Why You Need to Run a Vulnerability Assessment

Running a vulnerability assessment is fundamental for any organization. When an administrator is in the process of securing his network, there are a lot of things he needs to bear in mind. Unfortunately, when it comes to network security most stop at patch management and antivirus software. Little do they know that they also need to check configurations, known issues in third-party applications, as well as potentially troublesome hardware that in their default configuration can be harmful to the network's security. These processes are what constitute a vulnerability assessment.

Why is a vulnerability assessment indispensable for the security of your corporate network?

Once you secure your network by fully patching it and deploying antivirus solutions, hackers might still be able to exploit a number of misconfigurations. Below is a list of general issues one might find in a typical operating system installation:

- Unnecessary open shares
- Unused user accounts
- Unnecessary open ports
- Rogue devices connected to your systems
- Dangerous script configurations
- Servers allowing use of dangerous protocols
- Incorrect permissions on important system files
- Running of unnecessary, potentially dangerous services.

Apart from these misconfigurations, when running a vulnerability assessment on your network you might find several security issues with a wide range of software and hardware including:

- Default passwords on certain devices
- Unnecessary services running on some devices
- Running web services that contain known vulnerabilities
- Dangerous applications such as peer-to-peer applications
- Third-party applications that are a vulnerability to known exploits.

Some vulnerability scanners will also look for signs of known malware based on the computer's behavior rather than actually scanning the files for known malware signatures. In some cases, this approach can help uncover issues that an antivirus might miss, especially if that malware is being protected by a rootkit.

It is important to note that each of the issues mentioned above can jeopardize the network's security even if this is fully patched.

Take into account that some systems may still have accounts which belonged to employees who left or were laid off and are still active; such a vulnerability assessment will bring these to light and, until such accounts are disabled, these potentially disgruntled employees can log in your systems and cause havoc.

The same applies to open shares. These are one of the vectors hackers use to spread viruses, especially in cases where such needless open shares aren't password protected. In some cases, having a particular port open can also be an indication that the system is running a known malware. Most vulnerability scanners will point this out in their scan results.

Rouge devices are a big security concern for companies. From USB drives to wireless access points, these devices can provide an access into your network – intentionally or unintentionally. Monitoring for the existence of these devices is an essential part of securing your network. Dangerous scripts, misconfigured services, and incorrect permissions, can all be exploited by a skilled hacker whose objective is to gain access to his victim's systems.

Something that is generally overlooked when securing the network is the devices connected to it. Printers, routers and fax machines are generally seen as a minor concern in terms of security. However, some of these devices can be used as a gateway to networks when they carry a faulty configuration or they still use default settings. Some network printers, for example, by default allow unsecured telnet access to them without requiring any authentication. A subset of these will also store a copy of what is printed in their internal storage – something employees can copy even remotely over the internet.

Finally, there are vulnerabilities caused by software. Some web services contain known exploits that allow a malicious attacker to use that script as a gateway to send emails, potentially using your organization to launch spam runs; SQL injection exploits might allow an attacker to get hold of usernames and passwords, or inserting his own username, or even to run code remotely. Likewise the use of applications with known vulnerabilities can open your organization to targeted attacks. Malicious hackers might try to send people malicious payloads targeted at these vulnerable applications that, when triggered, would run the code the hacker would have embedded in the payload sent. When misconfigured, P2P applications can share confidential documents or source codes with the whole world. These applications can be a huge threat when installed on a corporate environment. Even if configured correctly, it is impossible to verify the origin or legitimacy of anything downloaded through their use. Employees using such an application might unknowingly download malware or even illegal material.

Clearly, patch management and antivirus protection are only the first step in securing your network. A good vulnerability assessment is the next logical move. Networks are a dynamic entity, they evolve and change constantly. A vulnerability assessment should be set to run constantly and inform the administrator every time change is detected to make the utmost of network security protection.