C NIST SP800-115

This appendix provides an overall view of the NIST Special Publication 800-115. It only parses the essential concepts and assessment techniques that this standard provides.

C.1 Introduction

NIST SP 800-115 provides, in the form of a technical guide, some guidelines concerning the organizations on planning and conducting technical information security assessment and testing. In addition, it proposes analysis and development methods of findings and mitigation strategies. It also contains an overview of the key elements of assessment and testing processes by giving practical instructions for implementing, designing and maintaining related technical information. Another important aspect is that this standard emphasizes specific techniques in this field discussing their benefits, limitations and recommendations of use. Note that, however, this focuses on explaining how these different techniques can be performed, and does not specify which techniques should be used for which circumstances. This is then to be considered as an How-To manual.

The most commonly used techniques are grouped into three categories : **Review Techniques**, **Target Identification and Analysis**, **Target Vulnerability Validation**. There is no one specific technique which can provide a complete picture of the security of a system or a network. That is why depending on the skill of the test team, the organizations should combine some appropriate techniques in order to ensure consistent assessment results.

However, there also exist many non-technical techniques that may be used in addition to or instead of the forementioned technical techniques. For example, physical security testing could confirm the presence of physical vulnerabilities by trying to bypass some physical security controls (e.g. locks, badge reader and so forth). This document does not focus on these techniques but it is interesting to mention them to understand their values and to consider when they may be more appropriate to be used.

C.2 Assessment Methodology & Methods

Terminology First, two important definitions are provided in the NIST SP 800-115, which are a foundation of what follows :

> **Security assessment** : This relates to the process of finding an effective way in order to ensure that an entity being assessed meets predefined security objectives.
>
> **Assessment object** : This represents an entity being assessed, e.g. a system, a network but also a person, a procedure and so forth.

Methodology According to NIST SP800-115, a documented security assessment methodology is beneficial in that it can provide consistency and structure to security testing (minimizing testing risks) and accelerate the transition of new assessment staff. Moreover, the methodology must address resource constraints associated with security assessment which requires resources such as time, staff, hardware and software. These resources are often limiting factors in the type and frequency of security assessments.

The organization should evaluate the type of security tests and examinations. By doing so, this gives it the ability to decrease time to conduct the assessment and the need to purchase testing equipment and software by reusing pre-established resources such as trained staff and standardized testing platforms which can considerably reduce overall assessment costs.

The security assessment methodology in different phases offers a number of advantages. The standard states that the methodology should contain at minimum the following phases :

1. **Planning** : First of all the security assessment should be planned as any other project by defining the scope, objectives, team roles and responsibilities, etc... Planning is critical to the success of a security assessment. This phase aims to gather the required information for the execution of the assessment (i.e. the entities to be assessed, the threats of interest and so forth).
2. **Execution** : The first goal of this phase is to identify vulnerabilities and validate them if appropriate. This phase concerns activities related to the intended assessment technique and allows the assessors to identify the system, network and eventual vulnerabilities in the organizational process.
3. **Post-Execution** : This phase concerns the determination of the root causes of identified vulnerabilities and contains eventual mitigations and recommendations in addition to reporting.

Assessment Methods According to the standard, three different methods are defined :

- **Testing** : The method that compares actual and expected behaviors of one or more assessment objects when exercising under specified conditions.
- **Examination** : The method of inspecting, studying or analyzing one or more assessment objects in order to facilitate understanding in order to obtain evidence or clarification.
- **Interviewing** : The method of conducting discussions with individuals or groups within the same organization in order to facilitate the understanding in order to obtain some clues or clarifications.

Examinations primarily concern the review of some existing documents as security requirements, architecture diagrams, engineering documentation or even system logs. The main goal behind examination is to determine weather a given system is well documented and to get an overview over some security aspects that are only available through documentation reading. The assessors should ensure that all procedures and configurations are compliant with predefined internal policies and consistent with security requirements.

Testing concerns hands-on work with systems (selected ones) and networks (entire enterprise) to identify security vulnerabilities. Moreover, testing allows to measure levels of compliance in different areas such as configuration management, patch management, etc. The combination of scanning and penetration techniques can provide important information regarding potential vulnerabilities and allows to predict the likelihood that an attacker will be able to exploit them.

