THE NATIONAL CYBERSECURITY SOCIETY

PEN TESTING

Penetration Testing (pen testing) is a process used to determine weaknesses that could be exploited by hackers to gain access to critical systems and data. IT security professionals outside the organization conduct the test to mimic real work conditions without negatively effecting operations. Typically, pen testers will provide the organization an overview of the process and will seek to obtain approval from management to conduct the test.

The “pen-tester” is hired to think like a hacker, determine what types of attacks the system may be susceptible to, and then implement them to see if they work. Once the technical work is complete, the pen-tester compiles a report for the organization. The report usually provides a step-by-step explanation of the types of attacks tried; which attacks were blocked and which were successful; and which actions are needed to correct, in priority order. At a minimum, the test will identify insecure configurations, software patches that weren’t applied, open ports, software or systems not supported by manufacturers. The test may also include a phishing scam to determine if employees fall victim to this type of attack.

DID YOU KNOW…

- ✓ The Open Web Application Security Project (OWASP) lists the top ten most critical web application security risks. OWASP 17 was recently released.
- ✓ Pen testers typically refer to OWASP to conduct pen tests.
- ✓ Remember – start with a risk based approach – determine the likelihood of an event and the requisite impact. Rank the risk and correct!
- ✓ Back up important data often to reduce overall vulnerability and mitigate potential impacts of an attack.
- ✓ Employee training is an essential prevention strategy to keep your systems safe.

FACT 1: TYPES OF PEN TESTS

There are three different types of pen tests that an organization can perform. A “white-box” pen test provides testers with full knowledge of the information system and all system documentation, such as vulnerability assessments and system diagrams. A “black-box” pen test occurs when the tester takes on the role of an attacker and has no prior knowledge of the information system. The pen tester in a black-box scenario must conduct their own reconnaissance to determine how to best “exploit” the weaknesses in the system. A “gray-box” test is when the testers are provided partial knowledge of the system and limited documentation. The type of test conducted is likely to be determined by the organization and what they are trying to learn from the test.

FACT 2: COMPLIANCE

If you are an organization that accepts payment for goods and services via credit card, you may be required to have annual pen tests completed, under

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

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.

PEN TESTING continued….

PCI-DSS #6 – Patch and Correct Vulnerabilities. See NCSS Tip Sheet for more information about the Payment Card Industry Data Security Standard. (PCI-DSS).

FACT 3: PENETRATION TESTING APPROVALS

One of the most important aspects of a penetration test is it must be approved by management. A signed agreement between management and the IT security firm must be in place before the test begins, or there could be legal ramifications should something go wrong. While not everyone in the organization needs to be aware of the test, upper management should know when it is occurring. The agreement between the managers and the testers may include information such as what type of tests will be performed; what if any systems are off limits/excluded from the test; where and when will the test be performed; and under what circumstances would the test be stopped and the organization notified immediately. These are just some of the elements in a penetration test agreement.

FACT 4: PREVENTION MEASURES

Conducting frequently scheduled penetration tests are important for organizations no matter their size. Because new cyber attacks are always being developed, system protections need to evolve in order to maintain a strong defensive security posture. Conducting a penetration test is one of the best ways to ensure that this is being done. By conducting a pen-test, your organization will be able to discover vulnerabilities on your system before malicious hackers do. Additionally, your organization can use the test to determine whether or not safeguards you have put in place are truly effective.

FACT 5: RESOURCES

The General Services Administration (GSA) has developed standardized IT security penetration services for federal, state and local governments. These services referred to as Highly Adaptive Cybersecurity Services (HACS) are listed at the U.S. GSA Advantage website. While these are resources for the public sector, they do have a list of approved vendors and examples of statements of work and items to consider for pen testing.

HACS 132-45A Penetration Testing, lists services to consider including: Network Mapping, Vulnerability Scanning, Phishing Assessment, Wireless Assessment, Web Application Assessment, Operating System Security Assessment (OSSA), and Database Assessment.

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

PEN TESTING continued….

NCSS is currently working with approved and vetted service providers to help small businesses access pen testing firms and professionals, see Membership Perks. Additionally, there are several vendors listed on the GSA Advantage website.

Reference: GSA Gallery Risk and Vulnerability Assessments:

https://www.gsaelibrary.gsa.gov/ElibMain/sinDetails.do?executeQuery=YES&scheduleNumber=70&flag=&filter=&specialItemNumber=132+45D

OWASP Top 10 - 2017 – Open Web Application Security Project, The Ten Most Critical Web Application Security Risks:

https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

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