Penetration testing

A step beyond missing patches and weak passwords

June 25th, 2012

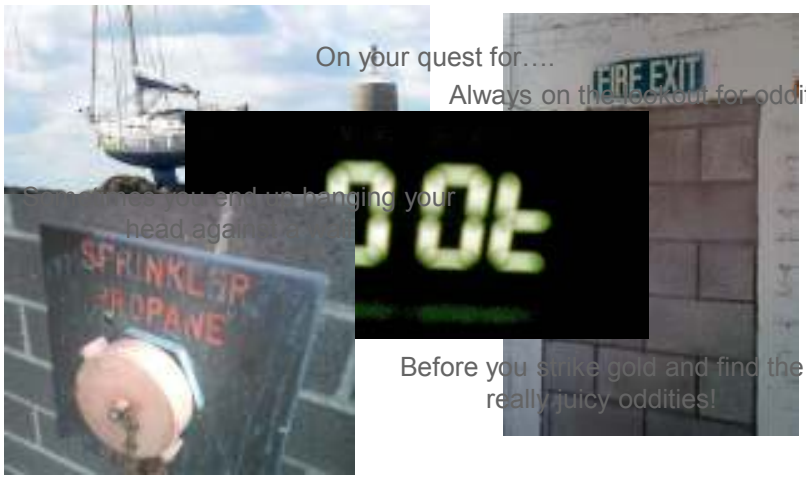
ERNST & YOUNG
Quality In Everything We Do

Eirik Thormodsrud

- Graduated from the ISG in 2006
- Employed by Ernst & Young Norway ever since (5 ½ years)
- Manager at IT Risk and Assurance
- Mainly performs:
  - attack and penetration testing
  - security audits
  - risk analysis
- Also a guest lecturer at Gjøvik University College
  - BSc/MSc course ”Ethical hacking and penetration testing”

ERNST & YOUNG
Quality In Everything We Do

What I like to do



On your quest for….

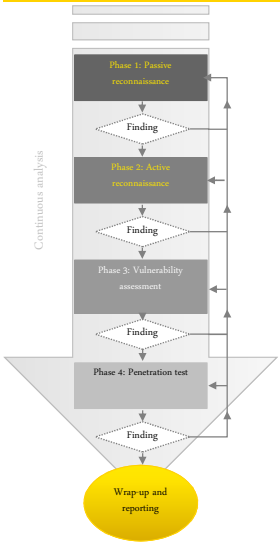
Always on the lookout for oddities

…soon you end up hanging your head again…

Before you strike gold and find the really juicy oddities!

ERNST & YOUNG
Quality In Everything We Do

Penetration testing



- Passive reconnaissance
  - Sniffing network traffic
  - Searching open sources
- Active reconnaissance
  - Port / vulnerability scanning
- Vulnerability assessment
  - Analysis of information from phase 2
- Penetration test
  - Attempts to exploit identified vulnerabilities, i.e. rule out false positives

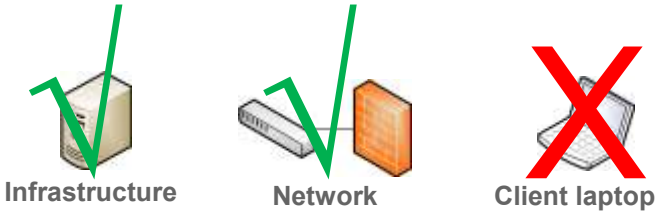
ERNST & YOUNG
Quality In Everything We Do

One example

- Scenario
  - Attacker with access to the internal network
  - Access to computer/software for hacking
  - Three days at disposal, test parts of infrastructure without credentials.
  - Test of client PC image with and without credentials
- Infrastructure:
  - Latest version Microsoft products
  - Strict patch routines
  - Strict password policy
  - Internally segmented network with strict firewall policies
  - 802.1x on all network end-points
  - Organization develops their own business applications in-house

