White Paper

Better, Faster NERC CIP Vulnerability Assessments Using NP-View

Network & Security Technologies // Network Perception

June, 2020

This white paper presents how to approach the NERC CIP-010 R3 Vulnerabilities Assessments requirements and build an automated assessment process using NP-View to save time and resources.

Table of Contents

Executive Summary 4

Introduction 4

Network Perception 4

N&ST 4

FERC, NERC and Regional Entities 5

Introduction to NERC CIP Vulnerability Assessments 5

NERC CIP Requirements and Guidelines and Technical Basis 5

Active Vulnerability Assessments vs. Paper Vulnerability Assessments 7

Preparation 8

Requirements 9

Paper Vulnerability Assessments 9

How This Is Manually Done Without NP-View 9

How This Is Automated With NP-View 10

Active Vulnerability Assessments 13

How This Is Manually Done Without NP View **Error! Bookmark not defined.**

How This Is Automated With NP-View **Error! Bookmark not defined.**

Documentation 15

How To Complete The Assessment Using NP-View's Results 15

Plan to Remediate or Mitigate 16

Other VA Activities 16

Network Discovery 16

Network Port and Service Identification 16

Vulnerability Review / Vulnerability Scanning 16

Wireless Review / Wireless Scanning 17

Other Possible VA Activities 17

Physical Port Assessments 17

Patch Assessments 17

Malicious Code Prevention Verification 18

Baseline Configuration Review 18

Conclusion 18

Executive Summary

The main objective of this paper is to receive recommendations and step-by-step instructions on how to build a better cyber vulnerability assessment methodology from the experience of leading experts in North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) cybersecurity Reliability Standards at N&ST and Network Perception.

Compliance to cybersecurity standards, such as NERC CIP, can become an opportunity for organizations to establish standardized processes and gain efficiency. In the electric industry, this opportunity means building a culture of risk assessment and mitigation across all the parties involved with managing, regulating, and overseeing the grid, with the goal of maintaining a more secure and reliable grid in the process. CIP-010 Requirement R3 stipulates that a paper vulnerability assessment (PVA) and an active vulnerability assessment (AVA) need to be performed annually and every three years, respectively. This paper presents each approach in detail through the lens of leveraging NP-View, a software solution to automate the review and analysis of network device configuration files. NP-View can not only help save significant time and resources, it is likely to also eliminate instances of potential human error when executing key tasks within CIP-010, R3. The controls provided in the AVA tasks can be more effective with the collection of fresh and updated evidence that will be reviewed and analyzed with NP-View. This paper concludes with a discussion of additional vulnerability assessment activities that can help an organization improve its program.

Introduction

Network Perception

Network Perception was launched in 2014 at the University of Illinois at Urbana-Champaign Research Park. Founded by a team of experts on network security and critical infrastructure protection, Network Perception delivers a pioneering solution, NP-View, that enables corporate compliance and cyber security managers to gain a complete view of their network security and immediately determine if its configuration is in alignment with best practices and regulatory standards.

NP-View is designed to solve complex compliance and security audit challenges by performing an automated and comprehensive analysis of network device configuration files. The solution works offline and performs an analysis of firewall, router, and switch configurations to determine connectivity and identify any deviation from security policies, standards, and best-practices. The network visualization enables technical as well as non-technical users to understand issues faster.

With the increase in architecture complexity, leveraging the right technology is crucial to understand network connectivity. This is critical to assess the exposure of protected assets to different network segments and to verify access to ports and services across different trusted zones.

N&ST

Network & Security Technologies (N&ST) is an employee-owned cyber security consultancy founded in 2003. Sharing a passion for utility cyber security, N&ST's founders created a consulting organization that distinguishes itself through its guiding principle of focusing on the customer's needs above all else. This focus has resulted in N&ST becoming leading experts in North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Cyber Security Reliability Standards since the Urgent

Action Standard 1200 in 2003. As an employee-owned business without outside investors, N&ST is built to last.

N&ST employees have been regular attendees and speakers at industry events and have been involved in the development and revision of industry standards and guidelines. N&ST employees have served as regional entity auditors, have supported our clients throughout the audit process, and have observed audits on behalf of our clients.

From its earliest days, N&ST has offered to help our clients complete their annual vulnerability assessments. N&ST has conducted nearly a hundred CIP-010, R3 Vulnerability Assessments (VAs) on behalf of responsible entities of all sizes across all of the NERC regions. The knowledge gained through these engagements has allowed N&ST to build an efficient VA methodology that also maintains the high level of thoroughness that its clients have come to expect.

FERC, NERC and Regional Entities

The Federal Energy Regulatory Commission (FERC) was established in 1977 as a replacement for its predecessor, the Federal Power Commission. Originally, its mandate was limited to determining whether wholesale electricity prices were unjust and, if so, to regulate its pricing. Over the next three decades the number of energy sectors it regulates grew. In 2005 the Energy Policy Act gave FERC authority to oversee the reliability of the bulk power system, also referred to as the bulk electric system or the power grid. The Energy Policy Act also gave FERC the authority to approve mandatory cyber security reliability standards.

