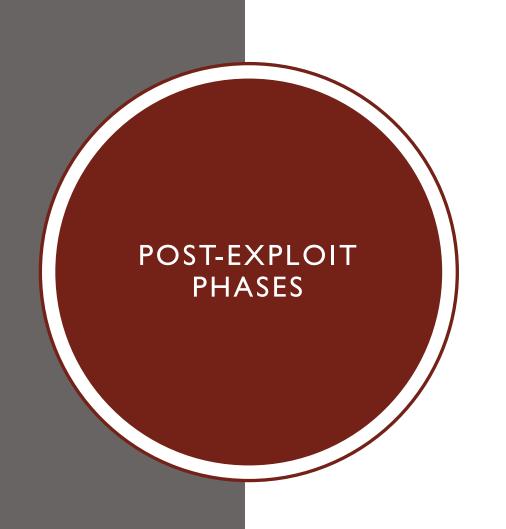
# AI-ENHANCED POST-EXPLOITATION

Harnessing Artificial Intelligence for Penetration Testing



- Gather Information
- Scanning
- Exploitation
- Maintaining Access
- Covering Tracks
- Reporting and Documentation



- Gather Information
- Scanning
- Exploitation
- Maintaining Access
  - Maintain Persistent Target Access
  - Execute Realistic Simulation
  - Display Long-Term Impact
  - Evaluate Detection Capabilities
- Covering Tracks
- Reporting and Documentation



- Gather Information
- Scanning
- Exploitation
- Maintaining Access
- Covering Tracks
  - Conceal Intrusion Evidence
  - Evaluate Detection Capabilities
  - Assess Information Retention
  - Check Corruption Difficulty
- Reporting and Documentation



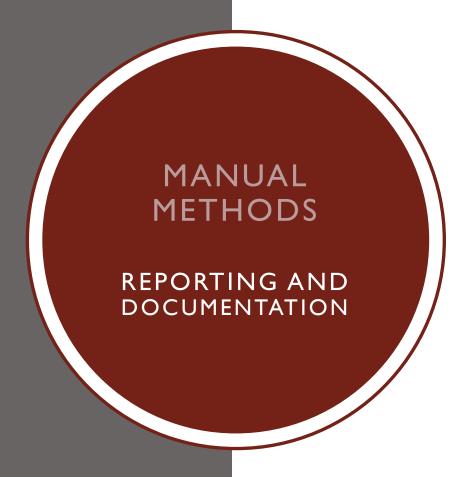
- Gather Information
- Scanning
- Exploitation
- Maintaining Access
- Covering Tracks
- Reporting and Documentation
  - Insights from Previous Phases
  - Convey Findings and their Impact
  - Risk Awareness
  - Prioritize Remediation



- Backdoor Creation
  - Netcat, Cymothoa, and Meterpreter
- Offline Password Attacks
  - John the Ripper and Mimikatz
- Online Password Attacks
  - CeWL and hydra



- Log Manipulation
  - AuditPol
  - ClearLogs, Logrotate, and WinZapper
- Erasing the Command History
  - Modify environment variable HISTSIZE
- Hiding Files
  - Modify File Attributes
  - Modify Alternate Data Streams



- Manual Note Taking
- Dradis
- Faraday IDE
- MagicTree



#### Password Attacks

https://tryhackme.com/room/passwordattacks

Evading Logging and Monitoring

https://tryhackme.com/room/monitoringevasion



### **Manual**

- Complex
- Human Behavior Dependent
- Scalability Limitations



# **Artificial Intelligence**

- Intuitive
- Predictive of Human Behavior
- Scalability Advantages





## **Manual**

- Time and Effort
- Reliance on Humans
- Limited Adaptability



# **Artificial Intelligence**

- Quick and Thorough
- Autonomous
- Scalable





#### **Manual**

- Time-Consuming and Tedious
- Manual Data Analysis
- Error-Prone



# **Artificial Intelligence**

- Quick and Thorough
- Automated Data Analytics
- Meticulous





Automated Post-Breach
Penetration Testing through
Reinforcement Learning

Explore Compromised Networks and Find Sensitive Files

Sujita Chaudhary, Austin O'Brien, and Shengjie Xu

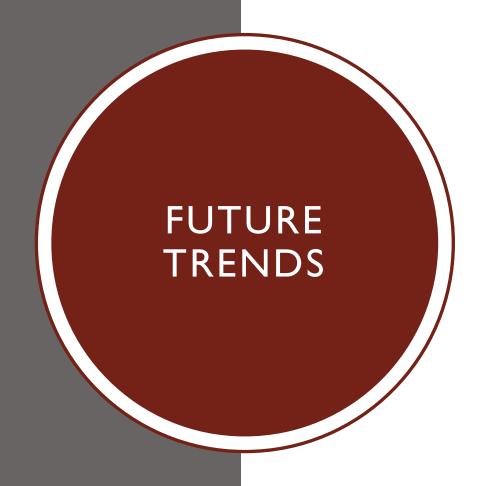
https://ieeexplore.ieee.org/document/9162301

Automating Post-Exploitation with Deep Reinforcement Learning

Automate Lateral Movement and Privilege Escalation

Ryusei Maeda, Mamoru Mimura

https://www.sciencedirect.com/science/article/pii/S0167404820303813







How can the RL agents introduced in the studies be effectively employed by future researchers to enhance and automate specific aspects of post-exploitation phases?

In what ways did the authors of the study lay the groundwork for future researchers, and what specific insights or methodologies can be built upon in subsequent studies?

What are some limitations that future researchers might encounter in the improvement of these methods?

## REFERENCES

- [1] S. Chaudhary, A. O'Brien and S. Xu, "Automated Post-Breach Penetration Testing through Reinforcement Learning," in Conference on Communications and Network Security (CNS), Avignon, 2020.
- [2] R. Maeda and M. Mimura, "Automating post-exploitation with deep reinforcement learning," Computers & Security, vol. 100, pp. 102-108, January 2021.
- [3] S.V. N. Parasram, A. Samm, D. Boodoo, G. Johansen, L. Allen, T. Heriyanto and S. Ali, Kali Linux 2018: Assuring Security by Penetration Testing, 4th ed., Packt Publishing, 2018.
- [4] S.-P. Oriyano, Penetration Testing Essentials, Sybex, 2016.
- [5] A.A.Alghamdi, "Effective Penetration Testing Report Writing," in International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), 2021.
- [6] M. N. Zakaria, P.A. Phin, N. Mohmad, S.A. Ismail, M. N. Kama and O.Yusop, "A Review of Standardization for Penetration Testing Reports and Documents," in International Conference on Research and Innovation in Information Systems (ICRIIS), 2013.
- [7] Market Research Report, MarketsandMarkets, 2022.