

Manuál ku generátoru Packet Cannon

Andrej Krivulčík

June 6, 2020

1 Generátor

Grafické užívateľské prostredie je vytvorené na subsystéme WPF, ktorý je priamo vytvorený pre programovací jazyk C#. Pri spustení vyskočí okno základnej konfigurácie, viz obrázok 1.

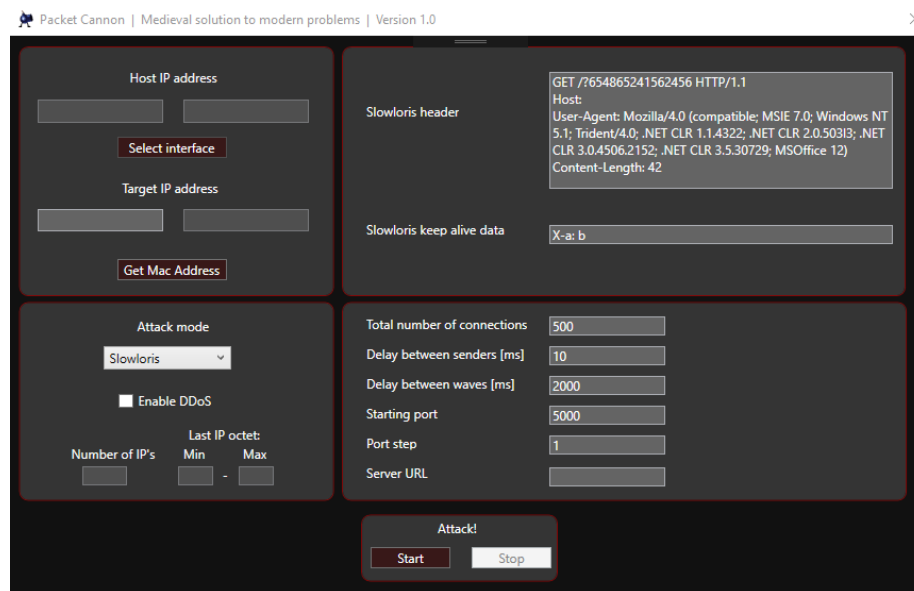


Figure 1: Konfiguračné okno pre generátor

Postup nastavovania:

1. Pri kliknutí na tlačítko **Select interface**, sa otvorí dodatočné okno s vybraním sieťového adaptéru, ktorý bude použitý pri útoku, viz obrázok 2. Treba si dávať obzvlášť pozor na to, ktorý adaptér je fyzický a ktorý je virtuálny, keďže cez virtuálny adaptér sa nedá dostať mimo virtuálnej siete.

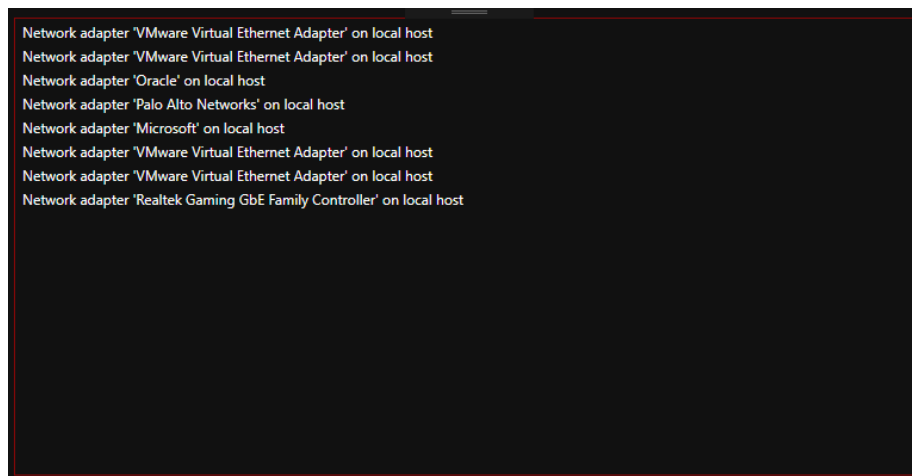
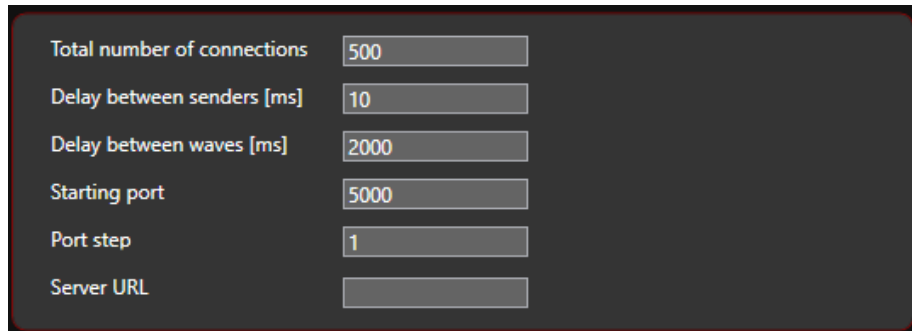


