1110111011011

1001100

110011001100

10101010101010

00011001001

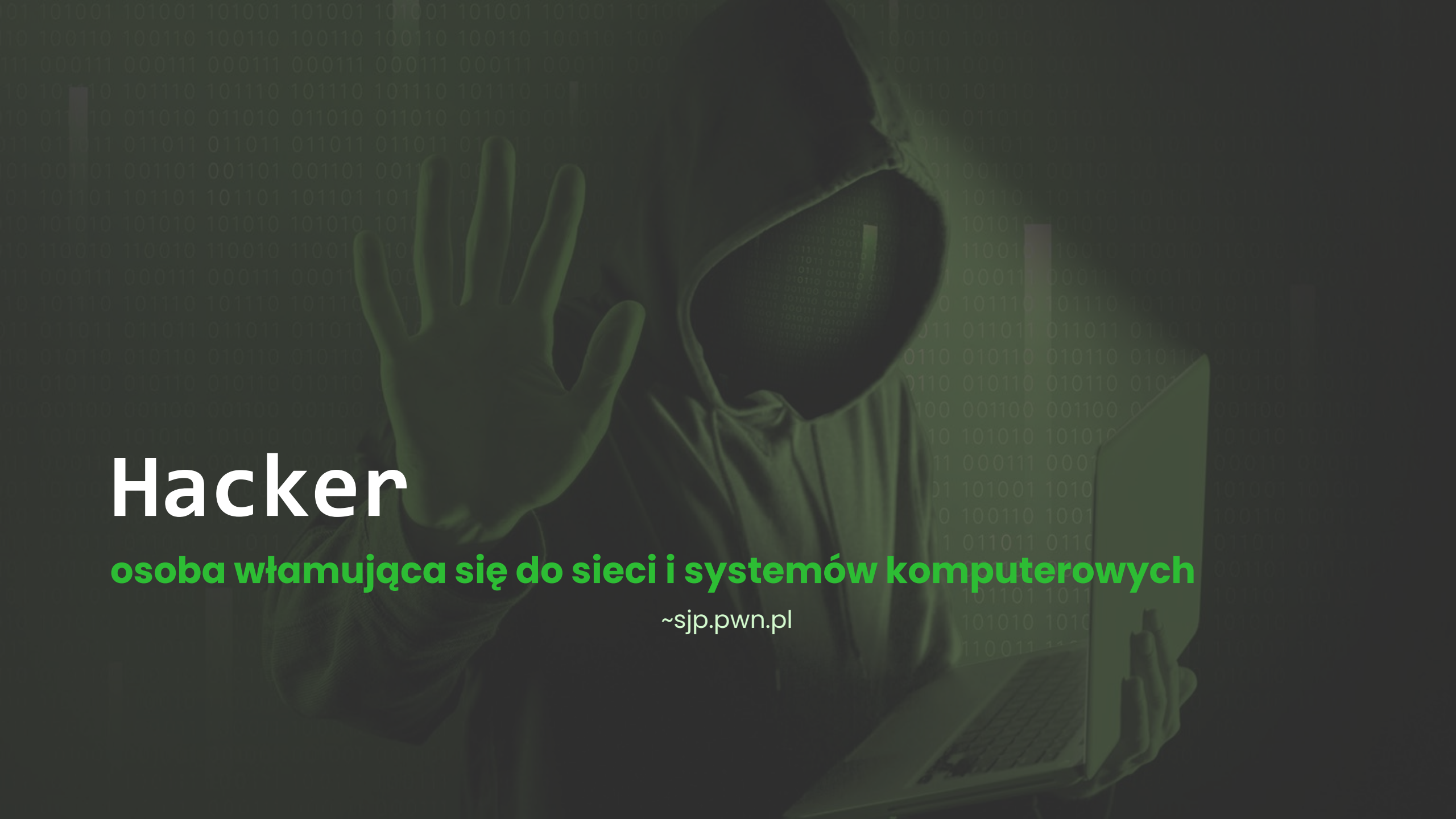
W świecie pełnym (cyber)zagrożeń

podstawowe pojęcia i ataki

