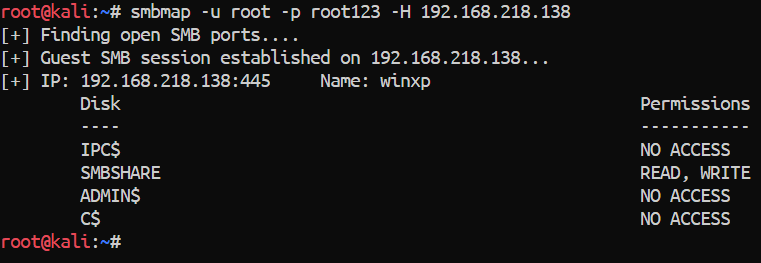
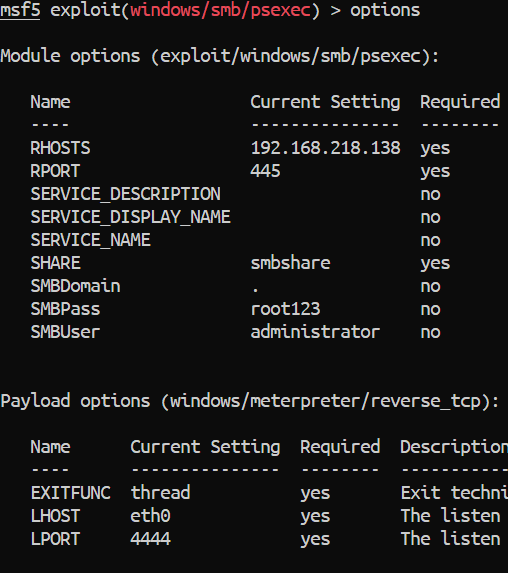
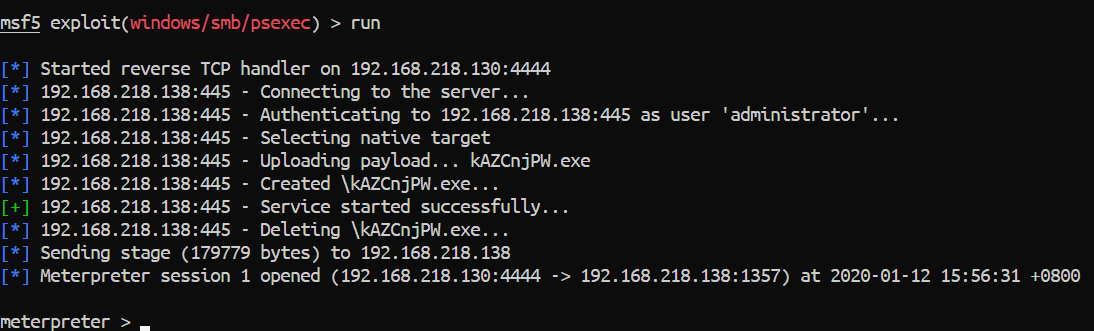
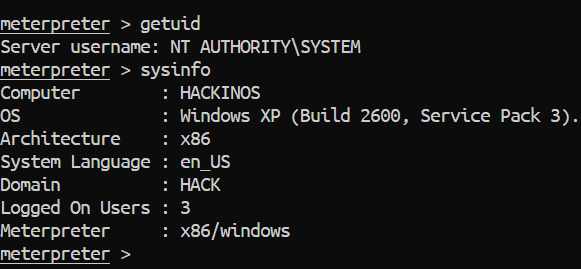
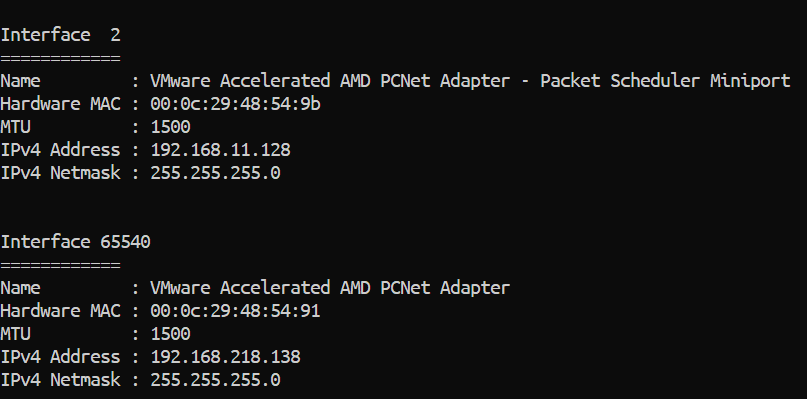
Given username: root and password: root123

