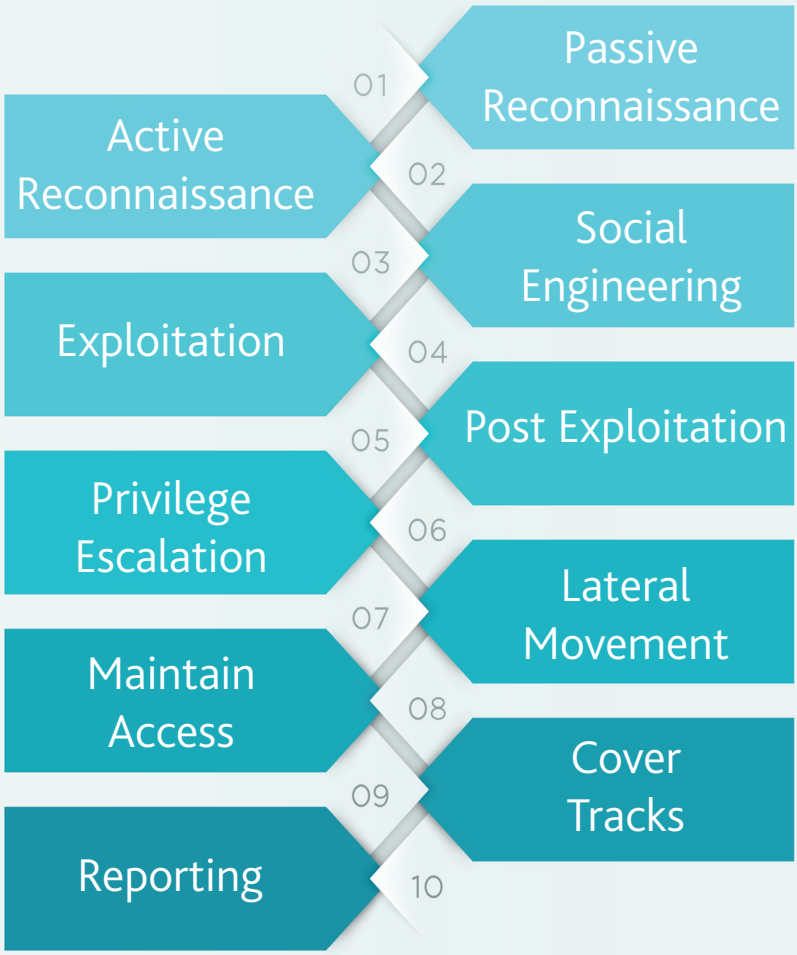
Penetration Testing

Identify, Exploit, and Mitigate Organizational Risks with Penetration Testing

In a penetration test, the OCD Tech team analyzes an organization's environment and leverages the found vulnerabilities, misconfigurations, and the functionalities available to a low privileged user. This process will take advantage of the results identified via a vulnerability assessment. Rather than simply reporting identified vulnerabilities, the assessment team will attempt to exploit these vulnerabilities, and demonstrate the potential exposure with the goal of reaching the highest possible level of privilege and gaining access to sensitive information. While our goal for the simulated attack may be reaching the highest level of privilege, our ultimate goal for an engagement is to identify risks and make recommendations for remediation that will strengthen your security posture. We provide plain English 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.

Braintree | Winchester
Tel: 617.471.1120 • www.ocd-tech.com • Twitter: @TheOCDTech

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	High
Low	Very Low	Low	Low	Low	Moderate
Low	Very Low	Very Low	Very Low	Low	Low

Industry Contributions

OCD Tech Staff regularly speak and provide research to the industry on our numerous product lines including penetration testing. Staff provided insight and research findings on Domain Name Collisions at BSides Boston 2020 and the NoVA Hackers Invitational. In addition, OCD Tech performed a password cracking demonstration at the 2020 ISACA AGM event. Lastly, check out our article entitled "A Crash Course in Splunk and Security" featured in Pentest Magazine's Best of 2020.

Presented at the Domain Name Collisions at BSides Boston 2020

Presented at NoVA Hackers Invitational 2020.

Performed Password Cracking Demonstration at 2020 ISACA AGM.

Published articles featured in PenTest Magazine.

To see the latest news from the industry and beyond, make sure to check out our blog at **https://ocd-tech.com/blog/**

CVE Identifications

During penetration testing engagements, OCD Tech has identified and publicly disclosed six (6) new CVEs over the past three years. 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 ascertain whether a user exists on the server, because the 2FA error page only occurs after a valid username is entered.
CVE-2020-51332	SonicWall SSL-VPN products and SonicWall firewall SSL-VPN feature misconfiguration.

About Us

OCD Tech is the IT Audit, Security, and Assurance division of O'Connor & Drew, P.C. Comprised of a team of IT industry veterans, OCD Tech utilizes industry recognized frameworks and leading practices to assess your company's technology risks and provide expert analysis and recommendations for actionable improvements to protect your systems, data, and your overall business from cyber threats and attacks. We have provided penetration testing services to countless organizations just like yours and would welcome the opportunity to answer your questions and address your specific needs.

OCDTECH O'Connor & Drew P.C. Certified Public Accountants

Contact Us

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

Robbie Harriman, Senior IT Audit Manager
CISA, ISACA CSX, CompTIA
Phone: 844-OCDTECH
Email: rharriman@ocd-tech.com