State of California
Independent Security Assessment (ISA) Phase-II
Assessment Criteria v 5.2

The following criteria identifies the minimum tasks, conditions, standards, and documentation requirements for the successful conduct of the State of California Independent Security Assessment (ISA), Phase-II. This criterion includes documentation for all required artifacts that must be provided at the time of ISA submission.

Revision 5.2 as of 22 June 2023 effective 1 July 2023. Prior versions are obsolete.
Latest revision 5.2 as of 6/22/2023.

Table of Contents

Effective 1 July 2023.
Last revision as of 6/22/2023. Prior versions are obsolete.

Usage Information

Public Records Act

Distribution Restrictions: This criterion is Confidential and Exempt from Public Disclosure in accordance with Government Code Sections 6254.19.

Scope of Assessment: The purpose of the assessment is to measure the widest possible scope of the entity assets in order to derive accurate results. Unless otherwise identified in a specific task within the assessment criteria, all assets, accounts, and information sources under entity control are considered in-scope for results analysis.

Generating Scoring Results Using this Criteria

When using this criterion for analysis, each task assessed and resulting score should be minimally represented in the following manner:

- Task ID
- Task Title
- Score
- Findings
- Proof of findings/visual documentation

Effective 1 July 2023.
Last revision as of 6/22/2023. Prior versions are obsolete.

Criteria-related Questions

For questions related to the criteria, contact California Department of Technology, Office of Information Security at security@state.ca.gov. Provide the Task number, summary of the concern, and recommended modification(s).

Alternative Information Collection (Contact Reduction Process)

To assist with the reduction of in-person contact, all tasks within the ISA assessment program have been deemed appropriate for collection and analysis via the alternative, limited contact method. This method seeks to maximize the use of the following:

- Video teleconference capabilities for entity/staff interactions (e.g., Teams, WebEx, etc.)
- Entity pre-staged configurations of required network connections, required accounts, and interactions with entity support staff
- Pre-authorized access to required entity buildings and workspaces

The reduced contact collection configuration requires maximum entity pre-planning and strict adherence to the pre-assessment guidelines set by the supporting ISA team. In situations where entity configurations, access, or generated artifacts fail to satisfy the requirements for successful analysis, the entity will be notified of the deviation and required to adjust their reduced collection plan to satisfy the requirement. Failure to resolve potential issues will result in a non-compliant rating for the impacted tasks. Reduced contact procedures do not eliminate the requirement for ISA team to physically access entity buildings or networks. Many of the tasks assessed under this program are not appropriate for remote access analysis. The provided pre-assessment guidance from an entity's ISA team should include guidelines for documented observation standards and artifact delivery.

Effective 1 July 2023.
Last revision as of 6/22/2023. Prior versions are obsolete.

Deconstructing Criteria Task Components

The following task deconstruction is provided to aid entity preparation for the ISA.

EXAMPLE ONLY

Task number and title	**Task: 10.1 – Account Naming Standards for Role-based Separation**
Primary and supplemental references	***References*** NIST SP 800-53 r5 AC-6(2) NIST SP 800-171 r2 3.1.6
Conditions assessed by the task	***Condition*** Entity demonstrates the practice of separate account provisioning for privileged rol management. This task specifically checks for a process or indication that allows f accounts when viewing user-level accounts. Validation is verified through the use accounts that is different from user accounts.
Detailed standards for determining level of compliance	***Scoring Criteria*** **I** Entity demonstrates uniquely identify standard to differentiate between priv enterprise. The standard applies to all privileged accounts in both the on-p **P** N/A. This is a compliant/non-compliant measured standard **N** Any of the following deficiencies are detected: - Absence of a distinct naming convention standard between privileged a - Incomplete application of the naming standard across all privileged acc - Presence of accounts with privileged role assignments that do not follo by the entity
Required source artifact that must be included for scoring validation	***Artifact*** Proof of non-compliant naming conventions is required.

Cross-Walk of Current Year to Previous Year ISA Phase-II Criteria Tasks

This task cross-walk provides ISA tasks from Fiscal Year 2021-2022 to ISA tasks from Fiscal Year 2022-2023.

Version 4.0.0 Task Number and Title		Version 5.1.0 Task Number and Title	
2.09.1	Access Control – User Account Privileged Role Standard Naming Convention	10.1	Account Naming Standards for Role-based Separation
2.08.2	Logical Verification – Least Privilege of Key Roles	10.2	Least Privilege Assessment of Key Roles
2.08.1	Logical Verification – Least Privilege of Key Hosts	10.3	Least Privilege Assessment of Key Hosts
2.11.1	FIPS Validation of VPN Encryption Implementation	10.4	FIPS Compliant Remote Access Solution Validation
2.10.1	Access Control – Account Testing	10.5	Account Testing of Applied Controls for Privileged User Access
		10.6	Account Testing of Applied Controls for Standard User Access
2.11.2	Remote Access Solutions Protected by Multi-Factor Authentication	10.7	Remote Access Solutions Protected by Multi-Factor Authentication (MFA)
2.04.2	React to Active Phishing Campaign – Risk Analysis Team Sourced Practical Exercise	10.8	Risk Analysis Team Conducted User Phishing Practical Exercise
2.01.1	Cloud Security Configuration Management	11.1	Cloud Security Configuration Management
2.08.3	Baseline Image Security Configuration and Analysis	11.2	Baseline Image Security Configuration and Analysis
2.09.2	Least Functionality Configuration – Continuous Surveillance for At-Risk Service Exposures	11.3	Continuous Surveillance for At-Risk Service Exposure
2.13.1	Boundary Protection – Prohibit use of Insecure Management Protocols/Access	12.1	Boundary Protection Solutions Prohibit Insecure Management Protocols
2.16.1	Malicious Code Protection – Central Client Management	12.2	Endpoint Security Deployment and Monitoring
2.04.1	Detection and Mitigation of Network Rogue Devices	12.3	Detection and Mitigation of Network Rogue Devices
2.15.1	Continuous Monitoring (Vulnerability Scans) of Assets	12.4	Host Scans for Continuous Monitoring and Vulnerability Management
N/A	New task in ISA Criteria version 5.0.0	12.5	Secure DNS Communication through CDT Managed Infrastructure
2.13.2	Boundary Protection – Validate Ingress / Egress Monitoring	13.1	Boundary Protection Ingress/Egress Monitoring

Effective 1 July 2023.
Last revision as of 6/22/2023. Prior versions are obsolete.

Version 4.0.0 Task Number and Title		Version 5.1.0 Task Number and Title	
2.13.3	Boundary Protection – Validate rules for Deny All, Permit by Exception (DAPE) configuration	13.2	Boundary Protection Device Deployed in an Industry Best Practice Configuration
2.13.4	Review IDS/IPS Event Monitoring and Escalation Process	13.3	IDS/IPS Event Monitoring, Review, and Clearance/Escalation Procedures
2.13.5	Review IDS/IPS Maintenance (Signature & Firmware)	13.4	IDS/IPS Signature & Firmware Updates
2.13.6	Information System Monitoring - SSL/SSH Traffic Inspection and Analysis	13.5	SSL/SSH Traffic Inspection and Analysis
2.17.1	Primary External Website Assessment – Exploitable Configurations / Input Validation	13.6	Reoccurring Primary External Website Analysis
2.05.1	Entity Log Generation and Retention	14.1	Entity Log Generation and Retention
2.14.1	Distribution of Cybersecurity Alerts, Messages, and Warnings	15.1	Distribution of Cybersecurity Alerts, Messages, and Warnings
2.21.9	Open-Source Meta Data Identity Collection (External)	16.1	Penetration Test External Open-Source User Identity Collection
2.21.6	Spear Phishing Acquisition of Plaintext User Credentials (External)	16.2	Penetration Test External Spear Phishing Attempt
2.21.7	Password Guessing, Spraying, and Default Credential Usage (External)	16.3	Penetration Test External Password Guessing Activities
2.21.8	Credential Hash Capture and Analysis (External)	16.4	Penetration Test External Credential Hash Capture and Cracking Operations
2.22.1	External Host Targeting Exposure (External)	16.5	Penetration Test External Undeclared Hosts/Networks
2.22.2	High-Risk Service Exposures (External)	16.6	Penetration Test External High-Risk Service Exposure Detection
2.22.3	Internet Exposed Host Management Services (External)	16.7	Penetration Test External Host Management Service Detection
2.22.4	Web Application Misconfigurations and Exposures (External)	16.8	Penetration Test External Web Application Misconfigurations and Exposures
2.22.5	Malicious Code Detection and Prevention (External)	16.9	Penetration Test External Execution of Malicious Code on Controlled Host

Effective 1 July 2023.
Last revision as of 6/22/2023. Prior versions are obsolete.