Set share to share folders we have read and write access

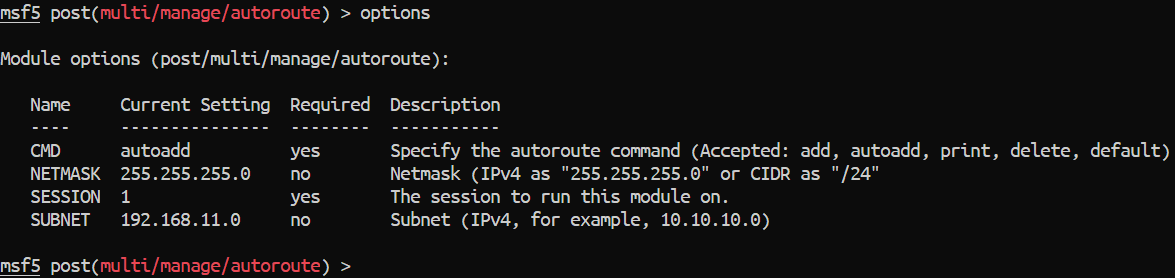
Connect to winxp workstation using PSEXEC a success

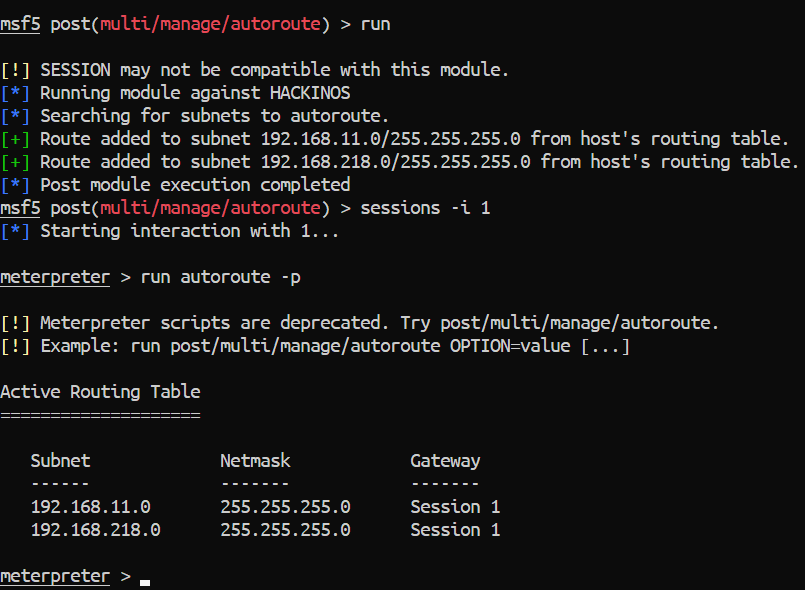


System authority on winxp

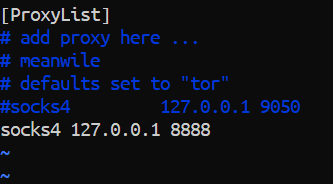
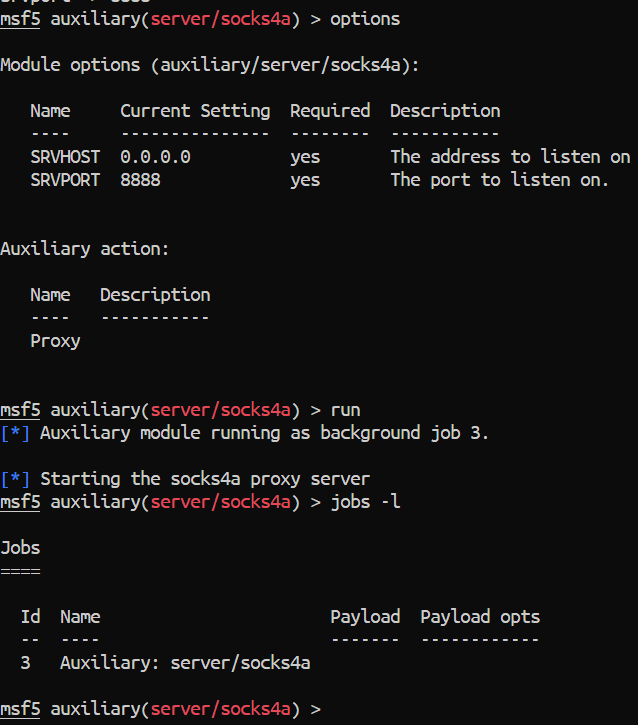
2 subnets

