Free career resource · Building evidence

Cyber security portfolio projects for beginners

A cyber security portfolio is a small set of written-up projects that show what you can do. Two or three good projects, matched to the job you want, beat a long list of courses. Each write-up should explain the goal, what you did, what you found and what you'd do next. Only ever test systems you own or have permission to test.

By the Cyberend team · Published and updated 22 November 2026

THE SHORT ANSWER

- **Quality over quantity:** two or three projects you can explain in an interview are enough.
- **Match the job:** a SOC applicant should show investigation, a GRC applicant should show risk and policy work.
- **Write it up:** an unexplained project is nearly invisible. The write-up is what employers read.
- **Stay legal:** testing a system without permission is a criminal offence in the UK legislation.gov.uk.

Why a portfolio helps

Most entry-level applicants list the same courses. A project shows something a certificate can't: that you can set something up, investigate it, make sense of what you found and explain it clearly. Those are the everyday skills of most security jobs.

It also gives you better interview answers. “Tell me about a time you solved a technical problem” is much easier when you can talk through a lab you built yourself.

Stay on the right side of the law

Only test what you own, or have written permission to test

Under the Computer Misuse Act 1990, accessing or interfering with a computer system without permission is a crime, even if you mean no harm legislation.gov.uk. That includes scanning your employer's network, your school's Wi-Fi or a website “just to see”.

Use your own virtual machines, deliberately vulnerable practice apps such as OWASP Juice Shop, and platforms built for practice. If a platform asks you not to publish answers to its challenges, respect that.

Eight project ideas

Pick two or three that match the kind of role you want. Each one can be done with free tools.

SOC

Build a home lab that collects logs

Run a Windows and a Linux virtual machine in VirtualBox, send their logs to a free tool such as Security Onion, then create a burst of failed logins and show how you'd spot it.

SOC

Investigate a phishing email

Take a phishing email from your own inbox and, without clicking anything, examine the sender, headers and links. Write a short report: what gave it away, and what you'd advise a colleague to do.

SOC or networking

Explain your own network traffic

Capture a few minutes of your own browsing in Wireshark and explain what you see: DNS lookups, connections being set up and encrypted HTTPS traffic.

SOC

Write up a blue team challenge

Complete a free investigation challenge on a platform such as CyberDefenders, then explain your method in your own words. Check the platform's rules on publishing first.

GRC

Assess a small business against Cyber Essentials

Invent a 20-person business and check it against the government-backed Cyber Essentials scheme NCSC: what passes, what fails and what you'd fix first.

GRC

Write a starter policy pack

For the same business, write one-page policies on passwords, acceptable use and reporting incidents, in language staff would actually read.

Cloud

Lock down a free cloud account

Open a free-tier account with AWS, Azure or Google Cloud, set a budget alert first so you can't be charged, then turn on multi-factor sign-in and logging, and document a hardening checklist.

Testing

Find and fix flaws in a practice app

Run OWASP Juice Shop on your own computer, find three vulnerabilities, and for each one explain how it works, why it matters and how a developer should fix it.

KEY TAKEAWAY

The fix and the explanation matter as much as the finding. Employers want people who can tell others what to do about a problem, not just spot it.

How to write a project up

Keep each write-up to a page or two, with screenshots. A consistent structure makes them quick to read:

WHAT EVERY WRITE-UP SHOULD COVER

- [x] The goal: what you set out to do, in one or two sentences
- [x] Your setup: the tools and environment, so someone could repeat it
- [x] What you did: the main steps, with screenshots
- [x] What you found: the result, and what it means
- [x] What you'd do next, or do differently
- [x] What you learned

DO

- ✓ Explain your reasoning, not just the commands you typed
- ✓ Admit what went wrong and how you worked around it
- ✓ Remove passwords, real IP addresses and anyone's personal data

DON'T

- ✗ Copy someone else's walkthrough and call it yours
- ✗ Publish answers to challenges where the platform asks you not to
- ✗ Include anything from a system you didn't have permission to test

Where to put it

GitHub

A repository per project with a clear README. Good for anything with scripts or configuration files.

A simple blog

A free blog or a basic personal site works well for longer write-ups with screenshots.

LinkedIn

A short post summarising each project, linking to the full write-up. Recruiters do look.

Then link your best two or three from the projects section of your CV. Our **cyber security CV guide** shows how to describe them, and our **interview guide** covers how to talk about them.

Common questions

How many projects do I need?

Two or three good ones, matched to the role you want. A short, clear portfolio is better than a long list of half-finished ideas.

Do I need to be able to code?

Not for most of these projects. Basic scripting, such as a little Python or PowerShell, helps in many roles, and a small script that automates part of a project is a good addition once you're comfortable.

Can I use rooms from TryHackMe or Hack The Box?

Yes, as practice and as the basis for a write-up in your own words. Check each platform's rules first, as some ask you not to publish answers to active challenges.

Does a home lab cost money?

Usually not. VirtualBox, Security Onion, Wireshark and OWASP Juice Shop are free. A computer with enough memory to run two virtual machines at once is the main requirement. With cloud accounts, set a budget alert before you build anything.

Sources and method

The project ideas are based on the skills UK employers ask for in entry-level adverts, as covered in our other guides, and on the free tools and practice environments listed in the Cyberend beginner roadmap. The legal position is from the Computer Misuse Act 1990.

The examples are illustrative. Your write-ups should describe what you actually did.

---

legislation.gov.uk: Computer Misuse Act 1990 Official guidance

The UK law that makes accessing or testing computer systems without permission a criminal offence.

National Cyber Security Centre: Cyber Essentials Official guidance

The UK government-backed scheme setting five basic technical controls for organisations.

Every figure and link in this guide was checked against its source on 22 November 2026. Live job listings update every few hours.

This is a PDF copy of a free Cyberend guide. Read it online, with today's live UK cyber security jobs, at cyberend.io/resources/cyber-security-portfolio-projects.