Computer Security Capstone

Project III: Ransomware Propagation and Payload

Chi-Yu Li (2024 Spring)
Computer Science Department
National Yang Ming Chiao Tung University

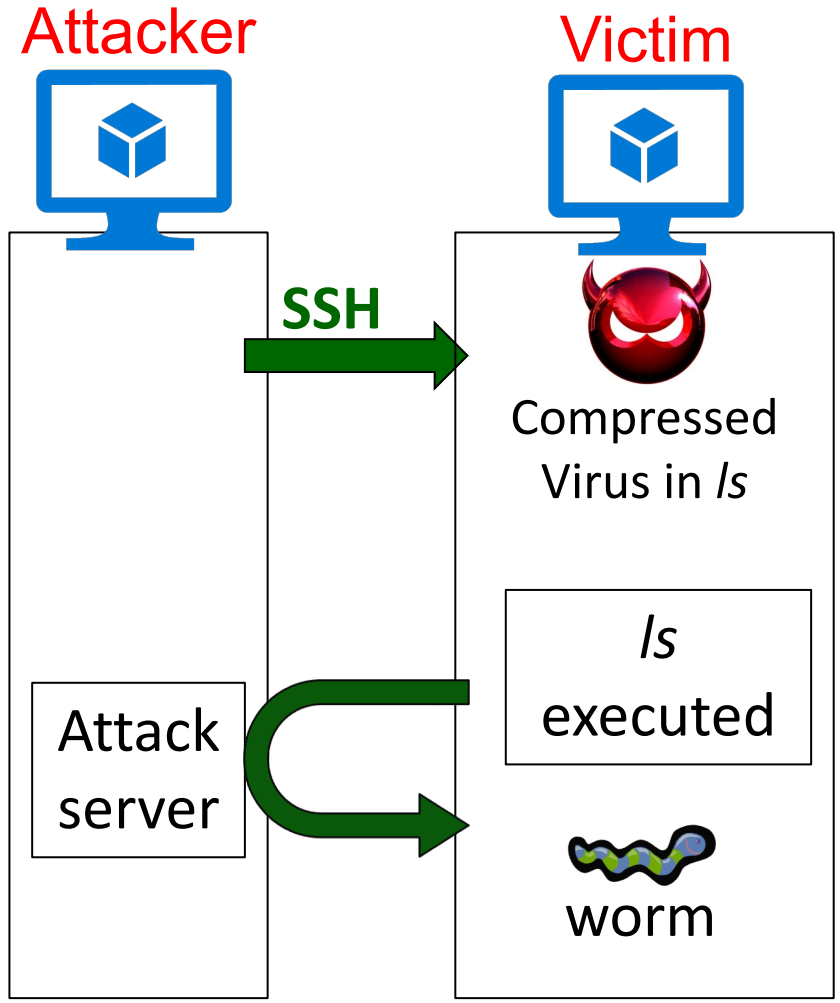
Goals

- Understand how a ransomware propagates and executes

- You will learn about the operation of
  - dictionary attacks
  - ciphering and deciphering
  - compressed viruses
  - worm propagation
  - ransomware

Attack Scenario

- You are going to play the role of an attacker
- Assume that you know the IP of the victim and the username of his/her SSH account, you are asked to
  - Crack the victim's SSH password
  - Install a compressed virus in an affected program
  - (virus payload) download and trigger a ransomware worm
- Consider the affected program: /app/ls in victim.
  - When it is run, the virus payload is executed



Three Tasks

- Task I: Crack SSH password (30%)
- Task II: Create a compression virus with the propagation of the ransomware worm (40%)
- Task III: Prepare the ransomware payload (30%)

Task I: Crack SSH password

- Cracking the victim's password by launching a dictionary attack
  - Assume that the victim's username is known as csc2024
  - Assume that the password is created based on the victim's personal information
    - A file including the victim's personal information: /app/victim.dat
      - One row contains an information entry
    - The password is composed of one or few information entries

- Hints
  - Trying strings combination in Python: **itertools**
  - Automatic SSH and SFTP operation in Python: **paramiko**

Task II: Compression Virus with Ransomware Propagation

- Infect /app/ls in victim by embedding your compression virus
- Infected ‘ls’ shall
  - keep the same size as the original ‘ls’
    - The original ‘ls’ shall be compressed
  - contain the virus payload and the functionality of the original ‘ls’
  - finish the execution of the payload before the end of the ‘ls’ execution
- The virus payload shall
  - fetch a ransomware worm from the attack server
  - execute the ransomware worm

