# Rebooting the Pentest

## Save money and improve resilience with a pragmatic approach to security scoring

HOLISTICYBER

DEFEND WHAT MATTERS

# TABLE OF CONTENTS

# EXECUTIVE SUMMARY

## The problem with pentesting

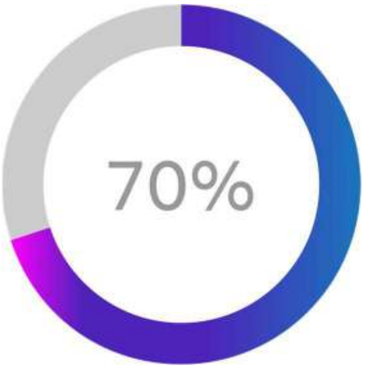
With an increasing number of pentesting assessments being treated as a compliance requirement or a tick-box exercise, it’s becoming ever-harder to understand security findings in a business context. While skipping over the context might enable speed and cost savings – which of course are significant business drivers – the real security value in pentesting relies on taking a holistic approach, where business impact, threat capability and the real-world seriousness of any vulnerabilities are well understood.

## What does this mean?

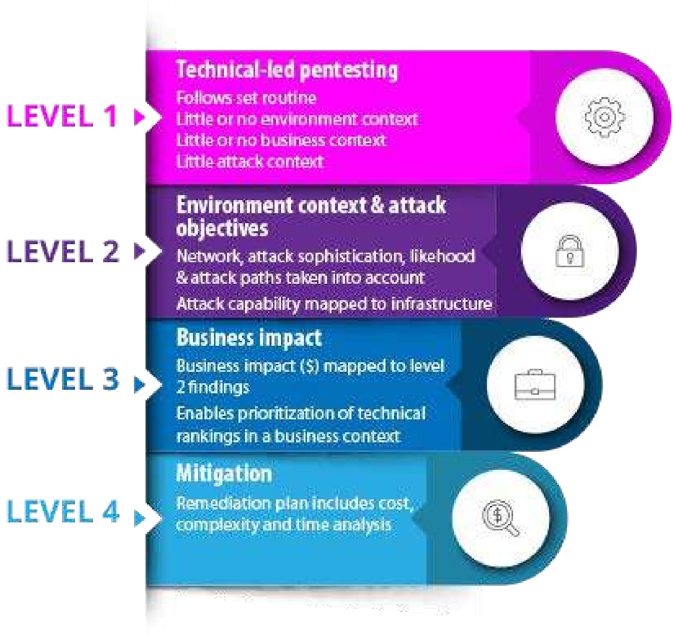
1) Organizations struggle to understand which findings really need prioritizing
2) Firms can waste thousands in fixing non-critical business issues, while leaving significant exposure to risk
3) Enterprises using a range of internal and external pentesting suppliers face difficulties in applying standardization across findings - with different suppliers scoring findings to different methods.

## So what’s the solution? Four steps to a holistic approach

A holistic approach involves understanding more than just the technical findings. We need to understand the organization, what it does, and why a pentest is needed. We also need to look at the threats, their capability and their motivation. Understanding these factors together will enable us to adjust the pentest simulation accordingly, and treat findings with the appropriate context. However, reaching a completely holistic view isn’t something that can be achieved overnight – instead we advocate a phased approach, which enables organizations to improve testing maturity step-by-step and in a practical way.



**70%** of security leaders do not believe their current pentest methods address priority security vulnerabilities (Bugcrowd, 2018)


LEVEL 1
Technical-led pentesting
Follows set routine
Little or no environment context
Little or no business context
Little attack context
LEVEL 2
Environment context & attack objectives
Network, attack sophistication, likehood & attack paths taken into account
Attack capability mapped to infrastructure
LEVEL 3
Business impact
Business impact ($) mapped to level 2 findings
Enables prioritization of technical rankings in a business context
LEVEL 4
Mitigation
Remediation plan includes cost, complexity and time analysis

## LEVEL ONE – Technical-Led Pentesting

This is where many organizations currently lie in their penetration testing maturity. While the penetration testing itself and the associated findings might be technically excellent – and enable compliance reporting and assurance, the lack of business context can severely limit the value from such an engagement. This can leave organizations prioritizing non-business critical issues, while leaving attack paths open to key assets.

