

Forum:[Hack Forums](#)

Thread: [New Here: Looking for Practical Cybersecurity Advice](#)

Frank0Trace - May 15, 2026, 7:48 pm

Hi everyone,

I'm new here and I wanted to introduce myself.

I'm a computer engineer, and lately I've been trying to take cybersecurity more seriously, not just from a theoretical point of view, but in a practical and concrete way. I already have a solid technical background, but I feel that reading concepts, definitions, and theory is very different from actually understanding how things work in the real world.

I'd like to start moving properly in this huge field and learn how to approach it with the right mindset. My goal is to build real skills, understand practical security concepts, and gradually become more confident with hands-on work.

I'm not looking for shortcuts. I'd really appreciate advice from people with more experience: where should I start, what should I practice, which resources or labs are worth using, and what mistakes should I avoid as a beginner?

Any guidance, roadmap, or personal experience would be very helpful.

Thanks in advance!?

OG-Pablo - May 15, 2026, 9:24 pm

(May 15, 2026 07:48 PM)Frank0Trace Wrote: [\[CITE\]](#) Hi everyone,

I'm new here and I wanted to introduce myself.

I'm a computer engineer, and lately I've been trying to take cybersecurity more seriously, not just from a theoretical point of view, but in a practical and concrete way. I already have a solid technical background, but I feel that reading concepts, definitions, and theory is very different from actually understanding how things work in the real world.

I'd like to start moving properly in this huge field and learn how to approach it with the right mindset. My goal is to build real skills, understand practical security concepts, and gradually become more confident with hands-on work.

I'm not looking for shortcuts. I'd really appreciate advice from people with more experience: where should I start, what should I practice, which resources or labs are worth using, and what mistakes should I avoid as a beginner?

Any guidance, roadmap, or personal experience would be very helpful.

Thanks in advance!?

Hi Frank and welcome!

It's great that you want to move beyond theory and get hands-on with cybersecurity. Since you already have a good technical background, you're in a strong position to build practical skills effectively.

Here's a roadmap to get you started:

1. Build a Strong Foundation

Understand the basics deeply: Networking (TCP/IP, DNS, HTTP/S), operating systems (Linux/Windows internals), and common protocols.

Security fundamentals: Confidentiality, integrity, availability (CIA triad), encryption, authentication, authorization, and common attack types (phishing, MITM, SQLi, XSS).

2. Set Up Your Lab Environment

Use virtual machines (VirtualBox, VMware) to create isolated environments.
Practice with tools like Kali Linux, Metasploit, Wireshark, Nmap, Burp Suite.
Use intentionally vulnerable applications (DVWA, WebGoat) to safely experiment.

3. Learn by Doing

Start with Capture The Flag (CTF) challenges on platforms like Hack The Box, TryHackMe, OverTheWire. They offer step-by-step challenges from beginner to advanced.

Participate in open-source security projects or bug bounty programs to gain real-world experience.

4. Study Practical Concepts

Focus on vulnerability assessment and penetration testing methodologies.
Learn incident response basics and how to analyze logs and alerts.
Explore scripting for automation (Python is very useful).

5. Use Good Resources

Books: "The Web Application Hacker's Handbook," "Practical Malware Analysis," "Hacking: The Art of Exploitation."

Online courses: Offensive Security's OSCP, Cybrary, SANS Cyber Aces, Coursera cybersecurity courses.

Forums and communities: Reddit r/netsec, Stack Exchange Security, Discord groups.

6. Common Beginner Mistakes to Avoid

Don't skip the basics; strong foundations make advanced topics easier.
Avoid copying solutions blindly—try to understand every step.
Don't rush into advanced tools without knowing what they do.
Be patient; building skills takes time and practice.

Final Tips

Document your learning process and write about what you do—it helps retention and builds a portfolio.

Stay curious and keep updated on the latest threats and tools.

Welcome once again!

Frank0Trace - May 16, 2026, 6:18 pm

(May 15, 2026 09:24 PM)OG-Pablo Wrote: [\[CITE\]](#) Hi Frank and welcome!

It's great that you want to move beyond theory and get hands-on with cybersecurity. Since you already have a good technical background, you're in a strong position to build practical skills effectively.

Here's a roadmap to get you started:

1. Build a Strong Foundation

Understand the basics deeply: Networking (TCP/IP, DNS, HTTP/S), operating systems (Linux/Windows internals), and common protocols.

Security fundamentals: Confidentiality, integrity, availability (CIA triad), encryption, authentication, authorization, and common attack types (phishing, MITM, SQLi, XSS).

2. Set Up Your Lab Environment

Use virtual machines (VirtualBox, VMware) to create isolated environments.
Practice with tools like Kali Linux, Metasploit, Wireshark, Nmap, Burp Suite.
Use intentionally vulnerable applications (DVWA, WebGoat) to safely experiment.

3. Learn by Doing

Start with Capture The Flag (CTF) challenges on platforms like Hack The Box, TryHackMe, OverTheWire. They offer step-by-step challenges from beginner to advanced.

Participate in open-source security projects or bug bounty programs to gain real-world experience.

4. Study Practical Concepts

Focus on vulnerability assessment and penetration testing methodologies.
Learn incident response basics and how to analyze logs and alerts.
Explore scripting for automation (Python is very useful).

5. Use Good Resources

Books: "The Web Application Hacker's Handbook," "Practical Malware Analysis," "Hacking: The Art of Exploitation."

Online courses: Offensive Security's OSCP, Cybrary, SANS Cyber Aces, Coursera cybersecurity courses.

Forums and communities: Reddit r/netsec, Stack Exchange Security, Discord groups.

6. Common Beginner Mistakes to Avoid

Don't skip the basics; strong foundations make advanced topics easier.
Avoid copying solutions blindly—try to understand every step.
Don't rush into advanced tools without knowing what they do.
Be patient; building skills takes time and practice.

Final Tips

Document your learning process and write about what you do—it helps retention and builds a portfolio.

Stay curious and keep updated on the latest threats and tools.

Welcome once again!

Thanks you mate, I appreciate