Linux jako cíl i zdroj síťových útoků

Petr Krčmář

ROOT.CZ_ vpsFree.cz

12. listopadu 2023

O mně

- linuxák od roku 1998
- správce serverů
- lektor a konzultant
- šéfredaktor Root.cz
- člen vpsFree.cz
- organizátor LinuxDays
- můj web je petrkrcmar.cz

ROOT.CZ_ vpsFree.cz

Prezentace už teď na webu

https://www.petrkrcmar.cz

ROOT.CZ_ vpsFree.cz

Linux patří na síť

- Linux dnes znamená připojení k síti
  - velmi univerzální, spousta různých rolí
- servery, VPS, síťové prvky, IoT, zařízení…
  - vše dnes komunikuje po síti (internet)
- běžně linky 1Gbps, žádná výjimka 10Gbps
  - velká kapacita sítí (CESNET)
- Linux se může stát **cílem i zdrojem** útoků
  - útočník ohrožuje nás, my ohrožujeme ostatní

ROOT.CZ_ vpsFree.cz

Rozumět sítím

- admini se často snaží správě sítě vyhnout
  - PNJ – Problém Někoho Jiného
- servery a sítě jsou úzce spojeny
  - brzy narazíte na znalostní limity
  - proč je síť organizována takto a jak se v ní pohybovat
- rozhraní, porty, DNS, rozsahy adres, VPN…
  - internet je plný dotazů z nepochopení základů
- neznalost plodí **bezpečnostní problémy**
  - osvěta je důležitou součástí bezpečnosti
  - víte o problémů, můžete mu bránit předem nebo ho identifikovat

ROOT.CZ_ vpsFree.cz

Linux jako cíl

Objevení cíle

- místní síť – malý prostor, snadno dostupný
  - bezpečnost místní sítě je iluze
  - nulová důvěra – zero trust architecture (ZTA)
- veřejná síť – velký prostor, ale **konečný**
  - IPv4 lze proskenovat za pět minut (masscan)
  - veřejné výsledky skenů na Shodan.io
  - IPv6 má obrovský prostor, je třeba sebrat data jinde
- data o adresách lze získat z různých zdrojů
  - NTP – automatická synchronizace času
  - TLS – veřejná úložiště certifikátů (crt.sh)
  - DNS – sledování provozu na rekurzorech

Útok na uživatelské účty

- snaha objevit účet bez hesla nebo **uhádnout heslo**
  - naprosto běžné – napříč službami (SSH, web, pošta…)
- útoky hrubou silou vs. slovníkové útoky
  - hesla unikají – na webu miliardy hesel (HIBP)
- řešení snížením dopadové plochy
  - omezení přístupu k citlivým službám (firewall)
  - omezení počtu pokusů (rate limiting)
  - vypnutí přihlašování heslem (SSH)
  - vícefaktorové přihlašování
  - aktivní hlídání kvality hesel

Vyhledání účtů bez hesla

```
# awk -F: '($2 == "") {print $1}' /etc/shadow
```

Útok na hesla

- hesla uložená v podobě hašů (otisků)
  - server hesla nezná, zná jen otisky
  - při přihlašování se porovnají otisky
- útočník může databázi získat chybou v systému (únik Mall.cz)
- poté může nasadit **offline útok** – počítá u sebe
  - rychlost neomezená linkou a limity, hrubá síla vs. slovníky
- nástroj Hashcat akceleruje na grafické kartě
  - výkon v miliardách hašů za sekundu (podle funkce a karty)
  - viz Odhaleno heslo tvůrce unixu Kena Thompsona
- řešením je dobře hašovat, solit a neomezovat sílu hesla
  - Yescrypt, Bcrypt, Argon2

Výchozí haš pro nová hesla

```
$ grep pam_unix.so /etc/pam.d/common-password
```

