Computer & Information Security (3-721-460-1)
Honeypots

Dept. of Software and Information Systems Engineering, Ben-Gurion University

Prof. Yuval Elovici, Dr. Asaf Shabtai
{elovici, shabtaia}@bgu.ac.il

Spring, 2019

Introduction
What is a honeypot ?

- "A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource." (L. Spitzner)
- As a complement to NIDS/HIDS, honeypots act as decoy systems that divert attacks from key resources, provide early detection of mainly external attacks, and enable learning about vulnerabilities in the real systems of the organization
- It is an artificial resource set up as a trap (i.e., usually as a computer, DB, Web/App server) aimed at detecting, deflecting or in some sense counteracting attempts at unauthorized use of information systems
- Filled with fabricated information that a legitimate user of the system wouldn't access

Introduction
What is a honeypot ?

- A honeypot should look genuine and part of a real production network, but also be available, isolated, intentionally unprotected / vulnerable, unobtrusively monitored and indistinguishable from real systems in order to draw the attacker who attempts to exploit it into the trap

- Any interaction with the honeypot is by definition an anomalous situation that should be further reported and investigated

- Forensic information provided by the honeypot is logged and analyzed to gain insight into various attack patterns (i.e., who the attacker is; where, how, and when was the attack launched)

Why use honeypots?

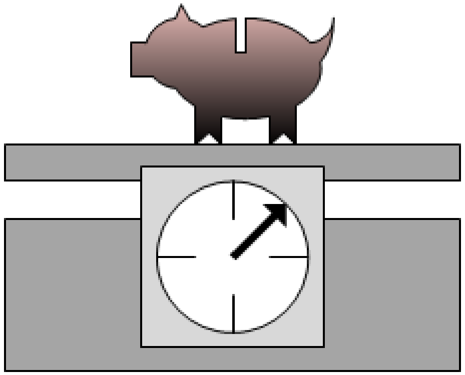
- Spitzner (2003) noted the following main advantages of honeypots:
  - Honeypots collect data only when someone or something malicious interacts with them
  - This makes the data collected by the honeypots highly succinct, accurate, easy to manage, and simple to analyze
  - Honeypots can identify and capture new attacks
  - Since any activity with the honeypot is anomalous by definition, new or unseen attacks are detectable and result in a low false negative rate

Basic terms

- High-interaction vs. low-interaction honeypots
- Server-side vs. client-side honeypots
- Specialized vs. multi-function honeypots
- Related concepts:
  - Honeynet
  - Honeywall
  - Honeytokens

Honeypots vs. honeytokens

- Honeypots consist of computers and/or networks
  A honeypot may detect and capture malicious agents and activity
- Honeytokens are anything but a computer
  A honeytoken is typically a fake resource which can be tracked and monitored if compromised
- Some fake-looking tokens may actually be real

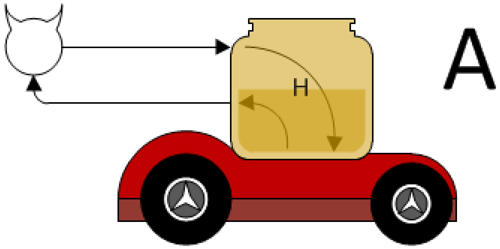


Honeypots categorization

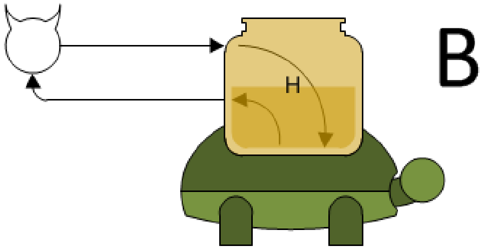
- Goal
  - Research – learn about attackers' methods, tools, and goals
  - Production – protecting real systems by diverting attackers to the trap
- Passive honeypots:
  - An information system resource that waits for an attacker to interact with it
- Active honeypots:
  - Actively attempts to interact with the attacker; for example:
    - Honeytokens are actively sent to untrusted entities, thus forcing them to interact with the honeytokens
    - Client machines actively searching the network for servers interact with the servers and monitor the interaction in order to identify malicious servers

Honeypots categorization
Real vs. virtual, high interaction vs. low interaction

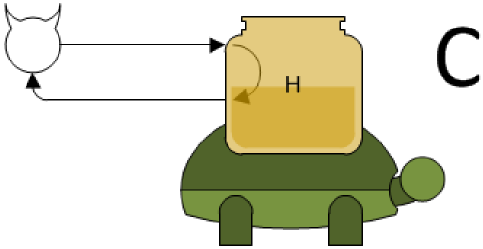
- Implementation
  - Virtual system (high interaction, low interaction)
  - Real/physical system (high interaction)
- A illustrates a real honeypot, while B and C illustrate virtual honeypots
- B depicts a high interaction honeypot, while C depicts a low interaction honeypot



A



B



C

Honeypots categorization
Low interaction vs. high interaction

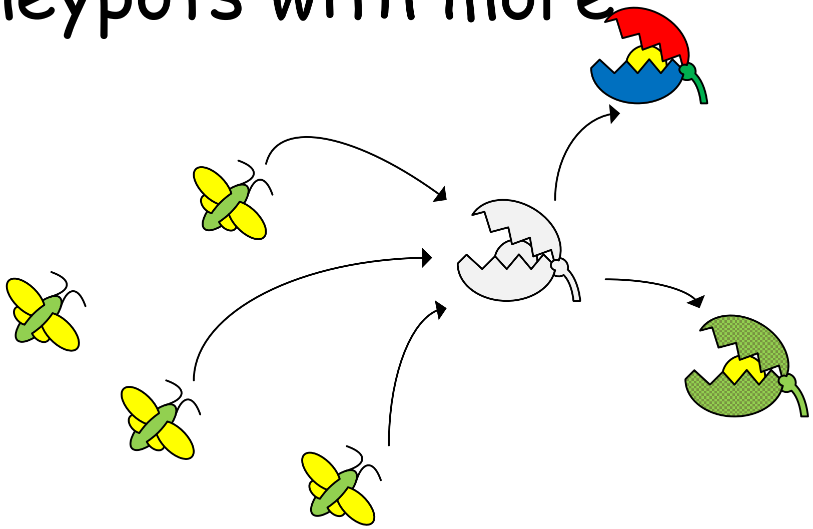
	Low interaction	High interaction
Accuracy	Limited fidelity of emulation Can be detected by skillful attackers	Full and accurate implementation of protocols and services
Detection capabilities	Detects mainly known attacks	Can detect zero-day attacks
Implementation	Emulation by scripts may cause some delays	Typically based on virtualization, with online malware detection instrumentation, incurring significant overhead
Deployment effort	Relatively simple to deploy and maintain	Difficult to deploy and maintain; complex implementation procedures
Detectability	Easily detected - limited interaction (response to the attacker's action)	Hard to detect - setup as real services and provides full/real interaction with the attacker
Forensics data	Limited forensics data can be collected	Complete forensics data can be collected
Security	No real system to be compromised	Can be compromised with harmful results. Needs special protective measures (e.g. Honeywall)

