Infrastructure & Application Penetration Test
Company A

Version: 2.0

Author: John Smith

Document Control

Document Template

Document Status	Version	Date	Author	Section / Nature of Changes
Draft	0.1		John Smith	First Issue
Baselined	1.0		John Smith	Baselined Template

Document Change History

Document Status	Version	Date	Author	Section / Nature of Changes
Draft	0.1		John Smith	Initial draft from generic template
Draft	0.2		John Smith	Test details added
Draft	0.3		John Smith	Summary completed, sent for internal review
Draft	0.4		John Smith	Minor updates following internal feedback
Draft	0.5		John Smith	Sent for initial customer review
Draft	0.6		John Smith	Minor updates following customer review
Baselined	1.0		John Smith	Baselined following customer review

Related Documents

Document	Location	Status
Penetration Test Scope	Shared Drive	Baselined
Certificate of Authority	Shared Drive & Appendix 1	Baselined
Penetration Test Remediation Plan	Shared Drive	Draft

Document Classification

Due to the nature of the information held in this document is has been classified by Company A as **OFFICIAL-SENSITIVE** and should be processed in accordance with Company A’s **OFFICIAL-SENSITIVE** document guidelines.

Contents

1. Management Summary

SafeTest Computing Limited is pleased to present the findings for the recent Infrastructure Penetration Test conducted for Company A.

1.1 Overview and Scope

SafeTest Computing Limited was contracted by Company A to conduct a Penetration Test of the company's Infrastructure in accordance with the agreed Penetration Test Scope. The reason for the testing was to identify whether Company A's systems and consequently business reputation could be compromised if an unknown issue led to data loss and/or system compromise.

The tests were performed between the 1st and the 10th of April and carried out by John Smith as authorised in the Certificate of Authority in Appendix 1.

The testing included:

- Workstation review
- Server review
- Wireless access point review

The IP Addresses/IP Ranges within this test were as follows:
Workstations

- ◆ 192.168.220.100-192.168.220.229 (Dynamic DHCP)

Servers

- ◆ 192.168.220.1-192.168.220.99 (Static)

Wireless access points

- ◆ 192.168.220.230-192.168.220.254 (Static)

1.2 Caveats

The systems were part of a live infrastructure, so tests were made during business hours. Checks that would have a high risk of causing disruption were excluded. Denial Of Service (DOS) and Distributed Denial of Service (DDoS) were excluded for the same reason. A separate test will be made in an agreed period outside of working hours to resolve these issues.

1.3 Risk Ratings

SafeTest Computing has adopted the Common Vulnerability Scoring System (V2). CVSS is a free and open industry standard for assessing the severity of computer system security vulnerabilities. CVSS attempts to assign severity scores to vulnerabilities. This allows responders to prioritise responses and resources according to threat. The score SafeTest Computing will assign is based on the technical risk only. The business risk is the responsibility of Company A. It is not within the scope of this Penetration Testing. Not all vulnerabilities fall within the scope of CVSS. Where this is the case, vulnerabilities will be highlighted as 'Custom' and assigned a risk severity of Critical, High, Medium, Low or Information. Notes on the reasons for the rating will be provided.

The table below gives a key to the icons used in this report to identify risk severity:

Symbol	**Risk Rating**	**CVSSv2 Score Range**	**Explanation**
⊗	CRITICAL	9.0 to 10.0	A vulnerability has been discovered that is rated as CRITICAL. This could mean that the system may be exposed to a known exploit allowing catastrophic damage/data breach. Company A has advised that these issues need immediate resolution in < 3 days
⊖	HIGH	7.0 to 8.9	A vulnerability has been discovered that is rated as HIGH. This could mean that the system has known vulnerabilities which could expose the associated system allowing unauthorised access. This requires a resolution in the short term and Company A has agreed that these issues need to be resolved in < 25 days
❗	MEDIUM	4.0 to 6.9	A vulnerability has been discovered that is rated as MEDIUM. This could mean that the system has known medium level vulnerabilities linked to maintenance such as missing security patches. Company A has advised that these issues should be addressed as part of the next maintenance cycle, eg system patch updates
△	LOW	1.0 to 3.9	A vulnerability has been discovered that is rated as LOW. This could mean that the system has known low level vulnerabilities linked to maintenance such as missing security patches. Company A has advised that these issues should be addressed as part of the next maintenance cycle, e.g. system patch updates
✓	INFO	0 to 0.99	A vulnerability has been discovered that is rated as INFORMATIONAL. This could mean that the system is not following best practice and should be reviewed for appropriate action

