CYBER WAR SIMULATION, TOOLS CHOOSING THE VICTIM CRITICAL INFRASTRUCTURE

Corneel Theben Tervile

CHOOSING THE VICTIM CRITICAL INFRASTRUCTURE

Attacker

Infrastructure

CHOOSING THE VICTIM CRITICAL INFRASTRUCTURE

Attacker

Infrastructure

CHOOSING THE VICTIM CRITICAL INFRASTRUCTURE

Attacker

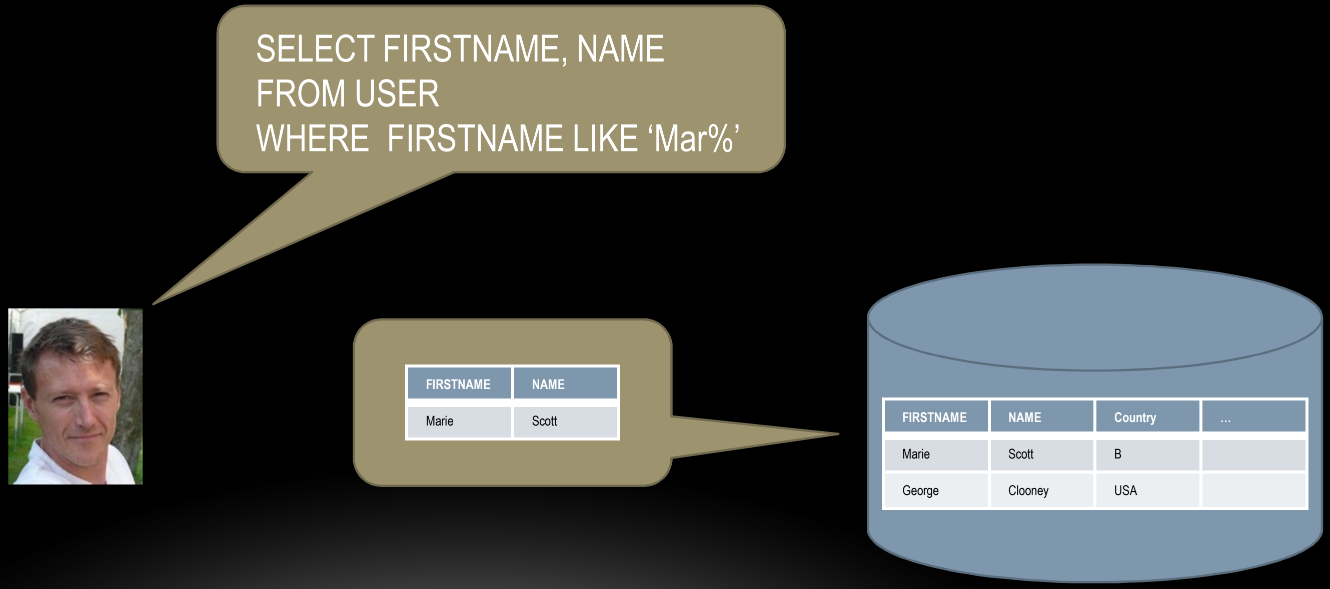
Infrastructure

EXAMPLE OF VULNERABILITY

- Recent data breach in The Netherlands (23/4/2012)
  - http://www.dutchnews.nl/news/archives/2012/04/sensitive_medical_information.php
  - http://www.demorgen.be/dm/nl/993/Gezondheid/article/detail/1426278/2012/04/20/Medische-gegevens-300-000-Nederlanders-gelekt.dhtml
- Reason: SQL-attack
  - What is SQL-injection?

