INTERNAL PENETRATION
TEST REPORT

[REDACTED] Infrastructure Assessment: Azure VM Environment

Prepared by:	Aussie Pentest Pty Ltd
Prepared for:	■■■■■■■■■■ - Client (Confidential)
Report Date:	■■ ■■■■ ■■■■
Assessment Type:	Internal Black-Box Penetration Test
Scope:	■■■■■■■■■■■■■■■ (■■.■■.■.■) | ■■■■■■■■■■■■■■■ (■■.■■.■.■)
Classification:	CONFIDENTIAL

Table of Contents

1. Executive Summary

Aussie Pentest Pty Ltd was engaged to conduct an internal penetration test against two Azure-hosted Windows virtual machines operated by the client. The assessment was conducted under a black-box, zero-credential methodology with no pre-supplied passwords or network diagrams. Testing was performed remotely via remote sessions on both target machines, with a strict constraint prohibiting file transfers or service interruption.

The assessment identified 10 findings across both hosts, including 3 Critical and 2 High severity issues. The most significant finding was the presence of a security event monitoring platform on both hosts accessible using default guest credentials, allowing unauthenticated access to security event data. Both machines exhibited identical misconfigurations, indicating a systemic absence of security hardening standards across the environment.

No sensitive data was exfiltrated, no services were disrupted, and all testing activity was conducted within the agreed scope. The client is advised to prioritise remediation of credential and access control findings before any further exposure of these systems to internal or external networks.

Critical	3	Requires Immediate Action
High	2	Requires Prompt Action
Medium	4	Requires Scheduled Action
Low	1	Requires Monitoring

2. Engagement Overview

Engagement Type	Internal Black-Box Penetration Test
Test Period	■■ ■■■■ ■■■■
Testing Method	Remote Sessions
Credentials Provided	None (Zero Credential Assessment)
File Transfers	Prohibited per client rules of engagement
Service Disruption	Prohibited per client rules of engagement
Tester	Aussie Pentest Pty Ltd

3. Scope & Rules of Engagement

In Scope Targets

■■■■■■■■■■■■■■■	■■.■■.■.■	■■.■■.■.■	Windows Server 2019 Datacenter
■■■■■■■■■■■■■■■	■■.■■.■.■	■■.■■.■.■	Windows Server 2019 Datacenter

Rules of Engagement

• No files unrelated to scanning may be transferred to target systems.

• No running services or programs may be stopped during testing.

• Testing confined to the two specified virtual machines only.

• Client to be notified immediately of any critical findings.

• All activity to be conducted via approved remote sessions.

4. Methodology

Testing followed a structured internal penetration testing methodology aligned with industry standards. Given the zero-credential, no-file-drop constraints, the assessment relied entirely on built-in Windows tooling (Living off the Land) and manual analysis.

Phase 1: Reconnaissance

Host discovery, network mapping, OS fingerprinting and service enumeration using native Windows commands (ipconfig, netstat, net commands, ping, arp).

Phase 2: Enumeration

Service-specific enumeration including SMB share enumeration, user account discovery, port scanning via PowerShell, and credential store inspection.

Phase 3: Vulnerability Analysis

Manual identification of misconfigurations, default credentials, legacy protocols, unpatched services, and privilege escalation vectors.

Phase 4: Exploitation

Attempted exploitation of identified vulnerabilities within scope constraints. Included default credential testing, UAC bypass attempts, SMB null session testing, and registry-based credential hunting.

Phase 5: Post-Exploitation

Privilege escalation attempts, lateral movement testing between VMs, and credential harvesting via native Windows mechanisms.

Phase 6: Reporting

Documentation of all findings with evidence, CVSS scoring, and prioritised remediation recommendations.

5. Risk Rating Matrix

Critical	9.0 – 10.0	Immediate exploitation risk. Direct path to full compromise or data breach.
High	7.0 – 8.9	Significant risk requiring prompt remediation. Could lead to serious compromise.
Medium	4.0 – 6.9	Moderate risk. Exploitation requires specific conditions but remains a concern.
Low	0.1 – 3.9	Minimal direct risk. Informational value or requires significant preconditions.
Info	N/A	Observation with no direct exploitability. Provided for awareness.