1.4 Summary of Findings

The following table summarises the risks found during the test: -

Area	**Critical**	**High**	**Medium**	**Low**	**Total**
Workstations	2	1	0	0	3
Servers	1	1	0	0	2
Wireless access points	0	1	1	0	2
Totals:	3	3	1	0	7

Note: the above figures do not include Informational issues as these are not deemed an immediate threat

1.4.1 Key Findings

The following summary shows the key findings for each area of the test: -

1.4.2 Workstation Review

Area	Workstations	Overall Risk Rating	**CRITICAL**
1. The Windows version is 20H2 and has not been updated in some time, this should be updated ASAP. 2. The organisation makes use of TeamViewer which has not been updated in some time, this should be updated ASAP. 3. The workstations all have a local administrator account with both the username and password as “admin”, this should be resolved ASAP.			

1.4.3 Server Review

Area	Servers	Overall Risk Rating	**CRITICAL**
1. The server contains an install of a web based ticketing system which is used by the customer services team, this has not been updated for a while, and does appear to not have any access levels configured – all users have full administration rights to the database. 2. There are also a range of missing security patches that should be updated on the server ASAP and all other servers should be checked.			

1.4.4 Wireless Access Points Review

Area	Networking Equipment	Overall Risk Rating	**High**
1. The building contains a number of different Ubiquiti Unifi Access Points (UAP), running a variety of firmware versions, these should all be update to the latest version ASAP. 2. The UAPs do not have a guest network configured and all guests are joined to the main network, this should be resolved ASAP.			

1.5 Conclusion

1.5.1 Workstation Review

The workstations reviewed were significantly behind in version number. This means that a considerable number of significant security and performance updates are missing. These should be applied as soon as possible. The inspection also identified that there is an old version of TeamViewer installed on all the machines. This means that there are potential vulnerabilities. Inspection also showed that each of the workstations has a local administrator account which has both the username and password as “admin”.

1.5.2 Server Review

This server does not appear to have any different access levels so everyone has access to all tickets, can create and delete tickets at will and remove any evidence of records from the audit logs. This should be dealt with immediately. These servers are also not up to date and should be updated as soon as possible.

1.5.3 Networking Review

The building contains some different Wireless Access Points that have not been maintained and monitored. They are all running different firmware versions and should be updated as soon as possible. There is also only one network, which both internal staff and visitor's access. Separate networks should be established.

2. Detailed Findings

The following sections give a detailed technical view of each issue identified. There is also technical views of any commands/tools used and the tools output. The sections also contain recommendations to resolve any vulnerabilities found.

2.1 Generic Notes

Company A has provided the details of 38 Workstations, 5 Servers and 8 Wireless Access Points on the network to test. The IP Address range is divided up as follows: -

- Workstations: 192.168.220.100-192.168.220.229 (Dynamic DHCP)
- Servers: 192.168.220.1-192.168.220.99 (Static)
- Wireless access points: 192.168.220.230-192.168.220.254 (Static)

The server is acting as a Windows Active Directory (AD) controller, a Domain Name Systems (DNS) server and a Dynamic Host Configuration Protocol (DHCP) Server. The company has told SafeTest that these services are used throughout the company, so they are not in scope for testing as this may disrupt other services. These services will be covered in a separate, out of hours test covering a larger server pool. This will be scheduled at a later date.

