**Hacking Windows Operating System (WAN attack).**

- [August 30, 2018](http://kalitutorialsforhacking.blogspot.com/2018/08/hacking-windows-operating-system-wan.html)

In this tutorial we are going to show you how to hack windows operating system over WAN

Here, we manage to hack into windows machine located on different Network. Where in previous practicals we hacked computers that are part of our local network.

**Ngrok Installation and configuration**

Ngrok is a tool that opens access to the local ports from the internet and creates a secure tunnel. Visit https://ngrok.com and register yourself to download a free version of the software.



To install ngrok application follow the process shown in below images (We can also get detailed installation steps from ngrok website).



To run ngrok on our computer (attacker’s kali linux machine), from ngrok directory execute

the command given on ngrok website.

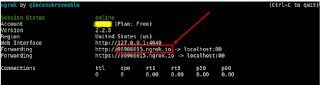




Execute below command that starts ngrok.



After executing the above command, ngrok opens a new terminal with links to forwarded ports.



Start Apache server and verify links created by ngrok





**Creating windows backdoor using ngrok**

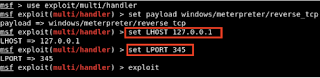
As we are using a free version of ngrok, we can forward only one port number. In this practical, we will use port 345 for listening reverse connections. Let us forward port 345 using ngrok and share malware file using send.firefox.com website.

To create a malicious .exe file, first, execute ngrok command for TCP port number 345.

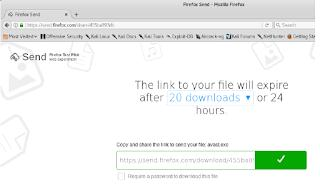
While creating malware using msfvenom it is important to note that we need to add ngrok provided link and port number as shown in below image.



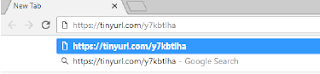
Start Metasploit Framework and load multi handler exploit. Set meterpreter payload and add localhost IP address (127.0.0.1) to LHOST and 345 as LPORT. Run exploit command and wait for a reverse connection.



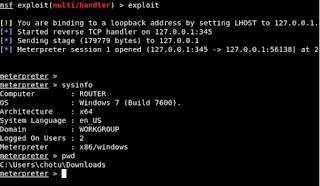
Now it is attacker’s turn to share the above-created malware file (avast.exe) with the target. Upload the malware file to https://send.firefox.com website and convince the target to download and execute the malicious file.



We can even shorten the above-generated link using [https://tinyurl.com](https://tinyurl.com/)



Once the target executes the malware file, a new meterpreter session starts on the attacker side.





By executing the above commands you will be able to hack any windows over WAN level.