Vulnerability Management

WHAT YOU WILL LEARN IN THIS CHAPTER:

- Managing vulnerabilities
- OpenVAS
- Continuous assessment
- Remediation
- Nexpose Community

I have years of vulnerability management experience. At first, it was theoretical when I was teaching at Louisiana State University. It became a more hands-on role when I worked as an IT director for a small private school and then again when I worked for the U.S. Department of Defense (DoD) as a contractor. If you are planning to take any security certification exams—whether it's ISACA, ISC2, or CompTIA—you need to be aware that the management of the vulnerability lifecycle and risk is a key component on those exams.

Some ships are titanic, and some boats are small. Some boats, like a kayak, could represent your home network, while a Fortune 50 company would be more like the *Queen Elizabeth II*. The goal of both vessels is the same: Don't sink. If you have been tasked with vulnerability management, your task is the same: Don't sink.

Managing Vulnerabilities

As I mentioned earlier, you must know your environment better than an attacker and use that attacker's mind-set in key controls to develop your security program. Now that you have all the opensource tools to troubleshoot your network and you know what assets you have to protect, you have to be able to assess those assets for vulnerabilities. It is a cyclic endeavor, as shown in Figure 4.1.

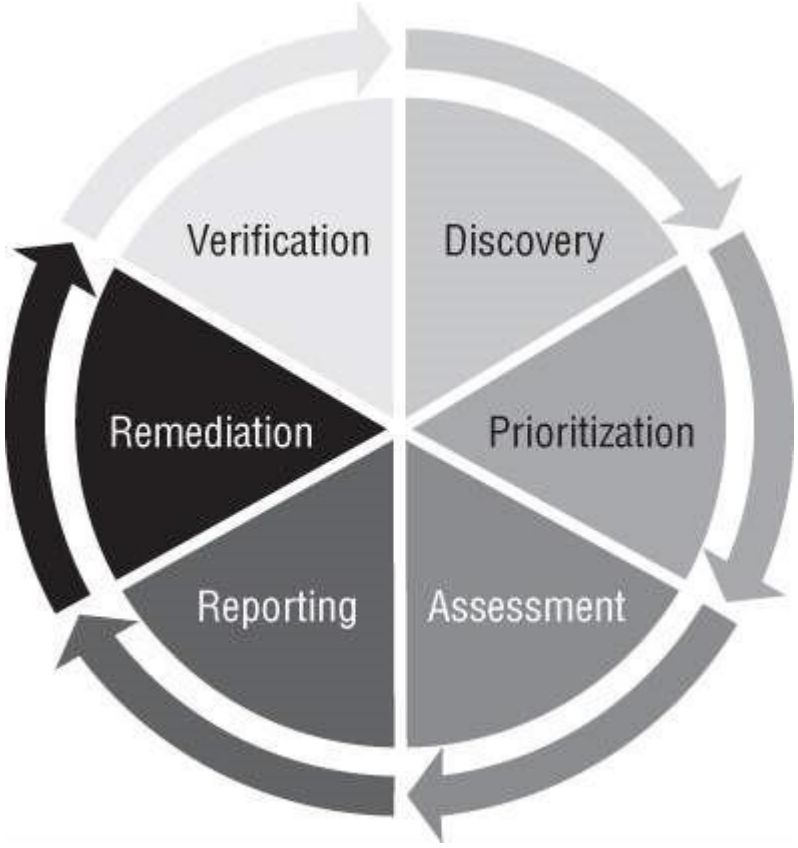


Figure 4.1: The vulnerability management lifecycle

In the discovery phase, you have to figure out what is on your network communicating to other devices. You cannot protect what you don't know you have. Once you're able to map out the assets, hosts, nodes, and intermediary devices on your network, then you're able to move to the next step.

Not all devices are created equal. A domain is a group of computers and other devices on a network that are accessed and administered with a common set of rules. A Windows domain controller (DC) is a Microsoft server that responds to login authentication requests within a network. In an enterprise environment, if a DC fails, your help desk will explode with calls because of the inability for users to log in to the domain. However, if you have a marketing department with a small file server that it backs up to once a month, if this machine fails, then it might warrant a phone call or two. After you know what machines exist on your network, you must prioritize which assets are mission critical.

