

6.4. ABE - 1

Friday, December 12, 2025 15:10

Tämä on harjotus demo , koskien mitä videossa menekään ja harjoitus jatkuu - **Access-Based Enumeration Explained + Hands-On Lab (Windows Server) - Final ton youtube videon playlist listan mukaan.**

Access-based enumeration - ABE

- Windows serverissä oleva joka pilottaa tiedostoa ja kansioita käyttäjältä kenellä EI OLE OIKEUTTA siihen.
- Ainoastaan käyttäjällä on oikeus niihin ja nähdä tiettyjä kansioita, mihin hänellä on oikeus.

Esim. Se pilottetti kansiolla on parannettu turvallisuus. Usein tämä on IT/Administrator päätös, että mitä oikeuksia mitä antaa käyttäjälle, että tarvittaessa kyskee sitten ja samahan kysyy omalta esihenkilöltä miksi ei ole oikeutta siihen kansioon ja jne - että vastaavasti pitää kysellä normaalisti.

ABE on Windows Serverin ominaisuus, joka **piilottaa tiedostot ja kansiot käyttäjiltä, joilla ei ole niihin käyttöoikeuksia**. Tämä tarkoittaa, että käyttäjä näkee vain ne resurssit, joihin hänellä on luku- tai muokausoikeus.

ABE:n toiminta:

- **Ilman ABE:tä**: Käyttäjä näkee kaikki jaetun kansion alihakemistot, vaikka hän ei voisi avata niitä.
- **ABE käytössä**: Käyttäjä näkee vain ne kansiot ja tiedostot, joihin hänellä on oikeus. Muut pysyvät täysin näkymättöminä.

Käyttökohteet:

- DFS-namespaces (Distributed File System)
- SMB-jaot (Shared folders)
- Parantaa tietoturvaa ja käyttäjäkokemusta
- Estää uteliaisuutta ja spekulointia esimerkiksi arkaluontoisten kansioiden nimistä

Miten ABE otetaan käyttöön?

- **DFS-namespaces**: DFS Management -konsolista
- **Jaetut kansiot**: Share and Storage Management -työkalusta tai PowerShellillä
- Ominaisuus ei ole oletuksena päällä, vaan se täytyy aktivoida erikseen

ABE toimii juuri kuten kuvaussessa: se **piilottaa kansiot ja tiedostot käyttäjiltä, joilla ei ole niihin oikeuksia**, ja näkyviin jää vain se, mihin käyttäjällä on pääsy. Tämä parantaa sekä tietoturvaa että käytettävyyttä.

Miksi ABE on tärkeä?

Access-Based Enumeration (ABE) ei ole pelkkä mukavuusominaisuus – se liittyy suoraan **tietoturvaan, käytettävyyteen ja organisaation riskienhallintaan**. Tässä syyt, miksi ABE on tärkeä:

- **1. Tietoturva – piilottaa arkaluontoiset resurssit**
 - Ilman ABE:tä käyttäjä voi nähdä kansioiden nimet, vaikka ei voisi avata niitä.
 - Tämä voi paljastaa **liikesalaisuksia, HR-tietoja tai projektien olemassaolon**, joita ei pitäisi edes näkyä.
 - ABE estää "tiedustelun" – käyttäjä ei voi edes arvata, mitä muuta jaossa on.
- **2. Käytettävys – selkeämpi näkymä käyttäjälle**
 - Käyttäjät näkevät vain sen, mitä he tarvitsevat.
 - Ei turhia virheilmoituksia tai epäselvyyttä siitä, miksi jokin kansio ei avaudu.
 - Parantaa käyttäjäkokemusta ja vähentää tukipyyntöjä.
- **3. Riskienhallinta – vähemmän hyökkäyspintaa**
 - Jos hyökkääjä pääsee käyttäjätilille, hän näkee vain rajatun osan tiedostoista.
 - Tämä **rajoittaa tiedonkeruuta ja estää laajempaa vahinkoa**.
 - ABE toimii kuin "visibility firewall" – näkymä on osa suojausta.
- **4. Yhteensopivuus auditoinnin ja compliance-vaatimusten kanssa**
 - ABE tukee **Zero Trust -periaatetta**: ei näkyvyyttä ilman oikeuksia.
 - Auttaa täytämään **GDPR:n ja muiden sääntelyjen vaatimuksia**, joissa tiedon minimointi ja pääsynhallinta ovat keskeisiä.

Kenelle ABE on erityisen hyödyllinen?

Käyttöympäristö

Yritykset, joissa on HR-, IT- tai talouskansioita

Hyöty ABE:stä

Piilottaa arkaluontoiset tiedot

Koulut ja oppilaitokset

Rajaa oppilaiden ja henkilökunnan näkymät

Jaetut palvelimet tai NAS-laitteet

Vähentää virheitä ja parantaa selkeyttä

DFS-namespaces-ympäristöt

Mahdolistaa dynaamisen ja turvallisen rakenteen

ABE toimii siis näin:

1. ABE tarkistaa käyttäjän NTFS-oikeudet

- Jos käyttäjällä ei ole *ainakaan* Read/Execute -oikeutta → kansio piilotetaan.

