PROJEKT

Multitenantné operačné centrum kybernetickej bezpečnosti riešené ako otvorená cloudová služba s prvkami strojového učenia

Podklad pre V4

Výber a implementácia nástroja pre skenovanie zraniteľností

Prepojené na pracovný balík KPB2 – Návrh SOCaaS služby

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

ÚRAD VLÁDY
SLOVENSKEJ REPUBLIKY

Obsah

1. VÝBER A IMPLEMENTÁCIA NÁSTROJA PRE SKENOVANIE ZRANITEĽNOSTÍ GREENBONE

Nástroj Greenbone Vulnerability Management (GVM) disponuje nasledovnými vlastnosťami, dôležitými pre tento projekt:

- **Bezplatná verzia s pravidelnými aktualizáciami**: Na rozdiel od iných nástrojov ponúka GVM aj bezplatnú verziu, ktorá dostáva pravidelné aktualizácie testov zraniteľností. Aj keď je rozsah týchto testov oproti platenej verzii limitovaný, je stále dostatočný na zabezpečenie minimálnej úrovne bezpečnosti.
- **Open source riešenie**: GVM je nástroj s otvoreným zdrojovým kódom, čo poskytuje možnosť flexibilného doplnenia jeho funkcionality v prípade potreby a aj overenie bezpečnosti tohto nástroja priamo v zdrojovom kóde, čím eliminuje riziká spojené s tzv. „blackbox" riešeniami.
- **Nasadenie on-premise**: GVM podporuje on-premise implementáciu, čím sa zaisťuje lepšia kontrola nad bezpečnostnými procesmi.
- **Bez potreby agentov**: Na rozdiel od niektorých konkurenčných nástrojov, GVM nevyžaduje inštaláciu agentov na skenovaných zariadeniach.
- **Kvalita a súlad s normami**: Nástroj pochádza z Nemecka a spĺňa požiadavky GDPR a ďalších noriem, ako napríklad ISO/IEC 27001.

Tab. 1 - Porovnanie nástrojov na skenovanie zraniteľností

Nástroj	Bezplatná verzia	Cena za licenciu bez DPH**	Open source	Agentless
Greenbone (GVM)	Áno, pravidelné aktualizácie v obmedzenom rozsahu	2450 € / rok	Áno	Áno
Nessus	Áno, limitovaná na 16 IP adries	4549 € / rok	Nie	Áno
Nexpose	Nie, len trial (30 dní)	~6000 € / rok (InsightVM)*	Nie	Áno

* Cena Nexpose nie je verejne dostupná. Uvádzaná hodnota vychádza z približnej ceny cloudového riešenia InsightVM pre 250 aktív a naznačuje, že náklady na Nexpose budú rovnaké alebo vyššie.
** Pre každý nástroja je uvedená cena najlacnejšej dostupnej licencie k dátumu 5.4.2025 a to konkrétne Greenbone BASIC a Nessus Professional.

V tomto texte budú použité názvy GVM, Greenbone, Greenbone Community Edition a OpenVAS zameniteľne. Všetky tieto názvy sú správne, pretože:

- **OpenVAS** bol pôvodný názov projektu, ktorý označoval skener zraniteľností. Teraz je to názov konkrétneho modulu v rámci širšieho riešenia.
- **Greenbone** je spoločnosť, ktorá vedie vývoj OpenVAS a pridala ďalšie komponenty, čím vzniklo komplexné riešenie.
- **GVM** (Greenbone Vulnerability Management) je názov pre celé riešenie správy zraniteľností, ktoré zahŕňa OpenVAS a ďalšie komponenty. Tento názov bude používaný najčastejšie, pretože je najkratší.
- **Greenbone Community Edition** je najnovší názov od roku 2022, ktorý zastrešuje všetky open source softvérové aktivity spoločnosti Greenbone.

1.1. Funkcie a možnosti nástroja Greenbone Vulnerability Management

GVM je robustný open source nástroj na skenovanie zraniteľností. Detailné preskúmanie jeho funkcií a možností je kľúčové pre pochopenie, ako efektívne ho môžeme implementovať v rámci SOC centra a ako výrazne dokáže posilniť úroveň kybernetickej bezpečnosti v celej infraštruktúre. Táto časť sa zameriava na podrobnú analýzu nástroja, vrátane jeho funkcionality, technických požiadaviek a architektúry, aby poskytla jasný prehľad o jeho prínose.

Funkcie GVM

Funkcionalita závisí od toho, ktorý konkrétny produkt na skenovanie zraniteľností od spoločnosti Greenbone bude vybraný. Podrobne sme analyzovali funkcie viacerých produktov, pričom k dispozícii sú 3 základné typy, ktoré sumarizujeme v tabuľke Tab. 2.

