Honeypots & Honeynets

Adli Wahid

Issue Date:
Revision:

APNIC

Contents

1. Objectives
2. Definition of Honeypot & Honeynets
3. Benefits & Risk consideration
4. Example of Honeypot tools
5. The Honeynet Project

Credits: David Watson (Honeynet Project) for the some of the contents of this slide david@honeynet.org.uk

Objectives

1. Understand the the concept of honeypots / honeynets and how they are deployed
2. Understand the value of honeypots and honeynets to security researchers, security response teams
3. Familiarize with different types of honeypots
4. Share experience deploying honeynets

Know Your Enemy

How can we defend against an enemy, when we don’t even know who the enemy is?

(Lance Spitzner 1999)

Know Your Enemy (2)

To learn the tools, tactics and motives involved in computer and network attacks, and share the lessons learned

(Mission Statement, The Honeynet Project)

Threat Intelligence, Indicators of Compromise

How do we detect attacks or vulnerabilities in our networks?

- Hint
  - How do attackers do it?
  - Name the controls that we have in place

- What are the limitations of the controls that we have in place?
- What are the targets & why ?

Honeypots and Honeynets

- A honeypot is an information system resource whose value lies in the unauthorized or illicit use of that resource
- Honeypot systems have no production value, so any activity going to or from a honeypot is likely a probe, attack or compromise
- A honeynet is simply a network of honeypots
- Information gathering and early warning are the primary benefits to most organisations

Honeypot and Honeynet Types

- Low-Medium Interaction (LI)
  - Emulates services, applications and OS's
  - Easier to deploy/maintain, low risk, but only limited information
- High-Interaction (HI)
  - Real services, applicatios and OS's
  - Capture extensive information, but higher risk and time intensive to maintain

Honeypot and Honeynet Types

- Server Honeypots
  - Listen for incoming network connections
  - Analyse attacks targeting the hosts, services and operating systems

- Client Honeypots
  - Reach out and interact with remote potentially malicious resources
  - Have to be instructed where to go to find something malicious
  - Analyse attacks targeting clients application

Honeypot and Honeynet Pros / Cons

Pros

- Simple Concept
- Collect small data sets of high value
- Few False Positives
- Catch new attacks
- Low False Negatives
- Can beat encryption
- Minimal hardware
- Real time alerting

Cons

- Potentially complex
- Need data analysis
- Only a microscope
- Detection by attackers
- Risk from compromises
- Legal concerns
- False negatives
- Potentially live 24/7
- Operationally intensive

