Andrew Plum

Mr. Alves-Foss

Cyb 110

12/12/21

Ch. 14 Homework

1) You can actively or passively detect new hosts in your environment. Actively discovering new hosts on the network is similar to the process used to map the network in which you go IP to IP to interrogate each to see if you get a response. Because this method is similar to mapping the network, it experiences many of the same limitations. Passively discovering new hosts on the network is often means placing a device at choke points on the network, like switches or routers, which eavesdrop traffic flowing through the network infrastructure. This way when traffic to or from new devices is detected, they can automatically be added to the lists of hosts on the network to scan.

4) Vulnerability assessments are different from penetration testing. A vulnerability assessment is a process which uses a tool that is specifically designed to scan for vulnerabilities. Penetration testing, also known as ethical hacking or pentesting, is the process of testing a system for vulnerabilities an attacker could exploit. Simply when you are conducting a vulnerability assessment, you are trying to find possible vulnerabilities in the system. Penetration testing takes it one step further in that it is checking to see which of a list of possible vulnerabilities could actually be exploited by an attacker.

5) Red and blue teams are terms of military origin. The red and blue team are opposed to each other. The red team plays the part of the attacker during the penetration testing and evaluates the security of the systems as realistically as possible while keeping the test reasonable and safe. The blue team is tasked with defending the organization and catching the red team during the penetration testing. The blue team should participate just as much during the penetration testing on the other side as the red team is attacking. Sometimes there is even also a purple team which usually exists to help both sides and act as though it is both on the red and blue team at the same time.

7) Static analysis involves directly analyzing the application source code and resources. This means looking through the code looking for errors in logic and vulnerabilities that exist due to certain lines of code or various libraries used. Static analysis usually requires a strong development background and understanding of the languages used. Dynamic analysis involves testing the application while it’s in operation. Although dynamic analysis doesn’t give the same insight into the code as static analysis does, this type of analysis more closely resembles real attacks against the application.

8) Bug bounty programs serve as a kind of penetration testing. Bug bounty programs essentially follow the same rules and process as a regular penetration test. The only difference is that there is a monetary award open to anyone who finds vulnerabilities in their resources. So, in bug bounty programs, there are bounty hunters not hired by the organization who only claim a monetary award if they find any vulnerabilities whereas in traditional penetration testing, a person or a team is hired by the organization to test vulnerabilities. In bug bounty programs, the organization is typically careful to define what scopes of issues reported they will pay out bounties for. The size of these monetary incentives usually varies based on the severity of the issue discovered.

9) The environment on which you test has a significant impact on the results of your test. For example, if you test on a test environment you set up, you want to make sure that the test environment is identical to the production environment as much as possible. You want to avoid having the testing environment from being idealized, thoroughly patched, and well secured unless the production environment is also those things. This way you make sure the test results of the test environment resemble as closely as possible to the what the test results would be if the test occurred in the production environment. It is also important to note that the attack surface of the environment impacts your test results. For example, it is much more difficult to conduct a successful attack if you are conducting it through a hosted cloud system than if you had physical access.

10) Alert fatigue is what may occur as a result of sending too many alerts. If you send too many alerts, especially if they're false alarms, eventually your blue team will start to ignore the alerts entirely. To avoid the blue team from experiencing alert fatigue, send alerts which prompt a specific response and send as few alerts as possible. Alert fatigue is actually a common phrase borrowed from the healthcare industry.