Tab. 2 - Porovnanie produktov Greenbone

Vlastnosti a funkcie	Greenbone Community Edition	Greenbone Enterprise Appliances	Greenbone Cloud Service
Systémové aktualizácie	V závislosti od distribúcie, manuálne alebo vlastná implementácia	Automatické, vrátane bezpečnostných + LTS	Automatické, vrátane bezpečnostných
Aktualizácie testov na zraniteľnosti	Community Feed	Enterprise Feed (Každodenné)	Enterprise Feed (Každodenné)
Integrované protokoly	Potrebná vlastná implementácia	NTP, GMP, OSP, HTTPS, SSH, SNMP, Syslog, IPv6, LDAP, RADIUS a ďalšie	NTP, GMP, HTTPS, SSH, SNMP, Syslog, LDAP, RADIUS a ďalšie
Integrácie a konektory	Potrebná vlastná implementácia	PaloAlto, Fortinet, Cisco FireSight, Nagios, Splunk, Verinice a ďalší	RESTful API pre všetky funkcie
Zálohovanie a Obnova	Potrebná vlastná implementácia	Používateľské a systémové údaje prostredníctvom LVM, prenos cez SCP alebo USB	Automatické
Upozornenia a plánovanie úloh (skenovanie)	Potrebná vlastná implementácia	E-mail, HTTP, SMS, konektor pre SIEM alebo ticket systém a ďalšie Kompletná podpora plánovania úloh	E-mail, Slack alebo Microsoft Teams
Architektúra skenovania	Monolitická	Master/senzor, Airgap pre vysoko zabezpečené časti siete	Cloud skener, gateway komponenty pre interné skenovanie
Remediation Tickets	Potrebná vlastná implementácia	Áno	Áno

Support	Komunitné fórum	Zaručené prostredníctvom SLA	Zaručené prostredníctvom SLA
Dáta boli získané z oficiálnej stránky Greenbone [6].			

Ako môžeme vidieť v tabuľke Tab. 2 vyššie, väčšina dodatočných funkcionalít okrem samotného skenovania sa nachádza v platených produktoch spoločnosti Greenbone a v prípade, že by sme chceli v projekte využiť bezplatnú Community Edition tak tak je potrebné akceptovať značne obmedzenú a veľmi základnú funkcionalitu, samozrejme aj s výrazným venovaním úsilia a času do údržby, prevádzky a používania tohto nástroja alebo využiť vlastné implementácie nami požadovanej funkcionality.

Podstatný rozdiel medzi touto trojicou produktov je, že „Greenbone Enterprise Appliances“ (GEA) a „Greenbone Community Edition“ sú on-premise riešenia, zatiaľ čo „Greenbone Cloud Service“ je cloudové riešenie. GEA sa ďalej delí spôsobom nasadenia na hardvérové a virtuálne riešenia. To znamená že buď si zakúpime priamo hardvérové zariadenie alebo len VM a použijeme vlastný hardvér. Od toho, ktoré riešenie si zvolíme taktiež závisí dostupná funkcionalita. Zaujímavosťou je, že pri VM nedokážeme dosiahnuť taký výkon skenovania ako je dostupný pri zakúpení hardvérového riešenia GEA. Výrobca zrejme schválne týmto spôsobom znevýhodňuje VM kvôli vyššiemu zisku z predaja hardvérových riešení.

Licenčný model tejto spoločnosti je teda založený na obmedzovaní využiteľného výkonu na samotné skenovanie zraniteľností a samozrejme aj rozličnej funkcionality ako to už býva zvykom aj pri iných výrobcoch. Čiže v praxi to znamená, že aj keď danej VM pridelíme vyšší výkon, samotná „aplikácia“ na skenovanie zraniteľností ho nebude v plnej miere využívať ale iba do úrovne, ktorú umožňuje zakúpená licencia. Detailné porovnanie jednotlivých hardvérových aj virtuálnych riešení (VM) je dostupné na oficiálnej stránke Greenbone v PDF formáte. Nachádzajú sa tam informácie, ktoré riešenie obsahuje akú funkcionalitu a aký je maximálny využiteľný výkon pri skenovaní pomocou daného riešenia, teda aké obmedzenia obsahuje. Keďže nie je hlavným cieľom projektu porovnanie jednotlivých riešení spoločnosti Greenbone a v priebehu času sa dostupné riešenia aj ich funkcionalita môže meniť a mohli by sa tak veľmi rýchlo stať neaktuálne, nebudú teda z tohto dôvodu uvádzane tieto informácie priamo v tomto texte.

Teraz sa pozrieme na samotné aktualizácie testov na zraniteľnosti, takzvané „Feed“ a aký je rozdiel medzi plateným Enterprise Feed a bezplatným Community Feed. Najskôr však vysvetlíme na čo sa dané Feed používajú a ako ovplyvňujú funkcionalitu samotného nástroja.

