

МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»**

Кафедра теоретических основ
компьютерной безопасности и
криптографии

Подгрузка PHP Payload Backdoor
ОТЧЁТ
ПО ДИСЦИПЛИНЕ
«ОСНОВЫ ПОСТРОЕНИЯ ЗАЩИЩЁННЫХ БАЗ ДАННЫХ»

студента 4 курса 431 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Серебрякова Алексея Владимировича

Преподаватель
профессор, д.ф.-м.н.

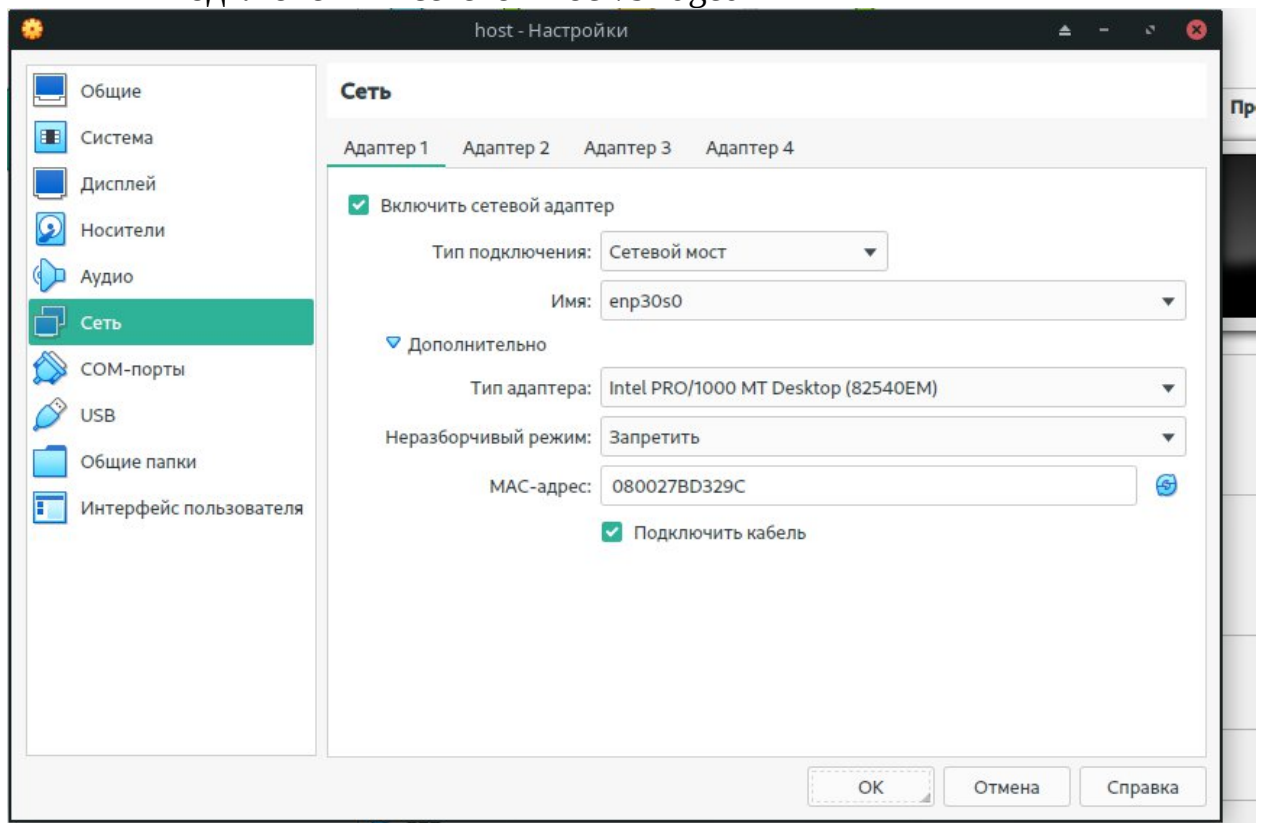
подпись, дата

А.С. Гераськин

Саратов 2023

Раздел 1. Настройка Fedora

1. Запустите Virtual Box, зайдите в настройки Fedora 14
2. Настройте виртуальную машину
 - а. Во вкладке «Сеть» в настройках виртуальной машины выберите тип подключения «сетевой мост/bridged»



Раздел 2. Вход в Fedora 14

Запустите виртуальную машину Fedora14

Войдите в систему

Login: student

Password: <Выбранный ранее пароль>.



