# Low Cost ICS Network Scanning for Vulnerability Prevention

Robert Foote[1], Niroop Sugunaraj[2(✉)], and Prakash Ranganthan[2]

[1] Minnkota Power Cooperative, Grand Forks, ND 58201, USA
rfoote@minnkota.com
[2] University of North Dakota, Grand Forks, ND 58201, USA
{niroop.sugunaraj,prakash.ranganathan}@und.edu

**Abstract.** As newer devices are added to operational technology (OT) networks or remote access to them becomes more prevalent, security best practices are increasingly important to reduce vulnerabilities. This paper goes deeper into the tactical level that is lacking in most other regulatory or strategic literature and references NIST where applicable. Targeted audience is that of personnel in the OT network space, looking for a good low cost starting place to enhance security or mitigate vulnerabilities. Layered security through network segregation, vulnerability scanning methods, and firewall use in these specialized systems are explored. Documenting a baseline of a network is covered as the first step to understanding how to secure the network. Insight into ICS-friendly Nmap settings to assist in the host, port, and service discovery to supplement the baseline is provided. Nmap is shown as a viable open-source intrusion detection testing tool for firewalls to ensure a complete vulnerability assessment of the network. The tests documented in this paper are conducted on a small number of power substation devices, the scans ran through Nmap, and all network traffic monitored via Wireshark. Metrics and simple drawings accompany the ideas and suggestions presented in the text to give readers a place to start their own vulnerability mitigation strategies.

**Keywords:** Industrial Control Systems (ICS) · Information Technology (IT) · Nmap · Operational Technology (OT) · Vulnerability Assessment (VA)

## 1 Introduction

The management of SCADA and ICS systems is evolving; no longer are they a set-and-forget type of network where security was considered after reliability. Information technology features are integrated with OT devices, and our younger workforce brings a culture that expects to have networked communication with everything. Therefore, as newer devices and equipment replace the old, these


S. Paiva et al. (Eds.): SmartCity360° 2021, LNICST 442, pp. 332–350, 2022.
https://doi.org/10.1007/978-3-031-06371-8_22

systems become much more capable with routable protocols and remote maintenance access. These actions are fostering the acceptance of merging Internet Protocol (IP) with SCADA/ICS technologies; however, with those actions come IT vulnerabilities, potential attack vectors, and mitigation requirements [12]. These issues are addressed at a high level in the Framework for Improving Critical Infrastructure Cybersecurity (FICIC), published by the National Institute of Standards and Technology (NIST) [24]. NIST sets the benchmark for industry best practices, therefore in this paper we will periodically compare our recommendation with the NIST framework. The first step is to properly document a baseline. This baseline includes a physical inventory of devices and networks to understand how SCADA and/or remote maintenance communication is handled. Next, the logical connections, ports, and services need to be assessed, and this is where OT network managers need to tread lightly. Today, cyber threats are constantly evolving, and so there is pressure to ensure the security of all networks. Unfortunately, older ICS/SCADA networks are being neglected because security audits and penetrations tests are geared more toward modern IT systems [5]. Assets, ports, and services discovery are a critical part of a baseline and vulnerability assessment; however, many IT tools can be too intrusive to be used in the OT environment. Nmap is a free, open-source port scanning tool which has been tested to work, but the right commands are critical and are explained in greater detail within this paper. We wanted to break down the testing and findings in detail, as well as to provide recommended settings based on the results. Adding firewalls in strategic locations within the OT network can provide additional layers of security, but these, too, require periodic vulnerability assessments to verify their effectiveness. Nmap is also a great tool to see what traffic can traverse the firewall, helping to assess vulnerabilities. Security is an investment; and can be costly if an organization becomes a victim of a malicious actor. The recommendations in this paper are very basic in implementation time and cost, and with the right combination of strategies for managing OT networks, vulnerabilities can be mitigated, keeping SCADA/ICS environments safe.

## 2 OT Security in Simple Terms

The amount of documentation available concerning network security is overwhelming and can frustrate anyone who may be tasked to manage such things. There are many cybersecurity publications addressing OT network management, including ICS/SCADA networks. Many of the recommendations tend to be high level, from program management to how network protocols work. Others are more cautious, warning of issues caused by using IT techniques in OT environments. NIST publishes tools such as guides and frameworks, but those too can be daunting to know where to begin. This paper was written to address the lack of simplistic recommendations with the goal of getting the security "ball" rolling in an organization. Figure 1 shows the Shodan's ICS Radar, which is their own search engine used to crawl the Internet for protocols that provide raw, direct access to ICS [22]. Metrics are provided by Shodan, showing common industrial

protocols, and the numbers of exposed devices their search has uncovered. Additionally, a SANS Institute survey found that the percentage of control systems that experiences three or more malicious incidents in the previous 12 months increased from 35.3% in 2017 to 57.7% in 2019 [14]. The Shodan and SANS information proves the need for even the most basic security. Keep in mind that implementing basic security in manageable layers does not need to be complex or costly to be effective, and the sooner an OT network is secured, the safer the systems are that reside within it.

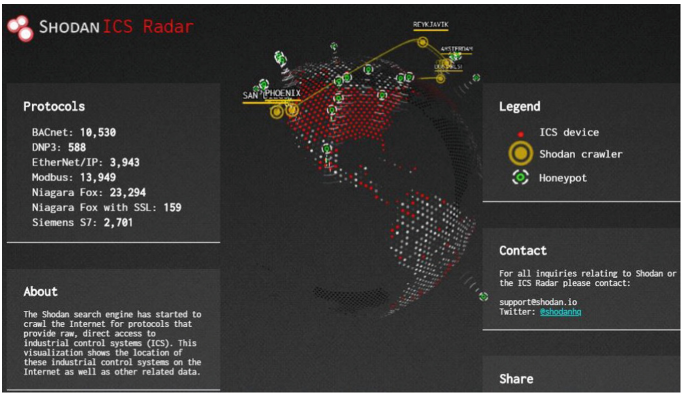



**Fig. 1.** Shodan ICS Radar

## 3 Related Work

Security for cyber physical systems (CPSs) such as ICSs and SCADA systems has observed measures that track the infrastructure's cyber health. Peterson [19] recommends using an application called "Quickdraw" funded by the U.S. Department of Homeland Security (DHS). This software was designed to create security event logs of all functional units such as remote terminal units (RTUs) or intelligent electronic devices (IEDs) within an ICS to passively detect any intrusions. This intrusion detection system (IDS) builds upon the open-source and well-known IDS Snort by: (1) augmenting Snort with industry standard protocols such as DNP3 to develop signatures of abnormal behavior for the IDS; and (2) developing a two-packet inspection technique that evaluates response and request packets to create security log events that are sent to authorized personnel for further action.

