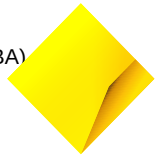
Vulnerability Scanning – Technical Scope

Table of Contents



1. Introduction

Vulnerability Management enables the Group to obtain information, evaluate and act upon security vulnerabilities within our environments. Vulnerability Scanning, is an automated service which scans Systems and Services to identify potential vulnerabilities, missing patches, and misconfigurations that adversely affect the security posture of the Group.

The IS Vulnerability Management Standard defines the scope of the Groups Vulnerability Scanning to include and define “Network Addressable” Systems and Services. However, the exact scanning methods, asset types, context are subject to revision and provided and in this document.

This document is based on Systems and Services currently used by the Group, significant changes to the Group’s use of technology may require amendments to this Technical Scope document.

2. Assets Classification

For the purposes of Vulnerability Scanning Systems and Services are categorised based on their technical characteristic into the following asset types for Vulnerability Management activities. This is agnostic of the Inventory used (i.e. is not aligned to CMDB or ServiceNow subtypes)

Type	Type Definition	Subtypes	Properties	Examples
Device	A devices consists of computer (virtualised or physical) with an **Operating System** (potential in firmware) instance **distinct** from any other device**.** Typically scanning will occur via primary or management IP address.	**Server**	Server device are intended to be modified to provide arbitrary business or technical services over a network.	Servers, Amazon EC2 instance, server virtual machine, mid-range, mainframes.
		Other Appliance	An appliance is designed for a single function, typically with specialised hardware, and has a restricted software-layer that not intended for reprograming for another purposes.	Telephony devices (IP phones), Smart Boards, Building Alarm and Control Systems, Printers, Storage devices, Lights Out Management System, HSMs, and most Virtual Appliances, Internet of Things (IoT).
		Network Appliance	Appliances that are provide functions specifically related to the filtering, manipulation, and transmission of network traffic.	Firewall, load balancer, wireless access point, Network Access Control device, switch, modem, router, proxy.
		Workstation End-user	End-user computing including laptops, desktops and virtualised desktop infrastructure.	Windows 10 end-user workstation, Mac OS X laptop, VDIs.
		Public End-user	Computing hardware provisioned for restricted physical access by the public.	ATM, Kiosk.
		Managed End-User	Tightly restricted/managed end-user devices, with comprehensive central control and monitoring of key configuration and security controls.	Microsoft Managed Desktop or MDM managed mobile, and tablet devices.
Application Endpoint	Network addresses (including URIs) that expose an application, or service with an additional address to the devices. Some end-point will not have a device at all (SaaS/Cloud Native/Container hosted service).	**Internal Endpoint**	The Service can only be reached from internal (controlled/restricted networks)	Examples include HTTP virtual hostnames (https://confluence.prod.cba/), Cloud Native database, applications exposed via a load balancer.
		External Endpoint	Services are accessible from the Internet, or via a public multi-party network. Services may be considered external even if internet traffic passes via intermediate assets if the data transferred is not substantially transformed in the process.	An external load balancer Virtual IP (VIP), Internet-facing Cloud Service, external HTTP hostname (http://www.commbank.com.au)
Container	A container provides code isolation within the operating systems of a device.	**Container**	A partially isolated virtualised software environment, without a fully-independent operating system of its own.	Docker Container or Solaris Zone.

Table 1 Classification of Assets for Vulnerability Management

3. Scan Method Definitions

3.1 Types of Scans

3.1.1 Remote Scan

Remote Scans are performed over a network without privileged access to the underlying system.

Remote Scans can be performed against network addresses making it suitable for asset types with a fixed-address, including application endpoints. The scan will attempt to discover a system's network exposed attack surface, identifying open ports and fingerprinting exposed service versions. The scan may also interact with services and web pages performing "dynamic analysis". For example the scanner may try and login to a service using a known weak password, or attempt to access a sensitive file.

Remote scans are strongest for discovering vulnerabilities that can be easily exploited by an unauthenticated actor, and for discovering vulnerabilities in custom web applications. Due to no system access, such scans are poor at assessing patch-levels, generally resulting in "Potential" vulnerabilities that may need to be investigated by the device owner.

