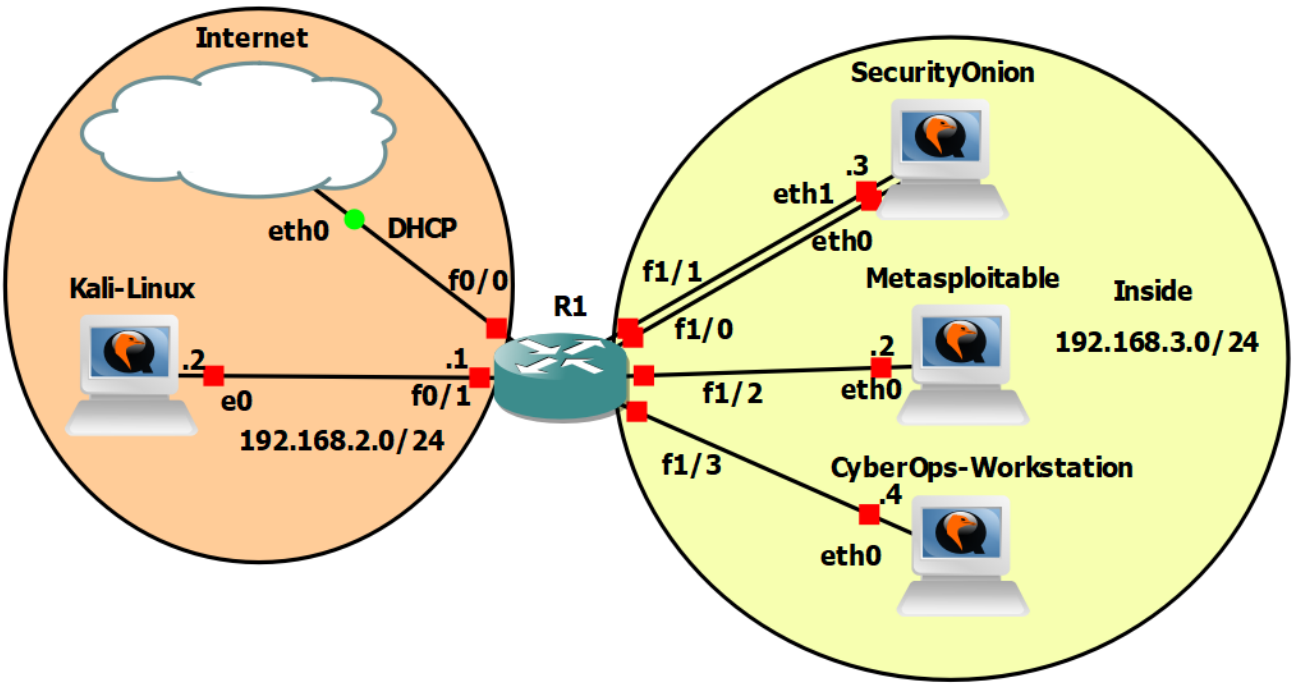
RBI / Cvičenie 09 / **Skenovanie zraniteľností**



Inštrukcie a scenár

V tomto cvičení budete pracovať s nástrojmi, ktoré slúžia na skenovanie zraniteľnosti. V prvej úlohe si predstavíme nástroj **owasp-zap**, ktorý slúži na zisťovanie webových zraniteľnosti. Tento nástroj použijeme na zraniteľnú webovú aplikáciu **Mutillidae.** Ako ďalší nástroj použijete webový skener **nikto.** Následne použijete nástroj **nmap** a skript **vuln,** ktorý slúži na skenovanie zraniteľnosti. Pomocou skriptu **vuln** zistíte zraniteľnosti na zariadení **Metasploit** a v ďalšom cvičení využijete zraniteľnosti, ktoré ste našli.

V druhej časti cvičenia budete v pozícií bezpečnostného analytika, kde vašou úlohou bude analyzovať skenovanie a s nimi spojené útoky vykonané v prvej časti, zistiť o útokoch a skenovaní informácie, a napokon výsledky vedieť vyhodnocovať. Pracovať budete na zariadení Security Onion a s jeho nástrojmi, **snort** a **zeek**, ktoré už s predošlých cvičení poznáte, ale aj s novými nástrojmi ako **sguil** a **kibana**. V samotnom závere sa pozriete na prevenciu niektorých zraniteľností zariadenia **Metasploitable**.

