

Wprowadzenie do cyberbezpieczeństwa (WCYB)

Moduł 2: Podstawy teleinformatyki dla cyberbezpieczeństwa | Cyberbezpieczeństwo ofensywne - skanowanie

Semestr: 19Z

Plan laboratorium

Podczas tego laboratorium:

- zapoznasz się z podstawami teleinformatyki niezbędnymi dla realizacji podstawowych i zaawansowanych zadań cyberbezpieczeństwa systemów i sieci
- zapoznasz się z technikami skanowania
- zapoznasz się z narzędziami do skanowania portów, usług i podatności

1. Podstawy teleinformatyki dla cyberbezpieczeństwa

1.1 Zagadnienia teoretyczne

Materiał od Prowadzącego będzie przekazany oddzielnie

1.2 Programowanie sieciowe w Pythonie

<https://realpython.com/python-sockets/>

1.2.1 Czym są sockety (gniazda)?

Gniazdo to mechanizm umożliwiający zestawienie kanału komunikacji pomiędzy hostami. Gniazdo jest obiektem zbliżonym do pliku i ma charakter procesu systemowego, który pozwala na m.in. ustanawianie połączeń, czy odbieranie danych (z wykorzystaniem odpowiednich protokołów). Każde gniazdo posiada określony adres IP oraz numer portu. Dwa podstawowe rodzaje wymienianych danych przez sockety to:

- strumienie (segmenty TCP) – czyli „stream sockets” – te gniazda wysyłają dane za pomocą protokołu TCP, co oznacza otworenie kanału komunikacji na określonym porcie, dane wysyłane są w segmentach TCP, gniazdo (socket) nie zamyka połączenia i oczekuje na odpowiedź od hosta docelowego. Przykładem usługi korzystającej z TCP jest HTTP (HyperText Transfer Protocol, port 80 – gdy przeglądarka internetowa chce pobrać treści z serwera WWW, robi to poprzez zestawienie kanału komunikacji TCP na porcie 80);
- datagramy (datagramy UDP) – są to tzw. „datagram sockets” – ten kanał komunikacji wykorzystuje protokół UDP, co sprawia, że połączenie jest bezstanowe. Gniazdo wysyła datagram UDP do docelowego hosta/portu i nie sprawdza, czy komunikacja zakończyła się powodzeniem. Przykładem usługi działającej z użyciem UDP jest DNS (Domain Name Server, port 53);

Do ćwiczeń tego zagadnienia proponujemy zastosowanie języka programowania Python. Na przestrzeni lat wiele narzędzi dla zadań cyberbezpieczeństwa napisano w tym języku lub

dodano możliwość skryptowania do narzędzi pisanych w innych językach (przede wszystkim C oraz C++).

Moduł `socket` dostarczony standardowo z interpreterem Pythona umożliwia bezpośredni dostęp do standardowego interfejsu dla gniazd (*gniazda BSD* - https://en.wikipedia.org/wiki/Berkeley_sockets), który wykorzystywany jest w większości współczesnych systemów operacyjnych.

Na zaprogramowanie funkcji serwera składa się:

- utworzenie gniazda,
- przypisanie gniazda do adresu IP i portu (rezerwacja zasobów w systemie),
- nasłuchiwanie nadchodzących połączeń,
- oczekiwanie klientów,
- zaakceptowanie klienta,
- wysyłanie i odbieranie danych.

By następnie zaprogramować aplikację klienta (klientem jest np. przeglądarka www lub aplikacja desktopowa) wymagane jest:

- utworzenie gniazda,
- połączenie się z serwerem
- wysyłanie i odbieranie danych

Interfejs BSD dla gniazd określa kilka typów rodzin adresów, przy czym najpopularniejszy jest `AF_INET`. Gniazdo IPv4 to gniazdo pomiędzy dwoma procesami, potencjalnie działającymi na dwóch maszynach używające adresacji IPv4. W Pythonie gniazda IPv4 reprezentowane są w postaci krotki (ang. *tuple*) (`host, port`), gdzie `host` to łańcuch a `port` to liczba całkowita - numer portu. Jako `host` można podać adres IPv4 np. `192.168.1.15`, adres URL np. `www.google.pl` czy nazwę domenową np. `localhost`,.

Aby stworzyć w Pythonie gniazdo należy użyć metody `socket()`, która domyślnie tworzy gniazdo TCP typu `AF_INET`. Metoda ta zwraca obiekt `socket`, który można użyć w celu wykonania na nim metod takich jak `bind()`, `listen()`, `accept()` lub `connect()`.

1.2.2 Prosta komunikacja klient-serwer.

Kod serwera znajduje się w pliku `tcp_serv.py`, kod klienta w pliku `tcp_client.py`.

2. Skanowanie

Po zakończeniu pasywnego gromadzenia informacji drugim zadaniem w realizacji zadań cyberbezpieczeństwa ofensywnego jest skanowanie. Etap zbierania informacji powinien być możliwie kompletny, gdyż pozwala zaplanować najlepszą lokalizację (domeny, sieci, podsieci itp.) oraz cele do skanowania. Skanowanie to proces lokalizowania systemów (hosty, urządzenia sieciowe, mobilne itp.), które są aktywnie działające i reagują na zapytania w sieci. Etyczni hakerzy wykorzystują skanowanie do zebrania takich danych jak:

1) adresy IP (v4/v6) systemów; 2) wersje systemów operacyjnych działających na urządzeniach; 3) uruchomione i dostępne usługi, aplikacje (także ich wersje); itp.

Na podstawie tych danych pentester może dobrać odpowiedni *arsenał* do realizacji zadania, jakim będzie przełamanie systemu i jego przejęcie. Przełamanie systemu

wykonuje się za pomocą złośliwego kodu określanego mianem *exploita*. Eksploatację systemów będziemy zajmować się w Module 3 niniejszego Laboratorium z Wprowadzenia do Cyberbezpieczeństwa.

Tabela poniżej prezentuje typy skanowania:

Typ skanowania	Cel skanowania
Skanowanie portów	Określenie otwartych portów i usług
Skanowanie sieci	Identyfikacja adresów IP w sieci i podsieci
Skanowanie podatności	Identyfikacja znanych podatności w skanowanym celu

2.1 Skanowanie portów i usług

Skanowanie portów to proces identyfikowania otwartych i dostępnych portów protokołów TCP oraz UDP w systemach operacyjnych. Narzędzia do skanowania portów umożliwiają także poznanie usług dostępnych w danym systemie, gdyż każda usługa lub aplikacja jest powiązana z dobrze znanym numerem portu.

Numery portów są podzielone na trzy zakresy:

- Porty usług standardowych dla sieci TCP/IP: 0-1023
- Porty zarejestrowane: 1024-49151
- Porty dynamiczne: 49152-65535

Sposób działania podstawowych narzędzi do skanowania portów bezpośrednio identyfikuje znane (standardowe) porty jako przypisane do nich usługi, np. gdy port 80 jest otwarty, to skaner określi, że w danym systemie działa serwer WWW. Specjaliści ds. bezpieczeństwa teleinformatycznego muszą znać dobrze znane numery portów. Popularnymi portami są:

Protokół aplikacyjny/usługa	Protokół transportowy	Numer portu
FTP	TCP	21
SSH	TCP	22
Telnet	TCP	23
DNS	UDP (TCP)	53
DHCP Server	UDP	67
HTTP	TCP	80
HTTPS	TCP	443

W cyberbezpieczeństwie defensywnym odkrycia takie jak:

- usługi (aplikacje) na niestandardowym dla siebie porcie
- wcześniej niewidzianej usługi na znanym bądź nieznanym porcie
- przekłamania monitora sieci - np. określenie z góry, że na porcie 80 działa serwer WWW (HTTP), kiedy stan faktyczny jest inny

są popularnymi anomaliami. Takie sygnały są analizowane ręcznie lub automatycznie w celu ustalenia stanu faktycznego.

