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/wireshark_ip_konfigurace_online`

Cíle cvičení

- Seznámení se se základní prací v OS Linux.
- Seznámení se se základními nástroji pro zjišťování konfigurace zařízení.
- Analýza síťového provozu pomocí programu Wireshark.
- Seznámení se s manuální konfigurací IPv4 a IPv6 na OS Linux.

Pokyny

- Pro práci v cvičení budeme používat virtuální stroje v programu VirtualBox[1].
- Odpovědi pište do odpovědního archu `protokol.md` který odevzdáte do WIS-u. Dostupný je na adrese `https://github.com/nesfit/ISA/blob/master/wireshark_ip_konfigurace_online/protokol.md`.
- Do WIS-u budete také odevzdávat všechny zachycené `pcap` soubory.
- Uživatelé a hesla pro přihlášení: `user - user4lab`, `root - root4lab`.
- Přihlaste se jako uživatel `user`. Veškeré potřebné příkazy následně spouštějte jako `root`.

Příprava laboratoře

Importujte stroj `ISA2020.ova` do programu VirtualBox. Při importu nastavte generaci nových MAC adres pro síťová rozhraní (MAC Address Policy: **Generate new MAC addresses for all network adapters**). Ve virtuálním stroji budete pracovat s rozhraním **enp0s3**.

Instalace Guest Additions

Tento krok je volitelný.

Pro pohodlnější práci s virtuálním strojem je možno nainstalovat vlastní verzi VirtualBox Guest Additions (doporučený virtuální stroj může obsahovat verzi nekompatibilní s vaší verzí VirtualBoxu). V menu VirtualBox zvolte *Devices* → *Insert Guest Additions CD image...* a spusťte instalaci tlačítkem *Run*. Po zadání hesla uživatele `root` by měla proběhnout instalace; po jejím ukončení restartujte virtuální stroj.

[1] `http://nes.fit.vutbr.cz/isa/ISA2020.ova`

Vytvoření snapshotu

Před zahájením cvičení si vytvořte snapshot za pomoci menu *Machine* → *Take snapshot* pro snadný návrat k výchozímu stavu. Následující cvičení budete řešit ve stejném virtuálním počítači, budeme očekávat, že použijete výchozí stav s volitelně nainstalovanými *Guest Additions*.

1 Zjišťování konfigurace

V případě, že se v OS Linux úplně neorientujete, přečtěte si kapitolu 3 v laboratorním manuálu — Základní konfigurace linuxového serveru. V této části cvičení se budeme zabývat převážně zjišťováním síťové konfigurace systému. Veškeré potřebné informace, které budete potřebovat ke splnění této části cvičení, naleznete v sekci 3.3 laboratorního manuálu — Konfigurace síťových zařízení. V případě, že si nejste jistí některým příkazem, neváhejte nahlédnout do manuálové stránky.

1. Vypište konfiguraci vašeho stroje (MAC adresu, IPv4 adresu, masku, síť, broadcastovou adresu).
2. Zobrazte si záznamy v routovací a ARP tabulce. Zapište IPv4 adresu výchozí brány a přiřaďte k ní MAC adresu.
3. Otestujte konektivitu k výchozí bráně a následně konektivitu do Internetu.
4. Vypište implicitní servery DNS a název souboru, ve kterém jste tuto informaci nalezli.
5. Upravte patřičný soubor tak, aby po spuštění příkazu `ping gw`, byl ping proveden vůči IPv4 adrese výchozí brány. Zapište jak a který soubor jste upravili a jaký záznam jste přidali.
6. Vypište aktivní TCP spojení, vyberte jeden záznam, zapište si ho a popište význam jednotlivých položek. Pokud se žádné TCP spojení nezobrazuje, nějaké vygenerujte, například pomocí webového prohlížeče.
7. Zobrazte systémové události pomocí programu `journalctl`.
8. Zobrazte pouze události týkající se NetworkManager.
9. Pokuste se jako uživatel user spustit Wireshark s pomocí programu `sudo`. Následně nalezněte v logu zprávu, která byla zaznamenána v případě správně zadaného hesla, ale odepřeného přístupu.

2 Wireshark

V této části cvičení se budeme zabývat analýzou a zachytáváním provozu v programu Wireshark. Spuštění Wireshark provedete příkazem `wireshark` pod uživatelem `root`. Veškeré potřebné informace, které budete potřebovat k této části cvičení, naleznete v kapitole 4 laboratorního manuálu — Analýza síťového provozu programem Wireshark.

