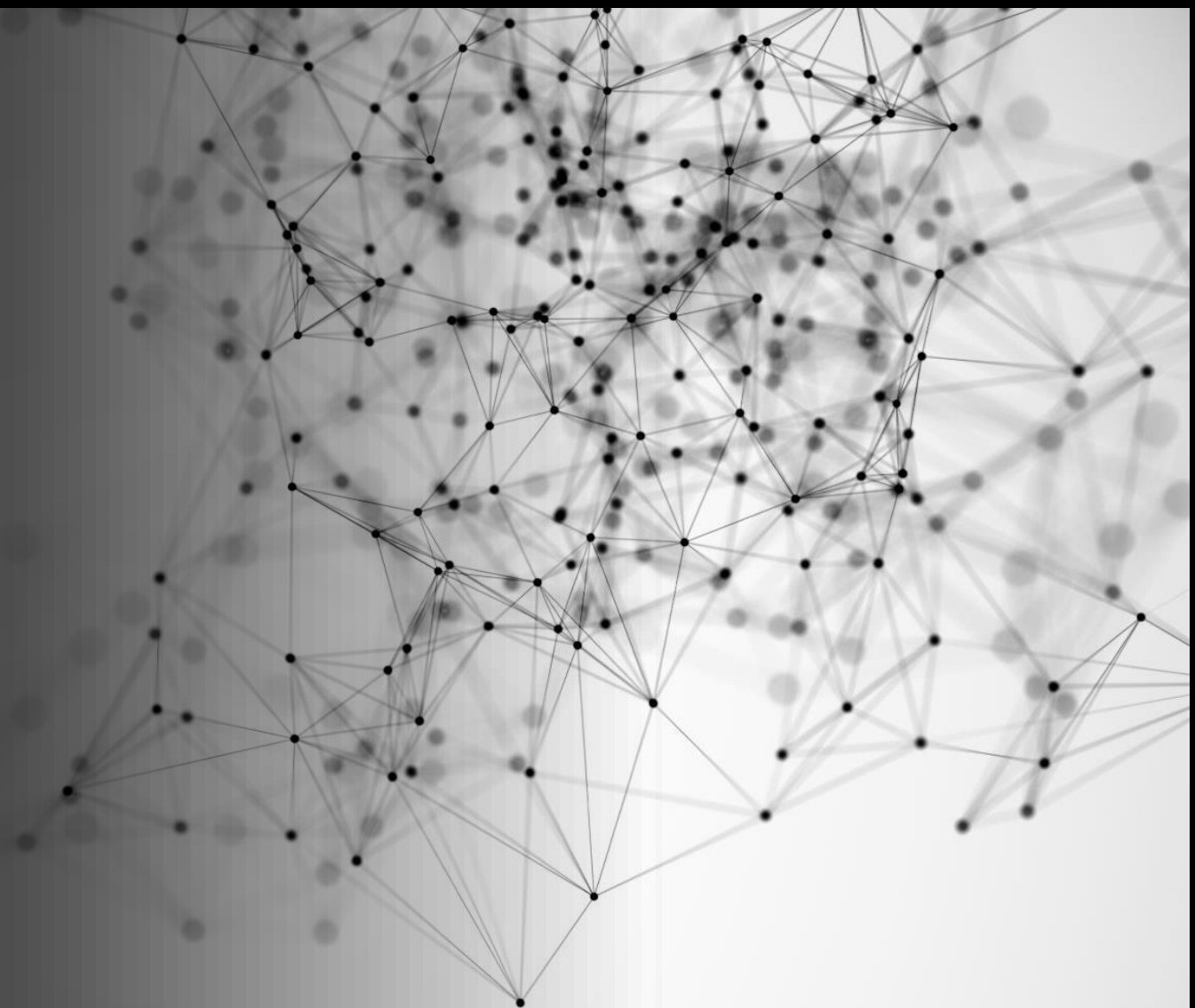




# Raport z Testów Penetracyjnych TryHackME "Retro" Michał Lissowski

---



Tester i autor raportu	Michał Lissowski Michallissowski@gmail.com
Miejsce wykonania	Gdańsk
Data wykonania	26.11.2022
Testowana aplikacja/system	Windows server 2016 , WordPress

Niniejszy dokument jest podsumowaniem testu penetracyjnego wykonanego na <https://tryhackme.com/room/Retro> .

# Skanywanie Nmap

Skanywanie nmapem pokazało 2 otwarte porty, 80 i 3389.

