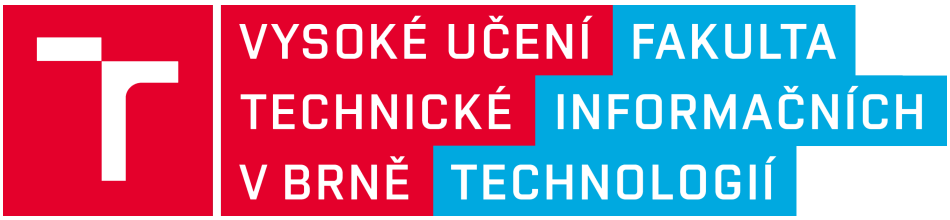


Implementačná dokumentácia k ISA projektu: Tunelování datových přenosů přes DNS dotazy

Veronika Molnárová, xmolna08

13.11.2022

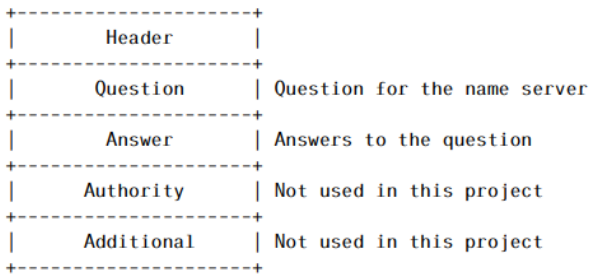
Obsah

1 Úvod

Cieľom projektu bolo vytvoriť serverovú a klientskú časť aplikácie pre tunelovanie dát cez DNS dotazy. Serverová aplikácie bude prijímať DNS dotazy, tie budú následne spracované a dáta z dotazu uložené na disk. Klientská aplikácia bude brať dáta zo zadaného vstupu a posielať ich vo forme DNS dotazov na server.

2 Základné informácie

DNS alebo Domain Name System vo všeobecnosti zabezpečuje preklad doménových mien na IP adresy, kde sa daný server domény vyskytuje. DNS klient komunikuje so serverom pomocou tzv. DNS queries, ktorými sa klient dotazuje na preklad daného doménového mena na IP adresu. Server mu posiela odpoveď na danú otázku spoločne so zistenými adresami a považuje komunikáciu za ukončenú. DNS packet má všeobecne nasledujúcu štruktúru:



2.1 Preklad doménového mena do DNS formátu

DNS protokol špecifikuje formát, v akom sa majú jednotlivé dotazy na doménové mená formulovať. Podľa RFCs 882, 883, 973 má otázka maximálnu dĺžku 255 znakov, do ktorých sa počíta aj ukončujúci znak 0. Dané doménové meno môže mať jednotlivé subdomény dĺžky maximálne 64 znakov vrátane oddelovača vo forme bodky. Tie sú pri prevádzaní do DNS formátu nahradené dĺžkou nasledujúcej subdomény v hexadecimálnom formáte. Takže preklad domény google.com by v DNS formáte by vyzeral: '0x06'google'0x03'com.

2.2 Komunikačný protokol

Vo všeobecnosti sú DNS dotazy posielané pomocou UDP protokolu, keďže otázka klienta sa mestí do jedného datagramu a v prípade straty sa môže daný dotaz opakovať, pokým klient nedostane odpoveď. Server môže využítať komunikáciu pomocou TCP protokolu v prípade väčšej odpovede, ktorá sa nemestí do jedného packetu. Prechod z UDP na TCP komunikáciu by mal prebiehať poslaním truncated UDP packetu od serveru, ktorý slúži na naznačenie klientovi na prepnutie na komunikácie do TCP protokolu. Po prevedení three-way-handshaku server pošle zvyšné dáta klientovi cez TCP komunikáciu.

