Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

Bezpečnostné opatrenia – test zraniteľností

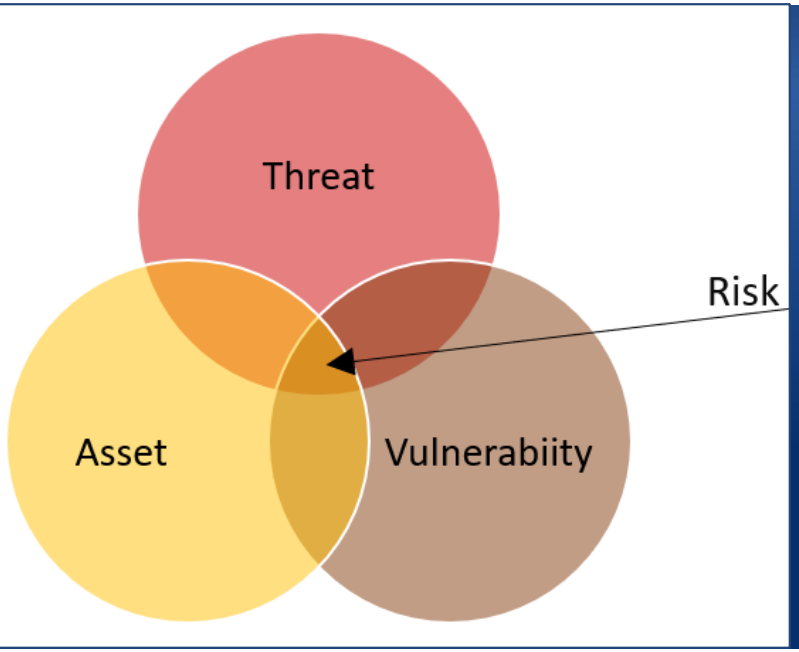
Bezpečnostné riziká, opatrenia a prevencia (Blok II)

Kurz: Odborný zamestnanec (laik) kybernetickej bezpečnosti

Mgr. Jana Uramová, PhD.

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

Jana.Uramova@fri.uniza.sk

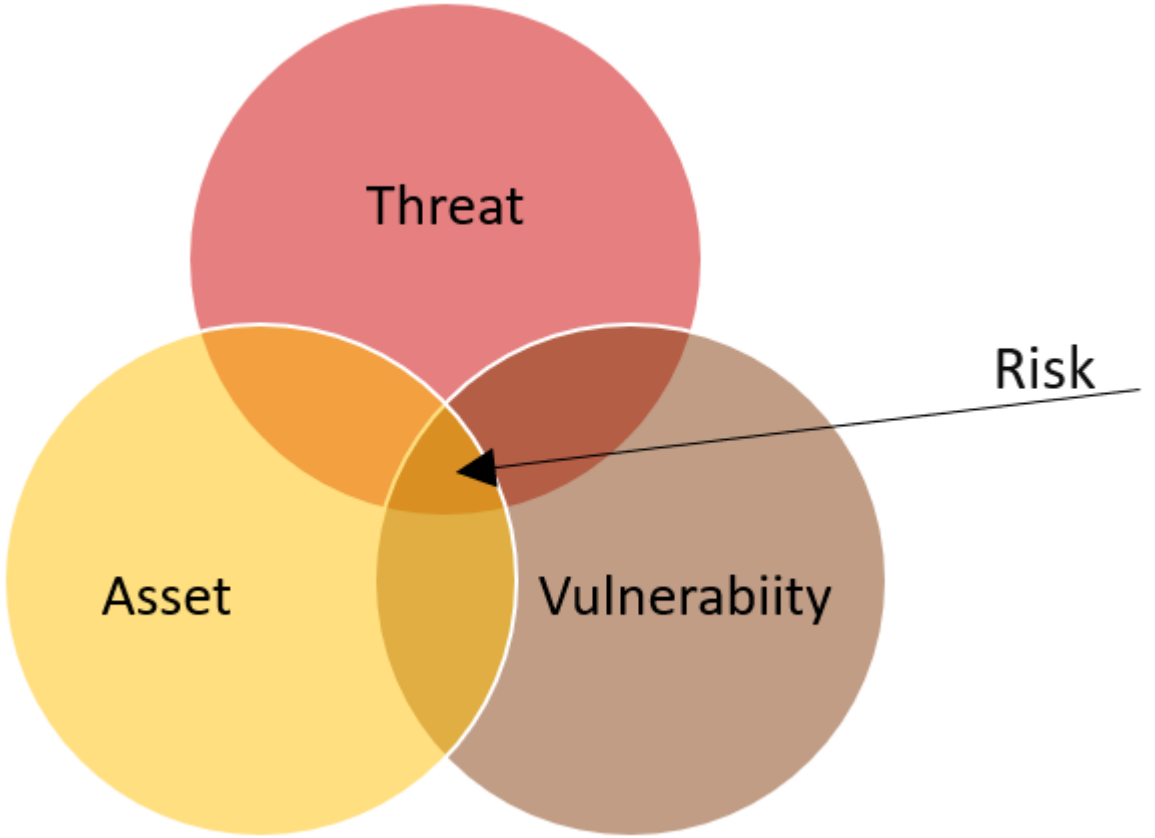


Nadviazanie na predošlé témy

Nadviazanie na predošlé témy

Aktíva, zraniteľnosti, hrozby

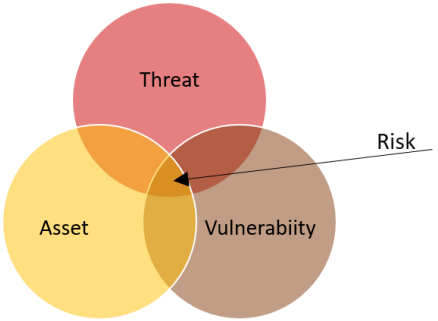
- Analytici KB musia byť pripravení na akýkoľvek typ útoku
  - ich úlohou je zabezpečiť aktíva siete organizácie.
- Na tento účel musia analytici kybernetickej bezpečnosti najprv identifikovať:
  - **Aktíva (assets)** - Všetko, čo má pre organizáciu hodnotu a musí byť chránené, vrátane serverov, infraštruktúrnych zariadení, koncových zariadení a najväčšieho aktíva – údajov a iného duševného vlastníctva
  - **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

Nadviazanie na predošlé témy

Hrozba, zraniteľnosť a riziko (Pokr.)



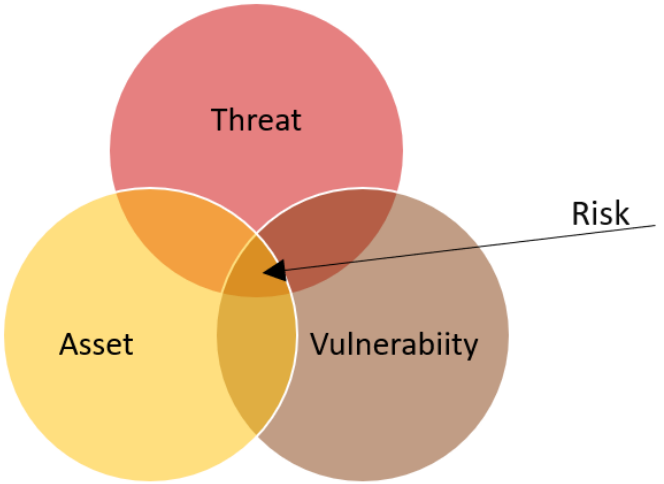
- Na pochopenie bezpečnosti siete je dôležité poznať nasledujúce pojmy:

Pojem	Vysvetlenie
Threat	**Potenciálne nebezpečenstvo** pre **aktívum** (údaje alebo samotnú sieť).
Vulnerability	**Slabé miesto** v systéme alebo jeho dizajne, ktoré môže byť **zneužité** hrozbou.
Attack Surface	**Celkový súčet zraniteľností** v danom systéme, ktoré sú prístupné útočníkovi. **Opisuje rôzne miesta**, kde by sa útočník mohol dostať do systému a kde by mohol získať údaje zo systému.
Exploit	**Mechanizmus**, ktorý sa používa na **využitie zraniteľnosti** s cieľom kompromitovať aktívum. Zneužitia môžu byť **REMOTE** alebo **LOCAL**. **Vzdialené** zneužitie je také, ktoré funguje cez sieť bez predchádzajúceho prístupu k cieľovému systému. Pri **lokálnom** zneužití má aktér hrozby určitý typ používateľského alebo administratívneho prístupu ku koncovému systému. Nemusí to nevyhnutne znamenať, že útočník má fyzický prístup ku koncovému systému.
Risk	**Pravdepodobnosť**, že konkrétna hrozba zneužije určitú zraniteľnosť aktíva a spôsobí nežiaduci následok.

Nadviazanie na predošlé témy

Identifikácia aktív

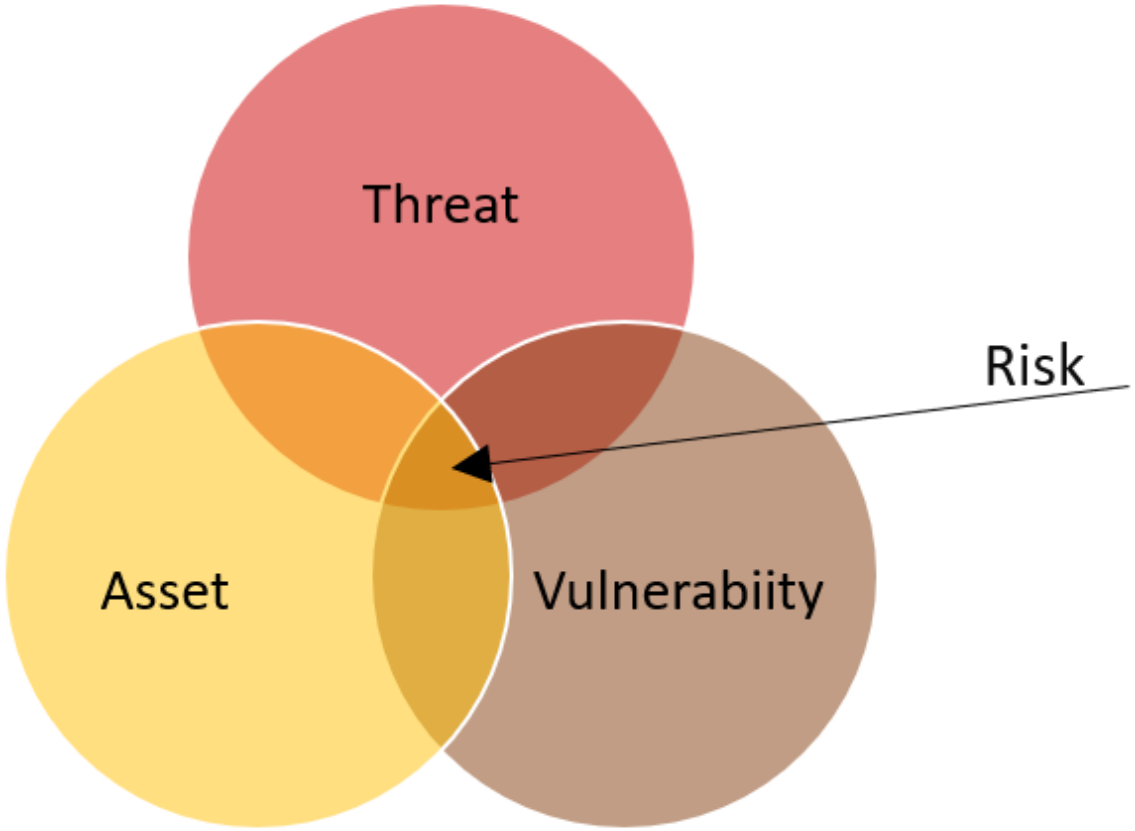
- Aktíva = súbor všetkých **zariadení** a **informácií**, ktoré organizácia vlastní alebo spravuje
- Správa aktív pozostáva z:
  - **inventarizácie** všetkých aktív
  - **posúdenia** z hľadiska úrovne ochrany potrebnej na prekazenie potenciálnych útokov
  - **vypracovania a zavedenia politík** a **postupov** na ich ochranu.
- Táto úloha môže byť náročná, keďže mnohé organizácie musia chrániť:
  - **interných** používateľov a zdroje,
  - **mobilných** pracovníkov
  - **cloudové** a virtuálne služby.
- Okrem toho musia organizácie určiť:
  - **kde** sú uložené kritické informačné aktíva
  - **ako** sa k nim získava prístup
- Informačné aktíva sa **líšia**, rovnako ako hrozby voči nim.
  - každé z týchto aktív môže prilákať **rôznych útočníkov**,
  - ktorí majú **rôzne úrovne zručností a motivácie**.



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

Identifikácia zraniteľností a hrozieb

- Identifikácia hrozieb poskytuje organizácii **zoznam možných hrozieb** pre konkrétne prostredie.
- Pri identifikácii hrozieb je dôležité položiť si niekoľko otázok:
  - **Aké** sú **možné** zraniteľnosti systému?
  - **Kto** môže chcieť tieto zraniteľnosti **zneužiť** na prístup ku konkrétnym informačným aktívam?
  - Aké sú **dôsledky (impact)**, ak sa zraniteľnosti systému zneužijú a aktíva sa stratia?



