Company Name

Penetration Test

# Document Control

The first page of this document should be the cover page that contains the organisation’s logo and the type of test.

In this section include the reporter’s name, their role, and a method of contacting them (Email, work No., etc). Additionally, it is best to write the version control and document properties inside of tables to allow a user to quickly locate the information they require without having to read a paragraph of information.

Finally, do not include an introduction section about your organisation since this can be distracting from the main content of the report and a brief introduction should be done in the executive summary.

Executive Summary

Contents

[Executive Summary 2](#_Toc157590951)

[Document Control 3](#_Toc157590952)

[Overview of Penetration Test 5](#_Toc157590953)

[Scope of Work 5](#_Toc157590954)

[Project Objectives 5](#_Toc157590955)

[Timeline 5](#_Toc157590956)

[Summary of Findings 5](#_Toc157590957)

[Summary of recommendations 5](#_Toc157590958)

[Overview of Methodology 6](#_Toc157590959)

[Reporting 6](#_Toc157590960)

[Detailed findings 7](#_Toc157590961)

[Critical Vulnerabilities 7](#_Toc157590962)

[Vulnerability 7](#_Toc157590963)

[High Vulnerabilities 9](#_Toc157590964)

[Vulnerability 9](#_Toc157590965)

[Medium Vulnerabilities 9](#_Toc157590966)

[Vulnerability 9](#_Toc157590967)

[Low Vulnerabilities 9](#_Toc157590968)

[Vulnerability 9](#_Toc157590969)

[Appendix 10](#_Toc157590970)

[Glossary 11](#_Toc157590971)

# Overview of Penetration Test

# Scope of Work

# Project Objectives

# Timeline

# Summary of Findings

# Summary of recommendations

# Overview of Methodology

# Reporting

# Detailed findings

Critical Vulnerabilities

**Unsupported Windows OS (remote)**

Description  
  
The remote Operating System found on {DEVICE NAME} is no longer supported by the developer or is possibly missing a service pack. The unsupported OS likely contains multiple security vulnerabilities.   
  
  
Impact  
  
The possible vulnerabilities from an outdated Windows OS could range from Remote Code Execution to Denial of Service, which would allow an unauthorised attacker to gain access to sensitive information or disrupt a section of the network, leading to downtime for the organisation’s online services.  
  
  
Likelihood  
  
The unsupported Windows OS was discovered by running a quick OS discovery scan with Nmap, which required little effort to conduct, an attacker is likely to discover the machine on the network. With the out-of-date OS, vulnerabilities will be easily discoverable once the version number has been identified. The Nmap command ran to discover the vulnerability was:  
  
Nmap -O $host  
  
Nmap -O $host  
  
  
Risk Evaluation  
  
Based on the severe impact and high likelihood, the vulnerability has been categorised as a critical vulnerability.   
  
  
Recommendation  
  
If possible, the machine should be updated to a more recent OS such as Windows 10/11.  
  
However, if it is not possible due to the services, alternative security controls should be implemented to mitigate the likelihood and impact that this vulnerability could cause.

**HP System Management Homepage SetSMHData admin-group Parameter Handling RCE**

Description  
  
The HP System Management Homepage (SMH) running on the machine {DEVICE NAME} is affected by a remote code execution vulnerability due to an overflow condition in the mod\_smh\_config.so library. This is caused by improper validation for supplying user input to the /Proxy/SetSMHData endpoint. This can be exploited by an unauthenticated attacker by crafting a request.   
  
  
Impact  
  
The exploitation would lead to a denial of service or remote code execution, which would allow an unauthorised attacker to bring the online service down causing downtime for the organisation or an attacker could gather sensitive information stored on the host.  
  
  
Likelihood  
  
As the vulnerability was found in an older version of HP SMH, it would be simple for an unauthorised attacker to discover the version of the HP SMH by scanning the network and using web developer tools against the webpage of the SMH to discover the outdated version.  
  
  
Risk Evaluation  
  
Based on the severe impact and high likelihood, the vulnerability has been categorised as a critical vulnerability.   
  
  
Recommendation  
  
If possible, the organisation should Upgrade to the latest version of HP SMH.  
  
Otherwise, the organisation should implement security controls to mitigate the severity of the vulnerability.

High Vulnerabilities

**Juniper Junos OS Vulnerability (JSA75739)**

Description  
  
The Juniper Junos OS version on the machine {DEVICE NAME}, is affected by a vulnerability that allows an attacker to cause a denial of service for the host. The vulnerability is caused by an improper validation in the input in the Routing Protocol Daemon of Juniper.   
  
  
Impact  
  
Denial of service could potentially lead to downtime for the organisation’s services which could halt service for clients as well as employees in the organisation.  
  
  
Likelihood  
  
The outdated OS was discovered by running a quick OS discovery scan with Nmap, which required little effort to conduct, an attacker is likely to discover the machine on the network.   
  
With the out-of-date OS, vulnerabilities will be easily discoverable once the version number has been identified.   
  
The Nmap command ran to discover the vulnerability was:  
  
Nmap -O $host  
  
Nmap -O $host  
  
  
Risk Evaluation  
  
Based on the high impact and likelihood for being exploited, the vulnerability has been categorised as a high vulnerability.   
  