2. ABE tarkistaa jaon (share) oikeudet

- Jos share estää pääsyn → kansio piilotetaan.

3. ABE piilottaa koko polun, ei vain yksittäistä kansioita

Jos käyttäjällä ei ole oikeutta *yläkansioon*, hän ei näe sen alikansioita, vaikka niihin olisi oikeus.

Esim.:

Jos käyttäjällä on oikeus Myynti\Asiakkaat, mutta ei oikeutta Myynti-kansioon, hän ei näe mitään — koska polku ei ole saavutettavissa.

Tämä on tärkeä suunnitteluperiaate.

Miksi tämä on tärkeää?

- Estää arkaluontoisten kansioiden paljastumisen (HR, IT, talous)
- Vähentää hyökkäyspintaa (vähemmän näkyvää = vähemmän tutkittavaa)
- Selkeyttää käyttäjän näkymää
- Tukee Zero Trust -mallia
- Vähentää tukipyyntöjä ("miksi en pääse tähän kansioon?")

ABE piilottaa vain niitä tiedostoja ja kansioita käyttäjältä jos sillä ei ole oikeutta siihen. Se ei ole vain ettei käyttäjällä ole myönnnetään tai kielettään pääsy. Se riippuu käyttäjästä mitä se näkee ja riippuu mitä ja onko sillä oikeuksia siihen tiettyyn kansioon.

ABE toimii ntfs volyymillä, koska ominaisuus on syvästi sidoksissa ntfs-käyttöoikeusrakenteeseen, se ei toimi vanhemmissa, yksinkertaisemmissa tiedostojärjestelmissä.

1. Toimiiko ABE vain NTFS-oikeuksilla?

ABE perustuu NTFS:n käyttöoikeuksiin (ACL:iin), koska se tarkistaa:

- käyttäjän **Read / List folder** -oikeudet
- ryhmäjäsenyydet
- periytyvät oikeudet
- DACL-rakenteen (Discretionary Access Control List)

ABE ei tee mitään "taikatemppua" itsenäisesti — se vain **piilottaa** ne kohteet, joihin NTFS ei anna vähintään listaus-/lukuoikeutta.

Jos NTFS-oikeuksia ei ole → ABE piilottaa kohteen. Jos NTFS-oikeudet ovat → ABE näyttää kohteen.

ABE ei siis toimi ilman NTFS:n ACL-tietoja.

2. Toimiiko ABE vain NTFS-volyymeillä?

ABE on syvästi sidoksissa NTFS:n:

- ACL-rakenteeseen
- SID-pohjaiseen oikeusmalliin
- periytymislogiikkaan
- objektienvälisten metadataan (security descriptors)

Tästä syystä ABE ei toimi:

- FAT32
- exFAT
- ReFS (tiettyissä vanhemmissa versioissa, riippuen SMB-palvelusta)
- muissa yksinkertaisissa tiedostojärjestelmissä

FAT32 ja exFAT eivät tue ACL:ia → ABE:llä ei ole mitään, mitä tarkistaa → ominaisuus ei voi toimia.

3. Miksi ABE vaatii NTFS:n?

Koska ABE ei tee päätöksiä itse — se vain **heijastaa NTFS:n oikeuksia näkyvyyteen**.

ABE = "visibility filter" NTFS:n päällä.

Ilman NTFS:n:

- DACL:ia
- SACL:ia
- SID-tietoja
- periytyviä oikeuksia

ABE ei pysty arvioimaan, mitä käyttäjä saa nähdä.

ABE on tukena vain tähän volyyymiin, ettei tue FAT32, exFAT ja APFS (tiedostojärjestelmä).

ABE ei suojele tiedosto/kansiota, ettei pääsyä jos oikeudesta on väärin konfiguroit/määritetty - eli ABE vain piilottaa kansion ettei suojele kansioita.

ABE luottaa oikeisiin NTFS-käyttöoikeuksiin - tämä tarkoittaa jos vahingossa antaa käyttäjälle oikeudensa päästäänkseen arkaluonteiseen tiedostoon ABE ei pysäytä sitä. Se vain näyttää tiedosto on olemassa ja järjestelmä luulee on pääsy/valtuutettu oikeudet päästäänkseen

arkaluontaiseen tiedoston alle.

ABE ei suojaa kansioita. Se vain piilottaa sen.

Tämä on koko totuus tiivistettynä:

- **ABE = näkyvyyden hallinta**
- **NTFS = varsinainen suojaus**

ABE ei lisää mitään uutta suojaustasoa. Se ei estää pääsyä, ei salaa mitään, eikä korvaa NTFS-oikeuksia. Se vain *piilottaa* ne kohteet, joihin käyttäjällä ei ole oikeuksia.

