



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

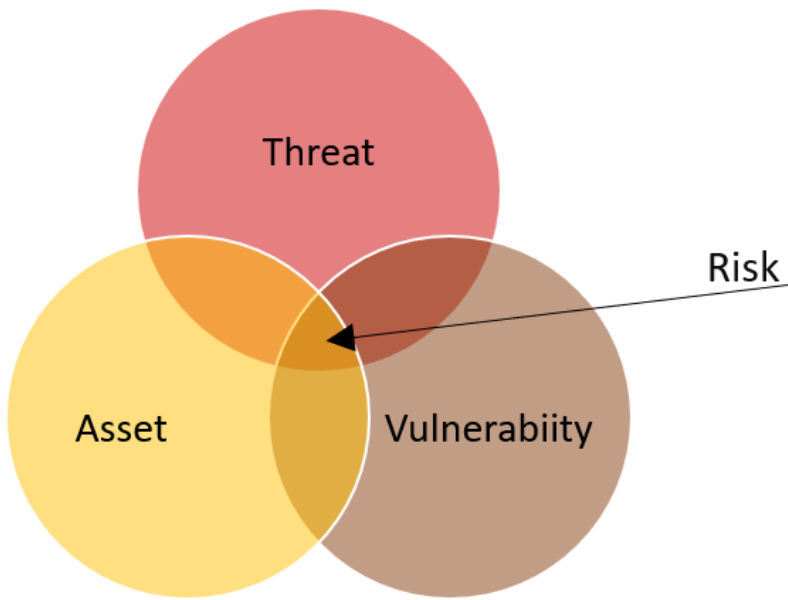
Bezpečnostné riziká, opatrenia a prevencia (Blok II)

Kurz: Odborný zamestnanec (laik) kybernetickej bezpečnosti

Mgr. Jana Uramová, PhD.

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

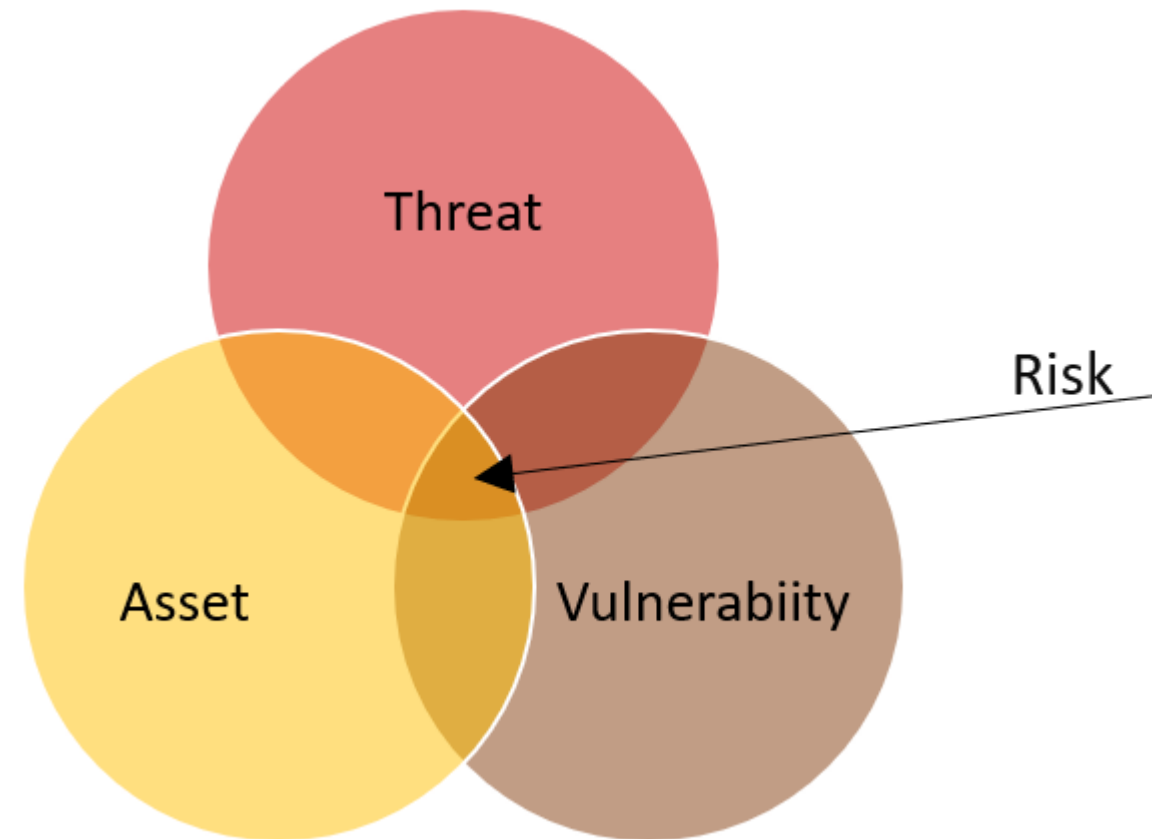
Jana.Uramova@fri.uniza.sk



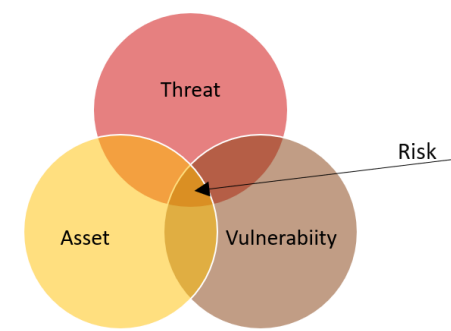
Nadviazanie na predošlé témy

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.



Hrozba, zraniteľnosť a riziko (Pokr.)

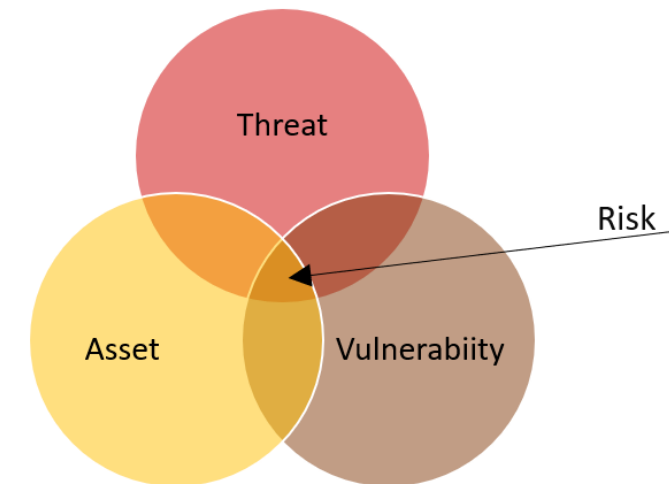


- Na pochopenie bezpečnosti siete je dôležité poznať nasledujúce pojmy:

Pojem	Vysvetlenie
Threat	Potenciálne nebezpečenstvo pre aktívum (údaje alebo samotnú sieť).
Vulnerability	Slabé miesto v systéme alebo jeho dizajne, ktoré môže byť zneužitá 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.

