# BackTrack 5 guide 4: How to perform stealth actions

Karthik R, Contributor

*You can read the original story here, on SearchSecurity.in.*

In previous installments of this BackTrack 5 how to tutorial, we have discussed information gathering and vulnerability assessment of the target system; explored network assessment, scanning and gaining access into the target; and, delved into privilege escalation tools. In this installment of the tutorial on BackTrack 5, how to perform stealth actions will be discussed.

## *Why stealth?*

The objective of penetration testing is to replicate the actions of a malicious attacker. No attacker desires discovery of surreptitious entry into the network, and hence employs stealth techniques to remain unnoticed. The penetration tester needs to adopt the same stealth methods, in order to honestly assess the target network.

***Figure 1.*** *The 'maintaining access' category in BackTrack 5, with a focus on OS backdoors.*

This installment of the BackTrack 5 how to tutorial deals with the "Maintaining Access" feature, within which are options for OS backdoors, tunneling and Web backdoors, as shown in Figure 1.

## *OS backdoors > Cymothoa:*

Cymothoa is a stealth backdooring tool on BackTrack 5 that injects backdoor shell code into an existing process. This tool has been developed by codewizard and crossbower from ElectronicSouls.

The general usage option of this tool is as follows:

```
Cymothoa -p <pid> -s <shellcode number> [options]
```

Cymothoa includes several payloads ready to be used. They are numbered from 0 to 14. The tool has various categories of options, including main options, injection options and payload options.

Figure 2 shows Cymothoa in action, affecting port 100 of process 1484, which is a bash process in the system.

