



# Security Best Practices for On-Premise Environments

Online Beer-Talk

24.06.2021 17:00

[ville.koch@compass-security.com](mailto:ville.koch@compass-security.com)

<https://www.compass-security.com>  [@compasssecurity](https://twitter.com/compasssecurity)  [info@compass-security.com](mailto:info@compass-security.com)

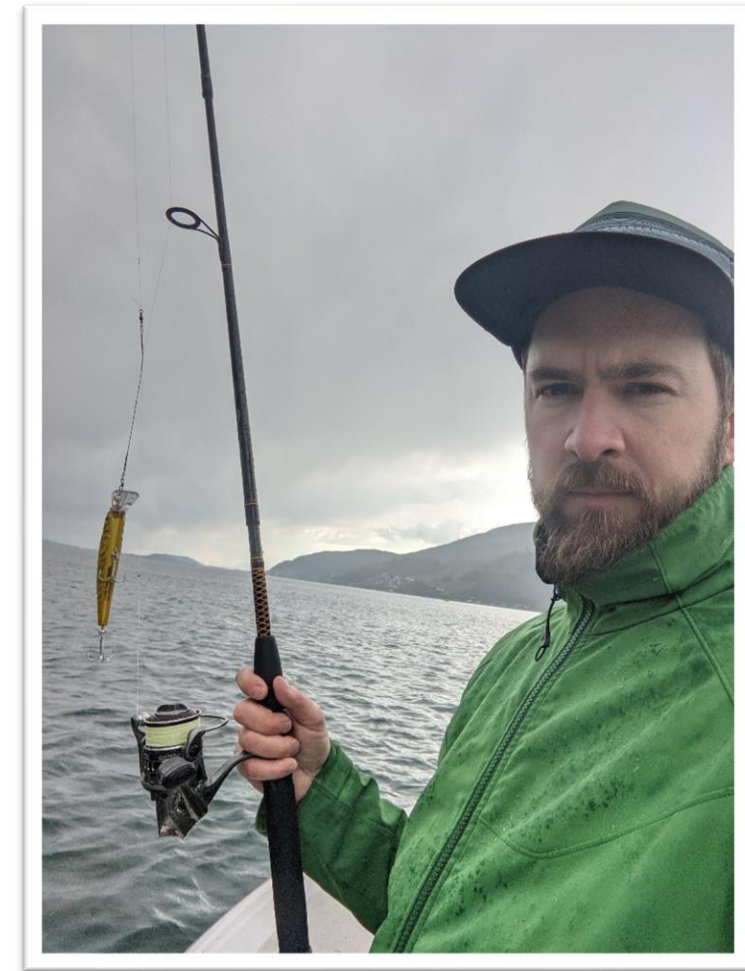
## \$ whoami

- Ville Koch (FIN / CH)
- 2003 – 2019: System Engineer @ Swiss Post / Swisscom
- 2018: CAS Cyber Security
- 2019 – now: IT-Security Analyst @ Compass Security
- Internal/External Pentests, Web Apps, Concept Reviews,...
- Besides hacking I like fishing, being in nature, travelling...

Email: [ville.koch@compass-security.com](mailto:ville.koch@compass-security.com)

Twitter: [@vegvisir87](https://twitter.com/vegvisir87)

LinkedIn: <http://www.linkedin.com/in/villekoch>



# Agenda

## Intro

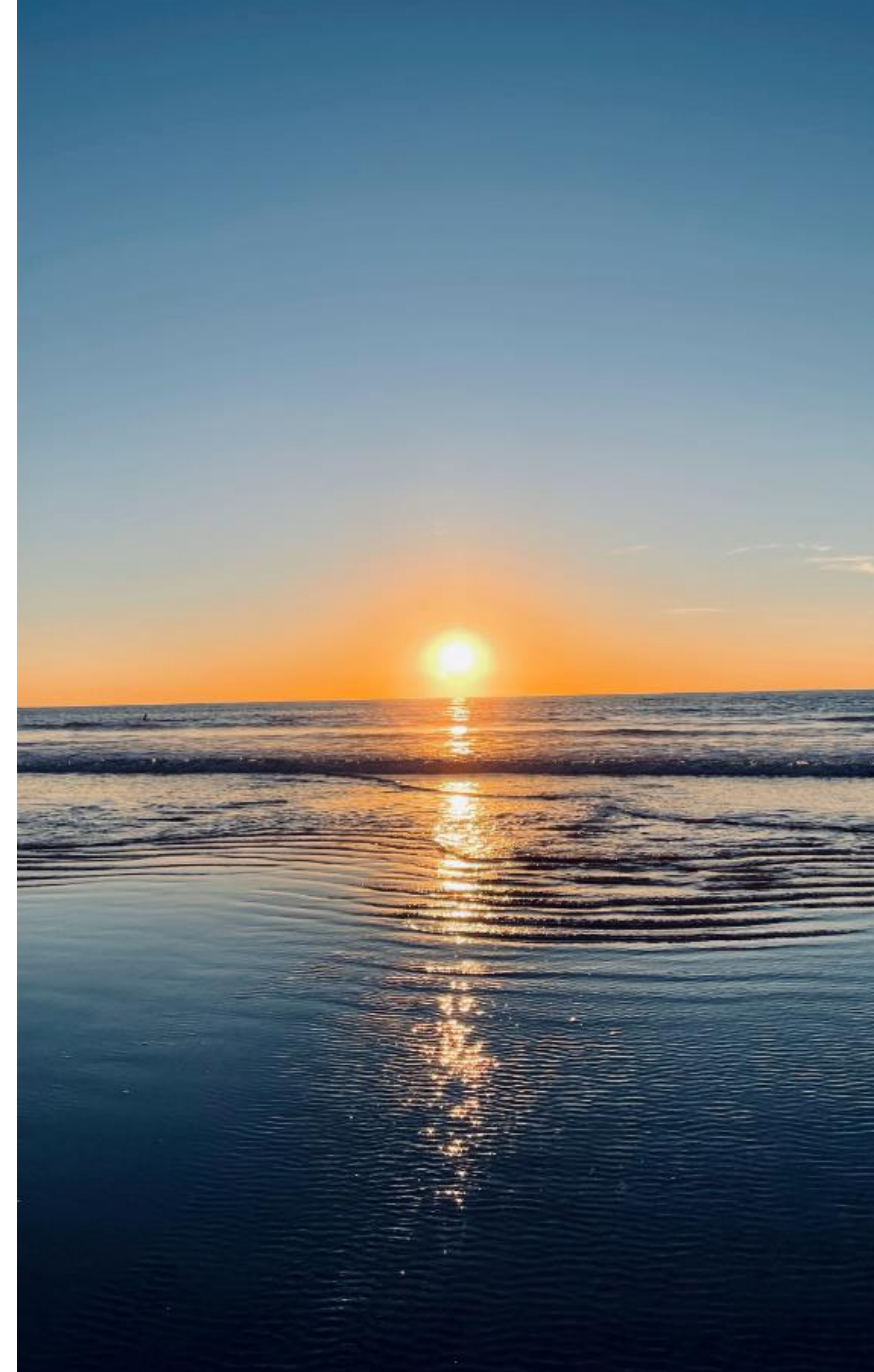
- Why this beertalk?
- Issues we find repeatedly

## The Security Best Practices

- Microsofts admin tier model
- Categorization of measures
- Our online guide

## End

- Tools for identification
- Questions



# Why this Beertalk?

- Same findings in many penetration tests
  - Documentation is endless and often complex
  - Smaller companies, less resources
  - Prioritization is difficult, without technical knowledge
- Research to provide guidance



# Issues we identify repeatedly...

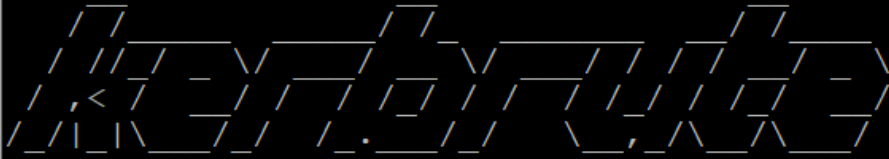


# Issues we identify repeatedly

## Bad Password Practices

→ Easy to guess passwords (initial passwords)

```
lab_admin@kali1:~/tools$ ./kerbrute passwordspray --dc 10.0.1.100 -d winattacklab.local userlist.txt Sommer2020
```



```
Version: v1.0.3 (9dad6e1) - 06/02/21 - Ronnie Flathers @ropnop
```

```
2021/06/02 05:02:47 > Using KDC(s):
2021/06/02 05:02:47 > 10.0.1.100:88
```

```
2021/06/02 05:02:47 > [+] VALID LOGIN: Hodor@winattacklab.local:Sommer2020
2021/06/02 05:02:47 > [+] VALID LOGIN: user03@winattacklab.local:Sommer2020
2021/06/02 05:02:47 > [+] VALID LOGIN: user04@winattacklab.local:Sommer2020
2021/06/02 05:02:47 > [+] VALID LOGIN: hans@winattacklab.local:Sommer2020
2021/06/02 05:02:47 > [+] VALID LOGIN: user01@winattacklab.local:Sommer2020
2021/06/02 05:02:47 > [+] VALID LOGIN: someone@winattacklab.local:Sommer2020
2021/06/02 05:02:47 > [+] VALID LOGIN: someoneelse@winattacklab.local:Sommer2020
2021/06/02 05:02:47 > [+] VALID LOGIN: frida@winattacklab.local:Sommer2020
2021/06/02 05:02:47 > [+] VALID LOGIN: jondoe@winattacklab.local:Sommer2020
2021/06/02 05:02:47 > [+] VALID LOGIN: user02@winattacklab.local:Sommer2020
2021/06/02 05:02:52 > Done! Tested 44 logins (10 successes) in 5.006 seconds
```

# Issues we identify repeatedly

## Bad Password Practices

→ Default passwords

The image shows two overlapping browser windows. The left window is CIRT.net, displaying a 'Default Password DB' section with a search form and a 'DOWNLOAD' button. The right window is Router Passwords, showing a search interface for 'F5 DEFAULT RO' with a table of results.

| Method   | SNMP      |
|----------|-----------|
| Password | comcomcom |
| Doc      |           |

| Manufacturer | Model     |
|--------------|-----------|
| F5           | BIGIP 540 |

The image shows a GitHub repository page for 'SecLists' by 'danielmiessler'. The repository contains a directory of password lists. A commit history table is visible, showing updates to various password lists.

| File Name                          | Commit Message  | Time Ago      |
|------------------------------------|---|---------------|
| db2-betterdefaultpasslist.txt      | standardize line endings  | 12 months ago |
| default-passwords.csv              | Update default-passwords.csv                                      | 15 days ago   |
| ftp-betterdefaultpasslist.txt      | strip trailing whitespace   | 12 months ago |
| mssql-betterdefaultpasslist.txt    | standardize line endings  | 12 months ago |
| mysql-betterdefaultpasslist.txt    | standardize line endings  | 12 months ago |
| oracle-betterdefaultpasslist.txt   | strip trailing whitespace   | 12 months ago |
| oracle-ebs-passwordlist.txt        | renamed files in Passwords/Default-Credentials for better parsing | 11 months ago |
| oracle-ebs-userlist.txt            | renamed files in Passwords/Default-Credentials for better parsing | 11 months ago |
| postgres-betterdefaultpasslist.txt | standardize line endings  | 12 months ago |
| scada-pass.csv                     | Fix #259 - Recover from bad merge                                 | 2 years ago   |
| ssh-betterdefaultpasslist.txt      | Update ssh-betterdefaultpasslist.txt                              | 5 months ago  |
| telnet-betterdefaultpasslist.txt   | Update telnet-betterdefaultpasslist.txt                           | 11 months ago |
| telnet-phenoelit.txt               | New Default Password List   | 2 years ago   |
| tomcat-betterdefaultpasslist.txt   | Create tomcat-betterdefaultpasslist.txt                           | 3 years ago   |
| vnc-betterdefaultpasslist.txt      | standardize line endings  | 12 months ago |
| windows-betterdefaultpasslist.txt  | strip trailing whitespace   | 12 months ago |

# Issues we identify repeatedly

## Bad Password Practices

→ Crackable passwords

```
C:\Users\lab_admin>net user camomilla 12345 /add /dom
The password does not meet the password policy require
history requirements.

More help is available by typing NET HELPMSG 2245.

C:\Users\lab_admin>net user camomilla Passw0rd123 /ad
The command completed successfully.
```

```
vkoch@cracker:~$ hashcat --attack-mode 0 --hash-type 1000 --optimized-kernel-enable hashes.txt
/srv/wordlists/uncompressed/kaonashi.txt --rules-file /srv/rules/kamaji34K.rule.txt

hashcat (v6.0.0-25-g15634059) starting...

CUDA API (CUDA 11.0)
=====
* Device #1: GeForce RTX 2070 SUPER, 7880/7982 MB, 40MCU
* Device #2: GeForce RTX 2070 SUPER, 7880/7982 MB, 40MCU
* Device #3: GeForce RTX 2070 SUPER, 7880/7982 MB, 40MCU
* Device #4: GeForce RTX 2070 SUPER, 7880/7982 MB, 40MCU

OpenCL API (OpenCL 1.2 CUDA 11.0.228) - Platform #1 [NVIDIA Corporation]
=====
* Device #5: GeForce RTX 2070 SUPER, skipped
* Device #6: GeForce RTX 2070 SUPER, skipped
* Device #7: GeForce RTX 2070 SUPER, skipped
* Device #8: GeForce RTX 2070 SUPER, skipped

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 27

Hashes: 2 digests; 2 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 34101

[ ... ]
Started: Wed Jun  2 09:22:55 2021
Stopped: Wed Jun  2 09:23:01 2021

077cccc23f8ab7031726a3b70c694a49:Passw0rd123
e19ccf75ee54e06b06a5907af13cef42:P@ssw0rd
```



# Issues we identify repeatedly

## Bad Password Practices

→ Passwords stored in plaintext

users - Notepad

```
File Edit Format View Help
logins for mgmt database:
admin
adgfs45654BDVGFDFG2222$
sa
9Zbgç45FvdJ$?a*vbhz

FTP service:
ftp01
Burp1sn0tB33f
```

Node Info

WINATTACKLAB.LOCAL

| Property     | Value |
|--------------|-------|
| Object Class | 0     |
| Object GUID  | 30    |
| Object Name  | ts    |
| Object Type  | 9     |
| Object ID    | 2     |
| Tree         |       |

