DNS / Hosts

Powszechnie używane narzędzia DNS

```
nslookup
host
whois
ping
dig
traceroute
IntoDNS
Digdns
MxToolbox
DNSRecon
Nmap
DNSEnum
Maltego
Amass
Subfinder
Massdns
Subjack
```

Zarządzanie nazwą hosta w systemie

```
### Przykład nazwy hosta łączącego się z Internetem za pomocą usługi Comcast

c-62=121-44-64.hsd1.co.comcast.net

### wyświetla lub ustawia systemową nazwę komputera
hostname
### wyświetla lub ustawia nazwę domeny NIS/YP
domainname
### wyświetla lub ustawia systemową nazwę domeny NIS/YP
ypdomainname
### wyświetla lub ustawia systemową nazwę domeny NIS/YP
nsdomainname
### wyświetla nazwę domenową systemu
dnsdomainname
```

Edycja nazwy hosta

```
### edycja pliku odpowiadającego za nazwę hosta

vi /etc/hostname

### Można też skorzystać z polecenia echo

echo "przykładowa_nazwa_hosta" > /etc/hostname

### FQDN jest to zazwyczaj nazwa hosta w połączeniu z nazwą domenową. W celu jej
sprawdzenia należy uruchomić polecenie poniżej
```

```
hostname -fqdn

### W celu wyświetlenia wszystkich adresów komputera oraz pełnych nazw domenowych i informacji o wersji należy skorzystać z trzech argumentów -V, -A, -A

hostname -VAI
```

Plik /etc/hosts

Zbudowany jest z dwóch części: adresu IP i adresu domenowego #

```
### Przykładowa treść pliku poniżej

127.0.0.1 localhost
```

Blokowanie stron

W celu zablokowania stron należy przypisać ich adres domenowy do adresu IP, który nie istnieje. Takim adresem jest 0.0.0.0 #

```
### Poniżej treść pliku /etc/hosts dla blokady domeny google.com

0.0.0.0 google.com
```

Czyszczenie pamięci podręcznej DNS

```
### Debian/Ubuntu ###

sudo service network-manager restart

### Linux Mint ###

sudo /etc/init.d/dns-clean start

### Linux with systemd ###

sudo systemctl restart network.service

### Fedora Linux ###

sudo systemctl restart NetworkManager.service

### Arch Linux/Manjaro with Network Manager ###

sudo systemctl restart NetworkManager.service

### Arch Linux/Manjaro with Wicd ###

sudo systemctl restart wicd.service

### RHEL/Centos ###
```

```
sudo /etc/init.d/network restart

### FreeBSD ###

sudo service nscd restart
```

Przydatne narzędzia i funkcje

```
### Skrypt do automatycznego analizowania pliku hosts
Maze https://github.com/tanrax/maza-ad-blocking
### Możesz  też w łatwiejszy sposób dodawać i usuwać informacje z pliku hosta
korzystając z narzędzia poniżej
Hostile https://github.com/feross/hostile
### Sieciowy serwer DHCP  i bloker reklam działający na Raspberry Pi
Pihole https://pi-hole.net/
### Blokowanie reklam i złośliwego oprogramowania za pośrednictwem lokalnego serwera
DNS
block-ads-via-dns https://github.com/mueller-ma/block-ads-via-dns
### Blokowanie reklam i złośliwego oprogramowania. Możliwość skorzystania z kontroli
rodzicielskiej
DualServer https://scripttiger.github.io/dualserver/
### Blokada reklam i złośliwego oprogramowania
Unbound https://deadc0de.re/articles/unbound-blocking-ads.html
```

DNS od strony Pentestera

Zanim przystąpimy do ataku warto zainstalować parę narzędzi #

```
### subfinder
sudo apt-get install subfinder

### ParamSpider
git clone https://github.com/devanshbatham/ParamSpider cd ParamSpider
pip3 install -r requirements.txt

### amass
sudo apt-get install amass

### subbrute
git clone https://github.com/TheRook/subbrute
cd subbrute

### EyeWitness
git clone https://github.com/FortyNorthSecurity/EyeWitness
cd EyeWitness/Python

### subjack
go get github.com/haccer/subjack
```

Można wyróżnić trzy główne fazy ataku. Rekonesans, eksploitacja, działania poeksploitacyjne. My zajmiemy się fazą pierwszą czyli rekonesansem, który może być

podzielony na dwie części

- rekonesans pasywny https://deadc0de.re/articles/unbound-blocking-ads.htmly
- rekonesans aktywny W przypadku rekonesansu pasywnego nie łączmy się z ofiarą. W tym przypadku możemy skorzystać z takich narzędzi jak Google Dorking # #

```
### # Przeszukiwanie Googla w poszukiwaniu wszystkich stron w domenie nadrzędnej
domain.com
site:domain.com

### Można też szukać poddomen pasywnie przy użyciu strony
https://crt.sh/
### która zwraca listę poddomen oraz odcisk certyfikatu
```

a także przy użyciu narzędzi do scrapowania domen czyli wyszukaniu nazw poddomen korzystając z otwartych źródeł informacji #

```
### Enumeracja domen korzystająca z takich źródeł jak Shodan, VirusTotal itd.

subfinder -d example.com

### Szukanie punktów końcowych tzw. endpointów

python3 paramspider.py -d example.com --output out.txt --level high
```