Identifikácia aktív

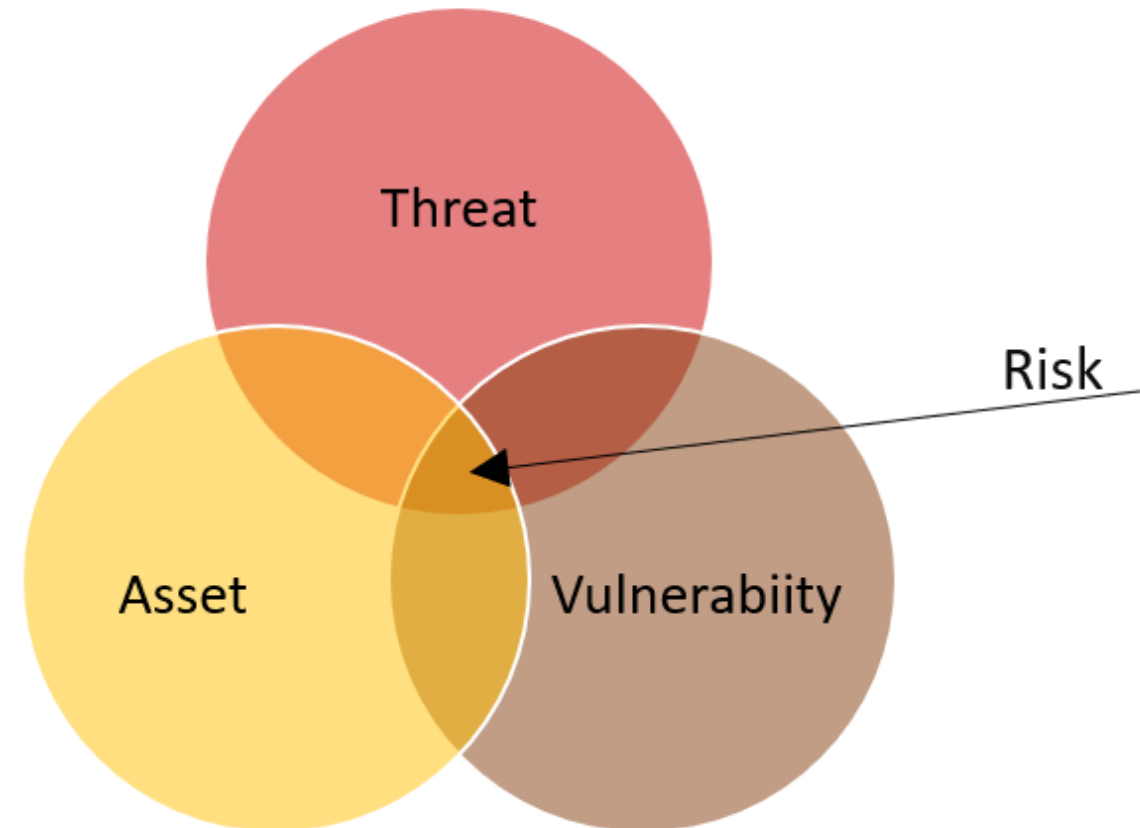
- Aktíva = súbor všetkých **zariadení** a **informácií**, ktoré organizácia vlastní alebo spravuje
- Správa aktív pozostáva z:
 - **inventarizácie** všetkých aktív
 - **posúdenia** z hľadiska úrovne ochrany potrebnej na prekazenie potenciálnych útokov
 - **vypracovania a zavedenia politík** a **postupov** 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**.



Prečo je manažovanie zraniteľností dôležité

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?





**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

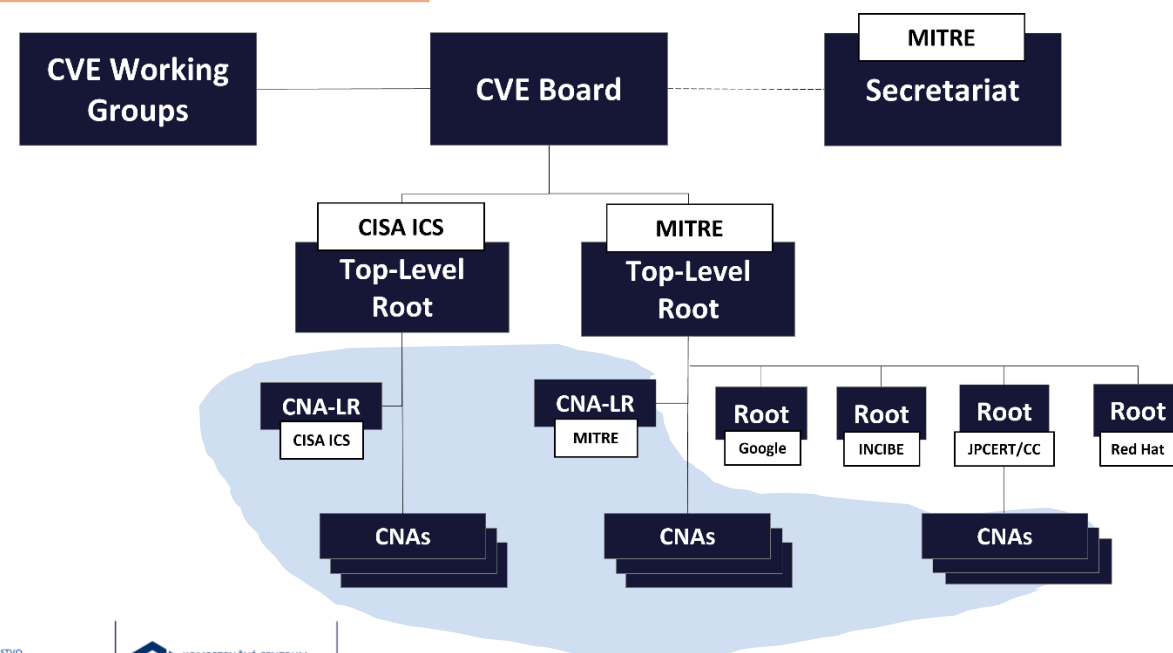
Root – **manažérske** funkcie

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

Každý [CVE záznam](#) obsahuje:

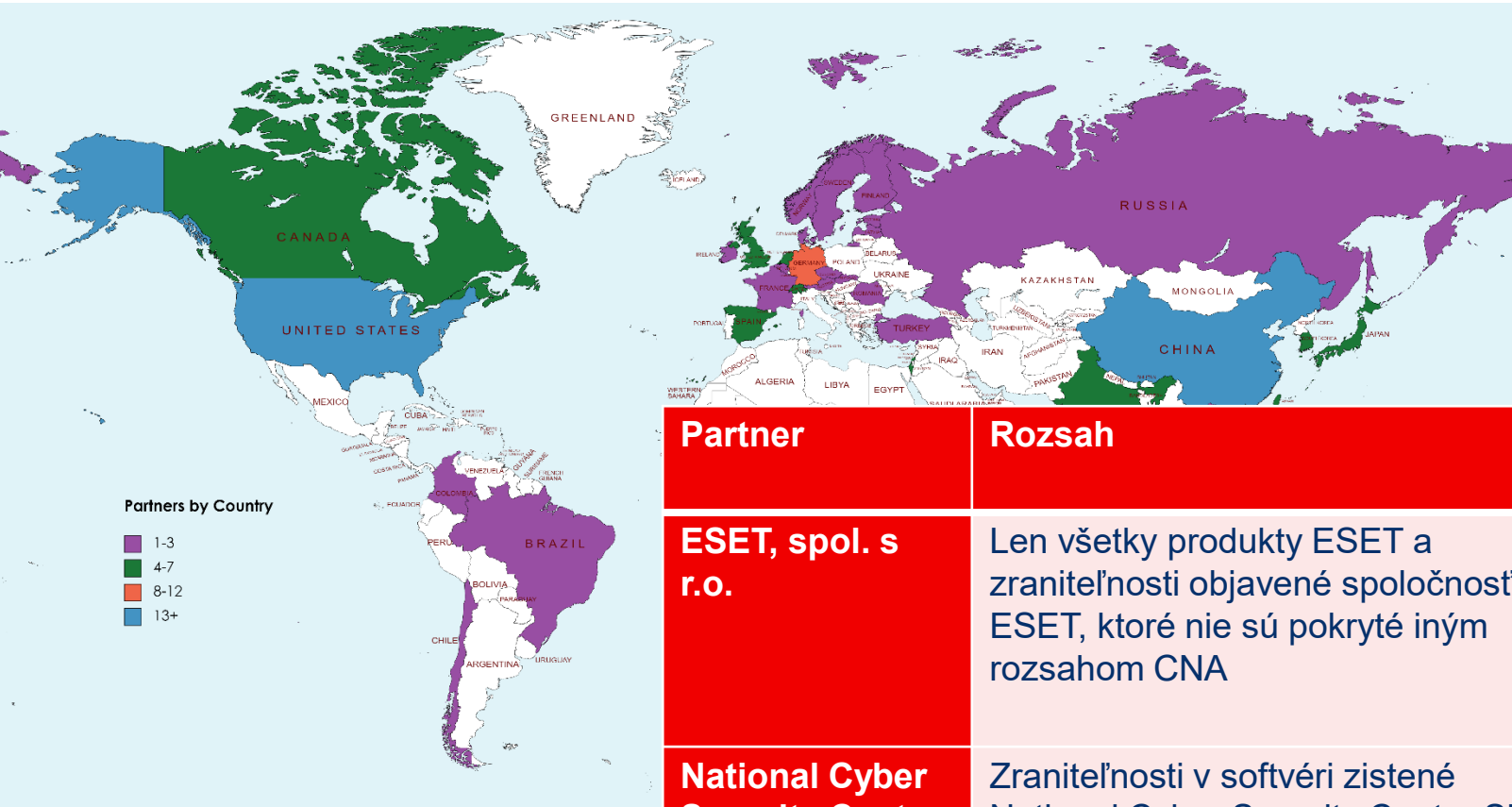
- CVE ID [číslo](#) so štyrmi alebo viacerými číslicami v časti poradového čísla daného ID (napr. „CVE-1999-0067“, „CVE-2014-12345“, „CVE-2016-7654321“).
- Stručný [popis](#) chyby zabezpečenia
- Akékoľvek relevantné [referencie](#) (t. j. správy o zraniteľnosti a upozornenia).
- Stav: Rezervované/Zverejnené/Odmietnuté

<https://www.cve.org/>



Viac ako 251 partnerov z 35 krajín participuje

Sú CNA partneri aj zo SR?