Once you have identified which assets have a heartbeat and you know which assets would cause chaos through failure or compromise, the next step is to determine the assets'

vulnerabilities. This is usually accomplished by analyzing the operating system, ports that are open, services running on those ports, and applications you have installed on those assets.

Now you're ready to build a report. Some reports will bubble up to upper management and require information such as trending analysis and vulnerability remediation plans. The decisions that upper management will make based on these reports could be budgetary or based on head count. The more technical reports will usually trickle down to the asset owner and contain what needs to be fixed on that device.

With the report in hand, you now have a list of vulnerabilities in your environment and on what device they reside. Some software with advanced capabilities will generate instructions on how to remediate those vulnerabilities. Most of these technical reports will give you a severity rating typically based on the Common Vulnerability Scoring
System (CVSS), as listed in Table 4.1. The National Institute of Standards and Technology (NIST) maintains the National Vulnerability Database (NVD). In this database, you can see a quantitative analysis of every vulnerability based on access vector, complexity, and authentication as well as the impact to confidentiality, integrity, and availability. Basically, this means every vulnerability will have a score of 0 to 10, with 0 being good and 10 being horrendously awful.

Table 4.1: CVSS v3.0 Ratings

Source: National Institute of Standards and Technology

SEVERITY	BASE SCORE RANGE
None	0
Low	0.1–3.9
Medium	4.0–6.9
High	7.0–8.9
Critical	9.0–10.0

In the vulnerability management lifecycle, building your remediation attack plan is a critical step. After completing the asset classification and vulnerability assessment, you correlate the findings to compile your plan of action. There are some

organizations I have worked with that have the goal of becoming 100 percent free of vulnerabilities, and that just isn't a realistic goal to have in our modern digital infrastructure. If you have devices connected and communicating to the world, there is a way into your network and a way out. On mission-critical devices, prioritize the repair of critical and highseverity vulnerabilities. Save the less critical devices to be remediated later.

There is nothing more frustrating than taking apart a PC, fixing what you think is the problem, putting that PC completely back together, and then realizing you didn't fix it and having to start over. Verification is vital to this process. If you do not rescan assets looking for the same vulnerability and you assume that your fix worked but it didn't, you will have a false sense of confidence in that item and leave yourself open to attack.

It has been my experience that the IT industry is one of the most dynamic, with constant change and evolution. There will be times in an enterprise environment that risky behavior will happen when change management processes and procedures are not followed. Our networks are constantly changing and evolving. The networking infrastructure staff throws a new server with no patches on the domain because the people who requested it have the authority to bypass security controls. There are people in the DoD with enough brass on their shoulders to ask for something like this without understanding the repercussions. Those assets still need to be scanned, and if they're not scanned before being added to your network, you get to scan them after.

Some organizations I have worked with have compliance needs that require they scan monthly. Some organizations have a robust security policy where they require assets to be scanned at least once a week. Either way, you vulnerability scanning is not just a one-time action. It is something that needs to be maintained to ensure your network/infrastructure is secure.

OpenVAS

The Open Vulnerability Assessment System (OpenVAS) is an opensource framework of several tools and services that offers powerful vulnerability scanning and management systems. It was

designed to search for networked devices, accessible ports, and services and then test for vulnerabilities. It is a competitor to the well-known Nexpose or Nessus vulnerability scanning tool. Analyzing the results from tools like these is an excellent first step for an IT security team working to create a robust, fully developed picture of their network. These tools can also be used as part of a more mature IT platform that regularly assesses a corporate network for vulnerabilities and alerts IT professionals when a major change or new vulnerability has been introduced.

At the center of this modular service-oriented product is the OpenVAS scanner, sometimes called an *engine*. The scanner uses the Network Vulnerability Tests (NVT) maintained by Greenbone Networks based in Germany. Greenbone Networks was founded by experts for network security and free software in 2008 and provides an open-source solution for analyzing and managing vulnerabilities, assessing risk, and recommending an action plan. According to the OpenVAS website, there are more than 50,000 NVTs, and this number is growing weekly.

The OpenVAS Manager is the actual manager of the processes, controlling the scanner using OpenVAS Transfer Protocol (OTP) and OpenVAS Management Protocols (OMP). The Manager component schedules scans and manages the generation of reports. The Manager runs on a SQL database where all the scan results are stored. The Greenbone Security Manager (GSM) web application interface is the easiest alternative to the command-line client to control the scanner, schedule scans, and view reports. Once you have OpenVAS installed, you will log in through the Greenbone Security Assistant, as shown in Figure 4.2.