ERNST & YOUNG
Quality In Everything We Do

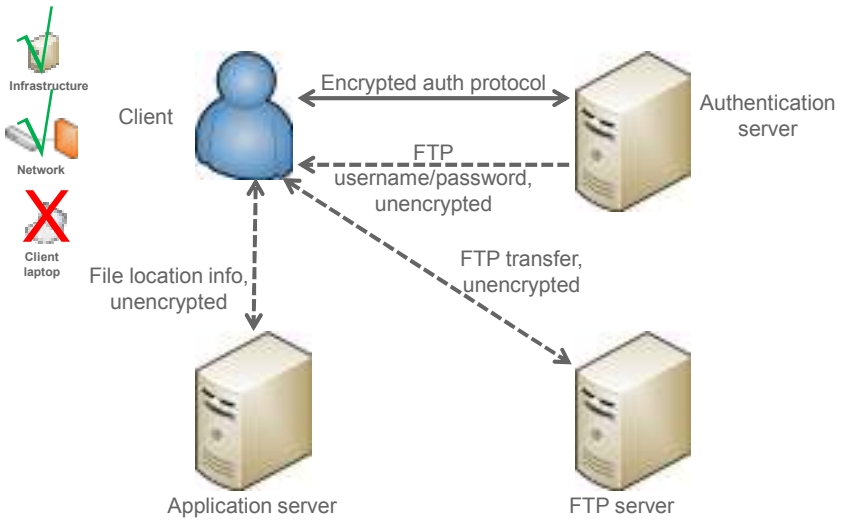
Results



- Client laptop
  - Users can freely obtain local admin rights through internal routines

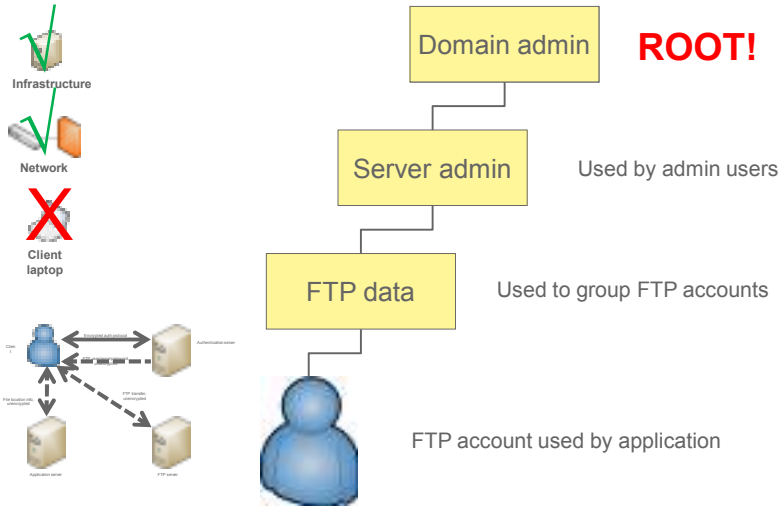
ERNST & YOUNG
Quality In Everything We Do

Results



ERNST & YOUNG
Quality In Everything We Do

Results



ERNST & YOUNG
Quality In Everything We Do

Findings

- In-house developed security and authentication solution
- Password in clear text during logon process
- Use of FTP with login per file transfer
- Use of application account to access data with no differentiation between user levels
- FTP account has OS admin privileges
- Nested group memberships give access creep, resulting in Domain Admin privileges

ERNST & YOUNG
Quality In Everything We Do

Short term fixes

- Change password of FTP account
- Revoke group memberships
- Change to encrypted file transfer mechanism, at least one that protects logon information
- Protect logon procedure of application
  - Use SSL/TLS or similar to encrypt the whole logon process.
  - Or change application so that logon process is secure

ERNST & YOUNG
Quality In Everything We Do

Long term recommendations

- Security must be embedded in development process for:
  - Application design
  - Infrastructure
- Define security requirements
  - Approved protocols
  - Reuse industry standard authentication and encryption standards
  - Security testing/assessments during design, implementation and prior to production setting

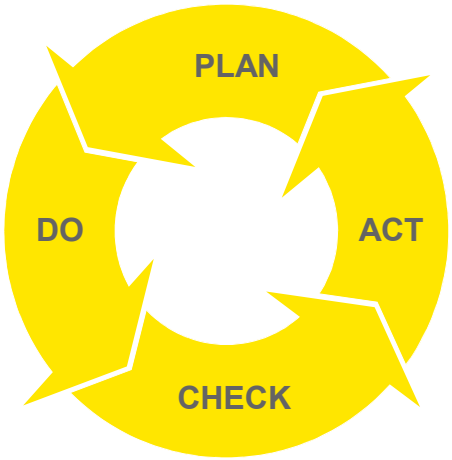
ERNST & YOUNG
Quality In Everything We Do

Long term recommendations

- Control of access privileges
  - Formal approval of change in access privileges
  - Regular verification of correctness
  - Analysis of effect of changes, in particular for nested groups
- Control of user accounts
  - Accounts for separate uses, e.g. application accounts should not have OS privileges etc.

ERNST & YOUNG
Quality In Everything We Do

In short…



- Typical culprit is:
  - Weaknesses in information security management and lack of focus

Ernst & Young
Quality In Everything We Do

If all else fails!

Ernst & Young
Quality In Everything We Do


Thank you for your attention
Questions?
ERNST & YOUNG
Quality In Everything We Do