Požiadavky

- Topológia v GNS3 alebo virtuálne zariadenia vo VirtualBox-e
- Úspešne vykonaný **Security Onion Setup** podľa dokumentu **Security Onion Setup - Navod.docx**

Používatelia

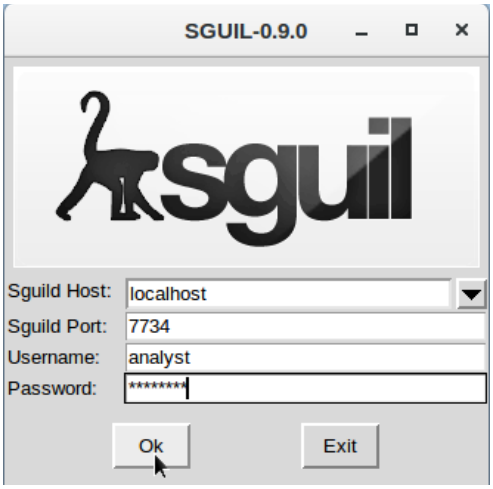
Názov	Meno	Heslo
KALI LINUX	kali	kali
METASPLOITABLE	msfadmin	msfadmin
SECURITY ONION	analyst	cyberops
CYBEROPS WORKSTATION	analyst	cyberops

Časť 0: Duplikácia VM Security Onion a jej nastavenie

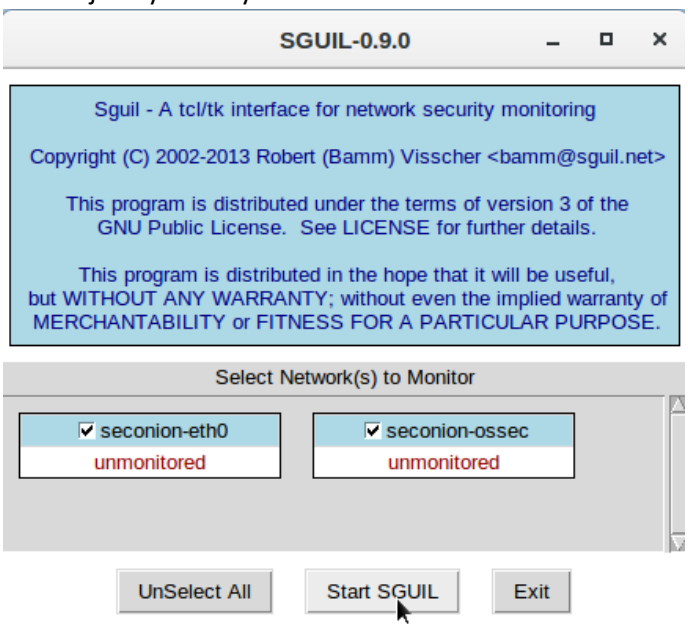
Spravte si vo vašej topológii duplikát zariadenia Security Onion, a zrealizujte preň nastavenia, ktoré máte uvedené v dokumente „Security Onion Setup – Navod.docx“. V jednom čase budete vždy využívať iba jednu inštanciu Security Onion, buď tú s demo údajmi (tá ktorú ste mali doteraz), alebo tú ktorú využijete na monitoring reálnych dát, ale nebudú v nej žiadne demo údaje (tú, ktorú ste si práve pridali). Zapojte do topológie nový Security Onion.

Časť 1: Skenovanie

Túto časť vykonávajte na zariadení Kali Linux. V tejto časti si vyskúšate prácu so skenovacími zariadeniami owasp-zap, nikto a použijete nmap so skriptom vuln. Skenovanie budete smerovať z Kali Linux na Metaspoitable. Pred tým, ako začnete skenovať s nástrojmi **nikto**, **nmap** a **owasp-zap**, spustite zariadenia Metasploitable a Security Onion. Na zariadení Security Onion, spustite nástroj **zeek** a **snort** na „port-mirroring“ rozhraní, rozhranie eth0, a taktiež spustite nástroj **sguil**. Ikona nástroja sguil sa nachádza na pracovnej ploche zariadenia Security Onion. Kliknite dva krát na danú ikonu a zadajte prihlasovacie meno a heslo, ktoré ste pri **Security Onion Setup**-e zvolili (username:priezvisko, password: cyberops) a kliknite na „Ok“.



Následne vyberáte rozhrania pre monitorovanie, kde môžete vybrať obidva z dostupných rozhraní, ale hlavné je aby bolo vybrané **seconion-eth0**. Môžete teda zvoliť **Select All** a zapnúť sguil cez **Start SGUIL**.



V časti 3. budete analyzovať skenovacie útoky z pohľadu bezpečnostného analytika na jednotlivých nástrojoch, ktoré ste ešte pred skenovaním zapli.

Niektoré skeny v bodoch 1.-3. sú časovo náročnejšie, hlavne skenovanie pomocou skriptu **vuln** na **nmap-e**, a tiež skenovanie s nástrojom **owasp-zap**. Preto počas vykonávania týchto skenov, namiesto čakania na ich koniec, môžete prejsť na časť 2. a analyzovať priebežne ich detekciu na zariadení Security Onion.

