Penetration test plan activity

Step 1: Design your data company

Instructions: Using the following exemplar, create a company that will undergo a penetration test. Describe its infrastructure and premises, as well as considering what kind of data the company is likely to store and who can access it.

Company name: Rufus Rants (RR)

Type of company: Social media company for angry people

Number of employees: 150

CEO: Sophia Samuels

Physical building security: Swipe card access for staff; visitors sign in with a receptionist; the company has its own central server room

Training provided to staff: No specific security training provided.

Data: Rufus Rants connects angry people from around the world and keeps data on all its users. Data includes profile names, demographic data of users, user photos, user blog posts, contact lists, and forum discussions. The data includes activity data such as login times and places for all users. The company also has advertisers who promote relevant products to its angry users, such as camomile tea and boxercise classes. The company keeps financial data about its advertisers on file, as they charge the advertisers for space on their site. The company also keeps financial data about the users, as they buy Rufus Rants merchandise through the online platform, including T-shirts and branded stress-relief toys.

Data storage: Currently, some staff have permanent desks with PCs, while others share desks using laptops, which they also take home and to the offices of their advertising clients. Users are allowed to plug devices into the USB ports. The company currently has a central server on-site, which also houses most business-critical company files, such as the website, human resources information, and financial information. Staff email is cloud-stored, though Gmail.

Software security: The company has firewalls and uses antivirus software. The IT department installs patches in a haphazard way and the directors are unaware of the need to plan properly to manage upcoming threats.

Step 1: Further instructions

When you design your company, remember that you are designing it to be penetration-tested, so don't try to design an extremely secure company. You can choose what kind of company to design and what type of data they hold, but include one A, one B, and one C from the following security options:

Physical security of the building
A: None: everyone wanders in and out
B: Swipe card access
C: Biometric scanning for all external and internal doors

Training provided
A: None
B: Some security training for new staff, e.g. staff advised not to share passwords
C: Staff attend monthly training updates about social engineering and general security

Data storage
A: Data is kept on a central server on the premises, USB sticks are permitted, laptops are used
B: All data is cloud-stored in a secure location
C: All databases are designed to prevent SQL attacks and the website is already equipped with the latest denial of service prevention measures, e.g. limiting the number of requests a user can make/send.

Software security
A: Company directors are nervous about IT and reluctant to invest in it; some regularly used software is pirated and staff share passwords
B: The IT department ensures that the basics of antivirus and firewall are present and patches are applied when exploits are known
C: The IT department is very well informed, software is patched, antivirus and firewall are present, and passwords are changed at regular intervals; the IT department and directors meet regularly to report on research about current threats.

Step 2: Swap with another group and design a penetration test for their company

Instructions: Using the following exemplar, design a penetration test for another group's company. Think about their security infrastructure and where the potential vulnerabilities are likely to be. You are acting as a group of white hat hackers who are exposing the company's vulnerabilities in order to address them. Include recommendations that could prevent successful attacks in the future.

The exemplar is not an exhaustive list of possible attacks.

Company name: Rufus Rants (RR)

Type of company: Social media company for angry people

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
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
Social engineering attacks		
Quid pro quo	Call an employee telling them that they have just downloaded a virus, which can be fixed if	Train staff to check any such requests with their

	they provide login details for the 'IT professional' to access their account remotely	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