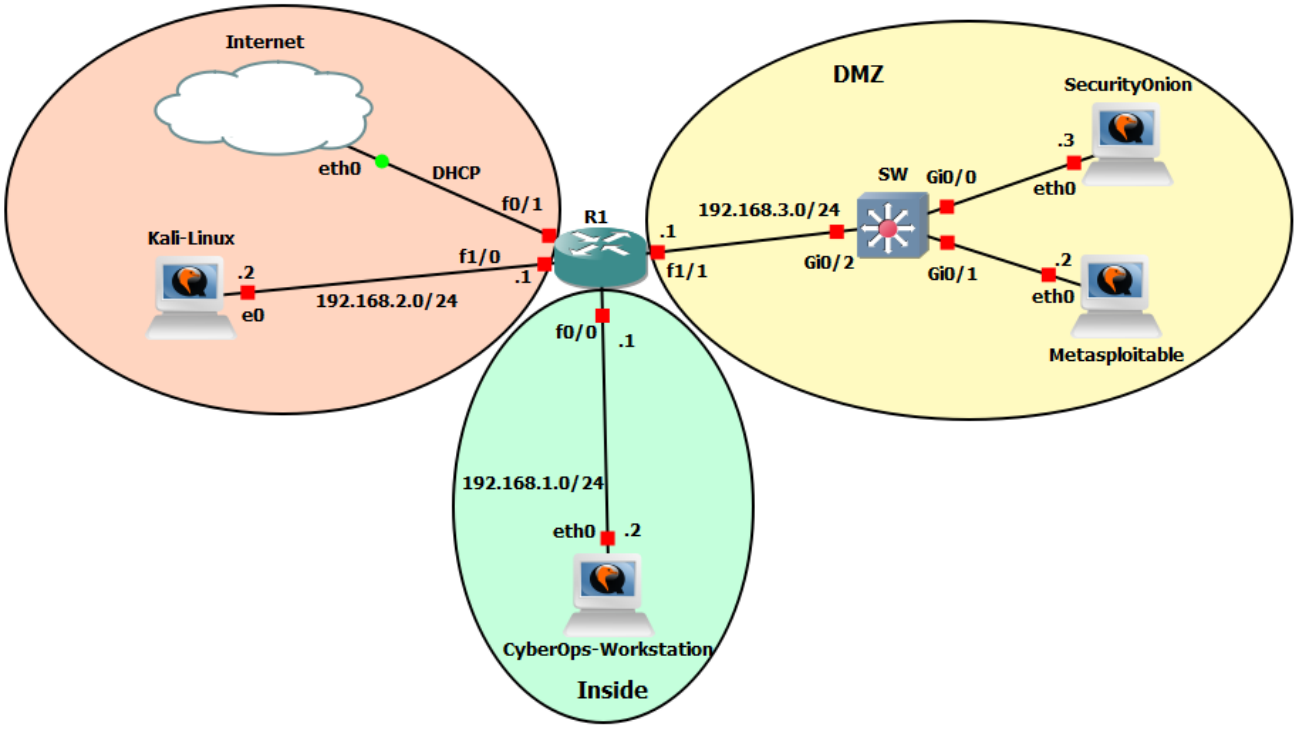
RBI / Cvičenie 03 / Logy a služby v Linux

Topológia



Požiadavky

- GNS3 alebo VirtualBox
- Internet a pripojenie na školskú VPN (ak mimo laboratória KIS a ak pracuješ s remote serverom v GNS3)

Inštrukcie a scenár

Operačný systém Linux je nevyhnutná súčasť sveta informačných systémov a sietí. V tomto cvičení si študenti precvičia lokalizáciu logov, prácu so službami a monitorovanie logov v reálnom čase. Tieto praktické poznatky sú nevyhnutnou súčasťou práce každého kybernetického analytika, preto je ich potrebné predstaviť a uviesť reálne využitie. Cvičenie bude zamerané na prácu so zariadeniami v našej topológii v GNS3 alebo vo VirtualBox-e, respektíve v NDG laboch (podľa toho akú alternatívu ste si vybrali na prvom cvičení), ale aj napriek tomu sa tieto poznatky ľahko uplatnia všade tam, kde sa pracuje s operačným systémom Linux.

