StaticSpeed Vulnerability Report

# Final Report of Security Findings

## Windows 10 ENT

Ex

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Host | High | Medium | Low | Log |
| xxx.xxx.xxx.xxx | xx | x | x | x |

**IP Address: xxx.xxx.xxx.xxx**

|  |  |  |
| --- | --- | --- |
| Service | Port | Sensitive Level |
| xxx | Xxx TCP | High |
| xxx | xxx TCP | Medium |
| xxx | TCP | Low |
| xxx | xx TCP | Log |

Expected detail format for vulnerabilities found

### High

**1- CVE-XXXX-XXXX and or finding**

**Issue**

Explain the vulnerability and add screenshots for proof of concept if applicable

**Impact**

Explain the impact of this finding and sensitivity level. I.E “Attacker can take over the system”

**Mitigation**

Add your suggestions and industry-accepted recommendations to mitigate this vulnerability.

**Reference**

Please add URLs that give context and guidance on how-to understand this finding and fix it.

### Medium

**1- CVE-XXXX-XXXX and or finding**

**Issue**

Explain the vulnerability and add screenshots for proof of concept if applicable

**Impact**

Explain the impact of this finding and sensitivity level. I.E “Attacker can take over the system”

**Mitigation**

Add your suggestions and industry-accepted recommendations to mitigate this vulnerability.

**Reference**

Please add URLs that give context and guidance on how-to understand this finding and fix it.

### Low

**1- CVE-XXXX-XXXX and or finding**

**Issue**

Explain the vulnerability and add screenshots for proof of concept if applicable

**Impact**

Explain the impact of this finding and sensitivity level. I.E “Attacker can take over the system”

**Mitigation**

Add your suggestions and industry-accepted recommendations to mitigate this vulnerability.

**Reference**

Please add URLs that give context and guidance on how-to understand this finding and fix it.

Example

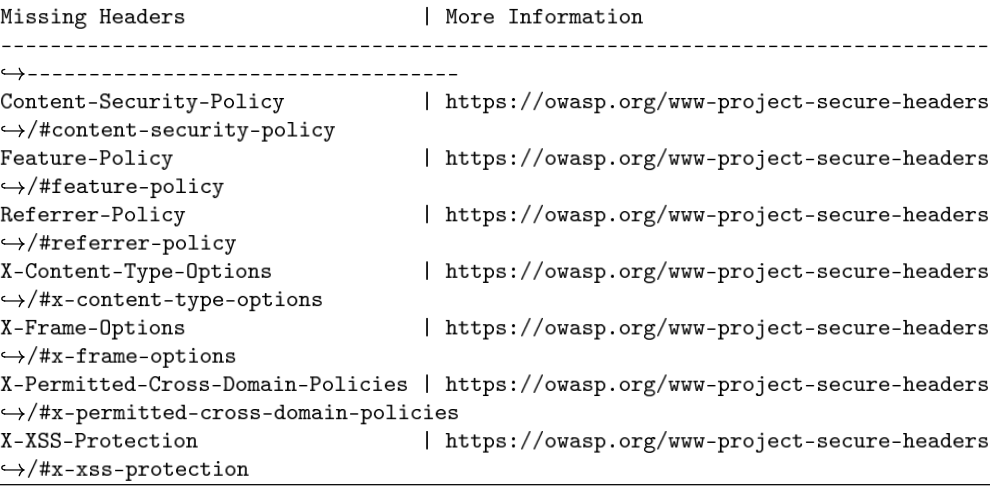
**Log**

**8- HTTP Security Headers Detection**

**Issue**

Known security headers are being checked on the host.

**Impact**



**References**

<https://owasp.org/www-project-secure-headers/>

<https://owasp.org/www-project-secure-headers/#div-headers>

<https://securityheaders.io>

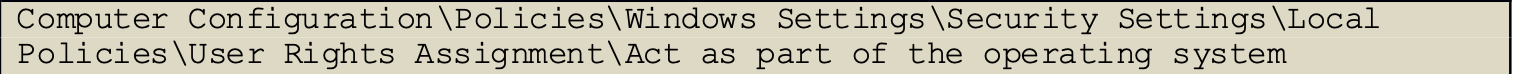
## 

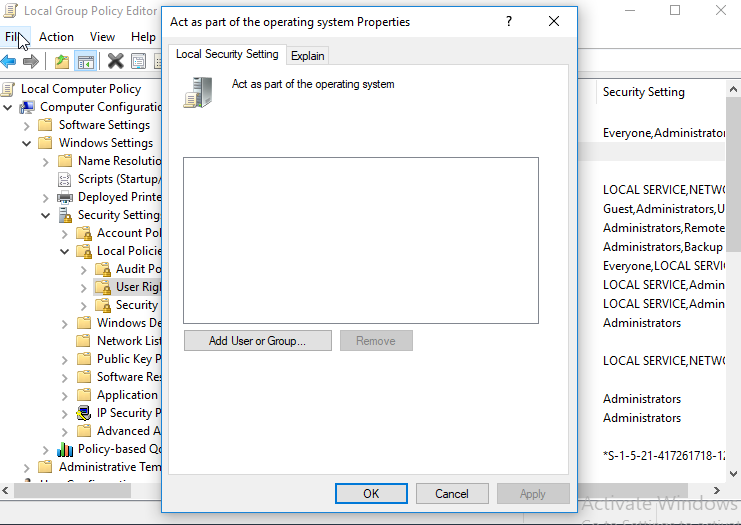
Example of control checks & CIS benchmarks Windows 10 ENT

**Control check - 2.2.3 Ensure ‘Act as part of the operating system’ is set to ‘No One’**

**Result:** Compliant, no user or group found in the setting

**Proof of check:**

****

****

**Impact:** The Act as part of the operating system user right is extremely powerful. Anyone with this user right can take complete control of the computer and erase evidence of their activities.This system is compliant with corporate policy CIS 2.2.3 for Windows 10 ENT.