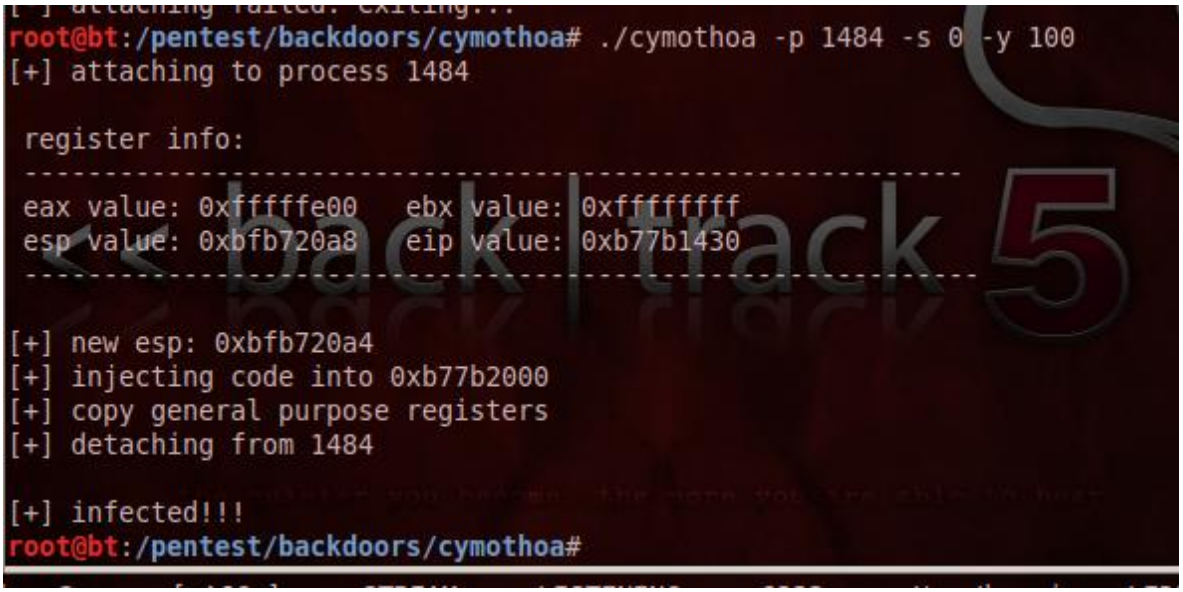


***Figure 2.*** *Running Cymothoa on pid 1484 on port 100.*


***Figure 3.*** *Before running Cymothoa infection.*

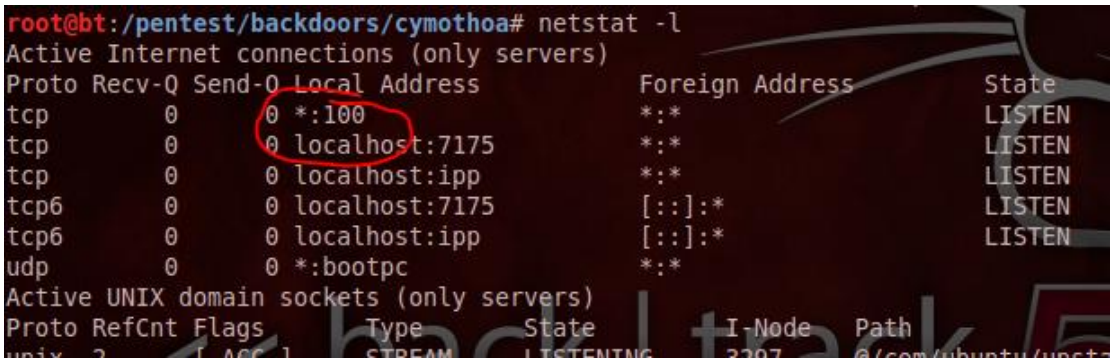


***Figure 4.*** *After running Cymothoa infection.*

As we progress in this BackTrack 5 how to, we can clearly see that the **netstat –l** command shows an additional port 100 added into the Listen category, since we have infected the port with the shell code numbered 0. Thus we can run Cymothoa on any system and infect any target port of the system and keep a backdoor open, to maintain access to the system. The target user will not have any knowledge of a backdoor running unless an inspection is made for any anomalies.

Getting the process id on BackTrack 5 is achieved using the command *ps –aux* in the Cymothoa shell.

## *Meterpreter as a backdoor*

In our previous series of tutorials we discussed meterpreter as an essential part of the Metasploit framework used in gaining system information of the target and also to carry out the tasks for spawning a shell into the target. In this section we shall explore along with BackTrack 5 how to use Meterpreter as a backdoor in BackTrack 5.

Usage:
*/opt/framework/msf3/msfpayload [<options>] <payload> [actions]*

This is effective when an attacker wants to connect back to a victim repeatedly, without having the user click on the malicious executable. For a clear understanding of Metasploit and meterpreter refer to our Metasploit tutorial and previous installments of our BackTrack 5 tutorial.

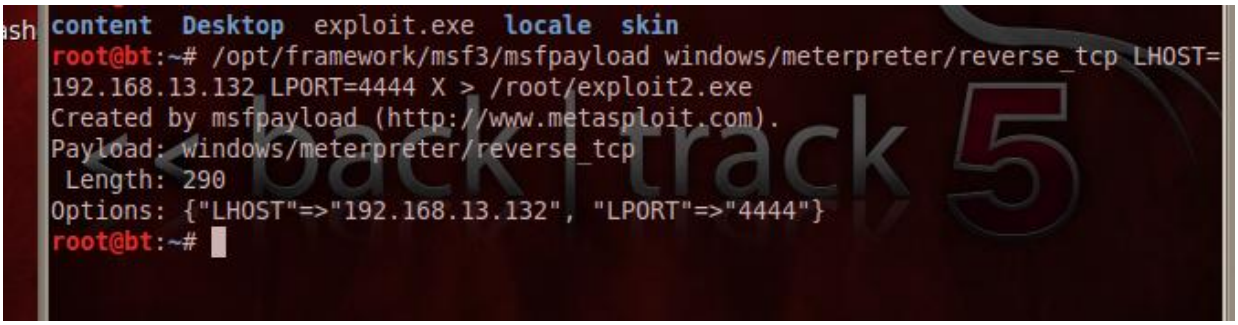


***Figure 5.*** *Creating the exe backdoor using msfpayload.*

In Figure 5 you can see that exploit.exe is the malicious msf meterpreter payload that is created using the msfpayload command. Continuing with this BackTrack 5 how to, we shall now create a listener to this payload, which would try to connect back to 192.168.13.132 on port 4444.