S

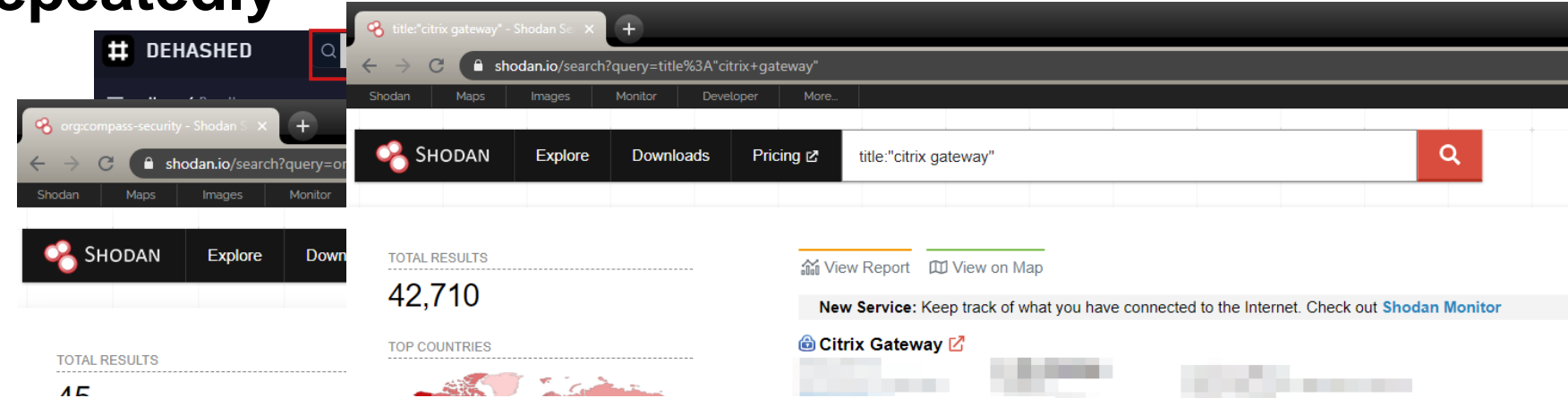
| Property                | Value  |
|-------------------------|--|
| Account Type            | Hales, Madison                                 |
| Account ID              | S-1-5-21-1051027935-4114171423-1363879386-1120 |
| Account Expiry          | Fri, 28 May 2021 10:32:07 GMT                  |
| Last Logon              | Never  |
| Last Logon (Replicated) | Never  |
| Enabled                 | True   |
| Email                   | mhales@winattacklab.local                      |
| Description             | password is SuperS3cret123                     |
| AdminCount              | False  |

MHALES@WINATTACKLAB.LOCAL Contains DOMAIN

# Issues we identify repeatedly

## Bad Password Practices

→ Password reuse



Cybersecurity

# Hackers Breached Colonial Pipeline Using Compromised Password

By [William Turton](#) and [Kartikay Mehrotra](#)

June 4, 2021, 9:58 PM GMT+2

<https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline>

- Breached password
- Reused for VPN account
- No MFA

|               |                         |     |
|---------------|-------------------------|-----|
| Apache httpd  | 8443                    | 269 |
| Postfix smtpd | 444                     | 235 |
| OpenSSH       | 4443                    | 120 |
|               | 9443                    | 76  |
|               | <a href="#">More...</a> |     |

| TOP ORGANIZATIONS                 |     |
|-----------------------------------|-----|
| Microsoft Corporation             | 889 |
| Comcast Cable Communications, LLC | 480 |
| Amazon Technologies Inc.          | 317 |
| Swisscom (Schweiz) AG             | 249 |

Organization:  
Sectigo Limited  
Issued To:  
Common Name:

# Issues we identify repeatedly

## Sensitive Data on shares

→ Open Shares

→ Files containing passwords

```
lab_admin@kali1:~$ crackmapexec smb 10.0.1.0/24 -u vmilton -p Passw0rd -d winattacklab.local --shares
SMB 10.0.1.10 445 Client1 [*] Windows 10.0 Build 18362 x64 (name:Client1) (domain:winattacklab.local)
SMB 10.0.1.100 445 DC1 [*] Windows 10.0 Build 17763 x64 (name:DC1) (domain:winattacklab.local)
SMB 10.0.1.10 445 Client1 [+] winattacklab.local\vmilton:Passw0rd (Pwn3d!)
SMB 10.0.1.100 445 DC1 [+] winattacklab.local\vmilton:Passw0rd (Pwn3d!)
SMB 10.0.1.10 445 Client1 [+! Enumerated shares
```

```
PS C:\Users\tmassie\Desktop> .\snaffler.exe -s -z .\default.toml
[Output of snaffler.exe showing ASCII art and version information]
```

by l0ss and Sh3r4 - [github.com/SnaffCon/Snaffler](https://github.com/SnaffCon/Snaffler)

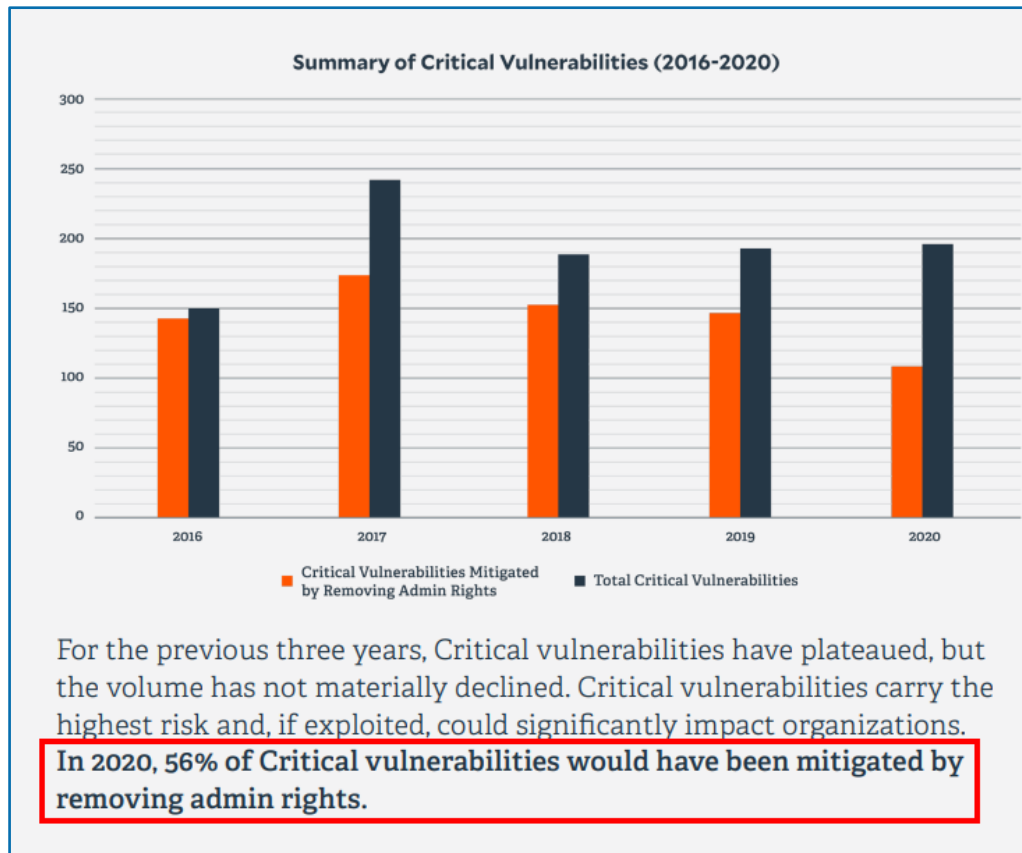


```
*ad_scanner [winattacklab\tmassie@Client1] 2021-06-03 06:08:20Z [Info] Parsing args...
File Edit Form [winattacklab\tmassie@Client1] 2021-06-03 06:08:20Z [Info] Read config file from .\default.toml
Computer [winattacklab\tmassie@Client1] 2021-06-03 06:08:20Z [Info] Parsed args successfully.
Client1.win [winattacklab\tmassie@Client1] 2021-06-03 06:08:20Z [Info] Getting users and computers from AD.
Client1.win [winattacklab\tmassie@Client1] 2021-06-03 06:08:20Z [Info] Got 3 computers from AD.
Client1.win [winattacklab\tmassie@Client1] 2021-06-03 06:08:20Z [Info] Starting to find readable shares.
Client1.win [winattacklab\tmassie@Client1] 2021-06-03 06:08:20Z [Info] Creating a sharefinder task for DC1.winattacklab.local
Client1.win [winattacklab\tmassie@Client1] 2021-06-03 06:08:20Z [Info] Creating a sharefinder task for Client1.winattacklab.local
Client1.win [winattacklab\tmassie@Client1] 2021-06-03 06:08:20Z [Info] Creating a sharefinder task for WS1.winattacklab.local
Client1.win [winattacklab\tmassie@Client1] 2021-06-03 06:08:20Z [Info] Created all sharefinder tasks.
WS1.winattac [winattacklab\tmassie@Client1] 2021-06-03 06:08:21Z [Share] {Black} \\Client1.winattacklab.local\ADMIN$
WS1.winattac [winattacklab\tmassie@Client1] 2021-06-03 06:08:21Z [Share] {Black} \\Client1.winattacklab.local\C$
WS1.winattac [winattacklab\tmassie@Client1] 2021-06-03 06:08:21Z [Share] {Green} \\Client1.winattacklab.local\D$
WS1.winattac [winattacklab\tmassie@Client1] 2021-06-03 06:08:21Z [Info] Creating a TreeWalker task for \\Client1.winattacklab.local\D$
DC1.winattac [winattacklab\tmassie@Client1] 2021-06-03 06:08:21Z [Share] {Green} \\Client1.winattacklab.local\share
DC1.winattac [winattacklab\tmassie@Client1] 2021-06-03 06:08:21Z [Info] Creating a TreeWalker task for \\Client1.winattacklab.local\share
DC1.winattac [winattacklab\tmassie@Client1] 2021-06-03 06:08:21Z [Share] {Green} \\WS1.winattacklab.local\Fileshare
DC1.winattac [winattacklab\tmassie@Client1] 2021-06-03 06:08:21Z [Info] Creating a TreeWalker task for \\WS1.winattacklab.local\Fileshare
DC1.winattac [winattacklab\tmassie@Client1] 2021-06-03 06:08:22Z [File] {Red} <KeepCmdRegExRed|RW|schtasks */[pff:space:1]*/[pff:space:1]}* [89B] 2021-06-03 05:58:09Z>\\WS1.winattacklab.local\Fileshare\IT\createtask.cmd) schtasks /create /xml update-hosts.xml /tn "update-hosts" /ru DOMAIN\User01 /rp Password1
DC1.winattac [winattacklab\tmassie@Client1] 2021-06-03 06:08:42Z [Share] {Green} \\DC1.winattacklab.local\NETLOGON
DC1.winattac [winattacklab\tmassie@Client1] 2021-06-03 06:08:42Z [Info] Creating a TreeWalker task for \\DC1.winattacklab.local\NETLOGON
DC1.winattac [winattacklab\tmassie@Client1] 2021-06-03 06:08:42Z [Share] {Green} \\DC1.winattacklab.local\SYSVOL
DC1.winattac [winattacklab\tmassie@Client1] 2021-06-03 06:08:42Z [Info] Creating a TreeWalker task for \\DC1.winattacklab.local\SYSVOL
t-ADAccountPassword [winattacklab\tmassie@Client1] 2021-06-03 06:08:42Z [File] {Red} <KeepPsRegExRed|R|-SecureString [121B] 2049-01-01 00:00:00Z>(\\DC1.winattacklab.local\NETLOGON\changeVMiltonPass.ps1) Set-ADAccountPassword -Identity vmilton -Reset -NewPassword (ConvertTo-SecureString -AsPlainText "RA3ehM1zxw!x1" -Force)
[winattacklab\tmassie@Client1] 2021-06-03 06:08:42Z [File] {Red} <KeepPsRegExRed|R|-SecureString [121B] 2049-01-01 00:00:00Z>(\\DC1.winattacklab.local\SYSVOL\winattacklab.local\scripts\changeVMiltonPass.ps1) Set-ADAccountPassword -Identity vmilton -Reset -NewPassword (ConvertTo-SecureString -AsPlainText "RA3ehM1zxw!x1" -Force)
[winattacklab\tmassie@Client1] 2021-06-03 06:08:50Z [Info] Status Update:
ShareFinder Tasks Completed: 0
ShareFinder Tasks Remaining: 3
ShareFinder Tasks Running: 3
```

# Issues we identify repeatedly

## Too many permissions

→ Local Administrators

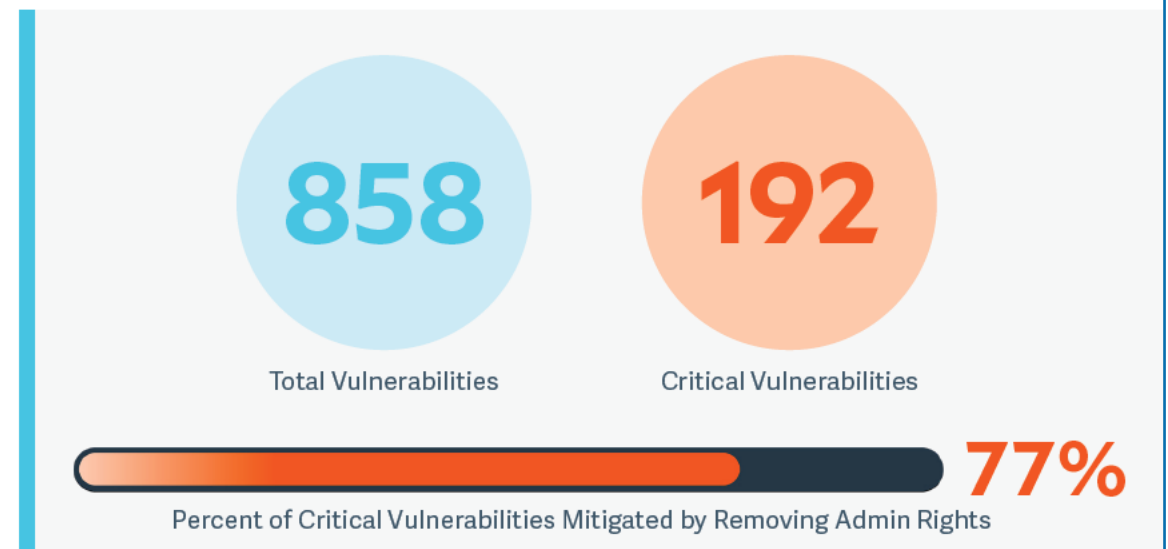


Source: BeyondTrust Microsoft Vulnerabilities Report 2021

### Executive Summary

Below are some of the key findings from this year's Microsoft Vulnerabilities Report, which analyzes all Patch Tuesday bulletins released throughout 2019.