Implementing Honeypot

Recap

Evilness

Malware

Badness

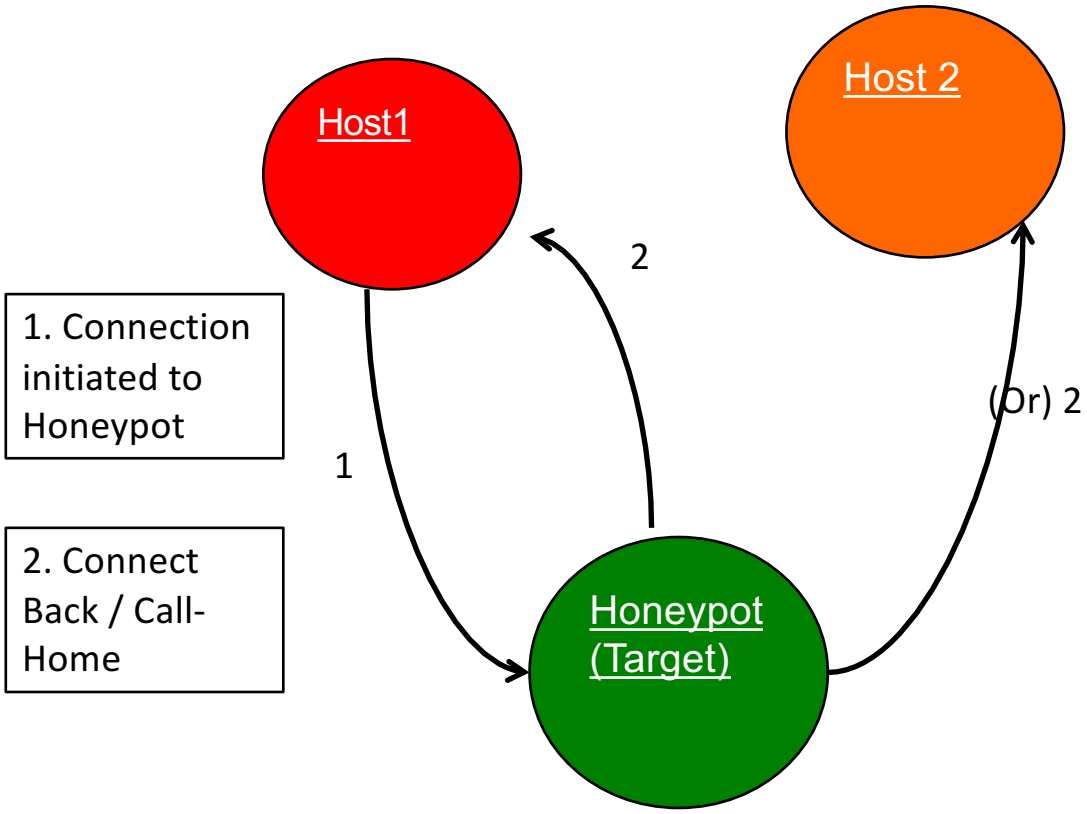
Noise

Honeypots: Computer resource(s) to be probed and/or attacked

Why would you want to do this?

- By right, you should not expect any real activity or traffic to/from/in your honeypot
- Detect anomalous activities in your network or system?
  - Infected / Compromised computers
  - Misconfiguration
- Learn about attacks on the Internet (in the wild)
  - Context
  - Attack source and techniques
  - Vulnerabilities exploited
  - Information Sharing opportunities
- Improve overall security

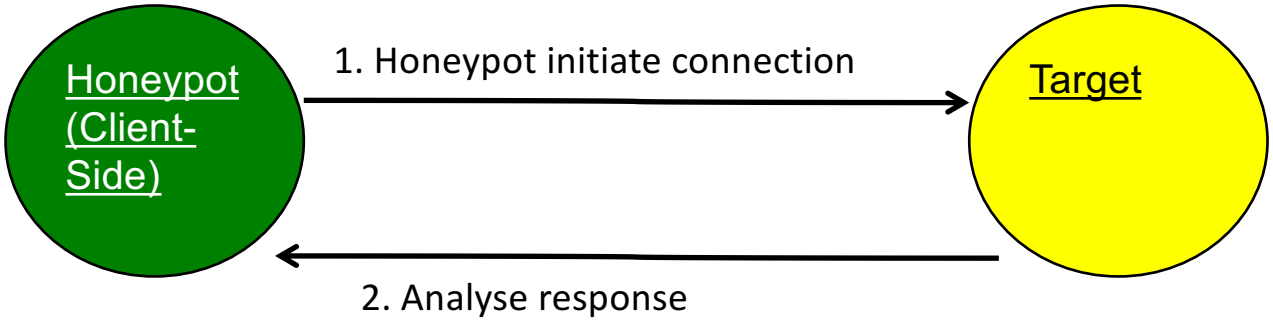
Scneario 1: Generic ‘Network-based Attack’



What can you learn?

