

Урок 4. Разведка 2.0

Задание 1:

Найдите в VM Metasploitable 3 (Linux) адрес страницы Login Page проекта Continuum.

(предварительно отключите межсетевой экран командой `iptables -F`, затем перезапустите continuum командой `service continuum restart`), который запущен на одном из кастомных портов. В ответе укажите адрес страницы.

Решение:

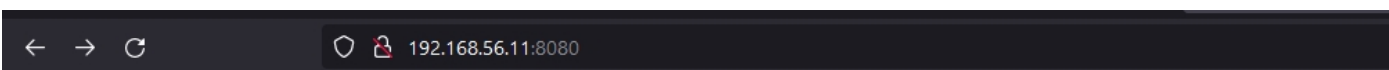
Прошёлся утилитой Nmap по серверу и нашёл несколько открытых портов (6697 не нашёл сразу почему-то).

```
root@kali: /home/kali
File Actions Edit View Help
Host is up (0.00022s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.3.5
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.11 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd
111/tcp   open  rpcbind      2-4 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp   open  ipp          CUPS 1.7
3306/tcp  open  mysql        MySQL (unauthorized)
6666/tcp  open  ftp          vsftpd 3.0.2
6667/tcp  open  irc          UnrealIRCd
8080/tcp  open  http         Jetty 8.1.7.v20120910
8181/tcp  open  http         WEBrick httpd 1.3.1 (Ruby 2.3.7 (2018-03-28))
MAC Address: 08:00:27:EF:DD:09 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: UBUNTU, irc.TestIRC.net; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.14 seconds

(root@kali)-[/home/kali]
#
```

Через браузер зашёл на порт 8080 и увидел следующую страницу:

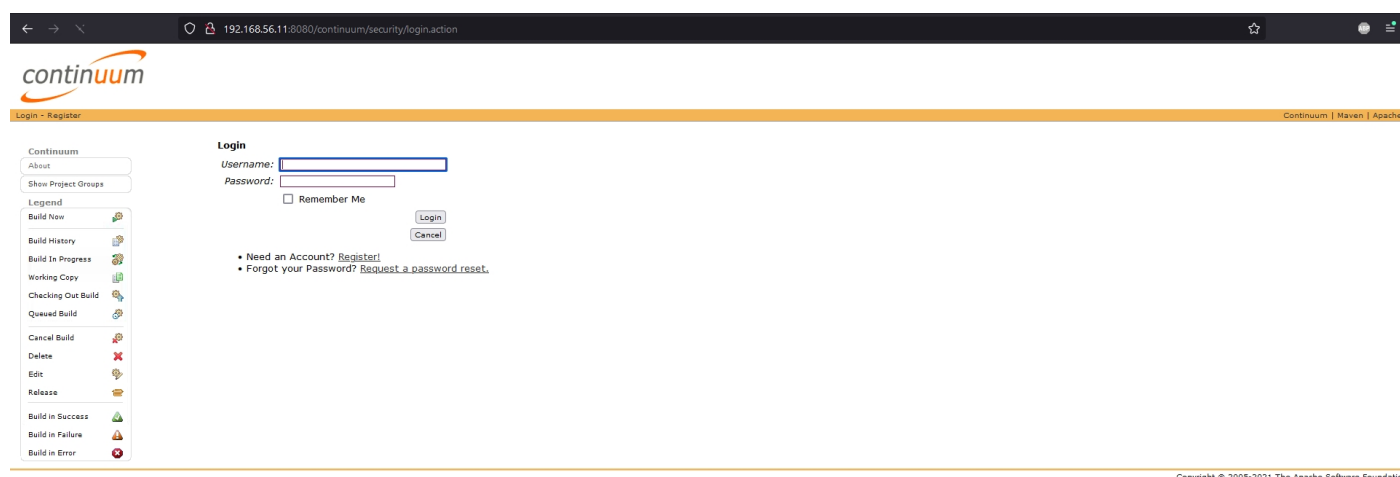


Error 404 - Not Found.

No context on this server matched or handled this request.
Contexts known to this server are:

- [/continuum ---> o.e.j.w.WebAppContext{/continuum_file:/opt/apache_continuum/apache-continuum-1.4.2/apps/continuum/}./apps/continuum](#)

Ссылка на этой странице как раз ведет на страницу авторизации Login Page проекта Continuum.



