

Forum:[Hack Forums](#)

Thread: [Non-local Network entry with cmd](#)

Gazilam - August 16, 2019, 3:26 am

Hi, i really find this amazing and scary at the same time. Art of war " become your enemy "

im fairly new at this and dont know where to start, i thought CMD would be a start off point but then again wouldnt i leave fingerprints or tracemarks as they call it.

first i need to know how to hide myself and not get into trouble. also i dont have much coding skills but i have the motivation to learn so if any what would be a great beginners program to start with? Python?

Im getting use to all the cmd functions but im sure there is atill a lot to figure out i.e combining commands,

i recently got fimalier with PStools and almost got into another network but it requested a -u and -p. is there a way to bypass this within the same command from cmd?

also if i use a 3G usb dongle not shared, can i access other networks?

i would really like to get to my previous employer's network and sell him a security solution but in order to do so i first need to make him aware that its needed. how would i achieve such mission.

If anyone that have traield and succeeded can give me a some hints or beginners guidance on where to start i will not let you down.

i only have a standard PC does it make a difference? should i get a 2nd and 3rd for trail and error and how will i set up a network between them if i only have access to 1 provider.

im sure i have still a lot to learn but i really find this could become a new hobby and that i could actually create a successful income source.

for exploiting security networks and vulnerabilities what programs should be used.

Also when a rat was opened and encrypted documents such as excel word a.s.f does the correct password repair it to normal state and when a new operating system was loaded can the rat " JRat,Loki" be recalled if no password were entered even after the new OS

I hope im in the right direction as we all need to start somewhere.

?

CyberStrike - August 16, 2019, 5:14 am

(Aug 16, 2019 03:26 AM)Gazilam Wrote: [\[CITE\]](#) Hi, i really find this amazing and scary at the same time. Art of war " become your enemy "

im fairly new at this and dont know where to start, i thought CMD would be a start off point but then again wouldnt i leave fingerprints or tracemarks as they call it.

first i need to know how to hide myself and not get into trouble. also i dont have much coding skills but i have the motivation to learn so if any what would be a great beginners program to start with? Python?

Im getting use to all the cmd functions but im sure there is atill a lot to figure out i.e combining commands,

i recently got fimalier with PStools and almost got into another network but it requested a -u and -p. is there a way to bypass this within the same command from cmd?

also if i use a 3G usb dongle not shared, can i access other networks?

i would really like to get to my previous employer's network and sell him a security solution but in order to do so i first need to make him aware that its needed. how would i achieve such mission.

If anyone that have trailed and succeeded can give me a some hints or beginners guidance on where to start i will not let you down.

i only have a standard PC does it make a difference? should i get a 2nd and 3rd for trail and error and how will i set up a network between them if i only have access to 1 provider.

im sure i have still a lot to learn but i really find this could become a new hobby and that i could actually create a successful income source.

for exploiting security networks and vulnerabilities what programs should be used.

Also when a rat was opened and encrypted documents such as excel word a.s.f does the correct password repair it to normal state and when a new operating system was loaded can the rat " JRat,Loki" be recalled if no password were entered even after the new OS

I hope im in the right direction as we all need to start somewhere.

?

Yes cmd/powershell will both leave traces, you figure that cmd leaves traces in conhost.exe and crss.exe if these processes are dumped commands issued can be found. In cmd and Powershell another thing is you have logging even with encoded commands, in the case of powershell.

So to your first question how to hide and not get yourself in trouble, well if you didn't access things which you don't own or have permission to do so, then you avoid that issue entirely. You actually don't need to access other peoples machines to practice, generally running a VM (VirtualMachine) is pretty much the same, in fact you can probably setup a more intricate environment.

You are taking the first steps to being actually proficient, you will find that working in a cli (cmd/powershell) will give you a better understanding of how Windows works. When you used psexec (guess) it asked for authentication -u user -p password, this is common authentication, generally using psexec actually will send alerts to admins since it was so commonly abused.

Getting into a previous employers network and selling them a security solution would work like so :

Attempt access, alerts then the security solution is you in prison OR You attempt access and are successful when you go to "sell" your solution they proceed to have you arrested, once again the same security solution, you in prison. If you plan on stealing information where in they encrypt

documents you need the password.

It's a bad idea just a bad idea unless you like crap food and dudes.