Version 4.0.0 Task Number and Title		Version 5.1.0 Task Number and Title	
2.22.6	Password Guessing, Spraying, and Default Credential Usage (Internal)	17.1	Penetration Test Internal Password Guessing, Spraying, and Default Credential Detection
2.22.7	Credential Hash Capture and Analysis (Internal)	17.2	Penetration Test Internal Credential Hash Capture and Cracking
2.22.9	Insecure / Weak Host Management Service Exposure (Internal)	17.3	Penetration Test Internal Use of Insecure Host Management Services
2.23.1	Web Application Misconfigurations and Exposures (Internal)	17.4	Penetration Test Internal Web Site/Application Risks
2.22.8	At-Risk Wireless Network Access Configurations (Internal)	17.5	Penetration Test Internal Wireless Network Breach Resistance
2.23.2	Host Exploitation, Command and Control via Malicious Code Execution (Internal)	17.6	Penetration Test Internal Execution of Malicious Code on Controlled Host

Assessment Criteria

This page intentionally blank

Task: 10.1 – Account Naming Standards for Role-based Separation

References
NIST SP 800-53 r5 AC-6(2)
NIST SP 800-171 r2 3.1.6

Condition
This task specifically checks for a process or indication that allows for the unique identification of privilege role accounts when viewing standard user accounts. The entity must demonstrate it identifies unique naming conventions across the various account types – privileged accounts, service accounts, and standard user accounts.

Scoring Criteria
I Entity identifies naming convention to differentiate between privileged accounts, service accounts, and standard user accounts within the enterprise

P N/A. This is a compliant/non-compliant measured standard

N Entity does not have a distinct naming convention between privileged accounts, service accounts, and standard user accounts within the enterprise

Scoring Note
Implementation of standard naming convention is scored in task 10.2 and 10.3.

Artifact
Proof of standard naming conventions for privileged accounts, service accounts, and standard user accounts is required.

Task: 10.2 – Least Privilege Assessment of Key Roles

References

NIST SP 800-53 r5 AC-6(1)
NIST SP 800-171 r2 3.1.5

Condition

This task reviews the entity's enterprise to determine if standard user accounts have privileged roles membership. The entity is assessed to validate it demonstrates the practice of separate account provisioning for privileged roles as part of its Principle of Least Privilege management. Examples of privileged roles for assessment include, but are not limited to, the following:

On Premises Roles

- Enterprise Administrators
- Domain Administrators
- Account Operators
- Backup Operators
- DNS Administrators
- Database Administrator (or equivalent)
- Power Users
- Group Policy Administrator / Creator Role

Cloud Service Roles

- Azure:
  - Azure AD Global Administrator
  - Security Reader
- Amazon Web Services
  - AWS Account Root User
  - Database Administrator
  - Network Administrator
  - Data Scientist
  - Developer Power User
  - Security Auditor
- Salesforce
  - Super Admin
  - Admin Only

Scoring Criteria

I Assessed privileged roles are absent of standard user accounts or non-compliant named account

P N/A. This is a compliant/non-compliant measured standard

N Assessed privileged roles contain a standard user accounts or non-compliant named account

Scoring Note

If entity scores a “N” in Task 10.1, then Task 10.2 is scored as “N”.

Artifact

Proof of non-compliant, standard user account or non-compliant named account within one of the assessed privileged roles is required.

Task: 10.3 – Least Privilege Assessment of Key Hosts

References

NIST SP 800-53 r5 AC-6(2), AC-6(5)
NIST SP 800-171 r2 3.1.5

Condition

This task evaluates a random subset of hosts within the entity's enterprise to assess the presence of any standard user accounts within the contained privileged roles on the target host. The entity is assessed to validate the implementation of the Principle of Least Privilege which requires the separation of provisioned standard user and privileged account access rights between two or more distinct accounts, as applicable.

Scoring Criteria

I All assessed hosts are absent of standard user accounts within privileged roles/rights

P Between 1-3 assessed hosts contain standard user accounts provisioned within privileged roles/rights

N 4 or more assessed hosts contain standard user accounts provisioned within privileged roles/rights

Scoring Notes

If entity scores a "N" in Task 10.1, then Task 10.3 is scored as "N". Standard users identified as local admin are scored within this task.

Artifact

Proof of non-compliant, standard user account within one of the assessed host is required.

Task: 10.4 – FIPS Compliant Remote Access Solution Validation

References
NIST SP 800-53 r5 AC-17(2), SC-7(4)
NIST SP 800-171 r2 3.1.13
SAM 5360.1

Condition
This task validates that network-level connections from external networks (e.g., VPN, VDI, etc.) require a FIPS 140-2 approved encryption implementation configuration and certification. The entity's deployed remote access solution must be FIPS compliant and operating in FIPS mode as part of the measured standard. The entity must meet the following conditions for all remote access solutions:

1. All entity VPN/3rd party remote access solution are deployed with encryption.
2. Remote access solutions are deployed utilizing vendor certified FIPS 140-2/3 configuration.
3. Entity provides vendor-approved Common Criteria certification at EAL Level 1 or higher.

Scoring Criteria
I Entity deployed solution meets all conditions

P Entity deployed solution meets condition 1 BUT fail to meet either conditions 2 or 3

N Entity deployed solution fails to meet condition 1

Scoring Notes
If multiple solutions are deployed (e.g., environment contains Citrix Receiver, AnyConnect, and Cisco VPN router solution), the solution with the least compliant score is used to score this task. Reference the NIST Cryptographic Module Validation Program and FIPS Compliant Ciphers and Cipher Suites for FIPS compliance. Reference the Common Criteria: Certified Products for EAL level 1 certifications.

Artifact
Proof of device configuration displaying the settings for FIPS 140-2 compliance (GUI or CLI output of the FIPS configuration setting activation) is required. Provide a copy of the Common Criteria Certification for the device. Reference the specific vendor guidance for FIPS configuration validation.

Effective 1 July 2023.
Last revision as of 6/22/2023. Prior versions are obsolete.

Task: 10.5 – Account Testing of Applied Controls for Privileged User Access

References

NIST SP 800-53 r5 IA-5(1)
NIST SP 800-171 r2 3.5.2

Condition

Password-based authentication is a type of authenticator that can support authenticator management. This task validates the enforcement of password settings and restrictions for privileged accounts by the application of strong characteristics for privileged account types – interactive and non-interactive logon. When privileged users are assigned rights used to perform system administration, configuration, or privilege escalation, their credentials are typically utilized as interactive logons. When privileged access is assigned to role-based functions such as service accounts, users are not expected to utilize the account as part of their routine duties; therefore, these accounts are classified as non-interactive logons.

