SK	Dokumentacja projektu
Autor	Bartłomiej Król, 125136
Kierunek, rok	Informatyka, II rok, st. stacjonarne (3,5-l)
Temat projektu	Skrypt do Sprawdzania Informacji DNS i IP

Wstęp

Opis Projektu

Skrypt powłoki dns_check.sh jest narzędziem do automatycznego sprawdzania informacji o domenach i adresach IP. Narzędzie odczytuje nazwy domen i adresy IP z pliku tekstowego, a następnie wykonuje zapytania WHOIS i DNS, aby uzyskać informacje o właścicielu, statusie oraz dacie wygaśnięcia domeny. Wyniki zapisywane są do raportu tekstowego.

Wymagania Systemowe

System operacyjny:

Unix-like (np. Linux, macOS)

Narzędzia:

whois, dig, grep, xargs

Interpreter bash:

/bin/bash

Narzędzia

whois

Narzędzie whois służy do uzyskiwania informacji o rejestracji domeny. Pozwala uzyskać szczegóły takie jak status domeny (czy jest zajęta), dane właściciela oraz datę wygaśnięcia domeny.

Zasada działania: `whois` wysyła zapytanie do odpowiedniego serwera WHOIS, który przechowuje informacje o rejestracjach domen. Odpowiedź zawiera szczegółowe dane dotyczące domeny, w tym status, dane właściciela oraz datę wygaśnięcia.

dig

Narzędzie dig (Domain Information Groper) jest używane do wykonywania zapytań DNS. W skrypcie jest używane do wykonywania zapytań reverse DNS, które zamieniają adresy IP na odpowiadające im nazwy domen. Dzięki temu można sprawdzić, czy dany adres IP jest powiązany z jakąś domeną.

Zasada działania: `dig` wysyła zapytanie do serwerów DNS, aby uzyskać informacje o danej nazwie domeny lub adresie IP. W przypadku reverse DNS lookup, `dig` zamienia adres IP na nazwę domeny.

grep

Narzędzie grep służy do wyszukiwania wzorców tekstowych w plikach lub danych wejściowych. W skrypcie jest używane do wyodrębniania specyficznych informacji z wyników zapytań WHOIS, takich jak status domeny, dane właściciela oraz data wygaśnięcia.

xargs

Narzędzie xargs służy do przekształcania danych wejściowych i przekazywania ich jako argumenty do innych poleceń. W skrypcie dns_check.sh jest używane do usuwania białych znaków z początku i końca linii tekstowych odczytywanych z pliku wejściowego.

Użycie

Uruchomienie Skryptu

W konsoli należy uruchomić skrypt komendą:

./dns_check.sh <input_file>

gdzie <input_file> to ścieżka do pliku tekstowego zawierającego listę domen i adresów IP do sprawdzenia.

Przykładowe Dane Wejściowe

Plik tekstowy input.txt powinien zawierać jedną domenę lub jeden adres IP na linię, np.:

example.com

8.8.8.8

google.com

192.168.1.1

facebook.com

Wyjście

Skrypt generuje plik raportu o nazwie Raport_DNS_<data>_<czas>.txt, gdzie <data> i <czas> to odpowiednio data i czas uruchomienia skryptu. Przykładowy plik wyjściowy:

Domena example.com jest zajęta.

Właściciel domeny: Nieznany

Data wygaśnięcia domeny: Registry Expiry Date: 2024-08-13T04:00:00Z

Adres IP 8.8.8.8 jest powiązany z domeną: dns.google

Domena dns.google jest zajęta.

Właściciel domeny: Registrant Name: REDACTED FOR PRIVACY

Data wygaśnięcia domeny: Registry Expiry Date: 2025-04-16T22:57:01Z

Domena google.com jest zajęta.

Właściciel domeny: Registrant Organization: Google LLC

Data wygaśnięcia domeny: Registry Expiry Date: 2028-09-14T04:00:00Z

Adres IP 192.168.1.1 jest powiązany z domeną: myrouter.home

Domena myrouter.home jest zajęta.

Właściciel domeny: Nieznany

Data wygaśnięcia domeny: Nieznana

Domena facebook.com jest zajęta.

Właściciel domeny: Registrant Organization: Facebook, Inc.

Data wygaśnięcia domeny: Registry Expiry Date: 2033-03-30T04:00:00Z

Struktura Skryptu

Wskazanie interpretera skryptu

```
#!/bin/bash
```

Sprawdzenie czy podano plik wejściowy

```
if [ $# -ne 1 ]; then
  echo "Usage: $0 <input_file>"
  exit 1
fi

input_file=$1
```

Utworzenie nazwy pliku wyjściowego

```
output_file="Raport_DNS_$(date +%Y-%m-%d_%H-%M).txt"
```

Funkcja do sprawdzania domeny

```
check_domain() {
  domain=$1
  echo "Sprawdzanie domeny: $domain"

  # Sprawdzenie czy domena jest zajęta
  whois_info=$(whois $domain)
  if echo "$whois_info" | grep -qi "No match"; then
    echo "Domena $domain jest wolna." >> $output_file
    return
  else
    echo "Domena $domain jest zajęta." >> $output_file
  fi
```

```
  # Właściciel domeny
    owner=$(echo "$whois_info" | grep -iE "Registrant Name|Registrant Organization|Organization" | head -n 1)
  if [ -z "$owner" ]; then
    owner="Nieznany"
  fi
  echo "Właściciel domeny: $owner" >> $output_file
  # Data wygaśnięcia
 expiry_date=$(echo "$whois_info" | grep -iE "Expiry Date|Expiration Date|paid-till" | head -n 1)
  if [ -z "$expiry_date" ]; then
    expiry_date="Nieznana"
  fi
  echo "Data wygaśnięcia domeny: $expiry_date" >> $output_file
  echo "" >> $output_file
}
```

Funkcja do sprawdzania adresu IP

```
check_ip() {
  ip=$1
  echo "Sprawdzanie adresu IP: $ip"
  # Reverse DNS lookup
  domain=$(dig -x $ip +short)
  if [ -z "$domain" ]; then
    echo "Adres IP $ip nie jest powiązany z żadną domeną." >> $output_file
    echo "" >> $output_file
  else
    domain=$(echo $domain | sed 's/\.$//') # Usunięcie końcowej kropki
    echo "Adres IP $ip jest powiązany z domeną: $domain" >> $output_file
    check_domain $domain
  fi
}
```

Główna pętla przetwarzająca plik wejściowy

```
while IFS= read -r line || [[ -n "$line" ]]; do

  # Usuwanie białych znaków z początku i końca linii
  line=$(echo "$line" | xargs)

  # Pomijanie pustych linii
  if [ -z "$line" ]; then
    continue
  fi
  # Sprawdzanie czy linia jest adresem IP
  if [[ $line =~ ^[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+$ ]]; then
    check_ip $line
  else
    check_domain $line
  fi
done < "$input_file"

echo "Raport zapisano do pliku $output_file"
```

Uwagi

Upewnij się, że masz odpowiednie uprawnienia do wykonywania skryptu (chmod +x dns_check.sh).

Skrypt działa na systemach Unix-like z zainstalowanymi narzędziami whois i dig.

Wyniki zapytania WHOIS mogą się różnić w zależności od rejestratora domeny i dostawcy usług DNS.