Up to the point you mentioned a previous employer I thought you were 14 and just figured you liked hacking maybe had an aptitude for it.. but now I just think you want to go to prison. Either way why not go and learn some networking and OS's before trying to go to the State/Federal Penitentiary.

ThisBearScat - August 16, 2019, 5:30 am

i wont knock you for using windows to hack but i would recommend using a more flexible linux OS

i cant see how 3g will help you enter your previous employers network other than giving you the possibility to download exploits etc on the fly unless you are trying by ip only.

if you wish to get a second pc and put it on a separate wifi network then you would have a testing environment to work in and practice and gain skills. this would also reduce the risk of damaging you previous employers system and being held legally accountable for it.

a questions for you to think about.....

is your employers network accessible by wifi or is it hard wired access only?

that can change the method of how you attempt to breach it. if its accessible over wifi then go sit outside with your laptop do some net scans and find out what router is running and then pwn the router which will then allow access to the connected computers, you will still have to breach the systems connected to the router then but once you have the router you are in the network.

as for by ip from a remote location, i have never done this but i would guess you need to gain control of the router or server that the network is connected to, again though it boils down to information gathering about the system/router you wish to target, like scanning for open ports, what OS/software is running, vulnerability checks etc once you know about your target, then you will know its vulnerabilities and are able to target the vulnerabilities.

i have rated in the past but not for ages, if the rat encrypted the file then i would find it hard to see how word excel would be able to change the password as ms office would not have the decryption key from the rat. regardless of a new OS or not. then again it would depend on how well the rat was written.

hope this helps and if i have got anything wrong please someone correct me because we are all learning together :)

Gazilam - August 16, 2019, 5:38 am

Thank you for the advice - i didn't mean to do any harm though and wont. i will avoid doing such stupid acts or using cmd as a learning exercise. i thank you again for the reply like i said it also scares the crap out of me by just knowing whats on your fingertips.

you are right on most things but most of all i should have been introduced to this when i was 14 kinda late when the 1st born is that age already.

i will take your advice to heart and will not try it again. was first attempt and failed but got me interested.

by saying virtual machine can that be done from the same pc? and how.. I'd appreciate some

proper guideline without getting into trouble.

CyberStrike - August 16, 2019, 5:48 am

Yes virtualmachines can be run on the same machine or another machine, I will get you resources and sources:

<https://www.vulnhub.com/> --vulnerable machines

<https://www.virtualbox.org/wiki/Downloads> - VirtualBox free software for creating VirtualMachines

<https://developer.microsoft.com/en-us/windows/downloads/virtual-machines> -- Windows 10

Development VM's (Free)

<https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/> -- Win 7 -10 (Free VM's)

<https://resources.infosecinstitute.com/how-to-make-your-own-penetration-testing-lab/> --HowTo

Setup your own lab

All of this is free minus a computer and time, it's a safe environment.

ThisBearScat - August 16, 2019, 6:01 am

(Aug 16, 2019 05:38 AM)Gazilam Wrote: [\[CITE\]](#) Thank you for the advice - i didn't mean to do any harm though and wont. i will avoid doing such stupid acts or using cmd as a learning exercise. i thank you again for the reply like i said it also scares the crap out of me by just knowing whats on your fingertips.

you are right on most things but most of all i should have been introduced to this when i was 14 kinda late when the 1st born is that age already.

i will take your advice to heart and will not try it again. was first attempt and failed but got me interested.

by saying virtual machine can that be done from the same pc? and how.. I'd appreciate some proper guideline without getting into trouble.

i have had an interest since i was about 14 and my kids are around that age now too lol, i dont class my self as an expert nor a beginner, sort of stuck somewhere in the middle, logs can be kept on servers and routers to show devices/ips that attempted access so either hide well or dont try it until you have a good understanding and method that you believe will allow you to access the network.

like i say setting up a testing environment to learn is always a good idea, any tool you download i recommend running in a VM because most are backdoor-ed by the creators or evil beings.

good luck on your journey and feel free to ask if you need anything else. :)

edit: good idea would be to learn how to change mac address, hwids as well as how to stay anonymous online. at least then the worry of being caught if you mess up is a lot less.

Gazilam - August 16, 2019, 9:27 am

Great thank you again. i will be sure to keep away from such actions.

if there is anything useful you think that might help in my path feel free to share.

Gazi out