

Forum:[Hack Forums](#)

Thread: [\[Easy Tutorials\] Metasploit And Armitage \[PART 3\]](#)

slober - January 1, 2012, 3:32 pm

[Easy Tutorials] Metasploit And Armitage [PART 3]

Content

Introduction

Requirement

Explanation [MA]

Useful links

Outro

Sources

1. Introduction

To use Armitage, it helps to understand Metasploit. Here are a few things you must know: Metasploit is a console driven application. Anything you do in Armitage is translated into a command Metasploit understands.

Metasploit presents its capabilities as modules. Every scanner, exploit, and payload is available as a module.

When you exploit a host, you will have a session on that host. Armitage knows how to interact with shell and meterpreter sessions.

Meterpreter is an advanced agent that makes a lot of post-exploitation functionality available to you.

Armitage is built to take advantage of Meterpreter.

2. Requirement

this is what i use there other ways to do it but in this tutorial i use a Windows Machine with virtuabox and backtrack (covered in PART 2)

Virtualbox[Opt.]

Backtrack[Opt.]

Armitage[\[http://www.fastandeasyhacking.com/\]](http://www.fastandeasyhacking.com/)

Metasploit[\[http://metasploit.com/\]](http://metasploit.com/)

3. Explanation

ok first go to armitage in backtrack ;)

Applications->Backtrack->Exploitation Tools-> Network Exploitation Tools->metasploit Framework->Armitage

[IMG]<http://img85.imageshack.us/img85/3593/19208966.png>[/IMG]

just press start msf

[IMG]<http://img28.imageshack.us/img28/2228/26858077.png>[/IMG]

ok just wait until it's done loading it can take a few seconds 30-40 maybe a minute if your unlucky

[IMG]<http://img20.imageshack.us/img20/2839/19420985.png>[/IMG]

then you need to scan for targets (hosts, you know people that are online)
goto hosts->Nmap scan and Quick scan (os detected)

[IMG]<http://img94.imageshack.us/img94/5184/17597945.png>[/IMG]

now you need to fill in your subnet 192.168.0.1 or 192.168.1.1 or ..
don't forget the /24 press ok ?

[IMG]<http://img195.imageshack.us/img195/694/26258672.png>[/IMG]

it can take a few minutes to complete

[IMG]<http://img822.imageshack.us/img822/7365/41234536.png>[/IMG]

now you need to preform the attack
goto attacks->Browser attacks->multi->java signed applet
you can chose another attack but i love the java applet it almost work every-time =)

[IMG]<http://img221.imageshack.us/img221/1624/88927671xr.png>[/IMG]

fill in the form (do it like me)

[IMG]<http://img828.imageshack.us/img828/5563/40217980.png>[/IMG]

lure the target to the site or use a dns spoof ;)

[IMG]<http://img196.imageshack.us/img196/4089/95323282.png>[/IMG]

if your attack was successful you will see that your target is infected

[IMG]<http://img31.imageshack.us/img31/686/m10kp.png>[/IMG]

ok there are allot of things you can do from here i suggest you take a look and try just from here
because you learn more by trying yourself i will post some useful links ;)

Notice.

DNS Spoof is so good ;)

Notice.

You learn more by trying yourself

5. Useful Links

<http://www.youtube.com/watch?v=iGue6r1xFXI>

<http://www.fastandeasyhacking.com/manual>

<http://shadeshroud.be> [my site with some other tutorial]

6. Outro

ok this was my tutorial there is one part more a plot =)

it will be great =)

WOW 3 tutorials today going overdrive LMAO

please comment it took a lot of time to make

7. Sources

<http://www.fastandeasyhacking.com/manual>

bernardbear - January 2, 2012, 11:02 am

hey guys Again very nice amazing tutorial :D

thanks for sharing,i already know it :D but i need help on pivoting over internet already hack 1 pc using backdoor.

also why in my armitage > Attacks >Find attack / Hail mairy

just 2 options ? and on find attack no options too by port or by bla bla bla

slober - January 2, 2012, 4:12 pm

(Jan 2, 2012 12:02 PM)bernardbear Wrote: [\[CITE\]](#) hey guys Again very nice amazing tutorial :D thanks for sharing,i already know it :D but i need help on pivoting over internet already hack 1 pc using backdoor.

also why in my armitage > Attacks >Find attack / Hail mairy

just 2 options ? and on find attack no options too by port or by bla bla bla

If manual exploitation fails, you have the hail mary option. Attacks -> Hail Mary launches this feature. Armitage's Hail Mary feature is a smart db_autopwn. It finds exploits relevant to your targets, filters the exploits using known information, and then sorts them into an optimal order. This feature won't find every possible shell, but it's a good option if you don't know what else to try.

it's trying to find the exploits over port and os

everything is explained in the manual of armitage ;) at fastandeasyhacking.com/manual

btw making a moderate tutorial series [phishing sites,..]

and a hard tutorial series really advanced stuff like making an operating system with assembly =)