- ▶ In 2019, a record high number of **858 Microsoft vulnerabilities** was discovered
- ▶ The number of reported vulnerabilities has **risen 64% in the last 5 years (2015-2019)**
- ▶ Removing admin rights would **mitigate 77% of all Critical Microsoft vulnerabilities** in 2019
- ▶ **100% of Critical vulnerabilities** in Internet Explorer & Edge would have been mitigated by removing admin rights
- ▶ **80% of Critical vulnerabilities** affecting Windows 7, 8.1 and 10 would have been mitigated by removing of admin rights

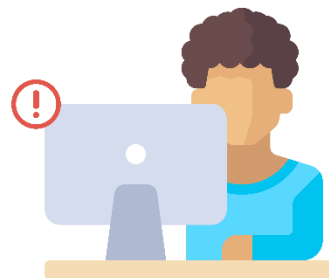


Source: BeyondTrust Microsoft Vulnerabilities Report 2020

# Issues we identify repeatedly

## Too many permissions

→ Local Administrators



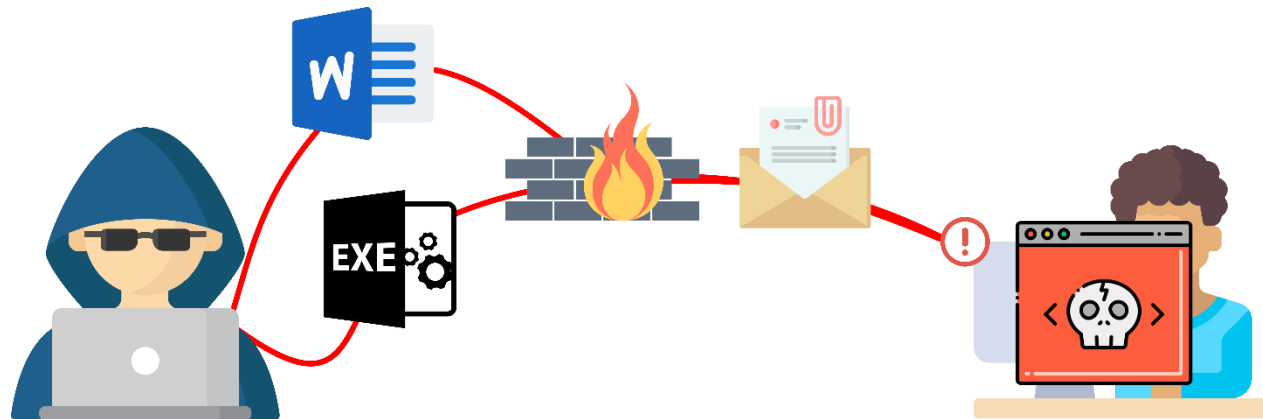
User Jesús (who is local admin) opens malicious attachment in email



# Issues we identify repeatedly

## Too many permissions

→ Local Administrators



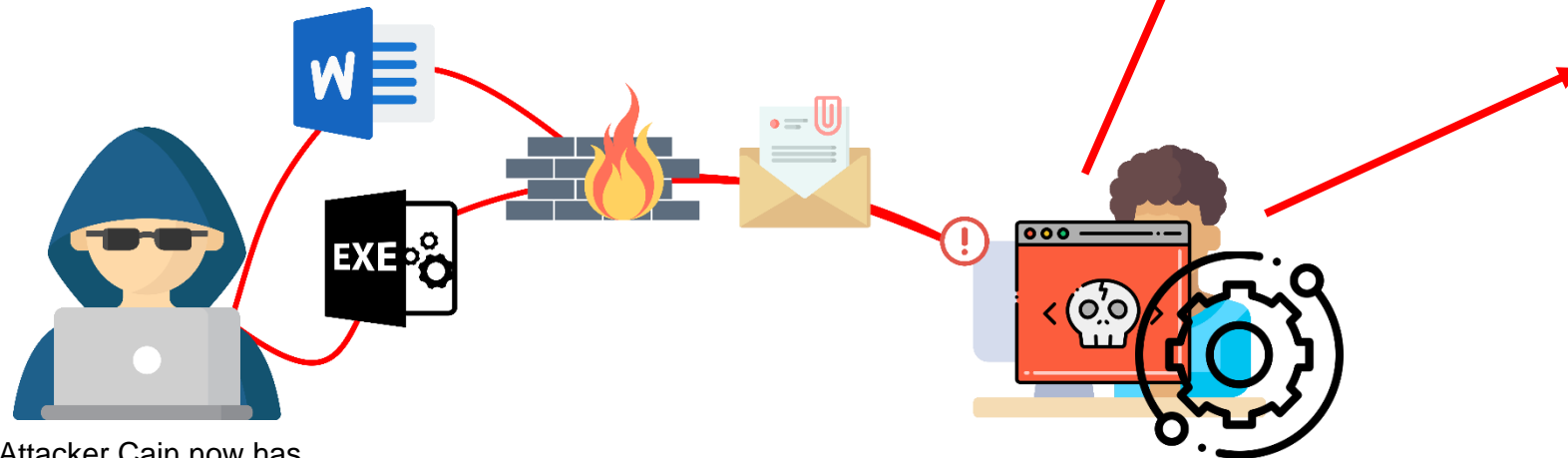
Attacker Cain now has a remote session on Jesús' machine with admin privileges

User Jesús (who is local admin) opens malicious attachment in email

# Issues we identify repeatedly

## Too many permissions

→ Local Administrators



Attacker Cain now has a remote session on Jesús' machine with admin privileges

Install persistence (Windows Service, Scheduled Task, Startup etc.)

Extract credentials of locally logged in users

```
PS C:\Users\tmassie\mimikatz_trunk\x64> .\mimikatz.exe

.#####.   mimikatz 2.2.0 (x64) #19041 May 31 2021 00:08:47
.## ^ ##.   "A La Vie, A L'Amour" - (oe.eo)
## / \ ##   /** Benjamin DELPY `gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ##   > https://blog.gentilkiwi.com/mimikatz
'## v #'    Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'    > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 49839303 (00000000:02f87cc7)
Session           : Interactive from 4
User Name         : vmilton
Domain           : winattacklab
Logon Server      : DC1
Logon Time        : 6/3/2021 9:32:05 AM
SID               : S-1-5-21-1051027935-4114171423-1363879386-1128

msv :
[00000003] Primary
* Username : vmilton
* Domain   : winattacklab
* NTLM     : a87f3a337d73085c45f9416be5787d86
* SHA1     : 34957e9ba3455a4a99d722b48693ac1123ba5dba
* DPAPI    : f2ffe7eb48e9cecb94d245991ed06a29

tspkg :
wdigest :
* Username : vmilton
* Domain   : winattacklab
* Password : (null)

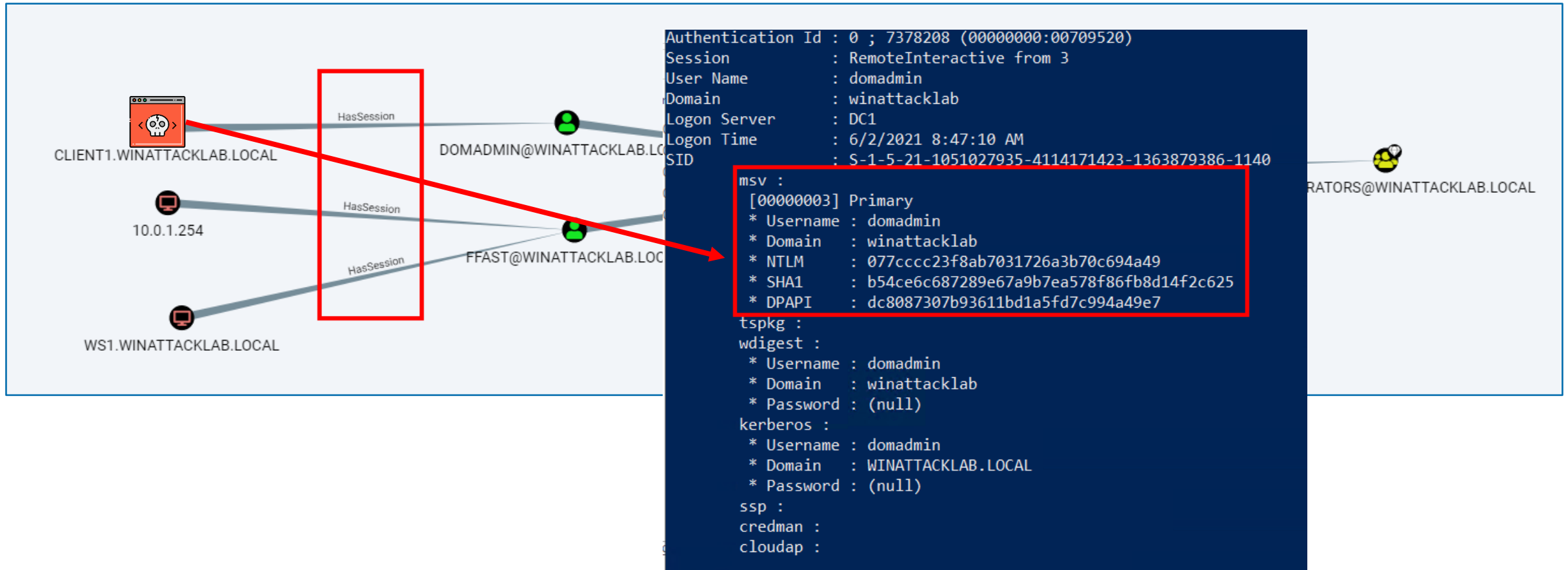
kerberos :
* Username : vmilton
* Domain   : WINATTACKLAB.LOCAL
* Password : (null)

ssp :
credman :
cloudap :
```

# Issues we identify repeatedly

## Too many permissions

→ Domain Administrators (sessions on workstations/servers)

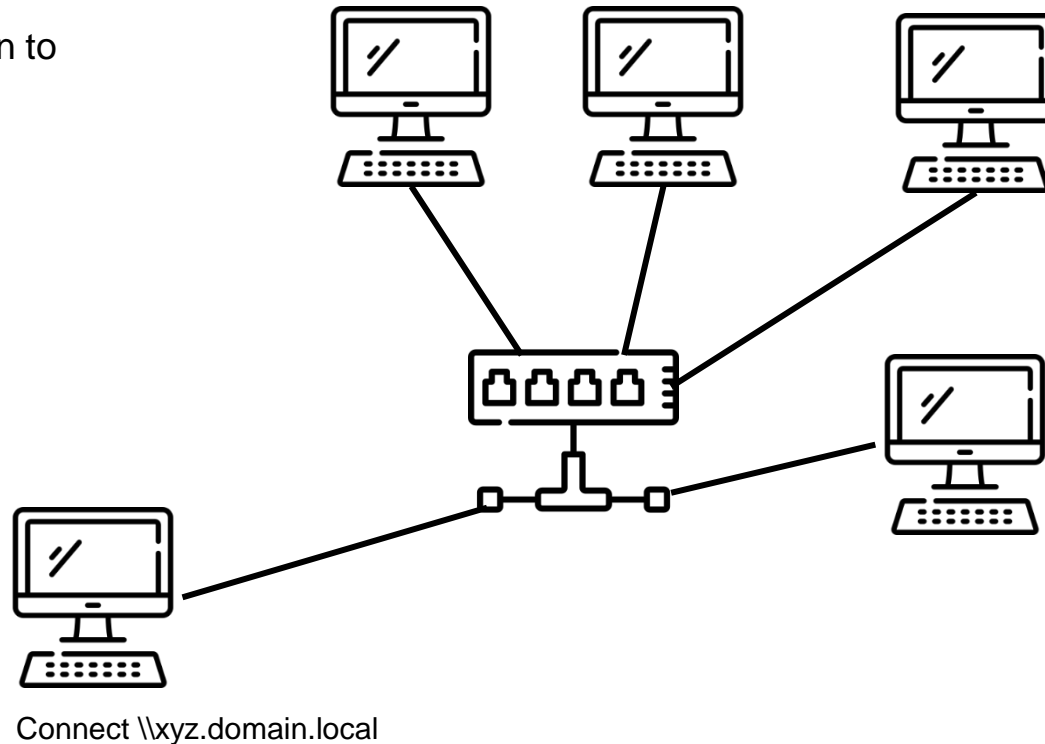


# Issues we identify repeatedly

## Too many permissions

→ Domain Administrators (authenticated network connections)

- Computer makes connection to [\\xyz.domain.local](#)

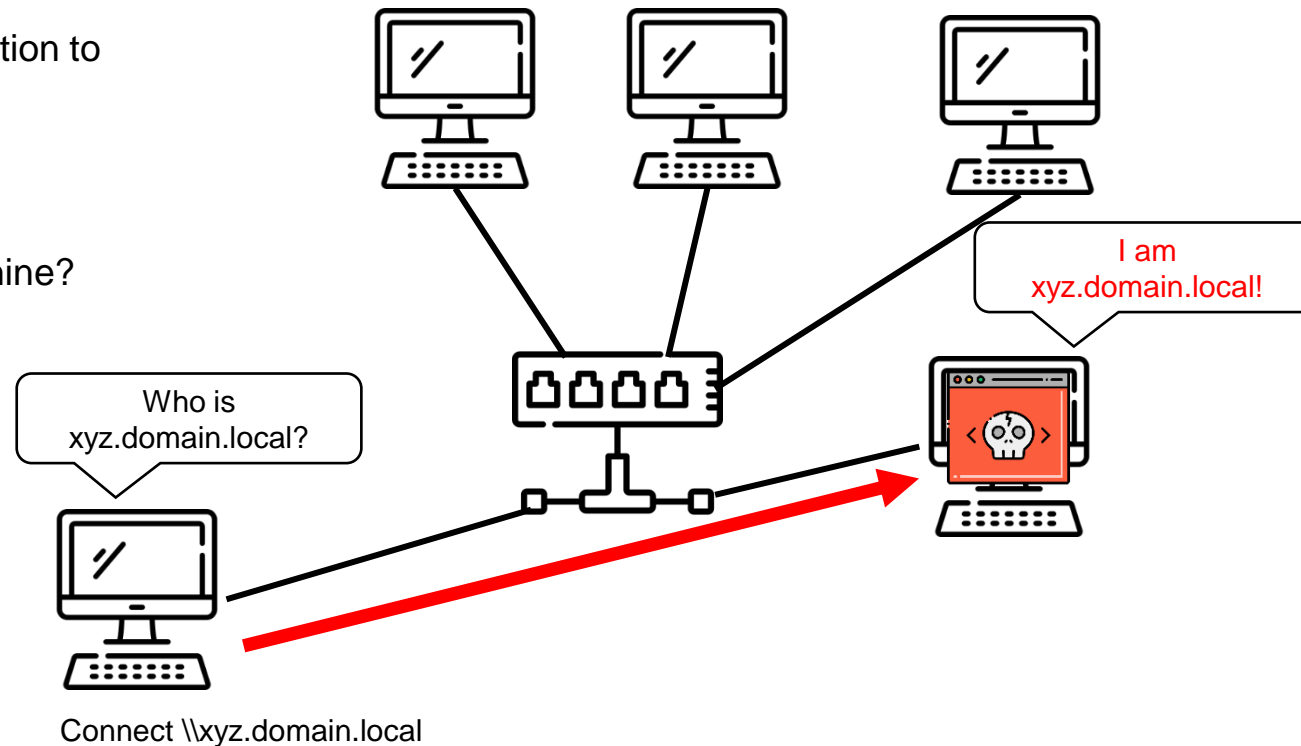


# Issues we identify repeatedly

## Too many permissions

→ Domain Administrators (authenticated network connections)

