CND Writeup

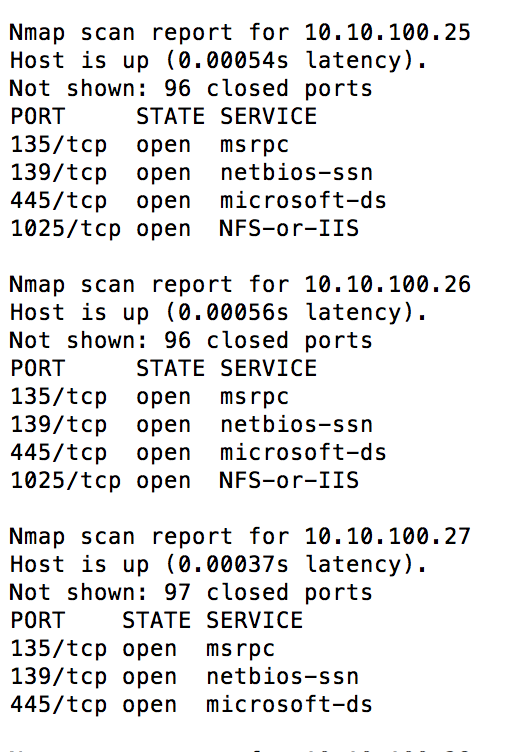
Rajat Vij

Step 1: Shell into kali box

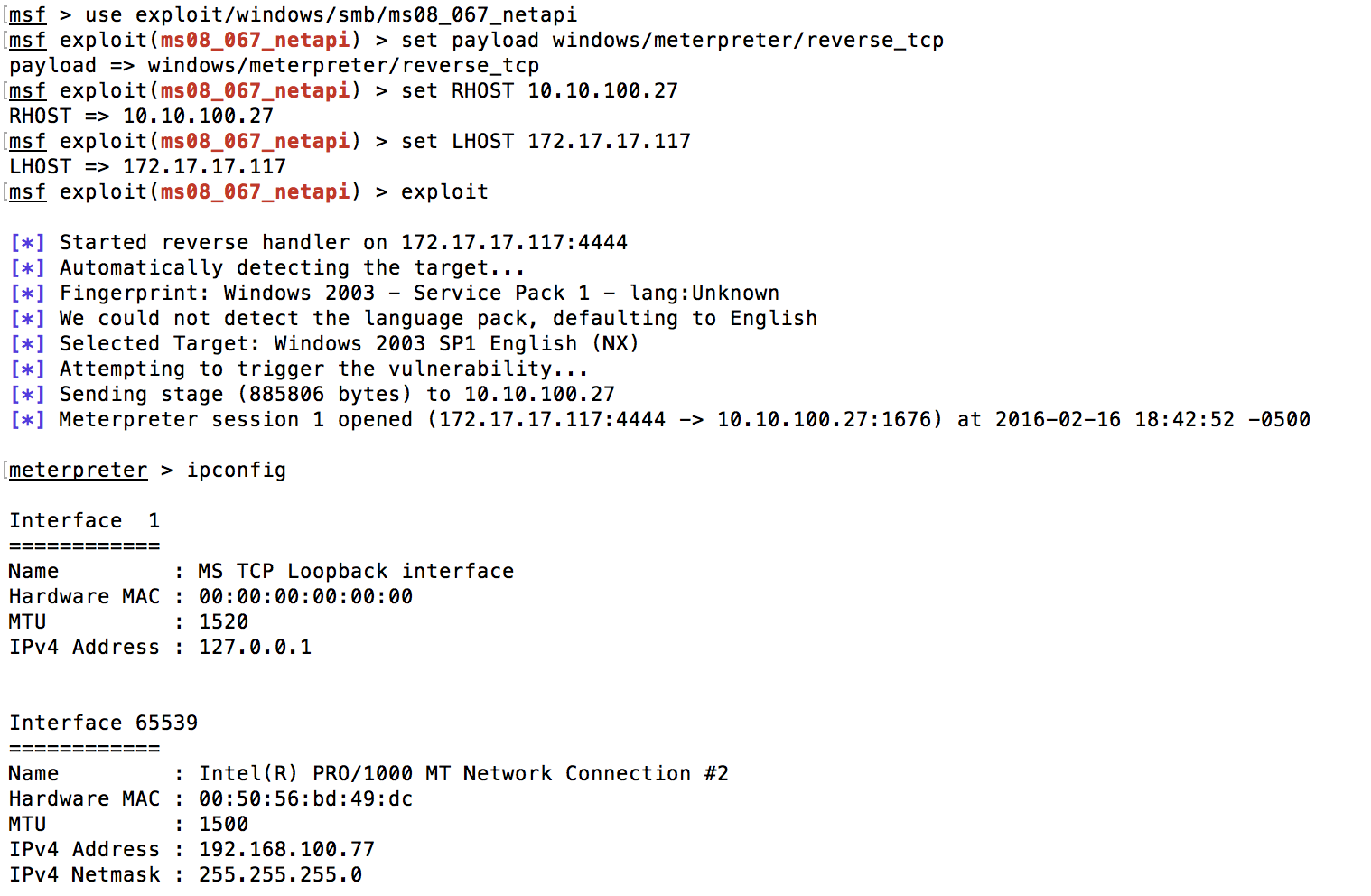


Step 2: nmap –F 10.10.100.0/24