Hybrid honeypots

- High interaction honeypots are difficult to maintain and re-configure or re-deploy
- Requires deep professional knowledge of honeypots and of the organization's resources that need to be protected
- Low interaction honeypots are easy to manage but may be easily detected by attackers
- The solution is hybrid honeypots

Hybrid honeypots

- A low-interaction honeynet (implemented by honeyd for example)
  can redirect specific types of attacks to high-interaction honeypots
-
- (or to other low-level honeypots with more specific instrumentation)



Low interaction honeypot - Hoenyd [Provos 2007]

- Honeyd is a popular honeynet deployment tools, created by Niels Provos

- Main features:
  - "Simulates thousands of virtual hosts at the same time"
  - "Configuration of arbitrary services via configuration files"
  - "Simulates operating systems at the TCP/IP stack level"
  - "Simulating of arbitrary routing topologies"
  - "Subsystem virtualization" (multiple honeypots using single service process)

Dynamic honeypots
Why bother?

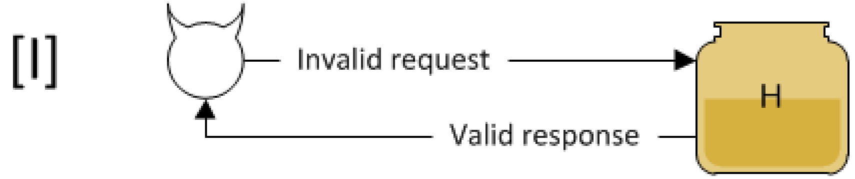
- Honeynets should provide a reliable representation of the network topology, where single honeypots match the current configuration of simulated computers and network devices
- Both the network topology and the nodes’ configuration are dynamic, and constantly change over time
- An improperly configured honeynet or honeypot can be detected and bypassed
- Deploying a honeynet in a large organizational network can be a daunting task, and may require tedious recurring configuration updates as the network mutates
- The solution is dynamic honeynets/honeypots

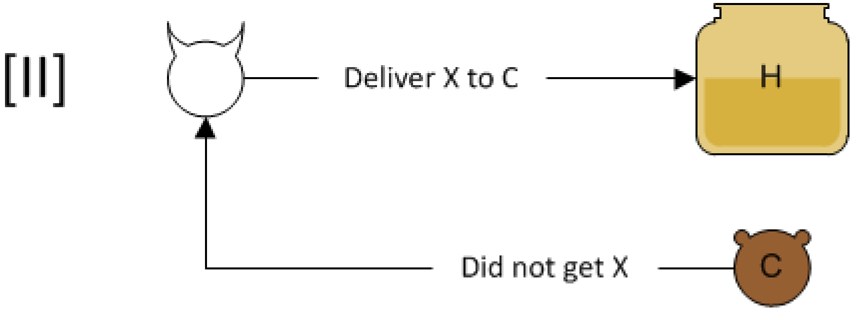
Dynamic honeypots

- "A dynamic honeypot is a plug and play solution that automatically determines how many honeypots to deploy, where to deploy them and what they should look like."
- "an appliance, a solution you simply plug into your network, it learns the network, it learns the environment, deploys the proper number and configuration of honeypots, and adapts to any changes in your networks." (L. Spitzner)

Detecting honeypots

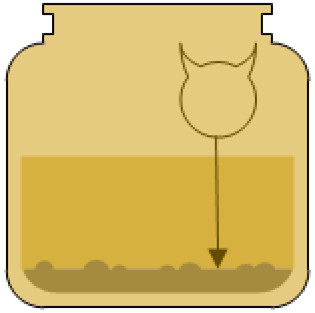
- In case [I], the attacker sends a malformed request to the honeypot. If the honeypot responds, it is detected.
- In case [II], the attacker requests the honeypot to deliver a message to C. If C does not get the message, the honeypot is detected.



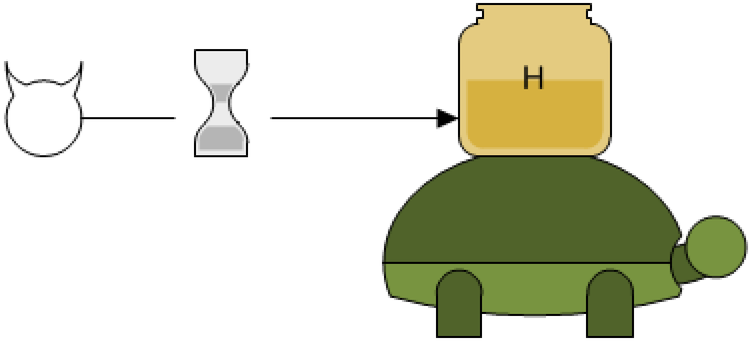


Detecting honeypots

- In case [III], the attacker detects a high-interaction honeypot by searching for residues of virtualization or monitoring instrumentation.
- In case [IV], the attacker measures the time it takes for the honeypot to respond. If the honeypot responds too slowly, it is detected.
- Security defenders who set up honeypots have liability constraint; they cannot allow their honeypots to send out real attacks to cause damage to others!



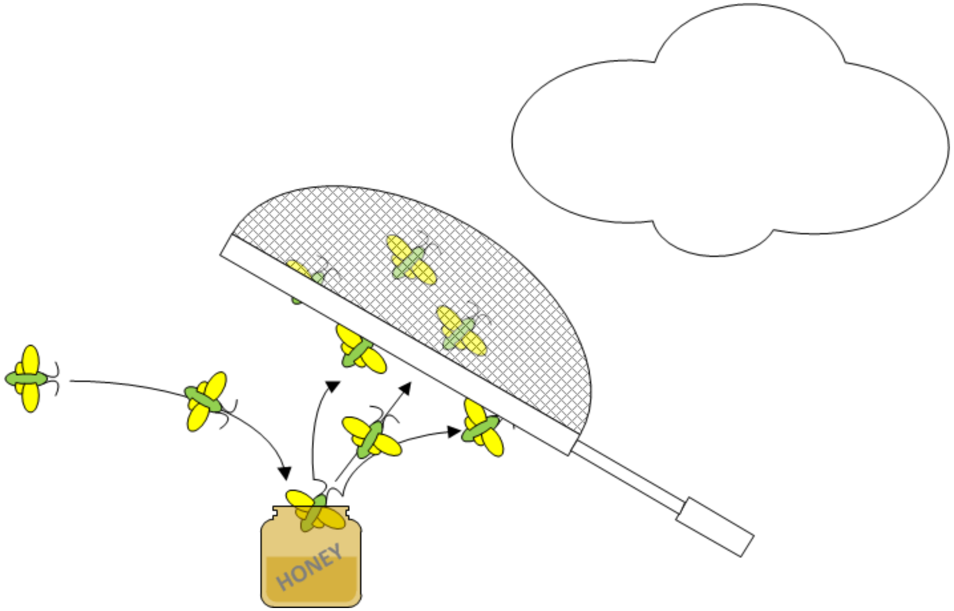
[III]



