Introduction to Honeypots

Adli Wahid
Senior Internet Security Specialist, APNIC
$whoami

APNIC since 2014

Security Engagement / Outreach Activities
Training, Workshops, Conferences
APNIC Community Honeynet Project

Let's Connect
Twitter: @adliwahid
LinkedIn: Adli Wahid
Keybase: https://keybase.io/adliwahid

Using Zoom for this webinar

- Keep chat settings to “All Panelists and Attendees”
- Use chat to share text, information, URLs amongst all attendees

- If you wish to ask a question to the presenters:
  - Click the Q&A button
  - Type your question
  - The presenters will then answer your questions at an appropriate time
  - Note: Only the presenters will see your question, not other attendees
  - Please don’t use chat to ask questions of the presenters, we might not see it

- If something goes wrong, re-join meeting 😊
Agenda

1. Honeypots & Honeynet
2. Practical Use Cases
3. Observation from our Community Honeynet Project
4. Questions / Discussions

Intended Outcomes

1. Learn about Honeypots
2. Assess if this is useful for your security (journey)
Introduction to Honeypots

Honeypots & Honeynet

The Cuckoo’s Egg – Clifford Stoll

- Book published in 1989
  - 1986 – over 10 months of investigations
  - $0.75 accounting error
- First person account of the hunt for a computer hacker who broke into the Lawrence Berkeley National Lab (LBNL)
- We have detected an intruder and intrusion, now what?
- Story about
  - Unauthorised Access
  - Vulnerability exploitation
  - Lateral Movement
  - Exfiltration
  - Detection / Monitoring
  - Deception
  - Collaboration
  - A bit of history of the Internet
- TL;DR
  - https://youtu.be/1h7tLHNXio8 (talk by Clifford Stoll)
  - https://en.wikipedia.org/wiki/The_Cuckoo%27s_Egg
Learning from compromised systems

- Can be a bit tricky or complicated
- Production
  - Real data / services
  - In principle should be hardened
  - Prioritise on recovery
- What if
  - We can emulate real systems
  - ‘Attract’ adversaries
  - Observe and collect information
  - Do the above in a controlled environment
Honeypots

• Know your enemy
  o How can we defend against an enemy, when we don’t even know who the enemy is? (Lance Spitzner, 1999 – The Honeynet Project)

• Purpose
  o To learn the tools, tactics and motives involved in computer and network attacks, and share the lessons learned – (Mission Statement, The Honeynet Project)
  o Today’s term: TTPs – Tactics, Techniques and Procedures
  o Research (Learning) vs Production (Detection / Detection)
    o MITRE ATT@CK Framework

Honeypots and Honeynet

• A honeypot is a resource (system) 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 attempt to 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-Interaction (LI)
- Emulates services, applications and OS’s
- Easier to deploy/maintain, low risk, but only limited information
- Example: Emulate SSH (22) / Telnet (23) Service and wait for connection

### High-Interaction (HI)
- Real services, applications and OS’s
- Capture extensive information, but higher risk and time intensive to maintain
- Example: Setup a real system with services enabled

### Server-based Honeypots
- Listen for incoming network connections
- Analyse attacks targeting host’s users, services and operating systems
- Example: SSH, RDP, Web, etc

### Client Honeypots
- Reach out and interact with remote potentially malicious resources
- Have to be instructed where to go to find suspicious
- Analyse attacks targeting clients and users
- Example: Browser
Introduction to Honeypots

Practical Use Cases

Web Honeypot

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 8dcad47f3e32e7dc1ae59167e67c601 http://domain.lv/inx/fx29id2.txt

