Computing

Lesson 6: Where is the Danger?

KS4 Security

Ben Garside

[1] *Materials from the Teach Computing Curriculum created by the National Centre for Computing Education*

Task 1 - Meet a real hacker

Watch the video and answer the questions below:

What is a hacker?	
What does the word ‘ethical’ mean?	
What does an ethical hacker do for a company?	
What is another name for an ethical hacker?	

Task 2 - Penetration tester methods

What do you think a penetration tester does in each of these phases? Reorder the column on the right hand side to match the title with the description:

1. Planning phase

2. Discovery phase

3. Attack phase

4. Reporting phase

A. Finds exploits for various vulnerabilities

B. Describes the risks of vulnerabilities and their impact on business, with solutions

C. Examines existing security policy standards

D. Collects information and data on the system; scans the available ports to check for vulnerabilities

Task 3 – Rufus Rants

Design a penetration test for The Rufus Rants Company. Think about its security infrastructure and where the potential vulnerabilities might be. You are acting as a penetration tester who is exposing the company's vulnerabilities in order to address them.

The next three slides show some potential tests you could do. Pick one type of test from **physical security**, **software security** and **social engineering**.

Type of test	**Action taken to test the company's defences**	**What company should do to prevent future successful attacks**
Physical security		
Tailgating	Tailgate a member of staff to gain physical access to the offices and network room servers	Train staff not to hold doors open for colleagues or guests
Shoulder surfing	Shoulder surf another member of staff to learn their username and password	Train staff to be conscious of this possibility and shield their password entry; ensure strong passwords are used and changed regularly

Task 3 – Rufus Rants

Software attacks		
Denial of service attack (DoS) on Rufus Rants website	Launch a DoS attack registering thousands of status updates to existing users	Rate-limit users so that attackers cannot automatically set up thousands of updates from the same accounts
SQL injection attack on Rufus Rants website	Instead of submitting a username and password, submit two strings that trick the database into giving up all its information	Review design of the databases within Rufus Rants; design the queries that request data from the database so that the input to the form does not get added directly to the query, i.e. input sanitisation

Task 3 – Rufus Rants

Social engineering attacks		
Quid pro quo	Call an employee telling them that they have just downloaded a virus, which can be fixed if they provide login details for the ‘IT professional’ to access their account remotely	Train staff to check any such requests with their managers and not to give their login details to anyone
Spear phishing/Trojan	Observe and take details of personal data on staff social media accounts, then use this data to email a particular staff, posing as a friend to persuade them to open a Trojan attachment that has the potential to delete the company’s financial systems	Train staff not to open unsolicited mail; update virus protection software to identify any virus entering the network via the email system
Baiting	Leave a number of USB sticks in strategic places around the company, labelled ‘Rufus Rants employee bonus scheme’	Disabled USB drives on individual PCs; allow only IT staff to open and scan USB contents

Task 3 – Rufus Rants

Complete the table below with your chosen methods

	Type of test	Action taken to test the company's defences
Physical security		
Software attacks		
Social engineering attacks		

Task 4 – Pen test report part 1

Now you know more about the Rufus Rants Company. Write a report outlining how you think your pen tests would have been successful or unsuccessful and then recommend extra security they could put in place.

How was your pen test successful?

	Successful? (Yes/No)	**If Yes, describe how it was successful, what data/system were exposed, what damage could have been done.**
Physical security		
Software attacks		
Social engineering attacks		

Task 4 – Pen test report part 2

What new security measures would you recommend that The Rufus Company puts in place to help protect them in the future from other forms of cyberattacks.