Remote scans are unsuitable for mobile devices like laptops with no fixed address to target, and remote scans techniques are not performed when using only an agent. While some remote scanning solutions may also support authentication with specific Application Endpoints this is not currently in-scope for vulnerability scanning.

3.1.2 Local Checks

Authenticated Scan and Agent-based scans use privilege access to perform local checks, primarily using "static analysis" such as inspecting files, patch-levels, and configuration. Local scans can provide a more complete view patching and the presence of outdated software. However the Local Check are may be less reliable at identifying externally exploitable network exposures, as exposed network services are not subject to dynamic analysis techniques.

Authenticated Scan and Agent-based scans have many compatibility considerations in terms of supported Operating Systems and products (for patch detections), and are often unsuitable for most endpoints, and many appliances.

Authentication Scans also requires privileged passwords and the exposure of administrative interfaces, which could create security risks in some circumstances, and may not be suitable over untrusted networks such as the Internet. Authenticated Scans are only suitable for targeting management interfaces, and remote scans are preferred for other end-points.

3.1.3 Local and Remote

Combining both methods (i.e. OS-level authenticated scans, or remote scans and a local agent), provides the best level of coverage of both vulnerabilities and tracking patch-levels. Qualys' VMDR can leverage local checks to confirm some remote detections, often removing Potential Issues that can be confirmed by validating local patch levels.

3.2 Oversight Methods

3.2.1 Inventory Reconciliation

Inventory reconciliation reports the deviations between an Asset Inventories (such as CMDB), with “in-the-field” scan results. It can help to identify,

- Incorrect or incomplete asset documentation.
- Devices which do not communicate (potentially blocking the scan or Cloud Agent is not running correctly).
- If the inventory used for comparison is accurate, asset inventory reconciliation provides an indicator of Vulnerability Management coverage.

3.2.1.1 Exclusion Process

Inventory Reconciliation may be enhanced with a **Scan Exclusions** process which can help recording expected deviation, such as manually removing records which should not be considered in-scope. This is often required as asset registries do not align to technical requirements in respect to vulnerability management

3.2.1.2 Automatic On-boarding

Inventory Reconciliation may be enhanced by Automated On-boarding

3.2.2 Discovery

Discovery methods support Vulnerability Management coverage by identifying systems in-the-field, without reliance on an inventory. Discovery is appropriate when discovered assets mapped to an owner, either automatically, or when the volume of discovered system is small and can be handled manually. Otherwise findings are unable to be reported for remediation.

Subnet Scanning	Perform discovery scanning across known subnets to detect responding addresses.
Cloud Integrations	Uses Cloud API (or connectors) to determine what assets are running in Azure, AWS or other hosting environment. This is similar to the inventory approach, but more dynamic.
Cloud Agent	When the Cloud Agent is built into an operating system image it can help to detect and track assets, such as desktops as the imaged and stood up.

Table 2: Potential Discovery Methods

3.2.3 Control Framework

The Technology Controls Library helps mitigate key technology risks by assessment and control of LCT-ITE-000024 - System vulnerabilities are identified and reported.

3.3 Target Coverage

The following tables denote the indicative Vulnerability Management treatment based on properties of the assets. The classifications provide the ability to map asset inventory records to Vulnerability Management requirements. Please note all assets are need to meet **Error! Reference source not found.** (pg. **Error! Bookmark not defined.**) and are subject to **Error! Reference source not found.** (pg. **Error! Bookmark not defined.**).

