precision CYBERTECHNOLOGIES & DIGITAL SOLUTIONS

CYBER DIGITAL WORLD

NEWSLETTER

Volume 4: Issue No. 1 **December:** 2021

Dr. Ronald Walcott
Managing Director

The pandemic remains a catalyst, driving movement to the digital arena. Increasingly businesses are shifting operations to online platforms. With this in mind, we take a more careful review of the security needed to support this greater online presence.

RECAP:

WHAT IS CYBER SECURITY?

Behind every business, there's an internal network. This network can vary in size and complexity. For a home business, a network can be as small as a few devices, such as a modem and laptop. For a big business, networks are typically comprised of several user desktops and laptops, switches and servers.

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative.

WHAT IS A VULNERABILITY ASSESSMENT?

Vulnerability assessment refers to the process of identifying risks and vulnerabilities in computer networks, systems, hardware, applications, and other parts of the IT ecosystem. Vulnerability assessments provide security teams and other stakeholders with the information they need to analyze and prioritize risks, assign severity levels to those risks, and recommend remediation or mitigation, if and when needed.

TYPES OF VULNERABILITY ASSESSMENTS:

There are several types of vulnerability assessments.

Host assessment – The assessment of critical servers, which may be vulnerable to attacks if not adequately tested or not generated from a tested machine image.

Network and wireless assessment – The assessment of policies and practices to prevent unauthorized access to private or public networks and network-accessible resources.

Database assessment – The assessment of databases or big data sys-

In this Issue:

tems for vulnerabilities and misconfigurations, identifying rogue databases or insecure dev/test environments, and classifying sensitive data across an organization's infrastructure.

Application scans – The identifying of security vulnerabilities in web applications and their source code by automated scans on the front-end or static/dynamic analysis of source code.

WHY VULNERABILITY ASSESSMENTS ARE IMPORTANT:

Vulnerability assessments allow security teams to apply a consistent, comprehensive, and clear approach to identifying and resolving security threats and risks.

The benefits to an organization include:

- Early and consistent identification of threats and weaknesses in IT security
- Remediation actions to close any gaps and protect sensitive systems and information
- Meet cybersecurity compliance and regulatory needs (like HIPAA and PCI DSS)
- Protect against data breaches and other unauthorized access

PENETRATION TESTING

A penetration test, also known as a pen test, is a simulated cyber-attack against your computer system to check for vulnerabilities. These tests give a clear picture of weaknesses and provide detailed analysis of the aftermath of a breach.

How do I perform penetration testing?

Penetration tests can be broken into 5 stages:

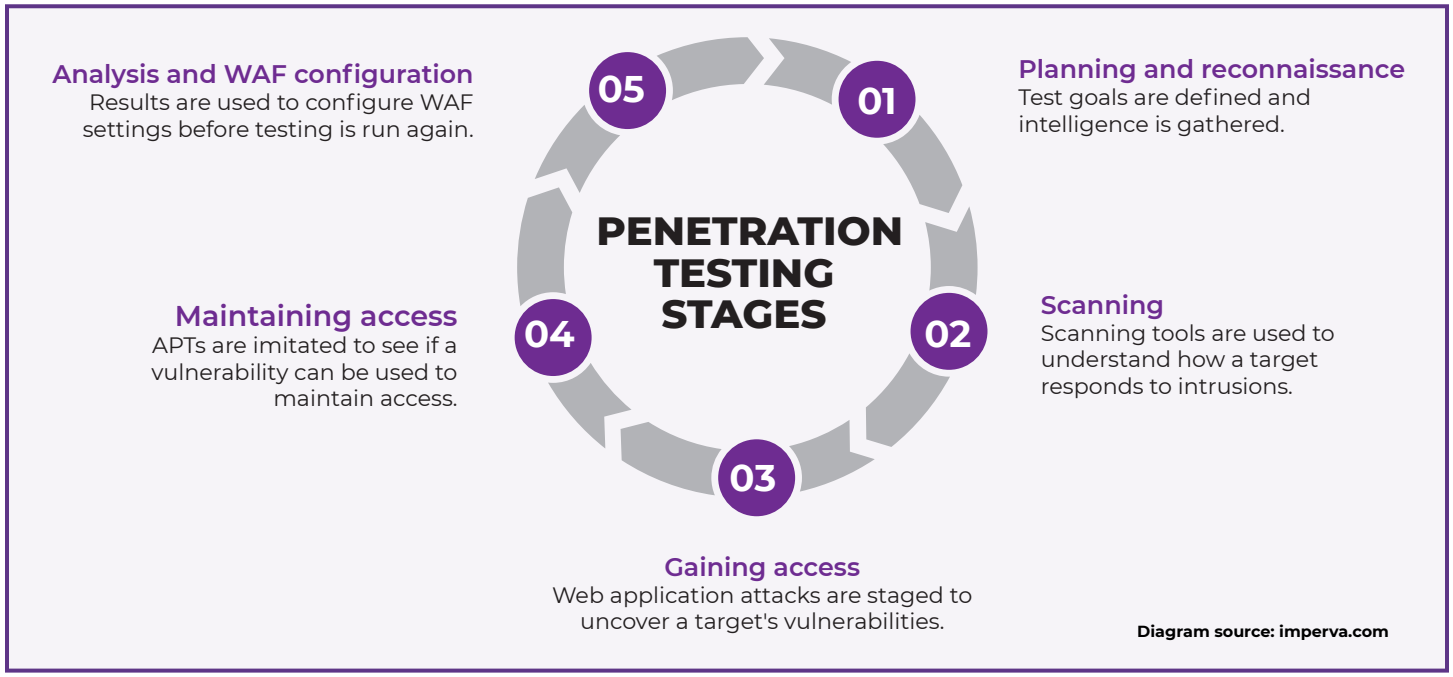

Diagram source: imperva.com

IS PEN TESTING THE SAME AS A VULNERABILITY ASSESSMENT?

Pen testing and vulnerability assessments are not the same. A vulnerability assessment is primarily a scan and evaluation of security. But a pen test simulates a cyber-attack and exploits discovered vulnerabilities.

Can a penetration test destroy my network?

Network integrity is the number one concern for businesses considering pen testing. Responsible penetration testing teams will have multiple safety measures in place to limit any impacts to the network.

Prior to a pen test, the business works with testers to create two lists: an excluded activities list and an excluded devices list. Excluded activities may include tactics like denial-of-service (DoS) attacks. A DoS attack can completely obliterate a network, so the business may want to guarantee it will not be done on a pen test.

What is ethical hacking?

Penetration testing is a type of Ethical hacking. . Basically, in pen testing an organization is ethically hacked to discover security issues. It requires consent between the business and the tester.

types of pen testing include:

- Network infrastructure
- Web Application
- Wireless
- Social engineering
- Physical

We will look at these in the next issue.

HEADLINE NEWS:

Massive Attack Targets 1.6 Million WordPress Sites

A massive wave of ongoing attacks against more than 1.6 million WordPress sites has been identified by researchers at security firm Wordfence Security. They report seeing more than 13.7 million different attack attempts over a 36-hour period, all of which focus on exploiting four different WordPress plug-ins and several Epsilon framework themes.

The attack campaign, which originates from more than 16,000 different IP addresses, makes it possible for attackers to take over vulnerable sites through the use of arbitrary option updating.

The researchers recommend that all sites be updated to the latest, patched versions of the plug-ins and themes.

WordPress plug-ins continue to be a major risk to any web application, making them a regular target for attackers, says Uriel Maimon, senior director of emerging technologies at threat protection services provider PerimeterX.Vulnerability Found

Wordfence researchers say attackers are targeting unauthenticated arbitrary options update flaws in four different plug-ins. Of the plug-ins, Kiwi Social Share was last patched in November 2018; WordPress Automatic and Pinterest Automatic on Aug. 23; and PublishPress Capabilities on Dec. 6.

"Due to the severity of these vulnerabilities and the massive campaign targeting them, it is incredibly important to ensure your site is protected from compromise," Wordfence says. "We strongly recommend ensuring that any sites running one of these plug-ins or themes has been updated to the patched version. Simply updating the plug-ins and themes will ensure that your site stays safe from compromise against any exploits targeting these vulnerabilities."

Wordfence researchers report seeing scant attempts to target these flaws before Wednesday. Given that timing, they suspect that the PublishPress Capabilities patch led attackers to reverse-engineer the flaw and begin targeting various arbitrary options update vulnerabilities.

"Shadow code introduced via third-party plug-ins and frameworks vastly expands the attack surface for websites," Maimon says. "As a result, website owners need to be vigilant about third-party plug-ins and frameworks and stay on top of security updates. They should secure their websites using web application firewalls, as well as client-side visibility solutions that can reveal the presence of malicious code on their sites."

In addition, attackers are also targeting a function injection vulnerability in various Epsilon framework themes to try and update arbitrary options.

The targeted Epsilon framework themes are Activello, Affluent, Allegiant, Antreas, Bonkers, Brilliance, Illdy, MedZone Lite, NewsMag, Newspaper X, Pixova Lite, Regina Lite, Shapely and Transcend. Another affected theme is NatureMag Lite, and as no patch is yet available, the researchers recommend that anyone with this theme installed on their WordPress site immediately delete it.

"In most cases, the attackers are updating the 'users can register' option to 'enabled' and setting the 'default role' option to 'administrator.' This makes it possible for attackers to register on any site as an administrator, effectively taking over the site," Wordfence says.

Upcoming Events

HYBRID FINANCIAL SERVICES SUMMIT
January 25, 2022

VIRTUAL ANZ SUMMIT
February 16, 2022

VIRTUAL ZERO TRUST SUMMIT
February 22, 2022

HYBRID CANADA SUMMIT
March 8, 2022

868-610-7237
salesinfo@precision-cyber.com
www.precision-cyber.com
1st Floor, Brair Place, 10-12 Sweet Road
St. Clair, Port of Spain, Trinidad