**Red Teaming: Breaking Things on Purpose (and Getting Paid for It)**

Meta: If hacking stuff, finding flaws, and embarrassing security teams (ethically) sounds fun, Welcome. This is Red Teaming, and it’s not just “fancy pen testing.”



Photo by [Towfiqu barbhuiya](https://unsplash.com/@towfiqu999999?utm_source=medium&utm_medium=referral) on [Unsplash](https://unsplash.com/?utm_source=medium&utm_medium=referral)

**1. What Is Red Teaming?**

Imagine if you hired someone to break into your house just to prove your locks suck. That’s red teaming.

But unlike your cousin who tested your front door with a credit card, Red Teaming is structured, authorized, and terrifyingly effective

At its core, *Red Teaming is adversarial simulation.*You mimic real-world attackers, their methods, their tools, their dirty tricks and find out if your defenses are anything more than a suggestion (or is entirely useless)

**2. Red vs. Blue vs. Purple: Who’s on Which Side?**

Let’s understand the cyber color war:

* **Red Team**: Offensive - break in, stay hidden, make defenders sweat.
* **Blue Team**: monitor, detect, respond, try not to cry.
* **Purple Team**: Peace negotiators - help both sides learn from each other without starting WWIII.

If cybersecurity were a ***movie***:

* **Red Team** = heist crew
* **Blue Team** = bank security
* **Purple Team** = film director making sure the shoot goes smoothly

**3. What Red Teams Actually Do (It’s Not Just Hacking Wi-Fi at Starbucks)**



Photo by [Growtika](https://unsplash.com/@growtika?utm_source=medium&utm_medium=referral) on [Unsplash](https://unsplash.com/?utm_source=medium&utm_medium=referral)

Red teaming isn’t just a 30-minute scan and report.

It’s an *end-to-end operation* that might take weeks or months.

Here’s what’s typically involved:

***A. Reconnaissance***

* Stalk the target online like it owes you money.
* Google dorking, OSINT, LinkedIn creeping, dumpster diving (optional but thrilling).
* Tools: Maltego, SpiderFoot, the company’s forgotten careers page from 2009.

***B. Initial Access***

* Phishing emails with just the right amount of urgency (“Your HR password expired!”).
* Exploiting known vulnerabilities.
* USB drops (yes, people ***still*** plug them in).

***C. Privilege Escalation***

* From “intern” to “domain admin” in five easy steps.
* Abusing weak permissions, password reuse, or misconfigured servers.
* **Bonus**: Dumping password hashes.

***D. Lateral Movement***

* You’re in, now start crawling.
* Use RDP, SMB, WMI, PSExec to spread across the network like a gossip in a small town.
* Hide in plain sight. The best Red Teamers are digital ninjas.

***E. Persistence***

* Establish your secret backdoors: scheduled tasks, registry keys, credential theft, or good old C2 beacons.

***F. Action on Objectives***

* Steal the crown jewels (not literally, unless it’s the …).
* Exfiltrate data, demonstrate impact, screenshot everything.
* **Bonus**: Drop a “proof.txt” file on the CEO’s desktop. Classic taunt.

**4. The Mindset: Think Like an Attacker (But Little Smarter)**

Red Teaming isn’t just about tools, it’s about *thinking like the enemy*. Creativity > automation.

***Ask yourself:***

* “If I were malicious, where would I start?”
* “What’s the easiest way in with the least noise?”
* “How can I blend in with regular user behavior?”

Red teaming rewards curiosity, patience, and being deeply paranoid in creative ways.

**5. Red Team ≠ Penetration Test**

Let’s break this myth similar to a bad router config.

A screenshot of a test

AI-generated content may be incorrect.

Red Teaming vs Pen Testing

Think of pentesting as checking for open windows. Red teaming is seeing if you can sneak in, steal the TV, and leave a note in the fridge.

