UŽITNÝ VZOR

(11) Číslo dokumentu:

33 119

(13) Druh dokumentu: **U1**

(51) Int. Cl.:

H04L 12/26	(2006.01)
H04L 12/22	(2006.01)
H04L 29/08	(2006.01)
H04L 9/32	(2006.01)
H04L 12/24	(2006.01)

(19) ČESKÁ REPUBLIKA

ÚŘAD PRŮMYSLOVÉHO VLASTNICTVÍ

(21) Číslo přihlášky: **2018-35598**

(22) Přihlášeno: **12.11.2018**

(47) Zapsáno: **20.08.2019**

(73) Majitel:
GiTy, a.s., Brno, Komárov, CZ

(72) Původce:
Ing. Martin Sýkora, Brno, Židenice, CZ
Ing. Jakub Rainisch, Ostrava, Moravská Ostrava, CZ
doc. Ing. Václav Zeman, Ph.D., Plasy, CZ
doc. Ing. Petr Čika, Ph.D., Brno, Veveří, CZ
Ing. Zdeněk Martinásek, Ph.D., Brno, Bosonohy, CZ

(74) Zástupce:
Kania, Sedlak, Smola - Patentová kancelář, Ing Tomáš Benda, Mendlovo náměstí 907/1a, 603 00 Brno, Staré Brno

(54) Název užitného vzoru:
Zátěžový tester informační a komunikační technologie

CZ 33119 U1

Zátěžový tester informační a komunikační technologie

Oblast techniky

Technické řešení se týká zátěžového testeru informační a komunikační technologie.

Dosavadní stav techniky

Při návrhu a optimalizaci informační a komunikační technologie je jedním z kroků testování systémů při extrémní zátěži, jedná se o tzv. útoky cílené na odepření služeb, ve zkratce DoS, tj. „Denial of Service“, nebo DDoS, tj. „Distributed DoS“. Testování probíhá buď pomocí specializovaných HW zařízení, nebo vytvářením zátěže pomocí SW distribuovaných systémů. Existují různé typy útoků na odepření služeb, jejichž četnost je každoročně vyhodnocována. Mezi nejčastější útoky patří: HTTP flood, SYN flood, ICMP flood, NTP flood, UDP flood, Slowloris, útoky DNS a DNS amplification. Pro testování systémů při extrémních zátěžích existuje celá řada testerů od renomovaných výrobců, které v závislosti na jejich výkonosti jsou schopné generovat různě silné DoD či DDos útoky.

Vedle uvedených testů je také často nutné ověřit chování informační a komunikační technologie za předem definovaných přenosových podmínek. K tomuto účelu opět slouží specializované HW a SW síťové emulátory, které umožňují definovat charakter přenosové sítě. Díky emulátorům je možné v libovolném místě sítě nastavit předem definované podmínky pro chování sítě vůči průchozím paketům. Je tedy možné uměle vytvořit síťový spoj s definovaným zpožděním, kolísáním zpoždění, ztrátovosti, propustnosti apod. Díky tomu je možné ověřit chování síťových prvků či služeb za různých podmínek v síti.

V současné době existuje řada výrobců zátěžových testerů a síťových emulátorů. Tato zařízení jsou ve většině případů jednoúčelová a nelze do jejich konfigurace zasahovat či ji škálovat.

Mezi zásadní nevýhody současných systémů patří špatná, mnohdy nemožná škálovatelnost, nemožnost zvýšení výkonu zařízení bez nutnosti koupit zcela nové, nemožnost implementovat nové útoky služby bez platby licenčních poplatků, současná řešení jsou proprietární.

Cílem technického řešení je představit zátěžový tester informační a komunikační technologie, který by výše uvedené nevýhody stavu techniky potlačil.

Podstata technického řešení

Výše zmíněné nedostatky odstraňuje do značné míry zátěžový tester informační a komunikační technologie obsahující uživatelské rozhraní datově propojené s generátorem útoků D(D)oS, systémem pro vyhodnocení útoků D(D)oS, a emulátorem serveru, kde generátor útoků D(D)oS, systém pro vyhodnocení útoků D(D)oS, a emulátor serveru jsou dále datově propojeny s datovým rozhraním, přičemž generátor útoků D(D)oS a systém pro vyhodnocení útoků D(D)oS jsou datově propojeny, jehož podstata spočívá vtom, že dále obsahuje emulátor přenosových parametrů síťového provozu datově propojený s uživatelským rozhraním a datovým rozhraním.

