Forum:Hack Forums

Thread: I need help with armitage

Citoa - *December 22, 2019, 6:40 am*

I am learning a bit about hacking, but I am still a newbie. I have a virtual machine with Kali Linux and learned how to make a reverse_tcp connection with a file that is FUD. But I really want to know how when I make a session with a PC how can I also hack other PCs in its network. Should I even use Armitage or just go back to the basic msfconsole?

CyberStrike - *December 22, 2019, 1:00 pm*

Pivoting I believe is the term you will be looking for, which allows you to make a route from your machine to a compromised machine and engage other devices on the network. (Sidenote: All Armitage does is just give you a graphical interface, use the console it's got more functionality and honestly is easy to use.)

Citoa - *December 23, 2019, 7:46 am*

(Dec 22, 2019 02:00 PM)CyberStrike Wrote: *[CITE]* Pivoting I believe is the term you will be looking for, which allows you to make a route from your machine to a compromised machine and engage other devices on the network. (Sidenote: All Armitage does is just give you a graphical interface, use the console it's got more functionality and honestly is easy to use.)

I saw a few videos about pivoting but now I have another problem. When I try to use nmap the session dies. And also the IP displayed on the host isn't the same as the IPV4 address of the target. Is this normal? Is the problem coming from armitage?

Edit: Are there any videos in particular that can help me figure out how to map the network of the victim and also exploit other PCs on the network? Or is it just by learning the different methods and tools for pivoting that I can do that?

CyberStrike - *December 23, 2019, 3:43 pm*

So the session is dying.. I got some questions :

1) What Payload? What handler is being used to catch the connection?
2) Actual Command to generate the payload?
3) Target OS?
4) Is this in a hypervisor? If yes, what hypervisor software?
5) Is there AV? If yes what AV? What happens if there is an exception? What about if AV is disabled?

Please include actual commands? Have you also tried using a debugger?

Citoa - *December 24, 2019, 3:38 am*

(Dec 23, 2019 04:43 PM)CyberStrike Wrote: *[CITE]* So the session is dying.. I got some questions :

1) What Payload? What handler is being used to catch the connection?
2) Actual Command to generate the payload?
3) Target OS?
4) Is this in a hypervisor? If yes, what hypervisor software?
5) Is there AV? If yes what AV? What happens if there is an exception? What about if AV is disabled?

Please include actual commands? Have you also tried using a debugger?
1) windows/meterpreter/reverse_tcp and multi/handler
2) I generated it with shellter
3) Windows 10
4) Virtual box
5) I don't have an AV. Shellter also makes the file FUD so it shouldn't be a problem if there is an AV right?

I use ngrok for the connection. The generated payload connects to ngrok's servers and then the server connects to me. It seemed easier to configure than port forwarding so that is why I use it. After I start up ngrok I use the following commands in msfconsole:
use multi/handler
set payload windows/meterpreter/reverse_tcp
set lhost 0.0.0.0
set lport 9999 (I decided to use this port for ngrok to connect through. Should I use another?)
exploit

Then I open the generated payload outside of the hypervisor and a session is made. After that I try to use nmap in armitage on the exploited host but the session dies when I do so.

CyberStrike - *December 24, 2019, 9:21 am*

(Dec 24, 2019 04:38 AM)Kristiqn Iliev Wrote: *[CITE]* 1) windows/meterpreter/reverse_tcp and multi/handler
2) I generated it with shellter
3) Windows 10
4) Virtual box
5) I don't have an AV. Shellter also makes the file FUD so it shouldn't be a problem if there is an AV right?

I use ngrok for the connection. The generated payload connects to ngrok's servers and then the server connects to me. It seemed easier to configure than port forwarding so that is why I use it. After I start up ngrok I use the following commands in msfconsole:
use multi/handler
set payload windows/meterpreter/reverse_tcp
set lhost 0.0.0.0
set lport 9999 (I decided to use this port for ngrok to connect through. Should I use another?)
exploit

Then I open the generated payload outside of the hypervisor and a session is made. After that I try to use nmap in armitage on the exploited host but the session dies when I do so.
So payload is to connect to a hypervisor:

More questions:

1) Is the VM NAT or Bridged?
2) Have you set port forwarding in the hypervisor software?
3) Could you try a msfvenom generated payload?
4) Would you be willing to run a debugger to check what the payload is doing?

5) Why have the payload use the internet? (This adds yet another link in the chain which could give you issues, since both of these machines are technically local try that first)

A word on Shelter, it is not FUD (dumbest term known to man) and is now rather well researched, unless you are a bonafide security professional and using the Pro edition, the community edition will probably be caught unless you have your own templates. Either way it does matter if there is AV.

Edit: Is the connection fully completed? I got a feeling it is dying before the connection is complete as you are not even pivoting yet. Is it dying like right after execution? If this is the case then probably something is killing it, have you looked at taskmanager or procexp at all during this?

