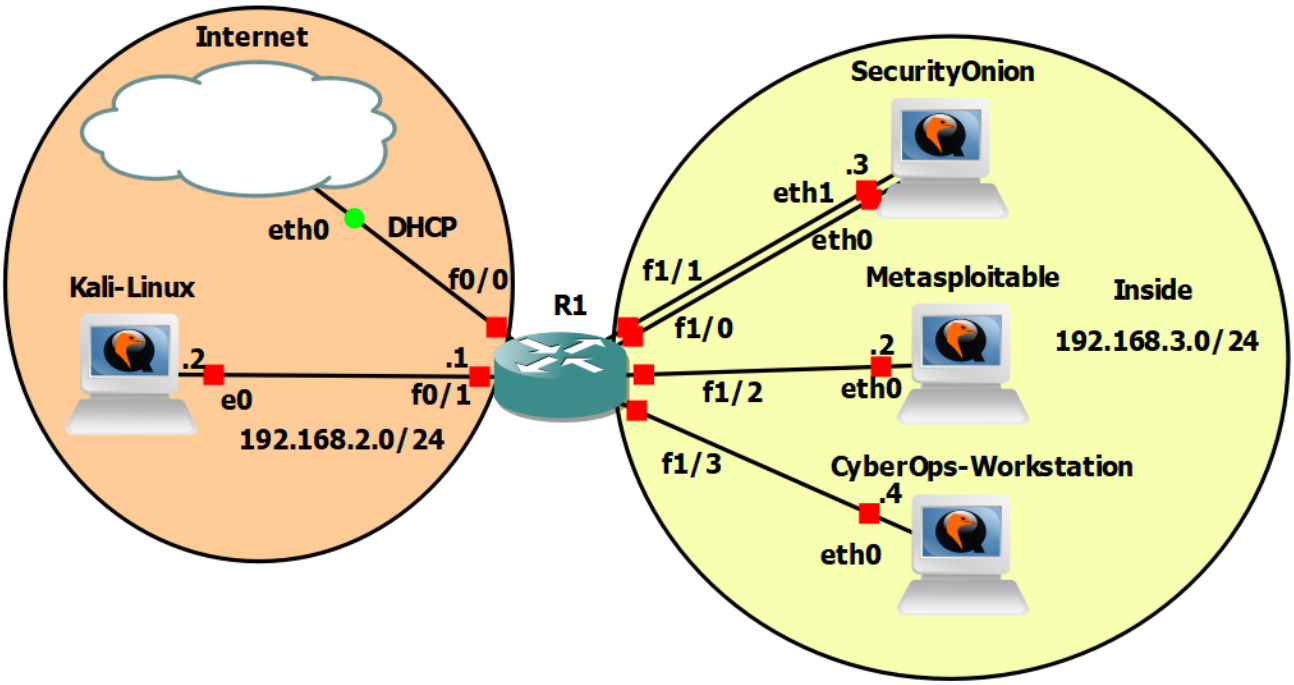
RBI / Cvičenie 10 / **Skenovanie zraniteľností na FRI pomocou nástroja OpenVAS**

Topológia



Požiadavky

- Topológia v GNS3/vo VirtualBox-e
- UNIZA VPN (ak chcete pracovať na vzdialenom GNS3 serveri a ste mimo UNIZA)
- Internetové pripojenie

Inštrukcie a scenár

V tomto cvičení budete pracovať s nástrojom OpanVas. OpenVas slúži na plnohodnotné skenovanie zraniteľností. Ak pracujete vo VirtualBox-e, alebo lokálne v GNS3, tak vašou úlohou bude zistiť aké zraniteľnosti sa nachádzajú na katedre, ktorá vám bude pridelena na cvičení. Ak pracujete na vzdialenom katedrovom GNS3 serveri, alebo pracujete lokálne, ale máte problém s pripojením topológie do Internetu (postačí pripojenie do internetu pre zariadenie Kali Linux), tak skenovať budete zariadenia z adresného priestoru 192.168.3.0/24. Nakoniec si vygenerujete report, ktorý nahráte na Moodle a odprezentujete výsledky z neho vyučujúcemu.

