Zajímavé funkce OpenSSH

Ondřej Caletka

cesnet

28. června 2018

Obsah

cesnet

Úvod

cesnet

OpenSSH

- svobodná implementace protokolu SSH od tvůrců OpenBSD
- nejde zdaleka jen o *šifrovaný telnet*
- standardizováno v IETF

cesnet

Běžné přihlášení

1. server drží privátní klíče od každého algoritmu
2. klient při prvním přihlášení potvrdí pravost otisku veřejného klíče serveru. Vazbu adresy a klíče si uloží klient v `~/.ssh/known_host`
3. uživatel se představí heslem
4. spustí se shell

cesnet

Jednoduchá vylepšení

- uživatelská konfigurace v souboru `~/.ssh/config`
- RandomArt obrázek `VisualHostKey yes`
- udržení spojení `ServerAliveInterval 10`
- ukončení mrtvého spojení pomocí `Enter ~ .`
- napovídání jmen z `known_hosts` pomocí `bash-completion` vyžaduje nehashovaná jména serverů: `HashKnownHosts no`

cesnet

Sdílené spojení

- multiplexování více nezávislých relací jedním SSH spojením
- realizováno pomocí řídicího soketu
  - *master* naváže spojení a vytvoří UNIX soket
  - *slave* se komunikuje soketem.
- autentizaci provádí pouze *master*

Konfigurace sdílení spojení

```
ControlMaster auto
ControlPath ~/.ssh/controlsock-%h-%p-%r
ControlPersist  30
```

cesnet

Uživatelské klíče

cesnet

Použití uživatelského klíče

- vygenerujeme klíč pomocí `ssh-keygen`
- dobrá praxe vyplnit smysluplný komentář `-C oskar@latte`
- klíč chráníme silným heslem
- různé algoritmy na výběr
  - DSA – 1024bit, deprecated, nepodporováno od verze 7.0 (2015)
  - RSA – volitelná délka, bezpečná výchozí 2048 bitů
  - ECDSA – 256, 384, nebo 521 bitů, k dispozici od 5.7 (2011)
  - Ed25519 – 256 bitů, k dispozici od 6.4 (2014)
- pro maximální kompatibilitu s ne-OpenSSH implementacemi jedině RSA
- kopírování na server ručně nebo pomocí `ssh-copy-id`

cesnet

Volby v souboru authorized_keys

`from="2001:db8::1,192.0.2.1"`	omezení IP adresy
`no-port-forwarding`	zakáže tunelování
`restrict`	vypne všechny tunely, pty, atd. včetně případných budoucích funkcí
`environment="NAME=value"`	nastaví proměnné prostředí (např. `GIT_AUTHOR_NAME`)
`command="command"`	vynutí spuštění konkrétního příkazu

cesnet

SSH agent

- klíčenka s privátními klíči uživatele, nepustí privátní klíč
- ad-hoc spuštění pomocí `ssh-agent bash`
- přidání klíče pomocí `ssh-add -c` vynutí vyžádání potvrzení před každým vystavením podpisu
- automatické přidání při prvním použití volbou `AddKeysToAgent confirm`
- lze omezit dobu života klíče v klíčence pro každý klíč i pro agenta: `-t8h`
- agenta je možné tunelovat pomocí `ssh -A` nebo volby `ForwardAgent yes`
  - (super-)uživatel vzdáleného systému **má ke klíčence přístup**!
  - lépe omezit jen na důvěryhodné servery a/nebo vyžadovat potvrzení před použitím klíče

cesnet

OpenSSH certifikáty

- možnost delegovat ověření klienta nebo serveru na certifikační autoritu
- nejde o X.509, CA je obyčejný SSH klíč
- certifikát v samostatném souboru `<jméno klíče>-cert.pub`
- použití například jako:

  osobní CA pro všechny klíče uživatele – není třeba pravidelně aktualizovat `authorized_keys`

  serverová CA automatická důvěra veřejným klíčům serverů

  centrální uživatelská CA v certifikátu je uvedené jméno uživatele, v konfiguraci sshd je globální volba `TrustedUserCAKeys`
- revokace pouze distribucí revokačních seznamů