Задание 2:

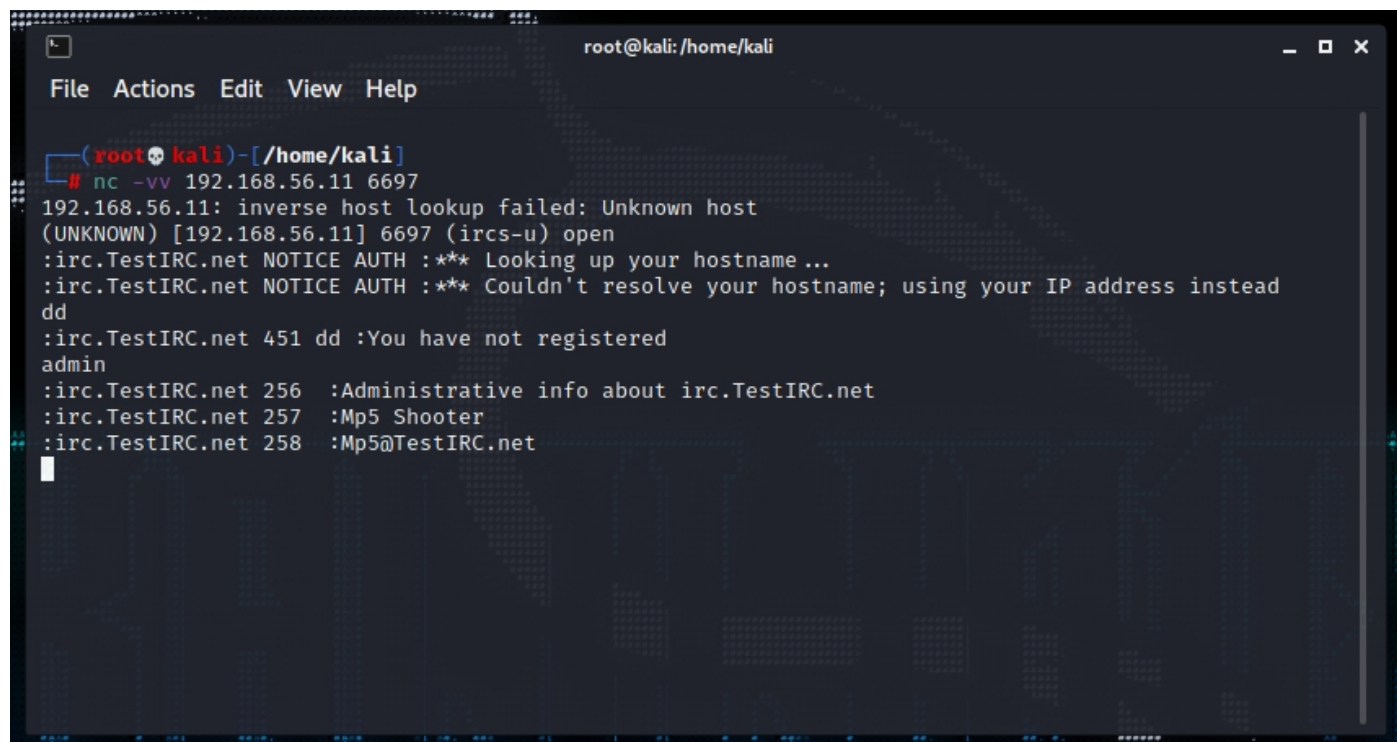
Какой сервис запущен на порту 6697 в VM Metasploitable 3 (Linux)?

