FENIX

Popis testů Fenix Checker

11.4.2023

NIX.CZ z.s.p.o.
Americká 23, Praha 2
130 52 Czech Republic
http://www.nix.cz

NIX·CZ

DNS for domain

Pro doménové jméno uložené v systému NIX.CZ jsou přeloženy IP adresy z DNS záznamů pro A, AAAA, NS a MX. Záznamy A a AAAA jsou překládány bez www prefixu i s ním.
Pro načtení záznamu je použitá Python třída dns, metoda

```
dns.resolver.Resolver.resolve(domain, record_type)
```

DNS servery použité pro překlad jsou následující (v daném pořadí):

- 93.190.134.172
- 2a02:38:2::172
- 193.17.47.1
- 2001:148f:ffff::1

Úspěšné splnění testů je v případě, kdy se povedlo **přeložení každého z těchto záznamů**.

Reachability

Test se skládá z pokusu o navázání spojení s každým ze serverů, jejichž adresy jsou získané v "DNS for domain". Na každou adresu je proveden pokus o spojení protokolem

- ICMP
- UDP a TCP
    - port 80
    - port 443
    - port 21
    - port 22
    - port 53
    - port 25

Testování probíhá programem Scapy (viz https://scapy.net/), voláním metody sr1 - port považujeme otevřený, pokud server odpoví (v případě UDP / ICMP), a pokud odešle zpět SYN-ACK packet (pouze v případě TCP). V případě, že komunikace není úspěšná, je test konkrétní adresy a protokolu/portu zopakován znovu po uplynutí 1s.
Vyžadována je odpověď ICMP, nebo odezva na alespoň jednom TCP / UDP portu - při nalezení již další porty ani protokoly pro danou adresu testované nejsou.
Pro **úspěšné absolvování testu** je nutné získat **odezvu od každé** testované **adresy**.

DNS AAAA for NS and MX

Test je považován za **splněný, pokud je alespoň jeden z NS záznamů**, získaných překladem v testu "DNS for domain", **IPv6 adresou**. V rámci testu je ověřena i IPv6 adresa pro MX záznam; její absence je označena oranžovou barvou výsledku a varováním.

DNSSEC

Pro doménové jméno uložené v systému NIX.CZ je získán první NS server - stejným způsobem jako v případě testování "DNS for domain". Na tento server je následně odeslán (pomocí Python třídy *dns*) požadavek pro vrácení DNSSEC klíče:

```
dns.message.make_query(f"{domain}.", dns.rdatatype.DNSKEY,
want_dnssec=True)
```

Dotaz na získání dat je proveden přes UDP protokol, v případě že dorazí odpověď, která je zkrácená (TC=1), je zopakována pomocí TCP protokolu.
V odpovědi jsou očekávány záznamy typu TYPE0 a DNSKEY - tyto jsou poté použity pro sestavení požadavku na validaci:

```
dns.dnssec.validate(type0_answer, dnskey_answer, {name: type0_answer})
```

Součástí testu je vyhodnocení použitých šifrovacích algoritmů.
(viz https://datatracker.ietf.org/doc/html/rfc8624#section-3.1)

Nepovolené algoritmy:

- RSAMD5
- DSA
- DSANSEC3SHA

Algoritmy, u kterých je zobrazeno varování (použitý klíč je příliš dlouhý):

- RSASHA1
- RSASHA1NSEC3SHA1
- RSASHA512

Test je vyhodnocený jako **nesplněný**, když volání validační funkce **vrátí vyjímku ValidationFailure** nebo je použitý **nepovolený algoritmus**.

Viz dokumentace na https://dnspython.readthedocs.io/en/latest/dnssec.html a
Pro kontrolu je vhodné použít nástroj https://dnsviz.net/f

DANE SMTP

Test na zjištění podpory DNS-based Authentication of Named Entities (DANE), používá pro ověřování adresu DNS serveru, získanou v DNSSEC testu - pokud tento test selže, není možné pokračovat v DANE SMTP.