Setting autoroute options for pivoting

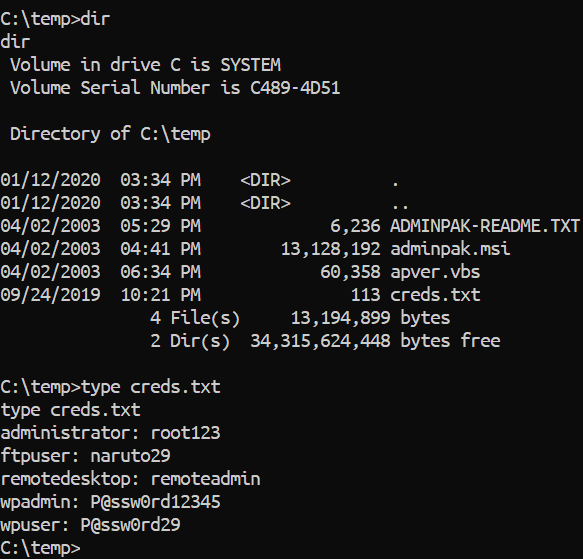


We have access to the hidden subnetwork

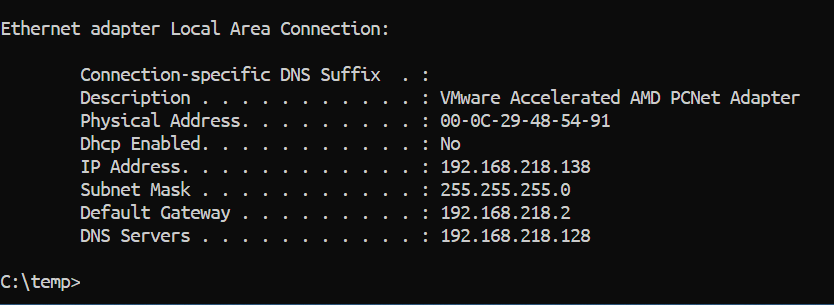
Setting socks4 option for proxychains



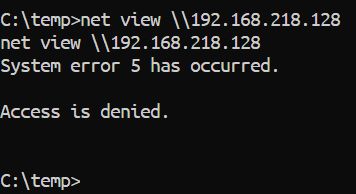
