

Dokumentácia pre vyučujúceho k laboratórnej úlohe

Laboratórna úloha č. 8

Autentizácia pomocou EAP a RADIUS

1. Základné informácie k laboratórnej úlohe

Laboratórna úloha č. 8 je venovaná možnostiam realizácie centralizovanej autentizácie v počítačových sieťach pomocou protokolov IEEE 802.1X, EAP a RADIUS. Cieľom úlohy je, aby si študenti prakticky osvojili základné pojmy súvisiace s autentizačným rámcom EAP, konfiguráciou prístupového bodu, autentizačného servera a klienta, a aby boli schopní analyzovať priebeh celého procesu autentizácie na základe použitých autentizačných protokolov.

Úlohou študentov je nakonfigurovať sieť s využitím troch zariadení – klienta, prístupového bodu a RADIUS servera. Využili pritom nástroje ako FreeRADIUS, hostapd a wpa_supplicant. Cieľom je teda vytvoriť úplnú funkčnú autentizačnú infraštruktúru a overiť správnosť autentizácie na základe rôznych nastavení.

2. Očakávané výstupy práce študentov

Praktická činnosť študentov v rámci tejto úlohy spočívala v simulácii procesu autentizácie klienta prístupujúceho do vytvorenej siete, a to s použitím nástrojov ako FreeRADIUS, hostapd a wpa_supplicant. Úlohou študentov bolo uskutočniť vhodné úpravy v konfigurácii použitých VM tak, aby dosiahli ich požadovanú funkčnosť pre plnohodnotné zapojenie do autentizačného procesu, t.j. bolo potrebné nakonfigurovať jeden VM ako prístupový bod sprostredkujúci komunikáciu overovaného klienta a autentizačného servera, a tiež ďalší VM ako samotný server RADIUS.

Po uskutočnení laboratórnej úlohy by mali byť študenti schopní popísať priebeh autentizačného procesu a analyzovať odosielané EAP správy vďaka záznamu komunikácie vo Wiresharku. Správnosť realizácie úlohy je možné overiť na základe splnenia nasledujúcich bodov:

- Na prístupovom bode správne beží služba hostapd s nakonfigurovaným smerovaním autentizačných požiadaviek.
- FreeRADIUS server je správne nakonfigurovaný a prijíma EAP požiadavky od prístupového bodu.
- wpa_supplicant na klientovi úspešne odosiela autentizačné správy (pozorovanie stavov "Authentication Success" v zachytenej komunikácii vo Wiresharku alebo v zobrazených logoch v termináli).
- Pomocou Wiresharku je zachytená komunikácia identifikujúca priebeh autentizácie klienta (pakety EAP, prípadne RADIUS správy Access-Request a Access-Accept).
- Výsledkom procesu je úspešná autentizácia klienta (logy potvrdzujú úspešný EAP *handshake* medzi klientom a RADIUS serverom).

2.1. Riešenie samostatnej úlohy

V rámci samostatnej úlohy majú študenti za úlohu implementovať použitie autentizačnej metódy EAP-TTLS a multifaktorovej autentizácie klienta s využitím kombinácie hesla a certifikátu. Pre konfigurácie autentizácie založenej na využití certifikátu bude potrebné, aby študenti vytvorili na RADIUS serveri vlastnú certifikačnú autoritu a následne vygenerovali dvojicu certifikátov:

- certifikát pre autentizačný server (resp. pre FreeRADIUS),
- certifikát klienta.

Následne vhodnou zmenou konfigurácie na serveri i klientovi zadefinujú použitie autentizačnej metódy EAP-TTLS, pričom je dôležité dbať na správnosť použitia vygenerovaných certifikátov. Taktiež je potrebné, aby študenti realizovali prenos certifikátov a súkromného kľúča klienta na jeho zariadenie (napr. pomocou scp).

Ak je `wpa_supplicant` správne nakonfigurovaný, tak bude úspešné pripojenie indikované správou: **"CTRL-EVENT-CONNECTED"**. Vo Wiresharku bude správne zachytená komunikácia, v ktorej bude možné pozorovať správy protokolu TLS prenášané vytvoreným šifrovaným tunelom.

2.2. Odpovede na kontrolné otázky

1. Ktoré tvrdenia správne popisujú fungovanie autentizačného mechanizmu podľa IEEE 802.1X?
 - A) Overenie identity prebieha ešte pred pridelením IP adresy klientovi ☒
 - B) IEEE 802.1X je vhodný len pre bezdrôtové siete
 - C) Komunikácia medzi klientom a prístupovým bodom prebieha cez EAPoL ☒
 - D) IEEE 802.1X zabezpečuje šifrovanie prenosu autentizačných údajov
2. Ktoré z nasledujúcich výrokov platia o úlohe prístupového bodu (*authenticator*) v architektúre IEEE 802.1X?
 - A) Posudzuje platnosť prihlasovacích údajov a vydáva rozhodnutie o prístupe
 - B) Vystupuje ako sprostredkovateľ komunikácie medzi klientom a autentizačným RADIUS serverom ☒
 - C) S klientom komunikuje prostredníctvom protokolu EAPoL ☒
 - D) Generuje prístupové heslá pre klientov v lokálnej sieti
3. Vyberte nesprávne tvrdenia o protokole RADIUS:
 - A) Komunikácia medzi klientom a RADIUS serverom prebieha prostredníctvom transportného protokolu UDP na porte 1812
 - B) RADIUS šifruje celé pakety pomocou TLS ☒
 - C) RADIUS umožňuje centralizované overenie identity
 - D) RADIUS prenáša EAPoL správy ako súčasť autentizačných požiadaviek ☒