**6. Real-World Red Team Tactics (Yes, They Happen)**



Photo by [Glen Carrie](https://unsplash.com/@glencarrie?utm_source=medium&utm_medium=referral) on [Unsplash](https://unsplash.com/?utm_source=medium&utm_medium=referral)

* Phishing campaigns that spoof HR or IT support.
* Malicious browser extensions to harvest cookies.
* Rogue Wi-Fi hotspots in company cafeterias.
* Cloning employee badges via RFID skimming.
* Abusing cloud misconfigurations (hello S3 buckets).

Red teams often find what everyone else missed, the human flaws, the oversights, the backdoors left open because *it’s just staging.*

**7. Red Team Tool Belt: What’s in the Arsenal?**



Photo by [Rohan](https://unsplash.com/@rohanphoto?utm_source=medium&utm_medium=referral) on [Unsplash](https://unsplash.com/?utm_source=medium&utm_medium=referral)

You’ll need more than Kali Linux and caffeine. Here’s the basic toolkit:

**A. Recon & OSINT**

* Recon-ng, theHarvester, Maltego
* Google (yes, seriously)

**B. Initial Access**

* **Phishing frameworks:** GoPhish, Evilginx
* **Exploits:** Metasploit, custom payloads

**C. Post-Exploitation**

* **C2 Frameworks**: Cobalt Strike, Mythic, Sliver
* **Privilege Esc:** Mimikatz, PowerUp, SharpHound
* **Lateral Movement**: Impacket, CrackMapExec, BloodHound

**D. Reporting (because yes, you have to)**

* Screenshots. Logs. More screenshots. Impact summaries. Executive-friendly graphs with scary red arrows.

**8. Red Team Ethics: Legal… Very Legal**

Red Teaming without permission is **illegal**. Period.



Photo by [Scott Graham](https://unsplash.com/@amstram?utm_source=medium&utm_medium=referral) on [Unsplash](https://unsplash.com/?utm_source=medium&utm_medium=referral)

You need:

* Explicit written authorization (Rules of Engagement)
* Defined scope
* Boundaries (no ransomware “just for fun”)

Red teaming is legal hacking with strict rules. Break them and you’re no longer a Red Teamer, rather you’re an episode of ***CSI: Cyber***.

**9. Learn Red Teaming**



Photo by [Ling App](https://unsplash.com/@lingapp?utm_source=medium&utm_medium=referral) on [Unsplash](https://unsplash.com/?utm_source=medium&utm_medium=referral)

**Want to Learn Red Teaming?**Here’s How to Start:

* **Build your fundamentals**: Networking, Linux, Windows internals
* **Get hands-on**: HackTheBox, TryHackMe, Offensive Security Labs
* **Certs** (if you’re into that): OSCP, CRTO, Red Team Ops, PNPT
* **Read**: Red Team Field Manual, MITRE ATT\&CK, and actual reports from real red teams

**10. Red Teaming Isn’t Glamorous**

There’s a lot of:

* Waiting for payloads to call back
* Writing reports
* Getting detected by an overzealous AV
* Explaining to managers that “yes, you ***allowed*** us to do this”

But it’s also:

* Exhilarating
* Impactful
* Incredibly satisfying when done right

**TLDR (But Make It Red)**

* Red Teaming = Ethical attacker simulation.
* It’s stealthy, structured, and way more than just a pentest.
* Real skill lies in blending creativity with technical prowess.
* Always operate ethically. Or don’t and enjoy prison Wi-Fi.

**Test Yourself?**

1. What’s the main goal of Red Teaming?

a) List all CVEs  
b) Cause panic  
c) Simulate real-world attackers  
d) Flex tools on LinkedIn

2. Which tool is used for command & control (C2)?

a) Wireshark  
b) Cobalt Strike  
c) Paint  
d) PuTTY

3. What’s the first step in a red team engagement?

a) Exploitation  
b) Reporting  
c) Reconnaissance  
d) Ask ChatGPT

*(Answers: 1c, 2b, 3c)*

**Enjoyed the read?**  
Smash the follow button, drop a comment, and share this with someone who still thinks “password” is a good password.