PV210 Bezpečnostní analýza síťového provozu

Jednoduché metody zpracovávající agregované záznamy o síťovém provozu

RNDr. Jan Vykopal, Ph.D.

22. 10. 2014

První domácí úkol: obsah souboru

Řešení prvního domácího úkolu I

- **Pokus o phishing facebook.com** skládající se z podvržení odpovědi ARP (L2) a následně DNS (L5-7).
- Broadcast *Já jsem brána!* na spojové vrstvě každé dvě sekundy.
- V odpovědi na DNS dotaz *Jakou IP adresu má facebook.com?* je adresa z lokální sítě!
- Útočník: IP 10.0.0.6/MAC a2:87:27:27:13:68 (Linux), útok na ARP je od 5 420. paketu v souboru, podvržení odpovědi DNS 52 431.
- Oběť: IP 10.0.0.3/MAC e8:2a:ea:09:34:63 (Windows).
- Byl útok úspěšný? Nejspíš ne.

Řešení prvního domácího úkolu II

- Ukázka řešení.
- Večer před termínem odevzdáno 12 řešení.
- Průměrná doba řešení několik hodin.
- Hodnocení se objeví v Poznámkovém bloku do přednášky 29. 10.

Shrnutí

- Pro bezpečnostní aplikace je výhodné trvalé pasivní monitorování.
- Nasazení SNMP či sběr Syslogu vyžaduje konfigurovat dotčené prvky.
- Analýza síťového provozu je pro uživatele transparentní.
- Prohledávání obsahu paketů je ve vysokorychlostních sítích nemožné.
- Používá se monitorování síťových toků (typicky na síťové až transportní vrstvě), které poskytuje kýženou agregaci a přitom zachovává informační hodnotu (na rozdíl od SNMP).

Síťové toky, zjemnění statistik SNMP

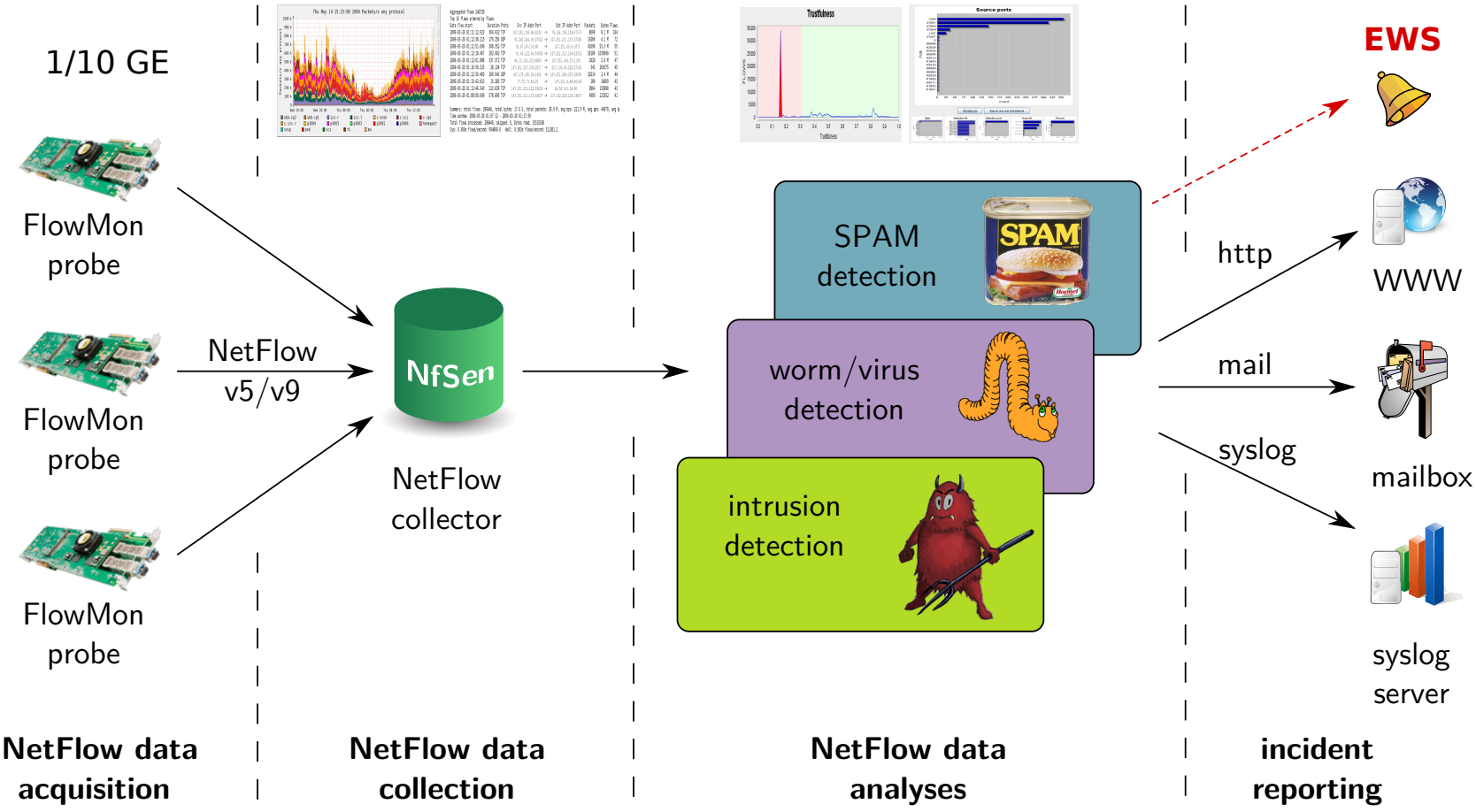
- Lze získat statistiky o počtu přenesených toků, paketů a bajtů – sumární, pro určité podsítě či dokonce jednotlivé stroje.
- Původní využití NetFlow bylo právě pro účtování.
- Tyto statistiky lze ale použít i u „objemově výrazných“ anomálií.
- Stejně jako v ostatních aplikacích je klíčové umístění sondy v infrastruktuře.

