Problem 1  It turns out that DNS names are case-insensitive: the IP address named by “www.google.com” is the same as the IP address named by “WWW.Google.Com” or “WWl.g00G1E.coM”. A recursive resolver can ask for a given name using any capitalization and the authoritative DNS server will answer the query. In addition, (almost) every authoritative DNS server will echo back the name in its response with the same capitalization as in the query.

1. Explain how LeEt raNdOM capiTaLiZAtiOn can be used to increase the resistance of DNS queries to Kaminsky-style DNS forgery attacks. Do all domain names benefit equally?

2. Does it matter if there are a few DNS servers that do not respect capitalization in DNS queries, always responding with the queried name in lowercase?

Problem 2  Why would someone want to register domain names such as a-azon.com, mic2osoft.com, fjcdn.net, or doubleslick.net? What would an attacker gain from owning such domains and having servers responding to requests made to them?

Hint: You may wish to refer to an ASCII table.

Problem 3  Yahoo has recently announced a plan to reclaim Yahoo e-mail accounts that have been inactive (in the sense of not seeing a login) for more than 12 months. The plan will free up e-mail handles that had been registered and abandoned long ago, and might allow new users joining Yahoo from the indignity of e-mail handles like “profshacham92093yolo@yahoo.com”.

Why is Yahoo’s inactive account reclamation plan a very bad idea from a security point of view?