Индивидуальный проект

Основы информационной безопасности

Галиева Аделина Руслановна

16 марта 2024

Российский университет дружбы народов, Москва, Россия

Вводная часть

Цели и задачи

Установить DVWA в гостевую систему к Kali Linux.

Материалы и методы

- Процессор `pandoc` для входного формата Markdown
- Результирующие форматы
  - `pdf`
  - `html`
- Автоматизация процесса создания: `Makefile`

Создание презентации

Процессор pandoc

- Pandoc: преобразователь текстовых файлов
- Сайт: https://pandoc.org/
- Репозиторий: https://github.com/jgm/pandoc

Формат `pdf`

- Использование LaTeX
- Пакет для презентации: beamer
- Тема оформления: **`metropolis`**

Код для формата pdf

```
slide_level: 2
aspectratio: 169
section-titles: true
theme: metropolis
```

Формат `html`

- Используется фреймворк reveal.js
- Используется тема `beige`

Код для формата html

- Тема задаётся в файле Makefile

```
REVEALJS_THEME = beige
```

Результаты

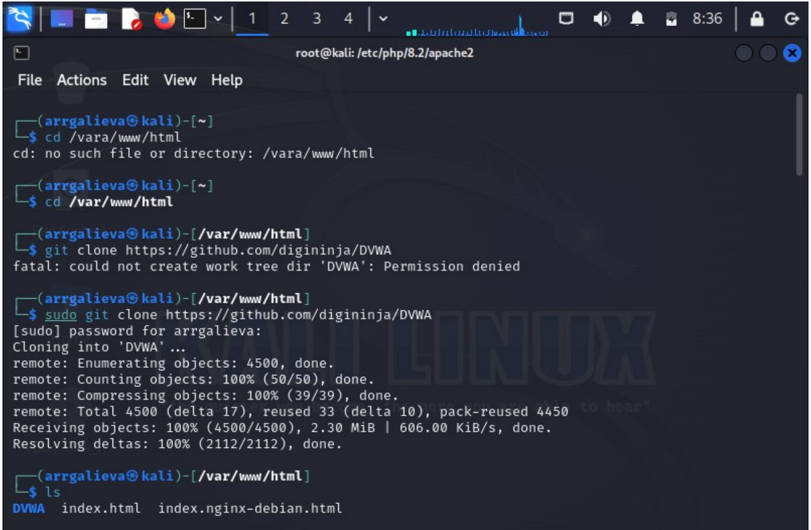
Получающиеся форматы

- Полученный `pdf`-файл можно демонстрировать в любой программе просмотра `pdf`
- Полученный `html`-файл содержит в себе все ресурсы: изображения, css, скрипты

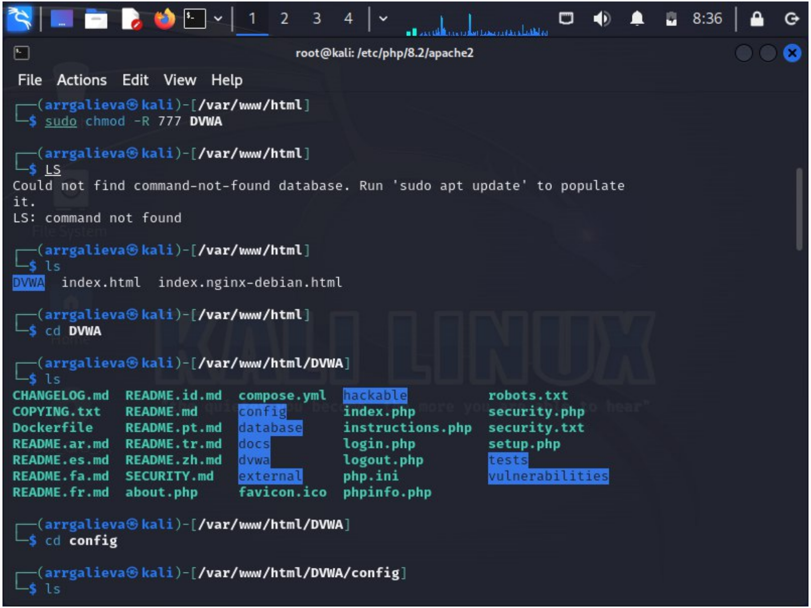
Элементы презентации

Содержание исследования

1. Устанавливаем DVWA при помощи различных команд и данного нам репозитория.

