

Honeypots: catching malware in the wild

Francesco Matarazzo

Si.Infor.

Società per la Sicurezza Informatica

Via A. De Gasperi, 1 - 83100 Avellino - tel. [+39] 0825 26653

ti<0x40>siinfor.it

17 Aprile 2009

Table of contents

Introduction

Intro

What is a Honey pot?

Nepenthes

Mendium Interaction Honey pot

The Platform

SurfIDS

Architecture

KlaatuProject

Exploit

Definition

An **exploit** is a piece of software, a chunk of data, or sequence of commands that take advantage of a bug, glitch or vulnerability in order to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic. [Wikipedia]

Shellcode

Definition

A **shellcode** is a small piece of code used as the payload in the **exploitation** of a software vulnerability. It is called "shellcode" because it typically starts a command shell from which the attacker can control the compromised machine. Shellcode is commonly written in machine code, but any piece of code that performs a similar task can be called shellcode. [Wikipedia]

Binary

Definition

An executable (file) causes a computer "to perform indicated tasks according to encoded instructions," as opposed to a file that only contains data. Files that contain instructions for an interpreter or virtual machine may be considered executables, but are more specifically called scripts or bytecode. **Executables are also called "binaries"**. [Wikipedia]

Malware Spreading



Malware Spreading Steps

- ▶ Exploiting vuln target
- ▶ Download malware binary
- ▶ Malware execution

Malware Spreading Steps

- ▶ Exploiting vuln target
- ▶ Download malware binary
- ▶ Malware execution

Malware Spreading Steps

- ▶ Exploiting vuln target
- ▶ Download malware binary
- ▶ Malware execution

Malware Spreading Steps

- ▶ Exploiting vuln target
- ▶ Download malware binary
- ▶ Malware execution

AV industry in 1998



AV industry in 2008



Image Copyright: IKARUS Security Software GmbH

- ▶ Why catching malware?
 - ⇒ fight bad guys
 - ⇒ monitor botnets
 - ⇒ tracking malicious activity

- ▶ How do that?
 - ⇒ honeypots

- ▶ Why catching malware?
 - ⇒ fight bad guys
 - ⇒ monitor botnets
 - ⇒ tracking malicious activity
- ▶ How do that?
 - ⇒ honeypots

- ▶ Why catching malware?
 - ⇒ fight bad guys
 - ⇒ monitor botnets
 - ⇒ tracking malicious activity
- ▶ How do that?
 - ⇒ honeypots

- ▶ Why catching malware?
 - ⇒ fight bad guys
 - ⇒ monitor botnets
 - ⇒ tracking malicious activity

- ▶ How do that?
 - ⇒ honeypots

- ▶ Why catching malware?
 - ⇒ fight bad guys
 - ⇒ monitor botnets
 - ⇒ tracking malicious activity

- ▶ How do that?
 - ⇒ honeypots

- ▶ Why catching malware?
 - ⇒ fight bad guys
 - ⇒ monitor botnets
 - ⇒ tracking malicious activity

- ▶ How do that?
 - ⇒ honeypots



Figure: A Typical Honeypot ;-)

Definition

In computer terminology, a **honeypot is a trap set to detect, deflect**, or in some manner counteract attempts at unauthorized use of information systems. Generally it consists of a computer, data, or a network site that appears to be part of a network but which is actually isolated, (un)protected, and monitored, and which seems to contain information or a resource that would be of value to attackers. [Wikipedia]

Types of Honeybots

- ▶ High Interaction
- ⇒ real host or virtual
- ⇒ runs real services
- ⇒ real problems
- ⇒ 0day YES

- ▶ Low Interaction
- ⇒ service emulator
- ⇒ limited emulation
- ⇒ less problems
- ⇒ 0day NO

Types of Honeybots

- ▶ High Interaction
- ⇒ real host or virtual
- ⇒ runs real services
- ⇒ real problems
- ⇒ 0day YES

- ▶ Low Interaction
- ⇒ service emulator
- ⇒ limited emulation
- ⇒ less problems
- ⇒ 0day NO