Zaawansowane analizatory ruchu sieciowego potrafią na podstawie ruchu sieciowego określić jaka usługa jest faktycznie uruchomiona pod danym portem, bez odwoływania się do katalogów usług.

2.1.1 Skanowanie portów za pomocą narzędzia nmap

Nmap to bezpłatne narzędzie typu open source, które szybko i skutecznie wykonuje komendy ping, skanowanie portów, identyfikację usług, wykrywanie adresów IP i wykrywanie systemu operacyjnego. Zaletą Nmap jest skanowanie dużej liczby maszyn w jednej sesji. Jest obsługiwany przez wiele systemów operacyjnych, w tym Unix, Windows i Linux. Stan portu określony przez skanowanie nmap może być **otwarty (open)**, **filtrowany (filtered)** lub **niefiltrowany (unfiltered)**. Otwarty oznacza, że skanowany zasób akceptuje przychodzące żądanie na tym porcie. Filtrowany oznacza, że zaporą sieciową lub filtr sieciowy monitorują port i uniemożliwiają narzędziu Nmap wykrycie, czy jest on otwarty. Brak filtrowania oznacza, że port jest zamknięty, a żadna zaporą sieciową ani filtr nie koliduje z żądaniami Nmap. Nmap obsługuje kilka rodzajów skanowania. Poniższa tabela przedstawia niektóre popularne metody skanowania.

Pełna dokumentacja rodzajów skanowań: <https://nmap.org/book/man-port-scanning-techniques.html>

Typ skanowania nmap	Opis
TCP connect	Podczas skanowania nawiązywane jest pełne połączenie TCP z systemem docelowym. Najbardziej niezawodny typ skanowania, ale także najbardziej wykrywalny. Odpowiedzią przy otwartym porcie jest SYN/ACK, a odpowiedzią przy zamkniętym porcie jest RST/ACK.
XMAS tree scan	Atakujący sprawdza usługi TCP, wysyłając pakiety XMAS: FIN, URG i PSH. Jeśli port jest otwarty nie będzie żadnej odpowiedzi. Zamknięte porty odpowiadają flagą RST. Skanowanie to jest podobne do skanowania z ustawioną opcją FIN
SYN stealth scan	Jest to również znane jako <i>skanowanie półotwarte</i> (half-open scanning), ponieważ sesja nawiązywania połączenia TCP nie przebiega do końca (SYN-SYN/ACK-ACK). Atakujący wysyła pakiet SYN i odbiera SYN-ACK z powrotem z serwera. Komunikacja jest niepełna, ponieważ pełne połączenie TCP nie jest otwarte. Odpowiedź na otwarte porty za pomocą SYN/ACK, a odpowiedź na zamknięte porty RST/ACK
Null scan	Jest to zaawansowany rodzaj skanowania, który może być w stanie przejść przez zapory sieciowe (firewall) niezauważony lub zmodyfikowany. Skanowanie typu null ma wszystkie flagi wyłączone lub nieustawione. Działa tylko na systemach Unix. Zamknięte porty zwracają flagę RST.
Windows scan	Ten typ skanowania jest podobny do skanowania ACK i może również wykrywać otwarte porty
ACK scan	Ten typ skanowania służy do mapowania reguł zapory. Skanowanie ACK działa tylko w systemie Unix. Port jest uważany za filtrowany według reguł zapory, jeśli w wyniku skanowania ACK zostanie odebrany komunikat nieosiągalnego miejsca docelowego ICMP.

Polecenie nmap ma wiele opcji do wykonywania różnych rodzajów skanowania. Poniżej przedstawiono niektóre z nich:

Opcja skanowania nmap	Przeprowadzany typ skanowania
-sT	TCP connect scan
-sS	SYN scan
-sF	FIN scan
-sX	XMAS tree scan
-sN	Null scan
-sP	Ping scan
-sU	UDP scan
-sA	ACK scan
-sW	Windows scan

Aby wykonać skanowanie nmap, w wierszu polecenia systemu Windows wpisz Nmap , a następnie dowolne opcje polecenia używane do wykonywania określonego rodzaju skanowania. Na przykład, aby przeskanować host za pomocą adresu IP 192.168.0.1 za pomocą typu skanowania TCP connect, wprowadź następującą komendę:

```
nmap 192.168.0.1 -sT
```

Domyślny skan TCP nmap skanuje 1000 najpopularniejszych portów na danym komputerze, zatem należy pamiętać aby przy skanowaniu większej liczby dodać odpowiednią opcję (-p 1- lub -p <nr portu 1>, <nr portu 2>, ...,)

Typy skanowania TCP są oparte na trójstronnym uzgadnianiu TCP. Połączenia TCP wymagają trójetapowego uzgadniania przed nawiązaniem połączenia i przesłaniem danych między nadawcą a odbiorcą. Aby ukończyć trójetapowe uzgadnienie i nawiązać udane połączenie między dwoma hostami, nadawca musi wysłać pakiet TCP z ustawionym bitem synchronizacji (SYN). Następnie system odbierający odpowiada pakietem TCP z ustawionym bitem synchronizacji (SYN) i potwierdzenia (ACK), aby wskazać, że host jest gotowy do odbioru danych. System źródłowy wysyła końcowy pakiet z ustawionym bitem ACK, aby wskazać, że połączenie zostało zakończone, a dane są gotowe do wysłania, ponieważ TCP jest protokołem zorientowanym na połączenie, procesem nawiązywania połączenia (trójetapowe uzgadnienie), restartującym nieudane połączenie, a zakończenie połączenia jest częścią protokołu. Te powiadomienia protokołu są nazywane flagami. TCP zawiera flagi ACK, RST, SYN, URG, PSH i FIN. Poniższa lista przedstawia funkcje flag TCP:

- SYN (Synchronize) Inicjowanie połączenia pomiędzy hostami
- ACK Acknowledge) Ustanowienie połączenie połączenia pomiędzy hostami
- PSH (Push) System przekazuje buforowane dane
- URG (Urgent) Dane w pakietach muszą być szybko przetwarzane
- FIN (Finish) Koniec transmisji
- RST (Reset) Reset połączenia

Ćwiczenia

1. Za pomocą skanera nmap wykonać skanowania TCP connect oraz skanowanie SYN dla hosta metasploitable

2. Za pomocą skanera `nmap` spróbuj przeskanować port 139 różnymi sposobami. Czy wszystkie dają te same wyniki? Z czego to wynika?
3. Na hoście `metasploitable` wprowadź komendę: `iptables -A INPUT -p tcp -m multiport --dports 25,445 -j DROP` a następnie uruchom skanowanie. Czym teraz różnią się wyniki? (Po zakończeniu ćwiczenia wprowadź komendę: `iptables -F`)
4. Za pomocą skanera `nmap` określ system operacyjny i wersję usług hosta `metasploitable`.

2.2 Skanowanie sieci

Skanowanie sieci to procedura identyfikowania aktywnych hostów w sieci, które będą podlegać dalszym operacjom cyberbezpieczeństwa. Hosty są identyfikowane według ich indywidualnych adresów IP. Narzędzia do skanowania sieci próbują zidentyfikować wszystkie aktywne lub odpowiadające hosty w sieci i odpowiadające im adresy IP.

