<Date>

CyberApprentice

Policy Plans based off NIST

By CyberApprentice

Table of Contents

[**Review** 2](#_Toc32083889)

# **Introduction**

This document will make you compliant with the following standards at they were referenced in the making of this document:

* NIST SP 800-115 (2008) – In Progress
* NIST SP 800-37R1 (2014) – Not Started

# **Review**

* System Configuration Review
  + System configuration review is the process of identifying weaknesses in security configuration controls, such as systems not being hardened or configured according to security policies.
  + The Security Content Automation Protocol (SCAP) is a method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation. SCAP is used to conduct system configuration review.
  + If automated checking is unavailable, manual review is utilized. Manual reviews are conducted using security configuration guides or checklists to verify that system settings are configured to minimize security risks. The checklist used is located at <http://checklists.nist.gov/>.

# IDS/IPS/Firewall

* Sensor placement
  + ­ At the perimeter, to assess traffic entering and exiting the network
  + ­ Behind firewalls, to assess that rulesets are accurately filtering traffic
  + ­ Behind IDSs/IPSs, to determine if signatures are triggering and being responded to appropriately
  + ­ In front of a critical system or application to assess activity
  + ­ On a specific network segment, to validate encrypted protocols.

# HIDS/File integrity checking

* File integrity checkers provide a way to identify that system files have been changed computing and storing a checksum for every guarded file, and establishing a file checksum database

# Cryptography

* Federal agencies are required by Federal Information Processing Standard (FIPS) PUB 140-2, Security Requirements for Cryptographic Modules11, to use SHA (e.g., SHA-1, SHA-256).

# Logs

* ­Logs to be collected
  + Authentication server or system logs may include successful and failed authentication attempts.
  + ­ System logs may include system and service startup and shutdown information, installation of unauthorized software, file accesses, security policy changes, account changes (e.g., account creation and deletion, account privilege assignment), and privilege use.
  + ­ Intrusion detection and prevention system logs may include malicious activity and inappropriate use.
  + ­ Firewall and router logs may include outbound connections that indicate compromised internal devices (e.g., rootkits, bots, Trojan horses, spyware).
  + ­ Firewall logs may include unauthorized connection attempts and inappropriate use.
  + ­ Application logs may include unauthorized connection attempts, account changes, use of privileges, and application or database usage information.
  + ­ Antivirus logs may include update failures and other indications of outdated signatures and software.
  + ­ Security logs, in particular patch management and some IDS and intrusion prevention system (IPS) products, may record information on known vulnerable services and applications.

# Security/Penetration Testing

* Testing is the process of exercising one or more assessment objects under specified conditions to compare actual and expected behaviors
  + Plan
    - planning phase is used to gather information needed for assessment execution—such as the assets to be assessed, the threats of interest against the assets, and the security controls to be used to mitigate those threats—and to develop the assessment approach.
  + Execute
    - Primary goals for the execution phase are to identify vulnerabilities and validate them when appropriate
  + Post-execution
    - The post-execution phase focuses on analyzing identified vulnerabilities to determine root causes, establish mitigation recommendations, and develop a final report
* A penetration focused methodology involves the following stages:
  + Planning
    - Put together a strategy to communicate with the asset owners
    - Receive consent
  + Discovery
    - Discover network port, services, hostnames, IP information, employee names and contact information, system information, shares, and application & service information.
    - Discover vulnerabilities
  + Attack
    - Exploit vulnerabilities
  + Reporting
    - Showcase vulnerabilities, those that were exploitable, potential mitigations, and provide a risk rating
* Organizations should consider conducting less labor-intensive testing activities on a regular basis to ensure that they are maintaining their required security posture. A well-designed program of regularly scheduled network and vulnerability scanning, interspersed with periodic penetration testing, can help prevent many types of attacks and reduce the potential impact of successful ones

# Social Engineering

* Social engineering is an attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks
* Examples: phishing, analog (e.g., conversations conducted in person or over the telephone) and digital (e.g., e-mail, instant messaging).

