Základní konfigurace síťových zařízení a analýza síťového provozu programem Wireshark

ISA - Laboratorní cvičení č.1

Vysoké učení technické v Brně

`https://github.com/nesfit/ISA/tree/master/lab1-konfigurace`

Cíl cvičení

- Seznámit se s nástroji pro konfigurací síťového rozhraní a testování komunikace v OS Linux.
- Zachytávat a analyzovat síťový provoz pomocí síťového analyzátoru Wireshark.
- Vytvořit a nakonfigurovat podsíť s adresami IPv4 a IPv6 v OS Linux.

Obecné pokyny

- Vypněte si mobily a uschovejte do tašek. Není dovoleno používat mobily během výuky.
- Do tohoto zadání nic nepište, slouží pro další skupiny. Výsledky zapisujte do protokolu, který na konci odevzdáte cvičícímu.
- Pro práci v laboratoři budeme používat OS Linux — při bootu počítače vyberte volbu F3.
- Přihlašovací jméno/heslo – běžný uživatel: `user/user4lab`, administrátor: `root/root4lab`.
- Přihlaste se do OS jako uživatel `user`. Pokud budete potřebovat oprávnění správce, zadejte v terminálu příkaz `su` (switch user).

Příprava laboratoře

Váš počítač je připojený ethernetovým kabelem do vnitřní sítě, která je oddělena od fakultní sítě. Jméno vašeho počítače je PCxx, kde xx je číslo počítače. Na počítači budete pracovat se síťovým rozhraním *enp2s0*.

1 Zjišťování konfigurace

Základní příkazy pro práci v OS Linux jsou popsány v kapitole 2 laboratorního manuálu, který můžete využívat jako referenční příručku pro laboratorní cvičení.

1. Pomocí příkazu `ip address show` zjistěte nastavení síťového rozhraní `enp2s0` vašeho počítače. Do protokolu zapište MAC adresu, IPv4 adresu, síťovou masku, adresu sítě a broadcastovou adresu na aktivním síťovém rozhraní.
2. Pomocí příkazů `ip route` a `ip neighbour` zobrazte záznamy ze směrovací tabulky a ARP tabulky. Vypište adresu výchozí brány a zjistěte její MAC adresu.

3. Příkaze `ping` otestujte konektivitu k výchozí bráně a následně do Internetu.
4. Vypište implicitní servery DNS ze souboru `/etc/resolv.conf`.
5. Pomocí příkazu `su` se přihlaste jako administrátor. Do souboru `/etc/hosts` přidejte záznam, který provede překlad jména `gw` (gateway) na IP address 10.10.10.1 (viz `man hosts`). Vyzkoušejte překlad příkazem `ping gw`. Vytvořený záznam zapište do protokolu.
6. Pomocí příkaz `ss -tun` vypište seznam aktivních TCP spojení. Ze seznamu vyberte jeden záznam a zapište ho s vysvětlením do protokolu (popište význam jednotlivých položek). Pokud je seznam TCP spojení prázdný, otevřete si například prohlížeč a načtěte libovolnou webovou stránku.
7. Jako administrátor zobrazte systémové události pomocí programu `journalctl`. Vyhledejte informace týkající se služby NetworManager (`journalctl -u NetworkManager`).
8. Pokuste se jako uživatel user spustit Wireshark pomocí příkazu `sudo wireshark`. Pomocí nástroje `journalctl` vyhledejte v logu zprávu, která tam byla při chybě zaznamenána. Využijte například parametr `-p` pro filtrování chyb s vyšší prioritou. Příkaz pro vyhledání zapište do protokolu.

2 Wireshark

V této úloze budeme pracovat s programem Wireshark. Spusťte aplikaci Wireshark z příkazového řádku příkazem `wireshark` pod uživatelem `root`. Další informace k práci s programem Wireshark najdete v kapitole 3 laboratorního manuálu.