6. Findings Summary

F01	Default Guest Credentials Active on Monitoring Platform (Both Hosts)	Both	Critical	9.8
F02	Legacy Remote Login Protocol Enabled (Port 513)	[REDACTED]	Critical	9.1
F03	Remote Management Protocols Exposed Internally	Both	Critical	9.1
F04	Administrative Shares Exposed (C$, D$, F$, ADMIN$)	[REDACTED]	High	7.2
F05	Account Lockout Triggered — Weak Lockout Policy	[REDACTED]	High	7.5
F06	Unrestricted User Enumeration via Net Commands	Both	Medium	6.5
F07	No Network Segmentation Between VMs	Both	Medium	6.5
F08	Monitoring Platform DB Password Hash Recoverable	[REDACTED]	Medium	5.5
F09	Database Running Without Authentication	Both	Medium	6.2
F10	Windows Server 2019 — Minimal Patch Coverage	[REDACTED]	Low	3.7

7. Detailed Technical Findings

FINDING 01 | Default Guest Credentials Active on Monitoring Platform (Both Hosts)			Critical CVSS 9.8
Affected Host	[REDACTED] (■■.■■.■.■) | [REDACTED] (■■.■■.■.■)	**CVSS Score**	9.8
CVSS Vector	`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H`		

Description

A security event monitoring platform was found running on both target hosts on TCP port 8400. Authentication was successful on both instances using the factory-default guest credentials with no modification required. These default credentials are shipped with the product and should be disabled or changed immediately upon deployment. Both instances granted dashboard access exposing collected Windows event data, device information, security alerts configuration, and system logs.

Technical Detail

```
[REDACTED HOST 1]: http://localhost:8400 — guest/guest login successful, dashboard shows 294K Windows events, 6,106 failure events. [REDACTED HOST 2]: http://localhost:8400 — guest/guest login successful, isolated instance. Both running as java.exe service with PostgreSQL backend on port 33335.
```

Evidence

Screenshots confirm successful guest login on both hosts, with dashboards exposing event counts, device lists, and security overview panels. [Screenshots withheld from redacted version]

Recommendation

Immediately disable the guest account in the monitoring platform on both hosts (Settings > User Management > Guest > Disable). Change the default admin password to a strong unique password. Restrict access to port 8400 via Windows Firewall to authorised IP addresses only.

FINDING 02 | Legacy Remote Login Protocol Enabled (Port 513)			Critical CVSS 9.1
Affected Host	[REDACTED] (■■.■■.■.■)	**CVSS Score**	9.1
CVSS Vector	`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N`		

Description

TCP port 513 (Rlogin) was found listening on the gateway host, bound to all interfaces. Rlogin is a legacy Unix remote login protocol designed for trusted host environments with weak or no authentication in many implementations. It transmits credentials in cleartext and can allow host-trust-based authentication bypass. Its presence on a Windows Server 2019 gateway machine is anomalous and represents a significant attack surface. The responsible process was identified as a ManageEngine System Event Collector service component.

Technical Detail

```
TCP 0.0.0.0:513 LISTENING PID [REDACTED]. tasklist identifies [REDACTED].exe. Port 514 (Syslog) also bound by same process.
```

Evidence

netstat -ano output confirms TCP 0.0.0.0:513 LISTENING. tasklist identifies process as system service component. Screenshot captured. [Screenshots withheld from redacted version]

Recommendation

Investigate why the system event collector service is binding to port 513. If Rlogin functionality is not required, disable it within the platform configuration. Block port 513 at both Windows Firewall and Azure NSG level.

FINDING 03 | Remote Management Protocols Exposed Internally on Both Hosts			Critical CVSS 9.1
Affected Host	Both Hosts	**CVSS Score**	9.1
CVSS Vector	`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N`		

Description

Remote Desktop Protocol (3389), Windows Remote Management (5985/5986), and SSH (22) are all listening on both hosts with no evidence of IP-based access restrictions. While blocked at the Azure NSG level externally, any compromise of either VM provides immediate lateral movement capability to the other via these protocols.

Technical Detail

```
Running netstat -ano on both hosts confirmed TCP 0.0.0.0:22, 0.0.0.0:3389, 0.0.0.0:5985, 0.0.0.0:5986, and 0.0.0.0:47001 were all in a LISTENING state. Internal reachability between hosts verified via PowerShell Test-NetConnection.
```

Evidence

Network port scan output confirms all remote management ports listening. [Screenshots withheld from redacted version]

Recommendation

Restrict RDP, WinRM and SSH to specific management IP addresses using Windows Firewall with Advanced Security rules. Enable Network Level Authentication (NLA) for RDP. Consider implementing a bastion server pattern for all remote management access.