Graham et al. [7] introduce a security pre-processor for SCADA systems called "SCADA-Guard" to balance and secure both legacy systems which are highly vulnerable, and newer systems. The software-side of the pre-processor has three modules built on the microkernel system seL4: 1) a message authentication module that verifies data from input hardware to grant authentication and 2) a Modbus filter, and 3) DF-1 filter, that implement role-based access control for

hardware messages that use the Modbus and DF-1 data communication protocols. Access control is granted or revoked based on on-site policies specified by the system administrator. A control system implemented with this technology demonstrated resistance against buffer overflow and man-in-the-middle attacks among other security issues. This system also performed acceptably in terms of timing delays, exhibiting a maximum delay of 229 ms for a single read/write operation.

Attack-tree based security models proposed in SCADA security are conceptual diagrams that depict how security for a system can be achieved or compromised with the root node of the diagram denoting the goal and several leaf nodes being the means to achieve that goal. Tian et al. [26] propose a multi-faceted approach that enables the SCADA network's analysis and protection. The analysis module utilizes a "preference attack tree (PAT)" architecture which quantifies attacks through frequencies of use, and labeling these frequencies as the attacker's "preferences". This security module recruits three action items from the authors: (1) usage of firewalls to set a bandwidth for network traffic, (2) encrypted communication network and software, and (3) a monitoring system to identify anomalous traffic data. Test results indicate an approximate 100% success rate in preventing DoS, replay, integrity, and data injection attacks.

A three-layered IDS was proposed by the authors in [20] where each layer from the bottom up handles one of three functions: protection of the communication network, authentication for the command-and-control stations, and authentication for field devices. The first layer of this method utilized machine learning algorithms such as random forest (RF) to classify DoS-based attack features. RF exhibited 99.9% accuracy in correctly classifying attacks. The second layer simulates threat scenarios using a high-performance computing environment to test effects and suggest countermeasures. The final layer addresses threats to RTUs and utilizes machine learning algorithms such as AdaBoost/JRipper and Naive Bayes to assist the RTU in identifying and differentiating between a malicious attack and a natural disturbance. The result from the AdaBoost/JRipper model indicates a 94% accuracy in correctly identifying threats.

Chalamasetty et al. [4] use a novel approach in incorporating multiple communication networks such as mobile ad-hoc networks (MANETs), wireless sensor nodes (WSNs), and web-based SCADA. This integration is said to enhance flexibility, scalability, and security. This approach contrasts with traditional SCADA networks which comprise of multiple local area networks (LANs) connected to a single wide area network (WAN). To test the security of this network, the authors propose an intrusion detection and prevention (IDP) system responsible for monitoring, detecting, and rehabilitation (MDR) [1] to prevent DoS attacks. Simulation results indicated that the network's throughput was maintained with the IDP system, while preventing significant delays. The ratio between the packets delivered and packets sent was approximately 100%.

**Table 1.** A comparison of existing SCADA security tools in research and commercial environments.

| Tool | Type | Key feature(s) | Scale | Platform |
|---|---|---|---|---|
| Quickdraw [19] | Academia | SIEM for SCADA controllers | Limited scaling | Software system |
| SCADA-Guard [7] | | Role-based access control for field devices | Possible Scaling | Hybrid System |
| PAT-based Model [26] | | Network partitioning for SCADA architectures | Possible scaling | Software system |
| Triple-layer IDS [20] | | Data authentication for RTUs using ML | Limited scaling | Software system |
| MDR-based [4] | | IDPS for WSNs | Possible scaling | Hybrid system |
| Security architecture [23] | | Anti-virus solution for SCADA systems | Possible scaling | Software system |
| QRadar | Commercial | Data recovery & regulatory packages | Possible scaling | Hybrid system |
| ArcSight | | SOAR Integration | Possible scaling | Software system |
| Exabeam | | Compatibility with Multiple vendors | Possible scaling | Software system |
| LogRhythm | | AI-based UEBA | Possible scaling | Software system |
| InsightIDR (InsightVM) | | Deception to detect Malicious behavior | Possible scaling | Software system |
| Securonix | | Open Data, Hadoop based architecture | Possible scaling | Hybrid system |

Slay and Miller [23] developed a defense-in-depth security framework to accommodate legacy ICS systems and modern corporate systems. The three main security mechanisms within the framework are implemented at the network gateway at the boundary of the network: (1) a firewall which enforces rules for the passage of network traffic, (2) an IDS to monitor incoming and outgoing traffic between the SCADA and corporate networks, and (3) a network-based antivirus software to prevent virus propagation to the corporate network. A demilitarized zone (DMZ) is implemented within the firewall architecture to create a neutral-resource sharing platform for any unsecured data from sources such as wireless access points (APs). This framework was developed in collaboration with an Australian SCADA integrator and was implemented by PowerSystems Australia to secure its control systems [16].

Table 1 lists and compares research-proposed and commercial tools to identify the current security landscape for SCADA networks and OT systems. 'Scale' is defined as the ability of a tool to augment its capabilities and adapt to

different requirements. 'Deployment' refers to the type of components (software, hardware, or a combination) that are required by the tool when deployed to an use-case. All the commercial tools selected for this analysis are offered by leaders in the SIEM space as listed by Gartner in 2020 [13].

## 4 Baseline Documentation

Before one can implement security in their networks, they need to understand what is contained within and connect to them. Network configurations vary greatly in OT environments, and management methods for these networks will vary based on their device makeup and communication protocols. Knowing where to start in assessing the makeup and current state of devices is a daunting, but necessary task. National Institute of Standards and Technology (NIST) is a great place to look to when first assessing any OT networks. The NIST 800 series of publications relate directly to the topics presented in this paper, albeit at a higher strategic level. NIST recommends forming a team to define, inventory and categorize applications, computer systems and networks in addition to the devices contained therein [24,25].

