Security Audit Report of All Ports Tour



[EXECUTIVE SUMMARY 2](#_Toc895888591)

[IMPACT ANALYSIS 3](#_Toc713275736)

[SCOPE 3](#_Toc587571937)

[NETWORK TOPOLOGY 3](#_Toc360020959)

[METHODOLOGY 3](#_Toc1570265559)

[PHASE I: RECON 3](#_Toc414556360)

[PHASE II: EXPLOITATION 3](#_Toc6562868)

[PHASE III: PRIVILEGE ESCALATION 3](#_Toc1908406351)

[PHASE IV: EXFILTRATION 4](#_Toc1386738689)

[TECHNICAL FINDINGS 4](#_Toc1179534766)

[Critical Security Findings 4](#_Toc1384137312)

[1.1. 4](#_Toc701421524)

[High Security Findings 5](#_Toc1045756457)

[2.1. 5](#_Toc158726484)

[APPENDIX 5](#_Toc1150115363)

[Appendix A: Scoring System 6](#_Toc1487183356)

[Appendix B: Tools Used 6](#_Toc1950809076)

## EXECUTIVE SUMMARY

## IMPACT ANALYSIS

## SCOPE

## NETWORK TOPOLOGY

|  |  |
| --- | --- |
| **Name** | **Machine Address** |
|  |  |

## METHODOLOGY

A penetration test (pentest) can vary in terms of how it is deemed successful. Typically, a successful pentest follows the following phases. Proper OPSEC (operational security) procedures and techniques must be implemented throughout the entire security audit.

### PHASE I: RECON

Pentester(s) will commence reconasisance and/or enumeration of the target(s) via passive and active OSINT (open-source intelligence) techniques to determine and verify vulnerabilities that are present on system(s).

### PHASE II: EXPLOITATION

Once vulnerabilities have been identified via the recon phase, pentester(s) will attempt to gain a point of entry into the system(s).

### PHASE III: PRIVILEGE ESCALATION

When pentester(s) successfully exploit the target(s) and a foothold is established, privilege escalation techniques are used to gain access to users and/or accounts with higher privileges such as “root” on Linux / Unix based systems, Administrator or NT AUTHORITY on Windows systems. Persistency is also established allowing pentester(s) to have persistent access to compromised system(s) to perform further attacks such as accessing private networks are not accessible via the public.

### PHASE IV: EXFILTRATION

Once the pentester(s) deem the security audit to be successful and no further actions are needed, they may perform an exfiltration as the last phase of the audit and report back to contractor(s) with a report based on their findings.

## TECHNICAL FINDINGS

|  |  |
| --- | --- |
| Critical | 9.0 – 10.0 |
| High | 7.0 – 8.99 |
| Medium | 4.0 – 6.99 |
| Low | 2.0 – 3.99 |
| Informational | 0.0 – 1.99 |

### Critical Security Findings

#### 1.1.

**Affected Assets:**

**Impact Score:**

**Description:**

**Remediation:**

### High Security Findings

#### 2.1.

**Affected Assets:**

**Impact Score:**

**Description:**

**Remediation:**

## APPENDIX

### Appendix A: Scoring System

To rank vulnerabilities, the CVSS ranking system was utilized. CVSS stands for the Common Vulnerability Scoring System, an open industry standard for assessing and ranking the severity of computer security vulnerabilities on a scale of 0 to 10.

### Appendix B: Tools Used

|  |  |  |
| --- | --- | --- |
|  | **Tools Used** | **Description** |
| 1. |  |  |
| 2. |  |  |
| 3. |  |  |
| 4. |  |  |
| 5. |  |  |
| 6. |  |  |
| 7 |  |  |
| 8 |  |  |
| 9 |  |  |