Hacking i Cyberbezpieczeństwo | Giganci Programowania

Opracowanie: Michał Suchoń

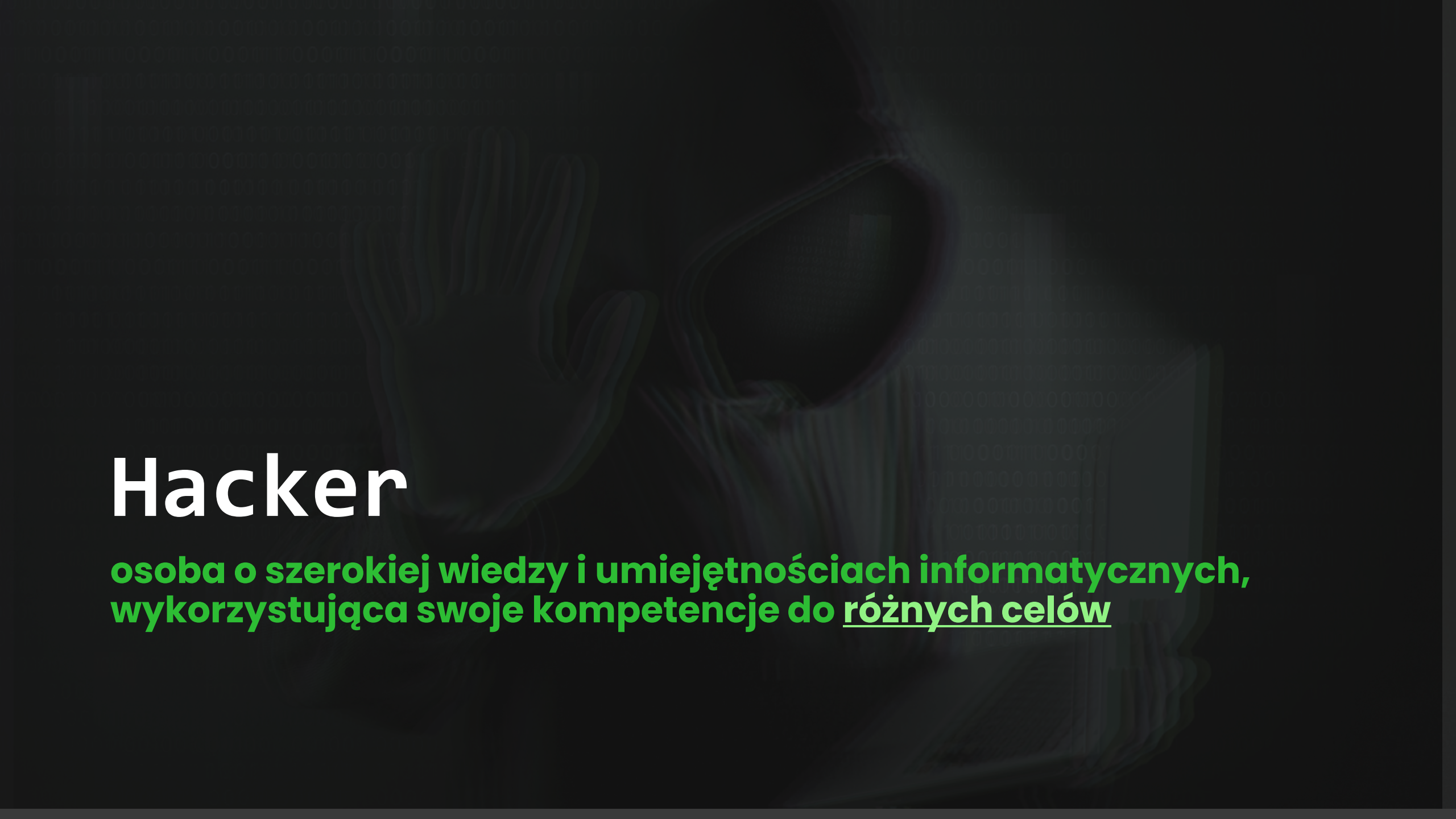

Kim jest hacker?



