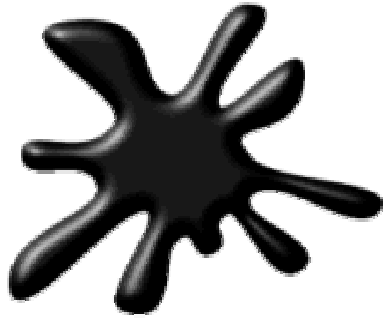


Counter Intelligence in Internet Security:
Honeypot Best Practices

LaBrea

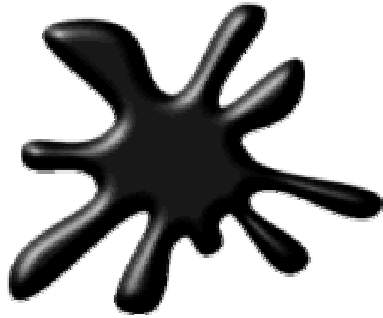
Mix a little tar with that honey...

Tom Liston
tliston@hackbusters.net



Counter Intelligence in Internet Security: Honeypot Best Practices

- Honeypots are about “*information*”
 - Tracking intruders.
 - Learning how blackhats operate.
 - Detecting unknown attacks.
- Tarpits are about information too, but they’re also about “*RETRIBUTION*”



Counter Intelligence in Internet Security: Honeypot Best Practices

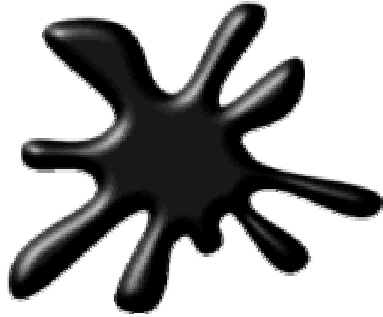
Every neighborhood has one...
Little Stevie, the neighborhood pest.

No one wants to play with him.

No one wants him around.

His parents had to tie a pork chop
around his neck to get the family
dog to play with him...





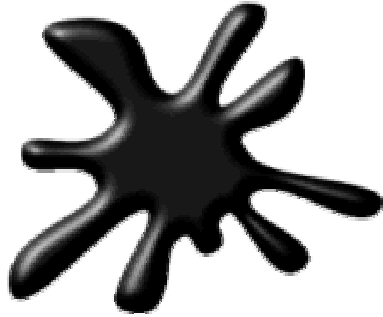
Counter Intelligence in Internet Security: Honeypot Best Practices

When Little Stevie shows up at our door, and asks us to come out and play, what are we to do?

1. We can talk to him.
2. We can decide not to answer the door
3. We can answer the door and tell him “Go away!”



But, perhaps there's a better way...



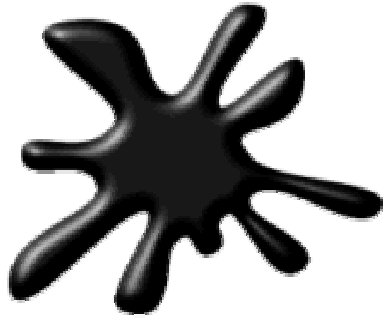
Counter Intelligence in Internet Security: Honeypot Best Practices

When Little Stevie comes to our door, we'll answer:

“Of course Little Stevie!

We want to come out and play!”

And then we'll go back to playing GTAIII on Nintendo...



Counter Intelligence in Internet Security: Honeypot Best Practices

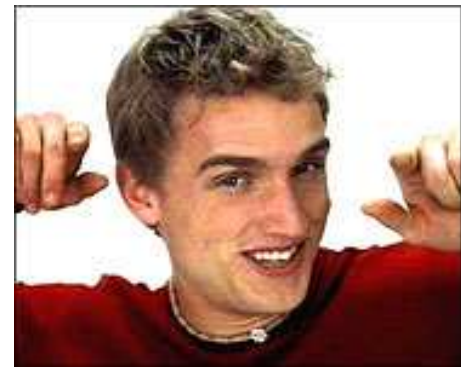
Little Stevie isn't particularly bright...

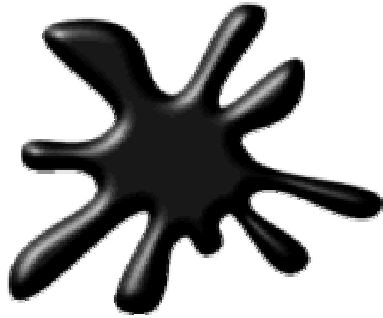
So... Little Stevie hangs around (lowering property values) until he finally gets the idea.. and goes home.

But...

We just wasted 10 minutes of Little Stevie's life.

Hmm...What if ***EVERYONE*** in the neighborhood helped out??





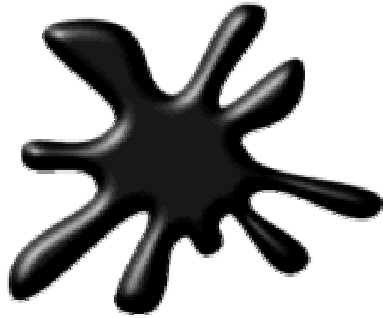
Counter Intelligence in Internet Security: Honeypot Best Practices

Bad News For Little Stevie

Everyone in the neighborhood has decided to use this same approach.