Nie znaleziono żadnych podatności.

```
Starting Nmap 7.60 ( https://nmap.org ) at 2022-11-26 14:52 GMT
Nmap scan report for ip-10-10-236-189.eu-west-1.compute.internal (10.10.236.189)
Host is up (0.00049s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft IIS httpd 10.0
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-title: IIS Windows Server
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
|_ssl-ccs-injection: No reply from server (TIMEOUT)
|_ssl-cert: Subject: commonName=RetroWeb
|_  Not valid before: 2022-11-25T14:50:08
|_  Not valid after: 2023-05-27T14:50:08
|_ssl-date: 2022-11-26T14:52:58+00:00; 0s from scanner time.
|_sslv2-drown:
MAC Address: 02:48:43:EE:8F:87 (Unknown)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 157.67 seconds
```

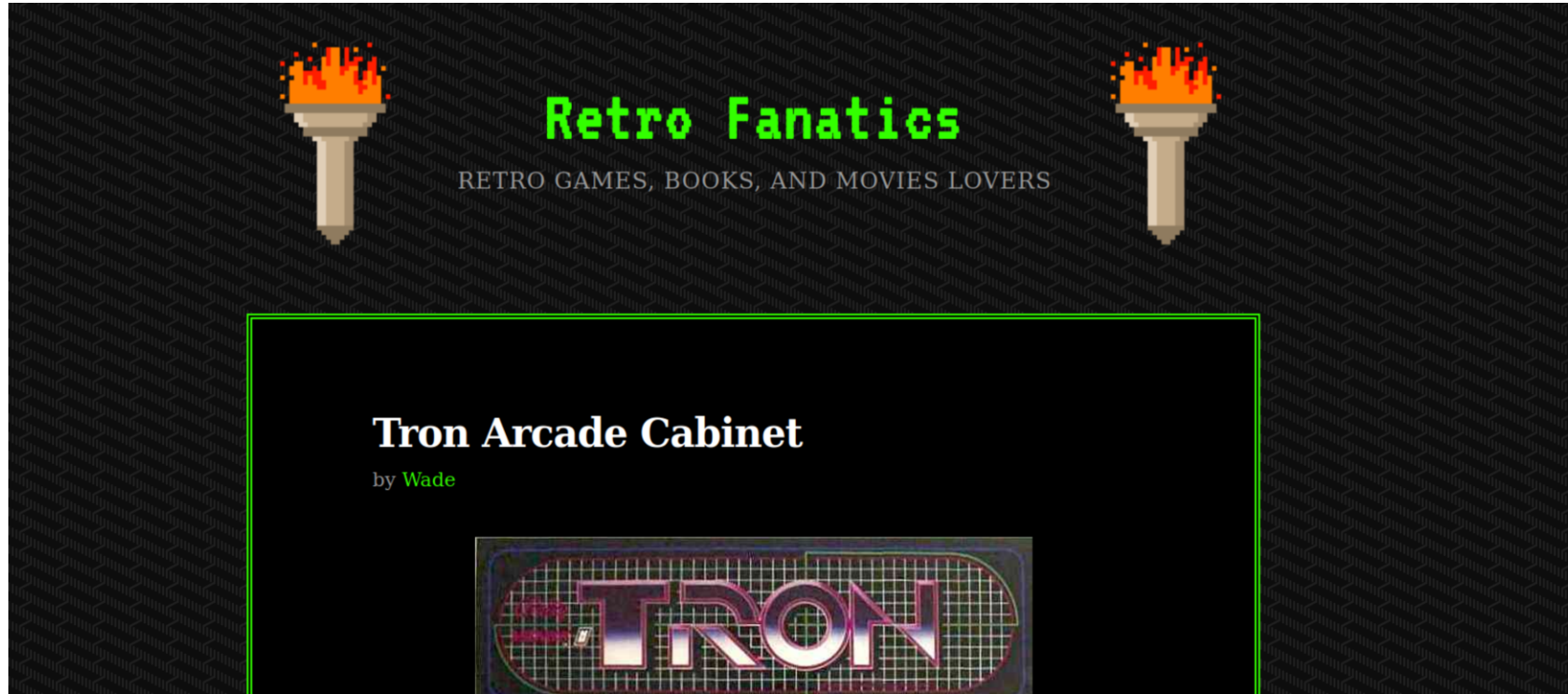
# Rekonesans

Za pomocą gobuster udało się znaleźć ukryty katalog, "/retro".

```
root@ip-10-10-211-42:~# gobuster dir -u 10.10.236.189 -w /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-small.txt -x php,html,txt -k

=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://10.10.236.189
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-small.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:    gobuster/3.0.1
[+] Extensions:  php,html,txt
[+] Timeout:      10s
=====
2022/11/26 14:59:53 Starting gobuster
=====
/retro (Status: 301)
/Retro (Status: 301)
```

Po wejściu na /Retro widzimy stronę. Po analizie można łatwo wywnioskować że użytkownikiem jest "wade".



