CTF

Christian Resell

November 10, 2016

Hva er CTF?

- Konkurranse innenfor informasjonssikkerhet

Hva er CTF?

- Konkurranse innenfor informasjonssikkerhet
- Fokuserer på angrep

Hva er CTF?

- Konkurranse innenfor informasjonssikkerhet
- Fokuserer på angrep
- Mange kategorier

Hva er CTF?

- Konkurranse innenfor informasjonssikkerhet
- Fokuserer på angrep
- Mange kategorier
    - Binary

Hva er CTF?

- Konkurranse innenfor informasjonssikkerhet
- Fokuserer på angrep
- Mange kategorier
  - Binary
  - Web

Hva er CTF?

- Konkurranse innenfor informasjonssikkerhet
- Fokuserer på angrep
- Mange kategorier
  - Binary
  - Web
  - Crypto

Hva er CTF?

- Konkurranse innenfor informasjonssikkerhet
- Fokuserer på angrep
- Mange kategorier
  - Binary
  - Web
  - Crypto
  - Forensics

Hva er CTF?

Knowing is not enough; we must apply. Willing is not enough; we must do.
— Johann Wolfgang von Goethe

Hvorfor?

- Lær deg nye ting

Hvorfor?

- Lær deg nye ting
- Alltid nye utfordringer

Hvorfor?

- Lær deg nye ting
- Alltid nye utfordringer
- Relevant arbeidserfaring

Misc: Coinslot

- Først: koble til serveren, prøve seg fram og se hva som skjer
- Én linje med en pengesum, så bes det om en input per følgende pengeenhet.

```
$0.03
$10,000 bills: 0
$5,000 bills: 0
$1,000 bills: 0
$500 bills: 0
$100 bills: 0
$50 bills: 0
$20 bills: 0
$10 bills: 0
$5 bills: 0
$1 bills: 0
half-dollars (50c): 0
quarters (25c): 0
dimes (10c): 0
nickels (5c): 0
pennies (1c): 3
correct!
$0.02
$10,000 bills:
```

Misc: Coinslot - løsning

- Verktøy: pwntools
- OBS! remote() MÅ slutte med interactive()!
- Mer detaljert beskrivelse på github

Misc: Coinslot

```python
from pwn import *

#Kobler til server
r = remote("misc.chal.csaw.io", 8000)

#Leser inn første linje: $0.03
data = r.recvline()
coin = get_coin(data)

#Leser inn andre linje: $10,000 bills:
#Setter verdien til å bli: 10,000
data = r.recvuntil("bills:")
words = data.split()
value = words[0][1:]
value = float(value.replace(',',''))*100
value = int(value)
```

Reverse: zwiebel

- C-program
- Hopper inn i en blob med kode
- Følger dette mønsteret:
  - Hent ett tegn fra input
  - Sjekk om én enkelt bit er satt eller ikke
  - Dekrypter neste del av koden
  - Gjenta

RuCTFE

- Attack Defence CTF

RuCTFE

- Attack Defence CTF
- Linux image med sårbare tjenester

RuCTFE

- Attack Defence CTF
- Linux image med sårbare tjenester
- Finn sikkerhetsfeil og fiks de

RuCTFE

- Attack Defence CTF
- Linux image med sårbare tjenester
- Finn sikkerhetsfeil og fiks de
- Angrip de andre lagene!

RuCTFE

- Attack Defence CTF
- Linux image med sårbare tjenester
- Finn sikkerhetsfeil og fiks de
- Angrip de andre lagene!
- Denne helgen!

Lenker

Lykke til!

- CTF Field Guide
- Practice CTF List / Permanent CTF List
- CTFtime
- Svett CTF (github)
- ctf.coffee