Privileged and Service Accounts

1. Minimum Length: no less than 15 unless system cannot support (applied via password policy).
    a. Entropy: None required
    b. Reuse Restriction: None required
    c. Password Lifetime (Privileged Accounts): Minimum expiration every 6 months.
    d. Password Lifetime (Service Accounts): Determined by entity. Reset upon compromise.
2. If system (domain functional level) cannot support 15:
    a. Minimum Length 12
    b. Entropy: Requires 4 of 4 Complexity types (Upper, Lower, Numeric, and Special characters)
    c. Reuse Restriction: 10 prior passwords
    d. Password Lifetime: 6 months for less than 15-character passwords
3. Account lockout:
    a. External: After 5th invalid attempt (Azure, AWS, external directory service, 3rd party cloud services, etc.)
    b. Internal: After 10th invalid attempt (On-premises directory service/local host)
    c. Lockout period: 120-minute lockout

Scoring Criteria

I Entity meets or exceeds all conditions

P Entity fails to meet any one sub-condition listed under 1 through 3

N Entity fails to meet more than one sub-condition listed under 1 through 3

Scoring Notes

- Fine-grained Password policies cannot be implemented in enterprises operating below Domain Functional Level 2008 R2
- If entity accounts are managed in Azure only AND no on-premises domain controllers exist AND all the following conditions are true, this task is scored as “I”:
    - MFA is required for access on all accounts
    - Conditional access is set to enforce MFA for suspicious logon activities/logons from IP ranges not managed by the entity

Artifact

The following artifacts are required for this task, as applicable:

- Proof of the domain functional level 2008 R2 or below
- Proof of the applied security control policies for both Privileged users and Service accounts
    - If using Command Line Interface (CLI) or PowerShell to validate outcomes, screenshot must show the attempt and result
- Proof of non-compliance such as a screenshot documenting the standards deviation
- For Azure only Active Directory, screenshots of MFA requirement, conditional access settings, and privilege role separation

Task: 10.6 – Account Testing of Applied Controls for Standard User Access

References

NIST SP 800-53 r5 IA-5(1)
NIST SP 800-171 r2 3.5.2

Condition

Password-based authentication is a type of authenticator that can support authenticator management. This task validates the enforcement of password settings and restrictions for non-privileged accounts by the application of strong password characteristics via implementation of fine-grained password policies.

Non-Privileged Accounts

1. Minimum Length: no less than 15 unless system cannot support (applied via password policy).
    a. Entropy: None required
    b. Reuse Restriction: None required
    c. Password Lifetime (Privileged Accounts): Minimum expiration every 6 months.
    d. Password Lifetime (Service Accounts): Determined by entity. Reset upon compromise.
2. If system (domain functional level) cannot support 15:
    a. Minimum Length 12
    b. Entropy: Requires 4 of 4 Complexity types (Upper, Lower, Numeric, and Special characters)
    c. Reuse Restriction: 10 prior passwords
    d. Password Lifetime: 6 months for less than 15-character passwords
3. Account lockout:
    a. External: After 5th invalid attempt (Azure, AWS, external directory service, 3rd party cloud services, etc.)
    b. Internal: After 10th invalid attempt (On-premises directory service/local host)
    c. Lockout period: 120-minute lockout

Scoring Criteria

I Entity meets or exceeds all conditions

P Entity fails to meet any one sub-condition listed under 1 through 3

N Entity fails to meet more than one sub-condition listed under 1 through 3

Effective 1 July 2023.
Last revision as of 6/22/2023. Prior versions are obsolete.

Scoring Notes

- Fine-grained Password policies cannot be implemented in enterprises operating below Domain Functional Level 2008 R2
- If entity accounts are managed in Azure only AND no on-premises domain controllers exist AND all the following conditions are true, this task is scored as “I”:
    - MFA is required for access on all accounts
    - Conditional access is set to enforce MFA for suspicious logon activities/logons from IP ranges not managed by the entity

Artifact

The following artifacts are required for this task, as applicable:

- Proof of the applied security control policies for non-privileged user accounts
    - If using Command Line Interface (CLI) or PowerShell to validate outcomes, screenshot must show the attempt and result
- Proof of non-compliance such as a screenshot documenting the standards deviation
- For Azure only Active Directory, screenshots of MFA requirement, conditional access settings, and privilege role separation

Task: 10.7 – Remote Access Solutions Protected by Multi-Factor Authentication (MFA)

References

NIST SP 800-53 r5 IA-2
NIST SP 800-63-3 5.1.3.1
NIST SP 800-171 r2 3.5.3
FIPS 140-2
SIMM 5360-A

Condition

Remote access is defined as the presentation of non-public logical access from locations external to entity security control. This task validates that the entity enforces NIST 800-63-2 compliant Multi-factor Authentication (MFA or 2FA). The entity must meet the following conditions for all remote access solutions:

1. MFA compliant remote access solutions are fully documented on Data Call prior to assessment
2. Configured to prevent single-factor authentication or at-risk factor for any configured user
   a. Compliant factors for MFA include Hardware Token, Software-based Token, Smartcard, Grid Card
   b. At-risk factors include SMS OTPs (device SIM can be cloned/spoofed) and phone calls (do not confirm recipient identity)
3. Determined compliant using documented observation of the MFA/2FA solution

Scoring Criteria

I Entity deployed solutions meets all conditions

P Entity deployed solutions meets conditions 1 and 3 but fail to meet condition 2

N Entity deployed solutions fail to meet two or more conditions

Scoring Notes

Score as “N” if all users are not implemented using MFA. Remote access solutions for assessment include, but are not limited to, the following:

- VPN (SSL or Client-based)
- SSH
- Direct Remote Desktop Access Solutions
- Azure Portal
- VDI (Digital Workspace Presentation Platforms)

If the entity does not allow remote access, then this task is scored as "I".

Artifact

Proof of compliance or non-compliance from all remote access solutions MFA validation is required.

Task: 10.8 – Risk Analysis Team Conducted User Phishing Practical Exercise

References
NIST SP 800-53 r5 AT-2(1)
NIST SP 800-171 r2 3.2.1

Condition
This task tests user participation in an unannounced simulated phishing exercise (MITRE ATT&CK ID: T1566). The entity must provide required user information in accordance with assessment standards and configuration requirements.

User Population Requirements

- A minimum user population of 100 users
    - If entity assigned user mailboxes are less than 100, then all mailbox users will be provided
- Nominated participants must not be notified of their participation and must include:
    - 3 Executives (or maximum assigned)
    - 3 System Administrators
    - 3 Management team members

Rules of Engagement for Proper Task Evaluation

- Entity is prohibited from notifying the participants of the phishing campaign prior to assessment or during campaign
- Entity will respond to participant detected phishing reports for this task as “We are investigating”
- Entity is prohibited from taking actions to mitigate phishing campaign such as the following:
    - Removing the message from users’ inboxes
    - Blocking the associated web site, phishing source IP address, etc.
- Entity is prohibited from opening Cal-CSIRS events or submitting a report of phishing attempt to external agencies

Scoring Criteria
I Less than 10.00% of phished participants click the link AND no phished participants provide credentials

P Less than 15.00% of phished participants click the link AND less than 5.00% of phished participants provide credentials

N Greater than 15.00% of phishing participants click the link OR 5.00% or more of phished participants provide credentials

Effective 1 July 2023.
Last revision as of 6/22/2023. Prior versions are obsolete.

Scoring Note

- Percentage **for clicked links** equals the total number of participants that clicked the link divided by total number of participants phished
    - Automated clicks from phishing analysis tools will adversely impact this score
- Percentage for credentials provided equals the total number of unique credentials submitted divided by total number of participants phished
    - All unique credentials submitted, to include false credentials, will adversely impact score
    - Duplicate credentials from a single user are removed prior to calculation

Artifact

A summary of phishing campaign results including the number of users phished, users clicks, and if any users surrender credentials during the campaign is required.

Task: 11.1 – Cloud Security Configuration Management

References
NIST SP 800-53 r5 CM-6(1)
SIMM 5315-B

Condition
This task validates that the entity applies automated cloud cybersecurity assessment measurements to each 3rd party cloud-operated environment. Using score results, the entity must perform continuous monitoring of compliance, applying security recommendations to reduce risk exposures while maintain business process operability, achieving a baseline secure configuration score. The entity must meet the following conditions for cloud secure scores:

1. Each cloud solution provides a compliance dashboard/report measuring the entity-deployed services
2. The entity demonstrates ability to access each cloud solution compliance scoring and controls

Scoring Criteria
I The cloud solution meets all conditions AND cloud secure score is 50.00% or greater

P The cloud solution meets all conditions BUT cloud secure score is between 30.01% to 49.99%

N The cloud solution fails to meet either conditions 1 or 2 OR cloud secure score is 30.00% or less

Scoring Note
Assessment is based on the lowest cloud secure score. Examples of monitored assessment measurements include, but are not limited to, the following:

- Microsoft 365 Secure score
- Amazon Web Services secure score (AWS self-service security assessment)
- Salesforce Health Check score
- Other 3rd party cloud provider score

Artifact
Proof of each cloud compliance dashboard/report displaying the overall compliance score is required.