Na stronie znajdują się posty tego użytkownika w którym znaleźć można  
Hasło : parzival.

## One Comment on “Ready Player One”

Wade  
December 9, 2019

Leaving myself a note here just in case I forget how to spell it: parzival

REPLY

## Leave a Reply

Your email address will not be published.  
Required fields are marked \*

Comment

December 2019

CATEGORIES

Uncategorized

META

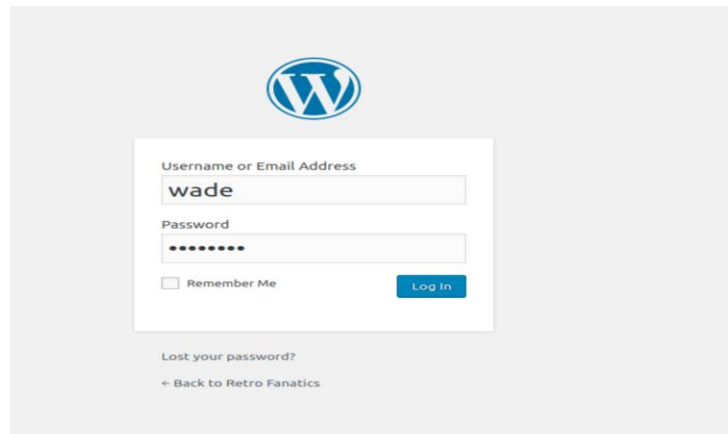
Log in

Entries RSS

Comments RSS

WordPress.org

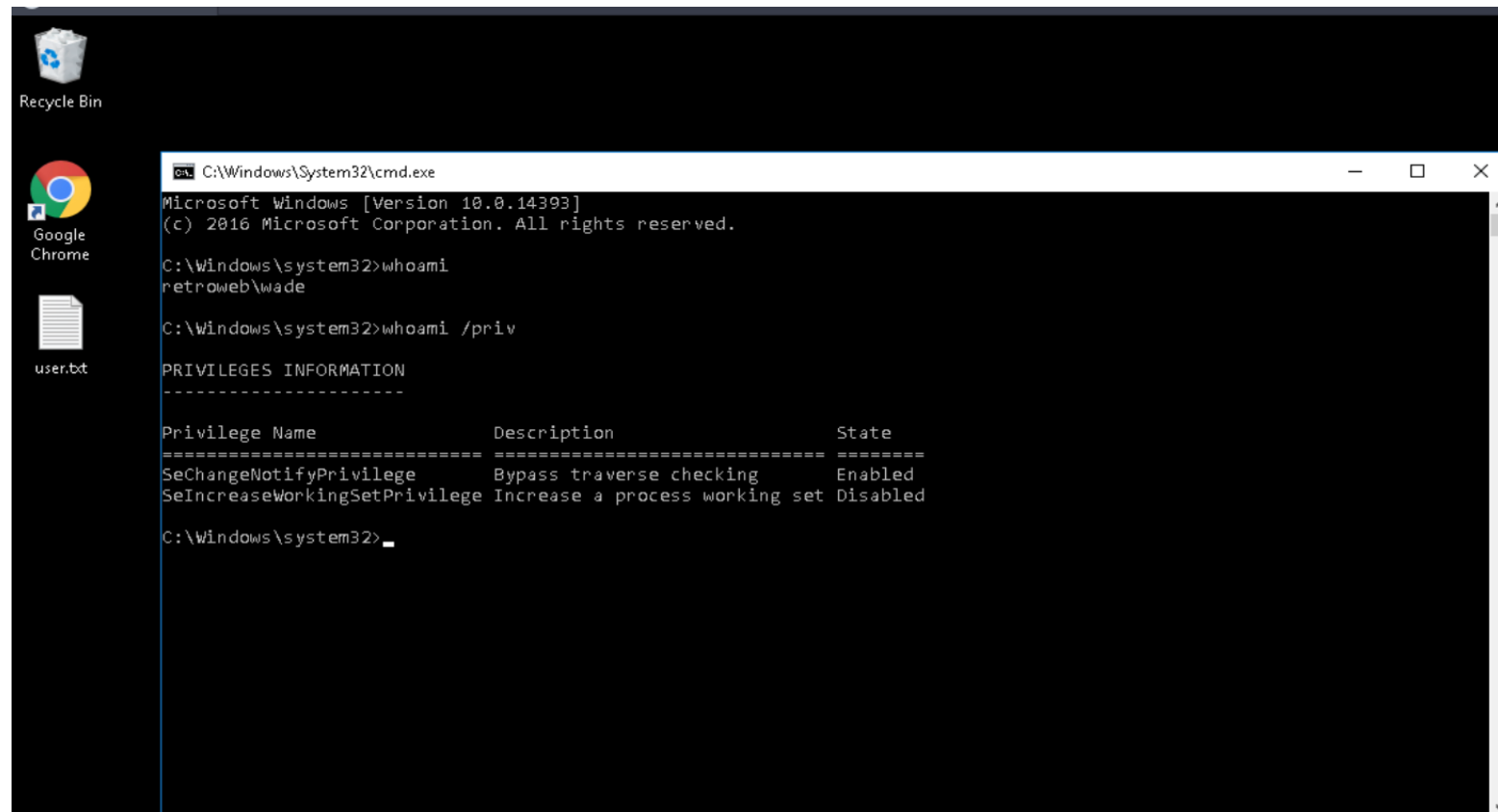
Strona pozwala na zalogowanie się za pomocy odnośnika " Log in". Przekieruje nas do panelu WordPress. Po zalogowaniu, próba "revers shell monkey" nie za działała <http://10.10.236.189/retro/wp-content/themes/90s-retro/404.php>