- Computer makes connection to \\xyz.domain.local
- Name resolution of xyz:
  - a. Is this the local machine?
  - b. Check local cache
  - c. Local hosts file
  - d. Query DNS server
  - e. LLMNR broadcast\*
  - f. NetBIOS broadcast\*



\* Same subnet



# Issues we identify repeatedly

## Too many permissions

→ Domain Administrators (authenticated network connections)

- Attacker can capture network traffic (broadcast!)

```
lab_admin@kali1:~$ sudo /usr/share/responder/Responder.py -I eth0 -w -r -f -d

-----
|       |       |       |       |       |       |
|       |       |       |       |       |       |
|       |       |       |       |       |       |
|       |       |       |       |       |       |
|       |       |       |       |       |       |
-----

      NBT-NS, LLMNR & MDNS Responder 3.0.6.0

Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CTRL-C

[+] Poisoners:
    LLMNR                    [ON]
    NBT-NS                   [ON]
    DNS/MDNS                 [ON]

[+] Servers:
    HTTP server              [ON]
```

```
*** Error starting responder on port 55, check permissions of other servers running.
[+] Listening for events...
[*] [MDNS] Poisoned answer sent to 10.6.207.71 for name networkshare123.local
[*] [MDNS] Poisoned answer sent to 10.6.207.71 for name networkshare123.local
[*] [MDNS] Poisoned answer sent to 10.6.207.71 for name networkshare123.local
[*] [MDNS] Poisoned answer sent to 10.6.207.71 for name networkshare123.local[*] [MDNS] Poisoned answer sent to 10.6.207.71 for name networkshare123.local
[*] [MDNS] Poisoned answer sent to 10.6.207.71 for name networkshare123.local
```

```
FTP server [ON]
```

```
[+] Listening for events...
[SMB] NTLMv2-SSP Client : 10.0.1.10
[SMB] NTLMv2-SSP Username : winattacklab\domadmin
[SMB] NTLMv2-SSP Hash : domadmin::winattacklab:7e2d762c59f56218:07B0749619B38BBC4C5AD12F94E5198E:010100000000000008007D6F73C00000000020008004A0045005300560001001E00570049004E002D005A003200480044004300440046004B004B004100320004003400570049004E002D005A006004B004B00410032002E004A004500530056002E004C004F00430041004C00030014004A004500530056002E004C004F00430041004C00050014004A0045000041004C000700080008007D6F73C58D7010600040002000000080030003000000000000000100000000200000D9319DF3904A0BBEFA357499603B1F58BF9E1B6AF60A0010000000000000000000000000000009001C0063006900660073002F00310030002E0030002E0031002E00310035000000000000000000
```

# Side Note about Windows and Broadcast...

- Using search bar in Windows → Broadcast!

The screenshot shows a Windows search interface with the search bar containing '\\something'. The search results show a 'Best match' for '\\something' with a 'Run command' option. A red arrow points from the search bar to a terminal window. The terminal window displays the following output:

```
[+] Listening for events...
[*] [MDNS] Poisoned answer sent to 10.6.207.71 for name s.local
[*] [MDNS] Poisoned answer sent to 10.6.207.71 for name s.local
[*] [MDNS] Poisoned answer sent to 10.6.207.71 for name so.local
[*] [MDNS] Poisoned answer sent to 10.6.207.71 for name so.local
[*] [MDNS] Poisoned answer sent to 10.6.207.71 for name som.local
[*] [MDNS] Poisoned answer sent to 10.6.207.71 for name som.local
[*] [MDNS] Poisoned answer sent to 10.6.207.71 for name some.local
[*] [MDNS] Poisoned answer sent to 10.6.207.71 for name some.local
[*] [MDNS] Poisoned answer sent to 10.6.207.71 for name somet.local
[*] [MDNS] Poisoned answer sent to 10.6.207.71 for name somet.local
[*] [MDNS] Poisoned answer sent to 10.6.207.71 for name someth.local
[*] [MDNS] Poisoned answer sent to 10.6.207.71 for name someth.local
[*] [MDNS] Poisoned answer sent to 10.6.207.71 for name somethi.local
[*] [MDNS] Poisoned answer sent to 10.6.207.71 for name somethi.local
[*] [MDNS] Poisoned answer sent to 10.6.207.71 for name somethin.local
[*] [MDNS] Poisoned answer sent to 10.6.207.71 for name somethin.local
[*] [MDNS] Poisoned answer sent to 10.6.207.71 for name something.local
[*] [MDNS] Poisoned answer sent to 10.6.207.71 for name something.local
[*] [MDNS] Poisoned answer sent to 10.6.207.71 for name somethi.local
[*] [MDNS] Poisoned answer sent to 10.6.207.71 for name somethi.local
[*] [MDNS] Poisoned answer sent to 10.6.207.71 for name somethi.local
[*] [MDNS] Poisoned answer sent to 10.6.207.71 for name somethi.local
[*] [MDNS] Poisoned answer sent to 10.6.207.71 for name somethin.local
[*] [MDNS] Poisoned answer sent to 10.6.207.71 for name somethin.local
[*] [MDNS] Poisoned answer sent to 10.6.207.71 for name somethin.local
[*] [MDNS] Poisoned answer sent to 10.6.207.71 for name somethin.local
[*] [MDNS] Poisoned answer sent to 10.6.207.71 for name something.local
[*] [MDNS] Poisoned answer sent to 10.6.207.71 for name something.local
[*] [MDNS] Poisoned answer sent to 10.6.207.71 for name something.local
[*] [MDNS] Poisoned answer sent to 10.6.207.71 for name something.local
```

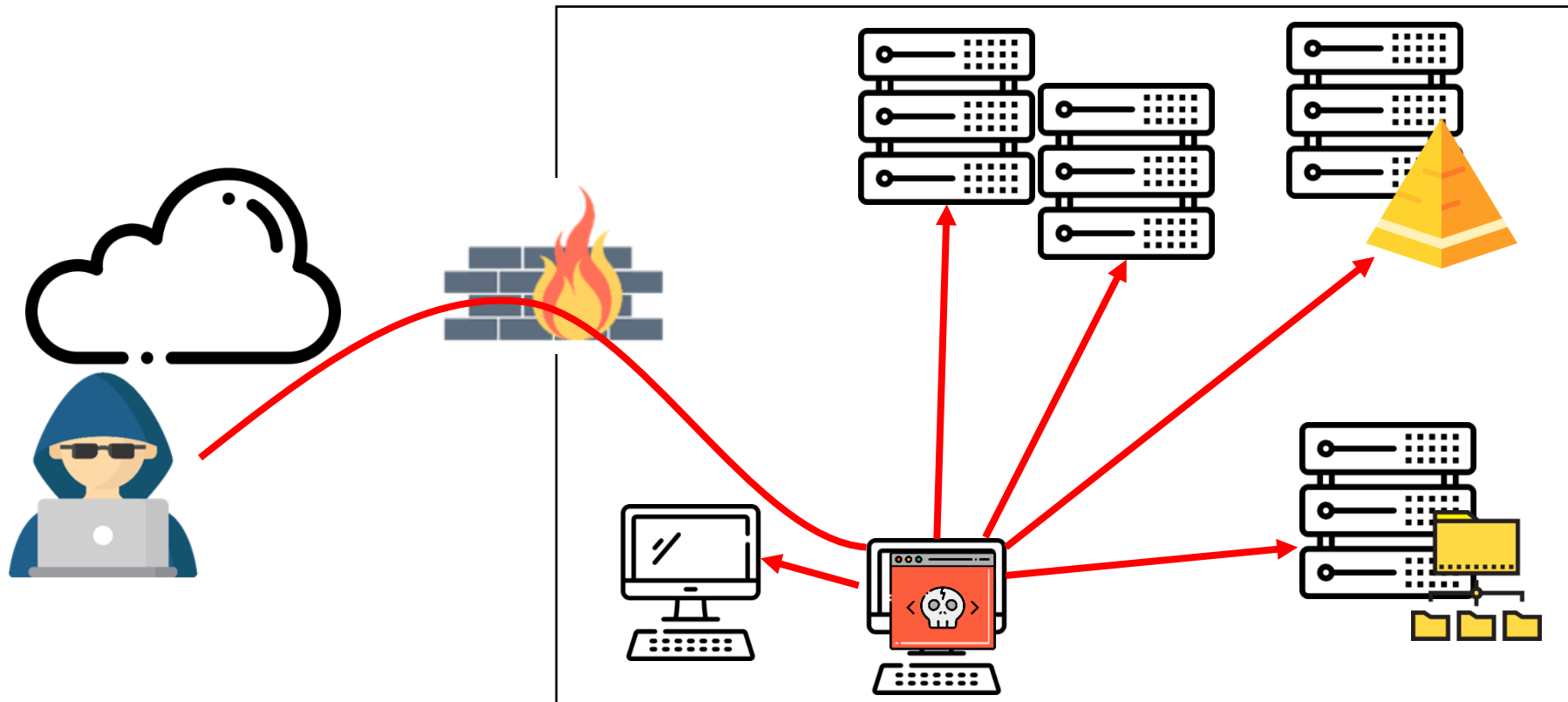
**Responder**  
@PythonResponder

Windows Server 2022, another most secure release.  
Thank you for sponsoring Responder @msftsecurity ! :)

Responder on Windows 2022 Preview.  
Same old as usual :)  
[youtube.com](#)

# Issues we identify repeatedly

## Missing Network Segregation



- Passwords (Login Interfaces)
- Sensitive Data (Shares, Databases etc.)
- Privileged Sessions ...

# Issues we identify repeatedly

Outdated (Vulnerable) Software

**Hackers are exploiting vulnerable Exchange servers to drop ransomware, Microsoft says**

Zack Whittaker @zackwhittaker / 9:11 PM GMT+1 • March 12, 2021

**Bank Hackers Exploit Outdated Router to Steal \$1 Million**

PIR Bank Robbed by Russia's MoneyTaker Gang, Investigators Say

Mathew J. Schwartz (euroinfosec) · July 20, 2018

**Outdated computer system exploited in Florida water treatment plant hack**

*Investigators are still trying to determine who's behind the hack.*

**WannaCry Ransomware Targeted Outdated HIT Infrastructure**

WannaCry ransomware attack exploited vulnerabilities in outdated health IT infrastructure systems, infiltrating networks around the world.

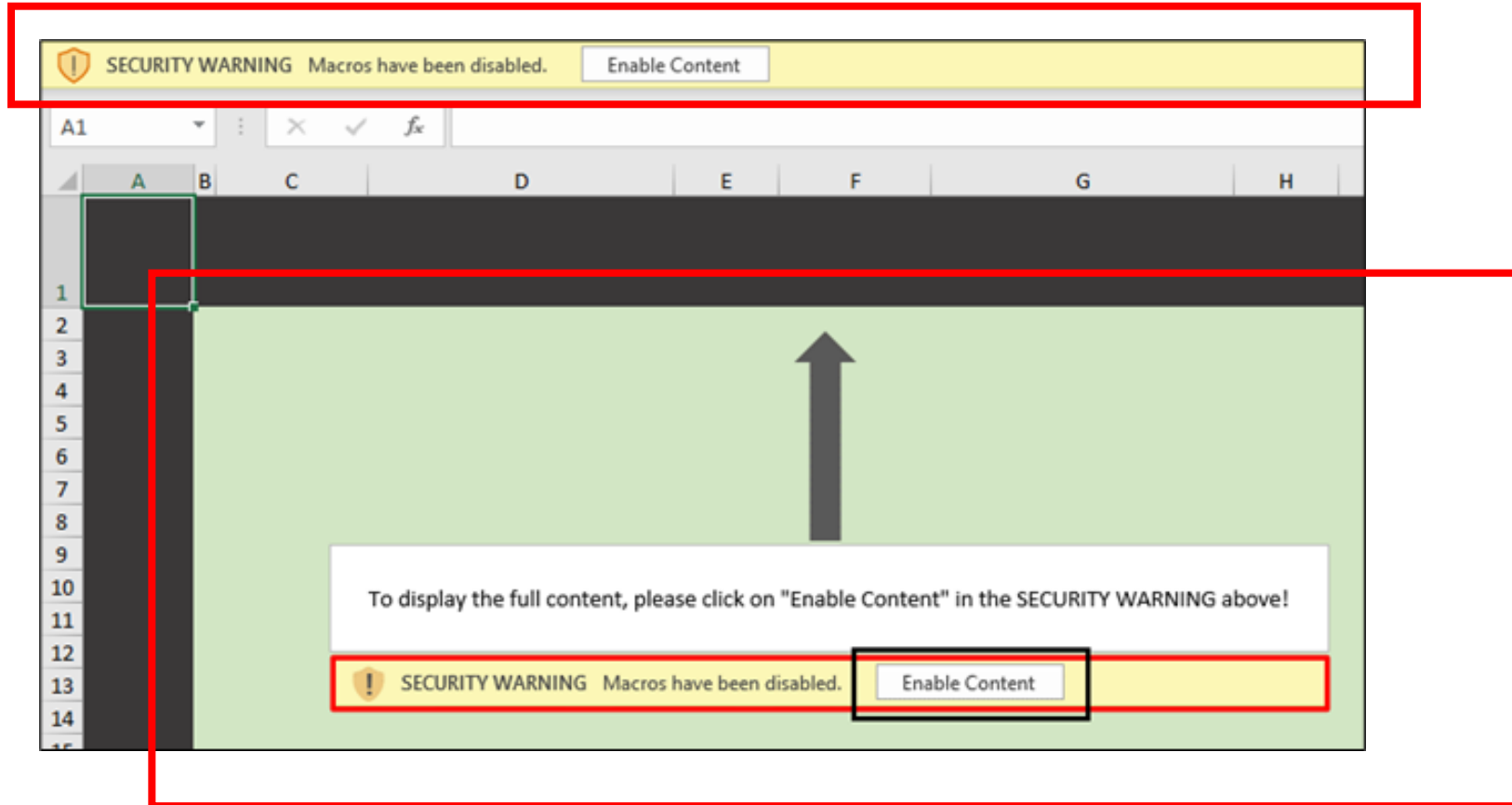


**At Least 30,000 U.S. Organizations Newly Hacked Via Holes in Microsoft's Email Software**

# Issues we identify repeatedly

## Missing Hardening

→ Default macro settings (prompt)



