Guide to Penetration Testing

What to consider when testing your network

HALKYN CONSULTING

06 May 11

T Wake CEH CISSP CISM CEH CISSP CISM

Introduction

Security breaches are frequently in the news. Rarely does a week go by without a report of hackers compromising an insecure computer network and placing customer details at risk. Often, the actual damage is minimal, but for the companies involved the reputational damage (as well as legal action in some cases) can be crippling. Even the largest brands can take years to recover customer confidence and smaller businesses are likely to never resurface.

Information technology is a great business enabler, and with the internet your business can trade anywhere on the planet opening up a huge market. But all this carries risks.

Part of the problem is working out exactly what the risks you face are and this is where a **penetration test** comes in.

Whatever your business, whatever your industry and whatever your size, if you use IT systems then you should consider carrying out a penetration test to see what risks you face and find out what the hackers can do to you before they do it.

This guide is provided by Halkyn Security Consulting to give an overview of what a penetration test is and what you can do and what you should look for in a testing company. Halkyn Consulting **is not** a pentesting company and we seek to provide completely independent advice to assist businesses of all sizes identify, quantify and mitigate the risks they face.

What is penetration testing and why do I need it?

These are the two most common questions people ask about penetration testing (pentesting) and, unless you are already heavily involved in IT systems development you may not have heard the phrase before.

Pentesting goes by several names but broadly speaking they all mean the same thing. You may hear terms like “vulnerability assessment” or “technical risk assessment” or “technical security audit.”

Simply put, a pentest is a way of checking the security of an IT system or network, by doing all the things a hacker would do. Depending on what you ask the pentesters to do this can range from them trying to sneak past your receptionists, probing your internet site to accessing your back-end databases.

As part of the process, the pentesters (sometimes called “Ethical Hackers” or “White Hat Hackers”) will run through combinations of known vulnerabilities which are often exploited by hackers to compromise systems – such as in the attack on the **SONY PLAYSTATION NETWORK**. Depending on the pentest company, and your requirements, they may also be able to work with you to identify threats which are not yet public knowledge.

When the testing has finished, you will be presented with a report identifying any vulnerabilities in your systems and giving advice on what should be done to close any gaps. A good pentest company will provide you with information on the likelihood of a weakness being exploited and the damage this could cause, but often this will fall to your security staff to assess.

Once completed, the findings of a penetration test, and any remediation activity you may undertake, can be presented to your shareholders, or other key stakeholders, as evidence that appropriate levels of security are in place. Additionally, depending on the nature of your business, a penetration test may be a regulatory requirement – such as if you handle credit card data.

Most importantly, by carrying out a proper pentest, and following through to remediate any relevant findings, you can prevent financial loss to your business, loss of reputation for your brand and retain customer confidence that you are looking after their data.

What can I test?

Pretty much anything you want.

Depending on who you use as a testing company, you can examine how you control visitors to your site, what your staff training is like, what applications you have running, what developments you have underway and much more.

From a technical point of view, you want to consider testing your computers, databases, Wi-Fi, wired networks, staff awareness and information disposal.

A good pentest will be driven by your own risk assessments, so you should already have an excellent understanding of where your priorities lie. If you are in anyway unsure here, Halkyn Consulting provides a dedicated risk assessment service which can work with your business to establish a realistic risk assessment.

When it comes to deciding what you want as the scope of your pentest then it is worth taking an outside-in approach. Begin with anything that has a public facing connection – such as e-commerce sites and email systems then work in to things that need physical access.

If you are in a regulated industry, or subject to standards such as PCI-DSS, then you may not have as much latitude when it comes to deciding what you need to test.

How do I pick a testing company?

Like any industry, there are good and bad testing companies out there, added to which testing companies often have varying strengths and weaknesses so it is important that you have a good idea of what you want before you go out to tender.

At a fundamental level, you must choose a testing company who can provide a test to the standard you require. For example, if you are carrying out a test to meet PCI-DSS requirements, then the testing company must be properly accredited by the PCI-Council.

