1110111011011

1001100

110011001100

1010101010101010

00011001001

„Wytrych dla włamywaczy”

Kali Linux. Information Gathering

Hacking i Cyberbezpieczeństwo | Giganci Programowania

Opracowanie: Michał Suchoń

Przypomnienie

1. Co to VPN, a co to Proxy? Jaka jest różnica między nimi?
2. W jaki sposób wejść do Deep Web'u. Czy to bezpieczne i czy legalne?
3. Jaka jest różnica między szyfrowaniem symetrycznym a niesymetrycznym?

Przypomnienie

1. Co to VPN, a co to Proxy? Jaka jest różnica między nimi?

   Proxy – z ang. *Pośrednik; usługa serwera pośredniczącego, zapobiega bezpośredniemu łączeniu się serwer np. celem uzyskania dostępu do strony internetowej (serwer docelowy widzi adres IP proxy – nie nasz). Związana głównie z protokołem HTTP.**

   VPN – *Virtual Private Network – ang. wirtualna sieć prywatna*; usługa tunelowania połączeń, gdzie naszym „wyjściem na świat" jest serwer VPN, który każde przesyłane dane przekazuje przez sieć rozlegle rozmieszczonych (na całym świecie!) urządzeń trasujących (np. routery / serwery). Docelowe urządzenia „widzą" adres IP serwera VPN, nie nasz.

   Podstawową różnicą między VPN'em a Proxy jest to, że Pośrednik działa w sposób niezabezpieczony i w ograniczeniu głównie do protokołu HTTP; VPN zaś może używać różne protokoły i porty, a sieć tunelowa jest zaszyfrowana.

2. W jaki sposób wejść do Deep Web'u. Czy to bezpieczne i czy legalne?

3. Jaka jest różnica między szyfrowaniem symetrycznym a niesymetrycznym?

Przypomnienie

1. Co to VPN, a co to Proxy? Jaka jest różnica między nimi?

   Proxy – z ang. *Pośrednik*;* usługa serwera pośredniczącego, zapobiega bezpośredniemu łączeniu się serwer np. celem uzyskania dostępu do strony internetowej (serwer docelowy widzi adres IP proxy – nie nasz). Związana głównie z protokołem HTTP.

   VPN – *Virtual Private Network – ang. wirtualna sieć prywatna*; usługa tunelowania połączeń, gdzie naszym „wyjściem na świat" jest serwer VPN, który każde przesyłane dane przekazuje przez sieć rozlegle rozmieszczonych (na całym świecie!) urządzeń trasujących (np. routery / serwery). Docelowe urządzenia „widzą" adres IP serwera VPN, nie nasz.

   Podstawową różnicą między VPN'em a Proxy jest to, że Pośrednik działa w sposób niezabezpieczony i w ograniczeniu głównie do protokołu HTTP; VPN zaś może używać różne protokoły i porty, a sieć tunelowa jest zaszyfrowana.

2. W jaki sposób wejść do Deep Web'u. Czy to bezpieczne i czy legalne?

   Wejście do Deep Web'u jest możliwe przez sieć Tor, z którą możemy się połączyć poprzez TorBrowser. Korzystanie z sieci Tor jest w pełni legalne w Polsce, lecz może się wiązać z wieloma zagrożeniami podczas nieostrożnego korzystania z sieci cebulowej.

3. Jaka jest różnica między szyfrowaniem symetrycznym a niesymetrycznym?

Przypomnienie

1. Co to VPN, a co to Proxy? Jaka jest różnica między nimi?

   Proxy – z ang. *Pośrednik; usługa serwera pośredniczącego, zapobiega bezpośredniemu łączeniu się serwer np. celem uzyskania dostępu do strony internetowej (serwer docelowy widzi adres IP proxy – nie nasz). Związana głównie z protokołem HTTP.**

   VPN – *Virtual Private Network – ang. wirtualna sieć prywatna*; usługa tunelowania połączeń, gdzie naszym „wyjściem na świat" jest serwer VPN, który każde przesyłane dane przekazuje przez sieć rozlegle rozmieszczonych (na całym świecie!) urządzeń trasujących (np. routery / serwery). Docelowe urządzenia „widzą" adres IP serwera VPN, nie nasz.