In 2006, FERC certified the North American Electric Reliability Corporation (NERC) as the nation's Electric Reliability Organization (ERO), which in turn developed a set of Reliability Standards addressing a wide array of topics to support the integrity of the bulk electric system. On January 18, 2008, FERC issued Order No. 706, the Final Rule approving the first version of the CIP Reliability Standards, while concurrently directing NERC to develop significant modifications addressing specific concerns.

In 2007, FERC approved agreements by which NERC delegates its authority to monitor and enforce compliance to the reliability standards, including CIP, to Regional Entities which today consist of: Midwest Reliability Organization (MRO), Northeast Power Coordinating Council (NPCC), ReliabilityFirst (RF), SERC Reliability Corporation (SERC), Texas Reliability Entity (Texas RE), and Western Electricity Coordinating Council (WECC). Although there are minor differences with how each Regional Entity is structured and how they conduct their activities, they share the same responsibilities as they pertain to the CIP Reliability Standards: compliance assistance, compliance monitoring, and compliance enforcement.

Introduction to NERC CIP Vulnerability Assessments

NERC CIP Requirements and Guidelines and Technical Basis

At the time of this writing, FERC has approved eleven mandatory NERC CIP Reliability Standards at various version levels subject to enforcement:

Standard	Standard Name
CIP-002-5.1a	Cyber Security - BES Cyber System Categorization

CIP-003-8	Cyber Security - Security Management Controls
CIP-004-6	Cyber Security - Personnel & Training
CIP-005-5	Cyber Security - Electronic Security Perimeter(s)
CIP-006-6	Cyber Security - Physical Security of BES Cyber Systems
CIP-007-6	Cyber Security - System Security Management
CIP-008-5	Cyber Security - Incident Reporting and Response Planning
CIP-009-6	Cyber Security - Recovery Plans for BES Cyber Systems
CIP-010-2	Cyber Security - Configuration Change Management and Vulnerability Assessments
CIP-011-2	Cyber Security - Information Protection
CIP-014-2	Physical Security

FERC has approved for future enforcement new versions of three of those Standards, as well as two new Standards:

Standard	Standard Name
CIP-005-6	Cyber Security - Electronic Security Perimeter(s)
CIP-008-6	Cyber Security - Incident Reporting and Response Planning
CIP-010-3	Cyber Security - Configuration Change Management and Vulnerability Assessments
CIP-012-1	Cyber Security - Communications between Control Centers
CIP-013-1	Cyber Security - Supply Chain Risk Management

Each Standard contains a section called Guidelines and Technical Basis (G&TB). This section provides insight into the Standard Drafting Team's intentions for each Requirement and Part as well as providing suggestions to entities for achieving compliance to those Requirements and Parts. While this information is beneficial to entities, this section of each Standard is not approved by FERC, nor are Regional Entities meant to audit against those suggestions (though in practice, that is not always the case). Still, with many areas of the NERC CIP Reliability Standards vague and up for analysis, the G&TB sections provide useful information for entities to develop their interpretations of Requirements and Parts that are not clearly defined.

Per CIP-010, Requirement R3, two types of Vulnerability Assessments are identified. There are requirements for an **annual Paper Vulnerability Assessment** (PVA) and **every-three-years Active Vulnerability Assessment** (AVA). For each assessment type, the G&TB "strongly encourage" entities to include at least the following elements, taken from NIST SP 800-115[1], as well as reviewing this NIST Technical Guide for guidance on approaches and methods to execute each:

- Network Discovery
- Network Port and Service Identification

[1] NIST SP 800-115 Technical Guide to Information Security Testing and Assessment (https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf)

- Vulnerability Review/Scanning
- Wireless Review/Scanning

Additionally, in The Lighthouse publication[2], ReliabilityFirst recommends entities review NIST SP 800-30r1[3] for guidance in conducting an Active Vulnerability Assessment.

Active Vulnerability Assessments vs. Paper Vulnerability Assessments

Per the G&TB in CIP-010, the following are "strongly encouraged" tasks for a PVA and an AVA, as well as the associated CIP-005, CIP-007, and CIP-010 Requirements and Parts for which they may provide detective controls:

Paper Vulnerability Assessment		
Task	**Description**	**Requirement / Part**
Network Discovery	A review of network connectivity to identify all Electronic Access Points.	CIP-005 R1 Part 1.2
Network Port and Service Identification	A review to verify that all enabled ports and services have an appropriate business justification.	CIP-007 R1 Part 1.1
Vulnerability Review	A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.	CIP-005 R1 Part 1.3 CIP-007 R5 Parts 5.4 - 5.7
Wireless Review	Identification of common types of wireless networks and a review of their controls if they are in any way used for BCS communications.	CIP-005 R1 Part 1.1