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

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

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

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.

Common Vulnerability Scoring System (CVSS)

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

Common Vulnerability Scoring System (CVSS-SIG)

- Calculator
- Specification Document**
- User Guide
- Examples
- Frequently Asked Questions
- CVSS v4.0 Documentation & Resources
- CVSS v3.1 Archive
- CVSS v3.0 Archive
- CVSS v2 Archive
- CVSS v1 Archive
- JSON & XML Data Representations
- CVSS On-Line Training Course
- Identity & logo usage

Common Vulnerability Scoring System version 4.0: Specification Document

Also available in PDF format [↗](#).

The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of four metric groups: Base, Threat, Environmental, and Supplemental. The Base group represents the intrinsic qualities of a vulnerability that are constant over time and across user environments, the Threat group reflects the characteristics of a vulnerability that change over time, and the Environmental group represents the characteristics of a vulnerability that are unique to a user's environment. Base metric values are combined with default values that assume the highest severity for Threat and Environmental metrics to produce a score ranging from 0 to 10. To further refine a resulting severity score, Threat and Environmental metrics can then be amended based on applicable threat intelligence and environmental considerations. Supplemental metrics do not modify the final score, and are used as additional insight into the characteristics of a vulnerability. A CVSS vector string consists of a compressed textual representation of the values used to derive the score. This document provides the official specification for CVSS version 4.0.

The most current CVSS resources can be found at <https://www.first.org/cvss/>

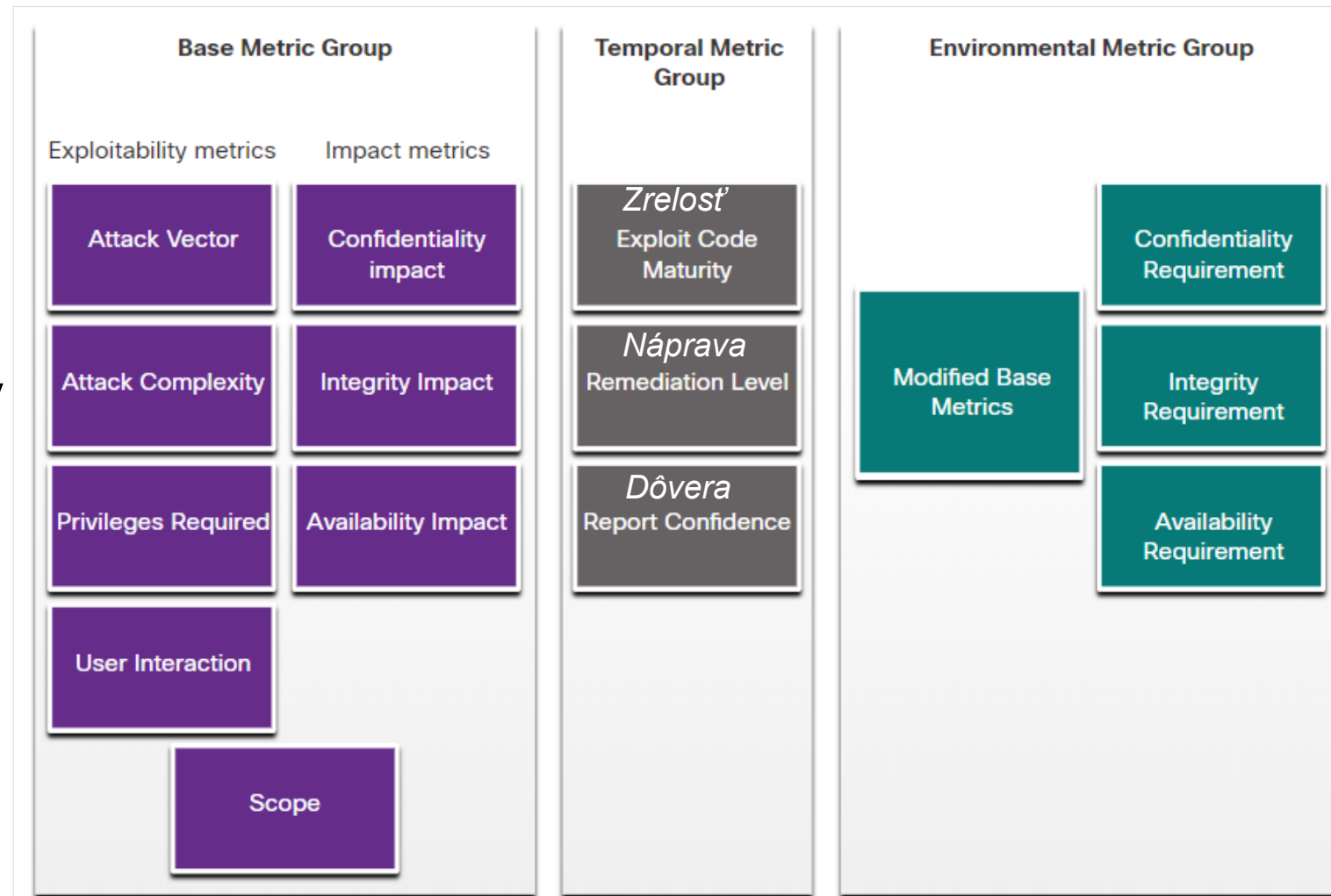
CVSS is owned and managed by FIRST.Org, Inc. (FIRST), a US-based non-profit organization, whose mission is to help computer security incident response teams across the world. FIRST reserves the right to update CVSS and this document periodically at its sole discretion. While FIRST owns all rights and interest in CVSS, it licenses it to the public freely for use, subject to the conditions below. Membership in FIRST is not required to use or implement CVSS. FIRST

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

Common Vulnerability Scoring System (CVSS)

CVSS Metric Groups

- CVSS používa tri skupiny metrick 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



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

3.8
(Low)

Base Score

Attack Vector (AV)

Network (N) Adjacent (A) Local (L) Physical (P)

Attack Complexity (AC)

Low (L) High (H)

Privileges Required (PR)

None (N) Low (L) High (H)

User Interaction (UI)

None (N) Required (R)

Scope (S)

Unchanged (U) Changed (C)

Confidentiality (C)

None (N) Low (L) High (H)

Integrity (I)

None (N) Low (L) High (H)

Availability (A)

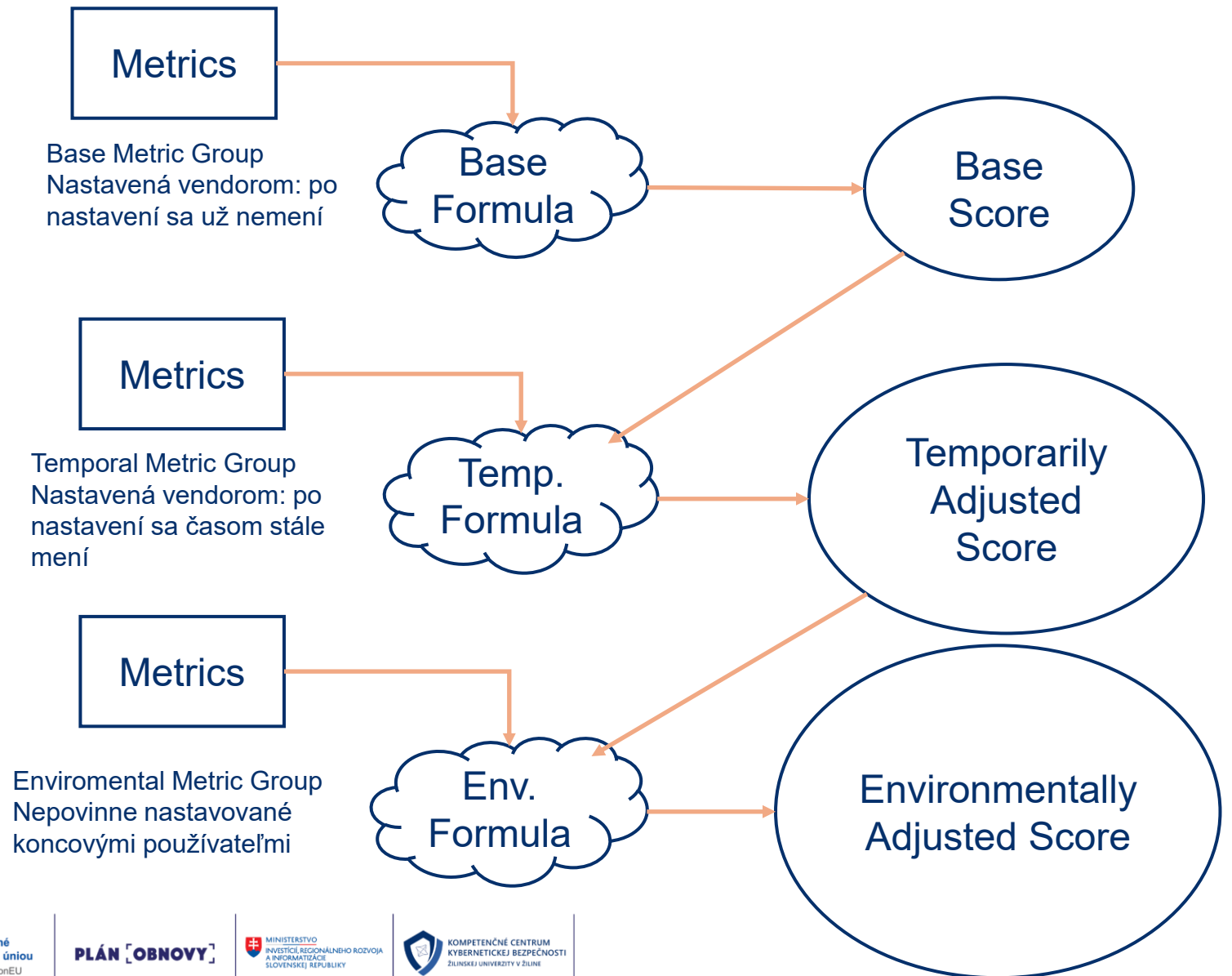
None (N) Low (L) High (H)

