## **Part 1: Password Cracking**

Your team has broken into a server and stolen the /etc/password file! You can find the file for your team in the "Project 3 Shadow Files" folder ([here](https://canvas.colorado.edu/courses/24996/files/folder/Project%20Files/Project%203%20Shadow%20Files)). Using a program like John the Ripper, see how many of the passwords you can crack! Afterwords, answer the following questions:

1. Which passwords did you crack?

We cracked 3 passwords:

* U: john pw: happy123
* U: student pw: 54321
* U: guest pw: virgil

1. What methods did you use to crack passwords? How long did you run the cracking programs?

We used John the Ripper to try and crack these passwords, those three were cracked very quickly like within a minute or two and we ran the program for about 30 minutes without the other 5 getting cracked

1. How long did most of the passwords take to crack? What kinds of passwords were cracked faster than others?

All of the passwords we were able to crack contained only numbers and/or lowercase letters, no upper case letters or special characters/punctuation. The speed did not seem dependent on format since we cracked 2 that were from sha512crypt,crypt and one from sha512crypt,HMAC-SHA256,crypt

1. For any passwords you didn't crack - why do you think you couldn't? What might these passwords do that makes them harder to crack?

We think they use more types of weird symbols—like !@$%, use different salt with hash function.

## **Part 2: Password Sniffing and Telnet**

One day you follow a specific target into a coffee shop. You manage to sniff about three minutes of wireless traffic from their computer, which can be found here: [project3\_capture.pcapng](https://canvas.colorado.edu/courses/24996/files/2784425/download?verifier=g4DcSF9aLE5RspaMrusLNINpADJ17Tr4rMYzXBXC&wrap=1). By watching their screen from across the room, you can tell that they log on to FOUR different servers, each with a different protocol, but can't make out which ones. Analyze the packet capture using Wireshark, then answer the following questions:

1. For the target:
2. What is the target's IP address?

10.233.64.173

1. What operating system are they running?

Windows NT 10.0.

1. For all FOUR servers:  
   *(Note: due to encryption and different protocols, some of this information may not be available for every server)*
2. What is the server's IP address?

52.0.167.5

172.217.12.4

35.196.233.141

34.204.250.133

1. What protocol does the target use to communicate with that server?

TCP

1. What was the username/password that the target entered?

username=crash & password=D4-V1nc1

1. Does the server have a domain name? What is it? *(Hint: the service to look up domain names is called DNS)*

ec2-52-0-167-5.compute-1.amazonaws.com

1. How much information can you get on which operating system and what programs the server is running?

Os: Windows XP

We were not able to find the programs for the server.

1. Many services are hosted on the cloud, through programs like Google Cloud, Microsoft Azure, or Amazon Web Service. Is this server hosted through one of these platforms? If so, which one? If not, can you find out who owns it instead?

Amazon Web Services

1. For any information you couldn't find, why not?

We did have some trouble with finding the operating system, but we definitely believe it is Windows. We also had some difficulty finding the exact programs the OS was running. We didn’t know where to look for those.

1. Did you find anything else interesting?

There are multiple different IP address pointing to the same page: https://google.com