****

Penetration Test Report

November XXth, 2025

Table of Contents

[1. Executive Summary 3](#_Toc212463796)

[Confidentiality 4](#_Toc212463797)

[Legal Disclaimer 4](#_Toc212463798)

[Recommended Immediate and Long-Term Changes 4](#_Toc212463799)

[Positive Security Measures 4](#_Toc212463800)

[Scope 5](#_Toc212463801)

[Scope Exclusions 5](#_Toc212463802)

[Network Topology 5](#_Toc212463803)

[2. Risk Assessment and Testing Methodology 5](#_Toc212463804)

[3. Comprehensive Vulnerability List 8](#_Toc212463805)

[4. Assessment Findings 9](#_Toc212463806)

[5. Conclusion 12](#_Toc212463807)

[6. Appendix 12](#_Toc212463808)

[Appendix A: Tools //CHANGEME 12](#_Toc212463809)

[Appendix B: Acronyms Used //CHANGEME 12](#_Toc212463810)

# Executive Summary

This report details the findings and recommendations from a penetration test conducted by US-Southeast Team-XX on the digital infrastructure of All Ports Tours, a growing competitor in the luxury cruise and commercial sectors. The assessment aimed to identify existing vulnerabilities and reinforce security controls protecting critical assets, especially following the recent, significant investment in guest-focused digital upgrades.

The scope of this comprehensive penetration test spanned user data management, application security, and network defenses essential to All Ports Tours' operational integrity. The assessment was executed on November 16, 2025, commencing at XX:XX AM EST and concluding at XX:XX PM EST. The final security assessment report was delivered on November 8th, 2025, at XX:XX AM EST.

Our assessment identified XX total vulnerabilities: XX Critical, XX High, XX Moderate, XX Low, and XX Informational. The top Critical vulnerabilities identified include: [list top critical vulnerabilities briefly]. These findings represent a critical step in fortifying All Ports Tours’s infrastructure. The postponement of routine security testing during the pandemic-era digital upgrades has resulted in security gaps that must be immediately addressed.

Given the importance of securing proprietary and user information, and maintaining operational integrity, the current state of these systems exposes All Ports Tours to an unacceptable level of risk. An intrusion could lead to severe regulatory fines, significant legal consequences, and irreparable loss of consumer trust. It is highly recommended that All Ports Tours implement the changes outlined in the full security assessment document to address and resolve these identified vulnerabilities. Immediate remediation, particularly for all Critical and High findings, is essential to uphold data confidentiality, integrity, and availability and ensure a safe and reliable experience for the expanding user base.

## Confidentiality

This document and all information contained within are confidential and proprietary to US-Southeast Team-XX and All Ports Tours. Extreme care should be exercised when handling, referring to, or copying this document. Extreme care should be exercised when handling, referring to, or copying this document. US-Southeast Team-XX authorizes All Ports Tours to view and disseminate this document as they see fit in accordance with US-Southeast Team-XX’s data handling policies. Further dissemination of this document should be marked as “CONFIDENTIAL'' and viewed internally on a “need-to-know” basis.

## Legal Disclaimer

In no event shall US-Southeast Team-XX be liable for the incidental, collateral, or consequential damage that occurs through the use of this information in replication and remediation. All information presented throughout this document is provided as-is and without warranty. Penetration tests and vulnerability assessments are a “point-in-time” analysis, and as such, any changes to the environment or discoveries made in vulnerability research after this assessment will result in this assessment becoming obsolete as time passes.

## Recommended Immediate and Long-Term Changes

Listed below are observations US-Southeast-XX made while conducting the vulnerability assessment within All Ports Tours to mitigate current high-risk issues and improve overall practices. These are meant to be “recommended improvements” and follow industry standards.

* Immediate Actions
  + Require credentials for authentication on the Tram Access Controls.
  + Upgrade the All Ports Tours domain controller to the latest version.
* Long-Term Strategies
  + Require secure software development training for all developers.
  + Invest in phishing awareness practices, such as monthly fishing emails curated by CSOC.
  + Change current password policies to follow NIST password policy standards

## Positive Security Measures

Listed below are observations US-Southeast-X made while conducting the vulnerability assessment within All Ports Tours.

## Scope

US-Southeast-X were permitted to assess several network ranges. In scope were the following ranges: 10.0.0.0/24, 10.0.1.0/24 and 10.0.200.0/24. The contents span All Ports Tours’s assets including but not limited to, All Ports Tours open-source intelligence (OSINT), and social engineering were both permitted for this engagement as designated by All Ports Tours.

