SOLUTION BRIEF

Penetration (Pen) Testing

Introduction

Third-party penetration (pen) testing is critical to ensure that your product is not vulnerable to cyber threats and to demonstrate your company's commitment to the security of customer data. By engaging with Phoenix Technologies, you can quicky and efficiently identify and prioritize security risks and then undertake any needed steps to mitigate problems and vulnerabilities. Engaging with Phoenix early in the development lifecycle is also a cost-effective first step before trying to meet stringent regulatory requirements and industry standards such as ISO 27001, GDPR, HIPAA or PCI DSS.

Phoenix provides comprehensive, independent pen testing for a large variety of devices including laptops, notebooks, tablets, servers (both standalone and cloud deployed), medical systems, IoT devices, home appliances, automotive systems and more. In addition to physical device pen testing, Phoenix also offers assessments and guidance with respect to software security best practices. Phoenix has engaged with many customers for pen testing including major cloud service providers, automotive companies, computer OEMs and more.

Phoenix has over 40 years of experience with BIOS and UEFI firmware and we are experts with Intel, AMD and Arm-based systems. We also collaborate with third parties such as federally funded security labs, universities, and other security entities to augment our service offerings. Through these deep relationships we can offer comprehensive services and responsibly share information regarding newly emerging threats and test methodologies.

Why do I need pen testing?

We live in a world that is smarter than ever. Many devices that do not look like traditional desktop or laptop PCs contain fully featured computing hardware, and this hardware is often connected to the Internet. This drastic increase in capability and connectivity has not gone unnoticed by cybercriminals. Because of this, industry leaders – and major enterprise customers – have transitioned from treating cybersecurity as an afterthought to proactively taking steps to ensure their products are secure across their entire lifecycle.

Even if security is considered during the development of a product, it is still possible for vulnerabilities to go unnoticed or emerge later, even years after first shipment. Development and QA teams may miss avenues of attack that are apparent only to outside observers, who see the product in a fundamentally different way. Penetration testing, provides a company with such a set of outside observers: trained cybersecurity professionals who do not know the product's internal workings but will instead approach it from the perspective of an attacker.

phoenix technologies

Engagement Process

Phoenix has a well-defined, seven step process to maximize the effectiveness of a pen testing engagement.

1. **Planning** – We begin by listening to your goals and objectives for the testing, so we can clearly define the entire scope of the engagement.

2. **Attack Surface Mapping** – We catalog all the externally facing interfaces and components (ex. OSINT gathering) for the product or device under test.

3. **Threat Modeling** – We perform a comprehensive assessment to understand what threats and threat actors are most relevant to the product.

4. **Vulnerability Research** – We identify n-day vulnerabilities (publically known) and 0-day vulnerabilities (novel, not yet public).

5. **Industry Standard Method**– We verify that the product is secure against n-day vulnerabilities and their documented exploits.

6. **Cutting Edge Analysis** – We discover new 0-day vulnerabilities such as (ex. fuzzing, symbolic execution techniques).

7. **Final Report** – The final deliverable is a comprehensive report which clearly identifies all findings and appropriate best practices, remediation, or mitigation strategies. The report is highly confidential, and Phoenix will not divulge any findings to any third party, security agency without explicit permission from you, our customer.

phoenix technologies

Final Report

At the conclusion of testing, all findings, vulnerabilities discovered, recommendations and mitigation strategies are clearly and systematically documented in a final report. The document is very comprehensive and mostly self-explanatory, but if the customer would like to have a walkthrough of the document to discuss specific sections or recommendations that is strongly encouraged.

phoenix 5

4 SAMPLE SYSTEM Penetration Test Results

This section describes the specific vulnerabilities found on the SAMPLE SYSTEM including their CVSS 3.1 Score, the steps required to reproduce each vulnerability and recommendations for vulnerability mitigation.

4.1 SAMPLE VULNERABILITY + ID [CRITICAL]

4.1.1 Vulnerability

DESCRIPTION...

