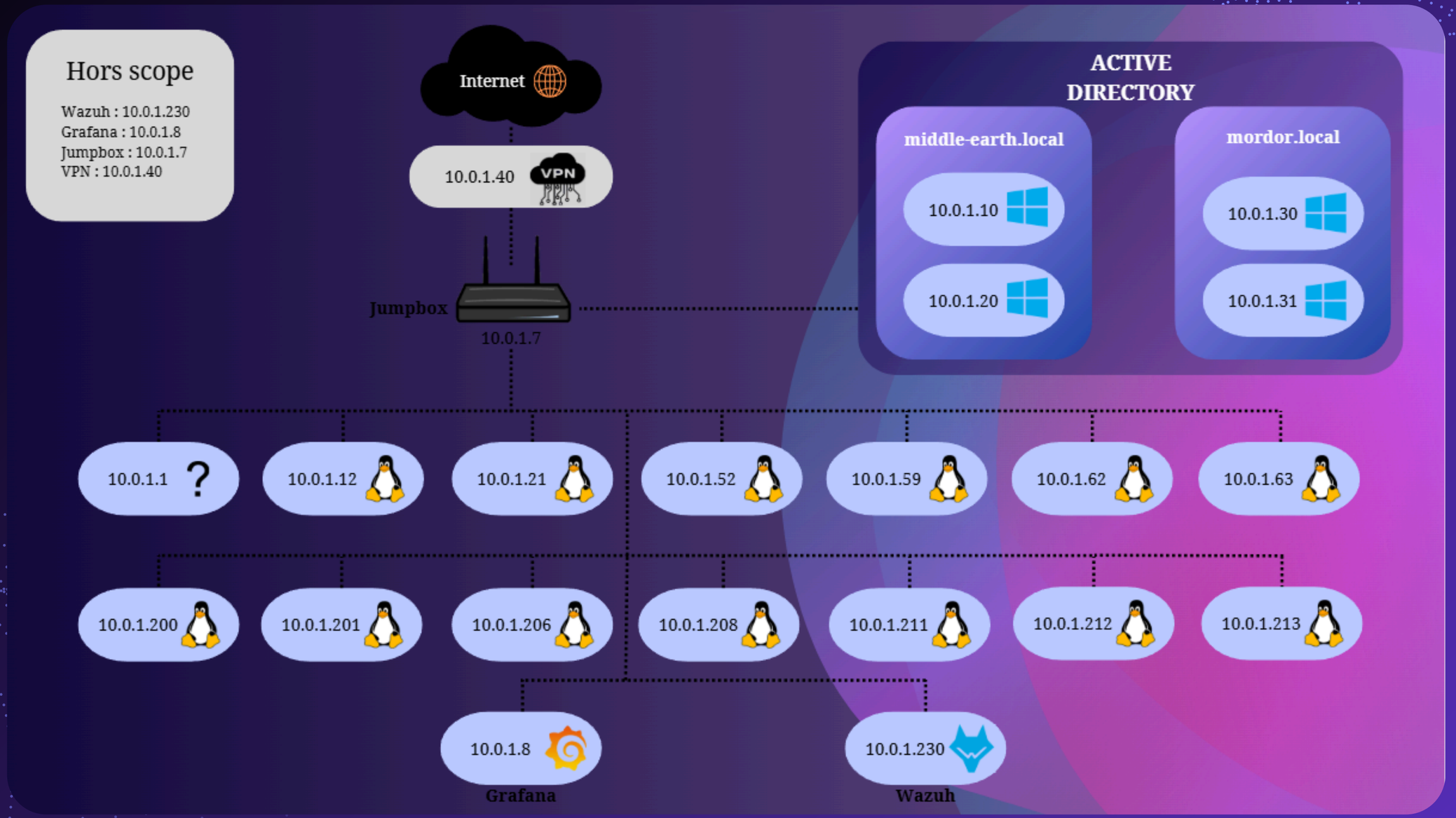
PATCH INFRASTRUCTURE

PRESENTÉ PAR
CÉDRIC BLONDEL

SOMMAIRE

- Infrastructure
- Description de la vulnérabilité
- Indicateur de compromission
- Score CVSS / Impact
- Description du correctif
- Procédure de déploiement
- Recommandations

