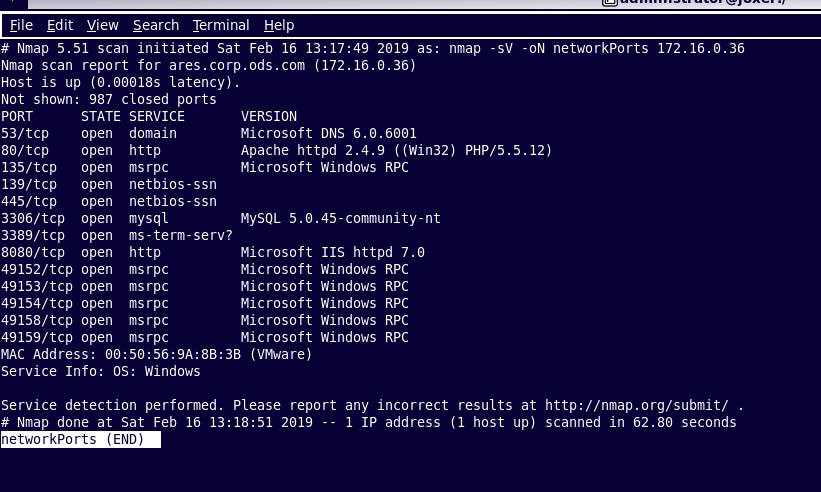
**Non-essential Services Report**

**Non-essential Service Analysis:** An analysis of the network services was conducted using NMAP. After the scan was completed, the owners of the machines were notified which services were running on their machines so that they could remove them to lessen the avenues of approach for unethical hackers.

**Example NMAP Results: (**The results below are a small fraction of what the output was, this is just to show how information was passed to machine owners)



**Minerva**

* Telnet: Disabled through a system command to shutdown services.

**Athena**

* Apache2: Disabled via rc-service *[service]* stop.
* SSH: Disabled via rc-service *[service]* stop.
* VSFTPD: Disabled via rc-service *[service]* stop.

**Amarice**

* No non-essential services running.

**Aphrodite**

* No non-essential services running.

**Flafel**

* RPC BIND: Disabled through a system command to shutdown services
* Apache2: Disabled through a system command to shutdown services
* Open vpn: Disabled through a system command to shutdown services

**Gabrielle**

* Team viewer: Disabled through a system command to shutdown services
* VPN Windows Server: Disabled through a system command to shutdown services

**Joxer**

* VNC: Disabled through a system command to shutdown services.
* Telnet: Disabled through a system command to shutdown services.

**Loki**

* Telnet: Disabled through a system command to shutdown services.

**Notares**

* No non-essential services running.

**Hercules**

* Telnet: Disabled Telnet and replaced with IIS.