TBBA

Raport na projekt zespołowy na temat:

Badanie bezpieczeństwa aplikacji. Bezpieczeństwo prywatności vs narzędzia typu Pegasus i inne. Skuteczne metody zabezpieczenia komputerów, sieci.

**Na początek zostały zebrane potrzebne informacje w celu pojęcia działania narzędzia Pegasus i skutecznych metod obrony przed nim i innymi narzędziami**

# 1.Zebranie informacji dotyczących tematu.

Złośliwe oprogramowanie to szkodliwe aplikacje lub kody, które uniemożliwiają lub zakłócają normalne korzystanie z urządzeń w punkcie końcowym . Gdy urządzenie zostanie zainfekowane złośliwym oprogramowaniem, może dojść do nieautoryzowanego dostępu, zaatakowania danych lub zablokowania urządzenia w przypadku niezapłacenia okupu.

Osoby rozpowszechniające złośliwe oprogramowanie, nazywane cyberprzestępcami, kierują się chęcią zysku. Używają one zainfekowanych urządzeń do przeprowadzania ataków, takich jak pozyskiwanie danych uwierzytelniających w usługach bankowości, zbieranie danych osobowych na sprzedaż, sprzedaż dostępu do zasobów komputerowych lub wyłudzanie opłat od ofiar.

**Czym jest Pegasus?**

Pegasus to zaawansowane oprogramowanie szpiegujące rozwijane przez izraelską firmę NSO Group, które jest zdolne do infiltracji w smartfonach, zarówno iPhone'ach, jak i urządzeniach z systemem Android. Pozwala ono na zdalne monitorowanie i zbieranie informacji z zainfekowanych urządzeń bez wiedzy użytkownika. Jest zdolny do przechwytywania wiadomości tekstowych, danych z połączeń telefonicznych, e-maili, zdjęć, historii przeglądarki oraz może aktywować mikrofon i kamerę urządzenia, co umożliwia podsłuchiwanie otoczenia użytkownika w czasie rzeczywistym. Oprogramowanie to jest sprzedawane wyłącznie rządom i agencjom wywiadowczym, a jego zastosowanie jest oficjalnie ograniczone do walki z terroryzmem i przestępczością. Jednakże, z biegiem czasu pojawiły się liczne doniesienia sugerujące, że był wykorzystywany do celów inwigilacji obrońców praw człowieka, dziennikarzy, polityków i innych osób postrzeganych jako zagrożenie dla rządów lub ich interesów, co wywołało międzynarodową kontrowersję i debatę na temat prywatności, nadużycia władzy oraz kontroli nad technologiami szpiegującymi.

**Wektory Infekcji Pegasusa**

**SMS Phishing**: Atakujący mogą wykorzystać phishing SMS-owy, aby wysyłać złośliwe wiadomości tekstowe z linkami do zainfekowanych stron internetowych lub załącznikami zawierającymi szkodliwe oprogramowanie. Ten wektor ataku może działać na smartfony i tablety pracujące na systemach operacyjnych iOS i Android.

**Złośliwe Linki**: Pegasus może być rozpowszechniany za pomocą złośliwych linków wysyłanych za pośrednictwem poczty elektronicznej, aplikacji do komunikacji lub platform społecznościowych. Nieświadomi użytkownicy mogą kliknąć te linki, co prowadzi do zainstalowania szpiegowskiego oprogramowania.

**Zero-Day Exploits**: NSO Group jest znana z wykorzystywania luk zerodniowych w systemach operacyjnych, takich jak iOS i Android, do instalacji Pegasusa na urządzeniach docelowych. Exploity te wykorzystują luki w zabezpieczeniach, które nie są jeszcze znane dostawcy oprogramowania ani publicznie.

**Network Injection**: Pegasus może być wstrzykiwany do ruchu sieciowego, co pozwala na zainstalowanie go na urządzeniach, gdy użytkownicy łączą się z kompromitowanymi sieciami Wi-Fi lub odwiedzają kompromitowane strony internetowe.

**Forced Installation**: W niektórych przypadkach Pegasus może być instalowany siłą na urządzeniach docelowych poprzez wykorzystanie słabości w zabezpieczeniach systemu operacyjnego lub aplikacji.

**Physical Access**: W rzadkich przypadkach Pegasus może być instalowany na urządzeniu docelowym poprzez uzyskanie fizycznego dostępu do niego. Może to obejmować techniki takie jak manipulowanie urządzeniem lub wykorzystywanie luk poprzez połączenia USB.

**App Stores**: Występują doniesienia o Pegasusie podszywającym się pod autentyczne aplikacje w sklepach z aplikacjami innych firm. Użytkownicy mogą nieświadomie pobrać i zainstalować te aplikacje, instalując przy tym szpiegowskie oprogramowanie na swoich urządzeniach.

**Interception of Software Updates**: Pegasus może przechwycić legalne aktualizacje oprogramowania i wstrzyknąć się do procesu aktualizacji, co pozwala na zainstalowanie szpiegowskiego oprogramowania na urządzeniach docelowych, gdy użytkownicy pobierają i instalują aktualizacje.

**Third-Party Services**: Pegasus może wykorzystywać luki w zabezpieczeniach usług lub aplikacji innych firm zainstalowanych na urządzeniach docelowych, aby uzyskać dostęp i zainstalować się.

**Social Engineering**: Pegasus może być także instalowany za pomocą taktyk inżynierii społecznej, gdzie atakujący manipulują użytkownikami, aby dobrowolnie pobierali i instalowali szpiegowskie oprogramowanie, często podając się za autentyczne podmioty lub wykorzystując perswazyjne metody.

**Mimicking System Updates**: Pegasus może przedstawiać się jako aktualizacja systemowa lub łata, oszukując użytkowników, aby pobrali i zainstalowali go pod pretekstem poprawy wydajności lub bezpieczeństwa urządzenia.

**Supply Chain Compromise**: Pegasus może infiltrować łańcuch dostaw oprogramowania lub sprzętu, umożliwiając jego wstępną instalację na urządzeniach przed dostaniem się do użytkowników końcowych. Metoda ta może być stosowana w celowanych scenariuszach, gdzie dostęp do konkretnego przemysłu lub organizacji jest możliwy poprzez zainfekowanych dostawców.

**Bluetooth Exploitation**: Pegasus może wykorzystywać luki w połączeniach Bluetooth do zainstalowania się na pobliskich urządzeniach, które mają włączony Bluetooth. Ta metoda może być stosowana w celowanych scenariuszach, gdzie fizyczna bliskość do celu jest możliwa.

**Social Media Messaging**: Pegasus może być rozpowszechniany poprzez wiadomości bezpośrednie lub załączniki wysyłane za pośrednictwem platform społecznościowych, wykorzystując zaufanie wypracowane w sieciach społecznościowych, aby przekonać użytkowników do pobrania i zainstalowania szpiegowskiego oprogramowania.

**Collaboration Tools:** Pegasus może wykorzystywać luki w narzędziach do współpracy używanych przez docelowe osoby lub organizacje, takich jak oprogramowanie do wideokonferencji lub platformy do udostępniania plików, w celu dostarczania i instalowania oprogramowania szpiegującego.

**PWNYOURHOME:** Ta metoda skupia się na systemie iOS 15 i iOS 16. Jest to proces dwuetapowy, gdzie na każdym z etapów wykorzystywany jest inny komponent systemowy urządzenia. Pierwszy etap wykorzystuje aplikację HomeKit, a drugi etap wykorzystuje aplikację iMessage. Ta metoda była aktywnie wykorzystywana w październiku 2022 roku.

