

# Passwords Are Everywhere!

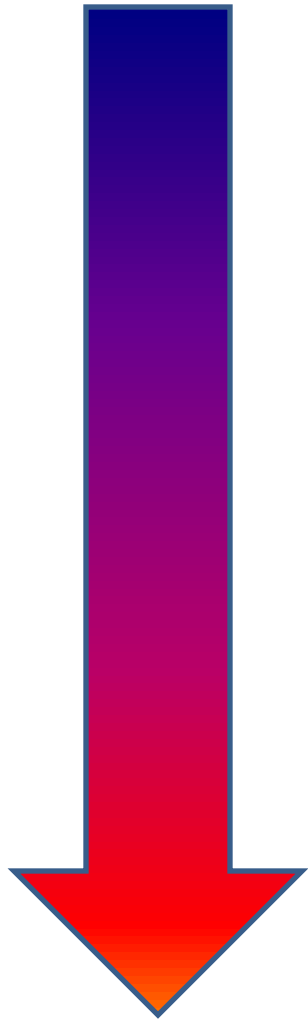
*Hal Pomeranz*

*Deer Run Associates*

# Why Is Password Evidence Useful?

- Attribution
- Evidence of conspiracy
- Cracking encrypted containers and archives
- Finding other data (including more passwords!)

# Easy or Hard?



Unencrypted  
(easy)

Command history  
Scripts  
Web apps/databases  
Mobile Apps

Obfuscated  
(not much harder)

App user profiles

Encrypted  
(give up)

LANMan Hashes

Cryptographic hashes

# Command History

Unix/Linux –

```
$HOME/.bash_history
```

```
$HOME/.mc/history
```

Windows – only in memory, unfortunately

```
mysql -u root -p SekretPass sekretdb
```

```
zip -r -P VerySekrit sekret.zip foo/*
```

```
net use x: \\server\myshare
```

```
/USER:somedomain\skippy MySekritPwd
```

# Scripts Are Great For...

- Database passwords
- Archive passwords
- Login passwords on remote systems

```
"C:\Pr open backupuser:BackupPass@remotehost  
/scr: option transfer binary  
option confirm off  
option batch continue  
get -delete /backup/*.zip C:\Backup\  
close  
exit
```

# Web Apps

- Apps connect to back-end databases
- Connection requires username/password
- Usually stored in "include file"

# Find That Password!

1. Look for the \*\_connect call:

```
$db = @mysql_connect($DBHOST, $DBUSER, $DBPASS) ...
```

2. Find the variable declarations:

```
$DBHOST = 'localhost';
```

```
$DBUSER = 'root';
```

```
$DBPASS = "";
```

```
# Yes, really. *sigh*
```

3. Profit!

# Now That You're In That DB...

```
mysql> select * from user;
```

```
+-----+-----+-----...  
| User          | Password      | ...  
+-----+-----+-----...  
| sally43       | DaisyDaisy    | ...  
| john316       | ?Beg8t23     | ...  
| frank42       | qwertyu      | ...  
| johanp22      | 111111111    | ...  
| mary314       | L0ng1tude!   | ...  
| ...
```



# (Mobile) Apps

- Users choose "save password" option
- Apps do not always encrypt password
- Mobile apps often the worst offenders:
  - TouchTerm SSH app
  - Livejournal

Get directly from device *or backup directory*

# Slightly More Difficult

- App stores password with minor obfuscation

PSI (Jabber/XMPP client) – **accounts.xml**

<http://blogmal.42.org/rev-eng/psi-password.story>

Total Commander (file manager) – **wcx\_ftp.ini**

<http://en.totalcmd.pl/download/add/tls/DecrypTC>

# Think Like a Hacker

- Consider extracting/cracking LanMan hashes
- Make sure this activity is within scope!
- Use LM hashes as input for NTLM cracking

# Get Your Hashes Here!

- Memory – **volatility hashdump**
- SAM/System hives – **fgdump**
- Active Directory NTDS.DIT  
<http://sourceforge.net/projects/libesedb/>  
<http://csababarta.com/en/ntdsxtract.html>

# Get Cracking!

- Free web-based cracking:  
<http://www.md5decrypter.co.uk/>
- Pre-computed rainbow tables:  
<http://project-rainbowcrack.com/>
- Old standby (see also "-rules=NT" for NTLM):  
<http://www.openwall.com/john/>

# Now That You've Got Passwords...

- Crack open protected archives and volumes
- Pivot!

# Gotcha!

```
# grep SekretPass strings.asc
```

```
1463480375      Password: SekretPass
```

```
# blkcat forensic.img 357295
```

```
Host: www.evil.com
```

```
User: root
```

```
Password: SekretPass
```

```
Host: www.botnet-admin.net
```

```
User: admin
```

```
Password: MySekritPwd
```

```
...
```

# Wrap-Up

- Thanks for listening!
- Any final questions?
- Please fill out your surveys!

Hal Pomeranz

hal@deer-run.com

Deer Run Associates

@hal\_pomeranz

<http://www.deer-run.com/~hal/>