Temasek Defence Systems Institute

Learning Cyberattack Patterns with Active Honeypots

Chong Wai Hoe (Singapore Air Force)
Koh Chong Khai Roger (ST Engineering – Electronics)
Thesis advisor: Neil C. Rowe
Second Reader: John D. Fulp

Objective

Design, develop and validate active SSH and Web honeypots that can employ a suite of deception techniques.

Problem Definition and Assumption

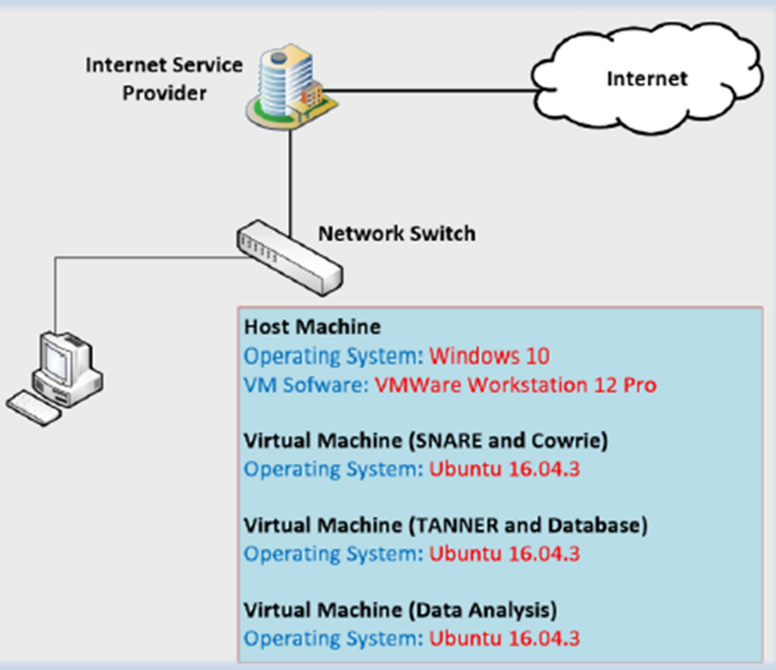
- Honeypots are typically passive in nature.
- They are poor at detecting sophisticated attacks carried out by state-sponsored actors.
- Traffic to the honeypots would mainly be bots and script kiddies.

We aim to determine if the application of deception techniques to honeypot improves their ability to engage cyber attackers and lead them into revealing their attacks tactics and techniques.

Methodology: Tools Used

- Cowrie as our SSH honeypot
  - ✓ Based on the Kippo honeypot
  - ✓ Uses a virtual filesystem to simulate the Debian operating system
- SNARE & TANNER as our Web honeypot.
  - ✓ SNARE generates vulnerabilities that an attacker can exploit
  - ✓ TANNER analyzes and classifies the attacks received from SNARE, evaluates them, and responds based on configured rules.

Network Architecture



Experiments and Analysis of Results

Total of five phases. (1 ,2A, 2B, 2C, 2D).

- Phase 1, we setup the honeypots with minimal changes and configuration, which is then used as a baseline for comparison against the different phases in Phase 2.
- Phase 2A (Fake Files and Defensive Camouflage),
  - ✓ On the Web honeypot, attackers were mostly non-interactive bots performing horizontal scanning to find vulnerable Web pages.
  - ✓ On the SSH honeypot after fingerprinting the server, the next most common action was transferring malicious files onto the honeypot.
- Phases 2B (Delay), 2C (False Excuses) and 2D (Modified Delay and False Excuses).
  - ✓ Most SSH sessions were non-interactive. Such sessions send all their commands at the start of session and do not interact with it thereafter. These clients will not respond to deceptions during the same session.

Conclusion and Future Work

There are limitations on the effectiveness of our deception techniques. For fake file deception, we need a human attacker or a bot that understands the value of different files in the server. Our data showed that most attackers were bots that scanned for vulnerable files and even if the files were available, these attackers did no further action.

We observed that SSH sessions were primarily non-interactive and the attackers did not check the responses we returned.

Attackers have alternative means of transferring files to the SSH server and it would be worthwhile to explore deception techniques against them.

NUS National University of Singapore