Effective 1 July 2023.
Last revision as of 6/22/2023. Prior versions are obsolete.

Task: 11.2 – Baseline Image Security Configuration and Analysis

References

NIST SP 800-53 r5 CM-2
NIST SP 800-171 r2 3.4.1
SAM 5315

Condition

This task measures the application of system hardening controls/settings of entity on-premises and cloud-based systems. System hardening is assessed via the percentage of compliance against the NIST Moderate standard (as applicable based on available host template) for the hosts listed below. Provided hosts must include a representative subset of operating systems, as available.

On-premises Hosts per Host Function

- 1 Domain controller
- 3 Application servers
  (e.g., Database servers, file servers, web servers, etc.)
- 6 Laptops/workstations

Cloud-based Hosts per Host Function

- 2 Servers

Scoring Criteria

I The average score is 75.00% or greater

P The average score is between 50.01% to 74.99%

N The average score is 50.00% or less

Scoring Notes

- For entities that do not have cloud-based hosts, additional on-premises hosts must be provided by entity for a total of 12 assessed hosts
- The standard for analysis is the Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) template
- In cases where Windows 7 or older operating system are in use, the U.S. Government Configuration Baseline (USGCB) standard will be applied. Reference the United States Government Configuration Baseline on NIST for OS USGCB
- The Center for Internet Security (CIS) Benchmark criteria is not an approved alternative assessment template for this task

Effective 1 July 2023.
Last revision as of 6/22/2023. Prior versions are obsolete.

Artifact

The following artifacts are required for this task:

- Total hosts assessed by operating system and CVE score grouped by servers and non-servers
- Averages will be provided by servers, non-servers, and overall total average
- A detailed findings report for each assessed host will be provided

Task: 11.3 – Continuous Surveillance for At-Risk Service Exposure

References
NIST SP 800-53 r5 CM-7
NIST SP 800-171 r2 3.4.6

Condition
Routine evaluation of the entity host/service exposures should be a part of the entity's continuous risk assessment and evaluation process. This task validates that the entity conducts monthly scans (at a minimum) of all hosts/devices to determine their service exposures. The entity must meet the following conditions for continuous surveillance of at-risk scans:

1. All entity allocated IP address spaces (e.g., on-premises, cloud, 3rd party) are scanned
2. All service scan results must include protocol (TCP/UPD), service port, and port status (e.g., open, filtered, closed)
3. A minimum scan interval of monthly
4. The entity provides proof of scan results distribution with system owners and communities of interest

Scoring Criteria
I Entity scans meet all conditions

P Entity scans meet conditions 1 and 2 BUT fails one other condition

N Entity fails to meet condition 1 OR fails to meet two or more conditions

Scoring Notes
BitSight reports that cover the entire external ranges may be used as documentation for the external portion of this task.

Artifact
Proof showing date, criteria, and distribution of external and internal scans is required.

Task: 12.1 – Boundary Protection Solutions Prohibit Insecure Management Protocols

References
NIST SP 800-53 r5 CM-7, SC-8
NIST SP 800-171 r2 3.4.7

Condition
This task validates that the entity perimeter firewall (entity or parent activity managed, as applicable) restricts insecure protocol usage on the management interface to prevent unauthorized access and information leaks. Insecure protocols for the purposes of this task include, but are not limited to, the following:

- HTTP
- Telnet
- SNMP v1/v2/v2c
- SSH supporting weak ciphers

Scoring Criteria
I The management port is configured to prohibit the use of insecure protocols

P Management port is configured to prohibit listed insecure protocols from external networks, but allows 1 of the listed protocols from a protected internal subnet

N Management port allows either 2 or more insecure protocols from an internal subnet or any of the insecure protocols from the external network

Scoring Note
For the purposes of this task, a weak cipher is defined using the criteria maintained by Open Web Application Security Project (OWASP) Web Security Testing Guide (WSTG) control WSTG-CRYP-01 and WSTG-CRYP-04.

Artifact
Proof of the Graphical User Interface (GUI) or Command Line Interface (CLI) is required, as applicable, showing management interface configuration allowed services and cipher strengths. A formal report documenting the management interface configuration is acceptable for this artifact.

Task: 12.2 – Endpoint Security Deployment and Monitoring

References
NIST SP 800-53 r5 PL-9, SI-4(25)
NIST SP 800-171 r2 3.14.3

Condition
The entity deploys endpoint protection on all entity managed hosts (MITRE ATT&CK ID: M1040) within its control (on-premises, 3rd party hosted, and cloud). For entities utilizing endpoint protection solutions managed via Active Directory membership, a separate enterprise management console must be provided for non-directory joined/stand-alone assets if they cannot be managed within a single enterprise solution. The entity must meet the following conditions:

- Enterprise console listing all assets within the console OR multiple enterprise consoles consisting of all enterprise assets based on category (AD joined, non-AD joined, and stand-alone)
    - Entity will provide a list of all non-domain joined hosts (on-premises, 3rd party hosted, and cloud)
    - Stale Active Directory clients with a last check-in date greater than 30 days are discounted
- Endpoint date of last console check-in must be within 15 days from ISA date
- Endpoint signature update must be within 30 days from ISA date

Scoring Criteria
I A score greater than 95.00% of expected clients under enterprise management meet all conditions within this task

P A score ranging from 75.00% to 95.00% of expected clients under enterprise management meet all conditions within this task

N A score less than 75.00% of expected clients under enterprise management meet all conditions within this task

Scoring Note
The formula used to calculate the centrally managed clients is the total assets up-to-date (assets with signatures within 15 days of ISA) divided by the total assets that have checked in to AD within the last 30 days.

Artifact
No artifacts required for the task. *Proof of AD total asset count is verified onsite.*

Task: 12.3 – Detection and Mitigation of Network Rogue Devices

References
NIST SP 800-53 r5 SI-4
NIST SP 800-171 r2 3.14.6

Condition
This task measures the ability of the entity to detect and mitigate unauthorized (rogue) device connections within the enterprise. The entity must deploy controls and monitor network for signs of network connected rogue devices, must confirm rogue device presence, and takes steps to disable network access and remove from network (MITRE ATT&CK ID: T1564.006. The entity must meet the following conditions:

1. Deploys controls to detect/alert for presence of unauthorized rogue device on the network
2. Identifies rogue host by host name, port, and location
3. Disables logical network access to business network
   - If rogue device draws an IPv4 link-local address (e.g., 169.254.255.x), then this condition is met
4. Reports security event to ISO and RA Team Lead within 60 minutes of device connection

Scoring Criteria
I Entity meets all conditions or rogue device did not receive an IP address

P Entity meets condition 1, 2, AND 3, BUT fails condition 4

N Entity fails to meet 1, 2, or 3

Scoring Note
Connection of physical rogue device is performed in an unannounced manner, to an active port in the entity environment. Assessment period is 60 minutes or until device is detected and network access terminated. Logical disablement can include movement to a quarantine VLAN through automated means; documentation of the automated port modification is required.

Artifact
The following artifacts are required for this task:

- Configuration settings identifying the date, time, and IP address assigned to the rogue device
- Proof of entity detection including date, time, and device location

Effective 1 July 2023.
Last revision as of 6/22/2023. Prior versions are obsolete.

Task: 12.4 – Host Scans for Continuous Monitoring and Vulnerability Management

References
NIST SP 800-53 r5 RA-5
NIST SP 800-171 r2 3.11.2

Condition
The entity must provide proof of recurring, privileged access authenticated vulnerability scans (MITRE ATT&CK ID: M1016). Scans must be sufficient to validate the status of system and installed application security patch states (including 3rd party security patching) on all systems under entity control (physical, virtual, cloud-hosted) as part of the entity continuous vulnerability monitoring program.

