
ATTACK
DEFENSE
by PentesterAcademy

Name	Windows Recon: IIS
URL	https://attackdefense.com/challengedetails?cid=2311
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 : 10.0.29.163

┌──(root㉿attackdefense)-[~]
└─#
```

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

Command: nmap 10.0.29.163

```
┌──(root💀 attackdefense)-[~]
└─# nmap 10.0.29.163
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-07 11:33 IST
Nmap scan report for ip-10-0-29-163.ap-southeast-1.compute.internal (10.0.29.163)
Host is up (0.0012s 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 1.67 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 whatweb tool to find all possible information about the target server.

Command: whatweb 10.0.29.163

```
┌──(root💀 attackdefense)-[~]
└─# whatweb 10.0.29.163
http://10.0.29.163 [302 Found] ASP_NET[4.0.30319], Cookies[ASP.NET_SessionId,Server], Count
ry[RESERVED][ZZ], HTTPServer[Microsoft-IIS/10.0], HttpOnly[ASP.NET_SessionId], IP[10.0.29.1
63], Microsoft-IIS[10.0], RedirectLocation[/Default.aspx], Title[Object moved], X-Powered-B
y[ASP.NET], X-XSS-Protection[0]
http://10.0.29.163/Default.aspx [302 Found] ASP_NET[4.0.30319], Cookies[ASP.NET_SessionId,S
erver], Country[RESERVED][ZZ], HTTPServer[Microsoft-IIS/10.0], HttpOnly[ASP.NET_SessionId],
 IP[10.0.29.163], Microsoft-IIS[10.0], RedirectLocation[/Default.aspx], Title[Object moved]
, X-Powered-By[ASP.NET], X-XSS-Protection[0]

┌──(root💀 attackdefense)-[~]
└─#
```

Using the whatweb tool 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 4: We could also use the [httpie] tool to gather target server information.

Command: http 10.0.29.163

```
┌──(root㉿attackdefense)-[~]
└─# http 10.0.29.163
HTTP/1.1 302 Found
Cache-Control: private
Content-Length: 130
Content-Type: text/html; charset=utf-8
Date: Thu, 07 Jan 2021 06:15:56 GMT
Location: /Default.aspx
Server: Microsoft-IIS/10.0
Set-Cookie: ASP.NET_SessionId=mfqus2njvlabdu5iyg5aykuw; path=/; HttpOnly; SameSite=Lax
Set-Cookie: Server=RE9UTkVUR09BVA==; path=/
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
X-XSS-Protection: 0

<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="/Default.aspx">here</a>.</h2>
</body></html>


┌──(root㉿attackdefense)-[~]
└─#
```

Step 5: Running the dirb tool on the target server port 80 to discover the web server's directories and subdirectories.

Command: dirb http://10.0.29.163

```
┌──(root㉿attackdefense)-[~]
└─# dirb http://10.0.29.163

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Jan  7 11:40:16 2021
URL_BASE: http://10.0.29.163/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.0.29.163/ ----
==> DIRECTORY: http://10.0.29.163/app_themes/
==> DIRECTORY: http://10.0.29.163/aspnet_client/
==> DIRECTORY: http://10.0.29.163/configuration/
==> DIRECTORY: http://10.0.29.163/content/
==> DIRECTORY: http://10.0.29.163/Content/
==> DIRECTORY: http://10.0.29.163/downloads/
==> DIRECTORY: http://10.0.29.163/Downloads/
==> DIRECTORY: http://10.0.29.163/resources/
==> DIRECTORY: http://10.0.29.163/Resources/
```