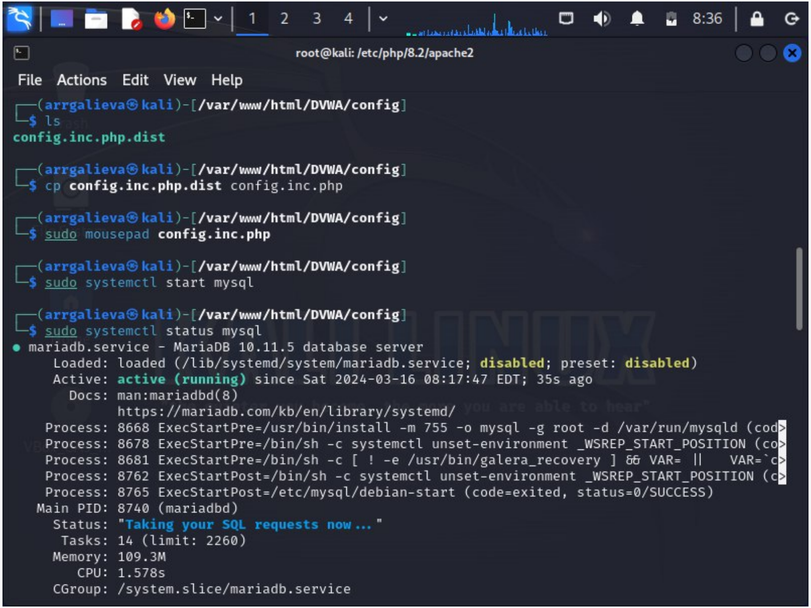


```
┌──(arrgalieva㉿kali)-[~]
└─$ cd /vara/www/html
cd: no such file or directory: /vara/www/html

┌──(arrgalieva㉿kali)-[~]
└─$ cd /var/www/html

┌──(arrgalieva㉿kali)-[/var/www/html]
└─$ git clone https://github.com/digininja/DVWA
fatal: could not create work tree dir 'DVWA': Permission denied

┌──(arrgalieva㉿kali)-[/var/www/html]
└─$ sudo git clone https://github.com/digininja/DVWA
[sudo] password for arrgalieva:
Cloning into 'DVWA' ...
remote: Enumerating objects: 4500, done.
remote: Counting objects: 100% (50/50), done.
remote: Compressing objects: 100% (39/39), done.
remote: Total 4500 (delta 17), reused 33 (delta 10), pack-reused 4450
Receiving objects: 100% (4500/4500), 2.30 MiB | 606.00 KiB/s, done.
Resolving deltas: 100% (2112/2112), done.

┌──(arrgalieva㉿kali)-[/var/www/html]
└─$ ls
DVWA  index.html  index.nginx-debian.html
```



