Penetration Testing Brief

Objective

The objective of this penetration testing engagement is to assess the cybersecurity posture of Apex Motorsport Technologies (Apex) and identify vulnerabilities that could be exploited by threat actors. The primary goal is to simulate a real-world attack targeting Apex through external facing infrastructure and determine the effectiveness of the company's existing security controls.

The greatest risk to Apex is intellectual property theft leading to the compromise of highly sensitive engine component designs which give Apex its competitive edge. The penetration tester is tasked with demonstrating if it is possible for an unauthorised party to acquire and exfiltrate the designs for Apex's **CarbonFuse** technology.

Scope

The scope of this engagement includes all assets and systems belonging to Apex Motorsports Technologies, including but not limited to their network infrastructure, web applications, and endpoint devices.

In-Scope Assets

All Apex systems are within the range **10.10.0.0/16**, any network addresses outside of this range are **not** owned by Apex Motorsports Technologies.

Out-of-Scope Assets

The following IP addresses are out of scope:

- 10.10.100.10/32
- 10.10.100.100/32

Any attempts to scan, exploit, or otherwise attack these addresses as part of the assessment may lead to termination of the penetration testing contract, and possible legal action.

Apex systems are all hosted by cloud infrastructure providers. Any attempts to break out of hypervisor layers and target underlying infrastructure is strictly forbidden.

Methodology

The penetration testing should be conducted in a manner that is safe, controlled, and minimizes the risk of disruption to the company's operations. The testing should follow a systematic approach that includes information gathering, vulnerability identification, exploitation, and post-exploitation activities. The engagement should be conducted in accordance with industry better practice and relevant standards.

Deliverables

At the end of the engagement, the penetration tester should provide evidence of any compromised systems by submitting the contents of "flags" which have been deliberately placed at key points across the environment. Flags should be submitted to the engagement tracking portal at https://ctf.bsidesbne.com

Timing

The penetration testing engagement should be completed within a reasonable time frame that minimizes the impact on the company's operations. As agreed within initial project meetings, the allocated time frame for the assessment is from 2023-07-14 16:00 AEST to 2023-07-15 16:30 AEST. Targeting the in scope assets outside of this time frame is not permitted.

Support

To keep the scenario as realistic as possible, minimal support will be provided to the penetration tester during the engagement. If for some reason a server has become unresponsive during the engagement, the penetration tester can reach out to Apex's IT operations team in the #ctf-support-requests discord channel.
https://discord.gg/A8KUcuuGQC

Confidentiality

All information obtained during the penetration testing engagement should be treated as confidential and should not be disclosed to any third parties (such as other penetration testing teams) without the prior written consent of Apex Motorsports Technologies.

Terms and Conditions

For a full listing of all terms and conditions, including additional rules and code of conduct requirements see the following URL: https://ctf.bsidesbne.com/rules