NESCOR Guide to Vulnerability Assessment for Electric Utility Operations Systems

Version 1.0

June 2014

National Electric Sector Cybersecurity Organization Resource (NESCOR)

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THIS DOCUMENT WAS PREPARED BY THE ORGANIZATION(S) NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED OR COSPONSORED BY THE ELECTRIC POWER RESEARCH INSTITUTE, INC. (EPRI). NEITHER EPRI, NOR ANY MEMBER OF EPRI, ANY COSPONSOR, THE ORGANIZATION(S) BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM:

(A) MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS DOCUMENT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B) ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUDING ANY CONSEQUENTIAL DAMAGES, EVEN IF EPRI OR ANY EPRI REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS DOCUMENT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT.

REFERENCE HEREIN TO ANY SPECIFIC COMMERCIAL PRODUCT, PROCESS, OR SERVICE BY ITS TRADE NAME, TRADEMARK, MANUFACTURER, OR OTHERWISE, DOES NOT NECESSARILY CONSTITUTE OR IMPLY ITS ENDORSEMENT, RECOMMENDATION, OR FAVORING BY EPRI.

THIS REPORT WAS PREPARED AS AN ACCOUNT OF WORK SPONSORED BY AN AGENCY OF THE UNITED STATES GOVERNMENT. NEITHER THE UNITED STATES GOVERNMENT NOR ANY AGENCY THEREOF, NOR ANY OF THEIR EMPLOYEES, MAKES ANY WARRANTY, EXPRESS OR IMPLIED, OR ASSUMES ANY LEGAL LIABILITY OR RESPONSIBILITY FOR THE ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION, APPARATUS, PRODUCT, OR PROCESS DISCLOSED, OR REPRESENTS THAT ITS USE WOULD NOT INFRINGE PRIVATELY OWNED RIGHTS. REFERENCE HEREIN TO ANY SPECIFIC COMMERCIAL PRODUCT, PROCESS, OR SERVICE BY TRADE NAME, TRADEMARK, MANUFACTURER, OR OTHERWISE DOES NOT NECESSARILY CONSTITUTE OR IMPLY ITS ENDORSEMENT, RECOMMENDATION, OR FAVORING BY THE UNITED STATES GOVERNMENT OR ANY AGENCY THEREOF. THE VIEWS AND OPINIONS OF AUTHORS EXPRESSED HEREIN DO NOT NECESSARILY STATE OR REFLECT THOSE OF THE UNITED STATES GOVERNMENT OR ANY AGENCY THEREOF.

THE FOLLOWING ORGANIZATION PREPARED THIS REPORT:

ELECTRIC POWER RESEARCH INSTITUTE (EPRI)

Primary Authors:

Glen Chason

Scott Dinnage

Annabelle Lee

Justin Searle

Dan Widger

Andrew Wright

Reviewers:

NESCOR Team 3 Members and Volunteers

The research was paid for by the Department of Energy (DOE) under the NESCOR grant.

Program Manager

A. Lee

Table of Contents

List of Tables

List of Figures

1 Introduction

This document provides guidance on vulnerability assessments for electric utilities. The objective of a vulnerability assessment as described here is to develop an in-depth view of a utility's security posture with a focus on system and network vulnerabilities. Results from a vulnerability assessment can be used to determine or recommend mitigations for the utility. A vulnerability assessment can serve as a key component in assessing a utility's overall cyber security posture and the results can be used to assist in prioritizing a utility's operating plans, programs, and budgets.

1.1 Scope

This document focuses on how to assess *technical* vulnerabilities for the endpoints, applications, and networks of utility *operations systems*. This document does not address non-technical issues, such as policies and procedures, nor assessments of enterprise networks.

For this document, operations systems include traditional utility control systems such as Distributed Control Systems (DCS), Energy Management Systems (EMS), and Supervisory Control and Data Acquisition (SCADA), as well as systems not typically considered control systems, such as Advanced Metering Infrastructure (AMI) Systems, Outage Management Systems, and Engineering Analysis Systems. When compared to enterprise systems, electric utility operations systems have different requirements and characteristics, such as:

- Specialized technologies, often including legacy equipment
- Different applications
- Real-time requirements
- Different resiliency and uptime requirements
- Deployment over wide geographic areas
- A higher ratio of machine-to-machine than human-to-machine communication

These differences necessitate an approach to vulnerability assessment for operations systems that is different than those used for typical enterprise systems. In cases where operations systems are intermingled with enterprise systems, vulnerability assessments must also consider threats that use enterprise systems and applications as an attack vector.

The security of a utility's operations systems depends upon many factors, which include:

- The security of individual endpoints, including computers, intelligent electronic devices (IEDs), switchgear, meters, phones, mobile devices, storage systems, backup systems, etc.
- The security of applications running on the endpoints
- The security of the communications and networking equipment
- The architecture of the network
- Interconnections to other networks, especially third party networks

Non-technical issues such as governance, plans, policies, awareness, and training can have as much to do with the security posture of a utility as the technical issues. However, these issues are not addressed in this document.

Physical security issues can also impact cyber security for operations systems, since many cyber assets are located in remote and unmanned facilities and locations. However, a full treatment of physical security assessments is beyond the scope of this document.

1.2 Attack Vectors

The key goals of a vulnerability assessment are to identify and understand the vulnerabilities that could be exploited and used to compromise the function of operations systems. The means by which these vulnerabilities can be exploited are known as attack vectors. Attack vectors against utility operations systems include:

- Exploitable software bugs in endpoints and applications
- Architectural flaws in the overall network
- Insecure wireless communications
- Weak internal practices, processes, and governance (e.g., weak password policies)
- Weak or absent cryptographic mechanisms
- Weak physical security
- Accessible media ports
- Inadequate supply chain controls

Exposing flaws in network architectures and system configurations can be used to improve the security posture of a target environment. While no network or system can be 100% secure, vulnerability assessments can produce data that may assist in identifying areas of weakness or finding obvious security gaps. These gaps may otherwise only be identified when exploited by an attack.

1.3 Testing Programs

An effective testing program should include, at a minimum, an application/functional test plan and a cyber security test plan. A functional test plan should be used to verify that the application under test correctly implements the specified system functionality. One purpose of a cyber security test plan is to ensure that the cyber security controls are still functioning correctly after a configuration change. The scope of the test plans may also extend into third party networks.

When the creation and maintenance of a separate test environment is not feasible or is cost prohibitive, simulation may be a viable alternative. A virtual environment should replicate the production systems to test configuration changes and patches. The virtual environment also provides a platform that can be used to perform vulnerability scans without risk to operational systems. This may require administrators to maintain both the production and the simulation environments under the same change and configuration control processes.

Testing the cyber system assets that comprise critical systems can be useful in establishing a baseline configuration. The baseline configuration is a required step in some regulatory compliance frameworks. For systems that cannot be effectively tested in simulated environments, it may be necessary to perform a vulnerability assessment in the production environment.

Performing a vulnerability scan is a specific testing function. The vulnerability scan produces critical information (including open ports and services) that should be included in the baseline configuration documentation. Further, it is important to determine if vulnerability scanning causes any adverse impact to the operation of the cyber asset. The functional test plan and the cyber security control test plan should be implemented to test the functions of each cyber asset after a vulnerability scan is completed.

Another effective strategy is to perform a vulnerability assessment on the cyber system assets before the system goes into production. Utility system support staff should assist in the performance of a vulnerability assessment. At the completion of a vulnerability assessment, mitigation strategies may be developed. Implementation of these strategies may be executed in a phased approach as a full deployment may take months or years due to operational constraints. Before the vulnerabilities are remediated, or if some mitigations are never implemented, the utility should be aware of and accept the residual risk associated with the known vulnerabilities. Mitigation strategies should be thoroughly tested both before and during implementation.

