

Nmap 7.93 scan initiated Mon Feb 17 10:13:07 2025 as: nmap -sT -p- --min-rate 10000 -oN tcp.txt 10.10.10.48

Warning: 10.10.10.48 giving up on port because retransmission cap hit (10).

Nmap scan report for 10.10.10.48

Host is up (0.28s latency).

Not shown: 65276 closed tcp ports (conn-refused), 253 filtered tcp ports (no-response)

PORT	STATE	SERVICE
------	-------	---------

22/tcp	open	ssh
--------	------	-----

53/tcp	open	domain
--------	------	--------

80/tcp	open	http
--------	------	------

1433/tcp	open	ms-sql-s
----------	------	----------

32400/tcp	open	plex
-----------	------	------

32469/tcp	open	unknown
-----------	------	---------

Nmap done at Mon Feb 17 10:13:46 2025 -- 1 IP address (1 host up) scanned in 38.94 seconds

Nmap 7.93 scan initiated Mon Feb 17 10:17:30 2025 as: nmap -sC -sV -p 22,53,80,1433,32400,32469,123,5353,32414 -O -oN detail.txt 10.10.10.48

Nmap scan report for 10.10.10.48

Host is up (0.28s latency).

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

22/tcp	open	ssh	OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
--------	------	-----	--

| ssh-hostkey:

| 1024 aaef5ce08e86978247ff4ae5401890c5 (DSA)

| 2048 e8c19dc543abfe61233bd7e4af9b7418 (RSA)

| 256 b6a07838d0c810948b44b2eaa017422b (ECDSA)

|_ 256 4d6840f720c4e552807a4438b8a2a752 (ED25519)

53/tcp	open	domain	dnsmasq 2.76
--------	------	--------	--------------

| dns-nsid:

|_ bind.version: dnsmasq-2.76

80/tcp	open	http	lighttpd 1.4.35
--------	------	------	-----------------

|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).

|_ http-server-header: lighttpd/1.4.35

123/tcp	closed	ntp	
---------	--------	-----	--

1433/tcp	open	upnp	Platinum UPnP 1.0.5.13 (UPnP/1.0 DLNADOC/1.50)
----------	------	------	--

5353/tcp	closed	mdns	
----------	--------	------	--

32400/tcp	open	http	Plex Media Server httpd
-----------	------	------	-------------------------

|_ http-cors: HEAD GET POST PUT DELETE OPTIONS


| http-auth:


| HTTP/1.1 401 Unauthorized\x0D

|_ Server returned status 401 but no WWW-Authenticate header.

|_ http-favicon: Plex

🎯 Target Url	http://10.10.10.48
🧵 Threads	50
📖 Wordlist	/usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
🔍 Status Codes	All Status Codes!
⌚ Timeout (secs)	7
👤 User-Agent	feroxbuster/2.10.0
📄 Config File	/etc/feroxbuster/ferox-config.toml
🔍 Extract Links	true
🚩 HTTP methods	[GET]
📏 Recursion Depth	4

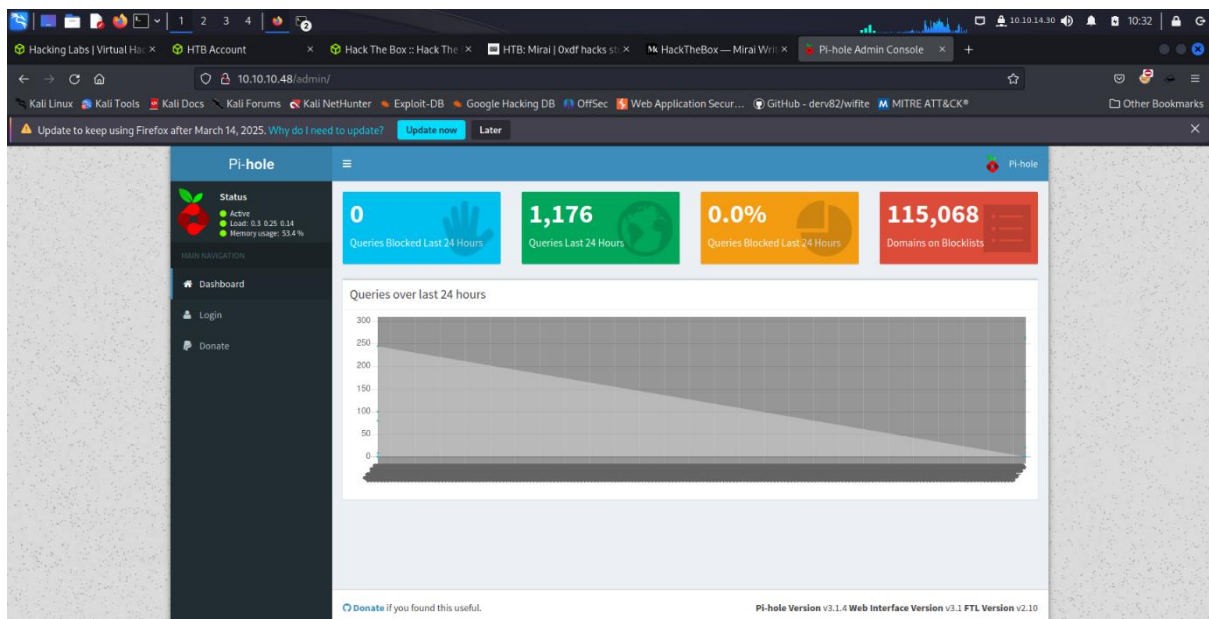
 New Version Available | <https://github.com/epi052/feroxbuster/releases/latest>