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

Common Vulnerability Scoring System (CVSS)

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.



Common Vulnerability Scoring System (CVSS)

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)

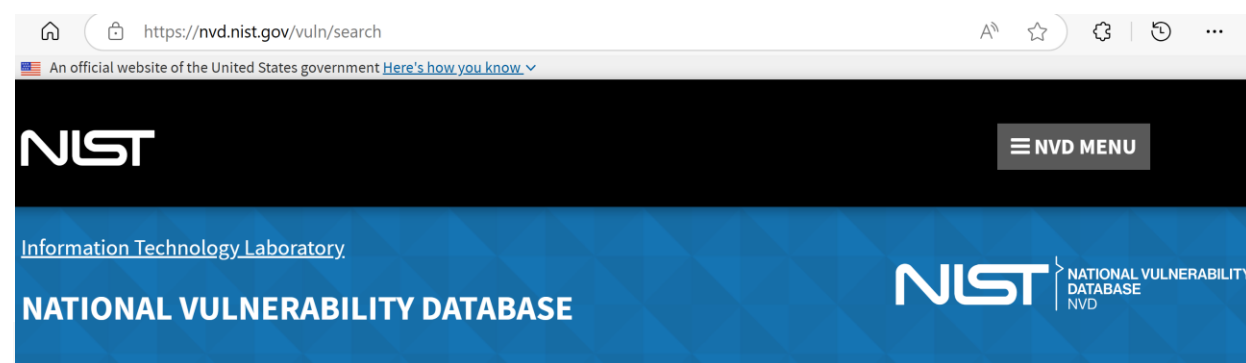
Ďalšie informačné zdroje o zraniteľnostiach

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.



Search Vulnerability Database

Try a product name, vendor name, CVE name, or an OVAL query.

NOTE: Only vulnerabilities that match ALL keywords will be returned, Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions.

Search results will only be returned for data that is populated by NIST or from source of Acceptance Level "Provider".

Search Type <input checked="" type="radio"/> Basic <input type="radio"/> Advanced	Contains HyperLinks <input type="checkbox"/> CISA Known Exploited Vulnerabilities <input type="checkbox"/> US-CERT Technical Alerts <input type="checkbox"/> US-CERT Vulnerability Notes <input type="checkbox"/> OVAL Queries
Results Type <input checked="" type="radio"/> Overview <input type="radio"/> Statistics	Contains Tags <input type="checkbox"/> Disputed <input type="checkbox"/> Unsupported When Assigned <input type="checkbox"/> Exclusively Hosted Service
Keyword Search <input type="text"/> <input type="checkbox"/> Exact Match	Search Type <input checked="" type="radio"/> All Time <input type="radio"/> Last 3 Months
<input type="button" value="Search"/> <input type="button" value="Reset"/>	

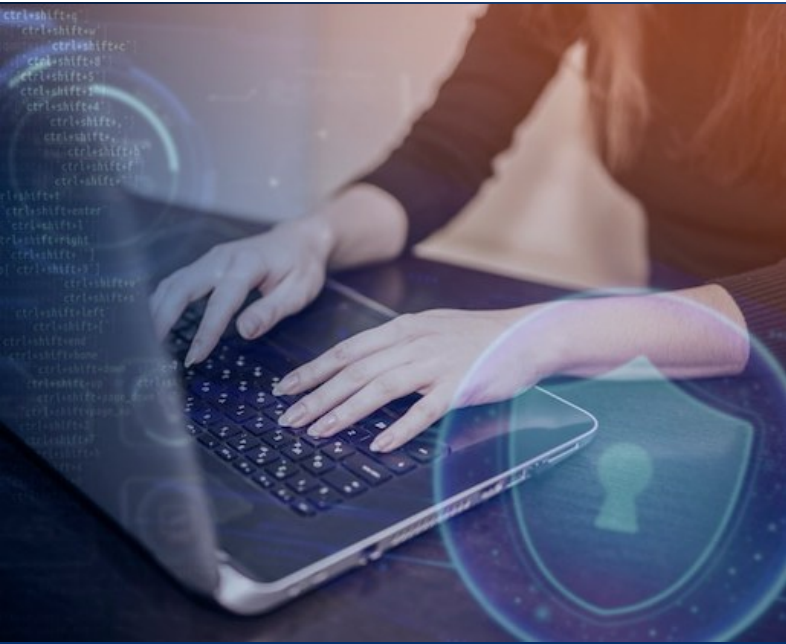
<https://nvd.nist.gov/vuln/search>

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 tester, red team, bezpečnostní konzultanti.



Konkrétna ukážka pre zisťovanie zraniteľnosti systému

**Z verejne dostupných informácií na internete
a internetových vyhľadávačov**

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

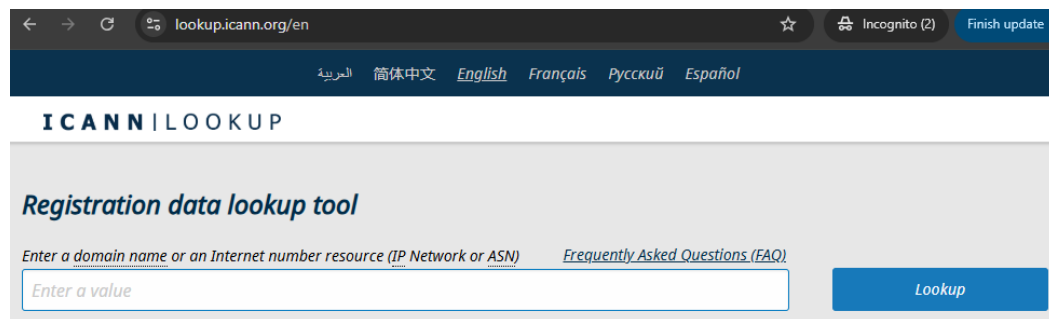
Tieto subdomény sú aktívne a prevádzkované ŠGÚDŠ, ale ich **IP adresy a rozsahy** nie sú verejne publikované.