2.2 Detailed Workstation Review

Workstations

We were not allowed to have a user login for the workstations so asked the IT Department to provide a list of patch levels for all of them.

The IT Department confirmed that: -

- All 38 workstations were created from the same image
- All 38 workstations were standard build containing and locked down with no additional software installs allowed
- Standard software installed is as follows: -
    - Microsoft Office 2019 standard (no MS Access)
    - Adobe Acrobat Reader
    - Google Chrome browser
    - Microsoft Teams
    - Microsoft OneDrive
    - OneNote for Windows 10
    - TeamViewer
- All patch management is managed via a central WSUS server with patches released manually
- All Workstations and Servers have their time set with an on-site Stratum 1 NTP server

Patch Levels

As no credentials were supplied for the Windows 10 clients, SafeTest Computing asked the IT Department to provide a list of all Windows 10 versions that are running on the workstations. The Windows 10 machines are running version 20H2 and have not been updated,

Risk Rating: ⊗ Critical
Risk Score: 9.1
Remediation Required: Within 3 days

Patch Levels

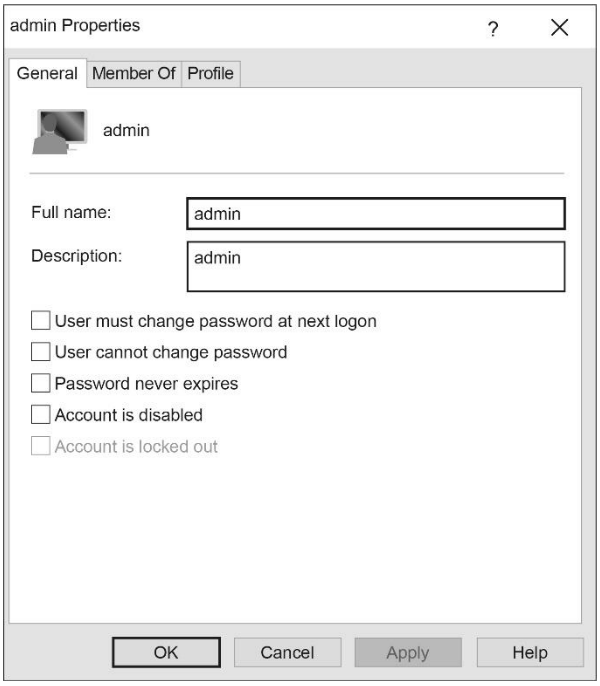
The version of TeamViewer (v12.0.259192) is severely outdated, it should either be updated or an alternative should be recommended to replace the remote access tool which is used for support across the organisation.

Risk Rating: ⊖ High
Risk Score: 7.5
Remediation Required: Within 25 days

Patch Levels

The workstations all have a local administrator account which has the username and password of “admin”.

Risk Rating: ⊗ Critical
Risk Score: 9.5
Remediation Required: Within 3 days



admin Properties

admin

Full name: admin

Description: admin

□ User must change password at next logon
□ User cannot change password
□ Password never expires
□ Account is disabled
□ Account is locked out

2.3 Detailed Server Review

Server

There are 5 Windows 2019 Servers with host names of Server, Fileserver, Backup, CRM1 and Finance. The IP addresses are as follows:

Server	192.168.220.10
Fileserver	192.168.220.18
Backup	192.168.220.21
CRM1	192.168.220.27
Finance	192.168.220.29

Patch Levels

As no credentials were supplied for the Windows Servers, SafeTest Computing asked the IT Department to provide a list of all Windows Server 2019 patches that had been applied to all servers.

