V rámci předmětu KKY/BSOI jste si vytvořili a nastavili virtuální stroj s operačním systémem Linux. Tento virtuální stroj používáte pro provozování Vaší distribuované aplikace vyvíjené v rámci předmětu KKY/ITE.

Jako semestrální práci KKY/BSOI práci odevzdáte referát popisující virtuální stroj, úkony a činnosti, které jste na něm provedli, dále popíšete nastavení operačního systému a realizaci biometrického způsobu autentizace pomocí charakteristik lidské tváře.

Pro ověření funkčnosti biometrického přihlašování využijte dodanou sadu snímků Vašich vyučujících, kterým přiřadíte jejich identity (Jan Švec, Martin Bulín, Vlasta Radová) a povolíte jim přihlášení do webové aplikace na uvedené vstupní stránce. Identity vyučujících, jejichž snímky nemáte k dispozici (Tomáš Lebeda), budou sloužit pro ověření, zda systém zamítne obličej „cizí“ osoby. Pro kontrolu práce ale ponechejte možnost přihlásit se jménem a heslem pro **všechny** vyučující.

Zároveň budete hrát s ostatními týmy hru na způsob „capture the flag“. V první části budete v roli hackera, který se snaží uložit nějaká data (mallware, škodlivý kód) na stroj tak, aby je nikdo jiný nenašel. V druhé části pak budete naopak v roli forenzního analytika, který se snaží na napadnutém stroji tento mallware nebo škodlivý kód odhalit.

Každý tým obdrží pět unikátních textových řetězců - flagů, které musí někde na svém virtuálním stroji „schovat“. Po uplynutí předem dané doby (řádově dny) dostanou ostatní týmy přístup (pod novým, Vámi vytvořeným uživatelem) na Váš virtuální stroj a budou se snažit Vámi schované flagy najít (opět v daném časovém limitu, řádově dny). Za Vaše prozrazené flagy dostanete záporné body, za nalezené flagy cizích týmů dostanete kladné body. Podle počtu získaných bodů budou na konci rozděleny bonusové body ke zkoušce.

Referát

Referát odevzdejte jako pdf soubor, nejpozději do konce ledna (31. 1. 2026 23:59). Odevzdání referátu je nutná podmínka pro zápočet a připuštění ke zkoušce.

V referátu není nutné vkládat zdrojové kódy nebo vysvětlovat detailní implementace, podstatné je vysvětlit a zdůvodnit svoje řešení, na jaké problémy jste narazili a jak jste postupovali při jejich překonání. Pokud jste něco řešili kreativním, netradičním nebo mimořádným způsobem, nebo jste udělali něco navíc, určitě neváhejte tyto věci v referátu popsat, mohou za ně být bonusové body.

Referát by měl fundovaným způsobem zodpovědět následující otázky:

- **Vlastnosti virtuálního stroje**
  Jaký virtuální stroj, s jakými parametry, jaký OS/distribuce, jste založili? Uveďte hostname a IP adresu.
- **Uživatelské účty**
  Jaké jste použili uživatelské účty? Používali jste SSH klíče a jak? Měli jste povoleno přihlášení jako `root`? Kdo mohl používat `sudo`?
- **Monitorování a zálohování**
  Jak jste realizovali monitoring? Jak jste stroj zálohovali?

- **Šifrování**
  Od jaké autority jste si nechali vystavit TLS certifikát, jakou má platnost a parametry?
- **Zabezpečení virtuálního stroje**
  Jaké porty a z jakých strojů máte otevřené ve Firewallu? Z jakých důvodů?
- **Provozování distribuované aplikace**
  Jaké součásti vaší aplikace máte spuštěny? Kam a pomocí jakých protokolů komunikujete? Jak máte zajištěno jejich automatické spuštění po restartu virtuálního stroje nebo pádu aplikace? Jak logujete jejich výstup? Jak provádíte nasazení nových verzí?
- **Biometrická autentizace pomocí charakteristik tváře**
  Jak jste postupovali při implementaci? Kolik identit a kolik příkladů od každé identity používáte? Jak jste stanovili rozhodovací práh?
- **Přihlášení a správa sezení**
  Jak realizujete přihlášení uživatele pomocí tváře? Jak realizujete záložní metodu ověření? Popište, jak postupujete při prvním přístupu nepřihlášeného uživatele a jak odhlašujete. Jaká je vstupní stránka Vaší webové aplikace?
- **Schovávání flagů**
  Jak a kam jste schovali a uložili Vaše flagy?
- **Hledání flagů**
  Jak a kde jste našli (nebo alespoň hledali) schované flagy ostatních týmů?
- **Krátký závěr**
  Shrnutí, klíčové body, co jste si odnesli a jak jste si poradili s případnými problémy.