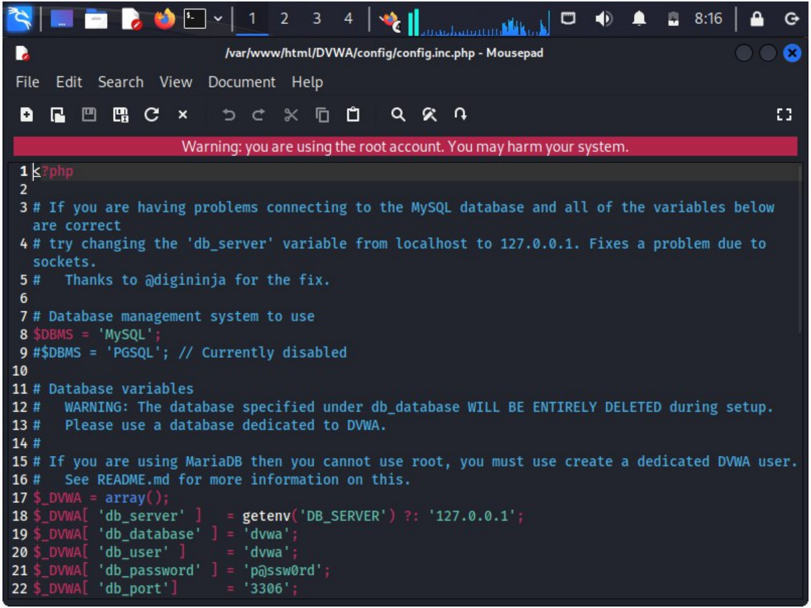
```
┌──(arrgalieva㉿kali)-[/var/www/html]
└─$ sudo chmod -R 777 DVWA

┌──(arrgalieva㉿kali)-[/var/www/html]
└─$ LS
Could not find command-not-found database. Run 'sudo apt update' to populate
it.
LS: command not found

┌──(arrgalieva㉿kali)-[/var/www/html]
└─$ ls
DVWA  index.html  index.nginx-debian.html

┌──(arrgalieva㉿kali)-[/var/www/html]
└─$ cd DVWA

┌──(arrgalieva㉿kali)-[/var/www/html/DVWA]
└─$ ls
CHANGELOG.md  README.id.md  compose.yml  hackable          robots.txt
COPYING.txt   README.md     config       index.php         security.php
Dockerfile    README.pt.md  database     instructions.php  security.txt
README.ar.md  README.tr.md  docs         login.php         setup.php
README.es.md  README.zh.md  dvwa         logout.php        tests
README.fa.md  SECURITY.md   external     php.ini           vulnerabilities
README.fr.md  about.php     favicon.ico  phpinfo.php

┌──(arrgalieva㉿kali)-[/var/www/html/DVWA]
└─$ cd config

┌──(arrgalieva㉿kali)-[/var/www/html/DVWA/config]
└─$ ls
```

Рис. 2: Прописываем команды



```
┌──(arrgalieva㉿kali)-[/var/www/html/DVWA/config]
└─$ ls
config.inc.php.dist

┌──(arrgalieva㉿kali)-[/var/www/html/DVWA/config]
└─$ cp config.inc.php.dist config.inc.php

┌──(arrgalieva㉿kali)-[/var/www/html/DVWA/config]
└─$ sudo mousepad config.inc.php

┌──(arrgalieva㉿kali)-[/var/www/html/DVWA/config]
└─$ sudo systemctl start mysql

┌──(arrgalieva㉿kali)-[/var/www/html/DVWA/config]
└─$ sudo systemctl status mysql
● mariadb.service - MariaDB 10.11.5 database server
     Loaded: loaded (/lib/systemd/system/mariadb.service; disabled; preset: disabled)
     Active: active (running) since Sat 2024-03-16 08:17:47 EDT; 35s ago
       Docs: man:mariadbd(8)
             https://mariadb.com/kb/en/library/systemd/
    Process: 8668 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/mysqld (cod>
    Process: 8678 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (co>
    Process: 8681 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR= ||   VAR=`c>
    Process: 8762 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (c>
    Process: 8765 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
   Main PID: 8740 (mariadbd)
     Status: "Taking your SQL requests now..."
      Tasks: 14 (limit: 2260)
     Memory: 109.3M
        CPU: 1.578s
     CGroup: /system.slice/mariadb.service
```