Figure 2: Výber sieťového adaptéru

2. Do políčka **Target IP address** sa zadáva IP adresa cieľu, následne sa pomocou tlačítka **Get Mac Address** preloží IP adresa na MAC adresu daného zariadenia, pokiaľ sa nachádza v lokálnej sieti, pomocou protokolu ARP. Pokiaľ sa dané zariadenie nenachádza v lokálnej sieti, MAC adresa cieľu sa nastaví ako východzia brána zo siete.
3. Pomocou rolovacej rolety **Attack mode** je možné si vybrať z 3 útokov:
 - Slowloris
 - Slow Port
 - Slow Read
4. Na pravej strane užívateľského prostredia sa nachádzajú parametre útoku, ktorý je aktuálne zvolený a už predvyplnené parametre na základnú hodnotu. Parametre jednotlivých útokov pre:
 - Slowloris: viz sekciu 1.1.
 - Slow Post: viz sekciu 1.2.
 - Slow Read: viz sekciu 1.3.
5. Nastavenie nasledujúcich parametrov pre útok:
 - **Total number of connections** – Počet falošných klientov snažiaci sa pripojiť na webový server (predvolená hodnota je 500 klientov).
 - **Time between senders** – čas medzi odpoveďami od falošných klientov (predvolená hodnota je 10 milisekúnd).

- **Time between waves** – keďže klienti odpovedajú takmer v jeden moment, tento rozostup slúži na simulovanie nedostupnosti klientov, keby sa všetci klienti tvária ako nedostupní (predvolená hodnota sú 2 sekundy).
- **Starting port** – začiatkový port, cez ktoré budú komunikovať falošní klienti, keďže niektoré dôležité aplikácie na systéme, môžu používať port viac ako je predvolená hodnota, v tomto prípade je predvolená hodnota na 5 000.
- **Port step** – hodnota o ktorú sa inkrementuje port predchádzajúceho falošného klienta, čiže ak prvý klient komunikuje cez port 5000 a Port step je nastavený na hodnotu 5, nasledujúci klient bude komunikovať cez port 5005, ďalší 5010 atď. (predvolená hodnota je 1).
- **Server URL** – slúži k tomu, aby bolo možné sa dostať aj na stránky, ktoré nie sú definované iba IP adresou ale majú aj tzv. Alias, čiže ich IP adresa je preložená do názvu stránky, ktoré sú uložené v záznamoch DNS serveru, keď sa budú jednotlivé stanice na ne dotazovať, napríklad pri doméne `www.google.com` sa jeho adresa prekladá na `172.217.23.238` a na túto adresu budú smerované jednotlivé pakety. Keďže ako klient málokedy pracuje s IP adresami, je veľa spôsobov ako zistiť IP adresu danej domény. Jednou z najjednoduchších je pomocou príkazového riadku a príkazom `ping <doména>`, v tomto konkrétnom prípade `ping google.com`.