Figure 4.2: The Greenbone Security Assistant login for OpenVAS

An ISO file is a replication of an entire CD or DVD that you use to install operating systems or software. Sometimes called an *ISO image*, you will need this file to deploy the OpenVAS image. Once you have the OpenVAS `.iso` file from the website, you can install on bare metal or in a virtual environment. If you want to install this on a
Linux system, I suggest 16.04. You will need a newly deployed Ubuntu server, a nonroot user with `sudo` privileges, and a static IP address. You also need to know how to use the following commands:

```
sudo apt-get update -y

sudo apt-get upgrade -y

sudo reboot
```

The `sudo` command is used on Linux systems and means “superuser do.” If you are more familiar with the Windows environment, `sudo` is similar to right-clicking a program and choosing Run As Administrator. When you add the `-y` option, it will bypass any yes/no prompt with an affirmative answer.

The `apt-get update` command will update the list of available packages and versions. The `apt-get upgrade` command will install the newer versions.

A little like plug-and-play in the old days, you need to install the

required dependencies using the following commands:

```
sudo apt-get install python-software-properties

sudo apt-get install sqlite3
```

OpenVAS is not a default in the Ubuntu repository, so to use the personal package archive (PPA), you must add it, update it, and install it using the following commands:

```
sudo add-apt-repository ppa: mrazavi/openvas

sudo apt-get update

sudo apt-get install openvas
```

By default, OpenVAS runs on port 443, so you need to allow this through your firewalls to enable the update of the vulnerability database. The NVT database contains more than 50,000 NVTs, and this is always growing. For online synchronization, use the following command:

```
sudo openvas-nvt-sync
```

If you skip this step, you will most likely have critical errors later. If you prefer, you can wait until you launch the program and go to the Administration feature inside the software to update the vulnerability database feed. Either way, it must be done.

Once the database is synced, use your browser (preferably Mozilla Firefox) to log into `https://your static IP address` with the default credentials *admin*/*admin*. You should then see the OpenVAS Security Assistant welcome page displayed on your screen, as shown in Figure 4.3.

