ROMHACK

PING CASTLE

How to impress your management

when you are an Active Directory noob?

Vincent LE TOUX – 15:15 -> 16:00

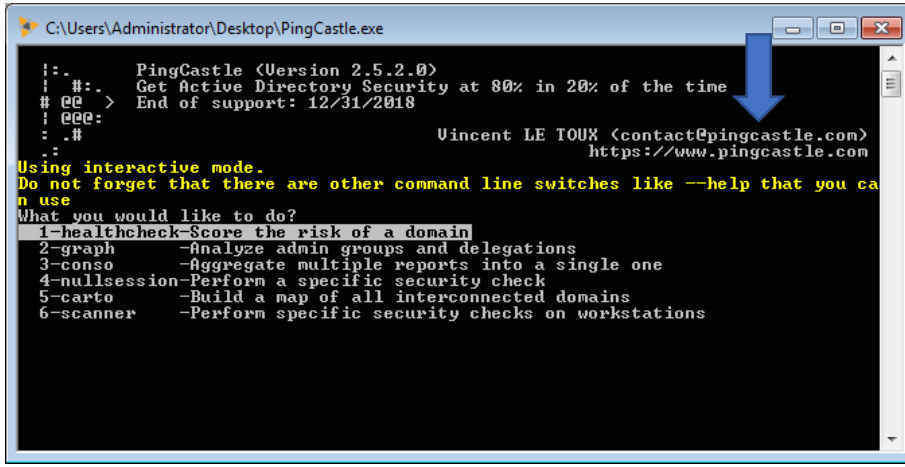
#RomHack2019
28th of September 2019 in Rome

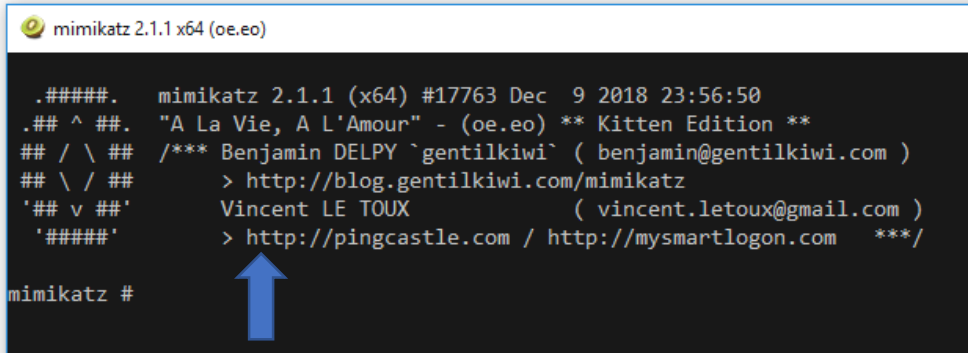
Whoami

Vincent LE TOUX

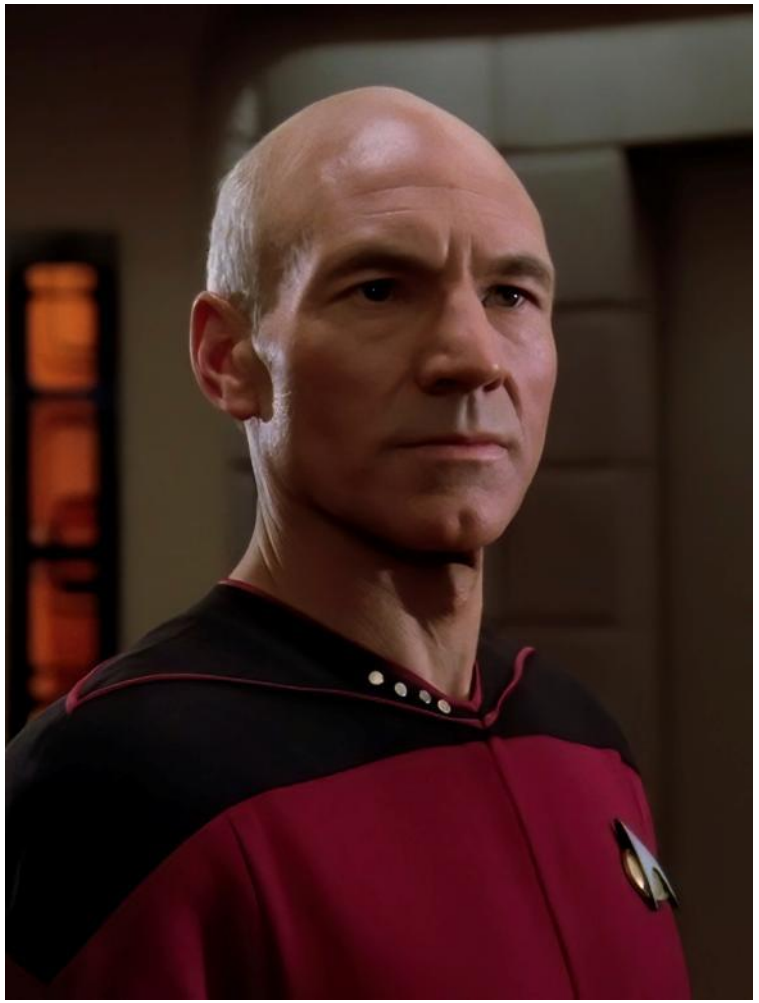
https://www.pingcastle.com / @mysmartlogon

- Management (Architect, Blue team, CISO)
- Former AD Newbie (not an admin)
- Write code (GIDS applet, OpenPGP card driver, OpenSC, mimikatz, PingCastle, …)
- Now Speaker (blackhat, bluehat, trooper hackinParis, first, …)





So you want to impress Jean-Luc?



- Jean-Luc (it's so French) is your manager
- He somewhat knows that AD is important for security (because he types his password to log on)
- But as a manager, he has 100+ subjects to cover
- You're the security guy: fix it without additional budget!

But…

What happens when you talk security in general

THE BASICS

BECAUSE JEAN-PIERRE ASKS FOR « BASIC » QUESTIONS

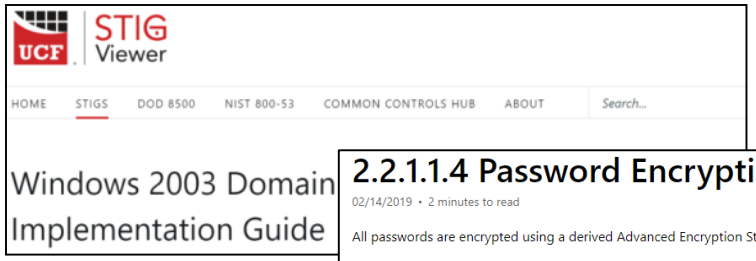
Where is the 101 AD course?