Рис. 3: Прописываем команды

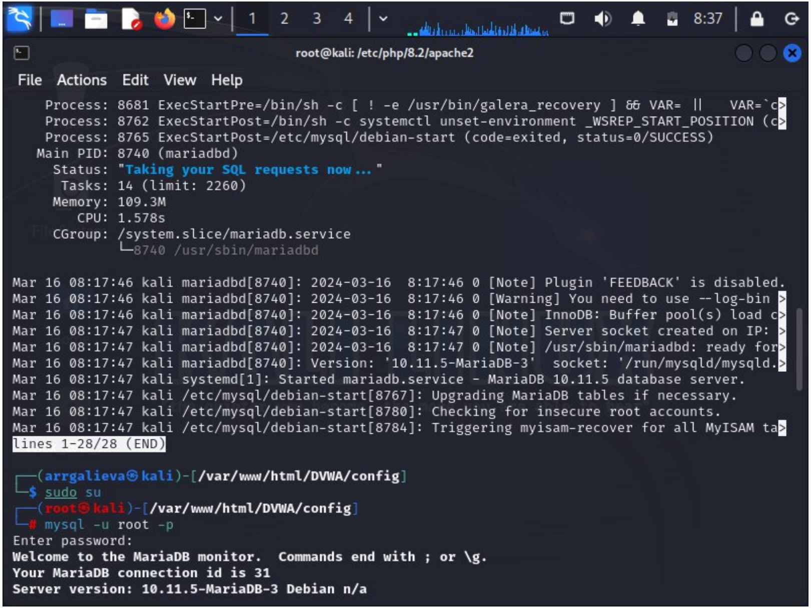


/var/www/html/DVWA/config/config.inc.php - Mousepad

Warning: you are using the root account. You may harm your system.

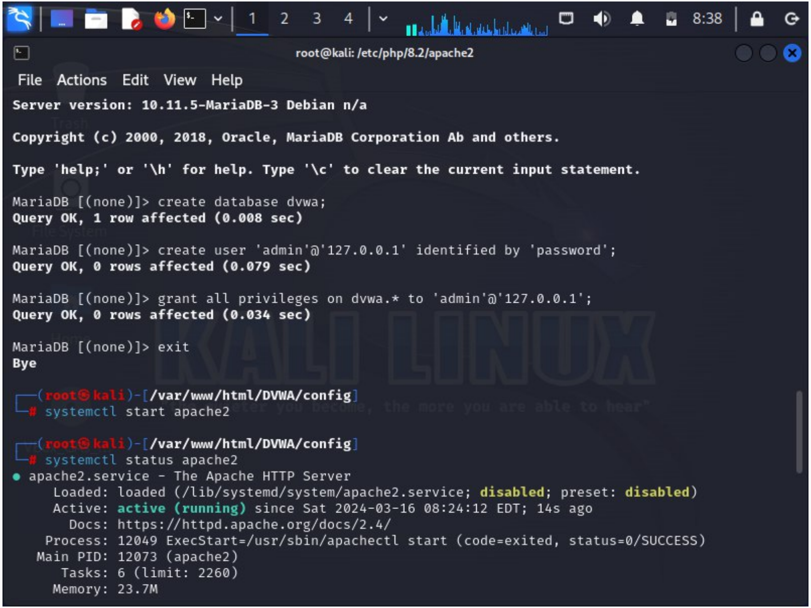
```
<?php

# If you are having problems connecting to the MySQL database and all of the variables below are correct
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
#   Thanks to @digininja for the fix.

# Database management system to use
$DBMS = 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

# Database variables
#   WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
#   Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
#   See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ]   = getenv('DB_SERVER') ?: '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ]     = 'dvwa';
$_DVWA[ 'db_password' ] = 'p@ssw0rd';
$_DVWA[ 'db_port']      = '3306';
```