Najprostszym, choć niekoniecznie najdokładniejszym sposobem ustalenia, czy systemy działają, jest wykonanie polecenia `ping` dla zakresu adresów IP - jest to tzw. *ping sweep*. Wszystkie systemy, które odpowiadają na polecenie `ping`, są rozpatrywane jako aktywne/działające w sieci. Polecenie `ping` jest oparte o protokół ICMP (*Internet Control Message Protocol*). ICMP jest używany do wysyłania komunikatów testowych i komunikatów o błędach między hostami w Internecie. Możliwość użycia ICMP Echo request i Echo replay jako testu łączności między hostami jest wbudowana w każde urządzenie z obsługą protokołu IP za pomocą polecenia `ping`. Jest to szybki test, który weryfikuje czy dwa hosty mają łączność. Zaletą skanowania ICMP jest to, że można go uruchomić równolegle, co oznacza, że wszystkie systemy są skanowane w tym samym czasie. Większość narzędzi do działań ofensywnych w systemach teleinformatycznych zawiera opcję skanowania `ping`, co zasadniczo oznacza wysyłanie żądań ICMP do każdego hosta w sieci. Skanowanie `ping` można przeprowadzić z wykorzystaniem narzędzia `nmap`:

```
nmap -sn 192.168.11.200-250
```

Prawie każdy system monitorowania sieci czy IDS (*intrusion detection system*) zaalarmuje administratorów o skanowaniu `ping` występującym w sieci. Większość zapór ogniowych i serwerów proxy blokuje odpowiedzi `ping`, więc haker nie może dokładnie określić, czy systemy są dostępne przy użyciu samego testu `ping`. Należy zastosować inne rodzaje skanowania portów, jeśli systemy nie reagują na zapytania `ping`. To, że skanowanie `ping` nie zwraca żadnych aktywnych hostów w sieci, nie oznacza, że nie są one dostępne - trzeba wypróbować alternatywną metodę identyfikacji.

Ćwiczenia

1. Za pomocą narzędzia `nmap` wykonaj *ping sweep* dla sieci wskazanej przez prowadzącego.

2.3 Skanowanie podatności

```
Przed wykonaniem dalszych ćwiczeń należy wpisać komendę iptables -F
```

Sieciowe skanowanie podatności to proces proaktywnego identyfikowania podatności systemów komputerowych osiągalnych w sieci. Skaner podatności najpierw identyfikuje system operacyjny i numer wersji (dla Windowsów starszych niż Windows 10 także dodatki Service Pack). Skaner na tej podstawie identyfikuje słabości lub luki w zabezpieczeniach systemu operacyjnego. Następnie następuje identyfikacja, które porty są otwarte. Na tej podstawie skaner określa jakie usługi i aplikacje są uruchomione

(wraz z ich wersjami). Po tym odbywa się główna faza działania skanera podatności - na podstawie bazy wzorców podatności sprawdzane jest występowanie tych podatności.

Ważne jest aby baza wzorców podatności była jak najczęściej uaktualniana.

W późniejszej fazie ataku haker może wykorzystać te słabości, aby uzyskać dostęp do systemu.

Chociaż skanowanie może szybko zidentyfikować hosty nasłuchujące i aktywne w sieci, jest to również szybki sposób na odrykanie działań przez systemy monitorujące włamania (IDS). Narzędzia do skanowania sondują porty TCP/IP w poszukiwaniu otwartych portów i adresów IP, a te są rozpoznawane za pomocą większości narzędzi do wykrywania włamań. Zwykle można wykryć skanowanie sieci i podatności, ponieważ skaner musi wchodzić w interakcje z systemami docelowymi za pośrednictwem sieci. W zależności od rodzaju aplikacji skanującej i szybkości skanowania IDS wykryje skanowanie i oznaczy je jako odpowiednie zdarzenie. Niektóre z narzędzi do skanowania mają różne tryby ominięcia IDS i istnieje większe prawdopodobieństwo, że działania ofensywne będą kontynuowane bez wykrycia.

2.3.1 Nmap NSE

Narzędzie Nmap oprócz możliwości skanowania portów ma również możliwość skanowania podatności za pomocą skryptów NSE. Wszystkie skrypty NSE znajdują się w folderze `/usr/share/nmap/scripts`.

```
root@kali:~# cd /usr/share/nmap/scripts/
root@kali:/usr/share/nmap/scripts# ls -l *vuln*
-rw-r--r-- 1 root root 6960 Dec 13 2012 afp -path -vuln.nse
-rw-r--r-- 1 root root 6190 Dec 13 2012 ftp -vuln -cve2010 -4221.nse
-rw-r--r-- 1 root root 7112 Dec 13 2012 http -huawei -hg5xx -vuln.nse
-rw-r--r-- 1 root root 8203 Dec 13 2012 http -iis -webdav -vuln.nse
-rw-r--r-- 1 root root 4021 Dec 13 2012 http -vmware -path -vuln.nse
-rw-r--r-- 1 root root 6519 Dec 13 2012 http -vuln -cve2009 -3960.nse
...
```

Jako krótkie wprowadzenie do skanowania podatności za pomocą skryptów NSE, możemy użyć skryptu **http-vuln-cve2010-2861** do przeskanowania serwera WWW Cold Fusion w poszukiwaniu podatności `path traversal`.

```
root@kali:~# nmap -v -p 80 --script=http-vuln-cve2010-2861 192.168.11.210

Starting Nmap 6.25 ( http://nmap.org ) at 2013-06-17 10:28 MDT
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Ping Scan at 10:28
Scanning 192.168.11.210 [4 ports]
Completed Ping Scan at 10:28, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:28
Completed Parallel DNS resolution of 1 host. at 10:28, 0.00s elapsed
Initiating SYN Stealth Scan at 10:28
Scanning 192.168.11.210 [1 port]
Discovered open port 80/tcp on 192.168.11.210
Completed SYN Stealth Scan at 10:28, 0.10s elapsed (1 total ports)
NSE: Script scanning 192.168.11.210.
```

```

Initiating NSE at 10:28
Completed NSE at 10:28, 2.08s elapsed
Nmap scan report for 192.168.11.210
Host is up (0.19s latency).
PORT STATE SERVICE
80/tcp open  http
| http-vuln-cve2010-2861:
|   VULNERABLE:
|     Adobe ColdFusion Directory Traversal Vulnerability
|       State: VULNERABLE (Exploitable)
|       IDs: OSVDB:67047 CVE:CVE-2010-2861
|       Description:
|         Multiple directory traversal vulnerabilities in the administrator console
|         in Adobe ColdFusion 9.0.1 and earlier allow remote attackers to read
arbitrary files via the
|         locale parameter
|       Disclosure date: 2010-08-10
|       Extra information:
|
|       CFusionMX
|         Not vulnerable
|       JRun4\servers
|         Not vulnerable
|       ColdFusion8
|         HMAC: 446EF3D6B348522E29F72ED6BB19A6BE9867A42C
|         Salt: 1371461992204
|         Hash: AAFDC23870ECBCD3D557B6423A8982134E17927E
|       CFusionMX7
|         Not vulnerable
|
|       References:
|         http://osvdb.org/67047
|         http://www.nessus.org/plugins/index.php?view=single&id=48340
|         http://www.blackhatacademy.org/security101/Cold_Fusion_Hacking
|         http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2861
|         http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2861
|_

NSE: Script Post-scanning.
Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.54 seconds
Raw packets sent: 5 (196B) | Rcvd: 2 (84B)

```

Widać w powyższych wynikach, że Nmap nie tylko stwierdził, że serwer jest podatny na ataki, ale nawet odzyskał również skrót hasła administratora.