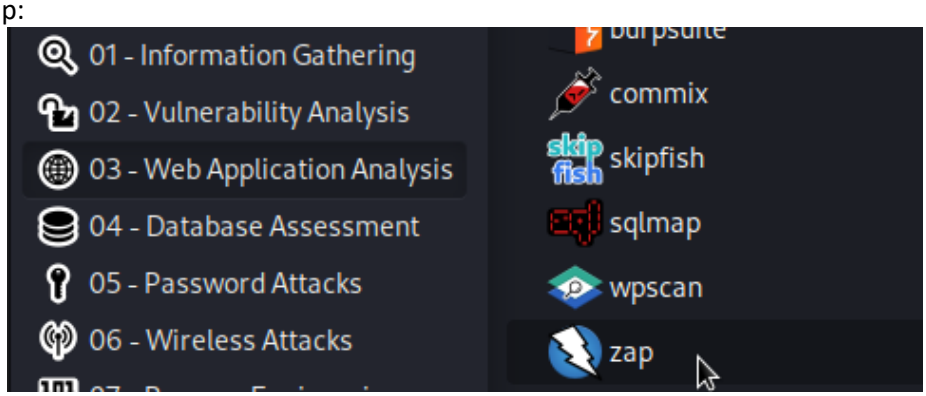
Upozornenie: Ak pracujete vo VirtualBox-e, skenovanie v tejto časti vykonajte aj na IP adresu pre Security Onion, nie len pre Metasploitable. A to z toho dôvodu, aby ste mohli vykonávať časť 2., analýzu detekcie skenovania s nástrojmi Security Onion-u. Taktiež zariadenia **snort** a **zeek** spustite na rozhraní, ktoré používa Security Onion ako manažovacie, aby ste mohli analyzovať útoky a skenovania voči samotnému Security Onion-u.

1. **Inštalácia nástroja owasp-zap**
   Upozornenie: Bod **b.** je časovo náročný, a preto je potrebné aby ste ho vykonali, v prípade práce na vzdialenom školskom serveri, dopredu, pred cvičením (t.j. nerobili to viacerí naraz).
   a. Je potrebné aby ste si najskôr upravili zdrojový súbor pre nástroj **apt**, ktorý spravuje balíčky
      - Otvorte si zdrojový súbor ako root : `$ sudo nano /etc/apt/sources.list`
      - Odkomentujte posledný riadok v súbore, tak aby bol váš stav súboru nasledovný:

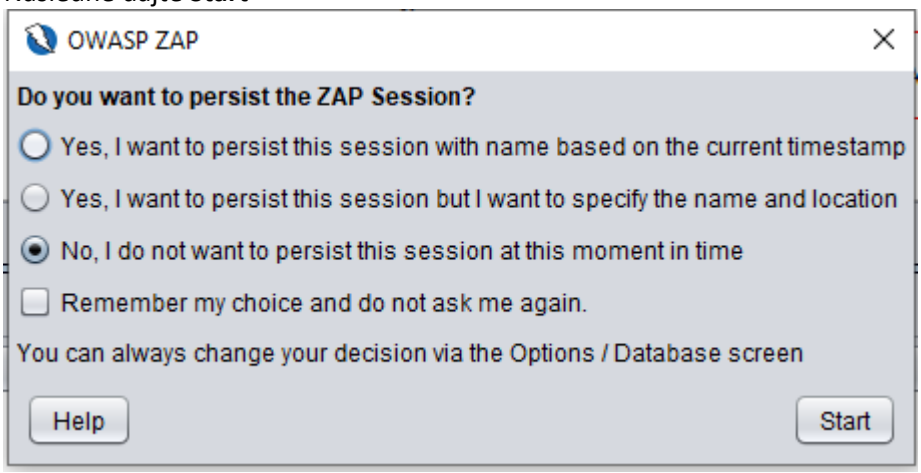
```
# See https://www.kali.org/docs/general-use/kali-linux-sources-list-reposito>
deb http://http.kali.org/kali kali-rolling main contrib non-free

# Additional line for source packages
deb-src http://http.kali.org/kali kali-rolling main contrib non-free
```

   b. Vykonajte update balíčkov systému: `$ sudo apt update`
   c. Inštalujte owasp-zap: `$ sudo apt install zaproxy`
2. **Skenovanie webových zraniteľností pomocou nástroja owasp-zap**

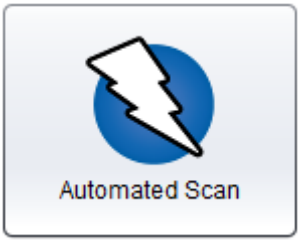
a. Spustime aplikáciu **owasp-zap**: Vľavo hore Applications -> 03 - Web Application Analysis -> zap:



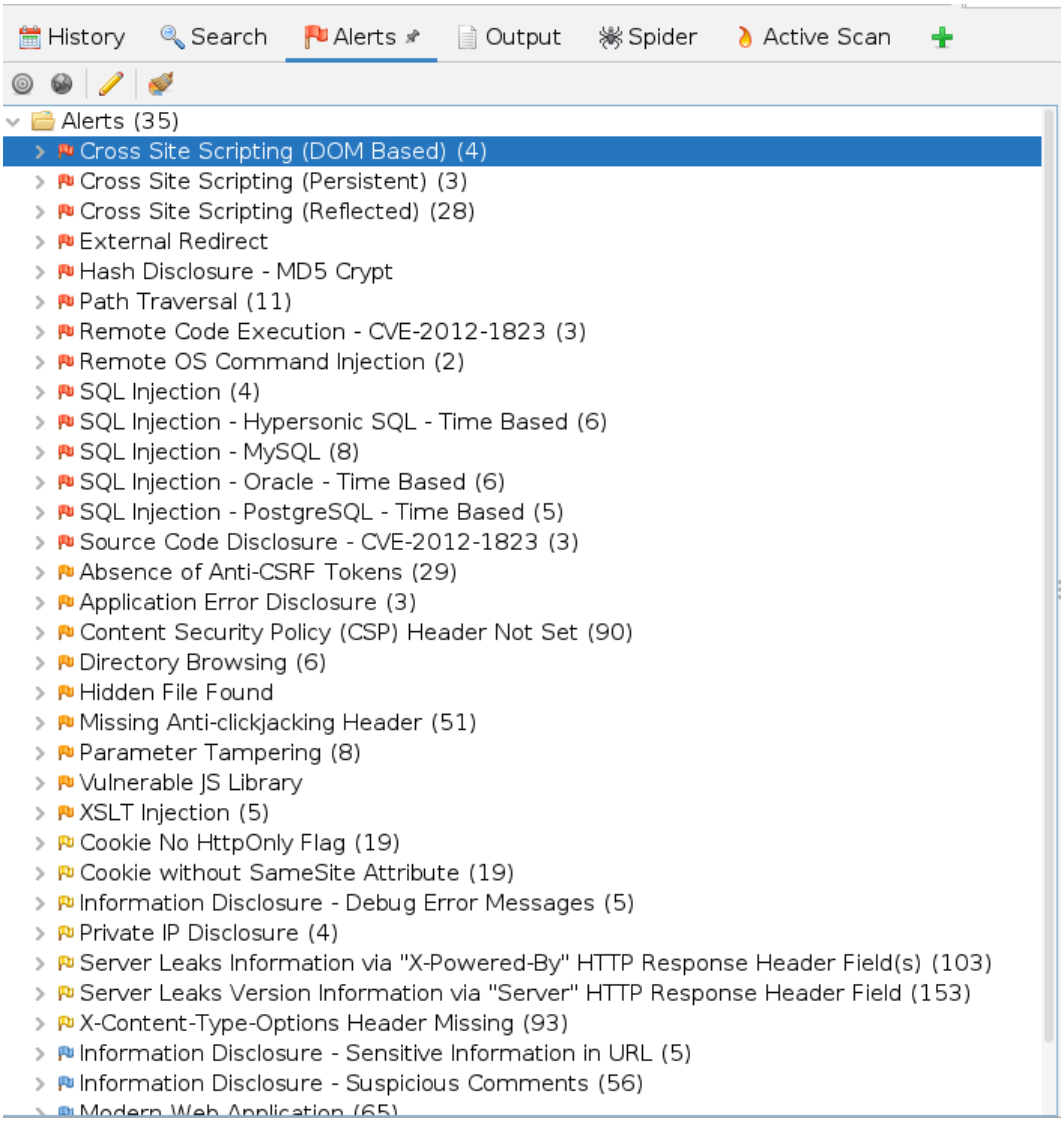
b. Následne dajte **Start**



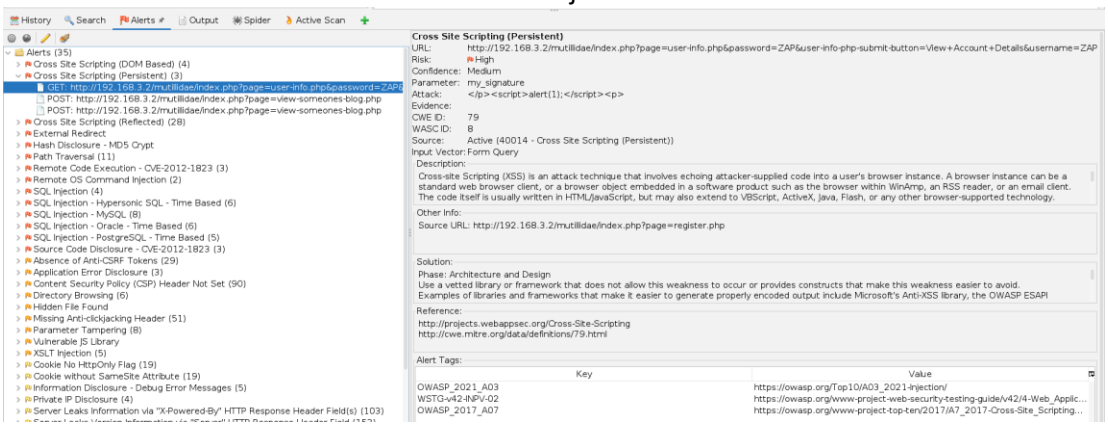
c. Kliknite na **Automated Scan**



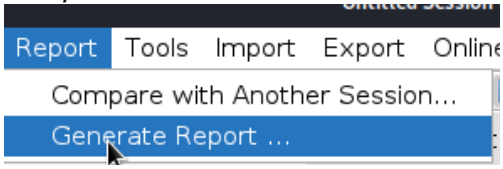
d. Do URL adresy zadajte: http://192.168.3.2/mutillidae/
e. Dajte **Attack**
f. Skenovanie bude trvať dlhšie
g. Zatiaľ sa presuňte na ďalší nástroj po skončení skenovania si pozrite výsledky. Výsledky skenovania môžete vidieť, keď kliknete na tlačidlo **Alerts:**



