**Úlohy na precvičenie – OPS 2024 – séria I**

Úlohy riešte samostatne a podrobne. Celý postup zaznamenajte a komentujte. Odpovedajte podľa možnosti na všetky položené otázky v úlohe. V záhlaví uveďte svoje meno, priezvisko a **zdroje, ktoré ste pri riešení použili** (citácie, URL adresy internetových zdrojov a mená osôb resp. generatívnych jazykových modelov, s ktorými ste riešenie prípadne konzultovali). Za každé správne a vyčerpávajúce riešenie (**s komentovaným postupom a slovnou odpoveďou**) možno získať bod. Zlomky bodov možno získať aj za čiastočné riešenia. Riešenia odovzdajte do 23. 4. 2024, 15:20. Neskôr dodané riešenia a plagiáty nebudú opravované ani hodnotené. Problémy môžete konzultovať po prednáške resp. elektronickou poštou.

1. Odsledujte Wiresharkom priebeh telnet spojenia (v Linuxe resp. pomocou PuTTY) k GPU serveru 158.197.31.56 – na port 2345 (v Analyze/Decode_As treba nastaviť TCP port 2345 current TELNET). Na server sa prihláste do svojho konta studentxx z tutoriálu GPU a odhláste sa. Odfiltrujte príslušnú TCP reláciu, dekódujte telnet protokol a komentujte začiatočné dohadovanie na parametroch komunikácie. Na akých parametroch bola dohoda? Vysledujte zadávanie mena a hesla a popíšte spôsob prenosu týchto údajov.

2. Odsledujte Wiresharkom priebeh SSH spojenia (Linux resp. PuTTY) k GPU serveru 158.197.31.56 – na port 225 (Analyze/Decode_As nastaviť na SSH) s prihlásením a odhlásením podobne ako v úlohe 1. Odfiltrujte príslušnú TCP reláciu a dekódujte ako SSH. Vypíšte obsah textových reťazcov v prvej výmene. Vypíšte tri najpreferovanejšie šifrovacie algoritmy klienta a tri servera a výsledný výber (pre obidva smery) šifrovacieho algoritmu, režimu šifrovania a autentifikačnej funkcie správ. Aký postup sa použil na generovanie kľúča relácie? Vypíšte prvé 4 bajty serverovho a prvé 4 bajty klientovho príspevku. Vypíšte aj prvé 4 bajty verejného kľúča servera – akým spôsobom klient overí dôveryhodnosť servera? Možno niekde nájsť jeho certifikát?

3. Na pripojenie protokolom SSH je možné namiesto hesla použiť asymetrické kľúče. Vyrobte si dvojicu kľúčov (pre podpis pomocou Edwardsovej eliptickej krivky Ed25519) napr. v PuTTYgen alebo pomocou ssh-keygen -t ed25519) a verejný kľúč (v textovom SSH formáte) pripíšte na server do súboru ~/.ssh/authorized_keys. Ak ste to urobili správne, pri prihlasovaní už server nebude vyžadovať heslo. Odsledujte Wiresharkom prihlasovanie teraz a porovnajte s prípadom v úlohe 2. Akým spôsobom použije server uložený verejný kľúč na overenie klienta?