Vulnerability Scanning

Greg Williams

CS 591

Fall 2010

The main objective of the IT security program here at UCCS is to maintain the integrity of all university systems. There are many awareness programs, policies, and procedures all geared to ensure the integrity of university systems. One such procedure is called the Minimum Security Standard. The Minimum Security Standard procedure outlines what should be in place on a university owned information system to ensure confidentiality, integrity and availability of systems. The minimum security standards procedure details items such as including vulnerability scanning. Vulnerability scanning is important in several different ways. Vulnerability scanning not only can identify security flaws in your network, but depending on the tools you use, it can also show you how to patch those vulnerabilities. This paper will focus on why we scan for vulnerabilities, vulnerability scanning software, and what is done after a vulnerability scan is performed.

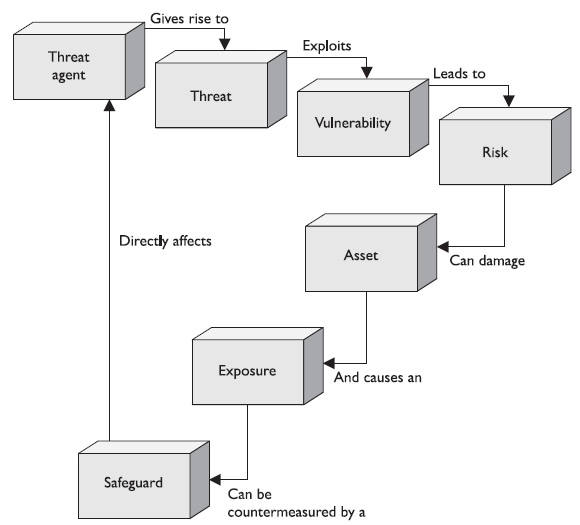
In order to better understand why we scan for vulnerabilities we first need to define vulnerabilities, threats, risk, exposure, and countermeasures. A vulnerability is any weakness in hardware, software, procedure, human processes that can be exploited. A threat is any potential danger to a system. Threats can be a person, an unsecure system sitting on a server vlan, a virus, etc.; anything that can identify and possibly exploit a vulnerability. Risk is the likelihood of a threat exploiting a vulnerability to a system and is assessed as business impact. Exposure is, simply put, being exposed to any type of loss to the organization. A countermeasure is any patch, procedure, system, etc., put in place to mitigate the vulnerability. The graph below represents how all these terms fit in together. 

Figure 1.1

I’ll give you a simple example starting from the top. The threat agent in this example is a server whose TFTP software hasn’t been updated in a while. The server does not have sensitive data on it, but it is essential to critical backups of switches and business continuity. Since the TFTP ports are open, a vulnerability can be identified by the software version the TFTP server responds with. If someone were able to identify this server as a vulnerable server, this person would be a threat. The threat could use a buffer overflow to exploit the system and gain access. This leads to risk. Since this server is critical to backups and business continuity, any breach would have serious business impact; the risk is very high. If a breach occurred on this system it would a serious exposure of data that shouldn’t be exposed. However if we were apply a countermeasure, in this case a software patch, the risk would be mitigated.

In order to maintain the integrity of systems you must run vulnerability scans on your systems. Vulnerability scans are sometimes the only way you know if you have critical flaws or holes in your systems. In the above example, the vulnerability was only found through a vulnerability scan. Vulnerability scanning needs to be performed by authorized individuals on your infrastructure before someone who doesn’t have authorization scans your infrastructure. Unauthorized users scanning your infrastructure not only can find and exploit found vulnerabilities, but they could also cause damage to the network if you have not properly patched previously known vulnerabilities. Authorized individuals need to come up with a detailed scanning plan before they just scan blindly.