[IV]

Protecting honeypots

- Some worms or bots may compromise the honeypot and use it to propagate further, infecting third-party machines. In such case, the honeypot owner may be held legally responsible
- A honeywall is intended to contain and eliminate such cases, by blocking suspicious outgoing transport



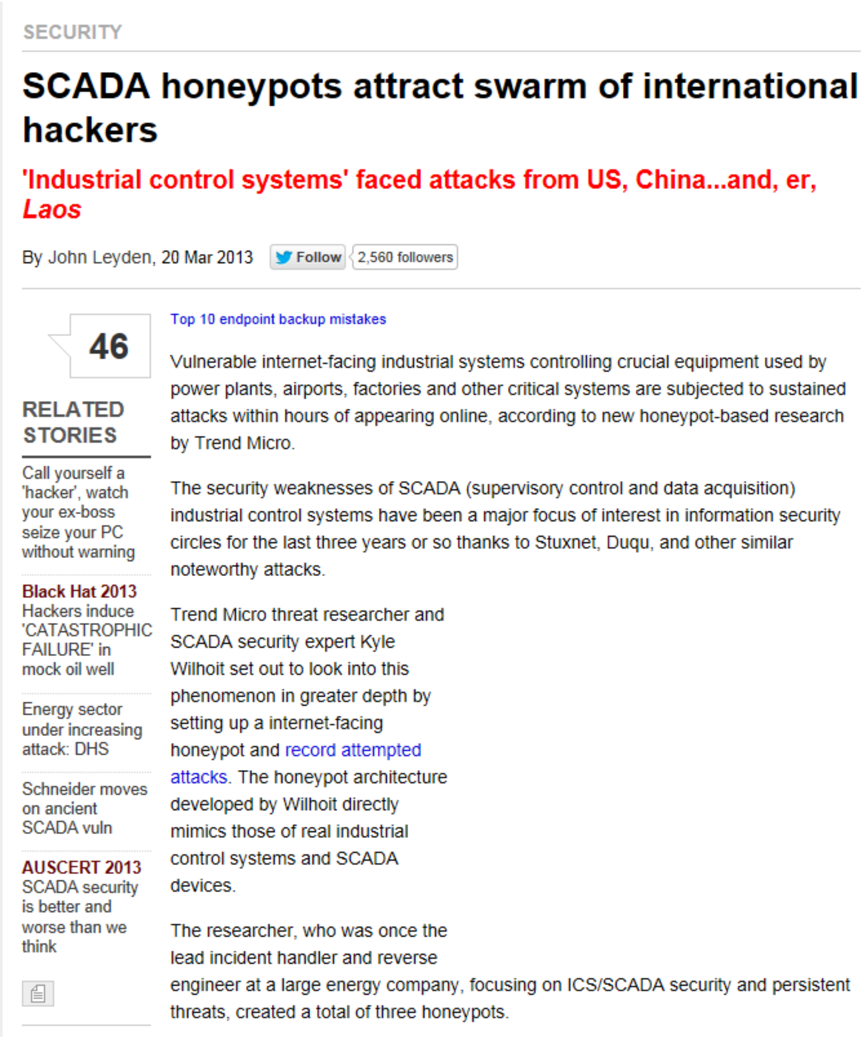
Relevant honeypots

Mobile Honeypot [Wahlisch, 2013]

- Detailed design and implementation of a mobile device honeypot
  - No need to operate the mobile honeypot on a real device – reduces complexity
  - Chose Linux as the underlying OS (Android OS cannot be distinguished from Linux; reuse of existing Linux-based honeypots)
  - Mobile honeypot should be connected to a real mobile network
- Implemented low-interaction honeypot
- Based on Kippo (SSH honeypot), Glastopf (Web-based media server), Dionaea (TFTP, FTP)
- Deployment: one iOS and two Android honeypots connected to DT UMTS network
- Analyzing malicious access via the Internet on smartphones - conclusions:
  - similar amounts of attacks targeting mobile\wired-honeypots – attackers tries to scan the Internet without considering specific network types
  - Observed specific manual attacks that first established SSH connection and then targeting the address book, stored photos
  - Map attackers IPs to the ASes – most of the attacks comes from China and Russia

Relevant honeypots

SCADA Honeypot



SECURITY

SCADA honeypots attract swarm of international hackers

'Industrial control systems' faced attacks from US, China...and, er, *Laos*

By John Leyden, 20 Mar 2013 Follow 2,560 followers

46

RELATED STORIES

Call yourself a 'hacker', watch your ex-boss seize your PC without warning

Black Hat 2013 Hackers induce 'CATASTROPHIC FAILURE' in mock oil well

Energy sector under increasing attack: DHS

Schneider moves on ancient SCADA vuln

AUSCERT 2013 SCADA security is better and worse than we think

Top 10 endpoint backup mistakes

Vulnerable internet-facing industrial systems controlling crucial equipment used by power plants, airports, factories and other critical systems are subjected to sustained attacks within hours of appearing online, according to new honeypot-based research by Trend Micro.

The security weaknesses of SCADA (supervisory control and data acquisition) industrial control systems have been a major focus of interest in information security circles for the last three years or so thanks to Stuxnet, Duqu, and other similar noteworthy attacks.

Trend Micro threat researcher and SCADA security expert Kyle Wilhoit set out to look into this phenomenon in greater depth by setting up a internet-facing honeypot and record attempted attacks. The honeypot architecture developed by Wilhoit directly mimics those of real industrial control systems and SCADA devices.

The researcher, who was once the lead incident handler and reverse engineer at a large energy company, focusing on ICS/SCADA security and persistent threats, created a total of three honeypots.