- Pripojíme sa na GNS3 server alebo si otvoríme VirtualBox so zariadeniami alebo pracujeme v NDG labe
- Vypracujeme zadanie podľa stanovených úloh

Toto laboratórne cvičenie vzniklo na základe týchto oficiálnych Netacad labov a ich doplnením:

- 4.4.4 – Locating Log Files
- 17.2.7 – Reading Server Logs
- 4.5.4 - Navigating the Linux Filesystem and Permission Settings

Používatelia

Názov	Meno	Heslo
KALI LINUX	kali	kali
METASPLOITABLE	msfadmin	msfadmin
SECURITY ONION	analyst	cyberops
CYBEROPS WORKSTATION	analyst	cyberops

Lokalizácia súborov s logmi

Pracujeme so všetkými zariadeniami.

1. **Súbory logov webových serverov**
   a. Príklad súboru logov
      i. Otvorte CyberOps Workstation
         1. Použite príkaz `$ cat /var/log/logstash-tutorial.log`
            a. O akú prevádzku sa z výpisu jedná ?
            b. Dokážete nájsť webové logy aj na skutočnom webovom servery Metasploitable ?
2. **Súbory logov operačného systému**
   a. Linux používa priečinok /var/log na ukladanie rôznych log súborov
      i. Otvorte súbor na CyberOps Workstation /var/log/messages
         1. `$sudo more /var/log/messages`
            a. Podľa čoho sú uložené logy v priečinku ?
            b. O aké typ logov sa jedná?
            c. Má zmysel prezerať tieto logy aj na iných zariadeniach ?
3. **Lokalizácia súborov logov neznámeho softvéru**

   Pracujeme stále v CyberOps Workstation

   a. Otvorte dokumentáciu nginx na zistenie podrobností o tomto softvéry
      i. Príkaz `$ man nginx`
   b. Vo výpise nájdite sekciu ohľadom logovania
   c. Predtým ako prejdeme k hľadaniu nginxsúborom overíme, či nginx beží
      i. Na overenie príkaz `$ ps ax | grep nginx`
   d. Ak zistíme, že nginx nebeží, tak ho zapneme
      i. Príkaz `$ sudo /usr/sbin/nginx`
   e. Ak potrebujeme resetovať server
      i. Príkaz `$ sudo pkill nginx`
   f. `Ak chcete zapnúť nginx s vlastnou konfiguráciou, ktorú ste vytvorili na prvom cvičení`
      i. Príkaz `$ sudo nginx -c custom_server.conf`
      ii. Otvorte webový prehliadač na adrese 127.0.0.1:8080 pre overenie funkčnosti servera
   g. Ak chceme zapnúť nginx s default konfiguráciou
      i. Príkaz `$ sudo /usr/sbin/nginx`
      ii. `Následne vo webovom prehliadači choďte na URL 127.0.0.1`
   h. Vyhľadajte nginx konfiguračné priečinky
      i. Zadaj príkaz `$ls /etc/`

ii. Vyhľadajte konfiguračný súbor nginx
    1. Príkaz `$ ls -l /etc/nginx/`
iii. Otvorte konfiguračný súbor nginx
    1. Použijeme napr. `$ cat /etc/nginx/nginx.conf`
    2. Môžeme použiť aj nano na edit alebo more a less na lepší výpis
    3. Riadky, ktoré začínajú s # sú komentáre ignorované nginx
    4. Keďže nevidíme žiadnu zmienku v konfiguračnom priečinku nginx o súboroch logov je dosť možné, že využíva default hodnotu pre logy
    5. Skontrolujme priečinok `$ ls -l /var/log`
        a. Vidíme tento priečinok logov vo výpise?
        b. Zapíšte si názov
    6. Vypíšeme obsah logovacieho priečinka pre nginx
        a. Príkaz `$ sudo ls -l /var/log/[názov]`
            i. Čo sme sa dozvedeli z obsahu priečinka pre logovanie nginx?

i. Vieme nájsť aj neznáme služby aj na iných zariadeniach ?

Monitorovanie súborov logov v reálnom čase

Na monitorovanie využijeme jednoduchý príkaz tail, ktorý je dostupný vo všetkých Unixovo založených systémoch.