Решение:

Прошёлся Nmap по серверу, обнаружил порт 6697,

```
kali@kali: ~  
File Actions Edit View Help  
-(kali@kali)-[~]  
$ sudo nmap 192.168.56.11 -p10-10000 -sV  
[sudo] password for kali:  
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-06 15:09 EDT  
Nmap scan report for 192.168.56.11  
Host is up (0.00053s latency).  
Not shown: 9981 filtered ports  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          ProFTPD 1.3.5  
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.11 (Ubuntu Linux; protocol 2.0)  
80/tcp    open  http         Apache httpd  
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
631/tcp   open  ipp          CUPS 1.7  
3000/tcp  closed ppp  
3306/tcp  open  mysql        MySQL (unauthorized)  
3500/tcp  open  http         WEBrick httpd 1.3.1 (Ruby 2.3.7 (2018-03-28))  
6697/tcp  open  irc          UnrealIRCd  
8181/tcp  open  http         WEBrick httpd 1.3.1 (Ruby 2.3.7 (2018-03-28))  
MAC Address: 08:00:27:EF:DD:09 (Oracle VirtualBox virtual NIC)  
Service Info: Hosts: UBUNTU, irc.TestIRC.net; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 38.90 seconds
```

На этом порту работает IRC чат, на сколько я понял.



```
root@kali: /home/kali
File Actions Edit View Help
(root@kali)-[/home/kali]
# nc -vv 192.168.56.11 6697
192.168.56.11: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.56.11] 6697 (ircs-u) open
:irc.TestIRC.net NOTICE AUTH :*** Looking up your hostname ...
:irc.TestIRC.net NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
dd
:irc.TestIRC.net 451 dd :You have not registered
admin
:irc.TestIRC.net 256 :Administrative info about irc.TestIRC.net
:irc.TestIRC.net 257 :Mp5 Shooter
:irc.TestIRC.net 258 :Mp5@TestIRC.net
```

А понял я это из этой статьи:

DDoS Perl IrcBot v1.0 анализ, воспроизведение и удаление

Предисловие

Недавно я столкнулся с бэкдором IRC на основе PERL. Я взаимодействовал с жертвой через протокол IRC. После простого анализа была создана среда для воспроизведения процесса работы бэкдора и подробного анализа его принципа и поведения. Цель состоит в том, чтобы на основе результатов анализа предложить некоторые бэкдоры, которые каждый мог бы изучить и использовать.

IRC

IRC - это английское сокращение от Internet Relay Chat, которое на китайском языке обычно называется Internet Relay Chat. Это протокол сетевого чата, впервые разработанный Финном Яркко Оикариным в 1988 году. После десяти лет развития более 60 стран мира в настоящее время предоставляют услуги IRC. Принцип работы IRC очень прост: вам нужно только запустить клиентское программное обеспечение на вашем ПК, а затем подключиться к IRC-серверу через Интернет по протоколу IRC. Он отличается очень высокой скоростью, почти без задержки при разговоре и занимает лишь небольшое количество ресурсов полосы пропускания. Все пользователи могут поговорить или тайно поговорить на тему в месте под названием "Канал". У каждого пользователя IRC есть псевдоним (ник).

