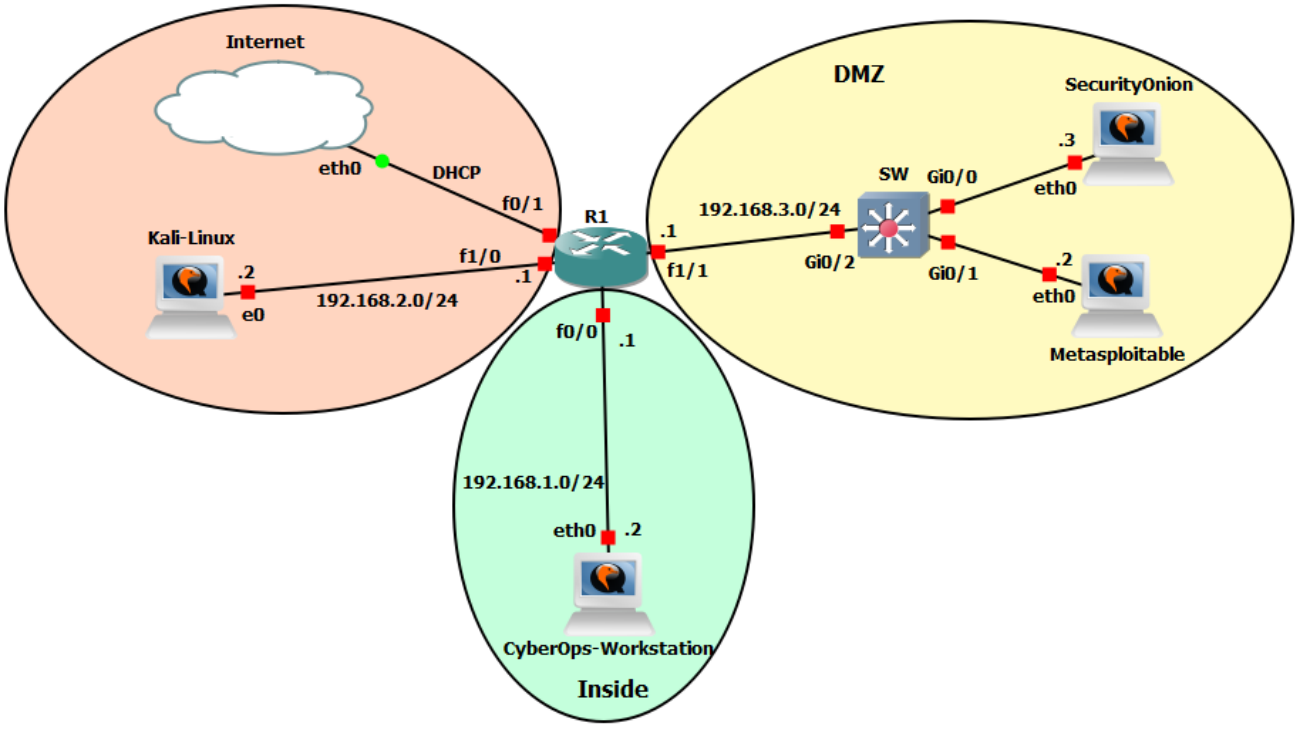
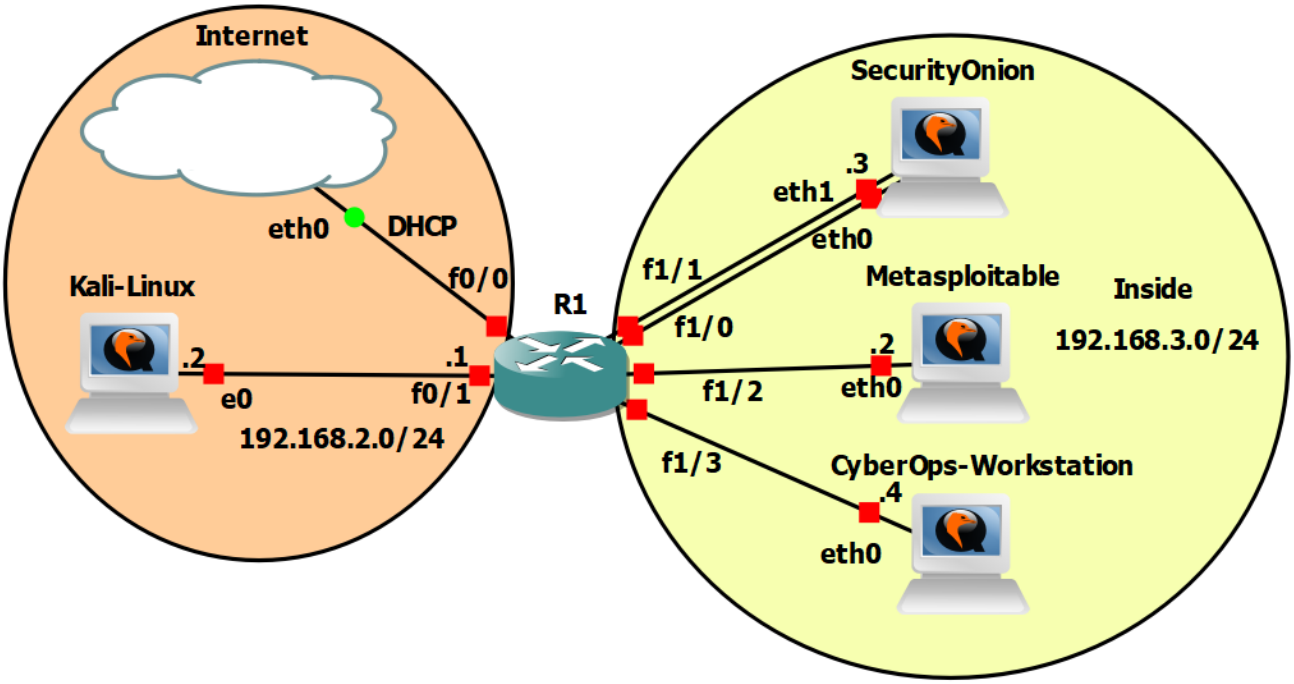
RBI / Cvičenie 04 / **Skenovanie sietí pomocou nástroja Nmap**