Ve výhodném provedení je datovým rozhraním Ethernet, WiFi nebo LTE.

Objasnění výkresů

Technické řešení bude dále přiblíženo pomocí obrázku, kde obr. 1 představuje blokové schéma

zátěžového testeru informační a komunikační technologie podle technického řešení.

Příklady uskutečnění technického řešení

Zátěžový tester informační a komunikační technologie podle technického řešení představuje unikátní přístroj, který v sobě kombinuje funkci zátěžového testeru, síťového emulátoru emulátoru serveru.

Jak je patrné z blokového schématu na obr. 1, tester podle technického řešení obsahuje uživatelské rozhraní A a řízení, generátor B útoků D(D)oS, systém C pro vyhodnocení útoků D(D)oS, emulátor D přenosových parametrů síťového provozu, emulátor E serveru, a datové rozhraní F.

Uživatelské rozhraní A je datově propojeno s generátorem B útoků D(D)oS, systémem C pro vyhodnocení útoků D(D)oS, emulátorem D přenosových parametrů síťového provozu a emulátorem E serveru. Datové rozhraní F je datově propojeno s generátorem B útoků D(D)oS, systémem C pro vyhodnocení útoků D(D)oS, emulátorem D přenosových parametrů síťového provozu a emulátorem E serveru. Generátor B útoků D(D)oS je datově propojen se systémem C pro vyhodnocení útoků D(D)oS.

Datovým rozhraním F může být Ethernet, WiFi, LTE, atd.

Použití jednotlivých výše uvedených bloků A, B, C, D, E, F se liší v závislosti na použití celého testeru. Při zátěžovém testování serverů, síťových prvků či síťové infrastruktury se v závislosti na testovacím scénáři použijí bloky A, B, C, F, nebo A, B, C, E, F nebo A, B, C, D, E, F pro testování síťové infrastruktury a síťových prvků. Při emulaci síťového provozu se použijí bloky A, D, F. Jedná se o emulaci přenosových parametrů sítě mezi dvěma uzly existující sítě.

Zátěžový tester podle technického řešení lze sestavit pomocí dostupných serverových komponent, je však nutné dbát na jejich výběr z hlediska jejich výkonnosti:

Základní deska musí obsahovat DIMM slot pro paměti typu DDR, dále by měla obsahovat sloty pro připojení datových rozhraní, popřípadě jiných potřebných komponent. Doporučuje se využít sloty PCIe a USBv3, je možné využít i jejich alternativy.

Procesor pro základní desku je volen s ohledem na požadovanou výkonnost testeru. Pro zpracování zátěže a generování útoků s rychlostí do 10 Gb/s je dostatečný procesor CPU Intel Xeon E5-2650 nebo výkonnější. Pro požadavky nižších přenosových rychlostí může být volen procesor s nižší výkonností.

Datová rozhraní testeru jsou v závislosti na požadované funkci testeru zastoupena jednou nebo více síťovými kartami. Síťové karty jsou osazeny do slotů základní desky. Volba typu slotu je závislá na požadované rychlosti přenosu. Pro přenosovou rychlost 10 Gb/s je možné použít například karty Intel Ethernet CNA X520-T2 pro připojení konektorem RJ-45 nebo Intel Ethernet CNA X520-SR2 pro připojení konektorem LS. Lze volit i jiné, například bezdrátové technologie. Minimální počet síťových karet pro funkci testeru je 1.

Operační paměť testeru se volí v závislosti na výkonnosti testeru. Pro schopnost generovat provoz 10 Gb/s je doporučené instalovat minimálně 128 GB, například osm modulů Kingston DDR4 16 GB 2133 MHz CL15.