## Ubuntu 18.04

Ex

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Host | High | Medium | Low | Log |
| xxx.xxx.xxx.xxx | xx | x | x | x |

**IP Address: xxx.xxx.xxx.xxx**

|  |  |  |
| --- | --- | --- |
| Service | Port | Sensitive Level |
| xxx | Xxx TCP | High |
| xxx | xxx TCP | Medium |
| xxx | TCP | Low |
| xxx | xx TCP | Log |

Expected detail format for vulnerabilities found

### High

**1- CVE-XXXX-XXXX and or finding**

**Issue**

Explain the vulnerability and add screenshots for proof of concept if applicable

**Impact**

Explain the impact of this finding and sensitivity level. I.E “Attacker can take over the system”

**Mitigation**

Add your suggestions and industry-accepted recommendations to mitigate this vulnerability.

**Reference**

Please add URLs that give context and guidance on how-to understand this finding and fix it.

### Medium

**1- CVE-XXXX-XXXX and or finding**

**Issue**

Explain the vulnerability and add screenshots for proof of concept if applicable

**Impact**

Explain the impact of this finding and sensitivity level. I.E “Attacker can take over the system”

**Mitigation**

Add your suggestions and industry-accepted recommendations to mitigate this vulnerability.

**Reference**

Please add URLs that give context and guidance on how to understand this finding and fix it.

### Low

**1- CVE-XXXX-XXXX and or finding**

**Issue**

Explain the vulnerability and add screenshots for proof of concept if applicable

**Impact**

Explain the impact of this finding and sensitivity level. I.E “Attacker can take over the system”

**Mitigation**

Add your suggestions and industry-accepted recommendations to mitigate this vulnerability.

**Reference**

Please add URLs that give context and guidance on how-to understand this finding and fix it.

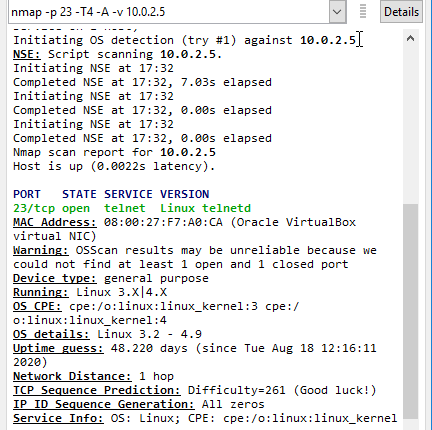
Example of Log

Log

**3 - Telnet Unencrypted Cleartext Login**

**Issue**

The host is running a Telnet service that allows cleartext logins over unencrypted connections



**Impact**

Attackers can uncover login names and passwords by sniffing traffic to the Telnet service.

**Mitigation**

Replace Telnet with remote access protocols that support encryption such as SSH.

**Reference**

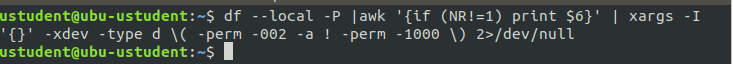
<https://attack.mitre.org/techniques/T1021/>

## 

Example of control checks & CIS benchmarks Ubuntu 18.04

**Control Check: CIS 1.1.21 Ensure sticky bit is set on all world-writable directories**

**Result:** Compliant. Not output from the audit command.

****

**Impact:** This feature prevents the ability to delete or rename files in world-writable directories (such as /tmp ) that are owned by another user. This system is compliant with corporate policy CIS 1.1.21 for Linux Ubuntu 18.04 machines.

**Note:** The CIS benchmarks that need to be checked are listed in all the previous steps.

|  |  |
| --- | --- |
| CIS for Windows Ent v1.9.0. | CIS for Ubuntu 18.04 v2.01 |
| **18.9.102.2** | **1.2.1** |
| **18.3.4** | **1.6.1, 1.6.2** |
| **1.1.5** | **4.2.1.3** |
|  | **5.3.1** |

# Final Assessment and Recommendations Based on Scans and Checks

In this section, provide a final recommendation, supported by the information above, on whether NuttyUtility should extend its network and integrate the StaticSpeed system into its current infrastructure.

Include the following in your assessment:

- Would integrating this network into the extended network of our company bring new risks and exposures?

- If it would be a risk to NuttyUtility, what recommendations would you make to mitigate these risks before implementing the integration, and why?

- Please provide reasoning based on the proof obtained throughout your assessment.

- Remember, the Stakeholders need to decide as to whether or not to complete this integration now.