



# Honeypotting with Nepenthes



Andrew Waite  
InfoSanity

# What is a Honeytrap?

- Any system designed to receive unauthorised connections
- High interaction honeypot
  - Windows....
- Low interaction honeypot
  - Honeyd
  - Nephthes

# Why is this useful?

- 'Live' threats
- Monitor malicious activity
- Canary system for early warning
- Locate infected machines
- Fresh samples for malware research



# How does it work?

- Emulate common services and vulnerabilities
- Monitor, record and alert on interactions with honeypot system
- Collect malware samples



# Considerations

- Time/Resource consuming
- Legal issues,
  - what happens if malicious users gain full access of the server
- Live malware
  - Handle with care

# Why Nepenthes?

- It's free
- Open Source
- Simple/complex
- Extendable
- It's interesting
- <http://nepenthes.carnivore.it/>

# Nepenthes in action

awaite@nepenthes: ~

```
[19052009 11:33:30 warn dia] Unknown ASN1_SMB Shellcode (Buffer 0 bytes) (State 0)
[19052009 11:33:30 warn module] Unknown PNP Shellcode (Buffer 0 bytes) (State 0)
[19052009 11:33:30 warn module] Unknown LSASS Shellcode (Buffer 0 bytes) (State 0)
[19052009 11:33:30 warn handler dia] Unknown DCOM Shellcode (Buffer 0 bytes) (State 0)
[19052009 11:34:01 warn dia] Unknown ASN1_SMB Shellcode (Buffer 189 bytes) (State 1)
[19052009 11:34:01 warn module] Unknown PNP Shellcode (Buffer 189 bytes) (State 1)
[19052009 11:34:01 warn module] Unknown LSASS Shellcode (Buffer 189 bytes) (State 1)
[19052009 11:34:01 warn handler dia] Unknown DCOM Shellcode (Buffer 137 bytes) (State 0)
[19052009 12:29:09 warn handler dia] Unknown DCOM Shellcode (Buffer 0 bytes) (State 0)
[19052009 12:29:10 warn handler dia] Unknown DCOM Shellcode (Buffer 0 bytes) (State 1)
[19052009 12:29:10 info down mgr] Link tftp://0.0.0.0/ssms.exe has local address, replacing with real ip
[19052009 12:29:10 info down mgr] Replaced Address, new URL is tftp://195.218.255.30
[19052009 12:29:10 info down mgr] Handler tftp download handler will download tftp://195.218.255.30:69/ssms.exe
[19052009 12:31:05 info down handler dia] Downloaded file tftp://195.218.255.30:69/ssms.exe 152576 bytes
[19052009 12:31:05 info mgr submit] File fd28c5e1c38caa35bf5e1987e6167f4c has type MS-DOS executable PE for MS Windows (GUI) Intel 80386 32-bit
[19052009 12:58:17 warn module] Unknown WatchDialogue 0 bytes, port 25
[19052009 13:16:36 warn dia] Unknown ASN1_SMB Shellcode (Buffer 0 bytes) (State 0)
[19052009 13:16:36 warn module] Unknown PNP Shellcode (Buffer 0 bytes) (State 0)
[19052009 13:16:36 warn module] Unknown LSASS Shellcode (Buffer 0 bytes) (State 0)
[19052009 13:16:36 warn handler dia] Unknown DCOM Shellcode (Buffer 0 bytes) (State 0)
[19052009 13:17:08 warn dia] Unknown ASN1_SMB Shellcode (Buffer 189 bytes) (State 1)
[19052009 13:17:08 warn module] Unknown PNP Shellcode (Buffer 189 bytes) (State 1)
[19052009 13:17:08 warn module] Unknown LSASS Shellcode (Buffer 189 bytes) (State 1)
[19052009 13:17:08 warn handler dia] Unknown DCOM Shellcode (Buffer 137 bytes) (State 0)
[19052009 13:30:34 warn module] Unknown WatchDialogue 0 bytes, port 25
[19052009 14:02:37 info dia] 60.161.78.144:1232 asked us to join his SQLSlammer Party
[19052009 14:22:19 info dia] 218.23.37.51:3472 asked us to join his SQLSlammer Party
[19052009 14:31:25 warn module] Unknown WatchDialogue 0 bytes, port 25
[19052009 14:35:28 warn dia] Unknown ASN1_SMB Shellcode (Buffer 0 bytes) (State 0)
[19052009 14:35:28 warn module] Unknown PNP Shellcode (Buffer 0 bytes) (State 0)
[19052009 14:35:28 warn module] Unknown LSASS Shellcode (Buffer 0 bytes) (State 0)
[19052009 14:35:28 warn handler dia] Unknown DCOM Shellcode (Buffer 0 bytes) (State 0)
[19052009 14:36:11 warn dia] Unknown ASN1_SMB Shellcode (Buffer 0 bytes) (State 0)
[19052009 14:36:11 warn module] Unknown PNP Shellcode (Buffer 0 bytes) (State 0)
[19052009 14:36:11 warn module] Unknown LSASS Shellcode (Buffer 0 bytes) (State 0)
[19052009 14:36:11 warn handler dia] Unknown DCOM Shellcode (Buffer 0 bytes) (State 0)
[19052009 14:36:13 warn dia] Unknown ASN1_SMB Shellcode (Buffer 0 bytes) (State 1)
[19052009 14:36:13 warn module] Unknown PNP Shellcode (Buffer 0 bytes) (State 1)
[19052009 14:36:13 warn module] Unknown LSASS Shellcode (Buffer 0 bytes) (State 1)
[19052009 14:36:13 warn handler dia] Unknown DCOM Shellcode (Buffer 137 bytes) (State 0)
```

# Statistics

Statistics engine written by Andrew Waite - [www.InfoSanity.co.uk](http://www.InfoSanity.co.uk)

Number of submissions: 2038

Number of unique samples: 939

Number of unique source IPs: 1359

First sample seen on 2008-05-09

Last sample seen on 2009-05-19

Days running: 375

Average daily submissions: 5

Most recent submissions:

2009-05-19, 12:31:05, 195.218.255.30, tftp://195.218.255.30:69/ssms.exe, fd28c5e1c38caa35bf5e1987e6167f4c

2009-05-19, 10:33:58, 195.54.22.122, link://195.54.22.122:17197/Pbzgew==, e2bdb43ad47d6f72ef97a7ddef41119a

2009-05-19, 08:53:17, 195.85.234.123, link://195.85.234.123:16328/DqAAcg==, 1cc7bcf664509b249fd4056c4d5eeaba

2009-05-19, 08:52:57, 195.96.129.69, link://195.96.129.69:13400/Pak6hw==, 1cc7bcf664509b249fd4056c4d5eeaba

2009-05-19, 06:05:09, 195.85.234.123, link://195.85.234.123:16328/DqAAcg==, 1cc7bcf664509b249fd4056c4d5eeaba

InfoSanity statistics engine:

- [infosanity.blogspot.com/2009/05/submissions2statspy.html](http://infosanity.blogspot.com/2009/05/submissions2statspy.html)

# Alternatives...

- Firewall/server logs
- IDS/IPS
- 'Faith'

## **Best Practice: Defence in Depth**

- go with all systems

# Questions?

- Further reading
  - <http://www.honeynet.org/>
  - <http://www.shadowserver.org/wiki/>
  - <http://nepenthes.carnivore.it/>

# Contact Details

- Contact Details
  - E-Mail: [aw@infosanity.co.uk](mailto:aw@infosanity.co.uk)
  - Web: <http://www.infosanity.co.uk>
  - Twitter: <http://twitter.com/infosanity>