jamk

Haavoittuvuustietokannat

Ryhmä 3

Anthony Bäckström

Sami Koivisto

Eino Puttonen

Jussi-Pekka Rantala

Harjoitustyö

Maaliskuu 2024

Tieto- ja viestintätekniikan tutkinto-ohjelma (AMK)

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Sisältö

1 Johdanto

Työn tarkoituksena on selvittää mitä haavoittuvuustietokantoja on olemassa ja vertailla niiden ominaisuuksia. Valitsimme työhön neljä eri haavoittuvuustietokantaa, joita lähdemme tarkemmin puimaan.

2 Haavoittuvuustietokanta

Haavoittuvuustietokanta on järjestelmä tai resurssi, joka kerää, tallentaa ja jakelee tietoa ohjelmistojen haavoittuvuuksista ja niihin liittyvistä turvallisuusuhat. Nämä tietokannat tarjoavat tärkeää tietoa kyberturvallisuuden ammattilaisille, auttaen heitä tunnistamaan ja korjaamaan haavoittuvuuksia, suojatakseen järjestelmiään mahdollisilta hyökkäyksiltä.

2.1 NVD

Yleistä: NVD on Yhdysvaltain hallituksen arkisto, joka sisältää standardeihin perustuvia haavoittuvuuksien hallintatietoja, jotka on esitetty SCAP-protokollan (Security Content Automation Protocol) avulla. Nämä tiedot mahdollistavat haavoittuvuuksien hallinnan, turvallisuuden mittaamisen ja vaatimustenmukaisuuden automatisoinnin. NVD sisältää tietokantoja tietoturvan tarkistuslistan viitteistä, tietoturvaan liittyvistä ohjelmistovirheistä, tuotenimistä ja vaikutusten mittareista. (NVD – General)

NVD suorittaa analyysin CVE-tietokannasta, joka on julkaistu CVE-sanakirjassa. NVD:n henkilökunnan tehtävänä on analysoida CVE-tietokantoja kokoamalla yhteen kuvauksesta, toimitetuista viitteistä ja kaikista lisätiedoista, jotka ovat julkisesti saatavilla kyseisenä ajankohtana. Analyysin tuloksena saadaan yhdistysvaikutusten mittarit (Common Vulnerability Scoring System - CVSS), haavoittuvuustyypit (Common Weakness Enumeration - CWE) ja sovellettavuuslausekkeet (Common Platform Enumeration - CPE) sekä muut asiaankuuluvat metatiedot. NVD ei suorita aktiivisesti haavoittuvuustestausta, vaan se luottaa siihen, että toimittajat, kolmannen osapuolen tietoturva-

tutkijat ja haavoittuvuuskoordinaattorit toimittavat tietoja, joita sitten käytetään näiden ominaisuuksien määrittämiseen. CVSS-arviointeja, CWE-luokituksia ja soveltuvuuslausuntoja voidaan muuttaa sitä mukaa, kun lisätietoa tulee saataville. NVD pyrkii analysoimaan muutetut CVE:t uudelleen ajan ja resurssien salliessa varmistaakseen, että tarjotut tiedot ovat ajan tasalla. (NVD – General)

Hinta: Ilmainen

Käytettävyys/Raportointityökalu: NVD tarjoaa hakutoimintoja ja voit käyttää hakutoimintoa löytääksesi tiettyjä haavoittuvuuksia. Voit hakea esimerkiksi CVE-tunnisteen, avainsanojen, valmistajan tai tuotteen mukaan. Voit kaventaa tuloksia erilaisilla suodattimilla, ja selailla saatuja haavoittuvuuksia. Löydät lisätietoa haavoittuvuudesta klikkaamalla sitä. Tietoihin kuuluu yleensä haavoittuvuuden kuvaus, CVSS-pisteet, vaikutuksen laajuus, hyväksikäyttömahdollisuudet ja mahdolliset korjaustoimenpiteet. (NVD - Search Vulnerability Database)

Mikäli olet kehittäjä (developer) tai haluat integroida NVD-tiedot omaan järjestelmääsi, voit käyttää NVD:n tarjoamaa API:a (Application Programming Interface) automatisoidaksesi haavoittuvuustietojen hakuja. (NVD – Developer)

Muuta: NVD:llä on oma dashboard, josta näkee nopeasti, kuinka monta CVE:tä on tullut ja kuinka monta NVD on analysoinut. Tämän lisäksi siitä näkee viimeiset 20:tä pisteytettyä haavoittuvuustunnusta ja yhteenvetoa.

2.2 CVE (Common Vulnerabilities and Exposures)

CVE on haavoittuvuustunnistejärjestelmä, joka tarjoaa yksilöllisen tunnisteen ja standardoidun nimen kullekin tunnetulle haavoittuvuudelle. CVE-tunnisteiden avulla kyberturvallisuuden ammattilaiset voivat helposti vaihtaa tietoa haavoittuvuuksista ja niiden korjaamisesta. CVE-järjestelmää

hallinnoi MITRE Corporation, ja se on keskeinen osa kansainvälistä tietoturvaekosysteemiä. (About the CVE Program. 2024).

Hinta: Ilmainen

Helppokäyttöisyys: CVE-tunnisteet ovat saatavilla monissa eri haavoittuvuustietokannoissa, mukaan lukien NVD, mikä tekee niiden käytöstä yleisesti helppoa.

Raportointityökalut: Ei tarjoa suoraan raportointityökaluja, mutta sen tunnisteita käytetään laajasti erilaisissa tietoturvatyökaluissa ja raportointijärjestelmissä.

Mahdollinen liitettävyys: Laaja liitettävyys, koska CVE-tunnisteet ovat standardi haavoittuvuuksien tunnistamisessa.

