Deploying Honeynets Outside and Inside Your Network and Integration with Your SIEM

A.N. Ananth, CEO, EventTracker
Preview of Key Points

- Honeypots and Honeynets
  - What are they? How do they differ?
  - How is Honeynet different than Threat Intelligence?
- Traditional strategic/pure purpose
  - Why were they created in the first place?
- Re-purposing for tactical/applied defense
  - How they can be used in practice?
- Pre-built tools
- The inevitable arms race
- Getting the benefit of a honeynet without all the work
- Examples of how they help
Honeypots

- Honeypot
  - Stand up a system
  - Turn on logging
  - Connect it to the Internet
  - Wait and watch
- Honeynet
  - Same idea but with multiple systems
- Virtual honeynet
  - Same idea but with 1 or just a few systems
  - Present a façade of many systems behind lots of IP addresses
  - High and low interaction
- Getting the benefit of a honeynet without all the work
  - Checkout EventTracker
Honeypots v/s Threat Intelligence

• Threat Intelligence
  • Malicious activity observed
  • Shared globally or to subscribers
  • Open Source or Paid
• Honeynet
  • Observe malicious activity
  • Add to watch list
  • Provide input to the SIEM
Traditional Strategic Purpose

- Learn about hackers techniques
- Not practical for most organizations
  - Requires loads of time and expertise
  - Honeynet project estimates 30-40 hours to analyze 30 minutes of hacking
Re-purposing for tactical/applied defense

- Honeynets are being recognized for another type of application
- Tactical defense by organizations that wouldn’t be able to justify a honeynet for research and learning purposes
- Honeynets provide 3 tactical defense capabilities
  - Highly reliable detection
  - Very timely and specific threat intelligence
  - Attacker resource sink
Tactical defense capabilities

- Highly reliable detection
  - Internal network
    - Intruders
  - External network
    - Attackers
    - Benign Internet scanners
Tactical defense capabilities

- Very timely and specific threat intelligence
  - More applicable to external networks
  - You can subscribe to bad reputation IP address threat feeds
    - How up-to-date and accurate?
    - Do they show targeted attacks specific to you?
- Collect source addresses from incoming traffic to your honeynet
  - Which connection attempts look likely to be malicious?
- Build that into a real-time feed to your other security technologies
  - Firewall
  - SIEM
  - IPS
Tactical defense capabilities

- Attacker resource sink
- Benefits
  - Slow down attacker’s advance
  - Simultaneously speed up detection
    - And response
Pre-built Tools

- [http://www.honeynet.org/project/](http://www.honeynet.org/project/)
  - Honeyd
  - Nepenthes
  - Glastopf
  - Honeywall
- The challenge
  - Most honeynet tools are designed for strategic researchers not tactical defenders
  - Overkill
    - All are going to generate more information than you can analyze
    - You are going to be able to use many of analysis features and add-on tools
- Concentrate on
  - Building a honeynet that looks realistic as possible
  - Hides your legitimate systems in a haystack
  - Provides automated alerting
  - Threat feed
  - Safe against capture and recycling by attacker
The inevitable arms race

- The inevitable arms race
- Low vs high interaction
- Dispersal level
- Circumvention
  - Find the honeynet documentation
  - Find legit network documentation
  - Reverse engineer dispersal scheme
Bottom line

- Concept: use honeynets to as a direct tactical defense
- Avoid getting hung on research analysis
- Redirect that energy to making your honeynet
  - Look as realistic as possible
  - Dispersed as widely as possible through your legit systems
  - And leveraging activity on the honeynet to
    - Alert you of internal attacks
    - Provide timely, accurate threat intelligence
Benefits

• Limits the effects of internal and external cyber-attacks by detecting suspicious activity, providing false data to attackers, and alerting network administrators of critical issues
• Acts as an excellent source of threat intelligence; information is current, locally relevant and timely with minimum maintenance
• Prevents hostile attackers from performing reconnaissance on private networks
• Improves situation awareness across networks
Capabilities

- Defeats hostile reconnaissance with deception
- Uses machine learning to automatically classify suspects without exploitable signature databases
- Complements and works well with existing intrusion detection systems
- Provides an easy-to-use web interface for viewing status and configuration
- Generates automated alerts to the EventTracker Incidents dashboard when a hostile entity is discovered
Examples

Good guys work from the map, bad guys work from the terrain

- Malware somehow makes its way inside the network
- Infection spreads laterally
- Trips over the honeynet
- Gets added to the active watch list

- Bad guy scans the network from outside
- Add IP Address to active watch list
- Check if that IP Address is seen inside
Thank you.