CYBER CITADEL

WHY PENTESTING IS ESSENTIAL FOR BUSINESS GROWTH

8 NOVEMBER 2022

CONTENTS

WHY PENTESTING IS ESSENTIAL FOR BUSINESS GROWTH

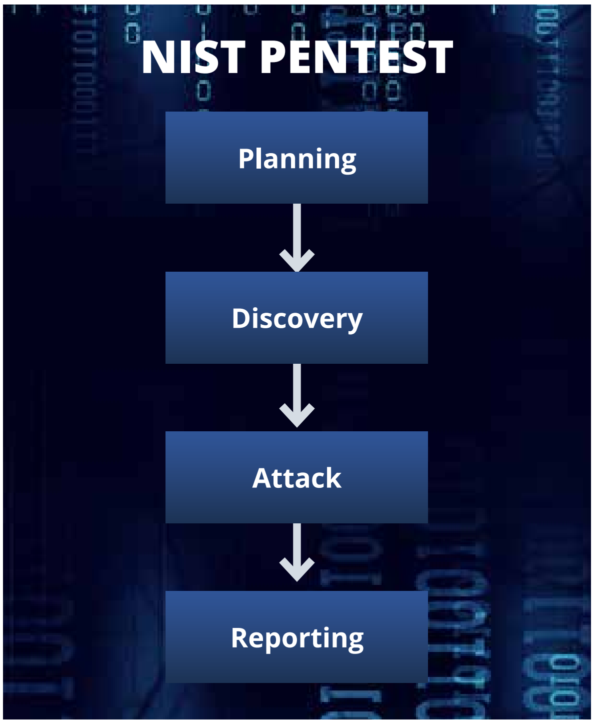
This article provides business leaders with a practical, concise, and informative guide to taking the most important step towards your digital security. The goal is to gain a good understanding of all you need to know about Pentesting to evaluate your network infrastructure and identify cybersecurity vulnerabilities.

What is a Pentest?

A Penetration Test (Pentest) is an investigation into a digital network to find and assess the severity of exploitable vulnerabilities. These tests aim to reveal how damaging a network security flaw could be in the event of a real cyberattack.

Vulnerability Assessment and Penetration Testing (VAPT) are two tests which go hand in hand. The former is often a comprehensive, automated scan of a network to detect security flaws, bugs, anomalies, and misconfigurations whilst a Pentest is best run as a *human-led* investigation and involves authorised attempts to gain access to network infrastructure, unauthorised data, user credentials, and potentially even take over the whole environment.

The NIST Pentest framework, part of the general [NIST Cybersecurity Framework](), outlines the phases of testing, and is a set of guidelines used by many professionals to instruct good Pentest practice.



What is the aim of a Pentest?

A Pentester is trying to find **vulnerabilities** in your information and security systems, as well as test your defences and security protocols. They succeed if they can take over a system from a web application, or steal privileged credentials from a mobile device, or gain access to unauthorised data. Anything in which the client loses control of their network or has data exfiltrated.

But a good Pentesting team won't stop there. Just because they have a golden ticket[1] doesn't mean there aren't other exploitable vulnerabilities, and they should continue to comb through your network to identify these and prioritise them in terms of their criticality.

Why do I need a Pentest for my business?

If assessing the ability of your security against the **risk of cyberattack and data breach** isn't enough for motivation, then also consider that it is the quickest, most efficient way to ensure compliance with all the latest cyber legislation and industry regulations. See our white paper – [A Guide for Board Directors]() – to understand how and why you should be engaging with cybersecurity.

▶ **Self-assessment.** Conducting a Pentest will essentially produce a security posture review of your

[1] A ticket is a digital object which allows nodes communicating over a network to prove their identity to one another. A successful golden ticket attack grants an adversary completely unrestricted access to a domain by forging tickets which disguise them as admin-level users.

digital network. This will help you identify, prioritise, and invest your time and money into solving the most pressing and risky security issues. A critical self-assessment is the best place to start in improving your cybersecurity.

▶ **Staying on top.** Pentesting enables companies to stay one step ahead of cybercrime. The quicker vulnerabilities are identified, the more proactive you can be in mitigating the risk, rather than reacting to network breaches when it's already too late. A good Pentesting team will use the absolute latest known exploit techniques against your network, making sure your business isn't left behind the times.