Topológia – pôvodná verzia/nová verzia





Inštrukcie a scenár

V tomto cvičení si ukážeme ako funguje nástroj **Nmap** (Windows verzia sa volá **Zenmap**). **Nmap** je bezplatný open-source nástroj na zisťovanie zariadení v sieti a môže slúžiť aj prre bezpečnostný audit. Tento nástroj používajú správcovia siete, penetrační testeri ale aj hackeri na identifikáciu zariadení v sieti, identifikáciu otvorených portov, a služieb ktoré bežia na zariadeniach. Nmap dokáže zistiť:

- Operačný systém zariadenia
- Otvorené porty
- Typ a verziu služby

V prvej časti sa naučíte pracovať s nástrojom **Nmap.** Tiež si vyskúšate nástroje ako **hping3**, **masscan**, **arp-scan**. Zo strany ochrany a zabezpečenia proti útočníkom sa tiež naučíte detekovať skeny pomocou IDS **snort** a tiež blokovať IP adresy rôznymi linuxovými nástrojmi. V druhej časti si vyskúšate nástroj Zenmap a spustíte skenovanie pre IPv4 rozsah jednej vybranej katedry FRI, ktorá vám bude pridelená.

Požiadavky

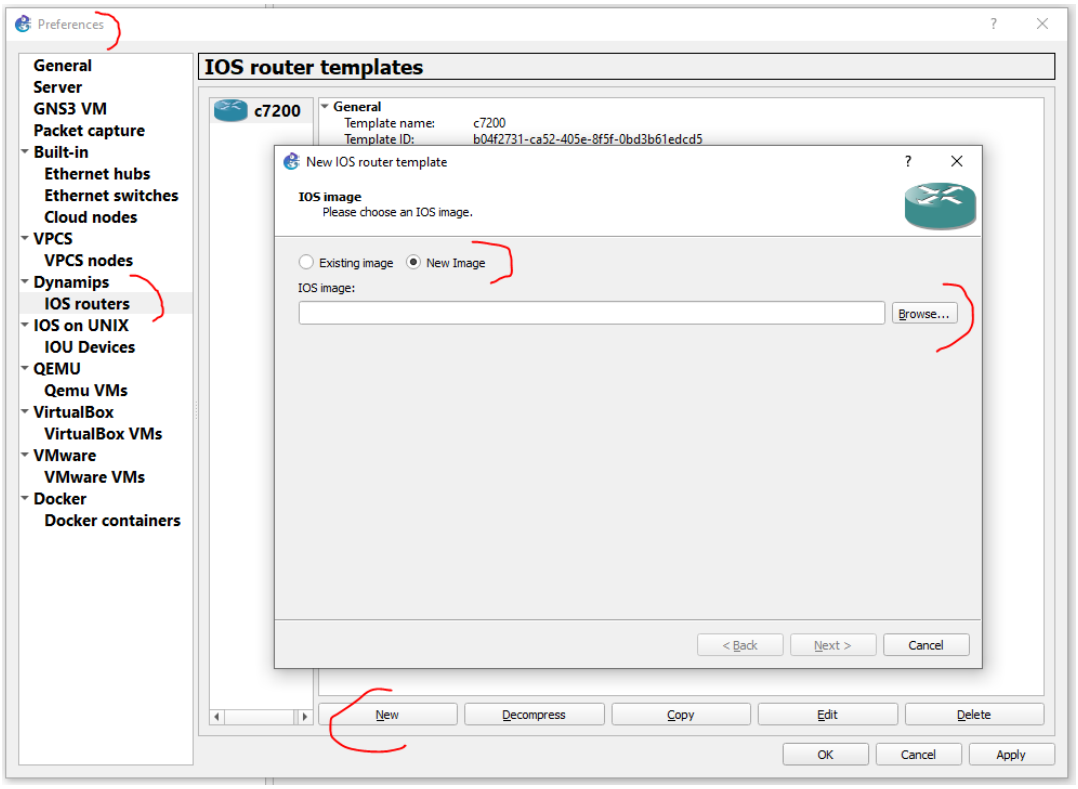
- Nakonfigurovaná topológia z prvého cvičenia v GNS3 (obrázok 1), ktorú si bude potrebné upraviť (obrázok 2), podľa inštrukcií v časti Zmenu v topológii
- Školská VPN (ak pracujete mimo siete UNIZA)
- V druhej časti nutná práca v počítačovom laboratóriu na KIS
- Zenmap pre Windows

Používatelia

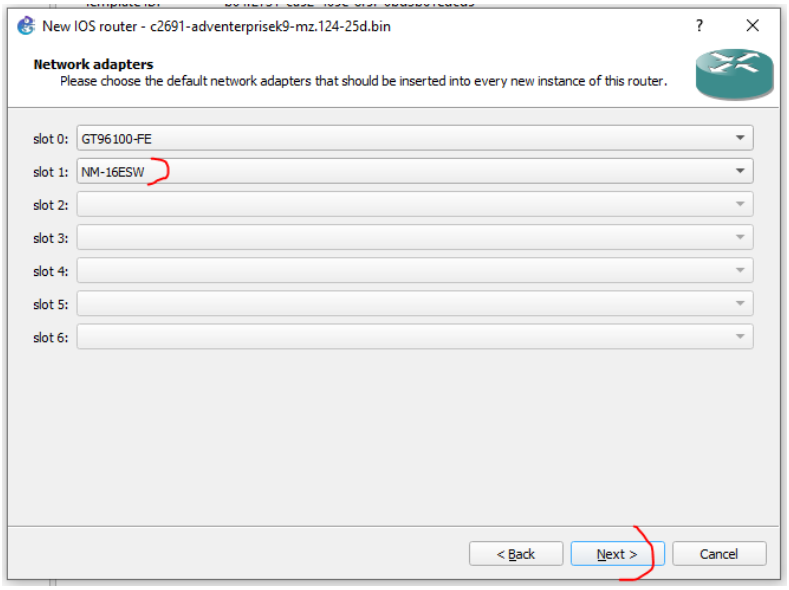
Názov	Meno	Heslo
KALI LINUX	kali	kali
METASPLOITABLE	msfadmin	msfadmin
SECURITY ONION	analyst	cyberops
CYBEROPS WORKSTATION	analyst	cyberops