Treba najskôr podotknúť, že existencia samotného Common Vulnerabilities and Exposures (CVE) ešte nutne neznamená, že vieme túto zraniteľnosť pomocou tohto alebo aj ktoréhokoľvek iného nástroja odhaliť. Najskôr v prípade Greenbone ale aj ďalších nástrojov potrebujeme Common Platform Enumeration (CPE) aby sme na základe neho čo najpresnejšie identifikovali napr. aký softvér alebo služba je spustená na danej IP. CPE je štandardizovaný systém na identifikáciu softvérových aplikácií, operačného systému a hardvérových komponentov.
Po identifikácií spustenej služby, ako napr. SSH na cieľovej IP, sa môžeme presunúť už k samotným zraniteľnostiam. Na to, aby sme zraniteľnosť dokázali odhaliť s týmto nástrojom, potrebujeme ešte tzv. Network Vulnerability Test (NVT) pre príslušné CVE a až potom dokážeme túto zraniteľnosť odhaliť. V jednoduchosti platí, že čím viac testov na zraniteľnosti máme, tým viac zraniteľností dokáže nástroj odhaliť. Pre názornosť o rozdieloch medzi Community a Enterprise Feed, uvádzame čísla v nasledujúcej prehľadnej tabuľke Tab. 3.

Tab. 3 - Porovnanie Greenbone Feed - číselné

	Community Feed	Enterprise Feed
CVE	288 463	288 463
CPE	1 387 760	1 387 760
NVT	159 122	203 717
CERT-Bund Advisories	23 067	23 067
DFN-CERT Advisories	37 318	37 318
Dáta sú aktuálne k dátumu 5.4.2025. Získané boli z inštalácie Greenbone Cummunity Edition a SecInfo portálu. [9]		

Ako sme si mohli všimnúť v tabuľke Tab. 3 vyššie, čo sa týka samotného skenovania zraniteľností rozdiel je naozaj predovšetkým v počte NVT, ktorý sa môže na prvý pohľad zdať ako nie až tak výrazný. Ale pravdou je, že v Greenbone si dali záležať a z Community Feed vybrali práve tie najpodstatnejšie testy na zraniteľnosti ako môžeme vidieť aj v tabuľke Tab. 4 nižšie a týkajú sa teda produktov určených práve pre podniky. Z tohto pohľadu majú vysokú hodnotu pre zlepšovanie úrovne zabezpečenia podnikovej siete, čím prispievajú k efektívnej ochrane pred potenciálnymi hrozbami.

Tab. 4 - Porovnanie Greenbone Feed funkcionality

	Community Feed	Enterprise Feed
Produkty určené na domáce použitie (napr. Ubuntu Linux, TP-Link, MS Office)	✓	✓
Nemecká bezpečnostná politika IT-Grundschutz	✓	✓
Produkty určené pre podniky (napr. MS Exchange, Palo Alto, Cisco, IoT/OT)	✗	✓
Politiky súladu s CIS normami*	✗	✓
Dodatočné politiky súladu**	✗	✓
Prístup k podpore Greenbone Enterprise	✗	✓
Prístup k expertným službám	✗	✓
*Obsahuje 23 politík. **Obsahuje 5 politík (BSI TR-02102-4, BSI TR-03116, MS Win Registry Check, SiSyPHuS Win10, Win 10 ver 1809 Security Hardening). Dáta boli získané z inštalácie GEA a z oficiálneho webu. [8]		

Okrem už spomínaných NVT sa tu nachádzajú naviac ešte politiky súladu s rôznymi normami, ale hlavne sa jedná o Center for Internet Security (CIS), ktorých sa tu k dátumu 26.3.2025 nachádza 23. Jedná sa síce o americké normy, avšak sú využívané a uznávané aj v iných častiach sveta, pretože bezpečnostné požiadavky sú všade takmer totožné až na drobné legislatívne zmeny. Čo sa týka dodatočných politík súlad, môžeme tu nájsť nemecké Bundesamt für Sicherheit in der Informationstechnik (BSI), ktoré sú veľmi dôkladné a vychádza sa z nich aj pri tvorbe iných noriem ako napr. CIS. Ďalej sa tu nachádzajú politiky súladu pre OS Windows 10. Tieto politiky môžu byť taktiež veľmi cenné najmä pre podniky, ktoré z rôznych dôvodov musia byť v súlade, alebo chcú udržiavať kybernetickú bezpečnosť na vysokej úrovni. Okrem zjednodušene povedané dodatočnej funkcionality je v cene Enterprise Feed zahrnutá aj technická podpora k produktom GEA s výnimkou najnovšieho produktu z portfólia s názvom Greenbone BASIC, kde je v Enterprise Feed zahrnuté všetko okrem technickej podpory.

Okrem rozdielu v aktualizáciách Feed v prípade GEA, vrátane Greenbone BASIC a aj pri Greenbone Free môže byť na zváženie aj verzia Greenbone OS (GOS). Aktuálne dostupné verzie a ich podporu produktov si môžeme pozrieť v prehľadnej tabuľke Tab. 5 nižšie.

Tab. 5 - GOS verzie

Verzia OS	GEA, Greenbone BASIC	Greenbone Free
GOS 22.04	✓	✓
GOS 24.10	✓	✗

Ako sme si mohli všimnúť, najnovšia verzia nie je aktuálne dostupná iba v prípade bezplatného produktu Greenbone Free, avšak v budúcnosti bude dostupná aj v tejto bezplatnej verzií na základe informácií na oficiálnom webe Greenbone. Keďže End of Life (EOL) GOS verzie 22.04 nastane 1.2.2026, tak zrejme najneskôr v tomto dátume dostane novú verziu GOS 24.10 aj produkt Greenbone Free.

