

Summary Points:

1. This report explores two aspects of cybersecurity within substation networks: vulnerability assessments and network security monitoring. These are both critical to substation network security.
2. An independent test lab makes it easier to test and validate cybersecurity processes. The controlled environment enables methodical exploration of cybersecurity requirements and capabilities.
3. A number of software tools are available on the market to help automate both vulnerability assessment and network security monitoring. This report explores some of the more popular tools.
4. Having a team of experts guiding the work enables successful development and deployment of validated processes in substation networks.

To receive a PDF copy of this newsletter quarterly, please send an email to scott.olson@powereng.com or call 406-237-2000 and ask for Scott Olson.

NEXSTATION LAB REPORT: Q2 2018

This edition of the quarterly NexStation Lab report will focus on substation cybersecurity and how using an independent test lab can help organizations perform testing and demonstration projects to validate design and cybersecurity control specifications.

We'll explore two common cybersecurity issues within the substation environment: vulnerability assessments and network security monitoring. We will also discuss the ways in which an independent test lab can provide a controlled environment to address these issues.

VULNERABILITY ASSESSMENTS

One of the primary cybersecurity activities described in the North American Electric Reliability Corporation (NERC) critical infrastructure protection (CIP) Standards is the management of substation assets, including the performance of vulnerability assessments.¹

An independent test lab can be used to methodically develop and test solutions for these substation vulnerability assessments. A number of software tools are also available on the market to help automate the vulnerability assessment process. The following sections summarize key aspects of performing vulnerability assessments as well as notable features of some of the most popular software applications.

Network Ports and Services

One of the most important parts of a vulnerability assessment is determining which network services are being used by the devices on the network. Most network-enabled devices turn on additional network services by default to make it easier for the devices to be integrated into the overall network, but this practice provides a broader range of vulnerabilities to be exposed for exploitation. Besides reducing the number of network services available on a system and the potential for additional vulnerabilities, it also reduces the amount of processing load on a system.

If you look at it from the attacker's point of view, they are interested in identifying a weak point on a system to try malicious code. The fastest way to determine weak points is to see what network protocols and services are available on a system.

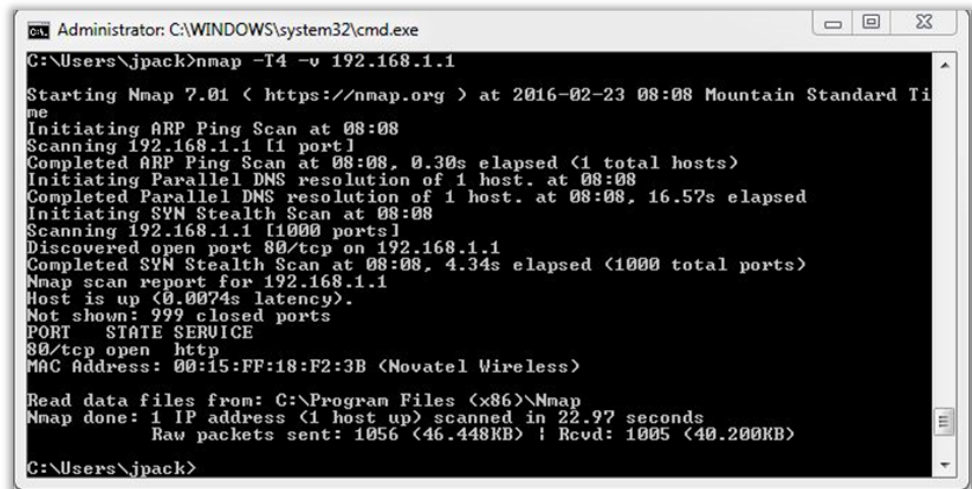
Nmap

The Nmap network port scanner is an open source program that queries network devices to determine several types of information. Nmap uses raw IP packets to determine what hosts are available on the network, which services (application name and version) those hosts are offering, which operating systems (and OS versions) they are running, which type of packet filters/firewalls are in use, and dozens of other characteristics.

