EITS
Enterprise IT Security

RELEASE DATE:	CONTACT:
January 27, 2021	Mike Sullivan
	Sr. Security Architect
RELEASE METHOD:	Enterprise IT Security
Social Media and Website	info@eits.com

Find Security Gaps with Pen Testing Before Adding New Tools

Cutting edge "buzzword" prevention technology or a new cloud solution to protect against some edge case scenario – vendors roll out the latest tools and it is easy for Information Security professionals to get caught up in the arms race, myself included. Survival in the Information Security industry requires that an organization keeps pace with technology but throwing money at security is not necessarily the place to start. Consider looking at the basics before adding another tool to the mix. One of these is the penetration test (or pen test) – assessing the vulnerabilities in an organization's environment by attempting to compromise various elements of the environment.

Why Pen Test?

Regulatory Compliance: The most profound purpose for businesses to pen test is arguably regulatory compliance. Many industries are required to follow a compliance framework that instructs them to have a third party perform this testing on an annual basis, at a minimum, and sometimes up to a quarterly basis. Organizations like this usually have a remediation program in place, and findings are resolved before the next test occurs. This regulated approach increases the chances that the organization will be prepared for an attack, as the organization is more aware of new threats and has a process to deploy the mitigations quickly after they are announced.

Test Defenses: Another reason that organizations request penetration testing is because they want to test their defenses. this could be scoped as testing an Intrusion Prevention System (IPS), the organization's Managed Security Service Provider (MSSP), or their entire security program as a whole. Some organizations may not have regular interval testing scheduled, or they may have never had a penetration test performed before.

Major Changes: The third most common reason organizations perform a pen test is when a major change has occurred. This might be a web application that has been converted to a new language or new functionality that has been added or deployed to a new location. It could also be to identify potential risks during the merger of two separate companies before connecting the two networks.

How Often Should Pen Tests be performed?

Because security threats evolve quickly, I recommend testing quarterly at a minimum. Most companies perform pen tests annually or not at all because of the cost of third-party participation. Ideally, though, security professionals should consistently test their defenses for gaps, especially when making configuration changes or otherwise altering the environment.

What Can I Do to Prepare?

Even if your organization performs routine testing, remember penetration testing time frames are highly compressed, so not all testers will look for these older problems – you may still be vulnerable to classic exploits even though previous pen tests did not flag them. Regardless of the reason for the penetration test or the preparation level of the organization, we see the same basic issues over and over again, such as:

- Default insecure Microsoft settings (old protocols enabled, security features not enabled, etc.) such as Link Level Multicast Name Resolution, Web Proxy Auto-Detect, and Server Message Block
- Incorrect Group Policy Object permissions
- Server out-of-band management interfaces enabled
- Overly permissive Antivirus exclusions

In simplified terms, if your organization has any of these issues, then your security program investment is not providing you with an acceptable return because it can all be bypassed with old attack methodologies.

So before adding new bells and whistles, make time to inspect these simple configurations, harden your environment, and prevent findings on your next pen test. If your team does not conduct penetration testing, develop a plan to systematically challenge your defenses, preferably with help from third-party professionals who can guide you through the process.

Next Steps

In the next installment about penetration testing, I will show you how you can pre-emptively remediate some of these vulnerabilities to "skip" the experience of those common findings in a pen test and – most importantly – eliminate easy attacks. Each of the issues described leads to quick compromise or quick elevation of privilege, resulting in a complete takeover of the environment, but each is easy to avoid.

The experts at EITS focus on helping industry professionals develop robust security practices. Please share with any peers and partner organizations you think may benefit from this – sharing information improves everyone's security posture.