

# Pracovní list – Scénáře na HTTP flood a TCP SYN flood útoky

**Obsah**

[Pracovní list – Scénáře na HTTP flood a TCP SYN flood útoky 1](#_Toc192000145)

[Úvod 1](#_Toc192000146)

[Potřebné materiály 1](#_Toc192000147)

[Instrukce 2](#_Toc192000148)

[Část 1. Zavedení topologie 2](#_Toc192000149)

[Krok 1. Stáhnutí a virtualizace strojů 2](#_Toc192000150)

[Krok 2. Nastavení síťových karet ve VB 3](#_Toc192000151)

[Krok 3. Komunikace (routery) 3](#_Toc192000152)

## Úvod

Tento pracovní list slouží pro procvičení základních znalostí ohledně DDoS útocích, Command and Control serverech a specificky se zaobírá HTTP flood a TCP SYN flood útokům.

V průběhu práce student bude konfigurovat základní prvky pro nadstavbu scénářů, nastaví scripty pro funkčnost celého útoku jako, bind shell na CnC server a scripty pro komunikaci s botnetem.

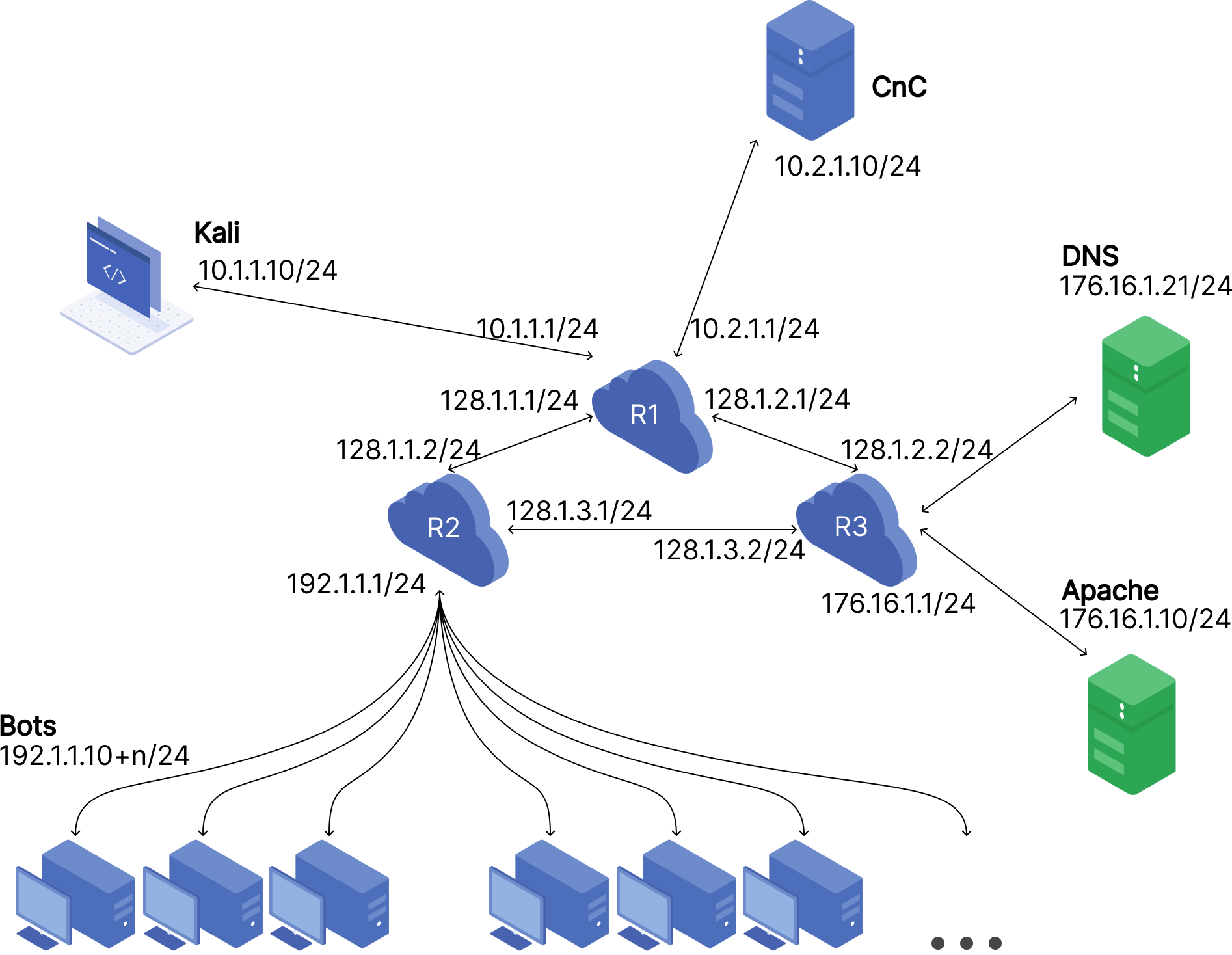
Na konci této práce by student měl mít větší porozumění o těchto útocích, jak jejich chování funguje a co mohou způsobit.

