7.2.2 Vulnerability Management Life Cycle Facts

Every business has sensitive information that, if accessed by hackers, could be used in ways that could put the company and its employees at risk. Even a non-malicious user, such as an untrained employee, could cause problems if proper security isn't in place. Unless a business physically unplugs its computers and never uses a network at all, the company can be a target. Therefore, vulnerability management should be implemented in every organization to identify, evaluate, and control risks and vulnerabilities.

This lesson covers the topic of the vulnerability management lifecycle.

Vulnerability Management Lifecycle

The following table identifies the vulnerability management lifecycle an ethical hacker uses to protect an organization.

Phase	Description
Baseline creation	The lifecycle starts by defining the effectiveness of the current security policies and procedures. You should establish any risks that may be associated with the enforcement of current security procedures and what may have been overlooked. Try to see what the organization looks like from an outsider's perspective, as well as from an insider's point of view. No organization is immune to security gaps. Work with management to set goals with start dates and end dates. Determine which systems to begin with, set up testing standards, get approval in writing, and keep management informed as you go. For your own protection, it is important to make sure that everything you do is aboveboard. Fully disclose to management what you are doing, how you will do it, and the timing for each phase of the project. This protects you and reassures the organization's management of your integrity and professionalism. It is also crucial to know the goals of the organization so that you are able to address specific concerns. This will also help you to know where to begin and what is expected of you.
Vulnerability assessment	The vulnerability phase refers to identifying vulnerabilities in the organization's infrastructure, including the operating system, web applications, and web server. This is the phase where penetration testing begins. It is important to decide the best times to test. You don't want to risk having systems shut down during peak business hours or other sensitive times. You must also choose the best security assessment tools for the systems you choose to test. Be sure that you understand what each option of every tool can do before you use it. This helps you avoid damaging the systems. Everything you do as an ethical hacker depends on your ability to perform effective penetration testing. You must conduct the correct tests with the correct tools to be able to accurately assess the security vulnerabilities. All remaining phases depend on the effectiveness of this vulnerability assessment phase.
Risk assessment	In this phase, you organize the results of your vulnerability testing according to risk level and then categorize by levels of sensitivity and access. You will need to create and present reports that clearly identify the problem areas, then produce a plan of action to address weaknesses, protect the information, and harden the systems. At this phase, it is critical to communicate with management about your findings and your recommendations for locking down the systems and patching problems. You will be protected and valued as you communicate and receive written approval for implementing the suggested remediation.
Remediation	Remediation refers to the steps that are taken regarding vulnerabilities, such as evaluating vulnerabilities, locating risks, and designing responses for the vulnerabilities. In this phase, you implement the controls and protections from your plan of action. Begin with the highest-impact and highest-likelihood security problems, then work through the lower-impact and lower-likelihood issues. It makes the most sense to protect the organization from its most vulnerable areas first and then work to the less likely and less impactful areas. It may be impossible to identify and fix every single vulnerability that exists in an organization. That is why it is essential to start with the most urgent issues based on what makes the most business sense, what management expects from you, and compliance with regulations.
Verification	The verification phase helps the security analyst verify whether all the previous phases have been effectively executed. In this phase, you retest the systems for verification. Even though you may be certain that you have corrected vulnerability issues and are confident in your work, it benefits you to prove your work to management and have verifiable evidence to show that your patching and hardening implementations have been effective. You will increase the value of your services when you can show the validity of your work.
Monitoring	After you have verified your work, move on to the post-assessment phase, which is also known as the recommendation phase. At this point, recommend ongoing monitoring and routine penetration testing to be proactive in protecting the organization and its customers or clients.

It may be tempting for an organization to feel secure after going through the process of penetration testing, implementing changes, and hardening the system. However, it's important for you to help management understand that hackers have time on their side and there will always be ongoing and new threats to security. Therefore, it is critical that the organization has monitoring tools in place and regularly schedules vulnerability maintenance testing.