Scan for Windows 2003 box in 10.10.100.0/24 network range



Step 3: exploit a target machine – Windows 2003



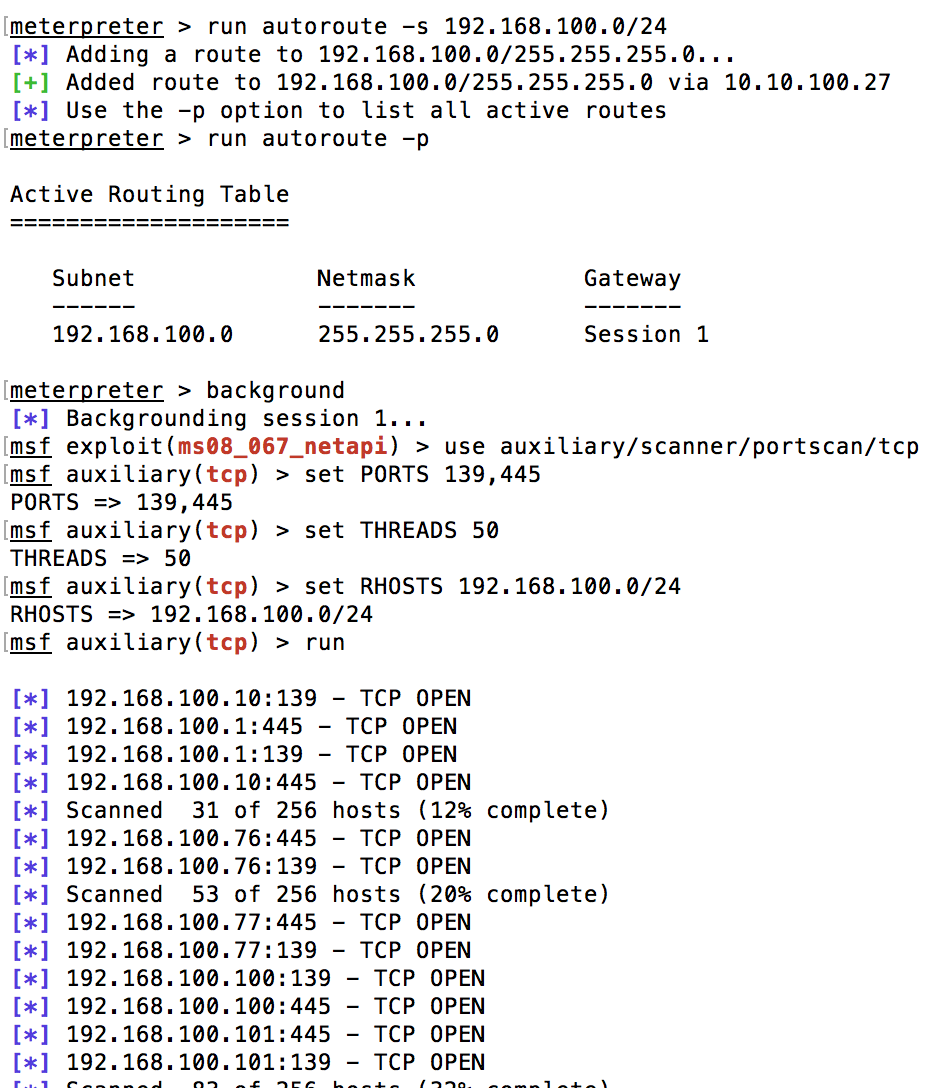
Step 4: Check ip address in 192 range for the machine and run autoroute