Vyhľadávače informácií o doménach a IP adresách

WHOIS nástroje

ICANN Lookup

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

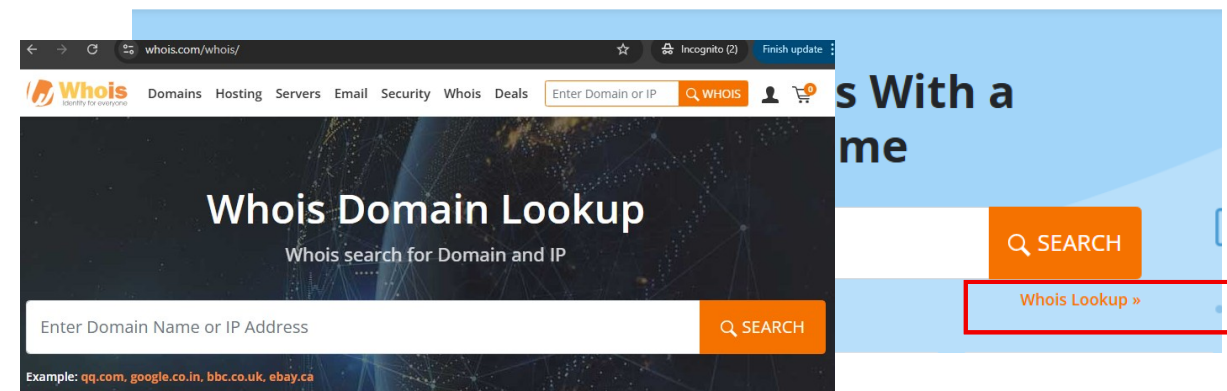


Je to užitočné pre:

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

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

← → ↻ 🌐 whois.com/whois/geology.sk



Domains Hosting Servers Email Security Whois Deals Enter [

geology.sk

Updated 1 second ago ↻

Domain:	geology.sk
Created:	2004-03-10
Valid Until:	2026-03-10
Updated:	2025-03-06
Domain Status:	ok
Nameserver:	ns.axonpro.sk
Nameserver:	ns2.axonpro.sk
Nameserver:	ns3.axonpro.sk
Domain registrant:	TTNY-0018
Name:	Štátny geologický ústav Dionýza Štúra
Organization:	Štátny geologický ústav Dionýza Štúra
Organization ID:	31753604
Phone:	+421.259375233
Email:	ladislav.nartinsky@geology.sk
Street:	Mlynská dolina 1
City:	Bratislava
Postal Code:	81704
Country Code:	SK
Authorised Registrar:	AXON-0001
Created:	2017-09-01
Updated:	2017-09-01

Príkazový riadok

```
C:\Users\Jana>ping geology.sk
```

```
Pinging geology.sk [194.160.66.21] with 32 bytes of data:  
Reply from 194.160.66.21: bytes=32 time=4ms TTL=56  
Reply from 194.160.66.21: bytes=32 time=3ms TTL=56  
Reply from 194.160.66.21: bytes=32 time=7ms TTL=56  
Reply from 194.160.66.21: bytes=32 time=7ms TTL=56
```

Ping statistics for 194.160.66.21:

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 3ms, Maximum = 7ms, Average = 5ms
```

Príkazový riadok - nslookup

```
Microsoft Windows [Version 10.0.19045.6216]  
(c) Microsoft Corporation. Všetky práva vyhradené.
```

```
C:\Users\Jana>nslookup  
Default Server:  dns.google  
Address:  8.8.8.8
```

```
> set type=SOA  
> geology.sk  
Server:  dns.google  
Address:  8.8.8.8
```

```
Non-authoritative answer:  
geology.sk  
    primary name server = geolsurv.geology.sk  
    responsible mail addr = postmaster.geology.sk  
    serial = 20240726  
    refresh = 10800 (3 hours)  
    retry = 3600 (1 hour)  
    expire = 604800 (7 days)  
    default TTL = 38400 (10 hours 40 mins)
```

Príkazový riadok - nslookup

```
> set type=A  
> geolsurv.geology.sk  
Server:  dns.google  
Address:  8.8.8.8  
  
