Úlohy na precvičenie – OPS 2024 – séria J

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 30. 4. 2024, 15:20. Neskôr dodané riešenia a plagiáty nebudú opravované ani hodnotené. Problémy môžete konzultovať po prednáške resp. elektronickou poštou.

1. Binárny súbor má veľkosť 5400 bytov. Posielame ho elektronickou poštou, pričom dĺžka jedného riadka nemôže presiahnuť 76 znakov. Aká bude veľkosť súboru po zakódovaní systémom Base64 ? Aká by bola jeho približná veľkosť po zakódovaní spôsobom Quoted-printable za predpokladu rovnomernej pravdepodobnosti výskytu hodnôt bytov v pôvodnom súbore?

2. Zobrazte si pôvodný (neinterpretovaný) text jednoduchej elektronickej poštovej správy, obsahujúcej aspoň jeden obrázok (zakódovanej SMTP protokolom s rozšírením MIME). Nájdite identifikátor hraníc častí správy (boundary). Vypíšte postupne všetky MIME hlavičky (riadky, začínajúce MIME typom hlavičky, ukončenom „:“) v každej časti a popíšte význam uvedených konkrétnych parametrov pre interpretáciu textu elektronickej pošty. Komentujte použité kódovania.

3. (úplné riešenie za 2 body) Wireshark podporuje dešifrovanie TLS streamov pre prehliadače (Firefox, Chrome), ktoré využívajú ukladanie dočasných pre-master kľúčov do súboru, identifikovaného v systémovej premennej SSLKEYLOGFILE. V Linuxe je možné ju nastaviť príkazom Export, vo Windows Advanced System Settings/Environment Variables. Systém treba reštartovať. Cestu k tomuto súboru je potom potrebné nastaviť tiež v Edit/Preferences/Protocols/TLS do (Pre)-Master-Secret log filename vo Wiresharku. Podrobný návod nájdete napr. na

https://www.comparitech.com/net-admin/decrypt-ssl-with-wireshark/ alebo

https://resources.infosecinstitute.com/topic/decrypting-ssl-tls-traffic-with-wireshark/

Vysledujte pri tomto nastavení priebeh TLS relácie pripojenia k HTTPS stránke www.upjs.sk. Najskôr zatvorte všetky otvorené stránky na tejto adrese. Po štarte zachytávania otvorte stránku a hneď ju zatvorte. Až potom ukončite zachytávanie. Odfiltrujte a dekódujte príslušný hlavný TLS stream. Aké RLP bloky sa vymenili medzi klientom a serverom počas fáze handshake? Aké verzie TLS podporuje klient a aké server? Aké šifrovanie a v akom režime si zvolil server? Aké algoritmy na dohodu kľúčov podporuje klient a aký a koľkobitový algoritmus vybral server? Vypíšte prvých 8 bitov klientovho a serverovho príspevku k tvorbe kľúča. V bloku Certificate vysledujte certifikáty servera. Koľko certifikátov posiela server? Vypíšte z každého certifikátu meno subjektu, meno certifikačnej autority a dokedy certifikát platí. Koľko bajtov zaberá v bloku certifikát www.upjs.sk a na čo je ho možné používať? Koľkobitový kľúč používa a aký je jeho verejný exponent? Nájdite v certifikáte www.upjs.sk adresu miesta, kde je uverejnený zoznam revokovaných (neplatných) certifikátov jeho certifikačnej autority. Zoznam (s príponou .crl) skopírujte a zistite, koľko certifikátov bolo na tejto autorite zrušených v nedeľu 21. apríla 2024. Okomentujte aj spôsob ukončenia celého TCP streamu relácie.