Once we are into the system we can check ip address for the windows 2003 box and check its ip address in 192 address range so we can use it as a pivot to laterally move to windows 7 boxes.

Run auto route to 192 address range.

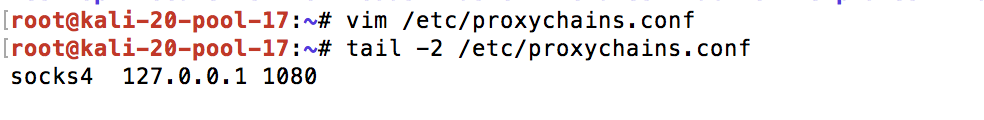
Step 5: run exploit/auxiliary/scanner/tcp to 192 range

We can use scanner to scan 192 address range of open ports on the boxes.

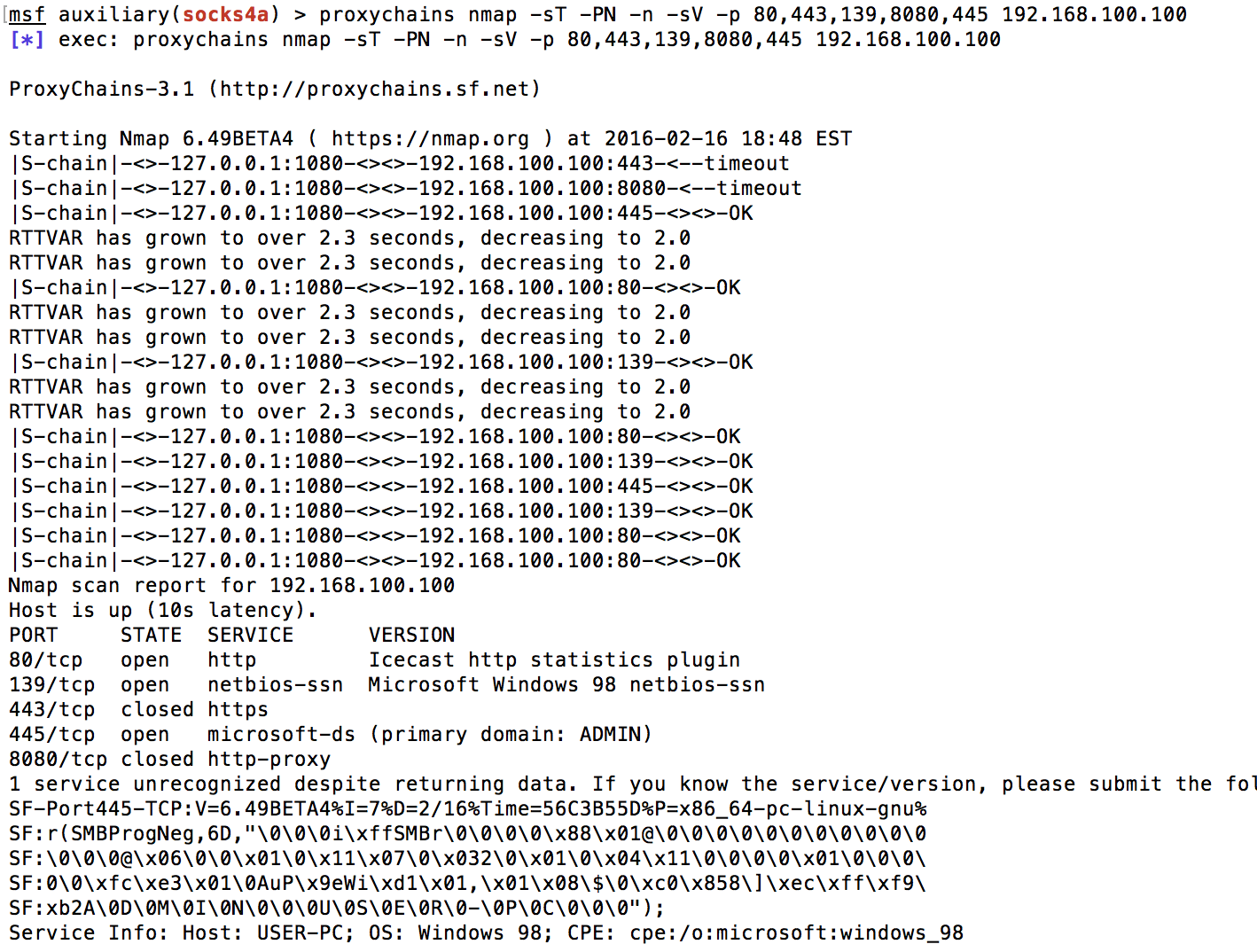


Step 6: edit /etc/proxychains.conf

Once we have identified the target machine in 192 address range we edit /etc/proxychains.conf file to run nmap via proxychains