Zmeny v topológií

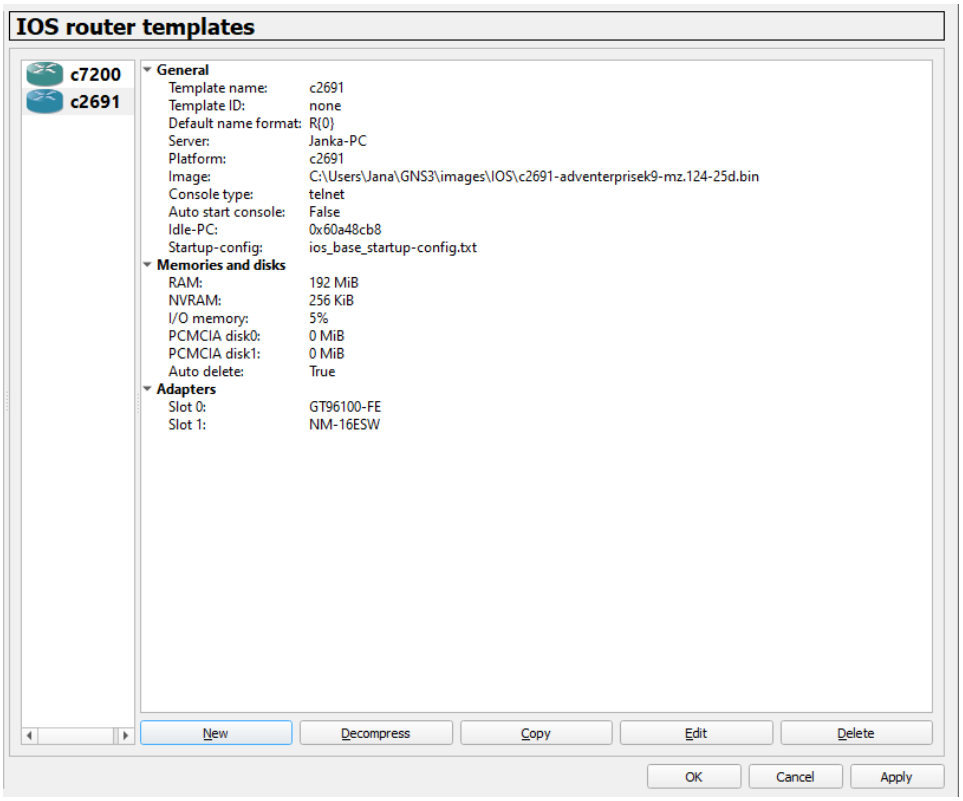
Pre potreby „port mirroring-u“, ktoré nie je podporované na modely prepínača, ktorý sme mali v topológii doteraz, je nutné vykonať v aktuálnej topológií niekoľko zmien. Je nutné, aby ste si vymenili smerovač 7200 za model smerovača c2691. Ak pracujete v lokálnom GNS3 servery, tak tento smerovač nájdete v kanály predmetu v „Laboratory excercises“ a importujete si ho na svoj server, cez Edit > Preferences:



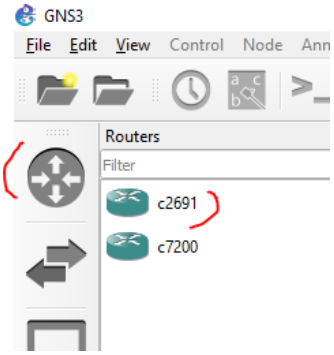
Hlášku „Would you like to copy..“ potvrdíte Yes, a ďalej Next, a na ďalších stránkach potvrdíte predvolené nastavenia, zastavíte sa až pri výbere rozhraní, kde ich rozšírite o 16 portový switchovaný modul:



WIC moduly nie sú žiadne potrebné. Vo výsledku budete mať pridaný template pre nový smerovač a potvrdíte cez Apply, a OK:



V ľavom panely zariadení vám pribudne nový smerovač, ktorý si pridajte do topológie:



Smerovač so zariadeniami spojte s linkami ako je to uvedené na obrázku v časti Topológia pre novú topológiu. Smerovaču je potrebné nastaviť pre rozhranie so zariadením Kali Linux novú IP adresu a default gateway. Pre všetky zariadenia, ktoré sú v spoločnej siete 192.168.3.0/24, nastavte smerovaču IP adresu pre rozhranie vlan1..

Ďalej je potrebné aby ste zmenili v konfiguračnom súbore pre CyberOps Workstation, IP adresu a default gateway, keďže toto zariadenie bude v sieti so zariadeniami Security Onion a Metasploitable, ako je uvedené na obrázku topológie.