2.3 Tunelovanie dát

Tunelovanie dát pomocou DNS je druh kybernetického útoku, ktorý kóduje dáta do DNS packetov. Keďže DNS komunikácia nie je pre zariadenie nič nezvyčajné a nepoužíva sa na prenos dát, takto poupravené packety dokážu obísť zabezpečenia ako firewall. Prichádzajúce nekontrolované dáta potom môžu obsahovať malware a napadnúť klienta. Existujú aj iné možnosti zneužitia DNS tunelovania.

3 Návrh a implementácia

V našom návrhu sme sa snažili, čo najviac zachovať rozhranie a spôsob komunikácie medzi klientom a DNS serverom. DNS server bude čakat na prichádzajúce UDP packety od klienta, ktoré následne spracuje a odošle prázdnu odpoveď klientovi, keďže nie je potrebné prekladať dané doménové meno v prípade našej aplikácie. Ak príde na server packet s flagom truncated, server packet spracuje a odpoveďou s flagon truncated naznačí klientovi, že je sa prepína na komunikáciu pomocou TCP protokolu. Následne spacuje zvyšné prichádzajúce packety a po ukončení komunikácie sa prepne naspäť do stavu UDP a čaká na prichádzajúcu komunikáciu.

3.1 Klientská aplikácia

Úlohou klienta je zabezpečenie toku dát vo forme DNS dotazov na server. Keďže DNS dotazy nie su prispôsobené na prenos dát, bol implementovaný návrh komunikačného protokolu popísaného vyššie. Dáta sú kódové do otázky dotazu, keďže sa málokedy využíva jej celá dĺžka. Tieto dáta musia byť prvotne rozparsované na dĺžky mestiace sa do jednotlivých subdomén, následne sú kódované a pridané sa ako prefix pred doménové meno servera, ktoré obsluhuje server, na ktorý sa dotazujeme. Posledne je potrebné danému serveru poslať cestu k súboru, kde majú byť dané dáta uložené. Tú posielame v prvom packete zahajujúcom komunikáciu so serverom ako prefix pred doménou, prípadne aj kódovanými dátami, oddelený znakom '-'. Ak je posielaných viacero packetov pre prenos jedného súboru, cesta na uloženie sa posiela len raz a naslednujúce packety obsahujú už len dáta s doménou.

3.2 Serverová aplikácia

Serverová aplikácia prijíma tok DNS packetov, spracováva ich a ukladá na disk. Spracovávanie packetu prebieha parsovaním cesty k súboru, v prípade, že packet predstavuje zahájenie komunikácie a teda server danú cestu nepozná, ďalej parsovaním a dekódovaním dát a posledne kontrolou domény dotazu sa zhodu či sa jedná o dotaz na doménu nášho serveru. V prípadne nevalidného dotazu je klientovi zaslaná chyba a ukončená komunikácia s ním. V prípade nezdhody domenových mien serveru a dotazu, je daný dotaz ignorovaný a žiadna odpoveď nezaslaná. Ak dotaz obsahoval správnu doménu, sú dekódované dáta uložené na disk a klientovi je vygenerovaná odpoveď.

3.2.1 Ukladanie dát

Ukladanie dát prebieha spôsobom, že pri neexistencií súboru je daný súbor vytvorený spoločne s jeho cestou v priečinku určenom na ukladanie prichádzajúcich dát na server. V prípade, že daný súbor existuje je jeho obsah prepísaný.

3.3 Kódovanie dát

Keďže URL domény môžu obsahovať len určitú obmedzenú skupinu znakov, na ktoré sa vzťahujú dalšie obmedzenia je potrebné kódovanie. Kódovanie tiež pomáha proti korupcií binárnych dát obsahujúce aj netextové znaky. V našom prípade sme zvolili kódovanie do base32 s využitím všetých velkých a zvyšné indexy sú zastúpené skupinou malých písmen po znak 'f'. Kódovanie funguje na báze prekladu dát na binárne a ich následne rozparsovanie na znaky po 5 bitoch. Tieto znaky zakódujeme podľa nasledujúcej tabulky po index 31.