Non-authoritative answer:  
Name:    proxy.geology.sk  
Address: 194.160.66.28  
Aliases: geolsurv.geology.sk
```

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



The global coordination of the DNS Root, IP addressing, and other Internet protocol resources is performed as the Internet Assigned Numbers Authority (IANA) functions. [Learn more.](#)

Domain Names

Management of the DNS Root Zone (assignments of ccTLDs and gTLDs) along with other functions such as the .int and .arpa zones.

- Root Zone Management
- Database of Top Level Domains
- .int Registry
- .arpa Registry
- IDN Practices Repository

Number Resources

Coordination of the global IP and AS number spaces, such as allocations made to Regional Internet Registries.

- IP Addresses & AS Numbers
- Network abuse information

Protocol Assignments

The central repository for protocol name and number registries used in many Internet protocols.

- Protocol Registries
- Apply for an assignment
- Time Zone Database

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

<https://whois.ipip.net/>

IP Address Ranges Graph v4 Graph v6 Upstreams Downstreams IX Whois

AS Number
AS2607

AS Name
SANET

Org Name
Zdruzenie pouzivatelov Slovenskej akademickej datovej siete SANET

Country
Slovakia

Registry
ripe

RegDate
2018-11-22T15:27:18Z

Updated
2018-11-22T15:27:18Z

AS2607 Looking Glass

IPv4Prefixes
39

IPv6Prefixes
3

IPv4 NUMs
526,080

IPv6 NUMs(64)
4,294,967,296

526,080 IPv4 Addresses

IPV4 Ranges IPv6 Ranges

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 datovej siete
193.87.128.0/17	🔍 ✓	NBSNET
194.160.0.0/17	🔍 ✓	Zdruzenie pouzivatelov Slovenskej akademickej datovej siete
194.160.0.0/16	🔍 ✓	Zdruzenie pouzivatelov Slovenskej akademickej datovej siete
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

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

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.

Shodan

SHODAN Explore Pricing ↗ Search Login

Search Engine for the Internet of Everything

Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.

SIGN UP NOW

Vyhľadávač pre zariadenia pripojené k internetu (vrátane ich zraniteľností)

Vyhľadanie informácií cez shodan.io

shodan.io/host/194.160.66.48

SHODAN Explore Downloads Pricing Search Account

194.160.66.48 Regular View Raw Data Timeline

// TAGS: eol-product // LAST SEEN: 2025-09-02

General Information

Hostnames	geology.sk 48.geology.sk
Domains	geology.sk
Country	Slovakia
City	Bratislava
Organization	State Geological Institute of Dionyz Stur
ISP	Zdruzenie pouzivatelov Slovenskej akademickej datovej siete SANET

Open Ports

80	443	1883	8000
----	-----	------	------

// 80 / TCP -70800581 | 2025-08-23T10:25:54.665599

nginx 1.20.2

Mapportal ŠGÚDŠ

HTTP/1.1 200 OK
Server: nginx/1.20.2
Date: Sat, 23 Aug 2025 10:25:54 GMT
Content-Type: text/html
Content-Length: 9619
Last-Modified: Wed, 06 Dec 2023 11:35:14 GMT

Vyhľadávač pre zariadenia pripojené k internetu (vrátane ich zraniteľností)

Vyhľadanie informácií cez shodan.io (pokrač.)

shodan.io/host/194.160.66.48

Organization: **State Geological Institute of Dionyz Stur**

ISP: **Zdruzenie pouzivatelov Slovenskej akademickej datovej siete SANET**

ASN: **AS2607**

Vulnerabilities All ports Latest

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

2023 (1)

CVE-2023-44487 7.5 The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

2021 (1)

CVE-2021-3618 7.4 ALPACA is an application layer protocol content confusion attack, exploiting TLS servers implementing different protocols but using compatible certificates, such as multi-domain or wildcard certificates. A MITM attacker having access to victim's traffic at the TCP/IP layer can redirect traffic from one subdomain to another, resulting in a valid TLS session. This breaks the authentication of TLS and cross-protocol attacks may be possible where the behavior of one protocol service may compromise the other at the application layer.

Server: nginx/1.20.2
Date: Sat, 23 Aug 2025 10:25:54 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,Ke
-Control,Content-Type
Accept-Ranges: bytes

Vulnerabilities

0 2 0 0 0

// 443 / TCP

nginx 1.20.2

Mapportal ŠGÚDŠ

HTTP/1.1 200 OK
Server: nginx/1.20.2
Date: Sun, 31 Aug 2025 14:54:37 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-Methods: GET, POST, OPTIONS
Access-Control-Allow-Headers: DNT,X-CustomHeader,Ke
-Control,Content-Type,Content-Range,Range
Access-Control-Expose-Headers: DNT,X-CustomHeader,Ke
-Control,Content-Type,Content-Range,Range

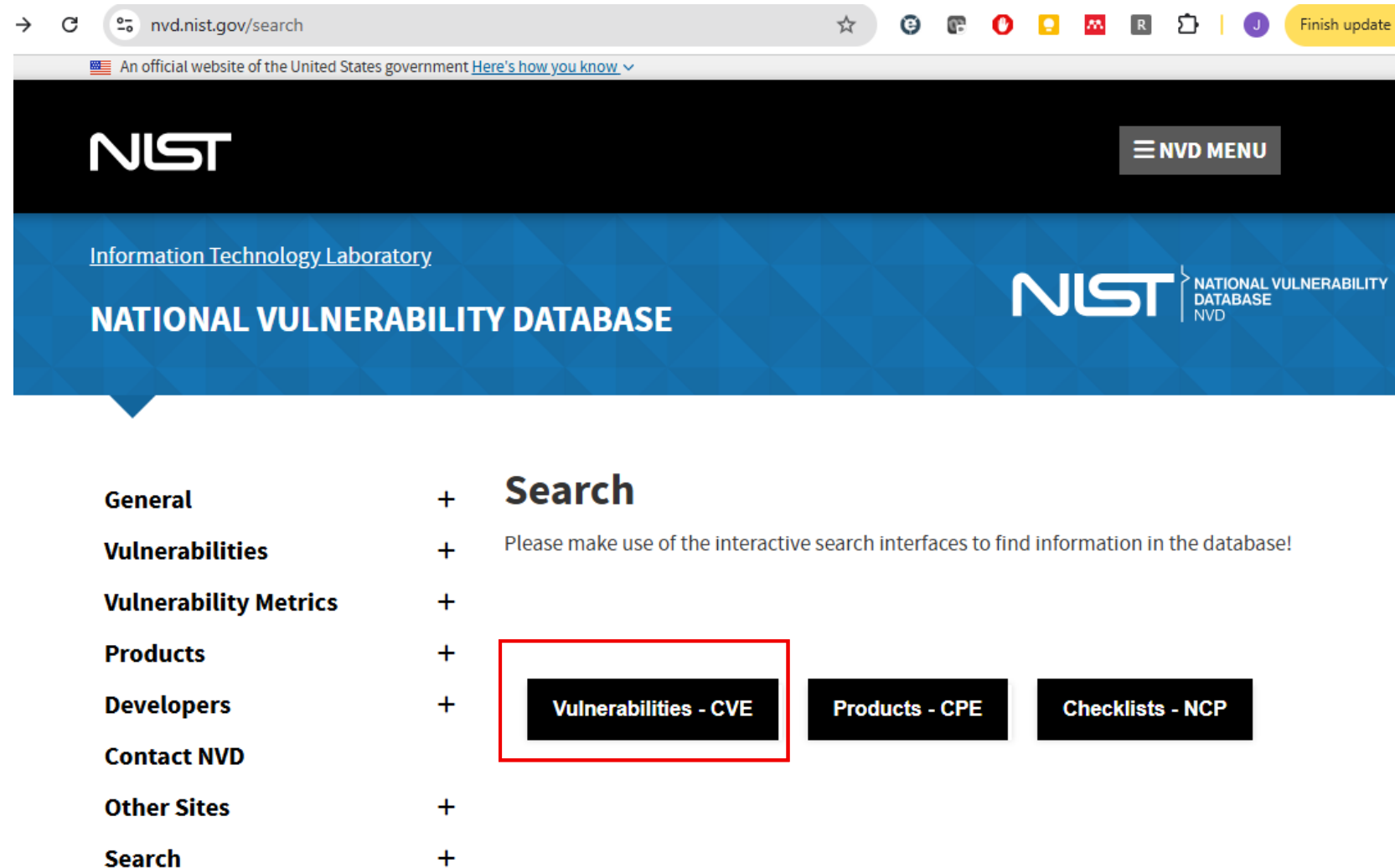
Filter na zraniteľnosti

The screenshot shows a web browser window with the URL `shodan.io/search?query=vuln:CVE-2023-44487`. The browser's navigation bar includes tabs for 'Shodan', 'Maps', 'Images', 'Monitor', 'Developer', and 'More...'. Below the browser, the Shodan website interface is visible, featuring a search bar with the query `vuln:CVE-2023-44487` and a search button. A prominent error message is displayed in a red box, stating: **Error:** The "vuln" filter is only available to Academic users or Small Business API subscription and higher.

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.



The screenshot shows the NIST National Vulnerability Database search interface. The browser address bar displays 'nvd.nist.gov/search'. The page header includes the NIST logo and 'Information Technology Laboratory'. The main heading is 'NATIONAL VULNERABILITY DATABASE'. Below the heading, there is a search section with the text 'Please make use of the interactive search interfaces to find information in the database!'. A red box highlights the 'Vulnerabilities - CVE' button, which is one of three buttons: 'Vulnerabilities - CVE', 'Products - CPE', and 'Checklists - NCP'. A sidebar on the left contains a list of menu items: General, Vulnerabilities, Vulnerability Metrics, Products, Developers, Contact NVD, Other Sites, and Search, each with a plus sign next to it.

Konkrétna ukážka pre zisťovanie zraniteľnosti systému

Vyhľadávanie informácií o zraniteľnostiach

- CVE-2023-44487

The screenshot shows the NVD Vulnerability Search interface. The search bar contains the text "CVE-2023-44487". Below the search bar, there is a button labeled "Advanced" and a "Reset" button. The search results are displayed in a table with the following columns: Identifier, CISA Key Info, Published Date, CNA, and Description. The first result is highlighted with a red box and shows the identifier "CVE-2023-44487", a green checkmark in the CISA Key Info column, a published date of "2023-10-10", and a CNA of "MITRE". The description for this entry is: "The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023."

Identifier	CISA Key Info	Published Date	CNA	Description
CVE-2023-44487	✓	2023-10-10	MITRE	The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

Konkrétna ukážka pre zisťovanie zraniteľnosti systému

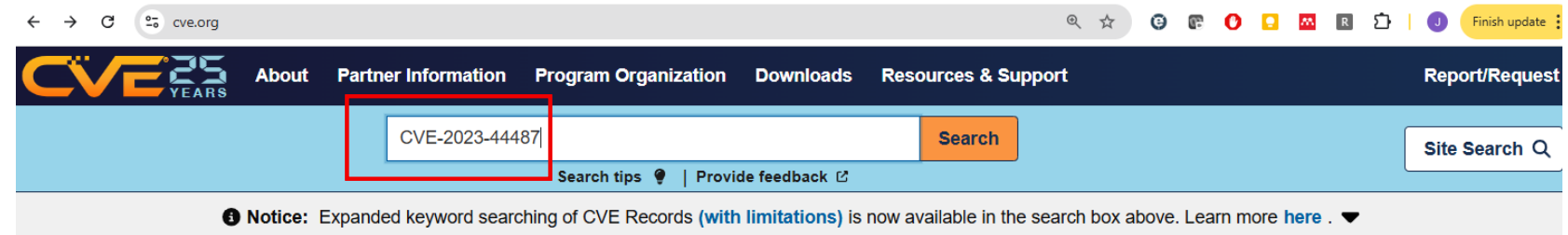
cve.org

- CVE Record User Guide

- <https://www.cve.org/CVERecord/UserGuide/#cve-key>

- Vyhľadávanie informácií o:

CVE-2023-44487



CVE™ Program Mission

Identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.

There are currently over **292,000** CVE Records accessible via **Download** or **Keyword Search** above.

The CVE Program partners with community members worldwide to grow CVE content and expand its usage. Click below to learn more about the role of **CVE Numbering Authorities (CNAs)** and **Roots**.

[Learn More](#) [Become a Partner](#)

News

- [Searching for Patterns Now Available in “CVE List Keyword Search” on CVE.ORG Website](#)
- [Vulnerability Data Enrichment for CVE Records: 243 CNAs on the Enrichment Recognition List for September 2, 2025](#)
- [CVE Program Report for Quarter 2 Calendar Year \(Q2 CY\) 2025](#)
- [AxxonSoft Added as CVE Numbering Authority \(CNA\)](#)

NEWS ICONS¹

Access

- [List of Partners](#)
- [CNA Rules](#)
- [CVE Record Lifecycle](#)
- [CVEProject on GitHub for Development](#)
- [Idea tracker](#)

Learn

- [About CVE](#)
- [Process](#)
- [Program Organization](#)
- [CVE 25th Anniversary Report](#)
- [Related Efforts](#)
- [Terminology](#)
- [CVE Services for CNAs](#)

Report/Request

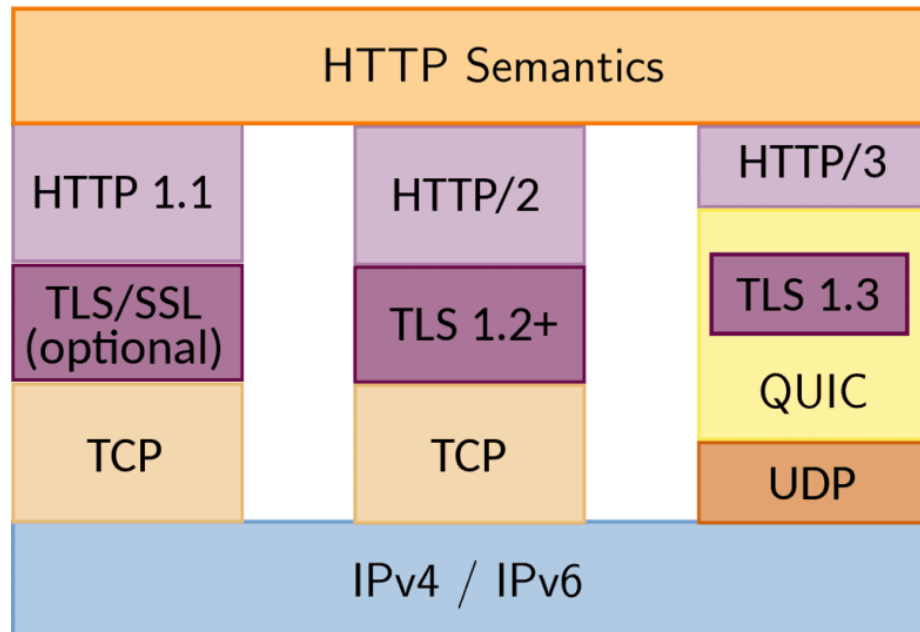
- [Report vulnerability/Request CVE ID](#)
- [Request CVE Record be published/updated](#)
- [Report the use of a reserved CVE ID](#)

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/>



CVE-2023-44487 PUBLISHED View JSON | User Guide

Required CVE Record Information

CNA: MITRE Corporation

Published: 2023-10-10 Updated: 2025-06-07

Description

The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

Product Status
Learn more

Information not provided

References 144 Total

- <https://github.com/dotnet/core/blob/e4613450ea0da7fd2fc6b61dfb2c1c1dec1ce9ec/release-notes/6.0/6.0.23/6.0.23.md?plain=1#L73>

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

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>

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 -

SUMMARY

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

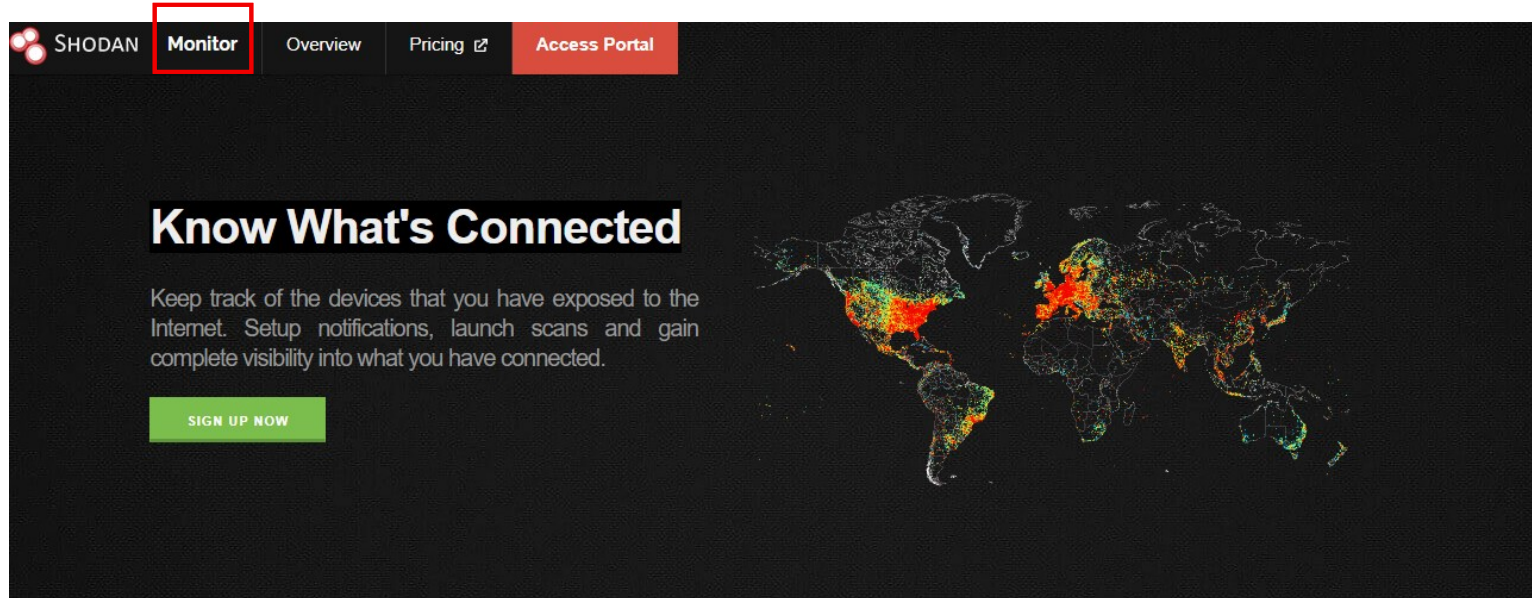
If you have any questions, contact us at support@shodan.io or call at +1 740-746-3261.

Choose Your Plan

No contracts. No setup fees. Cancel anytime.

Freelancer	Small Business	Corporate
\$69 /month	\$359 /month	\$1099 /month
LOGIN TO SUBSCRIBE	LOGIN TO SUBSCRIBE	LOGIN TO SUBSCRIBE
<ul style="list-style-type: none"> Up to 1 million results per month* Scan up to 5,120 IPs per month Network Monitoring for 5,120 IPs 	<ul style="list-style-type: none"> Up to 20 million results per month* Scan up to 65,536 IPs per month Network Monitoring for 65,536 IPs 	<ul style="list-style-type: none"> Unlimited results per month* Scan up to 327,680 IPs per month Network Monitoring for 327,680 IPs
<ul style="list-style-type: none"> Access to most filters Allows paging through search results Basic access to the Streaming API Commercial Use 	<ul style="list-style-type: none"> Access to most filters Allows paging through search results Basic access to the Streaming API Commercial Use 	<ul style="list-style-type: none"> Access to all filters Allows paging through search results Basic access to the Streaming API Commercial Use
<ul style="list-style-type: none"> Grandfathered Pricing E-Mail support 	<ul style="list-style-type: none"> Grandfathered Pricing E-Mail support Vulnerability search filter 	<ul style="list-style-type: none"> Grandfathered Pricing Premium Support Vulnerability search filter Batch IP Lookups Tag Search Filter InternetDB API Commercial Use Complementary Membership Upgrades

S liceniou: aj možnosť monitorovať (svoje) zariadenia



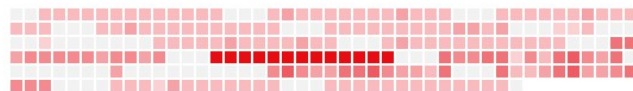
Network Monitoring Made Easy

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.



Small network

198.20.68.0/24



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)

monitor.shodan.io/networks

Shodan Maps Images Monitor Developer More...

SHODAN Monitor Dashboard **Manage Assets** Events Log Settings

Manage Assets

ADD NETWORK ADD DOMAIN ADD SEARCH QUERY

geology.sk	194.160.66.48/32	1 IP	malware, open_database, ai, iot, end_of_life, internet_scanner, industrial_control_system, new_service, ssl_expired, vulnerable	
gymrk.sk	194.160.142.194/32	1 IP	malware, open_database, ai, iot, end_of_life, internet_scanner, industrial_control_system, new_service, ssl_expired, vulnerable	
sczsk.sk	195.146.133.107/32	1 IP	malware, open_database, ai, iot, end_of_life, internet_scanner, industrial_control_system, new_service, ssl_expired, vulnerable	

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
Port

[geology.sk](#)
Asset Group

end_of_life
Trigger

nginx 1.20.2

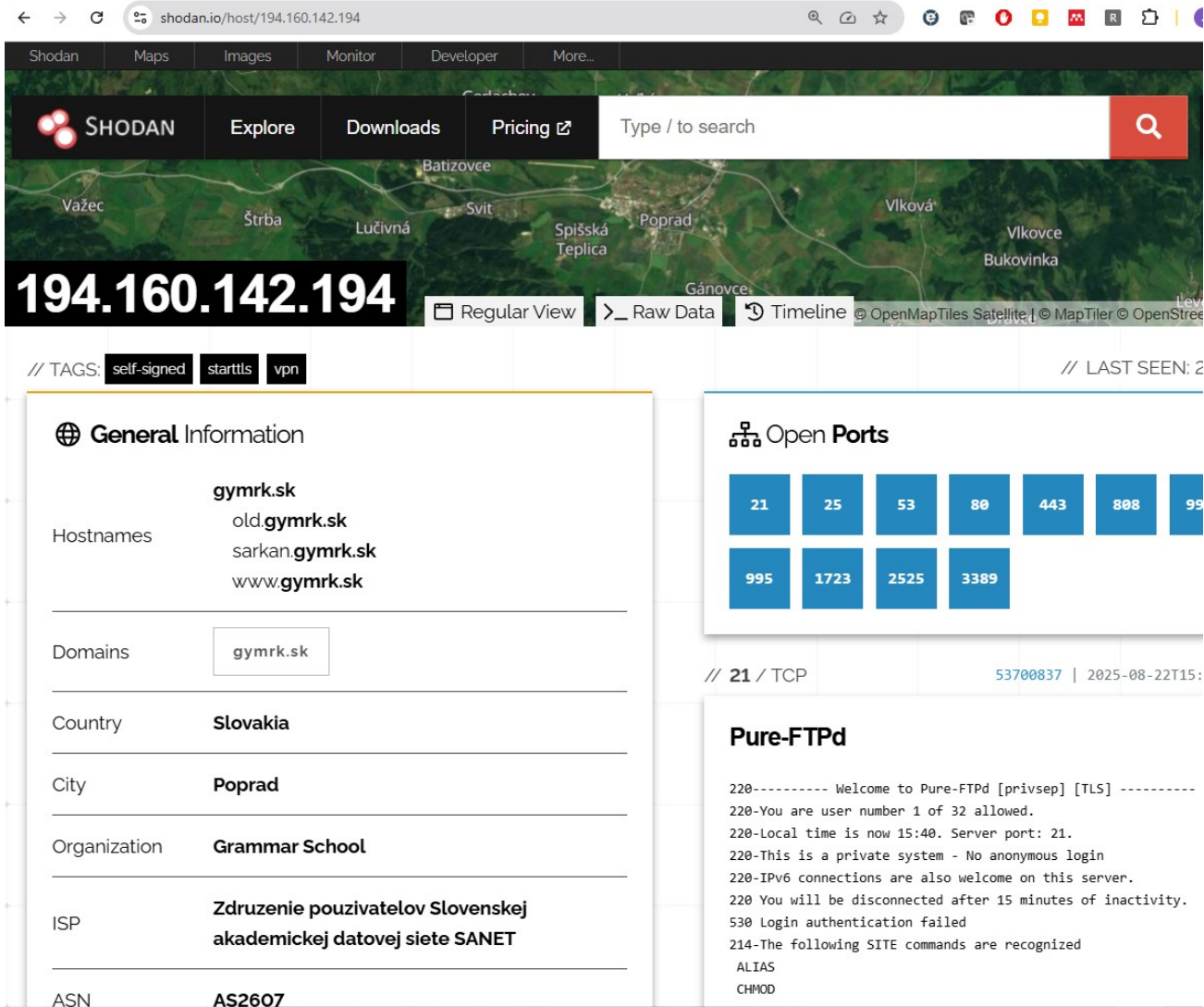
```
HTTP/1.1 200 OK
Server: nginx/1.20.2
Date: Thu, 04 Sep 2025 13:44:23 GMT
Content-Type: text/html
Content-Length: 9619
Last-Modified: Wed, 06 Dec 2023 11:35:14 GMT
Connection: keep-alive
ETag: "65705c72-2593"
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: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

