How to Build Your Own Escape Room
Bob Hewitt - CIO
• CISSP, GSEC, GCIH, GPEN, GWAPT, CIPP/e
• SANS Community Instructor
• linkedin.com/in/bobhewitt/
• @infosecbobh

Justin Perkins
• Systems Administrator
• Game Master
• Lego Builder
Death by PowerPoint

- Annual and new hire
- 50+ Slides
- > 2 hours
Escape Room

• 60 Minute Real Life Adventure Game
• Themed room
• Find hidden clues
• Solve challenging puzzles
• Requires Teamwork, Speed, Creativity, and Patience
Where to Start?

• Define your objectives
• Make it relatable to all groups
• Build teams that builds teams
The Mission

You have been assigned to the Information Security Team. (Yes! Your dream job!) Sadly an adversary has compromised one credit card record, that’s right, one!

A separate team is looking into how this happened, while your job is to define the scope of the breach to the single record, otherwise we may have an obligation to report to every credit card user on the system.
Rules

• The game master is always right.
• 60 Minute limit.
• All information associated with the game is classified as confidential and will be downgraded once all teams have completed.
• All policies and procedures must be followed.
• Workstations and partitions cannot be moved.
• The game master is always right….Really!
Penalties

- Hints upon request: 5 Minutes
- Security policy fail: 5 Minutes
- Breaking of a General Rule: 5 Minutes
Objective 1: Demonstrate passwords can easily be guessed or cracked.
Objective 2: Identify improperly stored PII.
There are two files on the desktop:

- Bank Rec Summary
- Bank Rec Details

Find the error in the digital files and use the PII in the printouts on the user’s desk to determine the code to unlock the box!
Objective 3: The level of protection should be proportionate to what we are protecting
Take one badge per player.
Keep the badge you take.

The Caesar Cipher requires an offset number and is read from the outside to the inside.
Objective 4: Demonstrate compliance of physical access control policies and procedures.
Objective 5: Recognize risk of password reuse.
Guiding Philanthropy through Technology
Objective 6: Identify Phishing attempt e-mails
Guiding Philanthropy through Technology

- Green-Y
- Black-P
- Grey-E
- Blue-B
Objective 7: Perform a manual cipher decryption.
Offset: 10

- Green: Y = O
- Black: P = F
- Grey: E = U
- Blue: B = R
Objective 8: Perform a file decryption using 7zip.
Guiding Philanthropy through Technology
Objective 9: Crack a hash using an online resource

0B20E35DE6FF81A819A7190DC4942C816525BDC915D11947D91E34CAA2469D86::narnia@gmail.com
07862D2A64F3D41C460387BF78160C92886EE5621A1714DC5B3BD8D931D493A5::legomylego@yahoo.com
1D92DAE504A70FBCAE6D3721A55D7EACAF94D3133EA5F0394B7D203D64841110::stillonaol@aol.com
1DA9133AB9D8D11D2937EC8D312E1E2569857059E73CC72DF92E670928983AB5::fullmetaljacket@gmail.com
A88A14ABDAB5DA4BD70E6960B01A6032C661502EA7650A2D853E8B0B3829C146::paulsimon@yahoo.com
BF4FFB1487762665C9B1059533745BB6190D2C60B9D85CE68DEA4D1C4C274::masterlegobuilder@yahoo.com
1DA9177AB98BD11D2937EC8D1925E1E2574957059E73CC72DF92E670928983AB5::<your company>awareness@gmail.com
56093992BC45C1319389321E31880279663A035A18C32077BF77002076C1DE3::itwasntme@compuserve.com
### Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
0CF289D2C237D4851AF3C2695FA4239CA2F4B0AEEF4EE35A0E677C56FFA9EE58
D639DA0678B0D30E49E1D194539EF68E62D6228BEDCF2OEC6503DA65991BEE05
EB06A291CFCE3E1F3B8BD34E5E3E8933C3CCE4FB4E5181F1F566079E81
0820E3D666FA81A19A7190DCA942C8165258DC0151D194F01E3CAAA46D86
076820DA64F3D41463C878BF78160C9286EE5621A1154C9BDD80931049A5
1D92DAA504A70FCBEA6037214A55D7ECAAF94D3133E4F3094B7D03D64841110
1DA91334B9BDD1102937C80332E125698575907E3C7722F92670928983A85
0A88A14A80B5A4B070E9680601A60326G1502E7A6560A20853E603829C146
BF8FFB1487762665C9B10595537458861902DC6099685CE68DEAD41C4C74
56F9892B8C45C13193839321E1388027965A03F5A18C32077BF770020761CDE3
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

<table>
<thead>
<tr>
<th>Hash</th>
<th>Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>0CF289D2C237D4851AF3C2695FA4239CA2F4B0AEEF4EE35A0E677C56FFA9EE58</td>
<td>Unknown</td>
<td>Not found.</td>
</tr>
<tr>
<td>D639DA0678B0D30E49E1D194539EF68E62D6228BEDCF2OEC6503DA65991BEE05</td>
<td>Unknown</td>
<td>Not found.</td>
</tr>
<tr>
<td>EB06A291CFCE3E1F3B8BD34E5E3E8933C3CCE4FB4E5181F1F566079E81</td>
<td>Sha256</td>
<td>Testing</td>
</tr>
<tr>
<td>0B20E3D666FA81A19A7190DCA942C8165258DC0151D194F01E3CAAA46D86</td>
<td>Sha256</td>
<td>Password123$</td>
</tr>
<tr>
<td>076820DA64F3D41463C878BF78160C9286EE5621A1714D5C3BBD80931049A5</td>
<td>Sha256</td>
<td>Insecure</td>
</tr>
<tr>
<td>1D92DAA504A70FCBEA6037214A55D7ECAAF94D3133E4F3094B7D03D64841110</td>
<td>Sha256</td>
<td>thisismypassword</td>
</tr>
</tbody>
</table>
Objective 10: Demonstrate methods to send sensitive information securely
BONUS! (not really)

USB Drive left on table:
10 Minutes

Send information insecurely:
10 Minutes
Fail!

- Remote Users
- Windows Updates
- Gmail not logged out
- Forgot to delete the decrypted 7zip file
- Forgot to empty the recycle bin
- Book safe not locked
- Prizes
Make it your own!

• Define your objectives
• Define your teams
• Present your objectives to management
• Set your budget
• Test and test again
• Let us know how it went
Questions?