In the security world, terms are abundant. Often, they appear to be describing the same function or capability when in fact they may be similar but with distinct differences. Such is the case with penetration testing (pentesting) and security assessments. This document will provide you with some quick facts on both in order to better understand the roles they have in mainframe security best practices.

**WHAT DO THEY HAVE IN COMMON?**

The following systems, subsystems, and components are considered:

- IBM® z/OS® and its controls
- ESM (IBM® RACF®, ACF2, and TSS) as it pertains to IBM® z/OS® and the below
- Network and firewall controls
- Unix® system services, permissions and controls
- Supervisor calls (SVCs) and program calls (PCs)

Neither the pentest or assessment standard offering perform analysis of IBM® CICS®, IBM® Db2®, IBM® MQ®, and IBM® IMS®.

**HOW ARE THEY DIFFERENT?**

- Security assessments are more in depth and resemble an audit. They are performed alongside an organization's staff. In order to obtain read only audit-level access, credentials are required. This is to allow the assessment team read access to system datasets, enterprise security manager (ESM) settings, and resources. These include IBM® RACF®, ROAUDIT, TSS (to create a CFILE and issue WHOHAS and WHOOwns commands), and ACF2 (to list all logon IDs and decompile resource and access rules).

- Pentests are more adversarial and are intended to test the customer's defenses. Low-privilege-level IDs modeled after actual users are used to find escalations, data leaks, at-risk configurations, and controls that an attacker could exploit for harm. Typically, trusted users or groups are compromised and used to uncover vulnerable areas. Examples of the tactics and methods used in pentesting include:
  - Adversarial—targeting data and areas that are most valuable to an attacker
  - Working against the client’s defenses—actively trying to evade or compromise defenses
  - Impersonating the client’s users—using IDs with low privilege that are modeled after actual users
  - Uncovering attack vectors—finding vulnerabilities that allow privilege escalations, data leaks, and controls that are configured in a way attackers can bypass
  - Acting like an attacker—treating the client environment as an attacker would. Nothing is “unfair” to an attacker!
  - Mapping scenarios—demonstrating how compromised IDs move from trusted or internal user to a rogue account
WHO ARE THEY FOR?

Security assessments are recommended for clients without extensive security background or previous services engagements who need a baseline. They should be performed before a pentest and serve as a detailed inspection rather than a security health check.

Pentests are best suited for:

- Organizations that have done a security assessment at least once
- Regular and ongoing checkups after the baseline work has been done (1-2 times per year)
- Evaluating security with a “real-world” attack-style versus traditional audits.

FOR MORE INFORMATION

To learn more, please visit bmc.com/mainframe-services.