

# **Dokumentace pro vyučujícího k laboratorní úloze**

Laboratorní úloha č. 8

## **Autentizace pomocí EAP a RADIUS**

# 1. Základní informace k laboratorní úloze

Laboratorní úloha č. 8 je zaměřena na možnosti realizace centralizovaného ověřování identity v počítačových sítích pomocí protokolů IEEE 802.1X, EAP a RADIUS. Cílem úlohy je, aby si studenti prakticky osvojili základní pojmy související s autentizačním rámcem EAP, konfigurací přístupového bodu, autentizačního serveru a klienta, a aby byli schopni analyzovat průběh celého autentizačního procesu na základě použitých autentizačních protokolů.

Úkolem studentů je nakonfigurovat síť využívající tři zařízení – klienta, přístupový bod a RADIUS server. K tomu využijí nástroje jako FreeRADIUS, hostapd a wpa\_supplicant. Cílem je tedy vytvořit plně funkční autentizační infrastrukturu a ověřit správnost autentizace při různých nastaveních.

## 2. Očekávané výstupy práce studentů

Praktická činnost studentů v rámci této úlohy spočívá v **simulaci procesu autentizace klienta připojujícího se do vytvořené sítě**, a to s využitím nástrojů FreeRADIUS, hostapd a wpa\_supplicant. Úkolem studentů je provést vhodné úpravy konfigurace použitých virtuálních strojů tak, aby bylo dosaženo jejich požadované funkčnosti pro plnohodnotné zapojení do autentizačního procesu. To znamená nakonfigurovat **jeden virtuální stroj jako přístupový bod** zprostředkovávající komunikaci ověřovaného klienta s autentizačním serverem a **další virtuální stroj jako samotný RADIUS server**.

Po splnění laboratorní úlohy by studenti měli být schopni popsat průběh autentizačního procesu a analyzovat odesílané EAP zprávy díky záznamu komunikace ve Wiresharku. Správnost provedení úlohy je možné ověřit na základě splnění následujících bodů:

- Na přístupovém bodu správně běží služba hostapd s nakonfigurovaným směrováním autentizačních požadavků.
- FreeRADIUS server je správně nakonfigurován a přijímá EAP požadavky od přístupového bodu.
- wpa\_supplicant na klientovi úspěšně odesílá autentizační zprávy (pozorování stavů "Authentication Success" v zachycené komunikaci ve Wiresharku nebo v terminálových výpisech).
- Pomocí Wiresharku je zachycena komunikace identifikující průběh autentizace klienta (pakety EAP, případně RADIUS zprávy Access-Request a Access-Accept).
- Výsledkem procesu je úspěšná autentizace klienta (logy potvrzují úspěšný EAP *handshake* mezi klientem a RADIUS serverem).

## 2.1. Řešení samostatné úlohy

V rámci samostatné úlohy mají studenti za úkol implementovat použití autentizační metody EAP-TTLS a vícefaktorové autentizace klienta s využitím kombinace hesla a certifikátu. Pro konfiguraci autentizace založené na použití certifikátu bude nutné, aby studenti vytvořili na RADIUS serveru vlastní certifikační autoritu a následně vygenerovali dvojici certifikátů:

- certifikát pro autentizační server (resp. pro FreeRADIUS),
- certifikát klienta.

Následně vhodnou změnou konfigurace na serveru i klientovi definují použití autentizační metody EAP-TTLS, přičemž je důležité dbát na správné použití vygenerovaných certifikátů. Studenti rovněž musí zajistit přenos certifikátů a soukromého klíče klienta na jeho zařízení (například pomocí scp).

Pokud je `wpa_supplicant` nakonfigurován správně, bude úspěšné připojení indikováno zprávou: **"CTRL-EVENT-CONNECTED"**. Ve Wiresharku bude správně zachycena komunikace, ve které bude možné sledovat zprávy protokolu TLS přenášené vytvořeným šifrovaným tunelem.