Síťové toky


```
Flow start    Duration Proto     Src IP Addr:Port          Dst IP Addr:Port    Flags   Packets  Bytes
09:41:21.763    0.101  TCP      172.16.96.48:15094 ->  209.85.135.147:80      .AP.SF    4       715
09:41:21.893    0.031  TCP    209.85.135.147:80    ->    172.16.96.48:15094  .AP.SF    4       1594
```

Praktická ukázka výstupu nástroje `nfdump` a kolektoru `NfSen`.

Architektura systému



Detekce TCP SYN skenů

- Obecně nás zajímají spíše stroje v naší síti, pod naší správou (ty lze nějak „usměrnit”).
- Skenování portů je typickým projevem šíření červů, často je velmi agresivní (mnoho pokusů za krátký čas).
- Velmi jednoduchou metodou je sledování TCP provozu, konkrétně TCP SYN toků.
- Pokud stroj překročí v daném časovém okně nastavený počet pokusů, je označen za skenera.[1]
- Pozor ale na falešné poplachy způsobené např. navázáním spojení s již vypnutých strojem, klienty P2P sítí (i Skype).
- I když jde o jednoduchou metodu, v praxi je velmi účinná se zanedbatelným počtem falešných poplachů.

[1] Jak to lze obejít?

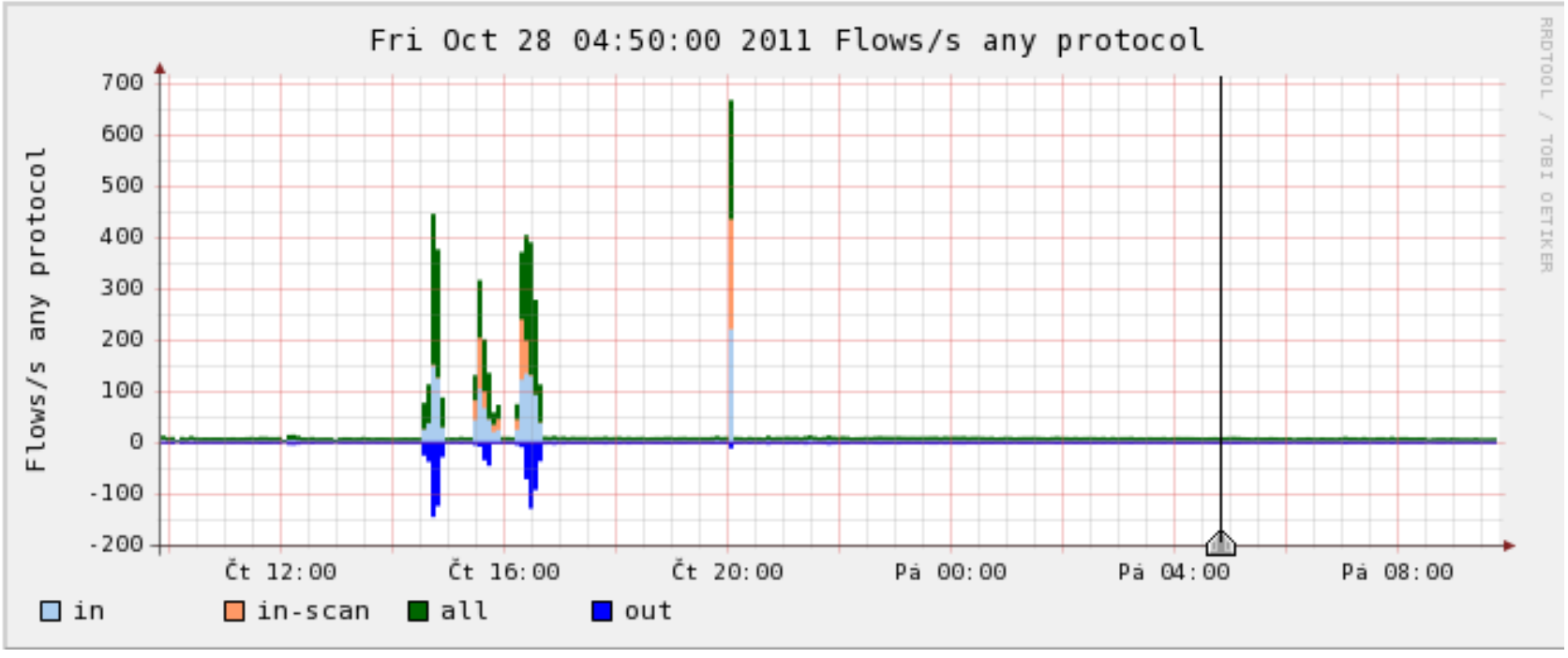
Detekce přístupu na síťové pasti

- Stavíme na předpokladu, že provoz přicházející na síťové pasti generují útočníci, ne legitimní uživatelé.
- Určitý rozsah sítě (čím větší, tím lepší) vyhradíme honeypotům a sledujeme veškerý příchozí provoz z naší sítě do tohoto segmentu.
- Nutno ale brát ohled na komunikaci iniciovanou honeypoty: např. synchronizace času přes NTP, kontrola aktualizací instalovaného SW, DNS dotazy, ICMP provoz atp.
- Opět jde o velmi jednoduchou a účinnou metodu, ale neodhalí tolik útočníků jako obecná detekce TCP SYN skenů.
- Podobně lze sledovat přístupy do dosud nealokovaného adresního prostoru (tzv. darknet nebo blackhole).
- Ukázka nástroje *Honeyscan*

Detekce na základě prahů

- Náhlé zvýšení celkového počtu toků, paketů a bajtů může indikovat útok či jinou tzv. objemově výraznou anomálii.
- Velmi primitivním druhem detekce sledování prahových hodnot těchto charakteristik a při překročení prahu hlášení útoku.
- Relativně dobré výsledky dává sledování pouze určitého portu či části adresního rozsahu.
- Nevýhody: ve velkých sítích je nastavení prahů pracné, uniknou objemově nevýrazné útoky (např. o velikosti 1 paketu).
- Místo prahů je lepší použít algoritmy pro analýzu časových řad (viz Holt-Wintersova metoda v další přednášce).