Nieprawidłowo zabezpieczone serwery FTP mogą często dostarczać wiele informacji, a czasem mogą prowadzić do całkowitej kompromitacji serwera. Skrypt NSE **ftp-anon** umożliwia szybkie skanowanie zakresu adresów IP w poszukiwaniu serwerów FTP, które umożliwiają anonimowy dostęp.

```

root@kali:~# nmap -v -p 21 --script=ftp-anon.nse 192.168.11.200-254
...
Nmap scan report for 192.168.11.217

```



```

Host is up (0.19s latency).
PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| total 20
| d----- 2 root      ftp  4096 Jun 12 07:49 =
| d--x--x--x 2 root      root 4096 Jan 18 2007 bin
| d--x--x--x 2 root      root 4096 Jan 18 2007 etc
| drwxr-xr-x 2 root      root 4096 Jan 18 2007 lib
|_drwxr-sr-x 2 root      ftp   4096 Feb 4      2000 pub

```

Kolejnym przykładem wykorzystania Nmap NSE do wykrywania podatności może być przetestowanie usługi SMB. Usługa Microsoft Windows SMB ma długą historię poważnych luk w zabezpieczeniach, a serwery często są narażone na ataki w testach penetracyjnych. SMB może często ujawniać wiele nieuwierzytelnionych użytkowników, które mogą być następnie wykorzystane do przyszłych ataków. Na przykład możemy sprawdzić poziom bezpieczeństwa serwera SMB za pomocą skryptu NSE smb-security-mode w następujący sposób.

```

root@kali:~# nmap -v -p 139, 445 --script=smb-security-mode 192.168.11.236
...
Nmap scan report for 192.168.11.236
Host is up (0.10s latency).
PORT      STATE SERVICE
139/tcp    open  netbios-ssn

Host script results:
| smb-security-mode:
|   Account that was used for smb scripts: guest
|   Share-level authentication (dangerous)
|   SMB Security: Challenge/response passwords supported
|_  Message signing disabled (dangerous, but default)

```

Poza testami penetracyjnymi administratorzy sieci wykorzystują skrypty NSE do sprawdzenia czy łatki zostały zainstalowane na wskazanej grupie serwerów lub stacji roboczych. Poniżej znajduje się przykład użycia Nmap do sprawdzenia, czy wszystkie serwery sieciowe domeny zostały załatane przeciwko CVE-2011-3192 (podatność denial-of-service na serwerze Apache).

```

root@kali:~# nmap -v -p 80 --script=http-vuln-cve2011-3192 192.168.11.205-210
...
Nmap scan report for 192.168.11.208
Host is up (0.19s latency).
PORT      STATE SERVICE
80/tcp    open  http
| http-vuln-cve2011-3192:
|   VULNERABLE:
|   Apache byterange filter DoS
|   State: VULNERABLE
|   IDs: CVE:CVE-2011-3192 OSVDB:74721
|   Description:
|   The Apache web server is vulnerable to a denial of service attack when
numerous

```

```
| overlapping byte ranges are requested.  
| Disclosure date: 2011-08-19  
| References:  
| http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192  
| http://osvdb.org/74721  
| http://seclists.org/fulldisclosure/2011/Aug/175  
|_ http://nessus.org/plugins/index.php?view=single&id=55976
```

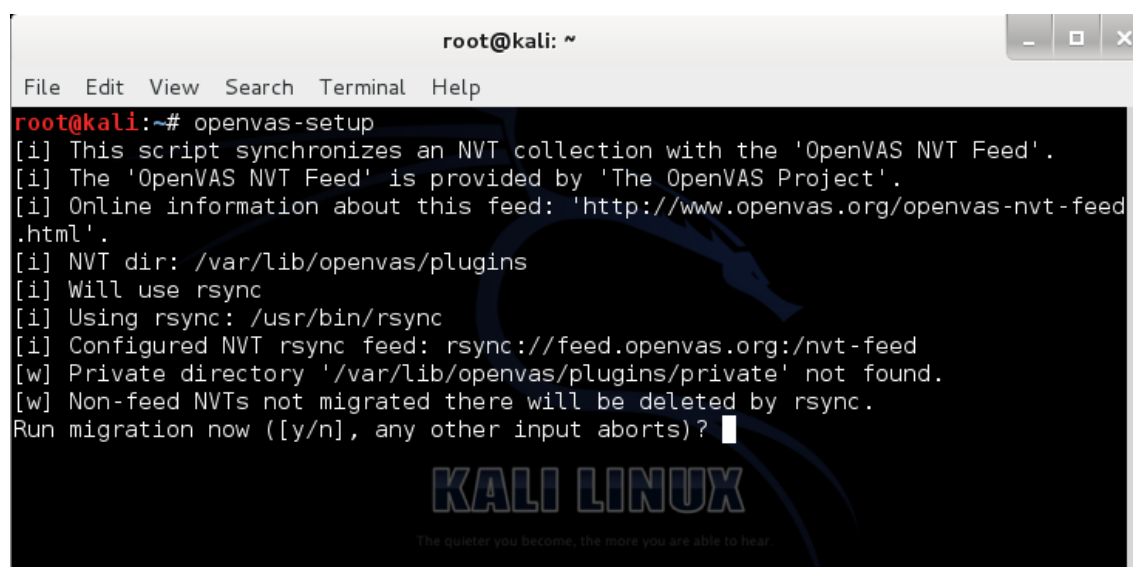
W wynikach powyżej stwierdzono, że serwer zawiera wskazaną podatność. Nmap zapewnia również łącza do różnych odnośników, które Użytkownik może odwiedzić, aby uzyskać więcej informacji o wykrytej podatności.

Ćwiczenia

1. Za pomocą skanera `nmap` znaleźć podatności `SMB` dla hosta `metasploitable`.
2. <https://sekurak.pl/nmap-i-12-przydatnych-skryptow-nse/>

