

Forum:[Hack Forums](#)

Thread: [Hack remote router without remote access](#)

Greenchill - September 15, 2016, 11:56 am

Hello peoples of Hack Forums.

I am a fairly inexperienced hacker. The most that I had done is install a reverse shell through USB on my friend's PC to later play around there with meterpreter.

I want to take another, but quite more complicated step.

The case:

I'm aiming to hack a router that's in a different city. So obviously all social engineering except for chatting on FB are unavailable to me. (As far as I know him, he won't download and exec any file I'd send him, but he will click webpage links - thats how I got his IP)

All I have for now is his IP (which is dynamic, thus I might need to regain it few times on the way I guess).

I've ran some nMap scans, which yielded me that info:

Code map: Host is up (0.089s latency).

[*] Nmap: Not shown: 998 filtered ports

[*] Nmap: PORT STATE SERVICE

[*] Nmap: 22/tcp closed ssh

[*] Nmap: 80/tcp closed http

[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 14.16 seconds

So, ports that aren't filtered are closed.

Also, it seems that his router has remote access disabled.

My original plan was to hack router -> enable port forwarding -> metasploit his pc (as he runs a shitton of torrented software, I BET that some have security flaws)

Anybody could help me / point me in the right direction how should I access his PC totally remotely?[/code]

Uzytkownik - September 15, 2016, 12:24 pm

How do you want "remote hack router"? Router may be available only from LAN.

Greenchill - September 15, 2016, 12:40 pm

(Sep 15, 2016 12:24 PM)Uzytkownik Wrote: [\[CITE\]](#) How do you want "remote hack router"? Router may be available only from LAN.

Well that's a part of the question. It IS available only from LAN.

Kali_GFX - September 15, 2016, 1:28 pm

Most likely you'll have run Armitage against his router and hopefully find a vulnerability and take it from there..

FractumSeraph - September 15, 2016, 3:13 pm

Unfortunately you can't do this remotely right now.

Learn more about him. Convince him to open up SSH on his router, convince him to start a minecraft server using a plugin that allows connections. Convince him he needs some sort of dynamic dns. Tell him that adding himself to DMZ will make his internet faster.

So many things to try, but without local access to the router, or the ability to talk to the guy, you can't do much except wait and hope he does something on his own.

Greenchill - September 15, 2016, 4:02 pm

(Sep 15, 2016 03:13 PM)Fallen Archangel Wrote: [\[CITE\]](#) Unfortunately you can't do this remotely right now.

Learn more about him. Convince him to open up SSH on his router, convince him to start a minecraft server using a plugin that allows connections. Convince him he needs some sort of dynamic dns. Tell him that adding himself to DMZ will make his internet faster.

So many things to try, but without local access to the router, or the ability to talk to the guy, you can't do much except wait and hope he does something on his own.

I had also learned that the IP Ive got is not his - its the ISP's.

As it is dynamic, it means that he is sitting behind NAT that the ISP set up.

But lets imagine another scenario - that I convince him to set up a tunnel to me (be it hamatchi or else). Could that be a way to exploit him, and if so, how?

FractumSeraph - September 15, 2016, 4:08 pm

(Sep 15, 2016 04:02 PM)Greenchill Wrote: [\[CITE\]](#) I had also learned that the IP Ive got is not his - its the ISP's.

As it is dynamic, it means that he is sitting behind NAT that the ISP set up.

But lets imagine another scenario - that I convince him to set up a tunnel to me (be it hamatchi or else). Could that be a way to exploit him, and if so, how?

I'm not 100% sure how hamatchi works as I've never used it. But I'm as assuming it give you LAN access. If so, you have two options. The first one is to attack his router while you're connected. Try to get in, open remote admin, and set up a ddns to track the IP. From there you can do whatever.

The second option, in case you don't get access to the LAN, would be to run an attack against him directly. See what you can get out of public SMB, look for open or exploitable services, enumerate usernames, etc.

Greenchill - September 15, 2016, 4:21 pm

(Sep 15, 2016 04:08 PM)Fallen Archangel Wrote: [\[CITE\]](#) I'm not 100% sure how hamatchi works as I've never used it. But I'm as assuming it give you LAN access. If so, you have two options. The first one is to attack his router while you're connected. Try to get in, open remote admin, and set up a ddns to track the IP. From there you can do whatever.

The second option, in case you don't get access to the LAN, would be to run an attack against him directly. See what you can get out of public SMB, look for open or exploitable services, enumerate usernames, etc.

Huge thanks for your insight. Ive just come up with one more idea, that I had actually eliminated previously due to my ignorance of "everything is possible if you try hard enough".

While that may be true, for me to do a direct attack on his router from my PC without any "side help" would mean to basically overtake ISP, set up nats, and overtake his router. No fun.

I just realised that with some social engineering, encrypting a kind of rootkit that bypasses AV and making him click it disguised as an ordinary file, I could get that going.

Do you by any chance have/know any sources that show how to bypass current AV software with a fair success rate? Most I had found seems fairly outdated, and I bet had been patched now. The best would be like a database of AV bypasses (like we have db of exploits).

Thanks again

FractumSeraph - September 15, 2016, 4:39 pm

(Sep 15, 2016 04:21 PM)Greenchill Wrote: [\[CITE\]](#) Huge thanks for your insight. Ive just come up with one more idea, that I had actually eliminated previously due to my ignorance of "everything is possible if you try hard enough".

While that may be true, for me to do a direct attack on his router from my PC without any "side help" would mean to basically overtake ISP, set up nats, and overtake his router. No fun.

I just realised that with some social engineering, encrypting a kind of rootkit that bypasses AV and making him click it disguised as an ordinary file, I could get that going.

Do you by any chance have/know any sources that show how to bypass current AV software with a fair success rate? Most I had found seems fairly outdated, and I bet had been patched now. The best would be like a database of AV bypasses (like we have db of exploits).

Thanks again

That's a lot of work. It would be far easier to send a file that would be safe to assume as a false positive.

What I mean is this, let's say you're downloading a keygen of some kind. Most antiviruses flag them as a hacktool. So adding a virus to one has no more or less suspicion than a virus-free one would.

BearScat - September 17, 2016, 5:50 pm

depends what file you are sending. if its an exe your infecting and you know how to use visual basic there is some source codes available for crypters on HF. although the free crypters are no longer fud and are detected becuase of people raping them you could learn how to refud them quite easy and make the source code unique so its not detected and then just infect and crypt any file and send it him. the plus side of refuding a crypter is that the source code is unique and only you have it which means that it remains fully undetectable for longer so chances of antivirus's picking it up are slim and when they do you just refud again.

dont know if that makes sense or helps you but if you do go down this route also search HF on how to make the icon FUD too as there are many guides on it and its amazing how just the icon of the exe can be the difference between fully undetectable or giving you a high detection rate.

and last but not least and you probably already know this but once you have built your infected file whichever way you chose, whatever you do dont run it through virustotal as they distribute to all the main virus company's and your infected file will be detected by most AVs really quick. i cant remember off the top of my head but again search HF as there are a few online virus checkers that do not distribute. :)

sorry for the essays especially if they not of assistance but hope that they are mate and best of luck.

i noticed from your posts it looks like hes a bit of a gamer, if he has a steam account try this [hackforums\(dot\)net/showthread.php?tid=5392011](http://hackforums(dot)net/showthread.php?tid=5392011) (sorry cant post links yet) it basically spoofs a fake email from steam with a download link. might get him to download your file lol.