Nmap is available for Microsoft Windows, MacOS and Linux, as well as source code. POWER's NexStation Lab offers Nmap on both Microsoft Windows and Linux. Most applications use the command-line version of the program for examples and scripting, but there is a graphical version (Zenmap) available. POWER also has Zenmap available in the lab.

¹ CIP-010-2 is the Configuration Change Management and Vulnerability Assessments Standard and describes the requirements needed for substations that have a significant impact on the bulk electric system (BES). CIP-010-2 also requires vulnerability assessments for high-and medium-impact locations.

Nmap should only be used on production networks and systems when the user is fully aware of the impact and consequences of using a network scanning tool. For example, using Nmap across a wide-area network (WAN) with limited bandwidth to remote substations will prompt network managers and potentially Energy Management System (EMS) operators to wonder why their SCADA information is delayed or lost, or prompt the communications and networking staff to ask why someone is scanning ports and filling up the connection tables on network firewalls. This is one major reason why using a test lab for this type of work is a major advantage over using production equipment and networks.



```

Administrator: C:\WINDOWS\system32\cmd.exe
C:\Users\jpack>nmap -T4 -v 192.168.1.1
Starting Nmap 7.01 ( https://nmap.org ) at 2016-02-23 08:08 Mountain Standard Time
Initiating ARP Ping Scan at 08:08
Scanning 192.168.1.1 [1 port]
Completed ARP Ping Scan at 08:08, 0.30s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:08
Completed Parallel DNS resolution of 1 host. at 08:08, 16.57s elapsed
Initiating SYN Stealth Scan at 08:08
Scanning 192.168.1.1 [1000 ports]
Discovered open port 80/tcp on 192.168.1.1
Completed SYN Stealth Scan at 08:08, 4.34s elapsed (1000 total ports)
Nmap scan report for 192.168.1.1
Host is up (0.0074s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 00:15:FF:18:F2:3B (Novatel Wireless)

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 22.97 seconds
Raw packets sent: 1056 (46.448KB) | Rcvd: 1005 (40.200KB)
C:\Users\jpack>
  
```

Figure 1. Example of what Nmap looks like when launched on Microsoft Windows. This scan shows a Novatel MiFi device to see what network services were running on it. Note that on the command line for Nmap there are two options followed by the target IP address.

OPTIONS	TARGET DESCRIPTION	EXAMPLE
None	<ul style="list-style-type: none"> Simplest case is target IP address or hostname for scanning. If a provided hostname resolves more than one IP address, only the first one will be scanned. Nmap also supports CIDR-style addressing. You can append /<numbits> to an IP address or hostname. Nmap supports octet range addressing also to allow different avoid scanning network and broadcast addresses. 	<ul style="list-style-type: none"> 192.168.10.0/24 (scans the 256 hosts between 192.168.10.0 and 192.168.10.255) 192.168.10.1-254 (scans the 254 host addresses and skips the all zero and all one subnet addresses)
-p <port range>	<ul style="list-style-type: none"> Specifies which ports you want to scan and overrides the default. Individual port numbers are OK, as are ranges separated by a hyphen (e.g. 1-1023). The beginning and/or end values of a range may be omitted, causing Nmap to use 1 and 65535, respectively. You can specify -p- to scan ports from 1 through 65535. 	<ul style="list-style-type: none"> -p 1-1023 (scans the TCP ports 1-1023) -p - (scans all 65535 TCP ports)
-sU	<ul style="list-style-type: none"> Enables UDP port scanning. 	<ul style="list-style-type: none"> -sU -p - (scans all UDP ports 1-65535)
-T	<ul style="list-style-type: none"> Provides six preset timing models to match desired results of scan. Some models are very slow with the intent to avoid detection. -T4 is a good compromise between fast scanning and waiting on TCP timeouts for inactive ports. 	<ul style="list-style-type: none"> -T4 (aggressive mode)

Table 1. Some of the important options and ways to specify targets that are useful for vulnerability assessments.