Active Vulnerability Assessment		
Task	**Description**	**Requirement / Part**
Network Discovery	Use of active discovery tools to discover active devices and identify communication paths.	CIP-005 R1 Parts 1.1 - 1.2
Network Port and Service Identification	Use of active discovery tools to discover open ports and services.	CIP-007 R1 Part 1.1 CIP-010 R1 Parts 1.1.2 - 1.1.4
Vulnerability Scanning	Use of a vulnerability scanning tool to identify known vulnerabilities associated with services running on open ports.	CIP-007 R2 Part 2.3 CIP-007 R5 Parts 5.2, 5.4 - 5.7

[2] The Lighthouse, May/June 2017 edition, pages 9-10 (https://rfirst.org/about/Newsroom/Newsroom%20Library/Issue%203%20May%20June%202017.pdf)
[3] NIST SP 800-30r1 Guide for Conducting Risk Assessments (https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf)

Wireless Scanning	Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BCS.	CIP-005 R1 Part 1.1

While both PVA and AVA tasks are used as detective controls for complying with the above requirements, the controls provided in AVA tasks are more effective. At a high level, the review of evidence in PVA tasks simply identify issues associated with the documenting and/or maintaining of that evidence. AVA tasks, however, include the collection of *fresh* (updated) evidence that is reviewed and analyzed. AVA tasks can not only identify those documentation issues, they can also identify issues associated with processes followed to meet their respective compliance obligations. As an example, the review of network port and service evidence in a PVA assumes that port and service list is accurate when identifying missing or insufficient business justifications. In an AVA, the network port and service assessment adds the compilation of a *fresh* network port and service list to compare to existing evidence. This comparison can shine a light on issues related to the methods followed when the list of ports and services were initially collected, how dynamic port ranges associated with services were determined, or if unaccounted for software was installed enabling a previously undocumented port.

As described above, executing PVAs and AVAs have a much greater importance to an entity's CIP compliance program than simply complying with CIP-010 Requirement 3 Parts 3.1 and 3.2. While automating PVA and AVA tasks improve the efficiency with which the tasks can be executed, that automation also eliminates instances of potential human error when executing the tasks. Thus, an automated solution, such as Network Perception's NP-View, can play an important role to assist entities with automating a number of the tasks above. NP-View is also leveraged by NERC regional auditors for validating evidence during audits.

Preparation

In either a PVA or AVA, one key factor for success is a detailed VA plan, which should include:

- Roles and responsibilities
- Preparation, including:
    - Personal protective equipment requirements,
    - Site access requests,
    - System access requests,
    - Change request tickets, and
    - VA data storage location.
- Data collection
- Onsite activities
- Data analysis

Another key success factor is entity subject matter expert (SME) engagement in the VA process. Regardless of how well versed the VA team members are in the VA process, inaccurate or incomplete data collected from the Cyber Assets ensures an unsuccessful VA. Additionally, SMEs typically provide the VA team with a more detailed view of the networks than can be collected from network diagrams alone.

Requirements

At a minimum, the needed data inputs for conducting a NERC CIP Vulnerability Assessment include:

- NERC CIP Cyber Asset Inventory lists, including:
    - Unique identifier, such as hostname,
    - IP addresses and subnet mask, and
    - Electronic Security Perimeter (ESP).
- List of Intermediate Systems,
- List of ESP networks with included network subnets and their respective Electronic Access Points (EAPs),
- CIP-007 R1 Part 1.1 ports and services justification evidence, and
- CIP-007 R5 Parts 5.4 - 5.7 password controls evidence.
- Configuration files in format readable by NP View

NP-View uses device configuration files from firewalls, routers, and switches to create a network diagram that allows compliance auditors and other users to understand objects, routes, permissions, and policies in a user readable format. To input the device files in the correct format, follow the instructions at https://portal.network-perception.com/static/kb/npview-supported.html. If a particular hardware/software platform is not supported, please contact support@network-perception.com to start the implementation of a new configuration parser.

Paper Vulnerability Assessments

The material difference between a Paper Vulnerability Assessment and an Active Vulnerability Assessment is that the Paper VA is performed offline with existing data and evidence while the Active VA relies on the results of plugging into the target network(s) to actively explore and interrogate discovered nodes to acquire *fresh* input data.

Performing a PVA Manually Without NP-View

A. Data Preparation:

Step A.1: Prepare the raw data for rule analysis. Collect the configurations for the in-scope firewalls designated as Electronic Access Points (EAPs). Endeavor to convert these into as common a format as possible to ease iterative comparison between the individual rulesets from the separate configurations. If the scoped EAPs are from a variety of firewall hardware vendors, be prepared to manually interact with each separate CLI and GUI management environment in order to export the rules into a portable format.

Step A.2: Normalize the protocol / port / application into a single format to enable grouping and comparison. Settle on a single format, and conform all input data into that format. For example, use a single string of characters for interactive service, converging onto a single style to enable comparison: “tcp/22”, “TCP/22”, “SSH”, or “Secure Shell”. Consistency in capitalization can ease comparison of the character strings.

