StaticSpeed Vulnerability Report

As you start your final project, you are expected to perform the following tasks in BOTH Windows and Linux systems. We need to decide if StaticSpeeds systems should be integrated into NuttyUtility's extended network and infrastructure. In the end, your report must support your recommendation. This document is a template that NuttyUtility uses similar system reviews. Some specific information is provided in certain places after initial talks with NuttyUtility. Please follow the format of this template and answer all questions for each section. **You will need to provide either the text outputs from the command line and/or screenshots as evidence** in all sections of this template to show that you have completed the required steps of our company's template and make it easier for stakeholders to see where there might be issues.

Your report must include the findings of your CIS Benchmarks and Security control checks along with the results of Openvas and NMap scans. As a security professional, it is expected that you will relay your findings in terms of industry language (i.e., CVE-xxxx-xxxx, Mitre Technique ID Txxx where applicable). Based on NuttyUtility's security policies, are these systems ready? Your report will be used by stakeholders to decide on the integration.

Control checks and CIS benchmarks for Windows & Ubuntu
In this section, outline your answers from the requested checks. Please provide either the **command-line outputs in the form of text** or **screenshots** that show a CIS check and/or control check has been performed. You must also answer the questions based on your assessments.

Step 1: Asset identification, address update, dependencies, patches, and native protections at targeted Server/ Desktop Operating Systems

Task 1

As seen in your lessons, you must have CIS Benchmarks for Ubuntu 18.04 v2.01 and Windows 10 Ent v1.9.0 to perform these checks. Use the MITRE website for the database of common vulnerabilities and exposures (CVE) https://cve.mitre.org and Mitre ATT&CK framework for referencing attack techniques, tools, and procedures attack.mitre.org.

Task 2

Let's get started in our assessment. We need to find out if software updates and third-party packages settings are correct. Verify-in both of your hosts the following checks.

Are software updates for the systems and third parties configured correctly in these systems?

What is your assessment of StaticSpeeds systems configuration for software updates and third-party packages? Please provide evidence to support your evaluation (command line output or screenshots for each as well)

Windows CIS 18.9.102.2

Ensure 'configure automatic updates' is set to 'Enabled.'

Ubuntu CIS 1.2.1

Ensure package manager repositories are configured correctly.

Task 3- Native Protections and Software Inventory

Next, verify that native protections for the operating systems are enough to protect systems from exploitation. (Hint: Think upgrades) We also need to know exactly what software is running in every machine. Also, please perform a software inventory on each computer and post your findings. The more you know about the systems you are defending, the better chance you will mitigate and harden them.

Windows CIS 18.3.4

Ensure 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' is set to 'Enabled.'

Is this system compliant?

Provide documentation as to what applications are installed on the Windows machine.

Is VNC viewer installed in this Windows System?

Ubuntu CIS 1.6.1, 1.6.2

1.6.1 Ensure XD/NX support is enabled

1.6.2 Ensure address space layout randomization (ASLR) is enabled

Please provide proof of checks via command output or screenshots. According to these checks, are native protections applied to these systems? What packages are installed in this ubuntu machine?

Is TightVNC installed on this Ubuntu machine?

Do these applications, both for Windows and Ubuntu, bring added risks to these systems? Please provide proof and reasoning for your answer.

Task 4

Perform a network asset inventory using Nmap to identify VMs with open ports on both Windows and Linux

What is your assessment of the Asset Inventory and what recommendations do you have to mitigate any potential issues. Please provide evidence to support your findings.

Step 2: Assess Access Management at Targeted Assets

Task 1

Check for current settings on Network Segmentation, VLANs, Domain Isolation, or IP Security Policies.

After completing your checks, what is your assessment of these settings? What recommendations do you have to improve the settings? Remember to provide evidence to back up your thoughts. Things to consider:

- Are there any VLANs?
- Are there any policies in place?
    - If there are any, are they applied?
- Is Anonymous access granted to any share?

Task 2

Investigate and assess the remote access services and protocols in place for StaticSpeed and determine their security level. After completing your investigation, include your assessment of how StaticSpeed is doing with remote access. Please have evidence to support your findings. Remember to consider IPv4 and IPv6. Also, include which Remote Service protocols are running on these systems? What would you recommend to make improvements to this system?