In some environments there are mechanisms where control of the operations system can be transferred to alternate sites or systems and components. Use of these mechanisms provides opportunities for the primary system to be taken offline and

assessed. This also provides opportunities to carry out maintenance that may need to be performed on production system assets. While the system is offline, intrusive vulnerability assessment tools may be used without the risk of impacting system availability. After using active vulnerability assessment tools, all cyber assets should be completely powered down and back up. After the equipment recovers from the power cycle, a full series of functional tests should be performed. These tests should ensure that the offline components are functional before being returned to production.

1.3.1 Active vs. Passive Assessment Techniques

A vulnerability assessment can be performed using active or passive testing methods. *Passive* methods introduce no traffic to the host network; only passive monitoring and data gathering techniques are applied. Passive testing methods are well suited for both test and production environments and can readily scale. *Active* methods involve injecting traffic into the network to test for responses and to determine if vulnerabilities are present. Active testing must be applied to production operational networks with great care.

Active vulnerability assessment procedures can sometimes disrupt operations systems, and could cause loss of visibility into utility operations, loss of control, or even power outages. Disruptions can be caused by abnormal traffic or traffic volume generated by tools used to perform vulnerability assessments. For example, performing a vulnerability scan on a production operations network can result in the lock out of production accounts, cause system reboots or hangs, exhaust system resources on legacy devices, or saturate the network. A general guideline is that the older the system, the greater the probability that active assessment tools may cause a disruption. An operations system where all assets are less than three years old should be more resilient to anomalous network traffic than an operations system in which some of the cyber assets are more than ten years old. Because of the potential for disruptions to operations, passive vulnerability assessment tools should be preferred for older cyber assets. When performing active scanning, utility personnel should participate in the testing and record any activities that cause adverse system impacts. Utility personnel should be prepared to reset affected assets and return them to an optimal operating state.

Passive vulnerability assessment techniques involve lower risk of disrupting systems. However, even passive techniques are not without risk. It may be necessary to modify a network configuration to allow traffic to be captured from span or mirror ports, or to install network taps. Switch resource depletion is possible when a network switch span or mirror port configuration update is made. In an environment where the switch infrastructure is already close to full utilization, adding the additional burden of mirroring

the data to a given port could cause resource depletion. Installing network taps may involve briefly interrupting network traffic.

An approach that is more effective than passive scanning - but requires greater resources - is to perform active vulnerability scanning in a test environment. A test environment should consist of cyber assets identical to those in the operations environment. Assuming that the test environment is maintained under effective change control in the same way as the operations environment, the results of vulnerability scanning activities in a test environment should closely reflect results that would be encountered in the operations environment.

1.4 Planning

A vulnerability assessment should be performed to meet specific goals. In some cases, assessments or audits are required for regulatory compliance. In addition, management may elect to execute vulnerability assessments for the purposes of reducing risk and increasing security.

Specific activities may be triggers for vulnerability assessment activities. For example, consider performing a vulnerability scan before assets are introduced into an operations environment or after a configuration change to determine if new vulnerabilities have been introduced. It is also useful to perform a vulnerability scan prior to a configuration change to establish a baseline to determine if a new vulnerability was introduced by the configuration change. Networks and systems may have changed or been modified outside of approved change management events. Periodic vulnerability scans of operations networks could identify new vulnerabilities. Finally, there is benefit to performing a vulnerability scan after patches are deployed to determine if the patches were successfully applied.

It is important to remember that all software systems contain latent vulnerabilities that will be discovered over time. One-time vulnerability assessments hold significant value, but periodically repeated assessments are a more effective risk management strategy. While there is a higher cost associated with continuous vulnerability assessment activities, the effort involved and cost per assessment goes down as assessments are repeated. Ultimately, the organization’s risk tolerance and budget drive the frequency of vulnerability assessments.

1.5 Mitigation and Implementation Plan

Once a utility is provided with information about vulnerabilities (whether from vulnerability scans, patch notices/security bulletins from a solution provider, or a public notice from the Department of Homeland Security or the North American Electric Reliability Corporation (NERC)), it is important to apply some form of remediation as

part of the utility's vulnerability management program. A vulnerability management program should include (but is not limited to) the following steps:

- Assess risks associated with the vulnerabilities.
- Test the proposed vulnerability remediation method (e.g., "patch").
- Implement the vulnerability remediation in the production environment.

There should be governance documentation that addresses the vulnerability management program. The governance documentation should address the vulnerability assessment process, roles and responsibilities, implementation timeframes, workflow or tracking mechanisms, exception handling mechanisms, and the evidence that will be produced. Establishing a vulnerability management program is typically a one-time effort but maintaining and tuning the program should be an ongoing effort.

The first step of vulnerability remediation is to do an assessment in a timely manner to determine the course of action. As each iteration of the vulnerability assessment process is executed, the results should be documented and evidence for each cycle preserved. The evidence for each cycle should identify who participated in the assessment, the vulnerabilities assessed, and the decisions that were agreed to regarding any vulnerability identified.

When a vulnerability risk assessment cycle identifies configuration changes/patches that are needed to reduce the risk within the environment, a best practices approach is to apply remediation in a phased progression. This includes deploying a patch or vulnerability remediation in a non-production/test environment. If the test deployment is successful, then the remediation package should be deployed in the production environment. The testing methodology employed should determine:

- Is the vulnerability adequately remediated?
- Is the functionality of the affected cyber asset still effective and operational?
- Are the security controls applied to the given cyber asset still effective?

Once testing confirms that the application of vulnerability remediation mechanisms reduces the risk associated with the vulnerability, then the process continues to the next stage. However if additional problems are identified in current stage, they should be investigated and resolved before proceeding to apply the vulnerability remediation to the production environment.

When the vulnerability assessment activities are completed, the next step is the vulnerability remediation to the production environment. The application of the vulnerability remediation mechanisms should be consistent with the utility’s change management process. The remediation mechanisms should not result in disruptions to the operation of the system.

The cost or risk of a vulnerability exists from the time the vulnerability was first discovered/publicized until the time the vulnerability is remediated. Therefore, it is important to minimize the cost of the vulnerability by remediating the risk as quickly as possible.

Vulnerability assessments are only a point in time exercise, and value to the organization is maximized if the identified vulnerabilities are remediated quickly.

1.6 Use of Third Parties

Vulnerability assessments are best performed by neutral and unbiased assessors to ensure neutral and unbiased results. Internal auditors who are independent of the typical engineering and administrative staff of the operations networks may be able to provide such an unbiased viewpoint. Internal auditors may already be familiar with aspects of the systems being assessed, thus reducing cost and effort. However, qualified internal staff may be difficult to find, especially in smaller utilities. Alternatively, third party contractors may have greater expertise and be able to leverage experience gained from similar vulnerability assessments at other utility environments. Third party assessors may be more efficient in conducting and documenting the vulnerability assessment but could require more time in preparation and planning. When engaging a third party to perform an initial vulnerability assessment, it is a good practice to have an inside staffer knowledgeable in cyber security shadow and facilitate the third party. This can serve as a learning process that can allow the staffer to facilitate future internally coordinated vulnerability assessment activities.

2 Vulnerability Assessment Overview

The following are the areas of focus in a vulnerability assessment of cyber assets for utilities:

- **Network:** Focuses on network devices and related software. How do networks interact? How are they connected? What protocols traverse the overall network? What risks or exposures are created by wireless networks?

- **System:** Focuses on individual host and systems analysis. What applications and services are running on a system? What level of "trust" does the given system have? Can the system be used to attack other systems?

- **Application:** Focuses on testing and verifying individual applications. What vulnerabilities do the applications create? What access control issues can the application generate? Are there vulnerabilities in the software that allow for attacks such as buffer overflows?

The scope of the assessment depends upon the overall goal. If the scope of the assessment extends into third party networks, the scope should be reviewed and agreed upon by the applicable third parties.

2.1 Vulnerability Assessment Tools and Resources

A vulnerability assessment requires similar tools to penetration tests and other assessments. Suggested tools and resources include some intrusive and potentially disruptive resources; therefore, caution should be used when applying any of the listed resources during execution of a vulnerability assessment.

