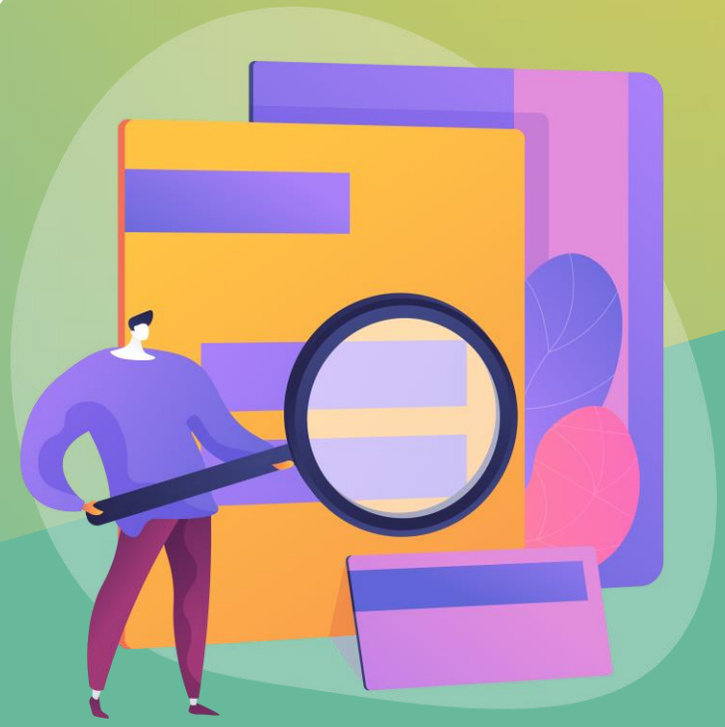
A Penetration Testing Checklist for

Finding Cybersecurity Risks



proarch

proarch

What is a Penetration Test?

Penetration tests are simulated real-world attacks done by ethical hackers to find gaps in the environment so they can be fixed.

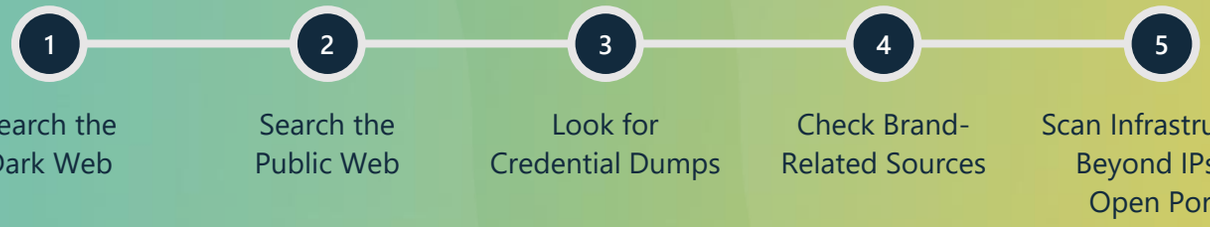
proarch

Most organizations rely on vulnerability scans and monitoring tools to alert them when there is a change in the network—and that's it. They're only looking for network-based exposures in services, ports, IP addresses, etc., not accounting for the continuously evolving dynamic of today's work environment.

Employees accidentally—or purposefully—exposing sensitive data, credential dumps on the dark web, and brand impersonation attempts all need to be considered for a true measurement of organizational risk.

The actions in this checklist are some of the ways ProArch's pen testers find weaknesses when performing penetration tests (pen tests). Automated tools and scanning are an important part of pen tests, but attaining a more accurate read on risk requires thinking and acting like a hacker.

Follow the steps in this checklist and make sure they are included in your next pen test to find weaknesses, vulnerabilities, and mistakes before a bad actor does.



1

Search the Dark Web

> Clients are always surprised that we found sensitive company information on the dark web. Penetration tests focus on how to pull that data out and determine the areas of concern that need to be addressed.
>
> **Michael Wurz**
> Security Consultant
> & Lead Pen Tester

The dark web can hold information like leaked employee credentials, sensitive data, proprietary source code, and details about vulnerabilities in the company's systems. Data breaches, hacking incidents, insider threats, or unauthorized access to internal systems can all lead to this type of information ending up on the dark web.

