Hints

Aleksa Sarai, John Cramb

SYD0x05

March 2015

Getting ready for r00t.

Getting ready for r00t.

- Point your `ssh` to `[REDACTED]`.

Getting ready for r00t.

- Point your `ssh` to `[REDACTED]`.
- The user is `ctf`, and the pasword is . . .

Getting ready for r00t.

- Point your `ssh` to `[REDACTED]`.
- The user is `ctf`, and the pasword is . . .
- `GodLovesKermitSex`

Getting ready for r00t.

- Point your `ssh` to `[REDACTED]`.
- The user is `ctf`, and the pasword is . . .
- `GodLovesKermitSex`
- . . . don't ask. It's a Hackers reference.

Hints for Stage 1.

- Your goal is to get the magic `flag{...}` from `s3cur3s4f3`. Use that to authenticate with `w00t` to get to stage 2.

Hints for Stage 1.

- Your goal is to get the magic `flag{...}` from `s3cur3s4f3`. Use that to authenticate with `w00t` to get to stage 2.
- Pay heed to the debugging information!

Hints for Stage 1.

- Your goal is to get the magic `flag{...}` from `s3cur3s4f3`. Use that to authenticate with `w00t` to get to stage 2.
- Pay heed to the debugging information!
- The person who wrote the pin generator got it from stack overflow.

Hints for Stage 1.

- Your goal is to get the magic `flag{...}` from `s3cur3s4f3`. Use that to authenticate with `w00t` to get to stage 2.
- Pay heed to the debugging information!
- The person who wrote the pin generator got it from stack overflow.
- Each pin digit is generated separately.

Hints for Stage 1.

- Your goal is to get the magic `flag{...}` from `s3cur3s4f3`. Use that to authenticate with `w00t` to get to stage 2.
- Pay heed to the debugging information!
- The person who wrote the pin generator got it from stack overflow.
- Each pin digit is generated separately.
- What happens with really big input in a note?

Hints for Stage 1.

- Your goal is to get the magic `flag{...}` from `s3cur3s4f3`. Use that to authenticate with `w00t` to get to stage 2.
- Pay heed to the debugging information!
- The person who wrote the pin generator got it from stack overflow.
- Each pin digit is generated separately.
- What happens with really big input in a note?
- `dmesg` gives you the `eip`.

Hints for Stage 1.

- Your goal is to get the magic `flag{...}` from `s3cur3s4f3`. Use that to authenticate with `w00t` to get to stage 2.
- Pay heed to the debugging information!
- The person who wrote the pin generator got it from stack overflow.
- Each pin digit is generated separately.
- What happens with really big input in a note?
- `dmesg` gives you the `eip`.
- Little Endian, motherfuckers.

Hints for Stage 2.

- Your goal is to get the flag in `/flag`.

Hints for Stage 2.

- Your goal is to get the flag in `/flag`.
- `ps aux`. What is `cron` doing?

Hints for Stage 2.

- Your goal is to get the flag in `/flag`.
- `ps aux`. What is `cron` doing?
- What is the first thing you do when given a random unix binary? Hau 2 help?

Hints for Stage 2.

- Your goal is to get the flag in `/flag`.
- `ps aux`. What is `cron` doing?
- What is the first thing you do when given a random unix binary? Hau 2 help?
- Use the directory permissions, Luke.

Hints for Stage 2.

- Your goal is to get the flag in `/flag`.
- `ps aux`. What is `cron` doing?
- What is the first thing you do when given a random unix binary? Hau 2 help?
- Use the directory permissions, Luke.
- The Sysadmin's Golden Rule: Log verbosely and log often.

Hints for Stage 2.

- Your goal is to get the flag in `/flag`.
- `ps aux`. What is `cron` doing?
- What is the first thing you do when given a random unix binary? Hau 2 help?
- Use the directory permissions, Luke.
- The Sysadmin's Golden Rule: Log verbosely and log often.
  - What is wrong (from a "too much information" perspective) with the log output?

Hints for Stage 2.

- Your goal is to get the flag in `/flag`.
- `ps aux`. What is `cron` doing?
- What is the first thing you do when given a random unix binary? Hau 2 help?
- Use the directory permissions, Luke.
- The Sysadmin's Golden Rule: Log verbosely and log often.
  - What is wrong (from a "too much information" perspective) with the log output?
- The person who wrote this program tried to sanitise symlinks. He didn't succeed.

Hints for Stage 2.

- Your goal is to get the flag in `/flag`.
- `ps aux`. What is `cron` doing?
- What is the first thing you do when given a random unix binary? Hau 2 help?
- Use the directory permissions, Luke.
- The Sysadmin's Golden Rule: Log verbosely and log often.
  - What is wrong (from a "too much information" perspective) with the log output?
- The person who wrote this program tried to sanitise symlinks. He didn't succeed.
- There are three types of symlinks. Those who care about the directories around them and those who don't. And the ones that are just wrong. **tl;dr**: `symlink(2)` is stupid.