Penetration Test Service @ ABN AMRO

Overview of the Penetration Test Implementation and Service.

Peter Kanters

Contents

1. Introduction.
2. The history of Penetration Testing @ ABN AMRO.
3. Penetration Testing Process overview.
4. Open Web Application Security Project (OWASP) top 10.
5. Penetration testing services.
6. Recommendations.
7. Recap.
8. Questions.

1. Introduction.

Peter Kanters
ABN AMRO Bank NV.
Information Security Office
Technical Security Assessment

Foppingadreef 22
1102 BS Amsterdam
Netherlands

+31 20 6285411
peter.kanters@nl.abnamro.com

25 + years experience at ABN AMRO.

Mainframe Systems Programmer.

Networking and E-Infra Specialist.

Security Specialist.

1.What we try to prevent!

November 10, 2009, 5:27PM

Anatomy of the RBS WorldPay Hack

by Dennis Fisher

Share Recommend (4) Print E-mail 2 Comments

The four men whom a federal grand jury indicted this week for their alleged roles in a scam that stole millions of dollars from RBS WorldPay were no fools. The small crew of hackers had a distinct division of labor, operated with skill and efficiency and left one of the world's larger banks holding the bag.

Viktor Pleshchuk, Sergei Tsurikov, Oleg Covelin and a fourth man, identified only as "Hacker 3," pooled their talents, and with the help of a worldwide network of "cashers" in more than 280 cities, they were able to walk away with $9 million of RBS WorldPay's money. The attack, detailed in a federal indictment announced Tuesday by the Department of Justice, illustrates clearly the level of organization and sophistication involved in ATM and payment-card fraud, as well as the difficulty banks face in guarding against these schemes.

http://threatpost.com/en_us/blogs/anatomy-rbs-worldpay-hack-111009

2. History of Penetration Testing @ ABN AMRO.

Pentests at AAB originally serviced by combination of Internal Team and External Vendor.

Internal team :

- More than Average Quality – Limitations in tooling and experience.
- High Cost – 7 team members / 1 Manager.
- Low Flexibility - Lead time 3 months.
- Global Service.

External Vendor :

- Good Quality – More divers experience.
- High Costs – Much Overhead in Intake and Reporting / High Rates.
- Good Flexibility – Lead time about 1 month.
- Service limited to the Netherlands.

Overall the service was good but expensive.

2. Setting up the new Penetration Testing @ ABN AMRO.

Rebuild of service necessary due to RBS separation.

Pentests at AAB now performed by two External Vendors.

Vendor selection :

- Request for Information / Request for Proposal.
- Proof of Concept (POC).
- Selected 2 Vendors from 7 vendors.

Improvements accomplished :

- Overhead external pentests reduced drastically.
- Discount on rates (reduction up to 30%) based on 80 Pentests per year.
- Lead time reduced from 3 months (internal team) to 10 business days.
- A noticeable quality improvement was achieved.

3. Penetration Test Process overview.

Process Overview :

•Internal Preparation:
- Documentation.
- What do we want tested.
- Which Vendor do we use for the test.

•Intake Meeting with selected Vendor (Conference Call +/- ½ Hour):
- Scope of the Test.
- Start Date.
- Number of Days needed.
- Letter of Authority Needed from Third Party.
- Credentials Involved.

•Preparation for Penetration Test.

•Vendors perform Penetration Test and deliver report within 5 Business Days.

•Administration.

4. Penetration testing services provided.

ABN AMRO Penetration Testing Services menu:

Penetration Testing Services:	Small	Medium	Large
1. Source code review	< 15K LOC*	15K - 50K LOC	50K - 100K LOC
2. Full "Grey Box" penetration test	3 Days	5 Days	7 Days
3. Lightweight penetration test (automated scan + credentials)	1 Day	2 Days	3 Days
4. Network Penetration Test	3 Days	5 Days	7 Days
5. Retest	¼ Day	½ Day	1 Day
6. Custom	Hourly Rate		
* LOC: Lines of Code			

Source code review: Identifying application level security issues by using a combination of manual review, and automated source code analysis on the applications source code.

Penetration test: The objective of the Penetration Tests is to protect sensitive and / or confidential data by identifying weaknesses in the application. A penetration test consist out of: Reconnaissance, Known Issues, Application Testing. Within the *Lightweight Penetration test* less effort is spend on application testing by using automated scanning tools. Information required; IP addresses, (virtual) hostnames, operating system, database and application versions, test accounts, tokens (when needed), application programming language.

Network penetration test: Identifies security weaknesses that could be exploited by motivated malicious individuals to gain unauthorised access to systems or data on network segments. The penetration testing should demonstrate the ability to gain unauthorised access to system resources and/or disrupt system services.

4.OWASP Top 10 –2010

OWASP
The Open Web Application Security Project
http://www.owasp.org

A1 –Injection Flaws, such as SQL, OS, and LDAP injection can lead to executing unintended commands or accessing unauthorized data.

A2 –Cross Site Scripting (XSS) allows attackers to execute script in the victim's browser

A3 –Broken Authentication and Session Management allowing attackers to compromise passwords, keys, session tokens , identity theft.

A4 –Insecure Direct Object References attackers can manipulate these references to access unauthorized data.

A5 –Cross Site Request Forgery (CSRF) allows the attacker to force the victim's browser to generate requests.

A6 –Security Misconfiguration for the application, framework, web server, application server, and platform.

A7 –Failure to Restrict URL Access Attackers will be able to forge URLs

A8 –Invalidated Redirects and Forwards Attackers can redirect victims to phishing or malware sites.

A9 –Insecure Cryptographic Storage Attackers may use this weakly protected data to conduct identity theft, credit card fraud.

A10 -Insufficient Transport Layer Protection Applications frequently fail to encrypt network traffic

http://www.owasp.org/images/0/0f/OWASP_T10_-_2010_rc1.pdf

5. Is Security Testing a normal part of the test methodology?

Security Testing is now often performed at the end of a project.

- This puts extra stress on the go life date.

- Extra expensive because findings have to fixed at the last minute.

OWASP certification becomes mandatory for programmers.

Is there a development similar in the test world ?

In “*TMap Next voor resultaatgericht testen”* over 900 pages only 5 pages are mentioning Information Security.

In the future the Test management Methodology should make Pentesting obsolete !

5.Recommendations.

- INPUT VALIDATION, INPUT VALIDATION and AGAIN …… !!!!
- Secure Programming (OWASP)
- Application security testing in development phase (OWASP)
- Proper Platform Hardening
- System and Network monitoring
- Proper security management

- Integrate Security testing in Test methodology in an early stage.
- Train Testers in OWASP principles.

6. Recap.

We discussed the past and present Penetration Testing @ ABN AMRO.

We reviewed the day to day Penetration Testing Process.

Open Web Application Security Project (OWASP) top 10.

We have seen the Penetration testing services.

We discussed Recommendations.

?

Questions ?

peter.kanters@nl.abnamro.com