Types of Honeybots

- ▶ High Interaction
 - ⇒ real host or virtual
 - ⇒ runs real services
 - ⇒ real problems
 - ⇒ 0day YES
- ▶ Low Interaction
 - ⇒ service emulator
 - ⇒ limited emulation
 - ⇒ less problems
 - ⇒ 0day NO

Honeypots vs IDS

- ▶ No false positives with honeypots
- ▶ IDS needs much more maintenance and analysis

Honeypots vs IDS

- ▶ No false positives with honeypots
- ▶ IDS needs much more maintenance and analysis

Honeypots vs IDS

- ▶ No false positives with honeypots
- ▶ IDS needs much more maintenance and analysis



Figure: The Nepenthes, popularly known as Tropical Pitcher Plants or Monkey Cups, are a genus of carnivorous plants [Wikipedia]

Honeypot Evolution

- ▶ MIH try to combine benefits of HIH and LIH
- ▶ Key = Application Layer Virtualization
- ▶ Sufficient responses to trick KNOW EXPLOITS



Honeypot Evolution

- ▶ MIH try to combine benefits of HIH and LIH
- ▶ Key = Application Layer Virtualization
- ▶ Sufficient responses to trick KNOW EXPLOITS



Honeypot Evolution

- ▶ MIH try to combine benefits of HIH and LIH
- ▶ Key = Application Layer Virtualization
- ▶ Sufficient responses to trick KNOW EXPLOITS



Honeypot Evolution

- ▶ MIH try to combine benefits of HIH and LIH
- ▶ Key = Application Layer Virtualization
- ▶ Sufficient responses to trick KNOW EXPLOITS



Nepenthes

- ▶ Is a Medium Interaction Honeypot
- ▶ Automatically collects malware
- ▶ Released under GPL
- ▶ Emulate known vulnerabilities
- ▶ Extract the exploits payload = shellcode
- ▶ Identify malware location from shellcode (*emulating a shell)
- ▶ Try to download malware (HTTP/ FTP/ proprietary protocol)
- ▶ Store malware locally and/or submit it somewhere

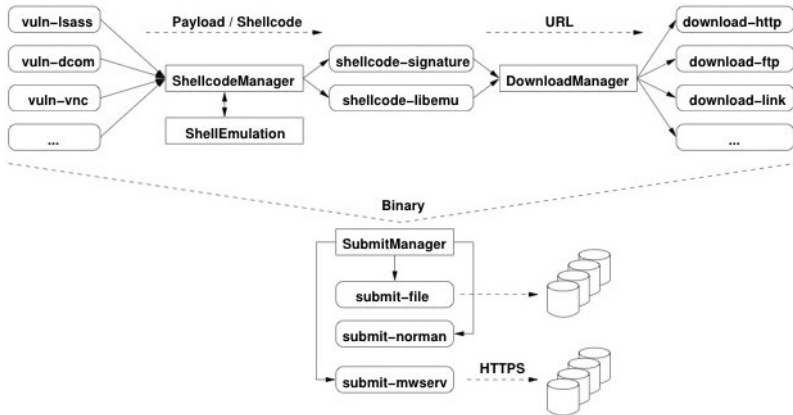


Figure: Nepenthes Structure

COURTESY OF GEORG WICHESKI

Problems

- ▶ No good tools to monitor
- ▶ IMHO No really open source
- ▶ IMHO Bad Documentation
- ▶ A little bit too much synthetic

Problems

- ▶ From "An Overview of ADSL Homed Nepenthes Honey pots In Western Australia":
 - ⇒ detected 70359 attacks
 - ⇒ 4814 (6.8%) believed malicious attacks
 - ⇒ 97.2 % (4678) offered malware
 - ⇒ only 20.2% (949) resulted in **successful** download of malware
 - ⇒ malware downloads represents **1.35%** of all connections made

Problems

- ▶ From "An Overview of ADSL Homed Nepenthes Honey pots In Western Australia":
 - ⇒ detected 70359 attacks
 - ⇒ 4814 (6.8%) believed malicious attacks
 - ⇒ 97.2 % (4678) offered malware
 - ⇒ only 20.2% (949) resulted in **successful** download of malware
 - ⇒ malware downloads represents **1.35%** of all connections made

