

Forum:[Hack Forums](#)

Thread: [Metasploit, nmap, and RAT used in conjunction? \(using Termux on Android\)](#)

stormcloudcypher - November 24, 2019, 1:34 pm

I have this idea of using nmap on the network of my victim to get info on their device then metasploit to initiate a reverse shell on a victim through an exploit, then using that shell to install a RAT/more permanent backdoor, escalate privileges, and further hide that backdoor. I plan on doing all of this using the termux app on Android behind tor and a VPN, and host my RAT server on a VPS.

Does this plan sound plausible?

If so, what could I do to make it more plausible?

If it is plausible, what could I do to ensure it is done more stealthily and effectively?

Aside from that, any general suggestions?

dan alhaji - November 24, 2019, 2:15 pm

hello please i need a very goo crypter can someone please advice

CyberStrike - November 24, 2019, 2:27 pm

(Nov 24, 2019 02:34 PM)stormcloudcypher Wrote: [\[CITE\]](#) I have this idea of using nmap on the network of my victim to get info on their device then metasploit to initiate a reverse shell on a victim through an exploit, then using that shell to install a RAT/more permanent backdoor, escalate privileges, and further hide that backdoor. I plan on doing all of this using the termux app on Android behind tor and a VPN, and host my RAT server on a VPS.

Does this plan sound plausible?

If so, what could I do to make it more plausible?

If it is plausible, what could I do to ensure it is done more stealthily and effectively?

Aside from that, any general suggestions?

Not quite sure why the RAT in the end, I am wondering could you please address this, thank you.

Edit: I will make it quicker, Metasploit does provide remote access, in addition nmap is integrated in Metasploit. Metasploit allows you to build multiple payloads much more than say an exe, the exploits may or may not be detected so modification is probably needed. Now I am not sure if you are in the end using a "RAT" because perhaps a shell or issuing commands to all of your clients might not sound too cool. There is very little you can do in GUI which cannot be done in say a shell.

stormcloudcypher - November 24, 2019, 4:11 pm

(Nov 24, 2019 03:27 PM)CyberStrike Wrote: [\[CITE\]](#) Not quite sure why the RAT in the end, I am wondering could you please address this, thank you.

Edit: I will make it quicker, Metasploit does provide remote access, in addition nmap is integrated in Metasploit. Metasploit allows you to build multiple payloads much more than say an exe, the exploits may or may not be detected so modification is probably needed. Now I am not sure if you are in the end using a "RAT" because perhaps a shell or issuing commands to all of your clients might not sound too cool. There is very little you can do in GUI which cannot be done in say a shell.

Hm, fair point. Specifically- I want to be able to have a keylogger, visual access to cameras where I can see what's going on through them but not record, view messages or web sessions on certain social applications, find saved password, have a backdoor that is activated on boot that I can come back and access, escalate privileges, and save the victims files on my own device.

I know that some RATs do all of this, but I don't know if the reverse shell on metasploit can do all of these things, hence the RAT. CAN the reverse shells made on metasploit do all that?

Also, does metasploit have the capabilities to make the payloads FUD?

CyberStrike - November 25, 2019, 4:20 pm

(Nov 24, 2019 05:11 PM)stormcloudcypher Wrote: [\[CITE\]](#) Hm, fair point. Specifically- I want to be able to have a keylogger, visual access to cameras where I can see what's going on through them but not record, view messages or web sessions on certain social applications, find saved password, have a backdoor that is activated on boot that I can come back and access, escalate privilege, and save the victims files on my own device.

I know that some RATs do all of this, but I don't know if the reverse shell on metasploit can do all of these things, hence the RAT. CAN the reverse shells made on metasploit do all that?

Also, does metasploit have the capabilities to make the payloads FUD?

"FUD" is a term which denotes an inability to modify Metasploit payloads. Generally we would emulate the target environment and tailor our payload. I have found that a simple custom reverse shell often will evade most security products, the same is true of a meterpreter payload, AV triggers off of metsrv.dll when that is loaded in memory, but you can easily modify metsrv.dll. While with a shell you will want to utilize other tools, for example a custom keylogger, or let's say we want to view specific applications what prevents you from polling window names where in there is a regexp and proceeds to send pictures/screenshots yes you can do this with the Windows API.

You want saved passwords, sounds great you have a couple of options dumping a process's memory and parsing through that (some security products protect against this) or let's say they are using Chrome well you have a sql database which is encrypted and to decrypt you have a json file.

