Blaster-THM

Enumeration

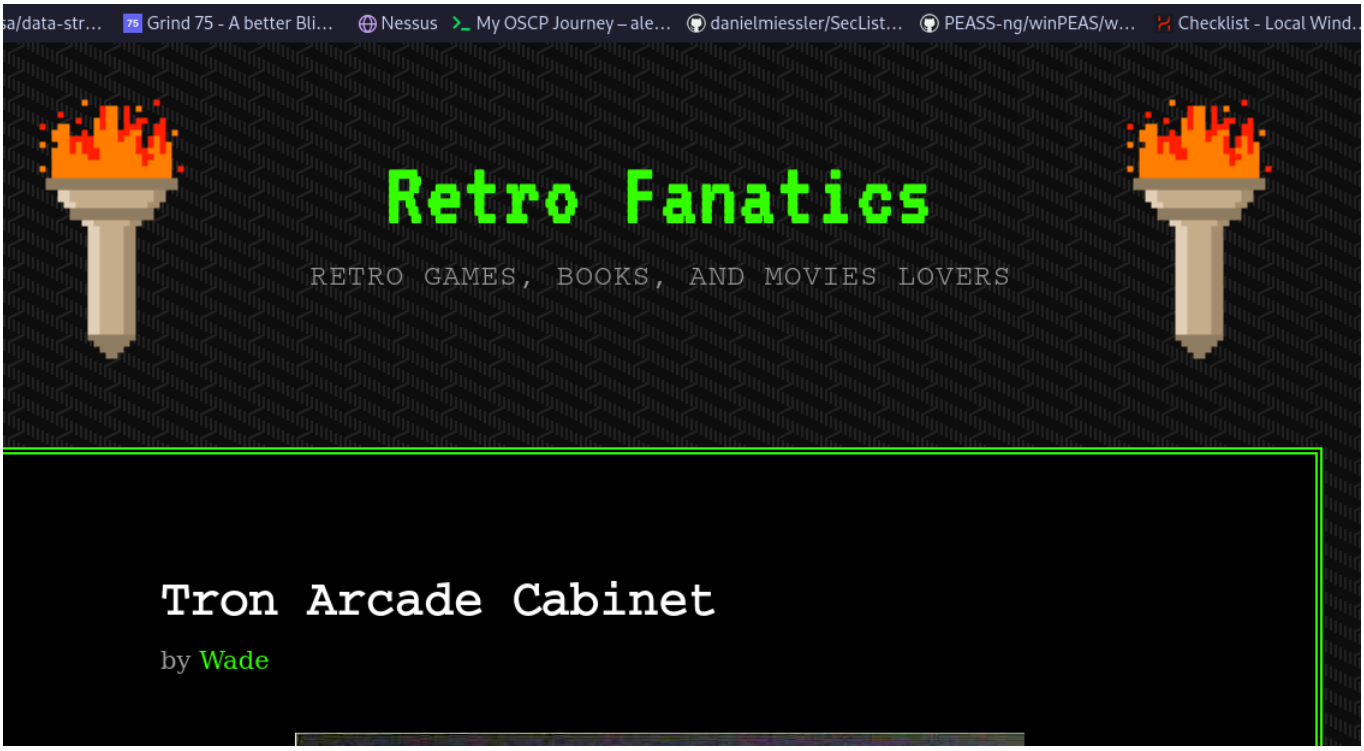
Using autorecon to enumerate:

```
# Nmap 7.94SVN scan initiated Sat Feb 17 21:04:12 2024 as: nmap -vv --reason -Pn
--version-all -A --osscan-guess -p- -oN
/home/kali/Downloads/buster/results/10.10.185.175/scans/_full_tcp_nmap.txt -oX
/home/kali/Downloads/buster/results/10.10.185.175/scans/xml/_full_tcp_nmap.xml 1
Nmap scan report for 10.10.185.175
Host is up, received user-set (0.16s latency).
Scanned at 2024-02-17 21:04:12 IST for 322s
Not shown: 65533 filtered tcp ports (no-response)
PORT     STATE SERVICE       REASON          VERSION
80/tcp   open  http          syn-ack ttl 124 Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-title: IIS Windows Server
3389/tcp open  ms-wbt-server syn-ack ttl 124 Microsoft Terminal Services
| ssl-cert: Subject: commonName=RetroWeb
| Issuer: commonName=RetroWeb
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-02-16T14:56:52
| Not valid after:  2024-08-17T14:56:52
