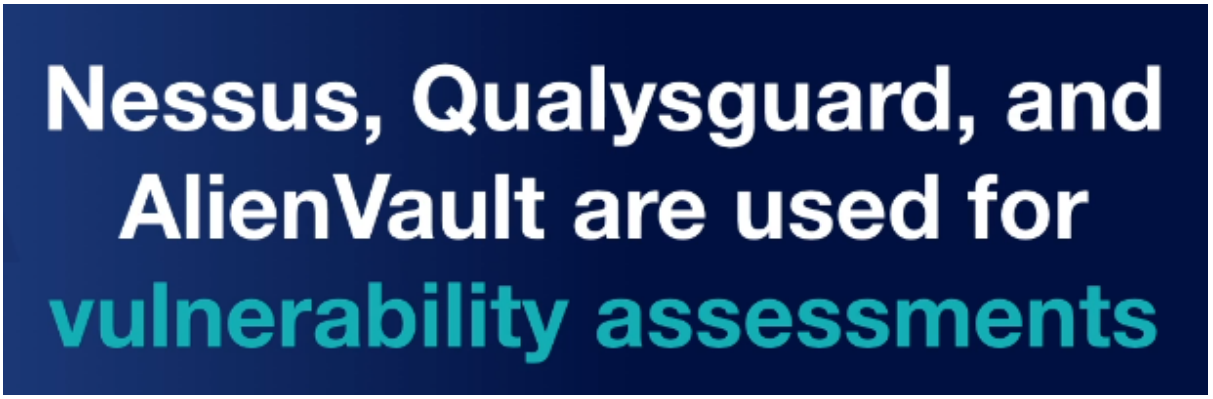
Vulnerability Management

A vulnerability assessment seeks to identify issues in a network, application, database, or other IT systems prior to it being inadvertently or purposely used to compromise a system. Vulnerability assessments are a formalized process that define, identify, and classify the security holes in an enterprise network architecture.

Now, once these countermeasures are put in place, a follow-up vulnerability assessment can help you to determine how effective your countermeasures truly are in protecting that network from attack. The management and oversight of this process is known as vulnerability management. Vulnerability management is the practice of finding and mitigating the vulnerabilities in your computers in your networks. This is a very cyclical process. Sometimes, you'll hear this referred to as scan, patch, scan because you need to scan the network for vulnerabilities to identify them, then you're going to prioritize all these vulnerabilities, you're going to fix them and patch them, and then you're going to scan again, and you're going to keep doing this until hopefully one day, you have no vulnerabilities left.

Common choices:



Penetration Testing

A penetration test is conducted by a team of professionals to simulate an attack on your network, its system, or its applications. Often, this is called a pentest. And the idea here is for the team to break into your network, just like a real hacker would.

Pentest vs Vuln Assessment

But, how does a penetration test differ from a vulnerability assessment? Well, vulnerability assessments are conducted often as a credentialed scan, where the tool can be provided with a username and password for the systems. This is going to provide you with an inside out look of your networks, just like a system administrator would see. Now, instead, a pentest is seeking to look at your networks as an attacker would, from the outside in. Often, your penetration tests are going to be conducted in the form of a black-box test, where the pentesters have to hunt for any information that they need in order to be able to penetrate the network's defenses. But some organizations are going to hire a pentester to perform the assessment as a white-box test, instead. This means they'll give them some kind of information about the network, usually IP addresses, the types of servers being run, maybe the software, and sometimes, even a basic standard user account.

Penetration tests follow five basic steps:

1. First, you get permission and you document information about the target network.
2. Second, you gather information about the target through reconnaissance.
3. Third, you're going to enumerate the target to identify known vulnerabilities.
4. Fourth, you're going to exploit the network to gain user or privilege access.
5. And fifth, you're going to document all of your results of the pentest and give that report to the organization.

Training & Exercises

Tabletop Exercises - TTX

Now, when we talk about tabletop exercises, we mentioned before that these are exercises that use an incident scenario against a framework of controls or a red

team. So, what we're going to do here is we are going to carry a discussion of simulated emergency situations and security events. These are great because they're really simple to set up, but they tend to be more theoretical in nature and they don't provide practical evidence of what could go wrong during a real event. For example, how long will a particular task take to complete? You really can't gather that from a tabletop, but if you actually go through the actions and motions in something like a penetration test, you'll be able to see that instead.

Pentest

Now, when you're dealing with a penetration test, this is a test that uses active tools and security utilities to evaluate security by simulating an attack on a system to verify that a threat really does exist, they actively test that threatened vulnerability, they bypass security controls, and then, finally, exploit those vulnerabilities on a given system.

Red Team

When we talk about red teams, these are the hostile or attacking teams in a penetration test or an incident response exercise. If you hire that third-party team, that is a red team. They're trying to attack your systems.

Blue Team

When we're talking about blue teams, this is our defensive teams in a penetration test or an incident response exercise. This is our system administrators. This is our network defenders. This is our cybersecurity analysts, like you. You're going to be part of the blue team.