   Podstawową różnicą między VPN'em a Proxy jest to, że Pośrednik działa w sposób niezabezpieczony i w ograniczeniu głównie do protokołu HTTP; VPN zaś może używać różne protokoły i porty, a sieć tunelowa jest zaszyfrowana.

2. W jaki sposób wejść do Deep Web'u. Czy to bezpieczne i czy legalne?

   Wejście do Deep Web'u jest możliwe przez sieć Tor, z którą możemy się połączyć poprzez TorBrowser. Korzystanie z sieci Tor jest w pełni legalne w Polsce, lecz może się wiązać z wieloma zagrożeniami podczas nieostrożnego korzystania z sieci cebulowej.

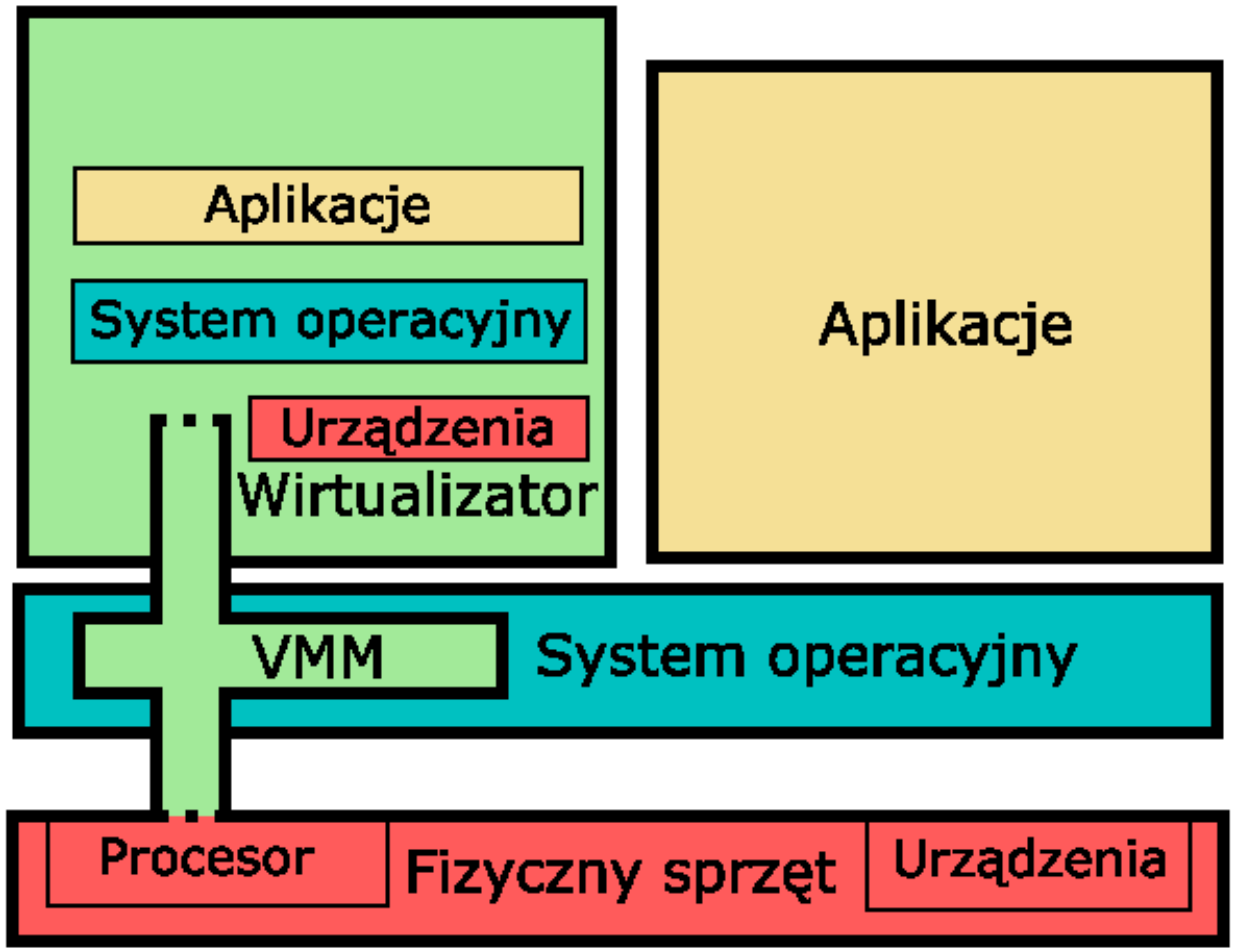
3. Jaka jest różnica między szyfrowaniem symetrycznym a niesymetrycznym?