TLSA request je vytvořen pro port 25, protokol TCP a první nalezený MX server, např. *_25._tcp.postino.cesnet.cz*

```
        import dns

        for answer in dns.query.udp(tlsa_request, ns_ip).answer:

                for record in answer:

                        if isinstance(record, dns.rdtypes.ANY.TLSA.TLSA):

                                tlsa_records.append((record, tlsa_request_addr))
```

Certifikát pro ověření je načten z poštovního serveru připojením přes knihovnu OpenSSL (pyOpenSSL).
V souvislosti s doporučení v RFC 7672 používáme pouze TLSA záznamy která mají v sekci *Certificate Usage* hodnoty

- 2 - certifikát CA (DANE-TA: Trust Anchor Assettation)
- 3 - certifikát serveru (DANE-EE: Domain Issued Certificate)

Kontrola je provedena podle kompletních Selector i Matching Type možností v TLSA záznamu -

```
from cryptography import x509

import hashlib

cert = x509.load_pem_x509_certificate(str.encode(pem_cert_z_openssl_mx))
```

Selector:

- 0 - celý certifikát

```
certdata = cert.public_bytes(Encoding.DER)
```

- 1 - veřejný klíč certifikátu

```
certdata = cert.public_key().public_bytes(Encoding.DER, PublicFormat.SubjectPublicKeyInfo)
```

Matching Type - porovnávána je cert část TLSA záznamu:

- 0 - celý obsah

```
result = tlsa.cert.hex() == certdata.hex()
```

- 1 - SHA-256 hash

```
result = tlsa.cert.hex() == hashlib.sha256(certdata).hexdigest()
```

- 2 - SHA-512 hash

```
result = tlsa.cert.hex() == hashlib.sha512(certdata).hexdigest()
```

Test je považovaný za **splněný**, pokud j**e DNS server zabezpečený**, a alespoň jeden nalezený **TLSA souhlasí s daty** daného **SMTP serveru**.

RPKI test

Podkladová data pro test jsou načtena ze dvou zdrojů -

- FTAS - data za předchozí den (případně nejbližší možný za který jsou dostupná data, kontroluje se 10 dnů zpět). Z těchto dat jsou vybrány 3 zákaznické IPv4, které mají nejvyšší počet přenesených B za daný den.
- DNS záznamy A pro testovanou doménu.

Pro každou z těchto IP adres je testováno spojení ze zdrojové adresy 91.207.231.10 pro IPv4 a 2a02:39::10 pro IPv6 protokolem

- ICMP
- UDP a TCP
    - port 80
    - port 443
    - port 21
    - port 22
    - port 53

Testování probíhá programem Scapy (viz https://scapy.net/), voláním metody *sr1* - port považujeme otevřený, pokud přijde ze serveru odpověď.
Do výsledku jsou zapsané všechny testované IP adresy. Pro ty, které testem neprojdou je uveden i protokol / port na který bylo provedeno testování.

Test je splněn, pokud **není nalezena** žádná **komunikující adresa.**

RTBH test

Podkladová data pro test jsou načtena ze tří zdrojů -

- FTAS - data za předchozí den (případně nejbližší možný za který jsou dostupná data, kontroluje se 10 dnů zpět). Z těchto dat jsou vybrány 3 zákaznické IPv4 a 3 zákaznické IPv6, které mají nejvyšší počet přenesených B za daný den.
- DNS záznamy A pro doménu.
- DNS záznamy AAAA pro testovanou doménu.

Pro každou z těchto adres je testováno spojení ze zdrojové adresy *93.190.130.10* (pro IPv4) a *2a02:38:bbbb::10* (pro IPv6) protokolem

- ICMP
- UDP a TCP
    - port 80
    - port 443
    - port 21
    - port 22
    - port 53

Testování probíhá programem Scapy (viz https://scapy.net/), voláním metody *sr1* - port považujeme otevřený, pokud přijde ze serveru odpověď.
Do výsledku jsou zapsané všechny testované IP adresy. Pro ty, které testem neprojdou je uveden i protokol / port na který bylo provedeno testování.

Test je splněn, pokud **není nalezena** žádná **komunikující adresa.**

BGP validity

Zdrojem dat jsou servery secrs-1.nix.cz a secrs-2.nix.cz, z nichž jsou vyfiltrovány ohlašované prefixy dle ASN testovaného subjektu.

```
https://birdspy.nix.cz/api/{route_server}/bgp/protocols

https://birdspy.nix.cz/api/{route_server}/bgp/protocol/{table}/routes

route_server = ["nix-secrs-1", "nix-secrs-2"]
```

V těchto tabulkách jsou vyhledány všechny prefixy označené komunitami:

- 47200:1101:*
- 47200:64512 RPKI_INVALID
- 47200:64513 RPKI_UNKNOWN

Test je úspěšný, pokud **není nalezen** žádný **prefix v nevalidní komunitě**.