## Potřebné materiály

* Software pro virtualizaci (VirtualBox)
* Software pro konfiguraci routeru (WinBox)
* Místo pro virtuální stroje ~50 GB.
* Obrazy Ubuntu server, Kali a RouterOS.

# Instrukce

## Část 1. Zavedení topologie



Obrázek Topologie virtualizovaného prostředí

Na Obrázku 1 je celá topologie práce i s přiřazenými IP adresami. V tomto zapojení tedy bude komponovat Útočník, na kterém běží distribuce Kali (dostupná z: <https://www.kali.org/get-kali/#kali-virtual-machines>), ze kterého budou pramenit útoky.

Centralizovaný CnC (Command and Control) server, ke kterému Útočník má root přístup a ze kterého se budou přeposílat útoky botnetu.

Boti, kteří reprezentují infikované zařízení s přístupem na internet a jsou tedy spouštěči škodlivého kódu.

Tři routery s operačním systémem RouterOS (dostupný z: <https://mikrotik.com/download>) a Ununtu, mají simulovat internet a umožnit load balancing, pokud je potřeba.

A samotné servery oběti, na kterých běží HTTP služba Apache a DNS služba Bind na překlad adresy z druhého serveru. Jak Boti tak servery běží převážně na Ubuntu (dostupný z: <https://ubuntu.com/download/server>).

### Krok 1. Stáhnutí a virtualizace strojů

V uvedených lincích minule si stáhněte vždy jen jeden soubor. Kali a RouterOS jdou stáhnout rovnou jako import do VirtualBoxu, ale ubuntu server se musí stáhnout jako .ios soubor.

Po stáhnutí Kali a RouterOS stačí jen otevřít (poklepat) a začne import. Pro Ubuntu jděte do VirtualBoxu a klepněte na nový.

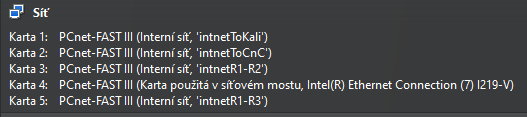


Vyplňte všechny potřebné informace jako jméno, místo staženého .iso souboru a ve položce hardware zvolte 10GB místa (v budoucnu budeme dělat co nejvíce propojených klonů pro co největší ušetření místa).

Každý stroj by měl už tedy jít spustit. (defaultní jméno/heslo pro kali je kali/kali, pro RouterOS není nastavené žádné a pro Ubuntu při instalačce si nastavíte vlastní (doporučuji nějaké krátké a lehce zapamatovatelné)).

### Krok 2. Nastavení síťových karet ve VB

Pro každou „cestu“ je potřeba založit novou interní síť a přiřadit ji ke síťové kartě. Např.: u routeru R1 (jediný RouterOS) bude síťové pole ve VirtualBoxu vypadat takto:



Pro nastavení páté síťové karty musíme zadat do našeho terminálu tento command (nejlépe v umístění VirualBoxu (defaultně ve C:\Program Files\Oracle\VirtualBox\)):

* .\VBoxManage.exe modifyvm “<Jméno R1 routeru>“ --nic5 none

Nakonec změnit na potřebný typ ve VirtualBoxu poklepáním na část ve závorce.

### Krok 3. Komunikace (routery)

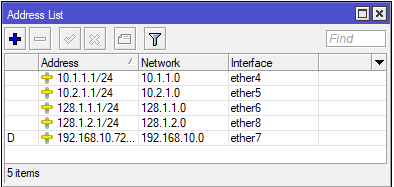
Po spuštění RouterOS, který bude naším „hlavním“ routerem, se vám ukáže CLI rozhraní. Buď můžete konfigurovat přes to, nebo se k němu připojíme přes WinBox (dostupný z: <https://mikrotik.com/download>), abychom mohli konfigurovat ve grafickém rozhraní.

Dejte si pozor abyste ve síťovém menu měly povolen síťový most, aby šel router vidět.