4.1.2 Sample Severity Rating

CVSS 3.1 Score: #.# (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS Base Metrics

- **Attack vector:** Network
- **Attack complexity:** Low
- **Privileges required:** None
- **User interaction:** None
- **Scope:** Unchanged
- **Confidentiality:** High
- **Integrity:** High
- **Availability:** High

A critical part of the final report is a detailed listing of all discovered vulnerabilities with a severity rating assigned to each exploitable vulnerability to simplify reporting, analysis, and remediation planning. Vulnerability classification based on the severity rating reflects both the probability of exploitation and the business impact on the organization. We use the industry standard CVSS 3.1 scoring system since it has been widely adopted for measuring the severity of security vulnerabilities. The chart below provides some details with respect to the various levels in the CVSS scoring system.

Severity Rating	CVSS 3.1 Score	Description
CRITICAL	9.0 - 10	Exploitation of the vulnerability allows an attacker administrative-level access to systems and/or high-level data that would catastrophically impact the organization. Vulnerabilities marked CRITICAL require immediate attention and must be fixed without delay, especially if they occur in a production environment.
HIGH	7.0 - 8.9	Exploitation of the vulnerability makes it possible to access high-value data. However, there are certain pre-requisites that need to be met for the attack to be successful. These vulnerabilities should be reviewed and remedied wherever possible.
MEDIUM	4.0 - 6.9	Exploitation of the vulnerability might depend on external factors or other conditions that are difficult to achieve, like requiring user privileges for a successful exploitation. These are moderate security issues that require some effort to successfully impact the environment.
LOW	0.1 - 3.9	Vulnerabilities in the low range typically have very little impact on an organization's business. Exploitation of such vulnerabilities usually requires local or physical system access and depends on conditions that are very difficult to achieve practically.
INFORMATIONAL	0.0	These vulnerabilities represent significantly less risk and are informational in nature. These items can be remediated to increase security.

As the industry moves toward widespread adoption of the new CVSS 4.0 standard, we will also provide these additional scoring results.

Specific Test Items for N-day and O-day Vulnerabilities

The specific actions taken to perform a penetration test on a product depend on the type of product being tested, the product's security model, and the category of testing being performed. Some common actions Phoenix would perform for "n-day" and "0-day" vulnerabilities as part of a penetration test are shown in the following table.

Note: "N-day" vulnerabilities are those that are publicly known, possibly for significant periods of time. Many n-day vulnerabilities are trivial for attackers to exploit and their continued presence in actively shipping products can be embarrassing for a manufacturer.

Note: "0-day" vulnerabilities are novel and hence unknown to the public, but could be found and exploited by attackers at any time.

N-Day Vulnerability Testing		
Hardware	**Software**	**Cryptography**
Standards validation	Port scanning	Algorithm validation
OSINT gathering (patents etc.)	API scanning	Channel security evaluation
Peripheral interface analysis	Web application analysis	Encryption-at-rest evaluation
	Manual service testing	Encryption-in-transit evaluation
	Host configuration testing	

0-Day Vulnerability Testing		
Firmware	**Software**	**Network Traffic Analysis**
Binary extraction from flash	Services fuzzing	Packet analysis
Static firmware analysis	Dynamic service analysis	Web penetration testing
Dynamic firmware analysis	Symbolic service execution	Cloud service testing
Firmware fuzzing		
RF communication analysis		

Test Offerings

There are many categories of penetration testing performed by Phoenix, including threat modeling, on-device testing, long-term physical presence testing, short-term physical presence testing, and network-based testing. Threat modeling can be performed for any product, while the four other categories are specific to certain product types.