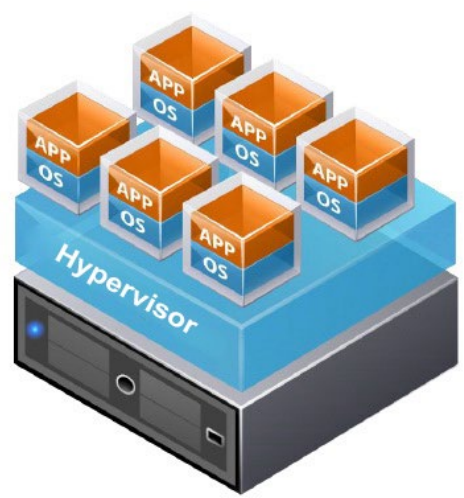
   Szyfrowanie symetryczne wykorzystuje jeden klucz do szyfrowania i deszyfrowania informacji. Asymetryczne – dwa osobne (publiczny do szyfrowania i prywatny do deszyfracji)

System w systemie… jak?

Wirtualizacja

sposób symulowania fizycznego zasobu poprzez jego wirtualny odpowiednik – opiera się o wydzieleniu części zasobów komputera (pamięci masowej, RAM, GPU, CPU) w celu uruchomienia na nim wybranego środowiska, np. system Windows, dystrybucje Linux etc. Maszyna wirtualna to po prostu system operacyjny, współdzielący zasoby z innym systemem, postawionym na rzeczywistym urządzeniu. Umożliwia elastyczne zarządzanie zasobami (zwalnianie i zajmowanie) oraz większe bezpieczeństwo oprogramowania (maszyna wirtualna jest izolowana od środowiska zewnętrznego) -> SZCZEGÓLNIE ZALECANE NA POTRZEBY TESTOWANIA