Útok na služby

- služby poslouchající do sítě jsou nejzranitelnější
  - přijímají vstupy – je možné zkoušet aplikační útoky
- problémy v konfiguraci a/nebo bezpečnostní chyby
- **infiltrace** do systému nebo **získání informací**
  - databáze uživatelů, hesla, verze služeb, konfigurace...
- neznámá poslouchající služba = vysoké riziko
  - zapomenutá nemá konfiguraci ani záplaty
  - úplně neznámá může znamenat úspěšný útok
- řešením je hlídat služby, segmentovat (kontejnery, SELinux)

Poslouchající služby

```
# ss -tulpn
```

Útoky odepřením služby

O asymetrii zdroje a cíle

- následující útoky často stojí na **asymetrii**
- útočník má něčeho více než obránce
  - výkonu, pásma, počítačů, času…
- nebo je pro něj **levnější** útočit
  - jeden paket s dotazem, sto paketů s odpovědí
- jednodušší, levnější, účinnější
  - lze způsobit velké škody při malých nákladech

Kybernetický útok je asymetrický, pokud útočník potřebuje relativně malý počet nebo nízkou úroveň zdrojů, aby způsobil poruchu nebo selhání výrazně většího počtu nebo vyšší úrovně cílových zdrojů.

ROOT.CZ_ vpsFree.cz

Útoky typu (D)DoS

- snaha **vyčerpat zdroje** na serveru
  - síťové pásmo, procesorový čas, paměť, diskový prostor…
- služby pak nejsou dostupné legitimním uživatelům
  - útočník zahltí svou oběť vlastními úkoly
- distribuovaná varianta komplikuje obranný postup
  - nestačí zaříznout jeden zdroj provozu
- motivace mohou být různé – útok lze objednat (botnet)
  - konkurenční boj – e-shopy před Vánoci
  - vydírání – zaplať výkupné, jinak zaútočíme
  - hacktivismus – prosazování politických názorů
  - odvedení pozornosti – podpora jiného útoku
  - získání výhody – v herním prostředí (TeamSpeak)
  - vyřazení bezpečnostního prvku – součást útoku

ROOT.CZ_ vpsFree.cz

Objemové útoky (volumetrické)

- obecně zaplavení linky množstvím provozu
- postihuje **síťovou vrstvu** (L3)
  - ucpe celou linku, znepřístupní často celou síť
  - efekt je možné znásobit použitím **botnetu**
- ICMP flood – servisní pakety ICMP (ping)
  - nízkoúrovňová bezestavová komunikace
  - možnost snadno zfalšovat odesílatelovu adresu
  - prvky mohou odpovídat na broadcastované požadavky (smurf attack)
- Teardrop – zahlcení chybnými IP fragmenty
  - zneužívá možnosti fragmentace paketů
  - vytváří chybně navazující pakety
  - zatěžuje cílový IP stack, starší systémy shodí

ROOT.CZ_ vpsFree.cz

Útoky na transportní protokol

- vyčerpání zdrojů na straně sítě
- postihují **transportní vrstvu** (L4)
  - vyčerpává prostředky směrovačů, firewallů a serverů
- SYN flood – napůl otevřená spojení
  - normální provoz: SYN, SYN-ACK, ACK
  - při útoku se otevírají spojení z náhodných adres
  - cíl čeká na dokončení sestavování spojení
- UDP flood – náhodný provoz na UDP
  - systém se musí požadavky zabývat
  - vyhledává správnou službu, případně odmítne spojení
  - nejčastěji odesílá ICMP Destination Unreachable

ROOT.CZ_ vpsFree.cz

Obrana

- filtrování provozu
  - nastavená pravidla mohou zastavit nelegitimní provoz
  - útočník se ovšem snaží posílat legitimně vypadající provoz
- nastavení limitů
  - omezení na počet přijatých ICMP paketů
  - doporučovaná metoda, dobře nastavená je šetrná
- detekce anomálií
  - dlouhodobé sledování standardního chování sítí
  - automatická detekce a filtrace anomálií
- vzdálená filtrace
  - pokud je linka ucpaná, místní filtrace nepomůže
  - je třeba filtrovat před ucpáním – v nadřazené síti
  - dálkové ovládání, možnost volit filtry (RTBH)

