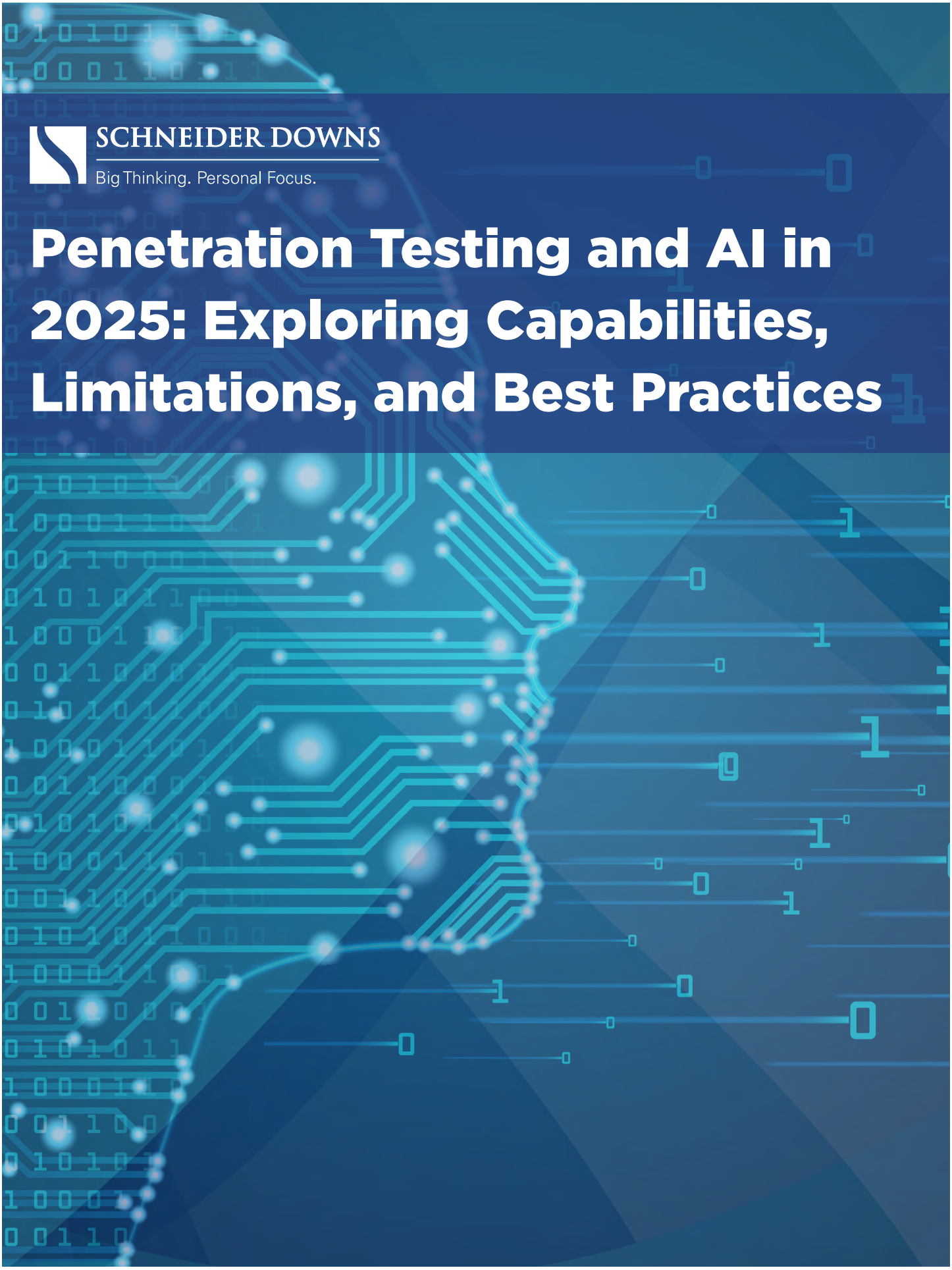


# Penetration Testing and AI in 2025: Exploring Capabilities, Limitations, and Best Practices

SCHNEIDER DOWNS

Big Thinking. Personal Focus.