**FINDMYPWN:** Znana również jako metoda infekcji skierowana na urządzenia z systemem iOS 15, opiera się prawdopodobnie na dwuetapowym procesie. Pierwszy etap infekcji wykorzystuje aplikację Find My, a drugi etap ponownie opiera się na wykorzystaniu aplikacji iMessage.

**LATENTIMAGE:** Jest to kolejna metoda infekcji, która była stosowana do ataków w 2022 roku. Wykorzystuje funkcję Find My, jednak bazuje na innych aspektach technicznych i podatnościach systemu.

Metody te nie wymagają interakcji ze strony użytkownika, co oznacza, że infekcja może nastąpić bez kliknięcia w złośliwy link czy pobrania zainfekowanego pliku. To znacząco zwiększa skuteczność ataków i utrudnia obronę przed nimi.

W odpowiedzi na te zagrożenia, Apple wprowadziło funkcję Lockdown Mode w systemie iOS 16, mającą na celu zapewnienie użytkownikom dodatkowej ochrony przed tego typu atakami. Funkcja ta może ograniczać niektóre funkcje systemowe i aplikacje, aby zmniejszyć ryzyko infekcji. Jednak badacze Citizen Lab zauważyli, że NSO Group opracowało metody obchodzenia tej funkcji, co umożliwia infekcję nawet przy jej aktywacji​​.

Powyższe informacje świadczą o ciągłym wyścigu zbrojeń między twórcami oprogramowania szpiegującego a firmami technologicznymi starającymi się chronić swoich użytkowników przed nieautoryzowaną inwigilacją.

**Jak Działa Pegasus?**

Przejmowanie danych: Pegasus może zostać wykorzystany do przechwytywania danych osobowych lub poufnych informacji. Atakujący wprowadzają model w taki stan, który generuje teksty zawierające poufne dane, do których atakujący ma pełny dostęp i może z nich korzystać jak chce.

Wycieki informacji: Atakujący mogą próbować wykorzystać Pegasusa do wygenerowania tekstów zawierających wrażliwe informacje, które mogłyby zostać nielegalnie ujawnione lub wykorzystane przeciwko organizacji lub jednostkom.

Ataki na integralność danych: Pegasus może być używany do generowania fałszywych informacji lub manipulowania opiniami poprzez propagowanie dezinformacji. Atakujący wprowadzają model w stan, który skłania go do generowania nieprawdziwych lub stronniczych treści.

Ataki z wykorzystaniem modelu: Model Pegasus może być również wykorzystywany jako narzędzie do przeprowadzania innych rodzajów ataków, takich jak ataki typu Denial of Service (DoS), w których generowane są ogromne ilości tekstu w celu zakłócenia działania systemów lub naruszenia integralności danych.

**Metody Zabezpieczeń Przed Pegasusem**

* Częste aktualizowanie oprogramowania
* Ograniczenie dostępności aplikacjom
* Renomowane oprogramowanie antywirusowe
* Używanie aplikacji szyfrowanych
* Używanie zaufanych źródeł

# 2.1 Poznanie zabezpieczeń.

**Jako świadomy użytkownik, powinieneś przede wszystkim:**

* odwiedzać wyłącznie bezpieczne, sprawdzone strony internetowe – unikaj zwłaszcza tych witryn, na których pojawiają się komunikaty o zagrożeniu oraz serwisów zawierających treści pirackie lub pornograficzne;
* zrezygnować z pobierania programów oraz plików z niesprawdzonych albo nielegalnych źródeł;
* uważać na reklamy, które widzisz w Internecie - Weryfikacja reklamodawców przeprowadzana jest zazwyczaj przez wszelkie platformy w sposób automatyczny i jest niewystarczająca
* nie otwierać plików albo linków, które pochodzą z niepewnych źródeł – zwłaszcza wysyłanych z nieznanych adresów na Twoją skrzynkę mailową;
* blokować wyskakujące okna w przeglądarce, które mogą być źródłami złośliwego oprogramowania.

**1.Instalacja oprogramowania antywirusowego**

To pierwszy krok do zabezpieczenia komputera czy telefonu przed złośliwym oprogramowaniem. Do Twojej dyspozycji jest wiele sprawdzonych programów antywirusowych, takich jak Norton, Kaspersky, Bitdefender, McAfee czy Surfshark, które nie tylko powiadomią Cię o obecności wirusa na danej stronie czy w pliku, ale również skutecznie usuną potencjalne zagrożenie.

Możesz korzystać zarówno z bezpłatnego oprogramowania, jak też wersji płatnych, które są rekomendowane przez specjalistów od cyberbezpieczeństwa. Wynika to przede wszystkim z wielu dodatkowych funkcji, takich jak:

* ochrona poczty e-mail czy bankowości internetowej;
* firewall, czyli zapora sieciowa;
* zabezpieczanie sieci WiFi;
* filtrowanie stron internetowych pod kątem złośliwego oprogramowania;
* VPN, czyli szyfrowanie ruchu sieciowego.

**2.Regularne aktualizacje systemu i aplikacji**

Programy, z których korzystasz na co dzień, mogą zostać zainfekowane przez różnego rodzaju wirusy szczególnie wtedy, gdy nie będą na bieżąco aktualizowane. Dzięki aktualizacjom możliwe będzie załatanie różnego rodzaju dziur i wyeliminowanie błędów, które mogą zostać skrzętnie wykorzystane przez hakerów. Dotyczy to również systemu operacyjnego, z którego korzystasz.

Na szczęście zarówno na komputerach, jak i telefonach czy tabletach możliwe jest włączenie automatycznych aktualizacji. Dzięki nim nie musisz samodzielnie pobierać oraz instalować łatek i możesz wybrać czas aktualizacji dopasowany do swoich potrzeb (np. w nocy, gdy nie korzystasz z urządzenia). Rekomendowane jest również korzystanie z systemów i aplikacji, które posiadają zapewnione wsparcie producenta.

**3.Korzystanie z bezpiecznej przeglądarki**

Jeżeli chcesz uniknąć złośliwego oprogramowania, zainstaluj na komputerze lub w telefonie sprawdzoną przeglądarkę internetową, w której zastosowano szereg zabezpieczeń. Google Chrome, Mozilla Firefox czy Opera, a więc te najbardziej znane, informują o zagrożeniu i blokują dostęp do zainfekowanych witryn, a nawet uniemożliwiają instalację złośliwego oprogramowania.

Bezpieczna przeglądarka internetowa to również taka, która zapewnia możliwość instalowania dodatkowych wtyczek i rozszerzeń. Mowa tu o rozwiązaniach, które umożliwiają nawiązywanie połączeń za pomocą szyfrowanego protokołu, skanują witryny pod kątem złośliwego oprogramowania, pozwalają generować bezpieczne hasła albo blokują niepożądane skrypty. Większość takich wtyczek jest darmowa.

# 2.2 Poznać działanie aplikacji i narzędzia atakującego, komputer bądź sieć.

**Rodzaje złośliwego oprogramowania:**

* **Wirusy:** Programy, które mogą samoreplikować się, wstawiając kopie samego siebie do innych programów lub dokumentów. Wirusy mogą prowadzić do uszkodzenia danych, spowolnienia systemu lub nieautoryzowanego dostępu do informacji.
* **Trojany:** Złośliwe oprogramowanie ukryte w pozornie nieszkodliwym pliku lub programie. Po aktywacji, trojan może dać atakującemu zdalny dostęp do zainfekowanego systemu, co umożliwia kradzież danych lub instalację dodatkowego złośliwego oprogramowania.
* **Robaki:** Samoreplikujące się programy, które rozprzestrzeniają się w sieciach komputerowych. Robaki mogą obciążać zasoby systemowe, powodując ich niedostępność (np. ataki DDoS) lub służyć do rozpowszechniania innych rodzajów złośliwego oprogramowania.
* **Ransomware (programy wymuszające okup):** Blokuje dostęp do systemu lub danych użytkownika, żądając od niego zapłaty okupu za odblokowanie. Ransomware może szyfrować pliki, uniemożliwiając dostęp do nich bez klucza deszyfrującego.
* **Spyware (programy szpiegujące):** Zbiera informacje o użytkowniku bez jego wiedzy, takie jak dane logowania, historię przeglądania, czy informacje kart kredytowych. Spyware może być wykorzystywane do kradzieży tożsamości lub fraudów finansowych.

