Affiliated Computer Services, Inc.
Security Engineering Group

Vulnerability Assessment and Penetration Test Report for **SampleNET**

---

v.1.0

Table of Content

Executive Summary

At the request of SampleNET, the ACS Penetration testing team performed the security assessment of the externally facing network infrastructure. The purpose of this assessment was to identify network and application-level security issues.

The objective of the analysis is to simulate an attack to assess SampleNET's immunity level, discover weak links and provide recommendations and guidelines to vulnerable entities discovered. This report is a report which contains sub-sections. Each Sub-section discusses in detail all relevant issues and avenues that can be used by attackers to compromise and gain unauthorized access to sensitive information.

Every issue includes an overview of issues found and security guidelines, which, if followed correctly, will ensure the confidentiality and integrity of the systems and applications.

ACS's assessment methodology includes structured review processes based on recognized “best-in-class” practices as defined by such methodologies as the ISECOM's Open Source Security Testing Methodology Manual (OSSTMM), the Open Web Application Security Project (OWASP) and ISO 27001 Information Security Standard.

Phase One (Footprinting and Enumeration) of the test was executed within ACS's Penetration testing Lab facility while phase two (Scanning, and Exploitation) was conducted again from the ACS's Penetration testing Lab facility.

This testing did not explicitly attempt Denial of Service (DoS) attacks against any of the SampleNET systems. However, we performed the security assessment of the external network and web application as an unauthorized user. Login credentials to the web applications systems were not obtained as part of the testing process. This was a complete blind test simulating a typical external hacker's view of the organization.

At the request of SampleNET, the ACS Penetration testing team performed the security assessment of the externally facing network infrastructure. The purpose of this assessment was to identify network and application-level security issues.

The objective of the analysis is to simulate an attack to assess SampleNET' immunity level, discover weak links and provide recommendations and guidelines to vulnerable entities discovered. This report is a report which contains sub-sections. Each Sub-section discusses in detail all relevant issues and avenues that can be used by attackers to compromise and gain unauthorized access to sensitive information.

Every issue includes an overview of issues found and security guidelines, which, if followed correctly, will ensure the confidentiality and integrity of the systems and applications.

ACS's assessment methodology includes structured review processes based on recognized “best-in-class” practices as defined by such methodologies as the ISECOM's Open Source Security Testing Methodology Manual (OSSTMM), the Open Web Application Security Project (OWASP) and ISO 27001 Information Security Standard.

Phase One (Footprinting and Enumeration) of the test was executed within ACS's Penetration testing Lab facility while phase two (Scanning, and Exploitation) was conducted again from the ACS's Penetration testing Lab facility.

This testing did not explicitly attempt Denial of Service (DoS) attacks against any of SampleNET systems. However, we performed the security assessment of the external network and web application as an unauthorized user. Login credentials to the web applications systems were not obtained as part of

the testing process. This was a complete blind test simulating a typical external hacker's view of the organization.

At the request of SampleNET, the ACS Penetration testing team performed the security assessment of the externally facing network infrastructure. The purpose of this assessment was to identify network and application-level security issues.

The objective of the analysis is to simulate an attack to assess SampleNET' immunity level, discover weak links and provide recommendations and guidelines to vulnerable entities discovered. This report is a report which contains sub-sections. Each Sub-section discusses in detail all relevant issues and avenues that can be used by attackers to compromise and gain unauthorized access to sensitive information.

Every issue includes an overview of issues found and security guidelines, which, if followed correctly, will ensure the confidentiality and integrity of the systems and applications.

ACS's assessment methodology includes structured review processes based on recognized “best-in-class” practices as defined by such methodologies as the ISECOM's Open Source Security Testing Methodology Manual (OSSTMM), the Open Web Application Security Project (OWASP) and ISO 27001 Information Security Standard.

Phase One (Footprinting and Enumeration) of the test was executed within ACS's Penetration testing Lab facility while phase two (Scanning, and Exploitation) was conducted again from the ACS's Penetration testing Lab facility.

This testing did not explicitly attempt Denial of Service (DoS) attacks against any of SampleNET systems. However, we performed the security assessment of the external network and web application as an unauthorized user. Login credentials to the web applications systems were not obtained as part of the testing process. This was a complete blind test simulating a typical external hacker's view of the organization.