Threat Modeling

Applicable to All systems

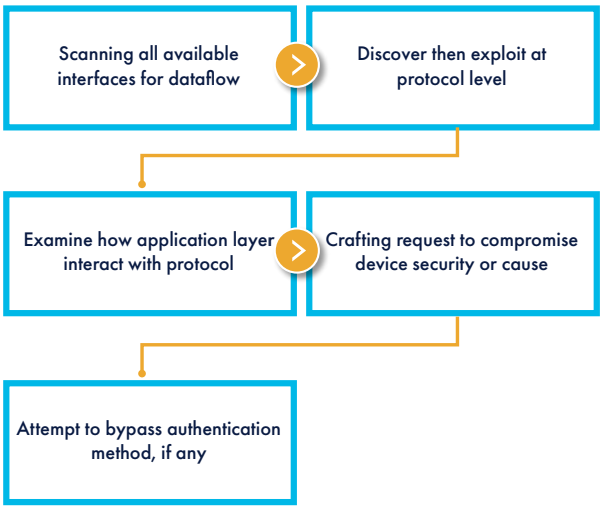
As part of any security testing, one of the first steps is to identify potential attack vectors, understand the threat landscape, and conduct threat modeling. The STRIDE framework is used to ensure a systematic approach to identifying and categorizing threats.

Through adopting a holistic approach to threat modeling – considering the varied factors that influence security – we ensure that our penetration testing provides a robust evaluation of the product's security posture within a secure and resilient computing ecosystem.

Network-based Testing

IoT devices, servers, PCs, smartphones, network hardware

For any device connected to the Internet, the most likely source of real-world attacks will almost always be the network. Even if a device is not directly accessible from the public Internet, LAN-based attacks may be used by network worms or attackers who have gained a foothold on one device to compromise additional devices.



phoenix technologies

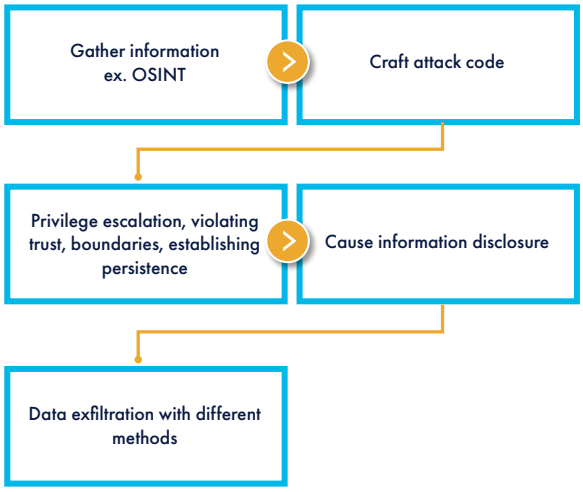
Test Offerings - Continued

On-Device Testing

PCs, smartphones, servers, app-enabled devices

Modern computing devices provide the ability for users to download and run third-party applications. Some of these applications are web pages or scripts embedded in files. Depending on the design of the system, there may be a trust boundary between these applications and the system core, between applications run by different users, or between individual applications.

If Phoenix is given the ability to run applications we develop on the device, or given access to a shell environment (command line or graphical), we can determine if the system is secure against malicious applications and attackers who have gained entry into the device.

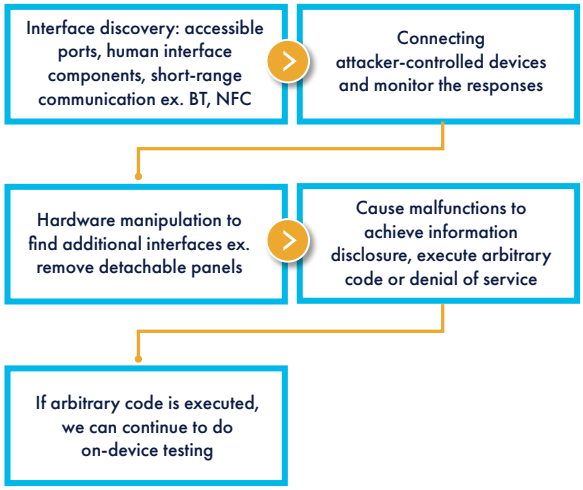


Short-Term Physical Presence Testing

Kiosks, POS/ATM systems, game machines, access panels, laptops

A person with short-term access to the device could install a malicious implant or exfiltrate data. This is a significant problem for many products.