**Metody ataków:**

* **Phishing:** Wysyłanie fałszywych wiadomości (np. e-maili, wiadomości na media społecznościowe), które wyglądają, jakby pochodziły z zaufanych źródeł, w celu wyłudzenia poufnych informacji (np. hasła, dane karty kredytowej).
* **Ataki brute force:** Metoda polegająca na automatycznym generowaniu dużej liczby kombinacji użytkownika i hasła, aby uzyskać dostęp do systemu lub konta online.
* **Exploity:** Wykorzystywanie znanych luk w zabezpieczeniach oprogramowania do uzyskania nieautoryzowanego dostępu do systemu lub sieci.
* **Ataki typu man-in-the-middle (MitM):** Podsłuchiwanie lub manipulowanie komunikacją między dwoma stronami w celu przechwycenia lub zmodyfikowania przesyłanych danych.

# 2.3 Sprawdzenie co wpływa na to czy sieć i komputer są dobrze zabezpieczone.

**1.Oprogramowanie antywirusowe i antimalware**

Instalacja i regularna aktualizacja oprogramowania antywirusowego oraz antimalware jest kluczowym elementem zabezpieczeń. Pomaga to wykrywać i usuwać złośliwe oprogramowanie oraz chroni przed wirusami, trojanami i innymi szkodliwymi programami.

**2.Zaktualizowane systemy operacyjne i aplikacje**

Regularne aktualizacje systemu operacyjnego oraz wszystkich zainstalowanych aplikacji są niezbędne do zapewnienia bezpieczeństwa. Aktualizacje zawierają poprawki zabezpieczeń, które łatają znane luki i zapobiegają wykorzystywaniu ich przez potencjalnych atakujących.

**3.Silne hasła i autoryzacja dwuetapowa**

Używanie silnych, unikalnych haseł dla każdego konta oraz włączenie autoryzacji dwuetapowej, gdzie to możliwe, znacznie zwiększa bezpieczeństwo kont i danych użytkownika.

**4.Firewall**

Włączenie zapory sieciowej (firewall) na komputerze oraz w routerze pomaga w blokowaniu nieautoryzowanego dostępu do sieci i komputera.

**5.Szyfrowanie danych**

Korzystanie z szyfrowania danych, zarówno podczas przechodzenia przez sieć (np. protokół HTTPS), jak i podczas przechowywania danych na dyskach twardych, zapewnia dodatkową warstwę bezpieczeństwa.

**6.Regularne tworzenie kopii zapasowych**

Regularne tworzenie kopii zapasowych danych jest kluczowe w przypadku wystąpienia awarii sprzętowej, ataku ransomware lub innego zdarzenia, które mogłoby spowodować utratę danych.

**7.Sensowne zachowanie online**

Ostrożne otwieranie załączników email, unikanie klikania w podejrzane linki, korzystanie z wiarygodnych źródeł pobierania oprogramowania i unikanie udostępniania osobistych informacji w niewiarygodnych miejscach online są również istotne dla bezpieczeństwa.

**8.Monitorowanie sieci**

Regularne skanowanie sieci w poszukiwaniu niezidentyfikowanych urządzeń lub podejrzanej aktywności może pomóc w wykryciu potencjalnych zagrożeń.

# 2.4 Kto ma dostęp do twoich danych w przeglądarkach.

**1.Google Chrome**

Właściciel: Google LLC

Kraj pochodzenia: Stany Zjednoczone

**2.Mozilla Firefox**

Właściciel: Mozilla Corporation (niekomercyjna korporacja zależna od Mozilla Foundation)

Kraj pochodzenia: Stany Zjednoczone

**3.Microsoft Edge**

Właściciel: Microsoft Corporation

Kraj pochodzenia: Stany Zjednoczone

**4.Safari**

Właściciel: Apple Inc.

Kraj pochodzenia: Stany Zjednoczone

**5.Opera**

Właściciel: Golden Brick Capital Private Equity Fund I Limited Partnership (konsorcjum chińskich firm)

Kraj pochodzenia: Norwegia (choć należy do chińskiego konsorcjum, Opera Software nadal ma siedzibę w Norwegii)

**6.Brave**

Właściciel: Brave Software Inc.

Kraj pochodzenia: Stany Zjednoczone

**7.UC Browser**

Właściciel: Alibaba Group

Kraj pochodzenia: Chiny

**8.Vivaldi**

Właściciel: Vivaldi Technologies AS

Kraj pochodzenia: Norwegia

**9.Tor Browser**

Właściciel: The Tor Project

Kraj pochodzenia: Stany Zjednoczone

**10.Yandex Browser**

Właściciel: Yandex LLC

Kraj pochodzenia: Rosja

# 3.1 Porównanie i znalezienie odpowiedniego środowiska do przeprowadzania testów

**Kali linux następca BackTrack:**

Zawiera około 600 programów (narzędzi) do testów penetracyjnych, w tym takie jak Armitage (graficzne narzędzie do zarządzania atakami cybernetycznymi), Nmap (skaner portów), Wireshark (analizator pakietów), Metasploit (platforma testów penetracyjnych), John the Ripper (łamacz haseł ), sqlmap (automatyczne narzędzie do ataków SQL injection i przejęcia bazy danych), Aircrack-ng (zestaw oprogramowania do testowania penetracyjnego bezprzewodowych sieci LAN), Burp Suite i OWASP ZAP (skanery bezpieczeństwa aplikacji internetowych)

**Security Onion:**

Security Onion to darmowa i otwarta platforma zbudowana przez obrońców dla obrońców. Obejmuje widoczność sieci, widoczność hostów, Honeypoty do wykrywania włamań, zarządzanie logami i zarządzanie przypadkami.

Oba środowiska mają swoje specjalizacje. Kali Linux skupia się głównie na narzędziach do przeprowadzania testów penetracyjnych, podczas gdy Security Onion oferuje bardziej zintegrowane podejście, obejmujące monitorowanie ruchu sieciowego, widoczność hostów oraz zarządzanie incydentami bezpieczeństwa. Wybór między nimi może zależeć od konkretnych potrzeb i preferencji użytkownika oraz od rodzaju testów penetracyjnych, które zamierza przeprowadzić.

Kali Linux jest rozwijany z myślą o ekspertach ds. cyberbezpieczeństwa, testerach penetracyjnych i etycznych hakerach. Istnieje kilka innych dystrybucji dedykowanych testom penetracyjnym, takich jak Parrot OS﻿[w innych językach], BlackArch i Wifislax. Kali Linux wyróżnia się spośród tych dystrybucji pod względem cyberbezpieczeństwa i testów penetracyjnych, a także ma funkcje, takie jak domyślny użytkownik będący superużytkownikiem w środowisku Kali Live.

# 3.2 Gdzie szukać błędów i ewentualnych luk

**Luki bezpieczeństwa można identyfikować na kilka sposobów:**

**Skanowanie podatności:** Użycie specjalistycznych narzędzi do skanowania systemów i aplikacji w celu wykrycia znanych luk bezpieczeństwa. Narzędzia takie jak Nessus, OpenVAS, i inne mogą automatycznie identyfikować słabe punkty.

