SSH pro paranoiky

Václav Mach

cesnet

11. února 2020

Úvod

Předpoklady

- Známe a používáme SSH
- Používáme host firewall
- Máme servery nastaveny bezpečně (pouze klíče, jiný port(?), zákaz roota(?), ...)

motivace pro dodatečné zabezpečení

- Dbáme na dobré zabezpečení
- Chceme zalepit „díry“
- Chceme předcházet potenciálním průnikům

cesnet

Restrikce na aplikační vrstvě

Přihlášení klíčem umožňuje definování dodatečných restrikcí v souboru authorized_keys.

Formát souboru authorized_keys

- Volby přihlášení (volitelné)
- Typ klíče
- Klíč (base64)
- Komentář (volitelný)

cesnet

Restriktivní volby přihlášení

- Spoutěný příkaz – `command="ukázkový_příkaz"`
- Proměnné prostředí – `environment="PROMĚNNÁ=hodnota"`
- Zdrojová adresa klienta – `from="203.0.113.0/24"`
- Všechny existující i budoucí restrikce – `restrict`
- ...

cesnet

Ukázka 1 – omezení spouštěného příkazu

ukázka.py

```
#!/usr/bin/env python3
import sys
print(', '.join(sys.argv[1:])) # vytiskni všechny parametry programu
```

Spoutěný příkaz – přesný formát

```
command="./ukázka.py parametr1 parametr2" ssh-ed25519 AAAA... user1
```

```
$ ssh user1@noob.cesnet.cz
parametr1, parametr2
```

Spoutěný příkaz – libovolné parametry

```
command="./ukázka.py $SSH_ORIGINAL_COMMAND" ssh-ed25519 AAAA... user1
```

```
$ ssh user1@noob.cesnet.cz a b c d
a, b, c, d
```

Ukázka 2 – omezení zdrojové adresy

Lze použít CIDR, doménová jména a wildcard matching.

Omezení zdrojové adresy

```
from="195.113.134.139/32" ssh-ed25519 AAAA... user1

$ ssh user1@noob.cesnet.cz
Permission denied (publickey).
```

sshd[28389]: Authentication tried for user1 with\
correct key but not from a permitted\
host (host=195.113.233.246, ip=195.113.233.246).

cesnet

Ukázka 3 – AuthorizedKeysCommand

Definuje program, který pro uživatele hledá klíče.

- Omezení v sshd_config
- Lze kombinovat s prázdným authorized_keys
- Umožnuje dynamicky přiřazovat klíče uživatelům
- Používá formát authorized_keys – můžeme využívat restrikce

Konfigurace

```
Match User user1
    AuthorizedKeysCommand /root/klíče_user1.sh
    AuthorizedKeysCommandUser root
```

klíče_user1.sh

```
#!/bin/bash
echo 'ssh-ed25519 AAAA... user1'    # můžeme dotazovat databázi, ldap, ...
                                    # nebo si definovat přístupy zcela podle vlastní logiky
```

Akce vyvolané přihlášením

PAM umožnuje definovat program, který je spuštěn na základě přihlášení uživatele.

Použití

- Naprosto kritický server, který ovládá ...
- Chceme vědět o každém (netypickém?) přihlášení
  - Přihlášení uživatele – notifikace (mail, SMS, monitoring, zpráva na IM, ...)
- Dodatečná příprava pracovního prostředí
- ...

cesnet

Ukázka – konfigurace

/etc/pam.d/sshd

```
...
# ukázka notifikace
session required pam_exec.so /root/notifikace.sh
```

notifikace.sh

```
#!/bin/sh
to="vaclav.mach@cesnet.cz"
from="ssh-alert@noob.cesnet.cz"
# pošli mi všechny proměnné prostředí
env | mail -s "ssh notifikace" -r $from $to
```

cesnet

Ukázka – výstup

```
...
...
PAM_USER=user1
SSH_AUTH_INFO_0=publickey ssh-ed25519 AAAA...
PAM_RHOST=195.113.134.139
PAM_TYPE=open_session
PAM_TTY=ssh
PAM_SERVICE=sshd
```

Na základě hodnot proměnných prostředí můžeme definovat logiku v našem programu.

cesnet

Omezení přístupu na servery

Problémy

- Přístupy z předem neznámých adres (pracovní cesta, dovolená, homeoffice, ...)
- Více správců, správci se v čase mění

Správa host firewallu může být težkopádná – nevhodné pro ruční správu.

Lze řešit pomocí VPN, ale i to má svoje nevýhody:

- SPOF
- Kombalitibilita napříč platformami
- Granularita přístupů v rámci VPN

cesnet

Port knocking/SPA (single packet authorization)

princip fungování

- Firewall – implicitní DROP (lze i REJECT) politika pro všechny adresy
- Po „zaťukání“ (nebo jiné formě autorizace) dočasně povolen přístup

Pro externího pozorovatele (shodan.io, ...) není vůbec zřejmé, že SSH běží.

Spíše pro osobní potřeby (pracovní stanice, VPS) než pro masivní korporátní používání.

cesnet

Port knocking/SPA (single packet authorization)

Port knocking

- Základní varianta dodatečné autorizace
- Sekvence paketů na definované porty
- Náchylné na odposlech (autorizační informace pouze v hlavičkách paketů)

Single packet authorization

- Vylepšuje port knocking
- jediný paket
- Využívá šifrování

cesnet

Port knocking/SPA (single packet authorization)

Výhody

- Výrazně snížená viditelnost služby i povrch útoku
- Dodatečná autorizace pro přístup ke sluzbě

Nevýhody

- Vyžaduje specializovaný software – klient i server
- Kompatibilita napříč platformami
- Není standardizováno – používat kompatibilního klienta a server (hlavně SPA)

cesnet

Dotazy

Dotazy?

cesnet