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

Prečo je testovanie zraniteľností dôležité

... súčasť bezpečnostných opatrení

Prečo je manažovanie zraniteľností dôležité

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 188 049 záznamov CVE (5.11.2022), ktoré je možné vyhľadať a stiahnuť

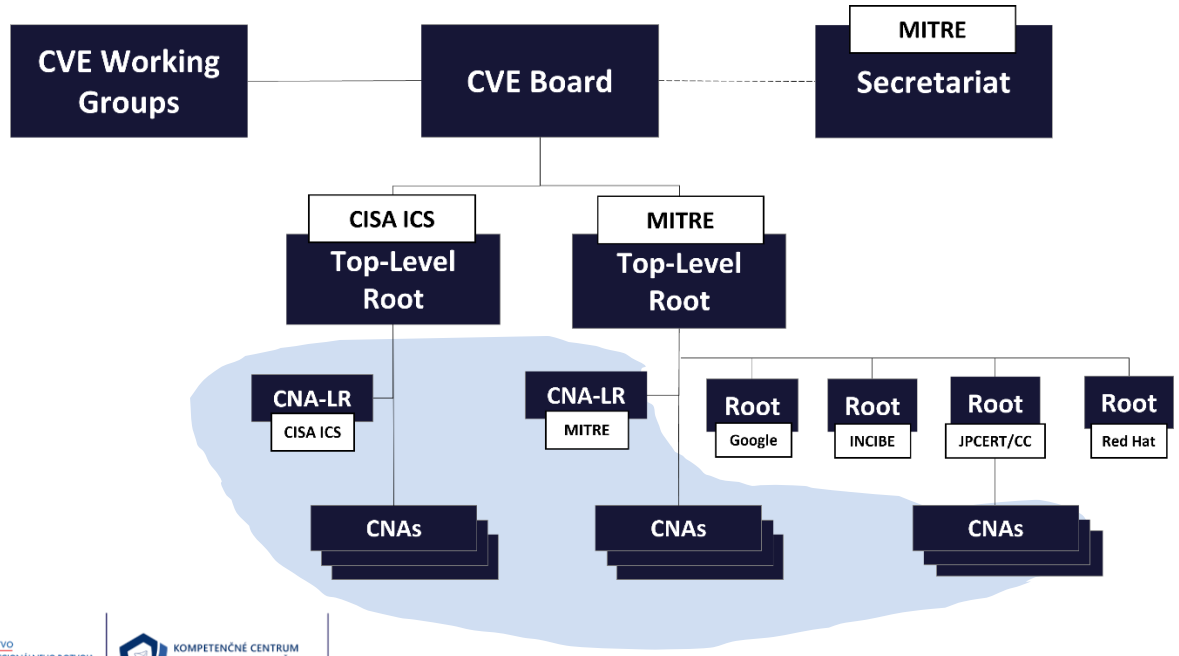
Root – **manažérske** funkcie

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

Každý CVE záznam obsahuje:

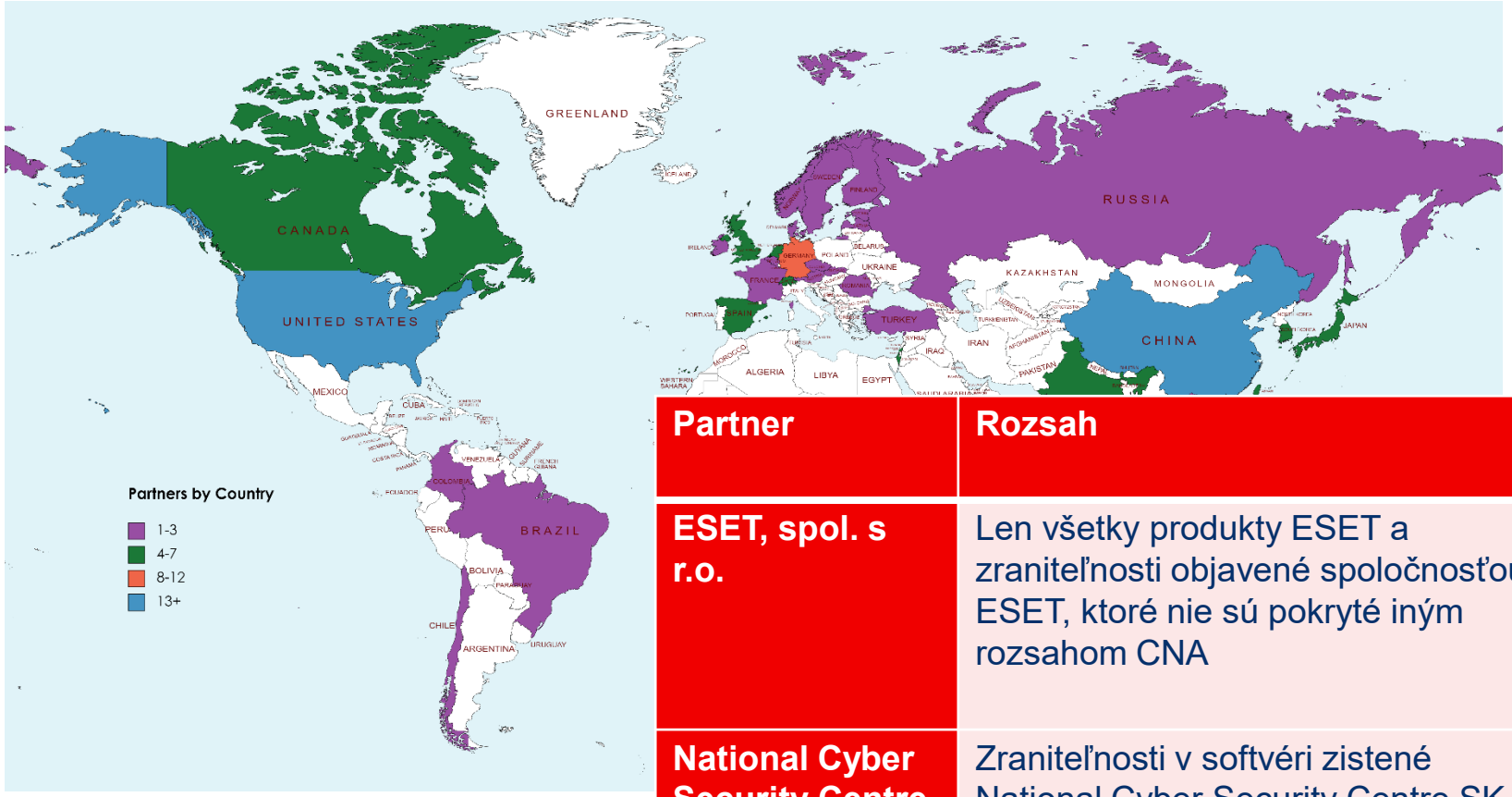
- CVE ID číslo so štyrmi alebo viacerými číslicami v časti poradového čísla daného ID (napr. „CVE-1999-0067“, „CVE-2014-12345“, „CVE-2016-7654321“).
- Stručný popis chyby zabezpečenia
- Akékoľvek relevantné referencie (t. j. správy o zraniteľnosti a upozornenia).
- Stav: Rezervované/Zverejnené/Odmietnuté

https://www.cve.org/



Viac ako **251** 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

Prečo je manažovanie zraniteľností dôležité

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

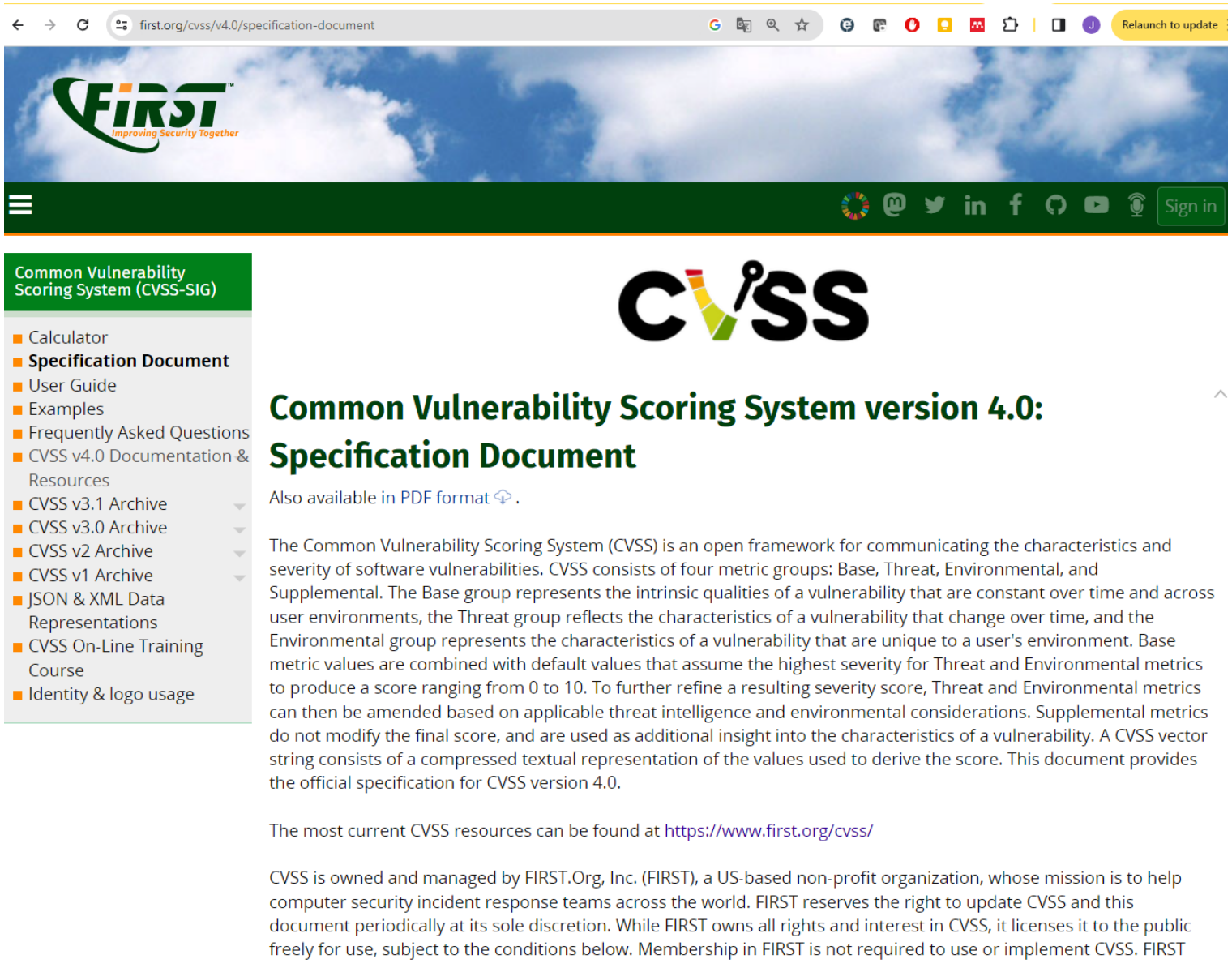
NVD Published Date: 08/31/2016

NVD Last Modified: 08/16/2022

Source: Red Hat, Inc.

Prehľad o CVSS

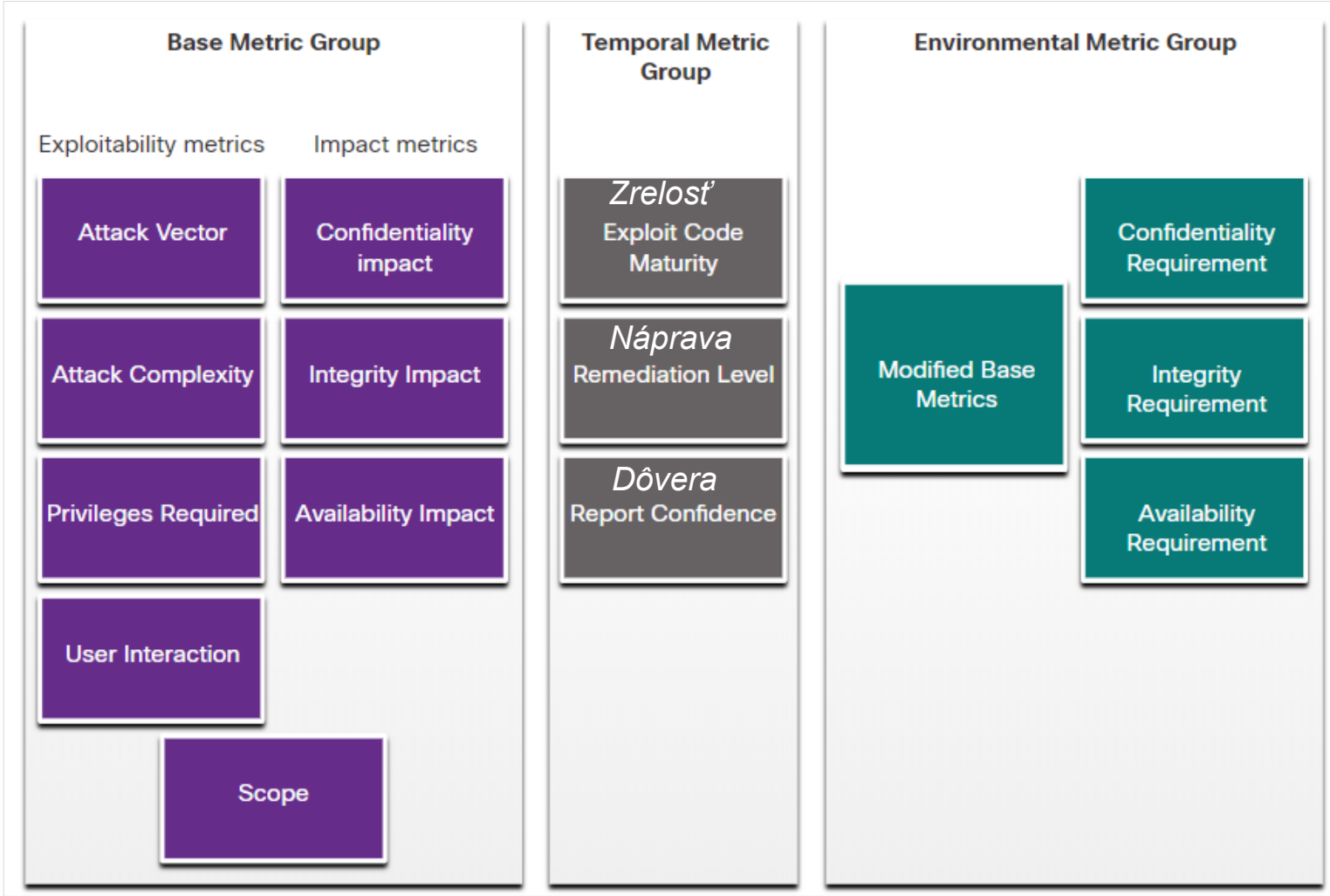
- nástroj na hodnotenie zraniteľností (**vulnerability assessment** tool)
- uvádza spoločné **atribúty** a **závažnosť** zraniteľností
  - v počítačových hardvérových a softvérových systémoch
- poskytuje **štandardizované** skóre zraniteľnosti
- poskytuje **otvorený rámec** s metrikami, pre všetkých 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