2.3 Vulnerability Database VulDB

VulDB eli Vulnerability Database on haavoittuvuustietokanta, joka dokumentoi ja selittää tietoturvahaavoittuvuuksia ja niiden hyödyntämisiä. VulDB on perustettu 1998. VulDB kuratoi ja dokumentoi kaikki tietoturvahaavoittuvuudet, jotka on julkaistu sähköisissä tuotteissa. VulDB on yksi tärkeimmistä lähteistä niille, jotka ovat vastuussa haavoittuvuuksien käsittelystä, haavoittuvuuksien hallinasta, hyökkäyksien analysoinnista, kyberuhkien tiedustelusta ja tapahtumien käsittelystä. (FAQ.)

Hinta: Ilmainen tai kaupallinen, joka maksaa 199 $ kuukaudessa. Kaupallisessa on enemmän API krediittejä käytettäväksi päivässä, kattavuus parhaalla tavalla ja laajennettu asiakastuki. (Pay.)

Helppokäyttöisyys: VulDB:n yksi keskeisimmistä ominaisuuksista on sen kyky integroitua saumattomasti kolmannen osapuolen palveluihin, kuten GRC-työkaluihin. Tämä onnistuu sen RESTful API:n avulla, joka mahdollistaa helpon pääsyn haavoittuvuustietoihin mikä auttaa organisaatiota reagoimaan nopeasti tietoturvariskeihin. (6 Powerful Vulnerability Databases to Search Publicly Disclosed Security Vulnerabilities 2023.)

Yleisesti VulDB:n käyttö on melko sujuvaa, jos työskentelee säännöllisesti haavoittuvuuksien hallinnan parissa mutta jos käyttäjä on aloittelija, VulDB:n käyttö saattaa vaatia hieman opettelua.

Raportointityökalut: VulDb:n moderointitiimi seuraa aktiivisesti lukuisia lähteitä ympäri vuorokauden ja kerää tietoja uusista tai olemassa olevista haavoittuvuuksista. Uuden uhan löytyessä, tiimi kerää lisätietoja eri lähteistä ja luo yksityiskohtaisen VulDB-entryn. Tämä VulDB-entry tuodaan saataviksi asiakkaille verkkosivun ja API:n kautta. (6 Powerful Vulnerability Databases to Search Publicly Disclosed Security Vulnerabilities 2023.)

Mahdollinen liitettävyys: VulDB voi integroitua saumattomasti kolmannen osapuolen palveluihin. (6 Powerful Vulnerability Databases to Search Publicly Disclosed Security Vulnerabilities 2023.)

2.4 Exploit Database

Expolit DB on tietoturvakoulutuksia pitävän OffSecin ylläpitämä non-profit palvelu. Se sisältää neljä erillistä tietokantaa: Expolits, Google Hacking, Papers sekä Shellcodes. (About The Exploit Database. 2024). Kuka vaan voi ilmoittaa haavoittuvuuden (exploitin), jonka OffSec testaa, ja todetessaan sen toimivaksi, se lisätään tietokantaan. (Answers to Common Questions People Have for Us 2024).

Hinta: Exploit DB:n käyttäminen on ilmaista. Ja sieltä haavoittuvuuksien sekä niihin liittyvien tietojen lataaminen on ilmaista. (About The Exploit Database 2024).

Käytettävyys: Yksinkertainen web-interface, mistä voit voi hakea haavoittuvuuksia mm. hakusanoilla, alustoilla ja kategorioilla. (About The Exploit Database. 2024).

Raportointityökalut: Ei tarjoa varsinaisia raportointityökaluja. Haavoittuvuuksia on kuitenkin mahdollista ladata itselle ja integroida niitä yrityksen omiin tarkastus- ja raportointiprosesseihin.

Liitettävyys: Exploit DB on mahdollista integroida käyttäjän järjestelmiin github-repositoriosta SearchPloit työkalulla. Sen avulla sitä on mahdollista käyttää myös off-line tilassa ympäristöissä, joissa internet-yhteyttä ei ole tarjolla. OffSec- tarjoaa kattavat ohjeet SearchPloitin asennukseen ja peruskäyttöön. (SearchPloit- The Manual 2024).

Muut seikat: Tietokantaa päivitetään päivittäin. Ei tarjoa ratkaisuita/korjauksia, vaan keskittyy haavoittuvuuksien ja niihin liittyvien tietojen julkaisuun. (The Exploit Database Git Repository 2018.)

Lähteet

6 Powerful Vulnerability Databases to Search Publicly Disclosed Security Vulnerabilities. 2023. Viitattu 23.3.2024. https://medium.com/thesecmaster/6-powerful-vulnerability-databases-to-search-publicly-disclosed-security-vulnerabilities-f703a23d0854

About The Exploit Database. 2024. Expolit Database. Viitattu 23.3.2024. https://www.exploit-db.com/about-exploit-db

About the CVE Program. 2024. CVE. Viitattu 23.3.2024. https://www.cve.org7About/Overview

Answers to Common Questions People Have for Us. 2024. Exploit Database. Viitattu. https://www.exploit-db.com/faq

FAQ. Viitattu 23.3.2024. https://vuldb.com/?kb.faq

NVD – General. Viitattu 24.3.2024. https://nvd.nist.gov/general

NVD - Search Vulnerability Database. Viitattu 24.3.2024. https://nvd.nist.gov/vuln/search

NVD – Developer. Viitattu 24.3.2024. https://nvd.nist.gov/developers

Pay. Viitattu 23.3.2024. https://vuldb.com/?pay

SearchPloit- The Manual. 2024. Exploit Database. 2024. Viitattu 23.3.2024 https://www.exploit-db.com/searchsploit

The Exploit Database Git Repository 2018. GitHub. Viitattu 23.3.2024. https://git-hub.com/perplext/exploit-database