

Forum: [Hack Forums](#)

Thread: [Nmap vulners vs nmap vulscan](#)

Max_Troy3 - February 25, 2020, 12:34 am

Hi forum, a little assistance here please.

I am fiddling about with nmap vulners and nmap vulscan in prep for my Pentest+ exam.

So with nmap vulners I am able to detect vulnerabilities with exploits as well as the CVE reference number and even as the exploit priority. This is great and is exactly what I am looking for. The command tends to not find much however.

https://i956.photobucket.com/albums/ae44/sporadic_kit/WebPix/nmap-vulners_zpsvbm7lhei.jpg

Then on the other hand with nmap vulscan it return a much larger list with some sort of reference number but no CVE ref and no priority. Are these just vulnerabilities that don't have documented exploits yet? I am wondering what I am supposed to do next with this list to exploit a vulnerability?

Appreciate your help...

Max_Troy3 - February 26, 2020, 10:06 am

I find it surprising that nobody here can give me an answer to this

Mad76e. - February 27, 2020, 2:33 pm

Ok i help you with the first one (CVE-2009-3023). the rest should be just as easy

Everything you need is right here.

<https://www.exploit-db.com/exploits/9559>

Edit: To think of it, this should already exist in metasploit btw

Edit again: Whats the purpose? You're aiming just for scanning? No penetrating?

How about a run with Nessus?

CyberStrike - February 27, 2020, 2:48 pm

(Feb 26, 2020 11:06 AM)Max_Troy3 Wrote: [\[CITE\]](#) I find it surprising that nobody here can give me an answer to this

It's more surprising that you didn't google any of these I Googled a couple and quickly found the exploit

Example:

<https://www.exploit-db.com/exploits/22132>

I don't mean to be a jerk but it's simple research mate.

Max_Troy3 - March 3, 2020, 5:06 am

OK so the exploitDB reference simply links back to the exploitDB that is online. That's good to know.

So during exploit recon I have two methods of identifying vulnerabilities:

nmap vulners (gives me a CVE ref for example CVE-2009-3023)

nmap vulscan (gives me an exploitDB reference for example 43360)

Moving into metasploit I am trying to load the module for use. Before loading the module one must find the module. This is where I am stuck.

With the CVE-2009-3023 I can do this just fine from within msfconsole with:

```
search cve:CVE-2009-3023
```

But with the exploitDB ref its not finding anything with:

```
search edb:43360
```

Googling exploitDB 43360 takes me right to the page where this exploit is detailed. How do I take the exploitDB vulnerability that has been identified and load it into metasploit for use?

CyberStrike - March 3, 2020, 7:17 am

(Mar 3, 2020 06:06 AM)Max_Troy3 Wrote: [\[CITE\]](#) OK so the exploitDB reference simply links back to the exploitDB that is online. Thats good to know.

So during exploit recon I have two methods of identifying vulnerabilities:

nmap vulners (gives me a CVE ref for example CVE-2009-3023)

nmap vulscan (gives me an exploitDB reference for example 43360)

Moving into metasploit I am trying to load the module for use. Before loading the module one must find the module. This is where I am stuck.

With the CVE-2009-3023 I can do this just fine from within msfconsole with:

```
search cve:CVE-2009-3023
```

But with the exploitDB ref its not finding anything with:

```
search edb:43360
```

Googling exploitDB 43360 takes me right to the page where this exploit is detailed. How do I take the exploitDB vulnerability that has been identified and load it into metasploit for use?

You got one of a couple of options:

1) If it's ported to MSF then you add the exploit wherever it is supposed to go you will see that in MSF there is a directory structure which should be copied and that is where you put the exploit.. generally in /root/.msf5 or whatever folder

a. If it's not ported then you can port it

(You probably will want to generate the shell code using msfconsole and paste that where the shellcode belongs)

b. If it's not ported and you have the exploit once again you can run it from a terminal of course you may have to edit it to suit your purposes as in option "a".

Generally you search exploithub from the terminal as well, using searchsploit so something like searchsploit apache 2.3.4 for example will search if there are any exploits/POC or a document detailing an exploit which is not publicly released but you can setup an environment and replicate the testing.