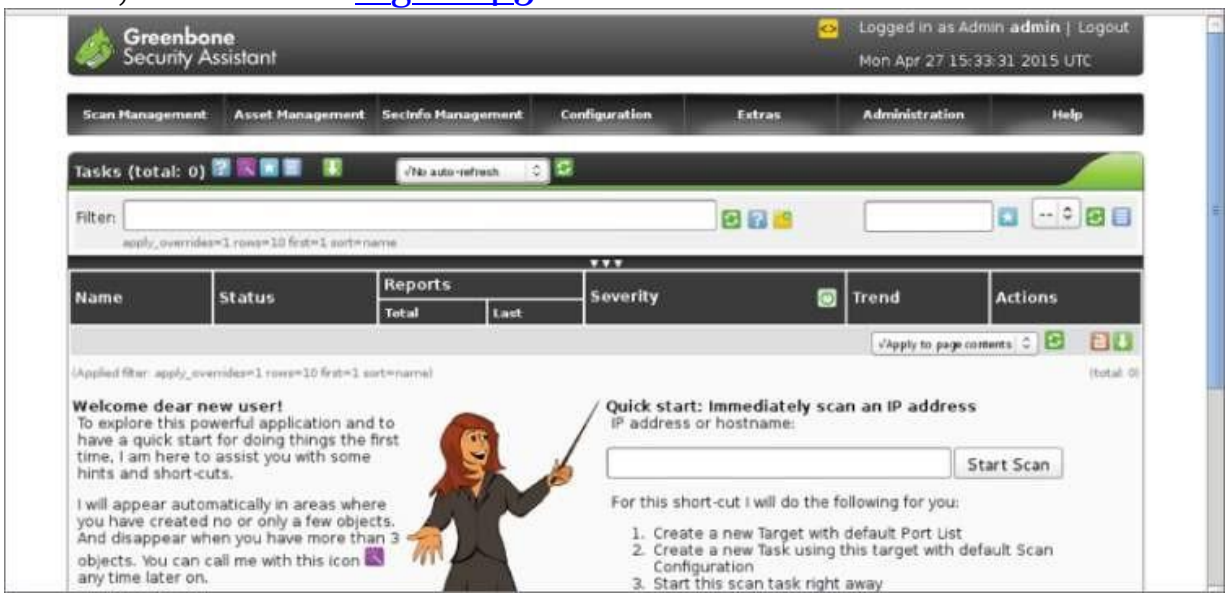


Figure 4.3: Greenbone Security Assistant welcome screen for OpenVAS

The blue star icon is one of the most important buttons on the home page. It will allow you to add a new object such as the configuration of a scan or host list. If you are looking to scan just one IP address, you can use the super-quick Scan Now button on the home page. To get familiar with the software, start with one such as in Figure 4.4 and then branch out to many.

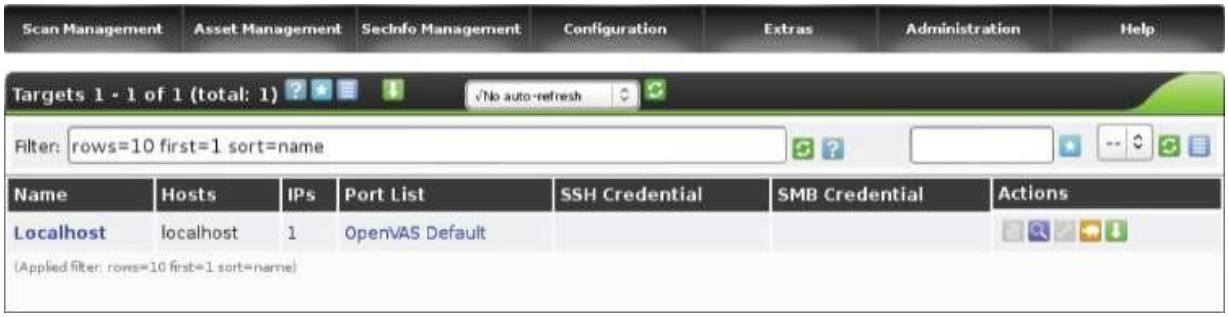


Figure 4.4: The default Localhost setup for launching a scan

As you may have noticed, there are multiple star icons. If you use the star icon on the right side of the program, you will create a new filter. To add a list of subnets, use the star icon in the top header of

the Targets page. The process from start to finish will look like what's shown in Figure 4.5.

Figure 4.5: Workflow for a scan of assets for vulnerabilities

1. To configure a list of hosts after you're done with the one, navigate to the Configuration tab. Look for Targets in the header portion of the page. This is where you can add a new list of subnets of IP address ranges. Please be aware that, depending on the size of your subnets of IP address ranges, CIDR notation can occasionally error out. You may just need to itemize the list of individual IP addresses. Your local host will be listed on the home page by default.
2. Name the scan appropriately. I usually try to name the scan in a way that allows me to refer to the name and know what I scanned rather than some type of numerical name where I have to actually open the scan to know what I was thinking at the time. The scanning configuration can be left at the default of Full And Fast Ultimate. Select your targets and click Create Task. The new task will show up with a green bar next to the status of New.
3. When you're ready, click the green arrow under Actions to run this new task and start your scan.
4. This is the part I love—watching in the task details page. To watch the scan live, set the No AutoRefresh option to Refresh Every 30 Sec. It's better than television. Depending on how many targets you listed, the scan should be done within a few minutes.

Reporting is vital to your vulnerability management lifecycle. After the scan has completed, check the summary of scan results. They will be classified into High, Medium, and Low and will also contain logs. Each issue that has been discovered will be detailed into vulnerabilities, impact, affected software, and (my favorite if it's available) how to fix what is broken. You can download and export this file as a `.pdf`, `.txt`, `.xml`, or `.html` file.

Figure 4.6 is an example of filtered results to include in a report. You have the IP address of the host, what operating system is on the host, and the security issues and threat level below.

Figure 4.6: Summary results of an asset

Nexpose Community

A lot of organizations offer free or community editions of their software. These editions are usually a lighter version of the paid copy with limited features. Once such community vulnerability management software is Nexpose by Rapid7. There are several versions of Nexpose but the community version is an excellent place to start learning because it's free. If you search in a browser for "Nexpose Community," one of the first options should be the community software directly from Rapid7. You could download from other third parties but I find it safer to download and verify software directly from the vendor whenever possible.