Baseline documentation starts with physical assessments and a knowledge of network access needs. Simply looking at devices and physical cabling will allow the creation of a rough network drawing. If network drawings are available, these will be valuable to verify the physical findings against. Drawings are a snapshot in time, so they may not accurately reflect the current state of the network. Assets with specific communication types such as routable, serial or dial-up access need to be documented as such, since protective measures added later will be different for each type. Determine the networks used or needed. Is there a single SCADA network, a remote maintenance network or maybe some other combination? By understanding the accessibility requirements in the organization and determining the needs of both the users and services required for remote connectivity, a balance can be struck between business needs and the appropriate protection methods for critical assets [9]. Once the physical and network baseline is documented, you have completed some of the NIST FICIC functions for IDENTIFY, PROTECT and DETECT; see Fig. 9. Now, the second phase of the baseline can be initiated.

## 5 Ports and Services Discovery

Knowing what ports and services are running on each device or between networks is key in vulnerability mitigation. There are many IT type network scanning tools which boast asset discovery and network mapping. These tools may require Simple Network Management Protocol (SNMP) to work, and this protocol is not typically utilized in ICS devices. Using IT type tools which have not been tested or properly configured to interact with SCADA networks and their unique devices could cause those devices to become unresponsive [9]. Worse yet, that could alter the actual data being received, transmitted by or stored within

the device [6]. That being said, this paper provides a solution to performing the required ports and services scan to obtain critical information about the networked devices.

The overall goal of conducting such a scan is the creation of a list for all active devices and their associated ports, operating and responding within the address block in which the port scanning tool was used [21]. There are a few key security steps to be performed using the new port and service list. First, each device must be accounted for on the scan, and each open port in the device should be validated. If there is not a need for a port or service to be available, it should be disabled within the device if possible. This will reduce exposure risks and may also prevent unneeded communication chatter within the network. Later, the same port and service list can be used when setting up firewalls or other network whitelists. If any of the ports or services were disabled after the scan validation, they will need to be noted as such when documenting the baseline. These actions satisfy some of the NIST FICIC functions for IDENTIFY, PROTECT and DETECT; see Fig. 9.

## 6 Network Scanning

There is a lot going on within networks that cannot be seen without the right tools. Wireless networks should be assessed to ensure one does not have any unsecured entry points. There are different wireless protocols and tools to sniff them out, however that is beyond the scope of this paper. Just be sure that wireless scanning is not forgotten when any networks are assessed. Many OT devices utilize serial connections since this is typical of older products, as well as basic SCADA requirements. Serial port scanning can only be done by physically connecting to each serial network and running a specific program to capture COM port data. This does not function the same way as a network scanner which can find devices by address connected on the same network. This paper does not discuss scanning serial ports since they do not have the same vulnerabilities as Ethernet.

What is the focus of this paper is Ethernet communication and a no-cost open source scanner which works well within an Ethernet-based environment is Nmap. The official Nmap guide summarizes it best; “Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics” [18]. While Nmap was designed for use within the IT environment, it has enough flexibility in its commands to be used in the OT networks as well. One goal of performing a network scan is to see what devices are responding and what ports they will respond to. TCP scans require a handshake and these are a bit more accurate. The device and Nmap send brief messages back and forth to know the status of the port. A UDP scan is important to perform because there can be commonly exploitable vulnerabilities in their services as well, but these scans are not as accurate as TCP since there

is no handshake. Nmap needs to make an educated guess if the port is closed based on the packet response, or lack thereof. Another goal mentioned in the previous section is to document the discovered ports and services for each device. This information is critical in the quest to reduce vulnerabilities. Many devices come with a multitude of capabilities, however only a few are typically used in most applications. Take measures to "harden" devices by turning off or disabling unused ports and/or features [17]. Nmap can be run initially to see what is active in the network. Once device settings are modified to reduce the open ports and services footprint, the scan can then be run again. The Nmap program has a simple Graphical User Interface (GUI) called ZENmap and it is shown in Fig. 2. This is where the scan commands are entered such as the device or network address, TCP or UDP scan type and other host discovery options. While the laptop performing the test was on the same network as the test lab devices, Nmap allows the user to exclude this from the scan.

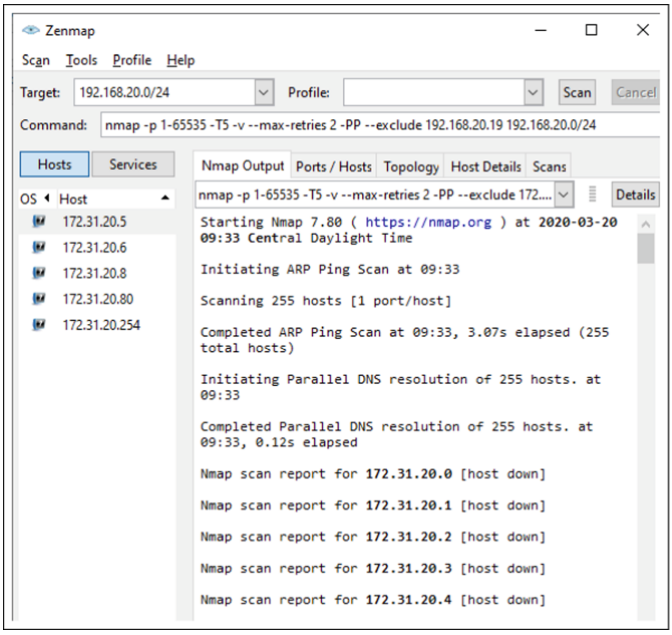
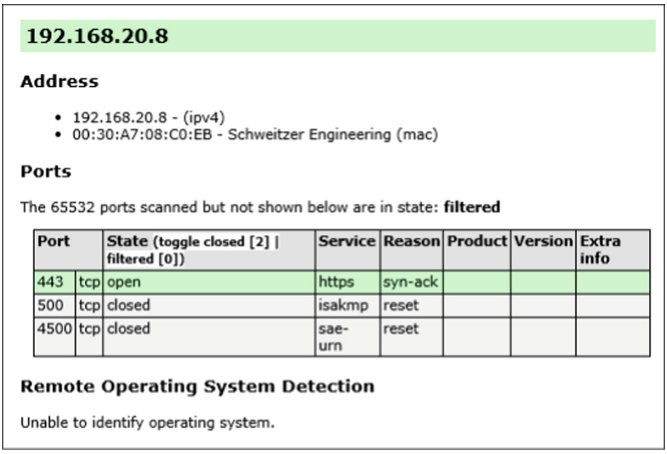