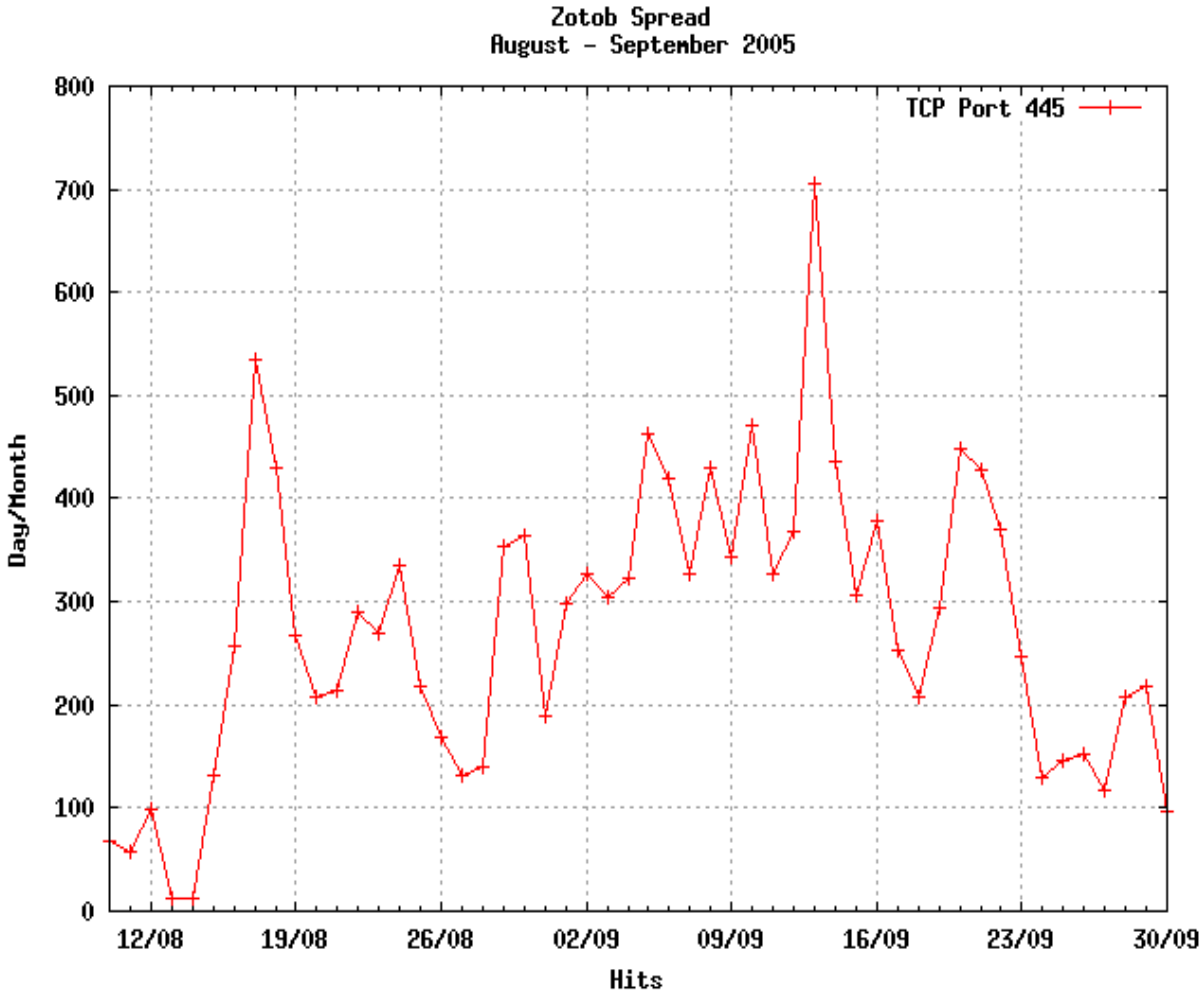
- Hosts that are trying to connect / scan you
  - Potentially already compromised or infected
- Scripts, binaries, files, toops fetched or dropped
- Requests being made, Login attempts
- Packets, netflows
- Source of attack
- Relationships with other systems
- Command potentially executed

Scenario 2: Client-based Honeypot



What you can learn?

- (0-days) or attacks on the Client Application (i.e. Web Browser)
- Learn about hosts / computers that are hosting malicious websites
  - <Iframes>
  - Javascript
  - Flash
  - PDF etc


Zotob Spread
August - September 2005
TCP Port 445
800
700
600
500
400
300
200
100
0
Day/Month
12/08
19/08
26/08
02/09
09/09
16/09
23/09
30/09
Hits

Logs

- 2010:09:14:07:13:10 < honeypot> 2010-09-14 07:19:27 GMT **184.y.z.144** **a05dfd7cca7771a7565a154d65f05ea2** **http://domain.lv/inx/fx29id1.txt????**

- 2010:09:14:07:13:11 < honeypot> 2010-09-14 07:19:30 GMT **184.y.z.144** **8dcad47f3e32e7dc1aee59167e67c601** **http://domain.lv/inx/fx29id2.txt?????**

Honeypot Systems

High Interaction Honeypot

- Think about your goals and objectives first
- Possible scenario
  - Setup a real system and make give it an IP address (so it is reachable to something)
  - i.e. Install a Windows, Linux, Unix server)
- Challenging to control & manage
  - What if attacker use system to launch attack to other systems
  - Keeping the computer in a usable state

Open Source Systems

- Honeyd, Amun – (open multiple ports)
- Dionaea, Nepenthes (Malware)
- Kippo, Cowrie - SSH honeypot
- Glastopf – Web Honeypot
- Ghost – USB Honeypot
- Thug – Client Honeypot
- Conpot – Industrial System

Dionaea

- 2nd Generation low interaction honeypot
  - Python, runs on *NIX
  - IPv6 Support
- Goals
  - Detect both known and unknown attacks
  - Better protocol awareness
  - Vulnerability modules in scripting language
  - Shell code detection using LibEmu
- Check out http://dionaea.carnivore.it
- Learn about attacks, malware and many more

