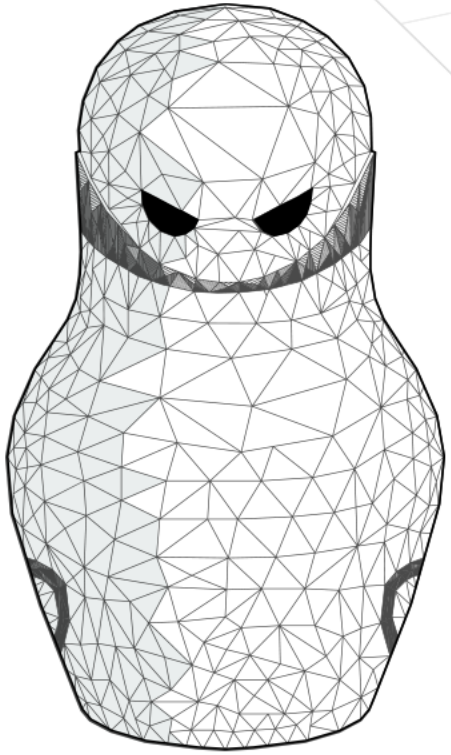


ZERO NIGHTS 2015

Let’s play the game.

Yet another way to perform penetration test.
Russian “red team exercise” experience from QIWI.

Kirill ‘isox’ Ermakov

#:whoami?

- Known as ‘isox’
- Web penetration tester
- QIWI CTO/CISO
- Member of “hall-of-fames” (Yandex, Mail.ru, Apple, and so on)
- JBFC participant ^___^

Captain obvious

- Penetration testing
- Just a way to check your security controls
- “Fast and dirty assessment”
- Performed by qualified specialists
- Part of PCI DSS certification as example
- Independent security review
- Need2do for security-aware companies

Traditional approach

- Single team (2-5 members)
- External, Internal and social-technology
- Restricted vectors and scenario
- Attackers whitelist
- No private information about a target
- Social attacks are often prohibited
- Limited attacks daytime

Pentester point of view

- Target-independent work scenario
- 1/3 time for well known vectors
- 1/3 time for new research
- 1/3 time for automated scanners
- No physical security bypass
- Limited social attacks
- Same story every time

Red team exercise

- They call it “Red-team”:
  - Security team is not notified
  - Trying to simulate “real” attack
  - Still a lot of restrictions and limits
  - One team
  - No information about the internals

Anyway cover is not enough

- Blind zones
- Time limits
- Does not use all available vectors
- Too much accurate and ethic
- Does not really looks like real hackers attack
- Pentest team insufficient resources

Hack me plz!

- Lets make a big (dream?) team
- Let them work on their own!
- No more “secret pentest technique”
- Forget “don’t attack that” and “don’t bruteforce us after 6PM”
- Scope = everything
  - Not kidding. Really everything.
- No preparations from security team

No restrictions

- Social attacks
- Malware
- Account bruteforce
- 0days
- Night/weekend attacks
- Physical penetration
- DOS
- Drop-devices
- Personal devices hijack
- Employee bribe

Let’s there be insider

- Sharing private information
- Network map
- Critical assets
- Security specialist as insider
- Hints and advises

Deep penetration

- Physical security bypass
- Drop-devices:
  - Wi-Fi and LAN back connects
  - Cable manipulations
  - USB Flash with malware
- Live social engineering
- Stealing laptops/pads/phones

Security reactions

- Security team awareness check
- Real incident investigation
- Bans and account lockouts
- Live system tuning
- Cooperation with physical security
- Logs, cameras, events and a lot of fun!

Challenge and goals

- For penetration team:
  - Application or SYS account for DB
  - AD enterprise administrator account
  - *nix root / admin account
  - Access to any critical system
- For security team:
  - Defend your home

And there is only one rule: no rules

QIWI Red Team Exercise

- Attackers: #ONSEC & #DSEC
- Defenders: #QIWI security team
- Insider: CISO (me)
- Timeline: 2.5 month
- Attack Goal:
    - SYSDBA, root, Enterprise Administrator
- Security team goal:
    - Notice at least 90% attacks and intrusions
    - Defend

