# t

test2

Date 04/06/2016

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Customer Information | | | | | |
| Company Name: | t | | | | |
| City: | t | State: | t | Zip Code: | t |
| URL: | t |  |  |  |  |

|  |  |
| --- | --- |
| Customer Contact Information | |
| Contact Name: |  |
| Title: |  |
| Telephone: |  |
| E-mail: |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Consultant Information | | | | | |
| Company Name: | Serpico Template Report, LLC | | | | |
| Contact Name: | hadhemiadmin | | | | |
| Title: | trainee | | | | |
| Telephone: | 1234 | | | | |
| E-mail: | hadhemisamali@gmail.com | | | | |
| Business Address: | 123 Paper St | | | | |
| City | TestCity | State: | MA | Zip Code: | 11111 |
| URL: | <http://www.serpicoreport.com> | | | | |

# Executive Summary

Serpico Template Company (STC) was contracted to perform a penetration test for t. This report discusses the results from the assessment. Really, if you are reading this you should update the template to match your executive summary. The symbols throughout this report are used to display the data. Please see the README to understand how they work.

Overall, STC was able to achieve the goals of the assessment and exfiltrate the targeted data. There were a number of critical findings during the assessment including the following:

|  |  |
| --- | --- |
| Finding Name | DREAD Score |

MOAR STUFF

# Attack Narrative

The following discusses the details of the assessment.

# Findings

## Findings Table

The following were the results from the assessment:

|  |  |  |
| --- | --- | --- |
| Finding Name | DREAD Score | Remediation Effort |
| **High Risk Findings (36-50)** |  |  |
|  |  |  |
| **Moderate Risk Findings (20-35)** |  |  |
|  |  |  |
| **Low Risk Findings (1-19)** |  |  |
| Clickjacking: X-Frame-Options header missing | 1 | Quick |
| End of Life Systems In Use | 15 | Quick |
|  |  |  |

|  |  |
| --- | --- |
| DREAD Score |  |
| Damage Potential | 3 |
| Reproducibility | 3 |
| Exploitability | 3 |
| Affected Users | 3 |
| Discoverability | 3 |
| Total | 15 |

### Summary

A number of End of Life Operating Systems were found on the internal network (e.g. Microsoft Windows XP). The consultant abused the lack of patching on a subset of these systems to gain a foothold in the internal network.

### Proof

### Remediation