ISA - Laboratorní cvičení č.5

Správa a monitorování sítě

Vysoké učení technické v Brně

`https://github.com/nesfit/ISA/tree/master/management`

Cíl laboratorního cvičení

- seznámit se s nástroji pro správu sítě
- seznámit se s formátem Cisco Netflow pro ukládání statistických dat a nástrojem pro čtení NetFlow **nfdump**
- naučit se pracovat s protokolem Syslog a nástrojem **rsyslog**
- konfiguraci nástrojů pro monitoring **Icinga2**

Pokyny

- Pro vypracování využijte virtualní stroje **cv5-master** a **cv5-provider** dostupné na *https://nes.fit.vutbr.cz/isa/isa-lab-cv5.ova*. Appliance obsahuje oba virtuální stroje.
- Před začátkem vypracování si vytvořte obraz obou virt. strojů pro snadný návrat do výchozího. Je vhodné si tyto obrazy vytvářet i průběžně po splnění části laboratoře. Dále zkontrolujte, zda je na obou strojích aktivní 2. síťové rozhraní a je nastaveno v režimu *Host-only*.
- Na obou strojích smažte pravidla ve firewallu příkazem `iptables --flush`

1 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 ze sítě VUT a anonymizovány. V druhé části úkolu budete pracovat s daty pořízenými sondou FlowMon.
- Příkazy:
  - `nfdump`
- Postup:
  1. Na virt. stroji **cv5-provider** se v adresáři `/home/user/nfdump-data` nachází anonymizovaná kolekce NetFlow dat. Tento adresář bude vstupem programu `nfdump`, který využijte ke kladení dotazů nad NetFlow daty.
  2. Prostudujte manuálovou stránku nástroje `nfdump`.
  3. Dotažte se na TOP 20 IP adres podle počtu přenesených bajtů.
     - V manuálové stránce si najděte, co dělají přepínače `-R, -s, -n, -O`.
     - Nezapomeňte, že zpracovávaná data jsou relativně objemná. Dosažení výsledku tedy chvíli potrvá.
  4. Zjistěte, jak velké datové přenosy připadají na jednotlivé protokoly. (Statistika protokolů)
     - Všimněte si rozdílů v podílech podle toků a podle přenesených bajtů.
  5. Vyfiltrujte si toky se zdrojovou IP *162.35.0.190*. Zaměřte se na čísla portů. Je aktivita zdroje něčím podezřelá?

2 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.
  - Pracujte ve dvojicích, kde jeden bude v roli serveru a druhý v roli klienta.
  - Pro práci využijte nástroj `rsyslogd`, který bude sloužit jako server i klient. K otestování využijte nástroj `logger`.
  - Na klientovi následně omezte přeposílání pouze na zprávy konkrétního typu.
  - Na obou stanicích pracujte jako uživatel root.
- Příkazy:
  - `rsyslogd(8)` – démon pro Syslog.
  - `rsyslog.conf(5)` – Popis konfigurace rsyslog démona.
  - `logger(1)` – Nástroj pro generování Syslog zpráv.
- Postup:
  1. **Na cv5-master** povolte naslouchání na síťovém soketu. Do souboru `/etc/rsyslog.conf` přidejte nebo odkomentujte:

```
$ModLoad imudp
$UDPServerRun 514
```

2. **Na cv5-provider** nakonfigurujte rsyslog démona tak, aby odesílal veškeré zprávy z klienta na serveru pomocí UDP. Jako oddělovač použijte výhradně tabulátor nikoliv mezery. Do souboru `/etc/rsyslog.conf` přidejte následující pravidlo:

```
*.*<TAB>@<ip_adresa_serveru>:<číslo_portu>
```

3. **Na cv5-master i cv5-provider** restartujte Syslog démona:

```
systemctl restart rsyslog
```

4. **Z cv5-provider** ověřte správnou konfiguraci vygenerováním testovací Syslog zprávy pomocí nástroje `logger`:

```
logger -d <obsah_zprávy>
```

5. Zpráva byla přeposlána na cv5-master, kde ji lze najít na konci souboru `/var/log/messages`.

```
tail -f /var/log/messages
```

