TOPIC: Cyber Security Threats: Penetration Testing

LEARNING OBJECTIVES:

- What is penetration testing?
- Advantages of penetration testing
- Disadvantages of penetration testing

	Teacher Activity	Pupil Activity
Starter activity (5-10 mins) [individual/paired or group]	***Explain what penetration testing is and what it is used for*** ***What is it?*** *A Penetration Test is an attack on a system that looks for security weaknesses and potentially gain access. This could be anything from physically entering a secure location or infiltrating a computer system.* ***White Box** – Background information and system information is provided before the attack on a computer system has begun* ***Black Box** – Only basic or no information except the company name is provided about the system that is to be tested.* ***Who uses it?*** *Many big companies use penetration testing as a way of securing their systems and physical security to the highest it can be. Companies either have a penetration team themselves or hire in third party companies to carry out the testing for their company. There is no doubt that penetration tests are very important where information security is paramount.*	Discuss (individual/paired or group) What is penetration testing? Who uses penetration testing?

Main activity one (15 mins)	***Advantages:*** • *Penetration testing identifies potential flaws in company's security, on a physical and cyber level. This therefore then enables the company to improve these areas and harden their security.* • *Compliance with industry standards - all organisations must conduct regular penetration tests and reviews on all their systems.* • *Guards reputation of the company by ensuring the flaws aren't found by malicious hackers and instead found by qualified, safe, penetration testers.* • *Reduces the amount of attacks to the company in the future.*	Discuss (individual/paired or group) What are the advantages?
Plenary one (5-10 mins)	*Assess learning against the learning objectives* *This is an open activity whereby the teacher will decide on the best approach to do this based on the pedagogical approach your school takes on assessment.*	**For example:** • 5 minute timed writing exercise on what has been learned so far • Fill in class notes • Have a discussion • Answer open questions • Answer directed questions
Main activity two (15 mins)	***Disadvantages*** • *Could upset the cyber defence team of the business as they will not have been informed if it is a red teaming penetration test* • *If the pen testing team aren't careful or don't know the importance of the data/systems they are attacking, they could do some serious damage.* • *If it is an untrustworthy tester, there is the potential to let someone in your system who will steal sensitive data or take advantage of vulnerabilities they find.* • *If the penetration testing is regularly scheduled this could lead to the defence team becoming complacent, as in a real attack situation, the defence team would not be told a time to be prepared for.*	Discuss (individual/paired or group) What are the disadvantages?

Plenary two (5-10 mins)	*Assess learning against the learning objectives* *This is an open activity whereby the teacher will decide on the best approach to do this based on the pedagogical approach your school takes on assessment.*	**For example:** • 5 minute timed writing exercise on what has been learned so far • Fill in class notes • Have a discussion • Answer open questions • Answer directed questions
Homework (optional)	*Teacher choice based on homework policy of school.*	• Understand the differences between white and black box penetration testing • Understand the advantages and disadvantages of using penetration testing for big companies.

Key Terms:	
Penetration Testing	A Penetration Test is an attack on a system that looks for security weaknesses and potentially gain access. This could be anything from physically entering a secure location or infiltrating a computer system. White Box – Background information and system information is provided before the attack on a computer system has begun Black Box – Only basic or no information except the company name is provided about the system that is to be tested. **Who uses it?** Many big companies use penetration testing as a way of securing their systems and physical security to the highest it can be. Companies either have a penetration team themselves or hire in third party companies to carry out the testing for their company. There is no doubt that penetration tests are very important where information security is paramount.