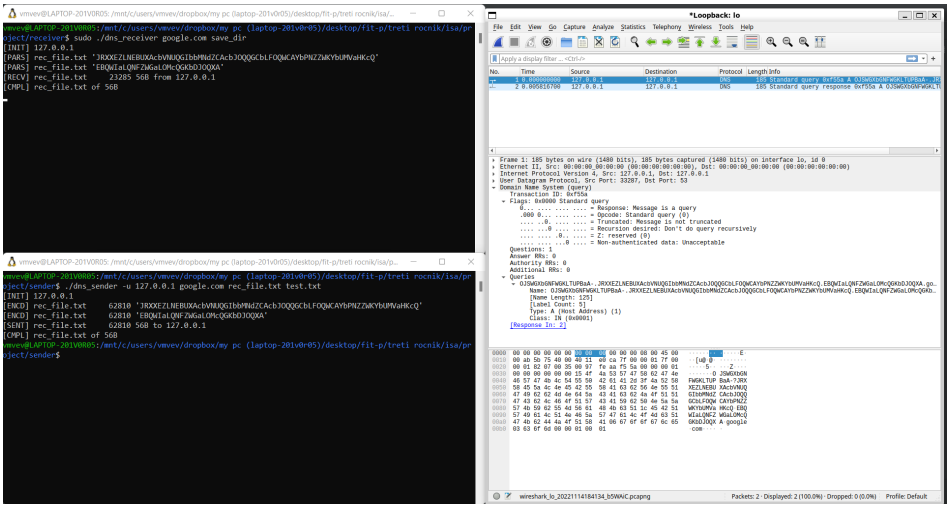
Base64 Encoding Table

Value	Char	Value	Char	Value	Char	Value	Char
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

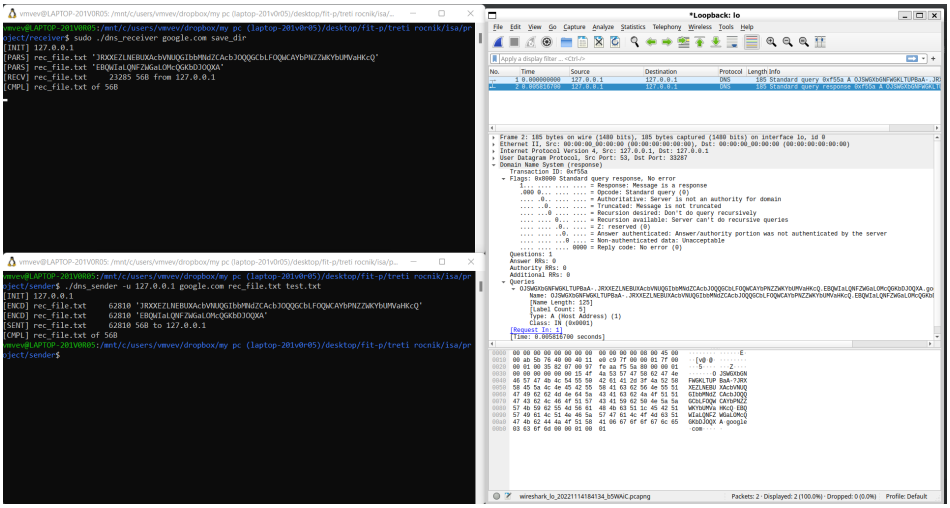
Takto zakódované dáta predstavujúce textový reťazec posielame po sieti.