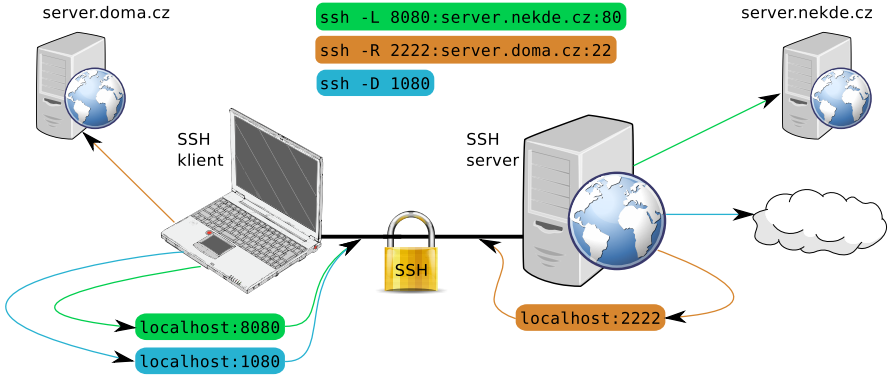
cesnet

Tunelování

cesnet

Tunelování

- statické i dynamické (SOCKS v4 / SOCKS v5)
- nejde o TCP-in-TCP ale tři nezávislá TCP spojení
- na poslouchací straně omezeno na localhost



cesnet

Režim netcat

- přepínač `-W <host>:<port>` spojí *stdio* klienta k TCP spojení na straně serveru
- hodí se na tunelování SSH spojení SSH spojením.
- výborně se kombinuje s volbou `ProxyCommand`

~/.ssh/config

```
Host server-behind-firewall
    ProxyCommand ssh -W 10.0.0.1:22 firewall.nekde.cz
```

cesnet

Přímá podpora `ProxyJump`

- k dispozici od OpenSSH 7.3
- automaticky naváže tunely skrz vyjmenované *jump hosts*
  `-J [<user>]@<host>[:<port>],…`
- spojení se po cestě nerozšifrovává
- vylučuje se s volbou `ProxyCommand`

~/.ssh/config

```
Host *.mgmt.cesnet.cz
    ProxyJump oskar@oskarpc.cesnet.cz
```

cesnet

Serverové klíče

cesnet

Serverové klíče

- stejné jako uživatelské klíče
- vygenerované při instalaci, nebo prvním startu
- nejsou chráněny heslem, je možné použít SSH agenta
- jeden[1] pro každý algoritmus
- obtížné rolování
- volba klienta `UpdateHostKeys yes` pro automatickou aktualizaci klíčů (od verze 6.8)

[1] nebo i více, ale používá se vždy první

cesnet

Ověření serveru pomocí DNSSEC

- vygenerujeme otisk **z klíče serveru na disku** pomocí `ssh-keygen -r <owner>`
- klientovi nastavíme volbu `VerifyHostKeyDNS <yes|ask>`
- výhoda – klíč je možné bezešvě rolovat

Příklad

```
The authenticity of host 'server.example.com (192.0.2.1)'
can't be established. RSA key fingerprint is
aa:55:cc:9c:a5:c6:1b:f1:a5:d2:be:eb:7e:1c:53:05.
Matching host key fingerprint found in DNS.
Are you sure you want to continue connecting (yes/no)?
```

cesnet

Ostatní

cesnet

OpenSSH HPN patche

- OpenSSH není optimalizováno na výkon
- pomalé při vyšší latenci kvůli malé a fixní velikosti bufferů
- velké buffery zase zabíjejí interaktivitu (*Bufferbloat*)
- problém řeší sada patchů označených jako HPN
  - dynamická velikost bufferu podle TCP okna
  - možnost nulového šifrování
  - možnost paralelizace některých procesů

cesnet

Mosh – Mobile Shell

- zcela nový protokol pro příjemnější terminálové sezení na nekvalitní lince
- využívá UDP zprávy a inteligentní lokální odezvu
- autentizace pomocí SSH, žádný nový démon
- usnutí a probuzení, či změna IP adresy klienta za běhu
- synchronizuje pouze stav obrazovky
- implementuje pouze UTF-8 terminál
- nedokáže nic tunelovat
- nedokáže roamovat mezi IP adresami serveru

cesnet

Závěrem

- chraňte osobní klíče heslem – **i na šifrovaném disku**
- používejte agenta, ale vyžadujte potvrzení každého použití klíče
- nemažte soubor `known_hosts`!
  Lepší je `ssh-keygen -R <jméno serveru>`
- zapněte ověřování SSHFP záznamů v DNS
- vyzkoušejte: `ssh whoami.filippo.io`
- více informací: Root.cz: Pokročilé vlastnosti OpenSSH

cesnet

Děkuji za pozornost

Ondřej Caletka
Ondrej.Caletka@cesnet.cz
https://**Ondřej.Caletka.cz**

Prezentace je již nyní k dispozici ke stažení.