LogicFinder
Consulting, Development and Training

Identifying Vulnerabilities with Network Penetration Testing

Introduction:

Penetration testing is an authorized simulated attack performed on a computer system to evaluate its security. It is a cybersecurity technique that uses the same tools and methods that actual attackers used, to find any impacts and weaknesses in the system.

Background:

Our client's company transmits and stores large amounts of sensitive information, which can be a target for cybercriminals. Sensitive information includes financial information, social security numbers, and contact details. Our customer was vulnerable to cyber attacks as a successful attack on this network can potentially expose information to millions of customers or be sold.

Due to their interconnected networks, there was an open chance of infiltration that opened doors to internal confidential information. Today's technological advances have made it easier for cyber criminals to find the most vulnerable points. There was a dire need to perform penetration testing to protect information through ethical hacking and find vulnerabilities.

Customer Challenges:

- To find out how the wireless connections were exposed in internal networks.
- To prevent and detect computer attacks, malware, attacks on user privacy, and network threats.
- Go beyond the assessment of applicable compliance mandates with a security-first approach to testing
- To create custom networking protocols
- To ensure the protection of IoT devices, networks, and the platform used.

LogicFinder Solutions and Services:

Logic Finder has a decade of proven experience in Networking, Data Centers, and Cyber Security, introducing innovative solutions to detect threats in real-time and advanced analytics for active network intrusions. Our mission is to bring value to the cybersecurity and networking sphere, globally, with top-notch Consultation, Development, and Training in wireless technology and modern communication networks.

Solutions Provided to the Customer:

Penetration testing requires a significant amount of trust, and therefore it is important to look at the payoffs of this method. Our skilled professionals were able to assess vulnerabilities and give immediate action against these vulnerabilities. We performed different types of testing; network testing, web application testing, wireless testing, and physical penetration testing to ensure businesses will be protected from all types of attacks. We identified different vulnerabilities on different systems by attacking network systems, servers, and their IoT.

We deployed penetration testing in the following steps:

Step 1: We first gathered information about the target systems like network topology, operation systems, applications, user accounts, servers, and end devices. We practiced reconnaissance of the information that was most important to test, where servers were located, filtered out the important connections, and understood the full picture of the target's vulnerabilities.

Step 2: In the next stage, we identified open ports, and web application ports, and analyzed the network traffic on the system we were trying to test. We also attempted to access the servers to check on vulnerabilities on them.

Steps 3&4: Vulnerability assessments were set up on a few Virtual Machines (VM). A Metasploitable VM was deployed intentionally vulnerable to attack. Our team ran a series of controlled attacks by attacking the Metasploitable VM and shifted the network traffic to our VM. Based on that information, our team was able to identify vulnerabilities.

Step 5: Once the vulnerabilities were identified, we exploited the vulnerability and stimulated real-world cyber-attacks. We also made sure that the target system was not compromised or damaged while we run cyber attacks.

Step 6: After utilizing penetration testing, we recorded the results and in the results, mentioned the vulnerabilities, how the attack has been done, and finalized mitigation rules and strategic recommendations of the system.

Security Flaws Detected:

1. No efficient mechanism was defined to defend against malicious attacks.
2. There was a dire need to identify and resolve system vulnerabilities
3. There was a need for security awareness

Company Info

LogicFinder

Website: https://www.logicfinder.net
E-mail: info@logicfinder.net