The Use of Honeynets to Detect Exploited Systems Across Large Enterprise Networks

John Levine, Richard Labella, Henry Owen, Didier Contis, Brian Culver

Proc. Information Assurance Workshop

IEEE, pp. 92-99, 2003

Presented by Bojan Zdrnja

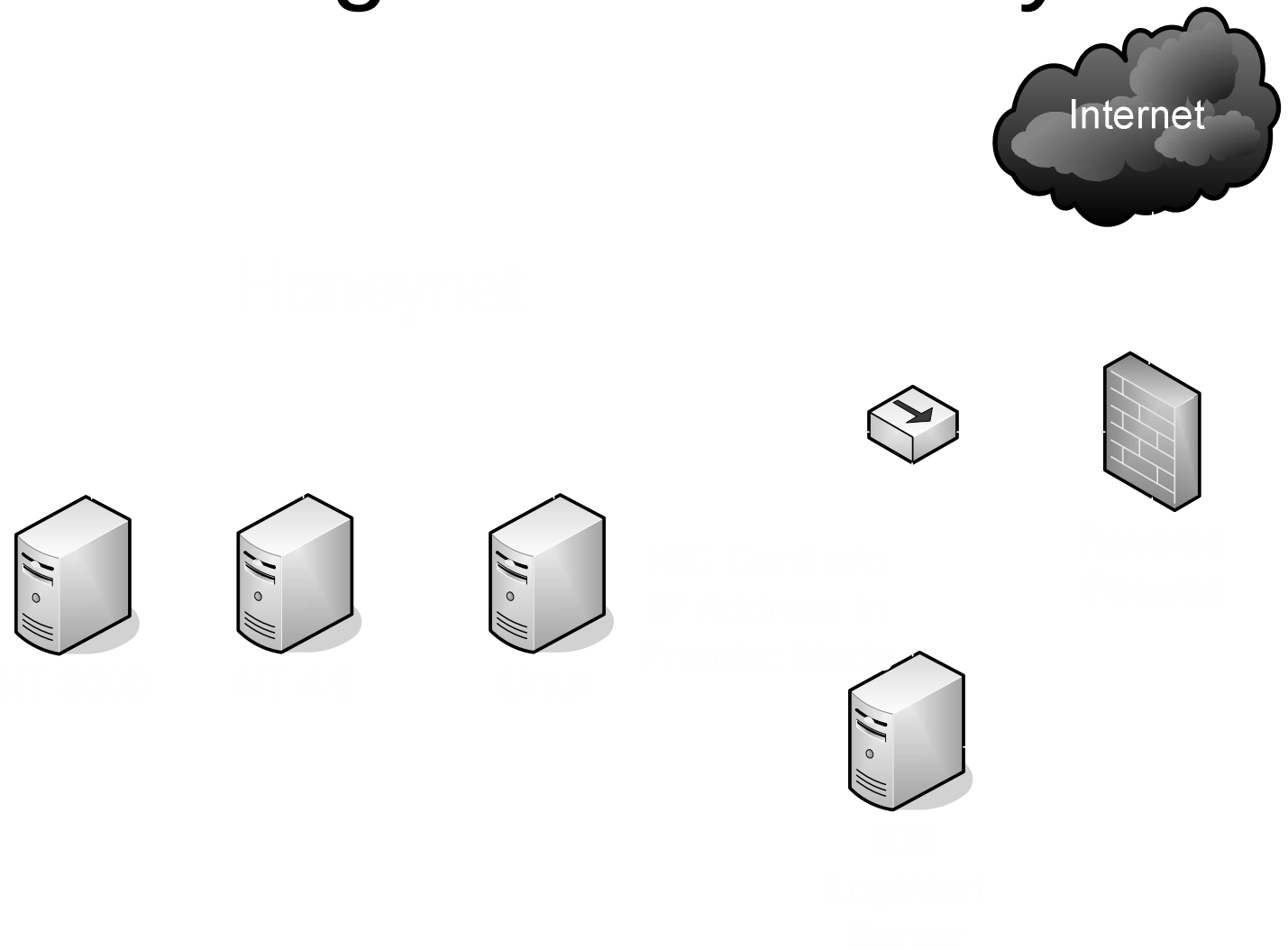
Article Summary

- Article defines purpose and usage of honeynets
- Two critical principles
  - Data capture
  - Data control
- Implementation of the honeynet on the Georgia Tech Campus
- A summary of learned lessons

Critical principles

- Data capture
  - Allows administrator to examine all activities coming to and going from the honeynet
  - A sniffer logs all data packets
- Data control
  - A reverse firewall controls outgoing traffic from the honeynet

Georgia Tech Honeynet



Appreciative comment

- Article is very easy to read and follow
  - It does not rely on the prior knowledge of the reader about honeynets
  - Gives simple definition of honeynets
- Article gives good overview of Georgia Tech honeynet

Critical comment

- Shortcomings in firewall technology are not completely accurate
- “The firewall cannot [completely] protect against the transfer of virus laden files and programs”
  - From my prior experience with firewalls, CVP (Content Vectoring Protocol) allows anti-virus scanning of files passing the firewall

Critical comment (2)

- “...high volumes of network traffic may overwhelm the network monitoring capability of the firewall resulting in the possible passing of malicious traffic between networks.”
  - Firewalls marketed today are fail safe
  - Firewalls certified by ICSA Labs have to conform to the setup rules under all circumstances

Questions

- In a research environment honeynets are used to capture and analyze malicious activities.
- Do you think that this would primarily be the case in a corporate environment as well?

- What possible legal problems can honeynet operators have when they are monitoring and capturing third party activities?