1. **Použitie tail príkazu**
    a. V terminály VM použime tail príkaz na zobrazenie konca logovacieho súboru
        i. Príkaz `$ sudo tail /var/log/nginx/access.log`
        ii. Použite prepínače -n a -f
            1. Napíšte, čo ovplyvnili prepínače a na čo slúžia
        iii. Necháme príkaz bežať v terminály a otvoríme webový prehliadač
        iv. Prejdeme na adresu 127.0.0.1
            1. Napíšte, čo sa udialo v terminály
2. Logovacie súbory a Syslog
    a. Syslog je systém navrhnutý tak, aby umožnil zariadeniam odosielať svoje logovacie súbory na centralizovaný server, známy ako syslog server. Klienti komunikujú so serverom syslog pomocou protokolu syslog. Syslog je bežne nasadený a podporuje prakticky všetky počítačové platformy
    b. CyberOps Workstation VM generuje logovacie súbory na úrovni operačného systému a odovzdá ich na syslog
        i. Použite príkaz cat ako root na zobrazenie obsahu súboru /var/log/syslog.1
            1. Čo obsahuje súbor?
        ii. Koľko ďalších syslog súborov sa nachádza v adresári? Prečo je ich viac?
            1. Na prezretie starších súborov syslog použite príkaz cat
3. **Nástroj Journalctl**
    a. Logovacia služba systémových udalostí
    b. Zobrazíme logovacie správy zo systému
        i. Príkaz `$ journalctl`
    c. Zobrazte správy, ktoré sa týkajú bootovania systému
        i. Príkaz `$ sudo journalctl -b`
            1. Aké typy správ vidíme ?
    d. Zobrazte správy, ktoré boli relevantné k posledným dvom bootovaniam systému
        i. Príkaz `$ sudo journalctl -b -2`
    e. Vyskúšajte ďalšie prepínače

i. –list-boots na zobrazenie predchádzajúcich bootovacích procesov
ii. –since „<time range>“ napr. –since „2 hours ago“ alebo „1 day ago“ alebo „today“
iii. -u nginx.service na zobrazenie logov generovaných serverom nginx
iv. -k na zobrazenie správ generovaných iba kernelom
v. -f pre „real-time“ monitorovanie
vi. –utc na zobrazenie časov v UTC formáte
vii. -u nginx.service -f
1. Čo príkaz z danými prepínačmi vykoná?
2. Otvor webový prehliadač a zadaj 127.0.0.1 (predvolená konfigurácia pre nginx) alebo 127.0.0.1:8080 (vlastná konfigurácia pre nginx) do adresného riadku. Aký nový log zobrazil journalctl?
3. Vyskúšajte rôzne kombinácie prepínačov

f. Funguje Journalctl aj na iných zariadeniach?

Súbory logov na iných zariadeniach

1. Otvoríme zariadenie Kali
   a. Otvoríme adresár /var/log
      i. Vypíšeme obsah adresára
         1. Aké súbory v tomto priečinku môžeme nájsť?
         2. Ktoré súbory v priečinku sú súbory logov?
         3. Sú tieto súbory čitateľné a editovateľné?
      ii. Preskúmajte obsah súborov
         1. Môžeme vypísať obsah súborov?
   b. Vyskúšajte použiť nástroj journalctl na tomto zariadení
      i. Funguje tento nástroj aj na tomto zariadení?
2. Otvoríme nástroj Metasploitable
   a. Nájdite adresár pre ukladanie logov webového servera
      i. Aké logy sa v tomto priečinku ukladajú?
      ii. Vypíšte logy súborov a preskúmajte, aké IP adresy žiadali o prístup k webovému serveru
   b. Nájdite logy pre prístup k databáze
      i. Sú tu nejaké súbory logov uložené?
      ii. Ak nájdete súbory, skúste popísať, čo obsahujú
3. Otvoríme nástroj Security Onion
   a. Spustíme terminál
      i. Vyhľadajte súbory logov pre nástroje Snort, Sguil a ELSA
         1. Aké typy logov obsahujú tieto nástroje a v akom formáte?

Konfigurácia vlastného syslog servera

V nasledujúcich krokoch si nakonfigurujeme syslog server na zariadení Security Onion. Taktiež si nakonfigurujeme smerovač R1,prepínač SW a zariadenie CyberOps-Workstation ako klientov, aby posielali svoje logy na syslog server Security Onion-u.

1. Otvoríme zariadenie Security Onion
   a. Vytvoríme nový konfiguračný súbor pre syslog-ng
      i. Premenujeme starý syslog-ng.conf súbor
         1. Príkaz `$ cd /etc/syslog-ng/`

2. Príkaz `$ mv syslog-ng.conf syslog-ng.conf.BAK`
3. Čo robia dané príkazy?

ii. Vytvoríme nový syslog-ng.conf súbor
1. Príkaz `$ sudo nano syslog-ng.conf`
2. Súbor bude mať nasledujúci obsah

```
source s_network { udp(ip(0.0.0.0) port(514)); };
destination d_syslog { file("/var/log/remotelogs/syslog"); };
log { source(s_network); destination(d_syslog); };
```