## Scope Exclusions

Other All Ports Tours infrastructure networks cover the network ranges 10.0.10.0/24 and 10.0.30.0/24, and are excluded from this assessment by request of All Ports Tours themselves. Physical social engineering was explicitly out-of-scope.

## Network Topology

# Risk Assessment and Testing Methodology

Adhering to a consistent methodology is vital when conducting vulnerability assessments. In our assessment, US-Southeast-XX utilized an approach based on the MITRE ATT&CK framework to model the engagement with All Ports Tours. By structuring the assessment around ATT&CK’s phases, each stage of testing corresponds directly to documented adversary behaviors, providing actionable insights that mirror genuine threat actor methods. Listed Below are the engagement phases our team followed in order:

* Reconnaissance & Enumeration - Collect Information on the target within the confines of our scope. Scanning networks and Identifying vulnerabilities that could lead to initial access.
* Exploitation - Exploit discovered vulnerabilities to gain initial access to targeted systems or networks.
* Persistence - Establish a foothold on networks/ systems to maintain access, even in the event of a reboot or attempts at remediation all while remaining undetected.
* Privilege Escalation - Escalate Low level privilege access to administrator or root, enabling further exploitation of network and systems.
* Exfiltration - Extract valuable data from compromised systems while remaining undetected, documenting the process throughout.
* Reporting - Report exploited vulnerabilities, document findings, and suggested remediation steps to the Blue Team to help harden company systems and improve future security posture.

The assessment findings in this report follow the Common Vulnerability Scoring System (CVSS) v3.1 to evaluate the severity of each vulnerability. The CVSS scoring system includes base vulnerability factors as well as temporal and environmental factors. Business impact is further explained in the technical details. The vector string in the risk classification tables contains every metric that is used to calculate the CVSS score, With categories separated with a forward slash (/). The main categories include Attack Vector (AV) which can be assigned with the values N (Network), A (Adjacent), L (Local), and P (Physical). To see all components and their values refer to the [CVSS 3.1 specification document.](https://www.first.org/cvss/v3-1/specification-document#Vector-String)

|  |  |
| --- | --- |
| **Severity** | **CVSS v3.1 Score** |
| **Critical** | **9.0 - 10.0** |
| **High** | **7.0 - 8.9** |
| **Moderate** | **4.0 - 6.9** |
| **Low** | **0.1 - 3.9** |
| **Informational** | **0.0** |

# Comprehensive Vulnerability List

|  |  |  |
| --- | --- | --- |
| **Severity** | **CVSS** | **Vulnerability Name** |
| **Critical** |  |  |
| **High** |  |  |
| **Moderate** |  |  |
| **Low** |  |  |
| **Informational** |  |  |

# Assessment Findings

|  |  |  |
| --- | --- | --- |
| **Name of Vulnerability** | | |
| **Risk** | **Vector** | **Score** |
| **Critical** |  |  |

**Affected Scope**

* 255.255.255.255 (Domain Name if applicable)

**Description**

Description of vulnerability.

**Technical Impact**

Explain the impact that this has on the affected service/machine

**Business Impact**

Explain the impact that this vulnerability has on the business

**Steps to Reproduce**

* Include screenshots and explanations of how to reproduce a vulnerability.

**Remediation Recommendation**

List steps they can take to remediate the vulnerability

**References**

Include hyperlinks used

**END OF FINDING**

|  |  |  |
| --- | --- | --- |
| **Name of Vulnerability** | | |
| **Risk** | **Vector** | **Score** |
| **Critical** |  |  |

**Affected Scope**

* 255.255.255.255 (Domain Name if applicable)

**Description**

Description of vulnerability.

**Technical Impact**

Explain the impact that this has on the affected service/machine

**Business Impact**

Explain the impact that this vulnerability has on the business

**Steps to Reproduce**

* Include screenshots and explanations of how to reproduce a vulnerability.

**Remediation Recommendation**

List steps they can take to remediate the vulnerability

**References**

Include hyperlinks used

**END OF FINDING**

|  |  |  |
| --- | --- | --- |
| **Name of Vulnerability** | | |
| **Risk** | **Vector** | **Score** |
| **Critical** |  |  |

**Affected Scope**

* 255.255.255.255 (Domain Name if applicable)

**Description**

Description of vulnerability.