Pre komplexný prehľad, uvedieme analýzu aký rozdiel je vo funkcionalite týchto dvoch verzií. Na úvod treba povedať, že vo verzií 24.10 pribudla funkcionalita naviac. Tým, že sa aktualizovali jednotlivé komponenty a systémové balíčky sa nebudeme zaoberať a uvedieme len podstatné zmeny:

1. **Pridaná podpora Exploit Prediction Scoring System (EPSS)**

   EPSS poskytuje ďalšie skóre pre nájdené zraniteľnosti okrem už známeho CVSS, pre ešte efektívnejšiu prioritizáciu. Toto skóre sa zakladá na pravdepodobnosti zneužitia zraniteľnosti v najbližších 30 dňoch v reálnom svete na základe rôznych dát. EPSS bolo vyvinuté organizáciou FIRST a je bezplatné. Greenbone spravil len jeho implementáciu do svojho riešenia.

2. **Nový vzhľad webového rozhrania**

   Hlavné menu sa z hornej časti premiestnilo vertikálne na ľavú stranu obrazovky, čo zlepšuje orientáciu a okrem toho bola zmenená farebná schéma. Vďaka tomuto novému vzhľadu pôsobí celé webové rozhranie modernejšie a viac používateľsky prívetivejšie.

3. **Pridaná podpora CVSS v4.0**
4. **Pridané konfigurovateľné formáty reportov**

   Formáty umožňujú prispôsobiť reporty ako napríklad v CSV formáte, kde sa dajú meniť zahrnuté stĺpce vo výstupe, čo robí report prehľadnejší.

5. **Notus Scanner bol nahradený openvasd**

   Pre zvýšenie rýchlosti vykonávania LSC počas skenovania zraniteľností.

6. **Pridaná podpora Secure Boot**
7. **Pridaná možnosť konfigurácie bezpečnostných parametrov SSH**
8. **Vylepšená rýchlosť aktualizácie Feed**

1.2. Možnosti nasadenia

V závislosti od toho, či sme sa rozhodli používať bezplatnú Greenbone Community Edition alebo platenú GEA, máme k dispozícií rozličné možnosti nasadenia.

1.2.1. Greenbone Community Edition:

1. **Kompilácia zo zdrojového kódu**

Jedná sa o najkomplexnejší spôsob nasadenia, ktorý si vyžaduje pokročilé technické znalosti ako znalosť kompilácie komplexného zdrojové kódu v programovacom jazyku C, znalosť CMake, make, pokročilú znalosť OS Linux, jeho súborovej štruktúry a skriptovania.

2. **Docker**

Trochu jednoduchšie oproti prvej možnosti, ale stále dosť komplexný spôsob nasadenia. Hlavne z pohľadu udržateľnosti. Je vyžadovaná pokročilá znalosť Docker, Docker Compose a OS Linux.

3. **Inštalácia z Kali Linux repozitára**

Pre túto možnosť je potrebná pokročilá znalosť OS Linux, kvôli riešeniu častých problémov s touto možnosťou nasadenia. Nevýhodou je, že sa v repozitároch Kali Linux nenachádza aktuálna verzie tohto nástroja a vždy sa jedná o trochu staršiu verziu, pretože tento balíček neudržiava spoločnosť Greenbone, ale spoločnosť Offensive Security, ktorá udržiava OS Kali Linux. Navyše, nástroj je predinštalovaný a podporovaný v jednej verzii OS Kali Linux, ale v ďalšej už nie, a potom opäť áno, a teda nejedná sa o kontinuálne podporovaný typ nasadenia. Pokiaľ chceme využívať len nástroj GVM na skenovanie, tak to nie je vhodné riešenie, pretože sa tu nachádza mnoho nástrojov naviac, vrátane GUI operačného systému, ktoré spotrebúvajú zbytočné hardvérové zdroje naviac. Okrem toho sú dané nástroje naviac vnímané za potencionálne vysoké bezpečnostné riziko v prípade kompromitácie takéhoto stroja, za predpokladu že by bežal nepretržite. Potencionálny útočník by to mal značne zjednodušené, keďže by nemusel riešiť ako dostane tieto útočné nástroje do lokálnej siete cez bezpečnostné riešenia. Takéto nasadenie je vhodné len na občasné manuálne použitie v rámci testovania.