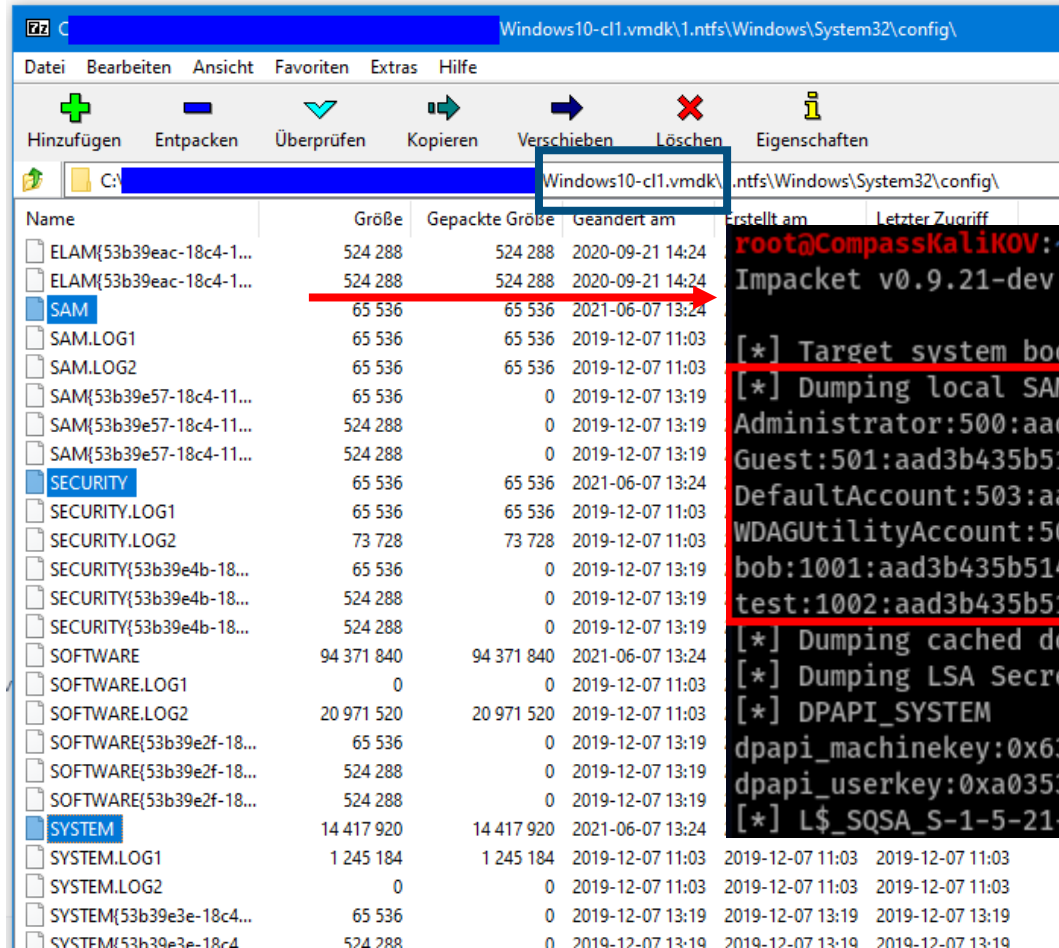
This is often used in social engineering attacks



# Issues we identify repeatedly

## Missing Hardening

→ No harddisk encryption



e. g. VMDK file found on share

```
root@CompassKalikov:~/Desktop/sam# secretsdump.py -sam SAM -system SYSTEM -security SECURITY LOCAL
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

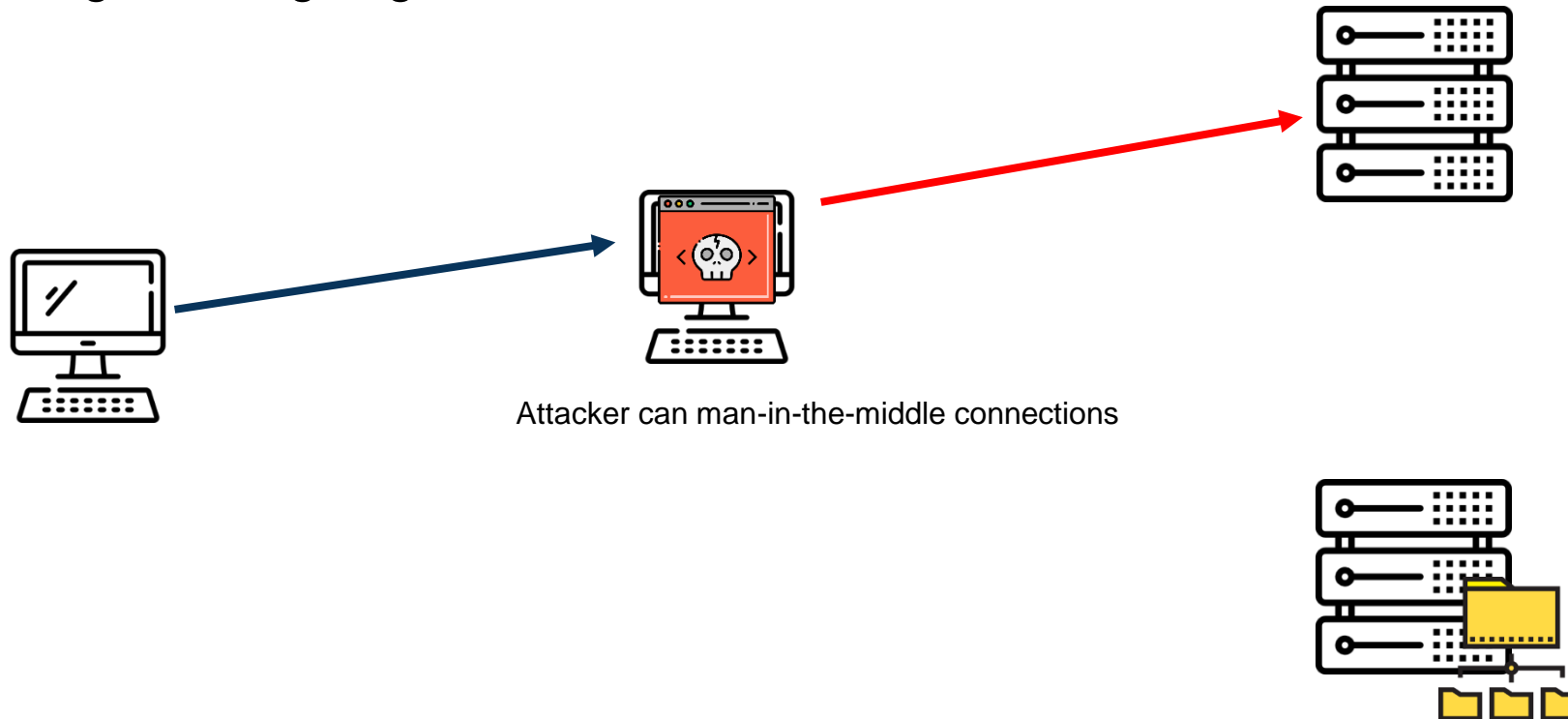
[*] Target system bootKey: 0x58340cf5f687864946375edcab5e5277
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:8c3...c:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:ba375de1814df6c2ce9dad5e39c38063:::
bob:1001:aad3b435b51404eeaad3b435b51404ee:e19...cef42:::
test:1002:aad3b435b51404eeaad3b435b51404ee:32e...818d4:::

[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] DPAPI_SYSTEM
dpapi_machinekey:0x6326c4529b96be82abfb879597da2e3df1e22945
dpapi_userkey:0xa0353497fdf4d4711bc99642ba43f21b4364ca6f
[*] L$SQSA_S-1-5-21-3625891453-2443669919-1211190329-1001
```