After you complete the form to receive your community license, you will end up on a page to download either the Windows or Linux version with its MD5 sum hash. The hash will verify that your download is not corrupt. Once the download is finished, run the installer. You will notice the community version of Nexpose will

only work on 64-bit architecture. To scan an enterprise for vulnerabilities takes a lot of resources including CPU and RAM. Historically, 32-bit architecture can only recognize 4GB of RAM. Nexpose Community cannot do a proper scan with only 4GB of RAM.

LAB 4.1: INSTALLING NEXPOSE COMMUNITY

1. Download and open the executable file. Click Next as you see in Figure 4.7.

Figure 4.7: Installing Nexpose Community GUI

2. You will choose Security Console with local Scan Engine. You will see the option for Scan Engine only which gives you the ability to deploy scanning engines close to the assets to do the scanning work and then bubble that information up to the scan console without compromising bandwidth. Nexpose runs on a PostgreSQL 9.4.1 database which comes included in the console. Because of the size of most environments, the recommended storage for the database is 80GB. The console will naturally bind to port 3780, which is important when we access the software through the browser through https://youripaddress:3780. The PostgreSQL database will communicate over 5432 unless you change it at this stage of installation.
3. You will add user details including First Name, Last Name, and Company. This is done to create the SSL certificate should you ever need to request help or send data to tech support.
4. Create secure credentials and remember them. You will not be able to easily recovery them. Please do not use admin/admin in these fields. Make them as robust as possible.
5. Click Next twice to review the settings and begin extracting files to complete the installation. In Figure 4.8 you see the hyperlink that you will be using to access the program. Install will require a reboot, be sure to save anything you have open and grab a bite to eat. Nexpose loads over 130,000 vulnerability definitions at startup and can take up to 30 minutes.

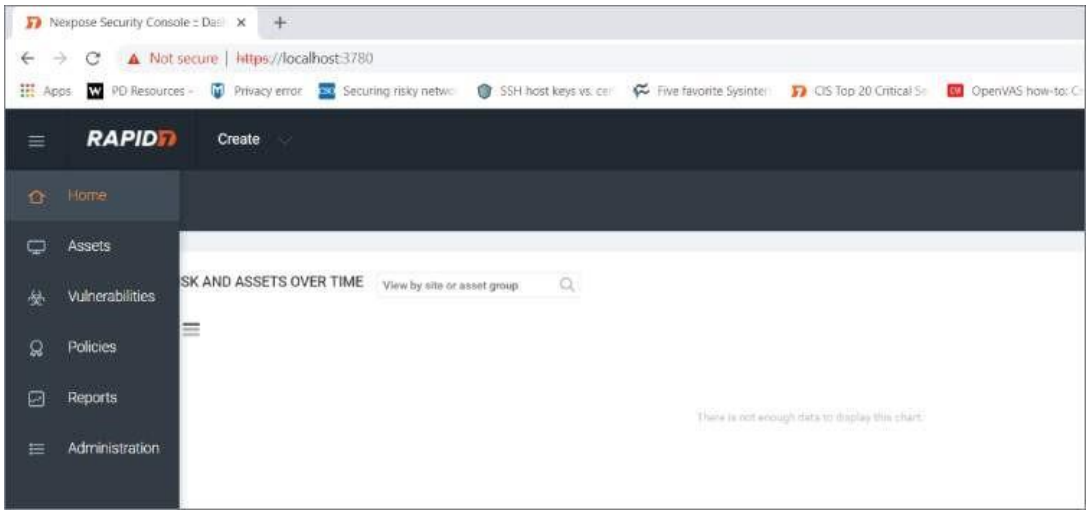


Figure 4.8: Nexpose Community Menu

6. When you come back after rebooting, you will see the orange Rapid7 logo on your desktop. You will need the license that was sent to the email you provided when you registered before you downloaded the software to complete the install process. Use the license that was sent to you to activate the product.
7. On the left side, you will have a vertical menu shown in Figure 4.8.

The home menu gives you a summary of assets, risk scores, and asset groups. The asset page will break down individual items you have scanned and the vulnerability page will give you information on those assets from a different vantage point, where and what makes you vulnerable. The policy tab will be empty since this is the community version but in a paid-for version, you can scan an asset to CIS or a federal guideline of configuration. Reports will be below policies.

