🔍 Részletes felderítési lista lépésenként

1. Eseménynaplók vizsgálata (Event Logs)

a) Hol keresd?

- **Event Viewer** (eventvwr.msc)
- Fájlok helye: C:\Windows\System32\winevt\Logs\

b) Melyik naplókat nézd különösen?

Napló	Mit keresel?
Security	Bejelentkezések (ID 4624, 4625, 4768, 4769, 4776), fiókhozzáférések, jogosultságemelések
System	Szolgáltatások indulása/leállása (pl. új szolgáltatás malware miatt)
Application	Alkalmazások hibái, gyanús crash-ek
Windows PowerShell	Futtatott PowerShell parancsok, szkriptek
Sysmon (ha van)	Process creation, hálózati kapcsolatok, DLL injection

c) Kritikus események:

- **4624** – Sikeres bejelentkezés (nézd meg az IP-címet, milyen fiók!)
- **4625** – Sikertelen bejelentkezés (brute-force próbálkozások jele)
- **4688** – Új folyamat létrehozva (pl. cmd.exe, powershell.exe, stb.)
- **7045** – Új szolgáltatás telepítve
- **4698** – Új Scheduled Task létrehozva

---

2. Folyamatok és memória ellenőrzése

a) Hogyan nézd meg?

- **Task Manager** (taskmgr.exe)
- **Process Explorer** (Sysinternals) → részletesebb nézet
- **RAM dump és memóriaanalízis** (például: DumpIt, FTK Imager)

b) Mit keresel?

- Furcsa nevű folyamatok (pl. svchost123.exe, msword.exe de System fiókkal fut)

- Folyamatok szokatlan helyről (C:\Users\Public, AppData\Roaming, stb.)
- Aláíratlan binárisok (digitális aláírás hiánya)
- Szülő-gyermek kapcsolat (cmd.exe → powershell.exe → unknown.exe → ez gyanús)

---

3. Hálózati aktivitás ellenőrzése

a) Hogyan?

- netstat -ano
- Sysinternals TCPView
- Wireshark / Microsoft Message Analyzer

b) Mit keresel?

- Külső IP-címek felé aktív kapcsolatok, főleg ismeretlen országokba
- Nem szokványos portok használata (pl. 4444, 3389 proxyzva)
- Folyamatok, amik hálózati forgalmat generálnak (powershell.exe, wscript.exe)

---

4. Fájlrendszer változások vizsgálata

a) Hol és hogyan?

- Új, módosított fájlok keresése:
    - C:\Windows\Temp
    - C:\Users\Public
    - C:\ProgramData
    - AppData\Local\Temp
- Time-stamping vizsgálata (fájl létrehozás/módosítás dátum)

b) Eszközök:

- dir /T:C /S C:\ > files.txt
- Everything kereső
- Forensic tools (pl. FTK, X-Ways)

---

5. Felhasználói fiókok, jogosultságok ellenőrzése

a) Hogyan?

- net user
- net localgroup administrators
- Active Directory esetén: dsquery user, Get-ADUser

b) Mit keresel?

- Újonnan létrehozott fiókok
- Normál userből adminmá emelt fiókok
- Szokatlan bejelentkezési idők, IP-k

---

6. Állandósítási módszerek keresése

a) Hol?

- Scheduled Tasks:

cmd

schtasks /query /fo LIST /v

- Registry indítókulcsok:
    - HKLM\Software\Microsoft\Windows\CurrentVersion\Run
    - HKCU\Software\Microsoft\Windows\CurrentVersion\Run
- WMI Persistence (haladó)
- Services:

cmd

sc query

b) Mit keresel?

- Új időzített feladatok
- Gyanús Registry indítási értékek
- Új szolgáltatások rejtett malware-ekhez

---

7. Malware nyomok, artefaktumok keresése

- **VirusTotal** ellenőrzés ismeretlen binárisokra

- **YARA szabályok** alkalmazása memóriadumpon vagy fájlokon
- **Prefetch** fájlok (C:\Windows\Prefetch) elemzése — indított programok nyomai
- **ShimCache / Amcache** analízis — futtatott fájlok metaadatai

---

🧠 **Összegzés: Mi mindent figyelj Windows Serveren támadás felderítéskor?**

Terület	Tipikus nyomok
Event Logs	Sikertelen/sikeres logonok, új folyamatok
Process	Gyanús futó folyamatok
Network	Külső ismeretlen IP kapcsolatok
Filesystem	Új/módosított fájlok
Accounts	Új fiókok, jogosultságemelések
Persistence	Scheduled tasks, registry run entries
Malware	Ismeretlen fájlok, forensics artefaktumok