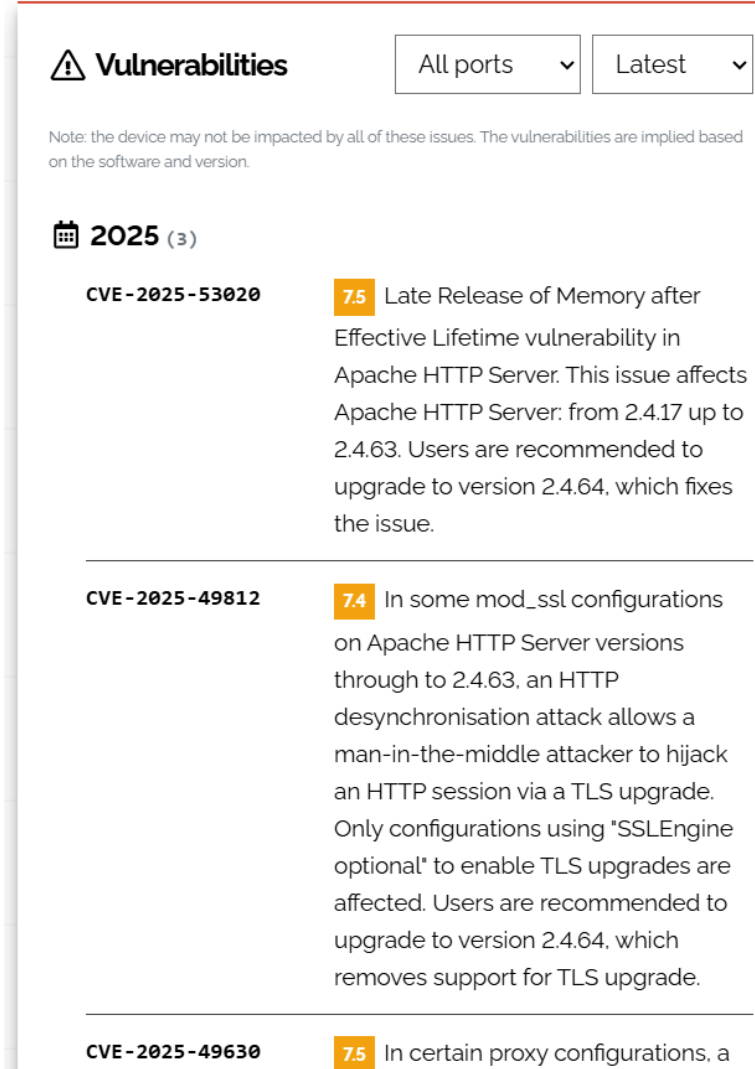
Konkrétna ukážka pre zisťovanie zraniteľnosti systému