Required Compliance Measures

1. Scan type: Authenticated Root, Domain Privileged, or Local Privileged or agent access rights (as applicable)
2. Scan findings:
    a. Results must minimally identify the vulnerability, CVE/vendor risk ID, and CVE vulnerability score
    b. Results based on signatures that are within 15 days based off the date of the ISA
3. A minimum continuous monitoring cycle of monthly
4. A minimum of 75% of total hosts joined to AD must be assessable
5. Provides proof of scan results distribution to responsible administrator(s), ISO, CIO
6. Scan history: Two continuous prior months, based on the date of the ISA
7. CCVM score is 3.9 or less

Scoring Criteria
I Entity meets all conditions

P Entity meets conditions 1-6 but fails to meet condition 7

N Any of the following conditions:
- Entity fails to meet conditions 1, 2, 3 OR 4
- Entity fails to meet 3 or more other conditions
- The minimum number of total hosts joined to AD during the ISA is not assessable

Scoring Note
Condition 4 is calculated based on the total number of entity-controlled assets that CND can assess compared to the total number of assets in AD (within 30 days of check-in)

Effective 1 July 2023.
Last revision as of 6/22/2023. Prior versions are obsolete.

Artifact

Proof of results distribution for the prior two months and signatures up to date on scanner. CND-derived artifacts consist of CCVM score, CVE table, OS chart and % of Critical/High CVEs. *Proof of AD total asset count is verified onsite.*

Task: 12.5 – Secure DNS Communication through CDT Managed Infrastructure

References
NIST SP 800-53 r5 SC-7(4)

Condition
This task measures how entity DNS internal requests are routed. Entity should ensure requests and responses are logged by entity perimeter security devices prior to being forwarded to CDT managed DNS resolvers. A Deny All, Permit by Exception (DAPE) DNS isolation policy must be in place to prohibit internal DNS queries from direct DNS root server query. This logical control enforces entity's DNS queries are routed and inspected by the CDT SOC. Any direct routing or CDT secure DNS by-pass fails this task standard. The entity must meet the following conditions:

1. All entity DNS forwarder services (on-premises and cloud) must use the following CDT managed DNS server infrastructure:

    - ns1.net.ca.gov 134.186.254.252
    - ns2.net.ca.gov 158.96.0.254
    - ns3.net.ca.gov 165.235.254.254
    - ns5.net.ca.gov 134.186.254.247
    - ns6.net.ca.gov 158.96.0.249
    - ns7.net.ca.gov 165.235.254.249

2. All entity perimeter firewalls (on-premises and cloud) contains a rule allowing DNS forwarding from all internal hosts to CDT managed DNS server infrastructure hosts only
3. All entity perimeter firewall (on-premises and cloud) contains a rule immediately following condition 2 that denies all DNS egress traffic from the network

Scoring Criteria
I Entity meets conditions 1-3

P Entity meets with condition 1 and 2 but fails to meet condition 3

N Entity fails to meet conditions 1 or 2

Scoring Note
Entity formal risk acceptance does not impact scoring criteria.

Artifact
Proof of entity's configurations is required.

Effective 1 July 2023.
Last revision as of 6/22/2023. Prior versions are obsolete.

Task: 13.1 – Boundary Protection Ingress/Egress Monitoring

References
NIST SP 800-53 r5 SC-7, SI-4(11)
NIST SP 800-171 r2 3.13.5
SAM 5350

Condition
The entity must conduct network monitoring using firewalls and intrusion detection/prevention systems of all ingress/egress points to the network. This task requires entities to demonstrate intrusion monitoring through device console access (3rd party/CDT managed devices require SLA/Statement of Boundary Protection). The entity must meet the following conditions:

1. All ingress/egress points must traverse through the following entity/3rd party compliant devices:
    - Firewall (SAM 5350)
    - Intrusion Detection/Prevention System
2. All points of ingress/egress are documented on provided network documentation

Scoring Criteria
I Entity meets conditions 1 and 2

P Entity meets condition 1 but fails to meet condition 2

N Entity fails to meet condition 1

Scoring Notes
If any entity perimeter security components assessed in this task are outsourced for 3rd party management (e.g., managed service provider), the entity is responsible for coordinating the required documentation/device access in advance of the ISA for assessment.

Artifact
- Screenshot of entity provided diagram
- Screenshot of border device connections or proof that all external connections are accounted for
- Screenshot of 3rd party/CDT managed devices must be verified through Statement of Boundary Protection from provider

Task: 13.2 – Boundary Protection Device Deployed in an Industry Best Practice Configuration

References
NIST SP 800-53 r5 SC-7(5)
NIST SP 800-171 r2 3.13.6

Condition
This task will perform an analysis of the primary boundary protection firewall rules to determine:

- Rules are implemented using a Deny All, Allow by Exception (DAPE) configuration
- Exceptions are specific to the minimum IPs and ports/protocols/applications required by role/host function
- The absence of unnecessary services allowed between externally accessible segments and their hosts (e.g., “any” rules between external or DMZ segments)
- Firewall conformed to the manufacture security best business practices
- Score overall firewall security rating is inclusive of at-risk rules, excessive ports/protocols, and best practices; security rating results are scaled from 1-100%

Scoring Criteria
I The security rating is 69.00% or greater

P The security rating is between 50.00% to 68.99%

N The security rating is 49.99% or less

Scoring Note
- The firewall for assessment will be the enterprise primary perimeter firewall. The firewall IP for this device will be provided on the assessor prior to assessment (e.g., using the Data Call worksheet).
- If the firewall is managed by a 3rd party, the entity is required to ensure the required command outputs/configuration files are provided to CND prior to the final day of the assessment period

Artifact
A formal analysis report is required of all active firewall rules configured on the device to determine if the rules implement a Deny All, Allow by Exception (DAPE) configuration. This will include the absence of excessive port assignments or use of “any” port/host/destination/service rules for external interfaces.

Effective 1 July 2023.
Last revision as of 6/22/2023. Prior versions are obsolete.

Task: 13.3 – IDS/IPS Event Monitoring, Review, and Clearance/Escalation Procedures

References
NIST SP 800-53 r5 SI-4(4)
NIST SP 800-171 r2 3.14.6

Condition
Intrusion detection/prevention controls (MITRE ATT&CK ID: M1031) should be in place for entity/3rd party provider to monitor, review, and conduct clearance/escalation of anomalous network events. The entity (or 3rd party management) must conduct routine reviews of all on-premises and cloud security appliances. The entity must meet the following conditions:

1. Entity Task 13.1 not scored as "N"
2. Routine review and clearance/escalation of events classified as Critical or High
3. Provides proof of alert distribution to responsible administrator(s), ISO, CIO
    - Clearance interval must be same day OR within 8 business hours
    - Events are investigated in accordance with entity security published plan until cleared or escalated
    - Escalated events are reported in Cal-CSIRS within 60 minutes of escalation

Scoring Criteria
I Entity meets conditions 1-3

P Entity meets conditions 1 AND 2 but fails to meet condition 3

N Entity either does not meet condition 1 OR 2

Artifact
Proof of entity's procedures of the following:

- Event review/clearance/escalation procedures
    - Escalated events are reported in Cal-CSIRS within 60 minutes of escalation
    - Entity provided proof of penetration test team detection and entry into Cal-CSIRS
- Verification of monitoring conducted via assessment provider's full network packet capture:
    - Capture location within entity's internal network; capture must include all ingress/egress traffic
    - Capture period no less than 24 hours or up to 14 TB of data
    - Summary of High/Critical risk indicators of compromise

Effective 1 July 2023.
Last revision as of 6/22/2023. Prior versions are obsolete.

Task: 13.4 – IDS/IPS Signature & Firmware Update

References
NIST SP 800-53 r5 SI-2(2)
NIST SP 800-171 r2 3.14.1

Condition
This task validates that the entity ensures the protection of hosts via maintenance of network IDS/IPS. The entity must meet the following conditions:

1. Task 13.1 is not scored as “N”
2. All deployed device signatures are within five (5) days from date of assessment
3. All deployed device firmware/software versions are EITHER:
   - Latest production maintenance release version
   - Latest stable (vendor recommended) version based on FIPS certification (vendor site confirmation required)

Scoring Criteria
I Entity meets conditions 1-3

P Entity meets conditions 1-2 BUT fails to meet condition 3

N Entity fails to meet condition 1 OR 2

Scoring Note
If release date of the newest software/firmware is within 30 days of assessment date, the prior version will be used to score this portion of the task.

Artifact
Proof of configuration output AND proof of vendor latest production/stable recommended version at time of assessment.