Раздел 3. Запуск консоли и определение IP адреса

Откройте терминал

Applications --> System Tools --> Terminal

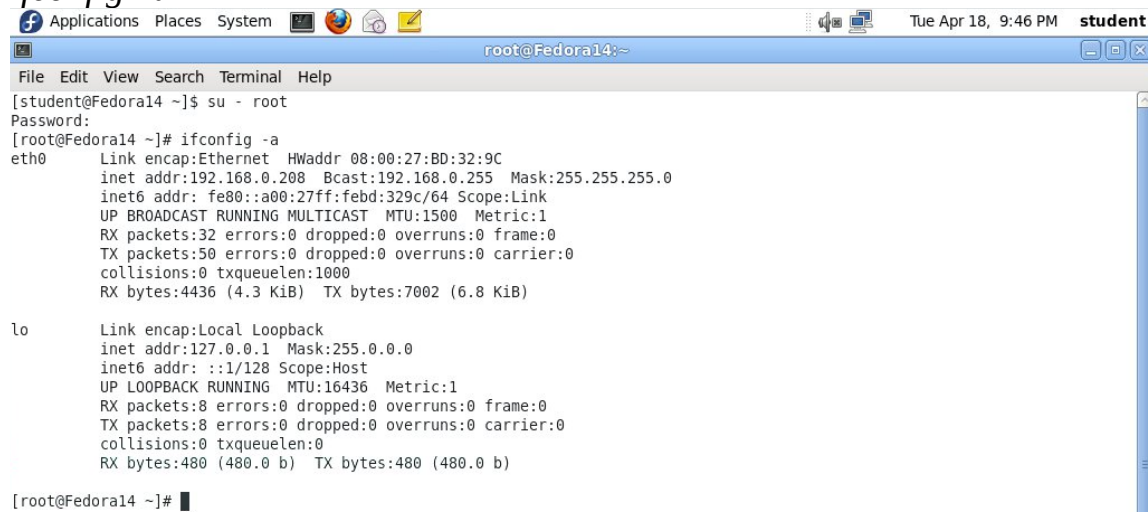
Смените текущего пользователя на root

`su - root`

<Ранее созданный пароль root>

Определите IP адрес

`ifconfig -a`



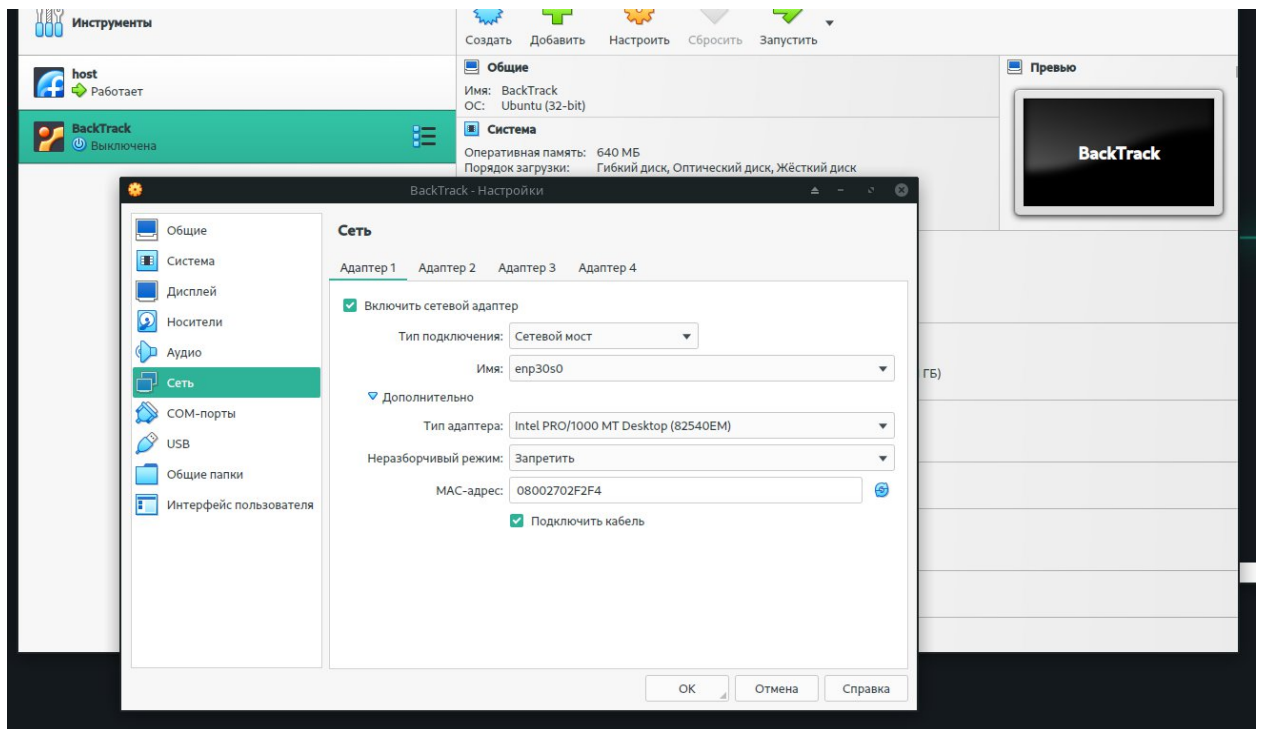
```
[student@Fedora14 ~]$ su - root
Password:
[root@Fedora14 ~]# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 08:00:27:BD:32:9C
          inet addr:192.168.0.208  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:febd:329c/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:32 errors:0 dropped:0 overruns:0 frame:0
          TX packets:50 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4436 (4.3 KiB)  TX bytes:7002 (6.8 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:480 (480.0 b)  TX bytes:480 (480.0 b)

[root@Fedora14 ~]#
```