 Press [ENTER] to use the Scan Management Menu™

```
404 GET 0l 0w 0c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200 GET 1l 1w 18c http://10.10.10.48/versions
200 GET 145l 2311w 14164c http://10.10.10.48/admin/LICENSE
200 GET 20l 170w 1085c http://10.10.10.48/admin/scripts/vendor/LICENSE
200 GET 20l 170w 1085c http://10.10.10.48/admin/style/vendor/LICENSE

[#####] - 4m 210000/210000 0s found:4 errors:3291
[#####] - 4m 30000/30000 131/s http://10.10.10.48/
[#####] - 4m 30000/30000 127/s http://10.10.10.48/admin/
[#####] - 4m 30000/30000 130/s http://10.10.10.48/admin/scripts/
[#####] - 4m 30000/30000 132/s http://10.10.10.48/admin/img/
[#####] - 4m 30000/30000 132/s http://10.10.10.48/admin/style/
[#####] - 4m 30000/30000 134/s http://10.10.10.48/admin/scripts/vendor/
[#####] - 4m 30000/30000 133/s http://10.10.10.48/admin/style/vendor/
```

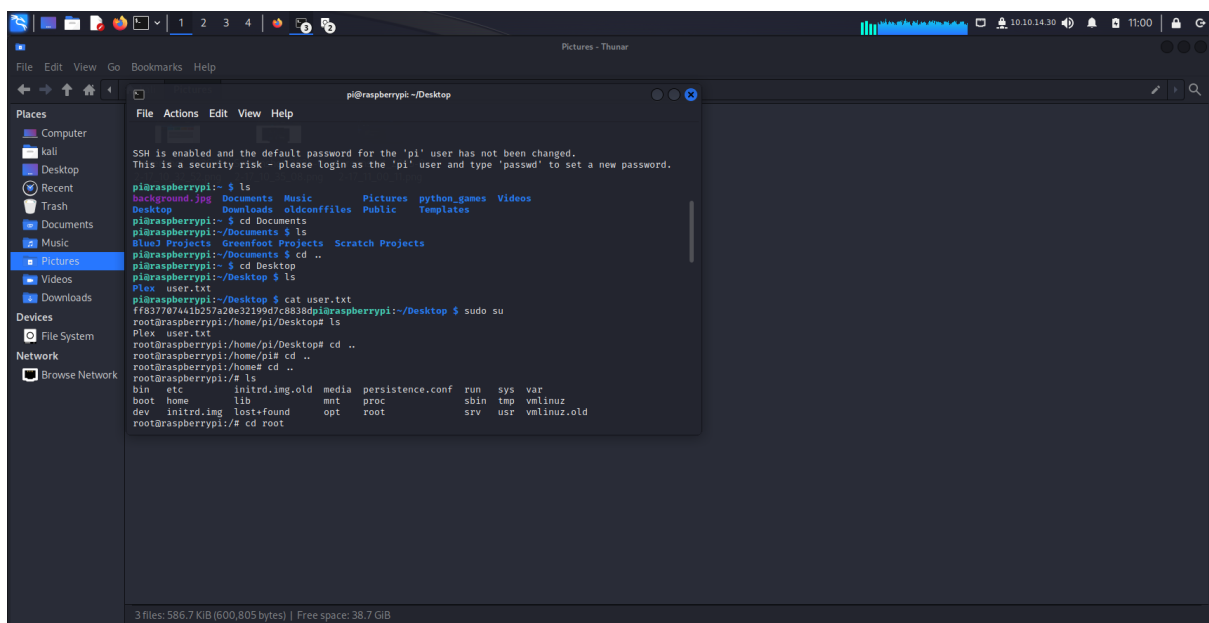
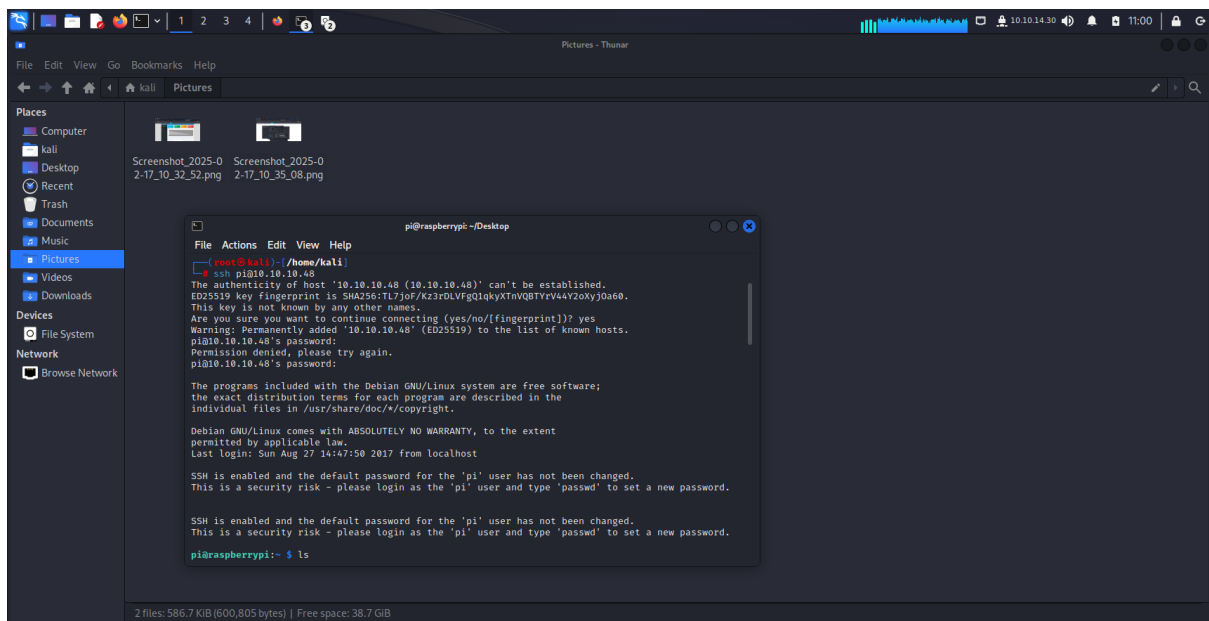
We get the admin domain from feroxbuster