There are several important questions that need to be answered when you are coming up with a plan to scan for vulnerabilities. The first question is “What am I going to scan?” Typically the first time you run a scan you have no idea what the scan will do to the system that the scan is being performed on. If you scan your production infrastructure, you want to configure your scans in such a way that it will cause the least amount of load on the servers. You don’t want to end up taking down infrastructure because your scans are set too aggressively. In addition you probably want to limit your scans to only a few systems or subnets at a time; this way if your scans tie up certain servers or infrastructure you still have production systems that can handle load. The next question that you should ask is “How do I want it scanned?” There are various types of settings that can either be very light on the infrastructure or very aggressive. You may want to start out with light scanning with “safe checks” enabled and move toward an aggressive scan later in your scanning schedule. I’ll talk more about this later in the paper. The third question that you should ask is “Do I have enough man power to fix problems with scanning or fix vulnerabilities that I find?” Once you scan your infrastructure it is very important that you fix your vulnerabilities that you find right away or document why you aren’t fixing the vulnerabilities. If a vulnerability you have found were to be exploited after you knew about it, you may be accountable as to why it wasn’t fixed. This could negatively impact your organization and your position. The last important question is “What monitoring do I have in place to watch for problems if they arise during a scan and will these logs affect other components in my infrastructure?” Generally scanning infrastructure causes a lot of “noise”. Log generation is expected to be very heavy even with a light scan. A server could generate thousands of logs because of a scan. You want to monitor your servers and logs to make sure the scan isn’t negatively affecting the infrastructure. You also want to make sure that your scanning server is whitelisted everywhere in your infrastructure. If your servers or IDS has commands to take action on a server based on scanning attempts, you want to make sure that your scanning server is going to be allowed to scan. If your scanning server generates too many logs and slows down or stops a production system, you want to monitor it so you can stop the scan if needed. Even with a light scan systems have been known to become unresponsive due to the way they are configured. Once you have answered these questions you should be ready to start scanning your infrastructure for vulnerabilities.

Scanning your infrastructure for vulnerabilities not only requires careful planning, but it also requires good software to perform the scan. There are several different types of scanning software out there. Choosing the right scanning software is outside the scope of this paper, however I will briefly mention three of the most widely used software programs and then dive into Nessus. First, Nmap. Nmap stands for “Network Mapper”. It is an open source security scanning tool that is mainly used for inventory, managing service upgrade schedules, and monitoring the network. It is an IP based scanner that can detect what OS, firewall, and other characteristics are on a system. The next piece of software is called OpenVAS. OpenVAS is an open source vulnerability scanner. It is a powerful tool that is used to identify over 19,000 vulnerabilities on many different platforms. The final piece of software is called Nessus. Nessus is a vulnerability scanner that not only scans for vulnerabilities, but provides configuration auditing, asset profiling, and sensitive data discovery. Nessus is in use by thousands of organizations including UCCS to scan for possible infrastructure vulnerabilities.

UCCS started using Nessus in October 2010 for scanning server subnets for vulnerabilities. UCCS has developed a scanning procedure using many of Nessus’ features that allow us to scan each subnet or potentially vulnerable system separately. In order to start using Nessus for scanning, it must be configured based upon how you want it to scan. When you first login to the Nessus server you’ll want to click on the “Policies” tab to start configuring a scanning policy. This is what the “Policies” screen looks like.