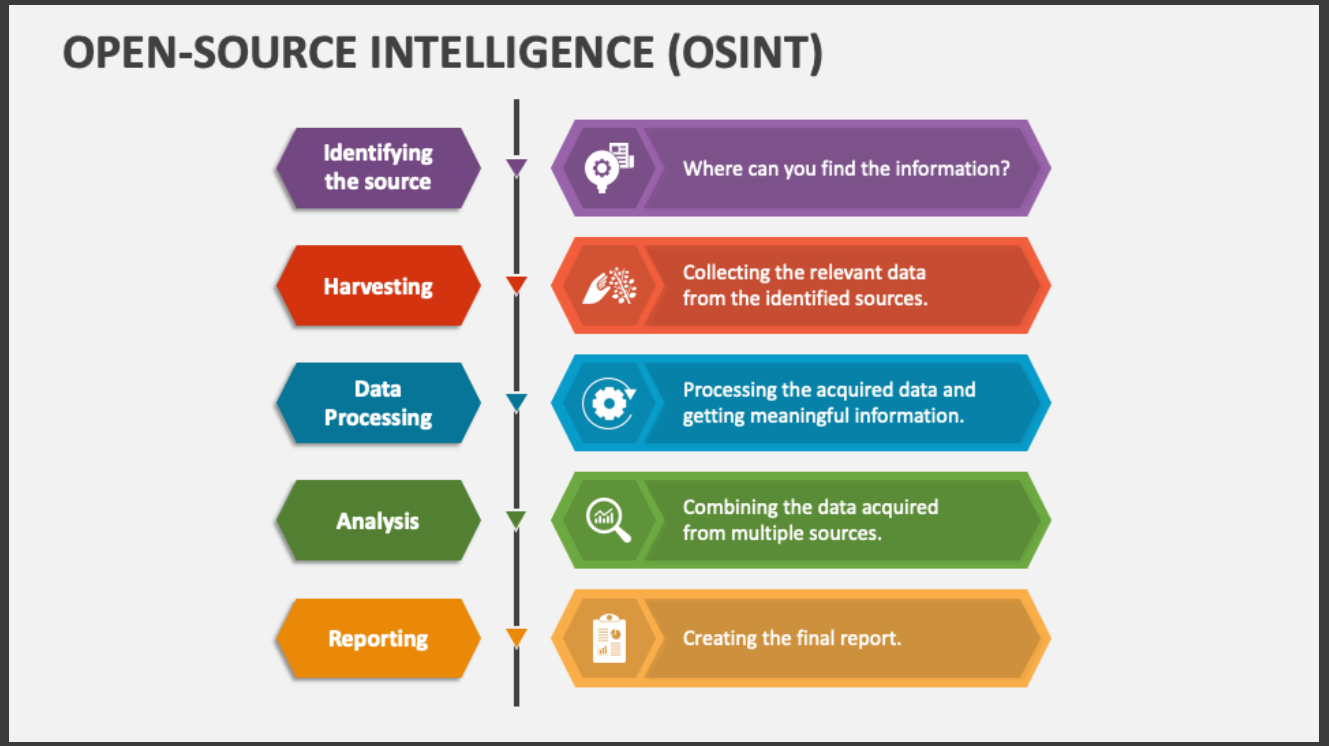
Architektura wirtualna

Tradycyjna architektura

Ważne katalogi w Kali Linux

NAZWA KATALOGU	OPIS
/boot	**Pliki rozruchowe systemu** kernel, initrd, bootloader (np. GRUB)
/etc	**Pliki konfiguracyjne systemu** (ustawienia systemowe)
/home	**Katalogi domowe użytkowników** na dane osobiste (dokumenty, obrazy, muzyka, etc.)
/media	**Dane wczytywane na nośnikach zewn.** (pendrive, CD-ROM)
/root	**Ustawienia właściciela systemu (root)** (użytkownik o maksymalnych uprawnieniach)
/tmp	**Pliki tymczasowe** (cache)
/usr	**Pliki programów użytkowników** (programy wykonywalne, współdzielone libki, pliki nagłówkowe języków, lokalne instalacje)
/var	**Pliki systemowe, których zawartość ulega modyfikacjom** (logi systemowe, source code aplikacji internetowych, dane zapisywane przez system)

https://medium.com/@derya.cortuk/open-source-intelligence-03156d3abe19



OSINT

Akronim: ***O**pen**S**ource **Int**elligence* – **wywiad z otwartych źródeł**; opiera się na uzyskiwaniu informacji, ich analizowania i oceny z ogólnodostępnych źródeł. Zdobywanie informacji w ten sposób danych jest **całkowicie legalne**, gdyż nie wymaga łamania zabezpieczeń autoryzacyjnych (brak uwierzytelnienia).

- ✓ OSINT często stosowany jest przez pracodawcę wobec kandydatów do pracy celem głębszego poznania ich sylwetek.

Aplikacje w Kali Linux

$ RECONAISSANCE (information gathering)

zbiór narzędzi do zbierania informacji
> skaner portów (nmap)
> pakiet do OSINT'u (maltego)

$ DATABASE ASSESSMENT

narzędzia do ataku baz danych

$ VULNERABILITY ANALYSIS

automatyczna analiza podatności systemów i urządzeń informatycznych

$ PASSWORD ATTACKS

narzędzia do łamania haseł i hashy
> **Offline Attacks** – lokalne łamanie haseł/hashy/plików
> **Online Attacks** – ataki na formularze logowania przez HTTP / bazy danych / hostingi / FTP

$ WEB APPLICATION ANALYSIS

Testowanie zabezpieczeń stron internetowych – web hacking
~ semestr 3

Aplikacje w Kali Linux – cz. 2

$ WIRELESS ATTACKS

atak na sieci bezprzewodowe – wifi / wardriving – **wymaga urządzenia ze specjalną kartą wifi z trybem „monitor”**

$ REVERSE ENGINEERING

szukanie exploitów w oprogramowaniu przez badanie kodu maszynowego

$ EXPLOITATION TOOLS

zbiór narzędzi do szukania luk w zabezpieczeniach

$ SNIFFING & SPOOFING

podsłuchiwanie i fałszowanie pakietów sieciowych (np. MITM)

