20 Dec 2022 |Dexter McGriff - President & CEO

What Is Red Teaming In Cybersecurity?

Being proactive with vulnerability detection is necessary for compliance and data protection. Without penetration testing, any government agency with public-facing applications could unknowingly host software vulnerabilities waiting for an attacker to exploit them. You need to find these vulnerabilities before attackers find them. Red teaming is a component in effective penetration testing to find unknown vulnerabilities so that developers can patch their applications. A red team will help you identify, define, and remediate vulnerabilities to keep your data safe. **Red Teaming vs. Automated Cybersecurity Scanning** You can install several automated tools in your development environment to find vulnerabilities, but scripted scans do not cover all exploit potential. Scripts probe applications for common vulnerabilities, and they emulate the ways an attacker will perform a simple scan prior to exploiting software. Scans on your software tell an attacker if the application has potential vulnerabilities, and some scripts will automatically exploit the issue, making the process of a compromise happen within a few seconds. Scans also give attackers information about the network environment so that they can perform future exploits. For example, a simple scan on the application server might give an attacker information about the operating system and hosting application if the server returns this data. Penetration testers recommend that organizations hide environment information from server responses, but many administrators still leave this information publicly available without knowing its consequences. The human factor is the primary difference between red teaming and software that automatically scans government applications. Automation in cybersecurity is common and speeds up application deployment because it alerts administrators to potential issues before code goes to production. Scripts only catch what they are programmed to catch, which is the main disadvantage of using automated scanning only. They only find common and well-known vulnerabilities and cannot detect complex issues from poorly coded business logic. **What Does a Red Team Do?** The human factor is what makes red teaming an advanced cybersecurity tool for government agencies. A red team is a group of hackers, usually called whitehat hackers. They might have a history of working in cybersecurity or do cybersecurity research as a hobby. It's important that a red team is a group of people with experience finding vulnerabilities, or your agency could have a poor experience. You need the red team to find as many vulnerabilities as possible, or your application could still maintain unknown issues leaving you open to a potential compromise. A red team of hackers can perform a white box or black box assessment. A white box assessment is more like a code review. A reviewer looks through the code and finds vulnerabilities based on code structure. A black box assessment is similar to how a hacker would compromise your system. The red team in black box testing has no knowledge of code or configurations and must find vulnerabilities based on simple access to a staging environment. You can also get a gray box assessment where the red team reviews your code and performs penetration testing on the network and application environments. You are responsible for setting up the staging environment, but the red team might help you with the basics. After the staging environment is set up, the work begins. The red team emulates every step in a typical attack. They will perform reconnaissance, especially if part of the penetration test is assessing corporate phishing defenses. Even though scanning tools aren't fully

effective, a red team will have their own scripts to find basic vulnerabilities. The team will take an additional step for application penetration testing and exploit vulnerabilities. Finding misconfigurations is also a component in penetration testing, so the red team will identify any vulnerable configurations if it's a part of the scope. If the red team finds any plaintext passwords, they will use them to gain unauthorized access to the system. Any vulnerabilities will be exploited, so this is why penetration testing is done in a staging environment. If phishing exercises are a part of the project scope, the red team will make phone calls to employees and send malicious email messages. The email messages usually contain a link to a web server; every click is recorded along with the user account who clicked the link. If the user enters credentials, the red team takes note of which users were successfully phished. The red team will use phone calls to identify any employees who are vulnerable to divulging their credentials or sensitive information over the phone. The red team might test for any physical vulnerabilities for an on-site assessment. A red team member might try to gain physical access to a location using a method called tailgating. Tailgating happens when employees let others follow them into the building using the employee's badge. It gives an attacker physical access to the premises and can lead to data theft or the installation of malicious software. **What Happens After the Penetration Test Is Finished?** Usually, penetration testers work on a list of vulnerabilities and know what to look for because they are professionals with experience. Every vulnerability is categorized to make assessing risks and prioritizing issues easier. When penetration testing is completed, the next step is to write up a report with all issues. A penetration testing report is a list of issues with an explanation of the vulnerabilities found and a proof of concept that displays how the red team found the issues. A risk level is given to the issue so that you can prioritize each issue. For every issue the assessment team finds, a description, proof of concept, and remediation suggestions are given to help administrators and developers determine what must be done to fix issues. **Conclusion** Automated scans are useful for cybersecurity but aren't as useful as having a red team run penetration tests on your environment. Red teaming is a great way to find vulnerabilities in your applications. For large enterprises, red teaming is an effective way to find vulnerabilities that an attacker could use to obtain massive amounts of sensitive data.