Device Type	Priority	Target Frequency	Scan Method	Target Remediation time	Target Oversight Methods	Current / Required State (and limitations)
Internet Facing **Internet Facing** endpoints are globally accessible and at the highest risk of direct cyber-attack.	**VHIGH**	< 24 hours	Remote Only	To align to E8 Timelines	Discovery Inventory Rec*	Subnets provided to Cyber Security are subject to continual discovery to detect and scan undocumented assets. **Pending Dependency:** *Inventory Reconciliation* has not yet been implemented. An inventory for external assets does not yet exist and therefore overall coverage is unknown, external end-points are only reported as without ownership in the Network Report. Undocumented cloud endpoints are outside monitored subnets and may not currently be scanned. Development of external end-point inventory to allow

Device Type	Priority	Target Frequency	Scan Method	Target Remediation time	Target Oversight Methods	Current / Required State (and limitations)
						reporting of issues and coverage to their respective owners and allow reporting of coverage.
End-user Workstation End-users devices are on the frontline e for attacks using malicious websites, documents, phishing and malware. They may be somewhat restricted in terms of configuration to protect users.	**HIGH**	<= 3 days	**Local Only**	45 days	Discovery Inventory Rec. (>85%)	Qualys CloudAgent is the preferred scan method for end-user computing. Embedding the agent in standard OS base-images provide *Automatic Onboarding* via the agent and also provides a *Discovery* method for new devices. *Inventory Reconciliation* is against "active" devices as defined by the relevant IT Service. Due to difficult accurately identifying inactive devices, target is 85% of devices confirmed scanned. *Inventory Reconciliation* is provided via the

Device Type	Priority	Target Frequency	Scan Method	Target Remediation time	Target Oversight Methods	Current / Required State (and limitations)
						following source of information: Windows 8/10: Devices have the agent maintained by DXC with oversight from EUX and Cyber Security. Windows devices currently have Inventory Reconciliation performed against Active Directory. Apple OS X: The agent is managed by the IT Service and JAMF is used as a registry. There has been no need for an *Exclusion* process as devices are largely heterogeneous, and devices subject to very transient issues.

Device Type	Priority	Target Frequency	Scan Method	Target Remediation time	Target Oversight Methods	Current / Required State (and limitations)
Server Servers are often the most critical assets in an organisations in terms of criticality considerations. Servers are also highly configurable and allow for a wide range of security weaknesses. This category does not include Internet Facing assets (covered above)	**HIGH**	<= 7 days	**Local* and Remote**	45 days	Inventory Rec (>95%) LCT-ITE-000024	*Inventory Reconciliation* is performed against CMDB assets and to support high-levels of coverage is enhanced with the following mechanisms - *Exclusions Process* is used as a mechanism improve reconciliation against the inventory. - *Automatic On-boarding* is attempted even if on boarding request is not raised. Note on Public Cloud: Uses a hybrid approach with inventory reconciliation performed at the Workspaces /Cloud Technology Container, and Cloud or Subnet Discovery to scan all running in-scope Cloud assets.

Device Type	Priority	Target Frequency	Scan Method	Target Remediation time	Target Oversight Methods	Current / Required State (and limitations)
						The use of Local (i.e. authenticated) scans is required only when supported. Server's assets are subjected to the most mature Vulnerability Management process and form part of an asset control in the Groups framework.
Network Appliance Network appliances generally have little attack surface of their own, but play a critical	**MED**	<= 15 days	**Local* and Remote**	45 days	Inventory Rec (>85%)	Network Devices (with a recorded network address) are reconciled against CMDB assets. A basic exclusion process exists. On-boarding is manual, however largely the responsibility of our network vendors (NTT, Telstra), or by request for internal devices. Low coverage target is due to poor quality of asset inventory information. The use of Local (i.e. authenticated) scans is required only when supported, and SSH based authenticated preferred over SNMP.

Device Type	Priority	Target Frequency	Scan Method	Target Remediation time	Target Oversight Methods	Current / Required State (and limitations)
Other Appliances Appliances may not have a recognised operating system, and rarely supported for local checks. Vendor hardened more tightly managed are lower priority targets.	**MED**	<= 15 days	Remote	45 days	Inventory Rec (>90%)n	Most appliances are currently treated as servers for VM reporting, and have additional oversight. However the target state aligns to network devices. The use of Local (i.e. authenticated) scans is not generally supported for most appliances and is optional. Low coverage target is due to poor quality of asset inventory information.
Public End-user Computing provisioned for restricted access for use to the public.	**LOW**	<= 15 days	**Local and Remote**	Not currently in scope	Inventory Rec* (TBA)	Not currently being on-boarded for scanned and however it is desirable to explore this further in the future.
Internal Endpoint Most internal endpoints will often have some coverage provided from the scanning of the underling device (i.e. hosting server) or SDLC practices.	**VLOW**	<= 15 days	Remote	Not currently in scope	None	Can be manually on-board by request with no oversight, findings are not assigned to an owner and reported in the network report. . Few internal endpoints are currently scan. There are limitation around