$ POST EXPLOITATION

do explorowania zaatakowanego już systemu. narzędzia do kontrolowania zaatakowanego systemu

Aplikacje w Kali Linux – cz. 3

$ FORENSICS

aplikacje używane w informatyce śledczej,
np. analiza dowodów

$ REPORTING TOOLS

narzędzia do pisania raportów po włamaniu i znalezieniu podatności

$ SOCIAL ENGINEERING TOOLS

Narzędzia wspierające ataki z użyciem inżynierii społecznej (automatyzacja ataków)

Polecenia w Linuxie (wybrane)

POLECENIE	OPIS
cd *{dir}*	**umożliwia przechodzenie między katalogami** *{dir} – nazwa katalogu* **CD .. - COFNIĘCIE SIĘ „O JEDNO OCZKO W GÓRĘ”**
ls {np. –l , -a}	**listowanie katalogów** *{-l} – pokazuje uprawnienia katalogu/pliku* *{-a} – pokazuje pliki/katalogi ukryte*
echo {text}	**powtarza tekst zapisany jako wartość polecenia** *{text} – tekst, który ma zostać wyświetlony w terminalu* **ECHO {TEXT} > file1.txt - WYŚWIETLENIE TEKSTU I ZAPISANIE DO PLIKU file1.txt** (jeśli nie istnieje – utworzy go; Inaczej: nadpisze)
mkdir {dir}	**tworzy katalog** *{dir} – nazwa katalogu*
rm {file}	**usuwa plik /katalog (również: rmdir)** *{file} – nazwa pliku / katalog* **JEŻELI USUWANY KATALOG JEST NIEPUSTY, NALEŻY DODAĆ PARAMETR –R (usunięcie rekursywne – również elementy wewnątrz)**
vim / nano **mousepad**	**edytory tekstu** *vim / nano – terminalowy, operujemy tylko klawiaturą (operacje przez skróty klawiszowe)* *mousepad – uruchamia edytor graficzny*
touch {file}	**tworzy plik**
pwd	**wyświetla aktualną ścieżkę**
cat {file}	**Umożliwia wyświetlenie zawartości pliku (w terminalu)**

Polecenia w Linuxie (wybrane)

POLECENIE	OPIS
useradd {-g , -G , -m – M, -p} {user}	**tworzenie nowego użytkownika** {user} – nazwa użytkownika **-g	ustawia domyślną grupę userowi** **-G	dodaje usera do istniejącej grupy** **-m	tworzy katalog domowy i ustawia tworzonemu userowi** **-M	zapobiega tworzeniu katalogu użytkownika** **-p	ustawienie hasła tworzonemu userowi**
usermod {user}	**umożliwia dokonywanie modyfikacji na istniejącym userze** {user} – nazwa użytkownika **ZMIANA GRUPY, KATALOGU DOMOWEGO, HASŁA, BLOKOWANIE/ODBLOKOWANIE KONTA, USUNIĘCIE ...**
userdel {user}	**usunięcie usera** {user} – nazwa użytkownika
passwd {user}	**zmiana hasła dla konta**
whoami	**wyświetla nazwę użytkownika**
id	**wyświetla id użytkownika (UID) oraz grupy (GID)**
finger	**wyświetla aktualnie zalogowanych userów**
logout	**wylogowanie się z terminala**
exit	**wyjście z terminala**

Polecenia w Linuxie (wybrane)

POLECENIE	OPIS
man {polecenie}	**Wyświetla stronę „manuala" (*instrukcja obsługi poleceń*)** {polecenie} – nazwa *polecenia*
info {polecenie}	***Podobne do man-a***
{polecenie} **--help**	**parametr do każdego polecenia, umożliwia sprawdzenie dostępnych parametrów polecenia, jego składnię etc.** {polecenie} – nazwa *polecenia*

WIĘCEJ POLECEŃ:

https://www.astrouw.edu.pl/~jskowron/pracownia/komendy/#r__data_srodowisko_txt

METODA REKONESANSU

Information Gathering

PROCES ZBIERANIA INFORMACJI NA TEMAT CELU DZIELIMY NA DWA RODZAJE:

- **pasywne** | wykorzystuje się zewnętrzne witryny by zdobyć informacje. **korzyść**: brak ryzyka wykrycia ataku przez ofiarę (strona nie będzie posiadała w logach żadnych wrażliwych informacji na nasz temat)

- **aktywne** | opiera się na nawiązaniu połączenia z celem ataku. **Istnieje ryzyka wykrycia**

(np. dostrzeżenie przez ofiarę w logach informacji nt. częstego skanowania portów)

ĆWICZENIE 1 | TECHNIKA PASYWNA

SCHODAN UMOŻLIWIA WYSZUKANIE URZĄDZEŃ, UDOSTĘPNIONYCH PUBLICZNIE W SIECI

1. Wejdź na stronę **www.shodan.io** (Niektóre polecenia wymagają uprzedniego zalogowania, np. przez Google)
2. W wyszukiwarce na górze wpisz poszukiwany typ narzędzia sieciowego, np. *raspberrypi, printer*
3. Kliknij „lupkę" i sprawdź uzyskane wyniki (dane na temat udostępnionych urządzeń.
4. Do wyszukiwania dopisz parametr *city: (nazwa miasta), np. city: Warszawa* ***– w ten sposób możesz sprawdzić listę urządzeń w danym mieście; country: „PL" (lista urządzeń w Polsce)***
5. Wyszukaj urządzenia dla frazy **rdp** (urządzenia, pozwalające na łączenie poprzez zdalny pulpit)

ĆWICZENIE 2 | TECHNIKA PASYWNA

BuiltWith

UMOŻLIWIA SPRAWDZENIE TECHNOLOGII, ZA POMOCĄ KTÓRYCH ZOSTAŁA STWORZONA DANA APLIKACJA / STRONA INTERNETOWA

1. Wejdź na stronę **https://builtwith.com/**
2. Po wyszukaniu wybranej strony (wystarczy podać do niej adres w pasku wyszukiwania), otrzymasz informację o tym, co zostało wykorzystane (jakie technologie, języki, środowiska czy frameworki...) przy danej aplikacji internetowej – **sprawdź dla witryny: giganciprogramowania.edu.pl**

ĆWICZENIE 3 | TECHNIKA AKTYWNA

Nmap/ZenMap

ANG. NETWORK MAPPER – PROGRAM, UŻYWANY DO SKANOWANIA PORTÓW CZY WYKRYWANIA USŁUG SIECI. TESTOWANIE PORTÓW ZA POMOCĄ TEGO PROGRAMU POZWALA NA OMINIĘCIE FIREWALLI CZY PLATFORMY INTRUSION DETECTION SYSTEM. W NMAP'IE MOŻLIWE JEST IDENTYFIKOWANIE SYSTEMÓW OPERACYJNYCH SKANOWANYCH PORTÓW

1. Na początku należy przestawić konfigurację karty sieciowej. W ten celu na dole w prawym dolnym rogu VirtualBoxa klikamy na ikonę dwóch komputerów prawym przyciskiem myszki i wybieramy *ustawienia.*
2. W sekcji „Sieć" dla zakładki *Karta 1* ustawiamy pole **Podłączona do: …** na: ***MOSTKOWANA KARTA SIECIOWA (BRIDGED)***
3. Kolejno wpisujemy następujące polecenia:
   1. **ip a** (sprawdzenie naszego adresu i jego adresacja)
   2. ***Skanowanie komputerów w sieci z ich otwartymi portami:***
      sudo nmap -T5 (podajemy adres IP odczytany z polecenia wyżej wraz z maską – liczbą ze znakiem „/"
      np.:

      UWAGA! W TEN SPOSÓB ODCZYTUJEMY OTWARTE PORTY NASZEGO KOMPUTERA. JEŚLI CHCEMY W CAŁEJ SIECI- NALEŻY OSTATNIĄ LICZBĘ (w przykładzie to 15) USTAWIĆ NA „0" (DLA SIECI O MASCE 24-BITOWEJ)

