2023 pentest

pre-test write-up

# Executive summary

## - Objective:

The purpose and objective of this penetration test is to enumerate the attack surface of [org]’s Information Services and Applications. The digital infrastructure of the company will be subject to an extensive series of cyber security attacks meant to gain a better understanding of the holes present in its existing security measures. Outlined below are the Scope, Methodology, and Rules of Engagement such that maximum information can be extracted from the penetration test with minimal risk to the service and daily functionalities of [org]’s information services. The findings of this examination will be used to harden [org]’s defenses towards a resilient cyber infrastructure.

## - Scope:

The scope of this penetration test is equal to the attack surface of [org]’s cyber infrastructure. Barring that which is excluded by the Rules of Engagement, this includes the [org]’s web services, virtual databases, active directory, password-protected Wi-Fi access points, ARP tables, mobile devices, the Avaya phone system, Visio camera systems, Net motion VPN access, shared file servers, and other information services.

## - Methodology:

A testing account has been created for the purpose of this test with variable privileges and access rights that will be used as a stepping-off point for most attacks. All tools are held on a virtualized Kali Linux machine with IP address [ip] running through and contained within a virtual switch on the machine with FQDN [name].[domain].local and IP [ip].

Throughout the penetration test, the test account will either gain or be given higher levels of privilege and access for the purpose of demonstrating “defense-in-depth,” which, according to NIST’s computer security resource center, is an information security strategy which establishes layered barriers meant to catch attacks that may be missed by a previous layer.1

Specifically, the methodology of the test will take the form outlined by OWASP’s Penetration Testing Execution Standard (PTES)2:

* Pre-engagement Interactions
* Intelligence Gathering
* Threat Modeling
* Vulnerability Analysis
* Exploitation
* Post Exploitation
* Reporting

- Rules of Engagement (EXAMPLE):

Aside from the Pentester’s Rules of Engagement outlined by OWASP2, zero service impact may be tolerated by the attacks. This extends to such attacks as Denial of Service and Distributed Denial of Services wherein information systems are intentionally overloaded with internet traffic using APR pings to deny accessibility to those services.

Also ‘off-the-table’ is social engineering attacks and phishing (barring explicit approval from the Information Services Director and/or other authorized persons).

Finally, all PII will be safeguarded and left in its encrypted state wherever applicable, all HIPPA rules and regulations will be followed3-, no state nor federal information security laws will be violated4-15, and no confidential information will be altered, read, or otherwise compromised without notice to the proper authorities.

# References:

1. (NIST, 2022) <https://csrc.nist.gov/glossary/term/defense_in_depth>
2. (OWASP, 2023) <https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies>
3. (Health and Human Services, 2023) <https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html>
4. (CDC, 2022), <https://www.cdc.gov/phlp/publications/topic/hipaa.html>
5. (HHS, 2013), <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>
6. (HHS, 2013), <https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html>
7. (HHS, 2013), <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html>
8. (ED, 2022), <https://studentprivacy.ed.gov/faq/what-ferpa>
9. (CDC, 2022), <https://www.cdc.gov/phlp/publications/topic/ferpa.html>
10. (FDIC, 2022), <https://www.fdic.gov/resources/bankers/affordable-mortgage-lending-center/glba.html>
11. (Proton AG, 2022), <https://gdpr.eu/what-is-gdpr/>
12. (EU, 2022), <https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG>
13. (Wikipedia, 2022), <https://en.wikipedia.org/wiki/Key_disclosure_law>
14. (Open Rights, 2021), <https://wiki.openrightsgroup.org/wiki/Regulation_of_Investigatory_Powers_Act_2000/Part_III>
15. (SoC DoJ, 2022), <https://oag.ca.gov/privacy/ccpa>