ISA - Laboratorní cvičení č.3

Správa sítě

připravili Matěj Grégr, Martin Žádník a Libor Polčák*

Zimní semestr 2010/2011, verze 1.2

Cíl laboratorního cvičení

- seznámit se s nástroji pro správu sítě
- naučit se pracovat s programem syslog
- konfigurace nástrojů pro práci s protokolem SNMP
- otestovat práci se syslog a SNMP
- seznámit se s protokolem NetFlow
- naučit se pracovat s nástroji `nfsen` a `nfdump`

Pokyny

- Do zadání nepište, slouží pro další skupiny. PDF verzi zadání i šablony konfiguračních souborů lze najít v IS u předmětu ISA.
- Na konci laboratorního cvičení nezapomeňte na poslední bod, tj. na **Ukončení práce v laboratoři**!

Průběžný test č.2

Vstupní test - 10 minut, maximálně 9 bodů. Při řešení není povoleno používat žádné pomůcky (poznámky, kalkulačku apod.), spuštět jiné aplikace než WWW prohlížeč, komunikovat se sousedem, připojovat se na jinou než zadanou IP adresu. V případě porušení pravidel je test hodnocen 0 body.

1. Spusťte počítač v systému FreeBSD
2. Po přihlášení (login `user`, heslo `user4lab`) spusťte systém XWindow (příkaz `startx`).
3. Spusťte WWW prohlížeč a přihlašte se na adresu `www.vutbr.cz/elearning`.
4. Vyberte předmět ISA a průběžný test č.2 podle pokynů vyučujícího.
5. Zadejte heslo pro přístup k testu a spusťte test.
6. Po ukončení testu vyčkejte v tichosti, než ostatní dokončí test.
7. Podrobné výsledky testu se dozvíte, až test dokončí všichni studenti ve skupině.

*FIT VUT v Brně, {igregr,izadnik,ipolcak}@fit.vutbr.cz

1 Syslog

- Úkol:
  - Seznámit se s protokolem Syslog, který slouží pro přenos logovacích zpráv ze spravovaných zařízení. Pojmem Syslog je často označováno také programové vybavení implementující samotný přenos, třídění a ukládání zpráv na disk.
  - Rozdělte se do dvojic. V každé dvojici zvolte jednu stanici jako klient a druhou jako server a nakonfigurujte přeposílání veškerých Syslog zpráv z klienta na server. Mějte na paměti možné zneužití Syslog protokolu útočníkem a omezte na straně serveru příjem pouze na zprávy od daného klienta a klientovi zamezte příjem jakýchkoliv zpráv ze sítě.
  - Pro práci využijte nástroj `syslogd`, který bude sloužit jako server i klient. K otestování využijte nástroj `logger`.
  - Na klientovi následně omezte přeposílání pouze na zprávy konkrétního typu.
- Příkazy:
  - `syslogd(8)` – Syslog démon.
  - `syslog.conf(5)` – Popis konfigurace Syslog démona.
  - `logger(1)` – Nástroj pro generování Syslog zpráv.
  - `tcpdump(1)`
- Postup:
  1. Rozdělte se do dvojic a určete server a klient stanici.
  2. Povolte spuštění Syslogd démona na serveru i klientovi, tj. přidejte následující řádek do `/etc/rc.conf`:

     ```
     syslogd_enable="YES"
     ```
  3. **Na serveru** omezte příjem Syslog zpráv pouze od konkrétního klienta, tj. přidejte do `/etc/rc.conf`:

     ```
     syslogd_flags="-a <plne_domenove_jmeno_klienta> -vv"
     ```
  4. **Na serveru** nakonfigurujte syslog démona tak, aby ukládal veškeré zprávy od klienta do souboru `/var/log/logclient.log`. Při editaci souboru `/etc/syslog.conf` použijte jako oddělovač výhradně tabulátor nikoliv mezeru. Na začátek souboru `/etc/syslog.conf` přidejte následující pravidlo a oddělte ho od zbytku pravidel prázdným řádkem:

     ```
     +<plne_domenove_jmeno_klienta>
     *.*<TAB><TAB><TAB>/var/log/logclient.log
     ```
  5. **Na serveru** je nutné vytvořit soubor pro logování, v opačném případě by Syslog démon do souboru nezapisoval:

     ```
     touch /var/log/logclient.log
     ```
  6. **Na klientovi** zakažte programu syslogd naslouchat na síťovém soketu, tj. přidejte do `/etc/rc.conf`:

     ```
     syslogd_flags="-s -vv"
     ```
  7. **Na klientovi** nakonfigurujte Syslog démona tak, aby odesílal veškeré zprávy z klienta na server. Jako oddělovač použijte výhradně tabulátor nikoliv mezery. Do souboru `/etc/syslog.conf` přidejte následující pravidlo:

     ```
     *.*<TAB><TAB><TAB>@<plne_domenove_jmeno_serveru>
     ```

8. **Na serveru i klientovi** restartujte Syslog démona:

   ```
   /etc/rc.d/syslogd restart
   ```

9. **Z klienta** ověřte správnou konfiguraci vygenerováním testovací Syslog zprávy pomocí nástroje `logger`:

   ```
   logger "Toto je testovaci zprava z klienta"
   ```

10. Zpráva byla přeposlána na server, kde ji lze najít na konci souboru `/var/log/logclient.log`.

    ```
    tail -f /var/log/logclient.log
    ```

11. Na klientovi pokračujte v generování Syslog zpráv a na serveru sledujte příchozí Syslog zprávy pomocí `tcpdump`. Na jakém portu a jakým protokolem jsou Syslog zprávy zasílány. Dále vysvětlete, co znamená zvýšený výskyt DNS komunikace po každém příchodu Syslog paketu [1].

12. Otevřete si manuálovou stránku syslog.conf a zjistěte, jaké zařízení a priority zpráv Syslog poskytuje.

    ```
    man syslog.conf
    ```

13. Ze znalosti zařízení a priorit nakonfigurujte klienta, aby posílal na server pouze zprávy při selhání autentizace, tj. upravte již existující pravidlo pro přeposílání veškerých zpráv na server v souboru `/etc/syslog.conf`. Nezapomeňte restartovat Syslog démona.

    ```
    Syntax pravidel: <facility>.<priority><TAB><TAB><TAB><action>
    ```

14. Ze serveru se následně pokuste o neúspěšné ssh připojení na klienta a podívejte se do souboru `/var/log/logclient.log` jakou zprávu zaslal klient serveru.

[1] Jedná se o překlad zdrojové IP adresy Syslog paketu na doménové jméno, aby bylo možné ověřit shodu jmen povolených klientů

2 SNMP

- Úkol:
  - Seznámit se s protokolem SNMP, který slouží pro přenos informací o stavu spravovaných zařízení (např. hodnot čítačů). Během tohoto cvičení si vyzkoušíte práci se synchronními SNMP událostmi, tj. model komunikace dotaz-odpověď.
  - Každou stanici nakonfigurujte tak, aby lokálně umožňovala čtení i zápis SNMP proměnných a při vzdáleném přístupu k SNMP proměnným pouze čtení.
- Příkazy:
  - `snmpd(8)` – SNMP démon.
  - `snmpd.conf(5)` – Popis konfigurace SNMP démona.
  - `snmpwalk(1)` – Nástroj pro procházení a získávání podstromu hodnot SNMP proměnných.
  - `snmpget(1)` – Nástroj pro získání hodnoty SNMP proměnné.
  - `snmpset(1)` – Nástroj pro změnu hodnoty SNMP proměnné.
- Postup:
  1. Povolte spuštění SNMP démona, tj. přidejte následující řádek do `/etc/rc.conf`:

     ```
     snmpd_enable="YES"
     ```

  2. Zkopírujte soubor `/usr/local/share/snmp/snmpd.conf.example` obsahující příklad konfigurace SNMP démona do `/usr/local/etc/snmp/snmpd.conf`.
  3. Otevřete si soubor `/usr/local/etc/snmp/snmpd.conf` pro editaci a postupně v něm proveďte základní konfiguraci:
     (a) Zvolte si vlastní název komunity - např. PUBLIC
     (b) Nastavte agenta, aby poslouchal na všech lokálních adresách `agentAddress udp:0.0.0.0:161`
     (c) Namapujte sítě, ze kterých bude možné přistupovat k SNMP hodnotám. Povolte počítačům v učebně zápis pro čtení `rocommunity <CUMMUNITY> 10.10.10.0/24` a lokálnímu počítači i zápis `rwcommunity <CUMMUNITY> localhost`
     (d) V konfiguračním souboru ještě nastavte SNMP proměnné `syslocation` a `syscontact` na Vámi vymyšlené hodnoty.
  4. Spusťte démona `snmpd`.

     ```
     /usr/local/etc/rc.d/snmpd start
     ```

  5. Ověřte, že démon běží. Na kterých portech naslouchá?

     ```
     /usr/local/etc/rc.d/snmpd status
     sockstat | grep snmpd
     ps -ax | grep snmpd
     ```

  6. Příkazem `snmpwalk` přečtěte podstrom `system` a zjistěte jak váš soused nastavil proměnné `sysLocation` a `sysContact`. Např.:

     ```
     snmpwalk -v 1 -c PUBLIC h01 system
     snmpwalk -v 1 -c <nazev_komunity> <domenove_jmeno> system
     snmpwalk -v 1 -c <nazev_komunity> <domenove_jmeno> system.sysLocation
     snmpwalk -v 1 -c <nazev_komunity> <domenove_jmeno> system.sysContact
     ```

7. Pokud znáte OID (Object Identifier) proměnné v databázi MIB (Management Information Base), pak můžete získat hodnotu této proměnné přímo pomocí `snmpget`, např. počet bytů přijatých na rozhraní em0:

```
snmpwalk -v 1 -c <nazev_komunity> \
         <domenove_jmeno_souseda> .1.3.6.1.2.1.2.2.1.16
snmpget -v 1 -c <nazev_komunity> \
         <domenove_jmeno_souseda> .1.3.6.1.2.1.2.2.1.16.1
```

8. Zjistěte další informace, například nastavenou MAC adresu (ifPhysAddress) na počítači Vašeho souseda. Pro získání potřebného OID využijte webové rozhraní Network management MIB nacházející se zde:

```
http://www.oidview.com/mibs/0/RFC1213-MIB.html
```

9. Zkuste nastavit svému sousedovi proměnnou popisující název jeho počítače pomocí nástroje `snmpset`:

```
snmpget -v 1 -c <nazev_komunity> <domenove_jmeno_souseda> system.sysName.0
snmpset -v 1 -c <nazev_komunity> <domenove_jmeno_souseda> \
        system.sysName.0 s <nove_jmeno>
```

10. Proč předchozí pokus o nastavení proměnné sousedovi selhal? Zkuste nyní nastavit svoji proměnnou popisující název Vašeho počítače pomocí nástroje `snmpset`:

```
snmpget -v 1 -c <nazev_komunity> localhost system.sysName.0
snmpset -v 1 -c <nazev_komunity> \
        localhost system.sysName.0 s <nove_jmeno_pocitace>
snmpget -v 1 -c <nazev_komunity> localhost system.sysName.0
```