Getting credentials



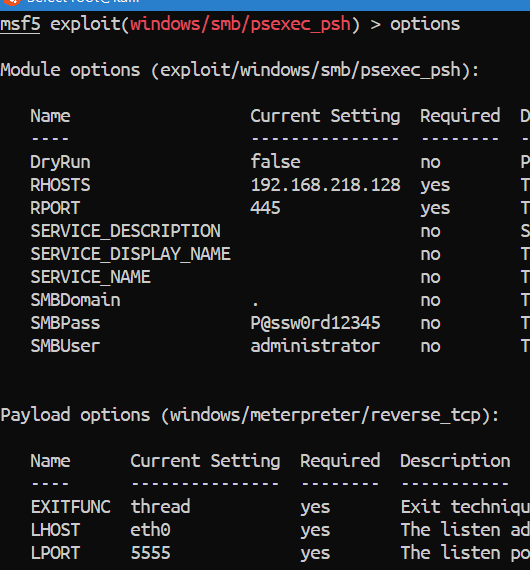
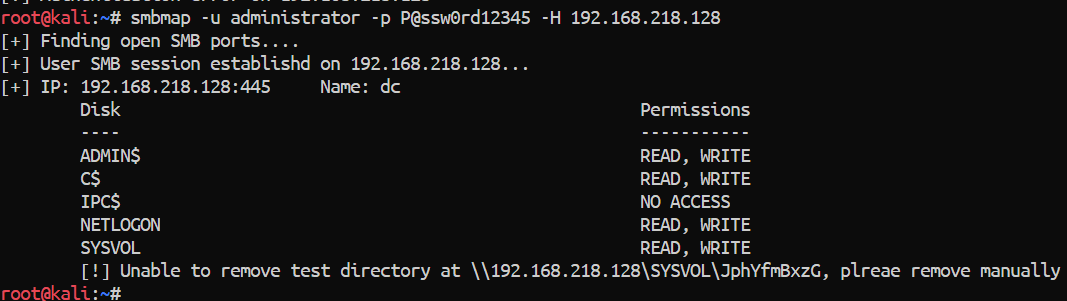
Determine ip for DC



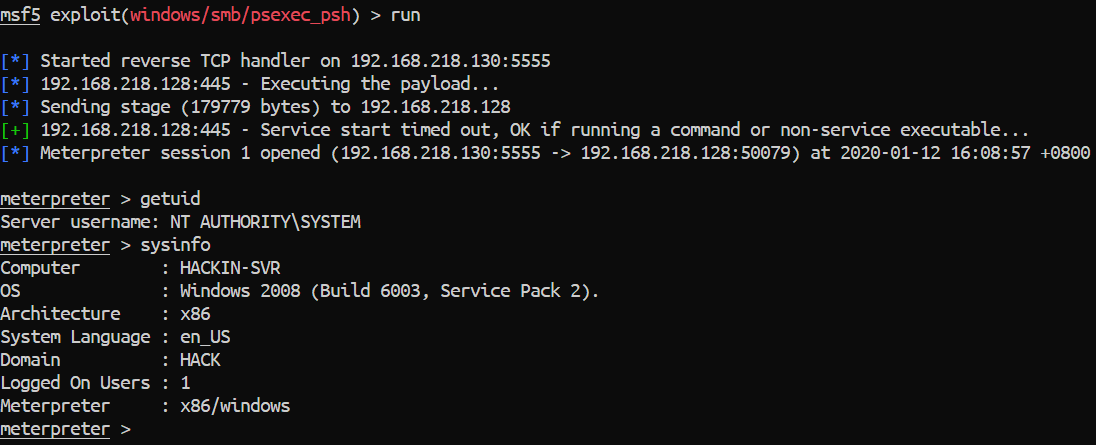
On our current creds, we have no access to view shares on DC



