bluedog
SECURITY MONITORING

VAPT Q&A

Q. What is VAPT?

A. VAPT stands for Vulnerability Assessment and Penetration Testing. A vulnerability assessment scans your public facing network interfaces and website to find any vulnerability that can be exploited by cyber criminals to gain entry to your network or the workings of your website. A vulnerability assessment usually takes the form of an automated scan of your network, whereas a Penetration Test is performed manually by highly skilled operatives.

Q. Why is a regular Vulnerability Assessment Scan or Penetration Test so important?

A. Every single day, over 300 new technical security weaknesses are discovered in technology that we use. This means that whenever an assessment is performed against your organisation, the results are quickly outdated. When you do these tests only once a year, you can imagine how many new potential weaknesses are lurking beneath the service. Therefore we perform frequent recurring assessments.

Q. What does a Vulnerability Assessment Scan check?

A. Vulnerability assessments are performed on your company infrastructure, internal or external. When these technical checks are performed, over a million different weaknesses are checked and tested against. Each weakness found is looked at and validated by the service.

Q. How long does a Vulnerability Scan take?

A. The Internal Vulnerability Assessment scan duration will depend on the network size together with the devices connected to the network and External Vulnerability Assessment scan will depend on the scope. Typically, a vulnerability scan takes anywhere from an hour to about a day to complete.

Q. How do I get the scan report?

A. This depends on which service you have purchased. For regular automated scans we provide you with a login to the bluedog dashboard which lets to see the results of each scan, you can drill down into the results, and from the dashboard you can produce a PDF report ready for print. For either manual penetration testing or one-off automated scans we will send you a comprehensive PDF report via Email.

Q. How do I fix the issues it finds?

A. Each issue highlighted in the scan report comes with a detailed description of the issue, in-depth insights to help you understand the issue, and also a recommended solution to the issue. If you have in-house IT skills they should be able to understand how to resolve any issues.

Many issues can be prevented by keeping your software or firmware to the latest version, these types of recommendations are also included in our assessment results.

Q. Can I use the results to show I am compliant?

A. Yes, vulnerability assessments and pentests provide you with detailed reports, helping organizations to keep track if they are still compliant against different compliance requirements. When manual assessments are done, recommendations are made beyond technical level, so that you also have a roadmap laid out on business level.

Q. How long does a Manual Penetration Test take?

A. Manual Penetration Testing requires more time compared to automated VAPT and the length depend on the scope and available budget. If an automated VAPT's function is to discover flaws in your system, a manual pentest is to exploit weaknesses that are difficult for automated assessments to find. Pentesters will check how they can exploit your company's weaknesses; how to bypass your employees in terms of security; and if your security policies are properly implemented. It mimics how cybercriminals work and this method requires more time due to its compexity.

Q. Does the Pen Tester get access to sensitive information in my network?

A. This depends. If our security operative can break into your organization by successfully exploiting a found weakness, there is a technical possibility that they could encounter sensitive information. However, as bluedog is a professional security organisation, no harm will be done. You rather have us seeing the data than a hacker with criminal intent, right?

Q. Can an Automated VAPT Scan be performed using Authentication?

A. Yes, this is referred to as an Automated Authenticated Scan. If your website or web application contains a login form, you can provide us with one or more login credentials that we feed into the automated scanning software. The scanner will then use these credentials to test the items inside the password protected sections of your website.

Please Note: Third party remote login systems such as Auth0 and 0Auth cannot be used by our automated VAPT system as they are on a different domain to the website. If your website uses one of the third-party remote login platforms, we can only perform a manual penetration test.

Also Note: An Automated Authenticated Scan is much more aggressive than a usual scan. It's therefore important that we only perform this kind of scan on a test or staging site. You will be asked to sign a Waiver Agreement before we can commence this type of scan.

Q. My website is built with WordPress – is this ok to scan?

A. Yes, however, there are a couple of things to bear in mind with Vulnerability Scans for WordPress sites. First of all, due to the enormous number of files created by WordPress, the scan can take well over 24 hours to perform. In many instances scans of WordPress sites will time-out before the scanning process is completed. Secondly, it must be remembered that there are many thousands of bug-bounty hunters around the world constantly trying to crack WordPress; any vulnerabilities are then reported back to WordPress and fixes are put out almost instantly. It's therefore very unlikely that we will discover any serious vulnerabilities in a WordPress site.

If you have part of your site built in WordPress and part built manually, then we suggest that the two things are kept separate (on different sub-domains) and that we scan the non-WordPress part of your website or web application.

To find out more about our VAPT Service and our other solutions, email us at **sales@bluedogsec.com** or visit **bluedog-security.com**.

CERTIFIED ISO 27001 CERTIFIED

bluedog SECURITY MONITORING