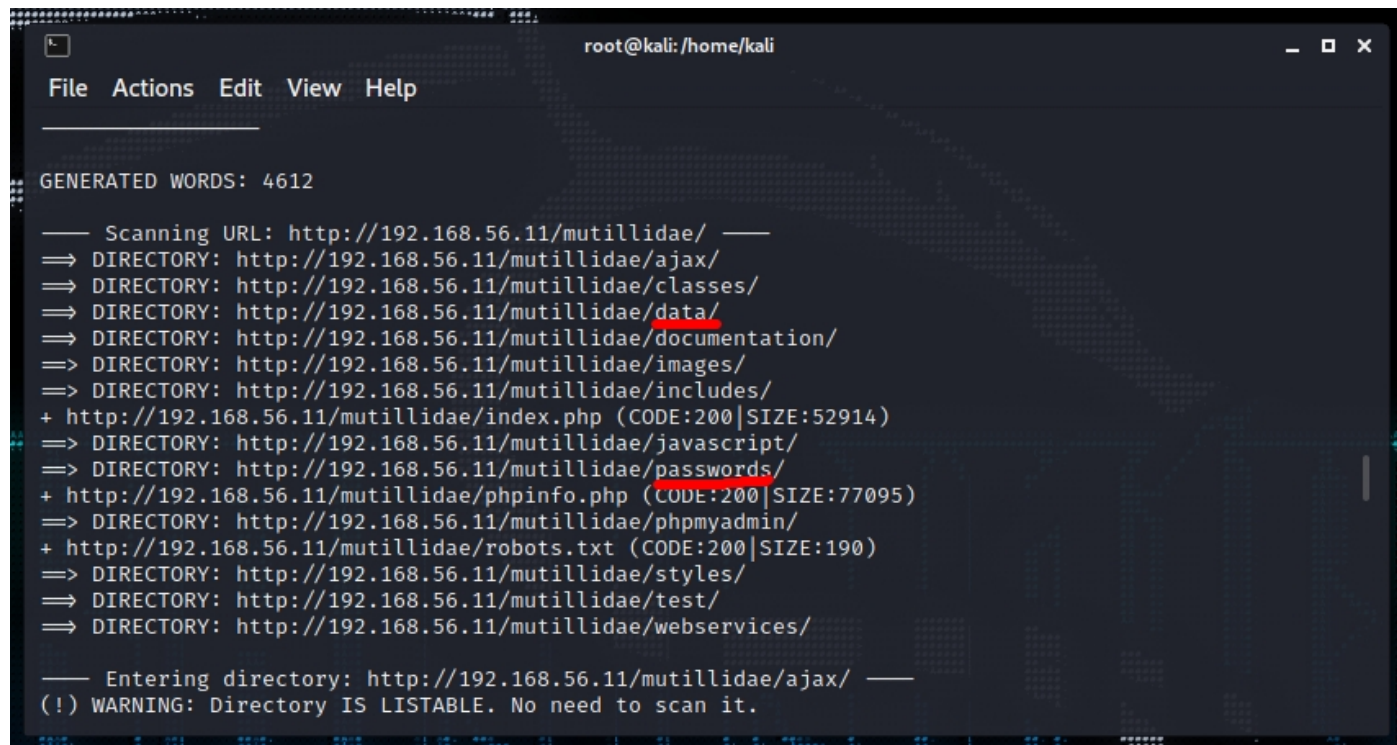
<https://russianblogs.com/article/4156850345/>

Задание 3:

Какой пароль пользователя tim из проекта mutillidae? В каком файле он содержится?

Решение:

Утилитой dirb нашёл несколько интересных каталогов:



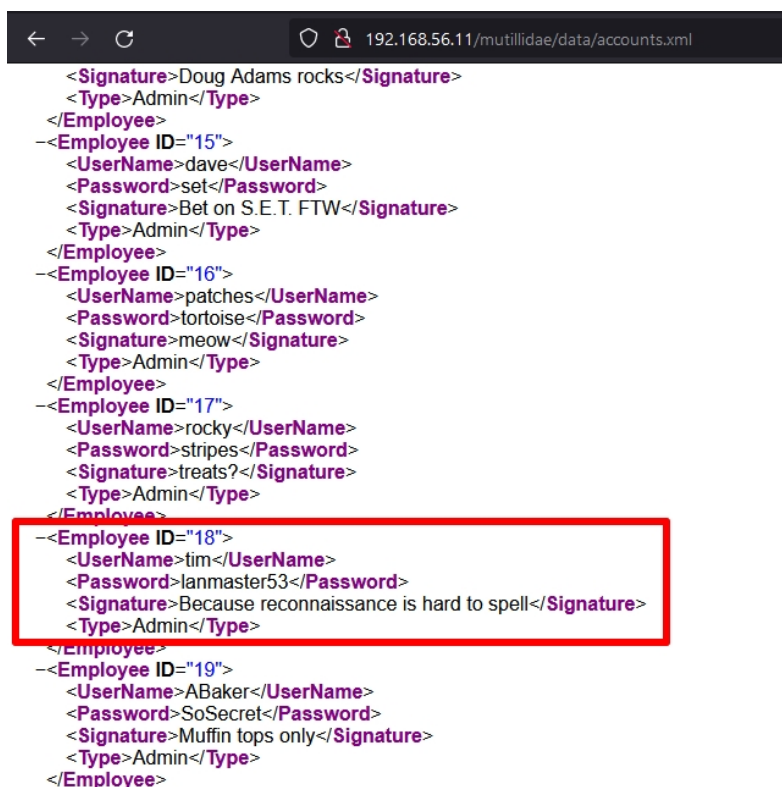
```
root@kali: /home/kali
File Actions Edit View Help

GENERATED WORDS: 4612

— Scanning URL: http://192.168.56.11/mutillidae/ —
=> DIRECTORY: http://192.168.56.11/mutillidae/ajax/
=> DIRECTORY: http://192.168.56.11/mutillidae/classes/
=> DIRECTORY: http://192.168.56.11/mutillidae/data/
=> DIRECTORY: http://192.168.56.11/mutillidae/documentation/
=> DIRECTORY: http://192.168.56.11/mutillidae/images/
=> DIRECTORY: http://192.168.56.11/mutillidae/includes/
+ http://192.168.56.11/mutillidae/index.php (CODE:200|SIZE:52914)
=> DIRECTORY: http://192.168.56.11/mutillidae/javascript/
=> DIRECTORY: http://192.168.56.11/mutillidae/passwords/
+ http://192.168.56.11/mutillidae/phpinfo.php (CODE:200|SIZE:77095)
=> DIRECTORY: http://192.168.56.11/mutillidae/phpmyadmin/
+ http://192.168.56.11/mutillidae/robots.txt (CODE:200|SIZE:190)
=> DIRECTORY: http://192.168.56.11/mutillidae/styles/
=> DIRECTORY: http://192.168.56.11/mutillidae/test/
=> DIRECTORY: http://192.168.56.11/mutillidae/webservices/

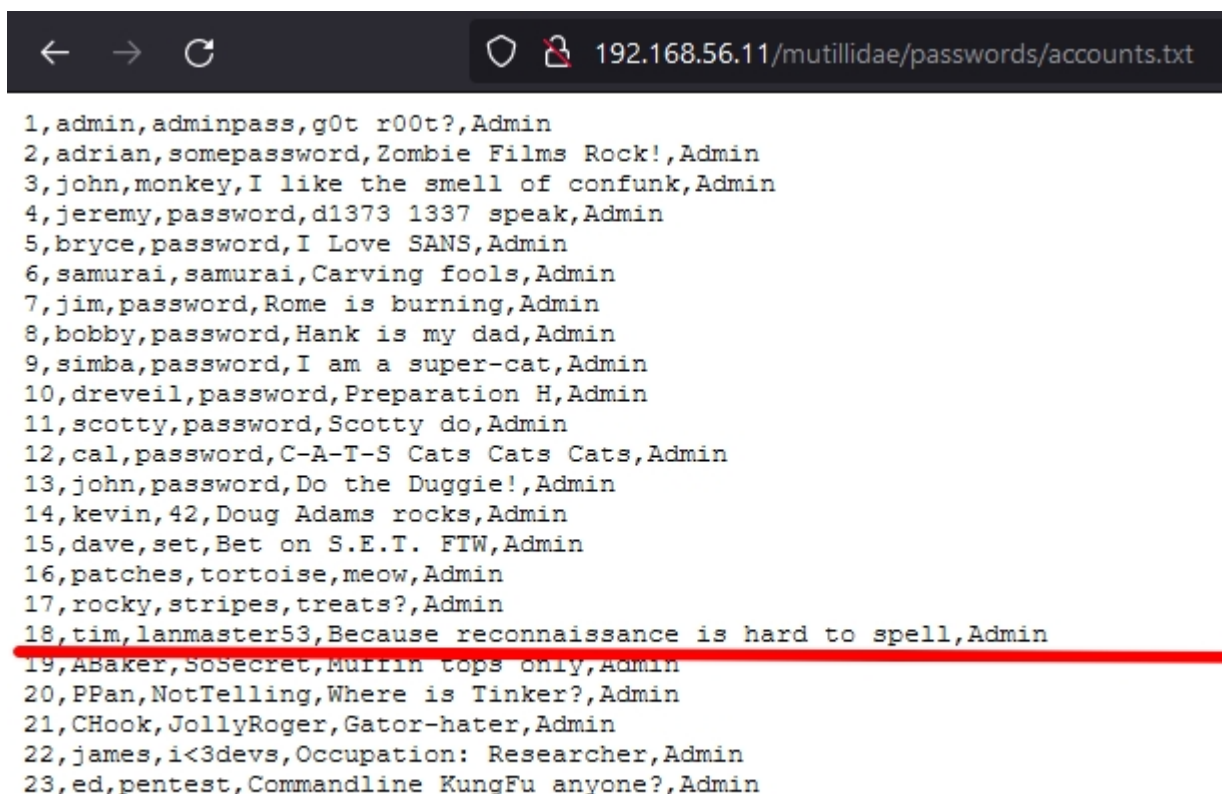
— Entering directory: http://192.168.56.11/mutillidae/ajax/ —
(!) WARNING: Directory IS LISTABLE. No need to scan it.
```