h. Následne si môžete kliknúť na konkrétnu nájdenú zraniteľnosť:



i. Výsledok skenovania si môžete uložiť ako report:



j. Vygenerujte si HTML Report

3. **Skenovanie zraniteľnosti pomocou nástroja nikto**
   a. Otvorte terminál a zadajte príkaz: `nikto -h`
      i. Pomocou tohto príkazu sa vám zobrazia prepínače, ktoré podporuje nástroj nikto
   b. Vytvorte si priečinok **ScanningVulnerabilities** do adresára `/home/kali/Documents`
   c. Choďte do priečinka `/home/kali/Documents/ScanningVulnerabilities` a spustite skenovanie **nikto** ako **root** s prepínačmi:
      i. `-h 192.168.3.2`
      ii. `-output nikto_scan.txt`
   d. Výsledok skenovania sa vám uloží do súboru `nikto_scan.txt`
   e. Otvorte si prehliadač na svojom počítači
      i. Bohužiaľ stránka OVSBD.org bola zrušená. Zraniteľnosti, ktoré ste našli, si však môžete pozrieť na stránke:
         - https://cve.mitre.org/data/refs/refmap/source-OSVDB.html
      ii. Taktiež pre viacej informácií o zraniteľnosti, môžete skopírovať jej referenčné OVSBD číslo a vyhľadať info na internete
   f. Následne použite nastroj **nikto** a spustite skenovanie na stránku http://192.168.3.2/mutillidae a výsledok uložte do súboru `nikto_scan_mutillidae.txt`
      i. `nikto -h` http://192.168.3.2/mutillidae -output nikto_scan_mutillidae.txt

4. **Skenovanie zraniteľností pomocou nástroja nmap**
   a. Otvorte si terminál a použite nástroj **nmap** ako **root** so skriptov `vuln`, ktorý slúži na zisťovanie zraniteľnosti a skenovanie si uložte do súboru. Použite jednotlivé argumenty:
      i. `192.168.3.2`
      ii. `--script=vuln`
      iii. `-o meno_suboru`
   b. Vo výsledku si všimnite zraniteľnosť na porte 21:

```
# Nmap 7.70 scan initiated Mon May 11 03:16:39 2020 as: nmap --script=vuln -o nmap_scan 192.168.3.2
Nmap scan report for 192.168.3.2
Host is up (0.11s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  OSVDB:73573  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/
vsftpd_234_backdoor.rb
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|_      http://osvdb.org/73573
|_sslv2-drown:
```

   c. Otvorte si prehliadač na svojom PC a prejdite na stránku: https://cve.mitre.org/cve/search_cve_list.html
   d. Vložte tam túto zraniteľnosť, ktorú ste našli na porte **21/tcp**: `CVE-2011-2523`
   e. Na ďalšom cvičení túto zraniteľnosť využijete pomocou nástroja **metasploit**

Časť 2: Detekcia skenovania a ich analýza na zariadení Security Onion

V tejto časti budete pracovať v roli bezpečnostného analytika, ktorého úlohou je, aby detegoval a zachytil neoprávnené útoky a skenovania. Budete pracovať s nástrojmi, ktoré dokážu zachytiť útoky a skenovania, a následne ich spracovať, vyhodnotiť. Nástroje, ktoré budete používať v tejto časti zahŕňajú: **zeek**, **snort**, **sguil** a **kibana**.

*„Sguil (pronounced sgweel) is built by network security analysts for network security analysts. Sguil's main component is an intuitive GUI that provides access to realtime events, session data, and raw packet captures. Sguil facilitates the practice of Network Security Monitoring and event driven analysis. The Sguil client is written in tcl/tk and can be run on any operating system that supports tcl/tk (including Linux, *BSD, Solaris, MacOS, and Win32).“*

„Kibana is an open source browser based visualization tool mainly used to analyze large volume of logs in the form of line graph, bar graph, pie charts, heat maps, region maps, coordinate maps, gauge, goals, timelion etc. The visualization makes it easy to predict or to see the changes in trends of errors or other significant events of the input source.“

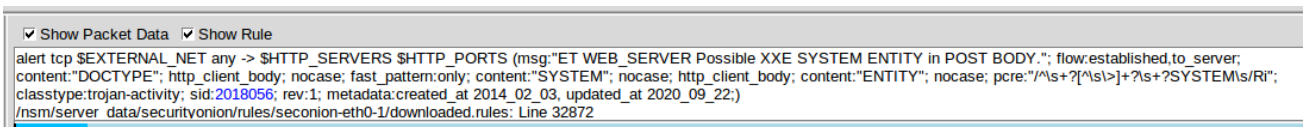
Upozornenie: Ak pracujete vo VirtualBox-e, analyzujete skenovanie uskutočnené voči Security Onion-u, keďže nemáte nakonfigurovaný „port-mirroring“.

