Semestrální práce KKY/BSOI

Green team: Jana Romová, Jan Šimek, Petr Železný

Virtuální stroj

Virtuální stroj je hostován na platformě **OpenNebula**. Při vytváření stroje jsme mu přidělili 2jádrový procesor, 1GB RAM a 8GB úložiště, což nám vzhledem k povaze úlohy přišlo jako dostačující. Větší než defaultní úložiště se v průběhu semestru ukázalo jako výhoda, neboť při trénování rozpoznávání tváří měly některé další týmy problém s tím, že jim úložiště nevystačilo na uložení všech datasetů, a museli tak zakládat nové stroje.
IP adresa virtuálního stroje je **147.228.173.95** a přidělený hostname je **sulis95**.

Na virtuální stroj mají přístup čtyři identity – všichni tři členové týmu Green a root, zároveň má každý člen práva root kvůli jednodušší práci na zadaných úkolech. V praxi bychom však byli s přidělováním práv root opatrnější, jednak kvůli bezpečnosti a jednak proto, aby si uživatelé navzájem neprováděli nechtěné či neočekávané změny na virtuálním stroji. K přihlašování na virtuální stroj využíváme **SSH klíče**. Ty jsme si nechali vygenerovat a nakonfigurovat pomocí příkazů `ssh-keygen` a `ssh-copy-id` v prostředí Linuxu (podle návodu zde). Jako pojistku máme nastavená i klasická hesla, ale pokud by se jednalo o nějaký prvek důležité infrastruktury (ne o školní úlohu), uvažovali bychom o jejich úplné deaktivaci.

Uživatelé

- Jan Šimek: username: honzik, heslo: ********, SSH klíč aktivován, sudo: ano
- Jana Romová: username: jana, heslo: *******, sudo: ano
- Petr Železný: username: petr, heslo: ********, sudo: ano

Přihlašování na webové rozhraní

Při vstupu na webové rozhraní se uživatel musí přihlásit rozpoznáním tváře z fotky vyfocené kamerou na jeho zařízení. Stránka mu poskytne informaci o tom kdo si myslí, že je a na kolik procent si je o této identitě jistá. Samotné rozpoznávání je zajištěno umělou inteligencí (knihovna OpenCV), která byla natrénována z datasetů, uložených v adresáři: /home/user/server/faceid/dataset v jednotlivých složkách, kde každá složka odpovídá jedné identitě.

Složky - celkem 337 snímků

- Jan Šimek: složka: simek_honza, velikost datasetu: 82 snímků,
- Jana Romová: složka: romova_jana, datasetu: 70 snímků,
- Petr Železný: složka: zelezny_petr, datasetu: 156 snímků,
- Unknown: složka: unknown, datasetu: 29snímků,

Dataset identity Unknown, který je navíc, obsahuje snímky neautorizovaných osob pro možnost rozpoznání neznámé osoby. Datasety jsou pouze pro členy týmu, protože pro jiné osoby nebyl dostatek snímků pro natrénování. Díky obsáhlejším datasetům jsme byli schopni nastavit práh pro ověření autorizované osoby na 80%. Pokud se uživatel pokusí přihlásit aniž by jeho pravděpodobnost rozpoznání byla alespoň tento práh, server ho přesměruje zpět na přihlašovací portál.

Pro držení si informace o tom, zda je uživatel přihlášen či ne, jsme použili secure cookies, které nelze přepsat uživatelem a je tím pádem zamezeno neoprávněnému vniknutí do systému. Pro zasílání dat o rozpoznání uživatele jsme využili protokol http/https.

Celé tornado aplikace pak spouští server s https certifikáty (mezilehlé CA) pro šifrovaný přenos dat, které jsme získali od certifikační autority **Let's encrypt** pro doménu sulis95.zcu.cz. K podepisování a šifrování je použit RSA (256 bitů) algoritmus, veřejný klíč je typu **ECC** (256 bitů, využití vektorových křivek.

Zálohování

Zálohování dat probíhá každých 5 minut do textového souboru na virtuální stroj. Samotné skripty jsou zálohovány na GitHubu ve veřejném projektu. Nepodařilo se nám provést automatické zálohování, a tak jsme data zálohovali každý týden ručně, na externí disk.

Monitoring

Běh serveru je monitorován službou UptimeRobot (monitoring URL https://sulis95.zcu.cz). Oznámení o stavu UP/DOWN přicházejí jako e-mailové notifikace jednomu členovi týmu (Jan Šimek), který nejprve kontaktuje pracovní skupinu, zda právě nedochází k úmyslným úpravám na stroji, a pokud se nedaří problém vyřešit restartem běžících programů či opravou chyb v kódech, restartuje virtuální stroj přímo na platformě OpenNebula, protože virtuální stroj je hostován na jeho Orion účtu. Tento monitoring funguje spolehlivě, neboť během vypracovávání semstrální práce jsme obdrželi mnoho notifikací, které korespondovaly s námi známým či předpokládaným stavem stroje.

Firewall

Náš virtuální stroj je chráněn perzistentním firewallem – tedy sadou pravidel zanesených v tabulce `iptables` virtuálního stroje s operačním systémem Debian 11. Tyto pravidla jsme nastavili tak, aby byla příchozí komunikace možná pouze skrz porty 22 (SSH, SFTP), 80 (HTTP) a 443 (HTTPS) a veškerá další příchozí komunikace byla zamítnuta. Toho jsme docílili posloupností následujících příkazů (s právy root):

```
iptables -A INPUT -p tcp --dport ssh -j ACCEPT
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -p tcp --dport 443 -j ACCEPT
iptables -P INPUT DROP
```

Dále jsme pravidla uložili do souboru a nastavili jako perzistentní, aby se při restartu stroje načetly automaticky. Ve výchozím nastavení se totiž po restartu stroje načtou výchozí pravidla, čímž stroj chrání uživatele před tím, aby si „uřízl větev”.