FINDING 04 | Administrative Shares Exposed (C$, D$, F$, ADMIN$)			High CVSS 7.2
Affected Host	[REDACTED] (■■.■■.■.■)	**CVSS Score**	7.2
CVSS Vector	`CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H`		

Description

The net share command revealed that Windows default administrative shares C$, D$, F$, and ADMIN$ are active and exposed on the internal host. These shares provide full filesystem access to any account with local administrator credentials. The presence of three drive shares indicates multiple storage volumes are accessible via this vector.

Technical Detail

```
net share command returned C$ (C:\), D$ (D:\), F$ (F:\) as Default shares and ADMIN$ (C:\Windows) as Remote Admin. All four administrative shares confirmed active.
```

Evidence

net share command output confirms all administrative shares active. [Screenshots withheld from redacted version]

Recommendation

Disable default administrative shares if not required by setting AutoShareServer=0 in the registry at HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters. If shares are required, restrict access via host-based firewall rules to authorised management IPs only.

FINDING 05 | Account Lockout Triggered — Weak Lockout Policy			High CVSS 7.5
Affected Host	[REDACTED] (■■.■■.■.■)	**CVSS Score**	7.5
CVSS Vector	`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N`		

Description

During SMB enumeration attempts against the gateway host, System Error 1909 was returned indicating that a referenced account had been locked out. This confirms that automated or repeated authentication attempts against the gateway can result in account lockouts, potentially enabling a denial-of-service condition against administrator accounts.

Technical Detail

```
Commands net use Z: \\[REDACTED]\C$ and net use Z: \\[REDACTED]\ADMIN$ both returned System error 1909: The referenced account is currently locked out.
```

Evidence

Error 1909 returned on both net use commands to gateway host, confirming the account lockout state. [Screenshots withheld]

Recommendation

Review and configure the account lockout policy via Group Policy. Implement account lockout alerting via the security monitoring platform. Consider implementing an intrusion detection mechanism to alert on repeated failed authentication attempts.

FINDING 06 | Unrestricted User Enumeration via Net Commands			Medium CVSS 6.5
Affected Host	Both Hosts	**CVSS Score**	6.5
CVSS Vector	`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N`		

Description

The net user and net localgroup administrators commands returned full user account listings without requiring elevated privileges. Multiple user accounts were enumerated on both hosts including standard users and an administrative account. The administrative account was identified as a local administrator on both machines, providing a high-value target for credential-based attacks.

Technical Detail

```
net user and net localgroup administrators executed successfully on both hosts, returning full account listings.
```

Evidence

All accounts and group memberships documented. [Screenshots withheld from redacted version]

Recommendation

Implement a naming convention for admin accounts that does not reveal privileged status. Consider enabling Windows Firewall rules to restrict SMB and RPC access to authorised hosts only. Ensure the Guest account is disabled on both machines.

FINDING 07 | No Network Segmentation Between Virtual Machines			Medium CVSS 6.5
Affected Host	Both Hosts	**CVSS Score**	6.5
CVSS Vector	`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N`		

Description

Both virtual machines reside on the same /24 subnet with unrestricted IP-level communication between them. Full ICMP reachability was confirmed in both directions with sub-millisecond response times. There are no host-based firewall rules or Azure NSG rules preventing lateral movement between the two machines.

Technical Detail

```
Ping from Host 1 to Host 2 returned 4/4 packets with 1ms average RTT. Ping from Host 2 to Host 1 also returned 4/4 packets. A PowerShell port scan confirmed all internal services reachable between hosts.
```

Evidence

ICMP connectivity and port scan results confirm unrestricted VM-to-VM communication. [Screenshots withheld]

Recommendation

Implement Azure NSG rules to restrict traffic between the two VMs to only required ports and protocols. Deploy host-based Windows Firewall rules on each VM. Consider placing each VM in separate virtual network subnets with controlled routing.