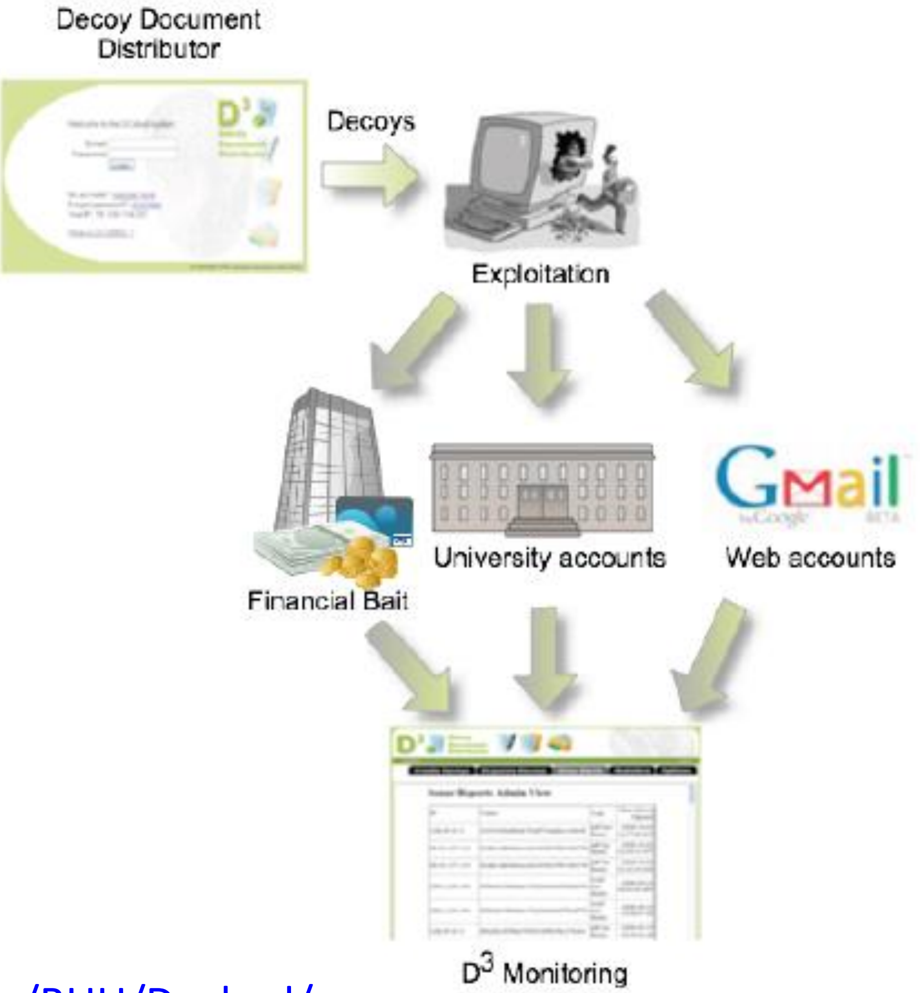
Honeypots/Honeytoken

Baiting Inside Attackers Using Decoy Documents [Bowen, 2009]

- Decoy Document Distributor (DDD) system is a web-based service that:
  - Generates and sends decoy documents with embedded honeytokens to registered users
  - Monitors any activity via the honeytokens and alerts the owner of these documents whenever such a document is exploited
- To increase detection rates multiple decoys are planted in the user's folders
- Detection mechanisms employed by the D3 system can be deployed at the network and/or host level in order to detect the decoy documents
- Examples of honeytokens deployed by D3 are fake banking login accounts specifically created, published and monitored for this trap-based technology specifically to entice financially motivated attackers

Honeypots/Honeytoken

Baiting Inside Attackers Using Decoy Documents [Bowen, 2009]



http://sneakers.cs.columbia.edu/ids/RUU/Dcubed/

Honeypots/Honeytoken

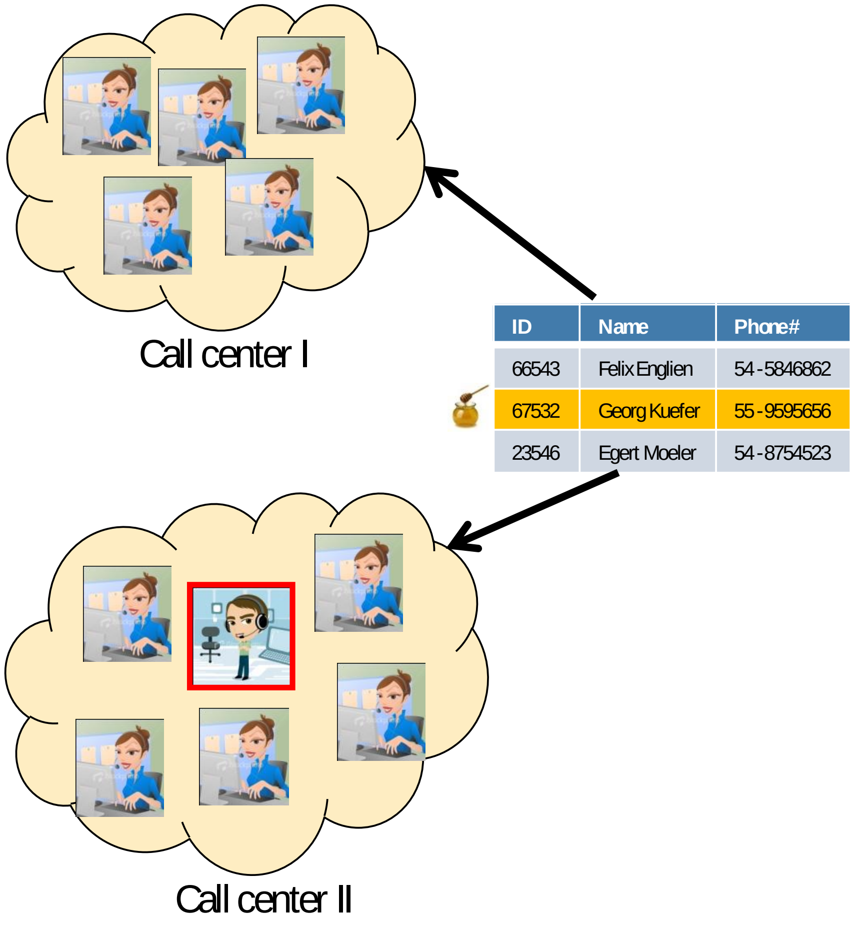
Implementation Of Honeytoken Module In Oracle DB [Čenys, 2005]

- Describes a honeytoken module for Oracle 9iR2 DBMS capable of detecting internal malicious activities
- The strategy is to insert a **honey-table**: a table with "sweet" name able to attract malicious user (e.g. "CREDIT_CARDS")
- These tables are not being used by any application and contain data with no real productive value
- The purpose is to detect attackers with access to the DB tables

Honeypots/Honeytoken

Challenges

- Honeytokens cost money
- How many honeytokens to create ?



