The Pros and Cons of an Authenticated Network Security Scan

www.alliancetechpartners.com

Alliance Technology Partners

The Pros and Cons of an Authenticated Network Security Scan

A common answer to many information security questions usually entails some form of "It all depends". This is especially true when it comes to whether or not you should perform a network security scan as an untrusted outsider or a trusted user.

The answer to this, of course, is – It all depends.

Unauthenticated testing means poking around your network and finding various flaws or weak spots as an untrusted user. This can be helpful if you

are only interested in some of the most basic forms of security threats. However, the most dangerous threats are the ones lurking around with internal access to your network already – and most malicious attacks from hackers occur with trusted user access.

Knowing this, the follow up to "It all depends" becomes – It all depends on if you're serious about your network security or not. But, before moving full steam ahead with an authenticated network security scan you'll need to fully understand the pros and cons of doing so and tempering expectations.

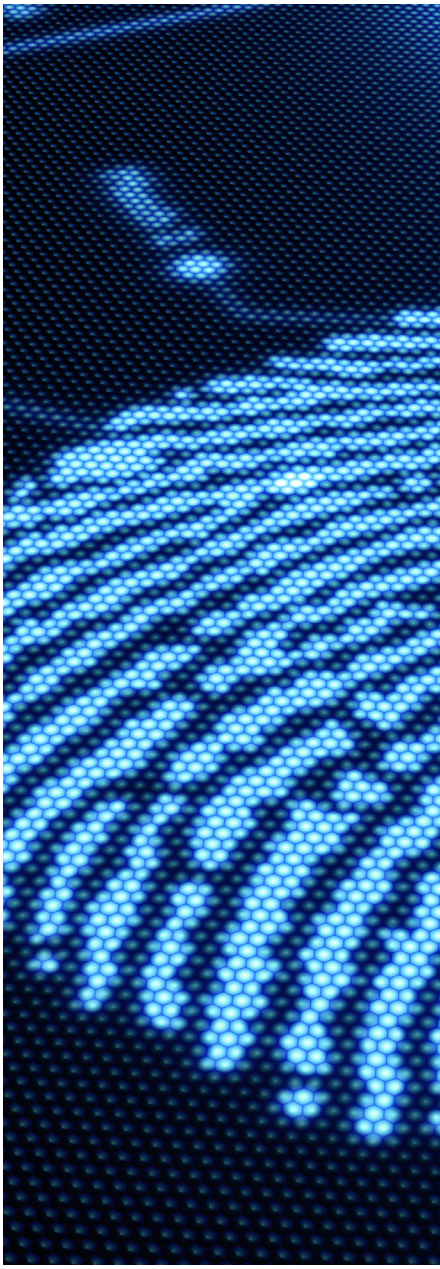
Pros of an Authenticated Network Security Scan

Authenticated network security scanning can add a lot of value to your overall network security health. Given the fact that more often than not criminal hackers and malware already have authenticated access into your network, it only makes sense to do the deep digging an authenticated network security scan provides.

Here are the major benefits of authenticated scanning:

- Provides more detailed information about the most serious security threats
- Identifies missing patches, weak share permissions, and misconfigurations

"...the most dangerous threats are the ones lurking around with internal access to your network already..."



- Helps maintain regulatory and PCI compliance, and business requirements
- Provides a true picture of where your network security stands
- Fully simulates how a targeted attack would behave deep within the network

Cons of an Authenticated Network Security Scan

Knowing the major benefits of authenticated scanning probably has you eager to get started – after all, who wouldn't want to take their network security to the max where possible. With that said, there are certain drawbacks to performing authenticated scans you must be prepared for.

Here are the major drawbacks of authenticated scanning:

- Authenticated scans will give you a ton of difficult to read information
- Scan times take two to three times longer than unauthenticated scanning
- The process is more difficult and requires advanced manual analysis
- More testing tools and system resources are required
- It requires the involvement of high-level staff (admins, developers)

Is Authenticated Scanning Right For You?

The pros and cons of an authenticated network security scan certainly highlight exactly what you can expect out of such a scan, but you still must decide what it is you are trying to accomplish with security testing.

If you only need to find, and are only interested in, what an outsider without internal network access can do then unauthenticated scanning should work just fine for your business. On the other hand, finding out exactly what kind of havoc anyone with even basic user access can wreak on your company is extremely beneficial.

Regardless of whether you want to take the time to go through an authenticated scan or not, it's highly recommended by Alliance Technology Partners' network security experts – even if you only perform one once a month. Besides, how do you really know where your business network security stands if you don't make the effort to understand where it's currently at?

Contact the network security experts with Alliance to bring your network security up to speed.

GET IN TOUCH

CORPORATE HEADQUARTERS

18102 Chesterfield Airport Rd. Suite E
Chesterfield, MO 63005

314 649 8888 **St. Louis**
314 649 8889 **Fax**
888 891 8885 **Toll Free**

sales@alliancetechpartners.com