A screenshot of the WordPress login page. At the top center is the WordPress logo, a blue 'W' inside a circle. Below it is a white rectangular login form. The form has two input fields: the first is labeled 'Username or Email Address' and contains the text 'wade'; the second is labeled 'Password' and contains ten black dots. Below the password field is a checkbox labeled 'Remember Me'. To the right of the checkbox is a blue button with the text 'Log In' in white. Below the login form, there is a link that says 'Lost your password?' and a link that says '← Back to Retro Fanatics'.



# Eskalacja uprawnień

Hasło i Login pozwolił na połączenie się przez RDP na użytkownika wade.  
Komenda "whoami /priv" nie pokazała nic interesującego.



The screenshot shows a Windows desktop with a dark background. On the left sidebar, there are icons for the Recycle Bin, Google Chrome, and a file named 'user.txt'. A command prompt window is open, displaying the following text:

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
retroweb\wade

C:\Windows\system32>whoami /priv

PRIVILEGES INFORMATION
-----
Privilege Name            Description                State
-----
SeChangeNotifyPrivilege   Bypass traverse checking   Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled

C:\Windows\system32>
```



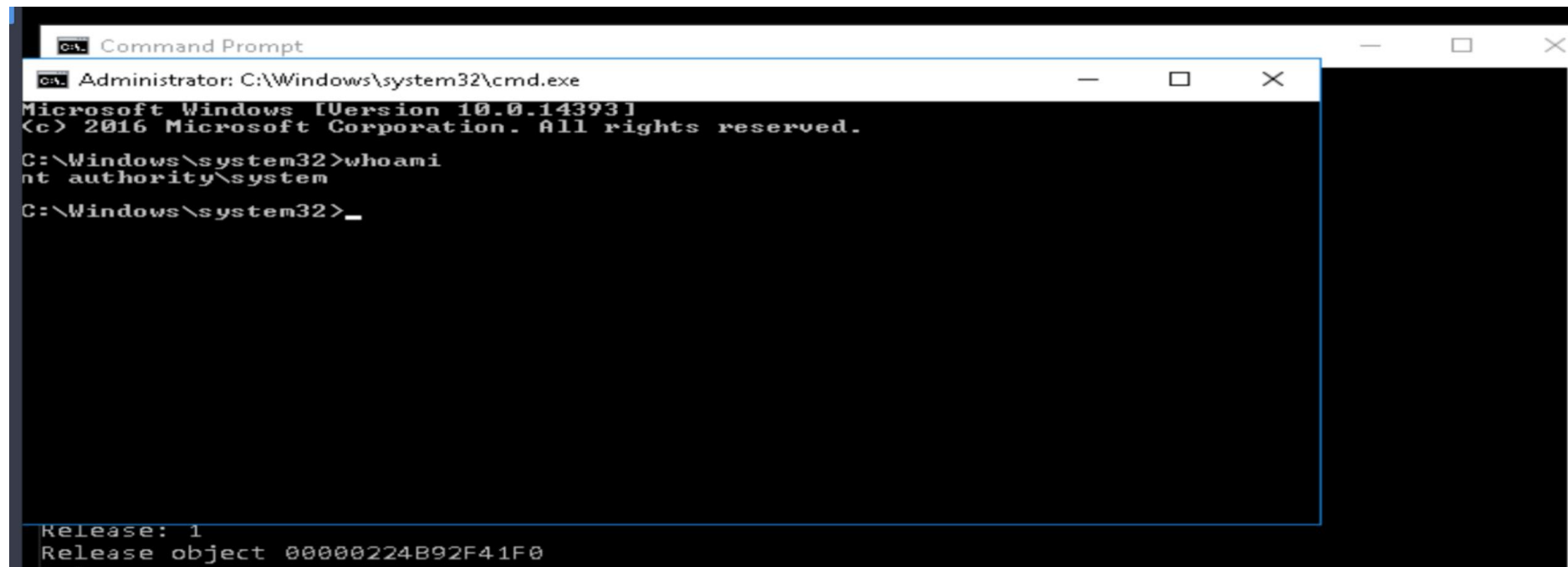
Komenda "systeminfo" dała wynik :

```
C:\Windows\system32>systeminfo

Host Name:                RETROWEB
OS Name:                  Microsoft Windows Server 2016 Standard
OS Version:               10.0.14393 N/A Build 14393
OS Manufacturer:         Microsoft Corporation
OS Configuration:        Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:         Windows User
Registered Organization:
Product ID:                00377-60000-00000-AA325
Original Install Date:     12/8/2019, 10:50:43 PM
System Boot Time:          11/26/2022, 6:49:12 AM
System Manufacturer:       Xen
System Model:              HVM domU
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 79 Stepping 1 GenuineIntel ~2300 Mhz