Security assessors should coordinate with utility staff to review asset lists and network diagrams to ensure that there is a common understanding of the current environment. Security assessors should have full physical access to the systems so that they may perform verification, discovery, enumeration, and exploration phases, as described below.

It is important to control the availability of vulnerability scanning tools to prevent, for example, vulnerability scanning software being used without appropriate coordination against production networks, or against other unauthorized targets. Policies should be established that prohibit vulnerability scanning tools from being present on utility systems, unless explicitly authorized. Also, usage should be restricted only to parties appropriately trained and authorized.

2.1.1 Resources

Many tools and resources may be required for active vulnerability assessments and planning ahead is important for completing the assessment in a timely manner. Security assessors will typically need a portable computing device capable of performing vulnerability scans and for acquiring and preserving configuration information for a variety of assets. To connect to different devices (e.g., network equipment, programmable logic controllers (PLCs), and SCADA devices, etc.) the security assessors will like need different type of converters (e.g., RS-232, RS-422) and cables. Security assessors will need external storage media to store configuration information and network captures. In some cases, security assessors may need portable monitors to connect to devices that don't have connected displays. For some tasks such as wireless network detection functions, security assessors may use special purpose devices or they may use software installed on general purpose mobile computing devices (laptops).

Table 1 lists some of the equipment that the security assessors should consider having available when performing a vulnerability assessment.

Table 1: Vulnerability Assessment Tools

Resource	Description
Cables	Security assessors may need multiple types and lengths of cables to perform the assessment including: various sizes of long RJ45 cables, Cisco crossover cable, null modem serial cables, straight-through serial cables, monitor cables (e.g., DVI or VGA).
Camera	Security assessors may want to take photographs (provided that prior approval by utility management has been received) that can aid in information recall. Visual evidence in the assessment report will aid in the understanding of particularly complicated technology setups. **Note**: It is not uncommon to have restrictions on the use of photographic equipment or cell phones in security sensitive areas. Security assessors should confirm the protections that are needed for photographic images that would be removed from an organization's premises.
Converters	Security assessors may need various media converters for protocol conversion to allow for communications with various types of equipment. One example would be a USB/serial converter.

Resource	Description
External Storage	Security assessors may need secondary storage for electronic documents or dumps of data obtained from the utility during the site assessment. **Note**: External storage will likely contain confidential information and should implement encryption using secure storage software.
Wireless Scanners	Security assessors should have tools for identifying wireless networks, whether built into laptops, personal digital assistants (PDAs) or purpose-built wireless audit devices.
Laptop	Security assessors typically need a laptop for assessment activities including network communication, information gathering (e.g., internet access), note taking, etc. **Note**: Security assessors need to coordinate with the utility regarding use of third party computing equipment versus an organization owned and maintained computing device.
Monitor	Security assessors may need to examine information from a cyber asset that does not have a display monitor. A monitor may be essential to quickly reviewing the information. **Note**: Security assessors should have DVI/VGA converters in case the cyber asset has an older VGA interface port.

2.1.2 Software

Security assessors will require various software tools to perform vulnerability assessment tasks. Some tools are listed below.

- Packet capture tools can passively capture network traffic. This information will be used by the security assessors to perform network traffic analyses.
- Port scanner tools are used for identifying hosts and network services on the hosts.
- Network topology mapping tools can convert packet captures into a network map.
- General-purpose vulnerability scanning tools are typically active vulnerability scanning tools that send packets to each host to determine if the host has known vulnerabilities.

- Wireless detection software tools manipulate wireless radios to search for wireless networks, and to provide similar functionality to purpose-built wireless network detection tools.
- Serial communication tools can be used to query assets or to obtain configuration information from devices that allow administrative or configuration control over serial interfaces.
- Diagramming tools enable security assessors to create and view network diagrams, which are critical resources in vulnerability assessments.
- Infrastructure assessment tools are used to perform security analysis of network infrastructure devices.

There are other advanced active vulnerability assessment tools used for industrial control systems (ICS) equipment (PLCs, SCADA equipment, etc.) that provide advanced vulnerability scanning functionality. **Table 2Error! Reference source not found.** lists some of the software resources that the security assessors should consider having available when performing a vulnerability assessment.

Table 2: Software Tools for Vulnerability Assessments

Type	Assessment Tool	Use
Passive Traffic Monitoring	Wireshark, tcpdump	Packet capture tool, typically on a span port or network tap
Port Scanner	NMap	Network Mapping, TCP and UDP interrogation
Network Topology Diagramming	Antfarm	Network Topology Mapper
General Purpose Vulnerability Scanner	Nessus, OpenVAS	Known vulnerability identification
Microsoft Vulnerability Scanner	MBSA	Known Microsoft vulnerabilities
Wireless Detection	Kismet, inSSIDer	Detection capability for wireless network
Serial Communications	Kermit, Minicom, HyperTerminal	Serial communications identification

Type	Assessment Tool	Use
Diagramming Applications	Visio, AutoCAD	Diagramming tool
Network Infrastructure Assessment Tool	Nipper, CIS RAT	Configuration assessment of network infrastructure devices
Custom ICS Assessment Tool	Samurai STFU	Vulnerability scanning tool for ICS environments
Encrypted Storage	TrueCrypt, WinZip	Protecting the confidentiality of acquired information

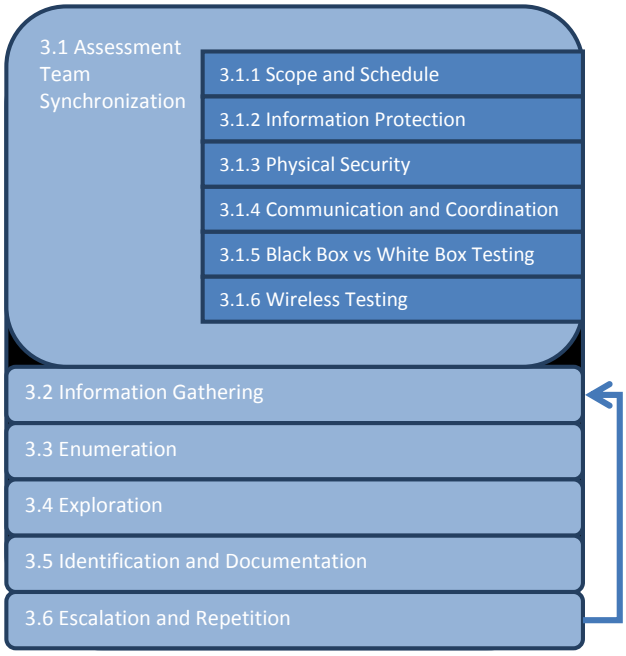
2.1.3 Information Protection

Vulnerability assessments can generate substantial volumes of sensitive information that is essential to accurately reporting the findings of the assessment. This sensitive information must be protected. The utility may have information labeling and handling controls that may impact whether documents can be removed from a facility. It is not uncommon for a utility to require electronic notes to be protected (stored encrypted) when the information is not inside a protected physical perimeter.

3 Assessment Methodology Overview

Figure 1 illustrates the vulnerability assessment methodology for utility operations systems. Phase 1 consists of preparatory activities to address coordination between the utility personnel and the security assessors. Phases 2 through 6 (from Information Gathering to Escalation and Repetition) are repeated for different domains (e.g., networks, systems, and application).

Figure 1: Assessment Methodology



3.1 Phase 1: Assessment Team Synchronization

Phase 1 of a vulnerability assessment ensures that the security assessors are synchronized with the utility's personnel regarding the scope, vision, and parameters of the assessment project, and that the agreement is documented.

A vulnerability assessment can provide useful information to a utility, but if not managed carefully it can also result in disruptions to operations and misunderstandings. Preparatory discussions and coordination can save many hours of rework and even more significantly, save the harmful and embarrassing effects of causing a disruption of normal operations.

