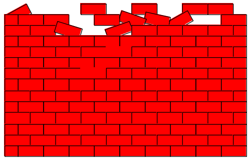
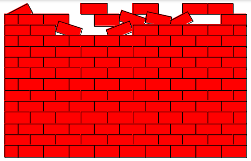


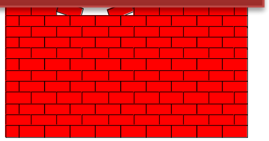
Security Policies

Security Policy Philosophies



- Flexibility
- Service-access
- Firewall Design
- Information
- Remote Access

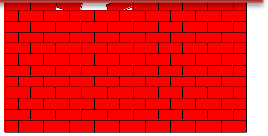
CONT.



Security Policy Philosophies (cont.)

- Flexibility
  - Ability to adapt or change the policy
  - Flexible due to the following considerations:
    - Internet changes
    - Internet risks

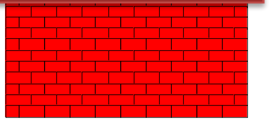
CONT.



Security Policy Philosophies (cont.)

- Service Access
  - Internal user issues
  - Remote access policies
  - External connections

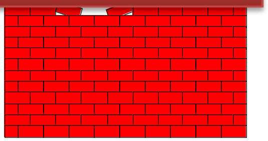
CONT.



Security Policy Philosophies (cont.)

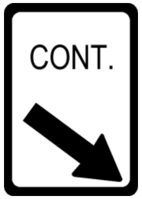
- Firewall Design
  - Permit any service unless it is expressly denied
  - Deny any service unless it is expressly permitted

CONT.



Security Policy Philosophies (cont.)

- Information concerns
  - E-mail
  - Web browsing



Security Policy Philosophies (cont.)

- Remote Access
  - A user’s dial-out capability might become an intruder dial-up threat
  - Outside users must be forced to pass through the advanced authentication features of the firewall

INTRUSION DETECTION AND PREVENTION SYSTEM FOR NETWORK SECURITY

List of topics

- What is an Intrusion Detection System?
- What is an Intrusion Prevention System?
- Honey token systems
- Conclusion

What is an Intrusion Detection System (IDS)?

- It's a technique of detecting unauthorized access to a computer system or a computer network.
  - The detection techniques used by IDS are as follows:
    1. Signature based Intrusion Detection Technique
    2. Anomaly based Intrusion Detection Technique
- Signature based detection scan all the packet on the network and compare them against the database of signatures.
  Example: E-mail an attachment filename of "freepics.exe", which are characteristics of a known form of malware.
- Anomaly based detection perform comparison against the established baseline.
  Example: The number of failed login attempts for a host, and the level of processor usage for a host in a given period of time.
- We use honey token based encrypted pointers for the detection of network attacks on critical infrastructure network

What is Intrusion Prevention System (IPS)?

- Defend the network by stopping the intruders.
  - They not only detect the intrusion but also take some preventive actions and

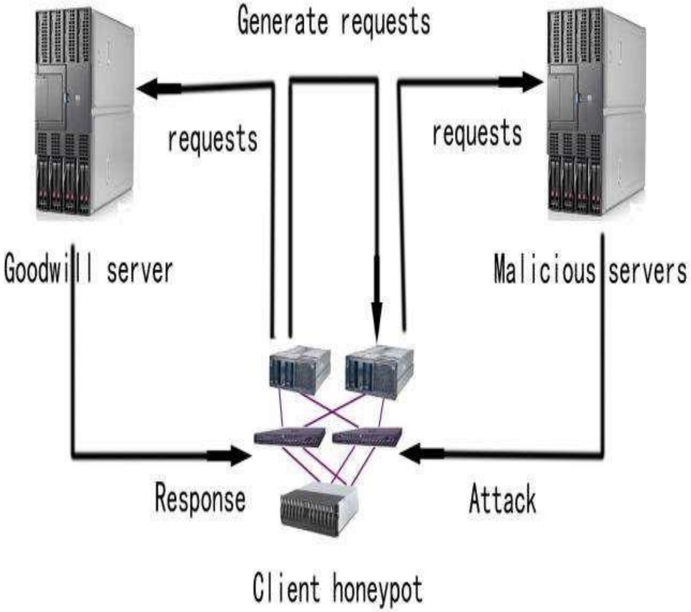
- The detection techniques used by IPS are as follows:

  1. Network-based Intrusion Prevention System (NIPSs)
  2. Host-based Intrusion Prevention System (HIPSs)

  - NIPSs performs packet sniffing and analyze network traffic to identify and stop suspicious activity.
  - HIPSs monitors the characteristics & events of a single host, such as monitoring network traffic, system logs, running processes, file access and modification, and system and application configuration changes.

Honey token systems

- Honey token is the security tool used for the purpose of intrusion detection.
- Its concept is derived from honeypots and honeynets
- A honeypot system is designed to attract hackers.
- After an intrusion, network administrators and security specialists can determine how the attacker succeeded.
- Then prevent subsequent attacks, and identify security gaps.



Conclusion

- Honeypot technology has matured after a leap in its development.
- This technology aims to lure hackers to a decoy system, thus delaying the attack and providing network security specialists a window of opportunity to prevent the threat.
- The technology allows system administrators to know the launch address, verify if the security strategy is effective, and determine if the defense line is solid.
- Network security can be improved when such technologies are combined with the honeypot system.
- We believe that honeypot technology will play a crucial role in global network security.

Reference

1. Practical malware analysis The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski and Andrew Honig ISBN-10: 159327-290-1, ISBN-13: 978-1-59327-290-6, 2012 2

2. Computer viruses: from theory to applications by Filiol, Eric Springer Science & Business Media, 2006

3. Android Malware by Xuxian Jiang and Yajin Zhou, Springer ISBN 978-1-4614-7393-0, 2005

4. Hacking exposed™ malware & rootkits: malware & rootkits security secrets & Solutions by Michael Davis, Sean Bodmer, Aaron Lemasters, McGraw-Hill, ISBN: 978-0-07-159119-5, 2010

5. Windows Malware Analysis Essentials by Victor Marak, Packt Publishing, 2015