LAB 4.2: CREATE A SITE AND SCAN

1. Click on the Create button at the very top of the page. Slide down to Site. You have seven sections to consider for optimal scanning and performance.
2. The General Tab is where you can name the site for future reference and reporting. Add the name TEST.
3. The Assets Tab will allow you to enter a single name, address, or CIDR range of IP addresses you would like to scan. In the community version, it may be wise to do an nmap scan first to build an inventory and then bring in those assets individually since you're limited to 32 assets. For this TEST site, add your IP address. If you are unsure of your IP address, open up a command prompt and do an ipconfig /all.
4. The Authentication tab gives you the ability to be authorized to scan those assets listed on the Assets tab. If you would like a deeper scan, use administrator credentials on this page. Skip this the first time and you will have the ability to create a baseline comparison report in the future.
5. There are several scan templates on the next tab to choose from. The default scan template is a full audit without web spidering. This is an ideal template to use first.
6. You only have one engine available to you in the community version. This is the local scan engine you installed in Lab 4.1.
7. Alerts are configured to notify an administrator that a scan has failed.
8. The schedule tab will allow you to stay on top of your assets vulnerabilities as Nexpose is updated and new assets are added to your environment.
9. Click Save And Scan in the upper right. This test scan on a single asset will start and you can watch the progress.
10. When the scan completes, review the vulnerabilities on your host. On the asset page, they will look like Figure 4.9.

VULNERABILITIES

Vulnerability	Severity	Instances
X.509 Certificate Subject CN Does Not Match the Entity Name	Severe	1
SMBv2 signing not required	Severe	1
Untrusted TLS/SSL server X.509 certificate	Severe	1
TLS/SSL Server is enabling the BEAST attack	Severe	1
TLS Server Supports TLS version 1.0	Severe	1
Self-signed TLS/SSL certificate	Severe	1
TLS Server Supports TLS version 1.1	Moderate	1
TLS/SSL Server Supports The Use of Static Key Ciphers	Moderate	1
TLS/SSL Server Does Not Support Any Strong Cipher Algorithms	Moderate	1

Figure 4.9: List of Vulnerabilities found in Nexpose Community sorted by severity

LAB 4.3: REPORTING

1. Click on the reports menu on the left.
2. Using the carousel under the reports, navigate to the circle that displays the last four default document reports as you see in Figure 4.10.

