Penetration Testing Attacks

Defensive Countermeasures

Module #34

Defensive Counter measures

As a defensive counter measure,organizations put their trust in solutions for defense from these cyber threats.

The problem with this strategy is the vendor is not the victim of an attack and doesn't absorb damages from a cyber incident. Vendors will offer protection; however, they can't be responsible for anything outside of their product's control.

All it takes is a missing update, configuration error, or millions of situations that can cause a breach for which the vendor will not be liable. Plus, many organizations leverage multi-vendor solutions that don't share security intelligence, making it possible for liability to be passed back and forth between vendors.

Defensive Counter measures

Sun Tzu from The Art of War:

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle"

The same foundational concepts are true; use Kali Linux to know yourself, and know your weakness.

Testing your defenses

Best approach for hardening your defense is attacking your existing security controls with the goal of identifying weakness.

Some key concepts to consider when developing a strategy for testing your cyber-security defenses are as follows:

- Black, white, or gray hat approach?
- Test a copy or the real system?
- Possible risks from Penetration Test?
- Who should be informed?
- Are you testing detection and response to threats or focusing on identifying vulnerabilities?
- Are any compliance standards being considered?

Baseline security

One common question asked by industry experts is what should be the minimal acceptable level for security.

Many organizations must be in compliance with mandates specified by their industry and government. Any system accepting payments must adhere to the Payment Card Industry Data Security Standard (PCI DSS).

Healthcare environments must meet Health Insurance Portability and Accountability (HIPAA) standards.

Common mandates like these are popular business drivers for showing value for Penetration Testing.

STIG

A Security Technical Implementation Guide (STIG) is a methodology for standardized secure installation and maintenance of computer software and hardware.

This term was coined by the Defense Information Systems Agency (DISA), which creates configuration documents in support of the United States Department of Defense (DOD).

The implementation guidelines include recommended administrative processes and security controls used during the lifecycle of the asset.

STIG

STIGs are great guidelines to secure operating systems, network devices, and applications.

You can download STIG guidelines from http://www.stigviewer.com/stigs. You will find STIG documents contain step-by-step guides for hardening a variety of systems, including web servers.

In addition, STIG guidelines are a starting point for configuring systems to meet several regulatory compliance standards. For US federal employees, STIGs are required for systems in networks controlled by the DoD and other government organizations.

Patch management

With targeted attacks and zero-day vulnerabilities reducing the window of time between when a vulnerability is disclosed and attackers develop an exploit, it's becoming more incumbent on security managers to understand the assets in their IT environment, and the patch levels of those systems.

Patch management is an ongoing process and can only be successful if there is a method to identifying when a patch is available, prioritize when to implement the patch, validate it regarding business compliance, and how to react when a patch is not available for a known vulnerability.

This also applies to applications within systems and software such as plugins.

Password policies

In general, having a policy that controls the possible outcomes can negatively impact the strength of passwords.

Users will by human nature, try to simplify passwords anyway.

Users will also typically not change passwords unless forced by a system. For these reasons, a password policy should follow the following guidelines:

- Have an expiration that is under 90 days
- Not permit the last five passwords as replacements
- Enforce a length of at least 12 characters
- Not limit any characters, such as special characters
- Mandate at least one uppercase, number, and special character

Mirror your environment

Before testing a system against a recommended security setting, checking for vulnerabilities, or validating a vulnerable system through exploitation, it may make sense to clone your system for testing purposes, rather than testing the real system.

Best practices are replicating everything from the hardware hosting the web application to all content because vulnerabilities can exist in all technology layers.

Testing a cloned environment will give the Penetration Tester freedom to execute any degree of attack while avoiding negative impact to operations. Although most people cannot mirror the exact environment, it is usually possible to set up a virtual environment with the same functionality.

Man-in-the-middle defense

Man-in-the-middle attacks are difficult to protect against. It happens outside the victim's controlled environment, and mostly, doesn't leave an obvious signature that alert the victims involved.

MITM is typically the first step of a more sinister attack such as SSL strip. One common way to protect against MITM is ensuring websites use SSL/TLS 3.0.

In other words, make sure the websites are accessed using HTTPS or HTTP secure connections. Verifying HTTPS is not as easy as looking for a little green address bar with a lock symbol, because attackers can serve victims certificates to make it appear like the session is secure. *To properly test a HTTP session, examine the certificate and look at the certificate authority.*

DoS Defence

DDoS/DoS attacks in most cases require abusing network infrastructure hardware.
One of the common methods to defend against DDoS/DoS is configuring network devices that can handle large influx of packets, the ability to detect anomalous behavior, and traffic patterns.

Malicious traffic identified should be automatically filtered to avoid interruption of service. Tools from vendors, such as load-balancers and web application firewalls, do a great job of detecting and defending against volumetric and application-type attacks.

Security tools with DoS detection capabilities are able to recognize network, session, and application layer traffic, which is imported for mitigating DoS risks that can exist in the entire protocol stack.

Thank You