TEKTUT

FREE GUIDE

How the Enemy Thinks

The attacker mindset every cyber analyst needs — and three things you can try right now, in your browser.

NO EXPERIENCE NEEDED | BROWSER ONLY | 15 MINUTES

KNOW YOUR ENEMY

Two and a half thousand years ago, a general wrote the book on winning.

Sun Tzu was a Chinese military strategist writing around 500 BC. His work, The Art of War, was not a celebration of violence — it was a study of how to avoid unnecessary conflict by understanding it completely. His most famous insight is as relevant to a cyber analyst today as it was to a general on a battlefield in ancient China.

> **“Know thy enemy and know thyself, and in a hundred battles you will never be in peril.”**
>
> — Sun Tzu, The Art of War, c. 500 BC

The principle is simple: you cannot defend against something you do not understand. A general who has never studied how their enemy fights, what weapons they carry, what tactics they prefer — that general is already losing before the first battle begins.

Cyber security is the same. Every alert you investigate as an analyst is the aftermath of an attacker doing something. To make sense of it — to know whether it matters, how serious it is, where it might lead — you need to understand how attackers think and what they are trying to achieve.

TWO ROUTES, ONE MINDSET

This is why the best cyber defenders are people who understand offence. CompTIA CySA+ trains you to recognise attacker behaviour at every stage of the Kill Chain so you can detect and respond to it. For those who want to go further — actively testing systems and finding vulnerabilities — CompTIA PenTest+ is the natural next step, and TekTut offers both.

THE REALITY

How attackers actually work.

Attackers do not just randomly try things and hope for the best. Real attacks follow a structured sequence — a chain of steps that security researchers have documented and named. Understanding this sequence is the foundation of everything an analyst does.

STAGE	WHAT THEY DO	IN PLAIN ENGLISH	WHAT ANALYSTS LOOK FOR
01 Recon	Reconnaissance	Research the target. Find open ports, employee names, software versions — all publicly available.	Unusual scans or probes against the network perimeter.
02 Access	Initial Access	Exploit a weakness to get in — a phishing email, an unpatched vulnerability, a weak password.	Failed logins, unexpected email links clicked, known CVE traffic.
03 Escalate	Privilege Escalation	Gain more powerful permissions. Move from a normal user account toward admin or system access.	Accounts accessing resources they never normally touch.
04 Persist	Stay Hidden	Create a backdoor or scheduled task so they can return even if the initial entry is closed.	New scheduled tasks, services, or accounts created at unusual times.
05 Act	Objective	Do what they came to do — steal data, encrypt files for ransom, disrupt systems.	Large data transfers, file encryption activity, systems going offline.

THE CYBER KILL CHAIN

This sequence is called the Cyber Kill Chain — a model developed by Lockheed Martin and used by security teams worldwide. Every time an analyst investigates an alert, they are asking: which stage of this chain are we looking at? That question shapes everything that happens next.

YOUR FIRST WINS

Three things to try right now — no experience needed.

Each activity below puts you in the attacker's seat for a few minutes — legally, safely, in your browser. No software. No setup. The point is not to learn to attack. The point is to see what attackers see, so you understand what you are defending.

WIN 01	See your target the way an attacker sees it
WIN 02	Read a real vulnerability — the same way attackers do
WIN 03	Try a safe, legal hacking challenge

ETHICAL & LEGAL

Everything you are about to do is completely legal and uses publicly available information or purpose-built training environments. Real ethical hackers operate under the same principle: understanding the tools of offence makes you a better defender.

WIN 01

See your target the way an attacker sees it

BROWSER ONLY — NO INSTALL NEEDED

5–8 minutes

Why this matters to a real analyst:

Before an attacker touches a single system, they spend time on reconnaissance — gathering intelligence using nothing but publicly available information. One of their most powerful tools is Shodan: a search engine that indexes internet-connected devices, open ports, running software, and exposed services. Analysts use it to understand what their organisation looks like from the outside. It takes seconds to find things that should never be publicly visible.

1 **Go to Shodan**

Navigate to shodan.io. No account is needed for basic searches.

2 **Search for a well-known organisation**

Try searching for a large company or public institution — for example, type org:"BBC" or org:"NHS". You will see a list of internet-connected devices that Shodan has found and indexed publicly.

3 **Look at what is exposed**

Click on a result. You will see the IP address, what port is open, what software is running, and sometimes the exact version number. Attackers use version numbers to look up known vulnerabilities.

