Log Analysis

Nginx (Medium)

This challenge evaluates the contestant's ability to analyze an Nginx access log. Basic scripting knowledge is necessary to complete the challenge in a reasonable amount of time.

Question 1 can be solved by using this Linux command to parse the log and find all unique IPs and count them:

```
cat access.log | cut -d " " -f 1 | sort | uniq -c | wc -l
```

Questions 2 and 3 can be solved by using this Linux command to parse the log and get the number of responses for each response code:

```
cat access.log | cut -d '"' -f3 | cut -d ' ' -f2 | sort | uniq -c | sort -rn
```

Questions 4 and 5 can be solved by searching for the strings "ring" and "googlebot" respectively.

Question 6 can be solved by recognizing that shellshock uses command injection and searching for requests that look like command injection. A search for "bash" should help with this.

Question 7 can be solved by using this Linux command to find all requests made by Firefox:

```
cat access.log | grep Firefox
```

Questions 8 - 10 can be solved by using this Linux command to parse the log and sort by the number of HTTP requests for each method. Note that for question 10, the requests do not follow proper HTTP conventions, so the answer can be found with the rest of the HTTP method counts.

```
awk -F" " '{print $6}' access.log | sort | uniq –c
```

Question	Answer
How many different IP addresses reached the server?	47
How many requests yielded a 200 code?	19
How many requests yielded a 400 code?	38
What IP address rang at the doorbell?	186.64.69.141
What version of the Googlebot visited the website?	2.1
Which IP address attempted to exploit the shellshock vulnerability?	61.161.130.241
What was the most popular version of Firefox used for browsing the website?	31
What is the most common HTTP method used?	GET
What is the second most common HTTP method used?	CONNECT
How many requests were for \x04\x01\x00P\xC6\xCE\x0Eu0\x00?	6

© 2017 Cyber Skyline. All Rights Reserved.
Unauthorized reproduction or distribution of this copyrighted work is illegal.