EXAMPLE OF VULNERABILITY

- Relational Database Management System
  - e.g. MySQL, Oracle, SQL Server,…
  - Communication with SQL (ANSI standard)



```
SELECT FIRSTNAME, NAME
FROM USER
WHERE  FIRSTNAME LIKE ‘Mar%’
```

FIRSTNAME	NAME
Marie	Scott

FIRSTNAME	NAME	Country	…
Marie	Scott	B	
George	Clooney	USA	

EXAMPLE OF VULNERABILITY

- Tool for communication with database
  - e.g. SQLyog for MySQL
  - We enter a SQL-statement and see the result in the tool
- Communication in a program via API
  - Let me show a very simple application
    - Existing username and correct password – I may enter
    - Non-existing username or wrong password – I may not enter

EXAMPLE OF VULNERABILITY

- Let me show and explain the code
  - username and password are entered via user interface and are hold in what an IT’er calls variables (value holders)
  - We construct a SQL-statement with those variables via concatenation

```
SELECT * FROM USER WHERE USERNAME = ‘
user1
‘ AND PASSWORD = ‘
p1
‘
```

EXAMPLE OF VULNERABILITY

- Let me show the vulnerability
- Let me explain the vulnerability
  - How could the “injection” happen?

```
SELECT * FROM USER WHERE USERNAME = ‘
admin
‘ AND PASSWORD = ‘
‘ OR ‘1’ = ‘1
‘
```

EXAMPLE OF VULNERABILITY

- It can even be worse

```
SELECT * FROM USER WHERE USERNAME = ‘
‘; DROP TABLE USER; --
‘ AND PASSWORD = ‘
‘
```

CHOOSING THE VICTIM CRITICAL INFRASTRUCTURE

- Choosing the victim
  Let’s think about the data breach in The Nederlands
  - Motivation (money, honor, harm, …)
  - Importance of victim (person versus company, enemy, …)
  - Infrastructure (up-to-date/out-dated, type, specialism, …)
  - Known vulnerabilities…
    - Database of vulnerabilities on operating systems, databases, services, standard applications
    - List of most dangerous software errors

CHOOSING THE VICTIM CRITICAL INFRASTRUCTURE

- If you know the type of infrastructure, operating system, platform, application, services you can check a vulnerability in one of the databases.
    - US National vulnerability database: http://nvd.nist.gov/
    - Vulnerability Notes Database of US-CERT http://www.kb.cert.org/vuls/
    - The open source vulnerability database http://www.osvdb.org/
    - …
- You can manually check the vulnerability and exploit it but that is cumbersome
- You can use a (specific) vulnerability scanner
    - Nessus, SATAN/SAINT/SARA, Nikto/Wikto, Nmap, OpenVAS, …

CHOOSING THE VICTIM CRITICAL INFRASTRUCTURE

- If you want to check the vulnerabilities of other non-standard applications
- Check the list of most dangerous software errors, but attack by hand can be cumbersome
  - http://www.sans.org/top25-software-errors/
- Automated tools for pentest
  - OWASP Zed Attack Proxy Project
  - Nikto/Wikto
  - …

RESOLUTION OF THE VULNERABILITY

- Let me test the vulnerability
- Let me solve the vulnerability
  - I have to use better API’s and programming practices
- Let me test if the vulnerability is solved

TRAINING AND GAMES ON VULNERABILITY

- Pentest training
  - Webgoat
    - Unsafe JavaEE app on Tomcat webserver
      - Install Apache Tomcat
      - Deploy the Java Web Archive
  - …
- Security games
  - UCSB International Capture The Flag http://ictf.cs.ucsb.edu/
  - Roothack http://www.roothack.org/
  - …

OTHER VULNERABILITIES

- If SQL injection problem is solved, is there still a way to enter the site?
  - Yes, I can send an e-mail in name of an official person asking to re-enter a password
    - I just can program it
    - I just need an SMTP-server (open relay)
  - I can always check if the password is not among the list of worst passwords
    http://techland.time.com/2011/11/22/the-25-most-popular-and-worst-passwords-of-2011/
    http://www.bmyers.com/public/1958.cfm
    1 out of 5 users uses one on this last list!

    Possibly the cause of the databreach!

TRAINING AND GAMES ON VULNERABILITY

- Pentest training
  - Webgoat
    - Unsafe JavaEE app on Tomcat webserver
      - Install Apache Tomcat
      - Deploy the Java Web Archive
  - …
- Security games
  - UCSB International Capture The Flag http://ictf.cs.ucsb.edu/
  - Roothack http://www.roothack.org/
  - …

THANK YOU FOR YOUR ATTENTION