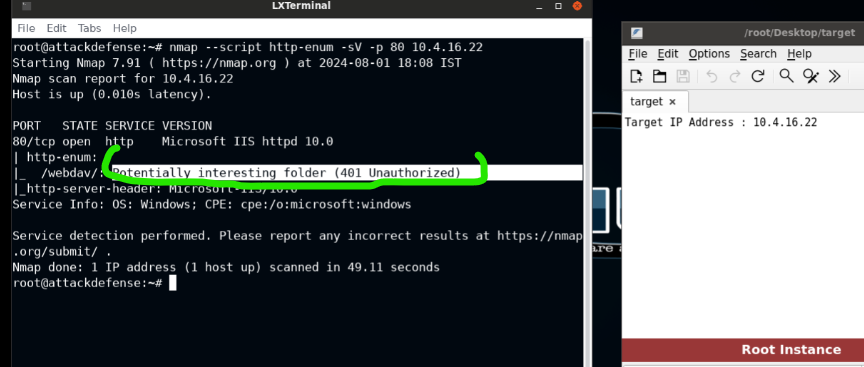
Web dav metasploit

Davtest looks for webDAV servers, which may allow us to execute code on the target system if certain vulnerabilities are found. This is a pen-testing tool.

As a given, the target ip is [10.0.17.27]. Port 80 is discovered open from a basic nmap scan just with nmap 10.0.17.27

The next step is to enumerate with http-enum as follows:

nmap --script http-enum -sV -p 80 10.0.17.27

Returns a folder labeled 401 unauthorized 

Assume another person in our team found the credentials to web-dav, being a username ‘bob’ and a password ‘password\_123321’. In our scenario, credentials are a given, perhaps swiped by one of our units infiltrating the physical location of the target (there is no overall scenario to make a coherent narrative from this lesson, but it would help a great deal to understand, rather than having all these floaty random things just flickering in and out of exisence).

We can test for webDav vulnerabilities quickly with :

davtest -auth bob:password\_123321 -url http://10.0.17.27/webdav

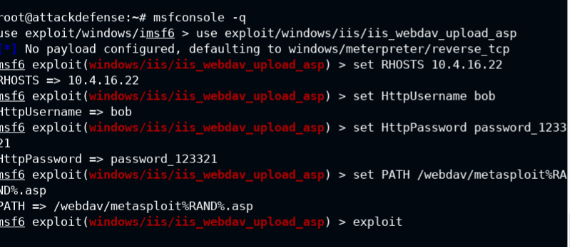
So, the results show a lot of put files, and all that noise is hard to parse, but the fact that anything responded at all is a pretty good shot that we can use a metasploit vulnerability here.

The course-work fails to explain how we identify the target exploit, but it’s assumed we will use ‘exploit/windows/iis/iis\_webdav\_upload\_asp’

How do we know this will work?

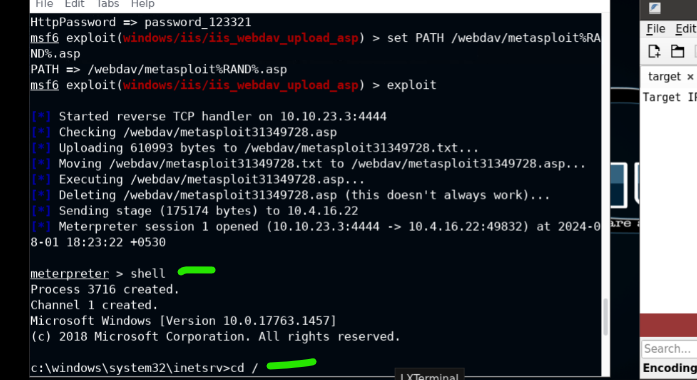
Don’t know, the teachers were too lazy to explain the significance, so we have to assume it’s a given. (blame INE for being scrubs, they’re the ones holding out on the explanation here)

The exploit allows us to open a shell into the target system and look at files (see screenshot for doing the configurations)



After the exploit runs, we can open a shell session into the target system.

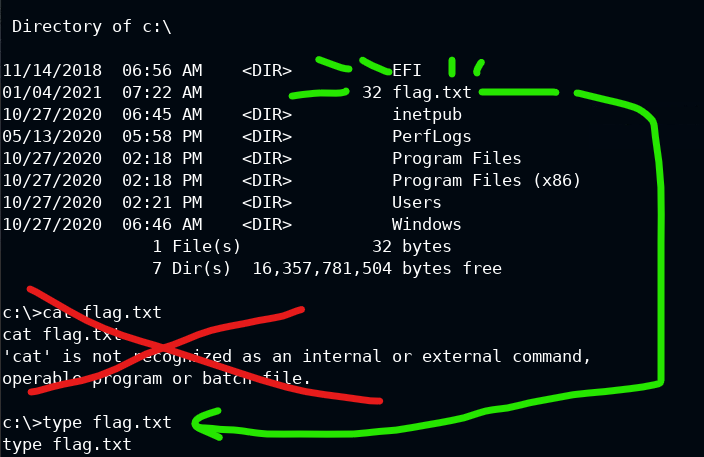
Thus, the expected behavior is that the above exploit offers us a shell session to get onto the target.



The ‘reverse TCP handler on [10.10.23.3]’ shows that we’re connecting to the target.

The rest is going through the motions of the exploit until the last blue-star, letting us know ‘meterpreter session 1 opened’. So, we’re specifically getting a meterpreter shell, but the linguistic difference between a “shell session” and a “meterpreter shell” is beyond the scope of this engagement, and INE certainly didn’t have a care in the world to clarify that little detail.

Point being, we can now change directories into the home, using the path of a single forward-slash.



From here, don’t be a n00b using “cat” out of idiotic habit, and instead use “type” because this is a shell session. That opens up the target file for the flag in this lab.