Capture The Flag (CTF) Lab - yaSSL Forensic Analysis Summary

==

Date: May 28, 2025

Phase: Reconnaissance and Exploration

1. .rhosts Backdoor Discovery:

- Found .rhosts file in home directory, which can allow passwordless RSH logins.

- Symbols like '+' in .rhosts act as wildcards: '+ +' means any user from any host.

- This is considered a serious vulnerability and is often used in CTFs as an intentional backdoor.

2. Remote Shell Access:

- Used RSH (remote shell) to connect from Kali to Metasploitable VM.

- Installed `rsh-client` on Kali to enable this.

- Logged in successfully using: rsh 192.168.56.102 -l msfadmin

3. yaSSL Directory Exploration:

- Navigated to: /home/msfadmin/vulnerable/mysql-ssl

- Found: yassl-1.9.8.zip then extracted to /tmp/yassl/yassl-1.9.8

4. Key Files Discovered:

- client-key.pem contains RSA private key (potential vulnerability)

- README, INSTALL, AUTHORS are common metadata files that may contain flags or sensitive data

5. testsuite Folder:

- Contains testsuite.cpp, input, quit, Makefiles, and test headers.
- Discovered the test program uses input and output to verify yaSSL functionality via MD5 comparison.

6. Suspicious Behavior to Investigate:

- quit file may be used to trigger server shutdown - might contain a hidden flag.
- testsuite.cpp has key testing code that compares hash of input/output files.

7. Tools & Commands Used:

- cat /path/to/file to view files without editors like nano
- strings /path/to/file to scan binaries for hidden flags or readable strings
- export TERM=vt100 to fix terminal issues inside rsh
- scp user@ip:/remote/path /local to secure copy files for analysis

Conclusion:

We've discovered critical weak points like .rhosts, private keys, and test suites which often contain juicy clues or flags in CTFs. Tomorrow, we'll continue by analyzing the echo server logic and reviewing input/output test files for potential flags.