2.3.2 OpenVAS

The Open Vulnerability Assessment System (OpenVAS) to skaner podatności, zawierający szeroką bazę podatności. Jest dostępny za darmo (open source) na licencji GNU General Public License (GNU GPL). OpenVAS jako rozbudowany framework wymaga przeprowadzenia wstępnej konfiguracji użytkownika. Pierwszym krokiem jest uruchomienie skryptu inicjalizacyjnego `openvas-setup` w celu zainicjowania wtyczek i uruchomienia różnych usług wymaganych przez OpenVAS. Gdy pojawi się monit o hasło, utwórz silne hasło dla administratora.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# openvas-setup  
[i] This script synchronizes an NVT collection with the 'OpenVAS NVT Feed'.  
[i] The 'OpenVAS NVT Feed' is provided by 'The OpenVAS Project'.  
[i] Online information about this feed: 'http://www.openvas.org/openvas-nvt-feed.html'.  
[i] NVT dir: /var/lib/openvas/plugins  
[i] Will use rsync  
[i] Using rsync: /usr/bin/rsync  
[i] Configured NVT rsync feed: rsync://feed.openvas.org:/nvt-feed  
[w] Private directory '/var/lib/openvas/plugins/private' not found.  
[w] Non-feed NVTs not migrated there will be deleted by rsync.  
Run migration now ([y/n], any other input aborts)?
```

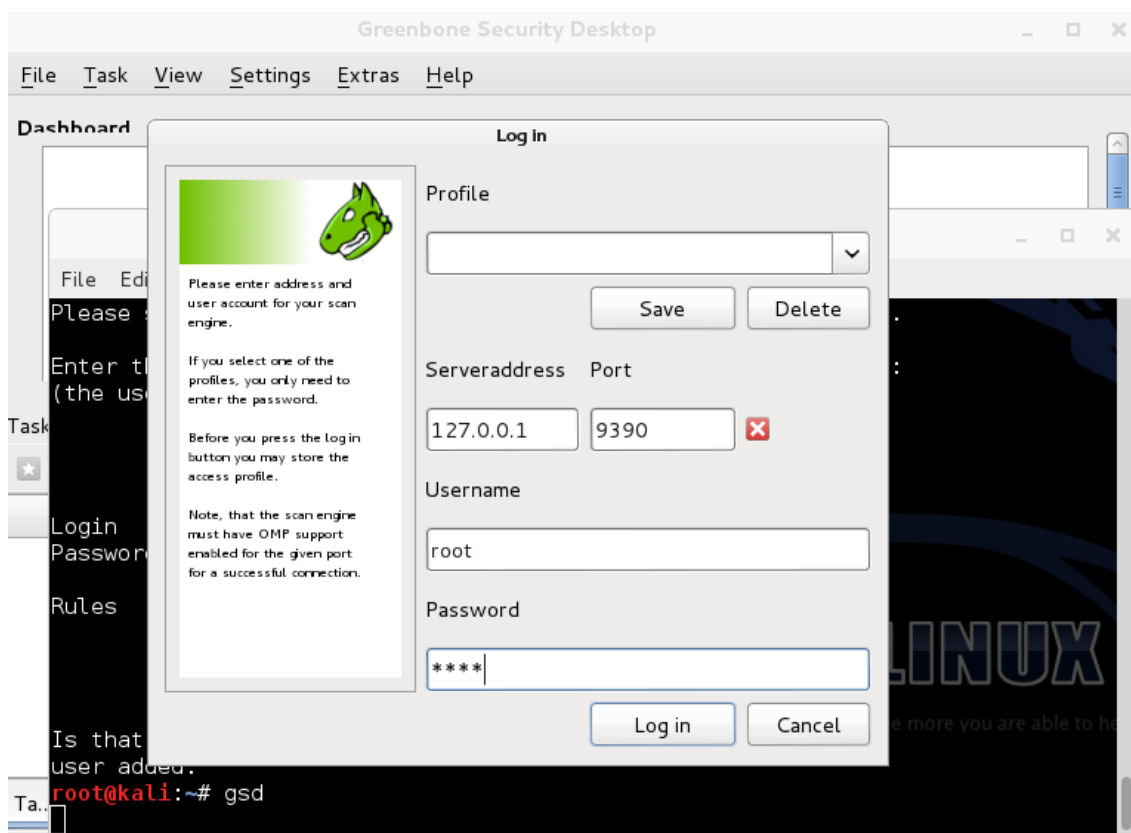
Następnie musimy utworzyć użytkownika, aby zalogować się do OpenVAS za pomocą skryptu `openvas-adduser`.

```
root@kali: ~
File Edit View Search Terminal Help
Stopping OpenVAS Scanner: openvassd.
All plugins loaded

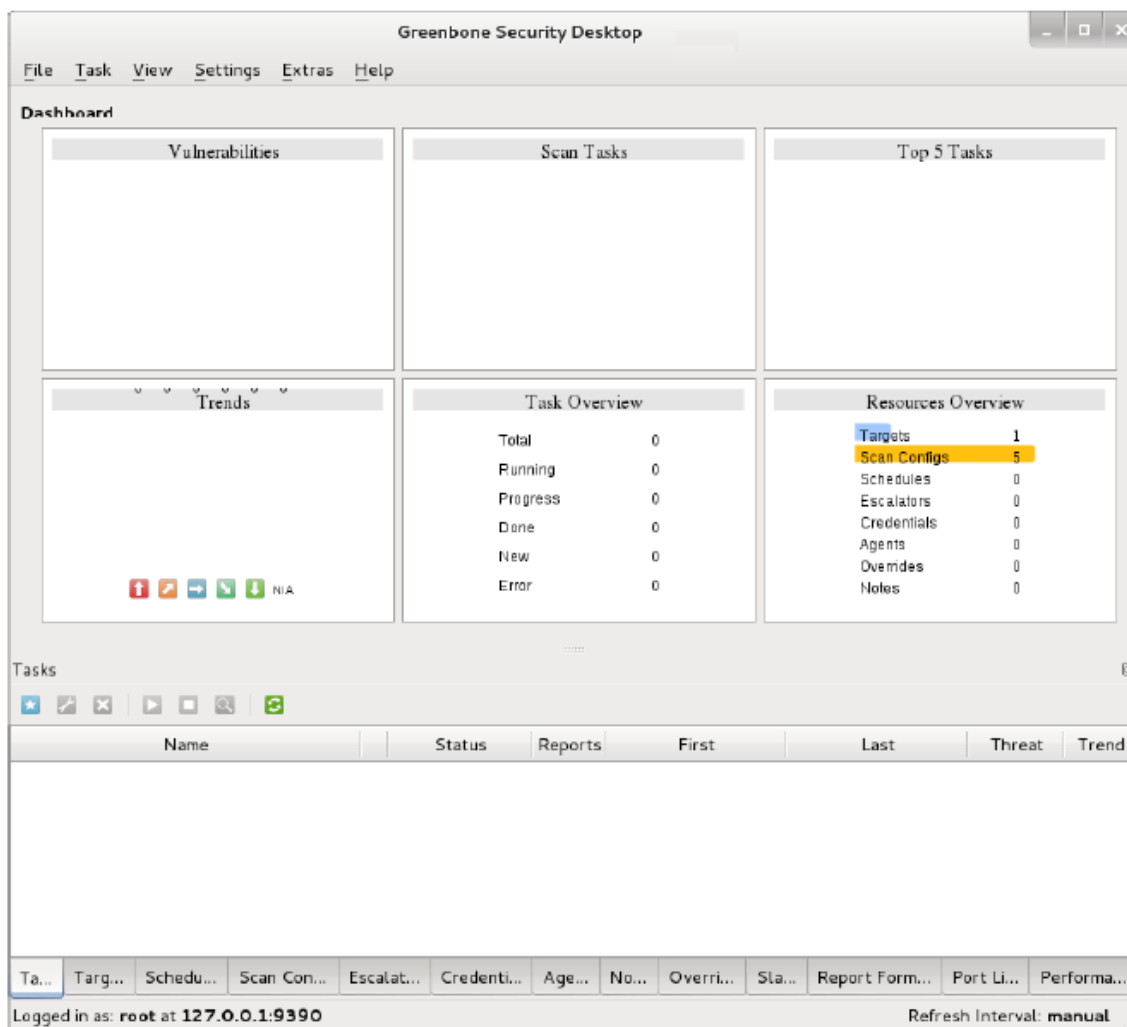
Starting OpenVAS Scanner: openvassd.
Starting OpenVAS Manager: openvasmd.
Restarting OpenVAS Administrator: openvasad.
Restarting Greenbone Security Assistant: gsd.
root@kali:~#
root@kali:~# openvas-adduser
Using /var/tmp as a temporary file holder.