What's more, some of the more determined folks have decided to build fake houses, complete with recordings that answer "Sure Little Stevie, we'll be right out!" when the doorbell rings...





Counter Intelligence in Internet Security: Honeypot Best Practices

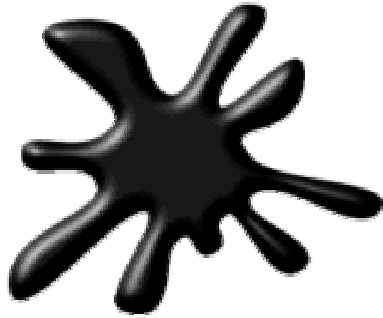
Worse News For Little Stevie

The more determined Little Stevie gets, *the more time he wastes*. Some folks have even figured out that by investing some effort, they can waste even more of Little Stevie's time.

When Little Stevie gets ready to leave, he always asks, "Hey, did you forget about me?"

Some really diligent people listen for him to say that and then reply "No, I didn't forget about you. I'll be out in a minute!"

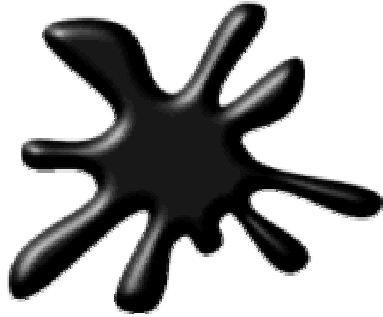




Counter Intelligence in Internet Security: Honeypot Best Practices

LaBrea

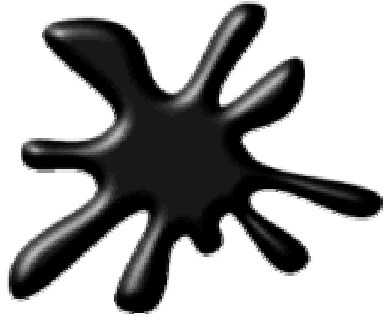
- A small, open-source, high-performance network application that monitors traffic on the local segment. (Unix and Win32)
- By watching traffic, LaBrea can dynamically determine what IP addresses are unused.
- LaBrea then creates “virtual machines” to sit on the unused IP addresses. These virtual machines then answer inbound traffic for those addresses.
- LaBrea answers connection attempts in two different ways that tie up the connecting process: Tarpitting and Persist Trapping



Counter Intelligence in Internet Security: Honeypot Best Practices

Tarpitting

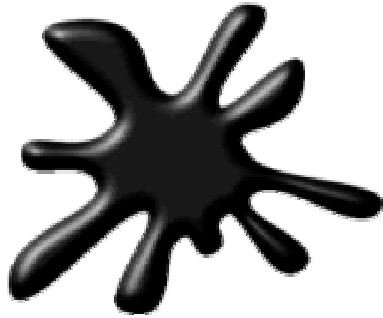
- LaBrea completes the connection initialization, tells the connecting machine that it will only accept small (~5 byte) chunks of data, and then ignores any other traffic.
- This is analogous to saying “Of course Little Stevie! We want to come out and play!”
- Trapping time: The connecting process waits for a TCP time-out that varies from about 5 to 30 minutes (depending on the OS)



Counter Intelligence in Internet Security: Honeypot Best Practices

Persist Trapping

- LaBrea completes the connection initialization, tells the connecting machine that it will only accept small (~5 byte) chunks of data.
- When the first data packet arrives, LaBrea sets the TCP RECV window to 0. Essentially this is saying “Hold on, I’m busy...”
- The connecting process will periodically poll the LaBrea virtual machine, attempting to see if it “forgot” about it.
- The LaBrea machine responds to with a packet maintaining the TCP RECV window at 0 bytes. Again, this is essentially saying “No, I didn’t forget about you. We’ll talk in a minute...”
- Trapping time: FOREVER.

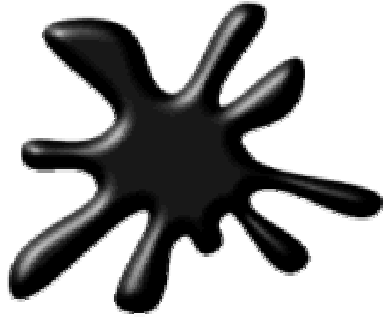


Counter Intelligence in Internet Security: Honeypot Best Practices

Important points to ponder:

- There is no legitimate reason for anyone unknown to you to attempt to connect to your unused IP addresses.
- The script kiddies and hackers have well written toolz, time, and the element of surprise on their side.
- If they're going to attack you, they first have to FIND you.
- As network administrators, we have only *one* strategic advantage at our disposal:

WE CONTROL THE BATTLEFIELD



Counter Intelligence in Internet Security: Honeypot Best Practices

Questions?

- <http://www.hackbusters.net>
- tliston@hackbusters.net