Používatelia

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

Časť 0: Príprava

Podľa toho v akej topológií pracujete, vykonajte potrebné kroky:

1. Práca na školskom GNS3 serveri

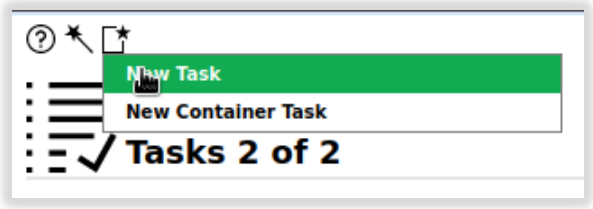
   Do topológie si pridajte nové zariadenia zo záložky „Browse End Devices“ s názvom „kali_linux-RBI“. Zariadenie nahraďte za váš pôvodný Kali Linux a taktiež ho nakáblujte so smerovačom R1. Keďže na tomto cvičení budete pracovať s nástrojom Openvas, ktorý na to aby vám šiel plynule, potrebuje väčšie zdroje, ako sme mali nastavené pre Kali Linux doteraz, je potrebné zväčšiť zariadeniu Kali Linux RAM na 8000 MB a CPU na 3. Spustite si zariadenie a vykonajte pre neho sieťovú konfiguráciu tak, ako ste to robili na cvičení 1. Následne vykonajte reštart zariadenia.