1. **Sguil - Analýza**
    a. Prezrite si hlásenia, ktoré vám sguil vygeneroval v rámci uskutočneného skenovania
        i. Identifikujte hlásenia, ktoré sa týkajú skenovania z Kali Linux-u voči Metasploitable.
        ii. Podľa čoho dokážete identifikovať dané hlásenia?
    b. Preskúmajte konkrétne hlásenie
        i. V tomto bode si preskúmate konkrétne hlásenie vygenerované nástrojom **sguil**. Jedná sa o hlásenie vygenerované počas skenovania s nástrojom owas-zap. Hlásenie sa týka webového útoku XXE (xml external entity)

            Upozornenie: Dané hlásenie bude vygenerované na základe skenovania nástrojom owas-zap, a teda je potrebné, aby tento skener bol zapnutý dostatočne dlho, najlepšie až do ukončenia jeho skenovania, aby bolo dané hlásenie vygenerované v sguil-e

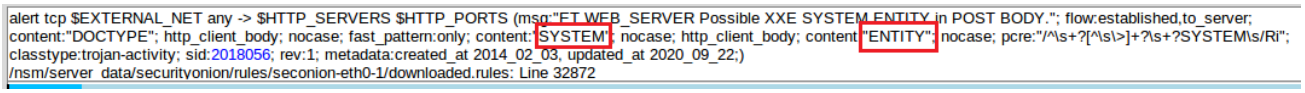
192.168.2.2	58258	192.168.3.2	80	6	ET WEB_SERVER Possible CVE-2014-6271 Attempt
192.168.2.2	37556	192.168.3.2	445	6	GPL NETBIOS SMB-DS IPC$ share access
192.168.2.2	51286	192.168.3.2	80	6	ET WEB_SERVER Possible XXE SYSTEM ENTITY in POST BODY.
192.168.2.2	44136	192.168.3.2	5815	6	ET SCAN Potential VNC Scan 5800-5820
192.168.2.2	44136	192.168.3.2	1433	6	ET SCAN Suspicious inbound to MSSQL port 1433
192.168.2.2	44136	192.168.3.2	1521	6	ET SCAN Suspicious inbound to Oracle SQL port 1521

        ii. V pravej dolnej časti sguil-u, zaškrtnite polia **Show Packet Data** a **Show Rule**, pre zobrazenie hlásenia podrobnejšie

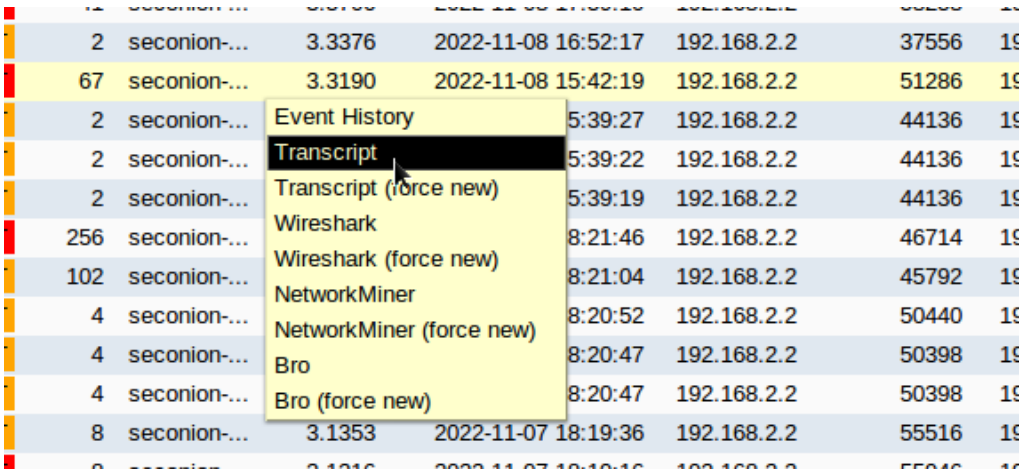


        iii. Všimnite si, že IDS pravidlá zistili prítomnosť webového útoku XXE na základe toho, že žiadosti odosielané na Metaspoitable, v rámci tohto útoku, obsahujú v tele

žiadosti kľúčové slová **SYSTEM** a **ENTITY.** Pri webovom útoku XXE sa tieto príkazy zadávajú ako súčasť škodlivého kódu



iv. Kliknite pravým tlačidlom myši na danú hlášku v squil-e a vyberte možnosť **Transcript**