ID	Name	Phone#
66543	Felix Englien	54-5846862
67532	Georg Kuefer	55-9595656
23546	Egert Moeler	54-8754523

Honeypots/Honeytoken

Challenges

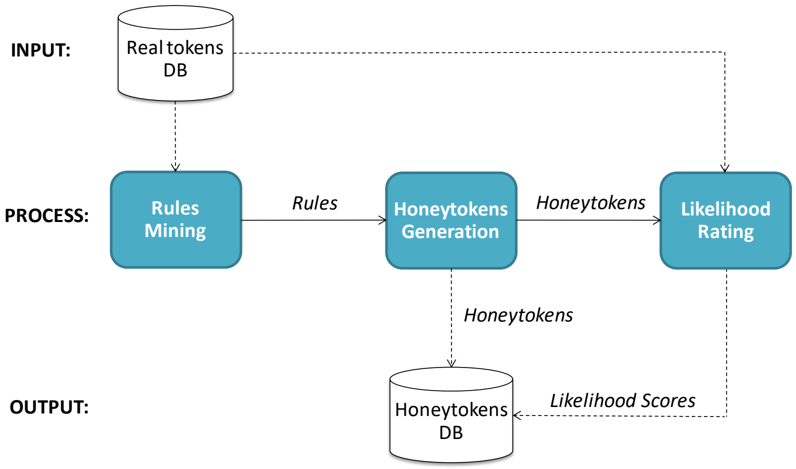
- Creating good honeytokens
  - HoneyGen: an Automated Honeytokens Generator [Berkovitch, 2011]

- A good honeytoken is an artificial data item that is hard to distinguish between real tokens and the honeytoken

- Proposed a generic method for **honeytokens generation** that given **any database** will be able to generate **high quality** honeytokens

Honeypots/Honeytoken Challenges

- Rule mining: extrapolates rules that describe the "real" data structure, attributes, constraints and logic (identity, reference, cardinality, value-set, attribute dependency)
- Honeytoken generation
- Likelihood rating: sort the honeytokens by similarity to real tokens in the input database, according to the commonness of its combination of values



SIPHON

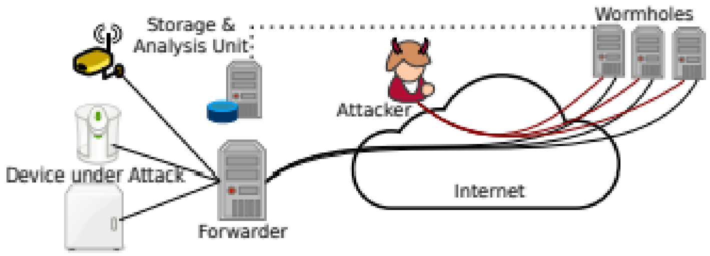


Figure 2: Abstract overview of distributed physical honeypot

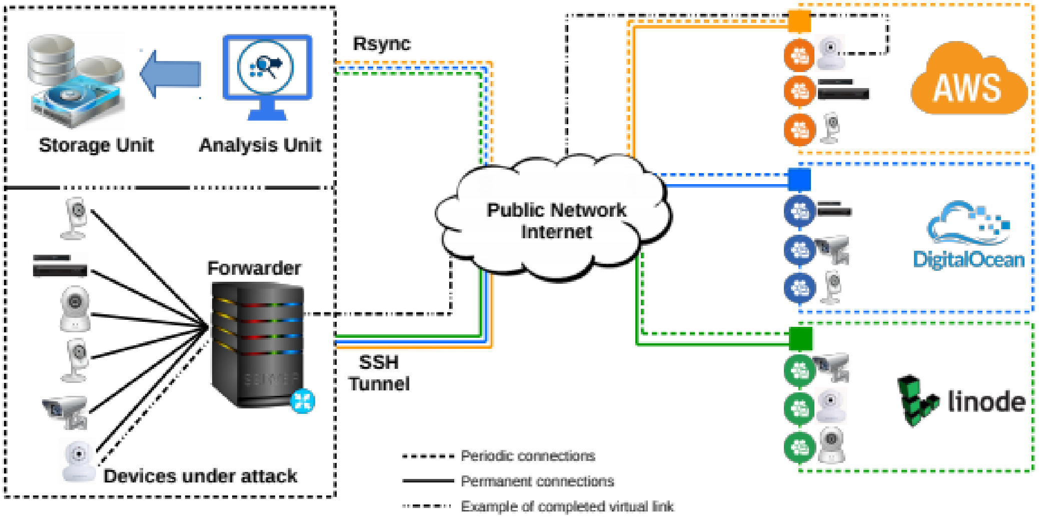


Figure 3: SIPHON prototype implementation in our lab

SIPHON

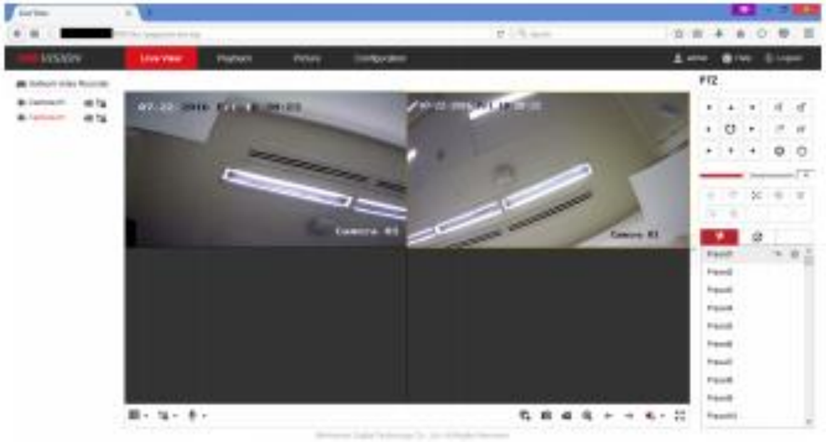


Figure 4: Example of device view through a wormhole

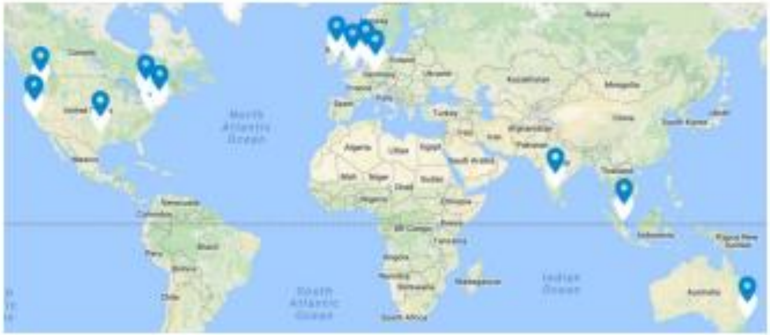
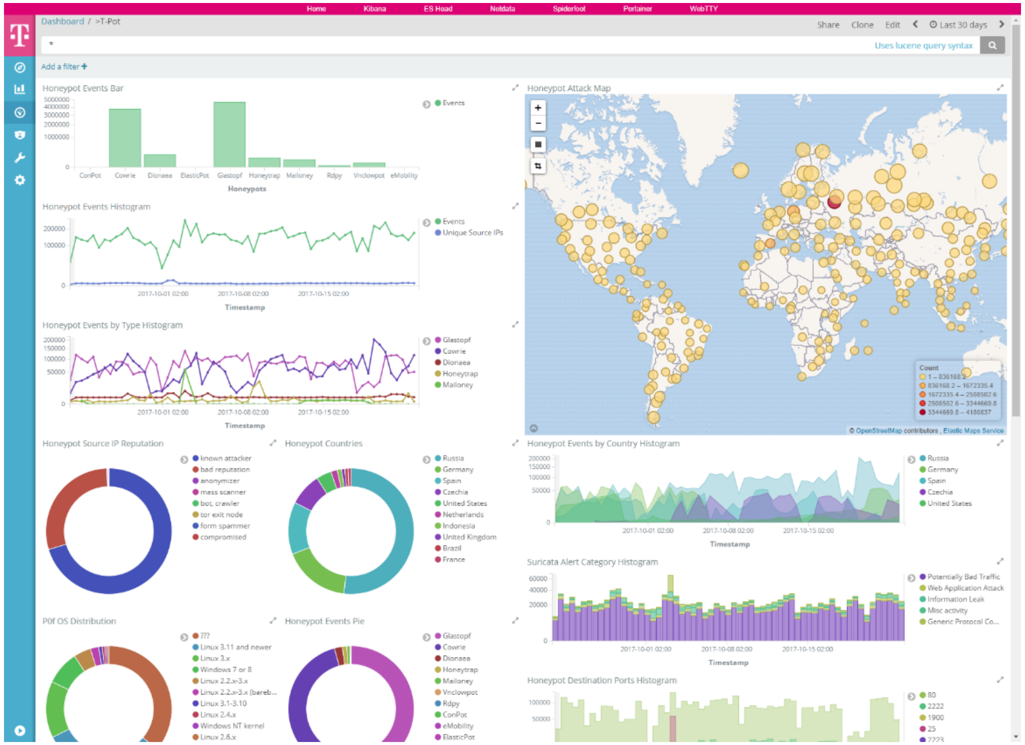