Typically, engagements at this level have little in the way of environmental context beyond the systems in scope, no real business context, and often lack an understanding of specific threat capabilities and motivations that are relevant to that organization. Rather than thinking about an actual attack, this can leave the activity as a tickbox exercise – significantly reducing the value of the overall engagement.

# LEVEL TWO – Environmental Context and Attack Objectives

To achieve level two, organizations need to start thinking about both the environmental context (where is the asset on the network, what is it linked to), and the attacker goals and capabilities. In order to make sense of these complex inputs, a scoring system can be implemented that may take into account factors such as network segment, proliferation degree, exploit sophistication and staging factor.

An example of how scoring findings to take this into account is detailed in Figure 1 overleaf. If the framework below is consistently applied to penetration findings, then organizations will be in a position where priorities can be assessed in accordance with attacker capabilities in the context of the IT estate. This approach may add significant value to a pentesting program (or even a wider risk-scoring exercise), although it still limited by a largely technical focus.

In order to practically apply this scoring, organizations may wish to use the method detailed in appendix (i) to standardize and bring together the complete range of factors.

### What about CVSS?

CVSS, or Common Vulnerability Scoring System is a widely used framework that focuses on technical exploitability. This approach does not take into account the relevance of the finding in terms of the IT environment, or what an attacker may seek to achieve.

As such, CVSS-led reporting can leave organizations with a long list of high-impact findings that they struggle to prioritize - which detracts from the true security and business needs.

## Figure 2: Scoring environmental and attack objectives

*Scoring between 1 - 10 is for illustration and should be tailored to your own organizational profile*

| Factor | Explanation | Scoring | | | |
|---|---|---|---|---|---|
| Network Segment | A finding on the outer layer of the network is more likely to be exploited because of higher accessibility | Public external, internet facing (10) | DMZ (8) | Internal network (5) | Private network (2) |
| Proliferation Degree | How likely is it that the vulnerability is actually known about by a potential attacker? | Very common, high proliferation (10) | Medium proliferation, known about by advanced groups (7) | | Rare, In possession only by distinct groups (2) |
| Exploit sophistication | How likely is it that even if known, the attacker has the ability to take advantage of the finding? | Novice (10) | Intermediate (8) | Advanced (6) | Elite attack expert (4) |
| Staging Factor | How likely is it that the finding may serve as a staging point to conduct additional attack vectors | High – it is certain that this finding unlocks additional attack vectors (10) | Medium – it is likely that the finding can be used as part of other staging attacks but it is not certain (5) | | Low – the finding by itself cannot be used to leverage other attack vectors (2) |

# LEVEL THREE – Adding Business Impact

In order to develop maturity further, we need to look more closely at the underlying business. Any good security strategy should be aligned in supporting the business strategy, and the extra level of scoring suggested here maps business impact to individual findings. This approach helps to further prioritize findings across different penetration tests, while ensuring all remediation activity is driven by business need. If the asset's Business Impact Analysis (BIA) is already known, then monetary value of the asset affected by the security finding can be taken into the scoring calculation as follows :

| Business Impact | Impact Range | Asset Score |
|---|---|---|
| High | $100m+ | 10 |
| Medium | $10m - $100m | 5 |
| Low | $1m - $10m | 2 |

The impact ranges suggested should be normalized to the size of the organization. If the monetary value of the asset or the BIA is not available, a similar scale of values can be used based on an alternative qualitative scale of High/Medium/Low. In order to incorporate Business Impact into our existing 'level two' scoring, organizations may wish to use the methodology further detailed in the appendix.

Furthermore, organizations with an existing and mature BIA may wish to jump straight to level 3, and enrich with level 2 in slower time.