▶ **Compliance.** Australia introduced new cybersecurity legislation in 2022, with a focus on critical infrastructure. The date for compliance passed on 8 October – so find out what you need to do, and show that you are ready now. On top of regional legislation, stay aware of your industry obligations. Both Maritime and Air Transport associations have regulatory standards, and the energy sector has recently developed a security framework. Check out our white paper for information on the latest legal requirements.

▶ **Smart business growth.** Adopting new technology like IoT or AI support for supply chains drives productivity and increases growth. But doing so without considering the cyber risk will leave your company vulnerable to attack. Every extra device and layer of complexity creates a potentially exploitable vulnerability. Pentesting can ensure that your new ways of doing business are integrated securely, and don't leave any back doors open. Smart growth, the smart way.

▶ **Trust.** In today's marketplace, trust is everything. Pentesting proves your business is serious about cybersecurity. Complying with regulations and getting certified, for example with the Australian Trusted Trader scheme, gives your clients confidence in your services, especially when it comes to handling their data. Cultivating trust in your organisation will improve your reputation and help beat off competition too, so it's a win-win.

How thorough is a Pentest?

A full Pentest will look at every connected device and every network node, from web and mobile applications to the unseen interfaces between software behind the scenes (APIs). But a good, human-led Pentest by experienced professionals will go far beyond this. They will test your staff for susceptibility to social engineering, and use business logic to inform their attempted exploits. A properly performed Pentest should assess **people** and **processes**, as well as the technology.

Business logic is not understood by automated scanners, even when it comes to just **Vulnerability Assessments**, since they don't have a strong perception of data flow in business. For example, they cannot see if one vulnerability leads to another, or if a vulnerability is irrelevant because of a security protocol upstream or downstream in the data flow. This leads to lots of false positive results, and the generation of a huge, mostly useless security report which no one in your business has the time to go through. That is, ultimately, what you pay professionals for.

What does a successful Pentest look like?

If a Pentest reveals very few vulnerabilities and even fewer exploits it was not successful. The **cybercrime landscape** moves too fast for companies to be that secure and any team revealing only a few flaws is either not testing the full scope of the network, not using the latest most appropriate tools, or are themselves inexperienced.

A successful Pentest should provide you with a **comprehensive but concise report of all the discovered vulnerabilities** and their potential to be exploited, with false positives filtered out. It should assess the risk of these vulnerabilities in the context of the company, and prioritise them based on criticality. The report should also outline remediations and recommend mitigation measures against the outlined vulnerabilities and exploits. These should also be prioritised.

Should you use Cybersecurity experts to provide a Pentest?

Ideally a third-party specialist security provider such as Cyber Citadel should carry out your Pentest. There are two reasons for this:

1. Testing is a specialist service, and the level of expertise, experience, and access to the latest tools that a security provider will have will far outweigh any in-house team.

2. It is easier to identify problems and critically assess a network from the outside looking in. It is also closer to reality if an external team assesses the network *including* your active IT department – an internal test would be run by them.

▶ Cybersecurity experts are different from IT experts

The former specialise in uncovering and assessing risk, vulnerability, and susceptibility to exploits. IT experts are experts in setting up, repairing, and maintaining systems, and organising the flow of data within an organisation. Unlike IT departments, **cybersecurity experts** have years of experience in deploying Pentests and are therefore more equipped and less likely to disrupt our networks by causing accidental downtime, system crashes, or denial of service (DoS). To understand more about the specialist skills required for Pentesting, watch our video online.

▶ Cybersecurity experts won't rely on automated scans

As discussed, automated scans are a fine place to start but return false positives and don't understand business logic or test the people in an organisation. Real experts *will* do all of this. They also look at the real-world impact of vulnerabilities when prioritising. For example, they might look at the business sector, location, or legislation requirements, and they will also consider the latest trends in cybercrime within your industry.

▶ Cybersecurity experts will provide support

Cyber Citadel categorise findings from their report and write them up in language that is understandable by the intended reader, whether that be the directors board, the IT department, or non-IT staff. On top of this clear report with prioritised and risk assessed vulnerabilities, Cyber Citadel suggest practical solutions to mitigate the risk, and offer ongoing support in implementing any suggestions.

How do I find a good Pentest provider?

To find the right Pentesting team, here are a few rules to go by:

▶ Look at the Pentesting team

Are they diverse and experienced? Cyber Citadel have world class multinational cyber security researchers, with different areas of expertise. The team should consist of more than one researcher, ideally four or more, each with a different area of expert knowledge such as in web applications, hardware tools, source code, API to name a few. **One team member should be a project manager**, who is able to put the test into the context of the business and document them in a useful way for that business. A global team is also useful, as this means testing across time zones and in different languages is possible.