4. **Komunitné repozitáre pre Linux**

Existujú aj mnohé komunitné repozitáre s týmto nástrojom ako napr. od Mohammad Razavi [10], ktoré stačí doinštalovať do manažéra balíčkov ako napr. APT a vieme si ho tak jednoduchšie nainštalovať. Avšak tieto repozitáre nikto nekontroluje a ich bezpečnosť je veľmi otázna a to nielen z hľadiska, že by potencionálny aktér hrozby mohol schválne vytvoriť repozitár, kde bude k tomu nástroju pribalený aj škodlivý kód, ale aj z dôvodu nedodržiavania osvedčených bezpečnostných postupov a využívania starších verzií SW pri vytváraní takéhoto balíčka, respektíve inštalátor pre tento nástroj. Zároveň je tu taktiež ako v prípade Kali Linux distribúcie problém s aktuálnosťou verzie tohto nástroja. Pri distribúcií na Kali Linux je verzia Greenbone ešte použiteľná, ale pri komunitných repozitároch býva často skôr historická. Na základe tohto usudzujem, že tento variant nie je vhodný pre použitie na akékoľvek účely, pretože môže spôsobiť viac bezpečnostných rizík ako ich odstrániť.

5. **Predpripravená VM**

Ide síce o málo známy spôsob nasadenia, ale asi najelegantnejší oficiálne podporovaný spôsob nasadenia tohto nástroja. Predpripravená VM s názvom Greenbone Free je podobná ako platené riešenie GEA. Jedná sa vlastne o jeho TRIAL verziu s obmedzenou funkcionalitou a Community Feed. Tento spôsob odstraňuje takmer všetky nedostatky predchádzajúcich možností nasadenia a pre úspešné nasadenie postačuje znalosť konfigurácie VM, respektíve hypervízora, ako napríklad VMware.

1.2.2. Greenbone Enterprise Appliance:

1. **Hardvérové zariadenie**

Tieto hardvérové zariadenia obsahujú predinštalovaný nástroj GEA a poskytujú vysokú úroveň bezpečnosti a výkonu. Vysoký výkon však nie je úplne spôsobený extra optimalizovaným hardvérom, ale skôr obchodnou politikou Greenbone, keďže pri nasadení pomocou VM obmedzuje využiteľný výkon hardvéru pri skenovaní. Pre toto nasadenie nie sú potrebné technické znalosti týkajúce sa konfigurácie hypervízora, čo môže byť praktické pre organizácie s obmedzenými IT zdrojmi alebo v prípade že sa nechceme starať o hardvér, ale stále chceme mať riešenie on-premise. V cene je zahrnutá aj bezplatná výmena hardvéru v prípade poruchy.

2. **Predpripravená VM**

Podobne ako v prípade Greenbone Free (pre Community Edition), aj GEA ponúka predpripravenú VM, ktorá poskytuje jednoduchú a bezpečnú možnosť nasadenia. Predpripravená VM umožňuje rýchle nasadenie bez potreby pokročilých technických znalostí, pretože všetky potrebné konfigurácie už sú súčasťou obrazu VM. Postačuje taktiež ako pri Greenbone Free iba znalosť konfigurácie VM, respektíve hypervízora. Táto možnosť je vhodná v prípade, že chceme použiť vlastný hardvér.

3. **SaaS (Cloud)**

Ide o ten istý nástroj GEA, ale dostupný formou služby v cloud. Nasadenie prostredníctvom SaaS eliminuje požiadavky na lokálnu inštaláciu a údržbu, čo môže byť praktické najmä pre organizácie s limitovanými IT zdrojmi. Zároveň umožňuje jednoduchý prístup k nástroju z rôznych miest, pričom aktualizácie Feed aj samotného softvéru sú plne v réžii Greenbone. Táto možnosť však vyžaduje dôveru v poskytovateľa. Toto riešenie je však plne v súlade s GDPR a prevádzkované v Nemecku, čo zaručuje dodržiavanie ochrany údajov. Pre skenovanie neverejných sietí je možné si stiahnuť gateway a nainštalovať ho tam, kde je skenovanie potrebné. Jedná sa o obdobnú funkcionalitu ako master-senzor v on-premise produktoch Greenbone. Licenčný model je postavený na počte rezervovaných IP adries určených na skenovanie, od čoho sa odvíja výsledná cena. Pre skenovanie nad 250 IP adries je možné dohodnúť individuálnu cenovú ponuku po kontakte s obchodným tímom.

Architektúra a technické požiadavky

Samozrejme aj v tejto časti rovnako ako v predchádzajúcich závisí od toho, či sme zvolili Greenbone Community Edition (GCE) alebo GEA. Tieto dve možnosti bližšie rozoberáme preto, že boli vybraté ako dve potenciálne riešenia pre nasadenie na KIS FRI UNIZA. Ako zdroj informácií pre túto časť boli použité oficiálne dokumentácie pre obidva produkty, čiže pre GEA aj GCE, keďže každý produkt disponuje vlastnou dokumentáciou.