# Issues we identify repeatedly

## Missing Hardening

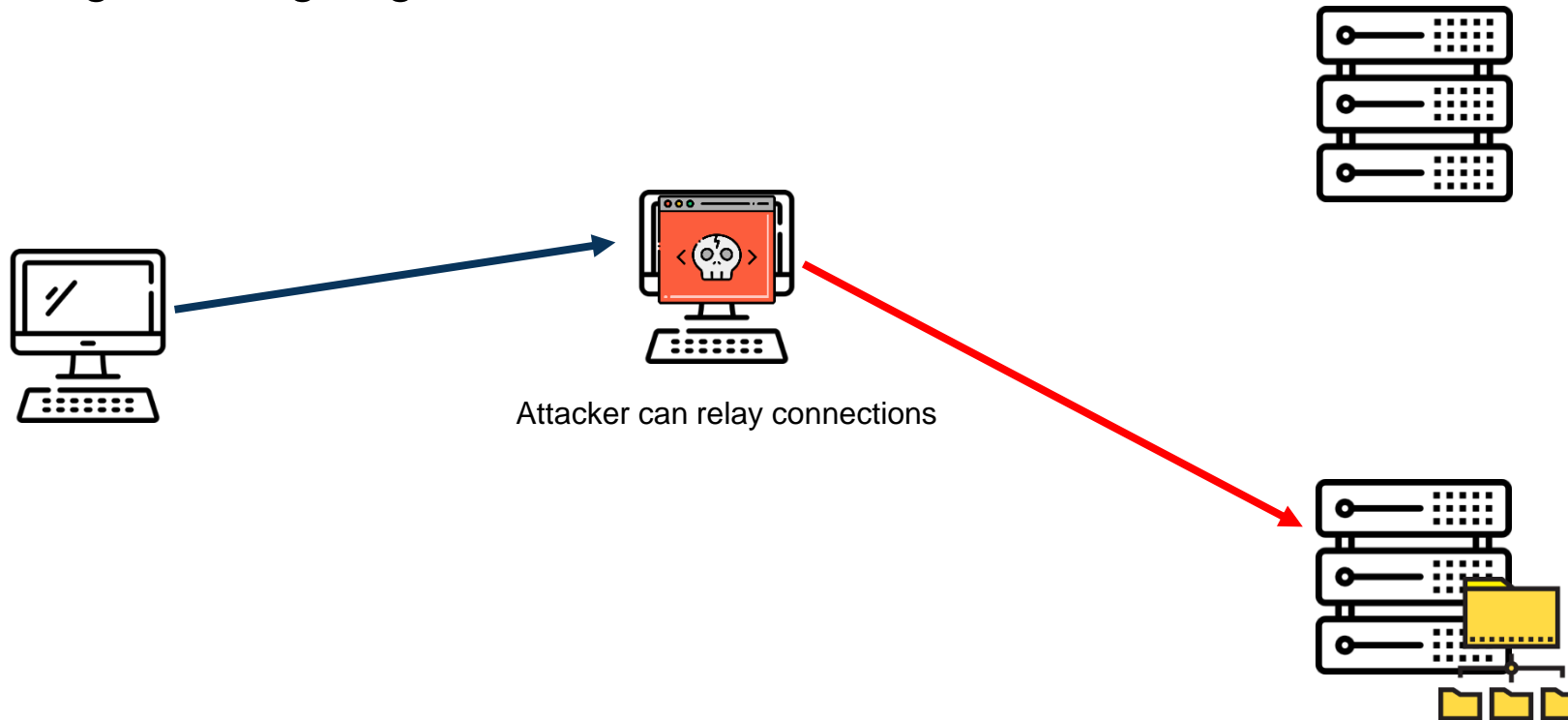
→ Missing SMB signing



# Issues we identify repeatedly

## Missing Hardening

→ Missing SMB signing





# The Security Best Practices





# Microsoft Admin Tier Model

## Tier 0:

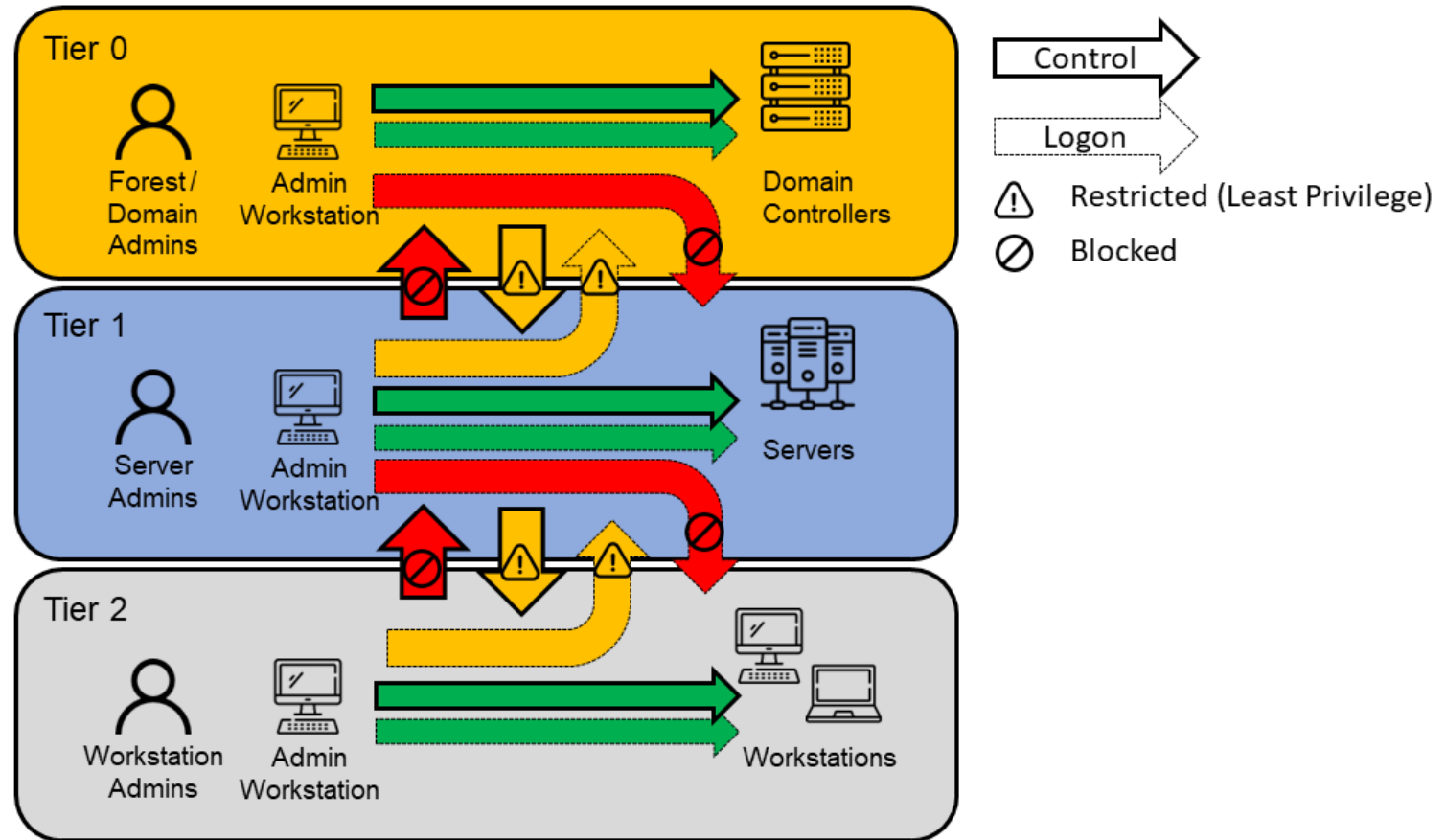
- Domain Admins

## Tier 1:

- Sensitive Business Data

## Tier 2:

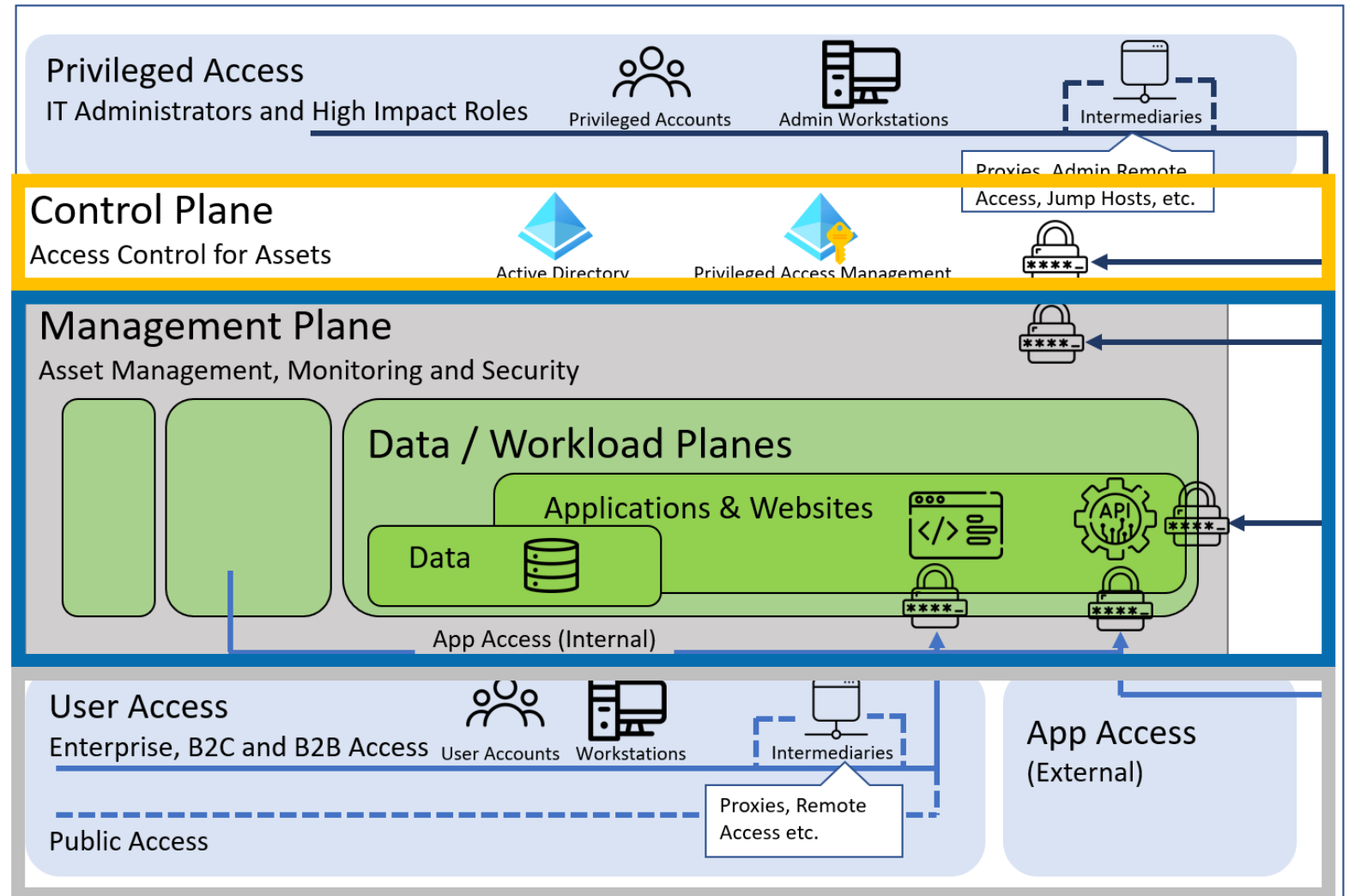
- End Users & Workstations



# Evolution from the legacy AD tier model...

## Enterprise access model

- Includes cloud architectures
- Zero-Trust approach



- <https://docs.microsoft.com/en-us/security/compass/privileged-access-access-model>

# Categorization of Measures

- Measures were categorized based on how they have to be addressed
  - **Organizational Measures:** Defining processes, training of employees etc.
  - **Configurational Measures:** Settings which have to be configured on workstations and servers.
  - **Account & Privilege Management Measures:** Creating of accounts and allocation of permissions.
  - **Password Management Measures:** Defining and enforcing of strong password policies.
  - **Network Measures:** Segregation of network, use of firewalls, etc.

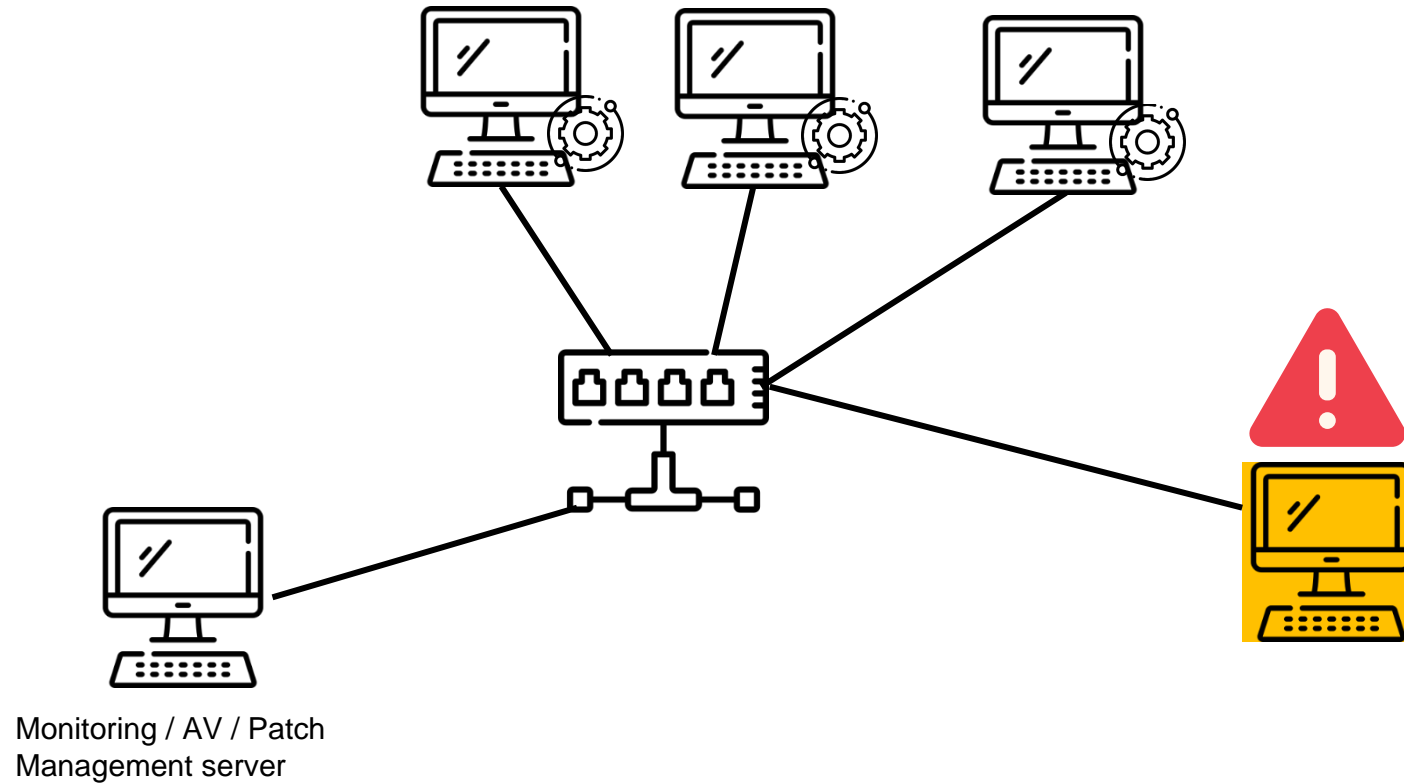


**Let's have a look at some measures...**

# Some Organizational Measures...

## Hardware & Software Inventory

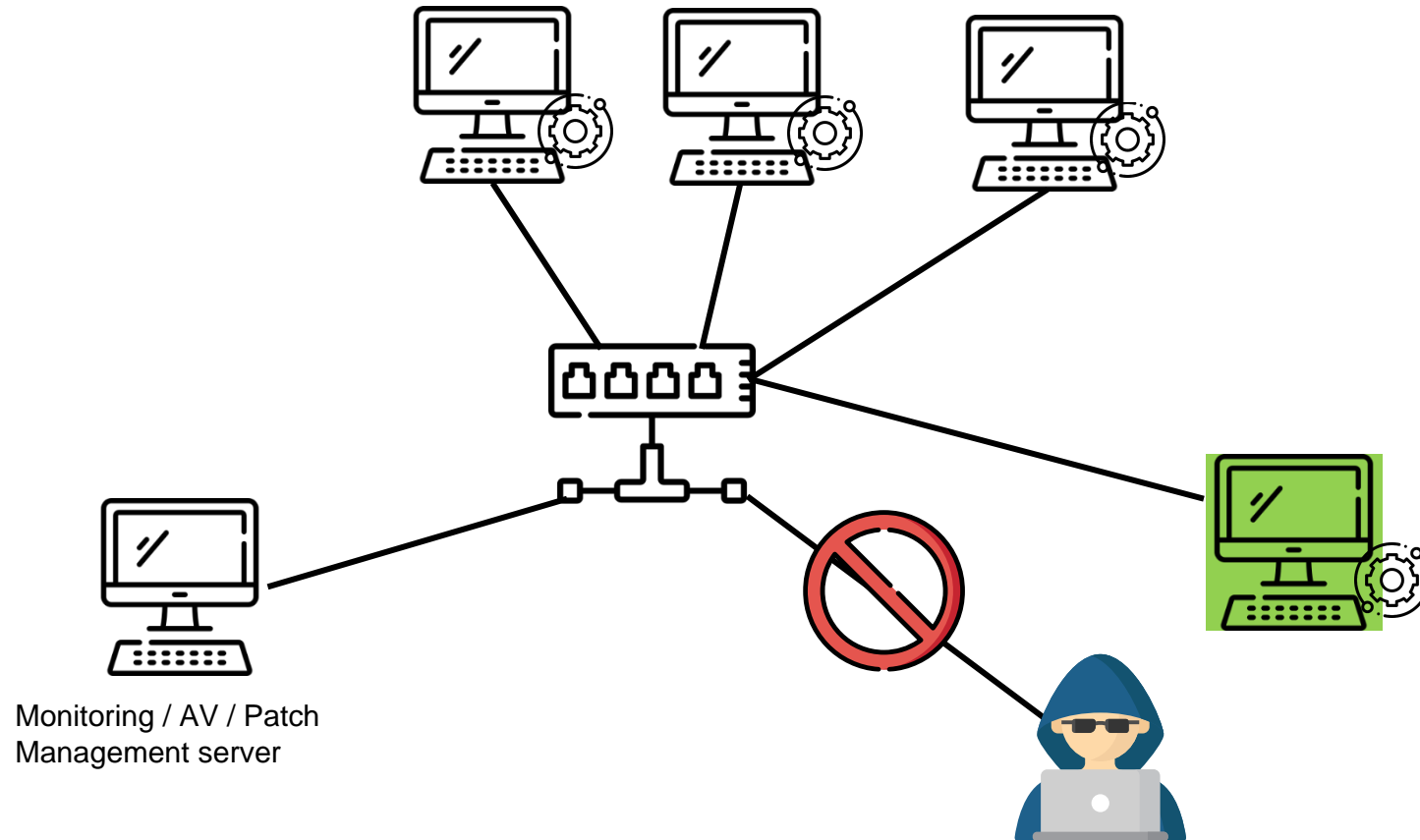
- Know your systems and their software (versions)
- Identify rogue systems



# Some Organizational Measures...

## Hardware & Software Inventory

- Know your systems and their software (versions)
- Identify rogue systems



# Some Organizational Measures...

## Offline / Off-Site Backups

- Define data and infrastructure and define retention period
- Store backups in a storage secured from unauthorized access
- Store backups encrypted
- Perform off-site backups (Disaster recovery)
- **Store backups offline, completely disconnected from any device**
- Use a separate backup infrastructure (e.g. Windows Server Backup) to perform backups of Domain Controllers (Tier-0 separation)

But the backups are only accessible through the backup console and access to the console is restricted!