Utility staff may find it useful to have the vulnerability information provided in a format that makes it easy to manage and track mitigation activities. Security assessors should work with utility staff to determine the best format for delivering the vulnerability information. For example, the utility's administrative staff may find that a spreadsheet is the best format to deliver the vulnerability information so that they can track action items and remediation. In other environments, the vulnerability information may be presented in XML format so that this information can be imported into a commercial database.

All discussions should include utility management having an interest in the vulnerability assessment activities. It is important that security assessors understand the utility's management expectations and any special conditions that may apply. The outcome or product of this synchronization phase should be a document such as a Memo of Understanding or a Vulnerability Test Plan.

A vulnerability assessment may identify that malicious parties have already compromised the target environment. It is important to establish methods for communicating such information to the utility management.

3.1.1 Scope and Schedule

An important task is to agree on the scope of the vulnerability assessment. Utility management should identify their expectations regarding the target set, such as "the operations system network." Security assessors should be clear on the definition of "the operations system," including but not limited to the IP address ranges that encompass the target network environment. Further, it is important to identify expected boundaries, including any firewalls or access gateways, and any third party interfaces (e.g., virtual private network (VPN) access points). It is important for the security assessors to know the "ownership" of the interfaces between internal networks and external networks and who is responsible for daily administration of the gateways and interfaces to external networks.

Peripheral or external entities should be aware of the vulnerability assessment activities, and any specific dates and times when there may be intrusive scanning activities for the affected networks and cyber assets. The owners and administrators of the border devices should be aware of assessment activities to ensure that they provide current and active configuration information for the network equipment to the security assessors, and to promote appropriate responses when assessment activities occur.

An additional area to be agreed upon, prior to starting the assessment, is the scope of machines that may be impacted. During a vulnerability assessment, the types of tests that can be performed on sensitive machines must be identified. Security assessors need to know which cyber assets are the most critical and which assets are the most sensitive. Certain cyber assets or systems may be critical or sensitive during a specific

time frame or critical processing period. This information will help the security assessors develop an appropriate test plan that should minimize disruptions.

It is important to verify the dates of the full project activities. This includes verification of when potentially disruptive scanning will be occurring. It is also appropriate to identify target time frames for delivery of the preliminary report and the final report.

3.1.2 Information Protection

Security assessors should coordinate with utility management to ensure that appropriate protections are applied to the information acquired and generated in the vulnerability assessment activities. The utility and the security assessors should have an agreement on the information that will be shared (e.g., network diagrams, TCP/IP addresses, firewall configurations, and vulnerability information). Agreement should be reached about what information (if any) is allowed to leave the client site, and under what conditions. Raw data captures, filtered data, photographs, and draft documentation may need to be encrypted. If information is to be exchanged from remote sites (e.g., an external security assessor's office), there should be agreement on the protections (such as file encryption) that should be applied to the information sent over untrusted networks such as the Internet. For example, any information set that contains TCP/IP addresses should be encrypted. The utility may not allow the exchange of sensitive information over public networks except with specific protections such as the use of encrypted transport mechanisms (secure mail or secure web sites). Some utilities may require that all vulnerability assessment efforts be performed only on company owned equipment.

Agreement on information protection methods should be addressed in the preliminary stages of the project before any work begins. This is important to prevent unnecessary risk or exposure to the utility organization or its infrastructure. At the completion of the vulnerability assessment project, the utility should specify how the information collected by the security assessors is to be disposed or stored.

3.1.3 Physical Security

Security assessors and utility management should have a clear agreement on the physical boundaries that encompass the systems that are in scope. Physical boundaries are also relevant to wireless network testing activities. Security assessors should identify any physical security controls are in place. Security assessors should also be aware of any physical security risks such as dangerous machinery that may be encountered during the engagement, and if any personal protective equipment (e.g., hearing protection, eye protection) may be necessary or appropriate. Security assessors should also know of any mishaps executed by third party visitors that have occurred previously.

Utility management and the security assessors should agree on physical security, including the use of cameras and cell phones. The utility (particularly utilities subject to regulatory compliance requirements) may require continuous escort for parties with physical or electronic access to sensitive operations systems. Other security controls may include background checks, cyber security training (such as pertinent to applicable regulatory requirements), and sometimes bonding or other personnel requirements.

Security assessors may need access to record and archive photographic configuration information for analysis. This may include the physical layout of a computer rack, cabling for specific components, or physical security attributes such as how close computing equipment may be to other equipment. A utility may have a prohibition against cameras or cell phones inside the physical perimeter that protects the operations system. However, the utility should understand that photographs may be useful in a vulnerability assessment.

3.1.4 Communication and Coordination

Security assessors and utility management should have an agreement on the frequency, content, and format of communication between the two groups. The security assessors should provide a written summary of progress and findings at each phase (Enumeration; Exploration; Identification and Documentation; and Escalation and Repetition). In addition, the security assessors should summarize key findings to the utility, particularly if there are indications of compromise or discovery of serious vulnerabilities.

If the vulnerability assessment activities have an adverse impact on operations, the utility will notify the security assessors. This type of notification should be defined prior to execution of any security assessment operations. There is significant room for failure in a vulnerability assessment project if these details are not addressed in the initial meetings between the utility and the security assessors.

Security assessors and utility management should agree on how to respond to anomalous activity alerts that are triggered during the vulnerability scans. Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS), Firewalls, and/or Security Information and Event Management (SIEM) systems may generate these alerts. Some security tools with active defense capabilities may disrupt security testing or modify network behaviors. Coordination with administration staff of any SIEM or Log Monitoring solution is important to ensure that the impact of a vulnerability assessment is considered in regards to storage capacity, alerting, etc. The security assessors should coordinate the vulnerability assessment activities with third party entities involved in monitoring the target network environment.

3.1.5 Black Box vs. White Box Testing

A key decision that needs to be addressed in initial discussions is regarding “black box” vs. “white box” testing. In white box testing, the security assessor is provided with initial information about the asset or environment and privileged access to the system to be tested. White box testing is a more efficient approach to finding cyber security vulnerabilities due to increased access. A black box testing approach provides the security assessor with no initial information, no privileged access, and the same level of access as any other general user. Security assessors may not be able to identify all the vulnerabilities if they are not given appropriate credentials and authorization. Alternatively, a utility may not be comfortable with different factors associated with security testing and may not be willing to open its environment to full examination. The decision regarding whether to allow full access to security assessors is a critical decision for a vulnerability assessment project, and will directly impact the results.

If a white box testing approach is selected, security assessors should be provided with privileged accounts for the duration of testing. Occasions for accounts to be created and shared with security assessors present valid opportunities for security assessors to observe the integrity of the processes for issuing authentication and authorization credentials. A good practice for white box security testing is to create specific authentication credentials for association with the vulnerability scans. The vulnerability scanning test accounts should be established as members of the roles that would legitimately have appropriate access to the cyber assets to be tested.

Some regulatory compliance frameworks require that privileged account credentials be changed at least annually. Using a security vulnerability scan is a way to validate and test for compliance of credential changes. Some organizations may keep a history of old privileged credentials, such as the previous year’s password credentials for known privileged accounts (i.e. service accounts). The previous year’s passwords should be provided to the security assessors so that tests can be performed for hosts whose credentials may not have been changed.

The remainder of this document on vulnerability assessment focuses on white box testing.

3.1.6 Wireless Networking Assessment

Most vulnerability assessments should include a wireless security audit. Even if a utility has no wireless connections to their operations network environment or has a policy against connecting wireless networks to the operations network environments, an assessment should include a determination if wireless connectivity exists. *All* wireless connectivity should be periodically revalidated to ensure the utility network owners are aware of the current state of wireless connectivity.

3.2 Phase 2: Information Gathering

The goal of this phase is to gather as much documentation and information from the utility as possible.

