

Forum:[Hack Forums](#)

Thread: [How AI Can Help With Cybersecurity Learning](#)

FatCat - October 6, 2026, 7:41 pm

AI has become a useful tool for learning cybersecurity, but I think it is important to understand how to use it correctly.

AI should not replace your own analysis. It can be used as an assistant to explain concepts, analyze information and help generate ideas.

1. LEARNING LINUX COMMANDS

If I find a command that I don't understand, I can ask an AI to explain what each part does.

For example:

```
sudo ss -tulpn
```

Instead of simply copying the command, I can ask:

"What does each option in ss -tulpn mean?"

This helps turn a command into something I actually understand.

2. ANALYZING LOGS

AI can also help explain large or complicated log entries.

For example, I could provide a sanitized log entry and ask:

"Explain what happened in this event and identify anything unusual."

The AI can help identify timestamps, IP addresses, usernames, processes and authentication failures.

However, sensitive information should be removed before sharing logs with an external AI service.

3. UNDERSTANDING NETWORK TRAFFIC

When learning Wireshark or tcpdump, AI can help explain unfamiliar

packets and protocols.

For example:

"Explain what this DNS request means."

or:

"What could cause repeated DNS queries from the same host?"

This can be useful when learning network analysis.

4. WRITING SECURITY SCRIPTS

AI can also help create small scripts for legitimate security tasks.

For example, a Python script could parse authentication logs and count failed login attempts.

Instead of blindly running generated code, I would first review:

- What files does it access?
- What commands does it execute?
- Does it modify anything?
- Does it send information anywhere?
- What permissions does it require?

5. AI DOES NOT GUARANTEE THAT THE ANSWER IS CORRECT

This is probably the most important point.

AI can make mistakes, misunderstand logs or generate commands that do not work in a particular environment.

For cybersecurity, blindly trusting an AI-generated answer can be especially problematic.

Information should be verified using documentation, system output, reliable security sources and controlled lab environments.

6. AI + HUMAN ANALYSIS

I think the best approach is:

Human -> defines the problem

AI -> helps explain and organize information

Human -> verifies the result
Human -> makes the final decision

AI is a useful assistant, but the analyst still needs to understand what is happening.

EXAMPLE

Suppose I find an unfamiliar listening port:

```
sudo ss -tulpn
```

Instead of asking AI:

"Is this malicious?"

I could provide the relevant information and ask:

"What service is associated with this process, what should I investigate next, and what evidence would help determine whether the service is legitimate?"

That produces a much better investigation process than simply asking the AI for a yes/no answer.

FINAL THOUGHT

AI is becoming another tool in the cybersecurity toolbox.

The important skill is not just knowing how to ask AI questions. It is knowing how to verify its answers and combine them with actual technical evidence.

How are you currently using AI for cybersecurity: learning, troubleshooting, coding, log analysis, or something else?