THE NATIONAL CYBERSECURITY SOCIETY

# VULNERABILITY ASSESSMENTS

An IT vulnerability assessment is a process to identify weaknesses within your computer system and infrastructure. A vulnerability assessment will rank and quantify the vulnerabilities found based on security risk. Common types of vulnerabilities include flaws in software code, poor implementations, and/or outdated software. Hackers look to exploit these weaknesses to gain access to your critical data.

Many security breaches occur because system patches were not kept up to date. Vulnerability assessments scan the IT environment to identify unpatched software and unsecure configurations. A hacker will use similar tools to identify the same weaknesses. A vulnerability assessment will allow you to discover them, **before** they do.

## FACT 1: TYPES OF SCANS

External scans – An external scan looks at your computer system or IP address from the outside to determine what vulnerabilities are publically facing. This type of scan looks for holes in your network firewall(s) and any open ports that can be used to “exfil” or steal data.

Internal scans – An internal scan looks internally at your computer system(s) to identify what patches or unsecure configurations exist.

## FACT 2: PRIORITIZING REMEDIATION

After the scans are complete, your security provider will provide a list of remediation activities based upon risk. Vulnerabilities will be categorized as critical, high, medium or low, based upon the risk as defined by the National Vulnerability Database (NVD) and the Common Vulnerabilities and Exposures (CVE).

The National Institute of Standards and Technology in partnership with the MITRE Corporation maintains the NVD and CVE – and can be found at http://cve.mitre.org/cve/cve.html. The website provides a description of the weakness and resources to remediate the vulnerability. When remediating vulnerabilities, correct the more severe vulnerabilities on your most valuable resources.

Still have questions, need help?

Contact us at our "**Ask-an-Expert**" service, **web@thencss.org** or visit us at the link below.

© 2018 National Cybersecurity Society. All Rights Reserved.

## COMMON HACKS

HERE ARE SOME COMMON HACKS THAT EXPLOIT CYBER VULNERABILITIES:

- ✓ WannaCry – exploited unpatched software
- ✓ Equifax – exploited flaw in software code
- ✓ Shellshock – injection vulnerabilities; exploits websites
- ✓ Kermuri Water Company – exploited the company’s use of out of date software

## JOIN THE NCSS

Become a member of **The National Cybersecurity Society** today and learn more about how to protect your business from a cyber attack.

WWW.NATIONALCYBERSECURITYSOCIETY.ORG

# VULNERABILITY ASSESSMENTS continued….

## FACT 3: VULNERABILITY SCANNING TOOLS

There is several vulnerability scanning tools on the market – including many free scanning tools. Many are industry leaders in the scanning business and can give your business the insights needed to correct any weaknesses found. Vulnerability scans should be completed annually (some do so continuously), as new vulnerabilities are continually identified. If an IT security vendor supports your business, ask the vendor the status of scanning and how the work is prioritized against other clients. These vendors may remediate issues based upon their schedule, not yours, and nor do they understand which assets are most critical for your business.

## FACT 4: RESOURCES

There are several free scanning tools on the market – one option is OpenVAS. OpenVAS is a framework of free services and tools of vulnerability scanning and vulnerability management solutions. The framework is part of the Greenbone Networks' commercial vulnerability management solution – visit www.openvas.org. Another option is to ensure your security provider is conducting scans of your infrastructure as part of the managed security services they offer.

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
**web@thencss.org** or visit us at the link below.

© 2018 National Cybersecurity Society. All Rights Reserved.