Fullstack Academy

Career Preparation Feedback Form

Unit 6: Red Team

Student: Insert name here

Vulnerabilities Assessment

Interviewer

Question	Best Answer
What is the difference between Red Teaming and Pen Testing?	Red teaming is like a simulation of a real attacker trying to achieve certain objectives, like gaining access to sensitive data without being detected. It can include social engineering and lateral movement over a longer period of time. Pen testing is when we focus on testing specific systems or applications for known vulnerabilities in a defined scope. It's like a snapshot in time, you test, you report, and you help fix what you find.
What are some tools you can use for passive reconnaissance? Active reconnaissance?	Passive reconnaissance is when you gather information about a target without direct contact. Tools used for passive reconnaissance are google dorking, the whois command, or sites like shodan to learn about the target's infrastructure. Active reconnaissance means actively sending traffic to the target. I'v practiced using tools like nmap for port scanning, netcat to probe services, and metasploit to expose vulnerabilities. These are used to find open ports, services, and potential entry points.
What is more dangerous, LFI or RFI?	From what I'v learned both are dangerous, but RFI, remote file inclusion is usually more severe. With LFI, local file inclusion, an attacker can read files on the server, like /etc/passwd or config files. That's bad because it exposes credentials or system details. But with RFI, the attacker can load and execute malicious code from a remote server. So instead of just reading files, they can upload web shells or run remote code, which can lead to full system compromise.

Question	Best Answer
You are running a pen test on a company, what are the different phases you would undergo to perform penetration assessments?	From my bootcamp, we learned that a penetration test usually follows a structured set of phases to stay organized and ethical. The phases I would undergo would be: Planning and scoping, Reconnaissance, Exploitation, Post-explotation, and Reporting. -Planning = Make sure I have permission, defining scope and rules of engagement -Reconnaissance = Passive or active to gather info by using OSINT, whois, nmap scans -Explotation = using what I find in my recon work to gain unauthorized access -Post-explotation = where I can see what I can do with my gained access, like pivoting to other systems or exfiltrating data. -Reporting = Documenting everything, showing evidence of findings and giving recommendations on how to fix issues.
Walk us up the Cyber Kill Chain.	Sure the cyber kill chain breaks down how an attacker typically progresses through an attack. First we do Recon (gather info) then we Weaponize (attacker builds a payload like malware or exploit) then Delivery (sending the payload though malicious link or phishing email) then Exploitation (when the payload is triggered) then Installation (attacker installs malware or backdoor) then Command and Control (attacker setups up communications to control and compromise remotely) then Actions on Objectives (which is when they do what they came for like stealing data, escalating privileges or moving laterally)

Writing

Question	Best Answer
What are some of the most important things to keep in mind when drafting a pentesting report?	A good pentest report should be clear, accurate, and useful to technical and non-technical audiences. First, it should include enough detail so someone else can understand how you found each issue, including evidence like screenshots, steps to reproduce, and the impact. Next, write professionally, no blaming or shaming, should help the organization improve, not embarrass them.

Question	Best Answer
What are the typical sections in a pentest report?	Cover page = Client name, project name, date, and version number. Executive Summary = High-level overview for non-technical stakeholders. Overall risk posture, most critical findings, general recommendations. Scope and Objective = What was tested, what was out of scope, and the goals of the engagement. Methodology = How the test was performed. Phases like reconnaissance, scanning, exploitation, post-exploitation, and reporting. Detailed Findings / Vulnerabilities = For each finding: Title of vulnerability, Description, Evidence (screenshots, output, logs), Impact, Risk rating (severity level), Steps to reproduce, Recommended remediation steps Conclusion = Summary of the overall security posture. Lessons learned, high-level next steps. Appendices = Raw tool output (like **`nmap`** scans), test credentials, command logs, or any extra technical details.