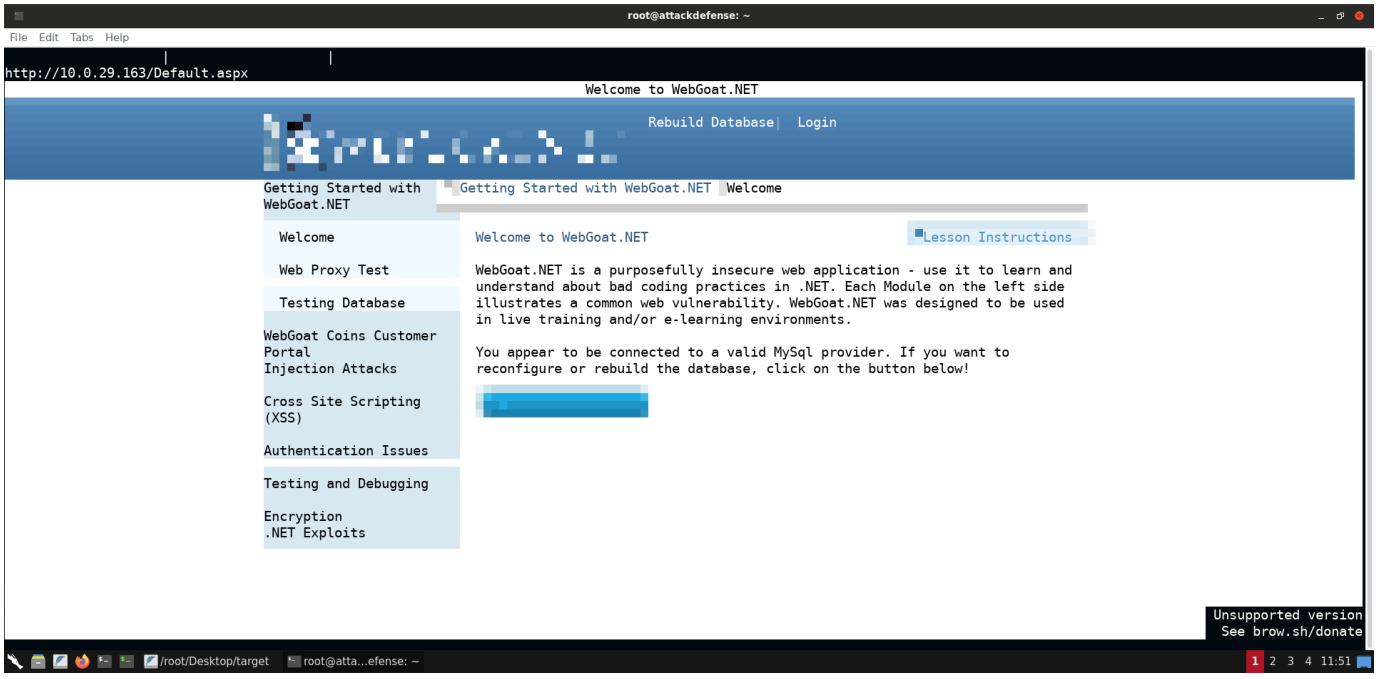
```
---- Entering directory: http://10.0.29.163/app_themes/ ----
==> DIRECTORY: http://10.0.29.163/app_themes/default/
==> DIRECTORY: http://10.0.29.163/app_themes/Default/

---- Entering directory: http://10.0.29.163/aspnet_client/ ----
==> DIRECTORY: http://10.0.29.163/aspnet_client/system_web/

---- Entering directory: http://10.0.29.163/configuration/ ----

---- Entering directory: http://10.0.29.163/content/ ----

---- Entering directory: http://10.0.29.163/Content/ ----

---- Entering directory: http://10.0.29.163/downloads/ ----

---- Entering directory: http://10.0.29.163/Downloads/ ----

---- Entering directory: http://10.0.29.163/resources/ ----
==> DIRECTORY: http://10.0.29.163/resources/images/
==> DIRECTORY: http://10.0.29.163/resources/Images/

---- Entering directory: http://10.0.29.163/Resources/ ----
==> DIRECTORY: http://10.0.29.163/Resources/images/
==> DIRECTORY: http://10.0.29.163/Resources/Images/
```

```
---- Entering directory: http://10.0.29.163/app_themes/Default/ ----
==> DIRECTORY: http://10.0.29.163/app_themes/Default/images/
==> DIRECTORY: http://10.0.29.163/app_themes/Default/Images/

---- Entering directory: http://10.0.29.163/aspnet_client/system_web/ ----

---- Entering directory: http://10.0.29.163/resources/images/ ----

---- Entering directory: http://10.0.29.163/resources/Images/ ----

---- Entering directory: http://10.0.29.163/Resources/images/ ----

---- Entering directory: http://10.0.29.163/Resources/Images/ ----

---- Entering directory: http://10.0.29.163/app_themes/default/images/ ----
==> DIRECTORY: http://10.0.29.163/app_themes/default/images/extras/
==> DIRECTORY: http://10.0.29.163/app_themes/default/images/listing/

---- Entering directory: http://10.0.29.163/app_themes/default/Images/ ----
==> DIRECTORY: http://10.0.29.163/app_themes/default/Images/extras/
==> DIRECTORY: http://10.0.29.163/app_themes/default/Images/listing/

---- Entering directory: http://10.0.29.163/app_themes/Default/images/ ----
==> DIRECTORY: http://10.0.29.163/app_themes/Default/images/extras/
==> DIRECTORY: http://10.0.29.163/app_themes/Default/images/listing/

---- Entering directory: http://10.0.29.163/app_themes/Default/Images/ ----
==> DIRECTORY: http://10.0.29.163/app_themes/Default/Images/extras/
==> DIRECTORY: http://10.0.29.163/app_themes/Default/Images/listing/
```

Step 6: We have found all the basic details about the target server without using the browser. We could also use browsh “A fully-modern text-based browser, rendering to TTY and browsers”

This utility is useful when we don’t have a browser i.e Firefox, Chrome, etc. to access the target application and we have to use the terminal to access the web application.

Command: browsh --startup-url http://10.0.29.163/Default.aspx



We can notice, the browsh has rendered the target application in the text-based browser and we have discovered that the target application is WebGoat.Net.

References:

1. Httpie (https://httpie.io/)
2. WhatWeb (https://github.com/urbanadventurer/WhatWeb)
3. Browsh (https://github.com/browsh-org/browsh)