**Testy penetracyjne:** Symulacja ataków hakerskich na systemy w kontrolowany sposób, aby znaleźć i wykorzystać luki w zabezpieczeniach.

**Śledzenie informacji o podatnościach:** Śledzenie baz danych podatności, takich jak National Vulnerability Database (NVD) czy Bulletins of software vendors, dla informacji o nowych podatnościach w używanym oprogramowaniu.

# 4. Przeprowadzanie testów penetracyjnych sieci. Badania i ich analiza (sukcesy, porażki, wnioski)

Naszym pierwszym zadaniem, było postawienie maszyny wirtualnej, aby móc pracować bezpiecznie na naszym komputerze, bez ryzyka infekcji. W tym celu skorzystaliśmy z

**„Oracle VM Virtual Box”,** na którym zainstalowaliśmy dystrybucje systemu operacyjnego Linux, czyli **„Kali Linux”.**

**Pobranie i instalacja VirtualBoxa:**

VirtualBoxa pobraliśmy ze strony: <https://www.virtualbox.org/>.

Zainstalowaliśmy VirtualBoxa zgodnie z instrukcjami na stronie. Obraz zawierający tekst, zrzut ekranu, Strona internetowa, Czcionka

Opis wygenerowany automatycznie

**Pobranie obrazu Kali Linuxa:**

Obraz Kali Linuxa pobraliśmy z oficjalnej strony: <https://www.kali.org/downloads/>.

Wybraliśmy odpowiedni obraz ISO zgodnie z naszą architekturą systemu. Obraz zawierający tekst, zrzut ekranu, multimedia, oprogramowanie

Opis wygenerowany automatycznie

**Utworzenie nowej maszyny wirtualnej w VirtualBoxie:**

Utworzyliśmy nową maszynę wirtualną, nadając jej nazwę i wybierając obraz ISO Kali Linuxa

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Oprogramowanie multimedialne

Opis wygenerowany automatycznie

Przydzieliliśmy odpowiednią ilość pamięci RAM dla maszyny wirtualnej.

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Oprogramowanie multimedialne

Opis wygenerowany automatycznie

**Utworzenie wirtualnego dysku twardego:**

Utworzyliśmy wirtualny dysk twardy, wybierając dysk dynamicznie alokowany i ustalając jego rozmiar.

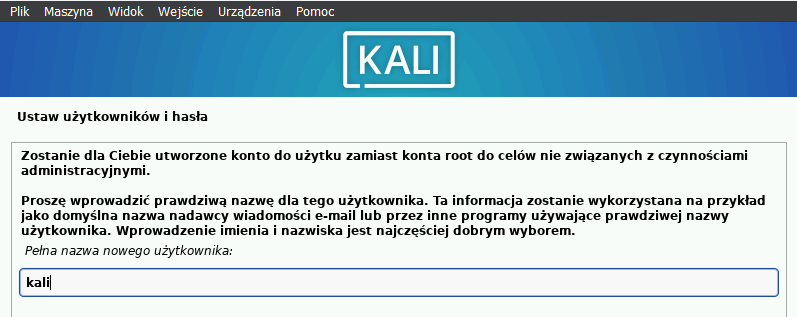
Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Oprogramowanie multimedialne

Opis wygenerowany automatycznie

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Oprogramowanie multimedialne

Opis wygenerowany automatycznie

**Uruchomienie maszyny wirtualnej i instalacja Kali Linuxa:**

Uruchomiliśmy maszynę wirtualną i rozpoczęliśmy proces instalacji Kali Linuxa. Obraz zawierający tekst, elektronika, zrzut ekranu, oprogramowanie

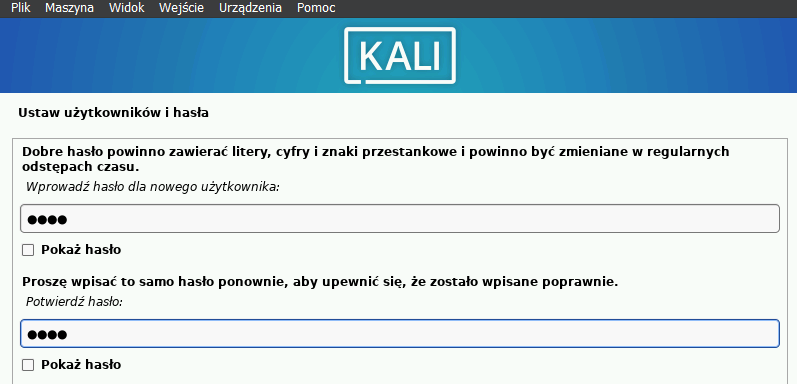
Opis wygenerowany automatycznie

Postępowaliśmy zgodnie z instrukcjami na ekranie, wybierając odpowiednie opcje instalacji.

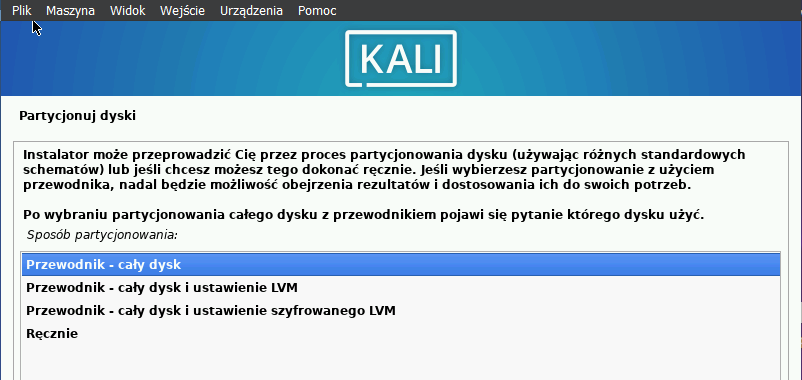
Obraz zawierający tekst, zrzut ekranu, oprogramowanie, System operacyjny