Step A.3: Translate and expand the firewall objects into the actual underlying IP addresses. This action may include expanding objects nested within other objects into the actual IP addresses to perform the analysis.

B. Data Analysis:

Step B.1: Analyze the collected rules to identify access permissions interacting with an ESP network range which could be considered broad, relaxed, and "overly permissive" by an RE audit team. This step should include checking for any of the following with either a source or destination of an ESP network or an individual BES Cyber Asset:

2. Use of wildcards or 'Any' for either source or destination,
3. Any access permissions which enable access to or from the Internet,
4. Any access permissions that cannot be demonstrated to be required (e.g., a network-level permissions based on an IP network mask of /24 or larger).

This step evaluates compliance with the following requirement:

- CIP-005 R1.3: "Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default."

Step B.2: Determine whether any access rules permit interactive protocols inbound to BES Cyber Assets without originating at a formally declared Intermediate System (IS), often described as a 'jump host'. The set of protocols that are considered 'interactive' within the relevant region should be used as a starting point; this list should be informed by the practices of the target entity being assessed for specific applications deployed and non-standard ports.

This step evaluates compliance with the following requirements:

- CIP-005 R2.1: "For all Interactive Remote Access, utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset."

Step B.3: All access rules should be verified to have business justifications. These justifications may be implemented as inline remarks and comments within the actual rules or might be references to an external list. Assess whether the justifications:

1. Are present for every access rule,
2. Adequately represent the actual business use. The name of a protocol or application alone is generally not considered an adequate business justification.

This step evaluates compliance with the following requirement:

- CIP-005 R1.3: "Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default."

Automating a PVA With NP-View

The manual approach described in the previous section can be extremely time consuming and prone to human error. In the following section, step-by-step instructions to leverage the NP-View are described. There are two core advantages to leveraging NP-View. First, the data preparation time is reduced from days to minutes. Secondly, NP-View allows for a much more comprehensive and efficient method for reviewing rulesets and checking network connectivity. In particular, NP-View shows information the same way regardless of the source manufacturers of the imported configuration files. Moreover, automated lookups of rules, their object groups, and how they translate into paths drastically reduce the amount of effort required to spot issues.

A. Data Preparation:

Step A.1: Import the collected network device configurations into a new NP-View project, so that the topology map can be visualized.

Step A.2: Review the asset inventory, and update the topology map with the correct labels, groupings, and criticalities:

1. Identify and label each EACMS on the map (right-click > Label options > Set display name),
2. Identify and label each EAP on the map,
3. Identify the BES Cyber Assets and PCAs, marking their criticalities (right-click > Criticality > High or Medium),
4. Select an EAP and the attached BCAs and PCAs to create a visual group named ESP.

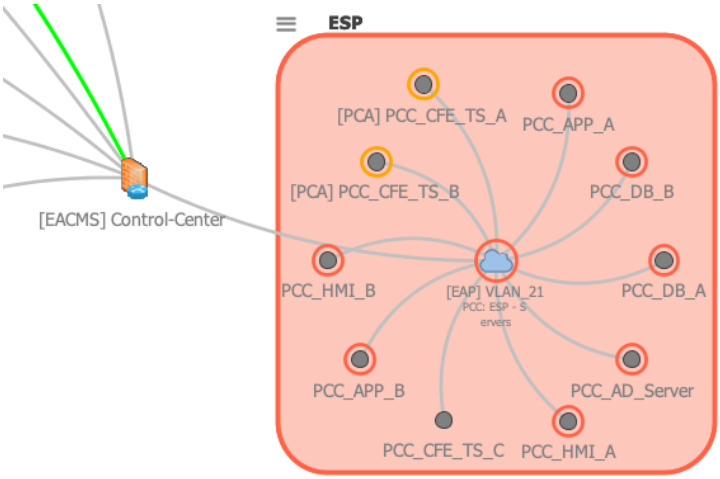


Figure 1: Visualizing the ESP with the grouping feature

B. Data Analysis:

Step B.1: Verify that the resulting topology map is consistent with the asset inventory. If discrepancies are found, they should be documented as part of the observations. Those 3 steps validate compliance with the following requirements:

- CIP-005 R1.1: "All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP."
- CIP-005 R1.2: "All External Routable Connectivity must be through an identified Electronic Access Point (EAP)."
- CIP-005 R1.3: Validates in part by detecting permissions to IP addresses that are not or are no longer associated with a Cyber Asset.

Step B.2: Check that the access policy rules bound to the EAP are correctly justified and that they allow only the traffic needed by reviewing in the Rule Audit table any Risk Alerts and Descriptions / Justifications:

- Use the Rule Marker to mark rules that do not have a documented justification or have an invalid justification,
- Use the Rule Marker to mark rules that are overly permissive and that triggered a risk alert.

The Risk Alerts can be customized through the Analyze menu. One should verify that the default alerts are enabled:

- CIP-005 R1.3: "Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default."