Раздел 4. Настройка BackTrack

1. Запустите Virtual Box, зайдите в настройки BackTrack
2. Настройте виртуальную машину
 - а. Во вкладке «Сеть» в настройках виртуальной машины выберите тип подключения «сетевой мост/bridged»



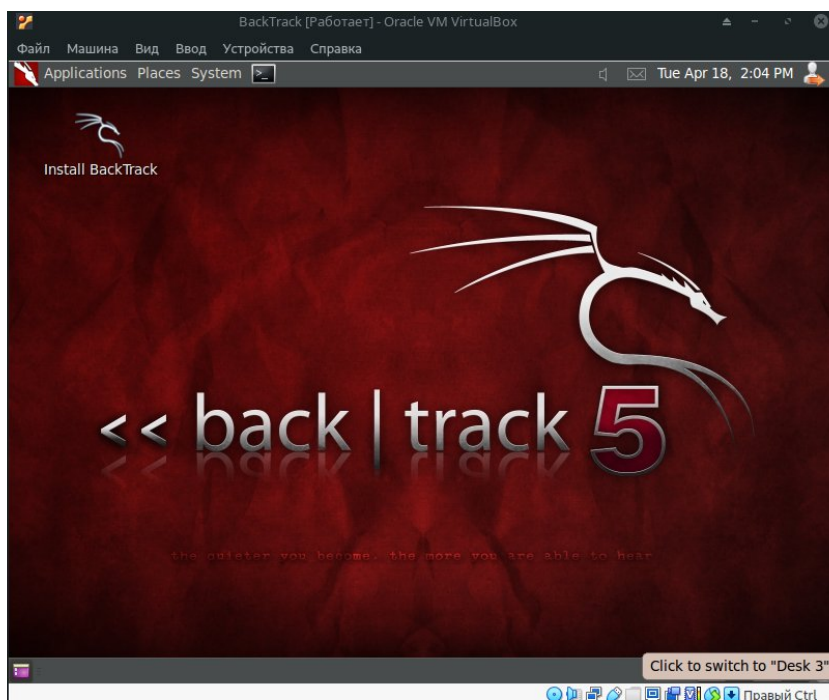
Раздел 5. Вход в BackTrack

Запустите виртуальную машину BackTrack

Войдите в систему

Login: root

Password: toor <Или измененный ранее пароль>.