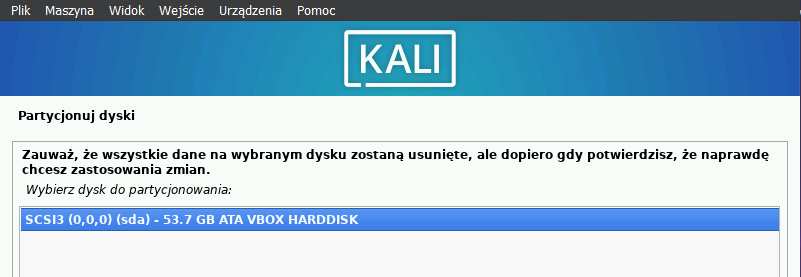
Opis wygenerowany automatycznie

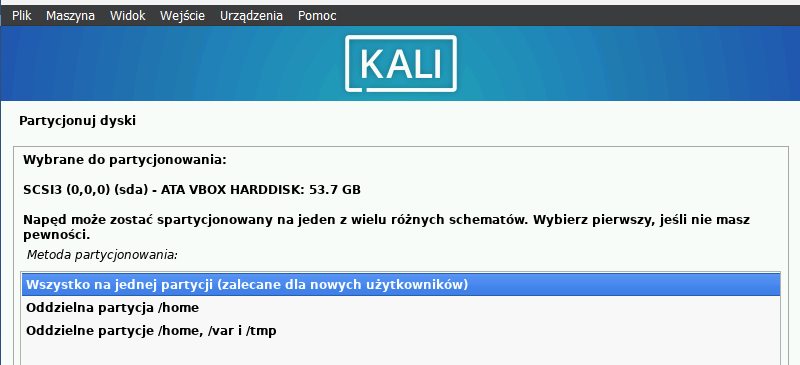
Ustawiliśmy nazwe i hasło uzytkownika

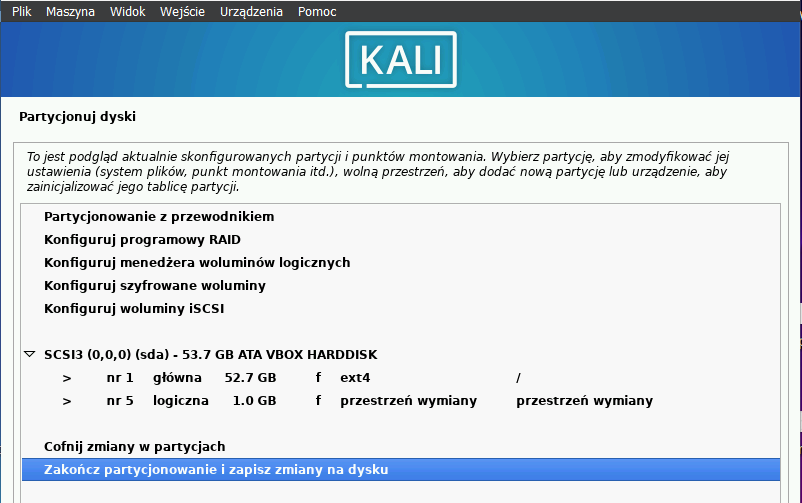


Partycjonowanie dysku

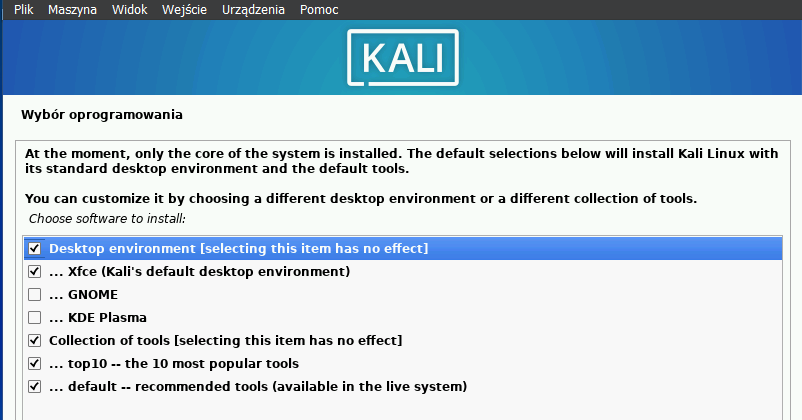








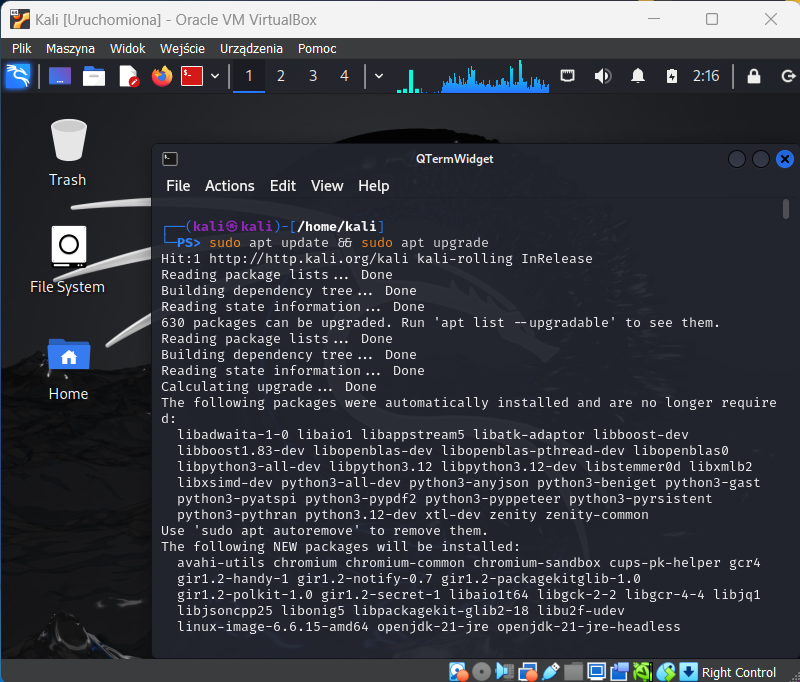
Wybór oprogramowania



**Konfiguracja Kali Linuxa:**

Po zakończeniu instalacji zalogowaliśmy się do systemu Kali Linux. Obraz zawierający tekst, elektronika, zrzut ekranu, wyświetlacz

Opis wygenerowany automatycznie

Zaktualizowaliśmy system i dostosowaliśmy go do naszych potrzeb. 

## 4.1 Stagefright

**Pierwszym testem penetracyjnym który chcieliśmy przeprowadzić był „Stagefright”.**

**Stagefright** jest to luka w oprogramowaniu systemu Android, odkryta w 2015 roku, umożliwiająca atakowanie urządzeń poprzez specjalnie spreparowane pliki multimedialne. Atakujący mogli zdalnie przejąć kontrolę nad urządzeniem, nawet bez interakcji użytkownika. **Sposób działania** Stagefright polegał na wykorzystaniu błędu w oprogramowaniu systemu Android związanego z przetwarzaniem danych multimedialnych. Atakujący mogli przesłać do urządzenia ofiary specjalnie spreparowany plik multimedialny, taki jak film wideo czy plik dźwiękowy, zawierający złośliwy kod. Gdy tylko urządzenie próbowało odtworzyć ten plik, luka w bibliotece odtwarzacza multimediów (Stagefright) została wykorzystana do wykonania kodu złośliwego. Atakujący mogli zdalnie uzyskać kontrolę nad urządzeniem, umożliwiając im szereg potencjalnie niebezpiecznych działań, takich jak kradzież danych, podsłuchiwanie rozmów czy nawet usunięcie zawartości urządzenia.

Pierwszym krokiem było w CMD przejście do **msfconsole** darmowego framework-u, stosowany przez pentesterów jak i hakerów. Przeniosło nas to po chwili do konsoli w której wyszukujemy frazę „stagefright”:



Wyskakują nam moduły i informacje o exploicie.

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Kopiujemy w do konsoli za komendą „use”:



Co przeniosło nas do danego exploit-a:



Wpisujemy w konsoli „Show options”, co daje nam taki wynik:

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Na powyższym zrzucie ekranu interesują nas tylko „SRVHOST” i „URIPATH” za SRVHOST ustawiamy nasze ip konsoli.

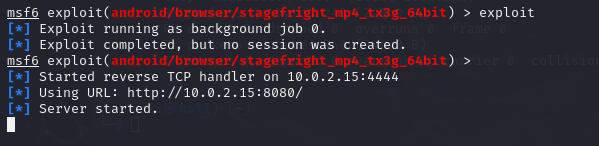
Tu pojawił się nasz pierwszy problem, ponieważ na naszej maszynie wirtualnej po wpisaniu komendy „ifconfig” pojawiły się dwa różne ip, więc próby przeprowadzaliśmy na obydwu ip.

Komendą „set SRVHOST ‘nasze ip’ ” ustawiliśmy SVRHOSTA i komendą „set URIPATH /” „/”oznacza root-a:

Obraz zawierający tekst, zrzut ekranu, Czcionka, menu

Opis wygenerowany automatycznie

Serwer uruchamiamy komendą „exploit”:



URL który wyświetliło wysyłasz do osoby nad którą telefonem chcesz przejąć kontrolę, niestety w naszym przypadku to nie zadziałało ponieważ, przy komendzie powyżej ”use” wyskoczył nam taki błąd.



Mimo wielu prób nie udało nam się ostatecznie skonfigurować payload-a, bez którego nie byliśmy w stanie sprawdzić ani przeprowadzić pentestu na telefonie.