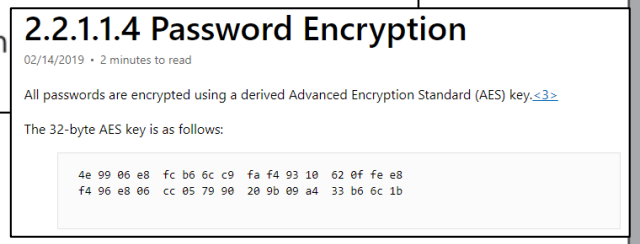
Framework

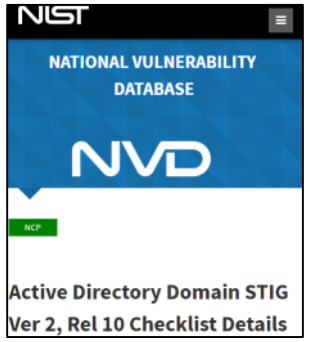
Focused

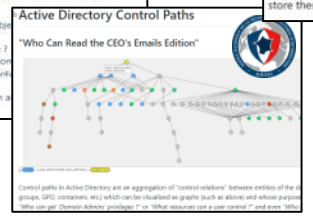
General

Tools









I just wanted to answer the stupid question
« How much domains do I have ? »

Starting with simple questions: How much users do I have in my domain?

Total number of user accounts in AD

```
PS> (Get-ADUser -filter *).count
```

Fast (2 minutes), but require RSAT

versus

```
(New-Object DirectoryServices.DirectorySearcher -Property @{
 Filter = '(&(objectClass=group)(!(member=*)))'
 PageSize = 100
}).FindAll()
```

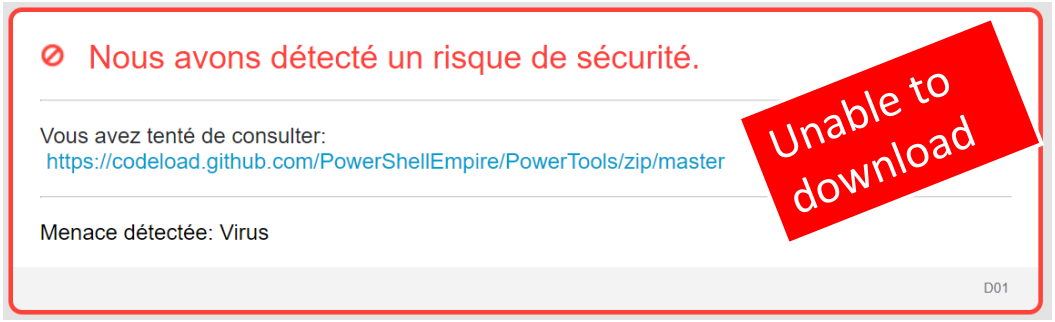
Slow (> 40 minutes), but no prerequisite

Starting with simple questions: How much domains are connected?

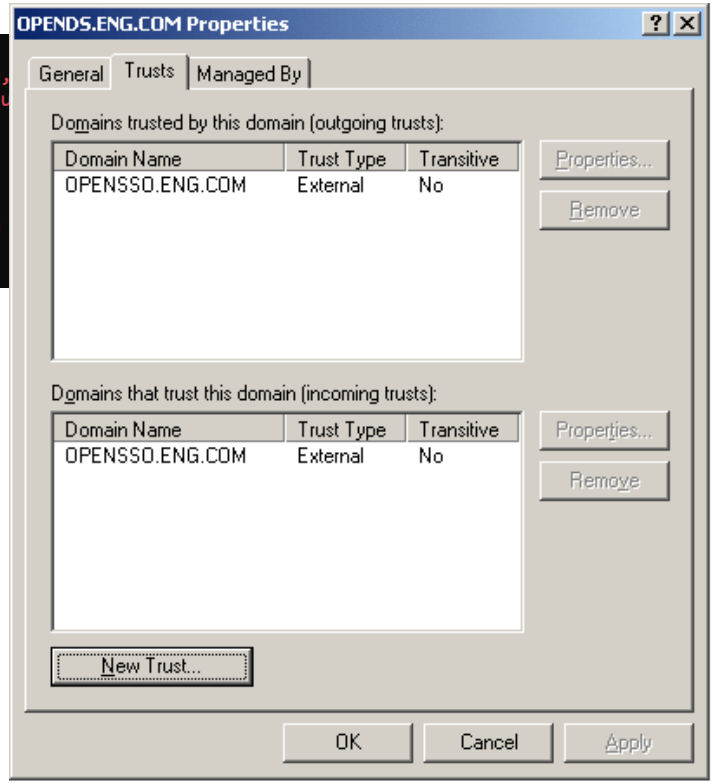
Get-ADTrust or netdom => Requires RSAT

```
PS C:\Users\HG2025> Get-ADTrust -Filter *
Get-ADTrust : Le terme «Get-ADTrust» n'est pas reconnu comme nom d'applet de commande, fonction,
programme exécutable. Vérifiez l'orthographe du nom, ou si un chemin d'accès existe, vérifiez qu
est correct et réessayez.
Au caractère Ligne:1 : 1
+ Get-ADTrust -Filter *
+ ~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (Get-ADTrust:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException
C:\Users\HG2025>netdom
'netdom' n'est pas reconnu en tant que commande interne
ou externe, un programme exécutable ou un fichier de commandes.
```

PowerView => part of Empire



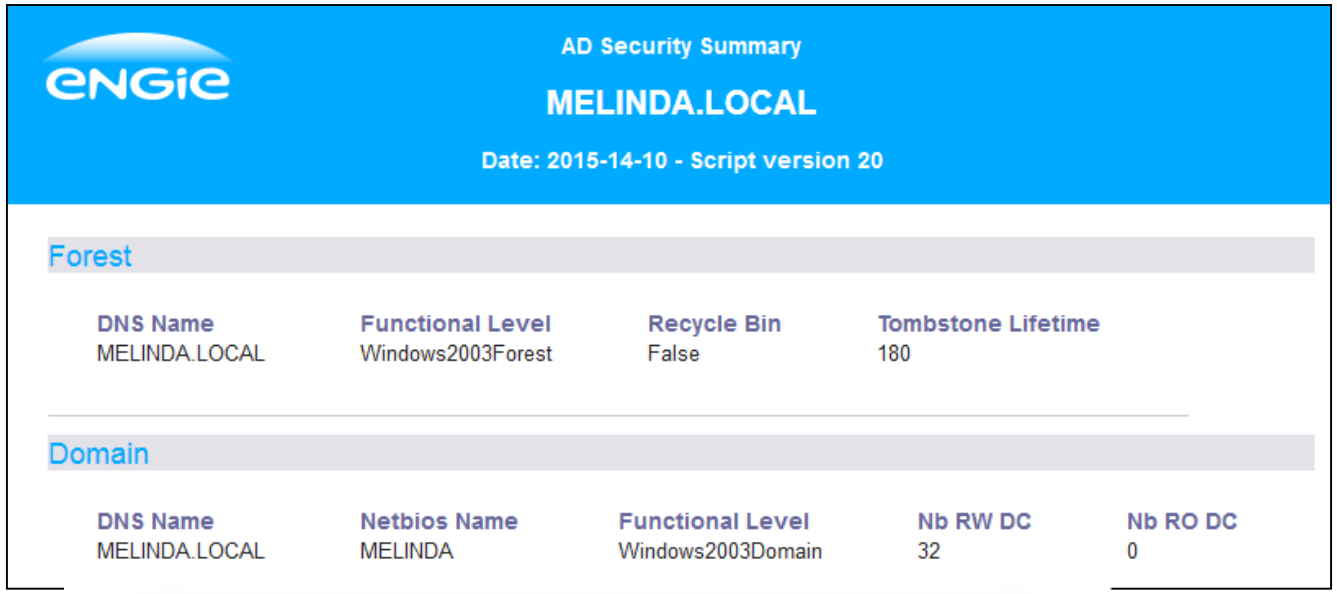
Trust dialog => requires RSAT



Need the Admin!
(but he has other things to do)