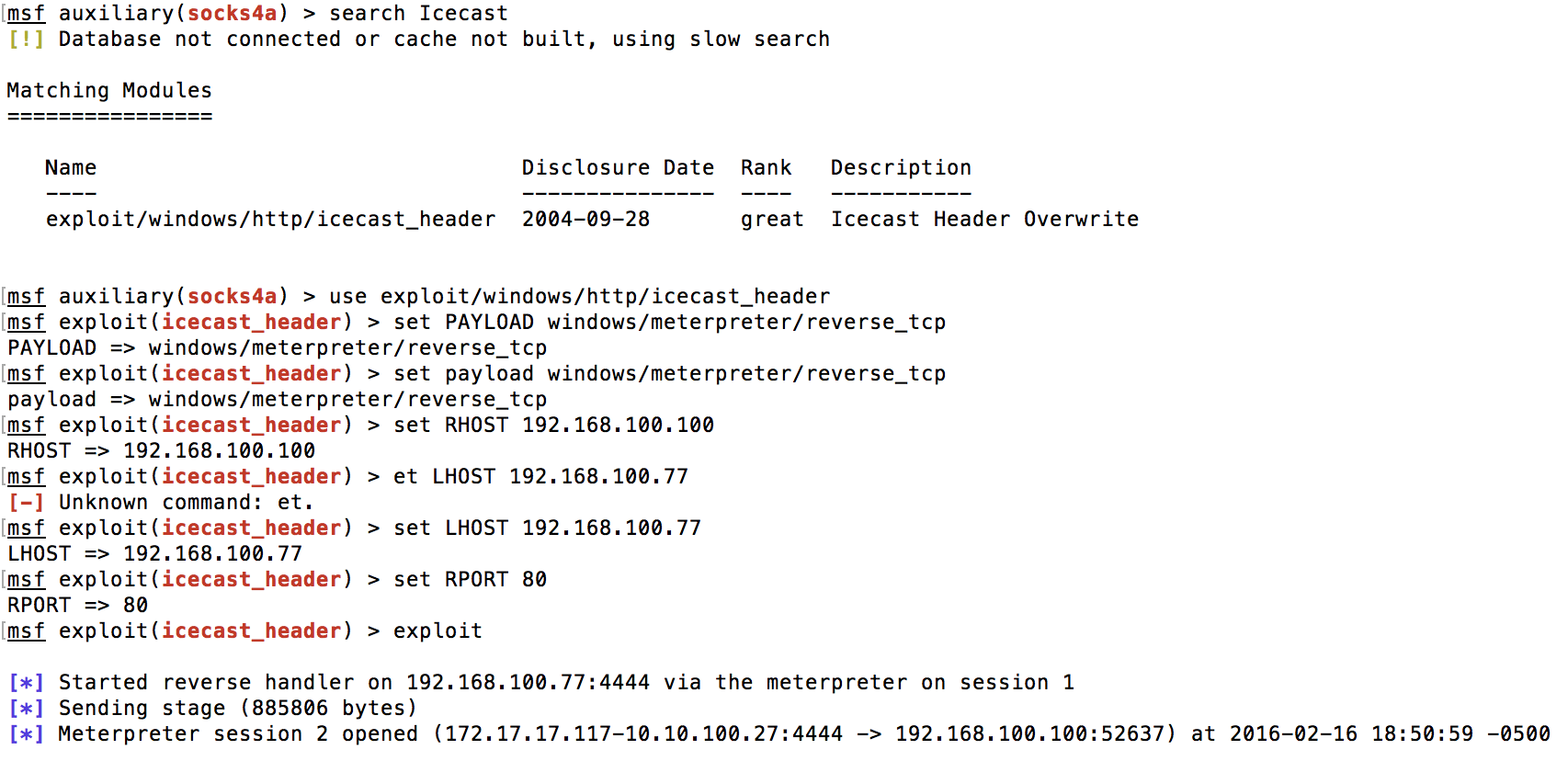
Step 7: run nmap via proxychaines



Step 8: Identify vulnerable service on target machine in 192 range

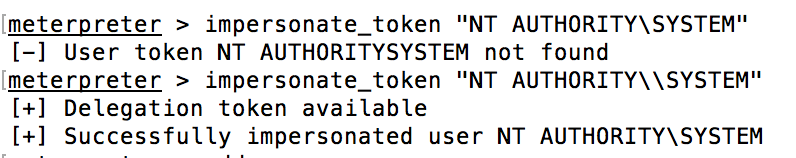
We got Icecast at 80 port. We can search this in msfconsole to exploit

Step 9: Exploit vulnerable service. – Windows 7

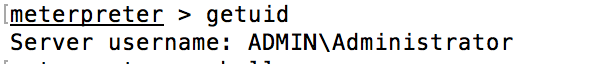


Step 10: getsystem privillages and impersonate\_token for system user.