CVSS Metric Groups

- 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

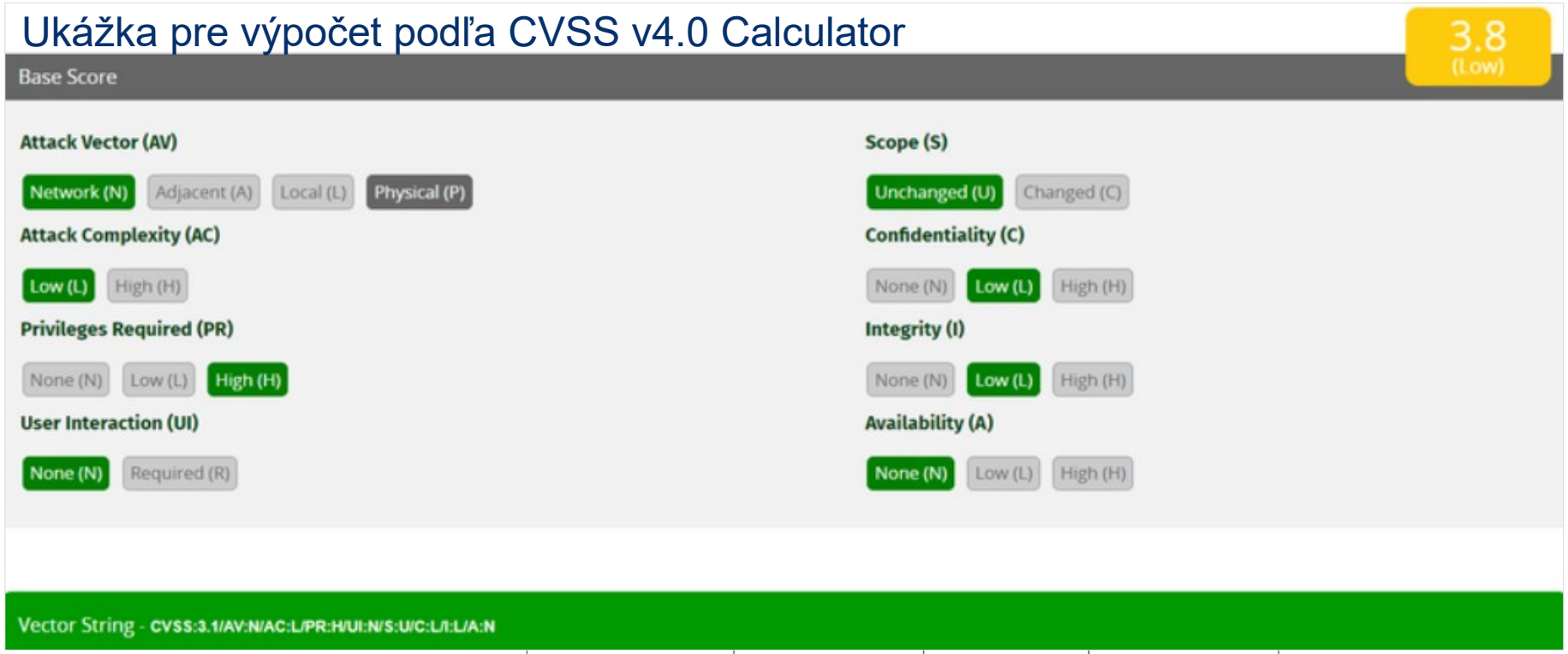


https://www.first.org/cvss/calculator/4.0

Proces CVSS

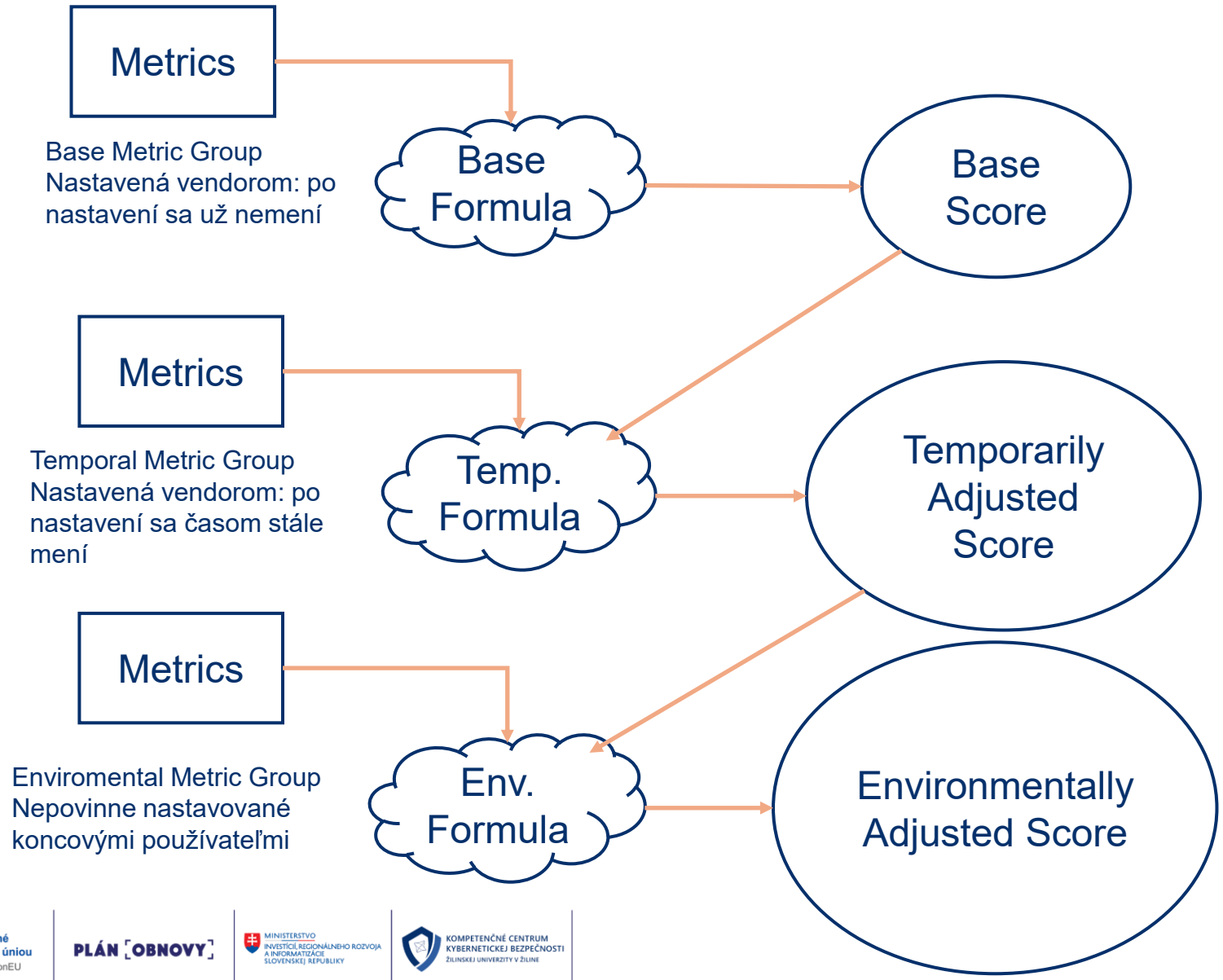
- Proces CVSS využíva nástroj s názvom **CVSS v4.0 Calculator**
- **Calculator** je ako **dotazník**, v ktorom sa robia voľby popisujúce zraniteľnosť v každej skupine metrík
- Neskôr sa **vygeneruje skóre** a zobrazí sa číselné hodnotenie závažnosti

Ukážka pre výpočet podľa CVSS v4.0 Calculator



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.



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 !!!

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

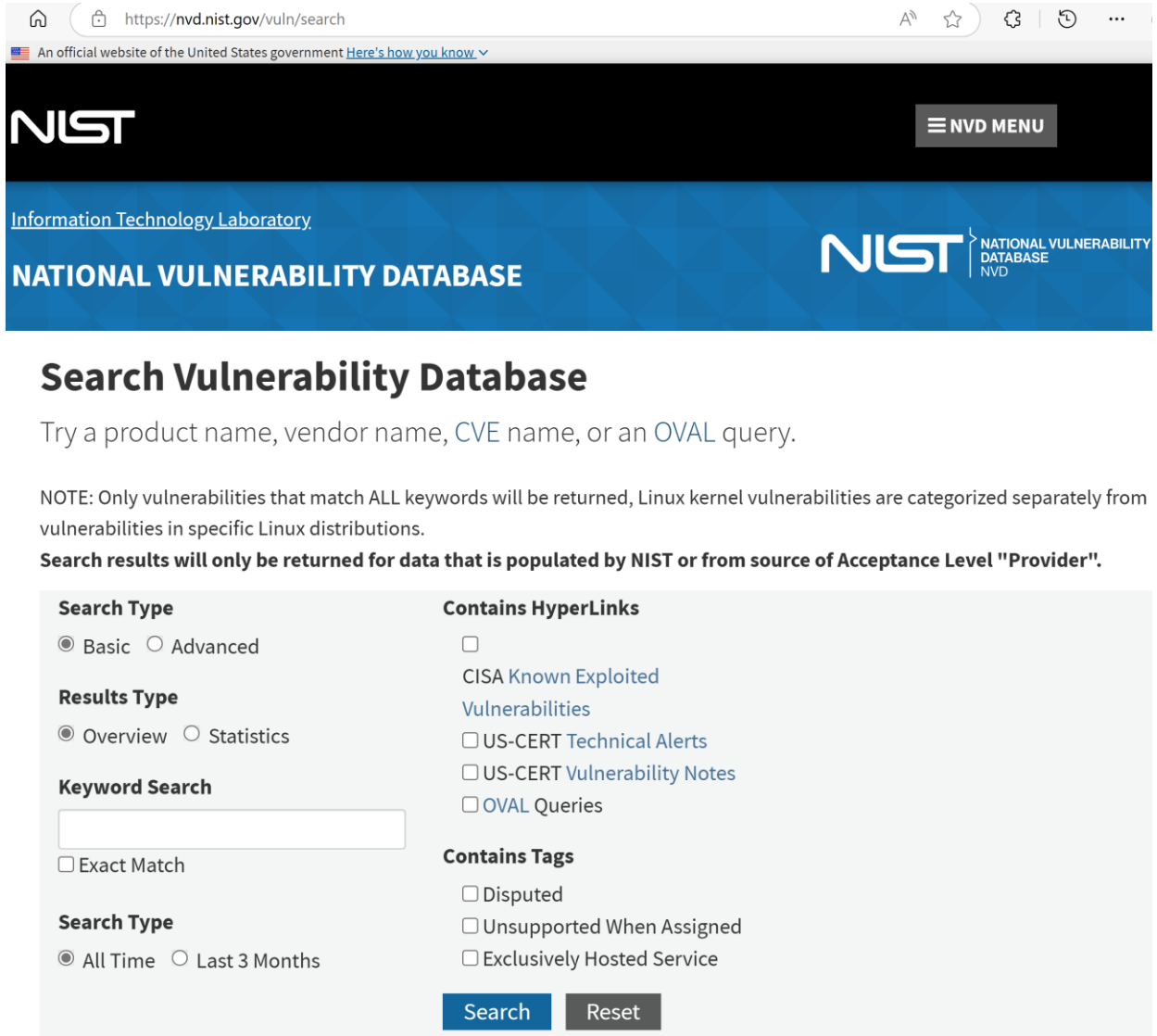
Ďalšie informačné zdroje o zraniteľnostiach

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

- Je uvedené v inej databáze, tzv. NVD:

National Vulnerability Database (NVD):

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



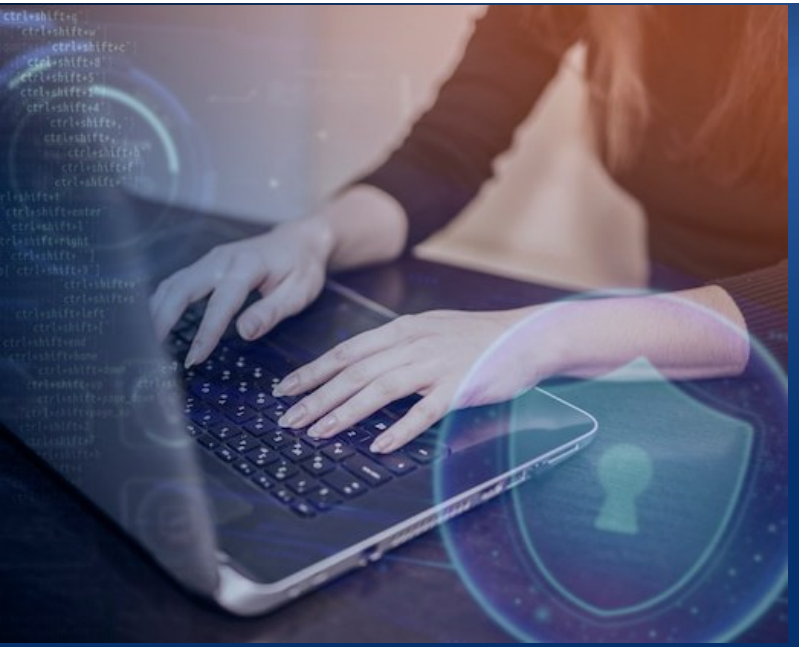
https://nvd.nist.gov/vuln/search

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 hostiteľa, 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, ... Etickí hackeri, penetrační testeri, red team, bezpečnostní konzultanti.



Konkrétna ukážka pre zisťovanie zraniteľnosti systému

Z verejne dostupných informácií na internete
a internetových vyhľadávačov

Konkrétna ukážka pre zisťovanie zraniteľnosti systému

Zoznam domén registrovaných pre organizáciu (ŠGÚDŠ)

Copilot

Nepodarilo sa mi nájsť verejný zoznam domén registrovaných pre **Štátny geologický ústav Dionýza Štúra (ŠGÚDŠ)** priamo cez NIC.SK alebo iné verejné zdroje. Takéto informácie nie sú štandardne dostupné ako centralizovaný zoznam, pokiaľ organizácia sama nezverejní svoje domény.

✅ Známe domény ŠGÚDŠ (overené z praxe):

Na základe predchádzajúcich technických analýz a verejne dostupných služieb sú známe tieto domény:

- **geology.sk** – hlavná doména ústavu
- **apl.geology.sk** – mapový portál (Aplikácie geologických údajov)
- **mapserver.geology.sk** – pravdepodobne interný alebo špecializovaný mapový server
- **geofond.geology.sk** – súvisiaci s geologickým fondom

Tieto subdomény sú aktívne a prevádzkované ŠGÚDŠ, ale ich **IP adresy a rozsahy** nie sú verejne publikované.