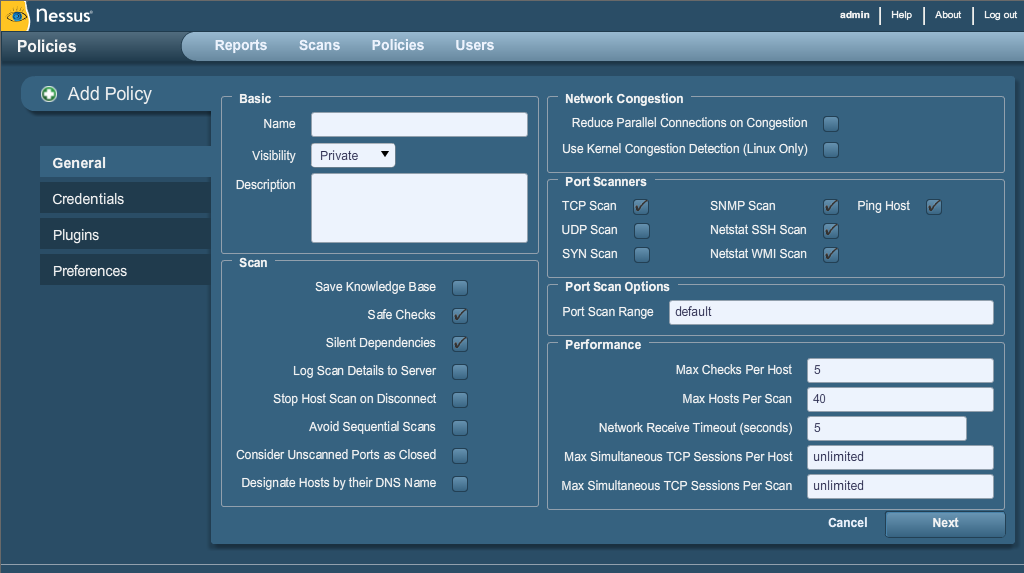


Figure 1.2  
There are several items on this page that need to be configured before we can start scanning. First we need to fill in the Name. Next we need to decide whether or not to enable “Safe Checks”. Enabling “Safe Checks” will disable all plugins that could potentially cause a server to crash when scanning. You want this option enabled the first time you are running a scan since you do not know how your infrastructure will respond to a scan. On the “Port Scanners” section, you can choose to enable a UDP scan as well, but the scans will take longer to complete. The rest of the defaults on this page should be sufficient to start a scan. The next screen that you will need to configure is the “Credentials” screen shown below.

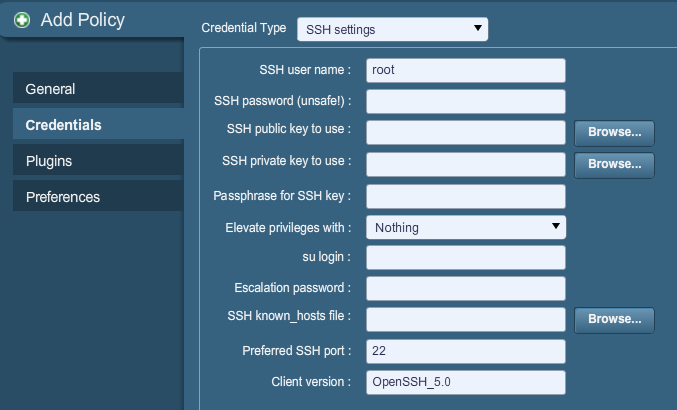
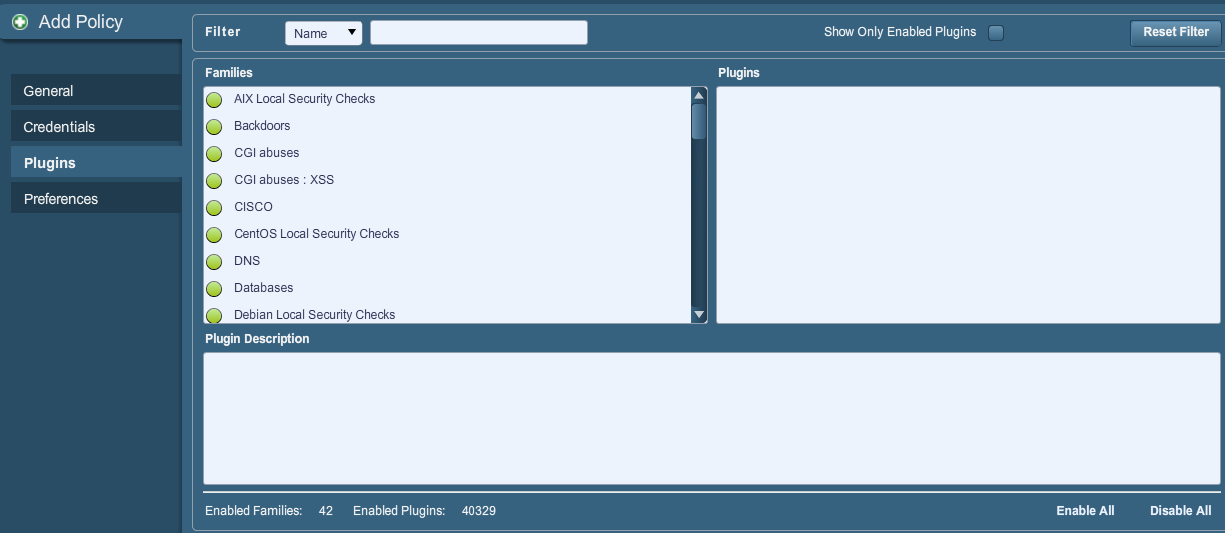
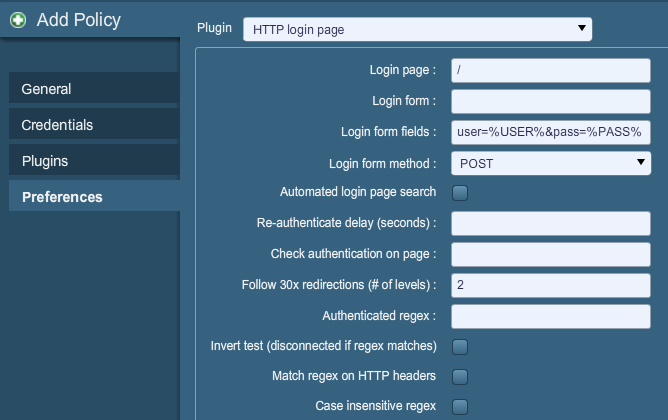