1. Nastavte v programu Wireshark vstupní filtr (tzv. *capture filter*) pro zachytávání provozu HTTP. Uvažujte komunikaci HTTP na standardním portu (viz `/etc/services`). Zapište použitý filtr do protokolu.
2. Spusťte zachytávání síťového provozu v programu Wireshark.
3. Ve webovém prohlížeči si otevřete stránku `http://cphoto.fit.vutbr.cz`.
4. Ukončete zachytávání síťového provozu ve Wiresharku.
5. Vypište zdrojovou a cílovou IPv4 adresu a MAC adresu zachycené komunikace[1]. Vysvětlete, jaký typ síťového zařízení či aplikace daná adresa popisuje.
6. Klikněte pravým tlačítkem na libovolný paket komunikace a zobrazte komunikaci TCP (volba *Follow TCP stream*) a HTTP (volba *Follow HTTP stream*). Popište do protokolu, v čem se liší zobrazená data.
7. Zrušte filtr pro zachytávání provozu.
8. Spusťte znovu zachytávání síťové komunikace bez použití vstupního filtru.
9. Pomocí příkaz `ip neighbour flush dev enp2s0` (spusťte jako `root`) odstraňte ARP záznamy z tabulky ARP. Pomocí příkazu `ping` vygenerujte ICMP na libovolný server.
10. V aplikaci Wireshark nastavte filtr zobrazení (`display filter`) tak, abyste zobrazili pouze komunikaci ARP a ICMP. Zapište, jaký filtr jste nastavili.
11. Ve Wiresharku nastavte filtrování provozu HTTP, HTTPS a DNS na standardních portech. Otevřete ve webovém prohlížeči několik stránek na různých adresách URL. Sledujte návaznost komunikace DNS a HTTP(S) v odchyceném provozu. Vysvětlete, jak spolu souvisí.

[1] Komunikaci OCSP můžete ignorovat. Slouží k ověřování certifikátů.

3 Konfigurace IPv4 a IPv6 (práce ve skupinách)

V poslední úloze budeme manuálně konfigurovat adresu IPv4 a IPv6. Podrobnosti ke konfiguraci můžete najít v části 1.1, 1.2 a 4 laboratorního manuálu. Pro řešení vytvořte dvojici či trojici se svými sousedy.

3.1 Výběr IPv4 a IPv6 adres

1. Jako adresu sítě IPv4 použijte `192.168.N.0`, kde N je číslo jednoho počítače z vaší skupiny.
2. Zvolte nejmenší možný prefix IPv4 sítě, který umožňuje adresovat až sto koncových stanic.
3. Každému členu skupiny přiřaďte jednu IPv4 adresu ze zadaného adresního prostoru IPv4.
4. Pro vytváření podsítě IPv6 využijeme privátní lokální adresy IPv6 ULA (Unicast Local Address). IPv6 adresa se skládá z 64bitové adresy sítě (tzv. prefix IPv6) a z 64bitového identifikátoru rozhraní (Interface ID). Prefix IPv6 u adresy ULA tvoří 7bitový prefix ULA se standardní hodnotou `fc00::/7`, jednobitový příznak lokální adresy, 40bitový unikátní globální identifikátor (Global ID) a 16bitovou hodnotu podsítě v dané síti. Unikátní prefix pro svou lokální podsíť IPv6 si můžete vygenerujte na webové stránce `https://cd34.com/rfc4193/`. Nezapomeňte, že IPv6 prefix má 64 bitů.
5. Každému členu vaší skupiny přidělte jednu adresu s vygenerovaným prefixem IPv6, např. `prefix ::1/64`, `prefix::2/64` apod. Druhou část adresy IPv6 (Interface ID) si můžete zvolit libovolně.
6. Vytvořené adresy zapište do protokolu. Uveďte také, kolik může být maximálně síťových zařízení v dané podsíti.

3.2 Manuální konfigurace IPv4 a IPv6

1. Na svém počítači klikněte vpravo nahoře v GUI na ikonu sítě. Zvolte připojení Ethernet a položku nastavení. Klikněte na konfiguraci připojení. Na záložkách IPv4 a IPv6 manuálně vyplňte přidělené adresy a prefixy. Konfiguraci uložte.
2. Manuálně vypněte (off) a zapněte (on) síťové rozhraní, aby se adresy aktivovaly.
3. Vypište nakonfigurované adresy na příkazovém řádku příkazem `ip address show`.
4. Ověřte komunikaci IPv4 a IPv6 mezi všem počítači skupiny pomocí příkazů `ping` a `ping6`.
5. Předveďte vyučujícímu funkční komunikaci IPv4 a IPv6 se svými sousedy.

4 Ukončení práce v laboratoři

Po ukončení všech úkolů a zapsání výsledku do protokolu ukažte výsledné nastavení vyučujícímu. Poté spusťte jako uživatel `root` skript `/root/isa1/clean`, který smaže vaše nastavení a vypne počítač.