

Forum:[Hack Forums](#)

Thread: [Hacking strategies, eg. neighbour](#)

MackyNous - March 9, 2017, 11:37 am

Hello all,

This will be my first thread and I wanted to make a usefull one :)

So as an ongoing pentester, when having a specific target. I'm always using a simple strategy on how to hack for example the PC of my neighbour.

1. The first step is to get in their WiFi. WiFi can be hacked in a couple of different ways.

You can:

- Hack the WEP key by recieving lots of IV's.
- Hack the WPA/WPA2 key by deauthenticating a client and capturing the handshake.
- Hack the WPS pin by bruteforcing.

Since most routers these days use WPA2 it's the most common target for hacking WiFi. When someone has captured a handshake you can try to crack it with a dictionary attack. Or you can try to crack the key by social engineering (with tools like fluxion).

2. The second step is to scan the network to look for targets.

Do a quick and easy scan with nmap like: "nmap -sS -O <targets ip range>". It is important to know what operating system is running on the machines, becuae you can use this information to find target-specific exploits.

Personally I would log the internet traffic and look for active moments in the network. In the periods when it is busy I will do some MiTM attack to give the target a fake router-update page (It will fit with the router update page used with fluxion). I will add the BeEF-hook.js file in the sourcecode of the page and start my armitage-BeEF setup.

3. Loot // persistance

If you want to keep the machine for later use, just upload a backdoor on it so it will stay persistant. You can start looting creds, files etc.

If you don't care about this just start looting.

I hope this was a good first thread, I would love to see some feedback and comments.

MackyNous

/bin/bash - March 9, 2017, 1:51 pm

(Mar 9, 2017 12:37 PM)MackyNous Wrote: [\[CITE\]](#) I hope this was a good first thread, I would love to see some feedback and comments.

MackyNous

Here's some feedback, you're not a penetration tester if you're illegally hacking your neighbors, so don't call yourself that and soil professionals.

You're a skiddie, that's all.

i6FsHaN - March 9, 2017, 1:53 pm

(Mar 9, 2017 02:51 PM)/bin/bash Wrote: [\[CITE\]](#) Here's some feedback, you're not a penetration tester if you're illegally hacking your neighbors, so don't call yourself that and soil professionals.

You're a skiddie, that's all.

Well at least he helped instead of being a bragging fgt like you.

Unit 61398 - March 9, 2017, 5:46 pm

(Mar 9, 2017 02:51 PM)/bin/bash Wrote: [\[CITE\]](#) Here's some feedback, you're not a penetration tester if you're illegally hacking your neighbors, so don't call yourself that and soil professionals.

You're a skiddie, that's all. Not really phineas fisher advocated for hacking neighbors wifi for anonymity and he hacked the hack team

MackyNous - March 10, 2017, 12:19 am

(Mar 9, 2017 02:51 PM)/bin/bash Wrote: [\[CITE\]](#) Here's some feedback, you're not a penetration tester if you're illegally hacking your neighbors, so don't call yourself that and soil professionals.

You're a skiddie, that's all.

The tutorial can be interpreted in many ways, I am a Whitehat myself. I use the neighbours example to make it more clear

(Mar 9, 2017 02:53 PM)i6FsHaN Wrote: [\[CITE\]](#) Well at least he helped instead of being a bragging fgt like you.

Tnx m8

Nik321 - March 12, 2017, 5:19 am

(Mar 9, 2017 02:51 PM)/bin/bash Wrote: [\[CITE\]](#) Here's some feedback, you're not a penetration tester if you're illegally hacking your neighbors, so don't call yourself that and soil professionals.

You're a skiddie, that's all.

I have to agree with him. What you are doing here is illegal and it is not "penetration testing" ... It is hacking, which is illegal... So he is correctly saying that you should not label your self as Pen Tester when what your doing is not Pen Testing...

BUT! You are honestly just trying to help the community! After all the forum is HACK forums not PENETRATION WHITE HAT Forums... So good job dude! A little more information probably needed but it is a start.

MackyNous - March 12, 2017, 11:38 am

(Mar 12, 2017 05:19 AM)Nik321 Wrote: [\[CITE\]](#) I have to agree with him. What you are doing here is illegal and it is not "penetration testing" ... It is hacking, which is illegal... So he is correctly saying

that you should not label your self as Pen Tester when what your doing is not Pen Testing...

BUT! You are honestly just trying to help the community! After all the forum is HACK forums not PENETRATION WHITE HAT Forums... So good job dude! A little more information probably needed but it is a start.

Thanks man ?

blurryfacce - March 13, 2017, 2:01 am

This is really just concept art. You haven't really defined or instructed anything here. Your effort is greatly appreciated, just offering constructive criticism. Try detailing as much as possible about what you are trying to show or demonstrate. Everyone is at different levels of knowledge and experience, so try to keep it simple :) Thanks for trying, and keep it up!

(Mar 9, 2017 02:51 PM)/bin/bash Wrote: [\[CITE\]](#) ...you're not a penetration tester if...OP didn't claim to be a pentester, professional or skiddie, just provided knowledge. No need to be rude. Learn to read what someone has written before chastising them, otherwise you are just being a post count whore.

And those are worse than camwhores. Don't be that guy, Dave.

MackyNous - March 13, 2017, 6:13 am

(Mar 13, 2017 02:01 AM)Vaeldious Wrote: [\[CITE\]](#) This is really just concept art. You haven't really defined or instructed anything here. Your effort is greatly appreciated, just offering constructive criticism. Try detailing as much as possible about what you are trying to show or demonstrate. Everyone is at different levels of knowledge and experience, so try to keep it simple :) Thanks for trying, and keep it up!

lol, thanks m8, I will keep it in mind ?

/bin/bash - March 13, 2017, 10:06 am

(Mar 13, 2017 02:01 AM)Vaeldious Wrote: [\[CITE\]](#) OP didn't claim to be a pentester, professional or skiddie, just provided knowledge.

In case you can't read: (Mar 9, 2017 12:37 PM)MackyNous Wrote: [\[CITE\]](#) So as an ongoing pentester, when having a specific target. I'm always using a simple strategy on how to hack for example the PC of my neighbour.

blurryfacce - March 13, 2017, 11:48 pm

:/ Guess I can't read. I stand corrected.