Add a new openvassd user
-----
Login : admin
This login already exists. Choose another one.
Login : root
Authentication (pass/cert) [pass] : pass
Login password :
```

Po utworzeniu nowego użytkownika możemy teraz uruchomić Greenbone Security Desktop (polecenie **gsd** w konsoli) i zalogować się przy użyciu nowo utworzonych danych logowania.



Po zalogowaniu zostanie wyświetlony interfejs Greenbone Security Desktop, w którym można konfigurować cele, tworzyć zadania i zarządzać wynikami skanowania podatności.



Przed uruchomieniem pierwszego skanowania podatności z OpenVAS musimy skonfigurować cel. Celem może być pojedynczy adres IP lub zakres hostów, jak pokazano poniżej.

New Target

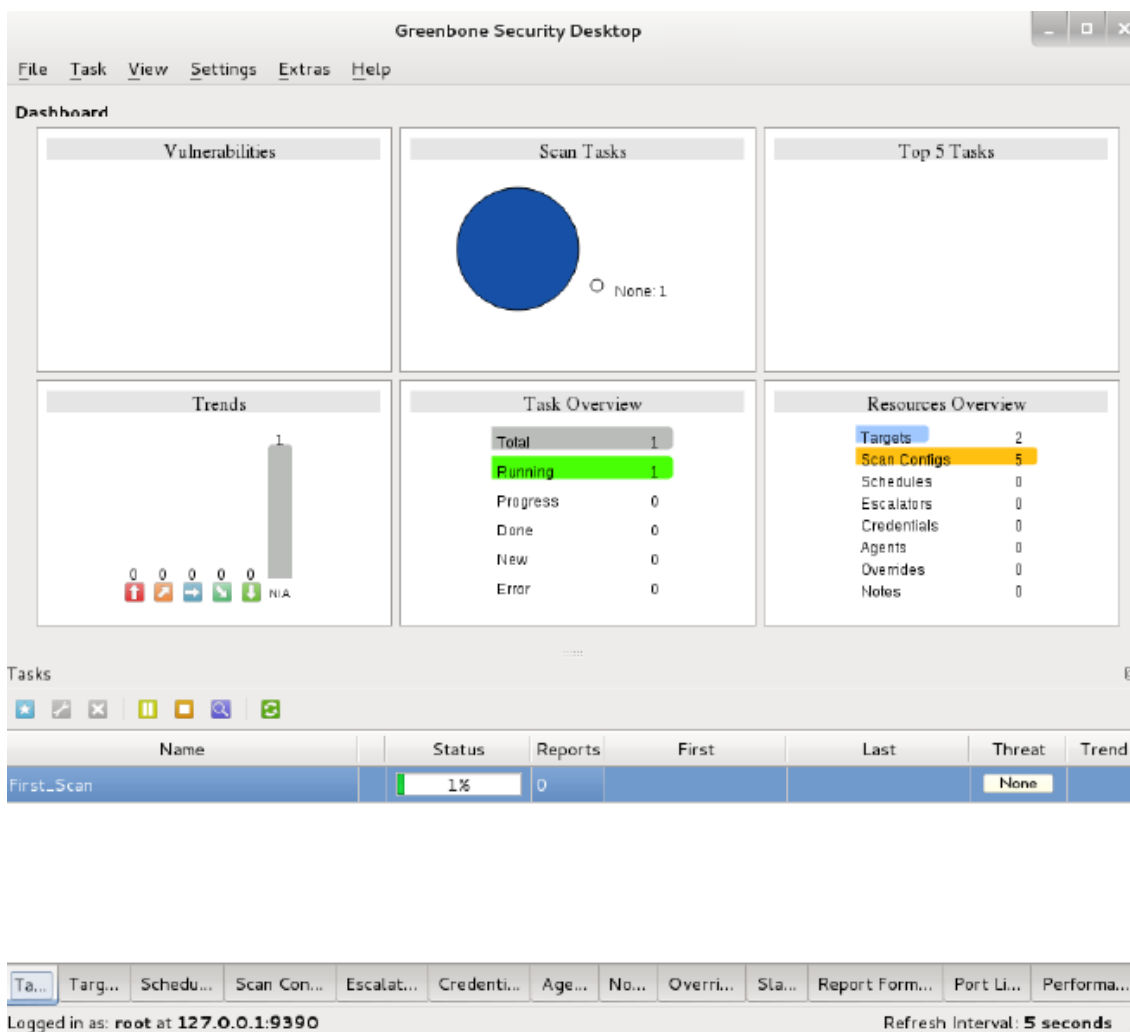
Name	<input type="text" value="subnet-1"/>		
Comment (optional)	<input type="text"/>		
Hosts	<input type="text" value="192.168.1.0/24"/>		
Port List	<input type="text" value="All IANA assigned TCP 2012-02-10"/>		
SSH Credential (optional)	<input type="text" value="--"/>		
SMB Credential (optional)	<input type="text" value="--"/>		

Po skonfigurowaniu celu możemy przystąpić do tworzenia nowego zadania skanowania, jak pokazano poniżej, przy użyciu jednej z wbudowanych konfiguracji skanowania.

New Task

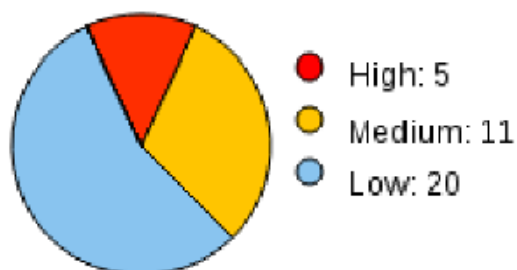
Name	<input type="text" value="First_Scan"/>		
Comment (optional)	<input type="text"/>		
Scan Config	<input type="text" value="Full and fast"/>		
Scan Targets	<input type="text" value="subnet-1"/>		
Escalator (optional)	<input type="text" value="--"/>		
Schedule (optional)	<input type="text" value="--"/>		
Slave (optional)	<input type="text" value="--"/>		

Nowe zadania nie uruchamiają się automatycznie - po zdefiniowaniu zadania należy zrobić to ręcznie. Następnie czekamy na zakończenie skanowania w poszukiwaniu luk bezpieczeństwa. W zależności od zasobów systemowych skanowanie w poszukiwaniu luk bezpieczeństwa może trwać długo.