Using Metasploit, create a handler and set the LHOST and LPORT options as set in the msfpayload console. Once this is done, run the exploit. This exploit runs on a wild target. Whenever a victim clicks on this file -- sent to him using social engineering or other

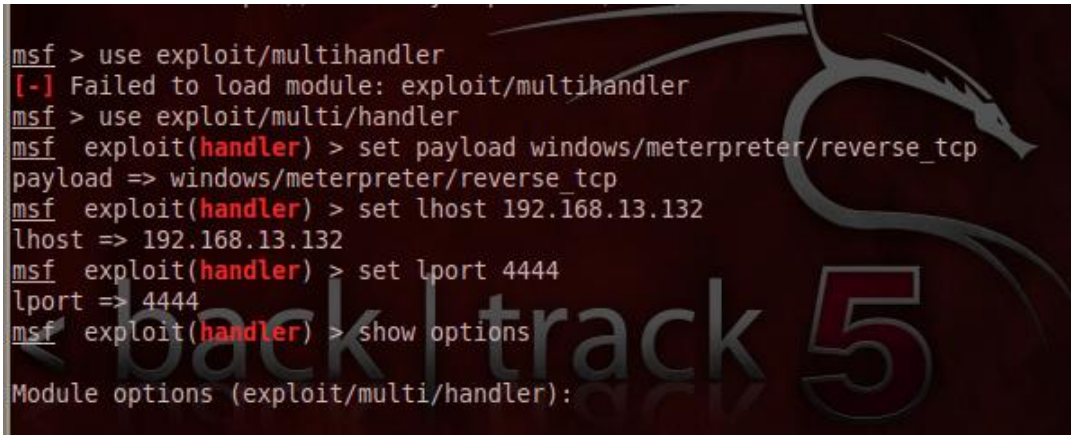


***Figure 6.*** *Handler created in Metasploit to listen to the backdoor.*

disguised methods -- it listens back to the LHOST and connects back to LPORT. As soon as the victim opens that exe file in his system, a meterpreter shell is spawned and the connection in initiated. The attacker can carry out the required post-exploitation tasks on the target once the connection is established.

## *Backdoor invasion vulnerabilities*

Backdoors are covert channels of communications with a system. The attacker can have longer, unrestricted access to a system by using a backdoor, saving the time and effort of engineering the attack from scratch. It is important for a penetration tester to check if the system is susceptible to backdoor invasions, so that unauthorized access can be prevented by providing suitable patches.


***Figure 7.*** *The victim system accessed by BT5 using a backdoor.*

The most common vulnerabilities that facilitate backdoor invasion of a system are buffer overflows, cross-site scripting (XSS) and remote administration. Preventive methods include regular change in the security policies based on the threat mitigation scenarios previously encountered by the organization; practice of secure software development cycle methodology; and, strictly following security standards in programming, making sure to check the application level security and any modifications done on a routine basis.

In this installment of the BackTrack 5 tutorial, we have seen how to use BackTrack 5 for including stealth in your attacks as a penetration tester. In the next and final part of this BackTrack 5 how to guide, we shall present a scenario-based attack using BackTrack 5, and carry out an attack from scratch while including all the methods and techniques covered in this BackTrack 5 how to series.

***Do not miss Part 5 of our BackTrack 5 tutorial which details how to perform penetration testing***

---

**About the author:** ***Karthik R*** *is a member of the NULL community. Karthik completed his training for EC-council CEH in December 2010, and is at present pursuing his final year of B.Tech. in Information Technology, from National Institute of Technology, Surathkal. Karthik can be contacted on rkarthik.poojary@gmail.com. He blogs at http://www.epsilonlambda.wordpress.com*

*You can subscribe to our twitter feed at @SearchSecIN. You can read the original story here, on SearchSecurity.in.*

---