Status: 403) [Size: 296]
/index.html           (Status: 200) [Size: 11321]
/robots.txt           (Status: 200) [Size: 929]
/server-status        (Status: 403) [Size: 300]
/simple               (Status: 301) [Size: 313] [--> http://10.10.240.29/simple/]

===============================================================
2022/07/22 08:32:32 Finished
===============================================================
```

Yukardaki simple sitesine girdim. Aşağıya bıraktığım versiyonu kullandığını gördüm.

Burada cve sitesindeki aşağıda gördüğümüz kısmında version ile birlikte arama yapıyoruz.



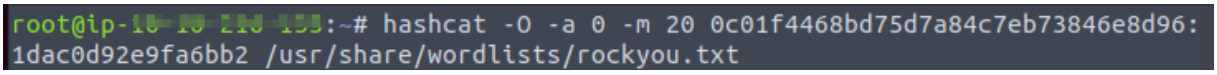
Simple sitesinde herhangi bir sayfasında bulabileceğimiz version ve sürümün verildiği kısım



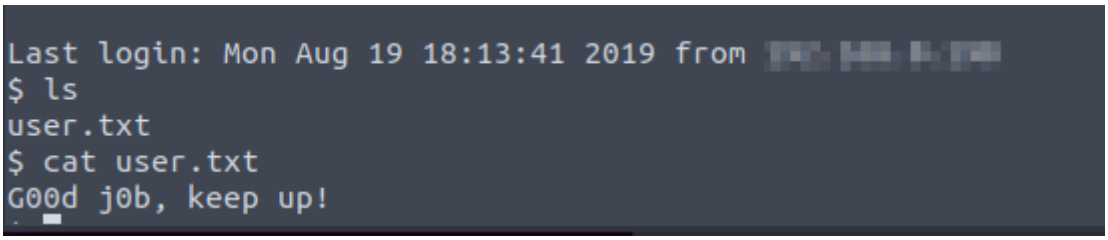
Bir tek simple ve robots çalıştığını görmüştük sitelerden. CVE' de bulduğumuz zafiyetli kodu indiriyoruz ve aşağıdaki şekilde çalıştırıyoruz. (pythonun kullandığı gerekli kütüphaneler yüklü değil ise "pip install" komutu ile gerekli kütüphaneleri indirip çalıştırmanız gerekebilir)

Zafiyetli python kodunu çalıştıracağız ve sonuçlara bakacağız.

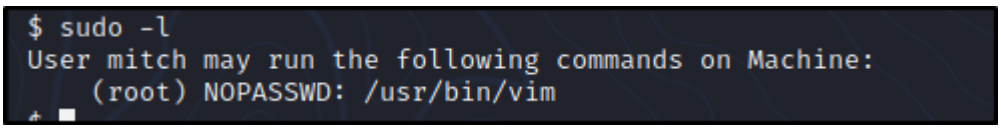
Sonuçlar bize flagleri veriyor. Fakat password şifrelenmiş şekilde burada hashcat toolunu kullanacağız. Bu tool hash algoritmalarına optimize çalışır ve decode eder. Hash algoritmaları parolaları şifreler. Burada bize kullanılacak wordlist gerekiyor, rockyou.txt kullandık. Böylece hash'li kodu decode edeceğiz.



Şifreyi bulduk. Şimdi SSH ile bağlantı kuracağız. Adresi de python çıktısından almıştık. User.txt dosyasını görebilmek için bağlantı kurduktan sonra "ls" komutunu çalıştırdık, okuyabilmek için ise "cat" komutunu çalıştırdık ve diğer flag de buradan geliyor



Pwd komutunu çalıştırarak nerde olduğumu görüyorum sonra kullanıcıların olduğu dizine kadar iniyorum ve iki kullanıcı olduğunu görüyorum mitch and sunbath. Diğer sorunun cevabının sunbath olduğunu görüyorum.



Hangi kullanıcıda olduğumu görmek için üstteki komutu çalıştırıyorum. Kullanıcı mitch usr/bn/vimde çalışıyomuş bunu gördüm. Yetki yükseltmek için sudo vim komutu ile ssh da çalıştırıyoruz. Cevap vim

Sudo vim -c ‘:!/bin/sh’ komutu ile cd /root yapıyoruz sonra dosyaları görmek için ls diyoruz. Root.txt çıkıyor. Bir sonraki flag de burada.