Link z którego braliśmy sposób do pentestu w Stagefright-cie:

<https://www.youtube.com/watch?v=NXMJhfbzjtE&t=179s>

## 4.2 StormBreaker

**StormBreaker** to oprogramowanie do testów penetracyjnych, które pomaga testerom w identyfikowaniu i wykorzystywaniu luk w zabezpieczeniach systemów komputerowych.

Może również służyć do ataków na każde urządzenie podłączone do internetu (telefon, tablet, komputer).

W naszym przypadku udało nam się dojść do możliwości pozyskania informacji o telefonie ip, jakie urządzenie, rozdzielczość ekranu, wersja androida.

Udało nam się również zdobyć lokalizacje urządzenia, dostęp do przedniej kamery i mikrofonu.

Poniższe kroki pokazują jak do tego dążyliśmy krok po kroku i jakie były efekty.

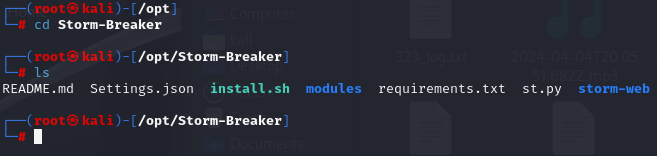
Na początku musieliśmy sklonować repozytorium na githubie, przechodzimy komendą do „otp” następnie w którym klonujemy repozytorium:



Po zainstalowaniu przy wpisaniu komendy „ls” pojawiło się repozytorium:



Przechodzimy do Storm-Breaker komendą cd i komendą ls możemy sprawdzić co zawiera:

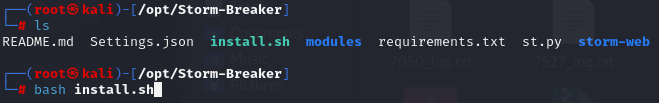


Aby działało wszystko jak trzeba, należy zainstalować wymagane pakiety:

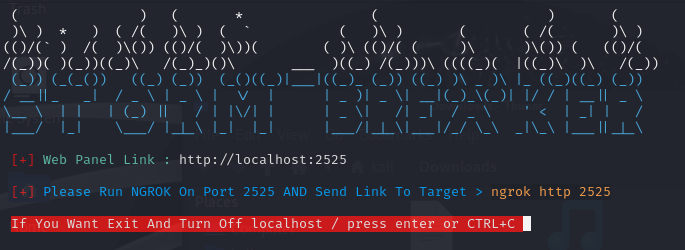




Po wykonaniu tych instalacji mogliśmy już zainstalować StormBreaker-a instalując plik o nazwie install.sh:



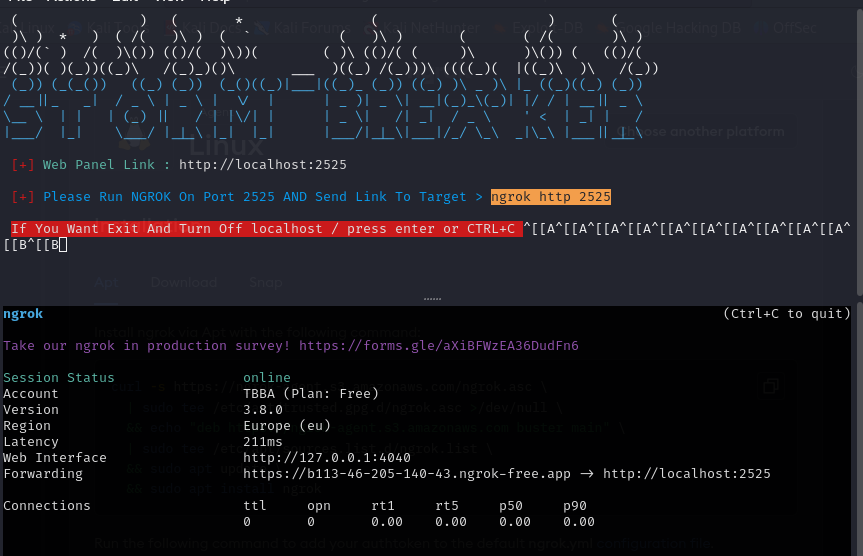
Następnie nadszedł czas uruchomienia programu komendą „python3 st.py” uruchamia to nasz program:



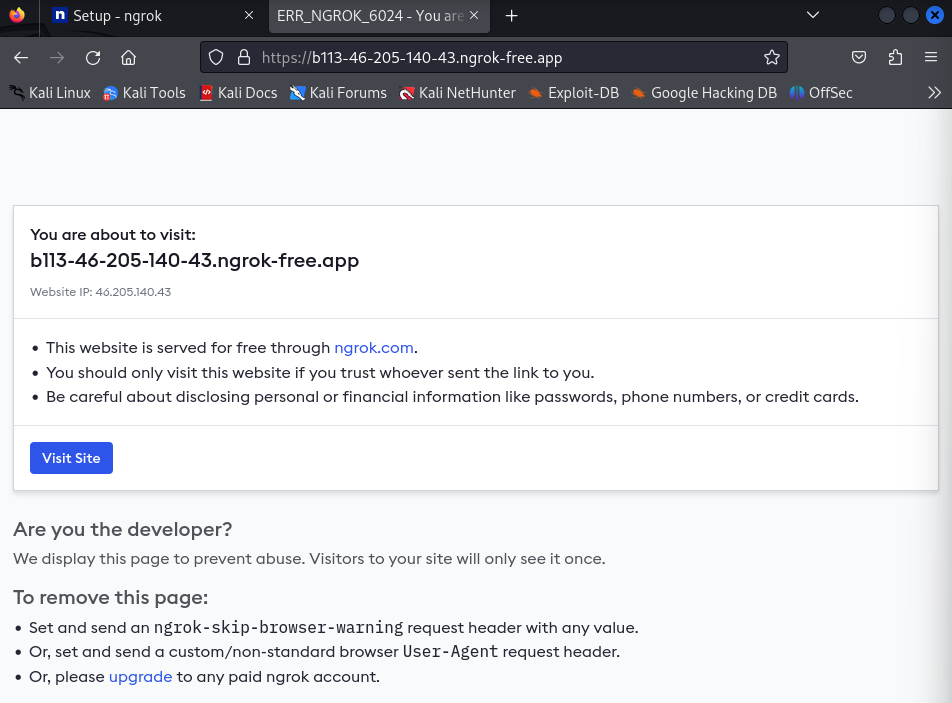
Na zrzucie ekranu powyżej widać link, ten link działa już jako nasz panel z którego będziemy mieć link w celu wysłania do osoby atakowanej aby uzyskać prywatne dane jak ip, lokalizacja itp. Jak i również dostęp do kamery i mikrofonu. W aktualnym stanie link działa tylko i wyłącznie na localhost, czyli urządzenia mogą być zainfekowane tylko wtedy gdy są podpięte do tego samego internetu. Aby móc działać na większą skalę czyli niezależnie od połączenia sieciowego. W tym celu należy pobrać ngrok i założyć w nim konto. Po założeniu konta otrzymujemy kod do powiązania ngroka z naszym komputerem:



Następnie za pomocą komendy „ngrok http 2525” uruchamiamy nasz serwer Storm-Breaker-a. Nasz serwer działa:

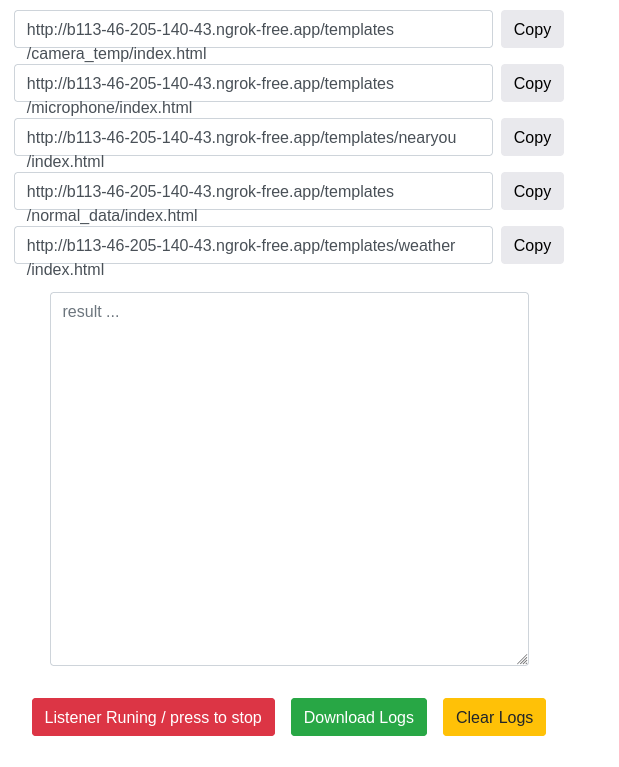


Na zrzucie ekranu możemy zobaczyć przy „Forwarding” pojawił się link, link ten prowadzi do naszego localhosta co pozwala nam działać nie tylko na naszej sieci i aby wszystko działąmy korzystamy właśnie z tego linku. Po wejściu w link wyskakuje okienko z ostrzeżeniami, klikamy visit side:



Wyskakuje okienko do logowania, logujemy się login: admin, hasło: admin

Otrzymujemy takie okno:



W okienku result wyświetlają się informacje o telefonie i potencjalne linki.

Pierwszy link powoduje dostęp do kamery, kiedy osoba go odpali i zaakceptuje dostęp co pare sekund będzie robiło zdjęcia z przedniej kamery: poniżej zdjęcie które wykonało w laptopie i z telefonu po otwarciu linka:

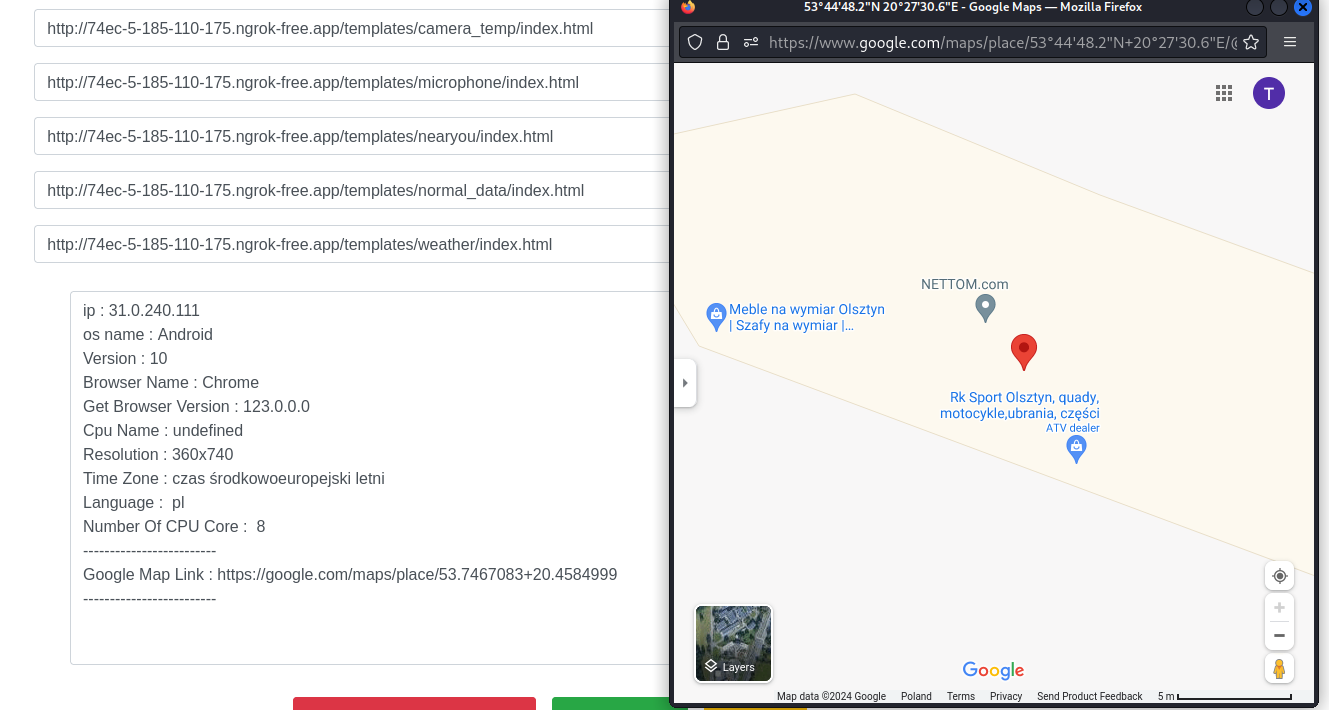
Obraz zawierający osoba, w pomieszczeniu, ubrania, Ludzka twarz

Opis wygenerowany automatycznie

Kolejny link daje dostęp do mikrofonu, nagrywa cały czas i co 6 sekund wysyła do nas ścieżkę do odtworzenia nagrania (tu zamieść przykład później)

Kolejne dwa linki dają dostęp do danych telefonu i lokalizacji, tak jak na kolejnym przykładzie.

Ostatni link daje nam dokładną lokalizacje urządzenia i generuje nam link do otworzenia w mapach google:



Po zakończeniu możemy pobrać logi które zostaną zapisane na naszym urządzeniu i do których możemy mieć dostęp gdyby były nam potrzebne.

Zauważyliśmy, że linki nie działają na urządzeniach z systemem IOS. <https://www.youtube.com/watch?v=h_f9lB4i-LA&t=310s>

## 4.3 Meterpreter

Kolejnym testem penetracyjnym który wykonaliśmy był „Meterpreter”.

Meterpreter jest to payload w ataku z wykorzystaniem narzędzia Metasploit, który zapewnia interaktywną powłokę, z której atakujący może zbadać maszynę docelową i wykonać kod. Meterpreter jest wdrażany przy użyciu iniekcji DLL w pamięci. W rezultacie Meterpreter znajduje się całkowicie w pamięci i nic nie zapisuje na dysku. Nie są tworzone żadne nowe procesy, ponieważ Meterpreter wstrzykuje się do atakowanego procesu, z którego może migrować do innych uruchomionych procesów. W rezultacie ślad po ataku jest bardzo ograniczony.

**Co oznacza i czym jest Payload:**

Jest to moduł exploita, jeden z trzech typów (singles, stagers, stages) wykorzystywanych przez framework Metasploit.

**Sposób działania:**

Meterpreter używa powłoki reverse\_tcp, co oznacza, że ​​łączy się z listenerem TCP na komputerze atakującego. Istnieją dwa popularne rodzaje powłok shell: bind i reverse. Bind shell otwiera nową usługę na maszynie docelowej i wymaga od atakującego połączenia się z nią w celu rozpoczęcia sesji. Reverse shell (znana również jako połączenie zwrotne) wymaga, aby atakujący najpierw skonfigurował listener, z którym może się połączyć maszyna docelowa.

**Poniższe kroki przedstawiają co zrobiliśmy i jaki był tego efekt:**

Do naszego testu wykorzystaliśmy maszynę wirtualną z systemem kali linux i telefon Samsung Galaxy S9 z systemem android 10.