We can get pi hole default credentials by searching the internet then use ssh

pi

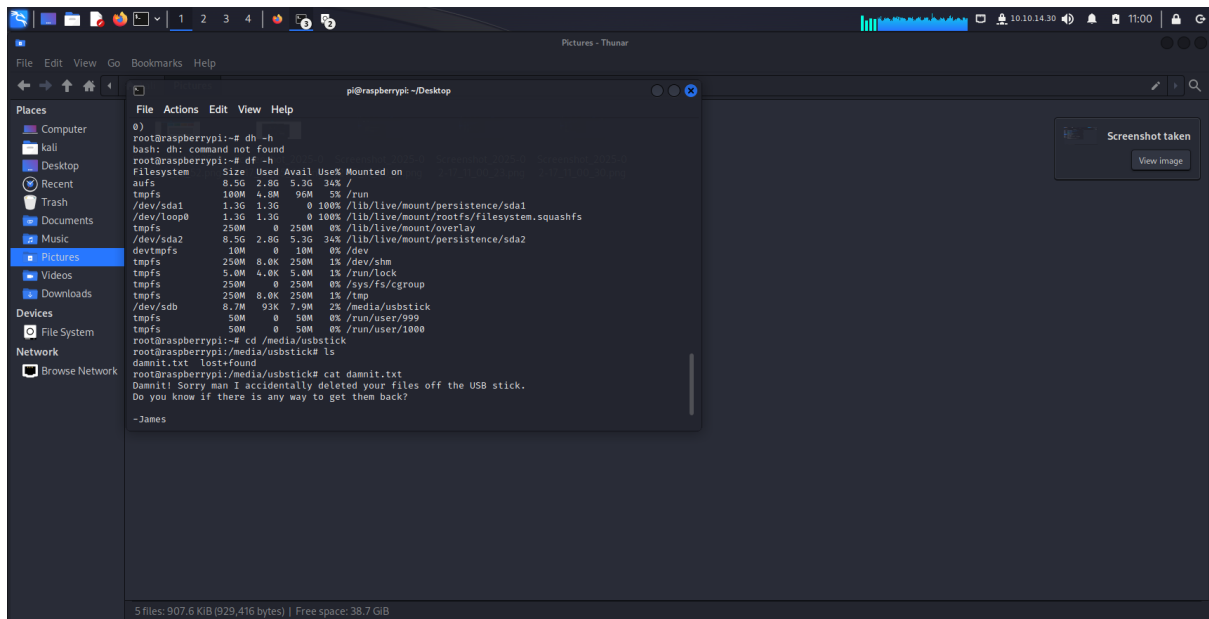
raspberrypi



For root.txt we can see that the file was in the mount devices as a hint to find the mount devices

dh -h

cd /media/usbstick



In damnit.txt we can see that it was deleted but no data is truly deleted only the pointer is null

strings /dev/sdb -n 32

or

grep -aPo '[a-zA-F0-9]{32}' /dev/sdb

for it will find it with grep