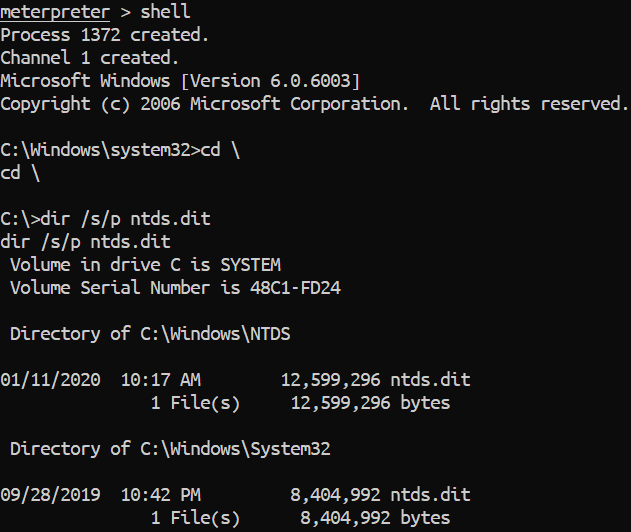
Password reuse(DC) / Guessing based on the creds that we have



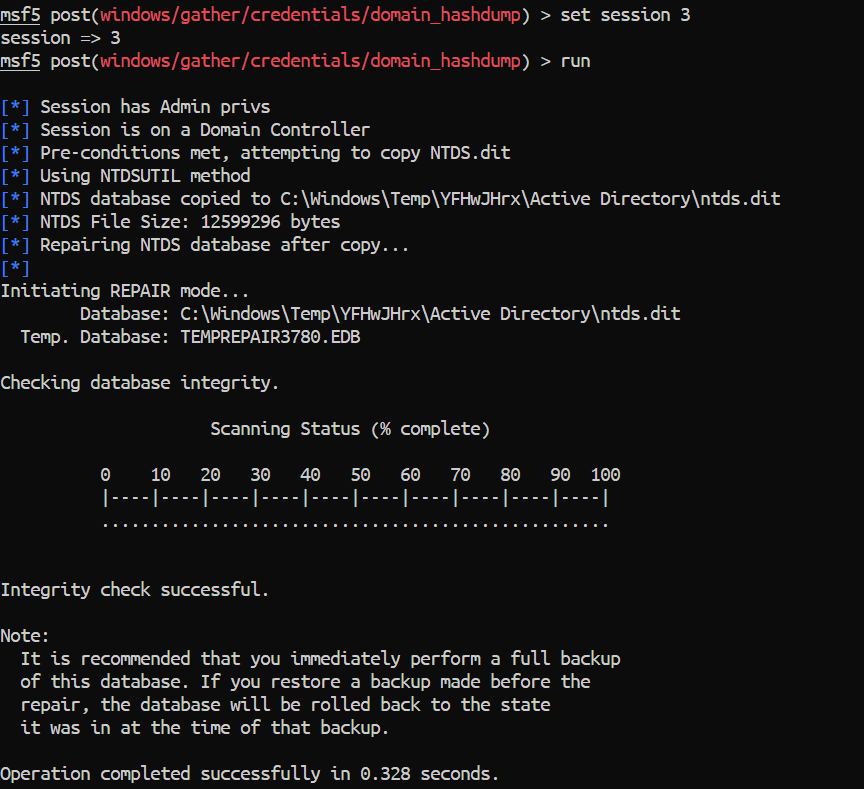