Phoenix's extensive experience protecting business computing devices against physical presence attacks forms the core of our broad knowledge on how to perform this type of testing.

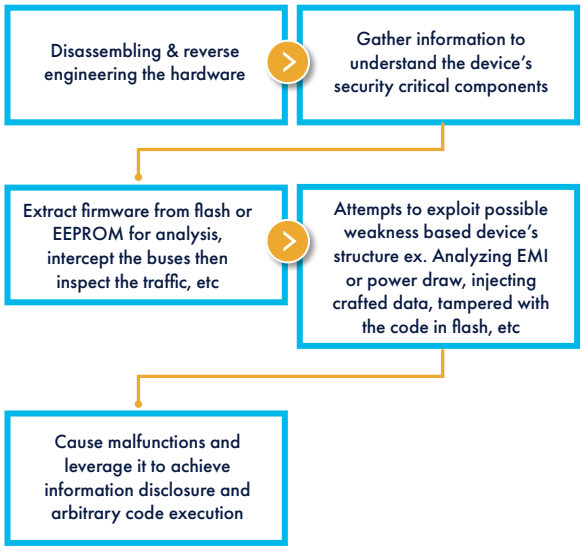


Long-Term Physical Presence Testing

High security devices, as determined by manufacturer

Corporate and government customers may demand that a device remain secure even if disassembled and electrically manipulated in a laboratory environment. This type of security is difficult to achieve and may conflict with commonly desired features; if such a high security level is required, it is absolutely imperative that the device is subjected to extensive testing, or else the development effort is wasted.

Our security researchers begin by disassembling the device and reverse engineering its electronic hardware. Public information is gathered from FCC data, patents, standards documents, and other sources in order to understand the device's security-critical components. Firmware is extracted from flash memory or EEPROM and subjected to automated and manual analysis. Buses are intercepted and traffic is inspected under various conditions. Once information about the device's internal structure is compiled, attempts are made to exploit possible weaknesses. Side channels such as EMI and power draw are analyzed for information disclosure. Crafted data is injected into buses, code in flash is tampered with, and the device's power distribution system is manipulated. Finally, any malfunctions that occur are leveraged to achieve information disclosure and arbitrary code execution.



phoenix technologies

Phoenix Security Team

Phoenix has a dedicated security team to provide rapid response and resolution, along with security-focused code reviews and pen testing services. The team has well defined internal and external processes for processing disclosures and providing customers with security updates. In addition to original research, the Phoenix security team maintains a database of security reports from various sources including silicon vendors, independent researchers, government organizations, academic labs and UEFI related groups such as the USRT (UEFI Security Response Team). In fact, Phoenix chairs the USRT and holds the vice chairmanship of the UEFI SBOM (Software Bill of Materials) Team (USBT).

Phoenix Technologies has been authorized by the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) as a CVE (Common Vulnerabilities and Exposure) Numbering Authority (CNA). A CNA designation is only provided to well-known entities that have a history of demonstrated security credentials and capabilities.

As a CNA, Phoenix has the ability to directly assign CVE numbers to vulnerabilities discovered in its own source code, as well as vulnerabilities in third-party software discovered by the Phoenix security team that are not in another CNA's scope. Phoenix can then publish that information via the CVE vulnerability list which feeds into the U.S. National Vulnerability Database (NVD) under NIST. Information technology and cybersecurity professionals around the world rely on the NVD to ensure they are discussing the same issue and to coordinate their efforts to prioritize and address vulnerabilities.

For more details, please
contact your Phoenix representative
or email **firmcare@phoenix.com**.

phoenix technologies