Exploit webDAV.... The Garage Way

Author:- micr0

Contact: micr0security@live.com

Thanks to garage4hackers and ICW

Well this paper is about the exploitation of webDAV service.

At the time of vulnerability assessment of web application we found out that the web application vulnerability scanner will show us a vulnerability which is webDAV enabled

This vulnerability is categorized as low level severity.

Actually this vulnerability can be used to manipulate the contain present in the web server and lot more.

Now the question is how can we exploit this vulnerability and how can we upload the files and download the files from the remote system?

Now just take a look at the Response of the server. And check what the options available to the public

Response
HTTP/1.1 200 OK
Connection: close
Date: Thu, 22 Dec 2011 10:15:59 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
MS-Author-Via: DAV
Content-Length: 0
Accept-Ranges: none
DASL: <DAV:sql>
DAV: 1, 2
Public: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
Allow: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK
Cache-Control: private

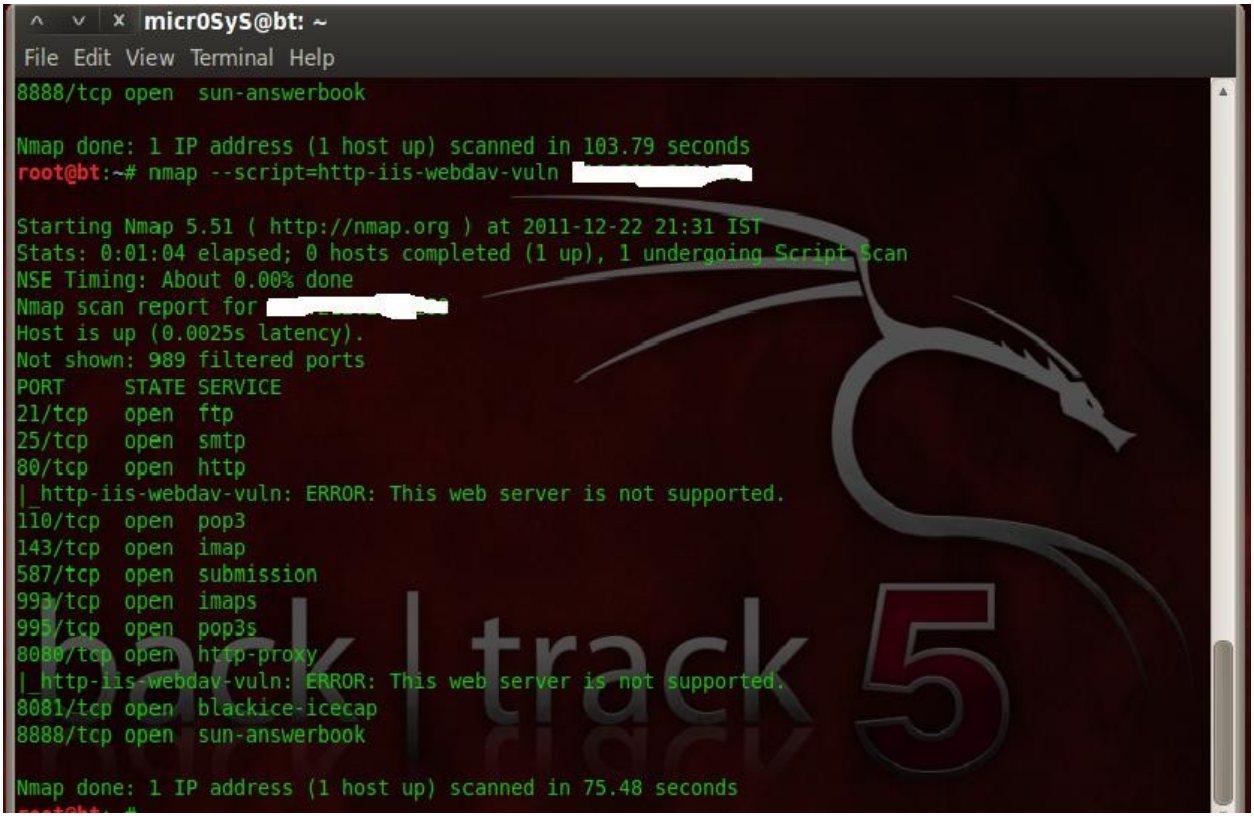
NOW we come to know that if we get an access over target host then we can put, get, move the files

To check this vulnerability out, we will use Nmap☺ the most useful tool in this kind stuff

The script which we will use for this is port-rule script which will help us to detect the vulnerable server

--script=http-iis-webdav-vuln REMOTE IP

After this you will get output like this



In this case now we are getting the output as the server is not vulnerable! Oh god ….