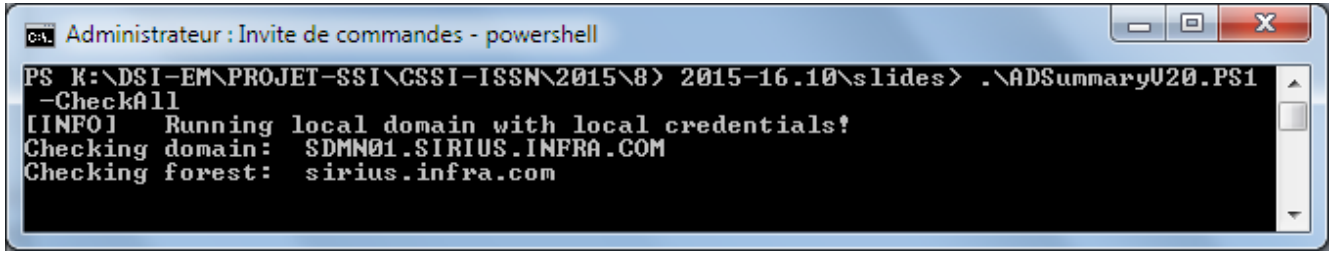
The 2 top pages of google search for « list active directory trust » return inapplicable links

Goal: provide a global overview



- **Objective:**
  Build a AD map and identify the major vulnerabilities
- **Inspired from:**
  Previous audit (ex: ADSA, …) + best practices
- **Idea:**
  Bind each problem to the team accountable for it

Powershell: Challenge of a scripting language



Script parameters

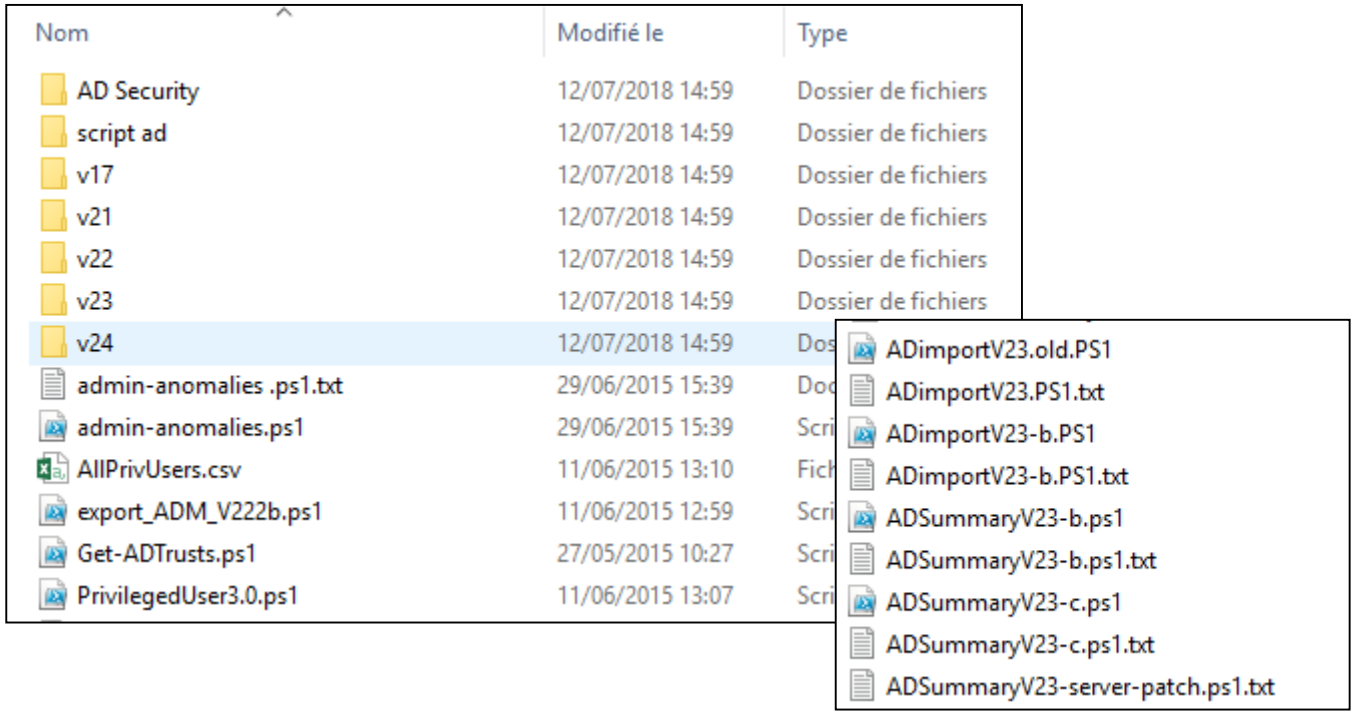
The script can be limited to a set of checks with the following parameters:
-CheckUpdates,
-CheckAll,
-CheckGroups,
-CheckUsers,
-CheckComputers,
-CheckTrusts,
-CheckPasswordPolicy,
-CheckAnomalies,
-CheckPWDmgmt,

Easy to modify

But

- Hard to debug (remotely)
- Output: NULL / an object / an array
- Enumerate group when a member is a FSP
- Few expertise locally

And as a consequence so many versions



About 6 months of trial & error process before getting something stable

- # history:
- # 2015-07 proof of concept made after the AD security workshop
- # 2015-09 bug fixing & adaptation for GSIT
- # 2015-10 first POC after adaptation made
- # 2015-11 POC finalization after comments from corporate security

Feedback from AD expert « challenging »
(a newbie coming to them)

Difficulties to share technical information vs KPI

Demo

IT'S HARD TO FIX THINGS

BECAUSE THERE IS NO MAGIC

102: the Vulnerability scanner

Microsoft Windows SMB NULL Session Authentication

MEDIUM Nessus Plugin ID 26920

Synopsis

It is possible to log into the remote Windows host with a NULL session.

Description

The remote host is running Microsoft Windows. It is possible to log into it using a NULL session (i.e., with no login or password).