Have the team members been **contributing to the cybersecurity research community**? Testers at Cyber Citadel are active cybersecurity researchers. They have designed modules for commercial vulnerability scanners such as Metasploit, contributed to opensource software, and added their Pentest findings to the database of Common Vulnerabilities and Exposures (CVEs)[2]. A team's contributions to the cyber community will indicate their experience and knowledge of the current cybercrime landscape.

▶ Look at the Pentest output reports they provide

One of the core values of a human-led, third-party Pentest is the report produced at the end. It should have **no false positives, no false negatives**, and the vulnerabilities should be prioritised and tailored to your business

[2] CVE is a database of publicly disclosed information security issues, each of which is assigned an identity number for referencing purposes.

type. At Cyber Citadel, the teams also perform a risk assessment alongside the Pentest so that the criticality of a vulnerability also depends on the risk associated with your business and your sector. This is something many providers don't do.

A good Pentester will also offer ongoing support, rather than provide a one-off test. At the least they should provide direction on implementing their own recommendations, and ideally offer some form of continuous support for any new applications or devices being added to the network.

▶ Ask about their Pentesting tools and checklists

A good Pentesting team of experienced researchers will use a combination of commercial scanners alongside their own custom toolkits for vulnerability assessment. If they just list off some well-known tools, even if they are good ones such as Metasploit, this is a red flag.

Checklists should always be measured by the number of tests, not the amount of time. A Pentest provider can offer you a shorter test for less money, and claim that they will still cover everything, but this doesn't add up and likely means you are just reducing the amount of testing. Ask about checklists and frameworks that the testers will use. Good testers will start with gold standards such as the OWASP Top Ten which represents a broad consensus on the most critical security risks to web applications, and then will move to other checklists such as SANS 25 which lists the most dangerous programming errors.

How can I make the most of Pentesting for business growth?

Be prepared. It's not just the Pentesting team that needs to prepare themselves; there's plenty that clients can do too, and both sides preparing together will maximise the efficiency of the testing. This can help keep the cost down by reducing delays and increasing the rate of network coverage.

TASK	REASON
Ensure systems are up to date.	Testing outdated systems wastes time.
Check network is running normally (systems, domains etc.).	Systems down will either not be tested, or time will be wasted getting them up and running.
Run a checklist against existing security practices such as patching and backing up.	Patches ensure the team are testing the latest security protocols and don't flag patch requirements you already know of. Backing up keeps all your data safe during the testing process, and also enables back-up comprehensiveness and security testing.
Ensure endpoints (devices accessing the network) are live and working.	One of the goals of testing is to make it to the endpoints, if they are off, faulty, or inaccessible, a full test cannot be run.
Check all credentials are working	If Pentesters manage to steal credentials but these are out of date, then it doesn't represent the real-world scenario
Plan with your Pentesters	Everyone needs to be on the same page when it comes to the scope and timing of the test

Remember that this is a real-world test, so having all your systems available and connected will best reproduce the scenario likely to be facing an adversary.

Engage with the Pentesting team. Before testing even begins, the scope for the test needs to be clear, well planned, and both client and test team need to be on the same page.

▶ When will the Pentest be run?

Discuss with the Pentesting team how best to capture your 'working' network. For most businesses there will be core hours, when the network is heavily used, data traffic is at capacity, and there are many active endpoints. This is a workday for most businesses, and ideally this would be when testing is run. If that's not possible, then discuss how best to put your network infrastructure to the test – you don't have to test your network live.

You may also want to consider more unusual hours, for example if you work across different time zones or have staff that work remotely. Testing quiet times can be beneficial too, because attacks outside of hours might occur through different means and can lead to delayed responses resulting from fewer staff.

▶ What variant of Pentest will be run?

White box = Normally for a specific test case. A large amount of information is provided about that case to thoroughly unpick its security.

Black box = No information given to the testing team other than company name and an IP address range. This test type most closely simulates the scenario faced by a real adversary.

Grey box = Some, often limited information given, usually a start point from which to launch an attack on the network. This is the most common test type for a general network assessment.

Blind black box = Single blind means the company name is the only thing given to the Pentesting team. A double-blind black box is where the company security team also has no information on the Pentest. This means the company can't prepare itself for testing and the company's security posture is really revealed for what it is.

