

## Security Assessments

An unsecure network can lead to information theft, privacy violations, and possible litigation. To these unfortunate outcomes, Alliance Technologies offers extensive assessments that help your business identify weaknesses and shore up security holes that could damage your bottom line.

In following with the philosophy of Alliance Technologies, our security assessments aim to be the right combination of assessing hardware, software and people to best meet the needs of our clients. No one wants to pay too much for an assessment nor do you wish to get too little information to secure your environment. Alliance helps in balancing these needs by combining different “blocks” of security assessment processes to create the stack is right for you.

### Assessment Processes

#### Initial Review

The Initial Review process involves a short one to two hour discussion with an individual who has reasonable knowledge as to networking, server and workstation technologies as well as business processes. The goal of this review is to identify most of the obvious security issues in an environment and identify areas on which to focus in the future.

#### Public Data Review

These days, a surprising amount of information on various companies is available via the Internet. What used to only be available through a trip to a courthouse or private investigator is now just floating around on the Internet. The Public Data Review uncovers publicly-accessible information that could be aggregated together for an attack. This data can range from networking information to information about key employees or owners to accidentally leaked data. Since attackers use this information, it is very important for an organization to identify what is out there.

#### Network Discovery

Next, it is important to identify what resources are available on the network that could be exploited by an attacker. Network Discovery uses various technologies to identify network devices, workstations and servers that exist on a network.

#### Network Vulnerability

Once a network is mapped out, we can begin to identify the vulnerabilities that exist on it. This can range from unpatched systems to misconfigured services. A Network Vulnerability assessment would consider the versions of the operating systems and applications running on a network, common password issues, and reviews of security configurations. It can be run with various credentials to cover the types of attacks that might be launched against you.

### Web Vulnerability

These days, it is no longer sufficient to identify vulnerabilities on a network. As an increasing number of users turn to the web for their daily work, vulnerabilities in any of your web applications could seriously impact your business. Web vulnerability tests can be done directly on the code or against the running system. They will identify areas where attackers may mislead users, access or alter sensitive data or bring the entire system down.

### DB Vulnerability

Even if you have solid security surrounding your network and the web, even a little public-facing web app can be a direct line of access into your database. If your database is not strongly secured, attackers could access, delete or alter the information within it. Digital information is remarkably portable and leaks of sensitive information have become common. Having your database scanned can help stop a leak before it happens.

### Compliance Review

If your business falls under regulations but is not assigned specific regulators, you may benefit from a compliance review. This will consider the requirements of regulations and standards like HIPAA, PCI or the FTC Red Flag Rules and tell you how your business measures up. Few businesses are ever 100% compliant, but it's always cheaper to work towards compliance before there is an outside entity driving you towards it. 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 portion of an assessment attempts to manipulate your users 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 may exploit them.

### Physical Review

We tend to think of security as ending at the network, but this is dangerous. Many organizations have been successfully breached by outsiders stealing equipment, backup tapes or even the trash. Areas of the network may be accessible from uncontrolled areas of the building. Even businesses with security cameras may not have adequate coverage. A Physical Review will identify many of the areas that could stand improvement.

### Penetration

Obviously an attacker will only be successful if they manage to actually penetrate your defenses. The Penetration phase models a successful attack from the beginning to the end. This could involve obtaining

sensitive data, bringing the entire network down or any other goal that you define. While this is often the most interesting aspect of a security review, Alliance strongly recommends that a Penetration test be postponed until most of the other holes that an attacker could exploit are identified and closed. This allows the organization to grow its security posture instead of simply getting serially compromised year after year.

Documentation

The last and most important aspect of a good set of 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 there is not a clear path to improvement. This should include all key systems identified, the problems uncovered 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 run like one of the following:

Network Discovery

## Documentation

A **Network Assessment** consists of a simple network discovery process followed by the documentation of the findings. 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

Initial Review

## Network Discovery

## Network Vulnerability

## Documentation

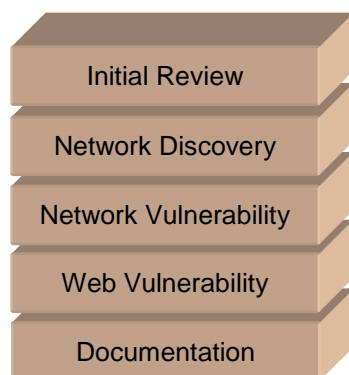
A **Vulnerability Assessment** consists of an initial review of the business and network followed by analysis of specific findings. It does not go all the way to complete exploitation, but does find the most common vulnerabilities and suggests ways to address them. This is the most common starting point for businesses just getting into security. The findings of a **Vulnerability Assessment** will often take a year to address, so future assessments tend to occur in the following budget cycle.



A **Compliance Review** builds on a vulnerability assessment base, but focuses on vulnerabilities as they apply to meeting specific compliance requirements for different 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 within the PCI scope, but only within the PCI scope.

Similarly, a HIPAA-focused review would identify where health information is stored and how it might be accessed. The vulnerabilities uncovered would focus on those areas.

While a **Compliance Review** will identify general security issues, it is primarily focused on your expectations under specific regulations.



A **Web Vulnerability Assessment** works much like the vulnerability assessment above, but focuses on specific web applications. It will start with a limited network discovery and analysis process, but will quickly shift focus towards 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 would be around user-controls and data leakage prevention technologies. It will focus on the web servers, database servers and other supporting infrastructure.

Due to the nature of how web applications work, these assessments can take more time than might be expected.