Penetration Testing
- a way for improving our cyber security

Adrian Furtună, PhD, OSCP, CEH
adif2k8@gmail.com
Agenda

- Who am I
- Why this topic
- Case study 1
- Case study 2
- Lessons learned
- Conclusions
- Q & A
Who am I

- Member of the Pentest Team at KPMG Romania
- Doing pentests against various applications and systems:
  - Internal networks, public networks
  - Web applications
  - Mobile applications
  - Wireless networks
  - Social engineering, etc
- Speaker at Hacktivity, DefCamp, Hacknet and other local security confs
- Teaching assistant at Information Security Master programs (UPB, MTA and ASE)
  - Teaching penetration testing classes
  - Organizing Capture the Flag contests
Why this topic?

- The need for more efficient cyber security
- Penetration testing is part of the defense-in-depth approach
  - Verify the effectiveness of defense mechanisms and people
  - Find weak spots in defense layers
  - Show the real risk of a vulnerability
  - Suggest corrective measures
  - Re-verify
- Penetration testing can be used for improving our cyber security

Is my data safe?

Penetration testing can be used for improving our cyber security
To better clarify terms...

- Penetration Testing a.k.a. Pentesting, Ethical Hacking, Red Teaming
  - Method for evaluating the security of an information system or network by simulating attacks from malicious outsiders or insiders
  - Exploit vulnerabilities and dig much deeper

- Penetration Testing is:
  - Authorized
  - Adversary based
  - Ethical (for defensive purposes)

- Penetration Testing is not
  Vulnerability Assessment / Scanning
Case Study 1
Pentesting the internal network (2011)

- **Objective:**
  See what an internal malicious user could do, given simple network physical access.

- **Malicious user:** visitor, contractor, malicious employee

- **Targets:** confidential data, client information, strategic business plans, etc

- **Initial access:** physical network port in users subnet
Pentesting the internal network (2011) – cont.
Pentesting the internal network (2011) – cont.

1. Network mapping
   - IP ranges
   - Host names
Pentesting the internal network (2011) – cont.

1. Network mapping
   - IP ranges
   - Host names

2. Service and OS discovery
   - Windows 7
   - Windows 2008 Server R2
   - Common client ports open
   - IIS, MsSQL, Exchange, etc
Pentesting the internal network (2011) – cont.

1. Network mapping
   - IP ranges
   - Host names

2. Service and OS discovery
   - Windows 7
   - Windows 2008 Server R2
   - Common client ports open
   - IIS, MsSQL, Exchange, etc

3. Vulnerability scanning
   - Nessus: 1 high, 30 medium, 39 low
   - MsSQL server default password for sa user
Pentesting the internal network (2011) – cont.

4. Exploitation
Pentesting the internal network (2011) – cont.

4. Exploitation
   - Add local admin

![SQL Server Management Studio screenshot showing the execution of commands to add a local admin user to the Administrators group. The commands executed are:

```sql
EXEC xp_cmdshell 'net localgroup Administrators KPMG /add'
EXEC xp_cmdshell 'net localgroup Administrators KPMG /add'
```
4. Exploitation
   - Add local admin

5. Post-exploitation
   - Info gathering
   - Credentials to other systems
4. Exploitation
   - Add local admin

5. Post-exploitation
   - Info gathering
   - Credentials to other systems

6. Pivoting
   - Connect to 2nd db server
   - Upload Meterpreter
Pentesting the internal network (2011) – cont.

4. Exploitation
   - Add local admin

5. Post-exploitation
   - Info gathering
   - Credentials to other systems

6. Pivoting
   - Connect to 2nd db server
   - Upload Meterpreter

7. Post-exploitation
   - List tokens
   - Impersonate Domain Admin token
   - Create Domain Admin user
Pentesting the internal network (2011) – cont.

- Game Over

on domain controller:
Case Study 2
Pentesting the (same) internal network (2012)

- **Objective:**
  See what an internal malicious user could do, given simple network access.

- **Test the findings from previous year**
  - **Malicious user:** visitor, contractor, malicious employee
  - **Targets:** confidential data, client information, strategic business plans, etc
  - **Initial access:** network port in users subnet
Pentesting the (same) internal network (2012) – cont.