Содержимое каталога **data**:



```
<Signature>Doug Adams rocks</Signature>
<Type>Admin</Type>
</Employee>
-<Employee ID="15">
  <UserName>dave</UserName>
  <Password>set</Password>
  <Signature>Bet on S.E.T. FTW</Signature>
  <Type>Admin</Type>
</Employee>
-<Employee ID="16">
  <UserName>patches</UserName>
  <Password>tortoise</Password>
  <Signature>meow</Signature>
  <Type>Admin</Type>
</Employee>
-<Employee ID="17">
  <UserName>rocky</UserName>
  <Password>stripes</Password>
  <Signature>treats?</Signature>
  <Type>Admin</Type>
</Employee>
-<Employee ID="18">
  <UserName>tim</UserName>
  <Password>lanmaster53</Password>
  <Signature>Because reconnaissance is hard to spell</Signature>
  <Type>Admin</Type>
</Employee>
-<Employee ID="19">
  <UserName>ABaker</UserName>
  <Password>SoSecret</Password>
  <Signature>Muffin tops only</Signature>
  <Type>Admin</Type>
</Employee>
```

И содержимое каталога **passwords**:



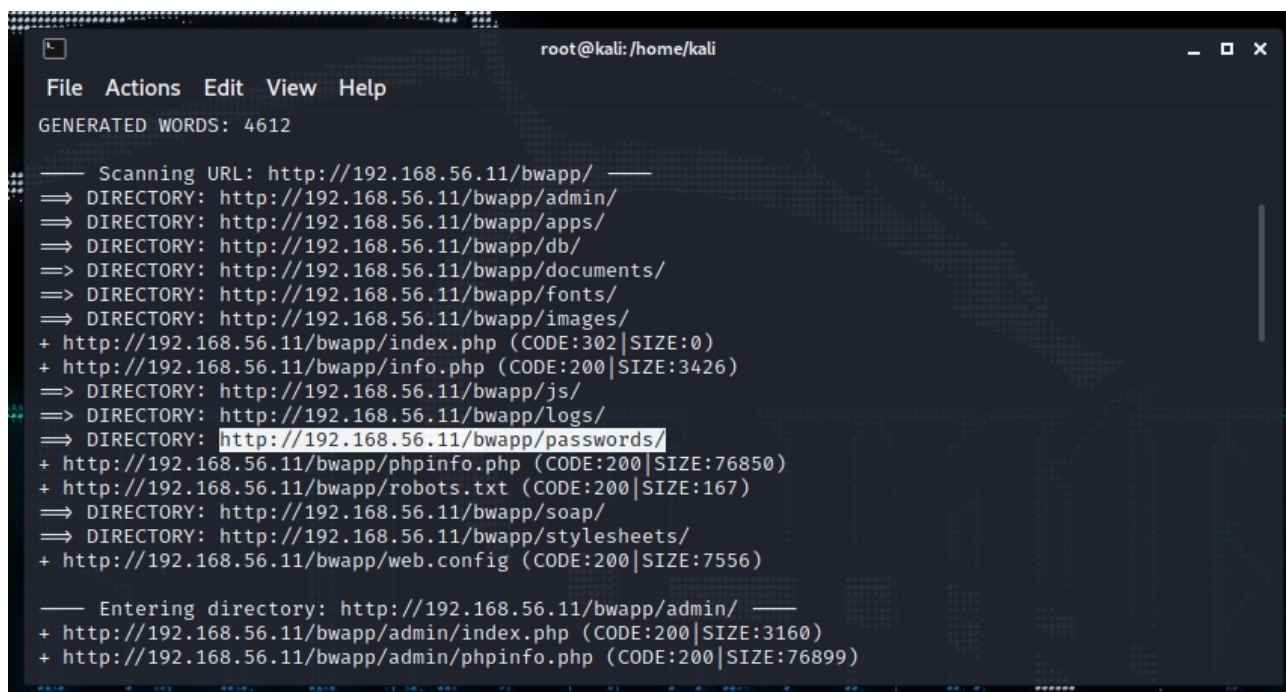
```
1,admin,adminpass,g0t r00t?,Admin
2,adrian,somepassword,Zombie Films Rock!,Admin
3,john,monkey,I like the smell of confunk,Admin
4,jeremy,password,d1373 1337 speak,Admin
5,bryce,password,I Love SANS,Admin
6,samurai,samurai,Carving fools,Admin
7,jim,password,Rome is burning,Admin
8,bobby,password,Hank is my dad,Admin
9,simba,password,I am a super-cat,Admin
10,dreveil,password,Preparation H,Admin
11,scotty,password,Scotty do,Admin
12,cal,password,C-A-T-S Cats Cats Cats,Admin
13,john,password,Do the Duggie!,Admin
14,kevin,42,Doug Adams rocks,Admin
15,dave,set,Bet on S.E.T. FTW,Admin
16,patches,tortoise,meow,Admin
17,rocky,stripes,treats?,Admin
18,tim,lanmaster53,Because reconnaissance is hard to spell,Admin
19,ABaker,s0secret,Murrin tops only,Admin
20,PPan,NotTelling,Where is Tinker?,Admin
21,CHook,JollyRoger,Gator-hater,Admin
22,james,i<3devs,Occupation: Researcher,Admin
23,ed,pentest,Commandline KungFu anyone?,Admin
```