**Fig. 2.** Nmap/ZENMap GUI.

In Fig. 3 you can see the output report from Nmap. This example shows one device and the ports and services discovered. There are Nmap command options which provide more information such as operating systems and versions; however these were not selected in the sample test shown. The reports can be saved as documentation for each network, or device depending on the target set in the scan. If a device is reconfigured to close an unused port, or a new device is added to a network, a new scan is a great way to validate settings.



**192.168.20.8**

**Address**

- 192.168.20.8 - (ipv4)
- 00:30:A7:08:C0:EB - Schweitzer Engineering (mac)

**Ports**

The 65532 ports scanned but not shown below are in state: **filtered**

| Port | | State (toggle closed [2] \| filtered [0]) | Service | Reason | Product | Version | Extra info |
|---|---|---|---|---|---|---|---|
| 443 | tcp | open | https | syn-ack | | | |
| 500 | tcp | closed | isakmp | reset | | | |
| 4500 | tcp | closed | sae-urn | reset | | | |

**Remote Operating System Detection**

Unable to identify operating system.

**Fig. 3.** Nmap output report.

## 7 Methods

A test lab was set up with a SCADA network and a separate remote access network, both utilizing RJ45 Ethernet connections to a test laptop. The end devices consisted of a NovaTech®Orion LX RTU, NovaTech®Orion LXm RTU, Sierra Wireless®RV50X Cellular Gateway, Schweitzer Engineering Laboratories SEL-3620 Ethernet Security Gateway and a SonicWall®TZ400 firewall. A laptop ran the Nmap program for port scanning, while a separate tool called Wireshark analyzed all network packets. See Fig. 4 for the network diagram. Wireshark is a free open source packet analyzer which allows the user to observe network communication as it happens. This tool was set to focus on dropped packets and other errors that signify disruption to the normal operation of the devices in the test lab. Wireshark observed the SCADA network, and the test was run again with it observing the remote access network. Ultimately we wanted to observe if the Nmap scans caused the devices to become erratic or lose SCADA information or drop polls.

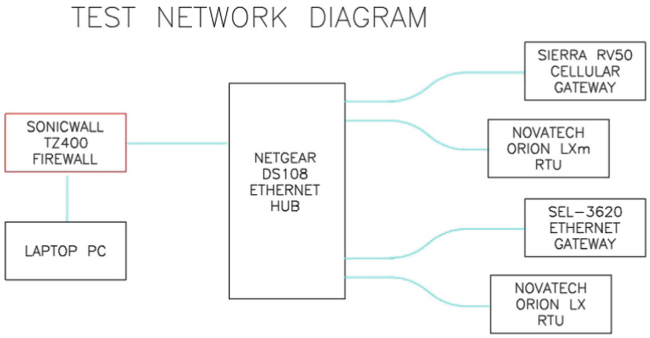



**Fig. 4.** SCADA test network setup.

Over fifty-five Nmap scans were completed in the test lab using different combinations of commands. Wireshark confirmed if each scan ran cleanly or if there were packet errors. Scan timing speeds were adjusted, the use of a discovery ping was toggled, and many other techniques from the Nmap user guide were explored. We tried using the command to get software and version information, however that introduced packet errors and there was not much data from the OT devices. Many different host discovery commands were tested which mainly consisted of various ping types. The standard Nmap scan uses an initial ping to find devices and that proved to be the most effective. Finally the scan techniques using Null, FIN, XMAS and others only proved to cause packet errors in Wireshark. A few of these scan types also fail to list ports at all. There were far too many combinations to easily present here, so we focused on the significant ones. See Fig. 5 and Fig. 6 for a detailed graphic which shows the focus of tests ran in the lab. The top portion of the chart shows UDP scans and the bottom shows TCP scans. Both scans were done inside the test network by connecting the laptop directly to the Netgear hub via Ethernet and we scanned all 65535 ports on each device and used echo ping for device discovery. Nmap has some prebuilt timing templates which range from T0 (very slow) to T5 (aggressive). These templates include many factors to include number of retries and the time between each host. You can actually specify any of the factors separately which can override that part of the timing template. The graphic focuses on the timing template, number of retries and errors generated in Wireshark. We wanted to understand what scan settings had the best combination of speed, accuracy and gentleness for the OT network. Overall it was noted that timing template T5 was too fast for reliable OT scans. This template leaves a max of only 5 ms of time between ports and some of our OT devices did not react well. While not shown in the graphic, the SEL-3620 seemed to have the most issues with fast T5 UDP scan rates, while the Sierra Wireless®cellular gateway locked up on a T5 TCP scan. Once the timing profile was turned down to T3 where there is 1000 ms maximum delay between ports, the devices seemed happy. Any slower timing profiles can be used, but keep in mind they add considerable time to the scans. The UDP Test graphic shows the T3 scan which is has a green column representing no Wireshark errors. This happens to use zero retries, but you can clearly see when retries are increased, the time the scan requires increases dramatically. This is because of the stateless connection with UDP. Nmap does not know if the port is open so it will retry and use a lot of time for each port to do so. While you may be concerned that there are not any retries, you could still run two of these scans in less time than a single scan using one retry. This would give a good average in case a second scan discovered something the first did not. The TCP Test graphic sows that all T5 through T3 timing profile scans finished in basically the same amount of time. The reason here is because of how TCP reacts. TCP uses a handshake and responds to the scan to state the port status. If the port is definitely open or closed, Nmap knows this right away and therefore there is not any need to retry that port. In effect, this is like using zero retries. We only had a small lab of five devices so the timing profile speed really did not differentiate themselves here.