Task 3

NuttyUtility only needs remote access ports for administrators on workstations. What is your assessment of the firewalls in StaticSpeed's systems? Please include evidence to support your thoughts. We need to know if the firewalls are configured correctly?
Also, what ports would you suggest to have open and running and why?

Task 4

Next, conduct a Principles of Least Privilege assessment of StaticSpeed's system. We need to know:

- Which users have high privileges?
- Do important PII folders have the correct permissions and ownership?
- Are the default settings correct, and are there any excessive permissions?
- On our initial scan, we found "data" shared folders that need further investigation.
- Are there "guest" accounts enabled? Are they allowed to use Sudo commands? Are they allowed to log in to ALL workstations?.

Based on your findings, what should be done to secure these accounts and permissions better? Please provide proof of your results and provide reasoning for your answer.

Step 3: Log Monitoring Setup for Detection at Targeted Assets

StaticSpeed has provided access to a monitoring device that has recorded some traffic marked as malicious. Please investigate and assess this further using Wireshark or tcpdump and the provided capture files (pcaps). It is also required of you to verify that appropriate logging is in place at your machines.
Complete your assessment of this traffic. Then, add your suggestions on any issues and improvements by following the steps below. Remember to provide evidence to support your work and recommendations.

Task 1

In this audit, use the pcaps named bruteforce2.pcap and lateralmovement.pcap, along with the other pcaps that may provide more insight into StaticSpeed's network. We recommend focusing on bruteforce2.pcap.

Use the pcap file to assess and determine the following:

- What type of attack was recorded?
- What is the source IP of the attack?
- What protocol was targeted?
- What password was used successfully?
- Which user was compromised?

Based on your findings from above, what is your assessment of what happened? Please provide evidence to back up your results.

Task 2

We suspect that an internal user may have compromised another machine inside StaticSpeed's network and pivoted to one of the devices you are auditing. Please use lateralmovement.pcap and determine the following:

- What was the source IP of the "initial" attack?
- Did the attacker try to access your machine from a compromised device - MITRE ATT&CK Technique T1021?
- What service and port were targeted?
- Was the attacker able to access a sensitive file at the machine you are auditing? Mitre ATT&ACK Technique - T1570

Please provide a narrative of what happened based on your findings. Justify your report based on the answers.

Task 3

Look at logs on the StaticSpeed Windows machine.
Using the logs, determine the following:

- Are there any issues with Windows Share? Please provide screenshots of your findings.
- Look at the audit logs setup at your Linux machine and find the audit.log file. What was the name of the attacker account? Please provide screenshots.

Based on what you found above, provide your assessment on whether these events are enough to start an investigation? Please explain your answer based on what you saw in the logs.

Task 4

NuttyUtility has a centralized log infrastructure using a SIEM product. You need to verify the machines you are checking from StaticSpeed have the settings enabled to use this.

Analyze StaticSpeeds systems and determine if these machines are currently shipping jobs to a centralized location and set up correctly for our SIEM.

Hint: Perform **Ubuntu CIS 4.2.1.3** and verify if remote Syslog is configured for sending logs. In **Windows,** verify in the event viewer if there are any remote subscriptions related to Windows Event Forwarder.

Based on your answers, suggest a course of action to ensure StaticSpeed meets our needs to use a SIEM.

Step 4: Assess Authentication Management at Targeted Assets

Task 1

Evaluate the authentication management situation of StaticSpeed's systems. In our initial look at StaticSpeed, we discovered what is called a "FLAT" network. This means there are no either Active Directory servers or OpenLDAP servers for Linux. We need these to provide us tools to administer the network and enforce access control models. Specifically, when it comes to separate departments, supervisors, end-users, administrators, contractors, visitors, etc.

We also suspected that anyone that accesses this network could pretty much access everything. Determine if the current authentication scheme at StaticSpeed is unacceptable. Make sure to include the following:

- Ensure only administrators can remotely access windows machines and verify if root access is permitted at the Linux host.
- Check for users with excessive permissions
- Is root remote login allowed?
- Are there users that should not have remote access via ssh in Linux?
- Remote Desktop Access should only be granted to administrators in Windows, are there other accounts that should not be given access?