1.2.3. Greenbone Community Edition

Architektúra tohto produktu pozostáva z nasledujúcich hlavných častí:

1. **Skenovacie aplikácie** (Notus Scanner a OpenVAS Scanner) vykonávajú testy zraniteľností (VT) na cieľových systémoch.
   - **OpenVAS Scanner** je hlavný skener, ktorý na detailné skenovanie zraniteľností používa pravidelne aktualizované databázy (Greenbone Community Feed alebo platený Greenbone Enterprise Feed). Tento skener je ovládaný ďalším komponentom prostredníctvom Open Scanner Protocol (OSP).
   - **Notus Scanner** je doplnkový skener, ktorý optimalizuje výkon a znižuje spotrebu systémových zdrojov porovnávaním zoznamu nainštalovaného softvéru so známymi zraniteľnými verziami. Tým eliminuje potrebu vykonávania individuálnych tzv. NASL-based local security checks (LSC) a vykoná teda toto porovnanie naraz.

2. **Greenbone Vulnerability Management Daemon** (gvmd): Je centrálny prvok, ktorý robí z obyčajného skenovania zraniteľností komplexné riešenie pre manažment zraniteľností. Démon komunikuje s OpenVAS Scanner komponentom prostredníctvom OSP. Ďalej spravuje PostgreSQL databázu pre konfigurácie a výsledky skenovania. Taktiež spravuje používateľov, skupiny, ich role a oprávnenia v rámci tohto nástroja. Spravuje aj plánované úlohy ako napr. pravidelné skenovania. Obsluhovať tento komponent môžeme pomocou Greenbone Management Protocol (GMP) API, ktorý je založený na XML.
3.
3. **Greenbone Security Assistant** (GSA): Je webové rozhranie, ktoré umožňuje používateľovi jednoducho ovládať skenovanie a pristupovať k výsledkom bez nutnosti používať API. Komunikácia tohto komponentu s gvmd je realizovaná prostredníctvom komponentu **Greenbone Security Assistant Daemon** (gsad) a protokolu GMP.

Samotnú architektúru môžeme vidieť na obrázku. Ešte je dôležité podotknúť, že jedinou výnimkou v tomto prípade je Greenbone Free, ktorý využíva architektúru GEA, ktorá je popísaná na nasledujúcej strane.

Minimálne technické požiadavky:

- CPU/vCPU jadrá: 2
- RAM: 4 GB
- HDD: 20 GB

Odporúčané technické požiadavky:

- CPU/vCPU jadrá: 4
- RAM: 8 GB
- HDD: 60 GB

Keď sú splnené minimálne technické požiadavky, tak v praxi to znamená, že sa nám úspešné podarí spustiť nástroj a môžeme s ním skenovať približne 1 zariadenie súčasne rozumnou rýchlosťou, pri zohľadnení toho, že nechceme čakať na výsledok skenovania nadmerne dlho (niekoľko hodín). Pokiaľ nám však nevadí si počkať na výsledok skenovania dlhšie (niekoľko hodín) alebo chceme tento nástroj použiť len na domáce použitie, pri malom počte zariadení a nemáme k dispozícii výkonnejší hardvér, je to skvelá voľba. Ak už však máme záujem používať toto riešenie s väčším počtom skenovaných zariadení, respektíve IP adries (cca nad 20), tak je vhodnejšie najmä kvôli rýchlosti skenovania zvoliť aspoň odporúčané technické požiadavky. S rastúcim počtom skenovaných IP teda stúpajú aj nároky na hardvér a najlepšou

možnosťou ako sa inšpirovať aký výkon je vhodný práve pre naše nasadenie je oficiálna dokumentácia Greenbone pre GEA.

1.2.4. Greenbone Enterprise Appliance

Architektúra tohto produktu je postavená na operačnom systéme Greenbone Operating System (GOS), čo je vlastne upravená verzia Debian Linux distribúcie, ktorý poskytuje jednoduché a efektívne ovládanie prostredníctvom používateľsky prívetivého menu založeného na Text-based user interface (TUI), ktoré môžeme vidieť na obrázku

GOS umožňuje konfiguráciu, spúšťanie a zastavovanie všetkých služieb. Prístup do systémovej úrovne je obmedzený a vyžaduje konzolový prístup (serial, hypervízor, monitor/klávesnica) alebo SSH. GEA zahŕňa aj podporu pre master-sensor model, kde master server komunikuje so senzormi prostredníctvom šifrovanej autentifikácie cez SSH. Ovládanie senzora, čo sa týka napr. spustenia skenovania a získania výsledkov, prebieha cez API Open Scanner Protocol (OSP) a celá táto komunikácia je zabalená do šifrovaného SSH tunela. Rovnako ako sa aktualizuje Feed na hlavnej jednotke master, tak je potrebné aktualizovať tento Feed aj na senzore, ktorý si stiahne tieto dáta priamo z jednotky master pomocou rsync a celá komunikácia je takisto zabalená do šifrovaného SSH tunela.

Okrem toho GEA samozrejme obsahuje aj tie isté komponenty čo GCE, len s tým rozdielom, že tento produkt má pár vecí naviac. Nejedná sa pritom väčšinou o príliš revolučnú funkcionalitu, avšak v tejto platenej verzií sa nachádza už predinštalovaná a predkonfigurovaná bez zbytočnej námahy a nutnosti technických znalostí. Okrem DNS, SSH a DHCP, ktoré sú zabudované aj v bezplatnej verzií, samozrejme v závislosti od zvolenej distribúcie, sa všetky ostatné nachádzajú len v platenej verzií a komunikácia prebieha na nasledujúcich portoch. Môžeme na ňom vidieť napríklad integráciu s Cisco FirePower alebo Verinice.PRO, ďalej e-mail pre doručovanie upozornení a výsledkov skenovania a mnohé ďalšie.