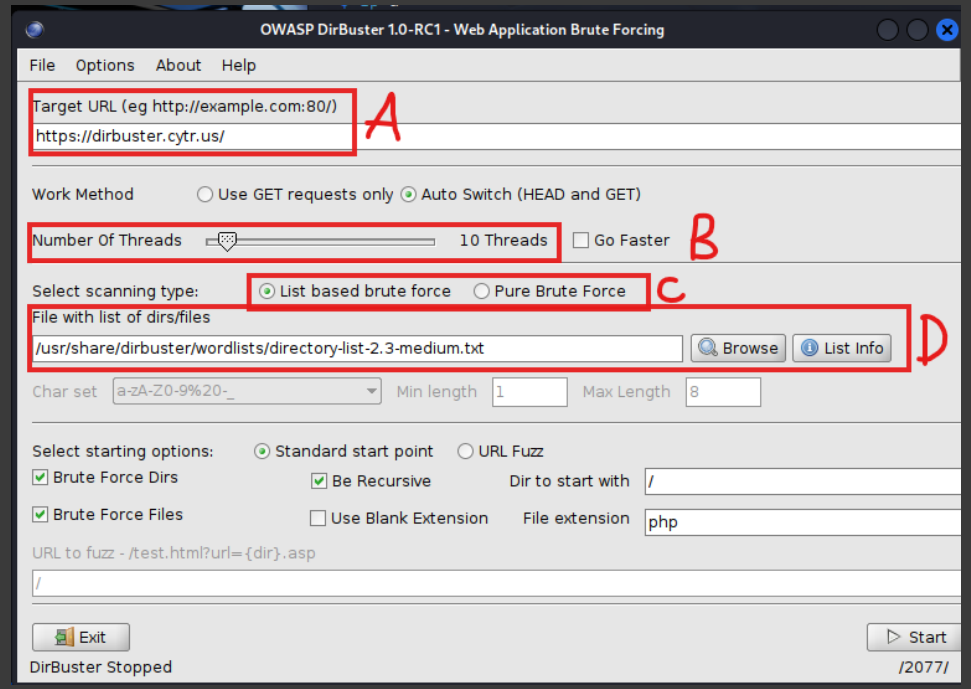
   3. ***Sprawdzenie routera i jego otwartych portów:*** **sudo nmap –p1-100 –sV –script=banner** {NASZ ADRES Z PUNKTU WYŻEJ, ALE Z 1 NA KOŃCU ZAMIAST 15 (dla maski 24-bitowej)}

ĆWICZENIE 4 | TECHNIKA AKTYWNA

DirBuster

PROGRAM, SKANUJĄCY APLIKACJE INTERNETOWE POD KĄTEM WYKRYWANIA STANDARDOWO NIEOSIĄGALNYCH Z POZIOMU NAWIGACJI SERWISU FOLDERÓW I PLIKU.

1. Z poprzedniego zadania, wejdź w ustawienia karty sieciowej i przestaw z powrotem na **NAT** (aby uzyskać ponowny dostęp do sieci zewnętrznej).
2. Wprowadź dane w programie **DirBuster** jak poniżej: (**UWAGA! NIE TESTUJEMY NA STRONIE giganciprogramowania.edu.pl**)



A – CEL ATAKU (ADRES STRONY)
B – ILOŚĆ WĄTKÓW PROCESORA DO ŁAMANIA **(IM WIĘCEJ, TYM WIĘKSZE OBCIĄŻENIE KOMPUTERA!!!)**
C – WYBÓR METODY ATAKU

- **List based brute force** - metoda słownikowa, w punkcie D. zaproponowany słownik, dodany do aplikacji. Przyciskiem „Browse" wybieramy w okienku plik ze słownikiem.
- **Pure Brute Force –** metoda siłowa, algorytm będzie szukał po różnych kombinacjach znaków (**zajmuje znacznie dłużej niż met. Słownikowa)**

3. Klikamy „Start" i obserwujemy wynik (zakładka *Results – List View: Dirs: _ Files: _*). Atak przeprowadzamy aż do znalezienia pliku **Hackme.txt**

Podsumowanie

1. Czym jest VirtualBox?
2. Wymień 2 przykładowe narzędzia do ataku w Kali Linux?
3. Czym się różni pasywna metoda rekonesansu od aktywnej? Która jest bardziej narażona na ryzyko wykrycia?
4. Wymień przykłady, jak możemy przeprowadzić pasywną metodę rekonesansu?
5. Wymień przykłady, jak możemy przeprowadzić aktywną metodę rekonesansu?