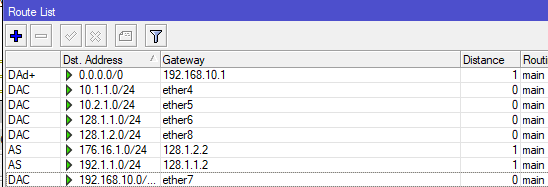
Ve IP -> DHCP client vytvoříme základního klienta (stačí dát rozhraní, které slouží jako síťový most (pokud si nejste jistí můžete se kouknout do kolonky Interfaces a kde bude provoz, to je síťový most)).

Ve IP -> Addresses vytvoříme adresy podle schématu

Celý adresový list by měl vypadat nějak takto:



Ve IP -> routes nastavíme routy do vzdálených sítí (ze schématu je vidět, že vzdálená sítě budou pro nás jenom sítě serverů a botnetu). Celý list by měl vypadat takto:



Nakonec abychom měli sice pomalou ale nějakou automatickou komunikaci do internetu v síti, tak je potřeba ještě nastavit NAT ve IP -> firewall a kolonce NAT.

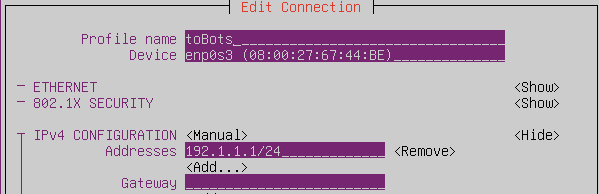
Ve vytváření nás zajímají jen 3 pole. Ve General pole Chain, který bude srcnat. Out. Interface, který je náš síťový most. A v Action zvolíme masquerade.

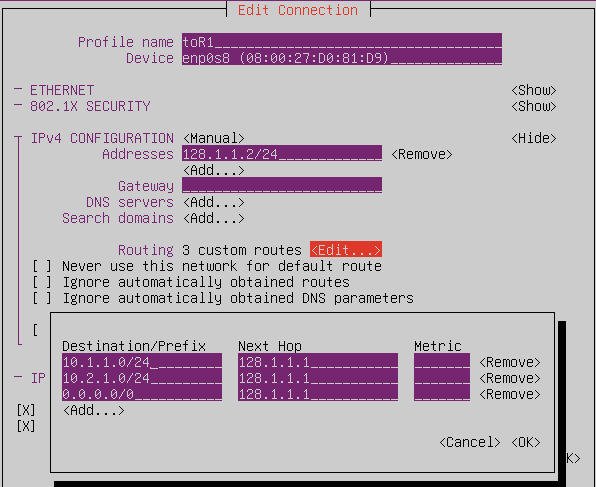
Pro další dva routery zvolíme ubuntu, protože zdarma verze RouterOS má limit na tx 1Mb/s.

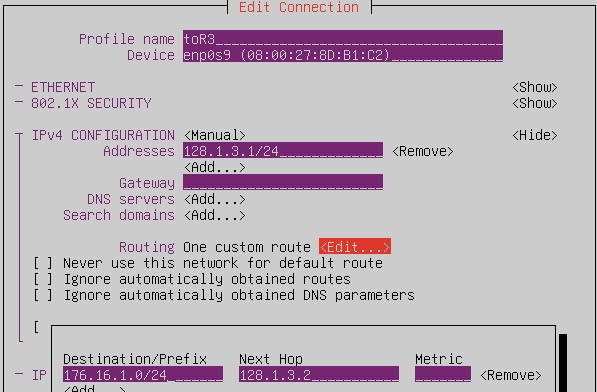
Ještě předtím, než naklonujeme ubuntu, tak na naše základní přidáme síťový most abychom měli rychlou konektivitu do internetu a nainstalujeme na něj nástroj nmtui pro konfiguraci síťových parametrů (budeme využívat i u koncových zařízení).

Poté můžeme naklonovat a upravit síťové karty ve VB.

Po spuštění nmtui dáme add connection a přidáme potřebné rozhraní. Např.: u routeru R2 budou rozhraní vypadat následovně:







U routeru R3 doplníme podle schématu (na servery 176.16.1.1./24, na R1 s 128.1.2.2/24 a třemi routy jak u R2 (ale next-hop je 128.1.2.1) a na R2 128.1.3.2/24 s routou na síť botnetu).

Pro propsání změn můžeme rebootnout, nebo deaktivovat rozhraní ve nmtui ve „Activate a connection“.