Architektúra GEA, ktorá je veľmi podobná ako pri GCE, avšak je tu pridaný GOS (vpravo), v ktorom sa nachádza GOS Administration a GOS Control Layer, ktoré značne zjednodušujú správu a používanie celého nástroja. Ďalším prídavkom je MQTT Broker, ktorý podľa obrázka architektúry GCE v dokumentácií nie je súčasťou GCE. Avšak dôvod jeho nezahrnutia v GCE nie je jasný, ale z najväčšou pravdepodobnosťou ide len o otázku neaktuálnej dokumentácie a nachádza sa tak rovnako v obidvoch produktoch o čom svedčí aj existencia kontajnera MQTT Broker pre Community Edition na DockerHub. Pre naše potreby však nie sú až takéto hlboké detaily interných komponentov podstatné. Prioritu má predovšetkým API rozhranie (GMP), webové rozhranie a GOS Administrácia, keďže tieto komponenty slúžia ako hlavné komunikačné body so systémom.

Minimálne technické požiadavky pre VM:

- vCPU jadrá: 2
- RAM: 12 GB
- HDD: 500 GB

Technické požiadavky sa líšia podľa toho, ktorú licenciu, respektíve verziu produktu si konkrétne zakúpime. Prehľad týchto požiadaviek pre všetky GEA produkty je možné nájsť v prehľadnej tabuľke v PDF na oficiálnom webovom sídle Greenbone . Od výkonu samozrejme závisí aj počet IP, ktoré dokáže za jeden deň tento nástroj skenovať a tento odhad je taktiež zahrnutý v spomínanom dokumente.

Funkcie, licenčný model tejto spoločnosti je teda založený na obmedzovaní využiteľného výkonu na samotné skenovanie zraniteľností. To v praxi znamená, že aj keby sme VM pridelili vyšší výkon ako je uvedený v tabuľke pre príslušnú licenciu, respektíve verziu, nebude ho pri skenovaní reálne využívať.

Výhody a nevýhody

Výhody:

- **Bezplatná verzia s pravidelnými aktualizáciami:** GVM ponúka bezplatnú verziu s pravidelnými aktualizáciami testov zraniteľností, čo je výhodné pre menšie organizácie s obmedzeným rozpočtom.
- **Open source riešenie:** Možnosť flexibilného doplnenia funkcionality a overenie bezpečnosti priamo v zdrojovom kóde.
- **On-premise nasadenie:** Zaisťuje lepšiu kontrolu nad bezpečnostnými procesmi a dátami.
- **Bez potreby agentov:** Zjednodušuje nasadenie a znižuje nároky na správu skenovaných zariadení.
- **Súlad s normami:** Spĺňa požiadavky GDPR a ďalších noriem, čo zvyšuje dôveryhodnosť a bezpečnosť riešenia.

Nevýhody:

- **Obmedzená funkcionalita bezplatnej verzie:** Bezplatná verzia má obmedzený rozsah testov zraniteľností a vyžaduje viac úsilia na údržbu a prevádzku.
- **Výkonnostné obmedzenia:** Virtuálne riešenia nedosahujú rovnaký výkon ako hardvérové riešenia, čo môže byť limitujúce pre väčšie nasadenia.
- **Komplexnosť nasadenia:** Niektoré možnosti nasadenia, ako kompilácia zo zdrojového kódu alebo použitie Docker, vyžadujú pokročilé technické znalosti.
- **Licenčný model:** Obmedzuje využiteľný výkon a funkcionalitu na základe zakúpenej licencie, čo môže byť nevýhodné pre organizácie s vyššími požiadavkami.

1.3. Zhrnutie

Na základe analýzy nástroja GVM môžeme konštatovať, že ide o robustné a flexibilné riešenie pre skenovanie zraniteľností, ktoré je vhodné viaceré podnikové prostredia. Jeho hlavnými výhodami sú bezplatná verzia s pravidelnými aktualizáciami, open source charakter a možnosť on-premise nasadenia. Na druhej strane, obmedzená funkcionalita bezplatnej verzie a výkonnostné obmedzenia VM môžu predstavovať výzvy pre niektoré väčšie organizácie. Celkovo však GVM ponúka spoľahlivé a bezpečné riešenie pre manažment zraniteľností, ktoré môže výrazne prispieť k zlepšeniu úrovne kybernetickej bezpečnosti.