Had we used a larger network or one that had more filtered ports which sometimes require more reties, the scan times would have been staggered further.

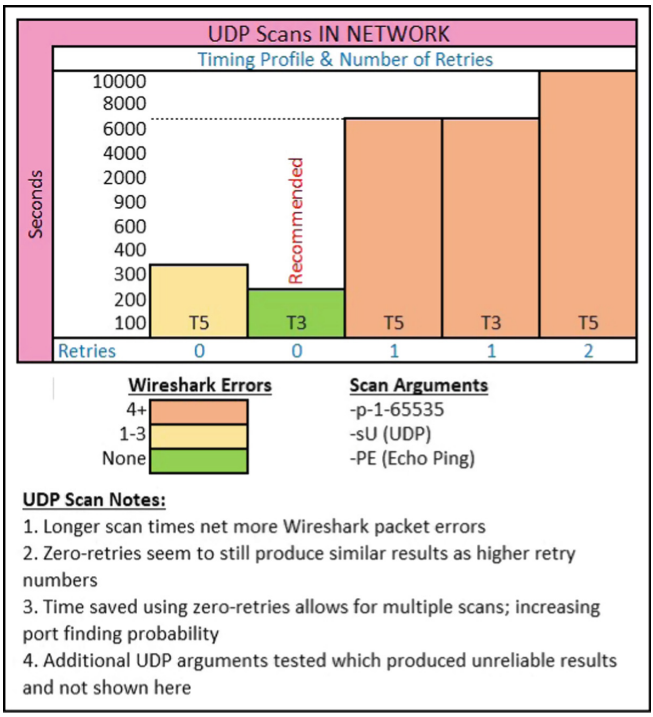



**Fig. 5.** UDP scans in network.

After thorough testing as noted above, we can recommend specific Nmap commands which are gentle on OT networks while having a good balance of speed and reliability for port and service baselines:

**TCP**: *nmap -sS -p 1-65535 -v –max-retries 2 –exclude x.x.x 0.0.0/24*
**UDP**: *nmap -sU -p 1-65535 -v –max-retries 0 –exclude x.x.x 0.0.0/24*

The TCP and UDP scans commands listed above differ slightly and require some explanation. The -sS command specifies a TCP scan, while -sU is the command for UDP. The *-p 1-65535* tells Nmap to scan every single port. If this was not included, Nmap only looks at the top 1000 most common ports and your baseline would be lacking. OT networks typically have less common protocols than IT networks and therefore need the extended port range. The -v allows for a verbose output. This simply gives status updates on the screen every few minutes and keeps you informed during long scans. The -max-retries are another key difference between TCP and UDP scans. As explained above, TCP uses handshakes and UDP scans are stateless which affect scan time. Setting

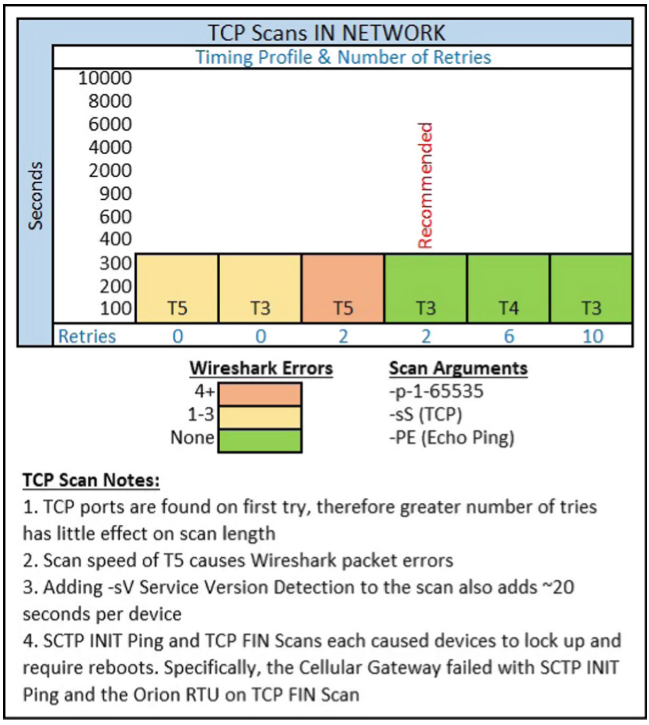



**Fig. 6.** TCP scans in network.

retries to zero drastically reduces the scan time, though surprisingly the error rate does not increase per our tests. If you are concerned with the potential for errors and have time to conduct lengthy scans, you can set this to 1 or 2 in a UDP scan. The *-exclude x.x.x* portion is how you exclude the computer address you are using for the scan. Substitute the x.x.x with the computer IP address. One would not want to scan the Nmap computer as this adds time and erroneous data to assessing a baseline. Finally, the 0.0.0/24 represents the target network or device being scanned, which should be changed to match the proper IP required for the target. One will notice no timing template is listed in the suggested command. This is because the default is T3 which works best with OT devices. With the steps and ICS-friendly Nmap commands provided, one should be able to quickly start scanning their networks for vulnerabilities.

## 8 Installing Firewalls

According to the Centre for Internet Security, "Defense in Depth (DiD) refers to an information security approach in which a series of security mechanisms and controls are thoughtfully layered throughout a computer network to protect the confidentiality, integrity, and availability of the network and the data

within" [11]. This term applies in the OT environment as well and the utilization of firewalls is an excellent security control layer. To prevent the discovery of ICS/SCADA devices should never be left unprotected connected to Internet or other public-facing network, because search engines such as Shodan, can easily find and track them [3]. Firewalls, Virtual Private Networks (VPNs) and/or Virtual Local Area Networks (VLANs) could all be used to protect these devices, however only firewalls fit in the scope of this paper. A firewall of the "stateful" variety inspects the source and destination IP addresses, as well as port numbers of all incoming or outgoing packets. Rather than using rules to reject or deny packets, use rules to silently drop them instead, as this masks the typical firewall response attackers could use during information gathering. The firewall should be invisible to a malicious hacker and not become a way to map the network based off of its responses [2]. Another benefit to using firewalls is their logs. You can set up logs which can alert when specific rules are challenged, if intrusion detection thresholds are reached or many other triggers. These logs are a great tool to use when troubleshooting communication issues across networks, or as forensics if a malicious event needs to be investigated. Finally, firewalls are a good way to segregate network addresses. Typically a Wide Area Network (WAN) address is set for the main traffic coming from a larger (possibly less secure) network. In the firewall, there is at least one additional network set up with a different network address. This is the Local Area Network (LAN) and using a different network address allows some separating of the end devices in the LAN from your WAN. It is in that "gap" where the firewall uses rules you specify to allow communication through based on addresses or services. Kind of like a bouncer at a club, one must have the right credentials to get in from the WAN to the LAN.

