Assignment 5: Password Attacks [40 points]

# Part 1: Sandbox Attack

There is an ssh service running on server.cs491. Note that because the ssh service has changed (again), you’ll first have to remove the existing host key using:

ssh-keygen -f /home/user/.ssh/known\_hosts -R server.cs491

Q1: The **toor** user on server.cs491 has a weak password. What is their password? [8 points]

sunshine

Q2: The **localuser** user on server.cs491 has a weak password, but doesn’t allow remote login. What is their password? How did you find it? *(hint: where are password hashes stored on Linux?)* [8 points]

soccer1

# Part 2: Hashing

Q1: For each password, provide the SHA-1 hash and an md5crypt hash (any salt will do) [8 points]

* secure\_password\_123
  + SHA-1: f13733f6dd9f1ed3118e2da31428c71eab5ffd99
  + md5crypt: $1$2wC.BHz9$bZOv0xoZknRgbWrcdtMP.1
* i\_love\_security
  + SHA-1: 1d0db231630082049d873d911bf498a47d56b606
  + md5crypt: $1$2wC.BHz9$QBwTJ7DOhgiwoh7BU5Ciy1

# Part 3: Password Cracking

**Note: all of the passwords in this section can be cracked using the rockyou wordlist combined with hashcat rulesets or hybrid attacks. You should not need a GPU or a custom wordlist. For all questions, provide the hashcat command you used.**

Q1: The following passwords were hashed using SHA-1. See if you can crack them. [4 points]

35f40b723e98c44633fa239cfce9b8051db26830

llcats

08fdcd9687d216e2d264f238139a5fbbc45928e2

hackerman1

ee65575f18987b05c07bdfa2ef5c3a2a1a6e93ca

hackerproof123

a491a2ec5967bbf4bf4741f4bfd0000aa089be85

secretcode

Q2: These passwords seem to be using leetspeak. Can you crack them anyway? [6 points]

80681d5ec9ef4475a28484bb48057ce3ca412f8d

b1gbra1n

05d1263ff1a06b2b6b10716b20a9f655111d3c84

rickastl3y

Q3: These passwords were previously found to be in rockyou, but company policy requires that users change their passwords every 6 months. Can get crack new passwords? [6 points]

73f17d9c859c4d372130c010e7151ddccda9b3be

Top\_secret1

b00efa4a3982da5a1e5cea9a5d4b497a2ba2b539

canthackme1