Рис. 4: Прописываем команды



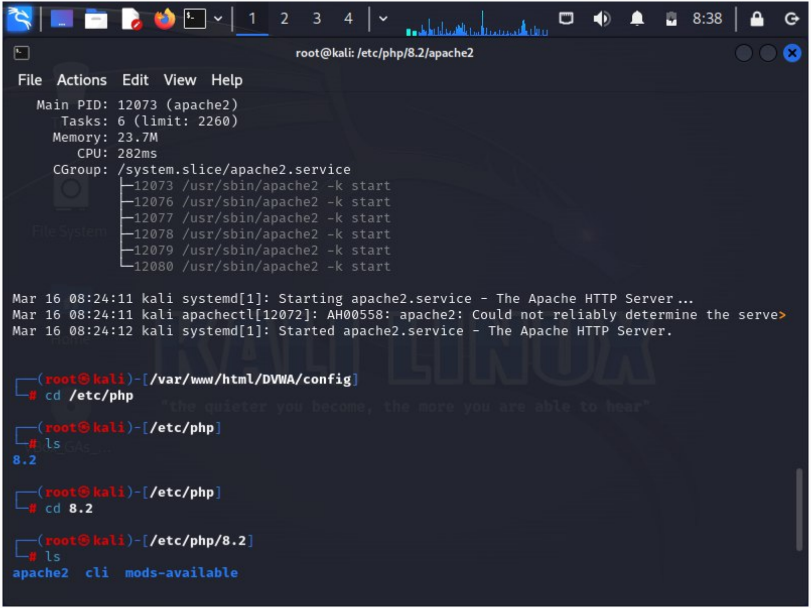
```
     Process: 8681 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR= ||   VAR=`c>
     Process: 8762 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (c>
     Process: 8765 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
    Main PID: 8740 (mariadbd)
      Status: "Taking your SQL requests now..."
       Tasks: 14 (limit: 2260)
      Memory: 109.3M
         CPU: 1.578s
      CGroup: /system.slice/mariadb.service
              └─8740 /usr/sbin/mariadbd

Mar 16 08:17:46 kali mariadbd[8740]: 2024-03-16  8:17:46 0 [Note] Plugin 'FEEDBACK' is disabled.
Mar 16 08:17:46 kali mariadbd[8740]: 2024-03-16  8:17:46 0 [Warning] You need to use --log-bin >
Mar 16 08:17:46 kali mariadbd[8740]: 2024-03-16  8:17:46 0 [Note] InnoDB: Buffer pool(s) load c>
Mar 16 08:17:47 kali mariadbd[8740]: 2024-03-16  8:17:47 0 [Note] Server socket created on IP: >
Mar 16 08:17:47 kali mariadbd[8740]: 2024-03-16  8:17:47 0 [Note] /usr/sbin/mariadbd: ready for>
Mar 16 08:17:47 kali mariadbd[8740]: Version: '10.11.5-MariaDB-3'  socket: '/run/mysqld/mysqld.>
Mar 16 08:17:47 kali systemd[1]: Started mariadb.service - MariaDB 10.11.5 database server.
Mar 16 08:17:47 kali /etc/mysql/debian-start[8767]: Upgrading MariaDB tables if necessary.
Mar 16 08:17:47 kali /etc/mysql/debian-start[8780]: Checking for insecure root accounts.
Mar 16 08:17:47 kali /etc/mysql/debian-start[8784]: Triggering myisam-recover for all MyISAM ta>
lines 1-28/28 (END)

┌──(arrgalieva㉿kali)-[/var/www/html/DVWA/config]
└─$ sudo su
┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.11.5-MariaDB-3 Debian n/a
```

Рис. 5: Прописываем команды



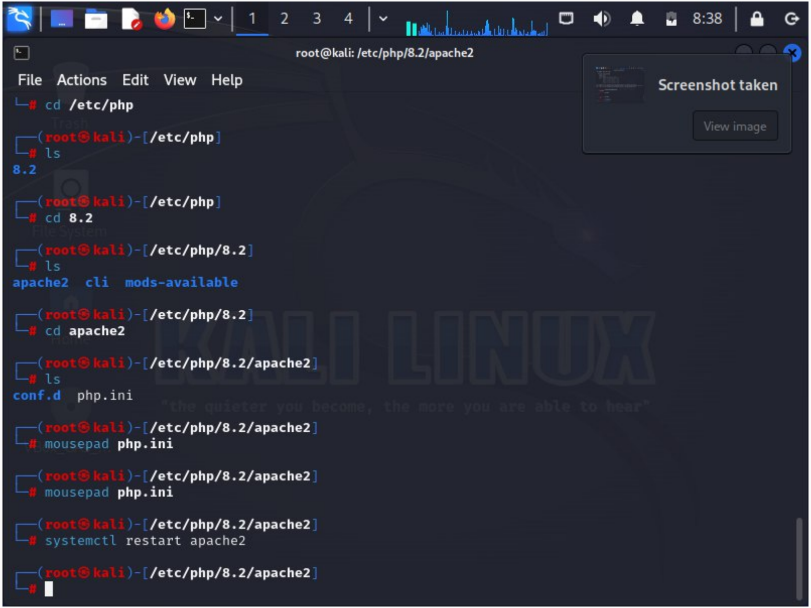
```
Server version: 10.11.5-MariaDB-3 Debian n/a

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create database dvwa;
Query OK, 1 row affected (0.008 sec)

MariaDB [(none)]> create user 'admin'@'127.0.0.1' identified by 'password';
Query OK, 0 rows affected (0.079 sec)

MariaDB [(none)]> grant all privileges on dvwa.* to 'admin'@'127.0.0.1';
Query OK, 0 rows affected (0.034 sec)

MariaDB [(none)]> exit
Bye

┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# systemctl start apache2

┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: active (running) since Sat 2024-03-16 08:24:12 EDT; 14s ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 12049 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 12073 (apache2)
      Tasks: 6 (limit: 2260)
     Memory: 23.7M
```