Depending on the configuration, it may be possible for an unauthenticated, remote attacker to leverage this issue to get information about the remote host.

Solution

Apply the following registry changes per the referenced Technet advisories :

Set :
- HKLM\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous=1
- HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\restrictnullsessaccess=1

Remove BROWSER from :
- HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\NullSessionPipes

Reboot once the registry changes are complete.

See Also

https://support.microsoft.com/en-us/help/143474/restricting-information-available-to-anonymous-logon-users

https://support.microsoft.com/en-us/help/246261

http://technet.microsoft.com/en-us/library/cc785969(WS.10).aspx

Plugin Details

Severity: Medium

ID: 26920

File Name: smb_null_session.nasl

Version: 1.32

Type: remote

Agent: windows

Family: Windows

Published: 2007/10/04

Updated: 2018/11/15

Dependencies: 10394

Risk Information

Risk Factor: Medium

CVSS v2.0

Base Score: 5

Temporal Score: 3.7

Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

Temporal Vector: CVSS2#E:U/RL:OF/RC:C

Vulnerability Information

- Scan systems and report vulnerabilities
- Run every month/quarter
- Provide list of fixes to apply

Forward to the admin, Right ?

Testing if the problem has been fixed

```
$ nmap -p 445 -Pn -n --open --script=smb-enum-users \
> --script-args=smbnoguest 192.168.57.105
Starting Nmap 7.70 ( https://nmap.org ) at 2018-04-28 18:35 SAST
Nmap scan report for 192.168.57.105
Host is up (0.00030s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-enum-users:
|   User-PC\Administrator (RID: 500)
|     Description: Built-in account for administering the computer/domain
|     Flags:       Account disabled, Normal user account, Password does no
t expire
|   User-PC\Guest (RID: 501)
|     Description: Built-in account for guest access to the computer/domai
n
|     Flags:       Account disabled, Normal user account, Password not req
uired, Password does not expire
|   User-PC\HomeGroupUser$ (RID: 1001)
|     Full name:   HomeGroupUser$
|     Description: Built-in account for homegroup access to the computer
|     Flags:       Normal user account, Password does not expire
|   User-PC\User (RID: 1002)
|_    Flags:       Normal user account, Password not required, Password do
es not expire

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
```

```
$ rpcclient 192.168.57.105 -U'%' -c'querydispinfo'
could not obtain sid from server
error: NT_STATUS_ACCESS_DENIED
```

```
TCP     57500 → 445 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=969964135 TSecr
TCP     445 → 57500 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSva
TCP     57500 → 445 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=969964135 TSecr=1641308
SMB     Negotiate Protocol Request
SMB     Negotiate Protocol Response
TCP     57500 → 445 [ACK] Seq=54 Ack=118 Win=29312 Len=0 TSval=969964135 TSecr=1641308
SMB     Session Setup AndX Request, User: anonymous
SMB     Session Setup AndX Response
SMB     Tree Connect AndX Request, Path: \\192.168.57.105\IPC$
SMB     Tree Connect AndX Response
SMB     NT Create AndX Request, FID: 0x4000, Path: \samr
SMB     NT Create AndX Response, FID: 0x4000
DCERPC  Bind: call_id: 1094795585, Fragment: Single, 1 context items: SAMR V1.0 (32bit NDR
SMB     Write AndX Response, FID: 0x4000, 72 bytes
SMB     Read AndX Request, FID: 0x4000, 2048 bytes at offset 0
DCERPC  Bind_ack: call_id: 1094795585, Fragment: Single, max_xmit: 2048 max_recv: 2048, 1
SAMR    Connect4 request
SMB     Write AndX Response, FID: 0x4000, 84 bytes
SMB     Read AndX Request, FID: 0x4000, 4097 bytes at offset 0
SAMR    Connect4 response
SAMR    EnumDomains request
SMB     Write AndX Response, FID: 0x4000, 52 bytes
SMB     Read AndX Request, FID: 0x4000, 4097 bytes at offset 0
SAMR    EnumDomains response
SAMR    LookupDomain request, User-PC[Long frame (2 bytes)]
SMB     Write AndX Response, FID: 0x4000, 80 bytes
SMB     Read AndX Request, FID: 0x4000, 4097 bytes at offset 0
SAMR    LookupDomain response
SAMR    OpenDomain request
SMB     Write AndX Response, FID: 0x4000, 76 bytes
SMB     Read AndX Request, FID: 0x4000, 4097 bytes at offset 0
SAMR    OpenDomain response
SAMR    QueryDisplayInfo request
SMB     Write AndX Response, FID: 0x4000, 60 bytes
SMB     Read AndX Request, FID: 0x4000, 4097 bytes at offset 0
SAMR    QueryDisplayInfo response
SAMR    Close request
SMB     Write AndX Response, FID: 0x4000, 44 bytes
SMB     Read AndX Request, FID: 0x4000, 4097 bytes at offset 0
SAMR    Close response
SAMR    Close request
SMB     Write AndX Response, FID: 0x4000, 44 bytes
SMB     Read AndX Request, FID: 0x4000, 4097 bytes at offset 0
SAMR    Close response
SMB     Tree Disconnect Request
SMB     Tree Disconnect Response
SMB     Logoff AndX Request
SMB     Logoff AndX Response
TCP     57500 → 445 [FIN, ACK] Seq=1943 Ack=2587 Win=35328 Len=0 TSval=969964141 TSecr=164
```

```
1  net use \\IP_ADDRESS\ipc$ "" /user:""
2  net use
```

- Because you don't want to wait for 1 month
- Require Linux, admin right, or mixed environment

And …

- Not 100% reliable

https://sensepost.com/blog/2018/a-new-look-at-null-sessions-and-user-enumeration/
https://www.adampalmer.me/iodigitalsec/2013/08/10/windows-null-session-enumeration/

Real null session enumeration

MS-SAMR

- Well known null session
- Aka: connect and enumerate users with the user named « »

MS-LSAT

- « Just » translate SID from « S-1-5-2345-34876-345-500 » to « administrator »

Then S-1-5-2345-34876-345-501
Then S-1-5-2345-34876-345-502
Then S-1-5-2345-34876-345-503
…

« Secret » Root causes

Windows 2003 DC installed 15 years ago

Sharepoint SPN missing (*)

- You can modify the AD behavior with the special attribute dSHeuristics

7	fLDAPBlockAnonOps

If this character is "2", then the fLDAPBlockAnonOps heuristic is false; otherwise, the fLDAPBlockAnonOps heuristic is true. If this character is not present in the string, it defaults to "2" when the DC functional level is less than DS_BEHAVIOR_WIN2003, and to "0" otherwise.

Section 5.1.3 specifies the effects of this heuristic.

Not obvious. How can you be 100% sure of a remediation?