Na záver zmeňte rozhrania pre zariadenia Security Onion podľa dokumentu „RBI_SecurityOnion_troubleshooting.docx“, ktorý je v tíme predmetu v kanáli „Laboratory excercises“.

Časť 1: Nmap

Vykonávajte na zariadení Kali Linux.

1. **Otvorte si terminál a zadajte príkaz:**
    a. Zadajte príkaz, ktorý vám vypíše všetky možne prepínače, ktoré môžete použiť v nástroji **Nmap**
        i. $ `nmap -h`
2. **Zistite aké IP adresy sa používajú v topológii**
    a. Zadajte príkaz:
        i. $ `nmap -sn 192.168.1-3.1-3`
    b. Prepínač -sn zisti, ktoré IP adresy reagujú na **ping** a vypne automatické skenovanie portov.
        i. Zistíte či ste našli všetky zariadenia v topológii (za predpokladu, že ste všetky zariadenia zapli cez zelené tlačidlo GNS3 klienta **Start all nodes**).
    c. Ako ďalší príkaz použite: $ `nmap 192.168.1-3.1-3`
        i. **nmap** skenuje štandardne 1000 portov ak chceme skenovať viac použijeme prepínač -p
            - Má zariadenie na nejakej IP adrese otvorené porty ?
              Ak áno, o ktoré zariadenie sa jedná?
              Aké porty sú na zariadeniach otvorené a aké služby na nich bežia?
            - Dokázali by ste otvoriť aj niektoré iné porty ?
    d. Použite prepínače pre nmap voči IP adrese 192.168.3.2
       Zistite, čo dané prepínače vykonávajú
       Vyskúšajte aj kombináciu prepínačov
        i. -p 1-65535
        ii. -sV
        iii. -sS
        iv. -O
        v. -T4
            -
    e. Použite nástroj Nmap aj na iných zariadeniach, a porozmýšľajte načo by nám mohol slúžiť z pohľadu kybernetickej bezpečnosti
3. Skenujte vzdialený server
    a. Upozornenie: Ak robíte na školskom GNS3 servery, tak túto úlohu robte, len ak viete, že ste jediný na ňom v danom čase, budeme využívať pripojenie do internetu.
        i. Alternatívou je využiť pre vás v tomto prípade Zenmap pre Windows a realizovať úlohu z vašeho notebooku, alebo školského PC. Môžete si ponechať na neskôr, po úlohe, ktorá sa nachádza v tomto zadaní neskôr so Zenmapom a potom sa sem vrátiť.
    b. Otvorte webový prehliadač a prejdite na stránku **scanme.nmap.org**. Prečítajte si správu na stránke.
        i. Aký je účel tejto stránky?
    c. Do príkazového riadka terminálu zadajte:
        i. $ `nmap -A -T4 scanme.nmap.org`
        ii. Čo znamenajú jednotlivé prepínače?
    d. Skontrolujte výsledky a odpovedzte na nasledujúce otázky.
        i. Ktoré porty a služby sú otvorené?
        ii. Ktoré porty a služby sú filtrované?
        iii. Aká je IP adresa servera?
        iv. Aký je operačný systém?

Časť 2: Hping3

Hping3 je sieťový nástroj schopný odosielať vlastné pakety na vzdialený server a zobrazovať odpovede zo vzdialeného servera na ne. Nástroj dokáže aj presúvať súbory, na základe určitých podporovaných protokolov. Pomocou hping3 sa dá testovať pravidlá brány firewall, vykonávať skenovanie portov (spoofing) a podobne.

1. **Na zariadení Kali Linux si otvorte terminál a zadajte príkaz:**
   a. Zadajte príkaz, ktorý vám vypíše všetky možne prepínače, ktoré môžete použiť v nástroji **Hping3**
      i. $ `hping3 -h`
      ii. Upozornenie: Ak nemáte hping3 nainštalovaný, tak si ho nainštalujete pomocou príkazu: $ `sudo apt-get install hping3`
2. **Skenujte zariadenie Metaspoitable**
   a. Pošlite jednoduchý ping
      i. $ `sudo hping3 -1 -c 1 <Metasploitable IP>`
      ii. Zisti, čo znamenajú jednotlivé prepínače
   b. Zadajte príkaz na skenovanie špecifického rozsahu portov pre zariadenie Metaspoitable
      i. $ `sudo hping3 --scan 1-512 -S <Metasploitable IP>`
      ii. Čo znamenajú jednotlivé pripínače?
      iii. Čo znamenajú jednotlivé stĺpce vo výpise a aké údaje ste zaznamenali?
   c. Pozrite sa na ďalšie možné prepínače a použite niektoré z nich