Device	Lin...	ACL/Binding	Source	Destination	Service	Action	Description	Risk
Control-Center	446	From_VLAN_21	*	*	Service_ICMP ICMP/8 ICMP/0/*	permit	Allow Echo and Echo-Reply to EMS Networks for...	
Control-Center	448	From_VLAN_21	PCC_App_Servers	All_Satellite_Clocks	UDP/123	permit	Allow App servers access to the satellite clocks	
Control-Center	450	From_VLAN_21	PCC_All_ESP_Servers	PCC_WSUS_Server	Service_WSUS	permit	Allow WSUS server access to supported systems	Low Risk alert: TCP/443 HTTPS
Control-Center	452	From_VLAN_21	PCC_All_ESP_Servers	PCC_RHEL_Server	Service_RHEL	permit	Allow RHEL server access to supported systems	Low Risk alert: TCP/443 HTTPS
Control-Center	454	From_VLAN_21	PCC_All_ESP_Servers	All_Jumphosts	Service_SCADA	permit	Allow SCADA/EMS communication	

Figure 2: Reviewing the ESP access policy rules to validate filters and justifications

Step B.3: Using the topology map, identify VPN access (highlighted in green), reviewing the configuration section related to those VPNs. Check if authentication is correctly configured. This step evaluates compliance with the following requirement:

- CIP-005 R1.4: "Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets."

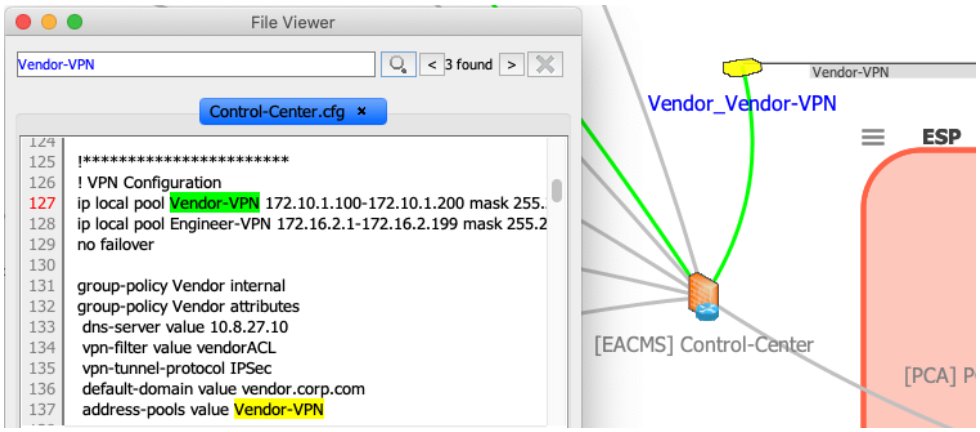


Figure 3: Reviewing VPN configuration to verify that authentication is correctly configured

Step B.4: Using the topology map and the asset inventory, identify network devices that have intrusion detection capabilities and/or application layer filtering capabilities (e.g., next-generation firewalls). Launch a path analysis to verify that network traffic entering and leaving the ESP is monitored by those devices. This step evaluates compliance with the following requirement:

- CIP-005 R1.5: "Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications."

Note: To be complete, the path analysis may require the import of route information into NP-View by exporting the routing table from a router into a text file and by naming the file according to the hostname of the router.

Step B.5: Launch a path analysis to visualize possible network connectivity:

- Right click on each component of a BES Cyber System, selecting "Filter path analysis…" > "Incoming paths",
- Verify that the paths using an interactive remote access protocol and that terminate at the selected BES Cyber System component originate from a valid Intermediate System. Also verify the use of non-traditional ports for the SCADA/EMS HMI and other applications.
- Right click on the jump host, selecting "Filter path analysis…" > "Incoming and outgoing paths" to review the interactive remote access protocols permitted to go through the jump host. Verify that the protocols used from remote hosts to the jump hosts use encryption.

This step evaluates compliance with the following requirements:

- CIP-005 R2.1: “For all Interactive Remote Access, utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.”
- CIP-005 R2.2: “For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.”

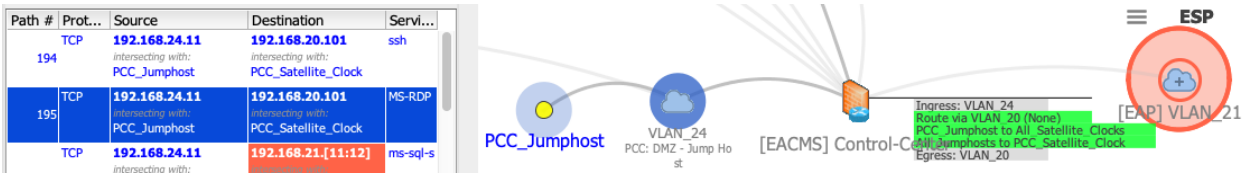


Figure 4: Reviewing network path originating from or terminating at the ESP to verify interactive remote access