ZOZNAM ZDROJOV

1. **Check Point Software Technologies Ltd..** *Check Point Software's 2025 Security Report Finds Alarming 44% Increase in Cyber-Attacks Amid Maturing Cyber Threat Ecosystem.* [online]. 17.2.2025 Dostupné na internete: < https://www.checkpoint.com/press-releases/check-point-softwares-2025-security-report-finds-alarming-44-increase-in-cyber-attacks-amid-maturing-cyber-threat-ecosystem/>
2. **Tlačová agentúra Slovenskej republiky.** *SIS Won't Comment on Cyber-attack on Land-Registry Office, It's Live Case.* [online]. 17.2.2025. Dostupné na internete: < https://www.tasr.sk/tasr-clanok/TASR:2025011000000195>
3. **Tlačová agentúra Slovenskej republiky.** *M.Chren: Ani po mnohých dňoch nefunguje kataster naplno,odráža sa to na službách.* [online]. 17.2.2025. Dostupné na internete: <https://www.tasr.sk/tasr-clanok/TASR:2025020600000155>
4. **Národný bezpečnostný úrad.** *Varovanie pred zvýšeným rizikom kybernetických bezpečnostných útokov.* [online]. 17.2.2025. Dostupné na internete: <https://www.nbu.gov.sk/28493-sk/varovanie-pred-zvysenym-rizikom-kybernetickych-bezpecnostnych-utokov/>
5. **Greenbone AG,** *Greenbone, GVM, OpenVAS and How They Are Connected.* [online]. 3.4.2025. Dostupné na internete: <https://greenbone.github.io/docs/latest/background.html#greenbone-gvm-openvas-and-how-they-are-connected>
6. **Greenbone AG,** *Product Comparison.* [online]. 3.4.2025. Dostupné na internete: <https://www.greenbone.net/en/product-comparison/>
7. **Greenbone AG,** *Product Overview of the Different Solutions.* [online]. 3.4.2025. Dostupné na internete: <https://www.greenbone.net/wp-content/uploads/solution_overview_en.pdf >
8. **Greenbone AG,** *Feed Comparison.* [online]. 3.4.2025. Dostupné na internete: <https://www.greenbone.net/en/feed-comparison/>
9. **Greenbone AG,** *SecInfo Portal.* [online]. 5.4.2025. Dostupné na internete: <https://www.greenbone.net/en/secinfo-portal/>
10. **Mohammad Razavi,** *Greenbone Vulnerability Management.* [online]. 5.4.2025. Dostupné na internete: <https://launchpad.net/~mrazavi/+archive/ubuntu/gvm>
11. **Greenbone AG,** *18 Architecture.* [online]. 5.4.2025. Dostupné na internete: <https://docs.greenbone.net/GSM-Manual/gos-22.04/en/architecture.html>
12. **Greenbone AG,** *Architecture.* [online]. 5.4.2025. Dostupné na internete: <https://greenbone.github.io/docs/latest/architecture.html>
13. **greenbone,** *greenbone/mqtt-broker.* [online]. 5.4.2025. Dostupné na internete: <https://hub.docker.com/r/greenbone/mqtt-broker>
14. **Greenbone AG,** *Roadmap & Lifecycle.* [online]. 6.4.2025. Dostupné na internete: <https://www.greenbone.net/en/roadmap-lifecycle/>
15. **Greenbone AG,** *4 Setting up the Greenbone Enterprise Appliance.* [online]. 6.4.2025. Dostupné na internete: <https://docs.greenbone.net/GSM-Manual/gos-22.04/en/setting-up-the-appliance.html#setup-requirements>
16. **U.S. Department of Homeland Security,** *Use Strong Passwords.* [online]. 8.4.2025. Dostupné na internete: <https://www.cisa.gov/secure-our-world/use-strong-passwords>

17. **Greenbone AG,** *Greenbone Free.* [online]. 8.4.2025. Dostupné na internete: <https://www.greenbone.net/en/greenbone-free/#toggle-id-4>
18. **Greenbone AG,** *10 Reports and Vulnerability Management.* [online]. 8.4.2025. Dostupné na internete: <https://docs.greenbone.net/GSM-Manual/gos-24.10/en/reports.html>
19. **Greenbone AG,** *11 Performing Compliance Scans and Special Scans.* [online]. 8.4.2025. Dostupné na internete: <https://docs.greenbone.net/GSM-Manual/gos-24.10/en/compliance-and-special-scans.html>
20. **Greenbone AG,** *8.5 Using a Central User Management.* [online]. 8.4.2025. Dostupné na internete: <https://docs.greenbone.net/GSM-Manual/gos-24.10/en/web-interface-access.html#using-a-central-user-management>
21. **Greenbone AG,** *9 Scanning a System.* [online]. 9.4.2025. Dostupné na internete: <https://docs.greenbone.net/GSM-Manual/gos-24.10/en/scanning.html>
22. **Komunita,** *GVM Example Scripts.* [online]. 9.4.2025. Dostupné na internete: <https://github.com/greenbone/gvm-tools/blob/main/scripts/README.md>
23. **Greenbone AG,** *14 Using the Greenbone Management Protocol.* [online]. 9.4.2025. Dostupné na internete: <https://docs.greenbone.net/GSM-Manual/gos-24.10/en/gmp.html>