Časť 3: Masscan

MASSCAN je TCP port skener, ktorý asynchrónne prenáša TCP segmenty SYN a produkuje výsledky podobné nmap, najznámejšiemu skeneru portov. Interne funguje skôr ako scanrand, unicornscan a ZMap s použitím asynchrónneho prenosu. Je to flexibilný nástroj, ktorý umožňuje skenovať ľubovoľné rozsahy adries a portov.

1. **Na zariadení Kali Linux si otvorte terminál a zadajte príkaz:**
   a. Zadajte príkaz, ktorý vám vypíše všetky prepínače, ktoré môžete použiť v nástroji **Masscan**
      i. $ `masscan -h`
      ii. Upozornenie: Ak nemáte masscan nainštalovaný, tak si ho nainštalujete pomocou príkazu: $ `sudo apt-get install masscan`
2. **Skenujte zariadenia**
   a. Zadajte príkaz na skenovanie špecifického rozsahu portov pre zariadenie Metaspoitable s rýchlosťou 10 000 paketov za sekundu
      i. $ `sudo masscan -p1-512 <Metasploitable IP> --rate=10000`
      ii. Čo znamenajú jednotlivé pripínače?
      iii. Analyzujte výstup, a stručne popíšte aký výsledok ste dostali
   b. Zadajte príkaz na skenovanie celého subnetu triedy B
      i. $ `sudo masscan 192.168.0.0/16 --top-ports 100`
      ii. Čo robí daný príkaz s prepínačom?
   c. Pozrite sa na ďalšie možné prepínače a použite niektoré z nich, a okomentuje výsledky, ktoré ste dostali

Časť 4: Arp-scan

Veľmi známy a rozsiahly sken, ktorý posiela ARP žiadosti cieľom v lokálnej sieti, a zobrazuje všetky prijaté odpovede. Má pomerne veľa modifikácii, ktoré sa dajú použiť ako napríklad --interface, pomocou ktorého

špecifikujeme, ktoré sieťové rozhranie chceme použiť alebo --bandwith pomocou ktorej nastavíme požadovanú výstupnú šírku pásma a mnoho ďalších.

1. **Na zariadení Kali Linux si otvorte terminál:**
   a. Zadajte príkaz, ktorý vám vypíše všetky možné prepínače, ktoré môžete použiť v nástroji **Arp-scan**
      i. $ `arp-scan -h`
      ii. Upozornenie: Ak nemáte arp-scan nainštalovaný, tak si ho nainštalujete pomocou príkazu: $ `sudo apt-get install arp-scan`
2. **Skenujte lokálnu sieť**
   a. Zadajte príkaz na skenovanie lokálnej siete a zistite všetky IP adresy, ktoré vám odpovedia
      i. $ `arp-scan -l`
      ii. Čo reprezentuje prepínač „-l“?
      iii. Aké IP adresy ste dostali vo výpise?
   b. Pozrite sa na ďalšie možné prepínače, použite niektoré z nich, a okomentuje výsledky, ktoré ste dostali

Časť 5: Zablokovanie útočníka

V nasledujúcej časti si ukážeme ako je možné detekovať Nmap sken pomocou IDS snort. Pokiaľ by bol Snort nasadení ako IPS, tak by bolo možné Nmap sken aj zablokovať. Tiež sa naučíte rôzne varianty ako je možné zablokovať IP adresu útočníka cez nástroje OS Linux.