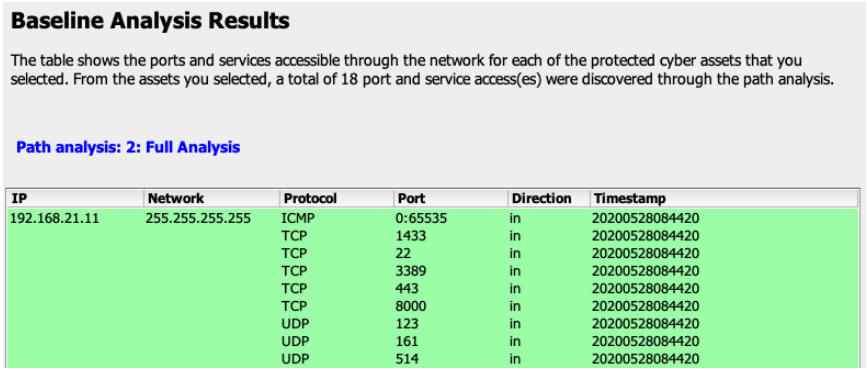
Step B.6: Select "Baseline Audit" in the Analyze toolbar:

- Select the "Create" option to generate a new baseline of ports and services,
- Choose applicable Cyber Assets to launch the analysis,
- Export the baseline table to a CSV file,
- Compare the baseline table from NP-View against the documented baseline data provided.

Differences found should be documented as part of the assessment of the following requirements:

- CIP-007 R1.1: “Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.”

Please note that this step only uses the firewall rulesets imported into NP-View to infer accessible ports and services inbound and outbound for devices in scope. This list may not be exhaustive. Getting the complete list of ports and services open on the device requires running an active tool such as netstat or a port scanner, which is detailed in the next section (Active VA Network Discovery).



Baseline Analysis Results

The table shows the ports and services accessible through the network for each of the protected cyber assets that you selected. From the assets you selected, a total of 18 port and service access(es) were discovered through the path analysis.

Path analysis: 2: Full Analysis

IP	Network	Protocol	Port	Direction	Timestamp
192.168.21.11	255.255.255.255	ICMP	0:65535	in	20200528084420
		TCP	1433	in	20200528084420
		TCP	22	in	20200528084420
		TCP	3389	in	20200528084420
		TCP	443	in	20200528084420
		TCP	8000	in	20200528084420
		UDP	123	in	20200528084420
		UDP	161	in	20200528084420
		UDP	514	in	20200528084420

Figure 5: Generating a baseline list of ports and services for a specific device using the path analysis

Active Vulnerability Assessments

Performing an AVA Manually Without NP-View

The earlier section on manual Rules Analysis steps for a Paper VA is expanded here to include Network Discovery as well as Port and Service Identification for an Active VA.

A. Data Preparation:

Step A.1: Beginning with network drawings, understand the structure of the network under assessment by acquiring drawings or creating them. Comprehension of the overall topology of the network is important, and the topology of the ESPs, in particular, is required. Verify that the discovered network architecture matches the documented architecture. Items to explicitly assess include:

- All ingress and egress traffic across an ESP boundary travels through an identified EAP,
- No undocumented access points to an ESP are found.

This step validates compliance with the following requirements:

- CIP-005 R1.1: "All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP."
- CIP-005 R1.2: "All External Routable Connectivity must be through an identified Electronic Access Point (EAP)."
- CIP-005 R1.3: Validates by detecting permissions to IP addresses that are not or are no longer associated with a Cyber Asset.

B. Data Analysis:

Step B.1: Select and use tools actively on the network to obtain *fresh* input data in accordance with the subject entity's Transient Cyber Asset (TCA) program. Example types of tools used to actively use:

- Port scanners, such as Nmap, netcat,
- Sniffer tools, such as tcpdump, Wireshark,
- Built-in command-line tools, such as ping, traceroute, etc.
- Vulnerability scanners, such as Nessus.

Specific operations to perform with the active tools:

- Discover and enumerate Cyber Assets with ping sweeps, comparing to the CIP-002 List,
- Capture traffic to identify any undocumented services,
- Probe for listening ports on the target Cyber Assets, comparing to baselines.

Step B.2: Document the discrepancies.

Automating an AVA With NP-View

The active VA with NP-View builds on top of the steps detailed in the previous section (paper VA with NP-View). The difference is that the output of active network discovery and port and service identification tools can be imported and visualized in NP-View to augment the observations.

A. Data Preparation:

Step A.1: Import the output of a network scanner such as Nmap or Qualys.

- From an existing NP-View project in which network device configuration files have been imported, select the "Nmap" option in the File toolbar,
- Select the Nmap XML output file (use the "-oX" flags when running Nmap),
- Once imported, the NP-View Topology Map automatically reloads to show new hosts identified in the Nmap file. Nodes in the map are updated with port and service information extracted from the Nmap report.