W przypadku rekonesansu aktywnego będą to takie narzędzia jak #

```
### Enumeracja aktywna subdomen
amass enum -active -d example.com -r

### W przypadku narzędzi subbrute i massdns możemy wykorzystać je jednocześnie.
Najpierw korzystamy z polecenia subbrute.py i jako argument podajemy listę domen, a
jako drugi, domenę którą atakujemy. Dzięki temu możemy brute-forcować poddomeny
korzystając z naszej listy. Te wyniki przekazujemy do polecenia massdns, która do
działania potrzebuje listy serwerów, które będzie odpytywała. W tym przypadku taka
lista znajduje się w pliku resolvers.txt
subbrute.py /home/karmaz/words/dns example.com |
/home/karmaz/tools/massdns/bin/massdns -r
/home/karmaz/tools/massnds/lists/resolvers.txt -t A -o S -w massdns.txt

###  Szczegółowe informacje o domenie w tym rekordy MX itd. (transfer stref)
dnsrecon -t axfr -d example.com
### Warto skorzystać też z polecenia host do określenia dostępności poddomen

host

### Ciekawym narzędziem rekonesansu aktywnego jest EyeWitness, które pozwala na
zrobienie zrzutu ekranu subdomen
### Zrzuty ekranu wszystkich domen z pliku domeny.txt zapisane w folderze screen
python3 EyeWitness.py -f domeny.txt -d screen

### Na sam koniec warto sprawdzić możliwość przejęcia domen
subjack -w domeny.txt -t 100 --timeout 30 -o wyniki.txt -ssl
```

Polecenie host

```
### informacje o hostach domeny example.com

host example.com

### To co wyżej, ale z bardziej szczegółowymi wynikami

host -a example.com

### Wyświetla identyfikator szesnastkowy komputera

hostid
```

Plik konfiguracyjny /etc/resolv.conf

Określa on kolejność przeszukiwania domen i zawiera adresy serwerów nazw DNS

```
### Przykładowa konfiguracja

nameserver 127.0.0.53
options edns0 trust-ad
search localdomain

### Dyrektywa nameserver wskazuje na adres IP serwera nazw
### Listę wyszukiwania na podstawie domeny lokalnej określa search
```

Identyfikator komputera w trybie szesnastkowym

```
hostid
```

Polecenie nslookup

```
# Zwraca informacje o serwerze nazw sieciowych, domen oraz ich adresów IP

nslookup example.com

## Instalacja nslookup w różnych systemach ##

## CentOs i RHEL ##
sudo yum install bind-utils
## Fedora ##
sudo dnf install bind-utils
## Debian i Ubuntu ##
sudo apt-get install dnsutils
```

Zapytania nslookup

```
### Zapytanie o rekord ns tj. wszystkie serwery z konfiguracją danej domeny

nslookup -type=ns
```

```
### Zapytanie o rekord mx związany z serwerami pocztowymi

nslookup -type=mx
```

Wyszukiwanie błędów w konfiguracji DNS

Jednym z narzędzi dostarczających podaną funkcjonalność jest IntroDNS dostępne pod linkiem poniżej https://intodns.com/

Polecenie dig

```
### Narzędzie do sprawdzania nazw DNS

dig example.com

### sprawdzenie wersji narzędzia dig

dig -v

### Sprawdzenie szczegółowej odpowiedzi z domeny

dig +noall +answer example.com

### szukanie nazwy host po adresie IP

dig -x

### Instalacja dig ###

## Ubuntu i Debian ##
sudo apt-get install dnsutils
## Fedora i CentOS ##
sudo yum install bind-utils
## Arch Linux ##
sudo pacman -S bind-tools
```

- Zapytanie o rekordy A - Aby uzyskać listę wszystkich adresów dla nazwy domeny, użyj opcji:
- Zapytanie o rekordy CNAME - Aby znaleźć nazwę domeny aliasu, użyj opcji cname:
- Zapytanie o rekordy TXT - Użyj opcji txt, aby pobrać wszystkie rekordy TXT dla określonej domeny:
- Sprawdzanie rekordów MX – Aby uzyskać listę wszystkich serwerów poczty dla określonej domeny
- Zapytanie o rekordy NS - Aby znaleźć wiarygodne serwery nazw dla naszej konkretnej domeny
- Zapytanie o wszystkie rekordy - aby uzyskać listę wszystkich rekordów DNS dla określonej domeny
- Odwrotne wyszukiwanie DNS - Aby wyszukać nazwę hosta powiązaną z określonym adresem IP, użyj opcji -x
- Zapytania zbiorcze - Odpytujemy domeny wymienione w pliku domains.txt

Zachowaniem polecenia dig można sterować, ustawiając opcje dla poszczególnych użytkowników w pliku ${HOME}/.digrc. Jeśli plik .digrc znajduje się w katalogu .digrc użytkownika, określone w nim opcje są stosowane przed argumentami wiersza poleceń.