White Team

And then we have the white team. This is a staff who administers, evaluates, and supervises a penetration test or incident response exercise. They're also going to be responsible for building the network if you're going to be using a third-party network as part of your test. Sometimes, organizations don't want to do active testing on their real live networks, so, they'll build a training ground and they'll put their red teams and their blue teams, if they have internal red teams and internal blue teams, against each other in this simulated environment. Well, somebody has to build and support this entire ecosystem, and that's what the white team will do. I like to think about the white team as the referees. They're also going to be the ones who are going to

report after the event and say, this is what the red team did well, this is what the blue team did well, and here's what they both did not so well.

OVAL

The Open Vulnerability and Assessment Language, or OVAL as it's known, is a standard that was designed to regulate the transfer of secure public information across networks and the Internet to utilize any security tools and services available at the time. Now, what does this really mean in layman's terms? Well, OVAL is an attempt to create a standard way for vulnerability management software, scanners, and other tools to share their data with each other and with other programs. Now, OVAL is comprised of two different parts. There's a language component to it, and an interpreter. The OVAL Language is written as an XML schema that's used to define and describe the information that's being created by the OVAL Language, and it's allowing it to be shared among various programs and tools. Now, the OVAL Interpreter, on the other hand, is a reference model that was developed to make sure that the information being passed around by all of these programs, it actually complies with the OVAL schemas and definitions that the language created. Because OVAL can be used by lots of different tools, it has become a large part of vulnerability assessments, patch management, auditing, the sharing of threat indicators, and multiple other uses. Now, for the Security+ exam, you just have to remember that OVAL stands for the Open Vulnerability and Assessment Language, and that it's used to share data between lots of different tools that are focused on vulnerability assessments and management. And if you do that, you're going to do just fine.

Tools for Vuln Assessments

Network Mapping

Network mapping tools are used for discovery and documentation of your physical and logical connectivity that exists within your network. By using these tools, you can determine how the network is set up, how the data is going to flow over that network, and all sorts of other things like that. This is usually one of the first tools that's used when you conduct a vulnerability assessment, because you have to understand how all these different network connections are, so you can understand the vulnerabilities that are going to lie within the network. For example, SolarWinds is a very popular commercially available network mapping tool. As you can see here on the screen, it's going to search your network and create a graphical representation of it for you. A

good open source and free option you can use is known as Zenmap. Zenmap is going to allow you to create a graphical topology of your network, as you can see here.

Vulnerability Scanning

A vulnerability scan is a technique that’s going to be used to identify threats that exist on the network, but it doesn't exploit those threats. Now, vulnerability scanners can vary greatly in their complexity and their level of detail. Some are very basic and only do a scan for open ports. Others can probe those open ports and determine the exact service and software that's being run by the server. Now, for example, Nmap is a port scanner that can perform a basic port scan or a more in-depth vulnerability scan of those ports once it finds one that's open. I'm going to show you that in a demonstration later on. There is very complex vulnerability scanning suites out there, things like Nessus and Qualysguard, and these can scan for open ports, enumerate the services on those ports, and then determine if a vulnerability exists on those services by checking if they've been patched for known exploits.

Network Sniffing

Network sniffing is the process of finding and investigating other computers on the network by analyzing the active network traffic, or capturing the packets as they're going across the network for later analysis. Network sniffing tools are also called packet sniffers, or protocol analyzers, because all three of these can conduct the concept of packet capturing on the network, but a protocol analyzer has the ability to give you much more information than just a network sniffer or a packet sniffer does. With a protocol analyser, you can actually capture, reassemble and analyze those packets that have gone across the network, look at them as packets, frames, or even at the bit level. The most commonly used protocol analyzer is the open source program known as Wireshark. Wireshark is free, available on just about every operating system out there, and it is really, really powerful.

Password Analysis

Well, it’s a tool that’s used to test the strength of your passwords to ensure that your password policies are being followed properly. Another name for these is a password cracker. Now, a password cracker uses comparative analysis to break passwords and systematically guess them until the password is finally determined. There's a bunch of different password crackers out there, but by far, the two most well-known are Cain and Abel and John the Ripper. There's password guessing, a dictionary attack, a brute-force attack, and a cryptanalysis attack.

Password Guessing

With password guessing, this occurs when a weak password is simply figured out by a person.

Brute Force Attack

A brute-force attack is where the computer program attempts to try every single combination of a password until it can find the right one. Now, this can take a lot of computing processing power, as well as a lot of time, depending on how long and strong your password is. But eventually, it will always find it.

Dictionary Attack

The next method is called a dictionary attack. In this type of attack, the password cracking program is going to attempt to use a dictionary to automatically guess the password by trying each and every word in that dictionary file. Now, a dictionary attack doesn't just use common dictionary words, though, because hackers have created their own dictionaries that consist of other variations, like commonly-used passwords, variations on real dictionary words using numbers, letters, and special characters, and other such variations.

Cryptanalysis Attack

Now, the final method covered by Security+ is called the cryptanalysis attack. This attack relies on comparing a precomputed, encrypted password to a value found in a lookup table. But if I have a database of all of those values already, I can just compare the encrypted password to the values found in the table, and if I find it, I can then look in the column next to it for its unencrypted value.
These tables of precomputed values are known as a Rainbow Table, and these files can be massively large. One of my favorite rainbow tables is actually found online at CrackStation.net. Their table contains 15 billion entries and is 190 gigabytes in size. That is a really, really big text file.