BGP consistency

Zdrojem dat jsou servery secrs-1.nix.cz a secrs-2.nix.cz, z nichž jsou vyfiltrovány ohlašované prefixy dle ASN testovaného subjektu.

```
https://birdspy.nix.cz/api/{route_server}/bgp/protocols

https://birdspy.nix.cz/api/{route_server}/bgp/protocol/{table}/routes

route_server = ["nix-secrs-1", "nix-secrs-2"]
```

V případě, že pro kontrolovaný prefix existuje nadřazená síť, která testem na konzistenci projde, je použitý její výsledek testu.
Hodnotí se shoda ohlašovaných prefixů na všech serverech. Skóre testu je vypočítané jako procentuální poměr celkového počtu nalezených nevalidních prefixů k celkového počtu prefixů.

Test je splněn, když není nalezen žádný nekonzistentní záznam - **skóre je** tedy **100%**.

CoPP test

Zdrojem dat jsou servery secrs-1.nix.cz a secrs-2.nix.cz, z nichž jsou vyfiltrovány ohlašované prefixy dle ASN testovaného subjektu. V průběhu procházení prefixů sestavujeme unikátní seznam next-hop IP adres.

```
https://birdspy.nix.cz/api/{route_server}/bgp/protocols

https://birdspy.nix.cz/api/{router_server}/bgp/protocol/{table}/routes

route_server = ["nix-secrs-1", "nix-secrs-2"]
```

Sesbírané next-hop IP adresy jsou podrobeny testu na otevřené porty:

- TCP, UDP
  - 7 *echo*
  - 9 *discard*
  - 13 *daytime*
  - 19 *chargen*
  - 53 *dns*
  - 123 *ntp*
- TCP
  - 20 *ftp-data*
  - 21 *ftp*
  - 22 *ssh*
  - 23 *telnet*
  - 80 *http*
  - 443 *https*
  - *830* *netconf*

K testování je použita knihovna Scapy (viz https://scapy.net/), voláním metody *sr1* - port považujeme za otevřený, pokud server odpoví (v případě UDP), či pokud odešle zpět SYN-ACK packet (pouze v případě TCP).

Pro splnění testu je nutné, aby nebyla nalezena **žádná adresa s otevřeným portem**. Do výsledku jsou zapsané všechny testované IP adresy, u kterých byl nalezen otevřený port - včetně informace o portu a protokolu.

CSIRT test

Jako podklad testu jsou použita data stažená z url:
https://www.trusted-introducer.org/directory/teams.json
Podle ASN jsou dohledány příslušené záznamy v polích
`["constituency"]["asns"]`

Pro splnění testu je nutné, aby záznam v poli `["classification"]` obsahoval hodnoty

- **Listed**
- **Certified**
- **Accredited**

Pro tento test je možné i zobrazení varování - pokud je nalezená klasifikace Listed, a certifikátu zbývají méně než 3 měsíce do uplynutí 3 let po vydání (reprezentované datem v poli `["classification"]["since"]`)

RFC1918 test

Pro tento test jsou klíčová data navrácená z FTAS systému.
https://ftas.srv.nix.cz/ftas_reports/NIX.CZ/NIX/NIX_private_IPs_from_peers/last_86400/results.json
Z této url jsou stažena podkladová data, ve který jsou následně podle ASN testovaného subjektu sečteny hodnoty v poli *pkts* pro každou nalezenou IP adresu.
Test je považován za **splněný**, **pokud je součet nalezených hodnot** roven **0**.
V současné době je test pozastavený, do doby vyřešení nekonzistentních dat vrácených FTAS systémem.

Port overload test

Test kontroluje počet sekund, kdy je kapacita linky směrem od (v PDF výstupu v poli *out*) testovaného subjektu a směrem k němu (v poli *in*) vytížena nad 50%.
Výsledek je vyjádřen jako počet sekund za posledních 30 dnů, pro **splnění testu** je nutné, aby **oba dva směry** měly **hodnotu 0**.

TLS/SSL test

Pro tento test je použitý skript z https://testssl.sh/, který vrací pro každý port na adrese https://www.{domain}/ seznam otevřených portů a jejich nalezené zranitelnosti.
Ve výstupu jsou vyhledány porty, u kterých je zranitelnost vyhodnocená jako

- HIGH
- CRITICAL

V případě testů *cert_expirationStatus* a *cert_notAfter* je pro účel Fenix Checkeru zkontrolován datum platnosti certifikátu, a výsledek je označený jako selhání pouze v případě, kdy do konce platnosti zbývá méně než 7 dnů (skript testssl.sh reportuje selhání již při zbývajících 30 dnech).

Test je považován za **splněný**, když **není nalezen žádný** tento **záznam**.