Ethical Hacking: Final Exam

Professor William Tolley

Spring 2024

Introduction

Welcome to the final exam for Ethical Hacking. This exam is designed to test your practical skills in digital forensics, reverse engineering, network analysis, and secure communication. You will be working with a compromised system from the fictional university, **Finely Tuned University** (FTU), where the system administrator's computer has been infected, bringing down their entire "finely tuned system."

Scenario

Finely Tuned University (FTU) prides itself on its impeccable network infrastructure, maintained by the diligent system administrator, Bob Tinker. Bob often boasts about his "finely tuned system" that supposedly runs without a hitch. However, recently, Bob's computer was compromised, causing the entire network to crash.

Bob is baffled and repeatedly exclaims, "I don't understand how my finely tuned system was brought down!" You can't count on Bob for much, but Bob always makes sure to constantly capture traffic on all his machines, making our investigation much easier. As a digital forensics investigator, you have been tasked with analyzing Bob's compromised machine to uncover the extent of the damage, analyze captured network traffic, and reverse engineer any suspicious binaries that could be responsible for the attack.

Your tasks are outlined below:

Tasks

Part 1: Digital Forensics and Incident Response (DFIR)

1. Download the forensic image from the provided link.
2. Mount the image and explore its contents.
3. Analyze the directories to identify either the point of entry for the attack or any other interesting details.
4. Document any signs of malicious activities.
5. Add your findings to the comprehensive report, including:
    - Point of entry for the compromise.
    - Timeline of the incident.

Part 2: Packet Analysis

1. Locate the PCAP files in the `/home/csci297/PCAPS` directory of the forensic image.
2. Open the PCAP files using Wireshark.
3. Analyze the traffic to identify any suspicious activity.
4. Extract and decode any suspicious payloads.
5. Add your findings to the comprehensive report, including:
    - Types of traffic present in the capture.
    - Signs of malicious activity.
    - Decoded suspicious payloads.
    - Timeline of events based on packet analysis.

Part 3: Reverse Engineering

1. From your packet analysis, identify any suspicious binaries transferred to the system.
2. Locate these binaries in the PCAP and reassemble them by analyzing the TCP stream and saving the raw bytes.

3. Use reverse engineering tools (e.g., GDB, Ghidra, Radare2, IDA Free) to analyze the binaries.
4. Determine the purpose of the binaries and identify any hidden functionalities.
5. Extract the secret key or any other significant information revealed by the hidden functions.
6. Add your findings to the comprehensive report, including:
    - Main functionality of the program.
    - Hidden features or backdoors.
    - Steps taken to reverse engineer the program.
    - The secret key or other significant information revealed by the hidden function.

Part 4: PGP Encrypted and Signed Email

1. Combine your findings from the DFIR analysis, packet analysis, and reverse engineering into a comprehensive report.
2. Encrypt the report using Professor Tolley's public PGP key.
3. Sign the report with your private PGP key.
4. *Submit the report to Canvas on Saturday between 9:00 AM and 2:00 PM.*

Submission Instructions

1. Send the PGP encrypted and signed email to `wtolley@wlu.edu`.

Professor Tolley's Public PGP Key

```
5AAA 763F BA83 6482 2061 8F64 C45D 867E AA16 E9BF
```

Conclusion

Remember, Bob Tinker is counting on you to find out how his "finely tuned system" was brought down. Good luck, and may your investigative skills bring clarity to the chaos at Finely Tuned University!