One objective of this phase is to learn the administrative staff's understanding of the target environment. The most useful approaches are remote or in-person interviews with subject matter experts and reviews of documentation (e.g., network diagrams and asset inventory lists) of the target environments.

The following activities in this phase should be focused on vulnerability assessments. The intent is not to have a general overview of all the functionality of every system, but to focus on what is required to perform the vulnerability assessment.

- Obtain network diagrams
- Obtain hardware asset inventory lists
- Obtain system inventories (such as all assets listed in CMDB/Asset lists, Active Directory, DHCP Service, IP Address reports, switch MAC tables, etc.)
- Obtain software lists, with application version information
- Obtain policy and procedure documentation (where applicable for vulnerability assessments)
- Obtain network monitoring information
- Obtain wireless networking information
- Obtain information flow diagrams or any documentation that may provide insight into the system (software, hardware, network protocols used, or other)
- Interview system administrators
- Interview typical users to understand their access privileges
- Interview third parties (if applicable)

A key activity in this phase is to compare the different asset lists and to get a preliminary idea of the assets in the target environments that are within the defined scope (IP address ranges).

3.3 Phase 3: Enumeration

Phase 3 of the vulnerability assessment focuses on cataloging information from the target environment. The objective of the Enumeration phase is to verify the presence of the cyber assets that were identified within the project scope in Phase 1. A secondary objective is to validate the information gathered in Phase 2. This is done using various network mapping tools.

Enumeration should confirm that the information gathered in Phase 2 is correct. Often there may be devices or software present in the environment, but that are unknown to the utility organization. A network mapping exercise may identify that there are hosts in

the target environment that are not included in network maps. This could indicate, for example, that the utility doesn't have sufficient configuration management knowledge about the network environments. It may also indicate that the target network has been compromised and that rogue electronic assets are present in the network.

Enumeration activities in this phase include the identification of:

- Access points
- Network devices
- Operating systems
- Services listening on the network
- Users, accounts, and profiles

It is important to coordinate with the network infrastructure support staff regarding ports that will be used for connecting the security assessors' testing equipment. In some environments, there are requirements that all inactive switch ports be deactivated if not in use. Therefore, these ports would need to be activated before the port could be used. In some environments, a change request may need to be coordinated to activate the switch port and modify the switch configuration so that vulnerability scanning equipment can be connected. Also, connecting a networked device to a network switch port that is supposed to be inactive could trigger a security alert, and may trigger a visit from a cyber security incident response team. The utility representative should identify the network switch ports that are activated for the security assessors to use in performing vulnerability scanning. For example, if security assessors attempt a passive network packet capture, there should be an agreement specifying which network switch ports are configured for span port mode, and identifying the network traffic to be directed toward the span port. It is never appropriate to connect foreign equipment to a network without approval and coordination with the host organization.

3.4 Phase 4: Exploration

This phase includes evaluation of the vulnerabilities in the system.

Activities in this phase include:

- Identification of the cyber assets within scope
- Preparation of vulnerability scanning tools
- Acquisition of appropriate authentication resources (applicable for white box testing)
- Updating the vulnerability scan testing tool with vulnerability signatures
- Testing of the vulnerability scan testing tool that has been configured with the appropriate policy against a limited target environment
- Verification of the test results

- Coordination with the network support staff regarding scheduling and identification of switch ports for vulnerability scan testing
- Execution of vulnerability scanning that has been configured with the appropriate policy against the full target environment. The schedule for such testing should be developed to minimize disruptions to operations (if the vulnerability scan is performed on a production system)
- Reviewing the results to confirm that target systems were effectively assessed

3.5 Phase 5: Identification and Documentation

This phase categorizes and documents vulnerabilities found in the previous section . After the vulnerabilities have been documented, the security assessors identify applicable mitigation strategies. The security assessors should validate the vulnerability findings, where feasible.

Activities in this phase include:

- Documenting the vulnerabilities, including the risk level
- Documenting how the vulnerabilities were discovered
- Documenting the steps that were taken and the tests that were performed on the given systems

3.6 Phase 6: Escalation and Repetition

In the escalation step, the security assessors evaluate the vulnerabilities identified during the previous phases and provide this information to the utility. The security assessors may prioritize the vulnerabilities. A good practice would be to identify the highest risk vulnerabilities.

Timely documentation development is important because security assessors may forget details as the project progresses. Documenting and providing notes is important to ensuring that all the vulnerabilities that have been discovered are acknowledged. The activities in this phase include categorizing and informing the utility immediately of “high risk, high impact” vulnerabilities that are found.

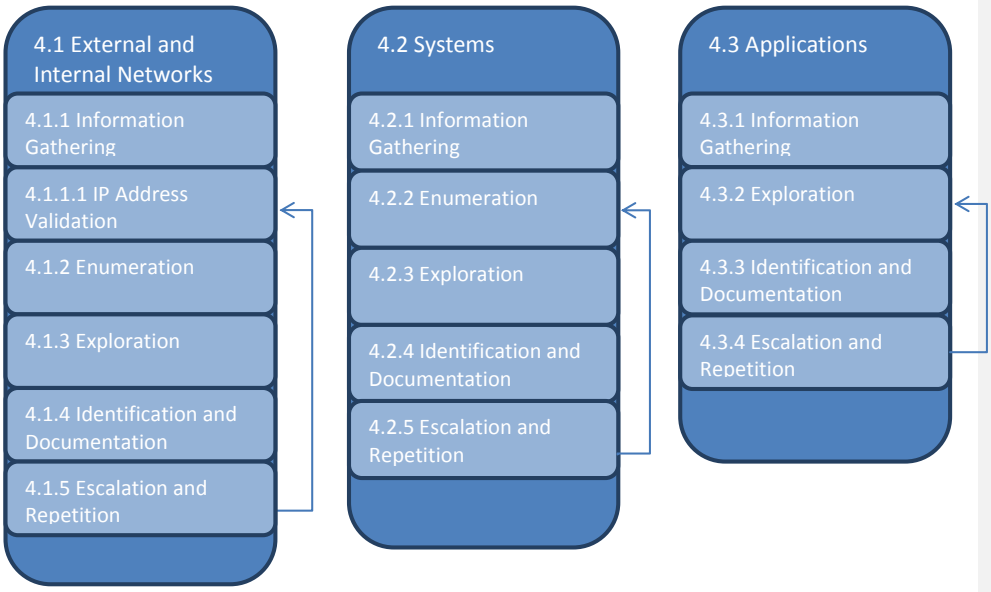
Management may elect to further investigate the vulnerabilities. In such cases, the security assessors may be granted additional limited access and use this access to perform additional testing.

4 Vulnerability Assessment Domains and Activities

This section expands on several activities previously identified in Section 1.

Vulnerability assessments include gathering information, enumerating resources, exploring assets (to identify vulnerabilities), documenting findings, and issuing escalations. This section describes the activities that are applicable to the following three vulnerability assessment domains, as illustrated in Figure 2.

Figure 2: Vulnerability Assessment Domains



Formatted: Font: 11 pt

Formatted: Font: 9 pt, Font color: Accent 1

4.1 External and Internal Network Evaluation

In this domain, security assessors gather information about the outward facing network perimeter as well as the internal network architecture elements of the target network environment. Special attention should be focused on externally accessible network components and zones (DMZ's). Some regulatory compliance regimes and security models prescribe that critical network services, such as authentication and logging, be segregated into separate network zones. Wireless network detection activities should also be addressed.

4.1.1 Information Gathering

Task Description: Security assessors should obtain information about the architecture of the network environment. This includes identifying external facing exposure points (e.g., firewalls facing business networks, demilitarized zones (DMZs), VPNs, remote access gateways, or third party connections), and internal network infrastructure elements (e.g., network switches including virtual local area networks (VLANS), internal firewalls, critical network services such as DNS, DHCP) of the target network environment.

