HONEYPOT
Lecture 15b

COMPSCI 726
Network Defence and Countermeasures

Nalin Asanka Gamagedara Arachchilage

Slides from Muhammad **Rizwan** Asghar

August 19, 2021

Source of some slides: **University of Twente** and **Northwestern University**

THE UNIVERSITY OF AUCKLAND
NEW ZEALAND

HONEYPOTS

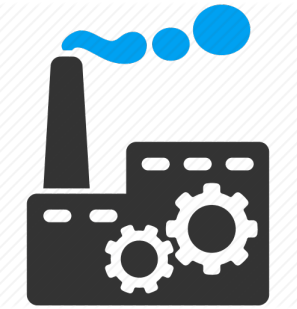
- Decoy systems
  - Filled with **fabricated** info
  - Instrumented with monitors / event **loggers**
  - Divert and hold attacker to **collect activity info without exposing** production systems

- Initially were single systems
- More recently are/emulate entire networks

HONEYPOT TYPES

- Two types
- Physical
  - Real machines
  - Own IP addresses
  - Often highly interactive
- Virtual
  - Simulated by other machines
  - Respond to the traffic sent to the honeypots
  - May simulate a lot of (different) virtual honeypots at the same time

PRODUCTION HONEYPOTS: PROTECT THE SYSTEMS



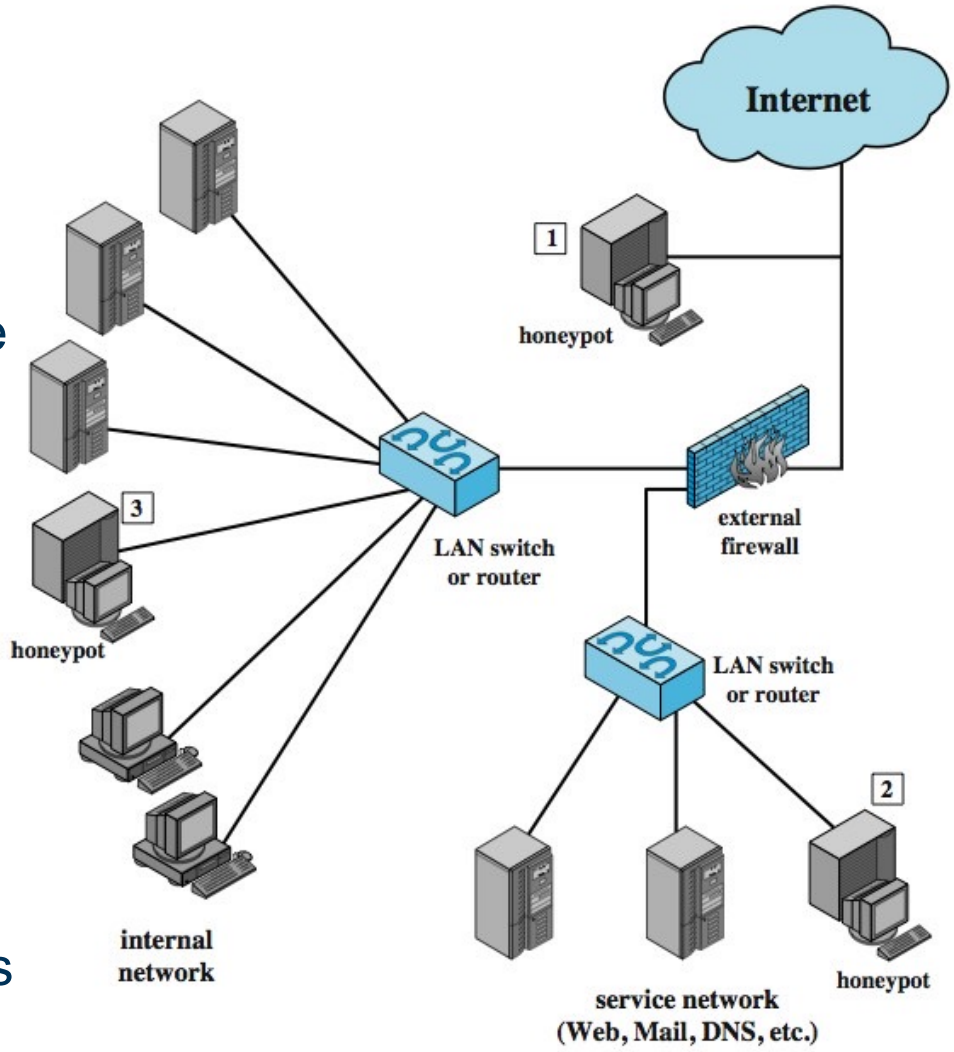
- Detection
  - Detecting the burglar when an attacker breaks in
- Response
  - Can easily be pulled offline
  - Little to no data pollution
- Prevention
  - Keeping the bad guys out

RESEARCH HONEYPOTS: GATHERING INFORMATION

- Collect compact amounts of high value information
- Discover new tools and tactics
- Understand motives, behaviour, and organisation
- Develop analysis and forensic skills

HONEYPOT DEPLOYMENT

1. Outside firewall
   - Good to reduce the burden on the firewall
   - Keeps the bad guys outside
2. Part of the service network
   - Firewall must allow attack traffic to honeypot (risky)
3. Part of the internal network
   - Same as 2
   - If compromised, riskier
   - Advantage is insider attacks can be caught



SUMMARY

- Honeypot IPs are typically not published on any public channels
- Any incoming traffic could be considered suspicious
- A honeypot could be physical or virtual
- A production honeypot uses break-in information for preventing potential attacks
- Honeypot could be deployed outside firewall or could be part of an internal network

RESOURCES

- Read Chapter 5 of
  Network Defense and Countermeasures: Principles and Practices
  Second Edition
  William (Chuck) Easttom
  ISBN-13: 978-0789750945

Questions?

Thanks for your attention!