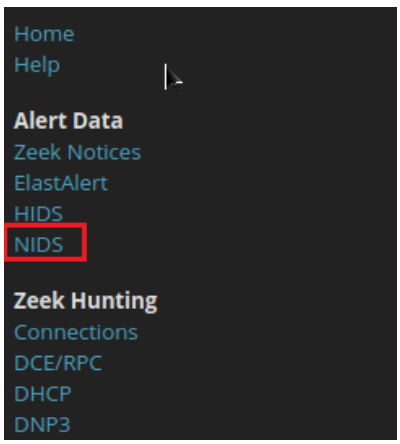
v. Otvorí sa vám nové okno, v ktorom žiadosti na Metasploitable server sú modrou a odpovede sú červenou. Nájdite žiadosť v ktorej nájdete v tele príkazy **SYSTEM** a **ENTITY.** Jedná sa konkrétne o XXE webový útok, ktorý sa snaží zobraziť obsah súboru **/etc/passwd** na zariadení Metasploitable. Skúste túto žiadosť nájsť aj u seba. Skúste odpovedať, či bol daný útok úspešný alebo nie.

vi. Podobnou logikou preskúmajte aj ďalšie vygenerované hlásenia, ktoré boli identifikované sguil-om počas skenovania zariadenia Metasploitable

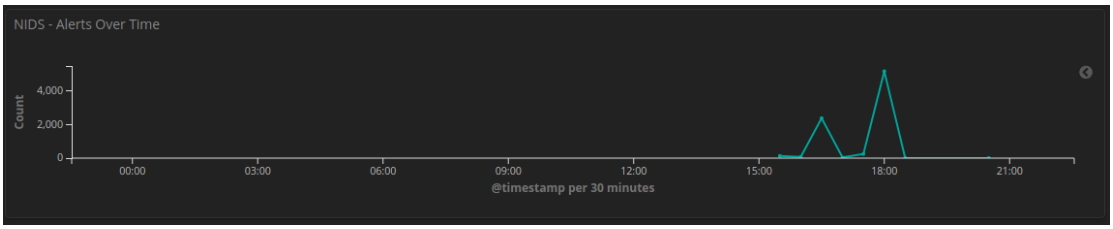
2. Kibana - Analýza

a. Na pracovnej ploche sa nachádza ikona tohto nástroja, spustite nástroj. Otvorí sa vám webový prehliadač v ktorom sa vám spustí Kibana. Prihláste sa rovnakými prihlasovacími údajmi ako do sguil-u. Otvorí sa vám **Dashboard**, kde v ľavom **Navigation** poli si vyberte **NIDS** (Network Intrusion Detection System), ktorý slúži práve na zachytávanie útokov a skenovaní pre naše monitorovacie rozhranie eth0

i. Upozornenie: Ak pracujete vo VirtualBox-e vyberáte si **HIDS,** ktorý zachytáva útoky a skenovania voči samotnému Security Onion-u

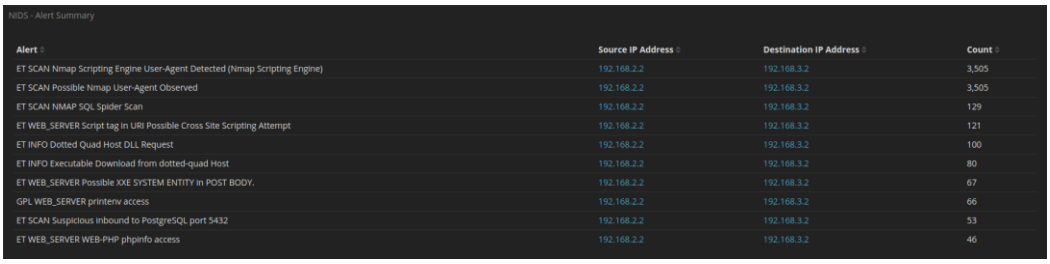


b. Vpravo hore si všimnite pole **NIDS – Alerts Over Time**, v ktorom nájdete časovú os zobrazujúcu počet zachytených hlásení v závislosti od času. Ako analytik viete teda určiť čas útokov a skenovaní, a tiež celkový počet vygenerovaných hlásení s nimi spojenými. Váš graf sa bude líšiť od grafu na obrázku nižšie, keďže časť 1. v tomto cvičení môžete vykonávať v inom časovom intervale



