

Security Assessments

An insecure network can lead to information theft, privacy violations and possible litigation. To help prevent these unfortunate outcomes, Alliance Technologies offers extensive assessments that help your business identify weaknesses and close up security holes. Because security touches on all aspects of a business, our assessments combine analysis of hardware, software and people to find the most significant issues without going deeper than necessary. No one wants to pay too much for an assessment or get insufficient information to secure the environment. Alliance helps in balancing these needs by combining different “blocks” of security assessment processes to create the right stack for you.

Assessment Process “Blocks”

Initial Review

The **Initial Review** process involves a short one- to two-hour discussion with people who understand networking, server and workstation technologies, as well as business processes. The goal of this review is to identify obvious security issues in an environment and identify areas that require future focus.

Public Data Review

These days, a surprising amount of information on various companies is available via the Internet. What used to be available only through a trip to a courthouse is now available for anyone to download. The **Public Data Review** uncovers publicly accessible information that could be aggregated for an attack. This can range from networking information to information about key employees, and may include leaked proprietary information. Since attackers use this technique, it is very important for an organization to identify leaks and make plans for containment.

Public Target Review

The classic analysis model is to look at what an organization has and identify flaws. A **Public Target Review** flips that model around and instead looks at what an attacker might do to cause the most damage to an organization. While most organizations do not face this level of dedicated attacker, malice for sake of maliciousness is increasing. If your organization is in a position to potentially anger others, this could be a very useful review.

Network Discovery

It is important to identify what resources are available on the network that could be exploited by an attacker. **Network Discovery** identifies network devices, workstations and servers that exist on a network. This information is then put into a map and used to speed up the assessment process and identify potential problems.

Network Vulnerability

Once a network map exists, we can begin to identify the vulnerabilities that exist on the network. This can range from unpatched systems to misconfigured services. A **Network Vulnerability** assessment analyzes the versions of operating systems and applications on a network and audits for configuration issues. It can be run with various credentials to cover the types of attacks that might be launched.

Web Vulnerability

These days, it is no longer sufficient to merely identify vulnerabilities on a network. As an increasing number of users turn to the web for their daily work, vulnerabilities in web applications can seriously affect your organization. **Web Vulnerability** tests can either audit the code directly or be conducted against the server itself. They identify areas where attackers may access or alter sensitive data or bring the entire system down.

Firewall Review

Firewalls exist in most organizations, but are often treated as a “set it and forget it” device. This often results in a situation where firewall rule sets grow more complex over time and could actually aid attackers as they assess a network. A **Firewall Review** analyzes the existing firewall configurations and matches them to current business needs. This both reduces exposure and, in many cases, improves the performance of the firewall itself.

Password Review

The topic of password security has been discussed for years. Companies can implement complex policies, but a single lazy user can often circumvent security with one weak or shared password. A **Password Review** pulls the encrypted passwords from servers and systems on a network and attempts to crack them. Weak passwords are identified so they may be fixed. Many recent public data breaches have been due to weak passwords.

DB Vulnerability

Even if you have solid security surrounding your network and the web, there could still be a direct line of access into your database. If your database is not secured, attackers could access, delete or alter the information within it. Digital information is remarkably portable and leaks have become common. Having a **Database Vulnerability** assessment can help stop a leak before it happens.

Compliance Review

If your business falls under one or more regulations, you may benefit from a **Compliance Review**. This review considers the requirements of regulations and standards like HIPAA, PCI, GLBA, SOX or the FTC Red Flag Rules, and identifies areas of potential improvement. Few businesses are ever 100% compliant, but it's cheaper to work toward compliance on your own, before the auditors get involved. A **Compliance Review** will help you lay out your plan.

Social Engineering

Technology is only part of the puzzle. If the people in your business are susceptible to manipulation, an attacker could bypass many of your security controls. The **Social Engineering** assessment attempts to manipulate your employees into granting an outside agent access to your systems. This is a very common attack on the Internet today, and it's a very good idea to find the flaws in your training programs before an attacker exploits them.

Physical Review

We tend to think of security as ending at the network, but this is dangerous. Not only are networks often accessible from unexpected areas, but many organizations have been successfully breached by outsiders stealing equipment, backup tapes or even trash. Security cameras may not provide adequate coverage. A **Physical Review** will identify many of the areas that could be improved.