Somehow we have system access on DC

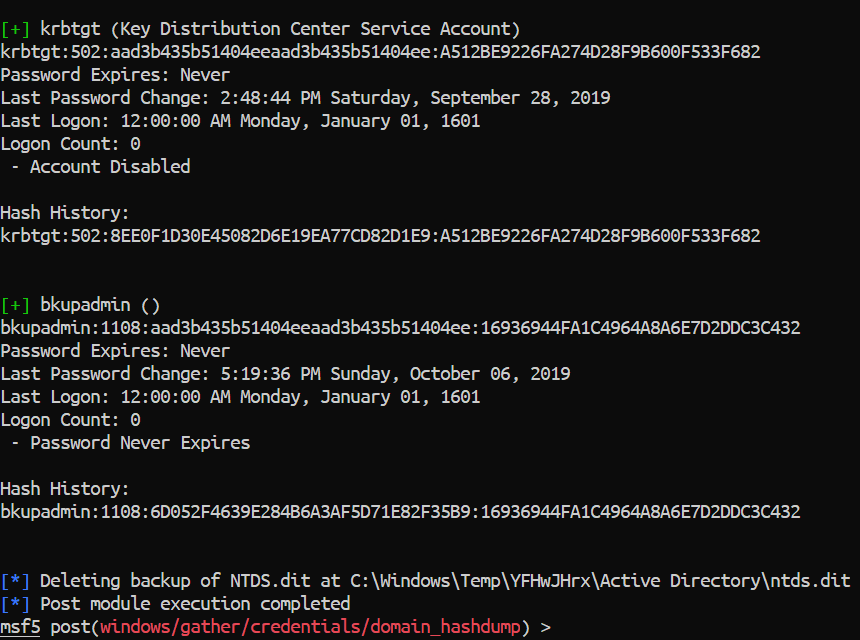
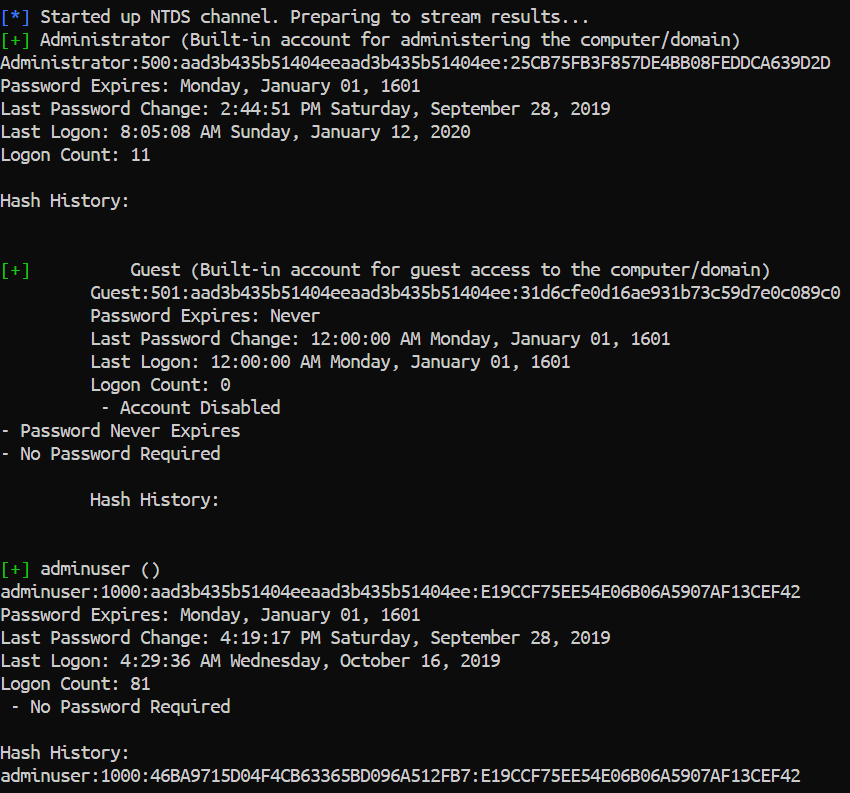


