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`

Cíle cvičení

- Seznámit se s konfigurací síťového rozhraní v OS Linux.
- Seznámit se s nástroji pro zjišťování konfigurace zařízení.
- Zachytávat a analyzovat síťový provoz pomocí síťového analyzátoru Wireshark.
- Manuálně nastavit síťovou konfiguraci IPv4 a IPv6 v OS Linux.

Pokyny

- Do tohoto zadání, prosím, nepište, slouží pro další skupiny. Výsledky zapisujte do protokolu, který na konci cvičení odevzdáte cvičícímu.
- Pro práci v laboratoři budeme používat OS Linux, při bootu vyberte volbu F3.
- Přihlašovací jméno/heslo – běžný uživatel: `user/user4lab`, administrátor: `root/root4lab`.
- Přihlaste se do OS vždy jako uživatel `user`. Pokud budete potřebovat oprávnění správce, využijte příkaz `su` (super user).

Příprava laboratoře

Váš počítač je připojený 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 3 laboratorního manuálu. Tato kapitola obsahuje podrobný popis příkazů, které budeme používat v této úloze.

1. Pomocí příkazu `ip address show` vypište konfiguraci vašeho stroje. Vypište MAC adresu, IPv4 adresu, síťovou masku, adresu sítě a broadcastovou adresu.
2. Pomocí příkazů `ip route` a `ip neighbour` zobrazte záznamy ve směrovací tabulce a ARP tabulce. 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 přihlašte 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`.

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 zaznamenána.

2 Wireshark

V této úloze budeme pracovat s programem Wireshark. Spusťte aplikaci Wireshark s příkazového řádku příkazem `wireshark` pod uživatelem `root`. Další informace k práci s programem Wireshark najdete v kapitole 4 laboratorního manuálu.

1. Nastavte v programu Wireshark vstupní filter pro zachytávání provozu HTTP (tzv. *capture filter*). Uvažujte komunikaci HTTP na standardním portu (viz `/etc/services`). Zapište použitý filter 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.

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 formát zobrazených dat.

7. Zrušte filter pro zachytávání provozu.

8. Spusťte znovu zachytávání síťové komunikace bez použití vstupního filtru. V příkazové řádce odstraňte ARP záznamy pomocí příkazu `ip neighbor flush dev enp2s0`. Vygenerujte ICMP komunikaci pomocí příkazu `ping`.

9. Nastavte filter zobrazení (`display filter`) v aplikaci Wireshark tak, abyste zobrazili pouze komunikaci ARP a ICMP. Zapište, jaký filter jste nastavili.

10. Ve Wiresharku nastavte filtrování provozu HTTP, HTTPS a DNS na standardních portech. Otevřte 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, 2 a 5 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 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 64-bitové adresy sítě (tzv. IPv6 prefix) a z 64-bitového identifikátoru rozhraní (Interface ID). IPv6 prefix adresy ULA tvoří tzv. prefix ULA se standardní hodnotou `fc00::/7` a unikátní globální identifikátor (Global ID). Tento identifikátor si pro svou lokální podsíť IPv6 vygenerujte na webové stránce `https://cd34.com/rfc4193/`.
5. Každému členu vaší skupiny přidělte jednu adresu s vygenerovaným prefixem IPv6, např. `prefix::1/64`, `prefix::2/64` apod.
6. Vytvořené adresy zapište do protokolu.

3.2 Manuální konfigurace IPv4 a IPv6

1. Na svém počítači klikněte na ikonu sítě vpravo nahoře v GUI CentOS. Vyberte 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) dané síťové rozhraní tak, aby se adresa aktivovala.
3. Ověřte komunikaci příkazem `ping` a `ping6` mezi všemi počítači skupiny.

4 Ukončení práce v laboratoři

Jakmile máte veškerou práci hotovou, ohlaste se u vyučujícího, který konfiguraci zkontroluje. Poté spuťte jako uživatel `root` skript `/root/isa1/clean`, který smaže vaše nastavení a vypne počítač.