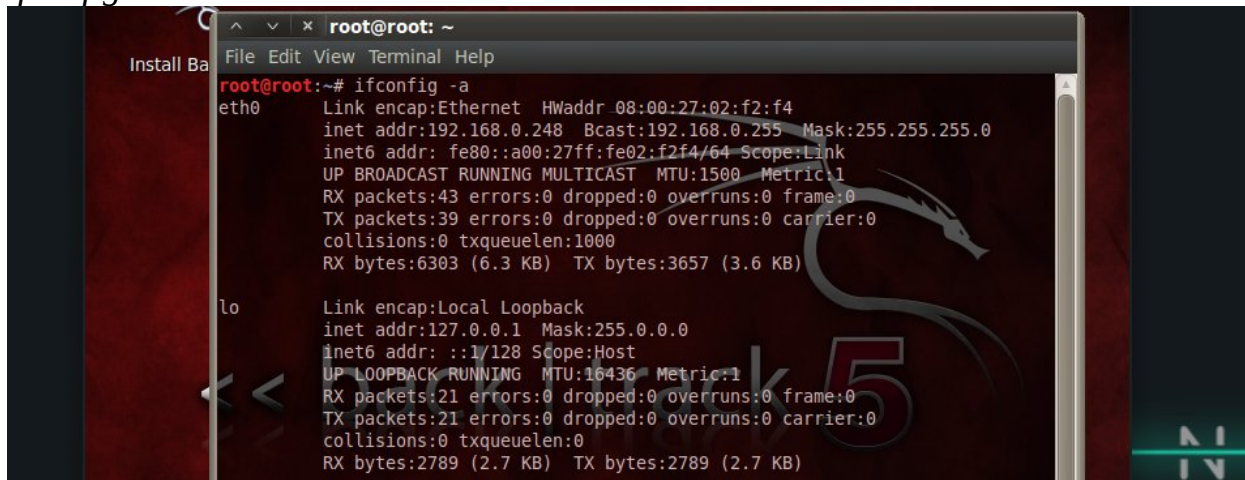
Раздел 6. Запуск консоли и определение IP адреса

Откройте терминал

Щелкните на значок консоли в строке быстрого запуска

Определите IP адрес

ifconfig -a

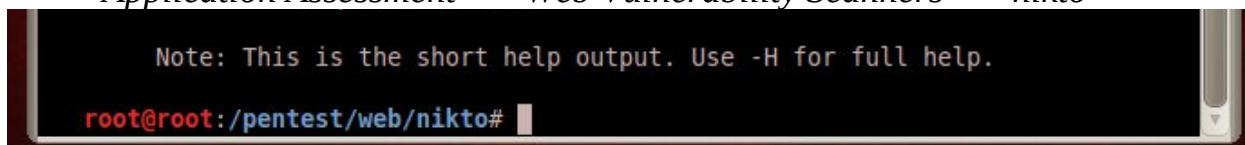


```
root@root: ~  
File Edit View Terminal Help  
root@root:~# ifconfig -a  
eth0      Link encap:Ethernet  HWaddr 08:00:27:02:f2:f4  
          inet addr:192.168.0.248  Bcast:192.168.0.255  Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fe02:f2f4/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:43 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:39 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:6303 (6.3 KB)  TX bytes:3657 (3.6 KB)  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1  Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
          UP LOOPBACK RUNNING  MTU:16436  Metric:1  
          RX packets:21 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:21 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:2789 (2.7 KB)  TX bytes:2789 (2.7 KB)
```

Раздел 7. Запуск nikto

1. Запустите nikto

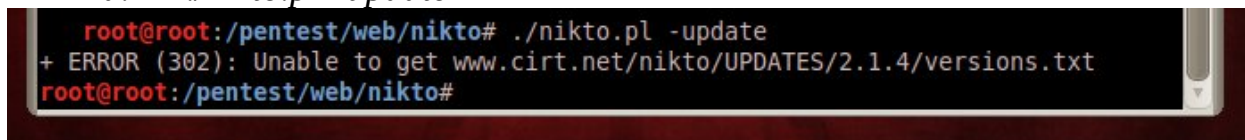
a. *Applications --> BackTrack --> Vulnerability Assessment --> Web Application Assessment --> Web Vulnerability Scanners --> nikto*



```
root@root: /pentest/web/nikto#  
Note: This is the short help output. Use -H for full help.
```

2. Обновите nikto

a. *./nikto.pl -update*



```
root@root: /pentest/web/nikto# ./nikto.pl -update  
+ ERROR (302): Unable to get www.cirt.net/nikto/UPDATES/2.1.4/versions.txt  
root@root: /pentest/web/nikto#
```