1. **Identifikujeme Nmap ping scan**
   a. Na smerovači R1 nastavte SPAN, zrkadlenie všetkej prevádzky z portu vedúceho k Metsploitable serveru na port vedúci k SecurityOnion .
      i. Ako zdroj bude preto pri konfigurácii rozhranie f1/2 (ako je uvedené na obrázku topológie) a ako cieľ bude rozhranie f1/0 (hint: `monitor session ...`, mali sme v predmete PS2)
   b. Otvoríme terminál na Security Onion
   c. Upozornenie pre Vbox: Ak pracujete vo VirtualBox-e, zmeníte IP adresu, ktorá je použitá nižšie, na takú, ktorú má váš Security Onion, voči ktorému budete testovať útok a aj dané snort pravidlo (keďže pri vašom nasadení nemáte smerovač, na ktorom by ste zrealizovali SPAN)
      i. Prihlásime sa ako root
      ii. Otvoríme súbor $ `sudo gedit /etc/nsm/rules/local.rules`
         1. Pridáme pravidlo
            a. alert tcp any any -> 192.168.3.2 22 (msg: "NMAP TCP Scan";sid:10000005; rev:2;)
               i. Čo znamená dané pravidlo? (Hint: šípka oddeľuje zdroj od cieľa)
      iii. Zapnite IDS mód pre Snort
         1. Odkomentujte riadok pre zahrnutie súboru local.rules, v ktorom sme vytvorili pravidlo. Otvorte konfiguračný súbor pre snort:
            a. $ `sudo nano /etc/nsm/seconion-eth0/snort.conf`
            b. Odkomentujte v ňom riadok vyznačený nižšie na obrázku(odstránením znaku „#“ pred slovom include)

```
##################################################
# Step #7: Customize your rule set
# For more information, see Snort Manual, Writing Snort Rules
#
# NOTE: All categories are enabled in this conf file
##################################################

# site specific rules
include $RULE_PATH/local.rules
include $RULE_PATH/downloaded.rules
```

2. Zapnite snort: $ `sudo snort -A console -c /etc/nsm/seconion-eth0/snort.conf -i eth0`
    a. Prečo sme zapli tento mód?

d. Otvoríme Kali Linux
    i. Otvoríme terminál
        1. Použijeme príkaz $ nmap -sT -p22 192.168.3.2
            a. Čo tento príkaz vykoná?

a. Otvoríme Wireshark v Security Onion
    i. Použijeme filter ip.addr == 192.168.3.2
        - Čo sme zistili z prevádzky?

b. V terminály v ktorom vám beží zapnutý snort, Môžeme vidieť vygenerovaný alert
    i. Čo tento alert naznačuje?

2. Zablokujeme útočníkovu adresu cez iptables

a. V operačnom systéme Linux je iptables nástroj na správu firewall pravidiel v OS
b. Otvoríme zariadenie Metasploitable
    i. Použijeme príkaz iptables
        - # `sudo iptables -A INPUT -s <Kali Linux IP address> -j DROP`
            - Čo robí daný príkaz s jednotlivými prepínačmi? (Zistite cez príkaz: `iptables -h`)
            - Spravte ping z Kali Linux na Metasplotaible
            - Čo sme z testovania zistili?
    ii. Ak chceme zablokovať len port
        - Vymažte najskôr pravidlo vytvorené v bode i. vyššie cez príkaz: # `sudo iptables -D INPUT -s <attacker IP address> -j DROP`
        - Spravte ping z Kali Linux na port 25 pre Metaspoitable cez príkaz: # `sudo telnet <Metasploitable IP> 25`
        - Je možné sa pripojiť na daný port?
        - Vytvorte pravidlo na zablokovanie portu 25
            - # `sudo iptables -A INPUT -s <attacker IP address> -p tcp --destination-port 25 -j DROP`
            - Čo teraz znamená príkaz s jednotlivými prepínačmi?
            - Vyskúšajte znova ten istý ping na port 25 (ping cez telnet na port 25). Je možné sa pripojiť teraz?
    iii. Pre ďalšiu úlohu v tomto laboratórnom cvičení odblokujeme IP adresu a port
        - # `sudo iptables -D INPUT -s <attacker IP address> -j DROP`
        - # `sudo iptables -D INPUT -s <attacker IP address> -j DROP -p tcp --destination-port 25`
        - Čo znamená prepínač „D“ v príkazoch vyššie?