# Network Discovery

* Network discovery uses a number of methods to discover active and responding hosts on a network. Network discovery may also detect unauthorized or rogue devices operating on a network.
* A disadvantage to active discovery is that it tends to generate network noise, which sometimes results in network latency. The ability to successfully discover all network systems can be affected by environments with protected network segments and perimeter security devices and techniques (e.g. Firewalls, fake information). The information received is seldom completely accurate since only on, connected, and those that respond will be identified.
* Techniques & terminology
  + Network port and service identification involves using a port scanner to identify network ports and services operating on active hosts (e.g. FTP, IIS)
  + Information gathered during an open port scan can assist in identifying the target operating system through a process called OS fingerprinting, but this is not foolproof.
  + Some scanners can help identify the application running on a particular port through a process called service identification.
  + identify the service application and application version is called version scanning. Banner grabbing involves capturing banner information transmitted by the remote port when a connection is initiated. This information can include the application type, application version, and even OS type and version.
* Perform external scanning first, then internal scanning. External scanning tests the security appliances (i.e. firewall, IDS) in place and logs can be reviewed to understand alerts and vulnerability of scans.
* Aggressive scans that may cause a DoS should be conducted during periods of low network traffic (e.g. overnight or weekends) to cause minimal impact to operations. Port scanning can disrupt network operations by consuming bandwidth and slowing network response times
* Vulnerability scanning identify vulnerabilities. It can help identify outdated software versions, missing patches, and misconfigurations, and validate compliance with or deviations from an organization’s security policy. In addition, it may provide information on targets for penetration testing and how to mitigate discovered vulnerabilities.
* Vulnerability scanners rely on a repository of signatures. This requires the assessors to update these signatures frequently to enable the scanner to recognize the latest vulnerabilities. In addition, this leads to a varied level of false positives. It is recommended to **use multiple scanners** to compare results.
* Wireless scanning should also be considered. Tools being considered should be capable of scanning IEEE 802.11a/b/g/n channels, Bluetooth, and additional radio frequency capturing capability (e.g. external antenna). Bonuses are mapping and GPS-enabled mapping. It is important to review signal strength.

# Passwords

* Passwords will be strong. Strong means they will be complex and have sufficient length according to the importance of the account. Complex is at least of and a combination of lowercase, uppercase, numbers, and special characters.
* Passwords will be tested through password cracking methodologies.

# Frequency/Scheduling Guidance

* Another consideration is whether any system or network activities required by the testing may impact the functionality or security of the environment— for example, if a major upgrade is about to be conducted, testing might be delayed until the upgrade has been completed.
* Assessment frequency is often driven by an organization’s requirements to demonstrate compliance with specific regulations or policies (i.e. NIST 800-53 series)
* This prioritization is based on system categorization, expected benefits, scheduling requirements, and applicable regulations where assessment is a requirement
* Me Stuff:
  + security configuration checklists for IT products at http://checklists.nist.gov/.
  + Documentation:
    - security policies, architectures, and requirements; standard operating procedures; system security plans and authorization agreements; memoranda of understanding and agreement for system interconnections; and incident response plans.
    - Logs
      * NIST SP 800-92, Guide to Security Log Management
      * Authentication server or system logs may include successful and failed authentication attempts.
      * ­ System logs may include system and service startup and shutdown information, installation of unauthorized software, file accesses, security policy changes, account changes (e.g., account creation and deletion, account privilege assignment), and privilege use.
      * ­ Intrusion detection and prevention system logs may include malicious activity and inappropriate use.
      * ­ Firewall and router logs may include outbound connections that indicate compromised internal devices (e.g., rootkits, bots, Trojan horses, spyware).
      * ­ Firewall logs may include unauthorized connection attempts and inappropriate use.
      * ­ Application logs may include unauthorized connection attempts, account changes, use of privileges, and application or database usage information.
      * ­ Antivirus logs may include update failures and other indications of outdated signatures and software.
      * ­ Security logs, in particular patch management and some IDS and intrusion prevention system (IPS) products, may record information on known vulnerable services and applications.
    - IDS/IPS/Firewall Rulesets
      * ­ For router access control lists
        + Each rule is still required (for example, rules that were added for temporary purposes are removed as soon as they are no longer needed) – Only traffic that is authorized per policy is permitted, and all other traffic is denied by default
      * ­ For firewall rulesets
        + Each rule is still required – Rules enforce least privilege access, such as specifying only required IP addresses and ports – More specific rules are triggered before general rules – There are no unnecessary open ports that could be closed to tighten the perimeter security – The ruleset does not allow traffic to bypass other security defenses – For host-based firewall rulesets, the rules do not indicate the presence of backdoors, spyware activity, or prohibited applications such as peer-to-peer file sharing programs
      * ­ For IDS/IPS rulesets
        + Unnecessary signatures have been disabled or removed to eliminate false positives and improve performance – Necessary signatures are enabled and have been fine-tuned and properly maintained.
    - NIST SP 800-53A discusses the framework for development of assessment procedures, describes the process of assessing security controls, and offers assessment procedures for each control. NIST SP 800-53A was developed to be used in conjunction with NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems. NIST SPs 800-53, 800-53A, and 800-37

**Bibliography (16th Edition Chicago Style)**