ROOT.CZ_ vpsFree.cz

Útoky na aplikace

- vyčerpání zdrojů na straně serveru
  - CPU, paměť, disk, otevřená spojení…
- postihují **aplikační vrstvu** (L7)
  - zatěžuje cíleně konkrétní aplikační procesy
- může zneužívat špatně napsanou aplikací
  - pomalý dotaz do DB, proces přihlašování uživatele
- nebo nedokonalostí v návrhu služeb
  - útok náhodnými dotazy do DNS
  - útok na šifrovací vrstvu (TLS v HTTPS/OpenVPN)

Příklad: HTTP/2 Rapid Reset

- zneužívá funkce proudů v protokolu HTTP/2
  - uvnitř TCP spojení více paralelních dotazů
  - multiplexace součástí samotné aplikace
  - na HTTP/2 dnes běží asi 62 % provozu
- klient má možnost odeslat zprávu RST_STREAM
  - jednostranné zrušení požadavku, zavření proudu
  - legitimní, pokud je zavřena stránka v prohlížeči
- útočník neustále otevírá a ruší nové proudy
  - rychlost je omezena jen jeho linkou
  - server má s vytvářením proudu náklady
- rekordní útok měl zatím 201 Mrps (dotazů za sekundu)
  - stačí k tomu jen několik tisíc členů botnetu
  - od léta je většina útoků tímto způsobem (Cloudflare)

ROOT.CZ_ vpsFree.cz

Pomalé útoky

- zdroje lze vyčerpat také opačným způsobem: **zdržováním**
- příklad: útok Slowloris – outloň váhavý
  - otevření mnoha spojení a jejich nekonečné udržování
  - před vypršením limitu pošleme jeden znak a stojíme
- server naprosto nezatížený, všechno běží, přesto nefunguje
  - otevřením spojení se vyčerpaly zdroje
  - typicky limit procesů nebo otevřených spojení
  - není další prostor pro obsluhu uživatelů
- velmi nenáročné na zdroje útočníka
  - **jediný stroj** takto dokáže odstavit webový server
  - silně to ale závisí na implementaci webového serveru
  - některé jsou náchylnější (Apache), jiné výrazně méně (Nginx)
- lze kombinovat – otevřít spoustu spojení a naráz dokončit

Obrana

- nasazení aktuálního software
  - moderní webové servery jsou odolnější
  - neforkují a používají asynchronní zpracování
- nasazení odolnějšího řešení
  - najít slabé místo – server nebo aplikace
  - vyměnit za odolnější variantu
- reverzní proxy
  - předsazení odolnějšího řešení (lze i CDN)
  - odbaví klienty a pustí až kompletní dotazy
  - možno doplnit o load balancer a rozložit zátěž
- nasazení limitů
  - omezení počtu dotazů z IP, snížení timeoutů, snížení keepalive
  - omezení doby komunikace, minimální rychlost komunikace

Linux jako zdroj útoků

Napadené zařízení

- útočník skrz službu ovládne zařízení
- nainstaluje vlastní útočný software
  - často automatizované, připojení do botnetu
- dokáže provádět dříve popsané útoky
- Linux není jen v počítačích
  - směrovače, kamery, disková pole, IoT…
- **aktualizujte** veškerý software v systému
- zabezpečte běžící služby proti průniku
- omezte počet nabízených služeb (Shodan.io)
- hlídejte zranitelnosti: Lynis, Chkrootkit, Nessus, OpenVAS…

ROOT.CZ_ vpsFree.cz

Ochrana SSH

- šifrovaný bezpečný komunikační kanál (port TCP/22)
  - šifrované, autentizované, velmi bezpečné
- nejčastěji napadaná služba: hádání účtů a hesel
  - lákavý cíl – úspěšné přihlášení otevírá cestu
- možnost přihlašování heslem a/nebo klíči
- uživatel si klíč serveru ukládá do `~/.ssh/known_hosts`
  - každé spojení – jiný symetrický klíč (DH pro PFS)
  - klient ověřuje identitu serveru, ochrana proti MitM

Přihlašování klíči

- přihlašování heslem nebezpečné, nepohodlné
  - možnost hádat, nutnost neopakovat hesla
- klíče automatizované, bezpečné, jednoduché
- privátní klíč u uživatele, veřejný na serverech
  - možno jeden klíč pro více serverů – neohrožuje bezpečnost
  - klíče možno mít i na hardware (tokenech, smart kartách…)
- přihlašování sdílejí všechny služby (ssh, rsync, sftp, mosh…)
- přihlašování heslem je možné úplně vypnout

/etc/ssh/sshd_config

```
PubkeyAuthentication yes
PasswordAuthentication no
```

Jak začít s klíči?

