Lauri Partinen ktkt23sp

Ryhmätyön loppuraportti

Active Directory ympäristön hyökkäys ja puolustus
Penetraatiotestaus

2025

Kaakkois-Suomen
ammattikorkeakoulu

SISÄLLYS

1 JOHDANTO

Ryhmämme aiheeksi valitsimme Active Directoryn hyökkäys ja puolustus, joka rajattiin projektissa IPv6-protokollaan. Projekti suoritettiin virtuaalilaboratoriossa, jossa on kaksi domain kontrolleria, jotka on asetettu Ipv6-protokolla aktiiviseksi. Laboratoriossa on kaksi Windows konetta, jotka toimivat käyttäjäkoneina laboratoriossa. Hyökkäysskenaario toteutettiin erillisillä kali-koneella, jolla suoritetaan dns spoofing, jossa kali esittää olevansa luetettava verkkolaite. Projektin rajaus toteutetaan keskittymällä IPv6-protokkolan haavoittuvuuksissa ja mitigointi keinoissa.

IPv6-protokolla on penetraatiotestauksessa ajankohtainen aihe, koska ipv4 osoitteen ovat loppu. Tulevaisuudessa yhä useammat Active Directoryt tulevat hyödyntämään IPv6-osoitteita, joten ylläpitäjän tulisi ymmärtää konfiguroidessa mahdolliset uhat, mitä ympäristöön voi kohdistua. Ympäristön hyökkäyksen seurauksena yrityksen toiminnan jatkuvuus, asiakkaiden ja työntekijöiden tiedot voivat olla vaarassa.

2 AIVORIIHI

Aivoriihi lähti käyntiin teorian keräämisellä eri lähteistä. Annettiin roolit toiset etsivät tietoa hyökkäysvaiheesta ja toiset mitigoinnista. Keräsimme lopulta aiheesta muistilapun, jossa oli kootusti tietoa aiheesta. Kun tietojen kerääminen oli saatu suoritettua tuli miettiä, mihin ympäristöön halutaan projekti toteuttaa. Aiemmissa opinnoissa olimme konfiguroineet valmiin Active Directory ympäristön, jota lopulta päätimme hyödyntää. Valmiin laboratorio instanssin hyödyntäminen säästi aikaa, ja ympäristö oli ennestään tuttu. Ainoan muutoksen teimme labraan, kun lisäsimme kali koneen, jolla suoritetaan hyökkäys ympäristöön. Toinen vaihtoehto olisi ollut toteuttaa projektin ympäristö rakentaminen Proxmox-palvelimelle. Päädyimme kuitenkin suorittaa tehtävän muutamaa muokkausta vaille olevaan valmiiseen laboratorioon.

Kun saimme tehtyä päätöksen ympäristöstä, johon projekti on tarkoitus suorittaa. Alettiin kartoittaa hyökkäystapaa, jolla voidaan demonstroida Active Directory hyökkäystä ja mitigointi keinoja sitä vastaan. Kävimme aivoriihen

aikana etsittyjä lähteitä läpi, josta löysimme artikkelin top 10 hyökkäystekniikoista Active Directory ympäristöä vastaan (Mistry 2025). Artikkelin avulla käytiin eri skenaarioita, mikä voisi toimia laboratoriossa. Päätimme kokeilla eri vaihtoehtoja ympäristössä ennen kuin päätettiin lopullisesta aiheesta. Hyökkäys taktiikoina valittiin LDAP Reconnaissance, BloodHound Reconnaissance ja Kerberoasting.

LDAP reconnaissance hyökkäyksessä motiivina on kerätä tietoa. Hyökkääjä lähettää LDAP-kyselyitä Active Directory ympäristöön, jos hyökkäys onnistuu hyökkääjä saa tietoa käyttäjistä, koneista ja pystyy tutkimaan ympäristöä. LDAP hyökkäyksen onnistuminen vaatii käyttäjätilin haltuunoton, joka kuuluu Active Directory ympäristöön. Järjestelmänvalvojan tunnnuksia ei vaadita hyökkäyksen suorittamiseen. (Netwrix.)

BloodHound Reconnaissance hyökkäyksessä hyödynnetään BloodHound-työkalua, joka tunnistaa mahdollisia hyökkäysreittejä Active Directoryssä. BloodHound-työkalun avulla automatisoidaan tiedonkeruuprosessi. Heikosti suojatussa ympäristössä työkalun avulla voidaan saavuttaa järjestelmän valvojan oikeudet. (Sans 2021).