Some business directors might be tempted to choose a black box approach to 'let the experts get on with it' but, again, engagement is key and this may not always be the best way to get the most from Pentesting. **Cybersecurity experts will always find some way in**, but a more fine-tuned approach and less brute force may be more revealing when it comes to assessing the security posture of an organisation. This is where grey box testing can really show strength.

Remember, every business, in every sector will be unique. There is no one-size-fits-all approach to cybersecurity.

▶ What will the scope of the Pentest be?

Time must be spent with the testers mapping out the scope. Scoping maps network complexity which helps to avoid system blind spots, inaccessible endpoints, outdated credentials, but most importantly lays out the expectations of the Pentest and how much (if not all) of the network will be tested.

Scoping also sets out a template for logging and report writing, to make sure everything is covered in the output. Good scope logging is essential for reviewing and improving the test for next time.

Even with Black Box Pentesting scoping is important, though of course it will be more one-sided. In Black Box scenarios it is even more important that the company prepares as best it can, and that the testing team logs their testing – sometimes things are found on a network that company IT staff didn't even know were there. This can be especially true for older companies operating legacy systems.

Don't worry if you don't really know your full scope. Scope, or asset, discovery to **determine the extent of your network** is always the first stage of a Pentest anyway, to double check for things the company might not know about. And a good Pentest provider such as Cyber Citadel will sit down with you and fill in the gaps, and help you decide what needs to be included.

What does a Pentest cost?

The larger, more complex the network (see video), the more time and money is required to run a Pentest. At Cyber Citadel, we will provide you with an estimate of the cost **based on the scope drawn up and a personalised test checklist**. This will be converted into a number of testing days. Whilst it is not advised to reduce the scope to save money, Cyber Citadel understands that every business has its budget and will be upfront about the amount of scope your budget will cover. Cyber Citadel also offers a one-time free re-test once you have implemented the recommended remediations. This would normally be an additional cost to consider.

Some advice from the experts:

- Don't be fooled by providers offering cheap Pentests due to short lead times – this just means they are testing less.
- Remember that time and money can be saved with good preparation, planning, and scope mapping. It may also be possible to reduce the lead time of a Pentest by changing the test type and providing more initial information.
- Consider what is most important to your business. You might handle lots of customer data, rely heavily on network connections to supply chains, or operate a remote workforce. **Understanding your priorities** can help a provider to reduce the scope in a way that doesn't place your most critical assets or operations at risk.
- Finally, whatever the cost is, a data breach will likely cost your company far more.

How often do I need to run a Pentest?

As often as possible.

The minimum frequency will depend on the business and how often you update or add software, or expand into new regions acquiring new clients and partners. Many factors can contribute and there is no exact frequency, though Cyber Citadel recommends **Pentesting twice a year**, or after any major release, update, or roll out of new software or protocols.

In-between big, external Pentesting companies should run internal Pentests or, at the very least, Vulnerability assessments. This will help you stay on top of obvious network flaws and help inform you when to plan your next external Pentest. Many companies dedicate a certain number of hours per month or days per year to VAPT, and this can be a positive way to improve your cybersecurity planning culture and polices.

Can things go wrong?

Rarely. Professional Pentesting teams do their research and understand the nature of your business and the potential effects of interfering with your network. Again, **engagement is key**. The scoping document completed beforehand will inform the team if there are particularly sensitive parts of the network, for example parts involved in an active supply chain or a production line. You can even request for a team not to interfere with network segments if you are really concerned.

This is why you need a human-led investigation. Real, human experts will know not to use scanners and other automated tools on sensitive networks where accidentally triggering an event could have real effects on a business. In addition, **experts can ensure that no data loss occurs** and that any effect on your business is immediately communicated to you.

What happens after a Pentest?

After testing, you will read the security report and understand what your vulnerabilities are and if they were exploitable. As we've said, a good service provider will have prioritised these vulnerabilities and exploits according to an accompanying risk assessment specific to your company and the business sector. Scoring metrics such as the Common Vulnerability Scoring System (CVSS) may be used to represent a measure of severity, and the latest version of the CVSS system ranks vulnerabilities as Low, Medium, High, or Critical.

Introduce remediations for security issues as quickly as possible. The Cybersecurity and Infrastructure Agency in the US suggests remediating all critical vulnerabilities within 15 days. However, Cyber Citadel strongly recommends **that actively exploitable critical vulnerabilities are addressed within 24 hours**. All other high priority vulnerabilities should be remediated within 30 days.