- **na klientovi** vygenerujeme klíče pomocí `ssh-keygen`
- pomocí `-t` možno vybrat algoritmus: rsa, ecdsa, ed25519
- pomocí `-b` se volí délka klíče, pomocí `-C` můžeme přidat popis
- klíče vzniknou v `~/.ssh/`, `.pub` je veřejná část
- veřejnou část nakopírujeme na server (`ssh-copy-id`)
  - klíče jsou v `~/.ssh/authorized_keys`
- pokud máme příslušnou privátní část, můžeme se přihlásit

Generování klíče na klientovi

```
$ ssh-keygen -t ed25519 -C petr@ananas
```

ROOT.CZ_ vpsFree.cz

Zneužití síťové služby

Falšování adresy odesílatele

- protokol IP má v hlavičce adresu odesílatele
- není nijak zaručena – kdokoliv může vyplnit cokoliv
  - pokud požadujeme odpověď, musí být adresa správně
  - pro sestavení TCP potřebujeme třícestný handshake
- pokud nás odpověď nezajímá, můžeme falšovat
- ochrana **nesmí záviset** jen na IP adrese zdroje
  - aktivní filtrace vnitřních adres na vnějším rozhraní
- pokud si stroje uvnitř věří, útočník se za ně může vydávat
  - aktivní filtrace vnitřních adres na vnějším rozhraní
  - nespoléhat se na adresu, ani na **reverzní záznam**

Odražený útok

- útok odrazíme od zranitelného zdroje (prostředníka)
- zfalšujeme adresu odesílatele a požádáme o odpověď
- prostředník odpovídá na **falešnou adresu**
  - nevědomky se tak účastní útoku
  - takto lze oslovit více prostředníků a distribuovat
- možnost zakrýt skutečnou IP adresu útočníka
- možnost obejít limity či filtraci
  - pokud má prostředník s cílem nějaký vztah
  - zařízení z DMZ může útočit do vnitřní sítě
- typický příklad: ICMP echo request (ping)

ROOT.CZ_ vpsFree.cz

Zesílený odražený útok

- výrazné vylepšení předchozího o zesilující efekt
  - provoz odrazíme a služba nám jej **zesílí**
  - tohle útočníky zajímá víc než samotný odraz
- zneužívá **asymetrie** dotazu a odpovědi
  - malý dotaz vyvolá u prostředníka výrazně větší odpověď
  - zneužívá se slabina protokolu (implementace), ne kompromitace
- podmínkou je možnost odpověď odrazit na cíl
  - typické pro služby postavené nad **UDP**
- opět možné distribuovat a dále zvětšit dopad
- různé služby (protokoly) mají různý faktor zesílení
  - vezmeme to od těch nejméně zesilujících po nejnebezpečnější

ROOT.CZ_ vpsFree.cz

portmapper

- někdy také uváděný jako rpcbind, portmap nebo RPC Portmapper
- podpora pro služby ONC RPC (RFC 5531), běží na TCP a UDP 111
  - Open Network Computing (ONC) Remote Procedure Call (RPC)
  - nejznámější službou tohoto typu je NFS
- slouží jako adresář dostupných služeb, podobně jako DNS
  - služba se zaregistruje a portmapper o ní umí informovat
  - klient poptá službu a dozví se port a transportní protokol
  - možno ručně poptávat nástrojem `rpcinfo`
- útočník může podvrhnout adresu tazatele a poslat mu odpověď
  - dotaz může mít 68 bajtů, odpověď 486 bajtů (zesílení **7×**)
  - odpověď ale může mít i 1930 bajtů (zesílení **28×**)
- pokud nepoužíváte NFS, vypněte ho včetně portmapperu
  - pokud RPC potřebujete, omezte přístup na firewallu