**Technical Impact**

Explain the impact that this has on the affected service/machine

**Business Impact**

Explain the impact that this vulnerability has on the business

**Steps to Reproduce**

* Include screenshots and explanations of how to reproduce a vulnerability.

**Remediation Recommendation**

List steps they can take to remediate the vulnerability

**References**

Include hyperlinks used

**END OF FINDING**

# Conclusion

The security assessment of the All Ports Tours network identified vulnerabilities of varying severity, ranging from Critical to Informational. This comprehensive report includes an analysis detailing the associated levels of risk, detailed explanations for each finding, and recommended remediations. Implementing these remediation steps must be prioritized to enhance the security posture of the All Ports Tours network and prevent future compromises to the confidentiality, integrity, and availability of user data, personal information, and host systems.

Our firm, US-Southeast-X, strongly recommends scheduling a comprehensive follow-up assessment to verify that all identified systems have been adequately patched and that the remediation process has not introduced any new security issues. We thank All Ports Tours for the opportunity to conduct this critical assessment and look forward to cultivating a successful and enduring professional relationship.

Very Respectfully,

US-Southeast-XX

# Appendix

## Appendix A: Tools //CHANGEME

* **BloodHound:** This tool is used to visualize and identify attack paths in Active Directory environment
* **Burpsuite**: An integrated web-application security testing platform centered on an intercepting proxy that lets testers inspect, modify, scan, and automate attacks on HTTP/S traffic
* **CrackMapExec**: A post-exploitation tool that can be used to quickly assess Active Directory domains.
* **Crackstation**: This tool is used to look up tables that are then used to crack password hashes.
* **Dig**: This tool is used to get information from a DNS.
* **EnumForLinux**: A tool for enumerating both Windows and Samba SMB.
* **GoBuster:** A fast directory, file, and DNS brute-forcing tool used to discover hidden paths and subdomains on web servers using wordlists.
* **Hydra**: A network logon cracker used to guess passwords.
* **LES**: A Linux privilege-escalation auditing tool that scans for misconfigurations, weak permissions, and exposed credentials.
* **LinEnum**: Windows privilege-escalation enumeration script that finds misconfigurations, weak permissions, and common escalation vectors.
* **Linpeas**: Linux privilege-escalation script that finds misconfigurations and exposed credentials.
* **Meterpreter**: A Metasploit attack payload that provides the user with an interactive shell and tools.
* **Metasploit**: An exploitation tool with the ability to launch attacks and pivot.
* **MSFVenom**: This tool is a combination of other tools that can be used to create a payload.
* **MySQL**: This tool is used to display database information from a server.
* **Nmap**: Nmap or “Network Mapper” is a free open-source utility that is used for network discovery.
* **NSLookup**: This tool is used to retrieve the records associated with a domain name.
* **Nitko:** A web server scanner that performs comprehensive checks for known vulnerabilities, misconfigurations, and outdated server components.
* **Putty**: An SSH and telnet client that allows a user to connect to another machine
* **Remote Desktop Connection**: This tool allows remote access to another computer with a GUI.
* **Responder**: This tool listens for a specific NETBIOS name and when it is triggered will answer.
* **SMBClient**: This tool can be used to communicate with an SMB server.
* **Sqlmap**: A web server scanner that performs comprehensive checks for known vulnerabilities, misconfigurations, and outdated server components.
* **Wpscan**: A WordPress-focused vulnerability scanner that enumerates plugins, themes, and users and checks them (and site configuration) against a database of known vulnerabilities and common weak credentials.
* **Wireshark**: A network protocol analyzer for capturing and inspecting live network traffic and packet-level details.

## Appendix B: Acronyms Used //CHANGEME

* **AD**: Active Directory
* **C2:** Command and Control
* **DNS**: Domain Name System
* **HTTP**: Hypertext Transfer Protocol
* **LLMNR**: Link-Local Multicast Name Resolution
* **MD5**: Message-Digest Algorithm 5
* **MITM**: Man-In-The-Middle
* **NBT-NS**: NetBIOS Name Service
* **PHP**: Hypertext Preprocessor
* **PLC**: Programmable Logic Controller
* **PoC**: Proof of Concept
* **RDP**: Remote Desktop Protocol
* **ROE**: Rules of Engagement
* **SMB**: Server Message Block
* **SSH**: Secure Shell
* **TLS**: Transport Layer Security