Задание 4:

* В каком файле можно найти информацию о том, какой любимый фильм у юзера с именем selene (не является УЗ в bwapp)?

Решение:

Всё там же dirb прошёлся по bwapp и нашёл каталог passwords:



```
root@kali: /home/kali
File Actions Edit View Help
GENERATED WORDS: 4612

— Scanning URL: http://192.168.56.11/bwapp/ —
=> DIRECTORY: http://192.168.56.11/bwapp/admin/
=> DIRECTORY: http://192.168.56.11/bwapp/apps/
=> DIRECTORY: http://192.168.56.11/bwapp/db/
=> DIRECTORY: http://192.168.56.11/bwapp/documents/
=> DIRECTORY: http://192.168.56.11/bwapp/fonts/
=> DIRECTORY: http://192.168.56.11/bwapp/images/
+ http://192.168.56.11/bwapp/index.php (CODE:302|SIZE:0)
+ http://192.168.56.11/bwapp/info.php (CODE:200|SIZE:3426)
=> DIRECTORY: http://192.168.56.11/bwapp/js/
=> DIRECTORY: http://192.168.56.11/bwapp/logs/
=> DIRECTORY: http://192.168.56.11/bwapp/passwords/
+ http://192.168.56.11/bwapp/phpinfo.php (CODE:200|SIZE:76850)
+ http://192.168.56.11/bwapp/robots.txt (CODE:200|SIZE:167)
=> DIRECTORY: http://192.168.56.11/bwapp/soap/
=> DIRECTORY: http://192.168.56.11/bwapp/stylesheets/
+ http://192.168.56.11/bwapp/web.config (CODE:200|SIZE:7556)

— Entering directory: http://192.168.56.11/bwapp/admin/ —
+ http://192.168.56.11/bwapp/admin/index.php (CODE:200|SIZE:3160)
+ http://192.168.56.11/bwapp/admin/phpinfo.php (CODE:200|SIZE:76899)
```

Зашёл в него через браузер и нашёл там файл heroes.xml, в котором и была найдена нужная информация:

```
-<hero>
  <id>6</id>
  <login>selene</login>
  <password>m00n</password>
  <secret>It wasn't the Lycans. It was you.</secret>
  <movie>Underworld</movie>
  <genre>action horror sci-fi</genre>
</hero>
</heroes>
```

Задание 5:

- * Составьте правило (или набор правил) для mod_rewrite, при помощи которого можно заблокировать доступ утилиты curl на веб сервер ВМ.

