**Implementation of Netstat**

## **Port Scanning:**

## **How to use of Netstat:**

* Open Start
* Open Command Prompt as administrator.
* Enter **netstat** to get a list of all active TCP connections.
* Enter **netstat -a** to get list of all TCP, UDP and all listening ports.
* Enter **‘****netstat -a >> <location to place file>\portscan.log'** to get netstat command output into portscan.log file.

MD System TS System

Logs

netstat -a

Fig1: Execution Of command.

## **Evidence:**

* Local Execution with Evidence

Below command executed on MD system

**Command:** netstat -a >> <location to place file>\portscan.log

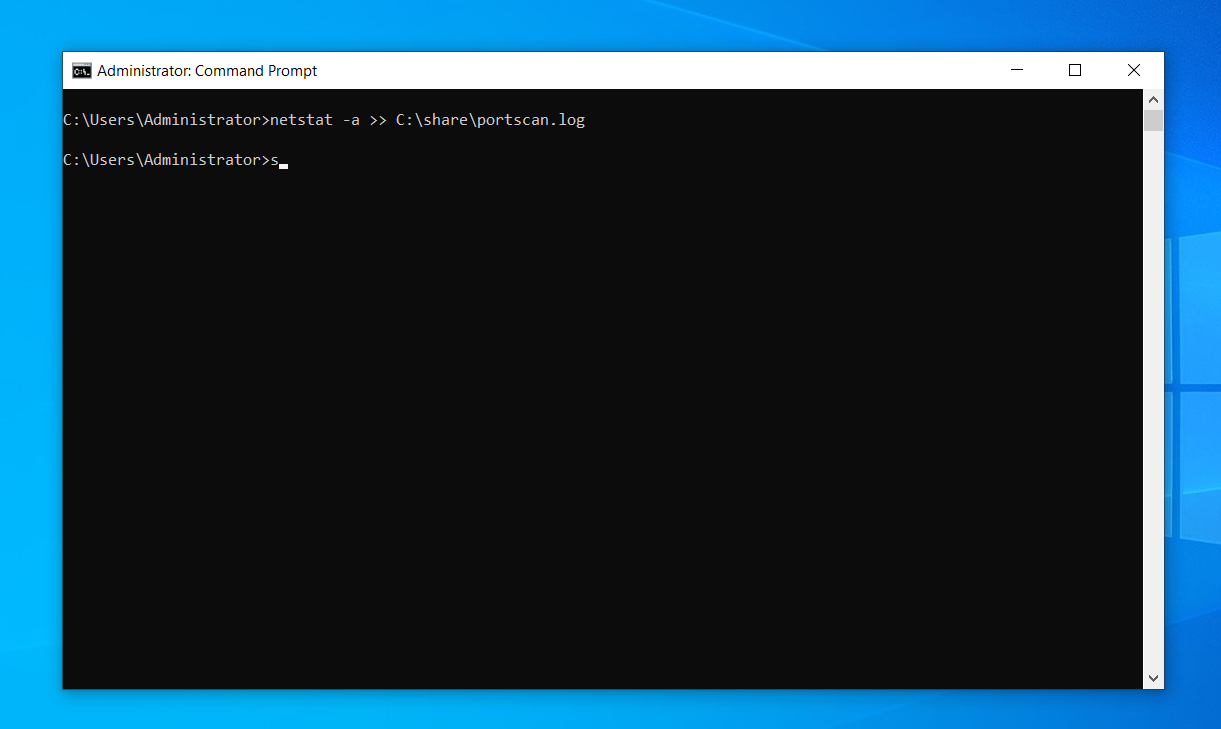


Fig 2.1: Executed Command on MD System

* Remote Execution with Evidence

Below command executed on MD system

**Command:**

python

import winrm

s = winrm.Session(‘<target\_machine\_ip>’, auth=(‘<user\_name>’,’<password>’))

r = s.run\_cmd(‘netstat -a >> <log\_file>’)

r.status\_code

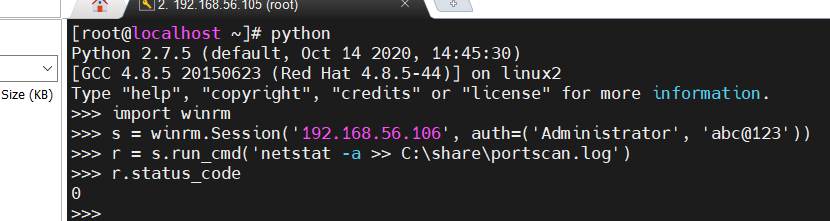


Fig 2.2: Remote Execution on MD System Successful status evidence

## **Verification:**

* Login TS system.
* Open This PC.
* Go into local disk (C)
* Go into Share folder
* “portscan” log file must be there

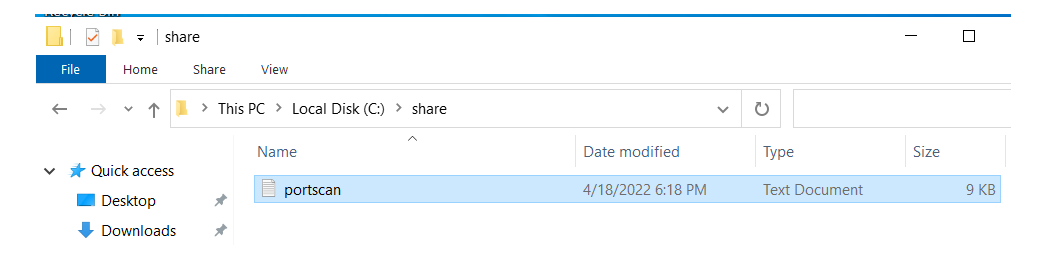


Fig 2.3: Port scan log created on TS system after remote execution on MD System Successful