**Further enhancements with a CIA breakdown**

Organizations looking to further enhance their understanding of business impact could look to apply separate values to security findings in terms of Confidentiality, Integrity and Availability as they relate to assets. While a complex endeavor, it can enable a more accurate understanding in business terms of financial, reputational, legal damage and human cost.

# LEVEL FOUR – Taking the Practical View of Remediation

The reality for most organizations is that pentest findings – and indeed cyber security risk as a whole, is a never-ending stream of tasks that can never actually be completed. There are simply too many findings and issues to address, alongside incidents and day-to-day ‘firefighting’ that are the mainstay of security teams the world over. As such, when drawing up remediation priorities it can be important to further score our level 3 findings above, with a Cost, Complexity and Time analysis (CCT), to ensure the sensible allocation of resources. Here, we are looking to ensure that we focus enough resource on the ‘quick wins’, and not sinking everything into a high priority long-term fix.

At this stage, we can also take an attacker goal-based view and apply scoring based on the criticality of the finding along an overall attack path. If the finding is critical to an attack path and has very few (if any) alternatives that an attacker could use instead, then it may warrant a higher remediation priority than if several attack alternatives remain available.

# FINAL THOUGHTS

Penetration test findings (or any cybersecurity findings) continue to be vast in number, and difficult to prioritize at the best of times. This becomes even more of an issue where different testers are involved across different parts of an organization. A well implemented pentest maturity program can help, by focusing business resources in a pragmatic way, onto those issues that really matter. By taking into account the attacker mindset and capability, as well as the business impact and the cost of remediation, a program such as this can deliver significant security enhancements, while also saving the organization time and money.

To discuss any of the themes raised in this paper in more detail, or to understand how HolistiCyber can help implement a pragmatic approach to your own maturity journey, please do get in touch.

**New York**

Anthony Carpinelli
VP Revenue
+16465685357
anthony.carpinelli@holisticyber.com

**London**

Peter Cohen
Managing Director EMEA
+442038075355
peter.cohen@holisticyber.com

**Tel Aviv**

Ran Shahor
CEO
+16465685357
ran.shahor@holisticyber.com

# APPENDIX I – Scoring Methodologies

## Level two scoring – Environmental context and attack objectives

The Level two scoring methodology helps us to understand technical context and attack objectives in a way that is relevant and accurate to the organization. The weightings applied to each input should be tuned in accordance with your own priorities – our suggested starting points are laid out here. Once set, the weightings remain constant across each finding (and indeed all testing) to ensure consistency in scoring.

| Contextual Input | Code | Weighting applied |
|---|---|---|
| Network Segment | NS | 4 |
| Proliferation Degree | PD | 5 |
| Exploit Sophistication | ES | 4 |
| Staging Factor | SF | 5 |

With the weightings above, scoring can be calculated as follows, with the values for inputs NS, PD, ES and SF based on factors described in Fig 1 on page 7.

$$\text{level 2 Score} = \frac{(NS\ *4) + (PD\ *5) + (ES\ *4) + (SF*5)}{4+5+4+5}$$

## Level three scoring – Using business impact analysis

Level three scoring methodology takes level two scoring as above, and adds business impact analysis into the equation. In keeping with level two, business impact requires a standardized weighting as a category, against the environmental and attack factors already scored at level two.

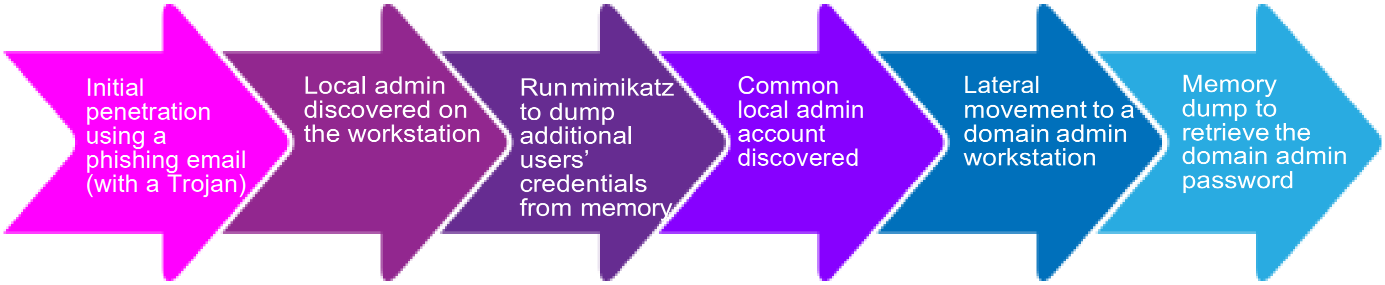
Here, we say that business impact is weighted to ‘3’, with environmental and attack factors weighted to ‘7’. As before, this should be tailored to your organization.