2. Práca na lokálnom GSN3 serveri/VirtualBox-e

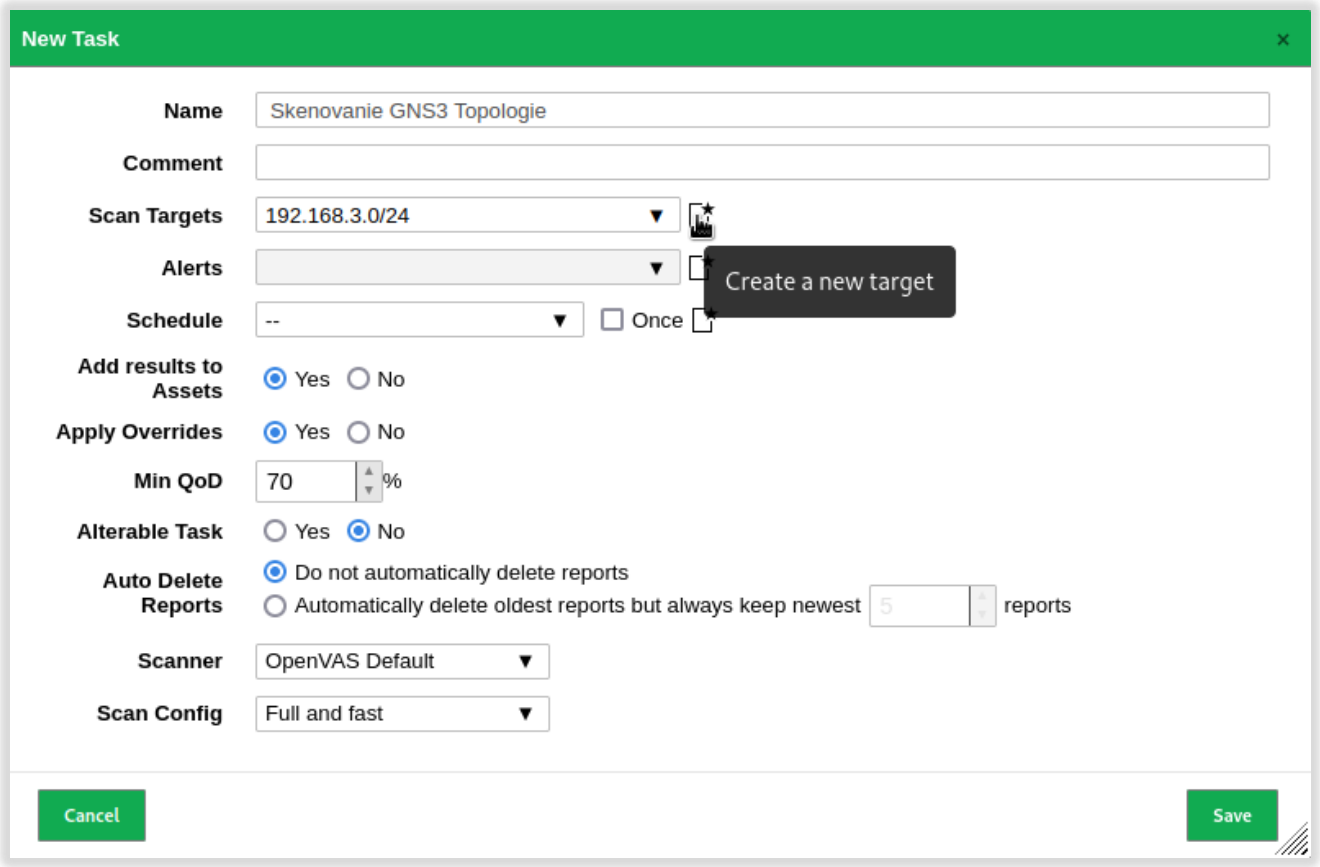
   Keďže na tomto cvičení budete pracovať s nástrojom Openvas, ktorý na to aby vám šiel plynule, potrebuje väčšie zdroje, ako sme mali nastavené pre Kali Linux doteraz, je potrebné zväčšiť zariadeniu Kali Linux RAM na 8000 MB a CPU na 3.
   Nainštalujte si na svoju inštanciu Kali Linux-u Openvas pomocou návodu v kanáli cvičenia s názvom „OpenVas Inštalácia“.
   Upozornenie: Ak pracujete v lokálnej GNS3 topológii bez GNS3 VM a nejde vám pripojenie do internetu, alebo nechcete z nejakého dôvodu inštalovať OpenVas, tak si importujte zariadenie s názvom kali_linux-RBI, ktoré nájdete v kanáli predmetu k cvičeniam. Následne vykonajte kroky v bode 1.