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

Vyhľadávače informácií o doménach a IP adresách

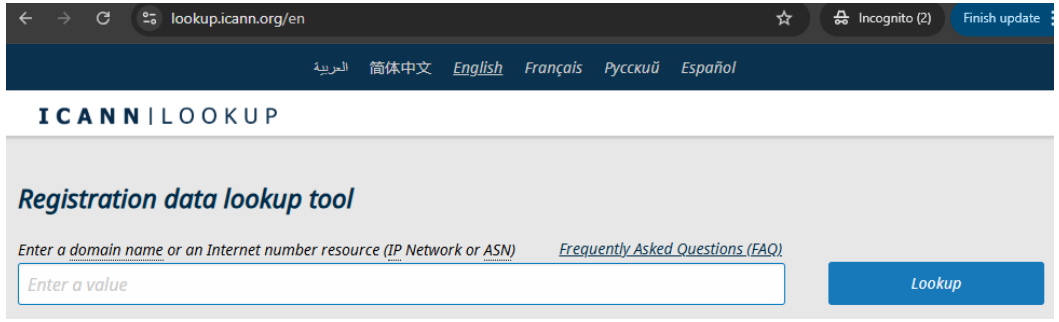
WHOIS nástroje

Je to užitočné pre:

- IT bezpečnostných expertov
- administrátorov sietí
- právnikov pri riešení sporov o domény
- bežných používateľov, ktorí chcú overiť dôveryhodnosť webu

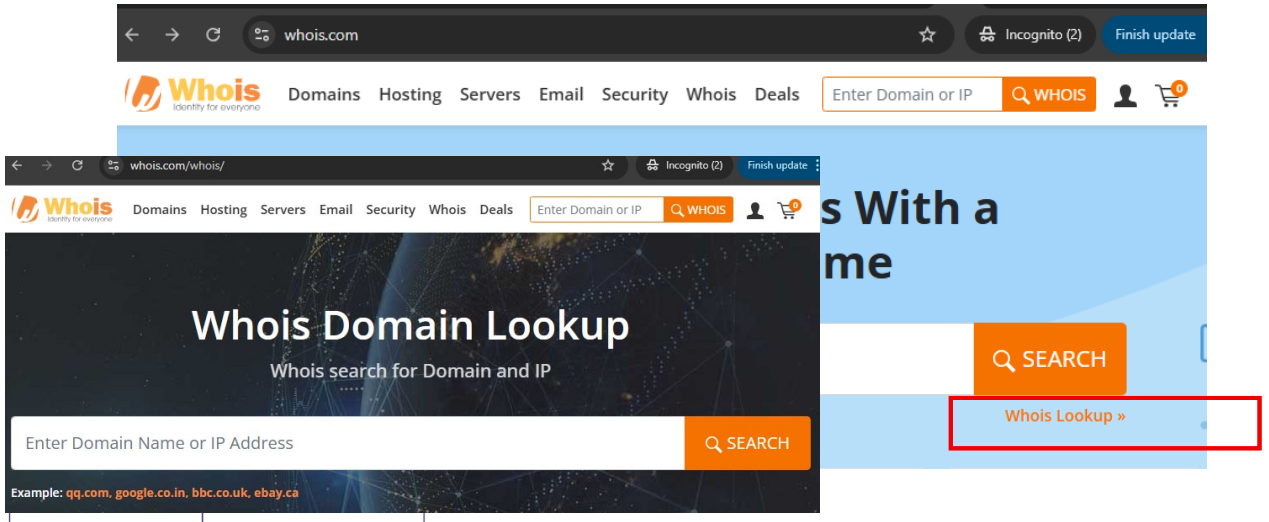
ICANN Lookup

- **ICANN** (Internet Corporation for Assigned Names and Numbers) je **globálna autorita**, ktorá spravuje prideľovanie domén a IP adries.
- Ich nástroj lookup.icann.org poskytuje **priamy prístup k oficiálnym WHOIS záznamom**.
- Je to najspoľahlivejší zdroj, pretože ICANN je **regulačný orgán** pre doménové mená.



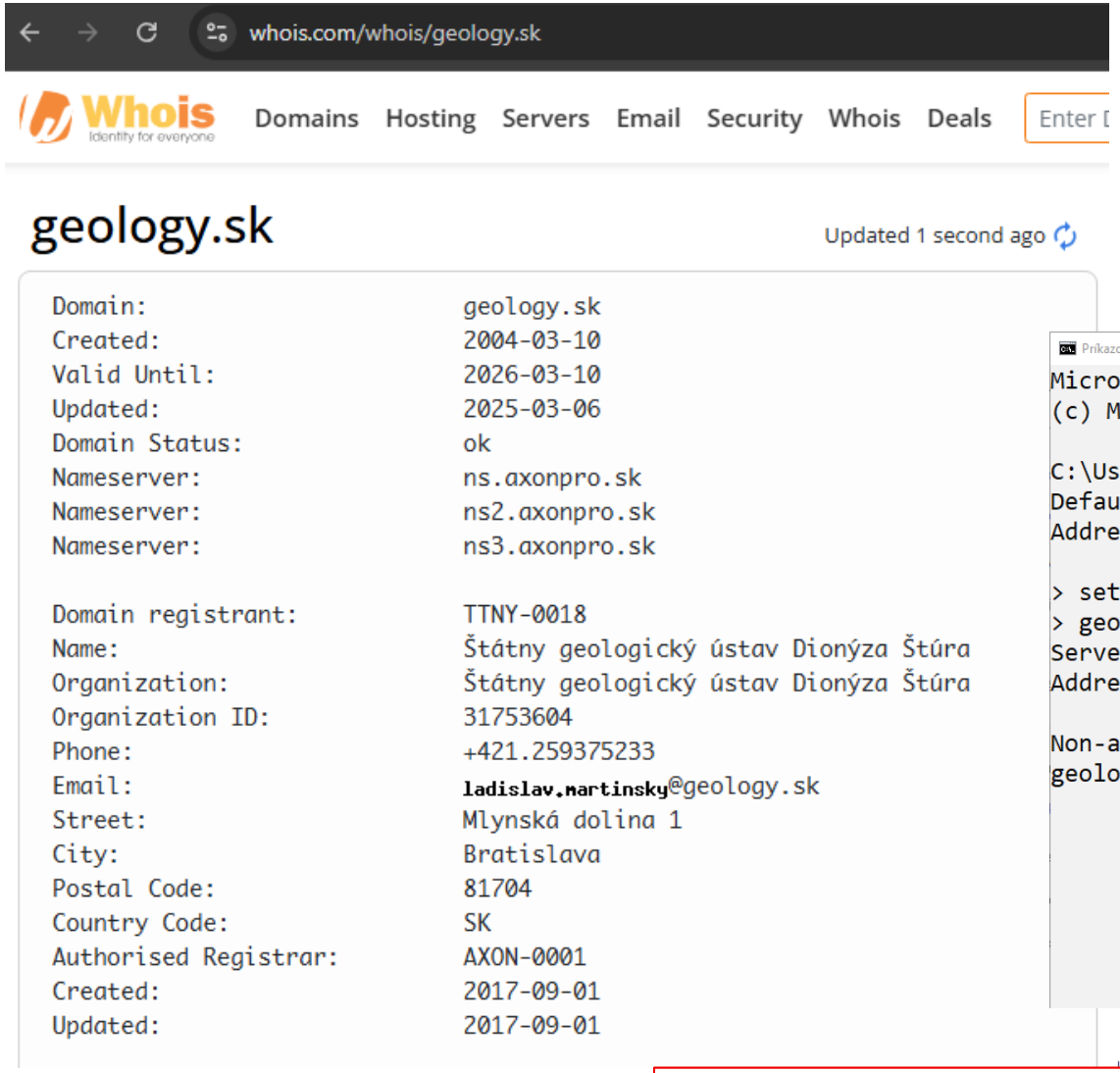
Whois.com

- Whois.com je **dlhoročný a známy poskytovateľ WHOIS služieb**.
- Aj keď nie je regulačným orgánom ako ICANN, je **široko používaný** a má **prehľadné rozhranie**.
- Získava údaje z rôznych registrátorov a často poskytuje aj doplnkové informácie (napr. hosting, DNS, lokalita).
- https://www.whois.com/whois/

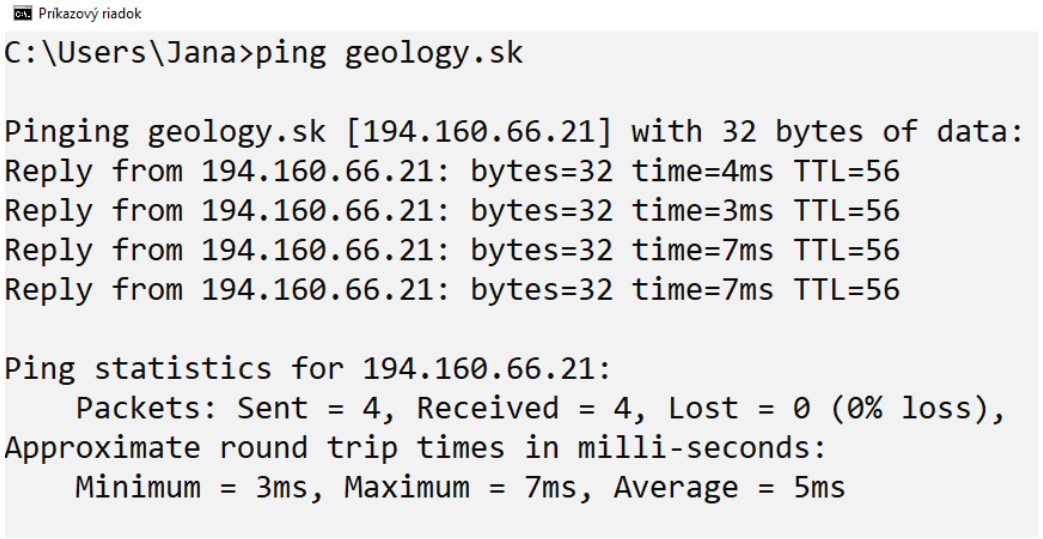


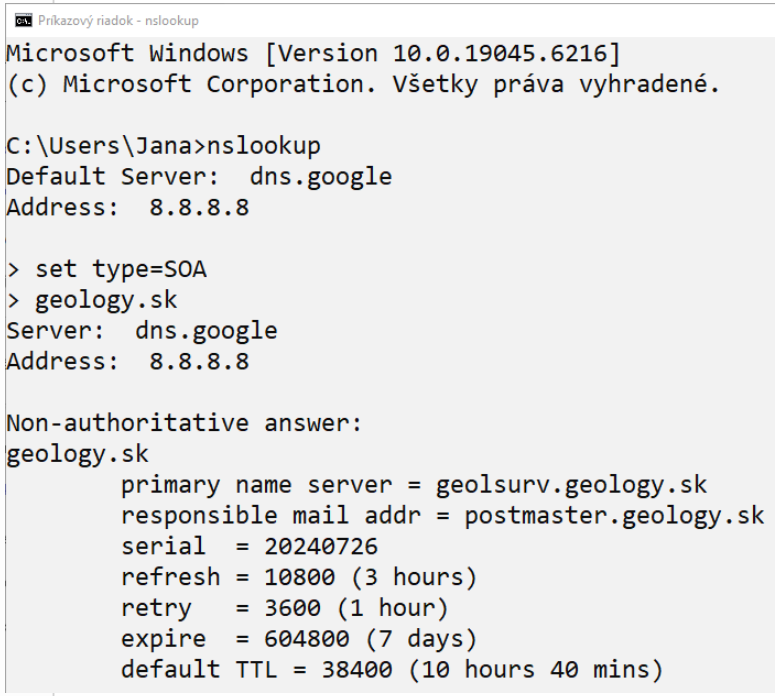
Zistime si logické (IP) adresy organizácie

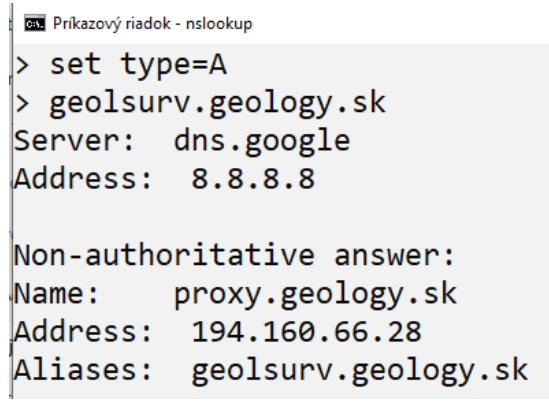
Prieskum logických IP adies



https://www.whois.com/whois/geology.sk







Zistené IPv4 adresy: 194.160.66.21, 194.160.66.28

WHOIS lookup

Zistenie rozsahu logických (IP) adries pre organizáciu

whois.com/whois/194.160.66.21

Whois Domains Hosting Servers Email Security Whois Deals

Whois IP 194.160.66.21

```
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See https://docs.db.ripe.net/terms-conditions.html

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '194.160.66.0 - 194.160.67.255'

% Abuse contact for '194.160.66.0 - 194.160.67.255' is 'abuse@sanet.sk'

inetnum:        194.160.66.0 - 194.160.67.255
netname:        GEOLOGY-DS-SK
descr:          State Geological Institute of Dionyz Stur
descr:          Slovakia
country:        SK
admin-c:        SK1370-RIPE
tech-c:         JB6619-RIPE
status:         ASSIGNED PA
mnt-by:         SWDB-SANET
mnt-lower:      SWDB-SANET
created:        2007-12-11T19:56:10Z
last-modified:  2007-12-11T20:04:22Z
source:         RIPE
```

```
person:         Juraj Baluch
address:        Mlynska dolina 1
address:        Bratislava
address:        817 04
address:        Slovakia
phone:          +421 2 5937 5248
fax-no:         +421 2 5477 1940
nic-hdl:        JB6619-RIPE
mnt-by:         SWDB-SANET
created:        2007-12-11T19:56:10Z
last-modified:  2008-10-22T14:16:36Z
source:         RIPE # Filtered

person:         Stefan Kacer
address:        Mlynska dolina 1
address:        Bratislava
address:        817 04
address:        Slovakia
phone:          +421 2 5937 5155
fax-no:         +421 2 5477 1940
nic-hdl:        SK1370-RIPE
mnt-by:         SWDB-SANET
created:        2007-12-11T19:56:10Z
last-modified:  2008-10-22T14:16:35Z
source:         RIPE # Filtered
```