| MD5:   ef08:2ac1:6579:bf34:cfb6:5f09:c0fc:4f28
| SHA-1: eac1:2a17:05b6:54b1:0cdd:a59f:942e:8c50:d77f:9a10
| -----BEGIN CERTIFICATE-----
| MIIC1DCCAbygAwIBAgIQQOkcKOJNI5FEsP4hJvNFEjANBgkqhkiG9w0BAQsFADAT
| MREwDwYDVQQDEwhSZXRyb1dlYjAeFw0yNDAyMTYxNDU2NTJaFw0yNDA4MTcxNDU2
| NTJaMBMxETAPBgNVBAMTCFJldHJvV2ViMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
| MIIBCgKCAQEAofLoPkz0r6KwTtCOEsTS5Vs09WtOivcHu1eTQ3ezJdD4mXyLr2Uf
| 1Trzbyjbkcv0g+HUxMAFZ3L3mM+gpShHwbU6M9NkX/hZskipobxRk41Y+JFXccve
| RoXeLbmJndBuY5qQJ1fzR+WOkYiLzCON84G8ccRStUFEdTWnq/SltthHXsMD5iGY
| buxipNUDRpyB9cww2GH87WaJWNfapANin9lMLrxU98lBMNnJFeGeS9WFeanJ6FdS
| LGdzEUh6sAqtQoq/AT9D+I0QWKkS7+BfalAJocP3sPssia11dNnMHlj5FuH8OBe0
| xfOLfoEsWKjMTItn9fTD6lPLnNgwSx26aQIDAQABoyQwIjATBgNVHSUEDDAKBggr
| BgEFBQcDATALBgNVHQ8EBAMCBDAwDQYJKoZIhvcNAQELBQADggEBAIiJlpsRpx4B
| mEvmY5pjP6Y57g2OfewIN3C19Vjbaj3zHRjq/SH87W8TWEY0nqaeDWedjCUcDIwc
| U938lLHne+IR0OdiNqquYV8+0K5ell+jqOhj0HmBQg1yv9GH3xgXv3AaQ4MLpDax
```