Časť 1: Skenovanie s nástrojom OpenVas

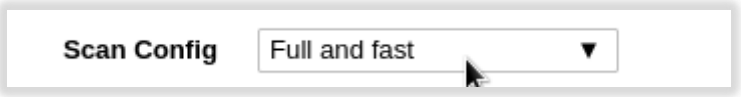
1. Spustenie OpenVas programu
   a. Spustite si Kali Linux
      i. Prihláste sa pomocou mena a hesla
      ii. Otvorte terminál
      iii. Spustite nástroj Openvas pomocou príkazu:
         - `sudo gvm-start`
         - Openvas bude prístupný na adrese `https://127.0.0.1:9392`
      vi. Otvorte si prehliadač a zadajte url: `https://127.0.0.1:9392`
         - Výplne údaje a prihláste sa:
            - Username: admin
            - Password: získate z textového súboru na pracovnej ploche s názvom openvas – credentials (druhý riadok v súbore je heslo)

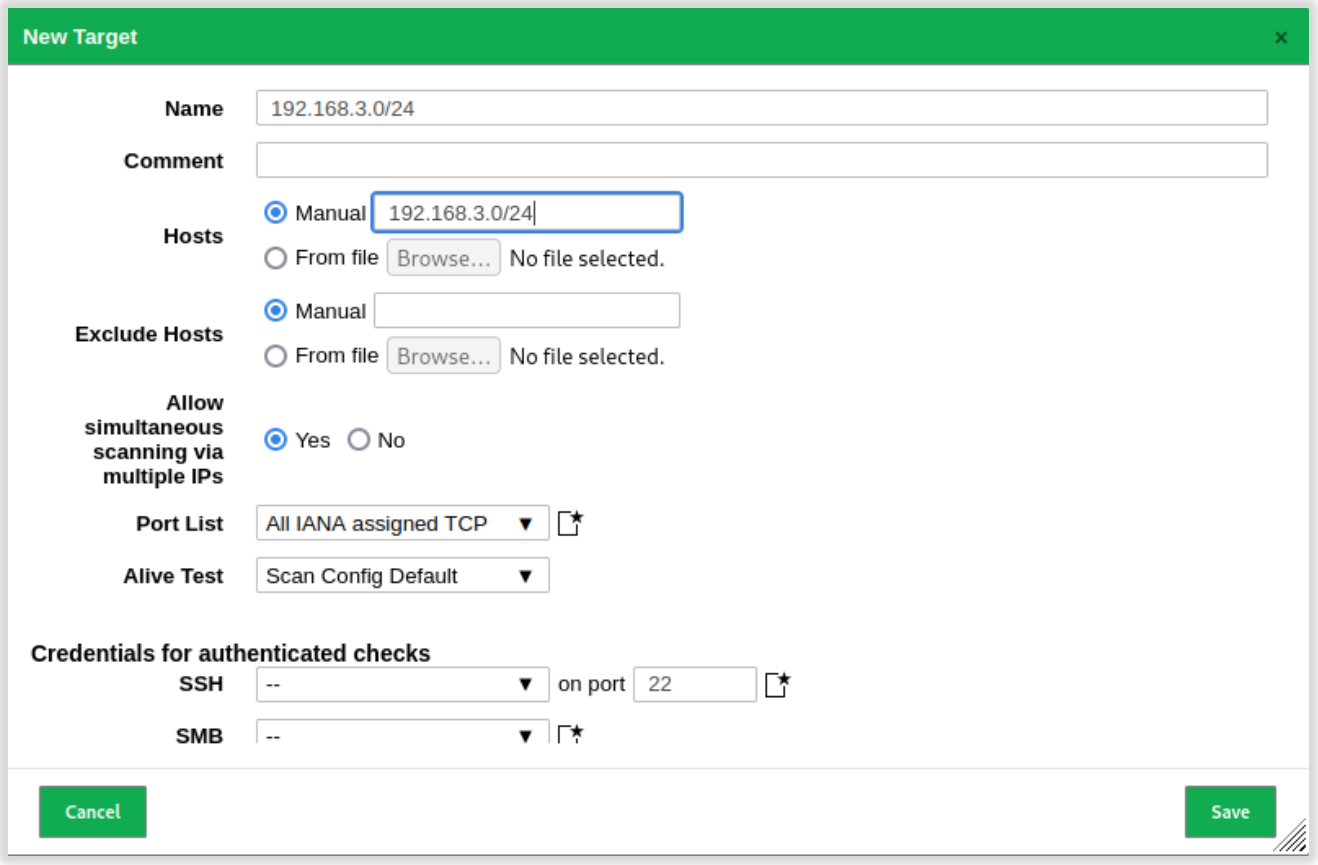
              Upozornenie: Toto platí pre tých, ktorí si pridali do topológie nový kali_linux-RBI. Ostatní si uložili heslo po inštalácií Openvas-u a teda zadávajú toto heslo.
   b. Príprava na skenovanie:
      i. Tí, ktorí nemajú problém s konektivitou do internetu pre zariadenie Kali Linux: V skupine si rozdelíte zariadenia alebo adresný priestor, ktorý ste zistili pre danú katedru, ktorá vám bola pridelená.
      ii. Tí, ktorí majú problém s konektivitou do internetu pre zariadenie Kali Linux: Skenujete adresný priestor 192.168.3.0/24 z topológie
   c. Spustite skenovanie:





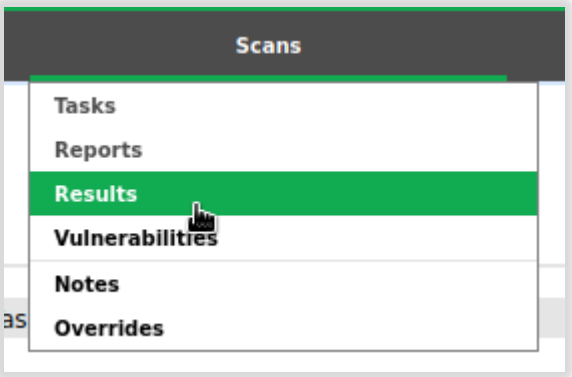
Scans → Tasks → New Task (vľavo hore) → Následne si vytvoríte **New target**
→ Ak skenujete katedru: Zadáte meno katedry a IP adresu/adresný priestor alebo nahraté súbor, kde budú IP adresy, ktoré chcete skenovať. Ak skenujete topológiu v GNS3, zadáte adresný priestor pre skenovanie 192.168.3.0/24.



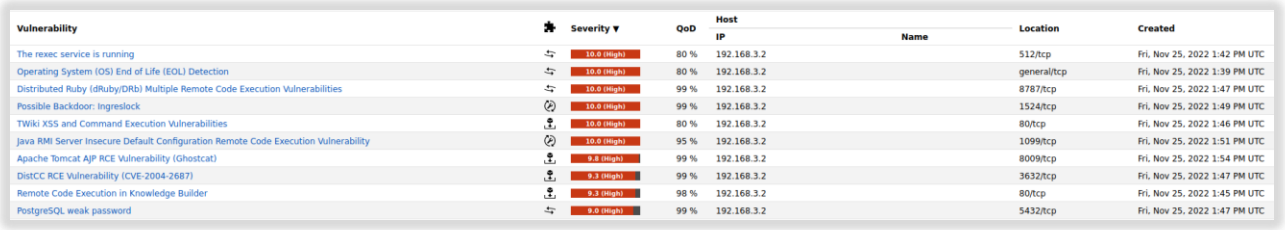


→ a potvrdíte **Save** → skontroluje nastavenie položky **Scan Config= Full and fast**
→ a potvrdíte **Save** → Scans → Spustite skenovanie pomocou **Start**

d. Počas skenovania si môžete pozerať výsledky:
   i. Scans->Results



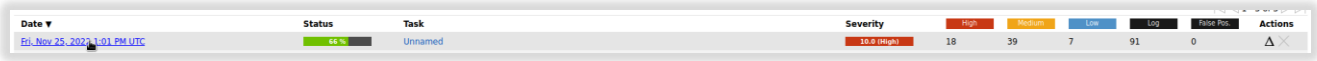
Ukážka nájdených zraniteľností:



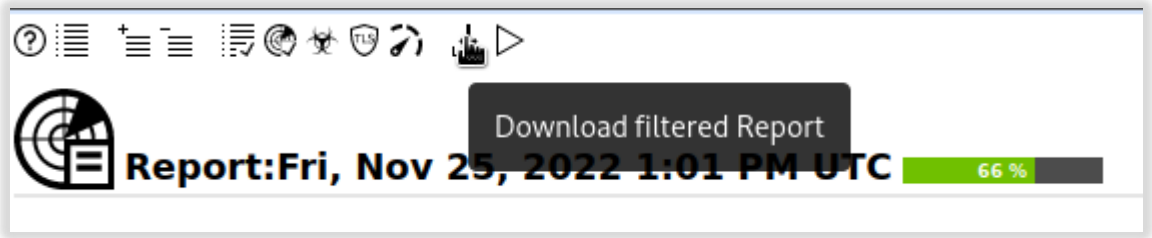
Vulnerability	Severity ▾	QoD	Host IP	Host Name	Location	Created
The rexec service is running	10.0 (High)	80 %	192.168.3.2		512/tcp	Fri, Nov 25, 2022 1:42 PM UTC
Operating System (OS) End of Life (EOL) Detection	10.0 (High)	80 %	192.168.3.2		general/tcp	Fri, Nov 25, 2022 1:39 PM UTC
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	10.0 (High)	99 %	192.168.3.2		8787/tcp	Fri, Nov 25, 2022 1:47 PM UTC
Possible Backdoor: Ingreslock	10.0 (High)	99 %	192.168.3.2		1524/tcp	Fri, Nov 25, 2022 1:49 PM UTC
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80 %	192.168.3.2		80/tcp	Fri, Nov 25, 2022 1:46 PM UTC
Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability	10.0 (High)	95 %	192.168.3.2		1099/tcp	Fri, Nov 25, 2022 1:51 PM UTC
Apache Tomcat AJP RCE Vulnerability (Ghostcat)	9.8 (High)	99 %	192.168.3.2		8009/tcp	Fri, Nov 25, 2022 1:54 PM UTC
DistCC RCE Vulnerability (CVE-2004-2687)	9.3 (High)	99 %	192.168.3.2		3632/tcp	Fri, Nov 25, 2022 1:47 PM UTC
Remote Code Execution in Knowledge Builder	9.3 (High)	98 %	192.168.3.2		80/tcp	Fri, Nov 25, 2022 1:45 PM UTC
PostgreSQL weak password	9.0 (High)	99 %	192.168.3.2		5432/tcp	Fri, Nov 25, 2022 1:47 PM UTC