A common method of using Nmap in a test lab is to scan a group of devices on a substation network for all available TCP and UDP ports. This is the standard required by NERC CIP-010-2. Assuming the devices are all on the IP subnet 192.168.10.0/24, the command line for Nmap to scan all devices on all ports would be:

```
nmap -sU -sS -p- 192.168.10.1-254
```

Network Vulnerabilities

While Nmap is a good tool for network mapping and network service identification, it does not look at network services for potential vulnerabilities. Vulnerability assessment applications take the next step and look at each individual network service on each device. These tools use signatures and configuration baselines to identify vulnerabilities and configuration issues. These applications also provide reporting capabilities that make it fairly simple to create any detail of report required.

Even more advanced tests are enabled if the tools are given approved access to devices via authentication. For instance, the tools can examine patch levels on computers running the Windows and Linux operating systems or perform password auditing using dictionary and brute force methods.

Nessus

There are different levels of sophistication and features available for Nessus, a vulnerability assessment tool. POWER has the open source version available in our test lab.

In typical operation, Nessus begins by doing a port scan with one of its four internal port scanners (optionally, it can use external port scanners) to determine which ports are open on the target before it tries various exploits on the open ports. Available as subscriptions, the vulnerability tests are written in NASL (Nessus Attack Scripting Language) which is a scripting language optimized for custom network interaction.

Severity	CVSS	Plugin	Name
CRITICAL	10.0	97737	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya)
CRITICAL	10.0	97743	MS17-012: Security Update for Microsoft Windows (4013078)
CRITICAL	10.0	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
CRITICAL	10.0	100051	MS Security Advisory 4022344: Security Update for Microsoft Malware Protection Engine
CRITICAL	10.0	100057	KB4019215: Windows 8.1 and Windows Server 2012 R2 May 2017 Cumulative Update
CRITICAL	10.0	100764	KB4022726: Windows 8.1 and Windows Server 2012 R2 June 2017 Cumulative Update
CRITICAL	10.0	101365	KB4025336: Windows 8.1 and Windows Server 2012 R2 July 2017 Cumulative Update
CRITICAL	10.0	102683	Microsoft Windows Search Remote Code Execution Vulnerability (CVE-2017-8543)
CRITICAL	10.0	103131	KB4038792: Windows 8.1 and Windows Server 2012 R2 September 2017 Cumulative Update
CRITICAL	10.0	105109	Microsoft Malware Protection Engine < 1.1.14405.2 RCE
HIGH	9.4	103137	Security and Quality Rollup for .NET Framework (Sep 2017)
HIGH	9.3	81264	MS15-011: Vulnerability in Group Policy Could Allow Remote Code Execution (3000483)
HIGH	9.3	85847	MS15-101: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (3089662)

Figure 2. Screenshot from a report created by Nessus, one of the original vulnerability assessment tools released as open source but now a commercial application.

Nessus is designed to be deployed in a distributed fashion, with scanning engines located throughout an enterprise in order to minimize the cross-network traffic required for vulnerability scanning. Many different types of commercial, free and open source tools are available for Linux and Windows to help manage individual or distributed Nessus scanners.

As with any network testing applications, caution must be taken when conducting vulnerability scanning in the substation environment. Historically, vulnerability scanners have impacted operational devices by overloading their network connections, so it is best practice to scan control system networks during a scheduled facility outage or a planned time where availability of the devices is not critical to operations and safety. If a primary and backup control center environment is available, plan on scanning the inactive system then switching to the backup and scanning the primary while the backup is active.

In the substation environment, most of the equipment is specialized for protection, control, and monitoring the electrical system. Vulnerability assessment tools may not have signatures for many of these devices. However, as more control systems utilize general purpose hardware platforms and software solutions for communications and management functions (IEC 61850 and Human Machine Interfaces), more advanced vulnerability detection is required.

Utilizing a separate lab facility to test the impact of the vulnerability assessment tool on device types is highly recommended before using the application in the field. Having this standalone lab allows the development of a more detailed assessment plan and protocol to avoid unnecessary downtime and impact on operations.