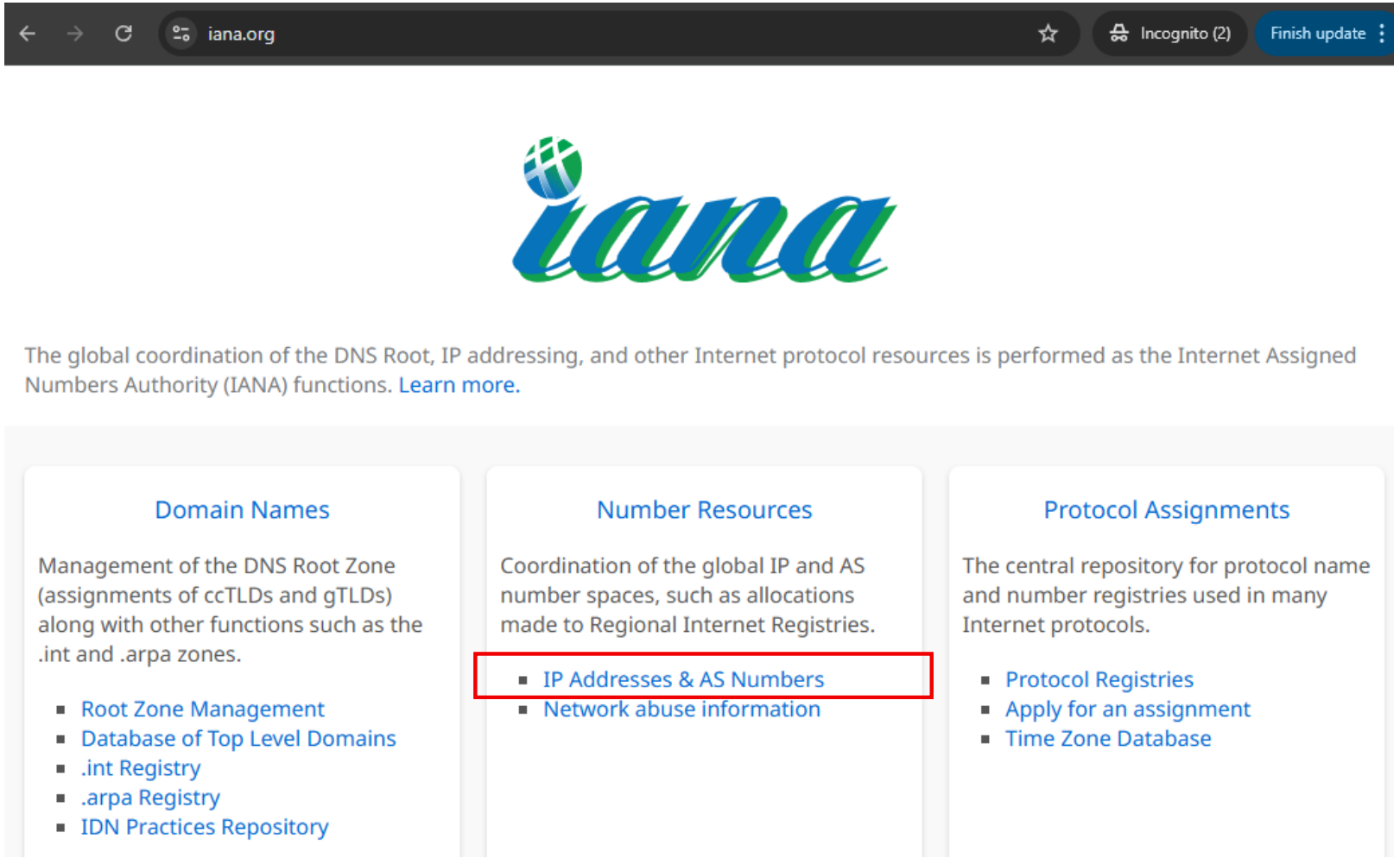
```
% Information related to '194.160.0.0/17AS2607'

route:          194.160.0.0/17
descr:          SANET-AS2607-BLOCK
origin:         AS2607
mnt-by:         AS2607-MNT
mnt-lower:      AS2607-MNT
created:        2022-10-10T12:06:38Z
last-modified:  2022-10-10T12:06:38Z
source:         RIPE

% This query was served by the RIPE Database Query Service version 1.118.1 (BUSA)
```

Kto spravuje (takmer) všetky číselné identifikátory na internete – dôveryhodná autorita

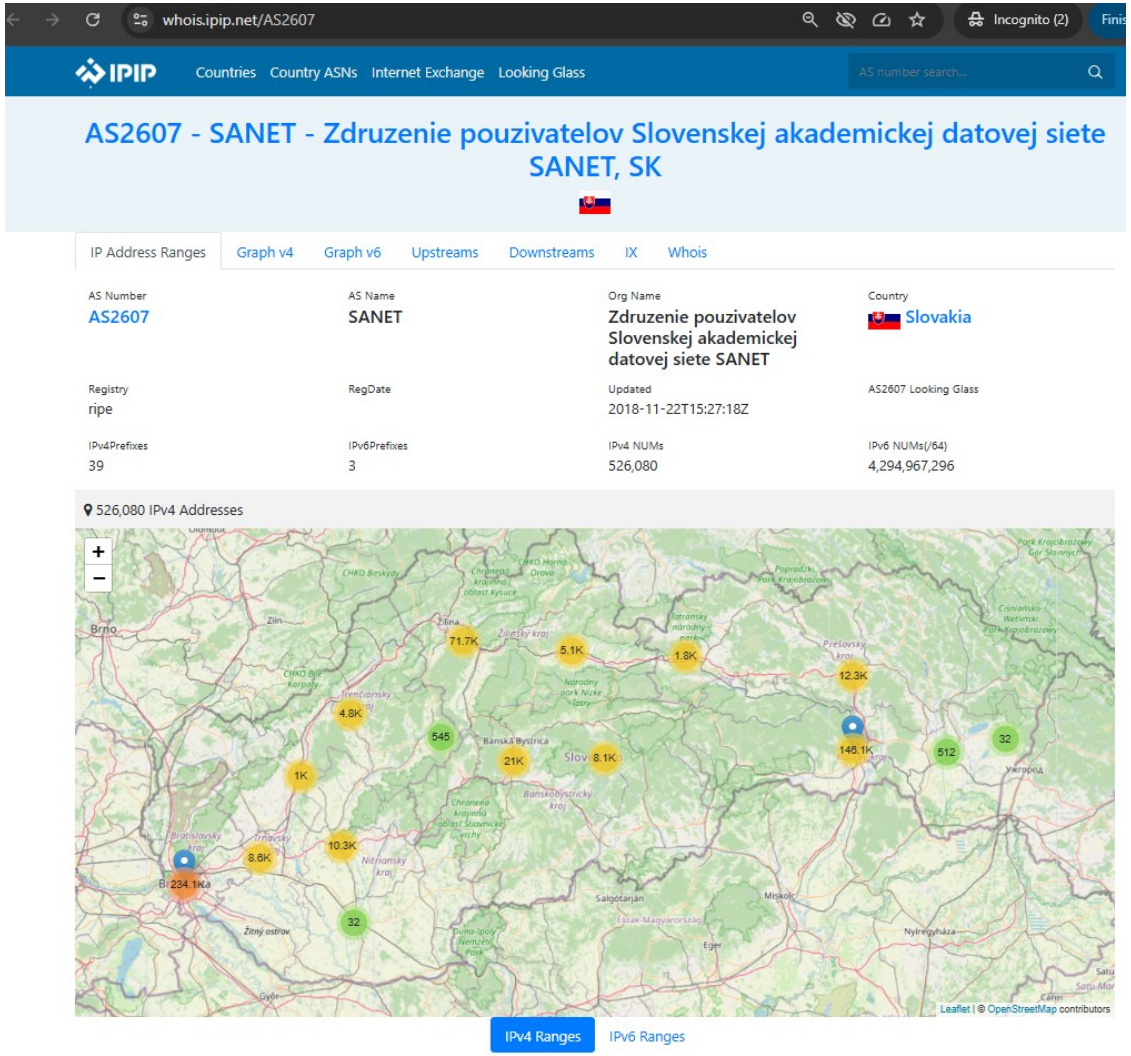
IANA.org



https://www.iana.org/

Nie je oficiálnym zdrojom informácií pre EU... Ale poslúži nám, lebo poskytne viac...

https://whois.ipip.net/



192.108.132.0/24	✓	VSEBBNET
192.108.132.0/23	✓	VSEBBNET
192.108.133.0/24	✓	VSEBBNET
192.108.138.0/24	✓	SANET
192.108.138.0/23	✓	SANET
192.108.149.0/24	✓	UAKOMBONE
193.87.0.0/17	✓	National Health Information Center
193.87.0.0/16	✓	Zdruzenie pouzivatelov Slovenskej akademickej dat
193.87.128.0/17	✓	NBSNET
194.160.0.0/17	✓	Zdruzenie pouzivatelov Slovenskej akademickej dat
194.160.0.0/16	✓	Zdruzenie pouzivatelov Slovenskej akademickej dat
194.160.128.0/17	✓	SSKNM-SK

Reverzné záznamy na https://whois.ipip.net/

Zisťovanie informácií

- 194.160.66.0/24
- 192.160.67.0/24

194.160.25.0/24	194.160.26.0/24	194.160.27.0/24
194.160.30.0/24	194.160.31.0/24	194.160.32.0/24
194.160.35.0/24	194.160.36.0/24	194.160.37.0/24
194.160.40.0/24	194.160.41.0/24	194.160.42.0/24
194.160.45.0/24	194.160.46.0/24	194.160.47.0/24
194.160.50.0/24	194.160.51.0/24	194.160.52.0/24
194.160.55.0/24	194.160.56.0/24	194.160.57.0/24
194.160.60.0/24	194.160.61.0/24	194.160.62.0/24
194.160.65.0/24	194.160.66.0/24	194.160.67.0/24
194.160.70.0/24	194.160.71.0/24	194.160.72.0/24
194.160.75.0/24	194.160.76.0/24	194.160.77.0/24

whois.ipip.net/cidr/194.160.66.0/24

IPIP Countries Country ASNs Internet Exchange Looking Glass AS number search...

BGP Announced

AS	CIDR	Description
AS2607	194.160.0.0/17	SANET - Zdruzenie pouzivatelov Slovenskej akademickej datovej siete SANET, SK
AS2607	194.160.0.0/16	SANET - Zdruzenie pouzivatelov Slovenskej akademickej datovej siete SANET, SK

Real Time BGP Data

AS / Info	IP / Time	AS Path
Loading...		

Reverse DNS List (Total:255)

IP	Host	DateTime
194.160.66.1	1.geology.sk	2025-09-04 14:23:12
194.160.66.2	proxy.geology.sk	2025-09-04 14:23:12
194.160.66.3	3.geology.sk	2025-09-04 14:23:12
194.160.66.4	4.geology.sk	2025-09-04 14:23:12
194.160.66.5	5.geology.sk	2025-08-30 12:41:16
194.160.66.6	6.geology.sk	2025-09-04 14:23:12

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)

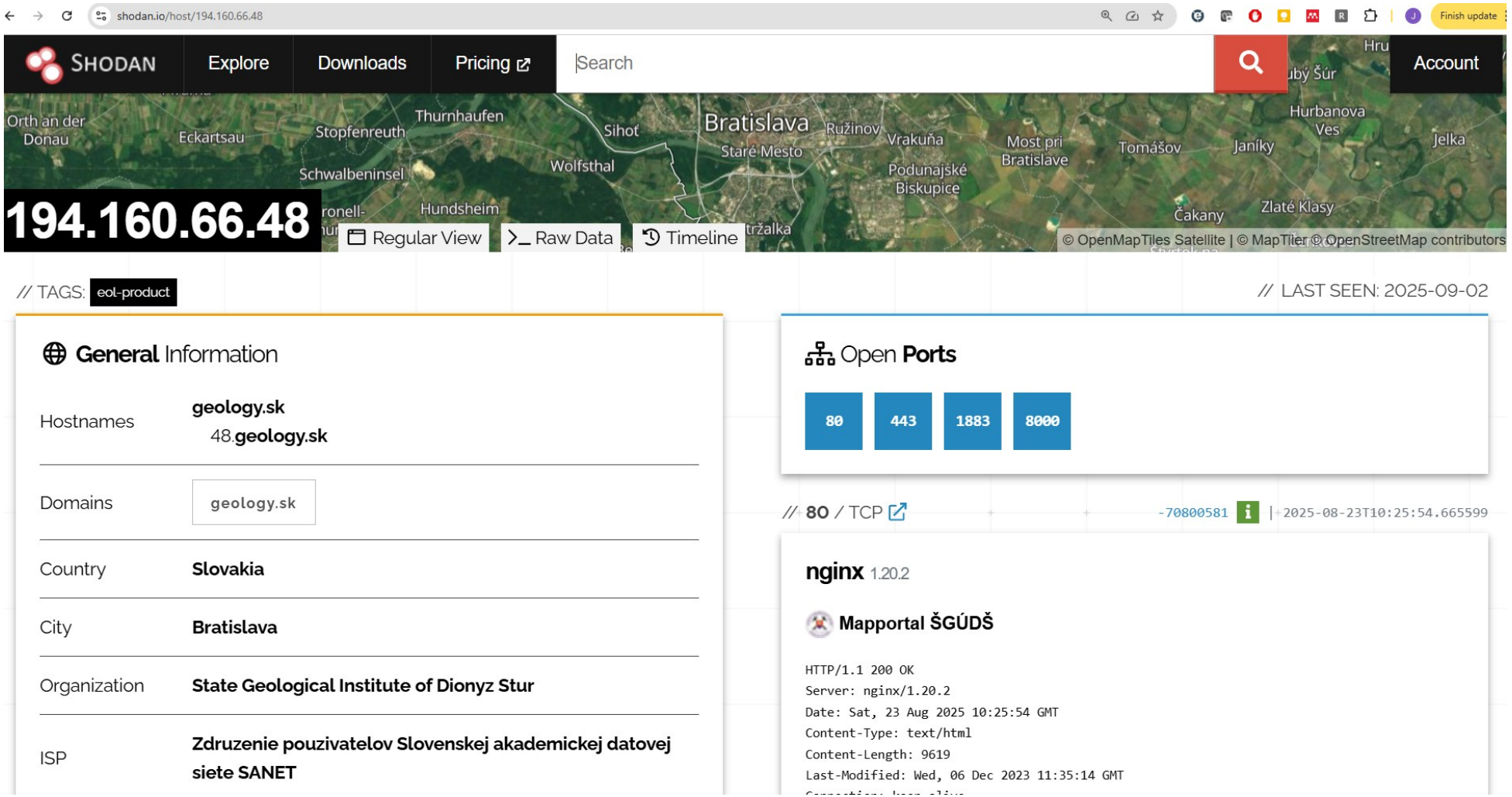
https://www.shodan.io/

- **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)** – teda:
    - 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

