**Hashing – Crypto 101**

Before we start, we need to get some jargon out of the way.  
Read these and take in as much as you can. We'll expand on some of them later in the room.

This room will likely involve some research. Get good at using search engines, it's crucial to infosec.

***Answer the questions below***

***Task 1:*** *Read the words and understand the meanings!  
Is base64 encryption or encoding?*

***Answer: encoding***

**Task 2:**

What's a hash function?

Hash functions are quite different from encryption. There is no key, and it’s meant to be impossible (or very very difficult) to go from the output back to the input.

***Answer the questions below***

*1# What is the output size in bytes of the MD5 hash function?*

*Answer: 16*

***2#*** *Can you avoid hash collisions? (Yea/Nay)*

*Answer: Nay*

*3# If you have an 8-bit hash output, how many possible hashes are there?*

*Answer: 256*

**Task 3:**

**Uses for Hashing**

## What can we do with hashing?

## Hashing is used for 2 main purposes in Cyber Security. To verify integrity of data (More on that later), or for verifying passwords.

***Answer the questions below***

*1# Crack the hash "d0199f51d2728db6011945145a1b607a" using the rainbow table manually.*

*Correct Answer: basketball*

*2# Crack the hash "5b31f93c09ad1d065c0491b764d04933" using online tools*

*Correct Answer: tryhackme*

*3#Should you encrypt passwords? Yea/Nay*

*Correct Answer: Nay*

**Task 4: Recognizing Password hashes.**

Automated hash recognition tools such as <https://pypi.org/project/hashID/> exist, but they are unreliable for many formats. For hashes that have a prefix, the tools are reliable. Use a healthy combination of context and tools.  If you found the hash in a web application database, it's more likely to be md5 than NTLM. Automated hash recognition tools often get these hash types mixed up, which highlights the importance of learning yourself.

***Answer the questions below***

*1# How many rounds does sha512crypt ($6$) use by default?*

*Correct Answer: 5000*

*2# What's the hashcat example hash (from the website) for Citrix Netscaler hashes?*

*Correct Answer: 1765058016a22f1b4e076dccd1c3df4e8e5c0839ccded98ea*

*3# How long is a Windows NTLM hash, in characters?*

*Answer: 32*

**Task 5: Password cracking:**

***Answer the questions below***

*1# Crack this hash: $2a$06$7yoU3Ng8dHTXphAg913cyO6Bjs3K5lBnwq5FJyA6d01pMSrddr1ZG*

*Correct Answer: 85208520*

Method:

Command : hashcat -m 3200 -a 0 -o cracked.txt bycrypt.txt /usr/share/wordlists/rockyou.txt

Cracked.txt – output will be saved.

Bycrypt.txt – hash value will be stored here.

*2#Crack this hash: 9eb7ee7f551d2f0ac684981bd1f1e2fa4a37590199636753efe614d4db30e8e1*

*Correct Answer: halloween*

*3#Crack this hash: $6$GQXVvW4EuM$ehD6jWiMsfNorxy5SINsgdlxmAEl3.yif0/c3NqzGLa0P.S7KRDYjycw5bnYkF5ZtB8wQy8KnskuWQS3Yr1wQ0*

*Correct Answer: spaceman*

*4# Bored of this yet? Crack this hash: b6b0d451bbf6fed658659a9e7e5598fe*

*Answer: funforyou*

Task 6:

**Task 6 — Hashing for integrity checking**

*1#What’s the SHA1 sum for the amd64 Kali 2019.4 ISO?*[*http://old.kali.org/kali-images/kali-2019.4/*](http://old.kali.org/kali-images/kali-2019.4/)

***Answer: 186c5227e24ceb60deb711f1bdc34ad9f4718ff9***

*This can be found by simply clicking the link and going to the SHA1SUMS link.*

*2.#What’s the hashcat mode number for HMAC-SHA512 (key = $pass)?*

***Answer: 1750***

*This can be found through the terminal using hashcat -h | grep -i 'hmac-sha512 (key = $pass) or*[*here*](https://hashcat.net/wiki/doku.php?id=example_hashes)*.*