EXPLOITATION WITH ML AND AI

Harnessing Artificial Intelligence for Penetration Testing

PHASE 3: EXPLOITATION

- Gather Information
- Scanning
- Exploitation
  - Demonstrate Vulnerability's Impact
  - Prove Practical Implications
  - Avoiding Real Harm
- Maintaining Access
- Covering Tracks
- Reporting and Documentation

MANUAL EXPLOITS

- Rely on Human Skills, Knowledge, and Creativity
- Examples
  - SQL Injection
  - XSS
  - Buffer Overflow
  - hundreds more

MANUAL-*ish* EXPLOITS

Metasploit

docs.metasploit.com
docs.rapid7.com/Metasploit

tutorialspoint.com/metasploit/
geeksforgeeks.org/what-is-metasploit/

tryhackme.com/room/metasploitintro

LIMITATIONS OF MANUAL METHODS

Lack of Adaptability to Evolving Threats

Complexity

Time-Consuming and Resource-Intensive

Expensive

LIMITATIONS OF MANUAL-*ish* METHODS

Lack of Adaptability to Evolving Threats

Complexity

Time-Consuming and Resource-Intensive

Expensive

EXPLOITATION PRACTICE

Metasploit: Introduction

https://tryhackme.com/room/metasploitintro

Metasploit: Meterpreter

https://tryhackme.com/room/meterpreter

1

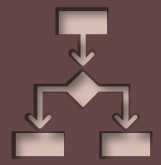
OR

SQL Injection

https://tryhackme.com/room/sqlinjectionlm

2

EXPLOITATION WITH AI AND ML

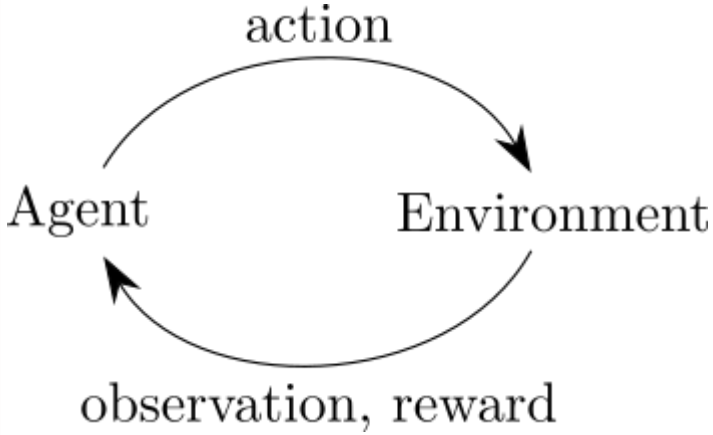


Decision Making

Continuous Learning

Real-time Updates

EXPLOITATION WITH AI AND ML



Machine Learning

Reinforcement Learning

- Q-Learning

REAL-WORLD EXAMPLES

- Social Engineering Toolkit (SET)
- DeepExploit
- Python Libraries
  - NumPy
  - TensorFlow

FUTURE TRENDS IN AI

- AlMajali, et al.
  - RL Agent that Leverages The Q-Learning
  - Evaluates Payloads Directly from Metasploit

https://www.researchgate.net/publication/370945041_Vulnerability_Exploitation_Using_Reinforcement_Learning

RESEARCH QUESTION

Considering the unpredictable nature of evolving cyber threats, how can AI models be trained to handle novel and unexpected attack scenarios effectively?

What challenges arise when the threat landscape diverges from the training data?

What kind of patterns should AI focus on to limit these challenges?

REFERENCES

[1] G. Stone, D. Talbert and W. Eberle, "Using AI/Machine Learning for Reconnaissance Activities During Network Penetration Testing," in International Conference on Cyber Warfare and Security, 2021.

[2] R. S. Jagamogan, S. A. Ismail, N. H. Hassan and H. Aba, "Penetration Testing Procedure using Machine Learning," in International Conference on Smart Sensors and Application (ICSSA), Kuala Lumpur, 2022.

[3] N. Singh, V. Meherhomji and B. R. Chandavarkar, "Automated versus Manual Approach of Web Application Penetration Testing," International Conference on Computing, Communication and Networking Technologies (ICCCNT), pp. 1-6, July 2020.

[4] Y. Stefinko, A. Piskozub and R. Banakh, "Manual and automated penetration testing. Benefits and drawbacks. Modern tendency," International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET), pp. 488-491, February 2013.

[5] Z. Ali, F. Hussain, S. Ghazanfar, M. Husnain, S. Zahid and G. A. Shah, "A Generic Machine Learning Approach for IoT Device Identification," in International Conference on Cyber Warfare and Security (ICCWS), Islamabad, 2021.

[6] J. M. Ortega, Mastering Python for Networking and Security, 2 ed., V. Boricha, Ed., Birmingham: Packt Publishing, 2020.

[7] P. Engebretson, The Basics of Hacking and Penetration Testing, A. Ward, Ed., Waltham, MA : Elsevier Inc, 2011.

[8] R. Maeda and M. Mimura, "Automating post-exploitation with deep reinforcement learning," Computers & Security, vol. 100, pp. 102-108, January 2021.

[9] E. Tsukerman, Machine Learning for Cybersecurity Cookbook, J. Cummings, Ed., Birmingham: Packt Publishing, 2019.

[10] C. Chebbi, Mastering Machine Learning for Penetration Testing, Packt Publishing, 2018.

[11] H. Singh and H. Sharma, Hands-On Web Penetration Testing with Metasploit, R. Brookes-Bland, Ed., Birmingham: Packt Publishing, 2020.

[12] A. AlMajali, L. Al-Abed, R. Mutleq, Z. Samamah, A. A. Shhadeh, B. J. Mohd and K. M. Ahmad Yousef, "Vulnerability Exploitation Using Reinforcement Learning," in Jordan International Joint Conference on Electrical Engineering and Information Technology, Amman, 2023.