Team 1

NETW07T

To the Information Technology team:

I am writing to report on the securing of SNMP traffic across our operating systems and networks. The objective of this was to ensure that SNMP is able to provide the services it needs to our network without overly compromising security.

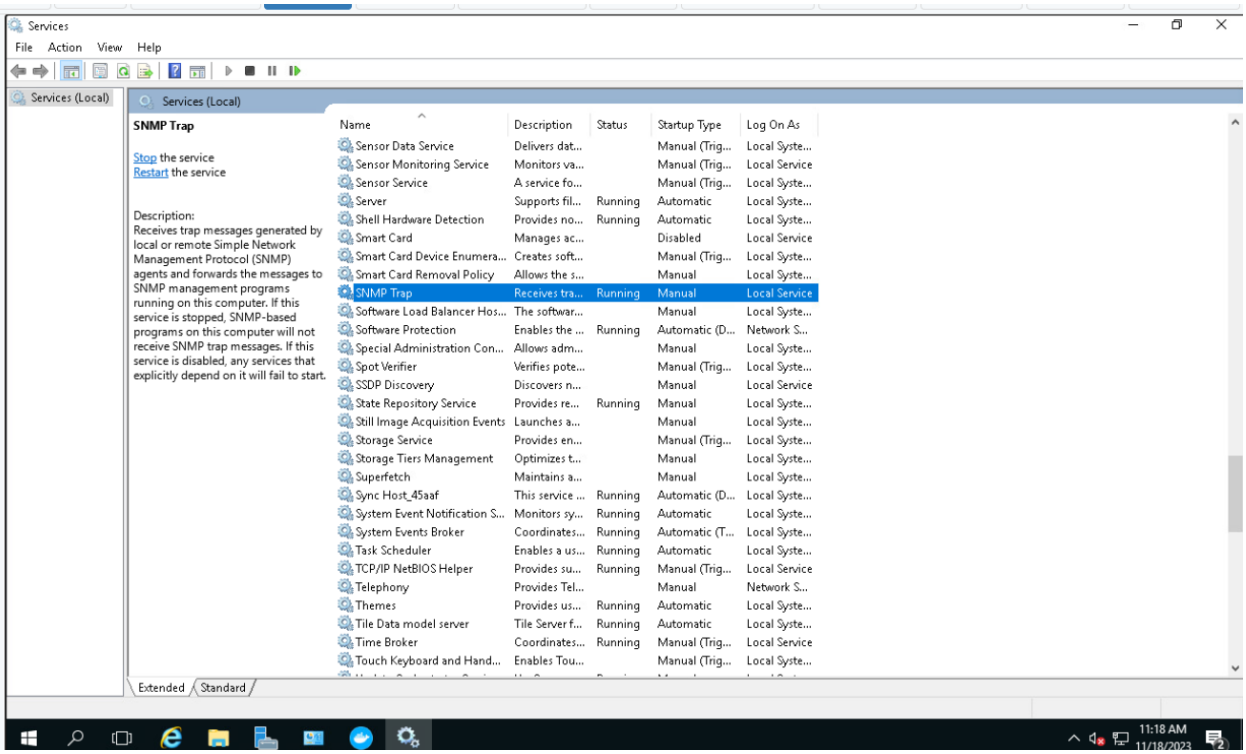
In order to achieve this objective, the Windows team configured the SNMP strings to be a strong ‘read-only’ community string, specified the only IP ranges allowed to operate in SNMP, and configured SNMP traps. For the Fedora Linux team, they simply disabled SNMP traffic through the firewall. The Firewall team did not provide any configuration information on SNMP traffic.

Please find attached screenshots of the server teams configuring the SNMP traffic.

If you have any questions or need further information, please do not hesitate to reach out.

Best regards,

Group 1




```
FedoraServer (default, active)
  interfaces: ens32
  sources:
  services: cockpit dhcpv6-client dns http https imaps pop3s smtp
  ports: 53/udp 53/tcp
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:

[root@fedora snmp]#
```