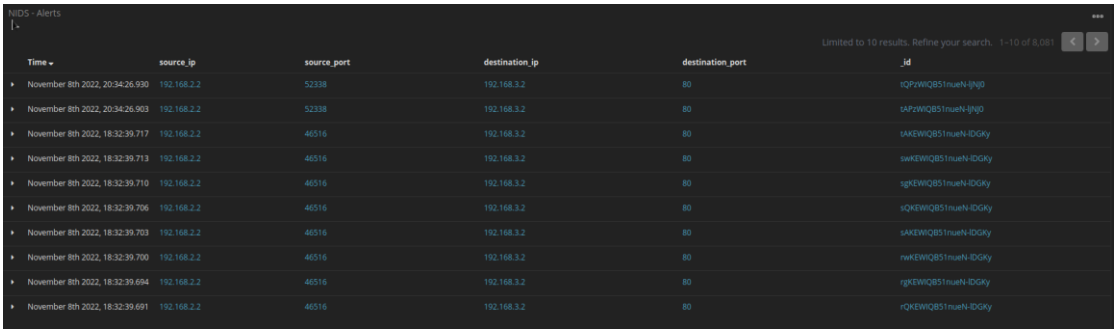
c. Ďalej na tej istej stránke nájdete v poli **NIDS Alerts - Category** histogram, zobrazujúci typ hlášok a ich pomer. Keďže v našom prípade, v časti 1. v cvičení sme vykonávali hlavne skenovanie, môžeme vidieť aj na grafe, že hlášky spojené práve so skenovaním boli identifikované najviac. Ďalej prevládajú hlášky spojené s webovým serverom. Viete povedať prečo je tomu tak? Čo iné zaujímavé ste si všimli?

d. V poli **NIDS – Alert Summary** môžete vidieť početnosť pre jednotlivé kategórie hlásení ako aj cieľovú IP adresu a zdrojovú IP adresu. Viete teda ako bezpečnostný analytik určiť IP adresu útočníka a tiež IP adresu servera, na ktorý smeruje svoje útoky, a na základe týchto informácií môžete útočníkovu IP adresu zablokovať. Na základe vašich pozorovaní z výstupu v tomto poli Alert Summary, ktoré kategórie hlásení dominujú a prečo? Pozrite sa aj na ďalšie hlášky a ich početnosti.



Alert	Source IP Address	Destination IP Address	Count
ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	192.168.2.2	192.168.3.2	3,505
ET SCAN Possible Nmap User-Agent Observed	192.168.2.2	192.168.3.2	3,505
ET SCAN NMAP SQL Spider Scan	192.168.2.2	192.168.3.2	129
ET WEB_SERVER Script tag in URI Possible Cross Site Scripting Attempt	192.168.2.2	192.168.3.2	121
ET INFO Dotted Quad Host DLL Request	192.168.2.2	192.168.3.2	100
ET INFO Executable Download from dotted-quad Host	192.168.2.2	192.168.3.2	80
ET WEB_SERVER Possible XXE SYSTEM ENTITY in POST BODY.	192.168.2.2	192.168.3.2	67
GPL WEB_SERVER printenv access	192.168.2.2	192.168.3.2	66
ET SCAN Suspicious inbound to PostgreSQL port 5432	192.168.2.2	192.168.3.2	53
ET WEB_SERVER WEB-PHP phpinfo access	192.168.2.2	192.168.3.2	46

e. V dolnej časti nájdete **NIDS – Alerts** v ktorej nájdete samotné hlásenia zobrazené od najskorších.



f. Kliknite na trojuholník nachádzajúci sa na ľavej strane vedľa času vášho hlásenie, ktoré je na najvyššom mieste. Takto si otvoríte vaše hlásenie a dozviete sa o ňom podrobnejšie informácie, ako napríklad: názov hlásenia, kategóriu, klasifikáciu, typ eventu a správu hlásenia. Aké informácie ste sa dozvedeli z vášho konkrétneho hlásenia?

3. **Snort a Zeek - Analýza**
    a. Obidva nástroje ste si mali zapnúť v časti 1. tohto cvičenia, takže teraz si ich môžete zastaviť
    b. S týmito nástrojmi ste sa už naučili pracovať na predošlých cvičeniach a teda samotná analýza jeho výsledkov a výstupov bude vo vašej réžií
    c. Porovnajte výsledky aj s výsledkami, ktoré ste už získali a analyzovali vyššie.

Časť 3: Nájdenie a odstránenie zraniteľností

Podobne ako útočník, aj analytik môže použiť rovnaké nástroje, pre vyhľadanie sieťových zraniteľností. Analytik môže následne prijať opatrenia, ktorými bude predchádzať zneužitiu týchto zraniteľností.

1. Zvoľte postup na odstránenie zraniteľnosti
    a. Zablokujte otvorený port
        i. `iptables -A INPUT -p -tcp –dport 21 -j DROP`
            - Ak chceme zablokovať FTP prístup úplne na serveri
        ii. `iptables -A INPUT -p -tcp -s <ip address> –dport 21 -j DROP`
            - Ak chceme zablokovať len konkrétnu ip adresu
        iii. `iptables -I INPUT -p tcp -s <ip address / netmask> --dport 21 -j DROP`
            - Ak chceme zablokovať celý subnet
    b. Po aplikovaní pravidiel treba uložiť a resetovať iptables
        i. `/etc/init.d/iptables save`
        ii. `/etc/init.d/iptables restart`
    c. Aké iné bezpečnostné opatrenia by bolo možné nasadiť, na mitigáciu daných zraniteľností?