1. Pomocí programu Wireshark začněte **zachytávat** pouze HTTP komunikaci na výchozím portě (výchozí porty je možné nalézt např. v `/etc/services`). Zapište použitý *capture filter* do odpovědního archu. Spusťte si prohlížeč a načtěte stránku `http://cphoto.fit.vutbr.cz` (po zapnutí zachytávání provozu). Zachycený provoz uložte do souboru `cv1-http.pcap` který budete odevzdávat.
2. Vypište zdrojovou a cílovou IPv4 adresu a MAC adresu odeslaného a přijatého paketu. Zamyslete se nad tím, co vypsané MAC adresy a IPv4 adresy identifikují — nalezené identifikátory porovnejte s identifikátory vypsanými v předchozích bodech zadání.

3. Zahajte znovu zachytávání komunikace, nyní bez použití filtru pro HTTP. V příkazové řádce odstraňte ARP záznamy (příkaz `ip neighbor ...`). Ve wiresharku zobrazte veškerou komunikaci, následně vyfiltrujte pouze ARP a ICMP pakety. Vygenerujte ICMP komunikaci. Analyzujte obsah ARP paketů. Zapište, co jste zadali do filtru. Zachycený provoz uložte do souboru `cv1-arp.pcap` který budete odevzdávat.

4. Zachyťte pouze HTTP a DNS provoz (na výchozích portech). Ve webovém prohlížeči zkuste otevřít několik stránek na různých URL adresách. Analyzujte obsah a posloupnost DNS paketů a následných HTTP paketů. Zachycený provoz uložte do souboru `cv1-dns.pcap` který budete odevzdávat.

5. Znovu si otevřete dříve uložený soubor s nešifrovanou komunikaci pomocí HTTP (`cv1-http.pcap`), zobrazte si TCP stream této komunikace (*Follow TCP stream*). Najděte dotaz, který odpovídá stránce zobrazené v prohlížeči. Pokuste se zachytit šifrovanou komunikaci HTTPS na libovolnou stránku, analyzujte zachycenou komunikaci, zaměřte se také na provoz DNS; využijte funkci *Follow TCP stream*.

6. Do odpovědního archu slovně popište význam funkce *Follow TCP stream*, zamyslete se nad formátem zobrazených dat funkcí *Follow TCP stream* a rozdílem oproti výchozímu pohledu na data ve formě paketů.

3 Konfigurace IPv4 a IPv6

Příprava virtuálních strojů

Vypňete virtuální stroj. V nastavení stroje zapňete druhé síťové rozhraní (*Network* → *Adapter 2*) a nastavte jej do módu *Internal Network* s názvem `isa`. Naklonujte stroj a opět nastavte generaci nových MAC adres. Použijte *Linked clone*. Nastartujte oba stroje a na jedném z nich spusťe záchyt na rozhraní `enp0s8`.

3.1 Manuální konfigurace IPv4

Teorie *IPv4 adresování* je popsaná v sekci 1 laboratorního manuálu — Adresy v IPv4 síti. Možnosti manuální konfigurace IP adres jsou v sekci 5 — Konfigurace síťování koncových zařízení.

1. Zvolte nejdelší možnou masku sítě `192.168.0.0` tak, aby síť obsahovala prostor pro 100 koncových stanic.

2. Jako adresu sítě použijte `192.168.0.0`. Na obou strojích nastavte libovolné adresy z dané síťe na novém rozhraní `enp0s8`.

3. Správnou konfiguraci si ověřte příkazem `ping`.

3.2 Manuální konfigurace IPv6

Teorie *IPv6 adresování* je popsaná v sekci 2 — Adresy v IPv6 síti. Možnosti manuální konfigurace IP adres jsou stejné jako pro IPv4.

1. Zvolte si adresu sítě vhodnou pro použití v privátních lokálních sítích, s prefixem délky 64 bitů. Prvních 48 bitů zvolte podle popisu v sekci 2, pro vygenerování unikátního Global ID můžete použít web `https://cd34.com/rfc4193/`, zbývajících 16 bitů (Subnet ID) si můžete zvolit libovolně.

2. Pro zajímavost si můžete unikátnost vygenerovaného Global ID zkontrolovat na `https://www.sixxs.net/tools/grh/ula/list`.
3. Na obou strojích nastavte libovolné adresy z dané síťe na novém rozhraní `enp0s8`.
4. Správnou konfiguraci si ověřte příkazem `ping6`.

Uložení zachycené komunikace

Uložte zachycenou komunikaci `ping` a `ping6` do souboru `cv1-ping.pcap`.

Odevzdávané soubory

Zkontrolujte, zda máte všechny soubory které se budou odevzdávat:

- `protokol.md`
- `cv1-http.pcap`
- `cv1-arp.pcap`
- `cv1-dns.pcap`
- `cv1-ping.pcap`

4 Ukončení cvičení

Do WIS-u odevzdejte vyplněný `protokol.md` a všechny zachycené `pcap` soubory. Vypňete virtuální stroje a obnovte snapshot ze začátku.