

Improving your network and application assurance strategy in an environment of increasing 0day vulnerabilities

An NGS Secure Whitepaper by Paul Vlissidis

whitepapers@nccgroup.com

2010



Contents

- 1 Abstract
- 2 Introduction
- 3 A Response using Managed Security Monitoring
- 4 Conclusion
- 5 References



1 Abstract

The past few years have seen a distinct shift in the pattern of security vulnerabilities and attack vectors targeted against Internet-facing systems and applications. The prevalence of an increasing volume of zero-day (0day) exploits and the targeting of application vulnerabilities has rendered traditional assurance strategies based on annual network penetration testing and timely installation of vendor patches less effective.

That said we do not want to “throw out the baby with the bathwater”. Assurance techniques such as penetration testing and vulnerability scanning are still powerful tools if used intelligently and cost-effectively. A multi-faceted strategy is now needed to minimise (although not completely mitigate) the threats posed by this new landscape.

2 Introduction

0day definition

For the purposes of this paper we define a 0day vulnerability as:-

Any vulnerability, in deployed software, that has been discovered by at least one person but has not yet been publicly announced or patched by the vendor/developer.[3]

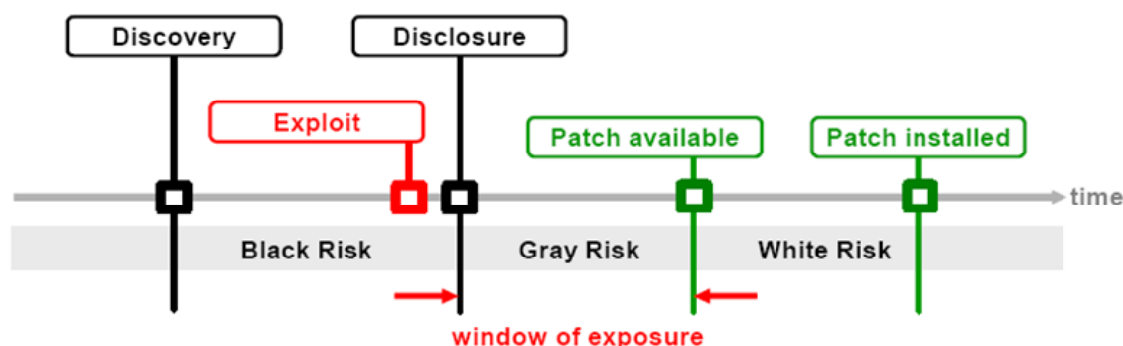
The 0day menace

The world of security vulnerabilities is often described as an arms race. As the “white hats” produce a new defence the “black hats” devise new and more sophisticated attacks. A better analogy would be a Darwinian system that continuously adapts attacks as the defence environment changes. Some of these ideas have been explored in [1]. Developing this analogy Network and Application Security Managers therefore need to adapt their assurance strategy to the next generation to improve their chances of survival.

Recent studies of vulnerability lifespans reveal that the average lifespan for a vulnerability from the point at which it is reported to a vendor is 131 days [2]. A ‘traditional’ annual testing cycle is clearly inappropriate by itself in such an environment. Even quarterly testing or scanning (still cited by many as best practice) is inadequate in today’s fast moving 0day security reality. The same study estimated that at any given day in the years studied there were between 2500 and 4500 0day vulnerabilities in existence. Another paper [3] has attempted to define the major steps in the vulnerability lifespan.

Stage	Description
Discovery-Time	The earliest date that a vulnerability is discovered and recognized to pose a security risk. The discovery date is not publicly known until the public disclosure of the respective vulnerability
Exploit-Time	The earliest date an exploit for a vulnerability is available. We qualify any hacker-tool, virus, data, or sequence of commands that take advantage of a vulnerability as an exploit.
Disclosure-Time	The first date a vulnerability is described on a channel where the disclosed information on the vulnerability is: (a) freely available to the public, (b) published by trusted and independent channel and (c) has undergone analysis by experts such that risk rating information is included.
Patch-Time	The time of patch availability is the earliest date the vendor or the originator of the software releases a fix, workaround, or a patch that provides protection against the exploitation of the vulnerability.