3. Čo znamenajú jednotlivé riadky konfiguračného súboru?

iii. Vytvoríme priečinok a súbor pre logy
1. Príkaz `$ sudo mkdir /var/log/remotelogs`
2. Príkaz `$ sudo mkdir /var/log/remotelogs/syslog`

iv. Spustíme a povolíme syslog-ng server
1. Príkaz `$ sudo systemctl start syslog-ng`
2. Príkaz `$ sudo systemctl enable syslog-ng`

v. Povolíme vstup (daný príkaz je nutné vykonávať vždy po zapnutí zariadenia Security Onion)
1. Príkaz `$ sudo iptables -P INPUT ACCEPT`

vi. Upozornenie: Pri veľkom množstve dát v súbore **syslog** (po určitom čase od zaznamenávania logov) je vhodné ho vymazať a vytvoriť nanovo

2. Otvoríme smerovač R1
   a. Zadáme sekvenciu príkazov
      i. Príkaz `# configure terminal`
      ii. Príkaz `# no logging trap warnings`
      iii. Príkaz `# logging trap informational`
      iv. Príkaz `# logging origin-id hostname`
      v. Príkaz `# logging host <ip adresa pre Security Onion>`
      vi. Čo znamenajú jednotlivé príkazy?
3. Otvoríme prepínač SW
   a. Zadáme tie isté príkazy ako na smerovači R1 ale ešte predtým nakonfigurujeme IP adresu a bránu pre prepínač SW
      i. Príkaz `# int vlan 1`
      ii. Príkaz `# ip add 192.168.3.4 255.255.255.0`
      iii. Príkaz `# no shut`
      iv. Príkaz `# exit`
      v. Príkaz `# ip default-gateway <ip adresa smerovača R1>`
   b. Ďalej zadávame už tie isté príkazy ako vyššie na smerovači R1
   c. Upozornenie: Nezabudnúť uložiť konfiguráciu na smerovači a taktiež aj na prepínači
4. Otvoríme CyberOps-Workstation
   a. Tak isto ako na zariadení Security Onion, najskôr premenujeme starý **syslog-ng.conf** súbor a následne vytvoríme nový
      i. Ktoré príkazy použijeme?
   b. Otvoríme nový **syslog-ng.conf** súbor a zapíšeme doň obsah z obrázka nižšie

```
@version: 3.22
source s_local {
  system();
  internal();
};
destination d_syslog_udp { syslog("192.168.3.3" transport("udp") port(514)); };
log { source(s_local);destination(d_syslog_udp); };
```

i. Čo znamenajú jednotlivé riadky?

c. Skontrolujte, či máte pravidlo v **iptables** pre **OUTPUT** chain nastavené na **ACCEPT**
   i. Príkaz `# sudo iptables -L`
   ii. Ak nie, zadajte príkaz `# sudo iptables -P OUTPUT ACCEPT`

d. Zapnite službu syslog-ng
   i. Príkaz `# sudo /usr/sbin/syslog-ng`

5. Sledovanie logov na zariadení Security Onion
   a. Môžeme sledovať logovací súbor
      i. Príkaz `# sudo tail -f /var/log/remotelogs/syslog`
      ii. Čo robí daný príkaz?
      iii. Vidíte logy zo všetkých troch zariadení(za predpokladu, že ich máte zapnuté a generujú vám logy)?

Navigácia v Súborovom Systéme Linuxu a Nastavenie Práv

V kanáli predmetu v záložke **Laboratory excercises** vypracujte:
RBI_LAB03-Netacad 4.5.4 Lab - Navigating the Linux Filesystem and Permission Settings

Záver

Súbory logov sú mimoriadne dôležité pri riešení problémov.
Umiestnenie súboru logov sa riadi konvenciami, ale v konečnom dôsledku je to voľba vývojára.
Informácie o súbore logov (umiestnenie, názvy súborov atď.) sú častejšie zahrnuté v dokumentácii.
Ak dokumentácia neposkytuje užitočné informácie o logovacích súboroch, kombinácii webového prieskumu a systémové vyšetrovanie by malo byť použité.
Hodiny by mali byť vždy synchronizované, aby sa zabezpečilo, že všetky systémy majú správny čas. Ak hodiny nie sú správne nastavené, je veľmi ťažké spätne vysledovať udalosti.
Je dôležité pochopiť, kedy sa konkrétne udalosti odohrali. Okrem toho udalosti z rôznych zdrojov sa často analyzujú súčasne.

Otázky

Porovnajte Syslog a Journald. Aké sú výhody a nevýhody každého z nich?