Security conferences & exercises

Jaanus Kääp

Jaanus Kääp

- Security expert at Clarified Security
  - Pentesting, Code analysis, research etc
- Background in Web and System development
- ~4 years fulltime in security
- Found some vulnerabilities:
  - Web: Facebook, Adobe, MS, Google...
  - System: Adobe reader, Apple Safari, Foxit reader...

This talk

- Black Hat europe
- Defcon
- Cyber defence exercises

Black Hat Europe

- In Amsterdam
- 4 days total
- 2/2 days of trainings/briefings (talks)

Trainings part

- Different companies
- Cost between 2K and 3K (w.o. VAT)

Briefings part

- Cost 1100 to 1500 euros (w.o. VAT)
- Multiple tracks
- Wide selection of topics
- Wide level of content
- Lot of additional marketing stuff

Black Hat europe 2015 day 1

- Cybersecurity for Oil and Gas Industries
- Attacking the XNU Kernel in El Capitain
- Hey Man Have You Forgotten to Initialize Your Memory?
- Lessons from Defending the Indefensible

Black Hat europe 2015 day 2

- (In-)Security of Backend-As-A-Service
- Fuzzing Android
- Vulnerability Exploitation in Docker Container Environments
- New Tool for Discovering Flash Player 0-day Attacks in the Wild from Various Channels

(In-)Security of Backend-As-A-Service

- Easy to use backend databases from Amazon and such
- Simple APIs in multiple languages
- Easy to set up
- Cheap

(In-)Security of Backend-As-A-Service

- Amazon DB connection tutorial
-
```
AmazonS3Client s3Client = new
AmazonS3Client(
   new BasicAWSCredentials(
      “ACCESS_KEY_ID“,
      “SECRET_KEY“
   )
);
```

(In-)Security of Backend-As-A-Service

- But security?
- Amazingly common practice:
  - Create account
  - BaaS provider gives username and password
  - Make your app to connect DB using these
  - Use DB quite similary to any other
  - ...

(In-)Security of Backend-As-A-Service

- Results:
  - Your app contains DB(possibly root) username and password
  - Reversing it from app is trivial in almost all cases

(In-)Security of Backend-As-A-Service

- How common:
  - ~56Mio Data
  - Personal data, pictures, purchase data etc
- How common 6 months later:
  - Less then 1% was fixed

Black Hat overall

- Quite many good talks
- Not that much to do outside of talks and talking
- Bit too high price tag for only talks

Defcon vs Black Hat

- Bit different environment and setting

Defcon

- Cost 230$
- 4 days
- Multiple tracks
- Very wide selection of topics
- Very wide level of content
- Lot of additional activities, villages, workshops etc...

Defcon

- Did not participate on lot of talks
- Participated on „ARM for Pentesters” workshop (free)
- Villages
- Competitions
- Meeting people in the community

Defcon workshops

- 1 day and shorter trainings
- Free but need quick reacting
- Topics are quite varied:
  - *Exploited Host Analysis*
  - *ARM for Pentesters*
  - *iOS Application exploitation*
  - *Embedded System Design*
  - *….*

Defcon villages

- Hands on events and talks
- Very different topics:
  - *Biohacking*
  - *Car hacking*
  - *Tamper evident*
  - *Packet hacking*
  - *Lockpicking*

Defcon competitions

- CTF
- Crash and Compile
- Hacker Jeopardy
- „Beverage” cooling
- Crack Me If You Can
- ….

Defcon pros

- More talks
- Much more activities
- More industry people

Black Hat pros

- More high level company events
- Closer (if in Europe)
- Cheaper (if in Europe)

Defcon vs Black Hat - cost

	Black Hat	Defcon
Travel	200 – 300 EUR	1200 – 1300 EUR
Participating	1100 EUR	234 EUR
Accommodation	200 – 300 EUR	200 – 300 EUR
Total	***1500 – 1700 EUR***	***1634 – 1834 EUR***

Difference less then 10%

Defcon vs Black Hat - overall

- Actually both are good
- If possible, participate in both
- If only one is possible, I would choose Defcon

About cyber exercises

- Many years of Locked Shields (red team)
- Some less known excercises (blue team or read team)
- In total around 10 different excercises

My approach

- Reasonably good idea about the attacking side
- All defence is based on that
  - *As an attacker what I would hate*
  - *What would stop most of my attacks*
  - *How to discover my attacks from logs*
  - *What about attack signatures*
  - *What tools would help me in these things*
  - *How much I can automate the setup*

Knowing the attacks

- Hard to protect against unknown
- Hard to select tools without internal knowledge
- Hard to find attacks from logs

Knowing the attacks

- Learn the attack methods
- Try them out yourself
- Learn the tools internals

Exercise dependent

- How does scoring works
- **How are attacks made (automated vs manual)**
- How much of the environment is known
- What is network setup

First steps

- Implementing fixes/conf changes

$$\frac{\text{how many attacks it blocks}}{\text{time to implement}}$$

- How to monitor attacks
- How to easily block attacks that you see (snort, modsec rules)

First steps example

1. Make almost everything unwritable by www-data
2. PHP hardening (configuration)
3. Tail the apache access log constantly
4. Enable and conf UFW as strictly as possible
5. Set up Snort (with most strict rules I found) as NIPS
6. Upload directory directly not accessible

Possible attacks & vectors

- XSS (some are blocked by Snort)
- SQL injection (some are blocked by Snort)
- OS Command injection (PHP hardening)
- Path traversal (PHP hardening & Snort for most)
- PHP code injection/backdoors (PHP hardening for most)
- DDOS (failed on that...)
- PHP file overwrite/upload (www-data & not accessible)

Automated vs manual attacks

- Automated - Question of luck and foresight
- Manual – Cat and mouse mostly. **Monitoring**

Monitoring

- Extremely important!
- Different tools
- Differencing between attacks and normal
- Have to think like an attacker
  - Does webserver log POST parameters?
  - Does webserver log headers?

Preparing

- As much information as possible
- Script EVERYTHING beforehand
- Predict possible attacks
  - Think what you would just hate as an attacker
- Write your own rules to Snort/ModSec
- Be ready to add new/remove old during the exercise
- Block everything that feels bad (be ready to reverse)

During exercise

1. Set up everything
2. Monitor
3. React to attacks (blocking and restoring)
4. Fix stuff (if there is time)

Q&A

Basic books

- Quite a bible of webapp security
  The Web Application Hacker's Handbook. Discovering and Exploiting Security Flaws
  http://www.amazon.com/The-Web-Application-Hackers-Handbook/dp/1118026470
- Very good beginner book about reverse engineering
  Reversing. Secrets of Reverse Engineering
  http://www.amazon.com/Reversing-Secrets-Engineering-Eldad-Eilam/dp/0764574817
- Basic memory exploitation and logic behind it
  Hacking: The Art of Exploitation
  http://www.amazon.com/Hacking-The-Art-Exploitation-Edition/dp/1593271441
- Some ideas how to look for and exploit vulnerabilities
  A Bug Hunter's Diary: A Guided Tour Through the Wilds of Software Security
  http://www.amazon.com/Bug-Hunters-Diary-Software-Security/dp/1593273851/
-

Advanced books and other stuff

- *„The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System”*
- *„The Shellcoder's Handbook”*
- *„Windows internals”*
- *„Understanding the Linux Kernel”*
- Very good collection of free training videos about reverse engineering, x86 and exploitation (highly recommend) https://www.youtube.com/channel/UCthV50MozQIfawL9a_g5rdg

- More questions: jaanus@clarifiedsecurity.com