Using this lifespan model [3] goes on to identify a series of risk periods as :-



Given these useful views on risk in the vulnerability lifecycle we should now ask: how can security testing and scanning services mitigate these risks? Clearly no penetration test or scan can provide complete assurance during the black risk period. More advanced penetration testing companies (such as NGS Secure) have extensive research capabilities and strong connections within the research community so some partial assurance can sometimes be achieved by using such a company. Most of the best-in-class vulnerability scanning tools can only produce code to test for issues during the gray risk period. In fact this is somewhat academic since many networks we test still carry considerable exposure right into the white risk period as patch management processes remain in the dark ages for many organisations (see [Project Quant](#))

Nevertheless this analysis suggests that much greater regularity in deep penetration testing and vulnerability scanning is needed to adequately manage these risks going forward. The problem is that this type of testing is expensive and time consuming and it is beyond many organisations' maturity levels to cope with the logistics, BAU interruption, and information overload that such an approach might produce. If we accept that 'do nothing' (or 'do nothing new') is not an option then a third way needs to be found that treads the line between cost and risk mitigation (benefit).

Let us first consider the respective differences between Penetration testing and Vulnerability Assessment scanning :-

Vulnerability Assessment Scanning (VA) can:

- Check patch levels across large parts of the estate
- Find 'low hanging fruit' issues such as default passwords
- Find basic configuration errors
- Perform many thousands of input tests on all identified fields within applications

Penetration Testing/Full breach testing can:-

- Provide a far deeper view
- Provide an in-depth focus on critical areas
- Identify issues with underlying processes/policy
- Test the human factor
- Perform more complex attacks by combining simpler weaknesses into more dangerous attack scenarios
- Check for business logic flaws in applications,
- Answer the question: "Are we secure at the moment?"



Clearly solutions based exclusively on either approach will not suffice or will be too costly. Even the best VA tools produce large amounts of false positives and offer little sophistication in reporting actual risk.

In a current 'best practice' model we typically see the above techniques being used in the following manner:-

Type of VA	Use	Frequency
Penetration Test	Infrastructure	Annually or after significant changes
	Applications	Annually or after significant changes
Vulnerability Scan	Infrastructure	Quarterly
	Applications	-----

The problem with this strategy is that it provides typically 5 'snapshots' of the network per year. Most networks undergo far more change than this over 12 months. In many cases these changes are small and short-lived but nevertheless present a window of potential vulnerability. One recent example was of a financial services company that had allowed a third party developer access to their website for maintenance. The result was that an anonymous FTP service was enabled just 1 week after a quarterly scan had been completed. Although only needed for a few hours the service remained live. In this case highly sensitive data files were available via this vulnerability, which is trivial to exploit. The above approach would have left the vulnerability exposed for almost 3 months.

If we adopt a tiered approach we can start to realise the benefits of both types of assurance without a significant cost increase. Furthermore if we supplement these activities with a new type of scan, namely change detection or 'delta scanning' we can dramatically improve our ability to detect and mitigate risks.

A tiered monitoring approach brings a number of additional benefits:-

- By running daily checks for any infrastructure changes it can detect inadvertent exposure of services. New or changed services can be tested individually on an ad hoc basis. Ad hoc manual testing in this way makes best use of the expensive security testing skills. Where there are compliance implications such as PCI, a QSA can be consulted and advice offered.
- A tiered monitoring approach can directly support and integrate with change control processes.
- By increasing the frequency of VA activity it allows a faster response as vendor patches are issued.
- Such an approach where issues are reported as they arise rather than in large reports fits testing and scanning more effectively into operational risk management.
- The increased level of scrutiny makes for a more robust audit compliance response to standards such as PCI DSS.

