SMB Servisi Üzerinden İşletim Sistemi Tespiti

SMB Windows işletim sistemlerinde cihazların birbirleriyle olan dosya paylaşımından sorumlu bir servistir. Bu servis Windows'un yerel ürünü olsa da ayrıca linux ve mac os x de de kullanıldığından dosya paylaşımı platformlar arasında gerçekleştirilebilmektedir. SMB servisi 445. portta çalışır.

> nmap 192.168.2.206 // WinXP (Dandik) IP Numarası

Output:

Port	State	Service
…	…	…
445/tcp	open	microsoft-ds
…	…	…

Bu servis üzerinden hedef sistemin işletim sistemini tespit etmek mümkündür. Böylece hedef sisteme saldırmak için gerekli exploit ve payload seçimimiz kolaylaşır. Metasploit'te SMB üzerinden hedef OS'u tespit etmenin yolu şu şekildedir:

> use auxiliary/scanner/smb/smb_version

> set RHOSTS 192.168.2.206 // WinXP (Dandik) IP Numarası

> setg SMBDirect false

> run

Output:

[*] 192.168.2.206:445 is running Windows XP SP2 (language:Turkish)
(name:PENTEST-WINXP) (domain: PENTEST-WINXP)

[*] Scanned 1 of 1 hosts (100% complete)

[*] Auxiliary module execution completed

Görüldüğü gibi işletim sistemi türü (XP) ve versiyonu (SP2) tespit edilebilmiştir. Bir de Ubuntu'yu tespit edebiliyor muyuz ona bakalım:

> nmap 192.168.2.201 // Ubuntu'nun IP Numarası

Output:

Port	State	Service
…	…	…
445/tcp	open	microsoft-ds
…	…	…

> use auxiliary/scanner/smb/smb_version

> set RHOSTS 192.168.2.201 // Ubuntu IP Numarası

> setg SMBDirect false

> run

Output:

[*] 192.168.2.201 could not be identified: Unix (Samba 4.1.6 – Ubuntu)

[*] Scanned 1 of 1 hosts (100% complete)

[*] Auxiliary module execution completed

Görüldüğü üzere hedef sistemin Unix türevi bir Ubuntu olduğunu öğrenmiş olduk.

Yararlanılan Kaynak: https://github.com/rapid7/metasploit-framework/issues/4963