Setting up the firewall to Deny by Default is the only recommended method. This will effectively block everything unless it is something specifically set as allowed within a rule. Nmap scans come in handy here since it is already known what ports, services and device addresses are within the network. Simply use the scan results to then configure firewall rules. Even though the firewall can be used to block unwanted communication, one should still disable unneeded ports and services in their devices as well in case the firewall ever becomes compromised.

In the test lab, the SonicWall®TZ400 firewall was initially used as an end device to be discovered by Nmap. We reconfigured the network to put the SonicWall®between the test laptop and the ICS devices to perform its designed firewall function. Nmap was again used to test different rules and to monitor packets to understand how this device protected the network. Over twenty Nmap scans were completed in the test lab through the firewall and Wireshark was again utilized to observe packets for problems. The Nmap commands were adjusted to understand how the firewall reacted, since we were trying to simulate a malicious actor attempting to perform network reconnaissance. TCP was the only scan type documented here, as all UDP packets were dropped because of the rules we had set up in the firewall.

Scanning through the firewall to the devices behind it tests the firewall rules as well as its alert capabilities. Our test lab was set up as shown in Fig. 4. Nmap has some intrusion detection evasion commands which were tested to see how the firewall logs and alerts would react. Fragmented packets and bad checksum packets were purposely sent and the firewall sent alerts on port scan detection. An IP spoof was launched which allowed the Nmap user to input a fake IP address so the firewall thought the sender was on a different network or on the same one. While these attempts are not captured in Fig. 7, we do show key information. Different timing profiles were used to see if the firewall would react differently. While the scan times do change a small amount, it is negligible for the first nine scans, which only scanned between 1 and 100 ports in each device. The last scan shown in the graphic scanned all 65535 ports and that dramatically increased the time. Another notable finding in the graphic is represented by colors. The green columns had no firewall alerts because those scans did not use Echo Ping (-Pn) to verify the hosts. This is more stealthy yet you can see how it does increase scan times a small amount. All scans using ping raised an IP spoof alert and some scans with higher port numbers generated SYN Flood alerts as well. These alerts will differ depending on firewall settings, however you can use Nmap to tune those settings. The recommended Nmap command for scanning TCP through a firewall would be:

*nmap -sS -Pn -p 1-65535 -v –max-retries 2 –exclude x.x.x 0.0.0/24*

One of the tests we were most interested in was observing how Nmap reported ports which are blocked by the firewall. If you want to prevent traffic from going to a specific port or service, a rule is set to either deny or discard the attempt. When the rule was set to DENY traffic, Nmap would show the port closed. This is good, but it actually also shows a malicious actor that there is a firewall specifically blocking the traffic. With the firewall rule set to DISCARD traffic, Nmap shows the port as filtered. This would make it harder for a malicious actor to know what is going on in the network. They would not definitively know there is a firewall rule, so it could buy some time and muddy their reconnaissance. Our recommended Nmap commands for scanning through a firewall are the same as the ones used in the network scanning section. One will be able to see how ports show open if a rule allows it, and closed or filtered if the rule denies or discards traffic. The same scan commands generate enough pings and port traffic to easily trigger intrusion detection alerts in the firewall. By utilizing firewalls within your networks, NIST FICIC functions for PROTECT and DETECT are accounted for; see Fig. 9.

## 9 Separated Networks

Typically, there are two functions for the OT network; to carry SCADA and provide remote access to devices. When the baseline was documented, it should have been noted as to how many and of what function each discovered network served. SCADA traffic should be kept separate from the remote access as much

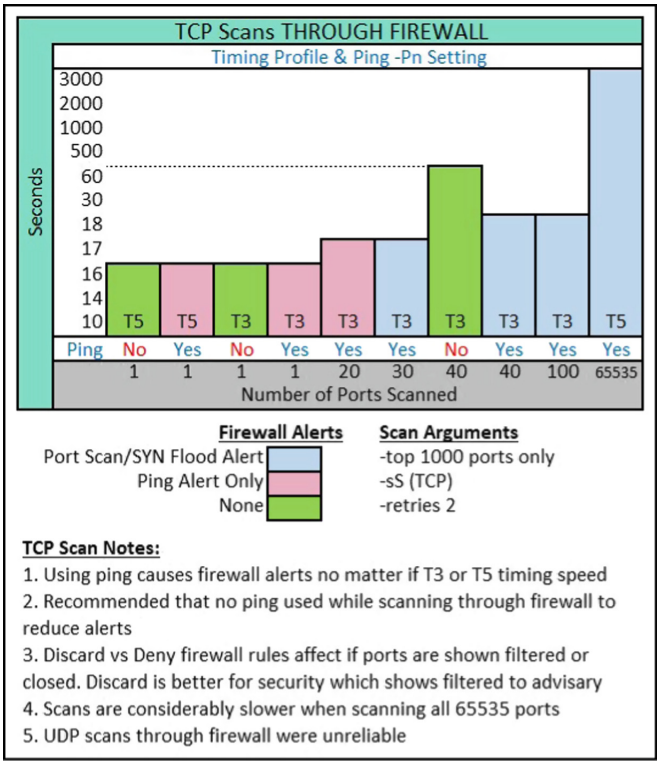



**Fig. 7.** TCP scans through firewall.

as possible. Large integrated or "flat" networks can easily fall victim to denial of service attacks [15]. Additionally, NIST FICIC and [17] recommends segmenting networks by, where possible, especially separating connected wireless and Internet from the SCADA/ICS devices and remote access networks. If raw SCADA traffic is accessible to anyone trying to remotely log into a device, then this issue should be immediately remedied. Not only could this be a security risk, but network congestion alone could potentially cause missed SCADA polls, lost packets or other anomalies. See Fig. 8 for an example of a separated network. The remote maintenance and SCADA networks are shown as Ethernet with some serial to IP converters, however separation can be accomplished a number of ways.

