PENETRATION TESTING

Identify, Exploit, and Mitigate Organizational Risks with Penetration Testing

A penetration test is a security exercise designed to identify risks to an organization by having OCD Tech act as a simulated threat actor. OCD Tech will analyze the environment and leverage found vulnerabilities, misconfigurations, and the functionalities available to a low privileged user to execute the test. The assessment team will attempt to exploit identified issues to demonstrate their potential exposure, with the goal of reaching a high level of privilege in the environment and gaining access to sensitive information. At the end of an engagement, we will have identified key risks and made recommendations for remediation that will strengthen your overall security posture. We provide plain, easy to read executive summaries of our findings, as well as actionable technical recommendations for addressing identified deficiencies.

Methodology

The methodology presented below is broad, and a carefully defined scope will drive the actual components of the test.

Passive Reconnaissance
Leverage sources of Open Source Intelligence to collect information about the organization and its employees.

Active Reconnaissance
Characterize the target network and target systems to identify potentially exploitable vulnerabilities or misconfigurations.

Social Engineering
Target end-users in an attempt to recover sensitive information or install malicious software. This can take several forms.

Exploitation
Gain unauthorized access to target systems.

Post Exploitation
Use the newly established foothold to gather information specific to the level of privilege gained that was previously not available.

Privilege Escalation
Gain administrator-level access to target systems.

Lateral Movement
Leverage collected data to move throughout the network, with a focus on obtaining access to critical systems.

Maintain Access
Depending on the scope of the test, ensure that compromised systems may be accessed throughout the test.

Cover Tracks
Depending on the scope of the test, ensure that all traces of attacker activity are removed.

Reporting
Compile all information gathered during the penetration test for management.

Report Preparation and Delivery

Our final deliverable will include risk-ranked findings, based on the NIST 800-30 Guide for Conducting Risk Assessments, assessment scale. This scale determines the level of risk based on a combination of likelihood and impact. Each observation will be categorized as VERY HIGH, HIGH, MODERATE, LOW, or VERY LOW, based on the intersection of impact and likelihood of exploitation by a threat actor. All findings will have corresponding recommendations for improvement and remediation.

Likelihood (Threat Event Occurs and Results in Adverse Impact)	Level of Impact				
	Very Low	Low	Moderate	High	Very High
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	Very High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

Industry Contributions

OCD Tech Staff are recognized industry experts who frequently deliver insightful presentations and conduct comprehensive research on our extensive range of product lines, including advanced penetration testing. Our team has shared their expertise and research findings at prestigious industry events, such as BSides Boston and the NoVA Hackers Invitational. We have also performed technical demonstrations at notable gatherings, including the ISACA AGM. Furthermore, our contributions extend to partnering with local colleges on CTF events and our 'Road to Ethical Hacker' lecture, as well as PenTest Magazine and Hakin9 article contributions.

To see the latest news from the industry and beyond, make sure to check out our blog HERE

CVE Identifications

During penetration testing engagements, OCD Tech has identified and publicly disclosed six (6) new CVEs. By working with the software vendor to fix the vulnerability, and MITRE for public disclosure, OCD Tech seeks to maximize the reach of each vulnerability discovery for the InfoSec community as a whole, while minimizing risk to existing users of the vulnerable software. More information on the vulnerability disclosures listed below can found online at https://cve.mitre.org/

Number	Description
CVE-2018-11628	Data input into EMS Master Calendar before 8.0.0.201805210 via URL parameters is not properly sanitized, allowing malicious attackers to send a crafted URL for XSS.
CVE-2019-7004	A Cross-Site Scripting (XSS) vulnerability in the WebUI component of IP Office Application Server could allow unauthorized code execution and potentially disclose sensitive information.
CVE-2019-19774	Zoho ManageEngine EventLog Analyzer 10.0 SP1 before Build 12110 security restrictions bypass.
CVE-2020-12679	A reflected cross-site scripting (XSS) vulnerability in the Mitel ShoreTel Conference Web Application.
CVE-2020-13998	Citrix XenApp 6.5, when 2FA is enabled, allows a remote unauthenticated attacker to a certain whether a user exists on the server, because the 2FA error page only occurs after a valid username is entered.
CVE-2020-5132	SonicWall SSL-VPN products and SonicWall firewall SSL-VPN feature misconfiguration that could lead to a domain name collision vulnerability.

CONTACT OUR IT EXPERTS FOR A CONSULTATION ON YOUR PATH TO SUCCESS

Michael Hammond, CISA, CRISC, CISSP
Principal
Phone: 844-OCD-TECH Email:
mhammond@ocd-tech.com

Robbie Harriman, CISA
Director, Advisory Services
Phone: 844-OCD-TECH Email:
rharriman@ocd-tech.com