Úložný prostor je nezbytný pro uložení operačního systému, softwarových komponent a ostatních dat. Dále jej lze využít pro rychlé výpočty během generování zátěže. Tester je vhodné osadit dvěma disky. 1 x SSHD s kapacitou alespoň 500 GB, 1 x SSD s kapacitou alespoň 100 GB. Pro

bezproblémový chod testeru s výkonem 10 Gb/s lze například použít SSHD 2 TB Seagate Desktop 64 MB SATAIII 8 GB NAND pro systém a SSD 400 GB Intel DC P3500 pro výpočty.

Grafická karta v testeru plní funkci přenosu obrazového signálu na zobrazovací jednotku. Lze použít například NVIDIA GeForce GT 730.

Ostatní periferie slouží k rozšíření testeru o různé další funkce. Lze k němu připojit například DVD mechanika, další úložiště apod. Nutné periferie k ovládání testeru jsou: klávesnice, myš a monitor.

Výše zmíněné komponenty testeru podle technického řešení nebo jejich alternativy je nutné použít k bezproblémovému chodu zařízení vyjma ostatních periferií. Tester lze ovládat i vzdáleně přes datová rozhraní F.

V konkrétním provedení je tester podle technického řešení osazen následujícími prvky:

Základní deska je od výrobce Asus, konkrétně ASUS X99-E WS s čipovou sadou Intel X99. Základní deska obsahuje 8x DIMM slot pro paměti typu DDR4 s kapacitou až 128 GB a s podporou frekvencí až 2133 MHz. K dispozici má 7 slotů PCIe (verze 3), což je dostatečné množství pro budoucí rozšíření systému. Dále základní deska obsahuje USB sloty verze 3.1, které mohu do budoucna sloužit k připojení dalších periferií.

Základní deska je osazena procesorem CPU Intel Xeon E5-2650 v4.

Síťová rozhraní integrovaná na základní desce disponují dvěma porty pro křížený kabel a podporují rychlost až 1 Gbit/s. Pro potřeby testeru jsou však nedostačující. Z tohoto důvodu jsou vybrány dvě síťové karty pro rozhraní PCIe a to konkrétně Intel Ethernet CNA X520-T2 se dvěma konektory RJ-45 a Intel Ethernet CNA X520-SR2 se dvěma konektory LC. Obě karty podporují přenosové rychlosti 10 Gbit/s.

Operační paměť je osazena do maximální podpory základní desky, a to osmi moduly Kingston DDR4 16 GB 2133 MHz CL15. Celková kapacita operační paměti je tedy 128 GB.

Základní deska je osazena dvěma disky. První disk, SSHD 2 TB Seagate Desktop 64 MB SATAIII 8 GB NAND, je určen pro operační systém a systémové soubory a dále pro ukládání statistik a ostatních potřebných dat. Disk je se základní deskou propojen přes rozhraní SATA III. Druhý disk slouží pro rychlé výpočty a komunikaci se síťovými kartami. Jedná se o disk SSD 400 GB Intel DC P3500 připojený přes rozhraní PCIe, což zajišťuje extrémně rychlou komunikaci se všemi periferiemi, zejména se síťovými kartami.

Základní deska je osazena grafickou kartou NVIDIA GeForce GT 730.

K základní desce je dále připojena DVD-RW mechanika a klávesnice a myš.

Zátěžový tester je vybaven bezplatným serverovým operačním systémem CentOS 7. Operační systém využívaná jádro ve verzi 3.10.0-514.10.2.el7.x86_64.

Operační systém CentOS 7 je vybaven open-source aplikací JMeter, která je následně upravena pro potřeby testeru. JMeter je nástroj vyvíjený v programovacím jazyce Java a je licencovaný pod licencí Apache verze 2.0. Koncept JMeteru je založen na výměnných modulech.

Operační systém CentOS 7 je vybaven nástrojem trafgen, jenž umožňuje generování paketů s podrobným nastavením. Trafgen patří do open-source balíčku síťových aplikací Netsniff-NG pro OS Linux. Nástroj je volně šiřitelný pod licencí GNU GPL. Nástroj trafgen je integrován do aplikace JMeter pro generování paketů pro D(D)oS útoky.