SCADA network traffic typically only flows in one direction from the device to the receiving master RTU or other collection point, therefore directional protections can be utilized. One such measure is utilizing a data diode which, like diodes used in electronic circuits, only allows one way flow. The diode can be purchased for serial or Ethernet networks and could be installed in specific locations as long as the SCADA network is separate from the remote access network. Ultimately they are cheaper than firewalls and do not introduce as much latency in the communications for time sensitive protocols. The diodes will prevent an

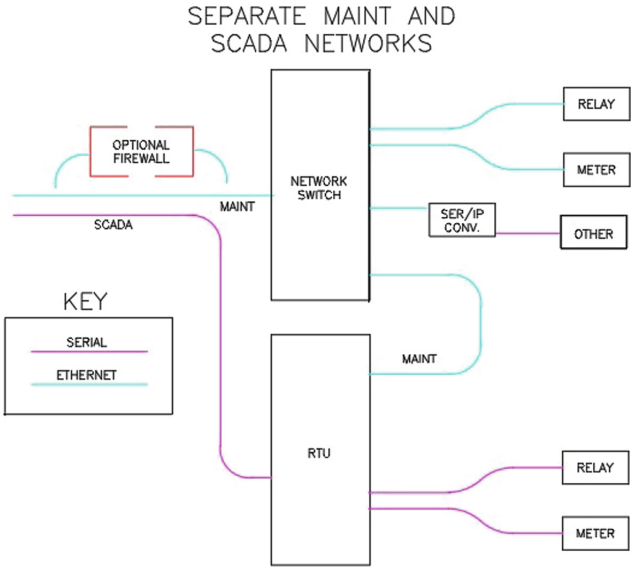



**Fig. 8.** Separated network.

attack back into a remote SCADA location, but may not be as effective for a man-in-the-middle attempt if the entry point is between the data diode and the SCADA collection point. These diodes require either a full serial connection, or serial to Ethernet conversions at certain points. Having a routable protocol break is actually useful as a way to limit an intruder's ability to move across networks or find specific device addresses.

Some devices allow the user to define the Quality of Service (QoS) settings for each network. If you are using a single radio or multiplexer to pass both networks through, they will typically allow someone to set prioritization rules to favor SCADA traffic, while assigning a lower priority to remote access activity. In the scanning and firewall experiments documented in Sects. 5 and 6, only the remote access network was utilized; not the separate SCADA network. If your network is a not separated and allows both SCADA and remote access, then be sure to test the recommended scans in a controlled environment before working on an operational system. Run Nmap scans against network gateways such as the radios and multiplexers to verify they are not allowing unexpected services. These devices can typically be configured remotely so check the equipment documentation to know what services or port number may be used. The last thing one wants is to configure the end devices and set up firewalls, only to leave their network telecommunication equipment exposed to denial of service attacks or malicious configuration changes.

## 10 Additional Recommendations

To maintain security, it is wise to try and continually improve one's security posture; after all, cyber vulnerabilities are constantly evolving as well. Keeping devices up to date with virus definitions or security patches is an easy step with minimal cost. Firmware updates or other types of system security patches are essential to improve or sustain device reliability and security [13]. A regular regimen of patching is a good way to ensure vulnerabilities inside the end devices are mitigated in case a malicious actor is able to penetrate current security layers. OT devices are designed to be used for many years longer that typical IT products. With such a long life, one may find that a manufacturer eventually stops supporting firmware updates. In this case, the lack of support should be noted and that risk must be addressed. Either with a plan to replace the device or a verification of the security layers protecting that device. The older the known vulnerabilities are within a device, the more chance that a malicious exploit is out in the wild.

| | NIST Cybersecurity Framework | | |
|---|---|---|---|
| **Relevant Section** | *FUNCTION/Category* | *Subcategory* | *Recommendation* |
| Baseline documentation | IDENTIFY/Asset Mgmt | ID.AM-1 | Physical device/Syst. Inventory |
| | IDENTIFY/Asset Mgmt | ID.AM-3 | Org comm and data flows mapped |
| | DETECT/Anomalies & Events | DE.AE-1 | Baseline of data flows |
| Ports and Services Discovery | IDENTIFY/Risk Assess | ID.RA-1 | Asset vulner., discov. and docum. |
| | DETECT/Continuous Monitor | DE.CM-8 | Vulnerability scans |
| | PROTECT/Protective Tech. | PR.PT-3 | Essential only capability |
| | PROTECT/Info Protection | PR.IP-1 | Baseline system config. |
| Installing Firewalls | PROTECT/Access Control | PR.AC-3 | Remote access mgmt |
| | PROTECT/Maintenance | PR.MA-2 | Remote maint access controls |
| | PROTECT/Protective Tech. | PR.PT-4 | Comm networks protected |
| | DETECT/Continuous Monitor | DE.CM-1 | Monitor for cyber events |
| | DETECT/Continuous Monitor | DE.CM-4 | Malicious code detection |
| Seperated Networks | PROTECT/Access Control | PR.AC-5 | Network segmentation |

**Fig. 9.** Mapping research findings to NIST framework.

Another layer of security would be to add in network monitoring software. Idaho National Laboratory conducted a survey of open source and licensed tools that could be extended upon to meet security needs [10]. Finally, another technology that could be utilized that meets security and redundancy needs is Software Defined Networking (SDN). This utilizes a network controller which efficiently determines data flow within the network. SDN is a hybrid of a firewall and network flow manager, where it will make decisions based on user-defined rules and application requirements giving greater control for network administrators [8]. SDN is much more costly than simply adding some firewalls or segregating SCADA and remote access networks, however this would be a technology to consider when performing a holistic network update. Ransomware, denial of service attacks or unauthorized remote access are some cybersecurity challenges

that never end well, nor can be prevented with a single solution. A good baseline and system understanding is a great foundation on which to build multi-layer defenses. Showing company leadership they are meeting several functions with the NIST Framework for Improving Critical Infrastructure Cybersecurity is a great way to get buy-in and for future improvements.