4. Ktoré typy EAP metód využívajú digitálne certifikáty?
- A) EAP-TLS ☒
 - B) EAP-MD5
 - C) EAP-PEAP
 - D) EAP-TTLS ☒
5. Ktoré tvrdenia o nástroji FreeRADIUS sú pravdivé?
- A) Podporuje rôzne autentizačné metódy, vrátane EAP ☒
 - B) podporuje použitie iba jednej autentizačnej metódy v jednom okamihu
 - C) Môže byť konfigurovaný na prácu s TLS ☒
 - D) Nepodporuje použitie autentizačnej metódy EAP-MD5
6. Aké informácie sú prenášané v správe *Access-Request* protokolu RADIUS?
- A) Užívateľské meno (User-Name) ☒
 - B) Hash hesla alebo autentizačný token ☒
 - C) ID a heslo užívateľa (klienta)
 - D) IP a MAC adresa klienta
7. Aký príkaz v Kali Linux slúži na spustenie služby FreeRADIUS?
- A) sudo start radiusd
 - B) sudo systemctl start freeradius ☒
 - C) radiusctl enable
 - D) freeradius --run
8. Ktoré EAP správy sú typicky súčasťou autentizačného procesu pri overovaní identity s využitím metódy EAP-MD5?
- A) Identity Request ☒
 - B) Identity Response ☒
 - C) EAPOL Success/Failure ☒
 - D) Access Request
9. Čo je typické pre komunikáciu medzi klientom a AP počas výmeny EAP správ?
- A) Komunikácia prebieha pomocou protokolu EAPoL ☒
 - B) Pakety sú prenášané v ethernetovom rámci na spojovej vrstve ☒
 - C) Všetka komunikácia je šifrovaná pomocou TLS
 - D) Klient komunikuje priamo s autentizačným RADIUS serverom
10. Ktoré z nasledujúcich tvrdení o EAP over LAN (EAPoL) sú nepravdivé?
- A) EAPoL sa používa na prenos EAP správ cez káblové alebo bezdrôtové LAN siete
 - B) EAPoL správy sú zapuzdrené priamo do IP paketov ☒
 - C) EAPoL zaisťuje komunikáciu medzi klientom a AP
 - D) EAPoL šifruje všetky EAP správy pomocou TLS ☒

2.3. Doplnujúce otázky

Nižšie uvedené otázky môžu byť využité pri kontrole výstupov samostatnej práce študentom s cieľom overiť, či skutočne porozumeli riešenej problematike v praktickej časti laboratórnej úlohy.

1. Aké sú výhody používania RADIUS servera v porovnaní s metódami umožňujúce lokálne overenie identity prístupujúceho užívateľa?

- Centralizované riadenie prístupu, možnosť správy veľkého množstva užívateľov, vyššia bezpečnosť a jednoduchšia správa prístupových politík.

2. Vysvetlite úlohu protokolu IEEE 802.1X v procese autentizácie.

- Riadi prístup do siete na základe overenia identity užívateľa pomocou externého autentizačného servera (napr. RADIUS).

3. Aké sú hlavné komponenty v architektúre 802.1X?

- Klient, resp. žiadateľ o overenie (*supplicant*), prístupový bod (*authenticator*), autentizačný server RADIUS.

4. Aké typy autentizačných metód podporuje RADIUS?

- Napr. EAP-TLS, EAP-PEAP, EAP-TTLS, EAP-MD5, PAP, CHAP.

5. Aké sú možné bezpečnostné riziká súvisiace s používaním protokolov EAP a RADIUS v otvorených sieťach? Uveďte príklad opatrení, pomocou ktorých by bolo možné tieto riziká zmierniť.

- Možnosť odpočúvania prebiehajúcej komunikácie alebo *spoofingu*, riziko MitM útokov, zneužitie slabých autentizačných mechanizmov. Riešením je používať pokročilé metódy pre šifrovanie komunikácie (napr. implementácia protokolu TLS).

6. Pomocou akého príkazu je možné spustiť RADIUS server na Kali Linux?

- `sudo systemctl start freeradius`

7. Aké filtre by ste použili vo Wiresharku pre zobrazenie EAP správ?

- `eap` alebo `radius`.