ROOT.CZ vpsFree.cz

DNS

- výchozím protokolem pro DNS je UDP na portu 53
  - s EDNS(0) můžeme signalizovat pakety větší než 512 bajtů
- můžeme si takto objednat velkou odpověď
  - DNSSEC a další data umožňují zvětšit odpovědi
- zranitelné jsou takto **rekurzivní servery**
  - můžeme se ptát donekonečna na mnoho záznamů
  - autoritativní server má omezený počet zón a limity
- zesílení více než **100×**
  - dotaz 64 bajtů, odpověď v řádu kilobajtů
- neotevírejte rekurzivní servery do internetu
  - omezte jejich použití na loopbacku nebo místní síť

ROOT.CZ_ vpsFree.cz

NTP

- Network Time Protocol (NTP) pro synchronizaci přesného času
  - velmi užitečná věc, přesný čas potřebujeme
- protokol umožňuje poslat příkaz **monlist**
  - odpovědí jsou informace o 600 posledních dotazech klientů
- implementační problém v NTP (ntp.org)
  - ve výchozím stavu otevřené rozhraní stavových informací
  - včetně nebezpečného (objemného) příkazu monlist
- zesílení více než **500×**
- používejte aktuální verze, které mají monitoring omezený
  - omezte přístup k servisním rozhraním
  - filtrujte příliš velké datové toky podobných služeb

ROOT.CZ_ vpsFree.cz

Memcached

- implementace distribuovaného kešovacího systému
  - velká hašová tabulka pro rychlou práci s daty
  - data uložena jako klíč-hodnota, klíč až 250 B, hodnota až 1 MB
  - používá se často na webu pro uložení keše nebo relací
- používá TCP nebo UDP port 11211
- nemá žádnou autentizaci, nepředpokládá se otevření ven
  - data používá jen aplikace na serveru přes loopback
- implementační chyba starších verzí
  - poslouchaly na všech rozhraních na UDP
- zesílení více než **51000×** – GitHub dostal 1,35 Tbit/s
  - rekordman v odražených útocích
- předcházejte takovým útokům, pozor na otevřené UDP
  - příjem jen přes loopback, firewall

ROOT.CZ_ vpsFree.cz

Prevence

Nebuďte součástí problému

- výše zmíněné útoky vyžadují falšování adres
- řada sítí dovolí libovolný odchozí provoz
  - klienti pak mohou provádět výše zmíněné útoky
- řešení popisuje BCP38 z **roku 2000**
  - filtrace na vstupu do sítě poskytovatele (ingress filtering)
  - od klientů přijímáme jen legitimní provoz
  - pouze z povolených rozsahů, ostatní zahodíme
- brání to také neúmyslným konfiguračním chybám
  - úniku privátního provozu do sítě poskytovatele
  - použití loopbackových adres ve veřejné síti
  - šíření multicastu špatným rozhraním

ROOT.CZ_ vpsFree.cz

Starejte se o své servery

- pravidelně **aktualizujte** veškerý software a systém
  - používejte podporované distribuce a nástroje
- uplatňujte zásady nejmenších **oprávnění**
  - nikomu nevěřte: uživatelům, počítačům ani službám
- **minimalizujte** používaný software a spuštěné služby
  - mějte pod kontrolou prostředí a co je kde spuštěno
- nasaďte silné **přihlašování** a vícefaktorovou **autorizaci**
  - donuťte uživatele i sebe pracovat podle pravidel
- důsledně **monitorujte** a hlídejte anomálie
  - bez monitoringu letíte naslepo a nevíte, co se děje
- sledujte aktuální trendy a **přizpůsobujte se**
  - hrozby se mění, vědění je síla a většina úspěchu

ROOT.CZ_ vpsFree.cz

Děkuji za pozornost

Otázky?

Petr Krčmář
petr.krcmar@iinfo.cz

ROOT.CZ_ vpsFree.cz