NETWORK SECURITY MONITORING

Another requirement listed in NERC CIP is the need to perform detection of potential malicious communications for both inbound and outbound communications. Examination of the Guidelines and Technical Basis portion of the Standard indicates that the intent for this requirement includes implementing some form of intrusion detection or intrusion prevention systems (IDS/IPS) or other forms of deep-packet inspection. These technologies go beyond source/destination/port rule sets and thus provide another distinct security measure at the electronic security perimeter.

Network Intrusion Detection Systems

Network intrusion detection systems (NIDS) are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network. The systems perform an analysis of passing traffic on the entire subnet, and match the traffic to the library of known attacks. Once an attack is identified, or abnormal behavior is sensed, an alert or alarm can be sent to the administrator or operator.

An example of an NIDS would be installing it on the subnet where access points to network boundaries are located, in order to see if someone is trying to break into the network. The NIDS should scan all inbound and outbound traffic for the most effective deployment. In high-traffic networks or traffic with low latency requirements, this is not always possible.

Using a test lab resource for testing NIDS deployments before putting them into an operational environment is extremely important. Even if you design the NIDS to be passive and not integrated into the operational network, having a way to develop and test the design with real control system devices and network traffic is important to reduce the level of troubleshooting needed during deployment and commissioning.

Snort

Snort is an open source network intrusion detection and prevention system capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis and content searching/matching, and it can be used to detect a variety of attacks and probes.

Like Nessus, Snort started out as open source but was developed into a commercial product. You can still use the open source version of Snort for free, but the available signatures are limited to the open source signatures or your own signatures. POWER has the open source version of Snort available in our test lab.

When designing a Snort implementation, there are several factors to consider in developing the architecture. From a substation security view, there are two basic ways to configure Snort.

1. You can configure Snort to be “inline” on the network, which allows Snort to take actions based on the network traffic seen. For example, if Snort detects a port scan from a remote IP address, it can take steps to terminate and block the scan. That sounds great at first—it prevents the attack from happening, right? Well, what if the “attack” was really a false positive—Snort flagged it as bad traffic, but it was legitimate traffic and now you’ve stopped that network traffic from flowing. In a control system network, availability is the design priority, so in most cases, “inline” mode is not used.
2. “Passive” mode is normally what is used for control networks. In this mode, Snort is configured to only analyze and alert or alarm when it sees suspicious traffic. The implementation of “passive” mode uses either network taps to duplicate all traffic through a specific point of the network, or the span port on a network switch which collects all traffic from the switch and sends it to a designated port on the switch. In either case, the network traffic is sent to a separate collection point where the Snort sensor can check the network traffic.

Another architecture choice for Snort is the use of stand-alone sensors or distributed sensors. Unless you are only collecting information on one or two substations, it will be much easier to deploy distributed sensors from each substation and gather the sensor output into a centralized management station. You can also use the centralized management station to correlate Snort alert information with system logs and other types of monitoring information.

Snort is also attractive for control system networks because it supports two popular communications protocols with preprocessor support for DNP3 and Modbus, along with a wide variety of snort signatures using these preprocessors to make it relatively easy to create your own signatures as needed.

SUMMARY

Vulnerability assessments and network security monitoring are central aspects of substation network security. While this report discussed two aspects of cybersecurity associated with substation networks, it is important to note that there are many other cybersecurity requirements and capabilities that must be taken into account.

Using an independent test lab helps organizations make these processes easier to prototype and demonstrate within a controlled environment. Additionally, having expert resources and staff guiding the work enables successful development and deployment of these validated processes in substation networks.

SOLICITING YOUR INPUT:

We value your feedback and welcome input. Send your testing ideas to:

scott.olson@powereng.com

Disclaimer

This report is meant for informational purposes only. POWER Engineers, Inc. cannot be held responsible for readers' interpretation or use of this information. No endorsement of products or vendors is intended or implied. Trademarks and brands noted herein are the property of their respective owners.