Na przykład, jeśli chcesz wyświetlić tylko sekcję odpowiedzi, otwórz edytor tekstu i utwórz następujący plik ~/.digrc : +nocmd +noall +answer.

Narzędzie dig w sieci

Narzędzie dig jest również dostępne w sieci pod linkami:

- https://www.digdns.info/index.php?domain=
- https://toolbox.googleapps.com/apps/dig/

A także jako wtyczka do Google Chrome

- https://chrome.google.com/webstore/detail/digdns/fggjddhipknbbgolpdomeocbpmedbmld?hl=pl

Whois

```
### Polecenie służące do odpytywania się nazwy domen, bloków IP, serwerów nazw oraz innych

whois

### Link do narzędzia online

https://www.whois.net/
```

Mxtoolbox

Bardzo wszechstronne narzędzie łączące ze sobą wiele programów w jeden. Dostępne jest pod tym linkiem: https://mxtoolbox.com/NetworkTools.aspx

Transfer stref

Transfer stref polega na kopiowaniu wpisów z serwera nadrzędnego do podrzędnego #

```
### W celu wykonania transferu DNS należy znaleźć najpierw adres jednego podrzędnego adresu DNS. Można skorzystać z polecenia host

host -ns example.com

### Następnie wystarczy dokonać transferu stref między serwerem nadrzędnym, a podrzędnym

host -l  example.com ns1.example.com
```

DNS Poisoning

To technika, która oszukuje serwer DNS, aby uwierzył, że otrzymał autentyczne informacje, podczas gdy w rzeczywistości tak się nie stało. Powoduje to zastąpienie fałszywego adresu IP na poziomie DNS, gdzie adresy internetowe są konwertowane na numeryczne adresy IP.

Ćwiczenie:

1. Otwórz terminal w Kali Linux i wpisz `nano etter.dns`. Ten plik zawiera wszystkie wpisy dotyczące adresów DNS, które są używane przez Ettercap do rozwiązywania adresów nazw domen.
2. W tym pliku dodamy fałszywy wpis „Facebook”. Jeśli ktoś będzie chciał otworzyć Facebooka, zostanie przekierowany na inną stronę. Teraz wstaw wpisy pod słowami „redirect it to www.linux.org”. Na powyższym przykładzie widać zmodyfikowane wpisy.
3. Następnie zapisz plik, w przypadku edytora tekstowego nano wciśnij kombinację klawiszy `CTRL + X`
4. Następnie cały proces jest taki sam, aby rozpocząć zatrucie ARP.
5. Otwórz terminal i wpisz `ettercap -G`, aby uruchomić graficzną wersję Ettercap.
6. Kliknij zakładkę „sniff” na pasku menu i wybierz „unified sniffing” i kliknij OK, aby wybrać interfejs. Będziemy używać „eth0”, co oznacza połączenie Ethernet.
7. Teraz kliknij zakładkę „hosty” na pasku menu i kliknij „skanuj w poszukiwaniu hostów”. Rozpocznie skanowanie całej sieci w poszukiwaniu żywych hostów.
8. Następnie kliknij zakładkę „hosty” i wybierz „listę hostów”, aby zobaczyć liczbę hostów dostępnych w sieci. Ta lista zawiera również domyślny adres bramy.
9. Teraz musimy wybrać cele. W MITM naszym celem jest maszyna hosta, a trasa będzie adresem routera do przekazywania ruchu. Podczas ataku MITM osoba atakująca przechwytuje sieć i podsłuchuje pakiety. Dlatego dodamy ofiarę jako „cel 1”, a adres routera jako „cel 2”. W tym scenariuszu naszym celem jest „192.168.121.129”, a router to „192.168.121.2”. Dlatego dodamy cel 1 jako adres IP ofiary i cel 2 jako adres IP routera.
10. Kliknij „start” i wybierz “start sniffing”. Spowoduje to zatruwanie sieci przez ARP, co oznacza, że włączyliśmy naszą kartę sieciową w „trybie promiscuous” i można teraz podsłuchać lokalny ruch.
11. Po uruchomieniu zatrucia ARP kliknij „plugins” na pasku menu i wybierz wtyczkę „dns_spoof”.
12. Po aktywacji DNS_spoof zobaczysz w wynikach, że facebook.com zacznie fałszować adres IP Google za każdym razem, gdy ktoś wpisze go w przeglądarce. Oznacza to, że użytkownik otrzymuje w przeglądarce stronę Google zamiast facebook.com.

W tym ćwiczeniu widzieliśmy, jak ruch sieciowy można przeszukiwać za pomocą różnych narzędzi i metod.

DNS z TLS

```
### Narzędzie służące do szyfrowania zapytań DNS
stubby

## Instalacja na systemach Debian i Ubuntu ##
sudo apt-get install stubby

### Uruchamianie usługi stubby
sudo systemctl start stubby
### Włączenie usługi stubby
sudo systemctl enable stubby

### Sprawdzenie adresu IP, portu na którym nasłuchuje narzędzie stubby
```

```
sudo netstat -Inptu | grep stubby

### Uruchamianie ponownie usługi Network Manager
sudo systemctl restart NetworkManager
```