Рис. 6: Прописываем команды



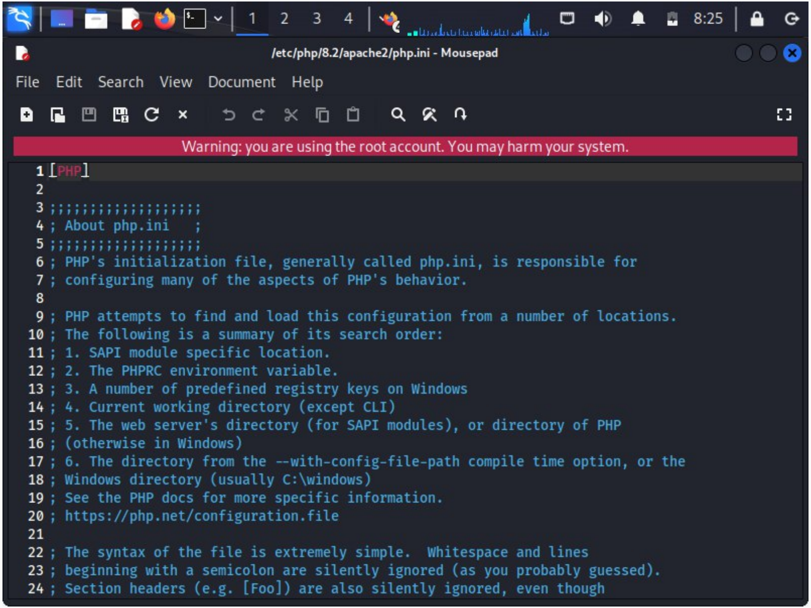
```
    Main PID: 12073 (apache2)
       Tasks: 6 (limit: 2260)
      Memory: 23.7M
         CPU: 282ms
      CGroup: /system.slice/apache2.service
              ├─12073 /usr/sbin/apache2 -k start
              ├─12076 /usr/sbin/apache2 -k start
              ├─12077 /usr/sbin/apache2 -k start
              ├─12078 /usr/sbin/apache2 -k start
              ├─12079 /usr/sbin/apache2 -k start
              └─12080 /usr/sbin/apache2 -k start

Mar 16 08:24:11 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
Mar 16 08:24:11 kali apachectl[12072]: AH00558: apache2: Could not reliably determine the serve>
Mar 16 08:24:12 kali systemd[1]: Started apache2.service - The Apache HTTP Server.

┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# cd /etc/php

┌──(root㉿kali)-[/etc/php]
└─# ls
8.2

┌──(root㉿kali)-[/etc/php]
└─# cd 8.2

┌──(root㉿kali)-[/etc/php/8.2]
└─# ls
apache2  cli  mods-available
```

Рис. 7: Прописываем команды



```
└─# cd /etc/php

┌──(root㉿kali)-[/etc/php]
└─# ls
8.2

┌──(root㉿kali)-[/etc/php]
└─# cd 8.2

┌──(root㉿kali)-[/etc/php/8.2]
└─# ls
apache2  cli  mods-available

┌──(root㉿kali)-[/etc/php/8.2]
└─# cd apache2

┌──(root㉿kali)-[/etc/php/8.2/apache2]
└─# ls
conf.d  php.ini

┌──(root㉿kali)-[/etc/php/8.2/apache2]
└─# mousepad php.ini

┌──(root㉿kali)-[/etc/php/8.2/apache2]
└─# mousepad php.ini

┌──(root㉿kali)-[/etc/php/8.2/apache2]
└─# systemctl restart apache2

┌──(root㉿kali)-[/etc/php/8.2/apache2]
└─# 
```