Testing versus Examination Testing is limited by resources (narrow scope) meaning that it does not always provide a comprehensive evaluation of the security posture. The main limitation is the time ; a malicious attacker has no time restriction in order to perform an exploit that allows him to penetrate a system or network. Another important thing is that the attacker is not constrained by the used testing techniques he/she can use whatever techniques they feel necessary. Globally testing is less likely than examinations to determine weaknesses related to internal policies or current configuration. Combining these two methods offers a more accurate view of security.

C.3 Review Techniques

Review techniques passively examine systems, generally manually conducted and aim to evaluate systems, applications, networks, policies and procedures in order to discover eventual vulnerabilities. This subsection presents some common review techniques that help assessors to gather information in order to optimize other assessment techniques.

C.3.1 Documentation review

Method Examination & Interviewing

Description This helps to discover some weaknesses and gaps which influence the implementation of security controls. The assessors must check that organization's documentation is compliant with some regulations and standards. The goal of this technique is not to ensure a proper implementation of security controls, it only helps to ensure that guidance exists to support the security infrastructure.

As previously mentioned, this technique can be used to fine-tune other testing or examination techniques. Concretely, if an organization has its own password management policy concerning the minimum password length and complexity, this information could be used in order to implement password-cracking tools then improving the performance and accuracy of the related tests.

C.3.2 Log review

Method Examination

Description This aims to determine if the security measures are logging the important information, and if the organization is compliant with log management policies. For example, if the logging policy states that all authentication attempts to a given critical server must be logged, this technique must ensure the existence of these logs and verify if there is an appropriate level of detail. This may also reveal problems at different levels such as misconfiguration of services and security controls, unauthorized accesses and so forth.

This technique shows the importance of automation in IT security controls area. Conducting manual log review can be extremely time consuming but there exist some automated audit tools that are able to reduce significantly the necessary time and generate customizable reports in order to summarize log contents arranging them by set of specific activities.

C.3.3 Ruleset review

Method Examination & Testing

Description This helps to identify gaps and weaknesses on a given system or network. It can also detect inefficiencies that negatively impact the performance. It encompasses logs from host-based and network firewall, IDS/IPS[1]and router access control lists.

A ruleset is a set of rules or signatures that a system activity or even network traffic is compared against in order to choose which action to take. The main benefit of assessing rulesets, by examination as well as by testing, is that it is critical that these are correctly designed and effectively implemented.

C.3.4 System Configuration review

Method Examination & Testing

Description This consists of identifying weaknesses in configurations according to the related policies. This may reveal, for example, unnecessary services and applications, improper password settings, improper logging and backup settings.

System settings can be checked relying on checklists or security configuration guides from many sources. Several repositories of checklists exist, namely NIST[2] Checklists, USGCB[3] or also CIS[4] Security Benchmarks. At the end of this process, assessors can then report if the settings meet an expected security level or not. SCAP[5] can also be used in order to automate the compliance checking based on settings baselines.

Both manual and automated methods need root privileges to look at security settings. Despite automated configuration reviews are faster than in a manual way, there often still remain settings that require to be checked manually. Whenever feasible, it will generally be preferred to use automated checks instead of manual ones these could be obviously error-prone and very time-consuming.

C.3.5 Network Sniffing

This technique requires a mean to connect to the network and has no impact on systems and networks. The relevance of acquired informations depends on the location of sniffers, e.g. behind a firewall, in front of a critical system, behind IDS/IPS and so forth.

[1] Intrusion Detection/Prevention System

[2] National Institute of Standards and Technology

[3] The United States Government Configuration Baseline

[4] Center for Internet Security

[5] Security Content Automation Protocol

Method Examination & Testing

Description This passive technique aims to monitor network communications and to understand used protocols by inspecting headers and payloads of exchanged packets. This can be either a review technique or a target identification and analysis technique (see next section). Its use allows to capture and replay network traffic in order to identify active devices on the network, identify operating systems, applications, services and protocols.

The main limitation of this technique is clearly the encryption which can hide malicious activities on a given network. The assessors can see that a communication is taking place, however, the content is unreadable. Another limitation concerns the working of sniffer which is only able to sniff the traffic of the local segment where it is installed. Assessors need to move it from segment to segment and install multiple sniffers throughout the network for a comprehensive evaluation. In addition, interpreting network traffic based on network sniffing is difficult and requires a high degree of human involvement.