Modul implementovaný v programu JMeter, jenž je založen na již existujícím sampleru nástroje JMeter a to HTTP Request. Modul umožňuje nastavit IP adresu a číslo portu Web serveru, na který mají být zasílány pakety, metodu (GET, POST, HEAD, PUT, OPTIONS, TRACE, DELETE, PATCH, PROPFIND, PROPPATCH, MKCOL, COPY, MOVE, LOCK, UNLOCK, REPORT, MKCALENDAR, SEARCH), rozsah zdrojových IP adres, masku sítě a sítové rozhraní, ze kterého mají být pakety odesílány.

Modul implementovaný v programu JMeter, jenž ke své činnosti využívá externí generátor trafgen. Modul umožňuje nastavit sítové rozhraní, ze kterého mají být pakety SYN odesílány. Na linkové vrstvě je možné nastavit rozsah zdrojových MAC adres a MAC adresu cíle útoku. Na síťové (IP) vrstvě je možné nastavit IP adresu cíle útoku, rozsah zdrojových IP adres a TTL. Na transportní vrstvě je možné nastavit rozsah zdrojových TCP portů, cílový TCP port a velikost okna. Dále je možné nastavit velikost výplně datového pole v bajtech, počet odeslaných paketů SYN a rychlost odeslání paketů v p/s.

Modul implementovaný v programu JMeter, jenž ke své činnosti využívá externí generátor trafgen. Modul umožňuje nastavit sítové rozhraní, ze kterého mají být ICMP zprávy posílány. Na linkové vrstvě je možné nastavit rozsah zdrojových MAC adres a MAC adresu cíle útoku. Na síťové (IP) vrstvě je možné nastavit IP adresu cíle útoku, rozsah zdrojových IP adres a TTL. Dále je možné nastavit typ a kód (t-k) ICMP zprávy (0-0, 3-0, 3-1, 3-2, 3-3, 3-4, 3-5, 3-6, 3-7, 3-8, 3-9, 3-10, 3-11, 3-12, 3-13, 3-14, 3-15, 4-0, 5-0, 5-1, 5-2, 5-3, 6-0, 8-0, 11-0, 11-1, 13-0, 14-0, 15-0, 16-0, 17-0, 18-0, 30-0, 31-0), počet odeslaných paketů a rychlost odeslání paketů v p/s.

Modul implementovaný v programu JMeter, jenž ke své činnosti využívá externí generátor trafgen. Modul umožňuje nastavit sítové rozhraní, ze kterého mají být pakety odesílány. Na linkové vrstvě je možné nastavit rozsah zdrojových MAC adres a MAC adresu cíle útoku. Na síťové (IP) vrstvě je možné nastavit IP adresu NTP serveru, na který bude zaslána žádost MON GETLIST, IP adresu cíle útoku, na který bude zaslána odpověď z NTP serveru a TTL. Na transportní vrstvě je možné nastavit rozsah UDP portů, na které budou zaslány odpovědi z NTP serveru a UDP port NTP serveru. Dále je možné nastavit počet odeslaných paketů a rychlost odeslání paketů v p/s.

Modul implementovaný v programu JMeter, jenž ke své činnosti využívá externí generátor trafgen. Modul umožňuje nastavit IP adresu a UDP port cíle útoku, sítové rozhraní, ze kterého mají být datagramy odeslány, rozsah zdrojových IP adres a UDP portů. Dále je možné nastavit počet odeslaných datagramů a jejich rychlost odeslání v kbit/s.

Modul implementovaný v programu JMeter, jenž ke své činnosti využívá externí generátor trafgen. Modul umožňuje nastavit IP adresu a UDP port cíle útoku (DNS serveru), rozsah zdrojových IP adres a UDP portů, žádost o převod doménového jména a sítové rozhraní, ze kterého mají být datagramy odeslány. Dále je možné nastavit počet odeslaných datagramů a jejich rychlost odeslání v kbit/s.

Modul implementovaný v programu JMeter, jenž ke své činnosti využívá externí generátor trafgen. Modul umožňuje vytvořit vlastní konfiguraci útoku pomocí textového pole či nahrání konfigurace již vytvořeného útoku. Dále je možné nastavit sítové rozhraní, ze kterého mají být pakety odeslány, počet odeslaných paketů a rychlost odeslání paketů v p/s.