Решение:

Настроил дефолтный конфигурационный файл в директории:

/etc/apache2/sites-available/000-default.conf

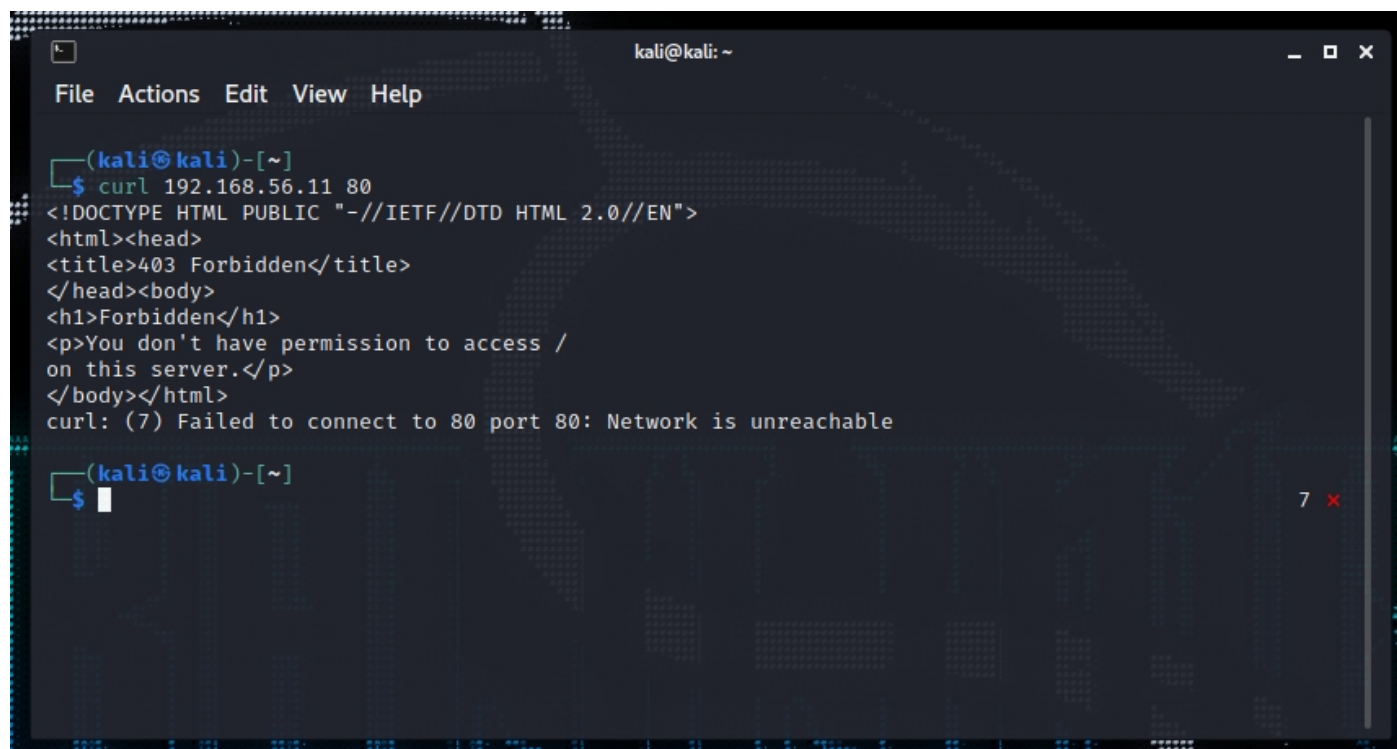
```
#####
<Directory /var/www/html>
Options Indexes FollowSymLinks
AllowOverride All
</Directory>
#####
#####
#####
</VirtualHost>
```

Далее командой **a2enmod rewrite** включил mod_rewrite, чтобы apache читал файл .htaccess.

Далее в директории /var/www/html я создал файл .htaccess и наполнил его следующим содержимым:

```
GNU nano 2.2.6      File: .htaccess
RewriteEngine on
RewriteCond %{HTTP_USER_AGENT} curl
RewriteRule ^.* - [F,L]
```

Теперь при попытке утилитой curl постучаться на сервер — будет 403 код ответа



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ curl 192.168.56.11 80  
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">  
<html><head>  
<title>403 Forbidden</title>  
</head><body>  
<h1>Forbidden</h1>  
<p>You don't have permission to access /  
on this server.</p>  
</body></html>  
curl: (7) Failed to connect to 80 port 80: Network is unreachable  
(kali@kali)-[~]  
$
```