BIOS Version:              Xen 4.11.amazon, 8/24/2006
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:                \Device\HarddiskVolume1
System Locale:              en-us;English (United States)
Input Locale:               en-us;English (United States)
Time Zone:                  (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory:      2,048 MB
Available Physical Memory:  1,075 MB
Virtual Memory: Max Size:   3,200 MB
Virtual Memory: Available:  2,154 MB
Virtual Memory: In Use:     1,046 MB
Page File Location(s):      C:\pagefile.sys
```

Dana wersja windowsa jest podatna na exploita CVE-2017-0213 który pomoże w eskalacji uprawnień.

Po pobraniu Exploita, wysłaniu i uruchomieniu, automatycznie uzyskujemy dostęp do administratora.



The image shows a Windows Command Prompt window titled "Command Prompt". The window is running as an administrator, as indicated by the title bar "Administrator: C:\Windows\system32\cmd.exe". The prompt shows the following text:

```
Microsoft Windows [Version 10.0.14393]  
<c> 2016 Microsoft Corporation. All rights reserved.  
  
C:\Windows\system32>whoami  
nt authority\system  
  
C:\Windows\system32>_
```

At the bottom of the window, the text "Release: 1" and "Release object 00000224B92F41F0" is visible.

# Podatności i naprawa

Treści poufne nie powinny być wystawiane w łatwo dostępnym miejscach dla osób trzecich. Na serwerze udało się znaleźć hasło i użytkownika. Należy je zabezpieczyć.

CVE-2017-0213 : Windows COM Aggregate Marshaler w systemach Microsoft Windows Server 2008 z dodatkiem SP2 i R2 z dodatkiem SP1, Windows 7 z dodatkiem SP1, Windows 8.1, Windows Server 2012 Gold i R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607 i 1703 oraz Windows Server 2016 umożliwia podniesienie uprawnień luka w zabezpieczeniach polegająca na podniesieniu uprawnień, gdy osoba atakująca uruchamia specjalnie spreparowaną aplikację, zwaną również „luką w zabezpieczeniach Windows COM Elevation of Privilege”.

Należy zaktualizować system do najnowszej wersji.