  
Recommendation  
  
If possible, Update the Juniper Junos OS to the latest version with all available software patches.  
  
Otherwise mitigate the severity of the vulnerability through alternative methods such as additional security controls.

**Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : Squid vulnerabilities (USN-6728-1)**

Description  
  
The Ubuntu machine {DEVICE NAME} has multiple packages installed all of which contain a denial-of-service vulnerability. The packages are all related to squid, which is a caching proxy for the web.   
  
  
Impact  
  
Denial of service could potentially lead to downtime for the organisation’s services which could halt service for clients as well as employees in the organisation.  
  
  
Likelihood  
  
The affected packages were discovered by running a quick scan with Nmap, which required little effort to conduct.   
  
With affected packages, vulnerabilities will be easily discoverable once the version number has been identified.   
  
  
Risk Evaluation  
  
Based on the high impact and likelihood for being exploited, the vulnerability has been categorised as a high vulnerability.   
  
  
Recommendation  
  
The affected packages should be removed if not required or updated if possible.

Medium Vulnerabilities

**IP Forwarding Enabled**

Description  
  
The hosts {DEVICE NAMES} have IP forwarding enabled.  
  
  
Impact  
  
IP forwarding could be exploited by an attacker to route packets through the hosts and bypass firewalls, routers, and/or NAC filtering.  
  
  
Likelihood  
  
The chance of an attacker using this for an attack is not likely compared to other methods discovered in this assessment however, the damage that can occur if this is used to bypass a firewall could be detrimental to the organisation.  
  
  
Risk Evaluation  
  
Based on the high impact and low likelihood for being exploited, the vulnerability has been categorised as a medium vulnerability.   
  
  
Recommendation  
  
Unless the hosts are routers, it is recommended that IP forwarding is disabled. On Linux, this can be done by inputting:  
  
0 > /proc/sys/net/ipv4/ip\_forward  
  
0 > /proc/sys/net/ipv4/ip\_forward  
  
On Windows, the key 'IPEnableRouter' should be set to 0 under:  
  
HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters  
  
HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters

**SMB Signing Not Required**

Description  
  
The hosts {Device Names} do not require authentication on the remote SMB server.  
  
Impact  
  
Due to this vulnerability, a remote unauthorised attacker could conduct man-in-the-middle attacks against the server, intercepting SMB traffic. The traffic could potentially contain sensitive information for an attacker to steal.  
  
  
Likelihood  
  
 SMB Signing not required is a common vulnerability which appears in many networks, which leads to attackers attempting to exploit it as apart of a standard procedure during an attack.  
  
To determine if the hosts above are vulnerable to this type of attack, an Nmap scan was performed using the “smb-security-mode" script. The command used was:  
  
nmap -p137,139,445 --script smb-security-mode $host  
  
nmap -p137,139,445 --script smb-security-mode $host  
  
  
Risk Evaluation  
  
Based on the medium impact and medium likelihood for being exploited, the vulnerability has been categorised as a medium vulnerability.   
  
  
Recommendation  
  
To remediate this vulnerability, if possible, enforce message signing in the host’s configuration. To do this on Windows, find the policy setting ‘Microsoft network server: Digitally sign communications (always)’. On Samba, the setting will be called ‘server signing’.

Low Vulnerabilities

**SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)**

Description  
  
The host is affected by a Man-In-The-Middle attack known as POODLE. This is an information disclosure vulnerability. This vulnerability is caused by the way SSL 3.0 handles padding bytes when decrypting messages that are encrypted using block ciphers in cipher block chaining (CBC) mode.  
  
  
Impact  
  
Attackers could decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.  
  
  
Likelihood  
  
To verify the presence of this vulnerability the following command was used:  
  
sudo nmap –sV –version-light –script ssl-poodle –p- $host  
  
sudo nmap –sV –version-light –script ssl-poodle –p- $host  
  
While the command is easy to identify, there is a requirement of forcing an application to send the same data over a request and exploit it as well. This makes the vulnerability less likely to be exploited.  
  
  
Risk Evaluation  
  
Based on the low impact and low likelihood for being exploited, the vulnerability has been categorised as a low vulnerability.   
  
  
Recommendation  
  
Disable SSLv3. Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until a point at which SSLv3 can be disabled.

**DHCP Server Detection**

Description  
  
It is possible to query the DHCP server, so it exposes information about its associated network.  
  
  
Impact  
  
An attacker can use the information they gather from the DHCP server to familiarise themselves with the organisation’s network.  
  
  
Likelihood  
  
A simple Nmap command was used to gather the information from the DHCP server:  
  
nmap -sU -p 67 --script=dhcp-discover $host  
  
nmap -sU -p 67 --script=dhcp-discover $host  
  
This command can be simply run by unauthorised attackers to gather information about a network.  
  
  
Risk Evaluation  
  
Based on the minimal impact and high likelihood for being exploited, the vulnerability has been categorised as a low vulnerability.   
  
  
Recommendation  
  
Remove any options that are not in use and apply filtering to keep the information off the network.

# Appendix

# Glossary