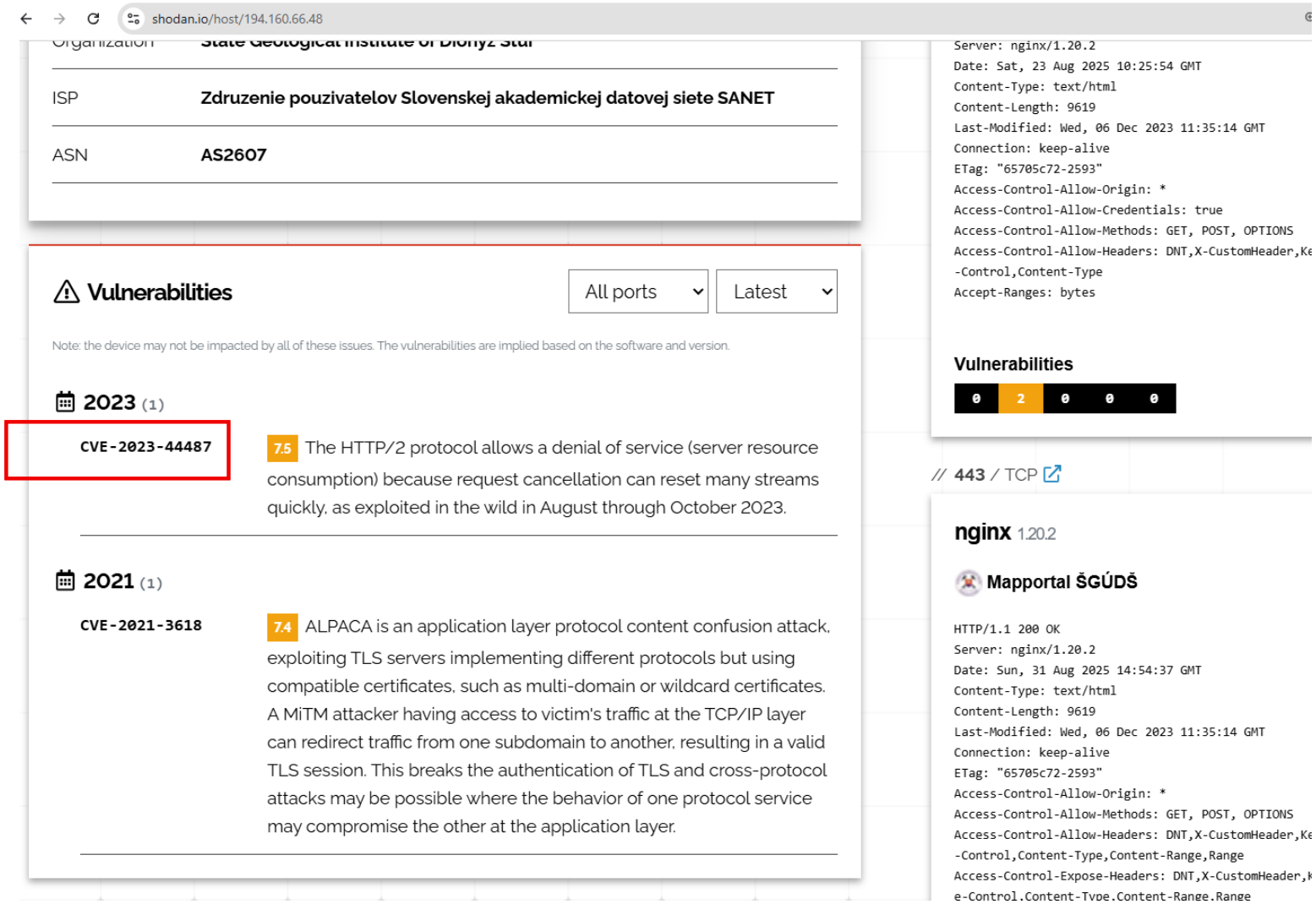
Vyhľadávač pre zariadenia pripojené k internetu (vrátane ich zraniteľností)

Vyhľadanie informácií cez shodan.io



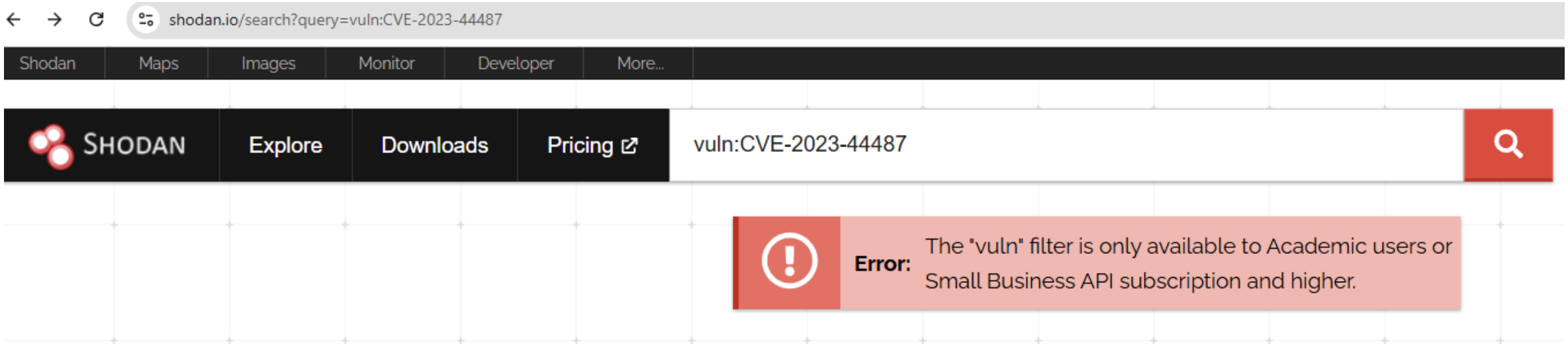
Vyhľadávač pre zariadenia pripojené k internetu (vrátane ich zraniteľností)

Vyhľadanie informácií cez shodan.io (pokrač.)



Vyhľadávač pre zariadenia pripojené k internetu (vrátane ich zraniteľností)

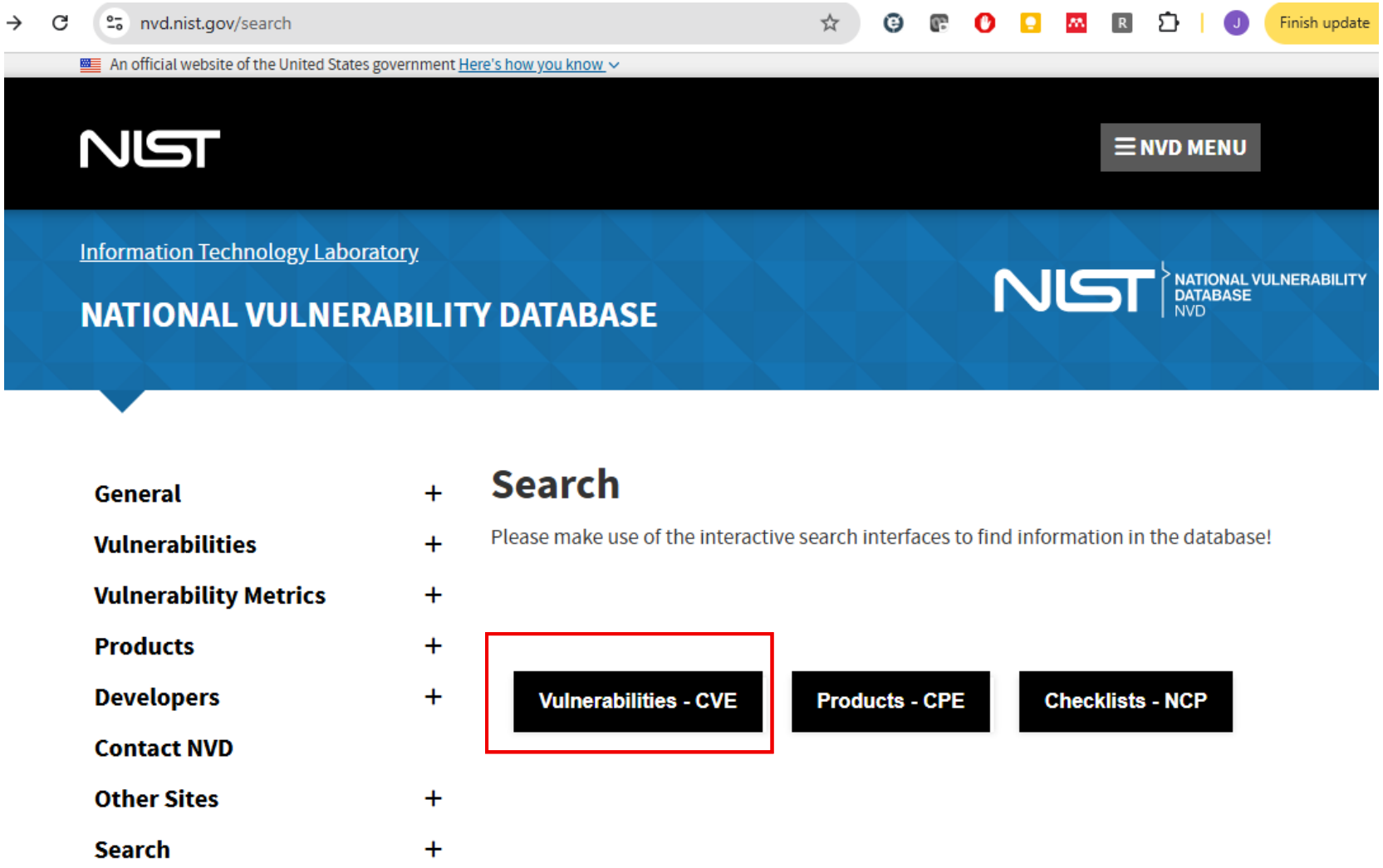
Filter na zraniteľnosti



Konkrétna ukážka pre zisťovanie zraniteľnosti systému

Vyhľadávanie informácií o zraniteľnostiach

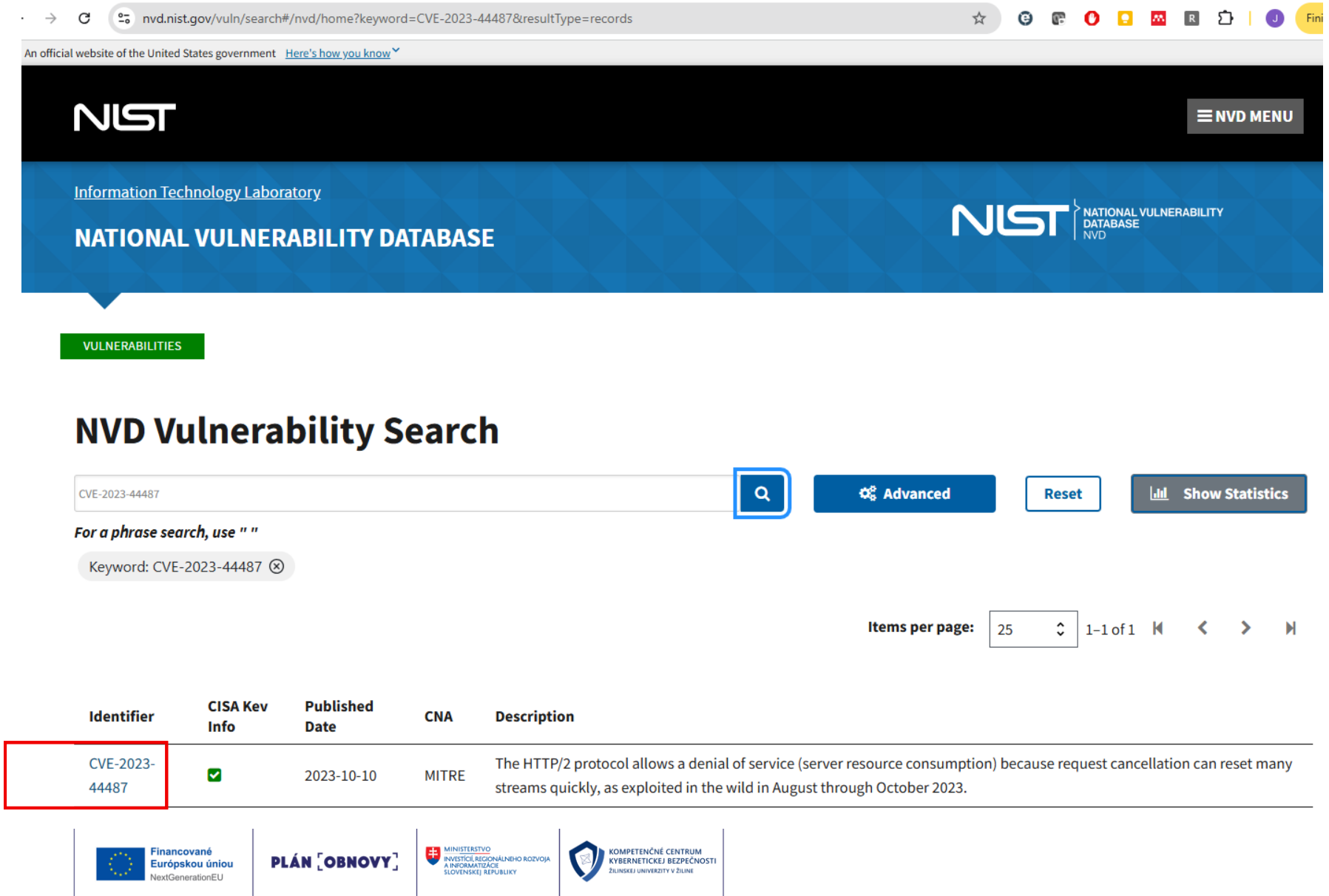
- NIST NVD (National Vulnerability Database) je oficiálna databáza kybernetických zraniteľností
  - spravovaná NIST (National Institute of Standards and Technology) v USA
  - zoznam známych zraniteľností softvéru a hardvéru, často označených identifikátorom CVE (Common Vulnerabilities and Exposures).
  - 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