Kippo

- Emulate SSH server
  - Allow ‘attacker’ to log-in using credentials (username and password)
  - Environment allow limited commands – i.e. ping, who, and wget
  - Record activities (keylog) of attackers and their activities
- Cowrie
  - Fork of Kippo
  - Also does Telnet honeypot

Glastopf Web Honeypot

- Minimalistic web server written in Python
- Scans incoming HTTP requests strings
- Checks for remote file inclusion (RFI), local file inclusion (LFI) and SQL injection
- Signatures and dynamic attack detection
- Attempt to download attack payloads
- Search keyword indexing to draw attackers
- MySQL DB plus web console
- Integration with botnet monitoring & sandbox
- Visit www.glastopf.org

Ghost

- USB Honeypot
- Runs on Windows
- Many malware spread across systems using thumbrive (and bypass network containment stragegies)
  - i.e. Stuxnet, Conficker
- Trick malware into thinking that a USB Thumbrive has been inserted
- Captures malware written on USB
- More: https://code.google.com/p/ghost-usb-honeypot

Thug

- Low Interaction Client-based honeypot to emulate web browser
  - Browser Personalities (i.e. IE)
  - Discovering Exploit Kits, Malicious Websites
- Scenario – your website have been compromised and attacker placed a malicious script on your website
- **Python vulnerability modules:** activeX controls, core browser functions, browser plugins
- **Logging:** flat file, MITRE MAEC format, mongoDB, HPFeeds events + files
- **Testing:** successfully identifies, emulates and logs IE WinXP infections and downloads served PDFs, jars, etc from Blackhole & other attack kits
- More information
  - http://www.honeynet.org/node/827

VOIP Honeypots

- PBX deployment lacks security / expose to the Internet
- Tools live SIPvicious are used to scan the Internet for PBX
- Miscreants exploit weak authentication & access control to make long distance calls
- Organisations lose $
- Honeypots can be used to identify source of attacks:
  - Artemisa

Canary - Honey Tokens

- Discover that you've been breached
- Tokens = a digital object - file(s), emails, web page, image
- Deployed in certain location to detect (attract) malicious activities
  - Example:
    - mail in inbox or mailserver,
    - Files (PDF, HTML, Doc, XLS, etc) in fileserver, usb stick, webserver, cloud
  - Confidential.pdf, analysis.xls, networkdiagram.ppt

- Canary Tokens by Thinkst
  - https://www.canarytokens.org
  - http://blog.thinkst.com/p/canarytokensorg-quick-free-detection.html

- Further reading
  - http://www.slideshare.net/chrissanders88/using-canary-honeypots-for-network-security-monitoring?from_action=save

Security Education

- USB Sticks
  - Associated with malware
  - Social Engineering or Targeted Attack
  - Create Awareness, test
- Canary Tokens
  - https://www.canarytokens.org
- Triggered!

One of your canarydrops was triggered.

Channel: HTTP
Time : 2016-05-26 05:47:49.009176
Memo : usbstix-03
Source IP: 203.119.X.Y
User-agent: Mozilla/5.0 (Macintosh; Intel Mac OS X) Word/14.61.0

Supporting Tools and Projects

- Cuckoo Sandbox
- Visualization
- The Honeynet Project
  - HPFeed
  - Information Sharing
- Log Analysis

Cuckoo Sandbox

- Automated Malware Analysis System
  - Why not just use Anti-Virus?
- Analyze Windows executables, DLL files, PDF documetns, Office documents, PHP Scripts, Python Scripts and Internet URLs
- Windows guest VMs in Virtual Box Linux
- Windows hooking / driver plus python modules for extracting and analysing sample executions

Cuckoo Sandbox (2)

- Analyze Binaries, Files captured in a honeypot
- Trace of relevant win32 API calls performed
- Dump network traffic generated (pcap)
- Creation of screenshots taken during analysis
- Dump of files created, deleted and downloaded by the malware during analysis
- Extract trace of assembly instructions executed by malware process
- http://cuckoobox.org
- http://www.malwr.com

