Penetration Testing Cheat Sheet

HITACHI
Inspire the Next

Definition

Simulated attacks in a controlled environment carried out by third-party security specialists who employ the same techniques as attackers located outside your infrastructure.

Objective

"Identify ways to exploit vulnerabilities to circumvent or defeat the security features of system components" (PCI SSC).
A pentest reveals whether your organization is potentially vulnerable to cyberattacks and provides recommendations on how to strengthen your security posture.

Why a pentest?

1. To uncover critical vulnerabilities in your environment
2. To prioritize and tackle risks based on their exploitability and impact
3. To comply with industry standards and regulations
4. Keep stakeholders and shareholders informed about your organization's risk exposure and security posture
5. Preserve your organization's integrity and reputation

When to conduct a pentest?

Pentest your environment at least 1x per year, ideally on a quarterly basis for optimal results.

- After a major breach or data leak, to find out which vulnerabilities may have led to exploitation
- During major changes or updates to a network or applications, e.g. when relocating offices or adding new infrastructure
- As part of the Software Development Lifecycle (SDLC) process, e.g. before application launches
- As part of a regular compliance practice, e.g. with PCI DSS v3.2, ISO 27001, HIPPA, NIST, or the 20 Critical Security Controls from the CIS
- If you want to find out how strong your cybersecurity posture really is against breaches and intrusions

Terms

- Black box: performed without any additional knowledge of the target and organization itself.
- White box: performed with knowledge of the internal structure of a network or application to better uncover potential vulnerabilities.
- Grey box: in between a black box and white box pentest, a grey box pentesting team will have partial knowledge of the network's or applications' inner-workings.
- Red Team: known as the attackers, Red Teams are external entities brought in by a client to exploit vulnerabilities in the environment
- Blue Team: known as the defenders, Blue Teams are internal entities mandated by the client to defend their environment against external attacker and Red Teams
- Purple Team: leveraging knowledge from both the attackers and the defenders, Purple Teams are a group of people who do both Red and Blue Team security testing to secure a client environment

Types

- Network/ Infrastructure Pentest: one of the most common pentests, aimed at discovering vulnerabilities and gaps in the client's network infrastructure
- (Web) Application Pentest: conducted on (web) applications, browsers and their related plugins
- Wireless Pentest: aimed at analyzing the wireless devices deployed at the client site, e.g. tablets, laptops, notebooks, iPads, smart phones
- Social Engineering: a targeted attack of the client's employees to attempt to initiate a breach from within the client environment
- Capture-the-Flag Pentest: a cybersecurity competition designed to challenge its pentesters to find a "flag" (a file, a snippet of code, a piece of hardware) within a specific environment.
- Cloud Pentest: conducted to reveal vulnerabilities on cloud systems and applications

Common findings

Password attacks and default passwords, Operating system attacks, Application level attacks, Misconfiguration issues, Injection attacks (SQL, NoSQL, LDAP, etc.), Cross-Site Scripting (XSS), Authentication issues, Authorization and access control issues, Misconfiguration issues, Vulnerable components.

Phases

1. Reconnaissance
2. Scanning
3. Gaining access
4. Maintaining access and
5. Covering tracks

Report elements

- Executive summary
- Technical approach and methodology
- Vulnerabilities and exploits
- Recommendations for remediation
- Appendix

How to select a vendor

1. Define the type of pentest you need
2. Evaluate the pentesting team skills
3. Ask for relevant references
4. Find out how your data will be secured
5. Ask for liability insurance
6. Get a sample report
7. Verify project management capabilities
8. Clarify the methodology and process
9. Ask about options for retesting
10. Get to know the pentesting vendor

Ethical hacking certifications

- Certified Ethical Hacker (CEH)
- GIAC Penetration Tester (GPEN)
- Offensive Security Certified Professional (OSCP)
- CREST Certified Tester
- Foundstone Ultimate Hacking
- Certified Penetration Testing Consultant (CPTC)
- Certified Penetration Testing Engineer (CPTE)

Tools

- Nmap
- Burp Suite
- Metasploit
- Netcat
- Python
- PowerShell and PowerSploit
- Scanning applications (Nessus, Qualys, Nexpose, OpenVAS)
- Python Script Responder
- Wireshark
- Cobalt Strike

Resources to Bookmark

- Offensive Security
- The Exploit Database
- The SANS Institute PentesterLab
- Cybrary
- Penetration Testing Practice Lab
- Ethical Hacking LinkedIn Group
- Kioptrix
- EHacking.net
- GitHub – Awesome Penetration Testing