Figure 6: Prototype wormhole locations in cities around the world.

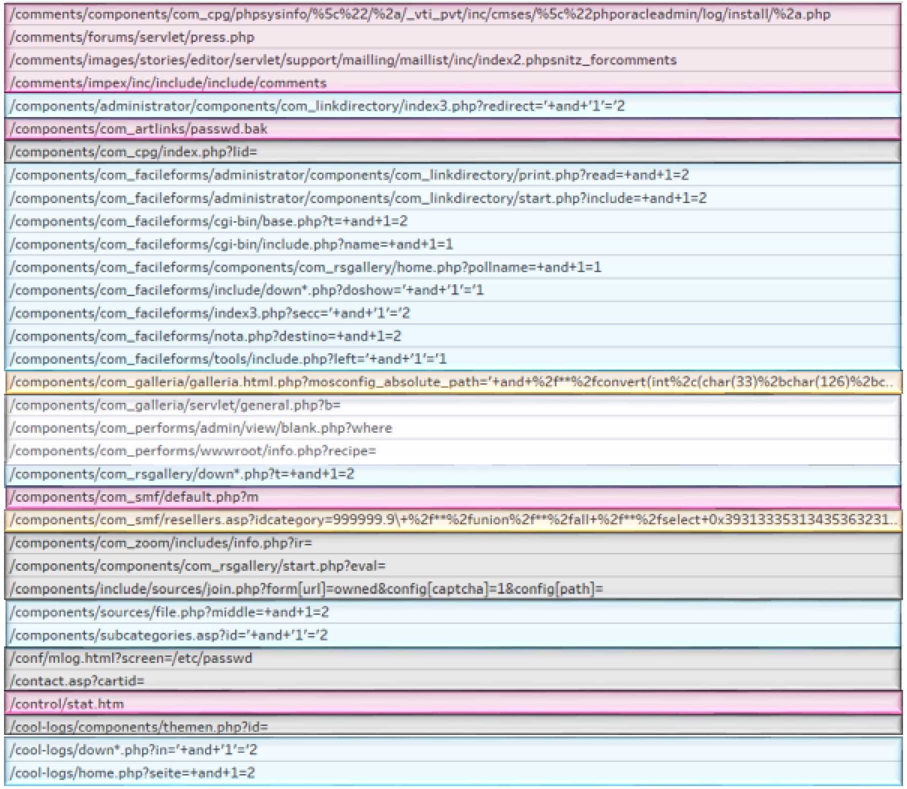
T-pot Multi-Honeypot Platform

- Low interaction honeypots
- 10 Honeypots types
- Over 200 running machines
- Open source
- Real time data visualization



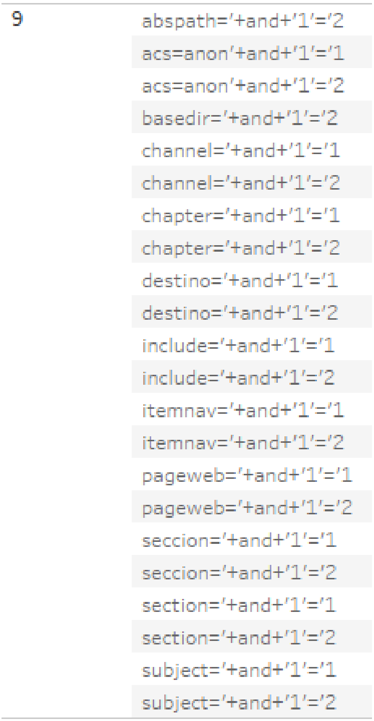
Web honeypot attack vectors An example from real world data

- Regular file scan
- Parameter abusage
- SQL injection always true
- Union-Select SQL injection