ii. Počas toho ako bude bežať skenovanie si prezrite zraniteľnosti aké nástroj našiel.
iii. Zistite:
- čo znamenajú jednotlivé ikony v druhom stĺpci vo výslednom výpise so zraniteľnosťami
- aká je stupnica pre závažnosť zraniteľností?
- Vyberte si jednu zraniteľnosť, ktorá vás zaujala, a má uvedené aj CVE ID, a bližšie ju analyzujte.
- Nájdite k danej zraniteľnosti aj odpovedajúce CWE.
- Nájdite pre dané CVE aj záznam v NVD, a informácie o
  - CVSS
  - Technické detaily
  - Ovplyvnené entity
  - Zdroje pre ďalšie preskúmanie informácií
- Vedeli by ste pre danú zraniteľnosť nájsť aj informáciu o hrozbách, ktoré by danú zraniteľnosť mohli využiť? Pokúste sa využiť tak MITRE ATT&CK ako aj CAPEC databázu, prípadne MAEC
- Čo iné zaujímavé vás zaujalo pri výsledkoch?

iv. Keď skenovanie skončí vygenerujte si report, uložte si ho a nahrajte spolu s reportom z cvičenia na Moodle a odprezentujte vyučujúcemu.



Date ▾	Status	Task	Severity	High	Medium	Low	Log	False Pos.	Actions
Fri, Nov 25, 2022 1:01 PM UTC	66 %	Unnamed	10.0 (High)	18	39	7	91	0	



Scans → Reports → Kliknete na dátum skenovania → Otvorí sa vám nová stránka →
→ Kliknite na **Download filtered Report** → Namiesto: **Anonymous XML** vyberiete **PDF** a potvrdíte **OK**

Časť 2: Sumarizácia výsledkov z predošlej časti za celú skupinu

Toto je dobrovoľná úloha za bonusový bod pre členov skupiny.

Pre pridelenú katedru sa pokúste vyprodukovať jeden report a odporúčania, ako by sa malo ďalej s výsledkami reportu pracovať, na odstránení nájdených zraniteľností.

Časť 3: Sken vašej domácej siete a sumarizácia výsledkov

Toto je dobrovoľná úloha za bonusový bod pre každého riešiteľa.

Zrealizujte sken pomocou nástroja OpenVas vo vašej domácej sieti, a s prihliadnutím na to, že ide o vašu domácu sieť, a zistené informácie nemusíte chcieť zdieľať s Moodlom, alebo učiteľom. Zosumarizujte a analyzujte výsledky skenu, a k akým zisteniam ste prišli. Toto nie je nutné dávať do reportu a odovzdať na Moodle, iba ukázať na cvičení učiteľovi a popísať zistenia.