Citoa - *December 24, 2019, 3:17 pm*

(Dec 24, 2019 10:21 AM)CyberStrike Wrote: [CITE] So payload is to connect to a hypervisor:

More questions:

1) Is the VM NAT or Bridged?
2) Have you set port forwarding in the hypervisor software?
3) Could you try a msfvenom generated payload?
4) Would you be willing to run a debugger to check what the payload is doing?
5) Why have the payload use the internet? (This adds yet another link in the chain which could give you issues, since both of these machines are technically local try that first)

A word on Shelter, it is not FUD (dumbest term known to man) and is now rather well researched, unless you are a bonafide security professional and using the Pro edition, the community edition will probably be caught unless you have your own templates. Either way it does matter if there is AV.

Edit: Is the connection fully completed? I got a feeling it is dying before the connection is complete as you are not even pivoting yet. Is it dying like right after execution? If this is the case then probably something is killing it, have you looked at taskmanager or procexp at all during this?
1) NAT
2) I haven't
3) I tried one and it also died when I was on virtual box
4) Yes
5) I study in one town and for the weekends I come back to my hometown. So if I do it with a localhost I would have to make 2 different payloads because of the different IPs and I would have to set up 2 port forwardings. Also the IPS in my hometown doesn't give me access to the settings of my router because of security reasons so I can't really set port forwarding.

What crypters would you recommend that work well and are low price? I don't really know which ones are out there, if they are good or even where I can get them from.

The connection is fully completed. I can open a meterpreter shell and execute different commands.

Today I changed the hypervisor to VMWare and I tried running an nmap scan after I opened the session. But I don't exactly know what is happening. It is giving me 256 different devices and no connection between them as I have seen in some videos. I scanned with 127.0.0.1/24 since that is what it shows me as the host's IP and it gives out these results.

When I try to scan 192.168.1.0/24 the session dies. Also I don't know why it recognizes the OS of

the exploited host as Linux. I am opening the payload from outside VMWare.

CyberStrike - *December 24, 2019, 5:27 pm*
(Dec 24, 2019 10:21 AM)CyberStrike Wrote: [CITE] So payload is to connect to a hypervisor:

More questions:

1) Is the VM NAT or Bridged?
2) Have you set port forwarding in the hypervisor software?
3) Could you try a msfvenom generated payload?
4) Would you be willing to run a debugger to check what the payload is doing?
5) Why have the payload use the internet? (This adds yet another link in the chain which could give you issues, since both of these machines are technically local try that first)

A word on Shelter, it is not FUD (dumbest term known to man) and is now rather well researched, unless you are a bonafide security professional and using the Pro edition, the community edition will probably be caught unless you have your own templates. Either way it does matter if there is AV.

Edit: Is the connection fully completed? I got a feeling it is dying before the connection is complete as you are not even pivoting yet. Is it dying like right after execution? If this is the case then probably something is killing it, have you looked at taskmanager or procexp at all during this?
(Dec 24, 2019 04:17 PM)Kristiqn Iliev Wrote: [CITE] 1) NAT
2) I haven't
3) I tried one and it also died when I was on virtual box
4) Yes
5) I study in one town and for the weekends I come back to my hometown. So if I do it with a localhost I would have to make 2 different payloads because of the different IPs and I would have to set up 2 port forwardings. Also the IPS in my hometown doesn't give me access to the settings of my router because of security reasons so I can't really set port forwarding.

What crypters would you recommend that work well and are low price? I don't really know which ones are out there, if they are good or even where I can get them from.

The connection is fully completed. I can open a meterpreter shell and execute different commands.

Today I changed the hypervisor to VMWare and I tried running an nmap scan after I opened the session. But I don't exactly know what is happening. It is giving me 256 different devices and no connection between them as I have seen in some videos. I scanned with 127.0.0.1/24 since that is what it shows me as the host's IP and it gives out these results.

When I try to scan 192.168.1.0/24 the session dies. Also I don't know why it recognizes the OS of the exploited host as Linux. I am opening the payload from outside VMWare.
Okay so using NAT you would have to port forward in the hypervisor software (I think this is the real issue). So you are on the internet to monitor your machine in another city. (Side Note: You may want to use SSH after all it is your machine. (I honestly hope you are not trying to hack your school and you actually own this machine and have permission to do all this.)) Now after you have "pivoted", remember you are using ngrok so port forwarding to your machine shouldn't be the issue, instead when the VM is on NAT it is on a different subnet/network all virtually within the hypervisor, for example the VM may have the ip of 10.10.10.1 and your main OS is 192.168.1.10 or something similar. Now 127.0.0.1 is your local host not sure why scanning a CIDR is required and I don't think is has 255 different IPs, it's local, so make sure you have pivoted and have your route added.

Another thing use x32/64dbg it really could be any number of things going on.

blackbox_hcker - *June 9, 2026, 8:50 am*

(Dec 22, 2019 07:40 AM)Citoa Wrote: [CITE] I am learning a bit about hacking, but I am still a newbie. I have a virtual machine with Kali Linux and learned how to make a reverse_tcp connection with a file that is FUD. But I really want to know how when I make a session with a PC how can I also hack other PCs in its network. Should I even use Armitage or just go back to the basic msfconsole?

I would use Armitage I really like it!

Watch this YouTube Video: watch?v=TaGKxwGNfdI&t=635s

enjoy! ?