Infrastructure & Application Penetration Test
KJR Solicitors

Version: 1.1

Author: Jaimie Morrison

16 November 2023

Document Control

Document Template

Document Status	Version No.	Date	Author	Section / Nature of Change
Draft	0.1	-	Jaimie Morrison	First issue
Baselined	1.0	15/12/2022	Jordan Smyth	Baselined Template

Document Change History

Status	Version #	Date	Author (optional)	Section / Nature of Change
Draft	0.1	07/12/2022	Jaimie Morrison	Initial draft from generic template
Draft	0.2	08/12/2022	Jaimie Morrison	Test details added
Draft	0.3	08/12/2022	Jaimie Morrison	Summary completed, sent for internal review
Draft	0.4	09/12/2022	Jaimie Morrison	Minor updates following internal feedback
Draft	0.5	10/12/2022	Jaimie Morrison	Sent for initial customer review
Draft	0.6	14/12/2022	Jaimie Morrison	Minor updates following customer review
Baselined	1.0	15/12/2022	Jaimie Morrison	Baselined following customer review
Updated	1.1	16/11/2023		Sample added as a watermark

Related Documents

Document	Location	Status
Penetration Test Scope	Shared Drive	Baselined
Certificate of Authority	Shared Drive & Appendix 1 below	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 KJR Solicitors as **OFFICIAL-SENSITIVE** and should be processed in accordance with KJR Solicitors **OFFICIAL-SENSITIVE** document guidelines.

Contents

1. Management Summary

PenComp Computing Limited is pleased to present the findings for the recent Infrastructure Penetration Test conducted for KJR Solicitors.

1.1 Overview and Scope

PenComp Computing Limited was contracted by KJR Solicitors to conduct a Penetration Test of the companies Infrastructure in accordance with the agreed Penetration Test Scope. The reason for the testing was to identify whether KJR Solicitors 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 01/12/2022 and 06/12/2022 and carried out by Jaimie Morrison as authorised in the Certificate of Authority in Appendix 1.

The testing included: -

- Server review
- Workstation review
- HP Printer review
- Epson Printer Review

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

Workstations

- 192.168.220.100-192.168.220.167 (Dynamic DHCP)

Servers

- 192.168.220.1-192.168.220.99 (Static)

Epson Printers

- 192.168.220.230-192.168.220.254 (Static)

Hewlett Packard Printers

- 192.168.220.254-192.168.220.260 (Static)

1.2 Caveats

As the systems in question were part of a live infrastructure and the testing was carried out during business hours, checks that would have an elevated risk of causing disruption were excluded. Denial Of Service (DOS) and Distributed Denial of Service (DDOS) were excluded for the same reason, and these will be addressed in a separate test which will be conducted during an agreed period outside of working hours.

1.3 Risk Ratings

PenComp Computing Limited 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, allowing responders to prioritize responses and resources according to threat.

It should be noted that the score PenComp Computing Limited will assign is based upon the risk from a technical standpoint, assessing the overall business impact of any risk found is the responsibility of KJR Solicitors and falls outside the scope of this Penetration Testing.

Not all vulnerabilities fall within the scope of CVSS and where this is the case they will be highlighted as 'Custom' and assigned a risk severity of Critical, High, Medium, Low or Information with notes on the reasons for the rating.

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. KJR Solicitors 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 KJR Solicitors 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. KJR Solicitors has advised that these issues should be addressed as part of the next maintenance cycle, e.g., 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. KJR Solicitors 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/Laptops	0	12	1	0	13
Servers	0	4	0	0	4
HP Printers	1	0	0	0	1
Totals:	1	16	1	0	18

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:	⛔High

1. There are 12 missing security patches that should be updated on all workstations and laptops ASAP
2. There is a physical security risk, with access to data possible

1.4.3 Server Review

Area:	Servers	Overall Risk Rating:	⛔High

1. There are 4 missing security patches that should be updated on the server ASAP and all other servers should be checked.

1.4.4 HP Printer Review

Area:	HP Printers	Overall Risk Rating:	⊗Critical

1. Printers not updated with latest firmware, creating vulnerability for potential remote access to local network

1.5 Conclusion

1.5.1 Workstation Review

The workstations reviewed were missing 12 critical security patches which need to be applied ASAP. In addition, physical security on site was not adequate. Access without challenge was possible with access to computer systems and USB devices possible in a short time period.

1.5.2 Server Review

The server was missing 4 critical security patches which need to be updated ASAP.