| Input | Code | Weighting applied |
|---|---|---|
| Level 2 scoring | Blue | 7 |
| Asset Value | AV | 3 |

$$\text{Level 3 Score} = \frac{\left(\frac{(NS\ *4) + (PD\ *5) + (ES\ *4) + (SF*5)}{4+5+4+5}\right)*7 + (AV*3)}{7+3}$$

# APPENDIX II – Case Study

The following example brings to life a series of penetration test findings which are scored in accordance with the Level 2 methodology, and uses the example input weightings as per appendix 1. The test scenario followed a common attack chain:


Initial penetration using a phishing email (with a Trojan)
Local admin discovered on the workstation
Run mimikatz to dump additional users' credentials from memory
Common local admin account discovered
Lateral movement to a domain admin workstation
Memory dump to retrieve the domain admin password

To enable a pragmatic approach to remediation than the initial technical scoring, findings were then calculated to level two in order to include environmental factors and attack objectives and capabilities.

## Findings and scoring

| **Finding: The email gateway filter is not sufficiently hardened, and allowed files with embedded malwares to pass** | | | |
|---|---|---|---|
| NS: **10** (the insertion of the embedded mail is enabled directly from the internet) | PD: **10** (the attack vector of a phishing mail with embedded malware is the most common vector in today's cyberattacks) | ES: **6** (creating a crafted Trojan require a certain level of expertise) | SF: **5** (upon breaching the GW the attackers can pursue their plan and possibly have more options to continue the attack) |
| **Total: (10*4+10*5+6*4+5*5) / (4+5+4+5) = 7.22** | | | |

| **Finding: Missing an internet proxy server that will monitor and filter all outgoing internet traffic (eliminating direct internet connection from internal workstations)** | | | |
|---|---|---|---|
| NS: **8** (the connection between the workstation should have been routed to the proxy in the DMZ) | PD: **7** (usage of meterpreter to remotely control the RAT while not rare, is not ubiquitous) | ES: **8** (using meterpreter requires some knowledge but not an expert level) | SF: **5** (the fact the adversary could use external C&C opens several options for the attacker to continue the attack internally) |
| **Total: (8*4+7*5+8*4+5*5) / ( 4+5+4+5) = 6.88** | | | |

| **Finding: Insufficient workstation hardening, missing a whitelist application enforcement (such as AppLocker) to prevent tools such as PowerShell and other tools that were used in the attack, from being run.** | | | |
|---|---|---|---|
| NS: **5** (internal network) | PD: **10** (usage of tools such as PowerShell is very common in such attacks) | ES: **8** (using PowerShell and other tools requires some knowledge but not an expert level) | SF: **10** (the attacker could use tools, scripts, key loggers etc. and basically pursue any direction) |
| **Total: (5*5+10*5+8*4+5*10) / (4+5+4+5) = 8.72** | | | |

| **Finding: Insufficient network segregation** | | | |
|---|---|---|---|
| NS: **5** (internal network) | PD: **10** (lateral movement is a common TTP of attackers) | ES: **6** (performing movement between workstation and servers requires a certain level of expertise) | SF: **5** (the adversary can move to any direction in the network as wished) |
| **Total: (5*5+10*5+6*4+5*5) / (4+5+4+5) = 6.88** | | | |