

Forum:[Hack Forums](#)

Thread: [Metasploit Db Autopwn. By Vipvince \(updated\)](#)

VipVince - March 11, 2011, 5:20 am

Fast-Track Metasploit Autopwnage.By VipVince.

I have made several small changes and tweaks to this tutorial.

I was in two minds about sharing this information, cause the reality is, its easily done, works, can cause alot of damage, and in the hands of a script kiddie could lead to compromised systems.

So to start of, locate Fast-Track..

Backtrack - Penetration - Fast-Track - Fast-Track Web GUI.

This will begin to load the Web App, wait several seconds, dont press anything and it will open an internet browser for you with Fast-Track.

[img]http://i205.photobucket.com/albums/bb181/1-VIP-/snapshot2.png[/img]

Select option from the list, 'Autopwn Automation', then scroll to the bottom of the Web page and you will see exactly what the screen shot below displays.

[img]http://i205.photobucket.com/albums/bb181/1-VIP-/snapshot1.png[/img]

It will then ask you for an IP address, you can put in the IP of a remote host to scan and exploit, or an entire network to scan and exploit eg 192.168.1.0/24

The handy but dangerous thing about this tool, is the fact that it takes next to no user input, once you specify the IP, and payload type online, the scan starts automatically, the Nmap commands are automatically typed out for you, once the Nmap scan finishes, the Metasploit Autopwn commands are also automatically typed out for you. All the attacker has to do is sit back and wait for the terminal to display the results.

For this attack, I am using the IP of a personal friend, he is aware the attack is underway, and in the end even gives me a screenshot of his firewall detecting the intrusion attempt lol.

So I specify the IP, then click the Metasploit Autopwn button, now at this point, no more user input is required, a terminal screen appears, and all the Nmap and Metasploit commands are typed out automatically.

Below shows it creating the database, and executing the commands for the Nmap scan.

[img]http://i205.photobucket.com/albums/bb181/1-VIP-/1-5.png[/img]

We simply have to wait now for the scan to finish and results to be displayed.

[img]http://i205.photobucket.com/albums/bb181/1-VIP-/3-3.png[/img]

The scan results show the victims host has some interesting ports open, I repeat do not press anything, this whole attack requires no user input in the terminal screen, as you can see at the bottom of the screenshot image, it has typed out the autopwn commands for us, lets just wait for it to execute.

[img]<http://i205.photobucket.com/albums/bb181/1-VIP-/snapshot7-1.png>[/img]

Boom the exploits are running, Metasploit is matching all the exploits in its database against the open ports, if it finds a vulnerable port, it will run a suitable exploit against it, and get for us a Meterpreter session (entry to the computer).

In this case it was just a demonstration, my friends Pc is not vulnerable, I knew this before starting the attack, I was simply using his machine to provide a visual guidance. Hope you enjoyed. Dont abuse this powerful and easy to use feature.?

Ps he sent me this after the attack lol.

[img]<http://i205.photobucket.com/albums/bb181/1-VIP-/attack-1.jpg>[/img]

X Makube - March 11, 2011, 5:49 am

great tutorial.. i'll try this later...

Thanks

thesmallgod - March 11, 2011, 6:12 am

great tut will test now

:)

Kill?Muvz - March 11, 2011, 6:15 am

OHMAGAD, awesome. Simply awesome, Imma bookmark this for future tries.

Thanks a bunch! Keep it up.

VipVince - March 11, 2011, 6:16 am

(Mar 11, 2011 07:15 AM)killamuvz Wrote: [\[CITE\]](#) OHMAGAD, awesome. Simply awesome, Imma bookmark this for future tries.

Thanks a bunch! Keep it up.

Thanks glad you like it broski.

Royliidoli - March 11, 2011, 7:47 am

Great looks really great I'll check it out in few min/hours :)

P.S

Does it work on any computer?

Cheloo - March 11, 2011, 9:21 am

nice tut :D i didnt know u were into hacking lol i thought u were into the lounge shit?

VipVince - March 11, 2011, 9:33 am

(Mar 11, 2011 10:21 AM)DanKKlol Wrote: [\[CITE\]](#) nice tut :D i didnt know u were into hacking lol i thought u were into the lounge shit?

Don't judge a book by its front cover.

Ironsides - March 11, 2011, 1:20 pm

For some reason I only have Interactive and Command Line in the Fast Track folder, no Web GUI.

flyhigh - March 19, 2011, 11:14 pm

Can I do this on ubuntu 10.10???

=HeX=- - March 19, 2011, 11:34 pm

I can tell you from lots of experience, this RARELY works properly. It is akin to using a shotgun as a sniper rifle... Sometimes work, often does not...

SIM-570417 - March 20, 2011, 1:08 am

Is a greate one

but tell me and evryone how to protect of it :d

«v?s??1337» - March 20, 2011, 1:57 am

Thank You for this. I really appreciate it :)

xarisis - March 20, 2011, 3:02 am

I would like to point out a mistake I detected. When searching for a range you can't use 192.168.1.0/24 simply beacuse 192.168.1.0 doesn't exist. So, instead, you can use 192.168.1.1/24.

stupefyyy - March 22, 2011, 3:09 am

full 100/100 Thanks dear .//./

Do0ks - March 22, 2011, 5:06 am

Nice tutorial man, I knew all about metasploit but nothing about fast track. Very easy to understand. Thanks for the share mate.

b1acktiger - June 10, 2011, 12:39 pm

Nice Tutorial. Keep sharing like this

eXeSoul™ - June 10, 2011, 1:01 pm

nice tut mate :-)

Jittery - December 10, 2011, 9:17 am

What a tutorial, thanks for sharing this. It was a nice read.

VipVince - December 10, 2011, 9:22 am

Thanks seems like such a long time when I wrote this lol.

TannerGuy - December 10, 2011, 10:34 am

What is this, what does it do? what is it used for?

saisrujan - December 12, 2011, 5:24 am

nICE tut

i am going to try this

thank for sharing,,,