Po zakończeniu skanowania raport można znaleźć na karcie **Reports**. Pierwsze skanowanie zostało przeprowadzone bez poświadczeń. Liczba wykrytych luk jest dość niska, ponieważ nie można wyszukiwać oprogramowania zainstalowanego w systemie docelowym ani innych luk wymagających uwierzytelnienia.

Vulnerabilities



Ćwiczenia do wykonania

1. Za pomocą skanera OpenVAS znaleźć podatności dla hosta `metasploitable`.

2.3.3 Nessus

Nessus jest jednym z najbardziej popularnych skanerów podatności dostępnym dla systemów Linux, Microsoft Windows, Mac OS X, FreeBSD, GPG. Jest to najbardziej zaufana platforma skanowania luk w zabezpieczeniach systemów. Audytorzy czy analitycy bezpieczeństwa mogą planować zadania na wielu skanerach, korzystać z kreatorów, aby łatwo i szybko tworzyć polityki czy wysyłać wyniki pocztą e-mail. Nessus obsługuje więcej technologii niż jakikolwiek inne rozwiązanie, w tym systemy operacyjne, urządzenia sieciowe, hiperwizory, bazy danych, tablety / telefony, serwery sieciowe i infrastrukturę krytyczną. Kluczowe cechy tego skanera obejmują:

- Szybkie odkrywanie zasobów
- Ocena podatności
- Wykrywanie złośliwego oprogramowania / botnetu
- Audyt konfiguracji i zgodności
- Skanowanie i audyt platform zwirtualizowanych i chmurowych
- Audyty urządzeń mobilnych
- Dostosowane raportów

Pracę z Nessusem należy zacząć od uruchomienia usługi:

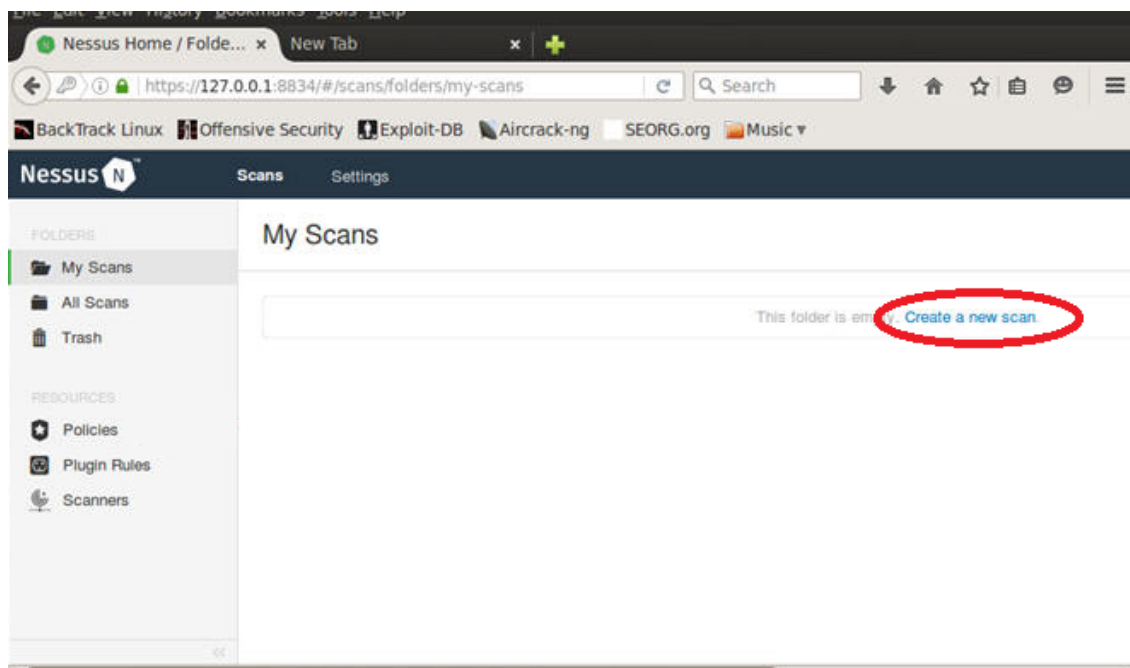
```
/etc/init.d/nessusd start
```

Następnie przechodzimy do przeglądarki internetowej i wpisujemy adres:

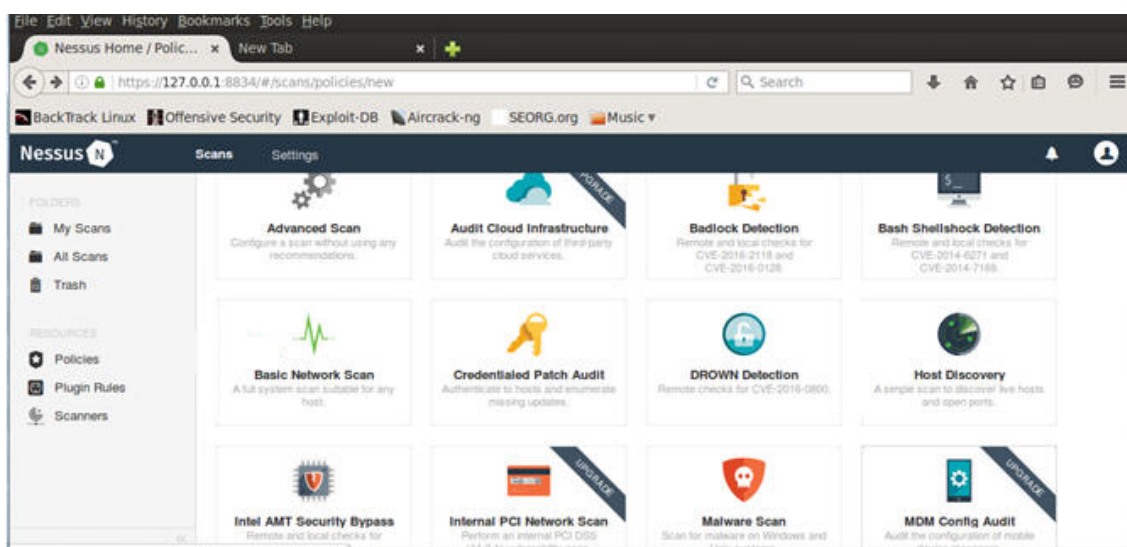
<https://localhost:8834>. System prosi o podanie loginu i hasła użytkownika (w przypadku pierwszego logowania będziemy musieli stworzyć nowego użytkownika i zarejestrować skaner). Nowego użytkownika możemy stworzyć za pomocą polecenia:

```
#/opt/nessus/sbin/nessuscli adduser NEWUSERNAME
```

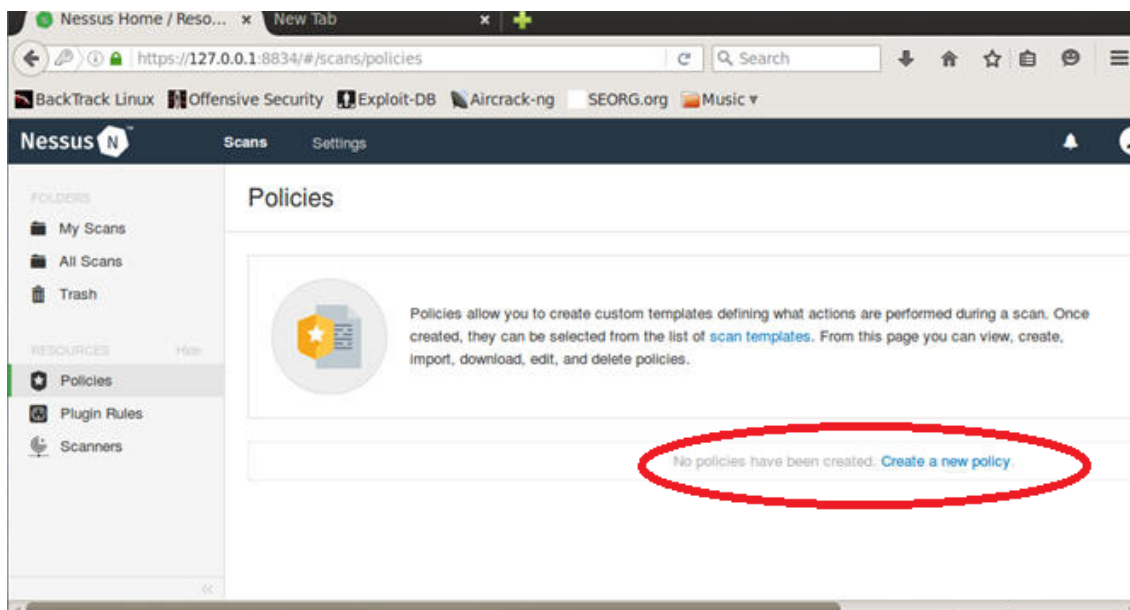
Po podaniu nazwy użytkownika system prosi o podanie hasła. Jeśli wszystko przebiegnie bez zastrzeżeń, to logowanie będzie od razu możliwe (ewentualnie trzeba będzie zrestartować usługę nessus). Po poprawnym zalogowaniu stan aplikacji powinien być podobny do tego, który prezentuje poniższy obrazek:



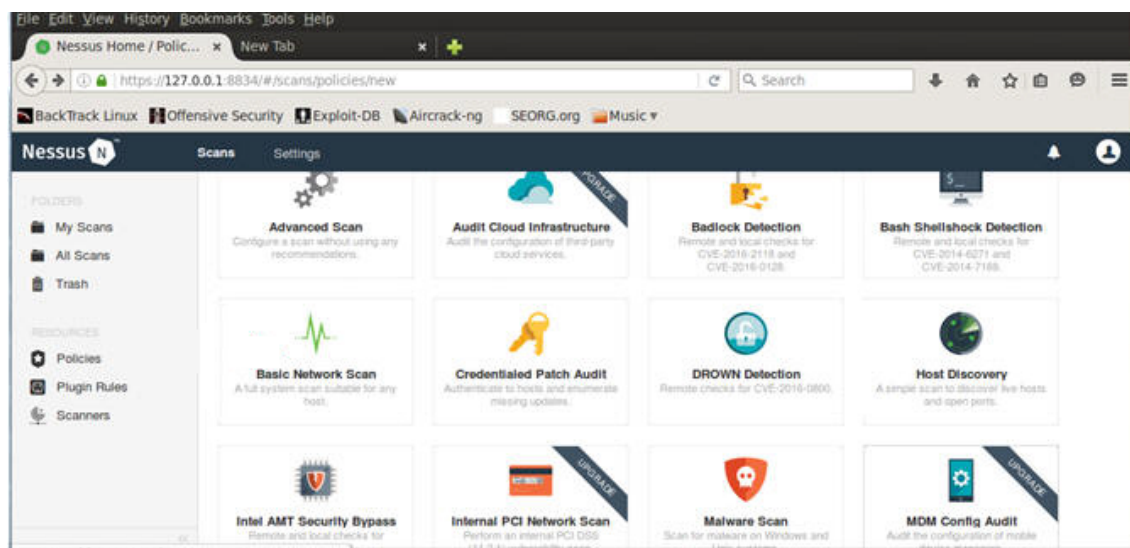
Po kliknięciu opcji **create new scans** pojawi się wiele opcji w zakresie rodzajów skanowania do wyboru, które można zobaczyć na poniższym obrazie:



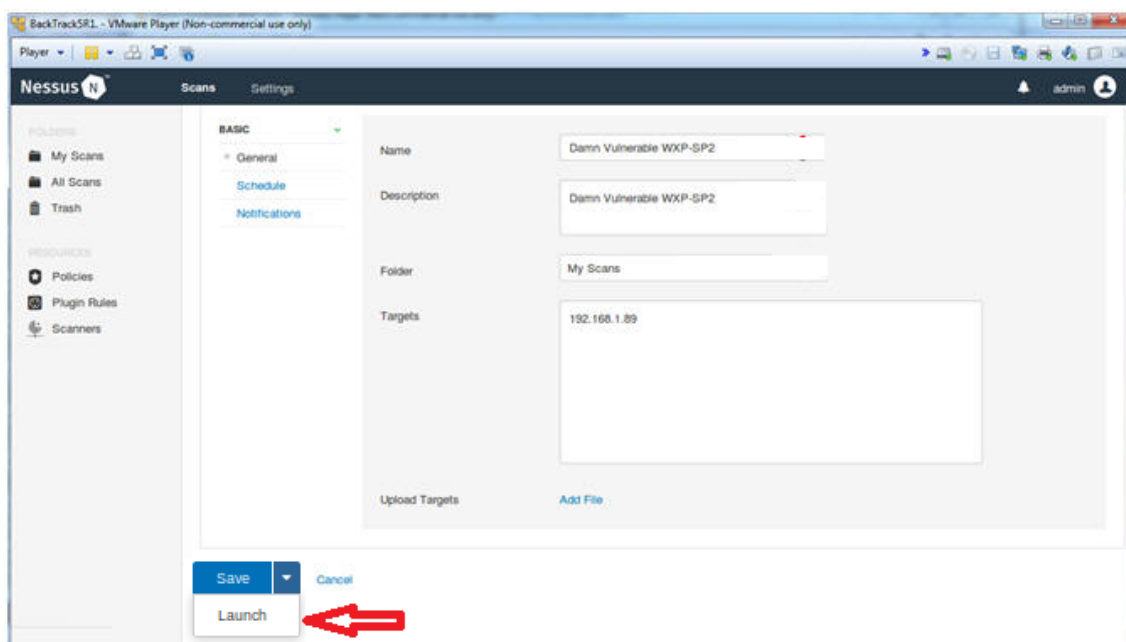
Następnie na karcie zasad możesz wygenerować różne zasady, na których oparte są zadania skanowania.



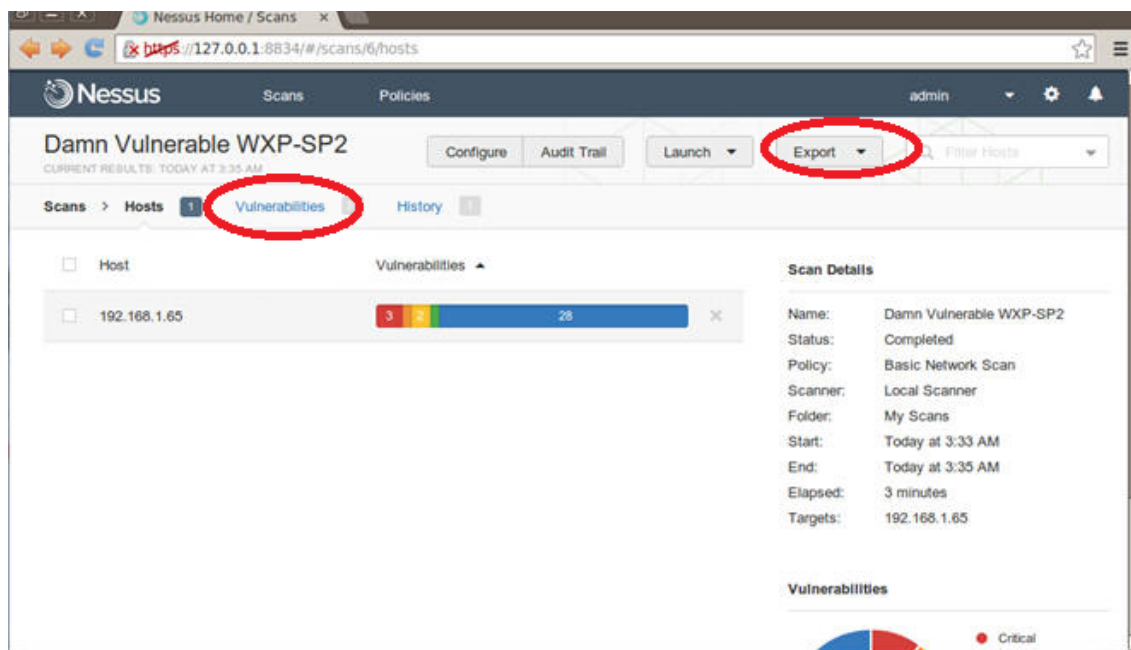
Istnieją również różne szablony zasad, jak pokazano na poniższym obrazku (tak jak dla szablonów skanów):



Aby rozpocząć nowe skanowanie, przejdź do szablonów skanowania i wybierz nowe skanowanie, a następnie nadaj mu nazwę i docelowy adres IP a na końcu opcję Launch, jak pokazano na poniższym obrazie:



Rezultat skanowania powinien wyglądać mniej więcej następująco:



Jest tu przedstawiony diagram obrazujący liczbę znalezionych podatności. Klikając w opcję **Vulnerabilities** przechodzimy do szczegółów tego skanu. Każdą podatność jest szczegółowo opisana wraz z rekomendacjami jak ją zmitigować (wystarczy kliknąć na daną pozycję podatności). Na podstawie wyników skanowania można utworzyć raport (opcja **Export**). Możliwe jest eksportowanie raportu do pliku w wielu formach np. PDF czy CSV.

Ćwiczenia

1. Za pomocą skanera Nessus znaleźć podatności dla hosta metasploitable. Porównać otrzymane wyniki z wynikami uzyskanymi z OpenVAS.