Device Type	Priority	Target Frequency	Scan Method	Target Remediation time	Target Oversight Methods	Current / Required State (and limitations)
						how these devices recorded.
Containers				Not currently in scope	None	Security framework for containers is under development and may not follow traditional vulnerability management practices.
Managed End-User				Not currently in scope	None	Not current known to be used. Coverage approach has not yet been developed. Service Owner to engage for review.

* Denotes a current gap under review or change.

4. Dependencies

4.1 Asset Inventory

Targeting Systems and Services with Vulnerability Scanning, and the reporting of vulnerability detections requires an accurate inventory of the assets. At a high-level these requirements are already a Group-wide policy requirement see Group IT Service Design and Transition Policy suitable for identifying and targeting assets.

> *"All Group IT Asset configuration information must be recorded and maintained in accordance with the configuration management directives within the Group IT Service Design and Transition Policy "*[1]

Owners of systems and services are required to ensure their records are accurate and complete, containing the following information (examples provided):

Asset targeting / identification	Asset Type Information	Ownership
• IP Address • DNS Name • Net Bios Name • NetBIOS • Serial Number	See Table 1 (pg. 3)	Entity (CBA/Bankwest/PTBC/) Service Platform Service Ownership

Table 3: Dependencies for Vulnerability Management

When assets are not documented adequately, they may not be able to be on-boarded for scanning, and may be in non-compliance. However it may also be possible to identify these gaps centrally as the devices are undocumented. It is the System or Service owner's responsibilities to raise a PACT and perform risk management of such items.

5. Scope Clarification and Exclusions

Some assets are considered **out-of-scope** for vulnerability management based on their properties others may not be able to scanned leaving a risk to management and subject to a **scan exclusion** This section provided guidance on when system may be removed from the scanning register, or managed to a lower standard.

In Scope	Is the asset part of the target scope for the vulnerability management programme?
Review Required	Should each situation be analysed and approved via a Scan Exclusion, or could the scope consideration potentially be applied automatically from asset data without any review or approval.
Gap / Risk Required	Is there a residual risk expected that may need assessment and management before a scan exclusion be approved.

This is guide only, a risk assessment may also be required by any Scan Exclusion approver and may need to record as part of the scan exclusion process even if not specified here. Discretion can be applied by Scan Exclusion approvers who may considered the specific circumstances of the request.

In the general reviewers are expected to weigh the following factors:

1. Is inclusion in the CBA internal vulnerability scanning programme feasible in this instance, could any is it reasonable that any applicable constraints could be overcome?
2. What is the technical level of benefit expected from scans (noting this may vary depending on the context of the asset, such as its exposure to attacks).
3. Are there other mitigating controls, such as alternative central management tools which may help to prevent or detect vulnerabilities?

5.1 Network

5.1.1 Network Protocol

Vulnerability Management control requires that assets are network addressable using Internet Protocol version 4 s standardised for Group-use Wide Area Network communications. Internal address must adhere to RFC 1918.

Items with internal addresses not adhering to RFC 1918 are deemed **out-of-scope and can** be subject to **exclusion without review or approval**.

Out-of-scope	Yes
Review Required	Not Required
Gap / Risk Required	No

5.1.2 Network Addressable

Devices with no remote network connectivity (i.e. air gaped) cannot be remotely scanned for vulnerabilities, but also present no remote network attack surface. Assets without a routable Internet Protocol address are not considered in-scope for Vulnerability Management scanning and may be excluded without review or approval.