Within 30 days, request a re-test. Within this time, having implemented remediations and mitigations, you need to check that these have successfully solved your security issues. This re-test is included within many Pentest fees, and as previously stated comes free with Cyber Citadel Pentesting.

What is Red Teaming?

Red Teams play an adversarial role and attempt to break into a target network

Like Pentesters, they are experienced cybersecurity specialists bringing together a deep understanding of the structure and behaviour of networks as well as security testing and system compromise. Red Teams launch offensive operations aiming to simulate a real, multi-layered attack to reveal network vulnerabilities, particularly to new and sophisticated techniques.

These attacks are designed to mimic real cybercrime as best as possible

The attacking team will have no prior knowledge of the target network, and the response team will have no information on the attack. However, no real damage will be caused to an organization's network infrastructure and no data will be lost permanently. The teams use frameworks such as Mitre Attack, which is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations, to test your defences against the latest developments in cybercrime.

Red Teaming also acts as a training exercise for your security provider, whether they are internal or external

The defending team is known as the Blue Team. There is usually also an Orange Team too, whose role it is to keep in constant communication with the Red Team and the company IT department and directors. This is so that if a breach occurs and triggers an incident response, you can immediately determine if this is a result of the Red Team or a genuine security breach.

Is Red Teaming for me?

Red Teaming goes beyond VAPT

Red Teaming is the closest you will get to simulating a real cyberattack. However, it isn't just about getting in: Red Teaming will also provide the comprehensive reports and assistance that you get with Pentesting, and will also help your Blue Team to improve their techniques. Whilst a Black Box Pentest might appear similar to Red Teaming, remember that Pentesting is there to assess your network security, Red Teaming is there to put it to a real-life test, using techniques used by real hackers, ransomware operators, and other cybercriminals. It isn't limited by a scope or a particular goal; it tries any way possible to breach your network.

Red Teaming requires resources

Red Teaming is only worthwhile if you have the security resources and setup to benefit from it. Many small and medium sized business will not have the necessary capabilities to form a blue team because their security relies mostly on automated systems or is entirely outsourced (i.e. they have no internal security specialist). However, if you are a larger enterprise, are part of critical infrastructure, or operate systems of national security, you really should consider testing your security with Red Teaming, and in this case if you don't feel you have the resources you should look at investing in them.

Red teaming is expensive

We would be lying if we said this would be cheap. This is another reason to carefully consider if you will benefit from it. The benefits can be great, just make sure they will be for you. A good security provider such as Cyber Citadel will always works with you to make sure you access the services that will benefit you the most.

For a broad overview of Red Teaming and why you need it, see our video Why You Need Red Teaming: Elite Threat Intelligence.

ACKNOWLEDGMENTS

Thanks to Jonathan Sharrock, CEO of Cyber Citadel, for his insight into Pentest project management and supply of client feedback. Thanks also to Rafay Baloch for his technical expertise in running Pentests and Red Teaming exercises.

PENTEST CHEAT SHEET

What?

- An investigation to find and assess exploitable vulnerabilities
- Involves attempts to gain access to a network including data and credentials
- Aims to reveal how damaging network security flaws could be

Why?

- Self-assessment
- Staying on top
- Compliance
- Smart business growth
- Trust

Who?

- Specialist third-party provider with a team of cybersecurity experts
- A team with diversity and experience, who are active researchers
- People with access to commercial and custom toolkits
- People who give back to their community

How?

- Be prepared – use the table as a checklist
- Engage with the Pentest team: determine when the test will run, what variant of Pentest, and what the scope is
- Plan for future testing as part of cybersecurity policy

How much?

- Think tests, not time
- Cost depends on scope, test type, and your business-specific priorities
- Plan more to save more – don't let testers waste time
- Whatever the cost, a data breach will cost you more!

CYBER CITADEL

Cyber Citadel

Jonathan Sharrock

jonathan.sharrock@cybercitadel.com

www.cybercitadel.com

Cyber Security specialists

With highly-satisfied clients in over 26 countries across 5 continents, we provide Penetration Testing, Vulnerability Assessments, Red Teaming, Incident Response, Malware Analysis, Asset Discovery, Source Code Review and Forensic Analysis. We have particularly deep expertise in multi-lingual Web Application and Network Infrastructure Penetration Testing.