Task II: Compression Virus with Ransomware Propagation

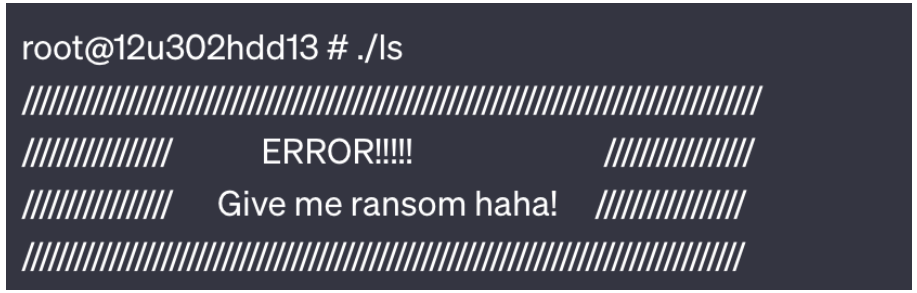
- Requirements
  - The infection cannot leave any files except the infected ‘ls’ on the victim container
  - Including “0xaabbccdd” in the last 4 bytes of the infected ‘ls’ as your signature
  - You can check the last bytes of a file with xxd

```
$ xxd ls | tail -n 1
000088f0: 2024 0000 aabb ccdd
```

- Hints
  - Compressing ‘ls’ using zip
  - Minimizing the virus size with various methods
    - e.g., using /dev/tcp/host/port to build tcp connections, gcc flags and strip
  - Executing a program using the exec() family

Task III: Ransomware Payload

- Two major actions
  - Encrypting all picture files in jpg in /app/Pictures at the victim using RSA
  - Show a graph indicating a message requesting ransom



- Requirements
  - Using a public key (*n* & *e*) for the RSA encryption:
    (22291846172619859445381409012451 & 65535)
  - Using a private key(n & d) for the RSA decryption:
    (22291846172619859445381409012451 & 144993092996733458446760035631 83)
- Hints
  - Sample codes for RSA encryption/decryption

Requirements

- You need to develop/run your program in the given Dockerfile
  - Resource is provided in /app
    - username/password: csc2024/csc2024
    - Note: the victim's password will be changed based on a new victim.dat file in the demo
  - Please complete your project under the path: /home/csc2024/${yourstudentID}
- You are allowed to use C/C++, Shell Script or/and Python
- You are allowed to team up; each team has at most 2 students
  - Teams: discussions are allowed, but no collaboration
- Please submit your source codes to E3
- Please email your questions to csc2024@mail.nems.cs.nycu.edu.tw

Important: How to set up environment?

- Build the project3 image
  - Linux: “ sudo docker build -t csc2024-project3 -f csc2024-project3.Dockerfile . ”
- Create the project3 containers
  - Linux: “ sudo docker compose -f csc2024-project3-docker-compose.yml up -d ”
- Enter the attacker container
  - Linux: “ docker exec -it attacker bash ”
- Enter the victim container
  - Linux: “ docker exec -it victim bash ”

Important: How to Prepare Your Attack Programs?

- Must provide a **Makefile** which compiles your source codes into at least two executable files: **crack_attack** and **attack_server**

- Test requirements for your program
  - Must be run in the given Dockerfile without any additional tools or libraries
  - Must work for the following two test commands
    - ./crack_attack <Victim IP> <Attacker IP> <Attacker port>
    - ./attack_server <Attacker port>

Important: Major Demo Steps (Not Exactly the Same)

- Attacker container
  - Run “make“ to compile your source codes
  - Run “./attacker_server <Attacker port>” to set up the attacker server
  - Run “./crack_attack <Victim IP> <Attacker IP> <Attacker port>” to crack the victim’s password and infect ‘ls’ in victim
- Victim container
  - Check the size of ‘ls’ and any additional files generated
  - Run 2 or 3 commands of ‘ls’
    - ‘ls’ shall perform its original function
    - Only the jpg files in /app/Pictures are encrypted with the given security context
    - A ransom graph shall show up
  - Check whether the encrypted files can be decrypted
- Note: no Internet access for both attacker and victim container

Project Submission

- Due date: 5/15 11:55 PM (Late submissions will not be accepted)
- Makeup submission (75 points at most): After the final
- Submission rules
  - Put all your files into a directory and name it using your student ID(s)
    - If your team has two members, please concatenate your IDs separated by "-"
  - Zip the directory and upload the zip file to E3
  - A sample of the zip file: 1234567-7654321.zip
    - 1234567-7654321
      - Makefile
      - crack_attack.c
      - attack_server.c
      - …

Questions?