Knowing that your company only wants administrators to log remotely, provide a summary of the current situation for StaticSpeed. Then, suggest what accounts should be allowed to log remotely and why. Include your recommendations on whether StaticSpeeds authentication is acceptable and how you would improve it if it is not. Don't forget to include evidence to back up your recommendations.

Task 2

NuttyUtility follows CIS Benchmarks. Therefore, we need to audit the password policies of StaticSpeed to see if they comply.
Audit the StaticSpeeds systems to verify that they comply with **CIS 5.3.1 Ubuntu** or **Windows 10 CIS benchmarks 1.1.5**? Please provide screenshots of current settings in both systems.

After you perform the checks, please provide an overview of your findings with the specific settings that should be in place and any other changes that should be made. Remember to justify your answer.

Task 3

NuttyUtility uses a strong encryption ciphers policy (FIPS 140-2). Verify that your target assets comply with this policy. Check that these systems are compliant?. Please provide proof of the checks and give specifics on what to do next to get these systems compliant.

Task 4

Conduct aggressive testing for password strength. Use a Nmap NSE Script to test how easy it would be to access StaticSpeed's FTP Server and SMB Shares if an attacker probed them. We have already requested and obtained permission to perform these audits.
Please use an NSE Script to test Mitre ATT&CK T1110 in your Ubuntu virtual machine. Also, use an NSE Script to test the security mode of your SMB shares at your Windows virtual machine. What are your findings? Please provide screenshots. Remember to give an explanation of the security state of these services based on your results.

Step 5: Final Report

After performing the project's tasks, you must produce a report that will include an overview of your findings using best practices industry format. You are expected to include ALL high, medium, low vulnerabilities, and informational findings (Things that are not necessarily scored but are relevant). Make sure to use and include the scanner switches and vulnerability scripts as they may provide conclusions that are not found in the default scanner settings.

The format expected for both virtual machine results is below. Please divide by Operating System
- Linux Ubuntu 18.04
- **Windows 10**

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

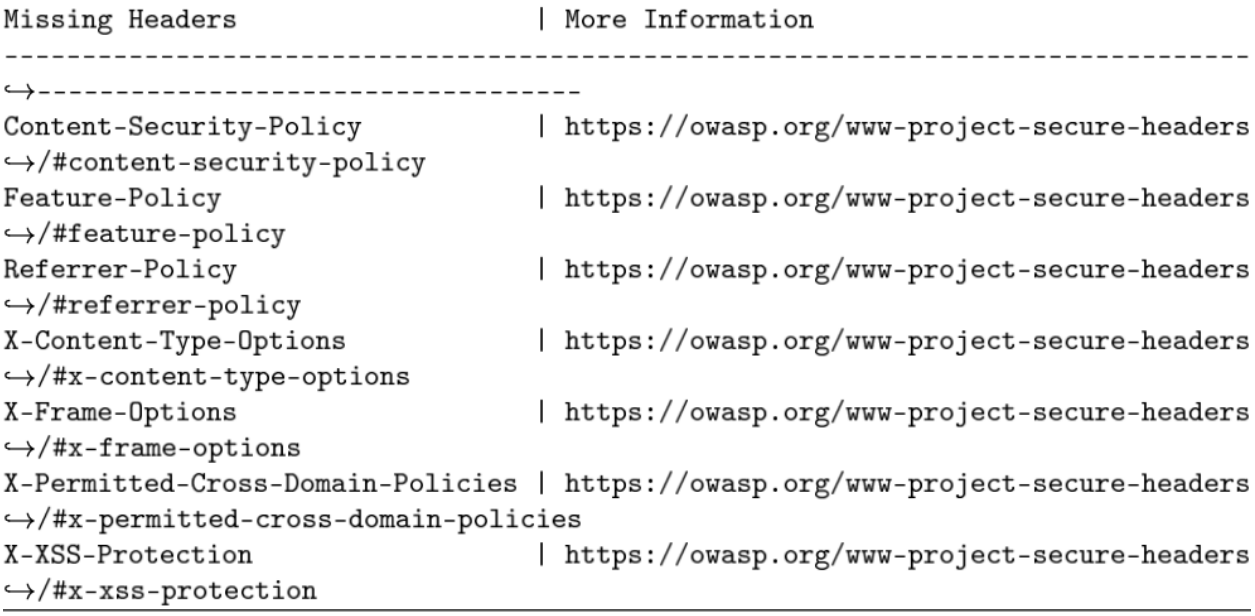
Log

8- HTTP Security Headers Detection

Issue

Known security headers are being checked on the host.