Virustotal.com

- Site for analyzing malware samples (or unknown files)
- Let’s scan some file

Traffic Analysis

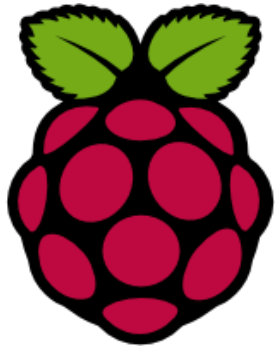
- Full Packet Capture (PCAP)
  - Supporting tools (Wireshark, TCPDUMP, Moloch)
  - Consider size of file
- Netflow
  - Argus
  - SurfNet IDS
- Malicious Traffic or Not?
  - Snort
  - Bro IDS

Visualization

- Many of the tools do not really have a GUI
- Reporting / Presentation is key
- Many visualization tools
  - HPFeeds
  - PicViz
  - Afterglow
  - Gnuplot
  - Splunk
  - Plug-ins or front-end for many of the existing tools

Hardware

- Any (old) hardware with network interface
- Single board computers (i.e. Raspberry Pi)
- Virtualization is another option



Community - The Honeynet Project

- The platform for those interested in running, building and learning from honeypots
  - http://www.honeynet.org
- Many Chapters from around the world
- Initiative for information sharing
  - HP Feeds
  - http://hpfeeds.honeycloud.net
- Google Summer of Codes (GSOC)

Commercial Solutions?

- Canary Tools
  - https://canary.tools
  - http://arstechnica.com/security/2015/05/canary-box-aims-to-lure-hackers-into-honeypots-before-they-make-headlines/
- (older?)
  - Spector (Symantec)
  - Mantrap

Consider!

- Installing and playing with Honeypots to learn about security
- Deploying it internally to catch malicious activities
- Joining the Honeynet Project
- Sharing your experience and knowledge
- Happy Honeypotting!

Demo

1. Kippo, SSH Honeypot
   - Bruteforce
   - Compromise Linux / Unix servers, routers
2. Deploymnent Experience
   - The Modern Honeypot Network (MHN)
   - Framework for managing and deploying honeypots

Kippo Demo

MHN Installation

- Running multiple honeypots
  - http://threatstream.github.io/mhn/
- Setup Experience
  - Using LXC
  - Debian/Ubuntu Systems
  - Easy to add & Remove Honeypots
  - Data aggregated
- Supporting System
  - Moloch (http://molo.ch)
  - Maltrail (https://github.com/stamparm/MalTrail)
  - BRO IDS
- Other Free Tools
  - Let's Encrypt (TSL/SSL Certificates)
- Demo! (no picture please)

Moloch https://molo.ch

- Moloch is an open source, large scale IPv4 packet capturing (PCAP), indexing and database system.
- A simple web interface is provided for PCAP browsing, searching, and exporting. APIs are exposed that allow PCAP data and JSON-formatted session data to be downloaded directly.
- Moloch is not meant to replace IDS engines but instead work along side them to store and index all the network traffic in standard PCAP format, providing fast access.
- Moloch is built to be deployed across many systems and can scale to handle multiple gigabits/sec of traffic.

Maltrail

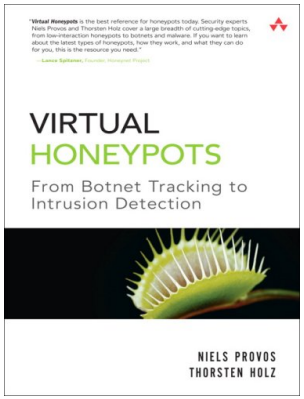
- **Maltrail** is a malicious traffic detection system, utilizing publicly available (black)lists containing malicious and/or generally suspicious trails
- Static trails compiled from various AV reports and custom user defined lists, where trail can be anything from domain name to ip addresses
- Trails are pulled from
- https://github.com/stamparm/MalTrail

Recap

- How can we use Honeypots / Honeynet in our envirionment?
- How can it complement existing security countermeasures
  - Detection
  - Education
  - Response
- What if the honeypot does not receive anything – hits/traffic/etc?

Learn More!

- Play with one
  - Honeydrive Virtual Machine
  - https://bruteforce.gr/honeydrive
  - Linux based honeypot distro
  - Many toos & honeypot systems
- Deploy one yourself
  - Inside the organization
  - On the Internet / DMZ
- Participate in a project
  - Write Code
  - Help / Document
- Honeynet Project
  - http://www.honeynet.org



More Honeypots

- https://github.com/paralax/awesome-honeypots
- Joint Honeypot / Honeynet projects
  - Distributed Sensors?
  - Share data and observation?
  - Automated alerts

Questions?

Email: adli@apnic.net
Twitter: adliwahid
LinkedIn: Adli Wahid
Blog: https://blog.apnic.net