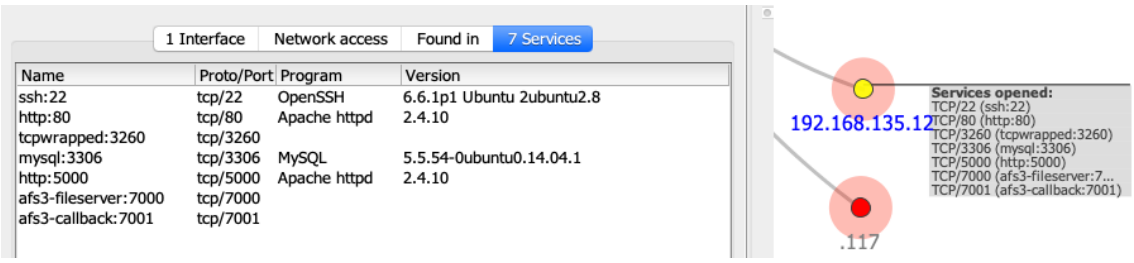


Figure 6: Showing port and service information from a Nmap report imported into a NP-View project

Step A.2: Import the output of the Netstat command.

- From an existing NP-View project in which network device configuration files have been imported, select the "Netstat" option in the File toolbar,
- Select the Netstat output file(s) (use the "-abon" flags when running Netstat on Windows and use the "-atunp" when running Netstat on Linux),
- Once imported, the NP-View Topology Map automatically reloads to show new hosts identified in the Netstat file(s). Nodes in the map are updated with port and service information extracted from the Netstat output.

B. Data Analysis:

Step B.1: Once network scans and/or Netstat files have been imported, compare the port and service information for devices in scope against the baseline data provided previously. These steps help to precisely evaluate compliance with the following requirements:

- CIP-007 R1.1: "Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed."

Documentation

Completing The Assessment Using NP-View's Results

The last step to complete the VA is to prepare a report detailing observations and recommendations. The report can be split into two document portions: a written summary with high-level conclusions and spreadsheets with detailed information to back up each observation. The summary can be written without including sensitive information (BCSI). The detailed spreadsheet should include the following sections:

- Discrepancies between the **Cyber Asset Inventory** and Cyber Assets identified in the network. For example, an IP address found in a configuration file that was not part of the documented inventory. The NP-View **Topology Map** can help present Cyber Assets and network segmentation.
- Observations about the rules, such as the level of permissiveness, the implementation of interactive remote access, and the justifications. The NP-View **Rule Audit Table** can provide this information through Rule Markers and Rule Comments. The NP-View **Path Analysis Table** that includes Path Comments can add contextual information about inbound and outbound network access control.

- Discrepancies between accessible ports and services and the existing baseline. For example, ports enabled on the firewall that are not identified in any baseline of a Cyber Asset within the ESP. The NP-View **Baseline Table** documents this information for each Cyber Asset.

Plan to Remediate or Mitigate

CIP-010, R3 Part 3.4 requires the documentation of an "action plan to remediate or mitigate vulnerabilities identified in the assessment". The documentation of the results of the assessment, or report, includes recommended actions to remediate and/or mitigate each identified vulnerability. Each recommended action should be recorded in the action plan and reviewed by responsible entity stakeholders to determine which course of action will be taken. In cases where remediating a vulnerability may not be possible for an extended period of time due to schedule or other factors, mitigation steps may be the short-term action taken with remediation the longer-term action. Each action item must include "the planned date of completing the action plan and the execution status of any remediation or mitigation action items", as required in CIP-010, R3 Part 3.4. It is also important to take into consideration the differences between production and test environments. Also, add a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting testing. For more information, please refer to Guidelines and Technical Basis (G&TB).

Other VA Activities

The CIP-010 Guidelines and Technical Basis suggest different approaches for the following VA activities depending on whether a passive or an active method is conducted. These activities can be part of the data preparation and collection phase.

Network Discovery

In a PVA, it is suggested that a review of network connectivity to identify each EAP for each applicable ESP. This can be accomplished through a review of network diagrams and applicable Cyber Asset network configurations. In an AVA, it is suggested that active network discovery tools be used to validate the documented network communications paths, as is described in the "Path Analysis for CIP-010-2 Active VA Network Discovery" section above. A sound practice for both a PVA and an AVA to include a physical walk down of each applicable ESP to confirm there are no undocumented wired network connections, wireless access points, or dialup modems, augmenting the network discovery review process.

Network Port and Service Identification

In a PVA, it is suggested that each applicable Cyber Asset's business justifications in CIP-007, R1 Part 1.1 evidence is reviewed for accuracy. In an AVA, it is suggested that an active discovery tool is used against each applicable Cyber Asset to identify its enabled logical network accessible ports. It is suggested that a responsible entity should use the currently enabled logical network accessible ports identified with the active tool to validate its CIP-007, R1 Part 1.1 and/or CIP-010, R1 Part 1.1.4 evidence.

