# AI TACTICAL SKILLS:

# CAR HACKING & DEFENSE

This 5-day course provides a comprehensive overview of ethical hacking in the automotive sector, combining theoretical knowledge with practical hands-on exercises to ensure participants are well-equipped to tackle real-world challenges in vehicle cybersecurity.

**5 DAYS | Online / In person / Hybrid | ALL LEVELS**

**EACH PARTICIPANT GETS:**

- **HACKING TOOLKIT**
- **6 months access to Premier Private Lab-Range**

Taking this automotive cybersecurity training is essential for staying ahead in the rapidly evolving automotive industry. It ensures that professionals are well-equipped to handle emerging threats, comply with regulatory standards, and contribute to the overall safety and security of modern vehicles.

**CYBER2 LABS**

*Build your AI Tactical Skills*

WWW.CYBER2LABS.COM
INFO@CYBER2LABS.COM

# AI TACTICAL SKILLS:
# CAR HACKING & DEFENSE

## OUTLINE

Day 1: **Introduction to Automotive Cybersecurity**

- Importance of cybersecurity in modern vehicles
- Overview of automotive systems and communication protocols
- Key concepts: CAN bus, OBD-II, and telematics
- Automotive Threat Landscape
- Common attack vectors and threats to vehicle systems
- Case studies of past automotive hacks
- Setting Up the Lab Environment
- Tools and software required for automotive hacking
- Setting up virtual environments and physical simulators

Day 2: **Understanding Vehicle Communication Systems**

In-Depth CAN Bus Protocol

- CAN bus architecture and communication
- Analyzing CAN bus messages
- Practical exercises with CAN bus simulators
- OBD-II and Diagnostics
- OBD-II protocol and its usage in diagnostics
- Reading and interpreting diagnostic trouble codes (DTCs)
- Hands-on exercises with OBD-II scanners and simulators

CYBER2 LABS

Build your AI Tactical Skills

WWW.CYBER2LABS.COM

INFO@CYBER2LABS.COM

# AI TACTICAL SKILLS:

# CAR HACKING & DEFENSE

Day 3: **Vehicle Network Vulnerabilities and Exploitation**

Wireless Attack Vectors

- Bluetooth and Wi-Fi vulnerabilities in vehicles
- Attacking keyless entry systems
- Hands-on exercises with Bluetooth sniffers and Wi-Fi tools
- Injection Attacks on Vehicle Networks
- Message injection techniques on CAN bus
- Replay attacks and fuzzing
- Practical lab exercises on message injection and analysis

Day 4: **Defensive Techniques and Secure Development Practices**

Defensive Strategies in Automotive Security

- Network segmentation and message authentication
- Intrusion detection systems for vehicles
- Hands-on exercises in setting up and testing defensive measures
- Secure Coding Practices for Automotive Software
- Principles of secure software development
- Common vulnerabilities and mitigation strategies
- Code review and static analysis tools

AI

→ BUILD

→ HACK

→ DETECT

→ DEFEND

CYBER2 LABS

WWW.CYBER2LABS.COM

INFO@CYBER2LABS.COM

# AI TACTICAL SKILLS: CAR HACKING & DEFENSE

Day 5: **Advanced Topics and Course Wrap-Up**

Telematics and Infotainment Systems Security

- Security challenges in telematics and infotainment
- Penetration testing telematics units
- Practical exercises on testing and securing infotainment systems
- Vehicle-to-Everything (V2X) Communication Security
- Introduction to V2X technology and its security implications
- Threats and defenses in V2X communication
- Practical lab on V2X security testing
- Final Project and Assessment
- Group project: Conduct a full security assessment on a simulated vehicle system
- Presentation of findings and recommendations

## TARGET AUDIANCE

- Cyber Security engineers / analysts
- Network and system administrators
- Motor car & Robotic Engineers & Developers
- RV Test Operators
- Digital Forensics Investigators
- Penetration Testers
- Cloud computing personnel
- Cloud project managers
- Operations support looking for career advancement


CYBER2 LABS

WWW.CYBER2LABS.COM
INFO@CYBER2LABS.COM

# AI TACTICAL SKILLS:

# CAR HACKING & DEFENSE

**We will utilize in this course:**

- A pre-built mobile hardware system such as a Raspberry Pi or a laptop
- Live Cloud based remote lab range and electronic interactive content

## CYBER2 LABS AI Hacking Toolkit

### Raspberry Pi 5 AI Hardware


### Toolkit Case

CYBER2 LABS

WWW.CYBER2LABS.COM

INFO@CYBER2LABS.COM

# AI TACTICAL SKILLS: CAR HACKING & DEFENSE

The automotive industry is undergoing a significant transformation with the integration of advanced technologies and connectivity features. This transformation has brought about numerous benefits but also introduced new cybersecurity risks. Here are several key reasons why it is crucial to undertake the described automotive cybersecurity training:

- **Increasing Connectivity and Complexity of Modern Vehicles**
  - Modern vehicles are equipped with numerous electronic control units (ECUs) and are interconnected through networks like CAN bus, making them susceptible to cyber-attacks.
  - With the advent of Internet of Things (IoT) and vehicle-to-everything (V2X) communications, vehicles are becoming more connected to external networks, increasing the attack surface.
- **Rising Cybersecurity Threats in the Automotive Sector**
  - High-profile cyber-attacks on vehicles, such as remote hijacking and disabling of vehicle functions, have demonstrated the potential for serious safety and security breaches.
  - Cybercriminals are increasingly targeting automotive systems to exploit vulnerabilities for malicious purposes.
- **Safety Concerns**
  - Cyber-attacks on vehicles can have direct consequences on passenger safety, potentially leading to accidents, injuries, or even fatalities.
  - Ensuring the cybersecurity of automotive systems is essential to protect the lives of drivers, passengers, and pedestrians.

CYBER2 LABS

*Build your AI Tactical Skills*

WWW.CYBER2LABS.COM

INFO@CYBER2LABS.COM

# AI TACTICAL SKILLS: CAR HACKING & DEFENSE


- **Compliance with Regulatory Requirements**
  - Regulatory bodies and industry standards, such as ISO/SAE 21434, are increasingly mandating stringent cybersecurity measures for automotive systems.
  - Training helps professionals understand and comply with these regulations, avoiding legal and financial repercussions.
- **Preserving Consumer Trust and Brand Reputation**
  - A single cyber incident can significantly damage a manufacturer's reputation and erode consumer trust.
  - By investing in cybersecurity training, companies can demonstrate their commitment to protecting their customers, thereby enhancing their brand image and maintaining customer loyalty.
- **Proactive Risk Management**
  - Understanding and identifying potential vulnerabilities in vehicle systems allows for proactive measures to mitigate risks before they can be exploited by malicious actors.
  - Training equips professionals with the skills to conduct thorough security assessments and implement effective defensive strategies.
- **Career Advancement Opportunities**
  - As cybersecurity becomes a critical aspect of automotive engineering, there is a growing demand for skilled professionals in this field.
  - Specialized training in automotive cybersecurity opens up new career paths and opportunities for advancement within the industry.
- **Enhancing Overall Vehicle Security**
  - Knowledge gained from such training enables the development and implementation of robust security protocols and secure coding practices in the automotive development lifecycle.
  - It contributes to building more resilient automotive systems that can withstand and recover from cyber-attacks.

**CYBER2 LABS**

*Build your AI Tactical Skills*

WWW.CYBER2LABS.COM
INFO@CYBER2LABS.COM