Impact



```
Missing Headers                   | More Information
--------------------------------------------------------------------------------
↪-----------------------------------
Content-Security-Policy           | https://owasp.org/www-project-secure-headers
↪/#content-security-policy
Feature-Policy                    | https://owasp.org/www-project-secure-headers
↪/#feature-policy
Referrer-Policy                   | https://owasp.org/www-project-secure-headers
↪/#referrer-policy
X-Content-Type-Options            | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-Frame-Options                   | https://owasp.org/www-project-secure-headers
↪/#x-frame-options
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
X-XSS-Protection                  | https://owasp.org/www-project-secure-headers
↪/#x-xss-protection
```

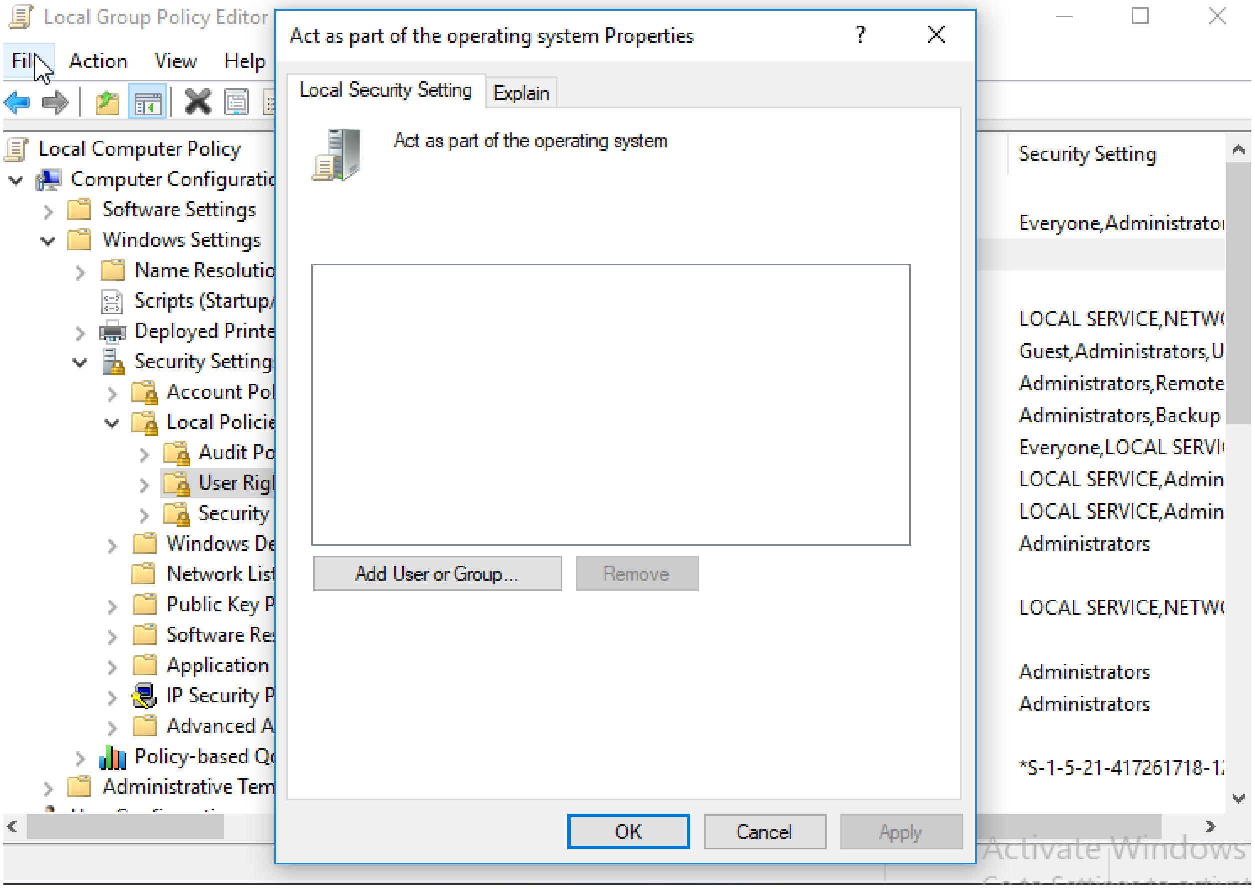
References

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:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Act as part of the operating system
```



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.

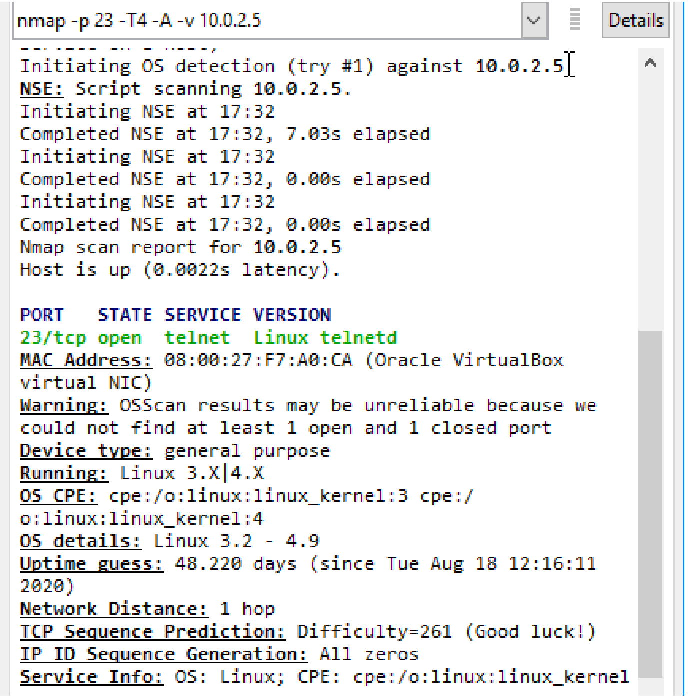
Example of Log

Log

3 - Telnet Unencrypted Cleartext Login

Issue

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



```
nmap -p 23 -T4 -A -v 10.0.2.5
```

```