Kerberoasting hyökkäys kohdistuu Active Directoryn palvelutileihin, joihin pyritään pääsemään käsiksi käyttämällä Kerberos-palvelulippuja jakamalla niitä. Kerberos vastaa TGS lipulla, joka sisältää salatun palvelutilin hash salasanalla. Hyökkääjä voi järjestelmän ulkopuolella purkaa salauksen valitsemalla työkalullaan ja murtautua sisään. (Benoit 2025).

Kokeilimme kaikkia edellä mainituista hyökkäyksistä. Olimme kokeilemassa hyökkäystä, kun vanhempi opiskelija kysyi, mitä olimme tekemässä. Hän ehdotti vaihtoehtoiseksi hyökkäystekniikaksi IPv6 spoofing hyökkäys. Hyökkäyksessä jätetään domain kontrolleriin IPv6 päälle, jota ulkopuolinen kone spoffaa. Kone esittää olevansa luotettava verkkolaite, joka lopulta kappaa tietoja järjestelmästä.

3 YKSILÖLLINEN OPPIMISTEHTÄVÄ

Yksilöllistä oppitehtävää jaoimme roolit ryhmän kesken. Kaksi vastasivat hyökkäys puolesta ja toiset ottivat puolustus puolen vastuulleen. Päätimme yhdessä Laurin ja Tuomaksen vastaavan puolustuksesta. Atro ja Joona huolehtivat hyökkäys puolesta. Puolustus puolella Lauri keskittyi Active Directoryn puolustukseen ja suojaukseen. Tuomas aiheena on tietoturva poikkeamien hallinta ympäristössä. Hyökkäys puolella Joona keskittyi ympäristön tiedusteluun. Atro aiheena on yleisimmät hyökkäysvektorit. Aiheiden jako kattaa hyökkäys elinkaaren tiedustelusta, hyökkäykseen, havaitsemiseen, reagointiin ja lopulta puolustamiseen.

Raporttien yhteenvetona voidaan todeta Active Directoryn olevan organisaation kannalta kriittinen järjestelmä, joka voi pahimmassa tapauksessa vaarantaa organisaation liiketoiminnan jatkuvuus. Onnistunut murtautuminen mahdollistaa käyttäjäoikeuksien eskaloinnin, sivuttaisliikkeen mahdollisuuden verkossa sekä arkaluonteisen tiedon varastamisen ympäristöstä. (Vaideeswaran 2025).

Active Directoryn tietoturva kannalta tärkeää on ennaltaehkäisy. Ennakoivaan valmistautumiseen sisältää esimerkiksi salasanapolitiikan, kaksivaiheisen tunnistautumisen, vähimmän käyttöoikeuksien periaatteen ja SMB allekirjoitus. Esimerkkien tarkoitus on pienentää hyökkääjän hyökkäys pinta-alaa. Jatkuva monitorointi ja ylläpito on erityisen tärkeää, jotta Active Directory pysyisi mahdollisimman turvallisena.

Hyökkäyksessä hyökkääjä hyödyntää Active Directorystä löytyviä eri osia esimeriksi kerberos hyökkäyksessä kerberos tunnistautumista. Hyökkääjän motiivi voi olla käyttöoikeuksien korottaminen tai palvelutilien haltuunotto. Yleisesti hyökkäykset johtuvat heikoista salasanoista, liiallisista oikeuksista työntekijöillä tai puutteelliseen ympäristön valvontaan.

Active Directoryn puolustaminen kattaa monia eri vaiheita sisältävän kokonaisuuden, jossa liikkuvia osia on jatkuvasti. Esimerkiksi työntekijä tarvitsee korottaa käyttöoikeuksia, jotta hän pääsee tekemään työnsä ja sama toisin päin. Puolustaminen vaatii jatkuvaa monitorointia ja ajankohtaisten hyökkäyksien huomioimista. Active Directoryn järjestelmän valvojalla pitää olla jatkuva tilannekuva ympäristöstä ja pyrkiä tekemään jatkuvia päivityksiä

järjestelmään, kun haavoittuvuuksia ilmenee, jotta tietoturva taso pysyisi mahdollisen korkeana. Puolustaminen elintärkeää yrityksen liiketoiminnan jatkuvuuden kannalta.