C.3.6 File Integrity Checking

Method Testing

Description This provides a way to check integrity of guarded files in a system by storing checksum and establishing a checksum database for all system files that have been changed. By comparing current and stored checksums, it is possible to identify file modifications.

A file integrity checker must be used carefully to be effective and does not require high degree of human interaction. To be effective, it is necessary to compare system files against a reference database which is stored on a system known to be secure. This database should be stored off-line in order to prevent from tampering attacks and requires to be kept up-to-date.

FIPS[6] PUB 140-2 about *Security Requirements for Cryptographic Modules* requires to use a strong cryptographic checksums such as Secure Hash Algorithm (SHA-1 and SHA-256) in order to ensure integrity of data stored in the checksum database.

C.4 Target Identification and Analysis

Generally conducted using automated tools, this category of techniques aims to identify ports, services, systems in order to discover eventual vulnerabilities. In other words, it helps to identify active devices with their related ports and services in order to find potential security flaws. This subsection presents some common identification and analysis techniques that help assessors to gather information in order to identify the assets of interest.

[6] Federal Information Processing Standard

C.4.1 Network Discovery

Method Examination & Testing

Description This aims to discover active hosts on a network, potentially revealing unexpected devices or weaknesses in the network infrastructure. Both active (testing) or passive (examination) techniques exist in order to learn the topology of active hosts on a network.

- **Active Network Discovery** consists of sending different types of network packets in order to solicit responses from any host, aiming to get informations such as the operating system, open ports, etc.
- **Passive Network Discovery** consists of using a sniffer in order to monitor network traffic and record information (addresses, ports) about the active hosts. This is done without sending out any packet.

The collected information may be used for multiple purposes such as for penetration testing, generating topology maps, determining firewall and IDS configuration and discovering vulnerabilities or weaknesses in systems or networks configuration. This is the technique used in what is referred to as the reconnaissance phase when preparing an attack. Note that a passive discovery takes more time than an active one for gathering information and if a host does not send or receive traffic during the monitoring period, it will simply not be reported.

C.4.2 Network Port and Service Identification

Method Examination & Testing

Description This is done through the use of a port scanner and is able to identify network services operating on active hosts (e.g. FTP, HTTP, Telnet, NetBIOS) and also some applications running on (e.g. a web server for an HTTP service).

There exist many scanners that can help to determine the application running on a given port through what is called the service identification process. In general, scanners use a list of common port numbers and services on which they rely on. For example, a scanner which detects that TCP port 80 is open on an active host may report that it is probably a web server running at that port. But in practice, it is not sufficient and additional steps are needed in order to be more accurate. That is why some scanners can initiate communications and analyze them to determine what service is behind a given port.

Port scanners can disrupt network operations by slowing down the network because it severely affects the bandwidth. In addition, they identify services running on active hosts, operating systems, ports, services and applications, they are not able to identify vulnerabilities. Although port scanning has some disadvantages related to the performance, it has a major value especially for helping an organization to ensure that hosts only run approved network services.

C.4.3 Vulnerability Scanning

Method Testing

Description This identifies some attributes of active hosts (e.g. operating systems, applications, open ports). In addition, it tries to identify potential vulnerabilities based on network's behavior reported on the scanning result.

This can be done by identifying outdated software versions, missing patches and misconfigurations by comparing the collected information with data about known vulnerabilities stored in scanners' vulnerability databases.

C.4.4 Wireless Scanning

Method Testing

Description This identifies the wireless-enabled technologies in the surroundings of wireless network interface so that it is possible to identify rogue devices or weaknesses in the wireless network infrastructure. It allows to collect information such that corrective actions can be taken to mitigate the risks caused by these technologies.

- **Passive Wireless Scanning** consists of capturing wireless traffic transmitted in the range of the scanning device's antenna without sending any data, extracting relevant information from this traffic so that devices can be identified.
- **Active Wireless Scanning** consists of using the data collected with a Passive Wireless Scanning in order to attach to discovered devices so that penetration of vulnerability testing can be performed.
- **Wireless Device Location Tracking** relates to attempting to locate and track suspicious devices so that it is possible to physically check who is behind the device.
- **Bluetooth Scanning** refers to a (either passive or active) scanning allowing to discover Bluetooth-enabled wireless devices so that it can be checked if they comply with security requirements.