3 NetFlow

- Úkol:
  - Seznámit se možnostmi měření provozu pomocí NetFlow. NetFlow slouží pro přenos statistik o jednotlivých tocích dat vznikajících při komunikaci po síti. Záznamy NetFlow, s nimiž budete během cvičení pracovat, jsou pořízeny z napojení sítě VUT a anonymizovány. V druhé části úkolu budete pracovat s daty pořízenými sondou FlowMon, která monitoruje dění v síti společností INVEA-TECH.
  - Seznámit se s nástrojem `nfsen`, který graficky zobrazuje záznamy NetFlow ve webovém prohlížeči. Seznámit se s nástrojem `nfdump`, který slouží k dotazování na uložená data NetFlow.
- Příkazy:
  - `nfdump`
- Postup:
  1. Naučte se používat nástroj `nfdump`, který slouží k dotazovaní se nad záznamy NetFlow.
     (a) Na Vašem počítači se v adresáři `/home/user/isa3/netflow` nachází [2] anonymizovaná kolekce NetFlow dat. Tento adresář bude vstupem programu `nfdump`, který využijte ke kladení dotazů nad NetFlow daty.
     (b) Prostudujte manuálovou stránku nástroje `nfdump`.
     (c) Dotažte se na následující statistiky. TOP 20 IP adres podle počtu přenesených bajtů.
        - V manuálové stránce si najděte, co dělají přepínače `-R , -s, -n`.
        - Nezapomeňte, že zpracováváte několik souborů o celkové velikosti 600 MB, tedy vytvoření statistiky chvíli potrvá!
     (d) Zjistěte, jak velké datové přenosy připadají na jednotlivé protokoly. (Statistika protokolů)
        - Všimněte si rozdílů v podílech podle toků a podle přenesených bajtů.
     (e) Na základě získaných statistik se zamyslete nad velikostí sítě. [3]
     (f) Zaměřte se na konkrétní stanici v síti, např. `194.179.74.239` a zjistěte, s kým komunikovala, a odhalte podezřelou aktivitu tohoto uživatele. [4]

     ```
     nfdump -R /home/user/isa3/netflow -o long -c 100 \
     "src ip 194.179.74.239"
     ```
  2. Přihlašte se na sondu FlowMon, běžící ve společnosti INVEA TECH
     (a) webová stránka: `https://demo.invea.cz`, kliknout na **FlowMon Monitoring Center**, login: `guest`, heslo: `flowmondemo`. Neměňte žádné nastavení.
     (b) Seznamte se s jednotlivými stránkami, které vytváří program `nfsen`. Zaměřte se na:
        - **Graphs** – poskytuje dlouhodobý pohled na trendy v síťovém provozu
        - **Details** – nabízí detailní pohled na aktuální provoz s možností rozdělení provozu na podle TCP, UDP, ICMP, dále pak možnost dotazovat se na TOP N statistiky nebo filtrovat a agregovat záznamy.
        - **Profile** – Toto menu umožňuje filtrovat a označit barvou specifické druhy provozu identifikované pomocí čísla portu a protokolu.

[2] Není-li tomu tak, adresář vytvořte. Netflow data získejte pomocí příkazů `fetch http://isa2.fit.vutbr.cz/nfcapd-isa.tar` a `tar xvf nfcapd-isa.tar`

[3] Jedná se o anonymizovaná data z páteřní sítě VUT získaná za 1 hodinu provozu od 21 hodin

[4] Příliš mnoho jedno paketových telnet spojení během krátké doby na různé počítače ale stejný port 23 ukazuje na skenovací aktivitu útočníka.

- **Stats** – tato stránka zobrazuje nastavení profilu a umožňuje ho měnit

(c) Úkoly:

- Zjistěte, jaké IM protokoly se v této síti používají.
- Zjistěte, jaké P2P protokoly se v této síti používají.
- Který protokol transportní vrstvy se používá nejčastěji? Jaký má přibližně podíl na celkovém provozu v síti? Jak se tento podíl mění v průběhu dne, týdne? Zamyslete se, proč tomu tak je.

- Pro zájemce:
  - Zájemci si mohou na stránce `https://demo.invea.cz` projít ostatní moduly vystavěné nad protokolem. Neměňte žádné nastavení.

Ukončení práce v laboratoři

- Pod uživatelem `root` spusťte dávku `/root/isa3/isa3` pro zrušení vytvořených konfiguračních souborů a pro vypnutí počítače.