Task: 13.5 – SSL/SSH Traffic Inspection and Analysis

References
NIST SP 800-53 r5 SI-4(25)
NIST SP 800-171 r2 3.14.6

Condition
This task validates that the entity enforces all SSL/SSH traffic entering or exiting the network through a break and inspect proxy (MITRE ATT&CK ID: M1020). The entity must meet the following conditions:

1. All traffic routed to the SSL/SSH proxy for evaluation
2. All traffic is evaluated based on content classification tag
3. Prior to forwarding, all traffic must be either:
    a. Force-decrypted and inspected by the entity intrusion detection/prevention system or 3rd party solution
    b. Logged as exempted due to specified written entity privacy requirements. These privacy requirements are to be identified in the traffic content classification tagging (e.g., religious consultation, legal consultation, medical diagnosis, personal financial transactions, etc.)

Scoring Criteria
I Entity meets conditions 1-3

P Entity meets conditions 1-2 and meets condition 3a but fails to meet condition 3b

N Entity fails to meet condition 1 OR condition 3a

Artifact
Proof of SSL/SSH inspection device configuration detailing break and inspect settings.

Task: 13.6 – Reoccurring Primary External Website Analysis

References
NIST SP 800-53 r5 SI-10

Condition
This task assesses the entity's analysis of its primary public external web site/application no less than quarterly. Assessment detects at-risk configurations, end-of-life applications, information leaks, and other security risks related to the provisioning of the content and data rendered (MITRE ATT&CK ID: T1190). Scans must cover the assessment of common web application vulnerabilities to include, but not limited to, the following:

- SQL injection
- Cross-site scripting
- Out-of-date/risky component usage
- Directory browsing
- Risky SSL implementations and configurations
- OS related exposures and risks
- Local/remote file inclusion vulnerabilities
- Local/remote code execution vulnerabilities
- Sensitive information/configuration leak/exposure
- Web input validate/sanitization errors

Scoring Criteria
I Entity conducts website scans for web application component and code-related risks in an interval of every 90 days or less

P Entity conducts website scans for web application component and code-related risks in an interval of between 91-364 days

N No evidence that entity conducts website scans for web application component and code-related risks within the past 365 or more

Scoring Note
This scan must be conducted using a product or analytics template specifically designed to assess and identify web-based risks. A standard host vulnerability scanner does not meet the criteria standard for this task. If the entity's external website is managed by a 3rd party provider, the entity is responsible to coordinate the required documentation/device access in advance of the ISA for assessment.

Artifact
Results of a web application analysis of the entity's primary web presence for at-risk configurations, data leaks, and vulnerabilities is required. Findings rated with a CVSS rating of Moderate or higher must be identified separately.

Effective 1 July 2023.
Last revision as of 6/22/2023. Prior versions are obsolete.

Task: 14.1 – Entity Log Generation and Retention

References
NIST SP 800-53 r5 AU-12
NIST SP 800-171 r2 3.3.2
SAM 5335.2

Condition
This task validates that the entity generates and retains the required minimum key audit logs identified for a period of 6 months or longer.

Minimum Key Audit Logs and Minimum Retention Period

1. IDS/IPS events (*minimum storage period of 90 days per CISO policy exemption*) is retained for at least 90 days
2. DNS ingress/egress is retained for 6 months
3. Web Usage (Proxy) is retained for 6 months
4. Firewall Events is retained for 6 months
5. Centralized File Storage Access Auditing (File Read/Write events; including OneDrive, SharePoint Online) is retained for 6 months
6. Domain Controller Events is retained for 6 months
7. Application User Account Creation, Login Events is retained for 6 months

Scoring Criteria
I Entity meets retention conditions for log types 1-7

P Entity meets retention conditions for log type 1 BUT fails to meet one of log retention conditions for log types 2-7

N Entity meets retention conditions for log type 1 OR fails to meet two or more of log types 1-7

Scoring Notes
Combined logs, utilization of SIEM devices, and off-line storage are acceptable, so long as the entity can demonstrate the task requirements are met. Log forwarding of all required logs to CDT SOC will meet the criteria of this task.

Artifact
Proof of the earliest retained log entry is required to demonstrate compliance of log retention. For logs forwarded to CDT SOC, verification of log type received by CDT SOC required.

Effective 1 July 2023.
Last revision as of 6/22/2023. Prior versions are obsolete.

Task: 15.1 – Distribution of Cybersecurity Alerts, Messages, and Warnings

References
NIST SP 800-53 r5 SI-5
NIST SP 800-171 r2 3.14.3

Condition
This task determines whether the entity documents subscription to CDT (e.g., Cal-CSIRS notifications), Cal-CSIC (Intelligence Bulletins), Government notification list servers, and industry cybersecurity notifications to stay updated on current threat tactics. The entity must provide timely distribution of relevant received alerts/notifications to appropriate (cleared) internal communities of interest (MITRE ATT&CK ID: M1019). The entity must meet the following conditions:

1. Demonstrates access to Cal-CSIRS reporting/notifications
2. Documents receipt of Cal-CSIC/CDT-OIS distributed security notices/bulletins
3. Documents receipt of other government/industry relevant cybersecurity notifications
4. Documents redistribution of relevant notifications to internal communities of interest

Scoring Criteria
I Entity meets conditions 1-4

P Entity meets conditions 1 and 2 BUT fails to meet condition 3 AND/OR 4

N Entity fails to meet EITHER conditions 1 or 2

Artifact
Proof of receipt and redistribution of alerts, messages, or warning received to associated internal communities of interest is required.

Task: 16.1 – Penetration Test External Open-Source User Identity Collection

References
NIST SP 800-53 r5 AT-2(3), AU-13
SIMM 5315A (II B)

Condition
This task identifies the entity's risk exposure to publicly available identity-based metadata pertaining to its users past and present. This information provides attackers insight to valid usernames, valid email addresses and format, applications in use, and associated users with business function. Using these collected data points, the attacker can more effectively form password spraying and spear phishing attacks against the target entity (MITRE ATT&CK ID: T1589). The Pen Test team will use active and passive reconnaissance techniques to acquire relevant and actionable information where possible.

Scoring Criteria
I Harvested users are 5.00% or less of total users

P Harvested users are between 5.01% to 9.99% of total users

N Harvested users are 10.00% or greater of total users

Scoring Notes
- Total users will be derived from authoritative directory (i.e., Active Directory, OpenLDAP, eDirectory, etc.) provided in Data Call
- Do not count non-user specific identities (e.g., Distribution groups, Info, Webmaster, etc.) in the total accounts collected
- Scoring Formula: Total unique identities collected/entity declared total user accounts

Artifact
Proof of non-compliant, deduplicated listing of identities collected from public sources is required.

Task: 16.2 – Penetration Test External Spear Phishing Attempt

References
NIST SP 800-53 r5 AT-2(1)
NIST SP 800-171 r2 3.2.2

Condition
This task assesses the entity's ability to react to a simulated threat actor directed spear phishing campaign derived from data collected via public/open sources only. This campaign must attempt to acquire credentials and may include a malicious code execution component. All campaigns by CND are initiated during the entity's normal business hours. The entity must meet the following conditions:

1. No phished users provided credentials
2. No footholds obtained on entity managed hosts from phished users
3. Entity complies with assessment rules of engagement and directives regarding this task

Scoring Criteria
I Entity meets all conditions

P Less than 6 phished users fail condition 1 AND entity meets conditions 2 and 3

N 6 or more phished users fail condition 1 OR entity fails either condition 2 or 3

Artifact
List of all user names/email addresses that provided plaintext credentials resulting from this task are required. Do not provide a copy of the password in this listing artifact.

Task: 16.3 – Penetration Test External Password Guessing Activities

References
NIST SP 800-53 r5 IA-5
NIST SP 800-63B Para 5.11
NIST SP 800-171 r2 3.5.7

Condition
This task simulates a threat actor's ability to derive logon credentials while external to the entity network using brute force techniques (MITRE ATT&CK ID T1110) including password spraying and password guessing. This process can include informed guessing via resources such as vendor documentation, key phrases on public websites, common passwords, and password dumps from public sources.