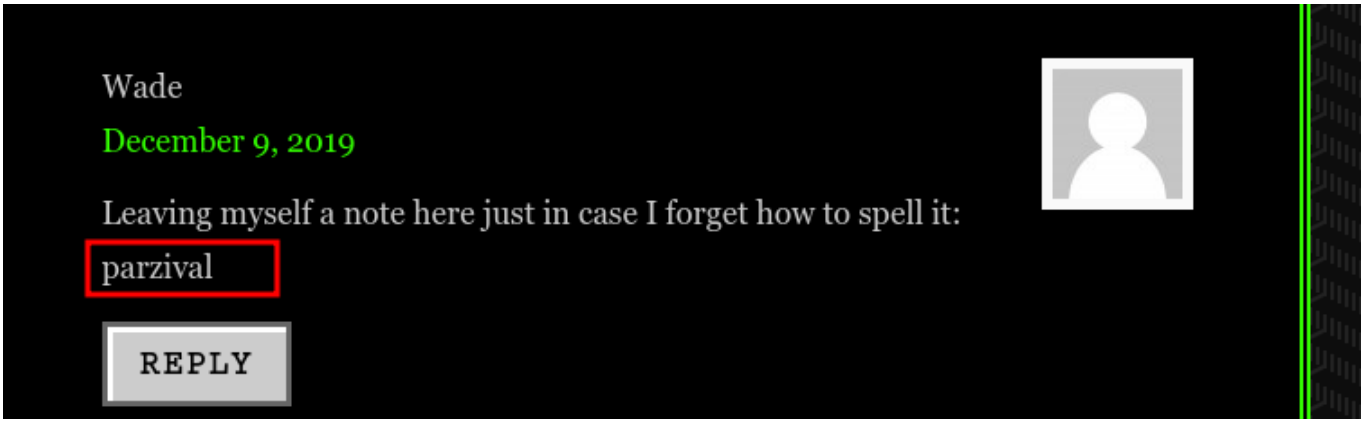
```
| 2tVHpAumKP2/o19u86mUmITghRf+biDyLbVf7tNQMgh94zWgoSf44UuipW0uQQ8a
| wHhbgK69Yfe6XC/NUecSIylyFirKXvsVjspn1DUkmGigrEZ08ch6CY3WMVQ3+KYb
| ismltQ3AnnzAb5ZdHWkSnud3RAwPba3I+u0sWo+uEwdcefpGyx/0rXFU+WHNpMeK
| I4XvRGgOkkM=
|_-----END CERTIFICATE-----
| rdp-ntlm-info:
|   Target_Name: RETROWEB
|   NetBIOS_Domain_Name: RETROWEB
|   NetBIOS_Computer_Name: RETROWEB
|   DNS_Domain_Name: RetroWeb
|   DNS_Computer_Name: RetroWeb
|   Product_Version: 10.0.14393
|_  System_Time: 2024-02-17T15:39:28+00:00
|_ssl-date: 2024-02-17T15:39:32+00:00; -2s from scanner time.
Warning: OSScan results may be unreliable because we could not find at least 1 o
closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplet
No OS matches for host
TCP/IP fingerprint:
SCAN(V=7.94SVN%E=4%D=2/17%OT=80%CT=%CU=%PV=Y%DS=5%DC=T%G=N%TM=65D0D336%P=x86_64-
gnu)
SEQ(SP=104%GCD=1%ISR=10A%TI=I%TS=A)
OPS(O1=M508NW8ST11%O2=M508NW8ST11%O3=M508NW8NNT11%O4=M508NW8ST11%O5=M508NW8ST11%
WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%W6=2000)
ECN(R=Y%DF=Y%TG=80%W=2000%O=M508NW8NNS%CC=Y%Q=)
T1(R=Y%DF=Y%TG=80%S=O%A=S+%F=AS%RD=0%Q=)
T2(R=N)
T3(R=N)
T4(R=N)
U1(R=N)
IE(R=N)

Uptime guess: 0.030 days (since Sat Feb 17 20:26:06 2024)
Network Distance: 5 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -2s

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   31.73 ms  10.17.0.1
2   ... 4
5   153.96 ms 10.10.185.175

Read data files from: /usr/bin/../share/nmap
```

```
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Sat Feb 17 21:09:34 2024 -- 1 IP address (1 host up) scanned in 3
seconds
```