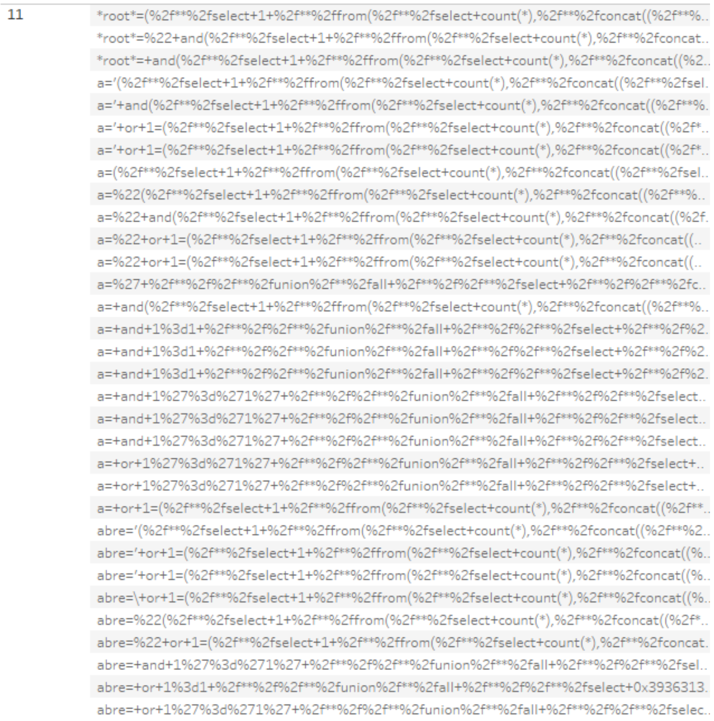


```
/comments/components/com_cpg/phpsysinfo/%5c%22/%2a/_vti_pvt/inc/cmses/%5c%22phporacleadmin/log/install/%2a.php
/comments/forums/servlet/press.php
/comments/images/stories/editor/servlet/support/mailling/maillist/inc/index2.phpsnitz_forcomments
/comments/impex/inc/include/include/comments
/components/administrator/components/com_linkdirectory/index3.php?redirect=’+and+’1’=’2
/components/com_artlinks/passwd.bak
/components/com_cpg/index.php?lid=
/components/com_facileforms/administrator/components/com_linkdirectory/print.php?read=+and+1=2
/components/com_facileforms/administrator/components/com_linkdirectory/start.php?include=+and+1=2
/components/com_facileforms/cgi-bin/base.php?t=+and+1=2
/components/com_facileforms/cgi-bin/include.php?name=+and+1=1
/components/com_facileforms/components/com_rsgallery/home.php?pollname=+and+1=1
/components/com_facileforms/include/down*.php?doshow=’+and+’1’=’1
/components/com_facileforms/index3.php?secc=’+and+’1’=’2
/components/com_facileforms/nota.php?destino=+and+1=2
/components/com_facileforms/tools/include.php?left=’+and+’1’=’1
/components/com_galleria/galleria.html.php?mosconfig_absolute_path=’+and+%2f**%2fconvert(int%2c(char(33)%2bchar(126)%2bc..
/components/com_galleria/servlet/general.php?b=
/components/com_performs/admin/view/blank.php?where
/components/com_performs/wwwroot/info.php?recipe=
/components/com_rsgallery/down*.php?t=+and+1=2
/components/com_smf/default.php?m
/components/com_smf/resellers.asp?idcategory=999999.9\+%2f**%2funion%2f**%2fall+%2f**%2fselect+0x393133353134353632 31..
/components/com_zoom/includes/info.php?ir=
/components/components/com_rsgallery/start.php?eval=
/components/include/sources/join.php?form[url]=owned&config[captcha]=1&config[path]=
/components/sources/file.php?middle=+and+1=2
/components/subcategories.asp?id=’+and+’1’=’2
/conf/mlog.html?screen=/etc/passwd
/contact.asp?cartid=
/control/stat.htm
/cool-logs/components/themen.php?id=
/cool-logs/down*.php?in=’+and+’1’=’2
/cool-logs/home.php?seite=+and+1=2
```

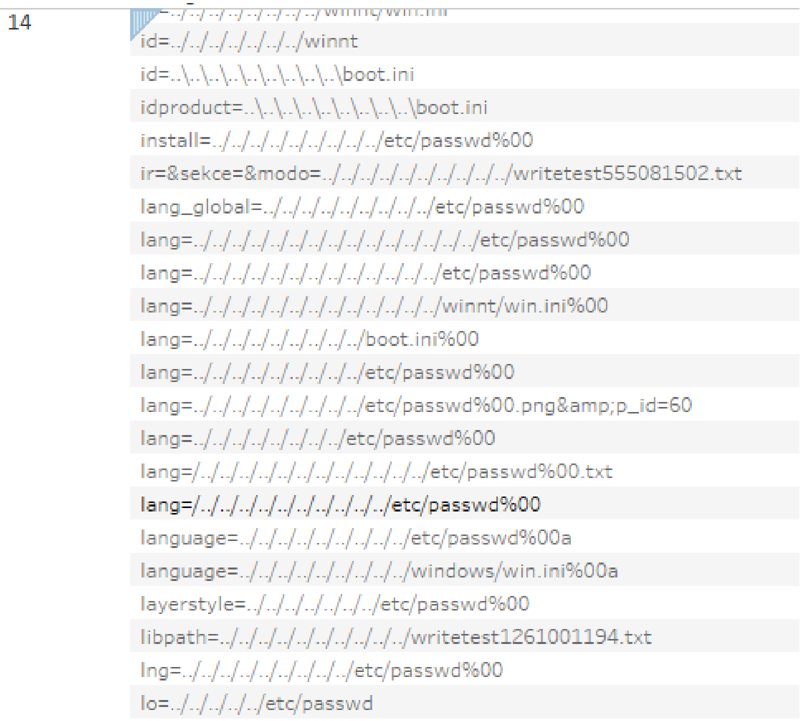
Clusters



9	abspath='+and+'1'='2
	acs=anon'+and+'1'='1
	acs=anon'+and+'1'='2
	basedir='+and+'1'='2
	channel='+and+'1'='1
	channel='+and+'1'='2
	chapter='+and+'1'='1
	chapter='+and+'1'='2
	destino='+and+'1'='1
	destino='+and+'1'='2
	include='+and+'1'='1
	include='+and+'1'='2
	itemnav='+and+'1'='1
	itemnav='+and+'1'='2
	pageweb='+and+'1'='1
	pageweb='+and+'1'='2
	seccion='+and+'1'='1
	seccion='+and+'1'='2
	section='+and+'1'='1
	section='+and+'1'='2
	subject='+and+'1'='1
	subject='+and+'1'='2