Typical steps include:

- Interviews with network administrative staff
- Interviews with third party network administrative staff, if applicable
- Review of firewall rule sets and network device configuration files
- Review of network diagrams
- Review of wireless connectivity
- Review of recent changes to the network infrastructure
- Review of asset manuals regarding TCP/IP ports and services
- Review of user guides for network communication functions

Task Goal: The goal is to gain insight into the critical network infrastructure elements of the system and to understand how the network is architected.

Considerations: Important information to capture would include IP address ranges for network components inside the target network environment, IP address ranges for perimeter access gateways, and DMZ components outside the target network.

The security assessors should understand the applications, any exposed DMZs, and the network traffic that should be traversing the perimeter. For example, if a system sends alerts using SMTP, it would be useful to know the source and destination (host names and TCP/IP addresses) of the host/address alerting mechanisms. The security assessors should also know what network traffic will be carrying operations system traffic and what other traffic such as network administration functions (backups, DNS, anti-virus) would be expected, including the associated source and destination addresses.

By interviewing the network administrative staff, security assessors should be able to gain a general understanding of the alerting mechanisms that will be exposed outside the protected perimeter. Ideally, security assessors should review the network traffic information (e.g., firewall rule set) before interviewing the network administrators to fully understand the details about the network perimeter.

4.1.1.1 IP Address Validation

Task Description: Security assessors should review and verify the IP address information for the hosts in the operations system and for the network devices on the perimeter of the target network environment. Security assessors should verify the TCP/IP address information by doing the following:

- Manually verify the IP address ranges against the IP addresses found in the network diagrams, and other available documentation.
- Verify the IP address ranges against the IP address found in live network traffic on the production network.

To verify the IP addresses found in live network traffic, security assessors may perform a packet capture from a span port configured to mirror all ports on core internal switches connected to the primary access gateways. Security assessors may also utilize logs from the access gateway (firewalls) to ensure that all traffic going through the firewall originates from or terminates at assets in the IP address ranges. Where applicable, the security assessors should verify IP address ranges used for wireless networking.

Task Goal: The goal of this task is to verify that the previously acquired IP address ranges match the IP addresses used within the internal network and hosts at the perimeter of the target network environment. The intent of the verification is to ensure that the list of IP addresses targeted in the fingerprinting or port scanning activities in the next task is complete and comprehensive.

Considerations: Anomalous IP addresses should be investigated, and brought to the attention of utility management if significant anomalies are identified.

4.1.2 Enumeration

Task Description: Security assessors should interactively obtain information about the network devices and architecture that are inside the network perimeter and the devices that are accessible on the perimeter of the system. The first task with active network traffic is to identify the hosts that are accessible (respond to network traffic), and the type of host, or device. This can be done by scanning IP address ranges using either ping tools (such as NMap) or SNMP queries. The security assessors should scan the IP address ranges of the target network environment from a network connection point (e.g., switch) inside the target network to identify the network infrastructure components. In a separate step, security assessors should use a similar scanning technique from outside the target network environment to identify the border hosts.

If the security assessors are performing active testing, coordination needs to be arranged in advance. This would include appropriate coordination through the change control process. It is particularly important that the network security monitoring functions

of the utility be properly alerted so that when active testing occurs, the alerts for anomalous network activity generated by the enumeration scans receive appropriate response.

Enumeration tasks may uncover cyber assets on the network with web administration interfaces (usually port 80 or 443). These interfaces may include all web servers, some printers, and nearly all wireless access points.

Security assessors should also perform scanning of wireless radio frequencies to identify any wireless access points. Scanning for wireless could be accomplished through Kismet or inSSIDer or other similar tools, as referenced in Table 2: Software Tools for Vulnerability Assessments. Identification of a rogue wireless point would be a critical find in the vulnerability assessment.

Task Goal: The goals for the security assessors are to identify:

- The network infrastructure for the target network environment,
- Each of the known external access points into the target network environments, and
- The hosts or devices that are accessible on the perimeter.

The objective is to identify assets that could be access points into the target network.

Considerations: Security assessors should include:

- Network infrastructure devices such as switches,
- Critical network services such as time sources, DHCP, DNS, backups, logging, network monitoring (SNMP), and file transfer (FTP, TFTP),
- Firewalls, VPN gateways, and DMZs (where web services and remote access services may exist).

Use of NMap as a scanning tool can be problematic within the perimeter of a production environment. Simple ping scans are useful for detecting devices. Port scans of modern network equipment should have no or minimal performance impact, but scanning of legacy control assets should be avoided as it may result in adverse performance impact.

4.1.3 Exploration

Task Description: Security assessors should assess the configuration of the:

- Access gateways (e.g., firewalls) that control access to the perimeter of the target network
- Network infrastructure devices (switches, routers, etc.)
- Wireless network infrastructure

- Hosts within DMZ's that provide network infrastructure services such as web access, remote access, or network support mechanisms (DNS, SMTP/email, file transfers hosts, backups, and security mechanisms such as malware-protection).

In-depth vulnerability analysis of network infrastructure device and access point configurations should be performed, where possible. Network device configuration assessment tools such as RAT (from CIS) or Red Seal (commercial) can be used to gain a more granular assessment of the network infrastructure. The results of these tools may be subject to error and therefore the device configuration file should be examined to validate the configuration vulnerabilities identified by a tool.

Because network switches can be used to segregate network traffic using VLANs and ACLs, switch configurations can be critical to protecting a target network environment. Security assessors should evaluate the VLANs by determining the ACLs that are applied to control the traffic. Best practices for VLAN and switch security must be followed to ensure that VLAN protection is not easily bypassed. Assessing the network infrastructure device configurations (including VLANs and ACLs) can be accomplished using passive network vulnerability assessment practices and should not have any adverse impact on the production network. Vulnerability scanning should be performed against hosts that offer critical network services (such as authentication, DNS, logging).

Where applicable, security assessors should also review the configuration of wireless infrastructure. Analysis of a wireless infrastructure should include:

- Authentication (including Radius) and encryption mechanisms
- Default settings and passwords
- Verification of unused functions are disabled
- Review of management controls
- Review of logging and monitoring (including IDS/IPS)
- Review of timeout functions

Vulnerability scanning of network service hosts should be performed with appropriate coordination.

Task Goal: The goal is to obtain as much information as possible into the assets that could be utilized as access points into the target network environment. Examples of this may include firewalls, switches or other network devices that control traffic with ACLs. Other goals are to find vulnerabilities in the network infrastructure components, systems missing the most recent patches and updates, or systems having unused ports or services open that could potentially be exploited.

Considerations: NONE

4.1.4 Identification and Documentation

Task Description: This step is the initial analysis and documentation of vulnerability findings. Automated testing tools such as network device configuration assessment tools and vulnerability scanners may produce voluminous reports on configuration enhancement opportunities.

Task Goal: The goal is to identify specific vulnerabilities, or configuration enhancement opportunities that would mitigate risks for the internal network resources and the perimeter of the target network environment.

Considerations: The security assessors should always inspect and vet tools obtained from untrusted and trusted sources to reduce the risk of introducing or exposing the system under test to unknown threat vectors such as malware.

4.1.5 Escalation and Repetition

Task Description: Security assessors should prepare a summary report on the initial findings for the security of devices on the perimeter and critical internal network services within the target network environment. This may include an assessment of significant vulnerabilities that were identified, and an initial assessment of short-term and long-term security mitigation strategies.

Task Goal: The goal is to identify vulnerabilities for critical network infrastructures inside the target network environments and their critical access points, prioritize them as appropriate, and present an information summary to the utility.

Considerations: Security assessors should meet with the utility technical staff to identify key concerns or specific vulnerabilities.

Findings should be communicated as outlined in Section 3.1.4.