IMPRESS THE AD GUY

BECAUSE THE AD GUY WILL DO 80% OF THE JOB

~~AND YOU DID A BAD JOB WILL VULNERABILITIES~~

Detect unpatched computers

2.2.4 SMB2 NEGOTIATE Response

05/01/2019 • 4 minutes to read

The SMB2 NEGOTIATE Response packet is sent by the server to notify the client of the preferred common dialect. This response is composed of an SMB2 header, as specified in section 2.2.1, followed by this response structure.

0	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1
StructureSize																SecurityMode															
DialectRevision																NegotiateContextCount/Reserved															
ServerGuid																															
...																															
...																															
...																															
Capabilities																															
MaxTransactSize																															
MaxReadSize																															
MaxWriteSize																															
SystemTime																															
ServerStartTime																															

Without any authentication!

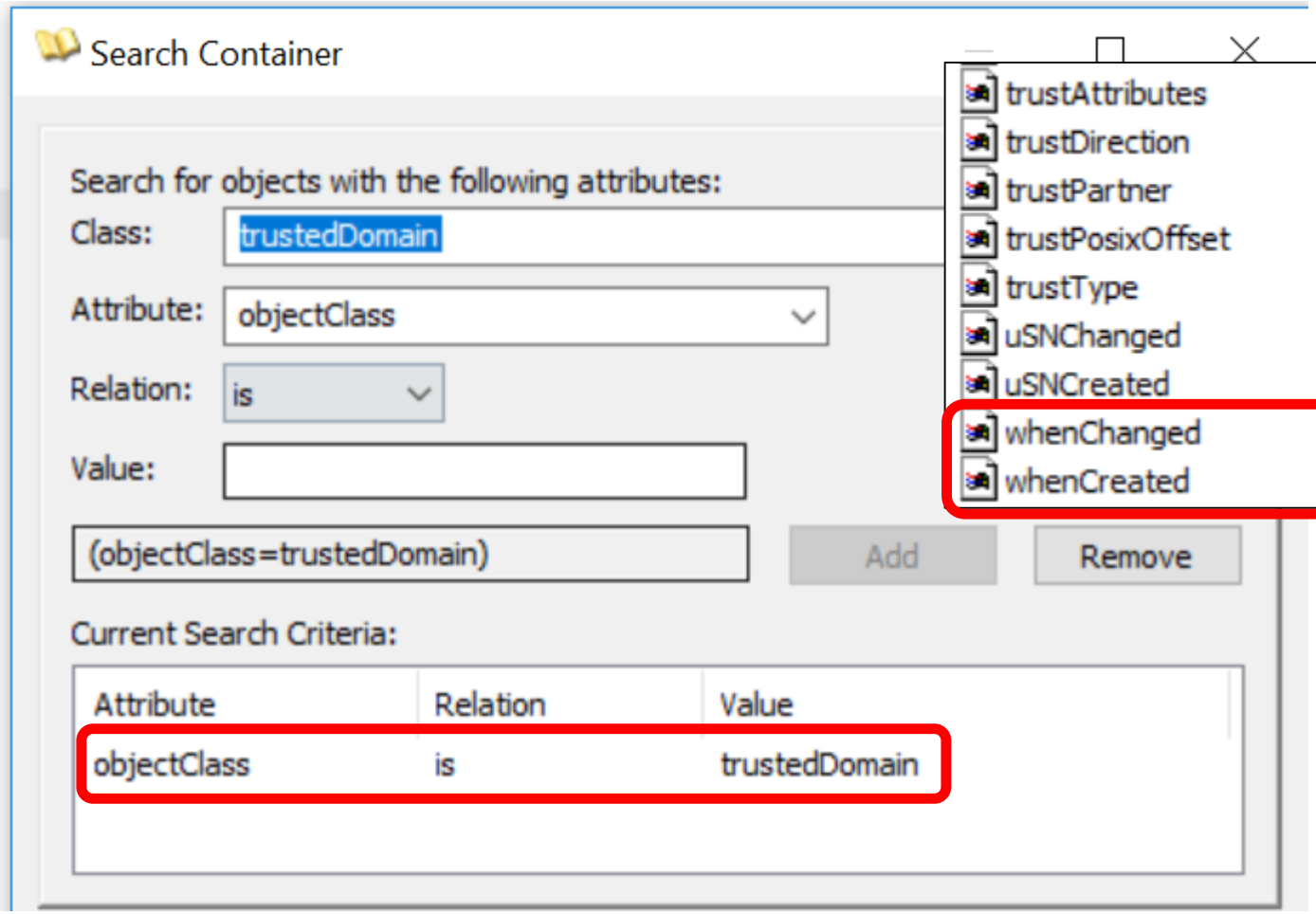
With normal authentication

net time \\domaincontroller1.corp.local

No public Windows Update info.
But if a server is unpatched, it is not rebooted for a while …

https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-smb2/63abf97c-0d09-47e2-88d6-6bfa552949a5

Trust creation time / is active

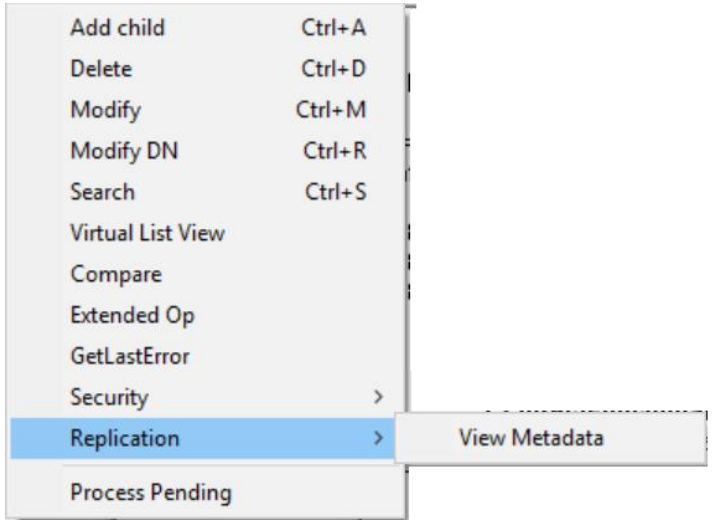


trustAttributes	Integer	1	0
trustDirection	Integer	1	1
trustPartner	DirectoryString	1	dmz.local
trustPosixOffset	Integer	1	0
trustType	Integer	1	2
uSNChanged	Integer8	1	0x55E8F58
uSNCreated	Integer8	1	0x7813C
whenChanged	GeneralizedTime	1	21/08/2019 13:33:00
whenCreated	GeneralizedTime	1	14/12/2017 14:31:01

- whenCreated=trust creation
- If whenChanged + 30 days < today, then trust is inactive

Meta « data » 1/2

- Help to answer many questions
- Retrieved by ldp.exe or ADSIEdit with computed attributes (not ADExplorer)



36 entries.

