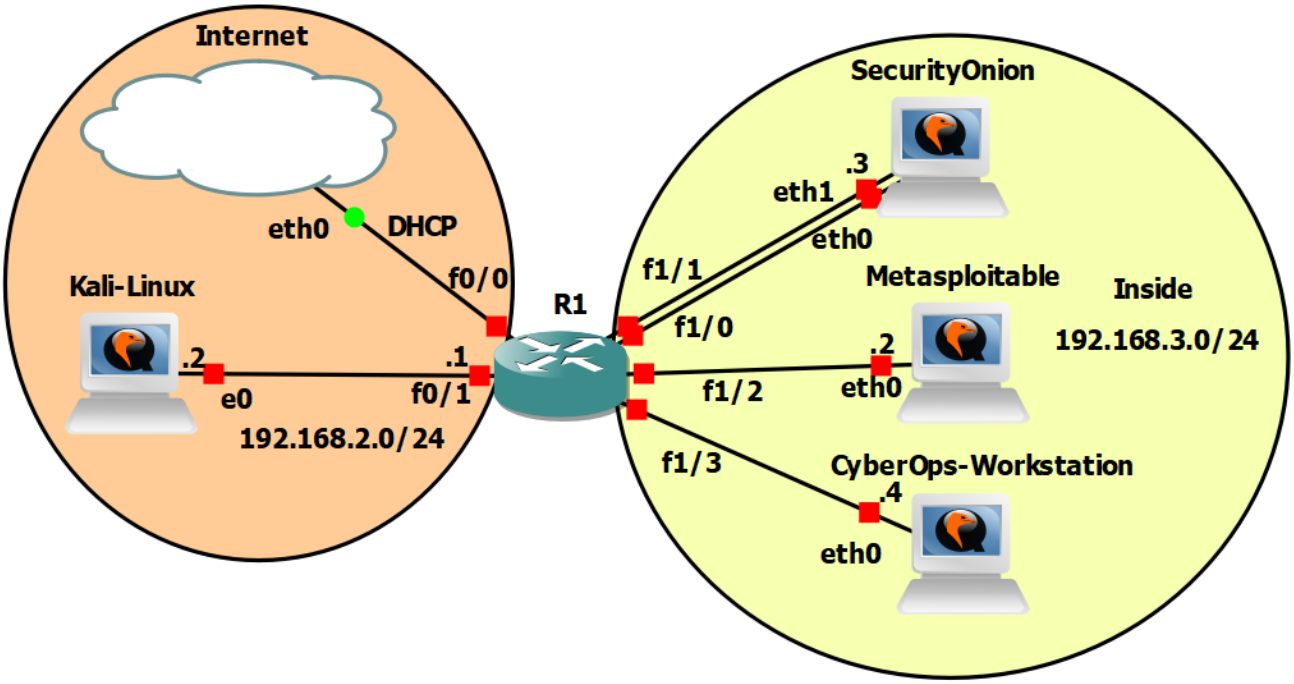
RBI / Cvičenie 12 / Analýza a vyšetrovanie incidentov

Topológia



Požiadavky

- Topológia v GNS3 alebo vo VirtualBox-e
- UNIZA VPN (Ak pracujeme mimo KIS)
- Internetové pripojenie
- Inštancia Security Onion-u s demo dátami

Inštrukcie a scenár

V tomto cvičení budete pracovať s inštanciou Security Onion-u, ktorá obsahuje demo dáta, a teda nebol na tomto zariadení vykonaný Security Onion Setup.

Používatelia

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

Časť 1: Interpretovanie HTTP a DNS dát na izolovanie aktéra hrozby

V kanáli predmetu v záložke **Laboratory excercises** vypracujte:
RBI_LAB12-Netacad 27.2.12 Lab – Interpret HTTP and DNS Data to Isolate Threat Actor.docx

Časť 2: Izolovanie kompromitovaného hostiteľa použitím 5-Tuple

V kanáli predmetu v záložke **Laboratory excercises** vypracujte:
RBI_LAB12-Netacad 27.2.14 Lab – Isolate Compromised Host Using 5-Tuple.docx

Časť 3: Vyšetrovanie malvér exploit-u

V kanáli predmetu v záložke **Laboratory excercises** vypracujte:
RBI_LAB12-Netacad 27.2.15 Lab – Investigating a Malware Exploit.docx

Časť 4: Vyšetrovanie útoku na Windows hostiteľa

Táto časť je dobrovoľná a nemusíte ju teda robiť. V kanáli predmetu v záložke **Laboratory excercises** dobrovoľne vypracujte:
RBI_LAB12-Netacad 27.2.16 Lab – Investigating an Attack on a Windows Host.docx

Časť 5: Prevod dát do univerzálneho formátu

Táto časť je dobrovoľná a nemusíte ju teda robiť. V kanáli predmetu v záložke **Laboratory excercises** dobrovoľne vypracujte:
RBI_LAB12-Netacad 27.1.5 Lab – Convert Data into a Universal Format.docx