ABE ei siis suojaa mitään — NTFS suojaaa.

ABE vain:

- vähentää näkyvyyttä
- estää uteliaisuutta
- siivoaa näkymää
- pienentää hyökkäyspintaa (koska hyökkääjä ei näe kansioita, joihin ei ole oikeuksia)

Mutta:

- jos NTFS-oikeudet ovat väärin → ABE ei pelasta
- jos käyttäjällä on oikeus → ABE näyttää kansion
- jos käyttäjällä ei ole oikeutta → ABE piilottaa kansion

Hyvä vertaus:

ABE = verhot ikkunassa **NTFS = lukko ovessa**

Verhot estävät näkemästä sisään. Lukko estää pääsemästä sisään.

ABE = verhot NTFS = lukko

Miksi tämä on tärkeää ymmärtää?

Koska jotkut luulevat, että ABE ”turvaa” kansion. Ei turvaa. Jos NTFS-oikeudet ovat väärin, ABE ei tee mitään.

ABE vain tekee näkyvyydestä siistimän ja turvallisemman käyttäjän *näkökulmasta*.

Jos haluat, voin näyttää konkreettisen esimerkin:

- mitä tapahtuu, jos NTFS-oikeudet ovat väärin
- miten ABE reagoi eri oikeusasetuksiin
- miten ABE käyttäätyy DFS:ssä vs. tavallisessa jaossa

Tai voin piirtää sinulle polkukohtaisen esimerkin, jossa näkyvä täsmälleen mitä käyttäjä näkee ABE ON vs OFF.

ABE pätee nimenomaan jaettuihin levyihin ja tiimikohtaisiin kansioihin

Kun organisaatiossa on esimerkiksi:

- **jaettuja levyjä (<\\SERVER\DATA>)**
- **tiimikohtaisia kansioita (IT, HR, Myynti, Talous...)**
- **pdf-, docx-, excel- ja muita materiaaleja**
- **henkilökohtaisia tai roolipohjaisia kansioita**
- **HR:n arkaluontoisia dokumentteja**
- **projektkohtaisia kansioita**

...niin ABE varmistaa, että käyttäjä näkee vain sen, mihin hänenlä on oikeus.

Esimerkki organisaatiosta (täysin realistinen)

<\\SERVER\DATA>

```
└── HR
    ├── Palkat.pdf
    ├── Sairaslomat.xlsx
    └── Rekryointi
└── IT
    ├── Skriptit
    └── Palvelinrakenteet
└── Myynti
    ├── Asiakkaat
    └── Raportit
└── Yhteiset
    └── Ohjeet
```

◊ HR antaa oikeuden vain HR-tiimille

→ ABE piilottaa HR-kansion kaikilta muilta.

◊ **Myynti-tiimi näkee vain Myynti-kansion**

→ ABE piilottaa IT- ja HR-kansiot automaattisesti.

◊ **Yhteiset näkyy kaikille**

→ ABE ei piilota sitä, koska kaikilla on oikeus.

ABE:n rooli tässä kokonaisuudessa

ABE ei suojaa tiedostoja

→ sen tekee NTFS-oikeudet.

ABE piilottaa tiedostot ja kiosiot

→ jotta käyttäjä ei edes näe, mitä muuta jaossa on.

Tämä on tärkeää esimerkiksi HR:n näkökulmasta:

- HR voi antaa oikeuden yksittäiselle käyttäjälle (esim. esihenkilölle) tarkistaa yhden kansion.
- ABE varmistaa, että tämä käyttäjä ei näe mitään muuta HR:n sisällä.
- Muut käyttäjät eivät näe HR-kansioita lainkaan.

Miksi tämä on kriittistä organisaatioissa?

 **1. Tietoturva**

Kansioiden nimet voivat paljastaa arkaluontoista tietoa:

- "Palkat"
- "Sairaslomat"
- "Irtisanomiset"
- "Auditointi 2025"

ABE estää tämän.

 **2. Käytettävyys**

Käyttäjä ei näe turhia kansioita → vähemmän virheitä ja vähemmän tukipyyntöjä.

 **3. Hyökkäyppinnan pienentäminen**

Jos hyökkääjä saa käyttäjätilin haltuunsa, hän näkee vain murto-osan tiedostoista.

4. Zero Trust -periaate

Ei näkyvyyttä ilman oikeuksia.

Yhteenveto

Kyllä — ABE on juuri sitä varten, että:

- organisaation jaetuilla levyillä
- tiimikohtaisissa kansioissa
- HR:n arkaluontoisissa materiaaleissa
- projektikohtaisissa jaoissa

käyttäjät näkevät **vain sen**, mihin heillä on oikeus.

ABE = näkyvyyden hallinta NTFS = varsinaisen suojaus