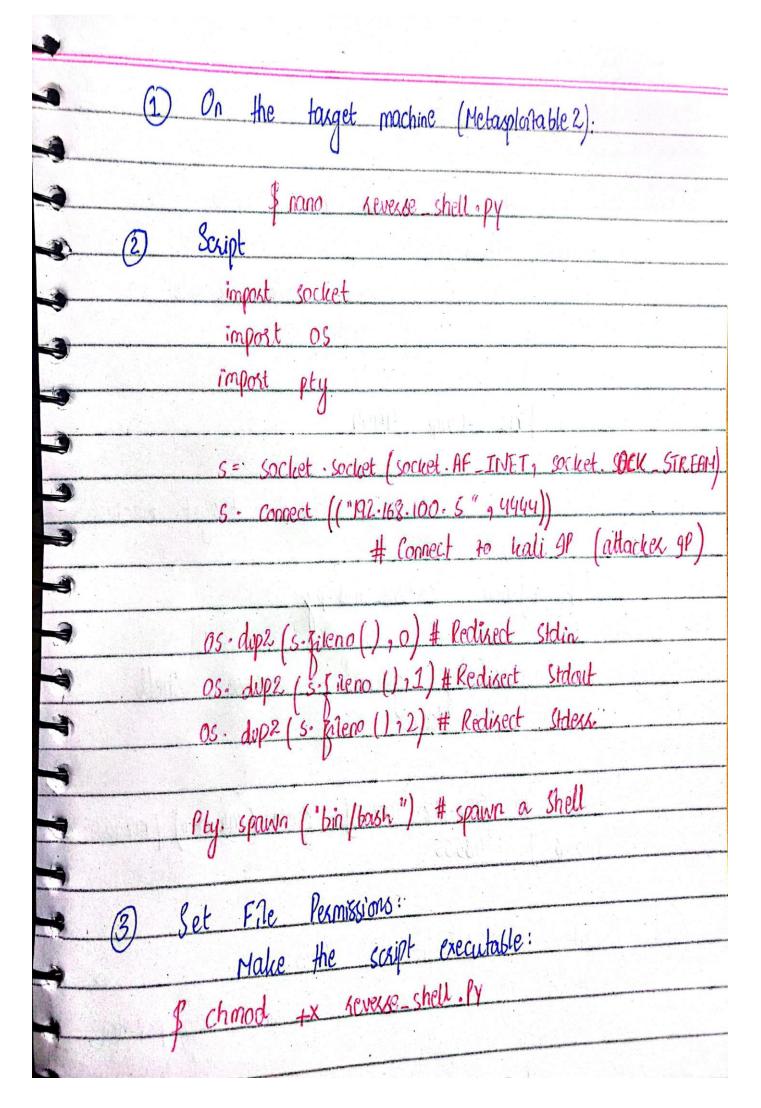
	9
What is shell shock vulnerability?	0
The shellshock vulnerability (CVE-2014-6271) is a	The state of the s
serious glaw in the Bash shell, which is	-
the program that handles commands in	4
many Unix-like system (like linux & macOS).	
This vulnerability allows an attacker to run	
1 a company of WilnexAble Wfom.	
The problem is that the Bosh incorrectly handles	
Il a Cenvisanment Vociobles. These variables are like	*
that stone information about the	
define a function inside the envisonment	×
variable. When Bash process this variable,	*
1 malicials	一
commands defined by the attacher.	*
What is an arbitrary Command Command	1
In arbitrary command means any command be executed on the system;	-
that can come or	
inthout restrictions. In the context of the	-01
Shell shock vulnexability, it sofess to the ability	0
of the attacker to execute any comman	1

they choose on a vulnerable system. Commands that give them more control over the System, such as spawning a reverse shell on installing malwave. Option # 1 Adentifying Vulnesability: to shell shock the following command was executed: env x= () { :: } i echo vulnerable bash -c "echo test" Lyenv: The environment variables and execute a command in a modified environment x='() \ ;; \ i echo vulnerable: • This sets an environment vasiable name [x]. · The value () [: if i echo vulnerable mimics a function I definition in Bash: e () declases a function is a no-op (doesnothing command)

e [] ends the no-op command

and executes the echo vulnerable command outside the Eunction body, making it malicious.	N. W. W.
This is a capted input to exploit the shell shock vulnerability.	
L> bash -c "echo test":	-
: This executes a new Bosh shell (bosh)	
: The [c] flag specifies that the following. String (" echo test") is a command to	Terrogramment of the second
	20
= 9n a non-vulnerable bash version, the commands simply echoes [test].	1 1
But here output was	The same of the sa
vilnerable	The second
test-	The same of the sa
(2) Geating the Reverse Stiell:	
I then excated a reverse shell payload	-
2 Creating the Reverse Stiell: I then executed a reverse stiell payload that exploited the still shock vulnerability.	-
The payload used the following python reverse	1



3 Execute the Script:	
	-
(hali linux):	
open terminal and start Netcot to	
11111	-
AND	9
(2) Rup the script on the target machine	
\$ python reverse-shell-py	
Success Fully gained reverse shell	
	-
connect to [192.168.100.5] from (unknown) [192.168.	2
	*
(4) Privilege Escalation Via Sudo:	-
(4) Privilege Escalation Via Sudo: Check if the user Msfadmin has previlege escalation capabilities:	7
\$ Sudo -L	4.0