An optimal cost effective, risk based model using a tiered approach might look like this:-

Type of Test	Use	Frequency
Full Penetration Test	Critical Infrastructure	Annually or after significant changes
	Critical Applications	Annually or after significant changes
Vulnerability Scan	Infrastructure	Weekly, monthly or quarterly
	Applications	Monthly, quarterly or after moderate changes
Change Detection	All infrastructure ranges	Daily delta change detection with ad hoc penetration testing of identified changes where appropriate

To further enhance the return on value from testing and to determine the frequency of testing it is recommended that Network assets and Internet facing applications be graded against a Risk method to ensure that the most sensitive assets attract the greatest Penetration testing and Vulnerability Scanning effort. Whilst all systems should be secure it is clear that an Internet banking site presents a greater threat risk if compromised than a 'brochure ware' site which has little value.

3 A Response using Managed Security Monitoring

NCC Group Secure Test offers a managed security monitoring service using the above tiered approach under the name of "Minerva".

Minerva takes the current best of breed in scanning technology and delivers it via a managed service such that a bespoke alert is issued to one or several pre agreed contacts where new issues are detected. IP ranges are scanned daily for changes and reported/investigated. As an example over a 121 day period a total of almost 500 changes were detected across approximately 16,000 IP addresses being monitored.

We continually monitor the Vulnerability Assessment market and ensure that we are using the most appropriate and most effective tools to scan your networks and your applications. We currently deploy:-

- Tenable Nessus
- nmap
- Netvigilance Securescout
- Rapid 7 Nexpose
- Accunetix
- HP Web Inspect
- Appscan
- + our in-house Security Event Monitoring Management Suite

A mixture of scanning technologies overcomes many of the problems that commercial scanners display such as false positives, slow response to new vulnerabilities and 'technology bias' (where more popular technologies are assessed better) A group of systems and applications is initially subjected to full testing and a 'baselining' process. This allows all issues to be identified, false positives removed and any initial mitigation/remediation to be completed before scanning begins.

Systems can be grouped and reported in any combination. Once the managed monitoring begins customers are informed daily should any new issues arise according to the scan frequencies set for the group. These include newly detected services, new live IP addresses, and new vulnerabilities (both infrastructure and application) on existing services. All changes and vulnerabilities detected are manually verified by an experienced penetration testing consultant, ensuring only relevant issues are reported in the context of business risk. By default reporting is done by exception to one of more contacts for each group of systems although reporting can be provided to any depth required. Weekly and monthly activity summary reports are also available.



Minerva offers daily assurance that external changes are alerted and reported within a 4 hour working day service level agreement and that vulnerability scanning reports are provided in line with the customers agreed requirements leaving clients confident their external facing infrastructure and applications are secure on an ongoing basis, not just on the day a manual test is completed.

This white paper focus on the external threats faced to Internet facing systems as these tend to attract the most attention. However many of the same threats are also faced on internal systems and applications. The same comprehensive systems scanning provided by Minerva for external assets can also be deployed for internal systems. The internal Minerva services are all fully managed by the same highly trained NGS Secure security specialists.

4 Conclusion

Security Testing and monitoring regimes need to adapt to the shifting risk landscape. In a climate where there is pressure on security budgets but no change in risk appetite then a new mindset using a tiered monitoring and testing approach is an appropriate response. In our view this type of approach also offers a more effective response to the increased level and sophistication of attacks.

Minerva augmented with the premium annual penetration testing by NGS Secure provides comprehensive and cost effective solutions to assure that all monitored/tested infrastructure and application assets are protected by the best security technologies and highly skilled security staff available.

5 References

- [1] Natural Security: A Darwinian Approach to a Dangerous World, Raphaël D. Sagarin, Terence Taylor
- [2] Empirical Estimates and Observations of 0Day Vulnerabilities, Miles McQueen et al, Idaho National Labs
- [3] 0-Day Patch - Exposing Vendors (In)security Performance, Stefan Frei CSG, Bernhard Tellenbach CSG, Bernhard Plattner CSG
- [4] Project Quant , Rich Mogull, Securosis