Devel, while relatively simple, demonstrates the security risks associated with some default program configurations. It is a beginner-level machine which can be completed using publicly available exploits.

Running nmap show ftp with anonymous login and a webserver which has a link to : https://www.iis.net/?utm\_medium=iis-deployment

A screenshot of a computer

AI-generated content may be incorrect.

FTP inside and we have the directories of the webpage.

A computer screen shot of a black screen

AI-generated content may be incorrect.

We can upload msfvenom reverse tcp handler which we can then exploit with Metasploit.

The file should be aspx format. A screenshot of a computer

AI-generated content may be incorrect.



After we create the shell.aspx we need to upload it via ftp.

We simply type “put shell.aspx”.

Then we head to msfconsole and use “multi/handler” and very important, to set the payload for windows/meterpreter/reverse\_tcp.

We set our port and ip and enter “run”.

A screen shot of a computer

AI-generated content may be incorrect.

We enter the /shell.aspx and we now have a session.

We need to upgrade our shell in order to get the root flag so, the most simple way is to use local\_exploit\_suggester.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer screen

AI-generated content may be incorrect.

I’ll use kitrap0d because I’ve used it for a IIS before and it worked great.

A screenshot of a computer program

AI-generated content may be incorrect.

The flags are under Users/babis/Desktop/user.txt and Users/Administrator/Desktop/root.txt.

A screenshot of a computer

AI-generated content may be incorrect.