Scoring Criteria
I No valid credentials guessed from the external network

P Less than 6 standard user credentials guessed from the external network

N 6 or more standard user credentials guessed OR any privileged user credentials guessed from the external network

Scoring Note
If the Pen Test team fails to locate a suitable and safe external application to conduct spraying operations against, lacks access via an improperly protected remote access solution, or lacks an internal foothold via external password spraying to conduct external spraying operations, this task will be scored as "I".

Artifact
Proof of the following is required in order of precedence:

- Screenshot of all privileged user credentials guessed
- Screenshot of all standard user credentials guessed
- Screenshot documenting failed password guessing attempt

Task: 16.4 – Penetration Test External Credential Hash Capture and Cracking Operations

References
NIST SP 800-53 r5 IA-5(1)
NIST SP 800-63B (Para 5.11)
NIST SP 800-171 r2 3.5.4

Condition
This task will assess the entity's risk exposure to Man-in-the-Middle authenticator hash capture (MITRE ATT&CK ID: T1040), hash harvesting from exploited hosts (MITRE ATT&CK ID: T1003), and extraction of authenticator hashes from network directory services (MITRE ATT&CK ID: T1558.003). Captured hashes will be subjected to offline cracking attempts using dictionary and brute force attack methods for a period not to exceed the assessment period to assess cracking resistance (MITRE ATT&CK ID: T1110).

Scoring Criteria
I Inability to successfully crack any hash captured/acquired during the engagement period

P Between 1-5 standard user hashes cracked during the engagement period

N 6 or more user level hashes cracked OR any administrative or elevated privilege level hash was cracked during the engagement period

Scoring Notes
- If the Pen Test fails to acquire access via an exposed web application credential store, an improperly protected remote access solution, or lacks an internal foothold via external password spraying to conduct hash capture/extraction operations, this task will be scored as "I"
- This task does not assess wireless hash cracking efforts. Reference task 17.5 for those activities

Artifact
Any of the following, listed in order of precedence (Do not display plain-text passwords in the artifact):

- Screenshot of any successful privileged user hash cracked
- Screenshot of any user successful hash cracked
- If a hash was captured but not cracked, display the hash

Effective 1 July 2023.
Last revision as of 6/22/2023. Prior versions are obsolete.

Task: 16.5 – Penetration Test External Undeclared Hosts/Networks

References
NIST SP 800-53 r5 CM-8

Condition
This task simulates a threat actor's attempt to gather information about the victim's networks as part of their pre-attack, targeting phase (MITRE ATT&CK ID: T1590). To validate the entity's knowledge and documentation of allocation assets/networks, a comparison of network exposures in the pre-attack phase is compared to the entity Data Call provided prior to assessment start date.

Scoring Criteria
I All entity (operated or controlled, internet exposed) hosts are declared within the external IP ranges provided for assessment

P Less than 6 entity (operated or controlled, internet exposed) hosts are not declared within the external IP ranges provided for assessment

N 6 or more entity (operated or controlled, internet exposed) hosts not declared within the external IP ranges provided for assessment

Scoring Note
If entity resources are potentially identified as not listed on the Data Call, then they must be verified as internet accessible and determined as operated or controlled by the entity to be scored as a finding in this task.

Artifact
- Proof of non-compliance for any entity undeclared host/IP range(s) is required.
- Proof of active host response documenting the finding is required

Task: 16.6 – Penetration Test External High-Risk Service Exposure Detection

References
NIST SP 800-53 r5 CM-7(1)
NIST SP 800-171 r2 3.4.7

Condition
This task assesses the entity's exposure of High-risk services to the internet (MITRE ATT&CK ID: T1557). Using results from various service analysis techniques of in-scope and undeclared assets, the CND will identify any detected instances of services including, but not limited to the following:

- NetBIOS
- SMB/NFS/CIFS
- Authenticated FTP
- Clear text administration services
- Unencrypted LDAP
- Externally exposed peripheral devices (i.e., printers, cameras, power management, environmental monitors, etc.)

Scoring Criteria
I Entity has no externally exposed high-risk services

P Less than 6 instances of externally exposed high-risk services

N 6 or more instances of externally exposed high-risk services

Scoring Note
- Validate exposed services using an appropriate tool/utility
- Perimeter devices that misrepresent open status of these services may adversely affect the entity score
- Proxy devices that perform redirects may adversely misrepresent service exposures

Artifact
Proof of non-compliance of scan output detailing the IP address and High-risk service exposure detected is required.

Effective 1 July 2023.
Last revision as of 6/22/2023. Prior versions are obsolete.

Task: 16.7 – Penetration Test External Host Management Service Detection

References
NIST SP 800-53 r5 SC-2(1), SC-7
NIST SP 800-171 r2 3.13.3

Condition
This task identifies poorly secured host management services and web application administrative interfaces exposed to the internet (MITRE ATT&CK ID: T1219). This entity external network must be absent of any instance of the following externally exposed services:

- Remote host management logins (RDP, VNC, SSH, Telnet, TFTP, Team Viewer, LogMeIn, GoToMyPC, etc.)
- Bare metal host management services (e.g., IPMI, AMT, ILO, or equivalent)
- Infrastructure/device administrative logon interfaces (Cisco Level-15 webpages, proxy/firewall/IPS Administrator, device/appliance logon pages that offer an administrator option, etc.)

Scoring Criteria
I No instances of externally exposed services

P Less than 6 instances of externally exposed services

N 6 or more instances of externally exposed services

Scoring Note
An attempt will be made to determine if the exposure is protected by CDT-approved MFA. If protection is validated, then the exposure will be noted but not scored.

Artifact
Proof of externally exposed services detected is required.

Task: 16.8 – Penetration Test External Web Application Misconfigurations and Exposures

References
NIST SP 800-53 r5 SA-11(3)
NIST SP 800-171 r2 3.11.2

Condition
This task identifies and probes selected in-scope and undeclared external websites and web applications to determine potential attack opportunities (MITRE ATT&CK ID: T1190). Research and analysis are conducted to identify exploits and misconfigurations, achieve unauthorized access, detect non-public data exposure, and/or obtain unauthorized remote host access. Measured web application/hosts should be absent of the following:

- Measured web application/hosts should be absent of non-public data exposure
- Insecure configurations that result in any findings of ≥ Moderate level risk(s)
- Browsable/directory listing
- Error messages with excessive/actionable details
- Exploitable database connections that result in the potential for data modification or extraction
- Misconfigurations that result in host or client compromise

Scoring Criteria
I No risk(s) rated as Moderate/Medium risk or higher based on industry best practice/CVE exposure score

P Less than 6 risk(s) rated as Moderate/Medium risk based on industry best practice/CVE exposure score

N Any of the following conditions:

- 6 or more risks rated as Moderate/Medium risk based on industry best practice/CVE exposure score
- Any risk rated at High or Critical level based on industry best practice/CVE exposure score
- Any condition that results in the successful alteration/extraction of sensitive host configuration information, exfiltration of host data (e.g., SQL Table extraction, non-public data acquisition, etc.), and/or exploitation of the host or application

Artifact
A detailed findings report, and an example of highest risk findings is required.

Effective 1 July 2023.
Last revision as of 6/22/2023. Prior versions are obsolete.

Task: 16.9 – Penetration Test External Execution of Malicious Code on Controlled Host

References
NIST SP 800-53 r5 CA-8

Condition
The successful exploitation of hosts or services operated, controlled, or provided via 3rd party to the entity. Exploitation of hosts must occur via the introduction of malicious code execution (MITRE ATT&CK ID: T1204.002) or host misconfiguration (MITRE ATT&CK ID: T1574) and result in any of the following outcomes:

- Establishment of host command and control (C2)
- Lateral movement
- Sensitive data exposure (including database exploitation not acquired via Task 16.8)
- Privilege escalation
- Credential acquisition via C2 implant/foothold (plaintext/hash)
- Any resulting configuration that leads to risky activity conducted via an external threat actor (e.g., non-privileged user joins host to the domain via VPN/remote access solution, anonymous directory enumeration, etc.)