Penetration

Obviously, attackers will only be successful if they manage to penetrate your defenses. The **Penetration** assessment models a successful attack from beginning to end. This could involve obtaining sensitive data, bringing the entire network down or any other goal you define. While this is often the most interesting aspect of a security review, Alliance strongly recommends it be postponed until the holes identified in earlier assessment blocks are identified and closed. This allows the organization to improve over time in a measureable way.

Strategy

In many cases, an assessment results in more findings than can be easily handled. Instead of drowning in potential projects, Alliance can help you define a long-term **Strategy** to help you meet your security needs, by balancing security and compliance projects against business needs. This also helps reduce complexity, which is a common indicator of future compromise.

Documentation

The last and most important aspect of good testing is the **Documentation** phase. It doesn't matter what a test identifies if it is not clear what that means to a business and if a mitigation choice is not presented. This should include all key systems identified, the problems discovered and a prioritized list of tasks.

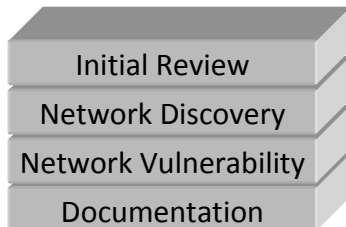
Common Analyses

While any of the above assessment blocks could be run independently, several of them can build on one another and maximize the benefit to your organization. Commonly, an assessment engagement will look like one of the following.

Network Discovery

Documentation

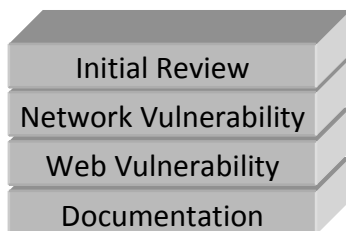
A **Network Assessment** consists of a simple network discovery process followed by documentation of the findings. Documentation in this case would consist of a set of network diagrams. It is intended for businesses that do not yet have the necessary information to discuss the network and any potential issues it may have. While most businesses start with the **Vulnerability Assessment** below, smaller organizations may wish to begin here.



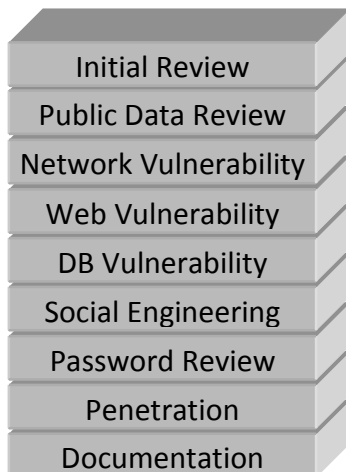
A **Vulnerability Assessment** consists of an initial review of the business network, followed by analysis of specific findings. This assessment does not typically involve exploitation of the vulnerabilities found, but does identify the most common vulnerabilities and suggests ways to address them. This is the most popular starting point for businesses just getting into security. Unless otherwise requested, the documentation consists of vulnerability-related findings only. The findings of a **Vulnerability Assessment** often take a year to address.



A **Compliance Review** builds on a vulnerability assessment base, but focuses on specific compliance requirements for appropriate regulations and standards. For example, a review focused on PCI would identify where credit cards are used and how that area of the network is isolated from the rest. It would identify vulnerabilities, but only within the PCI scope. Similarly, a HIPAA-focused review would identify where health information is stored and how it might be accessed. While a **Compliance Review** identifies general security issues, it focuses on your expectations under specific regulations.



A **Web Vulnerability Assessment** works much like the vulnerability assessment above, but focuses on specific web applications. It starts with a limited vulnerability analysis process, but quickly shifts focus toward web-specific issues. If your applications are Internet-facing, they will be analyzed for how an outside attacker could attack them directly. If they are internal only, the focus will be around user controls and data control technologies. This assessment focuses on the web servers, database servers and other supporting infrastructure. Due to the nature of web applications, these assessments may take a significant amount of time.



A **Penetration Test** combines numerous assessment blocks with the ultimate goal of identifying how an attacker could gain direct access to vital business data. A test likely involves multiple blocks to some extent, but most include at least those shown. Network servers, web servers and databases are all assessed. Vulnerabilities are taken advantage of and social engineering techniques are used to identify weak employees. If passwords can be captured, they are analyzed and used. Once the goal has been achieved, the entire process is documented, along with recommendations for improving the business and infrastructure to make future attacks more difficult.

Penetration tests tend to be very time-consuming and expensive. At this time, Alliance Technologies' penetration tests follow the most recent draft of the Penetration Test Execution Standard (PTES). Once the final version is released, this standard will guide the entire test.