Hacker

osoba włamująca się do sieci i systemów komputerowych

~sjp.pwn.pl



Hacker

osoba o szerokiej wiedzy i umiejętnościach informatycznych, wykorzystująca swoje kompetencje do różnych celów

Czy każdy hacker jest zły?

Rodzaje hackerów

Script Kiddie

skryptowy dzieciak – niedoświadczony hacker, który używa programów i narzędzi w celu uzyskania nieuprawnionego dostępu np. do kont użytkowników czy plików bądź przeprowadzenia ataków na systemy jak DoS bez odpowiedniej znajomości zasad działania udostępnianych przez innych skryptów.

Rodzaje hackerów

Black hat

czarne kapelusze – osoby działające na **granicy** lub **poza granicami prawa** poprzez wykorzystywanie luk w zabezpieczeniach (*exploitów*) oprogramowania, np. celem zdobycia korzyści materialnych, zastraszenia ofiary lub w formie buntu (np. Anonymous)

Rodzaje hackerów

White hat

białe kapelusze – grupa hackerów (najczęściej współpracująca ze służbami państwa), której zadaniem jest znajdowanie dziur w zabezpieczeniach poprzez ataki na oprogramowanie, a następnie zgłaszanie twórcom, jakie są potencjalne „słabości”, które należy wyeliminować.

Rodzaje hackerów

Grey hat

szare kapelusze – grupa pośrednia między **czarnymi** a **białymi kapeluszami**, która swoje działania opiera o nielegalne lub nieetyczne metody, jednak w celu powiadomienia twórców o lukach w zabezpieczeniach. Nie działają jednak w sposób zorganizowany (jak white hats) i nieraz publicznie nagłaśniają, jakie błędy i exploity występują w programie.

Pozostałe grupy

Green hat

nowi niedoświadczeni hackerzy, uczący się hackowania

Blue hat

hackerzy, którzy swoim działaniem pragną zemsty na kimś, w społeczności Microsoftu to grupa, która zajmuje się szukaniem luk w zabezpieczeniach

Red hat

grupa, którą określa się czasem „samozwańczymi stróżami prawa”.

Podobnie do białych kapeluszy, włamują się celem znalezienia luk w zabezpieczeniach, jednak czynią to by powstrzymać czarne kapelusze i odebrać im możliwości ataków.
Nie zawsze jednak działają legalnie i etycznie

Purple hat

Osoby, które atakują własne systemy celem testowania i szukania exploitów. Określa się też czasem mieszanką blue i red hats: ***testują program przed publikacją, ale używają legalnych metod, powstrzymując czarne kapelusze***

Cracker

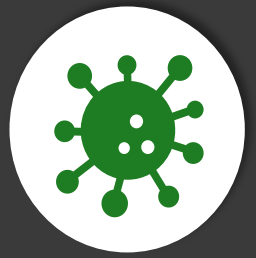
osoba, która **łamie zabezpieczenia** w oprogramowaniu, np. w celu uniknięcia **opłaty licencyjnej** *(cracking).* W odróżnieniu od **hackerów**, skupia się wyłącznie na osiągnięciu własnej korzyści, działając na szkodę twórców. Hacker działa czasem z pobudek moralnych, chcąc chociażby pokazać ignorancję firm czy organów rządowych.