## 11 Conclusion

There is so much recommended reading on cybersecurity out there and it can become overwhelming for anyone looking for a good place to start securing their own OT networks. The motivation behind this paper is providing insight on low cost steps to improve security posture while following NIST's industry best practices. Just like the armed forces will leave no man behind in battle; we too should leave no network behind in the cybersecurity fight. Build a strong foundation by knowing what devices make up the network and documenting that baseline. Scan all devices for that critical map of ports, ensuring any unneeded services are shut down to prevent exploits. We tested Nmap so others do not have to dedicate time doing so, and we found some effective Nmap commands to allow productive scans on OT networks. Keep in mind however, that we only ran Nmap on a remote access network that was not carrying SCADA traffic. This may differ from some environments, so controlled testing is highly suggested. We recommend adding firewalls because they greatly enhance security capabilities. The suggested rule recommendations can help mask the network configuration, and the firewall will also provide some historical logs for troubleshooting and investigations. Remember that network segregation not only allows more flexibility with protections, but it also prevents a single point of failure. If networks are not separated, then be sure to set a goal to work on this in the short term. Finally, maintaining all of one's initial work with the continuous upkeep of security patches or other improvements will bolster their vulnerability mitigation strategy, keeping them on pace with cybersecurity.

**Acknowledgment.** The authors would like to acknowledge the support from Dr. William Souza, Professor at the University of North Dakota (UND) for his guidance and feedback in improving and revising the manuscript.

## References

1. Alsumayt, A., Haggerty, J.: Using trust based method to detect DoS attack in MANETs. The Convergence of Networking, Broadcasting, and Telecommunications, UK, PGNet (2014)
2. Anderson, D., Kipp, N.: Implementing firewalls for modern substation cybersecurity. In: Proceedings of the 12th Annual Western Power Delivery Automation Conference, Spokane, WA (2010)
3. Ceron, J., Chromik, J., Cardoso de Santanna, J., Pras, A.: Online discoverability and vulnerabilities of ICS/SCADA devices in the Netherlands. University of Twente, Netherlands (2019). In opdracht van het Wetenschappelijk Onderzoek en Documentatiecentrum (WODC)

4. Chalamasetty, G.K., Mandal, P., Tseng, T.L.: Secure SCADA communication network for detecting and preventing cyber-attacks on power systems. In: 2016 Clemson University Power Systems Conference (PSC), pp. 1–7. IEEE (2016)
5. Coffey, K., Smith, R., Maglaras, L., Janicke, H.: Vulnerability analysis of network scanning on SCADA systems. Secur. Commun. Netw. (2018)
6. Duggan, D., Berg, M., Dillinger, J., Stamp, J.: Penetration testing of industrial control systems. Sandia National Laboratories (2005)
7. Graham, J., Hieb, J., Naber, J.: Improving cybersecurity for industrial control systems. In: 2016 IEEE 25th International Symposium on Industrial Electronics (ISIE), pp. 618–623. IEEE (2016)
8. Gray, C.: How SDN can improve cybersecurity in OT networks. In: 22nd Conference of the Electric Power Supply Industry, September 2018
9. Department of Homeland Security, C.f.P.o.N.I.: Configuring and managing remote access for industrial control systems, November 2010
10. Hurd, C.M., McCarty, M.V.: A survey of security tools for the industrial control system environment. Technical report, Idaho National Lab. (INL), Idaho Falls, ID, USA (2017)
11. for Internet Security, C.: Cybersecurity spotlight - defense in depth (DiD), January 2021
12. Kalbfleisch, D.J.: SCADA technologies and vulnerabilities, May 2013
13. Kavanagh, K., Bussa, T., Sadowski, G.: Magic quadrant for security information and event management. Technical report, Gartner (2020)
14. Keene, M.: The risks of an it versus OT paradigm. SANS ICS, July 2019
15. Manson, S., Anderson, D.: Practical cybersecurity for protection and control system communications networks. In: 2017 Petroleum and Chemical Industry Technical Conference (PCIC), pp. 195–204. IEEE (2017)
16. Mustard, S.: Security of distributed control systems: the concern increases. Comput. Control Eng. J. **16**(6), 19–25 (2006)
17. Newton, P.: SCADA/ICS dangers & cybersecurity strategies, April 2020. https://www.darkreading.com/endpoint/scada-ics-dangers-and-cybersecurity-strategies/a/d-id/1332278
18. Nmap.org: Nmap reference guide — Nmap network scanning, April 2018
19. Peterson, D.: Quickdraw: generating security log events for legacy SCADA and control system devices. In: 2009 Cybersecurity Applications & Technology Conference for Homeland Security, pp. 227–229. IEEE (2009)
20. Samdarshi, R., Sinha, N., Tripathi, P.: A triple layer intrusion detection system for SCADA security of electric utility. In: 2015 Annual IEEE India Conference (INDICON), pp. 1–5. IEEE (2015)
21. Scarfone, K., Souppaya, M., Cody, A., Orebaugh, A.: Technical Guide to Information Security Testing and Assessment, vol. 800, no. 115, pp. 2–25. NIST Special Publication (2008)
22. Shodhan: Shodhan ICS radar (2020)
23. Slay, J., Miller, M.: A security architecture for SCADA networks. In: ACIS 2006 Proceedings, p. 12 (2006)
24. of Standards, N.I., (NIST), T.: Framework for improving critical infrastructure cybersecurity, ver 1.1. NIST Cybersecurity Framework (2018)
25. Stouffer, K., Falco, J., Scarfone, K.: Guide to Industrial Control Systems (ICS) Security, vol. 800, no. 82. NIST Special Publication (2011)
26. Tian, Z., Wu, W., Li, S., Li, X., Sun, Y., Chen, Z.: A security model of SCADA system based on attack tree. In: 2019 IEEE 3rd Conference on Energy Internet and Energy System Integration (EI2), pp. 2653–2658. IEEE (2019)