11	*root*=(%2f**%2fselect+1+%2f**%2ffrom(%2f**%2fselect+count(*),%2f**%2fconcat((%2f**%..
	root=%22+and(%2f**%2fselect+1+%2f**%2ffrom(%2f**%2fselect+count(*),%2f**%2fconcat..
	root=+and(%2f**%2fselect+1+%2f**%2ffrom(%2f**%2fselect+count(*),%2f**%2fconcat((%2..
	a='(%2f**%2fselect+1+%2f**%2ffrom(%2f**%2fselect+count(*),%2f**%2fconcat((%2f**%2fsel.
	a='+and(%2f**%2fselect+1+%2f**%2ffrom(%2f**%2fselect+count(*),%2f**%2fconcat((%2f**%.
	a='+or+1=(%2f**%2fselect+1+%2f**%2ffrom(%2f**%2fselect+count(*),%2f**%2fconcat((%2f*..
	a='+or+1=(%2f**%2fselect+1+%2f**%2ffrom(%2f**%2fselect+count(*),%2f**%2fconcat((%2f*..
	a=(%2f**%2fselect+1+%2f**%2ffrom(%2f**%2fselect+count(*),%2f**%2fconcat((%2f**%2fsel..
	a=%22(%2f**%2fselect+1+%2f**%2ffrom(%2f**%2fselect+count(*),%2f**%2fconcat((%2f**%..
	a=%22+and(%2f**%2fselect+1+%2f**%2ffrom(%2f**%2fselect+count(*),%2f**%2fconcat((%2f.
	a=%22+or+1=(%2f**%2fselect+1+%2f**%2ffrom(%2f**%2fselect+count(*),%2f**%2fconcat((..
	a=%22+or+1=(%2f**%2fselect+1+%2f**%2ffrom(%2f**%2fselect+count(*),%2f**%2fconcat((..
	a=%27+%2f**%2f%2f**%2funion%2f**%2fall+%2f**%2f%2f**%2fselect+%2f**%2f%2f**%2fc..
	a=+and(%2f**%2fselect+1+%2f**%2ffrom(%2f**%2fselect+count(*),%2f**%2fconcat((%2f**%..
	a=+and+1%3d1+%2f**%2f%2f**%2funion%2f**%2fall+%2f**%2f%2f**%2fselect+%2f**%2f%2.
	a=+and+1%3d1+%2f**%2f%2f**%2funion%2f**%2fall+%2f**%2f%2f**%2fselect+%2f**%2f%2.
	a=+and+1%3d1+%2f**%2f%2f**%2funion%2f**%2fall+%2f**%2f%2f**%2fselect+%2f**%2f%2.
	a=+and+1%27%3d%271%27+%2f**%2f%2f**%2funion%2f**%2fall+%2f**%2f%2f**%2fselect..
	a=+and+1%27%3d%271%27+%2f**%2f%2f**%2funion%2f**%2fall+%2f**%2f%2f**%2fselect..
	a=+and+1%27%3d%271%27+%2f**%2f%2f**%2funion%2f**%2fall+%2f**%2f%2f**%2fselect..
	a=+or+1%27%3d%271%27+%2f**%2f%2f**%2funion%2f**%2fall+%2f**%2f%2f**%2fselect+..
	a=+or+1%27%3d%271%27+%2f**%2f%2f**%2funion%2f**%2fall+%2f**%2f%2f**%2fselect+..
	a=+or+1=(%2f**%2fselect+1+%2f**%2ffrom(%2f**%2fselect+count(*),%2f**%2fconcat((%2f**..
	abre='(%2f**%2fselect+1+%2f**%2ffrom(%2f**%2fselect+count(*),%2f**%2fconcat((%2f**%2..
	abre='+or+1=(%2f**%2fselect+1+%2f**%2ffrom(%2f**%2fselect+count(*),%2f**%2fconcat((%..
	abre='+or+1=(%2f**%2fselect+1+%2f**%2ffrom(%2f**%2fselect+count(*),%2f**%2fconcat((%..
	abre=\+or+1=(%2f**%2fselect+1+%2f**%2ffrom(%2f**%2fselect+count(*),%2f**%2fconcat((%..
	abre=%22(%2f**%2fselect+1+%2f**%2ffrom(%2f**%2fselect+count(*),%2f**%2fconcat((%2f*..
	abre=%22+or+1=(%2f**%2fselect+1+%2f**%2ffrom(%2f**%2fselect+count(*),%2f**%2fconcat.
	abre=+and+1%27%3d%271%27+%2f**%2f%2f**%2funion%2f**%2fall+%2f**%2f%2f**%2fsel..
	abre=+or+1%3d1+%2f**%2f%2f**%2funion%2f**%2fall+%2f**%2f%2f**%2fselect+0x3936313.
	abre=+or+1%27%3d%271%27+%2f**%2f%2f**%2funion%2f**%2fall+%2f**%2f%2f**%2fselec..



14	=../../../../../../../../winnt/win.ini
	id=../../../../../../../winnt
	id=..\..\..\..\..\..\..\..\..\boot.ini
	idproduct=..\..\..\..\..\..\..\..\..\boot.ini
	install=../../../../../../../../../etc/passwd%00
	ir=&sekce=&modo=../../../../../../../../../../writetest555081502.txt
	lang_global=../../../../../../../../../etc/passwd%00
	lang=../../../../../../../../../../../../../../../etc/passwd%00
	lang=../../../../../../../../../../../../../etc/passwd%00
	lang=../../../../../../../../../../../../../winnt/win.ini%00
	lang=../../../../../../../../../boot.ini%00
	lang=../../../../../../../../../etc/passwd%00
	lang=../../../../../../../../../etc/passwd%00.png&amp;p_id=60
	lang=../../../../../../../../etc/passwd%00
	lang=/../../../../../../../../../../../../etc/passwd%00.txt
	lang=/../../../../../../../../../../etc/passwd%00
	language=../../../../../../../../../etc/passwd%00a
	language=../../../../../../../../../windows/win.ini%00a
	layerstyle=../../../../../../../etc/passwd%00
	libpath=../../../../../../../../../../writetest1261001194.txt
	lng=../../../../../../../../../etc/passwd%00
	lo=../../../../../etc/passwd

Honeypot Deployment

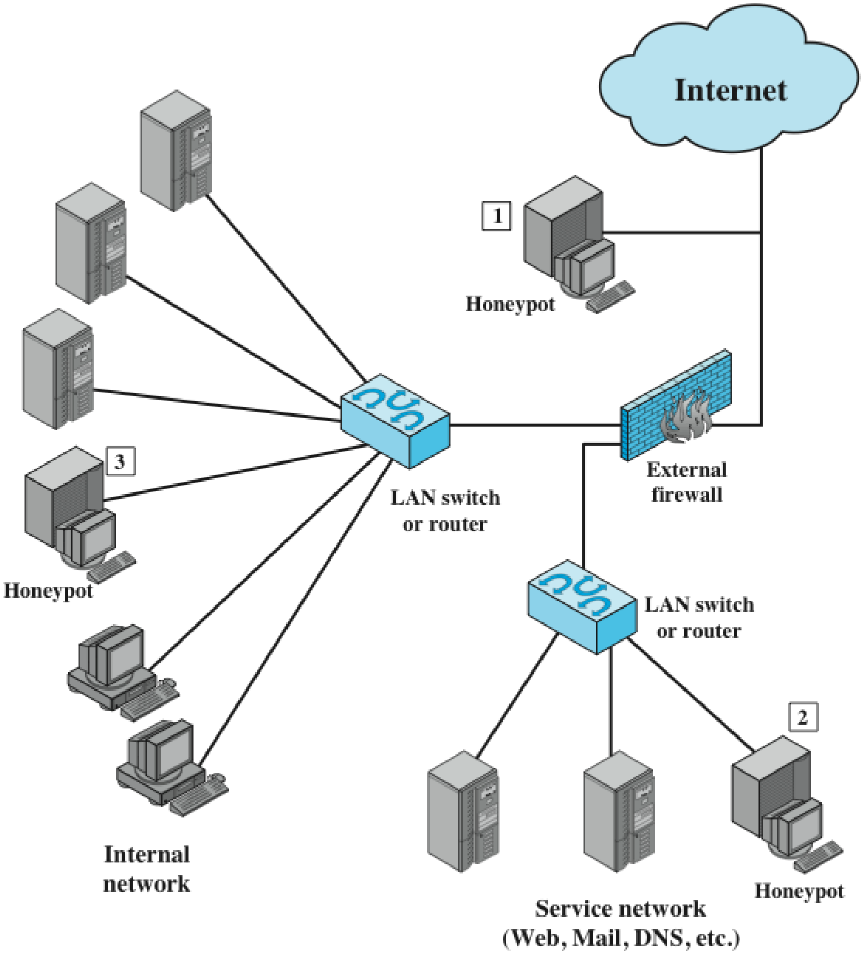


Figure 8.8 Example of Honeypot Deployment