You have to actually know how to do these a reverse shell doesn't have the command simplification where you type "getsytem" such as in meterpreter. I tend to have used Windows against itself to quickly move files around such as using the "expand" command in Windows to a system which has been designated for exfiltration.

When it comes to persistence, it's not hard schtasks is an option along with many other options.

Many of your questions or things you wish to do are actually rather trivial when it comes to post exploitation, even from a shell. Having the proper knowledge is what either makes you successful or not. These are important things which are important to learn, much like modifying metsrv.dll, it's okay to not know how to do things it's not okay though to continuing while knowing only hurts yourself. If you are unfamiliar a virtual lab is a good way to practice things safely.

You should know that a legit code signing certificate is a good idea and often well known malware can and does evade AV's.

stormcloudcypher - November 26, 2019, 12:34 am

(Nov 25, 2019 05:20 PM)CyberStrike Wrote: [\[CITE\]](#) "FUD" is a term which denotes an inability to modify Metasploit payloads. Generally we would emulate the target environment and tailor our payload. I have found that a simple custom reverse shell often will evade most security products, the same is true of a meterpreter payload, AV triggers off of metsrv.dll when that is loaded in memory, but you can easily modify metsrv.dll. While with a shell you will want to utilize other tools, for example a custom keylogger, or let's say we want to view specific applications what prevents you from polling window names where in there is a regexp and proceeds to send pictures/screenshots

yes you can do this with the Windows API.

You want saved passwords, sounds great you have a couple of options dumping a process's memory and parsing through that (some security products protect against this) or let's say they are using Chrome well you have a sql database which is encrypted and to decrypt you have a json file.

You have to actually know how to do these a reverse shell doesn't have the command simplification where you type "getsystem" such as in meterpreter. I tend to have used Windows against itself to quickly move files around such as using the "expand" command in Windows to a system which has been designated for exfiltration.

When it comes to persistence, it's not hard schtasks is an option along with many other options.

Many of your questions or things you wish to do are actually rather trivial when it comes to post exploitation, even from a shell. Having the proper knowledge is what either makes you successful or not. These are important things which are important to learn, much like modifying metsrv.dll, it's okay to not know how to do things it's not okay though to continuing while knowing only hurts yourself. If you are unfamiliar a virtual lab is a good way to practice things safely.

You should know that a legit code signing certificate is a good idea and often well known malware can and does evade AV's.

Thank you for the reply. I actually do plan on learning Ruby, C++, Python, and Bash shell so I can get a better grasp on code in general. Right now I am stuck with a simple Android phone which isn't really ideal for hacking, practicing, or coding. So until I get a PC it's hard to practice. I have Termux so I get to practice the Bash shell a bit but a lot of the more effective actions need root access.

CyberStrike - November 26, 2019, 12:33 pm

(Nov 26, 2019 01:34 AM)stormcloudcypher Wrote: [\[CITE\]](#) Thank you for the reply. I actually do plan on learning Ruby, C++, Python, and Bash shell so I can get a better grasp on code in general. Right now I am stuck with a simple Android phone which isn't really ideal for hacking, practicing, or coding. So until I get a PC it's hard to practice. I have Termux so I get to practice the Bash shell a bit but a lot of the more effective actions need root access.

Why not forget the VPS and RATs instead save up say 5 dollars a month and get a used computer where you install Linux, perhaps a hypervisor such as virtualbox and learn before finding yourself over your head with a VPS or other issues.

mcducks - December 4, 2019, 7:47 am

(Nov 26, 2019 01:33 PM)CyberStrike Wrote: [\[CITE\]](#) Why not forget the VPS and RATs instead save up say 5 dollars a month and get a used computer where you install Linux, perhaps a hypervisor such as virtualbox and learn before finding yourself over your head with a VPS or other issues. vpses tend to cause issues with pf and all of that.

junagrunge - December 8, 2019, 9:03 am

(Nov 24, 2019 02:34 PM)stormcloudcypher Wrote: [\[CITE\]](#) I have this idea of using nmap on the network of my victim to get info on their device then metasploit to initiate a reverse shell on a victim through an exploit, then using that shell to install a RAT/more permanent backdoor, escalate privileges, and further hide that backdoor. I plan on doing all of this using the termux app on Android behind tor and a VPN, and host my RAT server on a VPS.

Does this plan sound plausible?

If so, what could I do to make it more plausible?

If it is plausible, what could I do to ensure it is done more stealthily and effectively?

Aside from that, any general suggestions?

Bisa anda menjelaskan cara menggunakan nya