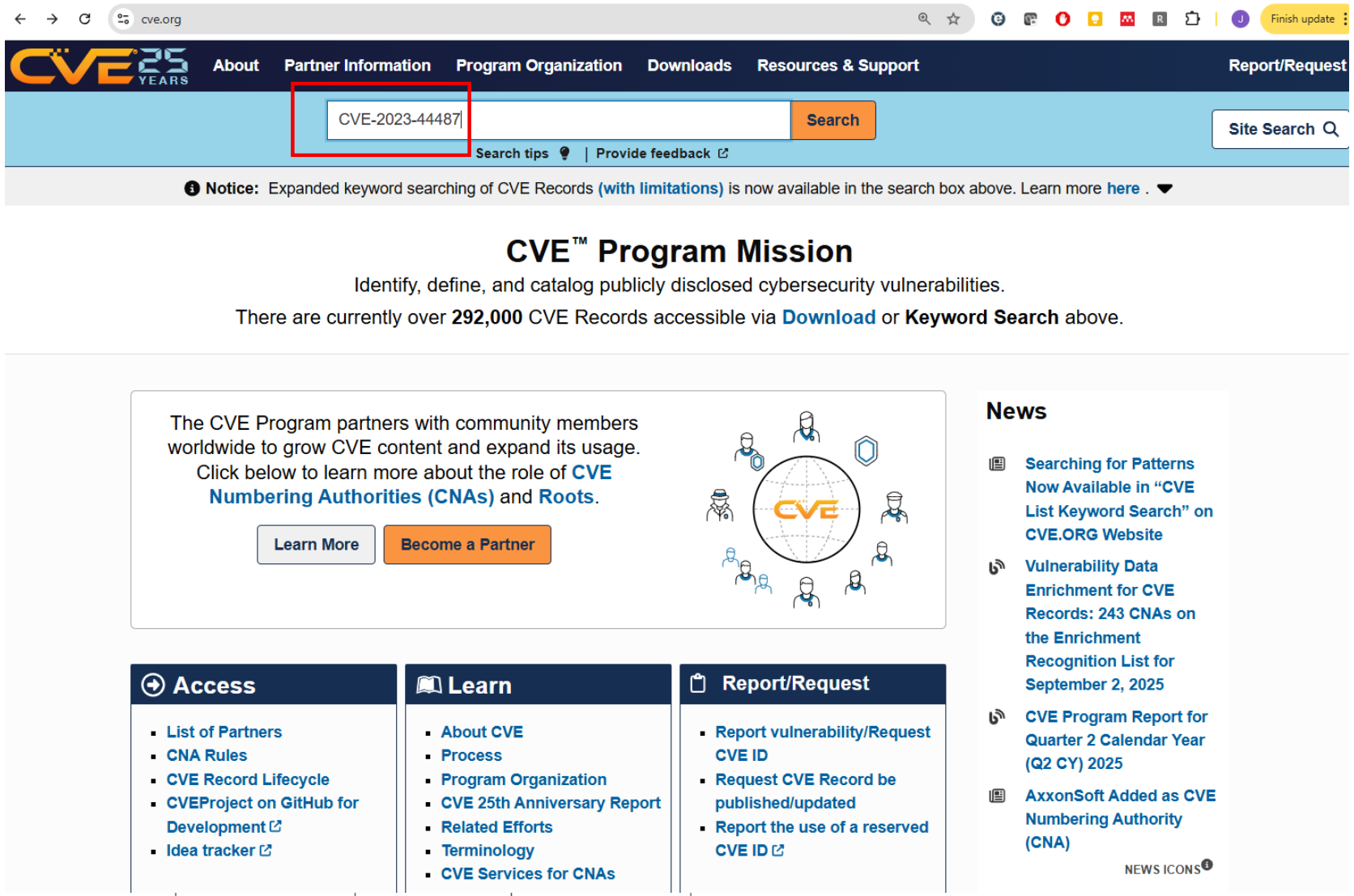
Konkrétna ukážka pre zisťovanie zraniteľnosti systému

cve.org

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

- Vyhľadávanie informácií o:

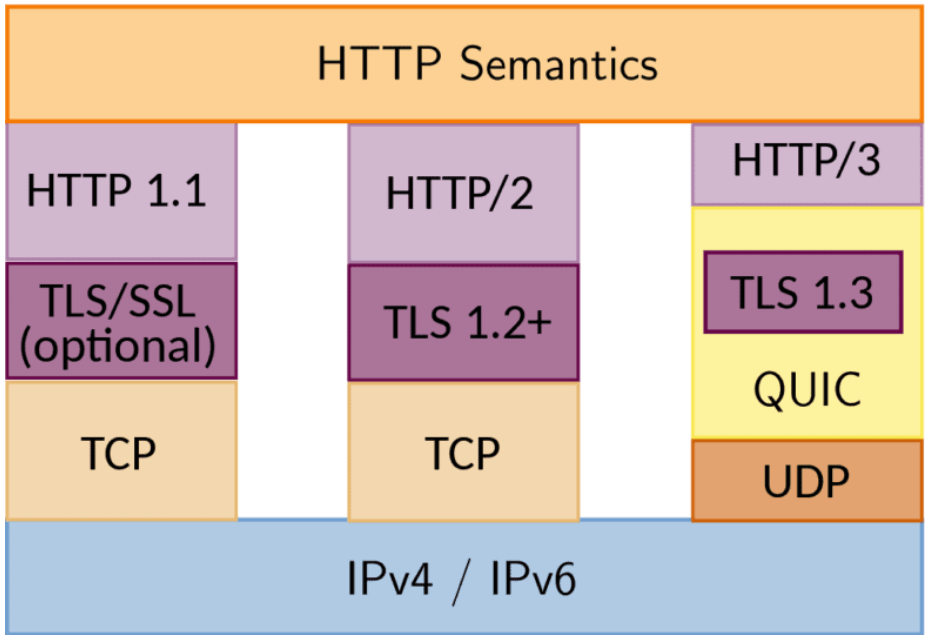
  CVE-2023-44487

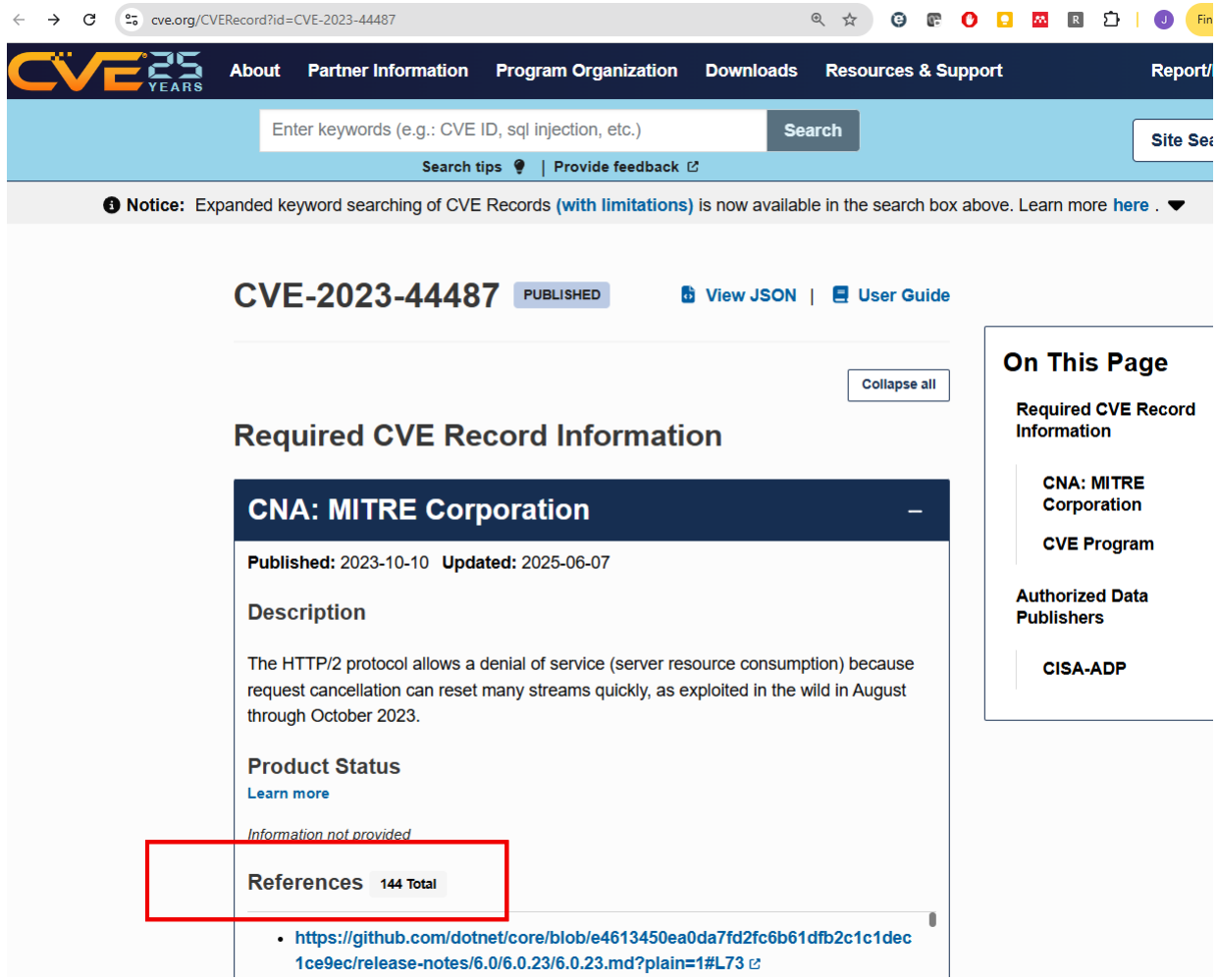


Konkrétna ukážka pre zisťovanie zraniteľnosti systému

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

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

Je viacero rôznych databáz zraniteľností

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).

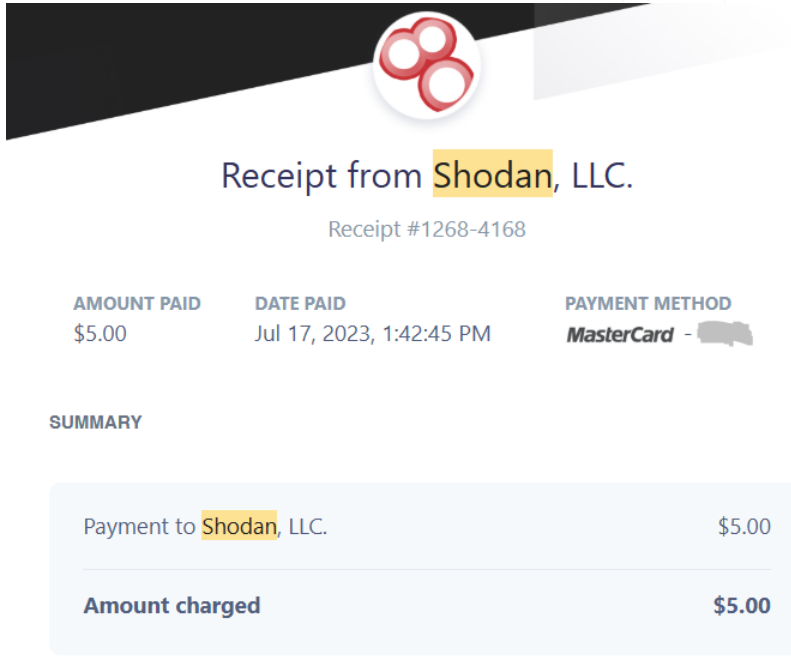
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

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

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.