There was a number of different security patches that were missing from the server, these should be installed:

Title	Classification	Date	Size
2023-03 Cumulative Update Preview for .NET Framework 3.5 and 4.8 for Windows Server 2019 for x64 (KB5023702)	Updates	14/03/2023	153.9MB
2023-02 Cumulative Update for Windows Server 2019 for x64-based Systems (KB5022840)	Security Updates	14/02/2023	499.5MB
2023-01 Servicing Stack Update for Windows Server 2019 for x64-based Systems (KB5022286)	Critical Updates	10/01/2023	13.7MB
Azure File Sync Agent v11.3 Release – April 2022 (KB4539953)	Update Rollups	07/04/2022	42.6MB

Risk Rating: ⊖ High
Risk Score: 8.1
Remediation Required: Within 25 days

Exploits

All servers were scanned and CRM1 with IP address 192.168.220.27 showed the following potential vulnerability that was investigated further: -

Risk Rating: ⊗ Critical
Risk Score: 9.7
Remediation Required: < 3 days

SuiteCRM is running on Version 7.11.6 which was released on 1st July 2019 and has not been updated since, release notes can be found here.

This is now running considerably behind the current version and has had a significant number of security updates since then.

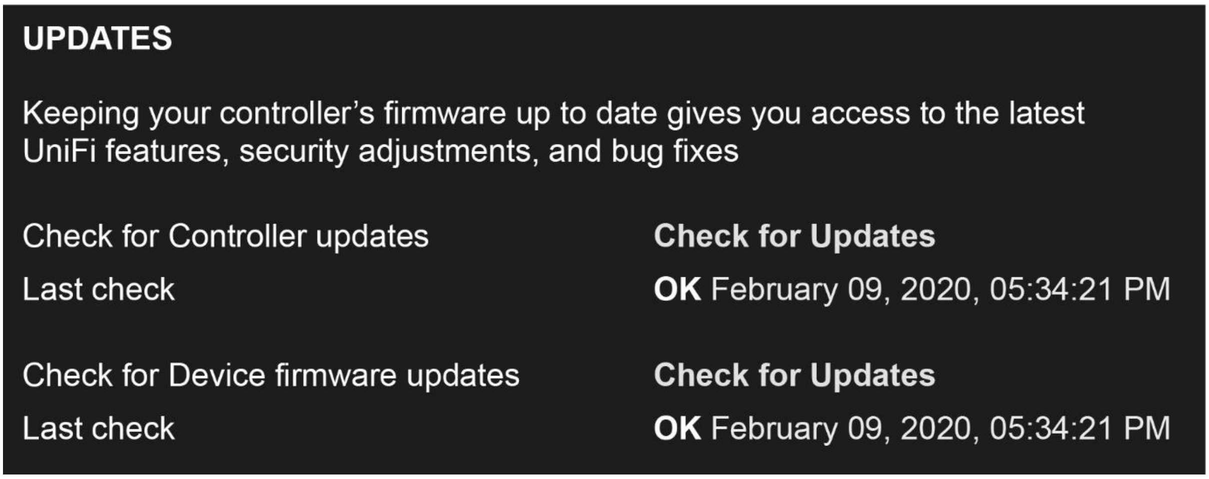
2.4 Wireless access points Review

Wireless access points

There are 8 Ubiquiti Wireless Access Points (UAC-AC-PRO) connected to the network (they sit in the IP address range 192.168.220.230-192.168.220.254 (Static)).

When connected to this network it was identified that the last time the Firmware was updated was 9th February 2020, there has been a significant number of updates since and means that these access point could have a number of various vulnerabilities.

Risk Rating: ⊖ High
Risk Score: 7.2
Remediation Required: Within 25 days



UPDATES

Keeping your controller's firmware up to date gives you access to the latest UniFi features, security adjustments, and bug fixes

Check for Controller updates — **Check for Updates**
Last check — **OK** February 09, 2020, 05:34:21 PM

Check for Device firmware updates — **Check for Updates**
Last check — **OK** February 09, 2020, 05:34:21 PM

There are 8 Ubiquiti Wireless Access Points (UAC-AC-PRO) connected to the network (192.168.220.230-192.168.220.254 (Static)).

Inspection showed that that there was only one network established – an internal staff network. There is no guest network. This means that guests have been connected to the internal network, which has not had its security changed since 9th February 2020.

Risk Rating: ❗ Medium
Risk Score: 6.1
Remediation Required: Within 25 days