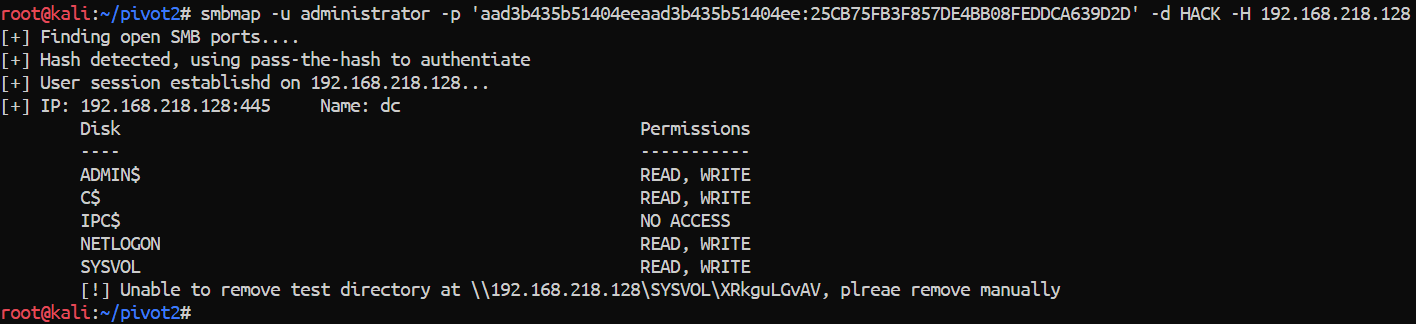
Doing post exploitation



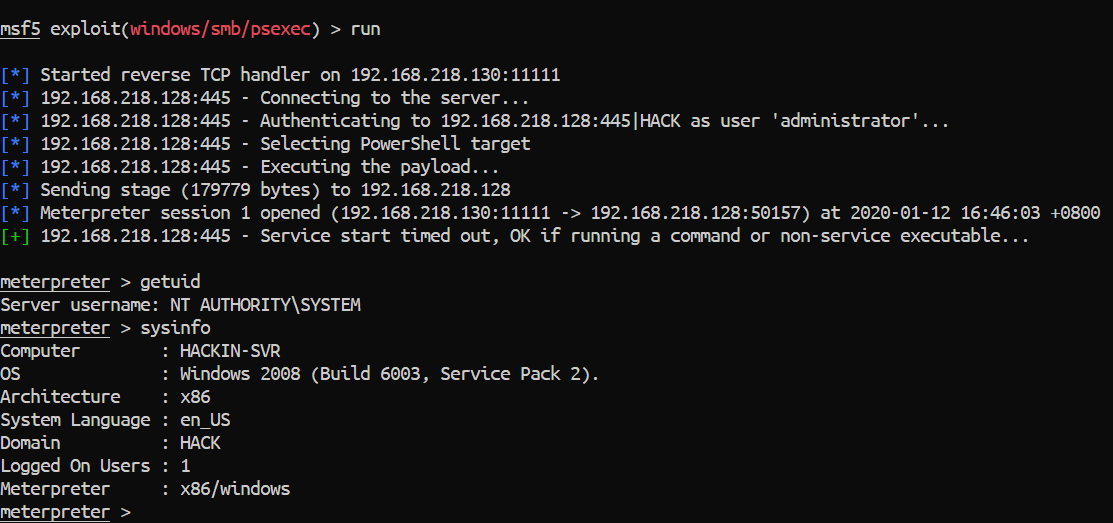
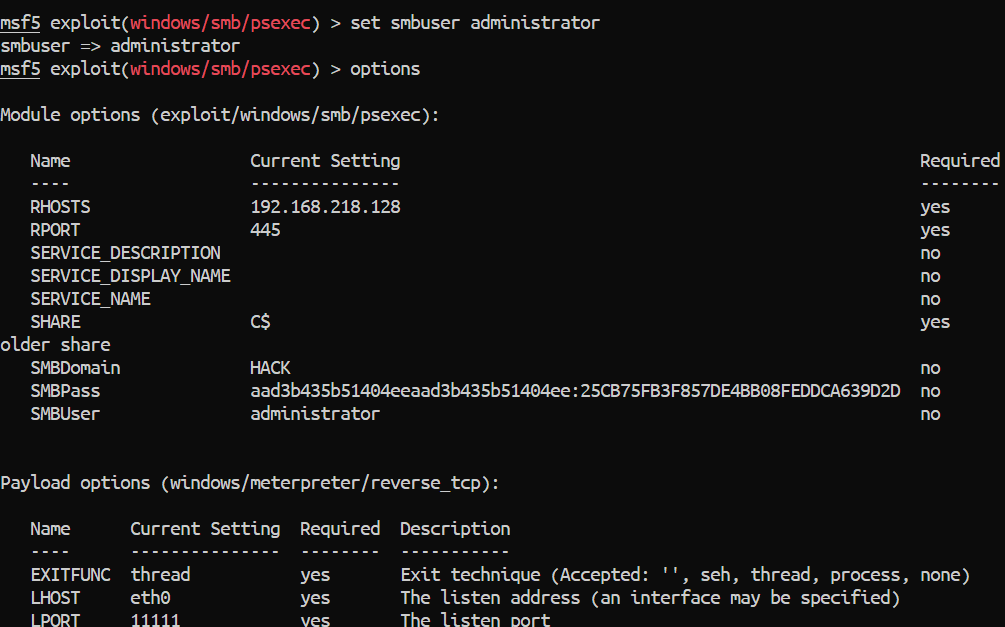
Password dump of dc



