
ATTACK
DEFENSE
by PentesterAcademy

Name	Windows Recon: IIS: Nmap Scripts
URL	https://attackdefense.com/challengedetails?cid=2312
Type	Windows Recon: IIS

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Step 1: Checking the target IP address.

Note: The target IP address is stored in the "**target**" file.

Command: cat /root/Desktop/target

```
root@attackdefense:~# zsh
┌──(root㉿attackdefense)-[~]
└─# cat /root/Desktop/target
Target IP Address : 10.0.28.146

┌──(root㉿attackdefense)-[~]
└─#
```

Step 2: Run a Nmap scan against the target IP.

Command: nmap 10.0.28.146

```
┌──(root💀 attackdefense)-[~]
└─# nmap 10.0.28.146
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-07 16:44 IST
Nmap scan report for ip-10-0-28-146.ap-southeast-1.compute.internal (10.0.28.146)
Host is up (0.0011s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
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 1.68 seconds

┌──(root💀 attackdefense)-[~]
└─#
```

Step 3: We have discovered that multiple ports are open. We will be focusing on port 80 where the IIS server is running.

Running http-enum nmap script to discover interesting directories.

Command: nmap --script http-enum -sV -p 80 10.0.28.146

```
┌──(root💀 attackdefense)-[~]
└─# nmap --script http-enum -sV -p 80 10.0.28.146
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-07 16:45 IST
Nmap scan report for ip-10-0-28-146.ap-southeast-1.compute.internal (10.0.28.146)
Host is up (0.0015s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 10.0
| http-enum:
|   /content/: Potentially interesting folder
|   /downloads/: Potentially interesting folder
|_  /webdav/: Potentially interesting folder
|_http-server-header: Microsoft-IIS/10.0
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.81 seconds

┌──(root💀 attackdefense)-[~]
└─#
```

We have found three interesting directories i.e content, downloads, and webdav.

Step 4: Running Header script to get the IIS server header information.

Command: nmap --script http-headers -sV -p 80 10.0.28.146

```
┌──(root㉿attackdefense)-[~]
└─# nmap --script http-headers -sV -p 80 10.0.28.146
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-07 16:46 IST
Nmap scan report for ip-10-0-28-146.ap-southeast-1.compute.internal (10.0.28.146)
Host is up (0.0013s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 10.0
| http-headers:
|   Cache-Control: private
|   Content-Type: text/html; charset=utf-8
|   Location: /Default.aspx
|   Server: Microsoft-IIS/10.0
|   Set-Cookie: ASP.NET_SessionId=1sc3udrc05cg225ihfzxsitc; path=/; HttpOnly; SameSite=Lax
|   X-AspNet-Version: 4.0.30319
|   Set-Cookie: Server=RE9UTkVUR09BVA==; path=/
|   X-XSS-Protection: 0
|   X-Powered-By: ASP.NET
|   Date: Thu, 07 Jan 2021 11:16:24 GMT
|   Connection: close
|   Content-Length: 130
|
|_  (Request type: GET)
|_http-server-header: Microsoft-IIS/10.0
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.77 seconds

┌──(root㉿attackdefense)-[~]
└─#
```

Using the Nmap header script, we found information about the running IIS Server as mentioned below.

- IIS Server version is 10.0
- ASP.NET Version is 4.0.30319
- XSS Protection is 0
- The default page of the target web application is /Default.aspx

Step 5: Running http-methods script on /webdav path to discover all allowed methods.

Command: nmap --script http-methods --script-args http-methods.url-path=/webdav/ 10.0.28.146

```
┌──(root㉿attackdefense)-[~]
└─# nmap --script http-methods --script-args http-methods.url-path=/webdav/ 10.0.28.146

Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-07 16:49 IST
Nmap scan report for ip-10-0-28-146.ap-southeast-1.compute.internal (10.0.28.146)
Host is up (0.0013s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
80/tcp   open  http
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST COPY PROPFIND DELETE MOVE PROPPATCH MKCOL LOCK UNLOCK PUT
|   Potentially risky methods: TRACE COPY PROPFIND DELETE MOVE PROPPATCH MKCOL LOCK UNLOCK PUT
|_  Path tested: /webdav/
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
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 1.92 seconds

┌──(root㉿attackdefense)-[~]
└─#
```

We have discovered all supported methods on /webdav directory.

Step 6: Running webdav scan Nmap script to identify WebDAV installations the script uses the OPTIONS and PROPFIND methods to detect it.

Command: nmap --script http-webdav-scan --script-args http-methods.url-path=/webdav/ 10.0.28.146

```
┌──(root㉿attackdefense)-[~]
└─# nmap --script http-webdav-scan --script-args http-methods.url-path=/webdav/ 10.0.28.146
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-07 16:51 IST
Nmap scan report for ip-10-0-28-146.ap-southeast-1.compute.internal (10.0.28.146)
Host is up (0.0012s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
80/tcp   open  http
| http-webdav-scan:
|   Public Options: OPTIONS, TRACE, GET, HEAD, POST, PROPFIND, PROPPATCH, MKCOL, PUT, DELETE, COPY, MOVE, LOCK, UNLOCK
|   Allowed Methods: OPTIONS, TRACE, GET, HEAD, POST, COPY, PROPFIND, LOCK, UNLOCK
|   Server Type: Microsoft-IIS/10.0
|   Server Date: Thu, 07 Jan 2021 11:21:15 GMT
|_  WebDAV type: Unknown
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
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 2.18 seconds

┌──(root㉿attackdefense)-[~]
└─#
```

References:

1. Nmap (https://nmap.org/)
2. Nmap scripts (https://nmap.org/nsedoc/scripts/)