Problems

- ▶ From "An Overview of ADSL Homed Nepenthes Honeybots In Western Australia":
 - ⇒ detected 70359 attacks
 - ⇒ 4814 (6.8%) believed malicious attacks
 - ⇒ 97.2 % (4678) offered malware
 - ⇒ only 20.2% (949) resulted in **successful** download of malware
 - ⇒ malware downloads represents **1.35%** of all connections made

Problems

- ▶ From "An Overview of ADSL Homed Nepenthes Honeybots In Western Australia":
 - ⇒ detected 70359 attacks
 - ⇒ 4814 (6.8%) believed malicious attacks
 - ⇒ 97.2 % (4678) offered malware
 - ⇒ only 20.2% (949) resulted in **successful** download of malware
 - ⇒ malware downloads represents **1.35%** of all connections made

Problems

- ▶ From "An Overview of ADSL Homed Nepenthes Honeypots In Western Australia":
 - ⇒ detected 70359 attacks
 - ⇒ 4814 (6.8%) believed malicious attacks
 - ⇒ 97.2 % (4678) offered malware
 - ⇒ only 20.2% (949) resulted in **successful** download of malware
 - ⇒ malware downloads represents **1.35%** of all connections made

Problems

- ▶ From "An Overview of ADSL Homed Nepenthes Honeypots In Western Australia":
 - ⇒ detected 70359 attacks
 - ⇒ 4814 (6.8%) believed malicious attacks
 - ⇒ 97.2 % (4678) offered malware
 - ⇒ only 20.2% (949) resulted in **successful** download of malware
 - ⇒ malware downloads represents **1.35%** of all connections made

How to monitor Nepenthes?

SURFIDS

- ▶ Distributed sensor-based HIDS
- ▶ A scalable IDS solution
- ▶ Easy to manage and maintain
- ▶ Monitors attacks to host
- ▶ Nepenthes as sensor
- ▶ Released under GPL
- ▶ Good Documentation

How to monitor Nepenthes?

SURFIDS

- ▶ Distributed sensor-based HIDS
- ▶ A scalable IDS solution
- ▶ Easy to manage and maintain
- ▶ Monitors attacks to host
- ▶ Nepenthes as sensor
- ▶ Released under GPL
- ▶ Good Documentation

How to monitor Nepenthes?

SURFIDS

- ▶ Distributed sensor-based HIDS
- ▶ A scalable IDS solution
- ▶ Easy to manage and maintain
- ▶ Monitors attacks to host
- ▶ Nepenthes as sensor
- ▶ Released under GPL
- ▶ Good Documentation

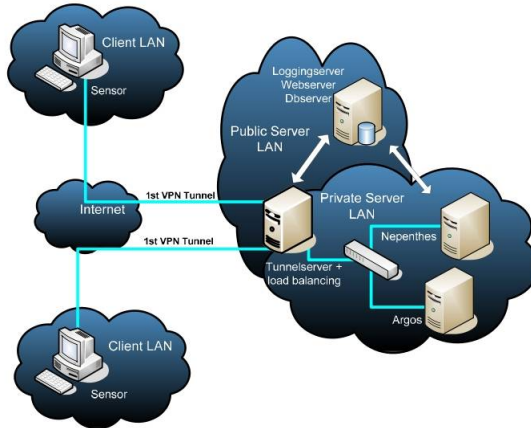


Figure: Global Overview

Sensor

- ▶ Sensor is maintenance free
- ▶ Open-vpn between Sensor and Central Server
- ▶ Could be remastered Knoppix distribution

Honeypot/Tunnel server

- ▶ Based on Nepenthes and/or Argos
- ▶ Open-vpn between Sensor and Central Server

Logging server

- ▶ Postgresql
- ▶ Web interface
- ▶ Show statistics of sensors
- ▶ Show statistics of different attacks
- ▶ Mail logging
- ▶ IDMEF