1.5.3 Printer Review

A critical threat identified regarding the firmware installed on Hewlett Packard printers leaves devices with remote access vulnerability. Recommend a system update along with update schedule created to prevent further vulnerabilities.

1.5.4 Next Steps

1.5.4.1 Immediate / Short Term

- Security patches for both Microsoft Server and Windows 10 should be applied as recommended. In addition, a review of the Patch Management process and toolset should be undertaken to ensure critical patches are applied in a timely manner.
- Device drivers on all Servers and Workstations should be reviewed for any potential exploits and updated in the patch management cycle where appropriate.
- Hewlett Packard printers to have immediate updates run for firmware.

1.5.4.2 Medium / Long Term

- All staff to be retrained on IT security, with an emphasis on physical checks and challenge
- Education provided on data security
- Staff involved in the vulnerability test to be provided with immediate remedial training

2. Detailed Findings

The following sections give a detailed technical view of each issue encountered including any commands/tools used along with the tools output. They also contain recommendations to resolve any vulnerabilities found.

2.1 Generic Notes

KJR Solicitors has provided the details of 67 Workstations/Laptops, 1 Server and 5 Printers on the network to test. The IP Address range is divided up as follows: -

Servers and Switches: 192.168.220.1-192.168.220.99 (Static)
Workstations: 192.168.220.100-192.168.220.344 (Dynamic DHCP)
Printers and Network Devices: 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. PenComp Computing Limited have been advised that, as these services are used throughout the company, they are not in scope for testing due to potential disruption to other services. They will be covered in a separate, out of hours test covering a larger server pool to be scheduled later.

2.2 Detailed Workstation Review

Workstations

We were not allowed to have a user login for the workstations/laptops so asked the IT Department to provide a list of patch levels for all 67 of them. The IT Department confirmed that: -

- All 64 workstations were created from the same image
- All 64 workstations were standard build containing and locked down with no additional software installs allowed
- All 3 Laptops were created from the same image
- All 3 Laptops were standard build containing and locked down with no additional software installs allowed
- Standard software installed is as follows: -
- Microsoft Office 365 standard (no MS Access)
- MS Teams 365
- Adobe Acrobat Reader
- Firefox browser
- Google Chrome Browser
- Microsoft OneDrive
- OneNote for Windows 10
- Trend Micro Maximum Security
- TeamViewer
- All patch management is managed via a central WSUS server with patches released manually
- An Epson Universal Print Driver is used for printer connectivity
- An Hewlett Packard Print Driver is used for printer connectivity
- All Workstations, Laptops 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, PenComp Computing Limited asked the IT Department to provide a list of all Windows 10 patches that had been applied to the workstations. The following critical patches seem to be missing: -

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

2022-03 Dynamic Update for Windows 10 Version 21H1 for x64-based Systems (KB5011577)	Windows 10 Dynamic Update,Windows Safe OS Dynamic Update
2022-03 Dynamic Update for Windows 10 Version 21H2 for x64-based Systems (KB5011577)	Windows 10 Dynamic Update,Windows Safe OS Dynamic Update
2022-03 Dynamic Update for Microsoft server operating system for x64-based Systems (KB5011653)	Windows 10 Dynamic Update
2022-03 Dynamic Update for Microsoft server operating system for x64-based Systems (KB5011578)	Windows 10 Dynamic Update,Windows Safe OS Dynamic Update
2022-03 Dynamic Update for Windows 10 Version 20H2 for x64-based Systems (KB5012419)	Windows 10 Dynamic Update,Windows Safe OS Dynamic Update
2022-03 Dynamic Update for Windows 10 Version 21H2 for x64-based Systems (KB5012419)	Windows 10 Dynamic Update,Windows Safe OS Dynamic Update
2022-03 Dynamic Update for Windows 10 Version 21H1 for x64-based Systems (KB5012419)	Windows 10 Dynamic Update,Windows Safe OS Dynamic Update
2022-03 Dynamic Update for Microsoft server operating system for x64-based Systems (KB5012415)	Windows 10 Dynamic Update,Windows Safe OS Dynamic Update
2022-02 Dynamic Update for Windows 10 Version 20H2 for x64-based Systems (KB5010524)	Windows 10 Dynamic Update
2022-02 Dynamic Update for Windows 10 Version 21H1 for x64-based Systems (KB5010524)	Windows 10 Dynamic Update
2022-02 Dynamic Update for Windows 10 Version 21H2 for x64-based Systems (KB5010524)	Windows 10 Dynamic Update
2022-02 Dynamic Update for Microsoft server operating system for x64-based Systems (KB5010454)	Windows 10 Dynamic Update