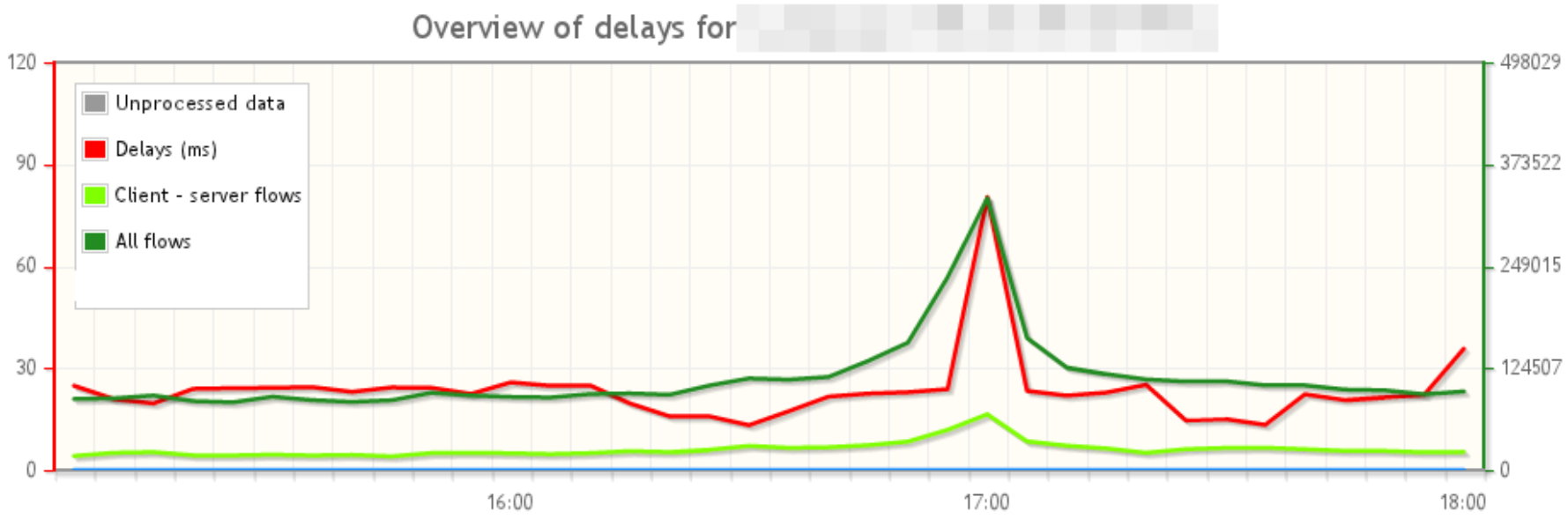
Detekce na základě prahů: služba SSH



Detekce na základě prahů: zpoždění

- Útok typu odepření služby (DoS) zvyšuje odezvu napadeného stroje.
- Některé typy útoků způsobí zpoždění i na úrovni transportní vrstvy – např. při navazování TCP spojení.
- Pro každý sledovaný stroj tedy vezmeme časovou známku požadavku (toku směrem na server) na požadavek a odečteme ji od časové známky odpovědi (toku ze serveru ke klientovi).
- Dostáváme RTT = zpoždění (s přesností na milisekundy), které porovnáme s nastaveným prahem a v případě překročení hlásíme útok.
- Neobvykle větší/menší zpoždění nemusí ukazovat pouze na útoky z vnějšku, ale i na chybu konfigurace služby/serveru či nedostatečně výkonný hardware.

Ukázka grafů zpoždění



Kontrola reverzních DNS záznamů

- RFC 1912:

  Every Internet-reachable host should have a name. The consequences of this are becoming more and more obvious. Many services available on the Internet will not talk to you if you aren't correctly registered in the DNS.
- Absence reverzního záznamu může ukazovat na zapomenutý a tedy i potenciálně nebezpečný stroj.

Kontrola reverzních DNS záznamů

- Předpoklad: trvale monitorujeme síťový provoz.[2]
- Zjistíme, jaké stroje komunikovaly v daném časovém okně.
- Vhodně využijeme agregaci.
- Máme seznam komunikujících strojů.
- Zavoláme překlad IP na jméno (např. `host`).
- Jsme hotovi? Všechno funguje bezvadně?
- Výsledky může ovlivnit firewall v cestě.
- Zajímá nás provoz reálných strojů, ne reakce firewallu na skenování.