Scoring Criteria
I No exploitation of entity controlled, operated, or 3rd party provided service/host

P Exploitation of one entity controlled, operated, or 3rd party provided service/host

N Exploitation of two or more entity controlled, operated, or 3rd party provided service/host

Scoring Note
A foothold is scored as successful if the external C2 channel remains attacker accessible for > 10 minutes. Entity/automated identification and termination of access prior to that time is not considered successful for the purposes of this task.

Artifact
Timestamped log entries of other documentation is required that demonstrates the window of creation and continued accessibility for the minimum validation window.

Task: 17.1 – Penetration Test Internal Password Guessing, Spraying, and Default Credential Detection

References
NIST SP 800-53 r5 IA-5
NIST SP 800-63B (Parag. 5.11)
NIST 800-171 r2 3.5.7

Condition
This task addresses two unique methods of obtaining passwords – password guessing and password spraying. Password spraying is the process of using informed knowledge such as acquired usernames in combination with common password dictionaries or common entity terminology to guess a username/password combination using brute force techniques (MITRE ATT&CK ID T1110). Default credential testing, when password guessing, utilizes well-known, often public information from application/hardware manufactures installation manuals to inform password guessing attempts on the targeted application/host (MITRE ATT&CK ID T1078).

Scoring Criteria
I No valid credentials guessed from the internal network

P Less than 6 standard user credentials guessed from the internal network

N 6 or more standard user credentials guessed OR any privileged user credentials guessed from the internal network

Artifact
Proof of the following is required in order of precedence:

- Screenshot of all privileged user credentials guessed
- Screenshot of all standard user credentials guessed
- Screenshot documenting failed password guessing attempt

Task: 17.2 – Penetration Test Internal Credential Hash Capture and Cracking

References
NIST SP 800-53 r5 IA-5
NIST SP 800-63B (Para 5.11)
NIST SP 800-171 r2 3.5.4

Condition
This task will assess the entity's risk exposure to Man-in-the-Middle authenticator hash capture (MITRE ATT&CK ID: T1040), hash harvesting from exploited hosts (MITRE ATT&CK ID: T1003), and extraction of authenticator hashes from network directory services (MITRE ATT&CK ID: T1558.003). Captured hashes will be subjected to offline cracking attempts using dictionary and brute force attack methods for a period not to exceed the assessment period to assess cracking resistance (MITRE ATT&CK ID: T1110).

Scoring Criteria
I No credential hash(es) cracked from the internal network assessment

P Less than 6 internally acquired standard user credential hash(es) cracked

N 6 or more internally acquired standard user credential hash(es) cracked OR any privileged user credential hash(es) cracked

Scoring Note
Wireless handshake cracking efforts are assessed in Task 17.5 – Penetration Test Internal Wireless Network Breach Resistance.

Artifact
Proof of non-compliance of all captured hashes and outcomes from cracking attempts/outcomes. Successfully cracked hashes should be masked for security purposes.

Task: 17.3 – Penetration Test Internal Use of Insecure Host Management Services

References
NIST SP 800-53 r5 AC-17(2), CA-8(2)

Condition
This task attempts to identify any management service/interface that allows unencrypted access, weak encryption services, utilizes well-known community strings, or can be exploited using remote code execution methods places the entity at enhanced risk (MITRE ATT&CK ID: T1219). The at-risk services searched for include, but are not limited to, the following:

- FTP services utilizing passwords
- SSH (with null passwords/guessable passwords)
- Acceptance of credentials in clear text by administration services
- Any occurrence of Cisco Smart Install
- SNMP (utilizing common/default/guessed community strings)
- Exploitable host management exposures (e.g., IPMI, AMT, ILO, etc.)

Scoring Criteria
I No insecure host management services

P Less than 6 instances of insecure host management services

N 6 or more instances of insecure host management services

Artifact
Proof of non-compliant service scan results or other documentation detailing the exposure of any of the remote management services identified in this task.

Task: 17.4 – Penetration Test Internal Web Site/Application Risks

References
NIST SP 800-53 r5 SA-11(3)

Condition
This task identifies and probes selected in-scope and undeclared, internal websites and web applications to determine potential attack opportunities (MITRE ATT&CK ID: T1190). Research of web risks and analysis are conducted to identify exploits and misconfigurations, achieve unauthorized access, detect non-public data exposure, or obtain unauthorized remote host access. Measured web application/hosts should be absent of the following:

- Sensitive data exposure without credentials
- Detailed Error messages exposing configuration errors
- Directory browsing/listing
- Exploitable database connections that result in the potential for data modification or extraction
- Insecure configurations that result in any findings of ≥ Moderate level risk(s)
- Misconfigurations that result in host or client compromise
- Management Authentication By-pass Methods (*excludes password guessing*)

Scoring Criteria
I No risk(s) that results in the successful alteration/extraction of sensitive host configuration information, exfiltration of host data (e.g., SQL Table extraction, non-public data acquisition, etc.), and/or exploitation of the host or application

P Less than 2 risk(s) that results in the successful alteration/extraction of sensitive host configuration information, exfiltration of host data (e.g., SQL Table extraction, non-public data acquisition, etc.), and/or exploitation of the host or application

N 2 or more risk(s) that results in the successful alteration/extraction of sensitive host configuration information, exfiltration of host data (e.g., SQL Table extraction, non-public data acquisition, etc.), and/or exploitation of the host or application

Artifact
A detailed finding report and example of highest risk findings is required.

Effective 1 July 2023.
Last revision as of 6/22/2023. Prior versions are obsolete.

Task: 17.5 – Penetration Test Internal Wireless Network Breach Resistance

References
NIST SP 800-53 r5 AC-18(1)
NIST SP 800-171 r2 3.1.17

Condition
This task assesses the entity's protection of their wireless access at the network perimeter. The successful breach of a wireless network requires the capture of the 4-way handshake between any client and access point. This data provides a hash value of the credentials required for authentication. Once captured, a series of dictionary and brute force attacks on the hash can be performed to attempt to crack the password. The entity wireless infrastructure must meet the following conditions:

1. Prevent capture of 4-way handshake via de-authentication or other threat actor methods
2. If 4-way handshake is captured, the password must not be cracked during assessment
3. Entity provided public wireless network service successfully isolates public users from entity internal network resources

Scoring Criteria
I Entity meets all conditions

P Entity fails to meet condition 1, but meets conditions 2-3

N Entity fails to meet two or more conditions

Artifact
The following artifacts are required for this task, as applicable:

- Proof of entity non-compliance thru the assessment provider's wireless breaching attempts
    - Cracking of 4-way handshake capture
    - Breach of public wireless boundaries
    - Successful capture of 4-way handshake
- Proof of entity compliance if assessment provider fails to capture/crack 4-way handshake and/or breach of public wireless boundary.

Effective 1 July 2023.
Last revision as of 6/22/2023. Prior versions are obsolete.

Task: 17.6 – Penetration Test Internal Execution of Malicious Code on Controlled Host

References
NIST SP 800-53 r5 CA-8

Condition
This task attempts the successful exploitation of hosts or services operated, controlled, or provided via 3rd party to the entity. Exploitation of hosts must occur via the introduction of malicious code execution (MITRE ATT&CK ID: T1204.002) or host misconfiguration (MITRE ATT&CK ID: T1574) and result in any of the following outcomes:

- Successful execution of malicious code resulting in unauthorized access/information leak on an entity-controlled device
- Establishment of host command and control (C2)
- Lateral movement
- Sensitive data exposure (including database exploitation not acquired via Task 17.4)
- Privilege escalation
- Credential acquisition via C2 implant/foothold (plaintext/hash)
- Any resulting configuration that leads to risky activity conducted by a threat actor (e.g., non-privileged user joins host to the domain, anonymous directory account enumeration, etc.)

Scoring Criteria
I No exploitation of entity controlled, operated, or 3rd party provided service/host and entity provided proof of penetration test team detection

P Exploitation of one entity controlled, operated, or 3rd party provided service/host

N Exploitation of two or more entity controlled, operated, or 3rd party provided service/host

Scoring Note
A foothold is scored as successful if the internal C2 channel remains accessible for > 10 minutes. Entity/automated identification and termination of access prior to that time is not considered successful for the purposes of this task.

Artifact
Proof of compliance such as timestamped log entries or other documentation that demonstrates the window of creation and continued accessibility for the minimum validation window.