AttID	Ver	Loc.USN	Originating DSA	Org.USN	Org.Time/Date
0	1	492375	627f897e-1e40-4bf8-9473-8bc879db6673	364556	2017-05-18 16:30:37
3	1	492375	9cfb2b44-0061-4abc-87ec-bfc0cfc2e2ae	492375	2018-10-12 11:00:23
d	2	492375	627f897e-1e40-4bf8-9473-8bc879db6673	364561	2017-05-18 16:30:37
20001	1	492375	627f897e-1e40-4bf8-9473-8bc879db6673	364556	2017-05-18 16:30:37
20002	1	492375	627f897e-1e40-4bf8-9473-8bc879db6673	364556	2017-05-18 16:30:37
2000d	1	492375	627f897e-1e40-4bf8-9473-8bc879db6673	364557	2017-05-18 16:30:37
200a9	1	492375	627f897e-1e40-4bf8-9473-8bc879db6673	364556	2017-05-18 16:30:37
20119	2	492375	627f897e-1e40-4bf8-9473-8bc879db6673	367273	2017-05-18 16:45:46
90001	1	492375	627f897e-1e40-4bf8-9473-8bc879db6673	364556	2017-05-18 16:30:37
90008	3	492375	627f897e-1e40-4bf8-9473-8bc879db6673	364558	2017-05-18 16:30:37
90010	1	492375	627f897e-1e40-4bf8-9473-8bc879db6673	364557	2017-05-18 16:30:37
90019	1	492375	627f897e-1e40-4bf8-9473-8bc879db6673	364557	2017-05-18 16:30:37
9002c	1	492375	627f897e-1e40-4bf8-9473-8bc879db6673	364557	2017-05-18 16:30:37
9002d	1	492375	627f897e-1e40-4bf8-9473-8bc879db6673	364557	2017-05-18 16:30:37
90037	28	93210844	600a60ea-3ed5-4c9d-ac9f-a4e7103bc27f	90235774	2019-08-22 02:06:39
9003e	1	492375	627f897e-1e40-4bf8-9473-8bc879db6673	364557	2017-05-18 16:30:37
90040	1	492375	627f897e-1e40-4bf8-9473-8bc879db6673	364557	2017-05-18 16:30:37
9005a	28	93210844	600a60ea-3ed5-4c9d-ac9f-a4e7103bc27f	90235774	2019-08-22 02:06:39
90060	28	93210844	600a60ea-3ed5-4c9d-ac9f-a4e7103bc27f	90235774	2019-08-22 02:06:39
90062	1	492375	627f897e-1e40-4bf8-9473-8bc879db6673	364557	2017-05-18 16:30:37
9007d	27	93210844	600a60ea-3ed5-4c9d-ac9f-a4e7103bc27f	90235775	2019-08-22 02:06:39
9008a	1	492375	627f897e-1e40-4bf8-9473-8bc879db6673	364557	2017-05-18 16:30:37
9008b	1	492375	627f897e-1e40-4bf8-9473-8bc879db6673	364557	2017-05-18 16:30:37
90092	1	492375	627f897e-1e40-4bf8-9473-8bc879db6673	364556	2017-05-18 16:30:37
90096	1	492375	627f897e-1e40-4bf8-9473-8bc879db6673	367273	2017-05-18 16:45:46
9009c	1	492375	627f897e-1e40-4bf8-9473-8bc879db6673	364557	2017-05-18 16:30:37
9009f	1	492375	627f897e-1e40-4bf8-9473-8bc879db6673	364557	2017-05-18 16:30:37
900a0	28	93210844	600a60ea-3ed5-4c9d-ac9f-a4e7103bc27f	90235774	2019-08-22 02:06:39
900dd	1	492375	627f897e-1e40-4bf8-9473-8bc879db6673	364556	2017-05-18 16:30:37
9012e	1	492375	627f897e-1e40-4bf8-9473-8bc879db6673	364556	2017-05-18 16:30:37
90303	1	492375	627f897e-1e40-4bf8-9473-8bc879db6673	364678	2017-05-18 16:30:51
9030e	1	492375	627f897e-1e40-4bf8-9473-8bc879db6673	364556	2017-05-18 16:30:37
90364	1	492375	627f897e-1e40-4bf8-9473-8bc879db6673	364556	2017-05-18 16:30:37
907ab	1	492375	627f897e-1e40-4bf8-9473-8bc879db6673	364666	2017-05-18 16:30:38

unicodePwd

https://github.com/vletoux/ADSecrets/blob/master/AttdIDToAttribute

Meta « data » 2/2

- Answer question such as: Number of time the krbtgt password has been changed and when is the last time (reset clears pwdlastset)
- See MS-ADTS 3.1.1.2.1 Schema NC:
  - Last time the schema has been changed
  - Number of changes since the creation of the forest

For example, here is a value of schemaInfo:

0xFF 0x00 0x00 0x07 0xC7 0x20 0x79 0x92 0xE6 0x84 0xB6 0xF6 0x40 0x99 0x47 0x21 0x8B 0xC9 0xE0 0xF1 0xF3

After a schema change is done on the schema master, the following is the new value:

0xFF 0x00 0x00 0x07 0xC8 0x20 0x79 0x92 0xE6 0x84 0xB6 0xF6 0x40 0x99 0x47 0x21 0x8B 0xC9 0xE0 0xF1 0xF3

- Backup time & strategy via dSASignature

```
PS C:\Users\Administrator\Desktop\Scripts\JIT> repadmin /showbackup halodc02

Loc.USN                              Originating DSA  Org.USN  Org.Time/Date        Ver Attribute
=======                              ===============  =========  =============        === =========
DC=ForestDnsZones,DC=halo,DC=net
  16412      8549be89-c654-4352-987c-96043bf55b98     16412 2012-08-08 10:09:03     1 dSASignature
DC=DomainDnsZones,DC=halo,DC=net
  16411      8549be89-c654-4352-987c-96043bf55b98     16411 2012-08-08 10:09:03     1 dSASignature
CN=Schema,CN=Configuration,DC=halo,DC=net
  16410      8549be89-c654-4352-987c-96043bf55b98     16410 2012-08-08 10:09:03     1 dSASignature
CN=Configuration,DC=halo,DC=net
  16409      8549be89-c654-4352-987c-96043bf55b98     16409 2012-08-08 10:09:03     1 dSASignature
DC=halo,DC=net
  16408      8549be89-c654-4352-987c-96043bf55b98     16408 2012-08-08 10:09:03     1 dSASignature
```

Demo

- Enumerate users of the bastion

- Check if Sysmon / AV is installed
  https://github.com/vletoux/TestAntivirus/blob/master/testAV.ps1

LESSONS LEARNED DEALING WITH « MANAGEMENT »