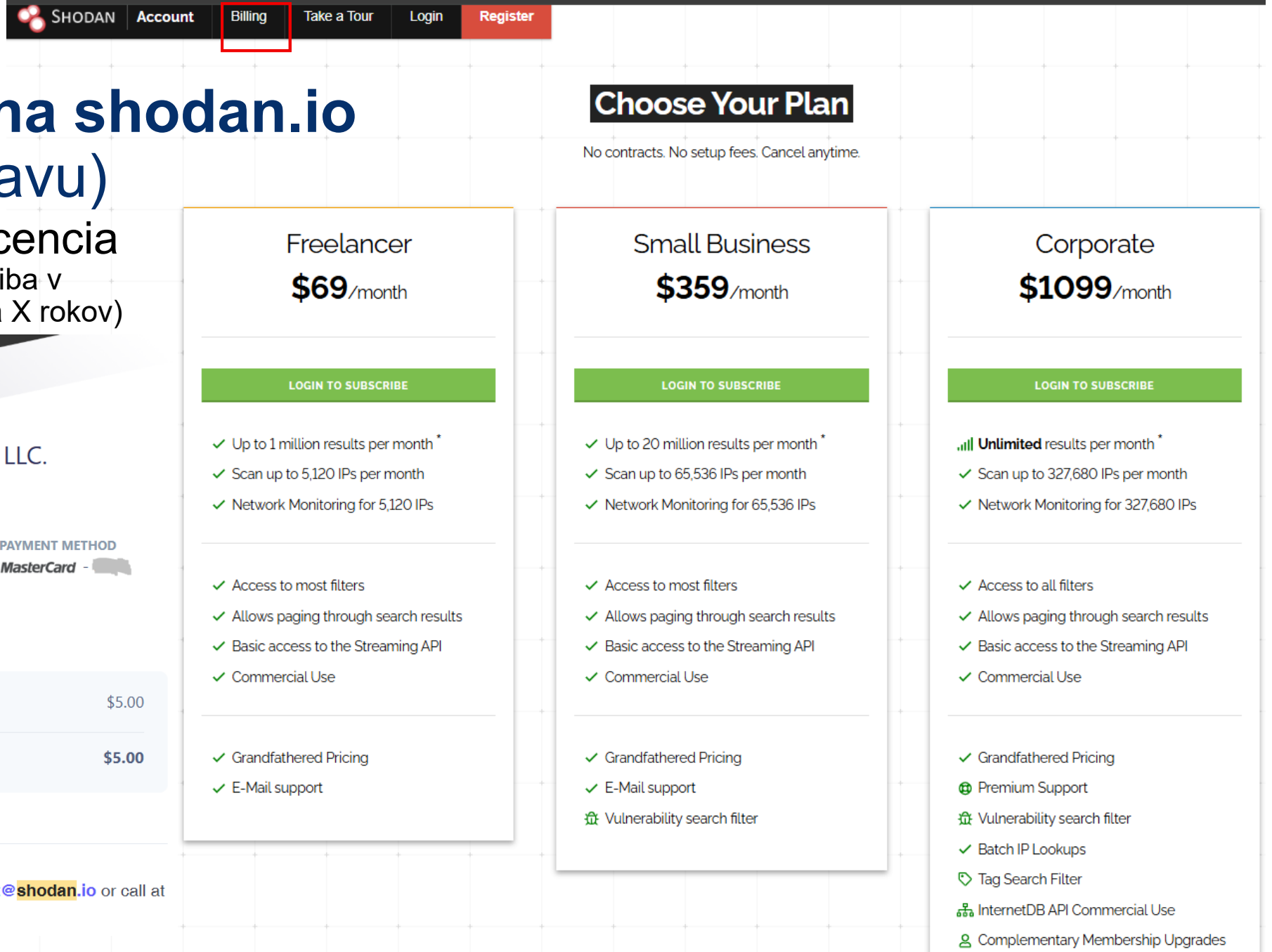
Receipt #1268-4168

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

SUMMARY

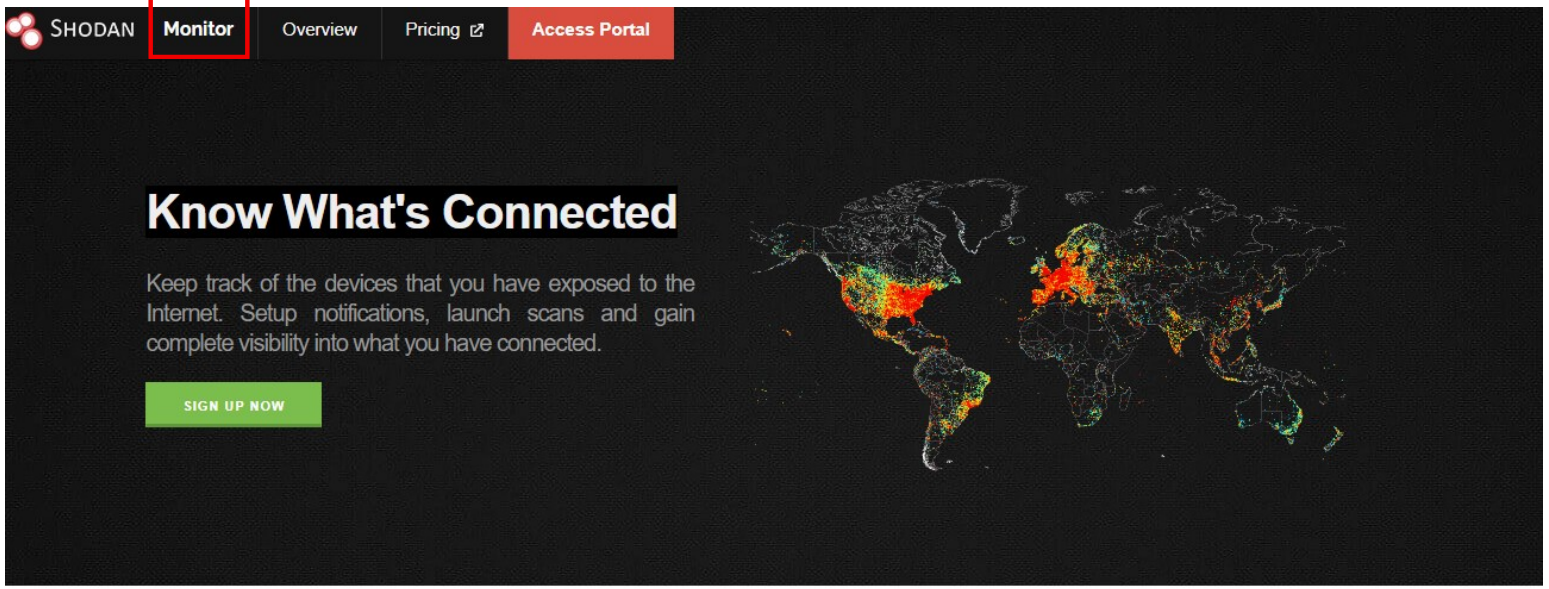
Payment to Shodan, LLC.	$5.00
Amount charged	**$5.00**

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



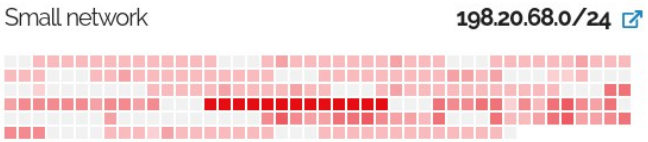
Identifikácia zraniteľností systémov so shodan.io

S liceniou: aj možnosť monitorovať (svoje) zariadenia



Network Monitoring Made Easy

Within 5 minutes of using Shodan Monitor you will see what you currently have connected to the Internet within your network range and be setup with real-time notifications when something unexpected shows up.

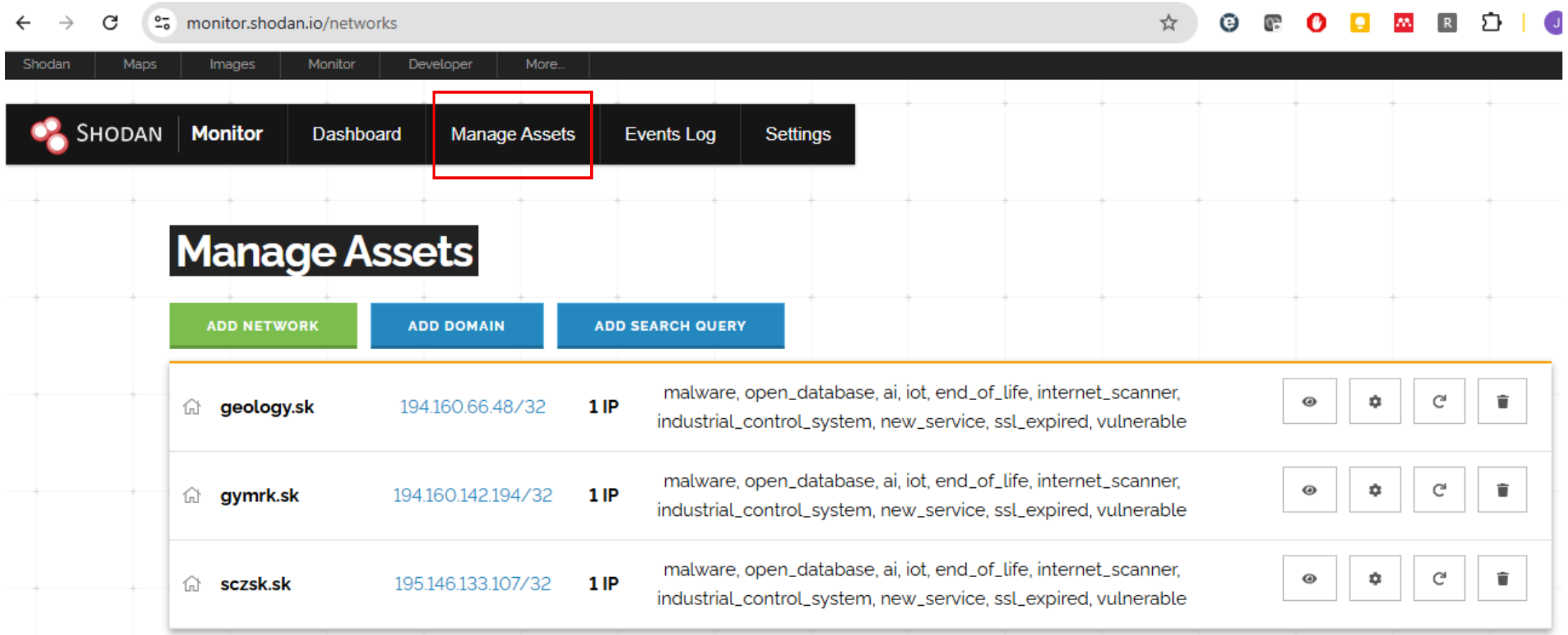


Built to Scale

Whether you want to monitor 1 IP or you're an ISP with millions of customers - the Shodan platform was built to handle networks of all sizes without breaking a sweat.

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

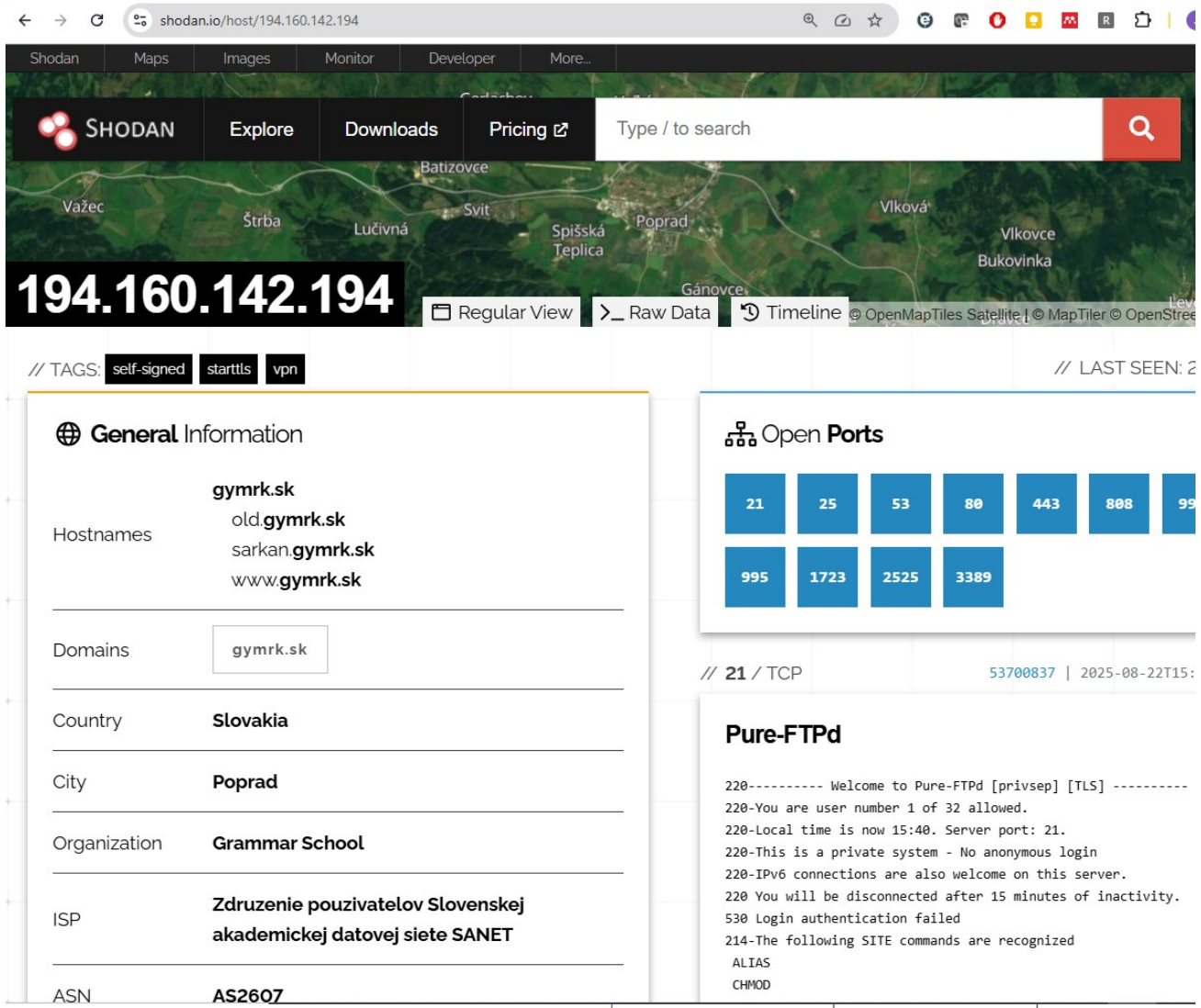
nginx 1.20.2

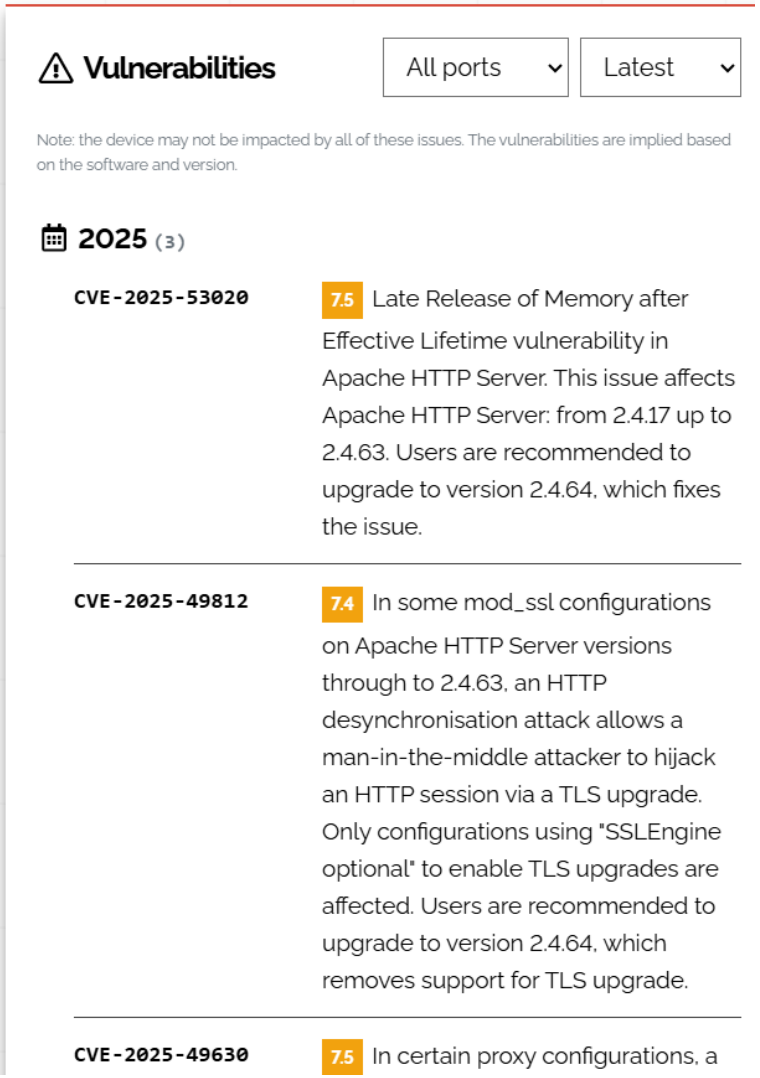
```
HTTP/1.1 200 OK
Server: nginx/1.20.2
Date: Thu, 04 Sep 2025 13:44:23 GMT
Content-Type: text/html
Content-Length: 9619
Last-Modified: Wed, 06 Dec 2023 11:35:14 GMT
Connection: keep-alive
ETag: "65705c72-2593"
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: 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
```

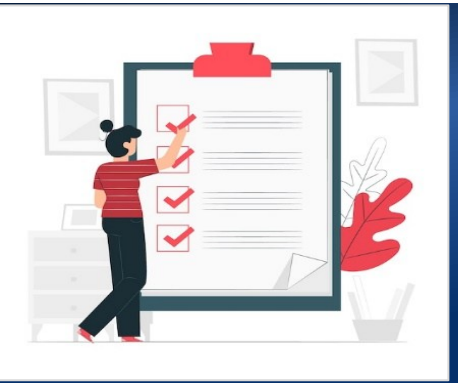
View Events Add to Whitelist

Konkrétna ukážka pre zisťovanie zraniteľnosti systému

Vyhľadanie informácií cez shodan.io







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

Bezpečnostné opatrenia – test zraniteľností

Bezpečnostné riziká, opatrenia a prevencia (Blok II)

Kurz: Odborný zamestnanec (laik) kybernetickej bezpečnosti

Mgr. Jana Uramová, PhD.

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

Jana.Uramova@fri.uniza.sk