3. Zablokujeme útočníkovu adresu cez príkaz route

a. Príkaz route alebo ip môže byť taktiež použitý na odstavenie nechcenej premávky. To je dosiahnuté pomocou takzvaného „null route“. Null route (tiež nazývaný ako blackhole route) je sieťová trasa alebo položka v smerovacej tabuľke jadra, ktorá nikam nevedie. Zodpovedajúce pakety sú skôr zahodené (ignorované), ako preposielané, čo funguje ako druh veľmi obmedzeného firewallu
b. Otvoríme zariadenie Metasploitable
c. „Null route“ cez route príkaz
    i. Požite príkaz route na zablokovanie útočníka
        - `# sudo route add <Kali Linux IP address> gw 127.0.0.1 lo`
    ii. Alebo alternatívne použiť „reject target“ cez príkaz route taktiež na zablokovanie
        - `# sudo route add -host <Kali Linux IP address> reject`
    iii. Taktiež je možné zrušiť celý subnet
        - `# sudo route add -net 192.168.2.0/24 gw 127.0.0.1 lo`
    iv. Spravte ping z Kali Linux na Metasploitable
d. „Null route“ cez ip príkaz
    i. Použite príkaz na vytvorenie „blackhole“ pravidla
        - `# sudo ip route add blackhole <Kali Linux IP address>`
    ii. Alebo môžete vytvoriť „blackhole“ pravidlo pre celý subnet
        - `# sudo ip route add blackhole 192.168.2.0/24`
    iii. Vyskúšajte ping z Kali Linux na Metasploitable
e. Odstráňte si vytvorený „null route“
    i. Pre route príkaz
        - `# sudo route delete <Kali Linux IP address>`
        - Alebo ak ste použili „reject target“
        - `# sudo route del -host <Kali Linux IP address> reject`
    ii. Pre ip príkaz
        - `# sudo ip route delete <Kali Linux IP address>`

Existuje niekoľko typov Nmap scans, nielen ping scan, napríklad TCP scan, XMAS scan, FIN scan, NULL scan alebo UDP scan. Ak budete mať čas, môžete si tieto scany a ich zablokovanie vyskúšať.

Nmap Scan	Príkaz na spustenie scanu	Snort pravidlo

TCP	`nmap -sP 192.168.3.3 --disable-arp-ping`
	
	`Upozornenie:`
	`Urobte ten istý sken ale s prepínačom -sn, ktorý je novou verziu pre starší prepínač -sP`
		`alert icmp any any -> <IP address> any (msg: "NMAP ping sweep Scan"; dsize:0;sid:10000004;)`

XMAS	`nmap -sX -p22 <IP address>`	`alert tcp any any -> <IP address> 22 (msg:"Nmap XMAS Tree Scan"; flags:FPU; sid:1000006; rev:1; )`
FIN	`nmap -sF -p22 <IP address>`	`alert tcp any any -> <IP address> (msg:"Nmap FIN Scan"; flags:F; sid:1000008; rev:1;)`
NULL	`nmap -sN -p22 <IP address>`	`alert tcp any any -> <IP address> (msg:"Nmap NULL Scan"; flags:0; sid:1000009; rev:1; )`

UDP	`nmap -sU -p68 <ip address>`	`alert udp any any -> <ip address> any ( msg:"Nmap UDP Scan"; sid:1000010; rev:1; )`

Časť 6: Zenmap

1. Na vašom počítací by ste mali mať nainštalovaný **Zenmap** (Windows verzia nástroja nmap). Nájdite tento nástroj. Pokiaľ ho nainštalovaný nemáte, doinštalujte ho, v školskom laboratóriu vám zadá učiteľ admin heslo na inštaláciu, ak bude potrebné.
   Rozdeľte sa do 4-5 skupín, každá skupina bude skenovať jednu katedru na FRI. Zvoľte vhodné prepínače aby ste zistili tieto informácie:
   a. IP adresy zapnutých zariadení
   b. Otvorené porty
   c. Služby/verzie na bežiacich zariadeniach
   d. Operačný systém zariadení
   e. Výsledok skenovania si uložte do textového súboru pomocou prepínaču `-oN /root/Dokumenty/Sken_kadetra_XXX.txt`
2. Rozdelenie skupín:
   a. Skupina 1: Katedra informačných sietí (Adresný priestor:)
   b. Skupina 2: Katedra informatiky (Adresný priestor:)
   c. Skupina 3: Katedra technickej kybernetiky (Adresný priestor:)
   d. Skupina 4: Katedra softvérových technológií (Adresný priestor:)
   e. Skupina 5: Katedra matematických metód a operačnej analýzy (Adresný priestor:)

Záver

Otázky

Nmap je výkonný nástroj na prieskum a správu siete. Ako môže Nmap pomôcť so zabezpečením siete? Ako môže byť Nmap použitý hackerom ako útočný nástroj?