Polecam!

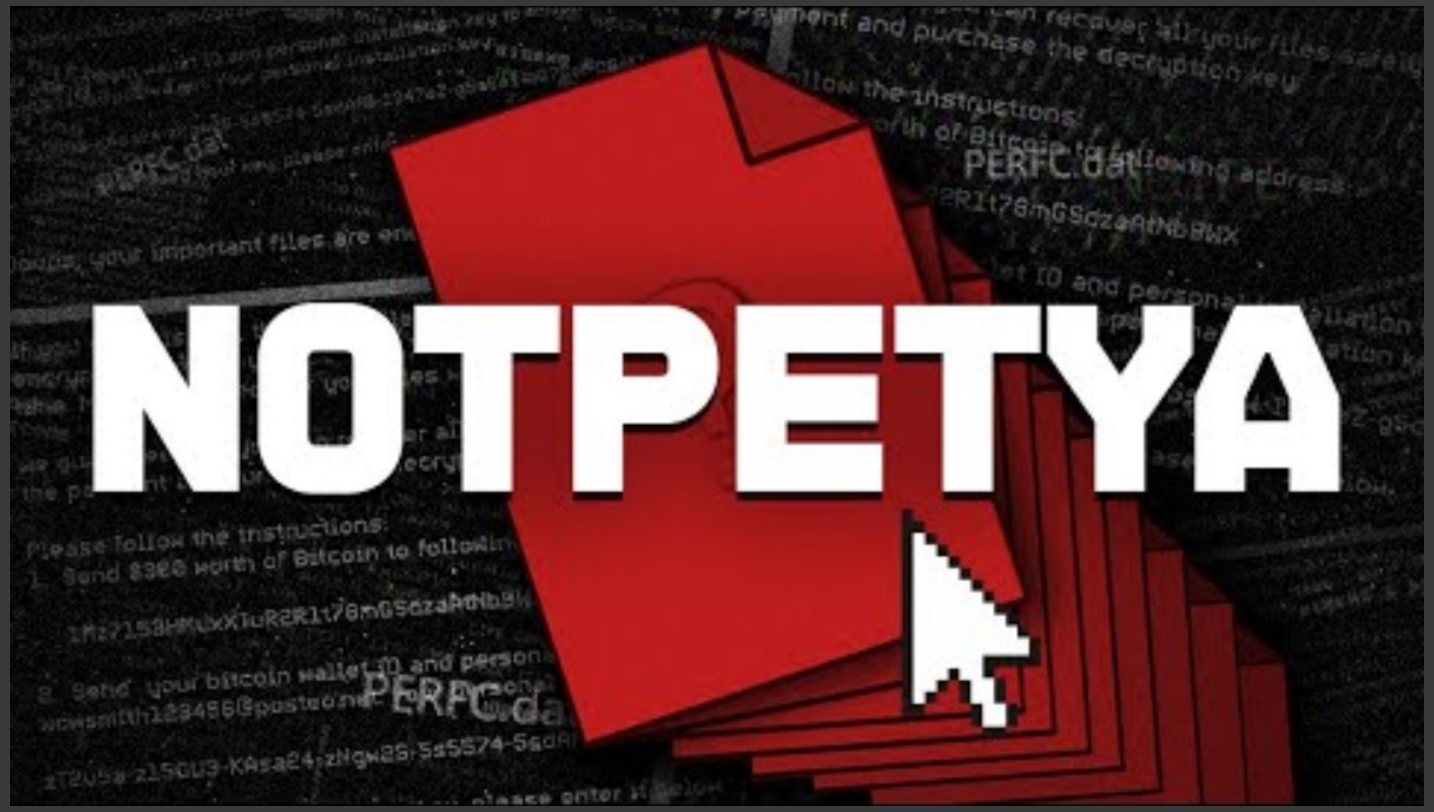
ŹRÓDŁO:
https://youtu.be/Xe5IZutxd58?si=v_jgwutxd7mP_-g4

Polecam!

ĆWICZENIE KOMEND LINUXOWYCH:

https://technikinformatyk.pl/soisk/trening-linux-komendy-terminala

Polecam!



ŹRÓDŁO:
https://youtu.be/3-MSlNVqzYY