4 Testovanie a meranie

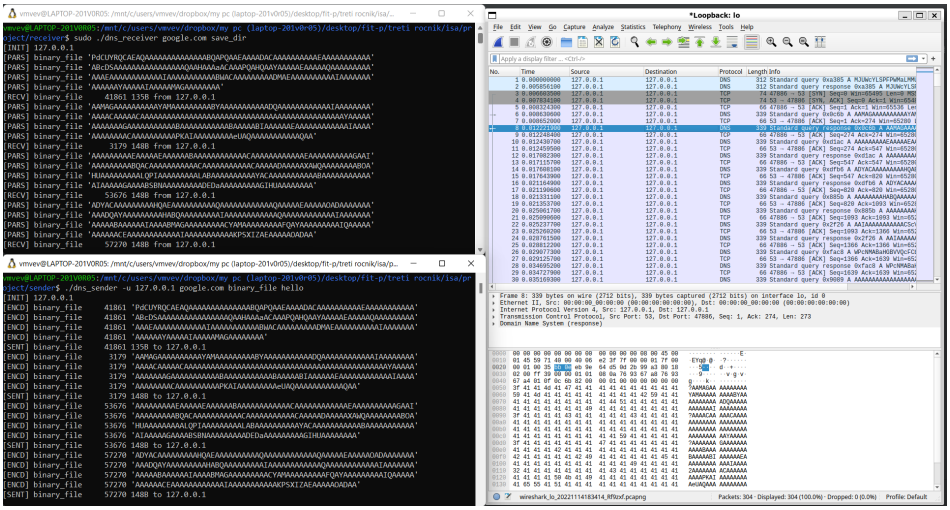
Pri testovaní sme využívali nástroj Wireshark, ktorý dokáže odchytávať jednotlivé packety na danom rozhraní a zobraziť ich obsah. Testovanie prebiehalo v prostredí WSL2, na ktorom prebiehala komunikácia klienta so serverom vo forme loopbacku. Spočívalo predovšetkým v pozorovaní packetov a následnej kontroly prenesených dát.



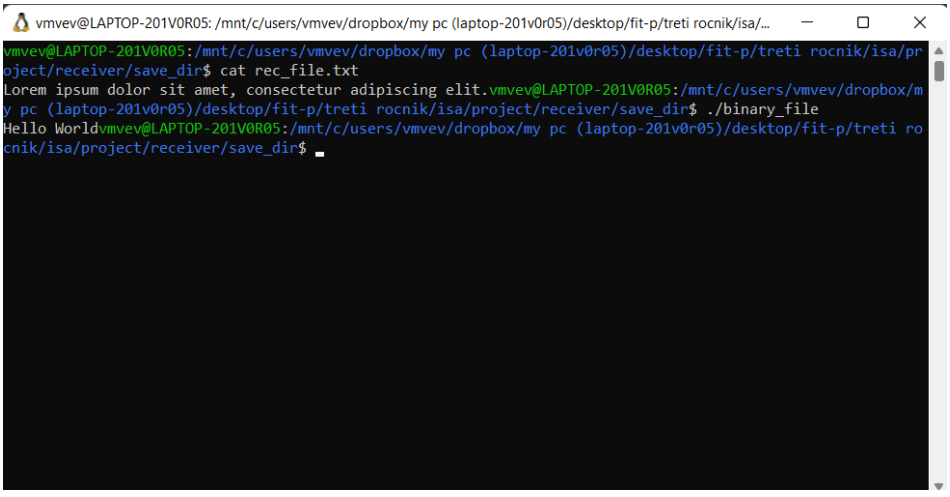
Príklad poslania dát jedným packetom



Odpoveď na DNS dotaz



Posielanie väčšieho množstva binárnych dát



Prenesené dáta na serveri, príklad spustenie preneseného binárneho súboru

5 Použitá literatúra

https://mislove.org/teaching/cs4700/spring11/handouts/project1-primer.pdf
https://www.ietf.org/rfc/rfc1035.txt
https://w3.cs.jmu.edu/kirkpams/OpenCSF/Books/csf/html/UDPSockets.html
https://serverfault.com/questions/698251/how-does-the-dns-protocol-switch-from-udp-to-tcp
https://www.infoblox.com/glossary/dns-tunneling/
https://www.paloaltonetworks.com/cyberpedia/what-is-dns-tunneling
https://stackabuse.com/encoding-and-decoding-base64-strings-in-python/