  Jedním z možných řešení je omezení na TCP a filtr na TCP SYN pakety.

[2] Opět je klíčové kde.

Příprava pro penetrační testování

- Další použití seznamu komunikujících strojů na základě síťových toků.
- Příklad: penetrační testování vzdáleného přístupu k tiskárnám a dalším zařízením (IP kamery, projektory, ...).
- Cíl: efektivní provedení testu, který může trvat dlouho (malý výkon zařízení)
- Postup:
  - periodické zjištění zařízení (IP adres), která odpovídala z TCP portu 80 a zároveň z portu 23
  - testování výchozích či často používaných jmen a hesel (= slovníkový útok)

Základní techniky analýzy

- Výběr vhodného časového okna a části sítě – globální vs. detailní pohled.
- Filtrování – např. skenování (hledáme TCP toky pouze s příznakem SYN).
- Agregace podle klíčových položek – např. podle `srcIP`, `dstPort`: služby a jejich klienti.
- Top talkers (kdo komunikuje nejvíc) – např. zdroje objemově výrazného útoku.

- Kombinace všech uvedených.
- Více iterací.

Shrnutí

- Agregace provozu v podobě síťových toků je dobrým stavebním kamenem jednoduchých metod.
- Metody zpracovávající záznamy o tocích jsou v porovnání s inspekcí paketů velmi rychlé.
- I jednoduché metody (např. detekce TCP SYN skenů) jsou v praxi velmi užitečné.

Další literatura

- Peter Haag: Tracking Incidents with NfSen. `http://www.switch.ch/export/sites/default/all/cert/downloads/presentations/_files_presentations/Tracking.pdf`
- Carnegie Mellon Software Engineering Institute: *Network Profiling Using Flow*. Technical Report. 2012 `http://www.sei.cmu.edu/library/abstracts/reports/12tr006.cfm`