Figure 1.3  
This screen allows you to configure login credentials to a server. By providing login credentials Nessus can log into your server and perform a more complete assessment of your system. This also will cut down on the number of false positive vulnerabilities reported by Nessus since Nessus usually can only scan software banners instead of the actual software patch level without logging into the system. Nessus can use Windows, SSH, Kerberos, and clear text credentials to log into systems. The next screen that you will need to configure is the Plugins screen, shown below.  
  
Figure 1.4  
This screen allows you to enable and disable specific checks or families of checks. Checks are what Nessus scans for when a vulnerability scan is run. There is one particular plugin that is important to note, the “Denial of Service” plugin. This is the check that is turned off when you enable “Safe Checks” on the general “Policies” page. Enabling this check could potentially cause a server to crash. The final configuration screen is the “Preferences” screen, shown below.  
  
Figure 1.5  
The Preferences screen allows you to fine tune your scans to specific services on servers. You can configure database logins, HTTP login pages, industry specific compliance checks, such as PCIDSS and HIPAA, and many more. UCCS uses the “PCI compliance” check to scan systems for any PCIDSS (Payment Card Industry Data Security Standard) violation. We also use web directory scanning. Once all these options have been configured, it is time to schedule a scan.  
 Nessus allows a user to schedule scans based on policy. It is important to note that you should watch your scans as they happen for the first time, since you don’t know how the scans will affect your infrastructure. The “Scans” screen will allow you to type in a single or range of servers based on IP address or DNS entry, or if you have a long list you can upload a file of IP addresses to scan. You will also need to select a scan policy to apply against the scan. Once you hit the submit button your scan will start. After the scan is complete, you can view the results of the scan on the “Reports” tab.

This is the part you have been either been waiting for or dreading; the results of the scan. In the scan report, Nessus will report anything that it found in the scan categorized by IP or DNS entry and will report high, medium, low vulnerabilities and also open ports. You can click on the individual vulnerability to show information on that vulnerability including the synopsis, description, solution, risk factor, CVSS base score, CVSS temporal score, plugin output, CVE number and if a public exploit is available. You can also compare reports to previous reports to see if the amount of vulnerabilities found in a system has increased or decreased. Once you know what vulnerabilities there are in a given system, you need to act on them.

Scanning is now complete and you know the vulnerabilities of a system. Now what? You need to determine what you are going to do with the vulnerabilities. Typically you will patch the vulnerabilities, however you may want to run a risk assessment of your own before you proceed. You may feel the risk in patching a system will decrease productivity in a system and decide to accept the risk. You may also decide that it is a high risk and the vulnerability needs to be counter measured right away. Once you have either patched your systems or come up with a plan to counter measure any vulnerability, you need to rescan to make sure the vulnerability is no longer a vulnerability. If you wish, you can also choose to setup a scanning schedule and baseline metrics. Both of these will help maintain infrastructure integrity when a new server or key piece of infrastructure goes into your network.

Vulnerability scanning is essential to the integrity of any organization’s infrastructure. Knowing why you need to scan, methods used in scanning and what you need to do after a scan are key to a successful scanning program. Knowing why you need to scan is an important part of any security program. Knowing the methods used in vulnerability scanning will help you fine tune your scans and maximize the effectiveness of your scans. Finally being able to patch your systems for any of the vulnerabilities that the scans find will ensure your systems are safe from internal and external threats.

References

Tenable Network Security. (2010, December 2). *Nessus 4.4 User Guide.* Retrieved December 5, 2010 from http://www.nessus.org/documentation/nessus\_4.4\_user\_guide.pdf  
  
Harris, Shon. (2010). *CISSP All-In-One Exam Guide, Fifth Edition.* Columbus, OH: McGraw-Hill Osborne Media