Initiating OS detection (try #1) against 10.0.2.5
NSE: Script scanning 10.0.2.5.
Initiating NSE at 17:32
Completed NSE at 17:32, 7.03s elapsed
Initiating NSE at 17:32
Completed NSE at 17:32, 0.00s elapsed
Initiating NSE at 17:32
Completed NSE at 17:32, 0.00s elapsed
Nmap scan report for 10.0.2.5
Host is up (0.0022s latency).

PORT   STATE SERVICE VERSION
23/tcp open  telnet  Linux telnetd
MAC Address: 08:00:27:F7:A0:CA (Oracle VirtualBox
virtual NIC)
Warning: OSScan results may be unreliable because we
could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/
o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Uptime guess: 48.220 days (since Tue Aug 18 12:16:11
2020)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Impact

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

Mitigation

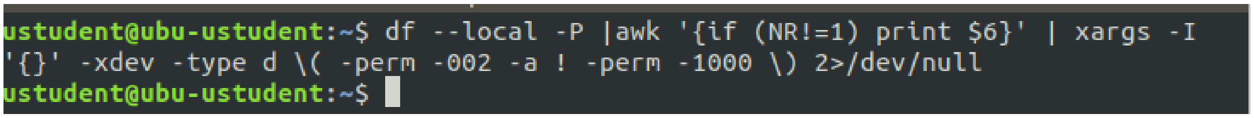
Replace Telnet with remote access protocols that support encryption such as SSH.

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 audit command.



```
ustudent@ubu-ustudent:~$ df --local -P |awk '{if (NR!=1) print $6}' | xargs -I
'{}' -xdev -type d \( -perm -002 -a ! -perm -1000 \) 2>/dev/null
ustudent@ubu-ustudent:~$ 
```

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.

Step 6: Final Assessment and Recommendations Based on Your 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.