Vyhľadanie informácií cez shodan.io



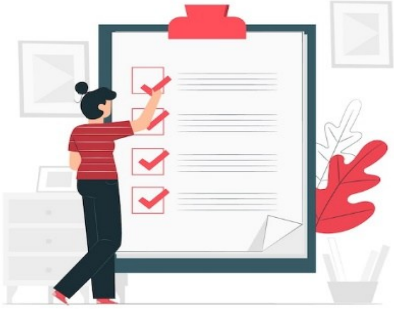
The screenshot shows the Shodan interface for the IP address 194.160.142.194. The main map area displays a satellite view of the Poprad region in Slovakia. Below the map, the IP address is prominently displayed. The interface includes navigation tabs like 'Shodan', 'Maps', 'Images', 'Monitor', 'Developer', and 'More...'. A search bar is present with the text 'Type / to search'. Below the map, there are view options: 'Regular View', 'Raw Data', and 'Timeline'. The page is tagged with 'self-signed', 'starttls', and 'vpn'. The 'General Information' section lists hostnames (gymrk.sk, old.gymrk.sk, sarkan.gymrk.sk, www.gymrk.sk), domains (gymrk.sk), country (Slovakia), city (Poprad), organization (Grammar School), ISP (Združenie používateľov Slovenskej akademickej datovej siete SANET), and ASN (AS2607). The 'Open Ports' section shows a grid of port counts: 21, 25, 53, 80, 443, 808, 995, 995, 1723, 2525, 3389. Below this, a specific port entry is shown: '21 / TCP' with IP '53700837' and timestamp '2025-08-22T15:'. The 'Pure-FTPd' section displays a sample log output.

```
220----- Welcome to Pure-FTPd [privsep] [TLS] -----
220-You are user number 1 of 32 allowed.
220-Local time is now 15:40. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
530 Login authentication failed
214-The following SITE commands are recognized
ALIAS
CHMOD
```



The screenshot shows the 'Vulnerabilities' section of the Shodan interface. It features a dropdown menu for 'All ports' and another for 'Latest'. A note states: 'Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.' Below this, there is a calendar icon and the text '2025 (3)'. Two vulnerability entries are visible:

- CVE-2025-53020** (7.5): Late Release of Memory after Effective Lifetime vulnerability in Apache HTTP Server. This issue affects Apache HTTP Server: from 2.4.17 up to 2.4.63. Users are recommended to upgrade to version 2.4.64, which fixes the issue.
- CVE-2025-49812** (7.4): In some mod_ssl configurations on Apache HTTP Server versions through to 2.4.63, an HTTP desynchronisation attack allows a man-in-the-middle attacker to hijack an HTTP session via a TLS upgrade. Only configurations using "SSLEngine optional" to enable TLS upgrades are affected. Users are recommended to upgrade to version 2.4.64, which removes support for TLS upgrade.
- CVE-2025-49630** (7.5): In certain proxy configurations, a



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 zraniteľností?** (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 zneužitá
 - 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