Thanks to this technique, rogue devices can be identified from the collected data by looking at unauthorized MAC address or SSID[7], of course, provided that the organization has a list of authorized devices and WLAN.

C.5 Target Vulnerability Validation

This category of techniques aims to confirm the existence of vulnerabilities in order to understand the security exposures that occur when a given weakness is exploited. Any of its techniques can be conducted either manually or by using automated tools. This section presents some common vulnerability validation techniques that help assessors to measure the actual risk after discovering a vulnerability. This is the continuation of the previous one in the sense that it is based on its output. The information produced by *Target Identification and Analysis* techniques must be deeply explored so that vulnerabilities can be discovered.

C.5.1 Password Cracking

Method Testing

Description This aims to attempt recovering passwords based on their hashes stored on systems in order to identify accounts with weak passwords.

[7] Service Set IDentifier

Typically, when a user enters its credentials containing a password, the system compares the hash of the entered password with a stored one of the user's actual password in order to authenticate the user. Sometimes, when weak passwords are used, it is easy for an attacker to try lots of combinations of characters and/or relevant information (e.g. a birth date), hoping that the password will be cracked. Several types of attack can be used to do so :

- **Brute-force attack** is a method that generates all possible words up to a certain length given an alphabet and their associated hashes. Theoretically, all passwords may be cracked by this method, given enough time and processing power. Assessors and attackers often spread the task of cracking passwords over multiple machines.
- **Dictionary attack** is based on a dictionary (text file) which lists possible words related to a specific language, name, popular television show or any other information that could be used to guess the password of the victim. There exist many dictionaries available freely on the Internet.
- **Hybrid attack** consists of mixing the Brute-Force and Dictionary attacks.
- **Rainbow Tables** consists of performing a lookup on tables with precomputed password hashes. This method requires large amounts of storage space and can take a huge time to be generated. It is ineffective against password hashing that uses salting, that's why many operating systems use salted password hashing mechanisms.

Password crackers can help assessors in order to ensure policy compliance regarding passwords and can be done during the execution of an assessment.

C.5.2 Social Engineering

Method Testing

Description This aims to trick someone in order to reveal information that may be used to perform an attack against systems. So it concerns the human element and more precisely it tries to test user awareness of security. This can be achieved through the use of many possible channels, e.g. a phone conversation, an e-mail or an instant messaging.

Phishing is certainly the most common form of social engineering where attackers try to make the victim reveal confidential data by seemingly behaving legitimately. From the organization's viewpoint, it is important to improve the security establishment taking into account results of social engineering testing. This process help organizations to tailor their security awareness training program based on reported results.

C.5.3 Penetration Testing

Method Testing

Description This consists of targeting and locating potential exploitable weaknesses in the design or implementation of an application, system or network. It is a security testing in which assessors try to reproduce real-word attacks in order to assess to which extend the security measures in place can be circumvented.

Amongst the most common vulnerabilities exploited via penetration testing, one can namely mention the followings :

- **Buffer Overflow** occurs when a user input is not correctly checked by a program so that it is possible to break its working and to execute arbitrary code with unauthorized privileges.
- **Kernel Flaws** are security flaws affecting an OS' kernel, then impacting the whole system if exploited.
- **Misconfigurations** are insecurely configured settings, often simply default settings.
- **Incorrect File/Directory Permissions** can lead to unexpected read or write operations on files or directories that should have be unauthorized.
- **Race Conditions** occur when a program has entered a privileged mode and it can be time-attacked so that it can be taken advantage of the elevated privileges.

The major limitations of penetration testing are that it is labour-intensive and necessitates a great expertise. It is very interesting for an organization that tries to determine the vulnerabilities of its infrastructure as well as the level of damage that can occur if the weaknesses are exploited. This process may present a risk to an organization's networks and systems in the sense that it uses real exploits and attacks against production systems and its associated data.

Because of its potential impact and its high cost, doing a penetration testing on an annual basis may be sufficient and reasonable. The results should be reported to the organization's managers and read carefully in order to mitigate all discovered vulnerabilities.