Management ♡ simplicity

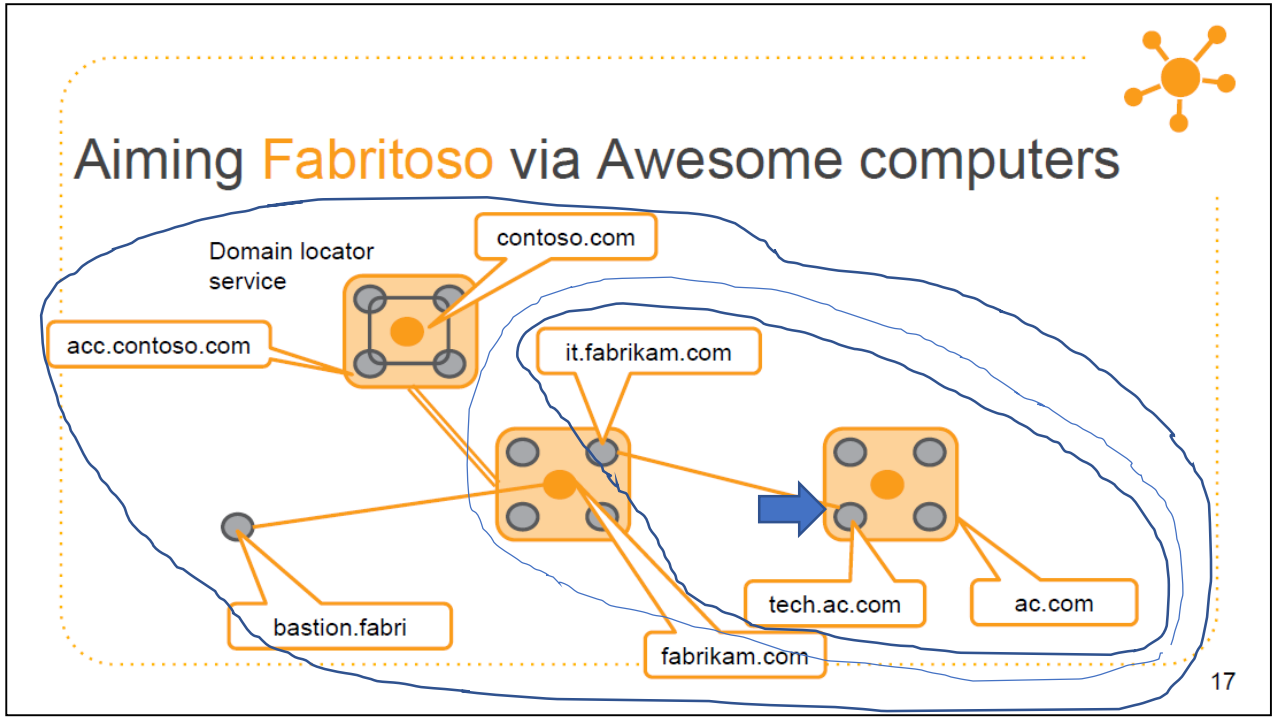
Make Actions

Simple enough

To be understood

By the Management

Do not waste the management's energy



- The more domains… the more you discover
- Tieredness if the discovery is too slow
- Published research on AD discovery (up to a depth of 5 levels)

https://www.bluehatil.com/2018/files/Active%20Directory%20What%20Can%20Make%20Your%20Million%20Dollar%20SIEM%20Go%20Blind.pdf

READY?

HOW TO IMPRESS YOUR MANAGEMENT?

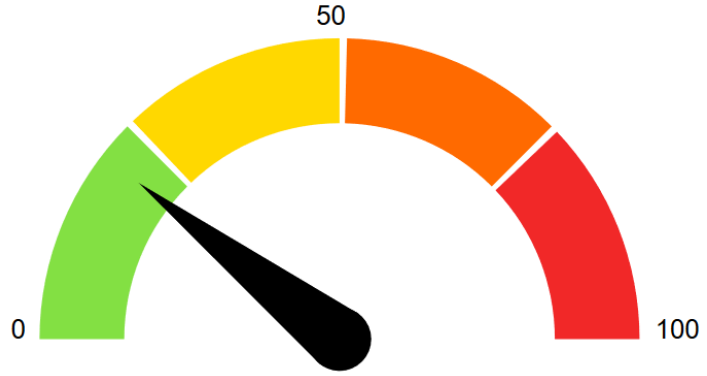
1. Ask to run PingCastle

- Ask Jean-Luc
- To make ALL AD Owner run PingCaslte ONCE this quarter
- To evaluate the budget for NEXT YEAR
- And it costs no money

