A Hands-on Digital Forensic Lab to Investigate Morris Worm Attack

Eric Xu • Alex Xu • Danny Ferreira • Lin Deng

UNIVERSITY OF BALTIMORE

TOWSON UNIVERSITY

RIDGE

Contact Us

Lin Deng: ldeng@towson.edu

Contributions

- Developed a hands-on digital forensic lab to investigate the Morris Worm attack
- Demonstrate a systematic approach to reconstructing the attack scenario
- Help students learn the fundamentals of digital forensic investigation, including identifying, collecting, and analyzing digital forensic evidence

Background

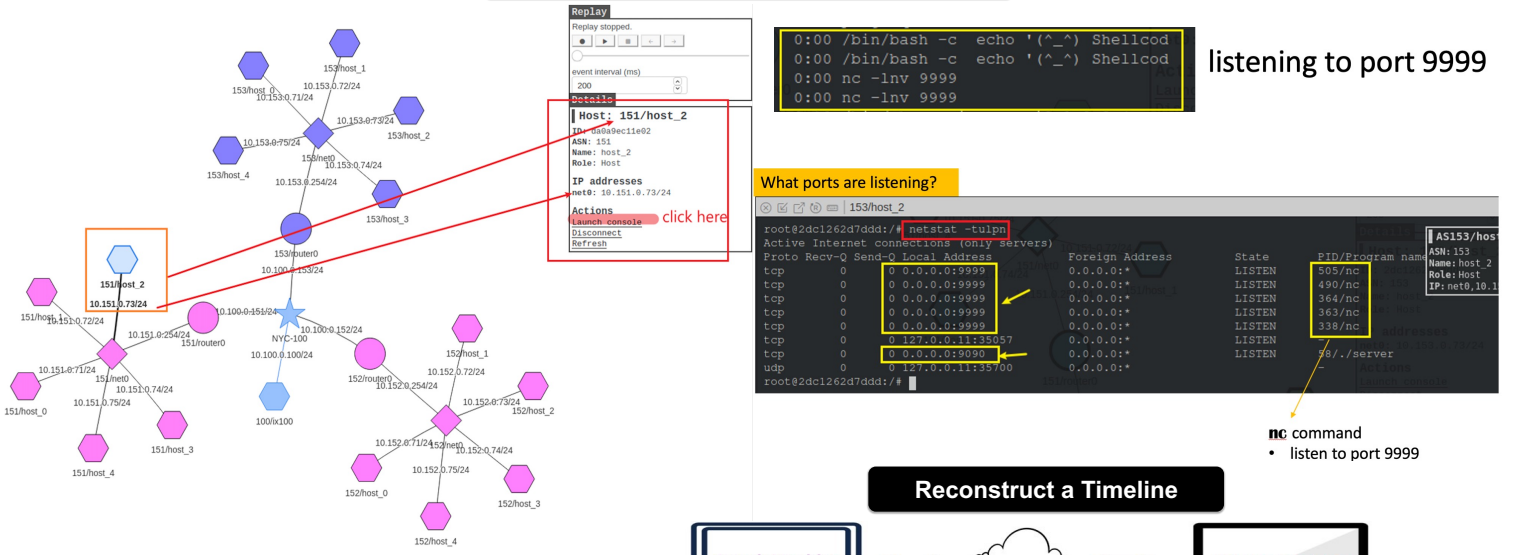
- **Morris Worm**
  - A malware was developed by Robert Tappan MORRIS
  - A program can self-spread across a national network
  - Demonstrate the inadequacies of security measures

Why Study Morris Worm ?

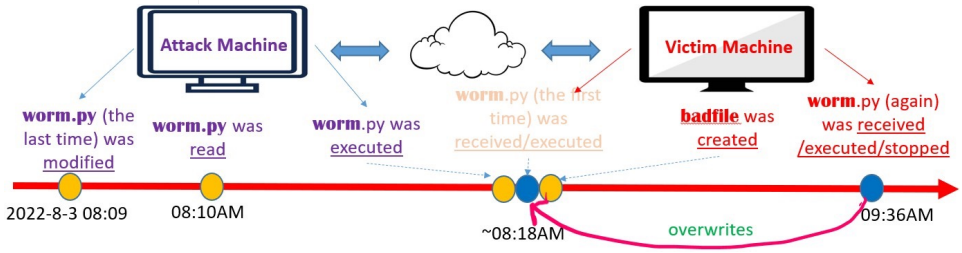
- **Morris Worm vs. Ransomware**
  - The techniques are still the same
  - Exploit vulnerabilities
  - Self-duplication
  - Self-spreading
  - Non-destructive vs. asking ransom fee (WannaCry)

Forensics Investigation

Analyze Network Ports and Process Used by Worm



Reconstruct a Timeline



Setup Environment

- Install Virtual Machine
- Running on an Internet emulator
- A simplified version of the attack code written in Python

Lab Resources

https://github.com/frankwxu/digital-forensics-lab

https://www.cyberforensics4all.org/

CYBER FORENSICS 4 ALL

SCAN ME

Acknowledgment

This Project is supported by the U.S. National Science Foundation #2039289 and the Department of Justice #2019-DF-BX-K001.