6. Na cv5-provider pokračujte v generování Syslog zpráv a na serveru sledujte příchozí Syslog zprávy pomocí `wireshark`. Na jakém portu a jakým protokolem jsou Syslog zprávy zasílány?
7. Otevřete si manuálovou stránku `rsyslog.conf` a zjistěte, jaké zařízení a priority zpráv Syslog poskytuje (kapitola **SELECTORS**).

```
man rsyslog.conf
```

8. Nakonfigurujte cv5-provider, aby posílal na server zprávy související s autentizací na úrovni info (je potřeba použít facility `authpriv` místo `auth`), tj. upravte již existující pravidlo pro přeposílání veškerých zpráv na server v souboru `/etc/rsyslog.conf`. Nezapomeňte restartovat Syslog démona.

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

9. Pokuste se o neúspěšné ssh připojení na cv5-provider a podívejte se ve wiresharku, jakou zprávu zaslal cv5-provider serveru. Následně odešlete z cv5-provider zprávu příkazem `logger`. Při správné konfiguraci by se tato zpráva neměla odeslat. Zachycenou komunikaci uložte do souboru `xlogin00-syslog.pcap`.

3 Icinga2

- Úkol:
  - Seznámit se s nástrojem Icinga2 pro monitorováni zařízení a služeb.
  - Na klientské stanici nakonfigurovat kontroly služeb a živosti stanic.
- Postup:
  1. Otevřete si webový prohlížeč v cv5-master a zadejte adresu *http://localhost/icingaweb2*. Dostanete se na webové rozhraní Icingy2. Přihlaste se pod uživatelem **user** a heslem **user4lab**.
  2. Na virt. počítači cv5-master ve složce */etc/icinga2/conf.d* najdete soubor **hosts.conf**. Odkomentujte a doplňte potřebnou konfiguraci, aby systém Icinga2 monitoroval virt. počítač **cv5-provider** a služby **http** a **snmp-free-memory**. Pole `host_name` se musí shodovat s názvem Host objektu.

```
object Host "Provider" {
    address = "<IP ADDRESS>"
    check_command = "hostalive"
}

object Service "http" {
    max_check_attempts = 4
    check_interval = 10m
    retry_interval = 10m
    host_name = "<OBJECT NAME>"
    check_command = "http"
}

object Service "snmp-free-memory" {
    host_name = "<OBJECT NAME>"
    check_command = "snmp"

    vars.snmp_oid = "1.3.6.1.4.1.2021.4.6.0"
}
```

3. Restartujte službu icinga2

   ```
   systemctl restart icinga2
   ```

4. Podívejte se na webové rozhraní Icingy2. Co se tam změnilo? Když je nějaká služba ve stavu **DOWN**, proč tomu tak je?
5. Na klientském počítači **cv5-provider** zapněte webový server.

   ```
   python -m SimpleHTTPServer 80 > /dev/null 2> /dev/null &
   ```

6. Na virt. počítači **cv5-provider** upravte soubor `/etc/snmp/snmpd.conf` tak, aby naslouchal na adrese rozhraní enp0s8 (příkaz `agentAddress`) a doplňte SNMP komunitu, aby se shodovala s isa-icinga-master. Komunita bude read-only a přístup bude povolen pro subnet 192.168.56.0/24. Jako jméno komunity použijte svůj login. Následně doplňte toto jméno do konfigurace Icinga2 do proměnné `vars.snmp_community` ve službě *snmp-free-memory*.

   ```
   Syntax pravidel:
   {ro,rw}community<TAB><community name><TAB><allowed subnet>
   ```

7. Restartujte SNMPD na **cv5-provider**.

   ```
   systemctl restart snmpd
   ```

8. Ve Webovém rozhraní Icingy2 v menu Overview → Services si vyhledejte předešlou kontrolu služby snmp-free-memory a klikněte na odkaz **Check Now**. Pokud jste službu nakonfigurovali správně, měli byste dostat informaci o dostupné paměti.

Ukončení práce v laboratoři

- Do WIS odevzdejte protokol5.pdf a pcap se syslog komunikací.
- Vypněte všechny virtuální počítače. Pro vypnutí můžete použít příkaz File → Close ... a volbu **Power off the machine**. Volbu **Restore current snapshot 'Clean'** ponechte zatrhnutou.