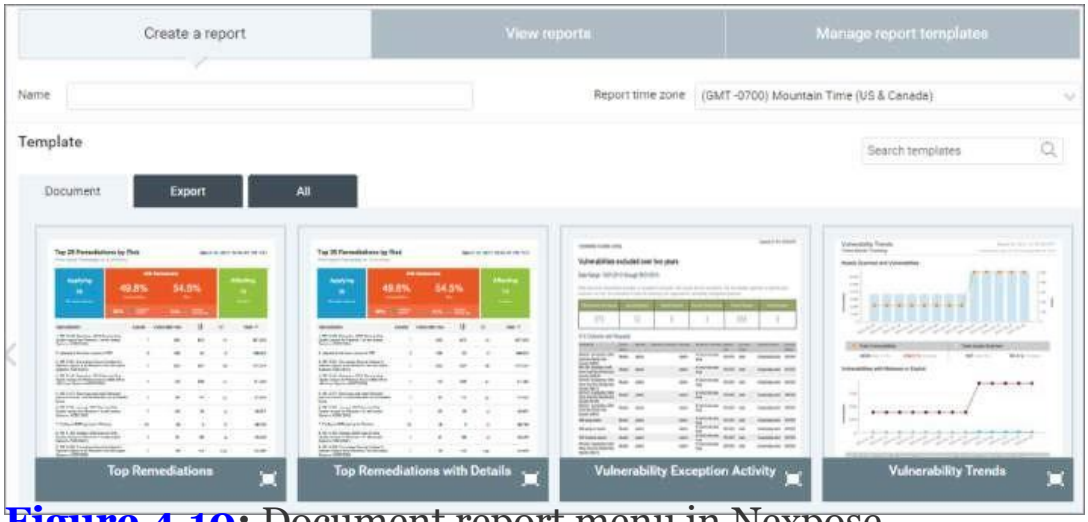
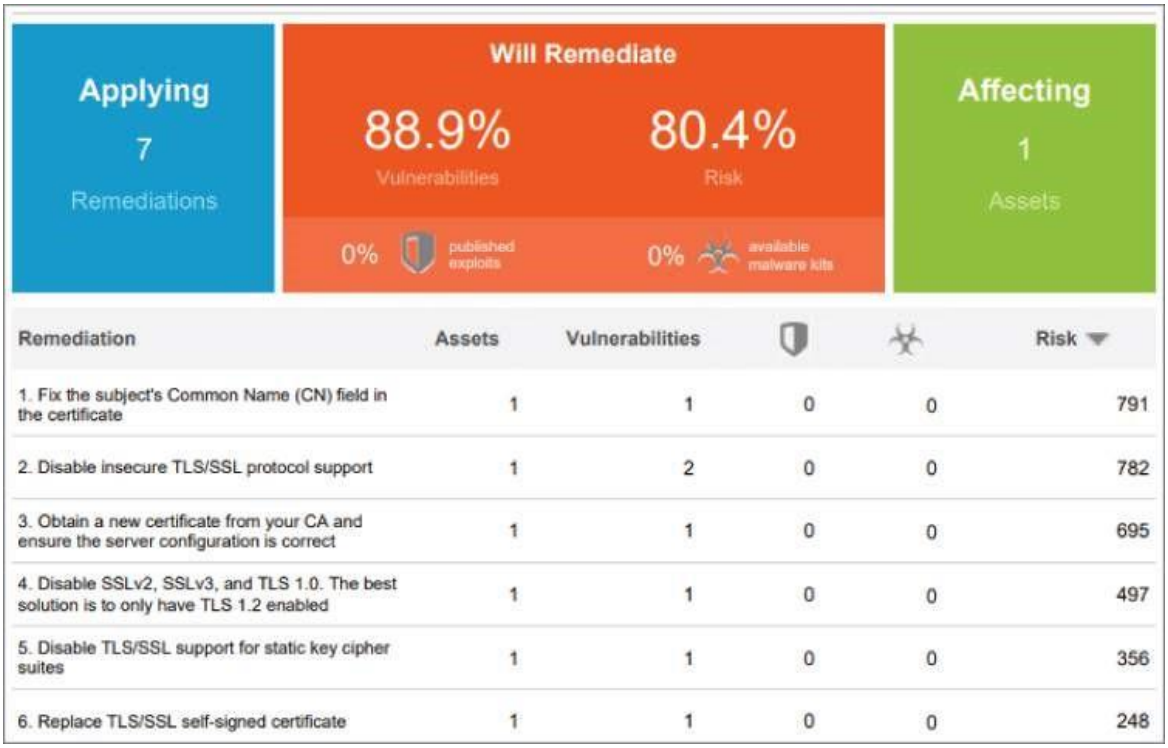


Figure 4.10: Document report menu in Nexpose Community

3. At the top of the page, name this report “Best VM Report EVER.”
4. You will see the Top Remediations with Details. Single-click on the report to select.
5. Leave the file format as PDF.
6. Under Scope, choose the big plus in the center and select your test site made in Lab 4.2.
7. Choose Save And Run The Report. The report will generate and when done, you will be able to click on the report name to open.
8. Scroll down through the preview of the report to see the impact of remediated vulnerabilities, the list of vulnerabilities, and the host the vulnerability is on, as

displayed in Figure 4.11. Navigate to page two to view the instructions on how to fix the vulnerabilities listed above.



Remediation	Assets	Vulnerabilities			Risk
1. Fix the subject's Common Name (CN) field in the certificate	1	1	0	0	791
2. Disable insecure TLS/SSL protocol support	1	2	0	0	782
3. Obtain a new certificate from your CA and ensure the server configuration is correct	1	1	0	0	695
4. Disable SSLv2, SSLv3, and TLS 1.0. The best solution is to only have TLS 1.2 enabled	1	1	0	0	497
5. Disable TLS/SSL support for static key cipher suites	1	1	0	0	356
6. Replace TLS/SSL self-signed certificate	1	1	0	0	248

Figure 4.11: Top Remediations

You now have a picture of how an attacker might see you and your network. This is exactly the methodology attackers would use to find the landscape of your environment and attempt to exploit what they find. If you can thwart their efforts by closing up the vulnerabilities that are exposed to the world, you will have a much safer ecosystem.