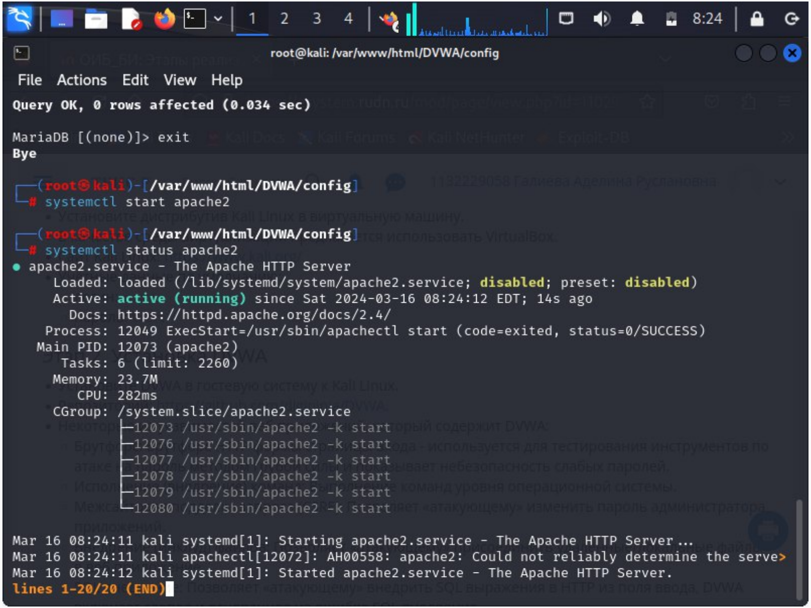
Рис. 8: Прописываем команды



Warning: you are using the root account. You may harm your system.

```
[PHP]

;;;;;;;;;;;;;;;;;;;
; About php.ini   ;
;;;;;;;;;;;;;;;;;;;
; PHP's initialization file, generally called php.ini, is responsible for
; configuring many of the aspects of PHP's behavior.

; PHP attempts to find and load this configuration from a number of locations.
; The following is a summary of its search order:
; 1. SAPI module specific location.
; 2. The PHPRC environment variable.
; 3. A number of predefined registry keys on Windows
; 4. Current working directory (except CLI)
; 5. The web server's directory (for SAPI modules), or directory of PHP
; (otherwise in Windows)
; 6. The directory from the --with-config-file-path compile time option, or the
; Windows directory (usually C:\windows)
; See the PHP docs for more specific information.
; https://php.net/configuration.file

; The syntax of the file is extremely simple.  Whitespace and lines
; beginning with a semicolon are silently ignored (as you probably guessed).
; Section headers (e.g. [Foo]) are also silently ignored, even though
```

Рис. 9: Прописываем команды



```
Query OK, 0 rows affected (0.034 sec)

MariaDB [(none)]> exit
Bye

┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# systemctl start apache2

┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: active (running) since Sat 2024-03-16 08:24:12 EDT; 14s ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 12049 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 12073 (apache2)
      Tasks: 6 (limit: 2260)
     Memory: 23.7M
        CPU: 282ms
     CGroup: /system.slice/apache2.service
             ├─12073 /usr/sbin/apache2 -k start
             ├─12076 /usr/sbin/apache2 -k start
             ├─12077 /usr/sbin/apache2 -k start
             ├─12078 /usr/sbin/apache2 -k start
             ├─12079 /usr/sbin/apache2 -k start
             └─12080 /usr/sbin/apache2 -k start

Mar 16 08:24:11 kali systemd[1]: Starting apache2.service - The Apache HTTP Server ...
Mar 16 08:24:11 kali apachectl[12072]: AH00558: apache2: Could not reliably determine the serve>
Mar 16 08:24:12 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-20/20 (END)
```

Рис. 10: Прописываем команды

Результаты

В ходе выполнения данного этапа я установила DVWA в гостевую систему к Kali Linux.