# Penetration Testing and AI in 2025: Exploring Capabilities, Limitations, and Best Practices

Artificial Intelligence (AI) is rapidly transforming many industries, and cybersecurity is no exception. With new AI tools and integrations emerging constantly, it's important to understand how AI is currently being applied in penetration testing, including its capabilities, limitations, and best practices.

## Penetration Testing and AI: The Capabilities

Without going into great technical depth, AI is trained to recognize and react to patterns. AI can work 24/7 without taking any breaks. AI can analyze small and large data sets, including massive code repositories and large security event logs, looking for non-standard entries. All these capabilities make AI skillful at continuously scanning assets such as networks, applications, and systems for known vulnerabilities (pattern matching). For penetration testing, AI is proficient at performing tasks such as port scanning, vulnerability scanning, and limited exploitation techniques. These exploitation techniques take advantage of known vulnerabilities and misconfigurations.

## Penetration Testing and AI: The Limitations

It is important to recognize that AI has limitations when performing penetration tests. Yes, AI is trained, but it cannot perform tasks of reasoning (yet). Therefore, when AI encounters a situation that requires an understanding of business logic, it can struggle. Currently, AI is unable to implement the type of problem-solving logic and/or intuition that humans possess. If there are no known patterns for AI to learn from, it cannot connect several exploits into a path to compromise to progress a penetration test. AI is unable to adapt to situations that occur with social engineering techniques such as vishing. It goes without saying, AI is unable to perform physical testing in a penetration testing engagement.

As far as the penetration testing scope, AI can follow the basics, such as IP lists. However, AI struggles with making the appropriate decisions related to other testing boundaries. Exceeding scope boundaries can lead to business operation interruptions, loss of data, and ultimately, reputation loss. AI can lack an understanding of business goals and risk appetite, which human testers use to guide their decision-making processes.

## When to Use AI for Penetration Testing

There are ideal environments for using AI in penetration testing. Those include environments that require continuous monitoring, large-scale environments, and/or environments that experience frequent changes. It can be impractical to have human testers perform continuous monitoring. AI has no problem working with large-scale environments that are made up of similar systems. This type of testing would be very time-consuming for a human tester. Also, when environments experience frequent changes, it can be cost-prohibitive to have human testers perform penetration testing at high frequency intervals.

## When to Use Human Penetration Testers

Human penetration testers can be experienced with complex systems that contain unique architectures. They are also adept at testing custom applications. Human penetration testers can chain several exploitation techniques in sequence in order to build a complex path to compromise. In addition, human testers can adapt to social engineering engagements like vishing, where conversations can take unpredictable paths.

During penetration test engagements, clients might request that the tester provide a transfer of knowledge to help build awareness and knowledge within the client staff. These are moments where the tester meets with the client, reviews their notes on screen, and describes in detail how a specific technique works within the client's environment. This session can also include an "over-the-shoulder" moment where the tester shares their screen and executes the attack in real time while answering any questions the client team presents.

## Best Practices for Penetration Testing and AI

In the right circumstances, AI and human testers can be used in a tiered approach. AI can be used for scanning networks, code bases, applications, and systems to develop a list of potential vulnerabilities. This information can then be provided to the human tester to review, confirm true/false positives, and exploit any vulnerability that would lead to a path to compromise. The human tester can also perform any complex exploitations, business impact analyses, and knowledge transfer sessions.

## How Can Schneider Downs Help?

Our network penetration testing services are designed to assess your organization's security by simulating real-world cyberattacks, such as phishing and ransomware, using the same tools and techniques employed by threat actors. As an impartial third party, we identify critical vulnerabilities across both internal and external networks. Our tests also evaluate whether these vulnerabilities are exploitable, providing a clear picture of the actual risks they pose to your IT security posture.

If you're new to network penetration testing, simply complete our **penetration questionnaire**, and a member of our team will reach out to assist you in the next steps.

### About Schneider Downs Cybersecurity

The Schneider Downs cybersecurity practice consists of experts offering a comprehensive set of information technology security services, including penetration testing, intrusion prevention/detection review, ransomware security, vulnerability assessments and a robust digital forensics and incident response team. In addition, our **Digital Forensics and Incident Response** teams are available 24x7x365 at 1-800-993-8937 if you suspect or are experiencing a network incident of any kind.

For more information, please contact our team at **contactsd@schneiderdowns.com** or visit **www.schneiderdowns.com/cybersecurity**.