SSH / Telnet Honeypot

```
{
  "sensor": "#123",
  "username": "root",
  "password": "12345",
  "session": "b2ec6f0b025e",
  "src_ip": "37.49.226.108",
  "message": "login attempt [root/12345] succeeded",
  "timestamp": "2020-01-31T05:32:17.840426Z",
  "eventid": "cowrie.login.success"
}
```

```
{
  "sensor": "#123",
  "username": "root",
  "password": "888888",
  "session": "dbd314a4bff7",
  "src_ip": "37.49.226.108",
  "message": "login attempt [root/888888] succeeded",
  "timestamp": "2020-01-31T05:32:25.090127Z",
  "eventid": "cowrie.login.success"
}
```
SSH / Telnet Honeypot

```json
{
  "eventid": "cowrie.session.file_download",
  "shasum": "8db2acdd3fee2c0377f0d15d5611555f0ca42533234553a9575d575b453a29",
  "url": "hxxp://45.84.196.85:80/Mirai/x86",
  "timestamp": "2020-01-30T00:17:14.279788Z",
  "destfile": "-",
  "src_ip": "45.84.196.85",
  "outfile": "var/lib/cowrie/downloads/8db2acdd3fee2c0377f0d15d5611555f0ca42533234553a9575d575b453a29",
  "session": "68ef416043c2",
  "message": "Downloaded URL (http://45.84.196.85:80/Mirai/x86) with SHA-256 8db2acdd3fee2c0377f0d15d5611555f0ca42533234553a9575d575b453a29 to var/lib/cowrie/downloads/8db2acdd3fee2c0377f0d15d5611555f0ca42533234553a9575d575b453a29",
  "sensor": "55632b82fd0b"
}

https://www.virustotal.com/gui/file/8db2acdd3fee2c0377f0d15d5611555f0ca42533234553a9575d575b453a29c4/detection
```

Generic ‘Network-based Attack’ Pattern

1. Connection initiated to Honeypot
2. Connect Back / Call Home

Or 2

Honeypot (Target)
Honeytokens

- A honeytoken is data or a computing resource that exists for the purpose of alerting you when someone accesses it
- Deception -> Detection
- How do I know if there’s an adversary in my network already?

Scenario

- Adversary _already_ inside your infrastructure or valuable target
- Detection on hosts & strategic locations
- Multiple Forms:
  - Usernames / Passwords
  - URL / Links
  - Files
  - Web Pages
  - ETC – Check out https://www.canarytokens.org

- Adversary access tokens and announce their presence
Use-Case Fileserver

Honeypot Software

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Feature / Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Cowrie</td>
<td>Telnet / SSH Emulation</td>
</tr>
<tr>
<td>2</td>
<td>Amun</td>
<td>Vulnerability emulation</td>
</tr>
<tr>
<td>3</td>
<td>Dionaea</td>
<td>Vulnerability emulation</td>
</tr>
<tr>
<td>4</td>
<td>Glastopf</td>
<td>Web honeypot</td>
</tr>
<tr>
<td>5</td>
<td>Conpot</td>
<td>Industrial Control System / SCADA Honeypot</td>
</tr>
<tr>
<td>6</td>
<td>RDPy</td>
<td>Microsoft Remote Desktop Protocol (RDP) honeypot</td>
</tr>
<tr>
<td>7</td>
<td>T-POT, CHN, MHN</td>
<td>All-in-one honeypot deployment (docker, database, ES)</td>
</tr>
</tbody>
</table>

More honeypots software - https://github.com/paralax/awesome-honeypots
Companion Tools

• Log collection and analysis
  – Database, Elastic Search, Splunk

• Malware analysis
  – Cuckoo Sandbox, VIPER

• Enrichment
  – TheHive/Cortex, logstash, API

• Network Related
  – Maltrail, Suricata, Zeek, Moloch, etc

Bottom Line

• What do you want to do?
• Helps to define
  – To setup a honeypot or not
  – Location
  – Companion Tools
Introduction to Honeypots

Observations from the APNIC Community Honeynet Project

About the Project NIC Community Honeynet Project

Context

- Part of network security training – using honeypots for understanding network security attacks / threats.
- Attackers are using your infrastructure to do evil things
- Lots of interests to deploy and ‘learn more’ after the training
- Opportunity to learn, share data and more!

Collaboration

- Partners deploy honeypots, APNIC support the backend
- Summary of information collected form distributed honeypots
- Explore opportunities to learn more & connect with security communities
extensively use opensource tools – CHN, MHN, Elastic, etc

Outcomes - so far

1. More than 100 honeypots in AP region (more to come) since 2017
2. Partners different economies. Some mentions: GEMNET (MN), MYREN (MY), UPSI (MY), EZCOM (KH), UII (ID), Fibre@HOME (BD), Bhutan Telecom (BT), BTCIRT (BT), TCC (TO)
3. Users from security response communities & researchers
4. DASH, collaboration with APNIC Product Team
5. Training/Workshops on Honeypots in various locations – live installation of honeypots in the cloud
Summary of all honeypots activities in 2019
- Mystery of Fbot in Security Affairs -
  https://securityaffairs.co-wordpress/96683/malware/linux-fbot-malware-analysis.html
- fbot.x86_64 downloads in November
- Some interesting observations
References

3. The Honeynet Project https://www.honeynet.org

Happy Honeypotting!