What to do now?

We have one another option: P

Let's search for a webDAV client now…

I used some webDAV client but I found http://www.webdav.org/cadaver/ this client very good

What you have to do is just get this application install on your box and run it ….

Make sure that you cadaver is updated and installed patch which is cadaaver-h4x

You can find it here http://www.skullsecurity.org/blogdata/cadaver-0.23.2-h4x.patch

Here we are ready with the stuff

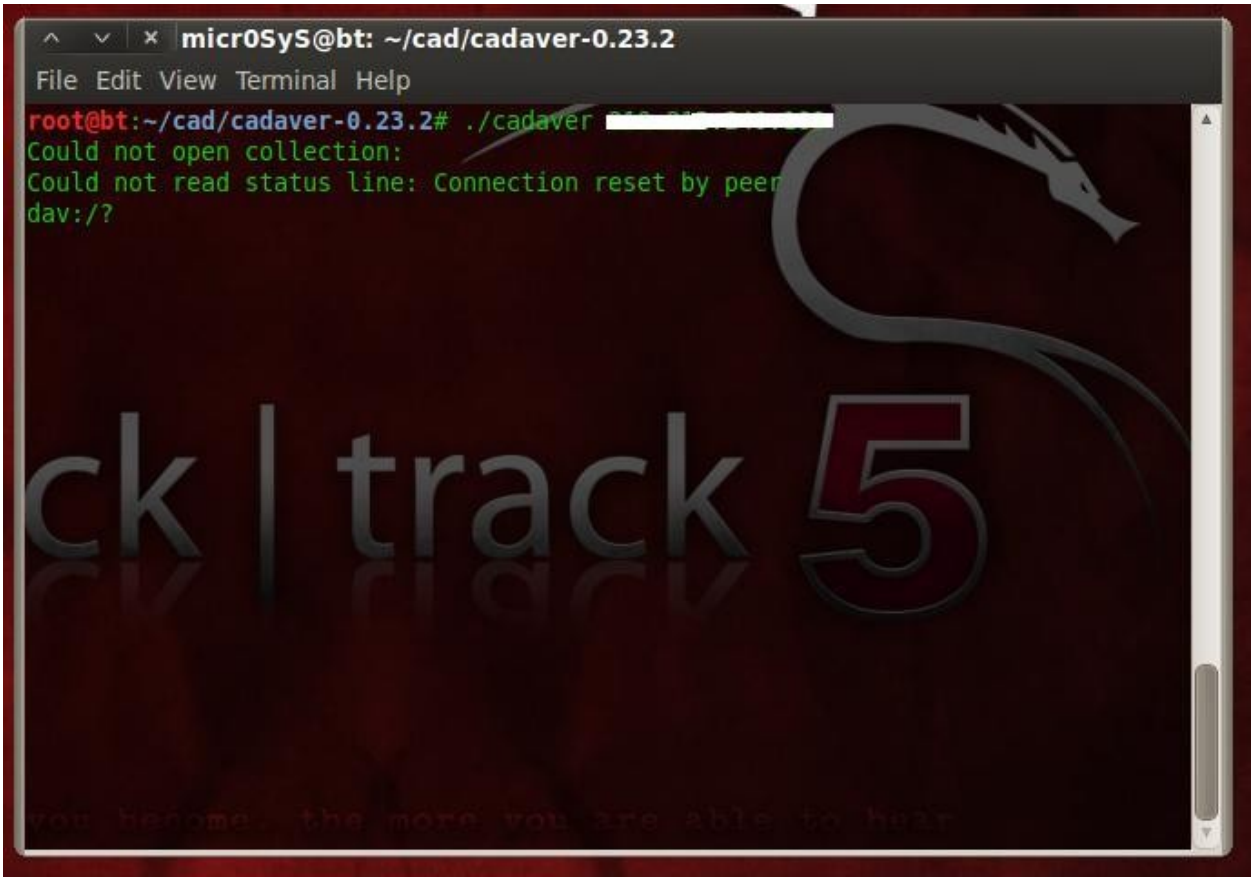
What we have to do is like

Go to cadaver directory through bash and

And type in

. /cadaver REMOTE IP

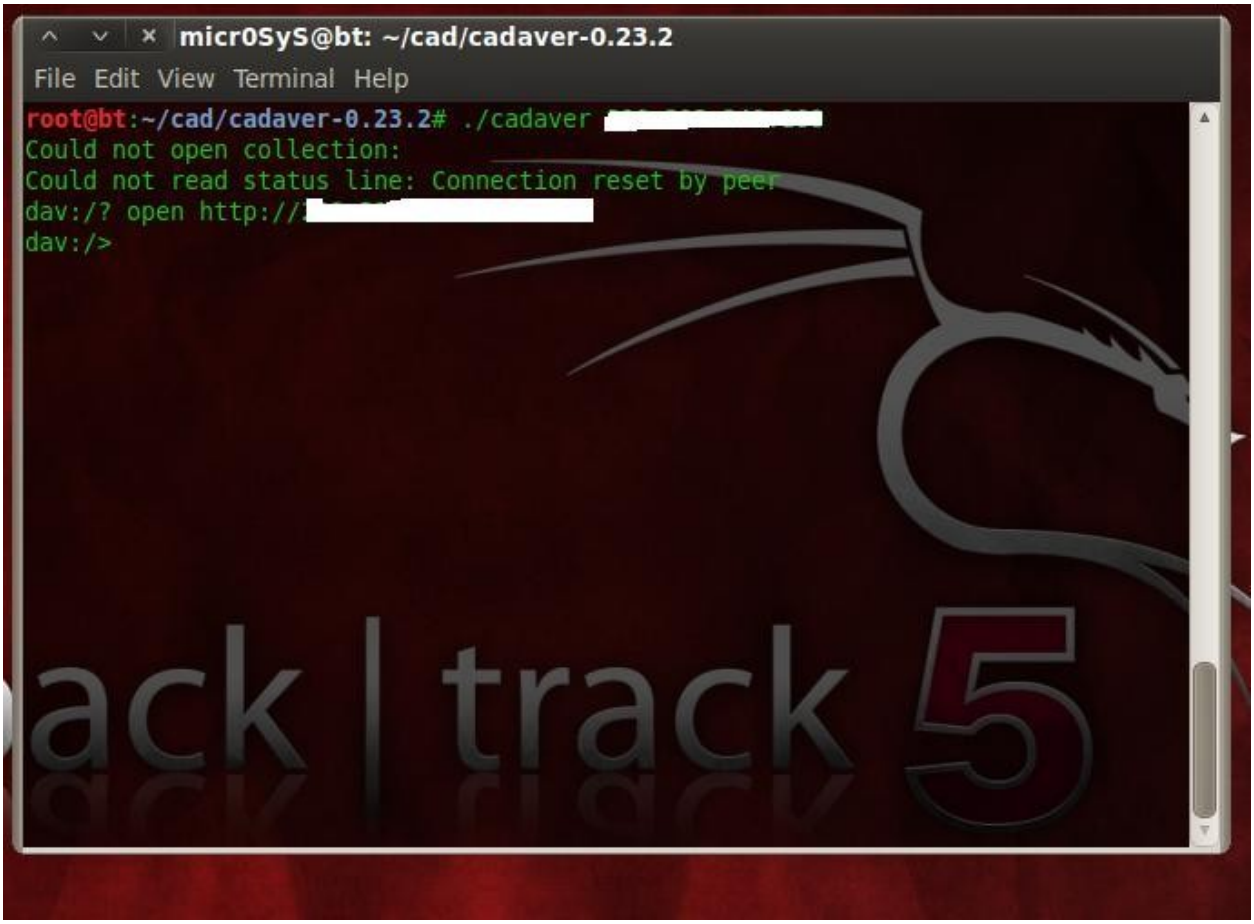
It will look like



Now from the above we understand that we can connect to the remote host using this client but we have missed something and that is *open* command

Well then for what we are waiting?

