Cyber Security Toolkit

19 free tools in 5 layers. Start with the yellow one in each layer.

SAVE THIS · START WITH YELLOW 19 TOOLS

1 Scan + Map

see what is on the network

- **Nmap** START nmap.org ↗
  Scan scanme.nmap.org (Nmap's own practice target) and read which ports are open.
- **Wireshark** wireshark.org ↗
  Capture 60 seconds of your own Wi-Fi, filter for dns, and see every site your devices reach.
- **Shodan** shodan.io ↗
  Make a free account (results are capped) and see what one exposed server reveals about itself.

2 Detect

catch the attack in the logs

- **Wazuh** START wazuh.com ↗
  Install it in a VM, add your laptop as an agent, fail a login 5 times, then find the alert.
- **Splunk** splunk.com ↗
  60-day trial, then a free licence (500 MB a day). Upload a log file and search for failed.
- **Elastic** elastic.co ↗
  Run Elasticsearch and Kibana, load some logs and build one chart of failed logins.
- **Security Onion** securityonionsolutions.com ↗
  A whole SOC in one free install. Run it in a VM on your home network and read what it flags.

3 Attack (in a lab)

think like the attacker

- **Kali Linux** START kali.org ↗
  Run it as a virtual machine. It is your attack box for every lab in this layer.
- **Burp Suite** portswigger.net ↗
  Community Edition is free. Send your browser through it and watch what a login form sends.
- **Metasploit** metasploit.com ↗
  Point it at a deliberately vulnerable VM like Metasploitable 2. Never at a real system.
- **Hashcat** hashcat.net ↗
  Crack the hash of a password you made up, and see how fast short passwords fall.

4 Investigate

work out what happened

- **VirusTotal** START virustotal.com ↗
  Paste a suspicious link or file hash. Don't upload private files: samples are shared with researchers.
- **Autopsy** autopsy.com ↗
  Open a practice disk image and recover the files someone deleted.
- **Volatility** volatilityfoundation.org ↗
  Run windows.pslist on a sample memory image to list what was running.
- **CyberChef** gchq.github.io/CyberChef ↗
  Runs in your browser, no install. Decode a Base64 string from a phishing email.

5 Automate

script the boring parts

- **Python** START python.org ↗
  Write a 10-line script that counts failed logins in a log file.
- **PowerShell** learn.microsoft.com/powershell ↗
  Pull failed Windows logons with Get-WinEvent, Event ID 4625.
- **Bash** gnu.org/software/bash ↗
  grep "Failed password" /var/log/auth.log | wc -l on a Linux VM.
- **Git** git-scm.com ↗
  Push every script here to GitHub. That is your portfolio.

START TODAY · 5 MINUTES

Install Nmap, open a terminal and run:

```
nmap scanme.nmap.org
```

Nmap's makers set that host up for practice. Read which ports come back open and what runs on them.

Only scan or attack machines you own or have written permission to test.
Links and free tiers checked 26 Nov 2026.

If this helped, please consider following @getuacademy.