## 2.2. Odpovědi na kontrolní otázky

1. Která tvrzení správně popisují fungování autentizačního mechanismu podle IEEE 802.1X?
  - A) Ověření identity probíhá ještě před přidělením IP adresy klientovi ☒
  - B) IEEE 802.1X je vhodný pouze pro bezdrátové sítě
  - C) Komunikace mezi klientem a přístupovým bodem probíhá přes EAPoL ☒
  - D) IEEE 802.1X zajišťuje šifrování přenosu autentizačních údajů
2. Která z následujících výroků platí o úloze přístupového bodu (*authenticator*) v architektuře IEEE 802.1X?
  - A) Posuzuje platnost přihlašovacích údajů a vydává rozhodnutí o přístupu
  - B) Vystupuje jako zprostředkovatel komunikace mezi klientem a autentizačním RADIUS serverem ☒
  - C) S klientem komunikuje prostřednictvím protokolu EAPoL ☒
  - D) Generuje přístupová hesla pro klienty v lokální síti
3. Vyberte nesprávná tvrzení o protokolu RADIUS:
  - A) Komunikace mezi klientem a RADIUS serverem probíhá prostřednictvím transportního protokolu UDP na portu 1812
  - B) RADIUS šifruje celé pakety pomocí TLS ☒
  - C) RADIUS umožňuje centralizované ověření identity
  - D) RADIUS přenáší EAPoL zprávy jako součást autentizačních požadavků ☒

4. Které typy EAP metod využívají digitální certifikáty?
- A) EAP-TLS ☒
  - B) EAP-MD5
  - C) EAP-PEAP
  - D) EAP-TTLS ☒
5. Která tvrzení o nástroji FreeRADIUS jsou pravdivá?
- A) Podporuje různé autentizační metody, včetně EAP ☒
  - B) Podporuje použití pouze jedné autentizační metody v jednom okamžiku
  - C) Může být konfigurován pro práci s TLS ☒
  - D) Nepodporuje použití autentizační metody EAP-MD5
6. Jaké informace jsou přenášeny ve zprávě *Access-Request* protokolu RADIUS?
- A) Uživatelské jméno (User-Name) ☒
  - B) Hash hesla nebo autentizační token ☒
  - C) ID a heslo uživatele (klienta)
  - D) IP a MAC adresa klienta
7. Jaký příkaz v Kali Linux slouží ke spuštění služby FreeRADIUS??
- A) sudo start radiusd
  - B) sudo systemctl start freeradius ☒
  - C) radiusctl enable
  - D) freeradius --run
8. Které EAP zprávy jsou typicky součástí autentizačního procesu při ověřování identity pomocí metody EAP-MD5?
- A) Identity Request ☒
  - B) Identity Response ☒
  - C) EAPOL Success/Failure ☒
  - D) Access Request
9. Co je typické pro komunikaci mezi klientem a AP během výměny EAP zpráv?
- A) Komunikace probíhá pomocí protokolu EAPoL ☒
  - B) Pakety jsou přenášeny v ethernetovém rámci na linkové vrstvě ☒
  - C) Veškerá komunikace je šifrována pomocí TLS
  - D) Klient komunikuje přímo s autentizačním RADIUS serverem
10. Která z následujících tvrzení o EAP over LAN (EAPoL) jsou nepravdivá?
- A) EAPoL se používá pro přenos EAP zpráv přes kabelové nebo bezdrátové LAN sítě
  - B) EAPoL zprávy jsou zapouzdřeny přímo do IP paketů ☒
  - C) EAPoL zajišťuje komunikaci mezi klientem a AP
  - D) EAPoL šifruje všechny EAP zprávy pomocí TLS ☒

## 2.3. Doplnující otázky

Níže uvedené otázky mohou být využity při kontrole výstupů samostatné práce studentů s cílem ověřit, zda skutečně porozuměli řešené problematice v praktické části laboratorní úlohy.

**1. Jaké jsou výhody používání RADIUS serveru ve srovnání s metodami umožňujícími lokální ověření identity přistupujícího uživatele?**

- Centralizované řízení přístupu, možnost správy velkého množství uživatelů, vyšší bezpečnost a jednodušší správa přístupových politik.

**2. Vysvětlete roli protokolu IEEE 802.1X v procesu autentizace.**

- Řídí přístup do sítě na základě ověření identity uživatele pomocí externího autentizačního serveru (např. RADIUS).

**3. Jaké jsou hlavní komponenty v architektuře 802.1X?**

- Klient, resp. žadatel o ověření (*supplicant*), přístupový bod (*authenticator*), autentizační server RADIUS.

**4. Jaké typy autentizačních metod podporuje RADIUS?**

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

**5. Jaká jsou možná bezpečnostní rizika související s používáním protokolů EAP a RADIUS v otevřených sítích? Uveďte příklad opatření, kterými by bylo možné tato rizika zmírnit.**

- Možnost odposlechu probíhající komunikace nebo *spoofingu*, riziko útoků typu MitM, zneužití slabých autentizačních mechanismů. Řešením je používání pokročilých metod pro šifrování komunikace (např. implementace protokolu TLS).

**6. Pomocí jakého příkazu je možné spustit RADIUS server v Kali Linux?**

- `sudo systemctl start freeradius`

**7. Jaké filtry byste použili ve Wiresharku pro zobrazení EAP zpráv?**

- `eap` alebo `radius`.