3. Изучите опции nikto

a. *./nikto.pl*


```
root@root: /pentest/web/nikto
File Edit View Terminal Help
root@root:/pentest/web/nikto# ./nikto.pl
- Nikto v2.1.4
-----
+ ERROR: No host specified

- config+          Use this config file
- Cgidirs+         scan these CGI dirs: 'none', 'all', or values like "/
cgi/ /cgi-a/"
- dbcheck          check database and other key files for syntax errors
- Display+         Turn on/off display outputs
- evasion+         ids evasion technique
- Format+          save file (-o) format
- host+            target host
- Help             Extended help information
- id+              Host authentication to use, format is id:pass or id:p
ass:realm
- list-plugins     List all available plugins
- mutate+          Guess additional file names
- mutate-options+  Provide extra information for mutations
- output+          Write output to this file
- nocache          Disables the URI cache
- nossl            Disables using SSL
- no404            Disables 404 checks
- port+           Port to use (default 80)
```

4. Проведите сканирование с помощью nikto.pl, заменив IPADDRESS на IP Fedora

a. `./nikto.pl -host http://192.168.0.208/dvwa`

```
root@root:/pentest/web/nikto# ./nikto.pl -host http://192.168.0.208/dvwa
- Nikto v2.1.4
-----
+ Target IP:          192.168.0.208
+ Target Hostname:    192.168.0.208
+ Target Port:        80
+ Start Time:         2023-04-19 21:01:43
-----
+ Server: Apache/2.2.16 (Fedora)
+ Retrieved x-powered-by header: PHP/5.3.3
+ Root page / redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ robots.txt contains 1 entry which should be manually viewed.
+ ETag header found on server, inode: 133005, size: 26, mtime: 0x481ddf3a0cd80
+ Apache/2.2.16 appears to be outdated (current is at least Apache/2.2.17). Apac
he 1.3.42 (final release) and 2.0.64 are also current.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to X
ST
```

5. Изучите результаты сканирования

- a. Nikto не только может определить версию сервера Apache, но и выяснить является ли она устаревшей.
- b. Кроме того, Nikto узнал ОС и версию PHP.

с. Nikto также отображает разные уязвимости, описание которых можно узнать тут: Open Source Vulnerabilities Database. (Свободно распространяемая база данных уязвимостей).

```
+ Root page / redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ robots.txt contains 1 entry which should be manually viewed.
+ ETag header found on server, inode: 133005, size: 26, mtime: 0x481ddf3a0cd80
+ Apache/2.2.16 appears to be outdated (current is at least Apache/2.2.17). Apache 1.3.42 (final release) and 2.0.64 are also current.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3268: /dwa/config/: Directory indexing found.
+ /config/: Configuration information may be available remotely.
+ OSVDB-12184: /index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3268: /config/: Directory indexing found.
+ OSVDB-3268: /dwa/docs/: Directory indexing found.
+ OSVDB-3268: /docs/: Directory indexing found.
+ OSVDB-3092: /CHANGELOG.txt: A changelog was found.
+ /login.php: Admin login page/section found.
+ 6448 items checked: 1 error(s) and 14 item(s) reported on remote host
+ End Time: 2023-04-19 21:02:10 (27 seconds)
-----
+ 1 host(s) tested
root@root:/pentest/web/nikto#
```

Раздел 8. OSVDB-877: Использование команды Telnet для получения информации о веб-сервере и ОС

1. Используйте Telnet для получения главной информации, заголовков (Banners)

a. telnet IPADDRESS 80

Где IPADDRESS - IP адрес DVWA, 80 - порт веб сервера по умолчанию.

b. Введите GET index.html

```
root@root:/pentest/web/nikto# telnet 192.168.0.208 80
Trying 192.168.0.208...
Connected to 192.168.0.208.
Escape character is '^]'.
GET index.html
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.2.16 (Fedora) Server at ::1 Port 80</address>
</body></html>
Connection closed by foreign host.
root@root:/pentest/web/nikto#
```

Замечания:

- Несмотря на то, что веб-сервер возвращает ответ с кодом 400: "400 Bad Request", он присылает информацию о веб-сервере и ОС.
- OSVDB-877:

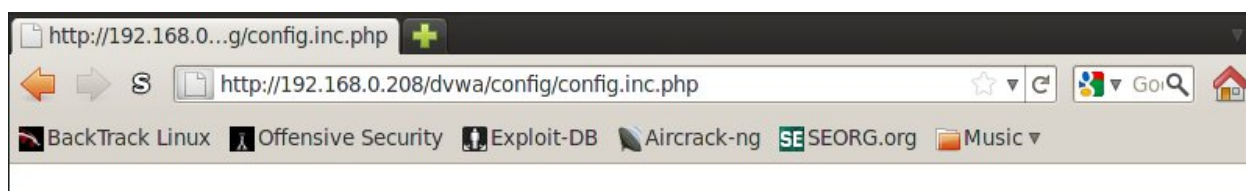
RFC совместимые веб-серверы поддерживают метод TRACE HTTP, содержащий недостаток, который может привести к несанкционированному раскрытию информации. Метод TRACE используется для отладки соединений веб-серверов и позволяет клиенту видеть то, что получено на другом конце цепи запросов.

Раздел 9. OSVDB-3268: /dvwa/config/: индекс директорий

1. Загрузите директорию /dvwa/config с помощью Firefox
a. *firefox http://IPADDRESS/dvwa/config*



2. Исследуйте /dvwa/config
a. Кликните на *config.inc.php*



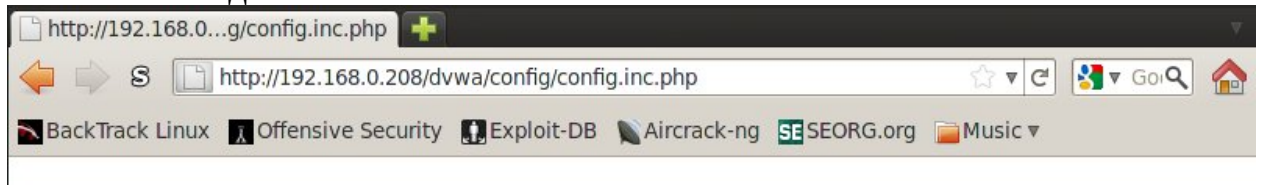
Замечания:

- Если веб директория не содержит файлов index.html, index.php, и т.д., тогда все файлы в этой директории будут отображаться.
- Запомните, никогда не следует разрешать открытый доступ к конфигурационной папке.
- OSVDB-3268: Просмотр директории оказался разрешен на этом веб-сервере. Пока что нет известных уязвимостей или эксплоитов, связанных с этим. Однако, эта папка может открывать доступ к важным данным или

директориям удаленным пользователям. А также помочь в осуществлении других атак.

3. Кликните по config.inc.php

- а. Файл *config.inc.php* ничего не запустил. Обычно файлы php, perl, asp, и тд выполняются как положено и не дают ничего на выходе.



4. Протестируйте запрос с символом ~

- а. *http://192.168.1.106/dvwa/config/config.inc.php~*



Замечания:

- Некоторые приложения создают резервную копию файлов, которые вы редактируете, с символом ~ на конце.
- Содержимое файла php отображается на экране, так как веб-сервер не воспринял этот файл как php скрипт, так как он заканчивается на ~.

Раздел 10. Отчет о работе

1. В Backtrack откройте консоль и выполните:

- cd /pentest/web/nikto*
- ./nikto.pl -host http://IPADDRESS/dvwa 2>&1 > /var/tmp/nikto.txt*
Замените IPADDRESS на IP адрес DVWA
- ls -l /var/tmp/nikto.txt*
- date*
- echo "IvanovII"* где вместо "IvanovII" - ваша фамилия и инициалы

```
^ v x root@root: /pentest/web/nikto
File Edit View Terminal Tabs Help

root@root: /pentest/web/nikto x root@root: /pentest/web/nikto x

root@root:/pentest/web/nikto# ./nikto.pl -host http://192.168.0.208/dvwa 2>&l> /
var/tmp/nikto.txt
^Croot@root:/pentest/web/nikto# ls
docs nikto.conf nikto.pl plugins templates
root@root:/pentest/web/nikto# ls -l /var/tmp/nikto.txt
-rw-r--r-- 1 root root 912 2023-04-18 21:14 /var/tmp/nikto.txt
root@root:/pentest/web/nikto#
root@root:/pentest/web/nikto# date
Tue Apr 18 21:15:29 EDT 2023
root@root:/pentest/web/nikto# echo "Serebriakov AV"
Serebriakov AV
root@root:/pentest/web/nikto#
```