Modul implementovaný v programu JMeter, jenž ke své činnosti využívá skript v jazyce Python pro generování paketů, jenž je licencován pod svobodnou MIT Licencí. Modul umožňuje nastavit použití HTTP či HTTPS, znáhodnění user-agenta při každé žádosti, IP adresu a port cíle útoku a počet žádostí (otevřených soketů).

Zátěžový tester obsahuje v aplikaci JMeter funkcionality pro vyhodnocení provedených testů

(tvorbu reportů).

V operačním systému CentOS je pro emulací přenosových parametrů využit open-source nástroj NetEm založený na systému front. NetEm je součástí jádra Linuxu od verze 2.6 jako část kolekce balíčků iproute2, konkrétně nástroje Traffic Control (tc). Nástroj NetEm je integrován do aplikace JMeter pro emulaci přenosových parametrů sítě. Síťový emulátor pro tvarování datového toku umožňuje nastavit spoje, které je možné dále konfigurovat. Emulátor umožňuje nastavit filtr pro zdrojovou IP adresu a port, cílovou IP adresu a port a použitý protokol. Dále umožňuje nastavit rychlost, zpoždění, kolísání zpoždění, korelaci zpoždění, rozložení zpoždění, ztrátovost a její korelaci, záměnu pořadí paketů a její korelace, duplikaci paketů a její korelaci a poškození paketů.

Zátěžový tester podle technického řešení obsahuje v aplikaci JMeter dva moduly pro analýzu síťového provozu a modul pro emulaci serverů.

Unikátnost řešení spočívá ve využití otevřených technologií a v kombinaci zátěžového testeru a síťového emulátoru, které využívají stejnou hardwarovou platformu. Zátěžový tester je jedno, snadno rozšiřitelné, hardwarové zařízení umožňující generování D(D)oS útoků, vyhodnocení testů (tvorbu reportů) a emulování přenosových parametrů síťového provozu. Pro analýzu síťového provozu obsahuje tester síťovou sondu a modul pro emulaci serverů.

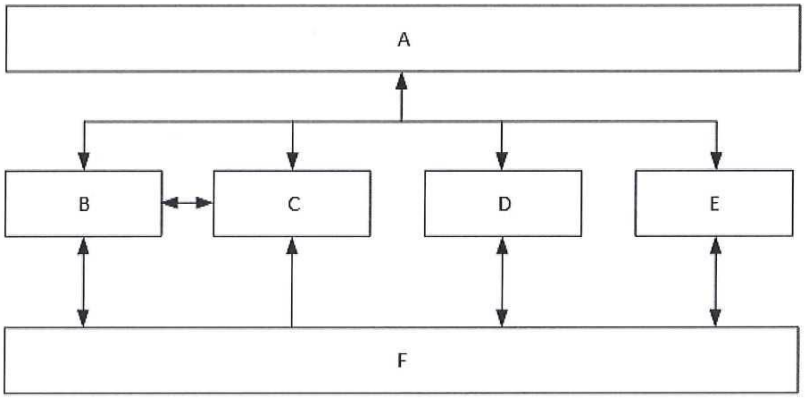
Celý systém je modulární a lehce rozšiřitelný.

NÁROKY NA OCHRANU

1. Zátěžový tester informační a komunikační technologie obsahující uživatelské rozhraní (A) datově propojené s generátorem (B) útoků DDoS, systémem (C) pro vyhodnocení útoků DDoS a emulátorem (E) serveru, kde generátor (B) útoků DDoS, systém (C) pro vyhodnocení útoků DDoS a emulátor (E) serveru jsou dále datově propojeny s datovým rozhraním (F), přičemž generátor (B) útoků DDoS a systém (C) pro vyhodnocení útoků DDoS jsou datově propojeny, **vyznačující se tím**, že dále obsahuje emulátor (D) přenosových parametrů síťového provozu datově propojený s uživatelským rozhraním (A) a datovým rozhraním (F).

2. Zátěžový tester podle nároku 1, **vyznačující se tím**, že datovým rozhraním (F) je Ethernet, WiFi nebo LTE.

1 výkres



Obr.1