Let's do it: D

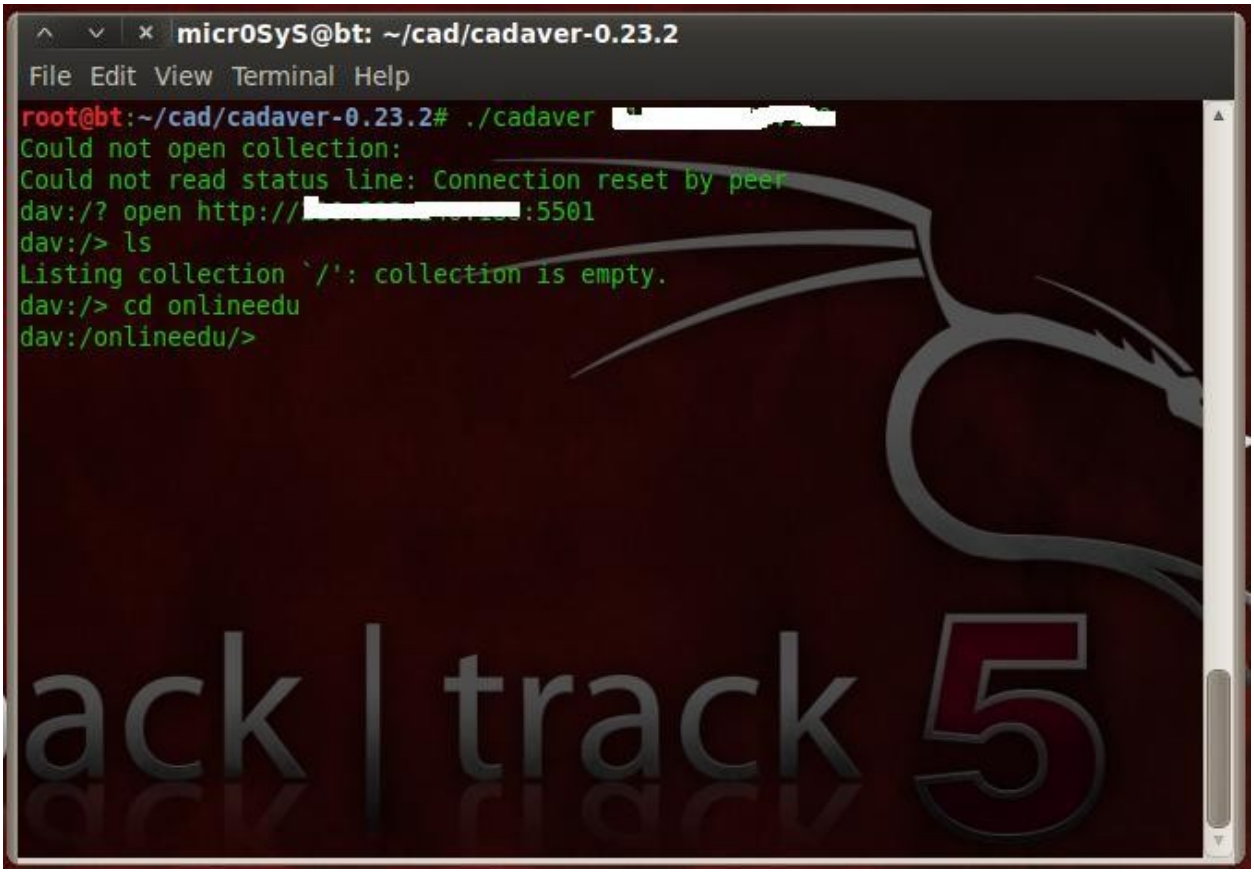


Now you must be thinking that how Nmap gave wrong result to us

It happened coz whenever we use this Nmap vulnerability scanning script it will test 80, 8080 port be default you can simply add –p WEBDAV port and scan again using Nmap it will provide you the details .again it is depend on the directories also if Nmap not able to find /webDAV or /secret then it may not show that it is vulnerable.

We can get the DAV commands from here http://www.webdav.org/perldav/dave.html

Now just go back to your web application and check out which directories are present there or you can just use crawler to check the directories. ☺



In my case one directory called “onlineedu” is present so I will use cd onlineedu: P

Here you go

After getting into it as we know we can put the files into the server we can upload the web shell

We can upload any malware

We can upload NetCat and listen to the ports to get access over servers

Or we can simply change the source code of the original file and make it for the mass phishing

References:-

Obviously god of the blue nowhere:-www.google.com

Nmap.org

Skullsecurity.org