FINDING 08 | Monitoring Platform DB Password Hash Recoverable from Config File			Medium CVSS 5.5
Affected Host	[REDACTED] (■■.■■.■.■)	**CVSS Score**	5.5
CVSS Vector	`CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N`		

Description

The monitoring platform database configuration file was readable by the standard user account. This file contained the PostgreSQL database username and a SHA-256 derivative password hash. Access to this file by unprivileged users could allow offline password cracking attempts.

Technical Detail

```
File: C:\[REDACTED]\conf\database_params.conf Username: [REDACTED] | Hash: [REDACTED SHA-256 HASH] |
DB: jdbc:postgresql://127.0.0.1:33335/eventlog
```

Evidence

The type command was run against the config file and returned database credentials including username and hash. File accessible without elevated privileges. [Screenshots withheld]

Recommendation

Restrict read permissions on monitoring platform configuration files to the service account only. Rotate the database password and use a strong randomly generated value. Consider encrypting sensitive configuration files.

FINDING 09 | Database Running Without Confirmed Authentication			Medium CVSS 6.2
Affected Host	Both Hosts	**CVSS Score**	6.2
CVSS Vector	`CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N`		

Description

Port 27019 (MongoDB default port) was identified listening on the loopback interface on both hosts. MongoDB instances have historically shipped without authentication enabled by default. While bound to localhost only, any process running on either machine could potentially connect and access all stored data without credentials.

Technical Detail

```
Output from netstat -ano on both hosts shows TCP 127.0.0.1:27019 LISTENING. On the gateway host the
process was identified as a platform service component (PID [REDACTED]). Evidence was documented
during the session.
```

Evidence

netstat output confirms MongoDB listening on loopback on both hosts. [Screenshots withheld from redacted version]

Recommendation

Confirm whether MongoDB authentication is enabled. If disabled, enable it immediately and create strong credentials. Review what data is stored and assess sensitivity. Ensure MongoDB remains bound to localhost only.

FINDING 10 | Windows Server 2019 — Limited Patch Coverage on Gateway			Low CVSS 3.7
Affected Host	[REDACTED] (■■.■■.■.■)	**CVSS Score**	3.7
CVSS Vector	`CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N`		

Description

The gateway host was found running Windows Server 2019 Datacenter (Build 17763) with only 11 hotfixes installed. Windows Server 2019 has received numerous security patches since release and a minimal patch count may indicate the system is not being regularly updated.

Technical Detail

```
systeminfo output shows Hotfix(s): 11 Hotfix(s) Installed. OS Build 17763 confirmed as Windows Server 2019.
```

Evidence

systeminfo output confirms 11 hotfixes installed. OS Build 17763 confirmed as Windows Server 2019. [Screenshots withheld]

Recommendation

Implement a regular patch management process for both VMs. Enable Windows Update or configure WSUS. Run a full authenticated vulnerability scan to identify specific missing patches and CVEs.

---

8. Remediation Recommendations

The following table provides a prioritised remediation roadmap ordered by severity and ease of implementation.

1 – Immediate	Disable monitoring platform guest account on both hosts	Low	Both
2 – Immediate	Change all monitoring platform default passwords	Low	Both
3 – Immediate	Disable legacy Rlogin (port 513) in service configuration	Low	[REDACTED]
4 – This Week	Restrict RDP/WinRM/SSH to management IPs via Firewall	Medium	Both
5 – This Week	Disable administrative shares if not required	Low	[REDACTED]
6 – This Week	Review and configure account lockout policy	Low	Both
7 – This Month	Implement NSG rules to segment VM-to-VM traffic	Medium	Both
8 – This Month	Restrict config file permissions on monitoring platform	Low	[REDACTED]
9 – This Month	Enable database authentication and audit stored data	Medium	Both
10 – Scheduled	Deploy full patch management process	High	Both

9. Conclusion

The internal penetration test of the client Azure VM environment identified a range of security weaknesses spanning both target hosts. The most critical finding — default monitoring platform credentials active on both machines — represents an immediate risk requiring remediation before any further use of these systems in a production or sensitive data context.

The consistency of findings across both machines indicates that security hardening was not applied as part of the initial deployment process. The environment would benefit from a structured hardening baseline aligned with CIS Benchmarks for Windows Server 2019, combined with regular vulnerability scanning and patch management.

Aussie Pentest recommends a follow-up assessment following remediation of the identified Critical and High findings to validate that controls have been implemented effectively. We are available to assist with remediation guidance, verification testing, or any questions arising from this report.