4.2 System Evaluation

In this domain, security assessors gather information about the internal hosts within the target environment. For this document, 'hosts' are typically multi-purpose operating system hosts with complex applications running on the hosts. System documentation may include:

- Specific hosts that are included in the system
- The data the system manages or processes and the security sensitivity of that data
- Data flow diagrams or network protocol flow diagrams
- The safeguards that are in place to monitor and protect the system
- Contingency plans, system restoration plans

4.2.1 Information Gathering

4.2.1.1 System Hardware Documentation Gathering/Review

Task Description: The security assessors should obtain documentation applicable to the hardware used in the system being assessed. This may include user guides or manuals, particularly for firmware based PLC devices, and remote management devices ("Lights out" boards) that may be used for management of general-purpose servers.

Task Goal: This information will guide the on-site work to be performed. For example, a list of running ports and services can be verified on-site and a vulnerability scan can be exercised in the exploration phase.

Considerations: NONE

4.2.1.2 System Software Documentation Gathering/Review

Task Description: The security assessors obtain and review system documentation for the software used on the applicable systems.

Task Goal: This information will guide the on-site work to be performed. For example, software guides can provide information regarding targets for security assessors to probe during vulnerability scanning.

Considerations: NONE

4.2.1.3 System Users Documentation Gathering/Review

Task Description: Security assessors obtain and review user guidance for interacting and operating the system.

Task Goal: This information will guide the on-site vulnerability assessment tasks.

Considerations: NONE

4.2.2 System Enumeration

The enumeration phase activities are an intrusive testing mechanism and are performed while connected to the network. This phase includes 'fingerprinting' which is an analysis of the hosts and services identified. The information gathered in this phase should be correlated with the systems that were expected to be found, as identified when the scope was defined for the engagement.

Requirements typically include providing an IP address on the network for the vulnerability scanning system, and a designated network (switch) port for connection of the scanning equipment. Switch ports may need to be configured to allow access to production VLANs.

Mature environments may have activated switch port protections on the network switches that may need to be temporarily opened/deactivated to accommodate the port scanning equipment.

In addition, the IDS/IPS security monitoring mechanisms should be adjusted to accommodate the port scanning activity.

4.2.2.1 Host Scanning

Task Description: The Host enumeration process typically starts with tools such as NMap to enumerate target hosts on the network, and is done while connected to the network that is being tested.

This step may be combined with the Port Scanning step.

Task Goal: The goal is to identify the hosts that exist on the network using ping scans.

Considerations: The security assessors should identify systems that may not tolerate such scans.

4.2.2.2 Port Scanning

Task Description: The port scanning task of the Enumeration phase requires the security assessors to use a tool (such as NMap) to identify the active (TCP/UDP) ports on a system.

Port scanning typically is a higher risk activity because it is intrusive. Port scanning uses abnormal TCP/UDP packets to probe IP-enabled devices to identify the target host device and to identify the TCP/UDP ports that are listening and responding on the device. Cyber assets with newer operating systems tend to be more robust than older assets/operating systems, and can better accommodate abnormal packets. Older (e.g., firmware based PLCs) devices may not have mature IP stacks and are more prone to choke or not respond well to abnormal traffic. While older devices may not have any clear indicators that they are malfunctioning, they normally respond appropriately after being power cycled. Port scans to detect ports and service should be slowed (e.g., 1-3 packets per second) to reduce the potential for disruption of legacy equipment.

Task Goal: The goal is to identify the hosts and determine what TCP and UDP ports are exposed to the network.

Considerations: The information produced in this step can facilitate verification of information previously obtained from the utility, including information about host operating systems. Other information previously obtained includes applications and other utilities that run on the operating system. The results from this step should be checked for devices or services that are not listed in the documentation.

4.2.2.3 Application and Service Enumeration and Fingerprinting

Task Description: Security assessors can analyze the data from the host and port scanning steps to acquire information about the applications and application attributes used in the system. For example, security assessors may be able to identify web applications that are being used (e.g., IIS, Apache, WebSphere or other), backend databases (Oracle, SQL Server, DB3 or other), mail services, backup applications, management tools, etc.

Task Goal: The goal is to identify the applications and detail attributes (e.g., version and patch levels) that are running on the individual hosts. This information will be used when performing the vulnerability scans.

Considerations: Information from this step may be used to support further analysis in Application domain.

4.2.3 Exploration

This phase primarily includes an analysis of the information previously gathered in preparation for vulnerability scanning. This phase does not include any intrusive network activity.

4.2.3.1 System Service Review

Task Description: This is a manual activity performed by security assessors using the information that was previously acquired. The intent is to understand the context of each system by looking at the open ports and services.

Task Goal: The goal is to identify the characteristics of each host and the services that are present.

Considerations: NONE

4.2.3.2 Enumeration of Possible Attack Vectors

Task Description: This is a manual activity performed by security assessors using the previously collected host and port information. Security assessors should profile the systems into classes, such as windows network systems (e.g., domain controllers), database servers, application servers, web servers, mail servers, etc). Analysis of these profiles may provide guidance about the types of attacks that would be most effective on that class of system.

Task Goal: The goal is to identify the attack surface for the system.

Considerations: None

4.2.3.3 System Authentication and Authorization Evaluation

Task Description: This is a manual activity performed by security assessors and should be coordinated with the administrative staff of the utility. In black box testing, no authentication credentials are provided to the security assessors. In white box testing, security assessors would be provided with authentication credentials.

Once the credentials are provided to the security assessors, they should be tested to ensure they work correctly. The security assessors may need to run separate vulnerability scans for systems that are not part of a domain (centrally authenticated). Also, the authentication credentials used for vulnerability scanning should not be used for production services.

Task Goal: The goal is to identify the vulnerability scanning approach, applicable target platforms, and appropriate authentication credentials.

Considerations: NONE

4.2.3.4 Evaluate Fingerprinting Results for Known Vulnerabilities

Task Description: Security assessors should confirm the software/hardware versions identified in Section 4.2.2 and check for known vulnerabilities in the identified components. This may include research to identify vulnerabilities that are associated with particular configuration versions of hardware and software.

Task Goal: The goal is to identify known system vulnerabilities and determine the access they may provide. As an example, a buffer overflow exploit may grant kernel level access for a particular system of a particular software version.

Considerations: NONE

4.2.3.5 Coordinate with Utility Staff and Management; Execution of Vulnerability Exploration

Task Description: Security assessors should plan the next stage of vulnerability scans to minimize impact. The assessors will group the assets and coordinate with utility staff. One objective is to ensure that all systems within scope are included. Therefore, it may be necessary to perform the vulnerability scanning on different systems at different times so that not all systems are impacted at the same time. Utility staff should be notified before and after each iteration of vulnerability scanning. Subsequent to the vulnerability scanning, the utility staff should test the functionality of the affected systems to verify that the affected systems remain operational. This enables the utility staff and the security assessors to understand the impact of the vulnerability scanning on the network in case adverse impacts are observed outside the testing environment.

Task Goal: The goal is to plan, coordinate, and then execute the vulnerability scans to minimize impact to the cyber assets and the systems in the operations environment.

Considerations: The security assessors should ensure that utility staff is aware of the testing schedule.

4.2.4 Identification and Documentation

4.2.4.1 Generate Documentation (Screenshots, tool readouts...etc.)

Task Description: The vulnerability scanning report will produce information about the various vulnerabilities that are found. The security assessors should perform a verification of the results where un-validated vulnerability information should be de-emphasized.

Task Goal: The security assessors should perform a review of the vulnerabilities identified by the vulnerability scan and validate the findings (which may include producing and reviewing data that would support or refute the findings).

Considerations: NONE

4.2.4.2 Generate Vulnerability Lists

Task Description: The security assessors should review the vulnerability list that was generated by the vulnerability scanning tool.

Task Goal: The goal is to create a list of vulnerabilities applicable to the target system.

Considerations: Vulnerability scans can produce erroneous data. Security assessors should examine the results to ensure that the findings are correct. Therefore, security assessors should filter the list of vulnerabilities that are inapplicable (e.g., vulnerabilities that don't fit, such as vulnerabilities for a given OS that isn't present in a given cyber asset). However, if the results aren't applicable, it would be useful to investigate the findings to determine the conditions that caused the inaccurate findings.