4 **Reflect on what you just found**

Everything on that screen is publicly available to anyone in the world, including attackers. Now imagine being the analyst responsible for making sure nothing dangerous is exposed. That is reconnaissance from a defender's perspective.

THIS IS WHAT ATTACKERS SEE FIRST

Shodan is used daily by penetration testers, security researchers, and analysts. It is not a hacking tool — it only indexes information devices broadcast publicly. But it shows you, in seconds, exactly what an attacker's first five minutes of reconnaissance looks like.

WIN 02

Read a real vulnerability the way attackers do

BROWSER ONLY — NO INSTALL NEEDED

5–8 minutes

Why this matters to a real analyst:

When a vulnerability is discovered in software, it is assigned a CVE — a Common Vulnerabilities and Exposures number. These are published publicly on the internet so that defenders can patch their systems. The catch? Attackers read them too. In 2021, a vulnerability called Log4Shell (CVE-2021-44228) was discovered in a piece of software used by millions of systems worldwide. Within 72 hours of the CVE being published, attackers around the world were actively exploiting it. Reading a CVE is something every analyst does during a threat investigation.

1 **Go to the CVE database**

Navigate to cve.mitre.org and search for CVE-2021-44228 — this is Log4Shell, one of the most significant vulnerabilities of the last decade.

2 **Read the description**

Read the plain-English description. You will see: what software is affected, what an attacker can do if they exploit it, and a severity score. The score is out of 10 — Log4Shell scored 10.0.

3 **Notice who can read this**

This page is public. No login. No credentials. The same information you just read is available to every attacker in the world. This is why patching quickly after a CVE is published is so critical.

4 **Look at the references**

Scroll to the references section. You will see links to vendor advisories, proof-of-concept code, and analysis. Analysts use these to understand scope and urgency when an alert fires.

YOUR FIRST CVE

Vulnerability management — knowing which CVEs affect your systems and prioritising which to patch first — is a core junior analyst responsibility covered in CySA+. If you want to go deeper into how those vulnerabilities are actually exploited, that is exactly what CompTIA PenTest+ teaches. You just read your first CVE.

WIN 03

Try a safe, legal hacking challenge

BROWSER ONLY — NO INSTALL NEEDED

5–10 minutes

Why this matters to a real analyst:

HackThisSite is one of the oldest ethical hacking training platforms on the internet. It was created specifically to give people a legal, safe environment to practice the kinds of thinking that ethical hackers and security analysts use. The Basic Missions start from absolute zero — Mission 1 requires no technical knowledge whatsoever, just careful observation and logical thinking. It is designed to give you the genuine feeling of working through a security puzzle.

1 **Go to HackThisSite**

Navigate to hackthissite.org. Create a free account — it takes under a minute and no payment is required.

2 **Go to Basic Missions**

From the menu, select Challenges → Basic. You will see a list of missions numbered 1 onwards. Start with Mission 1.

3 **Read the scenario carefully**

Each mission gives you a brief story explaining the setup. Read it carefully. The solution is usually hidden in the information you have already been given — the same kind of careful observation an analyst uses when reading an alert.

4 **Work through it**

Mission 1 should take under 5 minutes. When you solve it, you will get a confirmation message. Notice how that felt — that satisfaction of working something out is what experienced analysts describe when they crack an investigation.

KEEP GOING IF YOU ENJOYED IT

HackThisSite missions get progressively harder. If you enjoyed Mission 1, try Mission 2 and 3. Each one builds a slightly different analytical skill. The platform has been used for training by security professionals for over 20 years.

WHAT'S NEXT

You just thought like an attacker.

You researched a target using Shodan. You read a real CVE the same way attackers do. You worked through an ethical hacking challenge. That is the attacker mindset — and it is exactly the lens a good cyber analyst applies every single day.

The structured path from here is clear. CompTIA CySA+ trains you to recognise and respond to attacker behaviour — it is the gold standard entry-level analyst certification in UK hiring. CompTIA PenTest+ takes you to the next level: actively testing systems, finding vulnerabilities, and thinking like a professional ethical hacker. TekTut offers both routes, with live sessions, mentor support, and a direct path to your first role.

01	02	03	04
CompTIA Network+	**CompTIA Security+**	**CompTIA CySA+**	**CompTIA PenTest+**
How networks work	Core security skills	Analyst qualification	Ethical hacking

Take the next step

Take our free 8-question Career Route Quiz to find out which path fits you — or book a free 15-minute call with a course advisor.

tektut.academy

CompTIA Authorized Partner · CPD Certified · tektut.academy