INFRASTRUCTURE



DESCRIPTION DE LA VULNÉRABILITÉ

MISCONFIGURATION

```
ip-10-0-1-200:/usr/lib/samba/vfs# cd /etc/samba/smb.conf
-ash: cd: can't cd to /etc/samba/smb.conf: Not a directory
ip-10-0-1-200:/usr/lib/samba/vfs# cd /etc/samba
ip-10-0-1-200:/etc/samba# ls -la
total 16
drwxr-xr-x    2 root     root          4096 Nov 28 11:29 .
drwxr-xr-x    1 root     root          4096 Nov 28 13:11 ..
-rw-r--r--    1 root     root           340 Nov 29  2023 smb.conf
ip-10-0-1-200:/etc/samba# cat smb.conf
[global]
netbios name = SMB Share
workgroup = WORKGROUP
server string = SMB Share
server role = standalone
map to guest = bad user
usershare allow guests = yes

[homes]
comment = Home Directories
browseable = no
writable = yes

[share]
comment = Public File Sharing
path = /share
browseable = yes
read only = yes
guest ok = yes
ip-10-0-1-200:/etc/samba#
```

```
┌──(kali㉿kali)-[~]
└─$ smbclient //10.0.1.200/share
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Nov 28 06:29:57 2024
  ..                                  D        0  Thu Nov 28 06:30:07 2024
  secrets.txt                         N       27  Wed Nov 29 14:32:06 2023

                7941576 blocks of size 1024. 5321904 blocks available
smb: \> get secrets.txt
getting file \secrets.txt of size 27 as secrets.txt (0.3 KiloBytes/sec) (average 0.3 KiloBytes/sec)
smb: \> exit

┌──(kali㉿kali)-[~]
└─$ cat secrets.txt
JEDHA{Smb_Misconf1gur4ti0n}

┌──(kali㉿kali)-[~]
└─$
```

INDICATEUR DE COMPROMISSION

```
└─$ cat log file
[2024/12/03 14:30:00.123456,  0] ../source3/smbd/connection.c:connect_smbd()
  Client 10.10.0.7 connected to share 'public' as guest user.
[2024/12/03 14:30:00.123456,  0] ../source3/smbd/get.c:get_file()
  get_file: guest user requested download of file 'secret.txt'.
[2024/12/03 14:30:00.123456,  0] ../source3/smbd/file.c:file_close()
  close_file: guest user downloaded file 'secret.txt'.
[2024/12/03 14:30:01.123456,  0] ../source3/smbd/connection.c:disconnect_smbd()
  Client 10.10.0.7 disconnected.
```

CVSS / IMPACT

Score CVSS 7.5	Misconfiguration Serveur Samba
Gravité Élevée	

DESCRIPTION DU CORRECTIF


```
  GNU nano 5.7
[global]
netbios name = SMB Share
workgroup = WORKGROUP
server string = SMB Share
server role = standalone
map to guest = bad user
usershare allow guests = no

[homes]
comment = Home Directories
browseable = no
writable = yes

[share]
comment = Public File Sharing
path = /share
browseable = yes
read only = yes
guest ok = no
public = yes
valid users = root
```

PROCÉDURE DE DÉPLOIEMENT

```
ip-10-0-1-200:/etc/samba# nano smb.conf
ip-10-0-1-200:/etc/samba# smbpasswd -a root
New SMB password:
Retype new SMB password:
Added user root.
ip-10-0-1-200:/etc/samba# smbcontrol all reload-config
ip-10-0-1-200:/etc/samba#
```

```
┌──(kali㉿kali)-[~]
└─$ smbclient //10.0.1.200/share
Password for [WORKGROUP\kali]:
tree connect failed: NT_STATUS_ACCESS_DENIED
```

RECOMMANDATIONS

- Fail 2 ban
- Durcissement de l’accès au partage