A word of warning, though: Accessing the dark web is dangerous and should only be completed by those who are familiar with it and using well-known services; otherwise, it could put you at even greater risk.

However, there are methods to carefully access the dark web and specialized monitoring tools that can be used to **search for dark web chatter of your brand, executives, credentials, external exposures, or potential vulnerabilities**.

2

Search the Public Web

> We do both automated and manual public web information gathering in our pen tests. Threat Intelligence solutions play a big role in finding leaked information and keeping up with what attackers are doing.

Michael Wurz
Security Consultant
& Lead Pen Tester

Information that can help attackers identify potential entry points and exploitable vulnerabilities can be found on the search engines we use every day. **Do a thorough review of public websites, your company website, social media platforms, online forums and blogs, and public databases for what information is out there related to your brand.**

It's not always as straightforward as a PDF with client information that has public access by mistake. A motivated attacker is creative and persistent. Let's say they are trying to gain physical access to your facility. Based on pictures shared by the company's LinkedIn profile, they can see what attire employees wear and the badges they have. That type of intel makes it possible for the attacker to blend in and look like any other employee.

This is a rare situation, so you do not need to tell marketing to take all the photos down. But it can and has happened. **It's important that the people who regularly share information publicly understand the risks and that the needed safeguards are in place to prevent a breach**—especially if you have strict regulatory requirements and handle highly sensitive data.

3

Look for Credential Dumps

> If I find your credentials, I'm going to reuse them across third-party sites and company login portals to try and find a way into the network or uncover sensitive data. It almost always works.
>
> **Michael Wurz**
> Security Consultant
> & Lead Pen Tester

Compromised third-party sites can jeopardize your security without you even realizing it. **Employees use their company email address to sign up for all types of third-party sites.** When a third-party service is compromised, which is happening more and more often, the credentials tied to them can be shared across the public or dark web.

A big concern arises when employees use the same password as their business account. It's even worse if the account has any type of elevated privileges or access to sensitive information. Websites like Have I Been Pwned are a good start if you don't have other skills in house. **Good account monitoring and security awareness training can help with this.**

4

Check Brand-Related Sources

This is similar to checking the dark and public web but specific to your business name and domain. Be sure to monitor social media profiles or websites that may be impersonating your brand.

Check online platforms and discussion forums for any mentions of your brand and related vulnerabilities. It could be chatter from an attacker indicating an attack is about to occur or an ex-employee discussing sensitive business information in their personal blog.

Checking brand-related sources can provide you with valuable information about the public perception of your organization's security posture.

> When a company is being talked about on the dark web, that usually means an attack is going to or has already occurred.
>
> **Michael Wurz**
> Security Consultant
> & Lead Pen Tester

5

Scan Infrastructure Beyond IPs & Open Ports

> If you're only scanning IPs and open ports, you're missing critical vulnerabilities that are likely present in your digital infrastructure.
>
> **Michael Wurz**
> Security Consultant
> & Lead Pen Tester

IP-centric scanning can miss vulnerabilities across your digital footprint, including those hosted on external-facing web applications, cloud services, or third-party applications. **You need to review all your organization's domains in use, active subdomains, DNS records, owned IP space, and cloud resources as a starting point.**

External-facing web applications are often accessed through specific domain names rather than IP addresses. Similarly, cloud providers often use dynamic IP addressing, and services are accessed through domain names.

Just like IPs, you need to widen your attention beyond open ports. And while open ports are a risk and should be addressed, you need to go a step further and investigate services, configurations, and applications in use.

proarch

The actions in this checklist are some of the methods ProArch's pen testers utilize to uncover weaknesses that bad actors could use against you.

When conducting a pen test, whether you do it yourself or utilize a third party, it's important to look for what can turn into a problem, check public information sources, study attackers' tactics, and apply an understanding of compliance requirements, complex environments, and market situations to each exploit.

Securing today's interconnected and complex IT environments requires creative thinking and an advanced skill set. ProArch can help you get a deeper understanding of the risks facing your business and build a cybersecurity plan to make risk more manageable.

LEARN MORE →

ProArch was founded on the belief that a future where change is 'business as usual' is fundamentally more exciting than one where it is not. We accelerate value and increase resilience for our clients with consulting and technology—enabled by cloud, guided by data, fueled by apps, and secured by design.

United States • United Kingdom • India