Ethical Hacking Project Management Plan

Ethical Hacking F/618/5213
AC 3.1: Develop an ethical hacking plan to identify and test weaknesses.

Project Management (Networking and Cybersecurity) T/650/5009
AC 2.1: Produce a project specification for a networking and cybersecurity project in line with requirements

Learner Name	O. Folarin	**Tutor Name**	Shamim Khan

Scenario

"Pentest Ground" *are a security services company based in New York and have employed you as their Ethical Hacker. They require you to intentionally probe their website to identify vulnerabilities before malicious hackers can exploit them, so they can then implement countermeasures to enhance the security posture of their website and systems.*

Pentest Ground have given you authorisation to scan their URL https://pentest-ground.com:81/, has provided you with a £5000 budget and a time constraint of 3 days to conduct actions/attacks for physical, logical, and social exploits and report findings, vulnerabilities, potential risks, and the system's impact, along with recommendations for improving security policies and procedures.

Task
Based on the scenario provided, complete the fields below ensuring you are clear and concise with your answers to ensure your Ethical Hacking Project Plan is legible for your tutor to assess and IQA to review.

Project Title i.e. what is the title of your networking and cybersecurity project? Be descriptive so all stakeholders understand your goal. ***(PM AC 2.1)***

Pentest Ground Website and Network Vulnerability Checks
(detect, fix, and avert)

Project Context i.e. what is the purpose of your networking and cybersecurity project? What is the driver and benefit of it? ***(PM AC 2.1)***

The purpose of this project is to perform a thorough assessment of the Pentest Ground website and network. Identify any vulnerabilities before cyber criminals take advantage. After which, strong measures will be put in place to protect the Pentest Ground website, network, and improve its overall security.

Project Organising i.e. who are the key stakeholders for the networking and cybersecurity project, both internally and externally? Who are the networking and cybersecurity team? ***(PM AC 2.1)***

Pentest Ground - Funding
Oluwaseun Folarin - Ethical Hacker
IT Staffs: Provide periodic trainings to employees of other departments in the organization

Project Budget i.e. what expenses do you need to account for? What is the budget allocated to your networking and cybersecurity project? ***(PM AC 2.1)***

Budget - Initial £5,000 stretched to £10,000
Staffing cost
Software applications
Staff training equipment
Potential unplanned costs

Ethical Hacking Project Management Plan

Identification of system(s) to be tested i.e. a computer systems, networks, software applications etc. ***(EH AC 3.1)***

I will be testing for vulnerabilities on the Pentest Ground website and network. As an Ethical hacker for the organization, I have been granted access to perform ethical hacking on the Pentest Ground website and network to identify any vulnerabilities before cybercriminals detect and exploit them.

Project Parameters i.e. what are the constrains, risks and issues with the networking and cybersecurity project? Risks involved i.e. data breaches, data integrity, confidentiality, financial loss, reputational damage etc. ***(PM AC 2.1 and EH AC 3.1)***

Possible request for more funding after initial £5,000
Organization's reputation may be damaged
Organization could lose integrity
Unauthorized activities that could disrupt network performance
Unauthorized access that could cause the organization huge monetary and data loss
Unauthorized access to data that could lead to misinformation

Project Planning i.e. what is the timescale to complete your networking and cybersecurity project? When is the deadline? When are the key milestones reviewed? Timeline i.e. duration of testing and deadline. ***(PM AC 2.1 and EH AC 3.1)***

The testing is scheduled for 3 days starting from 17/04/2025 to 19/04/2025

Day 1
Gather information about the targeted website and network, scan to identify vulnerabilities and potential risks to the website and network. With authorization, gain access to the website and network and carry out ethical hacking activities. Maintain access and delete any digital footprints to avoid cybercriminals using it as a backdoor.

Day 2
Fix any outstanding issues that could make the website and network vulnerable. Set new security measures and test them against cybercriminal attacks to validate how it performs. Amend current or set new security policies regarding network and website usage.

Day 3
Make a report of all the activities that took place on Day 1 and 2 and arrange periodic trainings to other staffs of the organization

Actions/attacks to be undertaken for physical, logical and social exploits (consider Website Vulnerability Scanner, Network Vulnerability Scanner, Virtual Hosts Finder and SSL/TLS Scanner available in Pentest Tools.com) ***(EH AC 3.1)***

Action/attack 1	A network vulnerability attack will take place to identify any unwanted access or unusual activities within the systems network.
Action/attack 2	A website vulnerability attack will take place by scanning the website to identify weaknesses and areas of improvement on the website.
Action/attack 3	A port scanning action will take place to identify any open port available that can be used as a backdoor by cybercriminals to launch attacks.

Ethical Hacking Project Management Plan

Project Objective i.e. what are the expected results at the end of your networking and cybersecurity project? Deliverables i.e. report detailing the findings, vulnerabilities, potential risks, impact on the system along with recommendations for enhance security policies, procedures, and awareness programs for ongoing improvement etc. ***(PM AC 2.1 and EH AC 3.1)***

The expected result is to ensure Pentest Ground website and networks are fully secured, functional while maintaining its effectiveness and high performances.

Network Vulnerability Scan
Network performances may be slow due to unauthorized frequencies within the network. Their network will be vulnerable as a result of this.

Recommendation
A thorough analysis of the unauthorized frequency within the network and an upgrade to the affected software to flush out potential threats and risks.

Website Vulnerability Scan
There maybe potential site redirection issues where the site redirect to a different url but maintain the expected web page e.g. On Pentest Ground website (https://pentest-ground.com:81/), after clicking login, i would expect (https://pentest-ground.com:81/login) but in case of redirect issues, the url may be something like (https://pentest-ground.com:81/log or https://pentest-ground.com:81/index).

Recommendation
Scan through the website to identify any vulnerabilities. Also, verify each source code line to ensure there are no redirect issues.

Port Vulnerability Scan
Open ports may be discovered during or after scanning

Recommendation
Identify, analyze, and close these ports so they are not used as backdoors for cybercriminals.