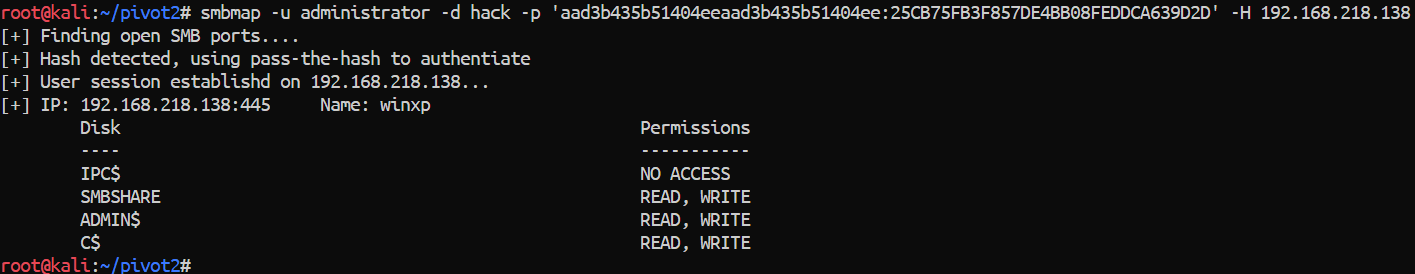


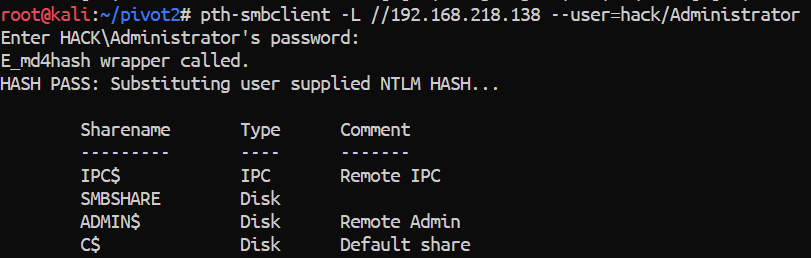
Checking creds for administrator

Testing creds on DC, success

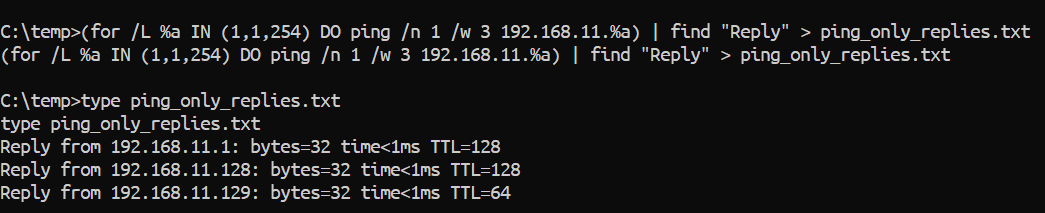


Testing creds on winxp workstation





Searching computers on hidden subnetwork



Priv escalation on hidden computer