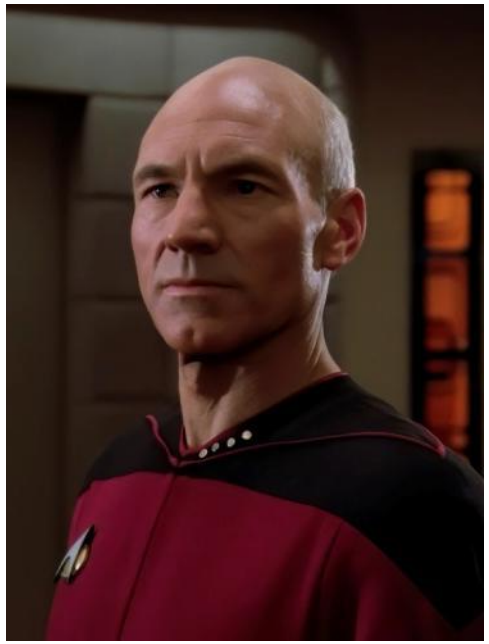
2. PingCastle Magic

3. Explain to the lower management

Happy Jean-Luc

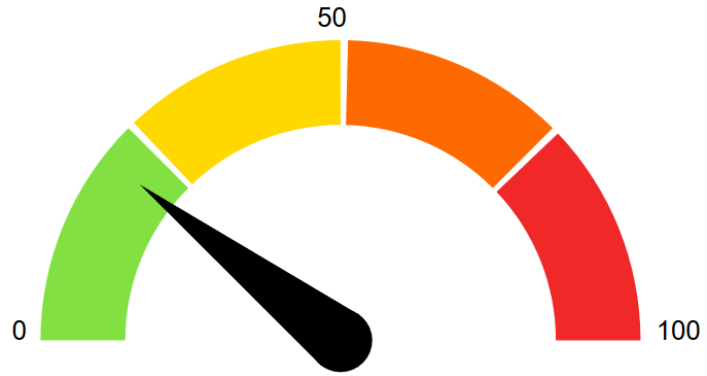


Domain Risk Level: 21 / 100



Angry Jean-Luc

4. Go back to Jean-Luc



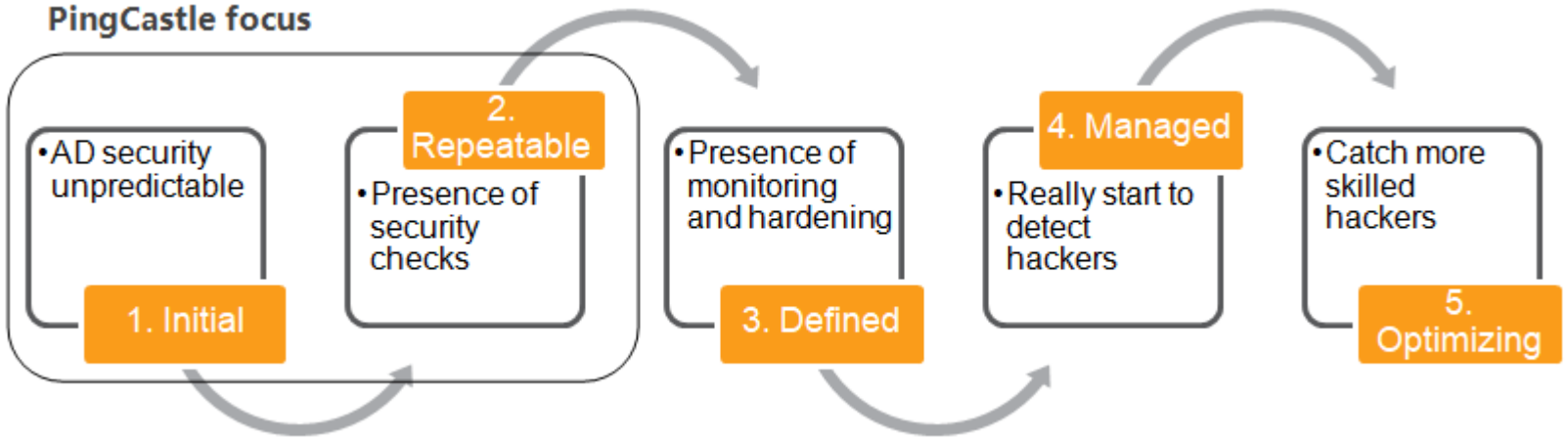
Domain Risk Level: 21 / 100

Thanks to Jean-Luc's decision:

- There is a NEW security indicator
- Jean-Luc can demonstrate to its management that the security subject is his own
- Jean-Luc can demonstrate measurable results … and get budget to get faster, or make its management accountable

This is called « maturity »

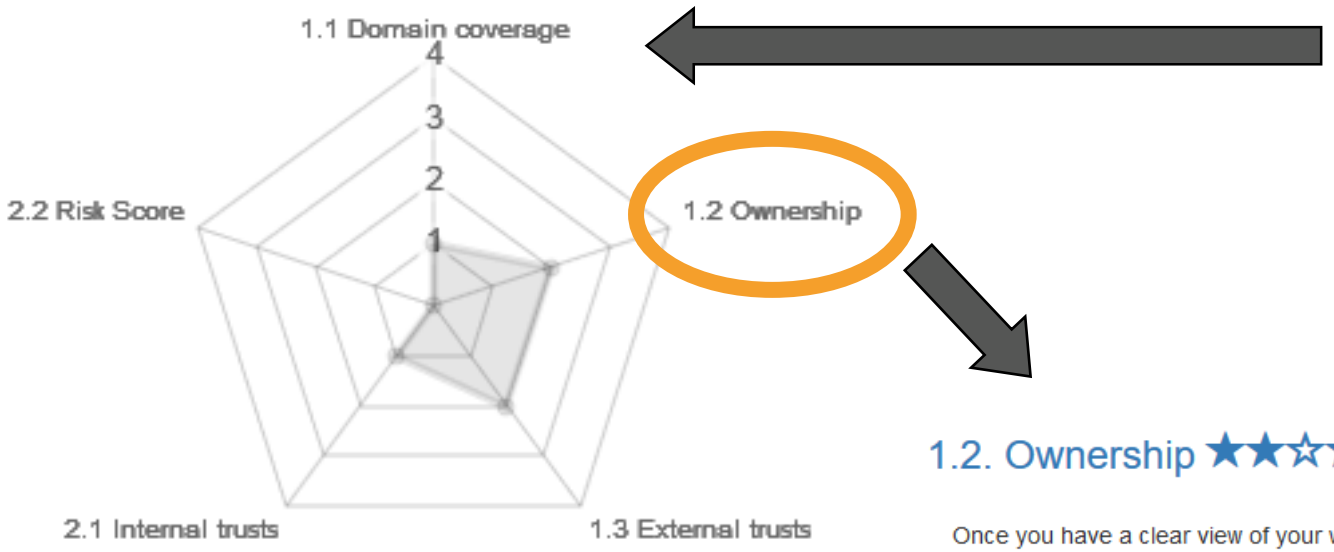
- Mix management & technical topics by calling « maturity »

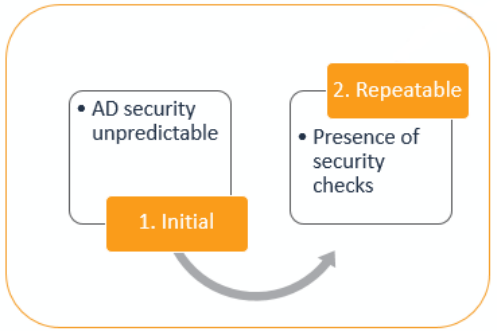


- Inspired from CMMI (from Carnegie Mellon which designed also CERT)

CMMI® Institute
AN ISACA ENTERPRISE

Full PingCastle methodology





Maturity Score: 6/20

1.2. Ownership ★★☆☆

Once you have a clear view of your whole perimeter, the best course of action to define clearly the ownership of each and every domains. It is critical that people actually feel included in the processes in order for the security to improve.
Click here to get more details

- [x] 1.2.1 Every domain has an identified owner
- [ ] 1.2.2 Every domain's owner is dully acknowledged
- [x] 1.2.3 There is less than 20% of domains set in derogation
- [ ] 1.2.4 There is no domain running a non supported functional level(Windows 2000, 2003, ...)

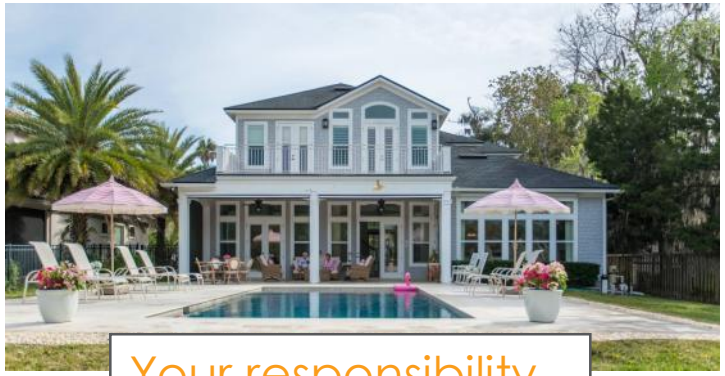
https://www.pingcastle.com/methodology/

CONCLUSION

PingCastle do not stop mimikatz

PingCastle's responsibility

- Vendors are selling big houses … without any foundation. As a consequence, it collapses. You got no mimikatz detection!
- PingCastle focuses on building the foundation. Then, it's up to you to build the mimikatz detection you want.



Your responsibility

- **No more excuse, just run PingCastle as Jean-Luc ordered**

https://www.pingcastle.com/download