4.2.4.3 Determine Impact Levels

Task Description: The security assessors should identify the vulnerabilities that have the most significant impact to the system.

Task Goal: The goal is to understand the potential risks associated with the vulnerabilities and prioritize the vulnerabilities for the utility.

Considerations: Some vulnerabilities will yield information about the system, while others may yield escalated privileges or the capacity to execute code. Other vulnerabilities may represent known exploits that are in circulation. Security assessors should assess the vulnerabilities and prioritize them according to multiple criteria, which may include:

- Exposure to external access from unlimited populations
- Ease of remediation

- Ease of compromise
- Impact of compromise

4.2.5 Escalation and Repetition

Task Description: Security assessors should augment the summary report that was prepared in the External and Internal Network Evaluation phase by adding vulnerability information on the internal hosts, and prioritizing these vulnerabilities based on risk and impact.

Task Goal: The goal is to identify critical application risk points for hosts and devices within the operations system prioritize them. This information will be presented to the utility.

Considerations: NONE

4.3 Application Evaluation

Security assessors should acquire information about the applications that run on the operational systems of the target environment. An application security profile will facilitate the security assessor's analysis. Application security profile documentation may include:

- Known weaknesses or vulnerabilities
- Solution provider programs for on-going support
- Security bulletin/enhancement programs to maintain the security of the applications

Also, information about common weaknesses (CWE) and common vulnerabilities (CVE) may be maintained. Additional information about CVE and CWE and other vulnerability frameworks is provided in Section 6.

These applications may be critical processing engines that support or manage the flow of utility services and/or provide situation awareness to the utility staff.

4.3.1 Information Gathering and Enumeration

Task Description: The objective is to gather information about the application without impacting the system and use this information in planning for subsequent vulnerability assessment activities.

Using the information obtained in Section 4.2.2.3, the security assessor should identify the areas that may need advanced vulnerability scanning. Tools and techniques that apply here may include:

- Web application vulnerability scanners for hosts with web interfaces

- Database application vulnerability scanners for hosts with (SQL) databases

Task Goal: The goal is to identify the appropriate tools and methods for advanced vulnerability scanning, using information previously acquired in the Application and Service Enumeration step.

Considerations: If there is an Application Security Plan, this should be analyzed. For the Application domain, the focus is on the security capabilities of the applications and security features that were enabled. This information will be used in developing the vulnerability assessment activities.

4.3.2 Exploration

Task Description: The objective is to execute vulnerability scans against the applications.

Task Goal: The goal is to identify vulnerabilities in the applications that are implemented in the systems in the target environment.

Considerations: Specialized tools will typically produce more accurate assessments against specific applications than general vulnerability scanning tools. For example, web application vulnerability scanners produce higher integrity results against web applications such as IIS, Apache and other web environments. Similarly, database vulnerability scanners will produce more effective results against database applications than will general-purpose vulnerability scanners.

4.3.3 Identification and Documentation

Task Description: Where possible, validate the findings of the vulnerability scan results.

Task Goal: The goal is to identify and prioritize specific vulnerabilities and mitigation strategies that would reduce the security risk of the applications in the system.

Considerations: A security best practice is that development tools such as compilers, etc. should not be present in a production environment.

4.3.4 Escalation and Repetition

Task Description: Security assessors should augment the summary report that was updated in the System Evaluation phase and include findings from this domain.

Task Goal: The goal is to identify critical application risks, prioritize them, and present the information to utility management.

Considerations: NONE

5 Analysis, Interpretation, and Reporting

The information produced by a vulnerability assessment is a measurable element that can be used as a metric by utility management. The vulnerabilities identified by an assessment can establish a baseline for current risk to the organization, and the mitigation of vulnerabilities can illustrate a reduction of risk to the utility. As utility operations systems become more complex, utilities need to implement a vulnerability management process to assist in identifying and prioritizing risk mitigation efforts.

Security assessors should perform the following tasks at the completion of the vulnerability assessment project:

- Write a draft report based on the summary reports developed for the three domains.
- Meet with the utility management to discuss preliminary findings and mitigation recommendations.
- Revise the report based on feedback from the utility staff.
- Write the final report.
- Meet with utility management and communicate the final results of the vulnerability assessment project.

The final report should, at a minimum, include the following sections:

- Executive Summary - a brief 1-2 page section discussing the focus of the vulnerability assessment and the major findings and recommendations.
- Introduction – a section describing the goals of the project, components that were in and out of scope, any special restrictions on the project, and the team involved with the project.
- Methodology – a section focusing on the technical reasons for the vulnerability assessment and the methodology and metrics used.
- Findings and Recommendations – this section of the report is the most detailed and technical. This section should include the recommendations relevant for the findings.
- Conclusion – a section similar to the executive summary but at a more technical level that recaps the major findings and recommendations. This section should also include any recommendations for future vulnerability assessment activities.

Security assessors should present the vulnerabilities in a format that also includes information about the meaning of the vulnerability, common reference points such as CVE information, and how to apply remediation to the vulnerability. Security assessors should prioritize the findings for the utility based on the criteria set by the utility and the judgment of the security assessors.

6 Risk Management Strategies

This section proposes strategies that utilities may use to reduce cyber security risk. Risk management is the process of taking actions to assess risks, and to avoid or mitigate risks to an acceptable level. A risk assessment process includes identifying system vulnerabilities that could be exploited by threats. Vulnerability assessments, including off-line vulnerability testing, are components of risk management practices.

6.1 Vulnerability Management Resources

Some public resources that provide information on vulnerabilities within digital asset configurations include:

- Center for Internet Security (CIS) Benchmarks
- Security Content Automation Protocol (SCAP)

The CIS is a public service organization that captures configuration information for commonly used computing platforms. SCAP is a suite of specifications for organizing, expressing, and measuring security-related information in standardized ways, as well as related reference data such as unique identifiers for vulnerabilities.

Following are some resources that utilities may use to address vulnerabilities:

- Common Vulnerabilities and Exposures (CVE)
- Common Weakness Enumeration (CWE)
- Common Weakness Scoring System (CWSS)
- Common Weakness Risk Analysis Framework (CWRAF)
- Common Configuration Enumeration (CCE)
- Common Platform Enumeration (CPE)
- Open Vulnerability and Assessment Language (OVAL)
- Common Vulnerability Scoring System (CVSS)

7 Conclusion

A comprehensive vulnerability assessment of a utility's operations systems is essential to provide an informed evaluation of a utility's security posture. No system or collection of systems as complex as a utility's operations network can ever be 100% secure. Selecting and deploying security protections is an exercise in cost/benefit analysis and judicious selection of appropriate cyber security protections and technologies. Armed with the information produced by a vulnerability assessment, a utility will be able to determine and prioritize mitigations for identified vulnerabilities, and more effectively apply resources to remediate the greatest risks.

8 Acronyms

ACL	Access Control List
AMI	Advanced Metering Infrastructure
CIP	Critical Infrastructure Protection
CIS	Center for Internet Security
CMDB	Configuration Management Database
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
DA	Distributed Automation
DCS	Distributed Control Systems
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name Service
DVI	Digital Visual Interface
EMS	Energy Management Systems
FTP	File Transfer Protocol
ICS	Industrial Control Systems
IDS	Intrusion Detection System
IED	Intelligent Electronic Device
IP	Internet Protocol
IPS	Intrusion Protection System
MAC	Media Access Control
NERC	North American Electric Reliability Corporation
NESCOR	National Electric Sector Cybersecurity Organization Resource
PDA	Personal digital assistant
PLC	Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition (SCADA)
SCAP	Secure Content Automation Protocol
SIEM	Security Information and Event Management
SNMP	Simple Network Management Protocol
SMTP	Simple Mail Transfer Protocol
TCP	Transmission Control Protocol

TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
VGA	Video Graphics Array
VLAN	Virtual Local Area Network
VPN	Virtual Private Network