Bob, Backup Admin

**Assume breach of your backup infrastructure!**

# Some Organizational Measures...

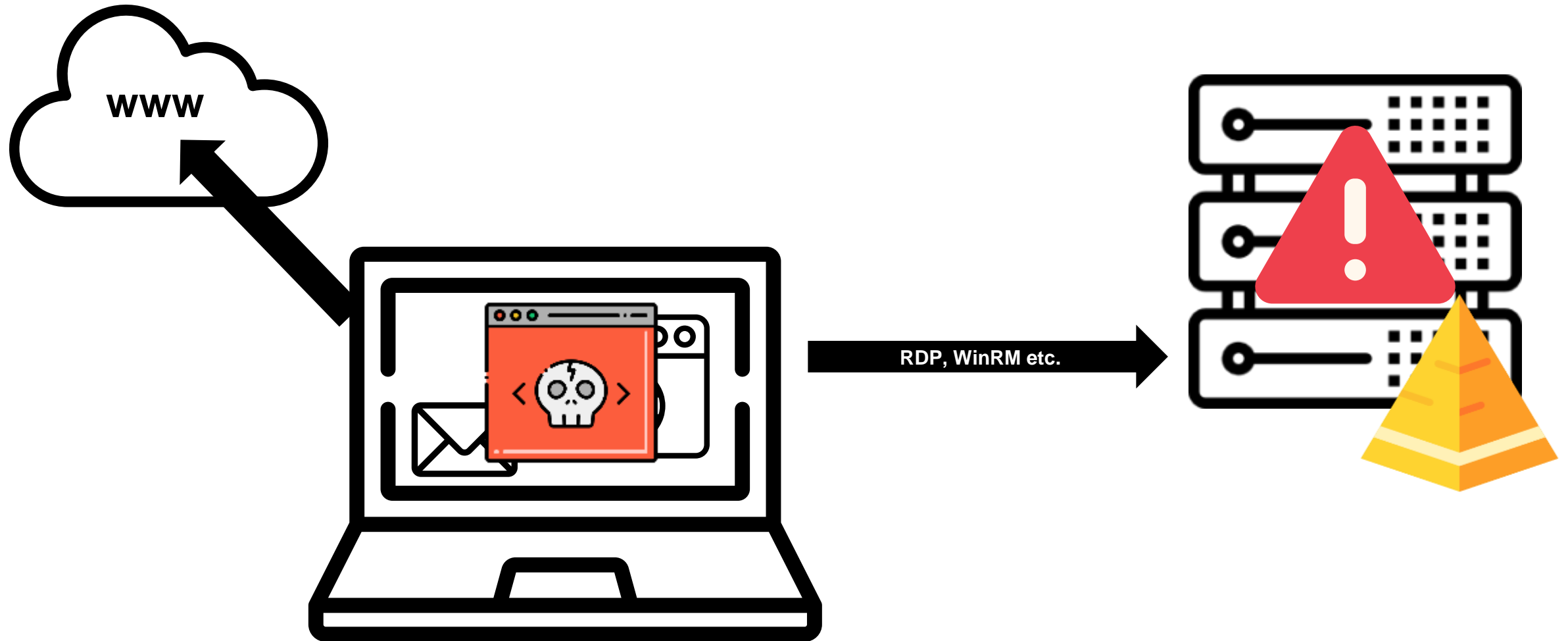
## Logging & Monitoring

- Centralized log server
- Enable all relevant logs (Windows audit policies, firewall, anti-virus, etc.)
  - Blog: <https://blog.compass-security.com/2020/09/101-for-lateral-movement-detection/>
  - Cheat sheet in repository of our guide
  - Compass Security is planning to publish new checklist
- Forward logs
- Define alert triggers (e.g., multiple failed login attempts, assignment of admin rights, etc.)
- Send out alerts to responsible (24/7)



# Some Organizational Measures...

## Privileged Access Workstations (PAW)



# Some Organizational Measures...

## Privileged Access Workstations (PAW)

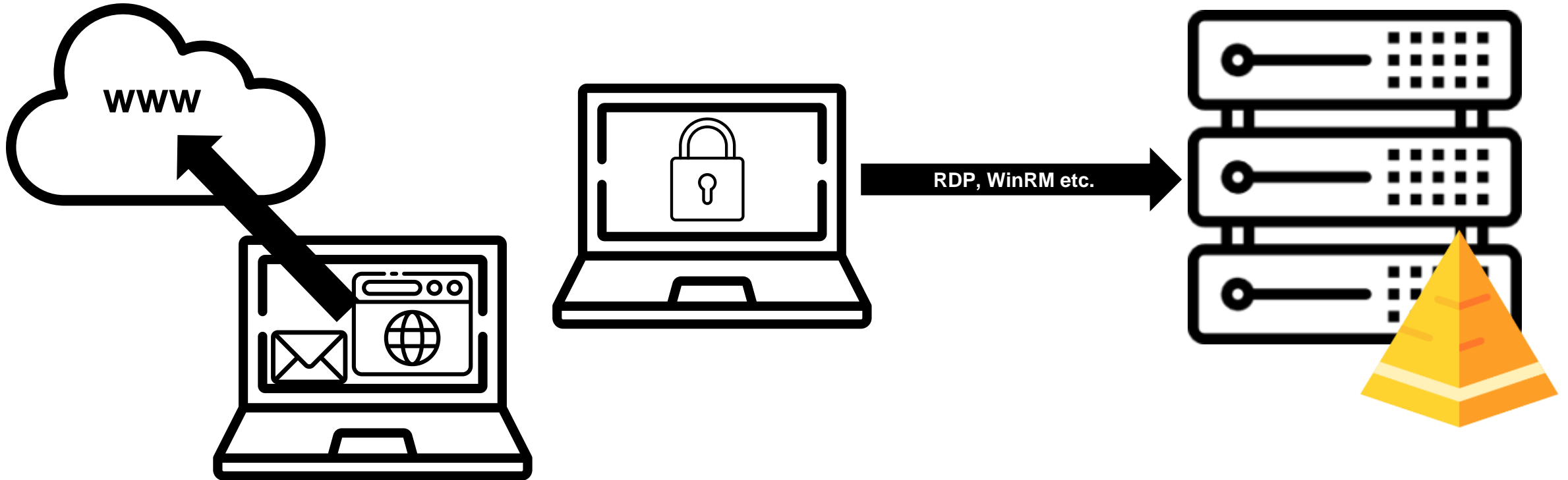
- Separate daily tasks (email, internet, etc.) from privileged access  
→ Privileged Access Workstation
- PAW has to be deployed regarding the “Clean Source Principle”!
- Different possibilities...



# Some Organizational Measures...

## Privileged Access Workstations (PAW)

- Two separate physical devices



# Some Organizational Measures...

## Privileged Access Workstations (PAW)

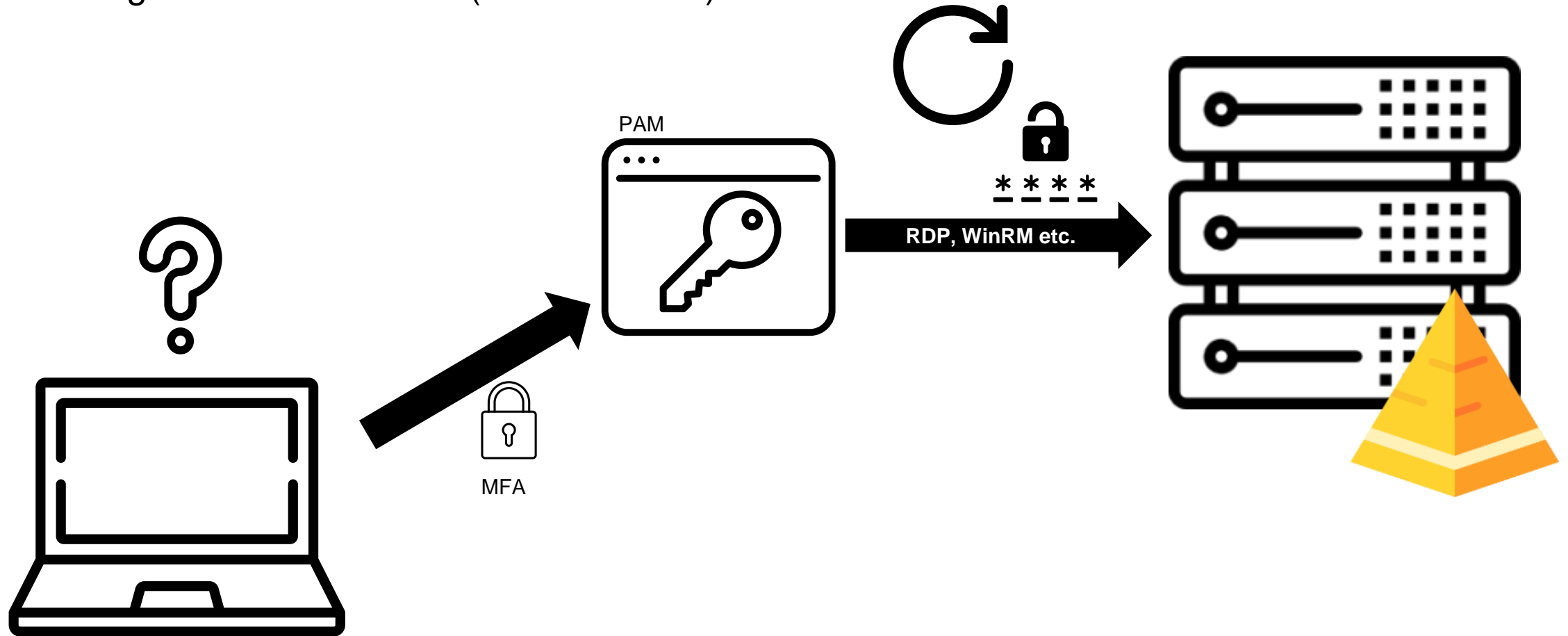
- Locked down host running shielded VMs



# Some Organizational Measures...

## Privileged Access Workstations (PAW)

- Privileged Remote Access (PAM Solution)



# Some Configurational Measures...

## Enforce Multi-Factor Authentication

- Enforce wherever possible, especially:
  - All externally (Internet) exposed interfaces
  - Management Interfaces (e. g. Firewall console, hypervisor, backup console, etc.)
  - Password Safe, Privileged access management
- Windows Login (e. g. SmartCards, YubiKey, Apps, ...) <https://duo.com/docs/rdp>

# Some Configurational Measures...

## Disable or restrict macros

The image displays the Trust Center settings in Microsoft Excel, specifically the Macro Settings section. The settings are as follows:

- Macro Settings:**
  - Disable VBA macros without notification (highlighted with a green box)
  - Disable VBA macros with notification
  - Disable VBA macros except digitally signed macros (highlighted with a yellow box)
  - Enable VBA macros (not recommended; potentially dangerous)
- Developer Macro Settings:**
  - Enable Excel 4.0 macros when VBA macros are enabled (highlighted with a green box)
  - Trust access to the VBA project object model

The Trust Center dialog box is also visible, showing the Macro Settings section with the same options. The 'Trust Center' tab is selected in the left-hand pane of the dialog box.

# Some Configurational Measures...

## Enforce SMB signing

The screenshot shows the Group Policy Editor for the 'Enforce\_SMBSigning' policy. The left pane shows the tree structure: Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options. The right pane lists several policies, with two highlighted in green:

| Policy  | Policy Setting |
|---|----------------|
| Interactive logon: Require Domain Controller authentication to unlock workstation | Not Defined    |
| Interactive logon: Require Windows Hello for Business or smart card               | Not Defined    |
| Interactive logon: Smart card removal behavior                                    | Not Defined    |
| Microsoft network client: Digitally sign communications (always)                  | Enabled        |
| Microsoft network client: Digitally sign communications (if server agrees)        | Not Defined    |
| Microsoft network client: Send unencrypted password to third-party SMB servers    | Not Defined    |
| Microsoft network server: Amount of idle time required before suspending session  | Not Defined    |
| Microsoft network server: Attempt S4U2Self to obtain claim information            | Not Defined    |
| Microsoft network server: Digitally sign communications (always)                  | Enabled        |
| Microsoft network server: Digitally sign communications (if client agrees)        | Not Defined    |
| Microsoft network server: Disconnect clients when logon hours expire              | Not Defined    |
| Microsoft network server: Server SPN target name validation level                 | Not Defined    |
| Network access: Allow anonymous SID/Name translation                              | Not Defined    |
| Network access: Do not allow anonymous enumeration of SAM accounts                | Not Defined    |

## Enforce LDAP signing

The first screenshot shows the Group Policy Editor for the 'Default Domain Controllers Policy'. The left pane shows the tree structure: Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options. The right pane lists several policies, with one highlighted in green:

| Policy  | Policy Setting  |
|---|-----------------|
| Domain controller: Allow vulnerable Netlogon secure channel connections         | Not Defined     |
| Domain controller: LDAP server channel binding token requirements               | Not Defined     |
| Domain controller: LDAP server signing requirements                             | Require signing |
| Domain controller: Refuse machine accounts                                      | Not Defined     |
| Domain member: Digitally encrypt and sign outgoing data over network            | Not Defined     |
| Domain member: Digitally sign outgoing data over network                        | Not Defined     |
| Domain member: Disable machine accounts   | Not Defined     |
| Domain member: Maximum machine account age                                      | Not Defined     |
| Domain member: Require strong authentication for client-to-client communication | Not Defined     |
| Interactive logon: Display user information during logon                        | Not Defined     |
| Interactive logon: Do not require authentication for anonymous connections      | Not Defined     |
| Interactive logon: Don't display names of previous logon attempts               | Not Defined     |
| Interactive logon: Machine accounts   | Not Defined     |

The second screenshot shows the Group Policy Editor for the 'Default Domain Policy'. The left pane shows the tree structure: Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options. The right pane lists several policies, with one highlighted in green:

| Policy   | Policy Setting  |
|--|-----------------|
| Network security: LAN Manager authentication level | Not Defined     |
| Network security: LDAP client signing requirements | Require signing |

The 'Require signing' dropdown menu is expanded, showing the selected option. A warning icon is present at the bottom of the policy setting window.

# Some Account & Privilege Management Measures...

## Reduce domain admin rights

The image displays three screenshots of Active Directory group properties windows, illustrating the membership of the 'lab\_admin' account in different administrative groups. A blue box labeled 'Builtin Administrator' has arrows pointing to the 'lab\_admin' entry in each of the three windows.

- Domain Admins Properties:** Shows 'lab\_admin' as a member of the 'Domain Admins' group.
- Enterprise Admins Properties:** Shows 'lab\_admin' as a member of the 'Enterprise Admins' group.
- Administrators Properties:** Shows 'lab\_admin' as a member of the 'Administrators' group.

| Group Name        | Member Name       | Active Directory Domain Services Folder |
|-------------------|-------------------|---|
| Domain Admins     | da-jwayne         | winattacklab.local/Users                |
|                   | lab_admin         | winattacklab.local/Users                |
| Enterprise Admins | lab_admin         | winattacklab.local/Users                |
| Administrators    | Domain Admins     | winattacklab.local/Users                |
|                   | Enterprise Admins | winattacklab.local/Users                |
|                   | lab_admin         | winattacklab.local/Users                |



# Some Account & Privilege Management Measures...

## Remove local administrator rights

```
Administrator: Windows PowerShell
PS C:\> Get-LocalGroupMember -Group Administrators

ObjectClass Name                PrincipalSource
-----
User           Client1\Administrator           Local
Group          winattacklab\Domain Admins     ActiveDirectory
```

LAPS\* managed

- For emergency scenarios
- Logon disabled by GPO

Domain Admins are, by default, members of the local Administrators groups on all member servers and workstations in their respective domains. This default nesting should not be modified for supportability and disaster recovery purposes. If Domain Admins have been removed from the local Administrators groups on the member servers, the group should be added to the Administrators group on each member server and workstation in the domain. Each domain's Domain Admins group should be secured as described in the step-by-step instructions that follow.