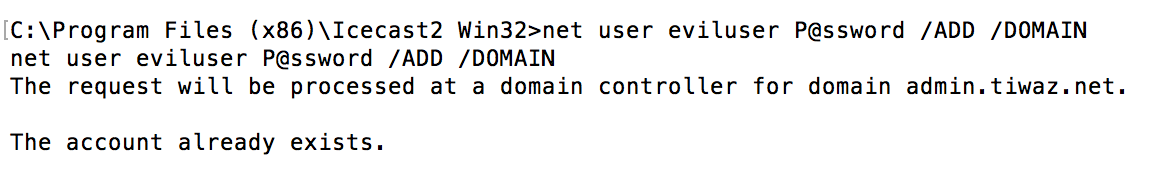




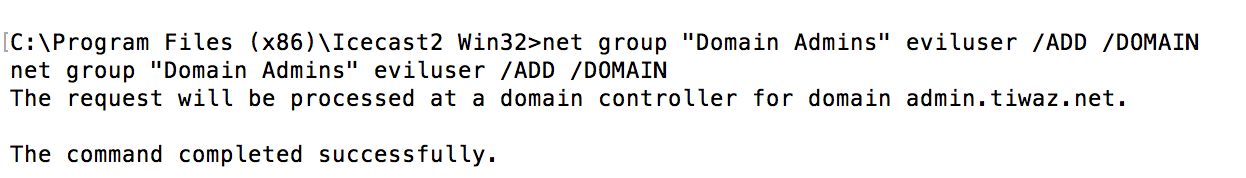
NOTE: Here we need to impersonate ADMIN/Administrator instead of system as that user can add a dummy user to domain controller. I was having issues here.



Step 11: add user to domain controller.



Step 12: Use added user to access or exploit Domain Controller – Windows 2008



Step 13: Use kiwi to create a golden ticket for persistent exploitation.