4 RYHMÄN ANALYYSI

Ryhmän havaintoja Active Directoryn murtamiseen. Hyökkääjät hyödynnetään harvoin vain yhtä haavoittuvuutta. Virhekonfiguroinnit, käyttöoikeuksien turha korottaminen ja puutteellinen valvonta avaavat hyökkääjälle mahdollisia haavoittuvuuksia, joita voidaan käyttää hyökkäykseen. Toinen merkittävä havainto, jonka huomasimme, oli tiedustelun merkitys hyökkäyksessä. Hyökkääjä suorittaa perusteellisen tiedustelu suunnitelman, jossa hyökkääjä voi hyödyntää työkaluja esimerkiksi BloodHound tai SharpHound. Työkalut luovat vaivattoman tavan saada tietoa ympäristöstä, joka tekee hyökkäyksen havaitsemisen entistä vaikeampaa. Kolmas havainto, minkä ryhmä teki, oli kuinka kauan hyökkäys voi kestää. Esimerkiksi Golden ticket -hyökkäyksessä hyökkäyksen havaitseminen ilman toimivaa loki- tai valvontajärjestelmää mahdollistaa hyökkäyksen kestämisen huomaamattomasti pitkään. (Crowdstrike 2025.) Jatkuvaa salasanojen rotaatio ja käyttöoikeuksien valvonta on tärkeää ympäristön turvallisuuden kannalta. Yhteenvetona havainnoista voidaan todeta sama, mikä raportissa aiemmin on jo mainittu. Active Directoryn puolustaminen on jatkuva prosessi, joka vaatii asiantuntevan järjestelmänvalvojan ja jatkuvan valvonnan.

Suurimmat ryhmän keskeiset haasteet liittyivät aiheen laajuuteen. Ryhmän kesken mietimme pitkään, miten rajataan aihe. Erilaisia hyökkäystapoja ja teoriaa löytyi todella paljon, ja sen tiivistäminen olennaiseen tuotti hankaluuksia. Tavoitteena oli pitää asiat yksinkertaisena, vaikka aihe oli laaja. Päästyämme yhteisymmärrykseen toteutustavasta. Aihe huomioon ottaen roolien jako onnistui mutkattomasti. Atro ja Tuomas tehtävänä oli konfiguroida ympäristöä ja Laurin ja Joonan tehtävä oli suunnitella ja toteuttaa hyökkäys. Lauri vastuulla oli kertoa myös teorian tasolla, miten hyökkäystä voitaisiin mitigoida.

5 JATKOKEHITYS

Projektin jatkokehityksen voisi jakaa kahteen osaan IPv6-ympäristön hyökkäyksen laajentaminen ja IPv6 spoofauksen havaitseminen. Hyökkäyksen laajentaminen voitaisiin simuloida esimerkiksi, miten spoofauksen jälkeen kaapattua salasanaa voidaan hyödyntää järjestelmässä. Voidaan demonstroida, miten käyttäjäoikeuksien eskalointi voi johtaa tai suorittaa sivuttaisliikettä verkossa, josta saadaan järjestelmästä kerättyä tietoa. Havaitsemisen näkökulmasta olisi hyvä demonstroida tarkemmin esimerkiksi Wiresharkilla, miten hyökkäys voidaan huomata tai kehittää työkalu, joka huomaisi epätavallisen toiminnan.

LÄHTEET

Mistry, A. 2025. Top 10 Active Directory Attack Techniques Still Working in 2025. Medium. WWW-dokumentti. Saatavissa: https://medium.com/@abhimistry06/%EF%B8%8F-top-10-active-directory-attack-techniques-still-working-in-2025-70e0787e86fe [viitattu 15.12.2025].

Pavithran, P. 2025. Active Directory Incident Response: Key Things to Keep in Mind. WWW-dokumetti. Saatavissa: https://fidelissecurity.com/threatgeek/active-directory-security/active-directoryincident-response/ [Viitattu 15.12.2025].

Vaideeswaran, N. 2025. Active directory security. WWW-dokumentti. Saatavissa: https://www.crowdstrike.com/en-us/cybersecurity101/identity-protection/active-directory-security/ [Viitattu 22.11.2025].

Baker, K. 2025. Golden ticket attack: What it is and how to defend. WWW-dokumentti. Päivitetty 26.3.2025. Saatavissa: https://www.crowdstrike.com/enus/cybersecurity-101/cyberattacks/golden-ticket-attack [viitattu 14.12.2025].

Benoit, P. 2025. What is kerberoasting? Attack and security tips explained. WWW-dokumentti. Saatavissa: https://www.vaadata.com/blog/what-is-kerberoasting-attack-and-security-tipsexplained [viitattu 22.11.2025].

SANS Institute. 2021. BloodHound – Sniffing Out the Path Through Windows Domains. WWW-dokumentti. Saatavissa: https://www.sans.org/blog/bloodhound-sniffing-out-path-through-windows-domains [viitattu 15.2.2025].