SURF IDS INTRUSION DETECTION SYSTEM

Contact Logout About SurfIDS

Logged in as: admin Thursday 20 Sep 2007 13:44 Active sensors 12 of 14

Home Report Analyze Configuration Administration

Attacks Exploits Malware Offered Malware Downloaded ARP Cache Search

Search

Criteria Actions

Destination: **ALL**

Source: **10.0.0.0/24**

Characteristics:

Save as PDF
Save as EMF
Save as search template

Period: 365 days
From: 01-01-2007 00:00 Until: 01-01-2008 00:00

Results (page 6: 100 - 119 of 119)

Timestamp	Severity	Source	Port	Destination	Port	Sensor	Additional info
24-05-2007 17:15:09	Possible malicious attack	10.0.0.32	54712	10.0.0.32	143	ARP test	
24-05-2007 17:15:09	Possible malicious attack	10.0.0.32	37562	10.0.0.32	220	ARP test	
24-05-2007 17:15:09	Possible malicious attack	10.0.0.32	57445	10.0.0.32	443	ARP test	
24-05-2007 17:15:09	Possible malicious attack	10.0.0.32	34026	10.0.0.32	42	ARP test	
24-05-2007 17:15:10	Possible malicious attack	10.0.0.32	33744	10.0.0.32	465	ARP test	
24-05-2007 17:15:10	Possible malicious attack	10.0.0.32	54755	10.0.0.32	445	ARP test	
24-05-2007 17:15:11	Possible malicious attack	10.0.0.32	45074	10.0.0.32	25	ARP test	
24-05-2007 17:15:12	Possible malicious attack	10.0.0.32	58963	10.0.0.32	993	ARP test	
24-05-2007 17:16:04	Possible malicious attack	10.0.0.32	36408	10.0.0.32	445	ARP test	
24-05-2007 17:16:04	Possible malicious attack	10.0.0.32	36409	10.0.0.32	445	ARP test	
24-05-2007 17:16:15	Possible malicious attack	10.0.0.32	36410	10.0.0.32	445	ARP test	
04-09-2007 14:45:53	Malicious attack - ARP Poisoning	00:11:22:33:44:55		10.0.0.1		ARP test	
05-09-2007 10:14:24	Malicious attack - ARP Poisoning	00:11:22:33:44:55		10.0.0.1		ARP test	
05-09-2007 11:27:38	Malicious attack - ARP Poisoning	00:11:22:33:44:55		10.0.0.1		ARP test	
05-09-2007 11:44:41	Malicious attack - ARP Poisoning	00:11:22:33:44:55		10.0.0.1		ARP test	
05-09-2007 17:12:38	Malicious attack - ARP Poisoning	02:40:55:ed:00:d1		10.0.0.32		ARP test	
05-09-2007 17:26:11	Malicious attack - ARP Poisoning	02:40:55:ed:00:d1		10.0.0.32		ARP test	
07-09-2007 10:33:33	Malicious attack - ARP Poisoning	00:11:22:33:44:55		10.0.0.1		ARP test	
13-09-2007 11:05:31	Possible malicious attack	10.0.0.31	42520	10.0.0.32	10000	ARP test	00:12:3f:0a:20:2f

SURFIDS version: 2.00 | <http://ids.surfnet.nl> SURFnet bv | Postbus 19035, 3501 DA Utrecht | T +31 302 305 305 | F +31 302 305 329

Figure: SurfIDS screenshot

KlaatuProject

- ▶ We are using SurfIDS on a academic network
- ▶ We do an all in one box installation
- ⇒ sensor/tunnel/logging on one computer
- ▶ Next Steps:
- ⇒ grow the sensors network
- ⇒ do a screenshot of local situation
- ⇒ Malware analysis
- ⇒ Improve tools

KlaatuProject

- ▶ We are using SurfIDS on a academic network
- ▶ We do an all in one box installation
- ⇒ sensor/tunnel/logging on one computer
- ▶ Next Steps:
- ⇒ grow the sensors network
- ⇒ do a screenshot of local situation
- ⇒ Malware analysis
- ⇒ Improve tools

Questions?

[HTTP://KLAATUPROJECT.WORDPRESS.COM](http://klaatuproject.wordpress.com)