Total number of connections	500
Delay between senders [ms]	10
Delay between waves [ms]	2000
Starting port	5000
Port step	1
Server URL	

Figure 3: Základné nastavenia pre falošných klientov

6. Tlačítka **Start** a **Stop** kompletne resetujú celý generátor, takže zakaždým, keď sa stlačí tlačítko **Start**, pôjde útok od začiatku.

1.1 Parametre útoku Slowloris

Slowloris header – samotná hlavička Slowloris útoku (predvolená hodnota je viz obrázok 4).

Slowloris keep alive data – Vlastné dáta pre udržiavacie pakety (predvolená hodnota je X-a: b).

Slowloris header	<pre>GET /?654865241562456 HTTP/1.1 Host: User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 1.1.4322; .NET CLR 2.0.50313; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; MSOffice 12) Content-Length: 42</pre>
Slowloris keep alive data	X-a: b

Figure 4: Základné nastavenia pre útok Slowloris

1.2 Parametre útoku Slow Post

Slow Post header – hlavička Slow Post útoku (predvolená hodnota je viz obrázok 5).

Slow Post payload size – celková veľkosť dát, ktoré budú posielané, mala by byť čo najvyššia aby bol útok efektívny (predvolená hodnota je 1 000 000).

Slow Post header	<pre>POST /textform.php HTTP/1.1 Host: User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 1.1.4322; .NET CLR 2.0.50313; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; MSOffice 12)</pre>
Slow Post payload size	1000000

Figure 5: Základné nastavenia pre útok Slow Post

1.3 Parametre útoku Slow Read

Slow Read window size – veľkosť okna pri čítaní (predvolená hodnota je 10 bytov).

Slow Read url – keďže Slow Read útok je efektívnejší na webových stránkach,

ktoré sú väčšie ako 1 MB, slúži na vybranie cesty k napríklad obrázku (predvolená hodnota je viz obrázok 6).



The image shows a dark-themed configuration window with two input fields. The first field is labeled "Slow Read window size" and contains the number "10". The second field is labeled "SlowRead Url" and contains the text "/index.html".

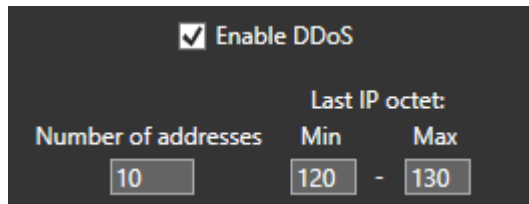
Parameter	Value
Slow Read window size	10
SlowRead Url	/index.html

Figure 6: Základné nastavenia pre útok Slow Read

2 DDoS

Poslednou z pridaných funkcií, je možnosť DDoS útoku, ktorá je ale efektívna iba v lokálnej sieti, ktorá nemá ARP spoofing ochranu. ARP spoofing je vytvorený poslaním požiadavku **ICMP-echo**, ľudovo povedané "ping", na dané neexistujúce adresy. Takéto adresy sú následne použité ako falošní užívatelia.

Po zaškrtnutí políčka **Enable DDoS**, viz 7, sa aktivujú políčka vedľa neho. Prvé políčko **Number of addresses** určuje, koľko falošných adries sa má vytvoriť. Ďalšie 2 políčka slúžia na zadanie minimálnu a maximálnu koncovú adresu. Adresy sú vytvorené z IP adresy vybraného sieťového rozhrania. Napríklad keby máme adresu sieťového rozhrania **1.1.1.1** a chceme vytvoriť 5 adries medzi 10 a 20, vytvorené adresy budú od adresy **1.1.1.10 až po 1.1.1.20** vybrané náhodne. Klienti na nich sú tiež vyberané náhodne, tzn. z jednej adresy môže byť viac klientov ako z druhej, poprípade určité adresy nebudú použité vôbec.



Last IP octet:		
Number of addresses	Min	Max
10	120	130

Figure 7: Nastavenia DDoS

3 GitHub

Všetky súbory a zkompilovaný spustiteľný súbor je uložený na GitHubu, link: <https://github.com/Mysfrit/PacketCannon/>.