Equally important, you should ensure that the testing company are independent of the company that installed (or supplied, or maintains) the systems being tested. If you don't ensure this separation then the test results can never be properly trusted.

Once you have got past the basics, some additional questions you may want to consider are:

- What do their reports look like? Can they provide you with a sample?
- Do they do their own research?
- What certifications do their testers hold? (Make sure this is actually the people who will do the test, not just certifications held by people in the company)
- What insurance do they have? Is it sufficient to cover you in the event of something going wrong?
- Are legal agreements in place to protect you if they are negligent in any way?
- What are their confidentiality policies?
- What security certifications and accreditations do they hold as a company? (ISO 27001 is the main one to look for here)
- Do they have any references? (Often this will be hard to get as confidentiality issues may arise, but it is worth asking).

Remember, the test is on your terms and whatever the company produces has to be of use to you. Make sure you are fully satisfied with the testing company before you commission their services.

One other thing to consider – testing should be done on a regular basis but make sure you change testing companies. If you keep using the same ones, there is a risk that complacency may set in or that familiarity will lead to gaps in the assessment.

What standards are there?

There are lots of security standards available for testing companies to use. The three most common ones are:

PCI – DSS: This is the "Payment Card Industry Data Security Standard," established in 2004 to control how payment card (credit card) data is protected. The PCI-DSS process will determine what elements need testing and set the criteria that the testing company will follow.

OSSTMM: This is the "Open Source Security Testing Methodology," and is the result of a collaborative effort to develop a standard for security testing. This standard details a thorough testing process that ensures all technical aspects of a system are properly assessed.

CHECK: This is the "CESG IT Healthcheck," and is often mandatory for systems connecting to UK Government infrastructure. CHECK has, in recent years, become the UK standard for pentesting and there is a rigorous process that practitioners must follow to achieve certification. **Note**: If you request a CHECK test, the results will be sent to CESG.

What do I do after the test?

First off, read the report and ask the testing company to clarify anything you don't fully understand.

If there is anything you are unsure of, or if you want independent advice on what the findings mean for your business then you can consider bringing in a separate security consultancy.

Once you are happy with the contents of the report you need to carry out a risk assessment to determine what findings are worth remediating and in what order you should fix things – it is unlikely you can fix everything at once.

Ideally, the pentest report will give you an idea of what is high risk and what isn't, but a lot of this will depend on how your business processes work so don't be afraid to set your own ratings. However, if you do decide to downgrade a risk in the report, make sure you have the full support of all key stakeholders in case you make a mistake. If you are going to ignore recommendations from the pentesting company, you are unlikely to be able to hold them liable for any subsequent breaches.

After prioritising your risks, it is time to develop a project to deliver the changes required to remove the risks. Depending on the nature of the problem this can take some time and it may be worth seeking the advice of external consultants to assist with the process.

Once you have finished all the remediation, then get a new pentest to make sure.

Halkyn Consulting have specialist advisors, experienced in working with businesses of all sizes to remediate pentest reports. If you have information assets of any type, then send an email to info@halkynconsulting.co.uk to arrange a no-obligation discussion on how we can help you protect your business and reassure your stakeholders.

Provided by

Halkyn Consulting Ltd

Specialist Security Consultants

For more information on how we can help you improve your security, visit us on the web at www.halkynconsulting.co.uk or send an email to info@halkynconsulting.co.uk and we will be in touch to discuss your needs.

As a fully independent consultancy, we are able to assess what measures best suit your requirements from a range of vendors to ensure that you get cost-effective security that fits your business.

We are experienced in advising and assisting all size of business protect their assets, reassure their customers and win new contracts based on their enhanced security posture.

Using SC cleared consultants with internationally recognised qualifications we are able to assess your security against a range of standards and work with our clients to ensure that the most suitable ones are applied.

Based in North Wales, we are able to work with clients anywhere in the world and, through on-site visits and assessments we ensure that all our advice is based on realistic, credible, threat assessments based on the local situation.

Our services will help your business grow, win new business and protect its assets and reputation in a changing world. Get in touch today.