L1: Network Security: The Attacks P1

This is a lesson for Year 10 students aimed at covering Network Security Attacks. This lesson aims to cover the main topics from 1.4.1 from the OCR specification.
https://www.ocr.org.uk/Images/558027-specification-gcse-computer-science-j277.pdf

Aims:
- Give students an idea of the types of Network Attacks including Malware, Social Engineering, Brute-Force Attacks, The concept of SQL Injection.

Time	Activity	How will learners be assessed?
9:45	**What is Network Security?** Students write every word they can think of to do with Network Security on a word cloud.	
9:50	**Malware, Viruses, Worms, Trojan Horses** - Teacher will give a short presentation covering Malware, Viruses, Worms, Trojan Horses - Students will then complete a matching up activity	They will have to write the main features of each Then have to apply that knowledge to work out from scenarios what they are.
10:00	**Social Engineering & Phishing** - Teacher will give a short presentation on Social Engineering - Students will then be given an email and have to highlight the common signs of social engineering. As an extension they can create their own in the same style.	To create the email they would have to know the common signs of phishing emails
10:10	**Brute Force** - Teacher will give a short presentation on Brute Force. - Students will try and think of lots of common passwords and use word cloud on menti.com	Students will have to think of common passwords that would be susceptible to Brute Force Attacks. Later we will try and use Brute Force to break into the
10:15	**DoS & DDoS** - Teacher will deliver a presentation explaining DDoS & Data Interception - Then using the heroku website we will simulate a DoS attack with the whole class with a countdown. The teacher can at the same moment simulate the attack by pressing the DoS button on the Website Controller. This will appear to students as if we've done a DoS attack giving them some real experience.	
10:25	**Brute Force Exercise** - Students will break into 3 different accounts following hints given to them.	
10:28	**END Lesson** Survey: Students should complete a google form on the lesson. Homework: Students will be given a set of questions and research to do on Actions of Malware.	This will be checked next lesson through a Kahoot based quiz at the start of the lesson to gauge understanding.

L2: Network Security: More Attacks and The Defences

This is a Year 10 students aimed at finishing off Network Threads and covering network defences. This lesson aims to cover the main topics from 1.4.2 from the OCR specification.

Aims:

-

Time	Activity	How will learners be assessed?
9:45	**Intro Kahoot** - Will contains a variety of questions covering the topics from the previous lesson	
9:55	**User Access Levels & Passwords** - Teacher will give a short presentation covering the main topics.	
10:05	**DoS & DDoS** - Teacher will deliver a presentation explaining DDoS & Data Interception - Students will then have 5mins to research a recent DoS attack and then we will feedback to the group and everyone explain one that they found.	
10:20	**Encryption + Caesar Cipher** - Teacher will deliver a short presentation on Encryption and Caesar Ciphers.	
10:30	**END LESSON** For Homework students will have to translate Ceasar Ciphers	

Resources Needed:

-

L3: Network Security: Physical Security & Penetration Testing

IN PROGRESS

This will depend a little but over this weekend I will build more of the website shown earlier and the idea is that I'll give them lots of bugs and issues and they will try and solve them all.