Vulnerability Review / Vulnerability Scanning

In a PVA, it is suggested that a review of controls for default accounts, passwords, and network management community strings on applicable Cyber Assets be executed to identify undocumented

enabled default accounts, accounts, or community strings with default passwords (CIP-007, R5 Part 5.4), weak account passwords or community strings (CIP-007, R5 Part 5.5), and any accounts passwords or community strings older than 15 months (CIP-007, R5 Part 5.6). Additionally, a review of EAP rule-sets is suggested, as described in the "Rule-set Review" section above.

Vulnerability scans are suggested in the CIP-010 Guidelines and Technical Basis for an AVA. While there is no additional guidance provided, a thorough vulnerability scan is executed when the tool being used has administrator level privileges on the target Cyber Asset. Among the information that can be collected from each applicable Cyber Asset, or its test environment equivalent, includes:

- Enabled logical ports and their associated services,
- Enabled user accounts,
- Controls for password age, history, complexity, and length,
- Antivirus definition file age,
- Operating system or firmware version,
- Missing security patches,
- Software vulnerabilities, and
- Configuration vulnerabilities.

Wireless Review / Wireless Scanning

In a PVA, a review of controls for wireless network communications, such as encryption type, authentication mechanism, and age of pre-shared keys, passwords, or certificates is suggested when used for BES Cyber System communication. In an AVA, the use of active wireless scanning tools in each applicable Physical Security Perimeter to identify broadcasting and non-broadcasting wireless network communications.

Other Possible VA Activities

Physical Port Assessments

CIP-007, R1 Part 1.2 requires entities to protect against the use of unnecessary physical input/output ports on applicable Cyber Assets. Examples of these protections include the physical locking of the ports, logical disabling of the ports, or using signage to warn of unauthorized use of the port. As discussed in the Network Discovery section above, it is suggested that physical walk downs be conducted during both PVAs and AVAs, verifying that physical port locks and/or signage on or in close proximity to applicable Cyber Assets are in place, is an easy addition and effective detective control. NP-View also provides tables of physical and logical port status based on the configuration file imported. These tables can be printed from the NP-View Project Report prior to conducting a physical walk down.

Patch Assessments

Patch assessments are an increasingly common addition to the suggested vulnerability assessment tasks in the CIP-010 Guidelines and Technical Basis, specifically in AVAs. Typical vulnerability scanning tools used in AVAs collect information related to operating system, firmware, and software versions, as well as security patch installations. The responsible entity can assess its CIP-010, R1 Parts 1.1.1 through 1.1.3 and 1.1.5 evidence, as well as its CIP-007, R2 evidence, against this collected data to validate the accuracy of both the applicable Cyber Asset's baseline configuration and security patch implementation evidence. Note that a new feature is being developed in NP-View to help with patch prioritization. The objective is to combine the path analysis with the vulnerability report so that the more exposed security

issues can be addressed first. Contact support@network-perception.com to learn more about this feature before its incorporation into an official release.

Malicious Code Prevention Verification

Verification of malicious code prevention software and the associated virus definition files has become a common addition to the suggested vulnerability assessment tasks in the CIP-010 Guidelines and Technical Basis, for PVAs and AVAs. Those same vulnerability scanning tools report the presence and status of anti-virus software as well as the version and release date of its associated virus definition file. This data can be used to validate a responsible entity's CIP-007, R3 evidence.

Baseline Configuration Review

The five components of a CIP-010, R1 baseline configuration, as detailed in Part 1.1, are:

- Operating system(s) (including version) or firmware;
- Any commercially available or open-source application software (including version) intentionally installed;
- Any custom software installed;
- Any logical network accessible ports; and
- Any security patches applied.

A PVA or AVA already includes a review of logical network accessible ports. In an AVA, the vulnerability scanning tool likely collects the remaining components of a baseline configuration. Adding a review of baselines configurations to the annual CIP-010, R3 vulnerability assessment using this already collected data is a logical addition as a detective control to a responsible entity's CIP-010, R1 and CIP-010, R2 Configuration Change Management/Monitoring programs.

Conclusion

Both the annual and 36-month Vulnerability Assessments are among a handful of CIP Requirements that act as internal detective controls for other NERC CIP Requirements and Parts. They are also two of the more resource intensive requirements for entities to perform when including tasks beyond what is minimally suggested in the G&TB.

Having a thorough, efficient, and repeatable methodology for vulnerability assessments lays the groundwork for its successful execution. Executing that methodology with personnel that both have expertise in the NERC CIP Reliability Standards and experience conducting vulnerability assessments with automated tools is crucial to that success. NP-View allows those executing vulnerability assessments to more efficiently complete a number of the tasks while minimizing the risk of human error during the more tedious ones. The time saving and completeness aspects are critical as network environment becomes more complex and our resources remain limited.

For any questions or feedback, please feel free to contact the Network Perception team at support@network-perception.com or the N&ST team at info@netsectech.com.