**Firewall (Hard)**

**Our security operations team needs help deciphering a firewall log, can you help them out?**

**What is the hostname from this log?**

1. Look at the beginning of the first log input.
2. Answer: apolo kernel

**What IP has the most connection attempts to the host?**

1. Type *cat ufw.log | cut -d "=" -f5 | sort | uniq -c | sort -rn | head -n 1* into the terminal.
   1. *uniq -c* : Displays in output the number of times a unique line is repeated.
   2. *sort -r* : Sorts the input file in reverse order, i.e. descending order by default.
   3. *sort -n* : Sorts the file numerically when numeric data is present.
   4. *head -n 1* : The head command, as the name implies, prints the top N number of data of the given input. By default, it prints the first 10 lines of the specified files. -n x will print the first x outputs; in this case x=1 so only the first output will be printed.
2. Answer: \*forgot to record answer.

\*Unanswered questions:

**What is the average time to live (rounded to nearest hop)?**

**How many unique destination IPs are there?**

**What destination port has the most connection attempts?**

**What is the total amount of bytes sent?**