DETAIL ZADÁNÍ

Předmět: ISA - Síťové aplikace a správa sítí

Ak. rok: 2022/2023

Název: Tunelování datových přenosů přes DNS dotazy

Vedoucí: Ing. Daniel Dolejška

1. Pearson, O. (1998). DNS Tunnel–through bastion hosts. Bugtraq posting.[Online] Available at: http://seclists. org/bugtraq/1998/Apr/0079. html. 2. Wang, Y., Zhou, A., Liao, S., Zheng, R., Hu, R., & Zhang, L. (2021). A comprehensive survey on DNS tunnel detection. Computer Networks, 197, 108322. 3. Aiello, M., Merlo, A., & Papaleo, G. (2013). Performance assessment and analysis of DNS tunneling tools. Logic Journal of the IGPL, 21(4), 592-602. 4. Merlo, A., Papaleo, G., Veneziano, S., & Aiello, M. (2011). A comparative performance evaluation of DNS tunneling tools. In Computational Intelligence in Security for Information Systems (pp. 84-91). Springer, Berlin, Heidelberg.

https://moodle.vut.cz/mod/folder/view.php?id=249182

Tento projekt se zaměřuje na implementaci nástroje pro tunelování dat prostřednictvím DNS dotazů [1] (použitelným například při DNS data exfiltration útoku [2, 3, 4]).

Vašim úkolem tedy bude implementace klientské i serverové části této aplikace dle požadavků uvedených níže.

Klient

Klientská aplikace bude odesílat data souboru/ze STDIN. V případě, že program načítá data ze STDIN je činnost aplikace ukončena přijetím EOF. Program bude možné spustit a ovládat pomocí následujícího předpisu:

```
dns_sender [-u UPSTREAM_DNS_IP] {BASE_HOST} {DST_FILEPATH} [SRC_FILEPATH]
```

```
$ dns_sender -u 127.0.0.1 example.com data.txt ./data.txt
$ echo "abc" | dns_sender -u 127.0.0.1 example.com data.txt
```

Přepínače:

- `-u` slouží k vynucení vzdáleného DNS serveru
  - pokud není specifikováno, program využije výchozí DNS server nastavený v systému

Poziční parametry:

- `{BASE_HOST}` slouží k nastavení bázové domény všech přenosů
  - tzn. dotazy budou odesílány na adresy `*.{BASE_HOST}`, tedy např. `edcba.32.1.example.com`
- `{DST_FILEPATH}` cesta pod kterou se data uloží na serveru
- `[SRC_FILEPATH]` cesta k souboru který bude odesílán
  - pokud není specifikováno pak program čte data ze STDIN

Server

Serverová aplikace bude naslouchat na implicitním portu pro DNS komunikaci. Příchozí datové přenosy bude ukládat na disk ve formě souborů. Komunikační protokol mezi klientem a serverem je implementační detail.

```
dns_receiver {BASE_HOST} {DST_FILEPATH}
```

```
$ dns_receiver example.com ./data
```

Poziční parametry:

- `{BASE_HOST}` slouží k nastavení bázové domény k příjmu dat
- `{DST_FILEPATH}` cesta pod kterou se budou všechny příchozí data/soubory ukládat (cesta specifikovaná klientem bude vytvořena pod tímto adresářem)

Programová dokumentace

Dokumentace vytvořeného řešení musí obsahovat a splňovat následující požadavky:

- popis mechanismu pro tunelování datových přenosů prostřednictvím DNS dotazů
- popis návrhu a implementace klientské a serverové aplikace
  - komunikační protokol mezi klientem a serverem
  - způsob kódování dat a informací
  - způsob ukládání souborů na serveru
  - možná rozšíření, omezení
  - atd.
- popis testování a měření vytvořeného softwaru
- minimální rozsah není stanoven, chybějící sekce či nedostatečné/nekompletní informace budou penalizovány
- odevzdání ve formátu PDF s názvem `dokumentace.pdf`

Formální požadavky zadání

1. přeložitelné a spustitelné na studentském serveru `eva.fit.vutbr.cz`
2. implementace v jazyce C
   - dodržení implementačního rozhraní
     - klientské rozhraní `dns_sender_events.h`
     - serverové rozhraní `dns_receiver_events.h`
     - zdrojové soubory jsou k nalezení v Moodle
     - rozhraní obsahuje funkce, které budou aplikací volány ve specifických momentech procesu aplikace (bude sloužit k ověření funkcionality projektu)

            - příjem/odeslání informací,
            - vytvoření souboru,
            - zápis dat,
            - aj.
        - další nestandardní knihovny nejsou dovoleny
        - dále také nejsou dovoleny hlavičkové soubory:
            - `resolv.h`
3. vytvoření Makefile
    - podpora `make sender`
    - podpora `make receiver`
    - podpora `make` + `make all` (přeloží sender i receiver)
4. vytvoření programové dokumentace obsahující:
    - nedostatky + rozšíření
    - princip fungování
    - testování
    - měření
5. odevzdání zdrojových souborů a dokumentace v jediném Tar+GZip (tar.gz) archivu prostřednictvím STUDISu
    - zdrojové soubory klientské aplikace v adresáři `sender`
    - zdrojové soubory serverové aplikace v adresáři `receiver`
    - dokumentace projektu

Části hodnocení

Hodnocení projektu sestává z několika částí. Negativní zisk bodů z kterékoliv části povede k dodatečnému ztržení bodů ze zbylých částí hodnocení.

1. kvalita zdrojového kódu
    - struktura programu
    - dekompozice na podproblémy
    - korektní použití datových struktur
    - odpovídající dokumentace kódu
    - atd.
2. funkčnost implementace
    - klient pracuje korektně
    - server pracuje korektně
3. kvalita dokumentace
4. rozšíření (max. bodů je stále 20)
    - podpora IPv6 (+1)
    - vlastní dokumentované rozšíření aplikace (+0-2)

V případě jakýchkoliv nejasností v zadání prosím napište na korespondující fórum projektu v elearningu (Moodle) tohoto předmětu.