Exercise – Parse NMAP results

Scenario

Your team is conducting a survey for a DCO mission. The command is in a hurry, and has told you that they suspect the network has a large number of vulnerable services. Given only nmap results, you, as a CTE (Cyber Threat Emulation) squad member, need to identify the 3 most open services in the network, as well as the most common open TCP service, amongst all of the scanned systems.

Exercise

- Develop a script that you can run on the provided nmap network scan results.
- Your script needs to output each open service, and the applicable IP addresses for each service.

Non-Scripted

- Output a summarized count of each open service in from the entire scan. Be sure to avoid output that isn't relevant to the mission.
- Include Screen-Capture of your script's output in your submission.

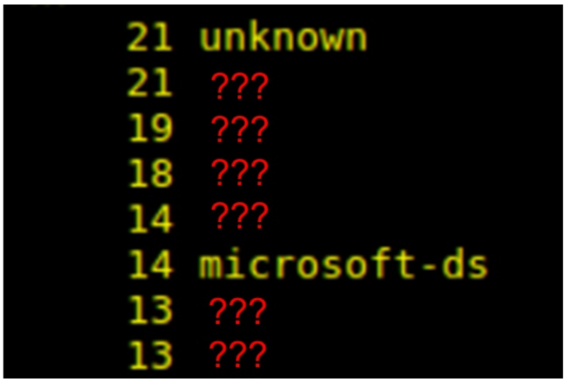
Each student must submit a script

nmap network scan results: /usr/share/cctc/NMAP_all_hosts.txt

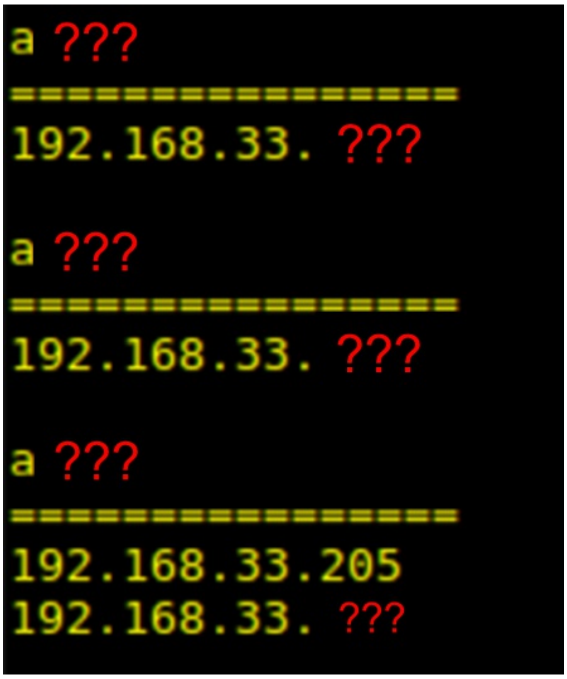
Hint: man pages - grep, sed, awk, cut, column, sort, uniq; REGEX.

Hint: watch out for command bleed-over into other system output.

Example Output



```
     21 unknown
     21 ???
     19 ???
     18 ???
     14 ???
     14 microsoft-ds
     13 ???
     13 ???
```



```
a ???
=================
192.168.33. ???

a ???
=================
192.168.33. ???

a ???
=================
192.168.33.205
192.168.33. ???
```

Grading

- 70% - Submit: Your Correctly Functioning Bash Script
- +10% - Submit: Screen-Capture: Services Summarized (see example: first image)
- +20% - Submit: Screen-Capture: Hosts by Service(see example: second image)

Learning Objectives / Outcomes

- Familiarity with more granular approaches to parsing through data via scripts
- Operational context

Last updated 2017-08-14 10:22:49 EDT