**Section 1, Step 7**

* Choose two nslookup parameters that would be helpful during the reconnaissance phase and mention why they would be of interest
  + **The two nslookup parameters I would use during the reconnaise phase would be -server and -querytype. The parameter -server would allow me to query different DNS servers other than the default configured on my machine. The second parameter would be the -querytype so I can query different types of DNS records.**

**Section 1, Step 17 – Take a screenshot of the nslookup output indicating the refusal to access the transfer information**

*Paste screenshot of credentials from Section 1, Step 17 here*

A screenshot of a computer

Description automatically generated

**Questions**

1. How can the nslookup and dig commands be useful in the reconnaissance phase? The nslookup can be used to gather domain names to IP addresses along with querying specific DNS records. The dig command provides a more detailed output compared to nslookup, dig allows someone to gather more information about certain DNS records during the reconnaissance phase.
2. In this lab the DNS transfer record was disallowed to the Kali machine.
   1. Why is this good security practice? The record that was trying to be transferred was a axfr record. This record is intended to replicate DNS records, if this record was allowed to be transferred, an attacker could have access to all DNS records.
   2. How could the contents of those records have aided an attacker if they were successful in obtaining them (be specific) If the attacker were to successfully obtain the DNS records, the attacker would have access to IP addresses and could start targeting specific addresses with DDoS attacks.