Na początku hostujemy serwer na ngrok-u z którego pobieramy dane takie jak: IP, Host i Port. (tu wstaw zdjęcie z ngroka jak odpalasz serwer)

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Oprogramowanie multimedialne

Opis wygenerowany automatycznie

Następnie uzyskujemy adres :



Startujemy serwer apache2:



Tworzymy payload-a wykorzystując reverse tcp za pomocą komendy msfvenom:

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Po stworzeniu tworzy się aplikacja w podanej ścieżce w kodzie powyżej:

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Oprogramowanie multimedialne

Opis wygenerowany automatycznie

Za pomocą Metasploit ustawiamy payload, LHOST(musi być taki jak stworzyliśmy serwer ngrok), oraz LPORT. Wszystko wykonujemy w msfconsole:

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Obraz zawierający tekst, zrzut ekranu

Opis wygenerowany automatycznie

To jest miejsce na start i na run itp.

Po podłączeniu urządzenia za po mocą aplikacji uruchamia nam się sesja, w której mamy dostęp w tym przypadku do telefonu.

Wpisując komendę „sysinfo” otrzymujemy podstawowe informacje na temat urządzenia:

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Komendą webcam\_snap wykonujemy zdalnie zdjęcie z telefonu(tu dodajmy przykładowe zdjecia):

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Komendą record\_mic -d 20 zdalnie uruchamiamy nagrywanie mikrofonu na czas 20 sekund, po czym dostajemy link do pliku z nagranym dźwiękiem(przykładowe nagranie):

Obraz zawierający tekst, Czcionka, zrzut ekranu

Opis wygenerowany automatycznie

Komendą dump\_contacts pobiera historię smsów w urządzeniu:

Obraz zawierający tekst, Czcionka, zrzut ekranu

Opis wygenerowany automatycznie

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Oprogramowanie multimedialne

Opis wygenerowany automatycznie

Komendą sms\_send -d „nr telefonu ” -t „treść sms”(zdj1) wysyłamy sms na podany numer z naszą treścią(zdj2) i zapisuje nam tą wiadomość(zdj3):



Obraz zawierający tekst, zrzut ekranu, oprogramowanie, multimedia

Opis wygenerowany automatycznie

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, multimedia

Opis wygenerowany automatycznie



Poniżej plik txt z zdjęcia powyżej:

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Oprogramowanie multimedialne

Opis wygenerowany automatycznie

Jeśli podejrzewasz, że ktoś używa Metasploita przeciwko twojemu systemowi, ważne jest podjęcie natychmiastowych działań w celu ochrony twoich danych i sieci. Oto kilka kroków, które możesz podjąć:

**Rozłącz się z internetem:** Jeśli to możliwe, odłącz dotknięty system od internetu, aby zapobiec dalszemu nieautoryzowanemu dostępowi.

Zidentyfikuj Atak: Użyj narzędzi bezpieczeństwa do zidentyfikowania rodzaju i zakresu ataku. pomoże to zrozumieć, które podatności są wykorzystywane i w jaki sposób atakujący uzyskuje dostęp.

**Zabezpiecz Podatności:** Po zidentyfikowaniu wykorzystywanych podatności, załataj je tak szybko, jak to możliwe. Może to obejmować instalowanie aktualizacji zabezpieczeń lub łatek udostępnionych przez dostawców oprogramowania.

**Zmień Hasła:** Zmień wszystkie hasła powiązane z dotkniętym systemem oraz innymi systemami, które mogły zostać skompromitowane.

**Przeglądaj Dzienniki:** Przejrzyj dzienniki systemowe i sieciowe, aby zrozumieć zakres naruszenia i sposób, w jaki atakujący uzyskał dostęp. Te informacje mogą pomóc Ci zapobiec przyszłym atakom.

**Wdrożenie Środków Bezpieczeństwa:** Wzmocnij bezpieczeństwo swoich systemów, wdrażając zapory sieciowe, systemy wykrywania włamań i inne środki bezpieczeństwa, aby zapobiec przyszłym atakom.

**Poszukaj Pomocy Specjalistów:** Jeśli nie jesteś pewien, jak postępować, rozważ skorzystanie z pomocy specjalisty ds. bezpieczeństwa cybernetycznego lub firmy ds. bezpieczeństwa informatycznego, aby pomóc Ci złagodzić atak i zabezpieczyć swoje systemy.

<https://cyberwiedza.pl/czym-jest-meterpreter/>

<https://www.youtube.com/watch?v=TQGhgckLDUw&t=751s>

# 5. Załatanie luk znalezionych w oprogramowaniu lub sieci. Sposoby zabezpieczenia przed przeprowadzonymi atakami

**Rodzaje luk w zabezpieczeniach:**

**Luki w oprogramowaniu:** Błędy w kodzie programów, które mogą być wykorzystane do wykonania nieautoryzowanych działań. Przykłady to błędy umożliwiające wykonanie kodu z zewnątrz (remote code execution), iniekcje SQL, przecieki informacji czy przepełnienia bufora.

**Luki w konfiguracji systemu:** Nieprawidłowe ustawienia systemów lub aplikacji, które mogą ułatwić nieautoryzowany dostęp, np. słabe hasła, niewłaściwe uprawnienia, otwarte porty niezabezpieczone odpowiednimi regułami firewalla.

**Luki w protokołach sieciowych:** Słabości w protokołach komunikacyjnych wykorzystywanych przez systemy informatyczne, które mogą być wykorzystane do przechwytywania lub manipulowania danymi.

**Jak załatać luki:**

**Aktualizacje oprogramowania:** Regularne instalowanie aktualizacji i łatek bezpieczeństwa wydawanych przez producentów oprogramowania. Większość systemów operacyjnych i aplikacji oferuje mechanizmy automatycznych aktualizacji, które należy mieć włączone.

**Zmiana konfiguracji:** Poprawienie konfiguracji systemów i sieci zgodnie z najlepszymi praktykami bezpieczeństwa, takimi jak zasada najmniejszych uprawnień, wyłączenie niepotrzebnych usług, silne polityki haseł.

**Zastosowanie narzędzi zabezpieczających:** Instalacja i konfiguracja dodatkowych narzędzi zabezpieczających, takich jak firewall, systemy wykrywania i zapobiegania intruzom (IDS/IPS), które mogą pomóc w ochronie przed wykorzystaniem niezałatanych luk.

**Szkolenie użytkowników:** Edukowanie użytkowników o zagrożeniach i najlepszych praktykach bezpieczeństwa może pomóc zapobiec atakom wykorzystującym inżynierię społeczną.

### 5.1 Avast Mobile Security

Antywirus Avast wykrył nieporządany plik o nazwie Payload.apk i od razu zaproponował usunięcie go.

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Czcionka

Opis wygenerowany automatycznie Obraz zawierający tekst, zrzut ekranu, oprogramowanie, System operacyjny

Opis wygenerowany automatycznie

Po usunięciu i próbie zainstalowania go ponownie antywirus nie pozwala na pobranie go i otrzymujemy komunikat „Nie udało się pobrać jednego pliku”.

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Po odinstalowaniu antywirusa i ponownej próbie instalacji wirusa próba przebiegła negatywnie.

Po zrestartowaniu telefonu do ustawień fabrycznych wirus zostaje usunięty w raz z antywirusem lecz można go ponownie zainstalować.

Po ponownym zainstalowaniu wirusa mamy pełny dostęp do urządzenia.

## McAffe

## Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Czcionka Opis wygenerowany automatycznieObraz zawierający tekst, elektronika, zrzut ekranu, oprogramowanie Opis wygenerowany automatycznie

Obraz zawierający tekst, elektronika, zrzut ekranu, Telefon komórkowy

Opis wygenerowany automatycznie