<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-f--securing-domain-admins-groups-in-active-directory>

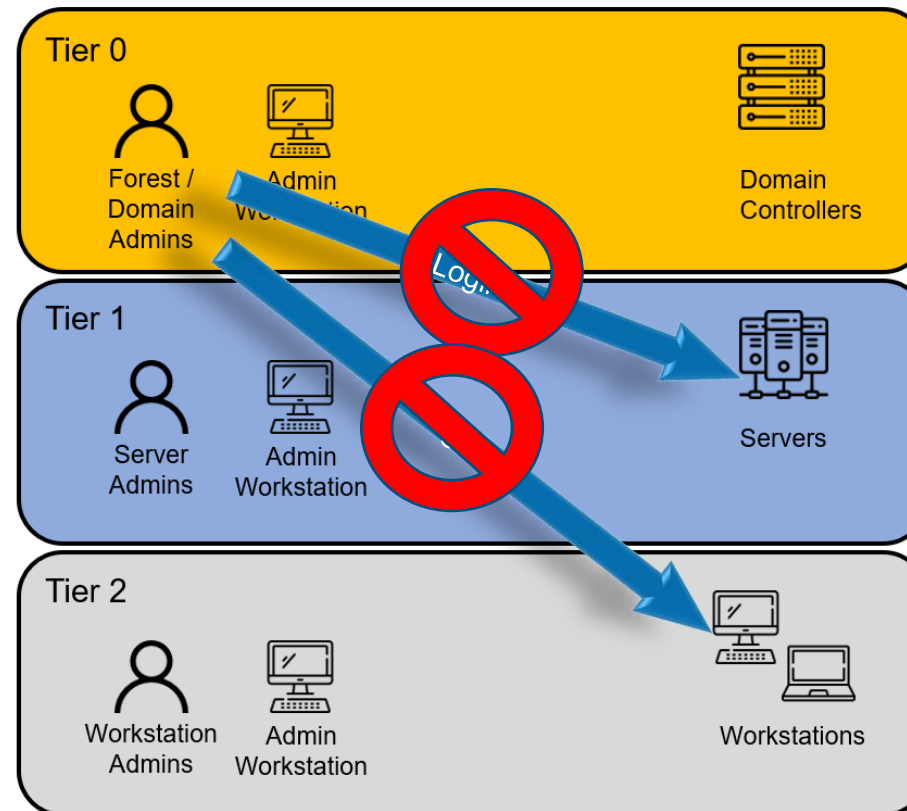
# Some Account & Privilege Management Measures...

## Deny logon to other tiers

### Minimum setup

- OU for each tier
- GPO for each tier to prevent logon types from other tiers:
  1. Deny access to this computer from the network (type 2)
  2. Deny logon as a batch job (type 3)
  3. Deny logon as a service (type 4)
  4. Deny logon locally (type 1)
  5. Deny logon through Terminal Services (type 10)

If not yet ready for tiering:  
Deny mentioned logon types of domain administrators to non-domain controllers



# Some Account & Privilege Management Measures...

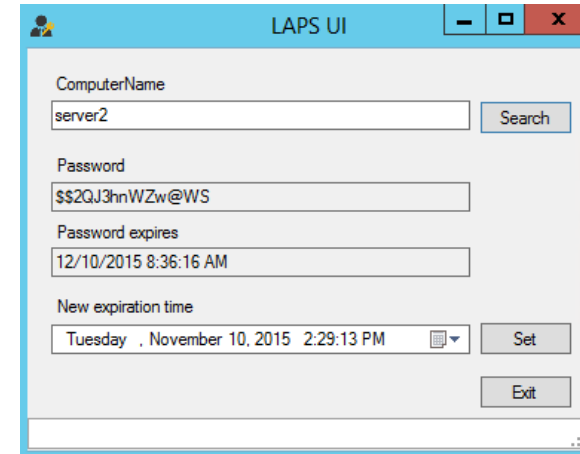
## Principle of Least Privilege

- Assign only required permissions
- Separate accounts:
  - Tasks (Support, DB Admin, Daily Business Users, etc.)
  - Classification (Public, Internal, Confidential)
  - Environment (Development, Pre-Production, Production, etc.)

# Some Password Management Measures...

## Make local admin credentials unique

- Local Administrator Password Solution (LAPS)
  - Manages local admin password for you
  - Regular change
  - Long and complex
  - Stored as LDAP attribute in AD
  - You have to decide who has access to the password
  - Provided custom UI or PowerShell cmdlets to retrieve and manage passwords
  - Easy to deploy
  - Free



# Some Password Management Measures...

## Store credentials securely

- Use password safe
- Consider using credential guard
  - Protects NTLM password hashes, Kerberos Tickets

## Do NOT store passwords in:

- Group Policy Objects
- Scripts / Files on shares (e.g. SYSVOL...)
- Object description in Active Directory
- Field userPassword in Active Directory

# Some Network Measures...

## Implement strict network segregation

### 1. Assign systems to zones based on classification:

- DMZ for systems exposed to the Internet
- Client network
- Server network
- Domain Controllers
- Management network for management interfaces and systems (e.g. Jump Hosts)
- Network for PAW
- Separate environments (Development / PreProduction / Production...)

### 2. Restrict traffic:

- Implement firewall rules which allow specific port / protocol from IP to IP
- Use whitelisting approach to only allow connections which are required!

### Side Note:

- Microsegmentation > Classic firewalling
- Windows Firewall with GPOs!

# Some Network Measures...

## Restrict outbound traffic via Proxyserver

- Connections to the internet (outgoing) must be blocked / controlled as well (Phishing)
- Force all outgoing traffic through a Proxyserver
- Disable internet access per default (Servers do not need internet connection\*)
- Filtering proxy with SSL/TLS splitting to filter malicious content

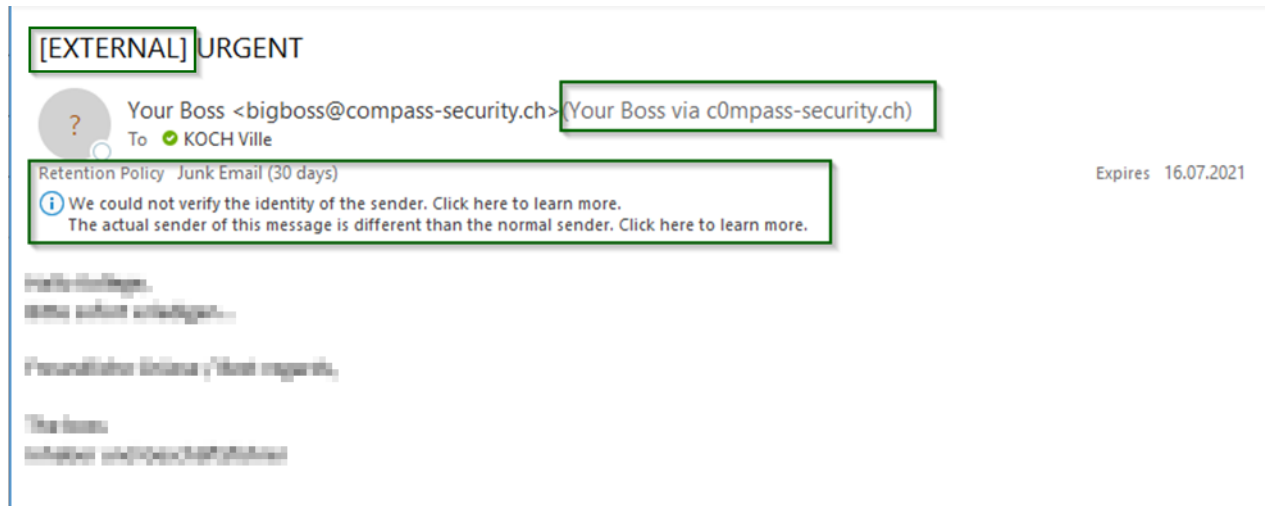
\* Whitelist required connections by specifying exact targets



# Some Network Measures...

## Use mail gateway with malware detection

- Attachments should be checked for malware (sandbox)
- Protect against spoofing:
  - Use SPF, DKIM and DMARC



# Some Network Measures...

## Secure your WiFi Networks

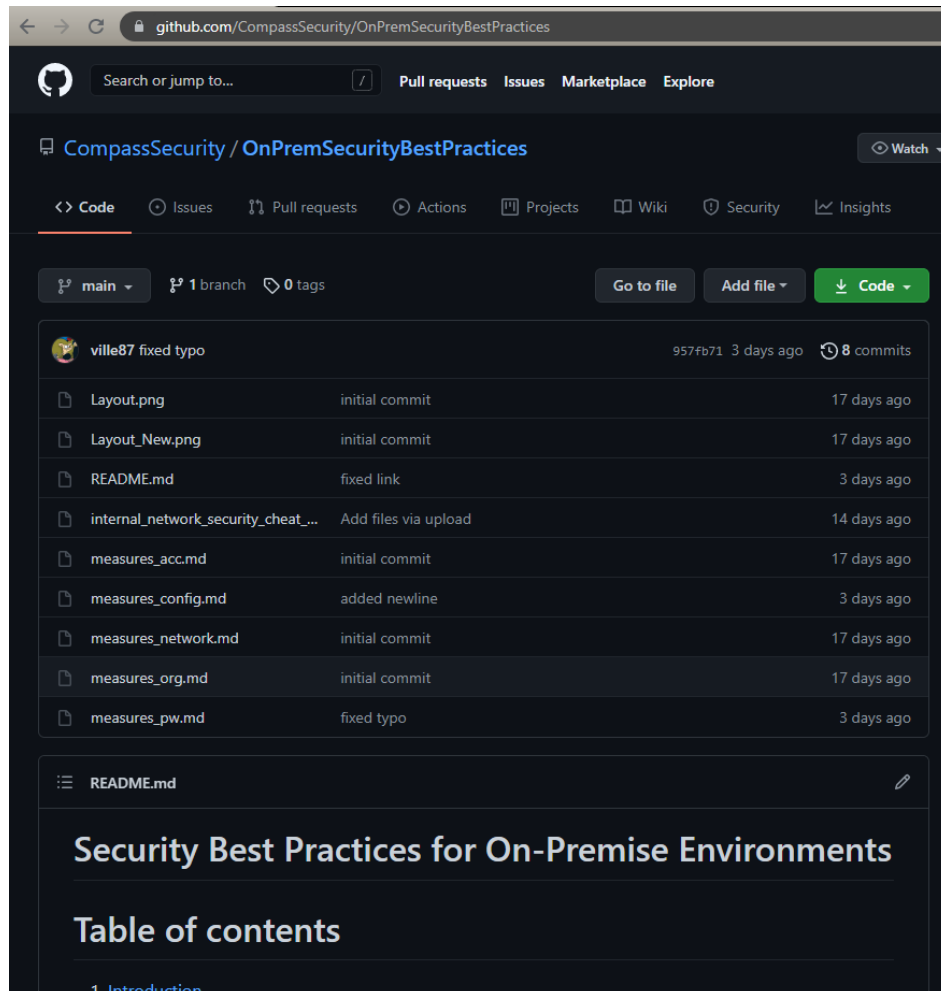
- Separate Guest and Enterprise Networks
- WPA2 Enterprise preferred (EAP-TLS), WPA2-PSK only with long complex key
- Don't use WPA or WEP (easy to break)
- Enforce client isolation

## Implement Network Access Control (NAC)

- Ideally: Certificate-based NAC (802.1X-2010) in combination with MACsec (IEEE 802.1AE)
- Exceptions:
  - Devices which do not support MACsec: Certificate-based NAC
  - Devices which do not support cert-based NAC: MAC Whitelisting & restrict on specific ports

# Our Online Guide

<https://github.com/CompassSecurity/OnPremSecurityBestPractices>



The screenshot shows the GitHub interface for the repository 'CompassSecurity/OnPremSecurityBestPractices'. The page is in dark mode. At the top, there is a search bar and navigation links for 'Pull requests', 'Issues', 'Marketplace', and 'Explore'. Below the repository name, there are tabs for 'Code', 'Issues', 'Pull requests', 'Actions', 'Projects', 'Wiki', 'Security', and 'Insights'. The 'Code' tab is selected. The main content area shows a list of files and their commit history. The files listed are: 'Layout.png', 'Layout\_New.png', 'README.md', 'internal\_network\_security\_cheat\_...', 'measures\_acc.md', 'measures\_config.md', 'measures\_network.md', 'measures\_org.md', and 'measures\_pw.md'. Below the file list, there is a section for 'README.md' with the title 'Security Best Practices for On-Premise Environments' and a 'Table of contents' section.

| File Name                           | Commit Message       | Time Ago    |
|-------------------------------------|----------------------|-------------|
| Layout.png                          | initial commit       | 17 days ago |
| Layout_New.png                      | initial commit       | 17 days ago |
| README.md                           | fixed link           | 3 days ago  |
| internal_network_security_cheat_... | Add files via upload | 14 days ago |
| measures_acc.md                     | initial commit       | 17 days ago |
| measures_config.md                  | added newline        | 3 days ago  |
| measures_network.md                 | initial commit       | 17 days ago |
| measures_org.md                     | initial commit       | 17 days ago |
| measures_pw.md                      | fixed typo           | 3 days ago  |

Security Best Practices for On-Premise Environments

Table of contents

1 Introduction

# Tools for Identification

## «Click and Run»

- PingCastle: Report about Active Directory security level  
<https://www.pingcastle.com>
- CIS Benchmarks: Report about Windows security level & best practices  
<https://www.cisecurity.org/cis-benchmarks/>

## Requires technical knowledge

- BloodHound: Identify possible attack pathes in Active Directory  
<https://github.com/BloodHoundAD/BloodHound>
- Nmap: Identify systems and open ports in your network  
<https://nmap.org/>
- Snaffler: Identify files with sensitive content (Credentials) on shares  
<https://github.com/SnaffCon/Snaffler>

More to be found on: <https://git.io/secres>

Questions?