1. Network mapping
   - ~ the same as last year

2. Service and OS discovery
   - ~ the same as last year
Pentesting the (same) internal network (2012) – cont.

1. Network mapping
   - ~ the same as last year

2. Service and OS discovery
   - ~ the same as last year

3. Vulnerability scanning
   - Nessus: 0 high,
     21 medium, 20 low
Pentesting the (same) internal network (2012) – cont.

1. Network mapping
   - ~ the same as last year

2. Service and OS discovery
   - ~ the same as last year

3. Vulnerability scanning
   - Nessus: 0 high, 21 medium, 20 low

Now what?
   - No default/weak passwords
   - No missing patches
   - No exploitable config problems
   - No sql injection...
Pentesting the (same) internal network (2012) – cont.

4. Attack the clients – method 1
Pentesting the (same) internal network (2012) – cont.

4. Attack the clients – method 1
   - Setup a fake local NetBIOS server
   - Respond to every request with my IP address
   - Setup multiple local services (HTTP, SMB)
   - Request Windows authentication on connection
     => capture password hashes

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>12.697618</td>
<td>10.1.1.166</td>
<td>10.1.1.255</td>
<td>NBNS</td>
<td>92</td>
<td>Name query NB KWSHQAPP01&lt;20&gt;</td>
</tr>
<tr>
<td>201</td>
<td>12.713457</td>
<td>10.1.1.14</td>
<td>10.1.1.166</td>
<td>NBNS</td>
<td>104</td>
<td>Name query response NB 10.1.1.14</td>
</tr>
</tbody>
</table>

NTLMv1 Response Captured from 10.1.1.14
DOMAIN: RO USER: am...lu
LMHASH: Disabled
NTHASH: 00366da6607a1e1d8408b51...3d2b9a0e7596612a
Pentesting the (same) internal network (2012) – cont.

   - Captured around NTLM 50 hashes
   - Cracked about 25% using dictionary attack with mangling rules in a few hours
   - Gained network access as domain user (low privileges)
   - Could access some shared files on file server
   - Not enough

#june2012*
Wizard123!
aprilie_12
fatfrumos58./martie02
andree@1987
iulie_2012
april.12
aprilie.2012
aprilie.1988
primavara2012!
mai.2012
bob02010/
4. Attack the clients – method 2

- Man in the middle attack between victim and proxy server
- Setup a fake local proxy server
- Request Basic authentication
- Receive user’s credentials in clear text (base64 encoded)
Pentesting the (same) internal network (2012) – cont.

4. Attack the clients – method 2 – cont

The victim sees this:

What would you do?
Pentesting the (same) internal network (2012) – cont.

5. Exploitation

- Got local admin password (global) from a special user 😊
- Could connect as admin on any workstation
Pentesting the (same) internal network (2012) – cont.

5. Exploitation
   - Got local admin password (global) from a special user 😊
   - Could connect as admin on any workstation

6. Pivoting
   - Search the machines from IT subnet for interesting credentials / tokens
   - Found a process running as a domain admin user
5. Exploitation

- Got local admin password (global) from a special user 😊
- Could connect as admin on any workstation

6. Pivoting

- Search the machines from IT subnet for interesting credentials / tokens
- Found a process running as a domain admin user

7. Exploitation

- Impersonate domain admin
- Add user to domain admin group

Game Over
Lessons Learned
# Pentest comparison

<table>
<thead>
<tr>
<th></th>
<th>2011</th>
<th>2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low hanging fruits removed</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>IT personnel vigilance</td>
<td>low</td>
<td>high</td>
</tr>
<tr>
<td>Network prepared for pentest</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Existing vulnerabilities</td>
<td>yes</td>
<td>yes (lower nr)</td>
</tr>
<tr>
<td>Overall exploitation difficulty</td>
<td>medium</td>
<td>high</td>
</tr>
</tbody>
</table>
Consultant’s advice

- Make yourself periodic vulnerability assessments (e.g. Nessus scans)
- Prepare your network before a pentest (you should always be prepared, btw)
- An homogeneous network is easier to defend then an heterogeneous one
- Do not allow local admin rights for regular users
- Patch, patch, patch
- Educate users for security risks
Conclusions

- Penetration testing can be used for improving our cyber security
- Do it periodically with specialized people
- Mandatory for new applications / systems before putting in production
- Vulnerability assessment is not penetration testing
Q & A
Thank You!

Adrian Furtună, PhD, OSCP, CEH
adif2k8@gmail.com
http://ro.linkedin.com/in/adrianfurtuna