Weeks of pain

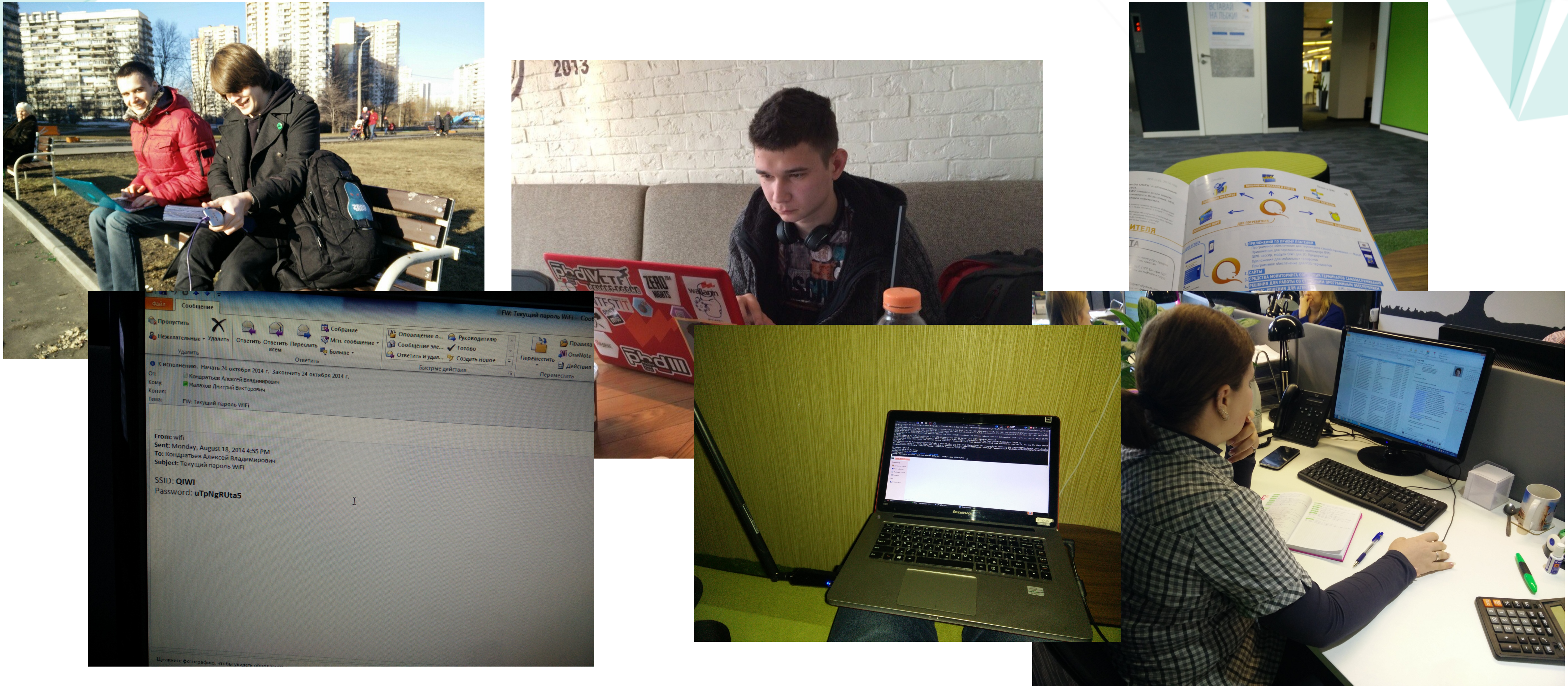
- 7 social attacks in 2 weeks
- Few times of “emergency”
- System crashes
- Ordinary users butthurt:
    - Locked accounts
    - Spam/phishing emails
    - Viruses
- Malware investigations

Really cool vectors

- Successful office building intrusion
- Wi-Fi’ed and LAN’ed laptops gateways
- Mac OS X domain issues
- Smart House hacking
- Power Supply takeover
- Compiling dsniff for DVR

… even more in @d0znpp presentations

Some memos



FW: Текущий пароль WiFi - Сооб

К исполнению. Начать 24 октября 2014 г. Закончить 24 октября 2014 г.

От: Кондратьев Алексей Владимирович
Кому: Малахов Дмитрий Викторович
Копия:
Тема: FW: Текущий пароль WiFi

From: wifi
Sent: Monday, August 18, 2014 4:55 PM
To: Кондратьев Алексей Владимирович
Subject: Текущий пароль WiFi

SSID: **QIWI**
Password: **uTpNgRUta5**

And we lost this game

- System accounts were compromised
- Social engineering as a best attack vector
- SSH access to security team member’s Macbook
- Downloaded dumps of network devices with password hashes
- Tons of successful brutes

Successful vector

- Gained credentials using social engineering
- Loss of isolation in guest Wi-Fi network
- Laptops, connected both to cable networks and Wi-Fi
- Bad MacOS active directory configuration, allowing any AD account to connect using SSH
- Keeping sensitive data plaintext in ~/
- Insufficient monitoring of the office traffic

Results

- Better than one-team classics
- Simulate near real hacker attacks
- Excellent scope fulfill
- Testing security as it is, not as it wants to be
- You will be disappointed in your security toys
- ‘Little’ bit expensive
- Systems will crash sometimes

See ya!

- Thanks to @videns for a good trip to the Troopers
- Thanks to #DSEC and #ONSEC for a great job
- Excuses to my security team for this two and a half months of hell

- Any questions?
- Contact: isox@qiwi.com