Recommended Actions

1. The above patches are downloaded, tested and if OK applied to the Server ASAP
2. As the workstation patching is manually distributed via WSUS it is recommended that the patch management process including WSUS are revised to ensure patches are applied in a timely manner

Physical Security Vulnerability Test

Risk Rating: ❗ Medium
Risk Score: 5.3
Remediation Required: Within 3 months

As the workforce have transitioned in part to a remote working environment, it was appropriate to determine the knowledge and security consciousness of staff. As staff members were recruited during the last two years – many staff members have not been introduced to each other and there may be vulnerability on site in gaining access to systems and data.

The test involved 2 members of PenComp attempting to access the office, and to remove digital storage devices whilst on site. The employees would not wear any name tags or security passes – if challenged they would immediately identify themselves and report to IT.

The PenComp staff were instructed to follow staff members into the office, and to walk around the location and attempt to:

- Gain access to server room
- Remove USB storage devices
- Identify and stand next to a PC open for 30 seconds
- Any other breaches of opportunity.

No material was to leave the office, and they are expected to report to IT after the test and hand over anything gathered.

The results:

Both employees were able to gain access to the site (North East office) at midday without any challenge

1 USB device was removed from an employees desk (Handed to IT)

3 x Computers were left unlocked – PenComp was able to stand next to the PC's in question for extended period of time – in one case for 10 minutes before it locked

No access to the server room was possible – magnetic locks in place.

This shows that there is a vulnerability in the decision making of employees and their understanding of data security. Leaving significant vulnerabilities on site of physical access to systems and data possible.

Recommended Actions

1. All staff to be retrained on IT security, with an emphasis on physical security
2. Education provided on data security
3. Staff to be provided with security passes and automatic locking system implemented on site
4. Staff involved in the vulnerability test to be provided with immediate remedial training

2.3 Detailed Server Review

Server Build Review

There are 3 X Windows 2019 Servers with a host name of CCR01, CCR02, CCR03 with IP addresses as follows: -

CCR01	192.168.220.10
CCR02	192.168.220.16
CCR03	192.168.220.19

Patch Levels

As no credentials were supplied for the Windows Server PenComp Computing Limited asked the IT Department to provide a list of all Windows Server 2019 patches that had been applied to all servers. The following critical patches seem to be missing: -

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

2022-04 Cumulative Update Preview for .NET Framework 3.5, 4.7.2 and 4.8 for Windows Server 2019 for x64 (KB5012796)	Updates	4/21/2022
2022-04 Cumulative Update Preview for .NET Framework 3.5 and 4.7.2 for Windows Server 2019 for x64 (KB5012162)	Updates	4/21/2022
2022-04 Cumulative Update Preview for Windows Server 2019 for x64-based Systems (KB5012636)	Updates	4/21/2022
2022-04 Cumulative Update Preview for .NET Framework 3.5 and 4.8 for Windows Server 2019 for x64 (KB5012158)	Updates	4/21/2022

Recommended Actions

1. The above patches are downloaded, tested and if OK applied to the server ASAP
2. As the servers seems to have missed patching since initial build and deployment it is either missing from patch management or patch management is not centralised
3. If patch management is available all servers should be added and updated
4. If a patch management system is not deployed consideration should be given to deploying an in-built Windows solution such as Windows Server Update Service (WSUS) which is a free to deploy service for managing updates

2.4 Detailed Printer Review

Epson and Hewlett Packard Printers

There are 2 X Epson Workforce WF2845-DF LaserJet Colour printers, and 3 x Hewlett Packard HP Colour LaserJet Enterprise CM4540 MFP

PenComp Computing Limited were given the IP addresses for all printers (192.168.220.230-192.168.220.254 (Static)).

CVE-2022-3942

Certain HP Print products and Digital Sending products may be vulnerable to potential remote code execution and buffer overflow with use of Link-Local Multicast Name Resolution or LLMNR.

Risk Rating: ⊗ Critical
Risk Score: 8.4
Remediation Required: < 3 days

Access

It was noted that Epson printers are up to date, but HP printers have not been updated since January 2021 – critical update requires that immediate firmware security updates are completed.

Recommended Actions

1. Printers should be immediately updated
2. Regular firmware checks completed with agreed schedules.