Hodnocení

Za semestrální práci je možné získat až 60 bodů, bodování je rozděleno do následujících kategorií:

Kategorie	Max. počet bodů
virtuální stroj	8
uživatelské účty	8
monitoring a zálohování	6
TLS certifikát	6
zabezpečení VM	6
provoz aplikace	10
biometrická autentizace	8
správa uživatelů	8

***Poznámka**: schovávání a hledání flagů není v tabulce bodování uvedeno, protože slouží pouze pro bonusové body ke zkoušce. Nicméně fáze schovávání a vytvoření účtů je povinná!*

Pro udělení zápočtu je nutné získat alespoň 30 bodů celkem a z každé kategorie alespoň 1 bod. Za mimořádně kvalitní vypracování některých částí je možné získat bonusové body (lze přesáhnout hranici 60 bodů), jejichž počet závisí na úsudku vyučujícího.

Body ze semestrální práce se sčítají s body ze zkoušky (až 40) a podle součtu bude udělena známka.

Pravidla hry

- Každý tým obdrží 13. 10. pět flagů ve formátu `blue_team_flag_R6xFAB1jQX`.
  - Poslední část bude vždy unikátní řetězec deseti ASCII znaků (`a-z`, `A-Z`, `0-9`).
- Nejpozději do 27. 10. musíte na svém VM všech 5 přidělených flagů schovat.
  - Musí se jednat o stejný virtuální stroj, na kterém poběží zbytek semestrální práce!
- Text flagu nesmí být modifikován (nelze ubírat/vkládat znaky nebo šifrovat).
- Flag musí být uložený celý (flag nelze rozdělit na části a každou z nich uložit jinde/jinak).
- Flag musí být získatelný/vypsatelný běžnými nástroji, které jsou k dispozici na VM.
- Flag musí být uložený „fyzicky“ na daném virtuálním stroji (zákaz mountování vzdálených disků nebo ukládání a stahování flagů z internetu nebo jiných VMs).
- Každý flag musí být schovaný/uložený fundamentálně jiným způsobem (nemůžete „vsadit všechno na jednu kartu“ a schovat všechny flagy jedním stylem).
  - Záměna kódování, název souboru a podobné menší „parametrické“ změny nejsou považovány za jiný způsob uložení. Pokud si nebudete jistí, jestli jsou nějaké dvě metody „dostatečně odlišné“, neváhejte se zeptat vyučujícího.
  - Výjimkou je schování flagů do plaintext souborů, tato jediná možnost lze opakovat pro více flagů.
- Na VM vytvoříte nejpozději do 27. 10. uživatele `seeker`, který bude sloužit pro hledání Vámi schovaných flagů.
  - Přihlášení na uživatele `seeker` musí být pouze přes SSH (zablokovat přihlášení přes login+password).
  - Pro uživatele `seeker` sami nahrajete SSH klíč vyučujícího, který dostanete všichni společně zároveň s flagy.
  - Svůj vlastní SSH klíč, který budete používat později pro přihlášení k cizím VM, pošlete soukromě vyučujícímu nejpozději do 27. 10. a on je všechny v jeden moment nahraje k uživateli `seeker` na všech VM, takže se budete moci všichni naráz přihlásit na cizí stroje.
  - Práva a přístupy pro uživatele `seeker` kontrolujete na svém virtuálním stroji sami, dle vlastního uvážení. **Všechny ostatní týmy se budou moci přihlásit na Váš virtuální stroj jako `seeker`!**
  - Po zahájení hledání (27. 10.) nesmíte ostatním týmům jakkoli blokovat přístup na VM nebo přihlášení uživatele `seeker`.
- Po zahájení hledání 27. 10. již nesmíte uložené a schované flagy měnit, přesouvat nebo jakkoli modifikovat.
- Kromě výše zmíněných pravidel můžete flagy uložit a schovat na libovolné místo (na celém Vašem VM), libovolným způsobem.
  - Sami musíte umět vlastní flagy najít a získat zpět do 10 minut, **24. 11. to budete demonstrovat**!
  - Při demonstraci budete muset postupovat stejně, jako byste byli cizí tým (pod stejným uživatelem `seeker` a se stejnými právy). Nelze tedy „jen“ vědět přesně do kterého souboru se podívat, nebo použít nějaký připravený backdoor, ale musíte umět zdůvodnit a ukázat, jak by ostatní týmy museli postupovat, kdyby chtěli Váš flag najít.
- Aby nešlo znemožnit hledání flagů vypnutím stroje, musí během fáze „hledání“ Váš VM běžet neustále.
  - Může se stát, že VM spadne, někdy tomu nelze zabránit. V takovém případě udělejte vše pro to, aby se stroj co nejdříve zase rozběhl (měli byste mít ze cvičení nastavený monitoring). Postup (a časy!) detekce pádu VM a podniknuté kroky k nápravě si poznamenejte, může je po Vás vyučující požadovat.
  - Pokud detekujete, že cizí VM neběží, zapište si IP adresu a čas a informujte zodpovědný tým. Pokud by problém přetrvával déle než pár hodin, informujte o tom vyučujícího.