Using dirbuster found a website:



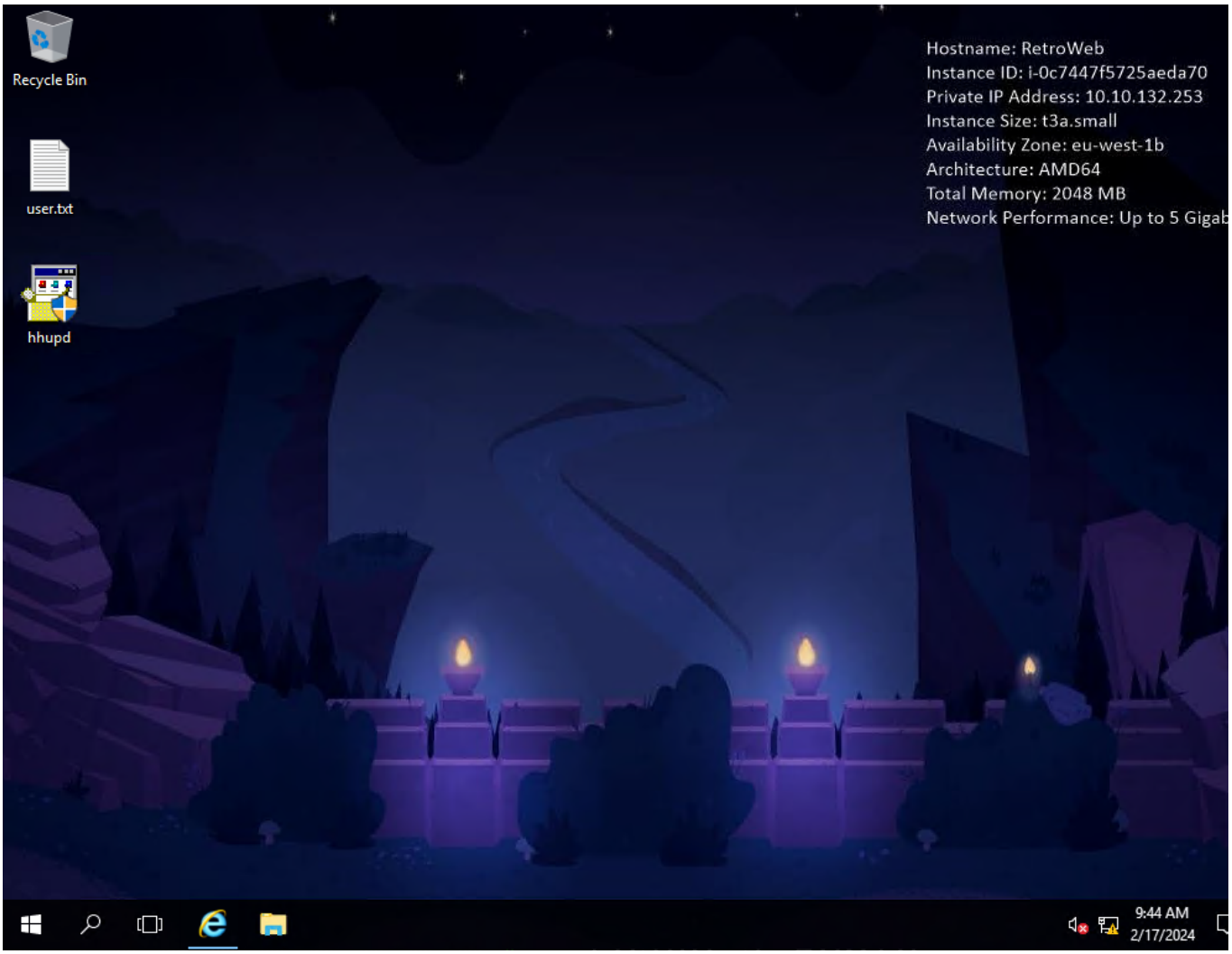
Found a potential password:



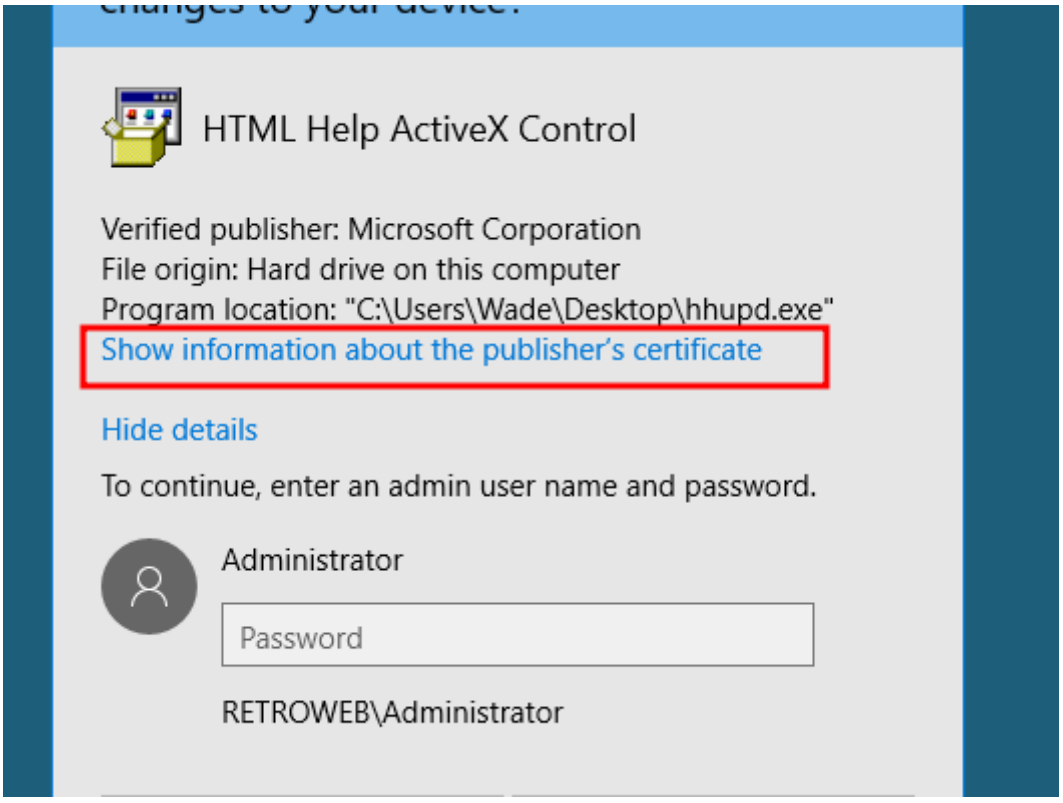
Exploitation

Now using rdp to login:

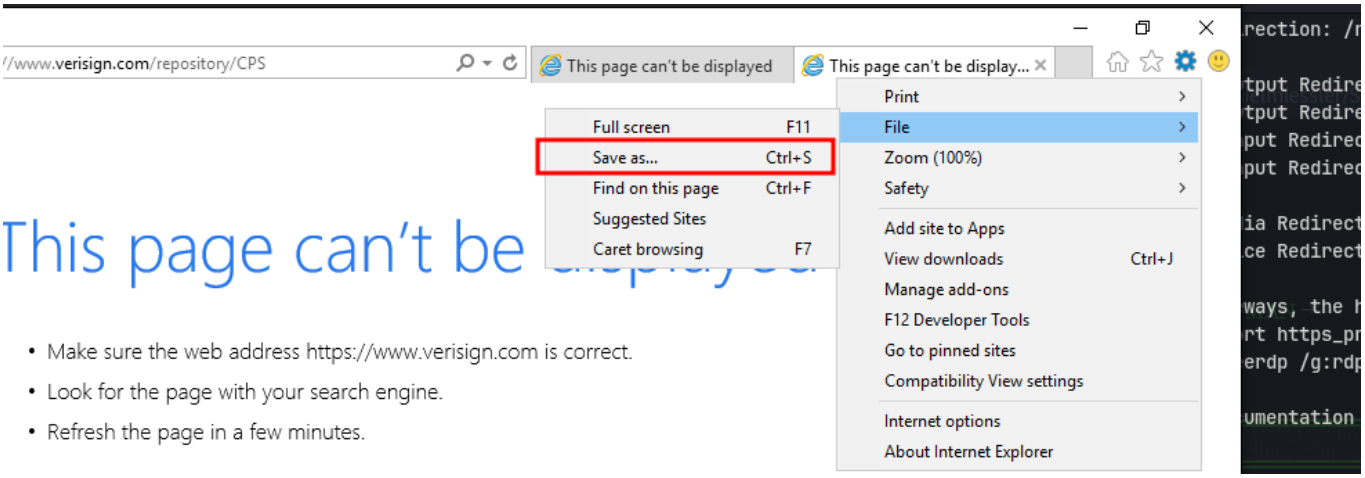
```
xfreerdp /u:Wade /v:10.10.132.253
```

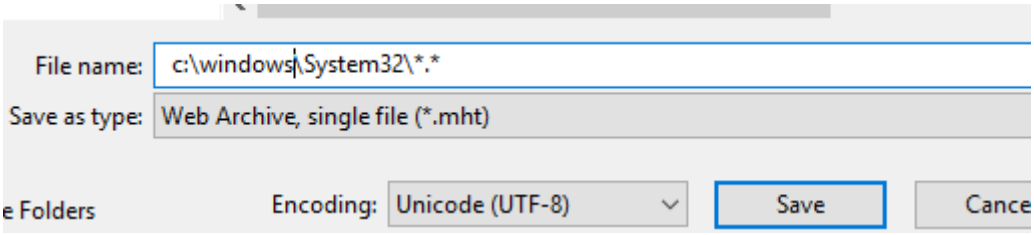


Running the hhupd app:



We get internet explorer as system





This lets use open cmd.exe