Out-of-scope	Yes
Review Required	Not Required
Gap / Risk Required	No

5.1.3 Network Zoning

Some assets may be present in network zones designed not to be able to be reached by existing Vulnerability Management infrastructure due to their security architecture. Violating these zones may have a negative impact on security posture.

For instance, some systems may be dependent on network-level controls, and have internal components demanding total isolation from the outside of a restricted network.

The following guidance is provided on considering scan exclusions for **devices**:

- When the number of **devices** is low and level of isolation high, deploying new scanning infrastructure may not be recommended, and a discretionary scan exclusion (without risk) may be approved.

- If an unreachable network zone contains a larger number devices, then a risk assessment should be recorded as part of the scan exclusion process, with an aim to produce actions to address the imitation.

When considering end-points, consideration should be applied to their exposure - the number of entities (people, systems, organisations) who can reach the end-point, and the risk these entities present

Such items may be **excluded with review to determine if risk management is required**.

Out-of-scope	Yes
Review Required	Not Required
Gap / Risk Required	No

5.2 Device Specific Consideration

5.2.1 Security Model

Some devices may have a security model which forbids the installation of an agent or Qualys scans.

Out-of-scope	Yes
Review Required	Yes
Gap / Risk Required	Review Dependant

5.2.2 Offline / No attack surfaces

Some devices may not respond during Remote Scans as they have no external attack surface.

In-Scope	No (for period not responding)
Review Required	Not Required
Gap / Risk Required	No

5.3 Ownership

The Group's Vulnerability Management practice is limited to assets that are owned and/or controlled by the Group or are deployed internal on the Group's private networks. The scope of scanning **does not** extend to systems owned and controlled by vendors, industry associations, suppliers, partners, divested entities and customer systems.
While in some cases it may be possible review and complete a form of scanning and monitoring or reporting of some non-CBA endpoints. This is not performed by default and requires engagement with Cyber Security. Arrangement currently exists for:

- Telstra Network Devices in Network Perimeter Services
  Results from owned devices scanned by Telstra are included in the CBA networks reports

In-Scope	No (for period not responding)
Review Required	Not Required
Gap / Risk Required	No

5.3.1 Platform-as-a-Service

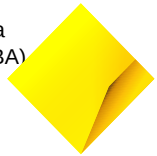
Platform-as-a-Service (PaaS) model services (including Cloud Native) will often provide end-points which are provided solely for use by the customer, such as a database or message queue. Such end-points are considered as in-scope vulnerability management scanning.

In Scope	Yes (no differential treatment)
Review Required	-
Gap / Risk Required	-

5.3.2 Managed Infrastructure

External support arrangements for CBA owned infrastructure does not alter the requirements for Vulnerability Management scanning and remain in-scope.

In Scope	Yes (no differential treatment)
Review Required	-
Gap / Risk Required	-



5.3.3 Externally Owned and Managed Infrastructure

Some assets may be provided solely for the Groups use, but are owned and managed by an external party, and at least partially isolated from Group networks'. While it is preferable to scan such assets when practical, it is mandated, and rarely possible due to commercial and technical considerations. As such they are NOT considered a standard part of the target scope for vulnerability management.

It may still be possible request a review to determine if a Vulnerability Management activity can occur on non-CBA infrastructure.

In-Scope	No
Review Required	No
Gap / Risk Required	No

5.4 Other Reasons for Scan Exclusions

There are ranges of reasons for why scanning may not be performed for a period of time.

- Causes an outage / incident
- Commercial Constraint (i.e. contact terms incompatible with policy)
- New scanners or infrastructure required to be built to support scanning
- Unable to deploy agent due to error

These potentially legitimate reasons for preventing scanning do not mean the asset is out-of-scope for scanning. The situation will typically be addressed by risk management and risk actions to address constraints that cause the issues within acceptable timeframes (i.e. action due dates).

In-Scope	Yes
Review Required	Yes
Gap / Risk Required	Yes (although discretion allowed)

6. Relevant documents

Related internal documents	IS Vulnerability Management Standard
Leveraged internal documents	Vulnerability Management Home

7. Material revisions

Version	Approval Date	Effective Date	Details
1.0	10 February 2023	10 February 2023	New guideline.