Jakie znacie metody ataków (rodzaje wirusów)?

malware

ogólne określenie na program, mający za zadanie zaszkodzić użytkownikowi w specyficzny dla siebie sposób

rodzaje zagrożeń



wirus

ogólne pojęcie na szkodliwy program, który wykonuje w systemie niepożądane czynności

trojan

program podszywający się pod inną aplikację, często instalowany z docelowym zpiraconym programem

robak

rodzaj wirusa, który potrafi w krótkim czasie się powielić i rozprzestrzenić na inne urządzenia w sieci

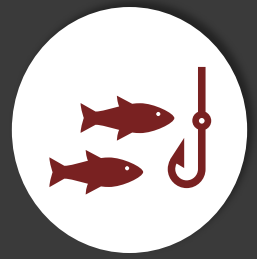
keylogger

rejestruje interakcje użytkownika, np. miejsca kliknięć myszką czy jakie klawisze zostały naciśnięte

crypto miner

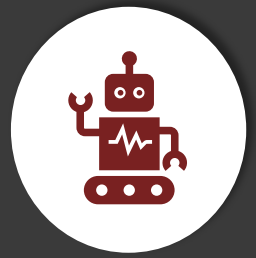
zamienia komputer w koparkę kryptowalut, znacząco obciążając komputer i blokując zasoby innym aplikacjom

rodzaje zagrożeń



zdobycie poufnych informacji poprzez podszycie się pod kogoś innego, np. pracownika banku, urzędu czy kogoś bliskiego

phishing



wysłanie nadmiarowej ilości połączeń celem zablokowania jakiejś usługi, np. awaryjne zatrzymanie działania serwera

DoS/DDoS

DENIAL OF SERVICE /
DISTRIBUTED DENIAL OF SERVICE

- DoS – jeden system do ataku
- DDoS – sieć wielu, nawet kilku tysięcy komputerów atakujących jednocześnie

„wstrzyknięcie” fałszywych danych do atakowanej bazy danych

SQL injection

„man in the middle” – atak polegający na udziale osoby „pomiędzy” aplikacją a użytkownikiem, np. kradzież danych przez podstawioną sieć WiFi

MTM

program, który szyfruje pliki i blokuje dostęp do komputera, żądając okupu za odblokowanie danych

ransomware

Do ataków używa się różnych narzędzi codziennego użytku jak CMD czy pliki wsadowe BAT

SPRAWDŹMY SAMI!

Czym się będziemy zajmować w tym kursie? Co będzie omawiane?

- ✓social engineering
- ✓dos /ddos
- ✓phishing
- ✓ataki na aplikacje web
- ✓keyloggery – stworzymy własny
- ✓ransomware – stworzymy własny
- ✓podsłuchiwanie ruchu sieciowego
- ✓łamanie haseł

Podsumowanie

1. Za pomocą jakiej komendy...

   poruszamy się między katalogami
   wyświetlamy zawartość katalogu
   kopiujemy katalog

2. Do czego używamy komendy

   ping
   ipconfig

3. Czym jest **wirus overload memory**, jak działa?

Podsumowanie

1. Za pomocą jakiej komendy...

   poruszamy się między katalogami **cd**
   wyświetlamy zawartość katalogu
   kopiujemy katalog

2. Do czego używamy komendy

   ping
   ipconfig

3. Czym jest **wirus overload memory**, jak działa?

Podsumowanie

1. Za pomocą jakiej komendy...

   poruszamy się między katalogami **cd**
   wyświetlamy zawartość katalogu **dir**
   kopiujemy katalog

2. Do czego używamy komendy

   ping
   ipconfig

3. Czym jest **wirus overload memory**, jak działa?

Podsumowanie

1. Za pomocą jakiej komendy...

   poruszamy się między katalogami **cd**
   wyświetlamy zawartość katalogu **dir**
   kopiujemy katalog **copy**

2. Do czego używamy komendy

   ping
   ipconfig

3. Czym jest **wirus overload memory**, jak działa?

Podsumowanie

1. Za pomocą jakiej komendy...

   poruszamy się między katalogami **cd**
   wyświetlamy zawartość katalogu **dir**
   kopiujemy katalog **copy**

2. Do czego używamy komendy

   ping ***sprawdzenie połączenia z innym komputerem / serwerem***
   ipconfig ***sprawdzenie konfiguracji karty sieciowej***

3. Czym jest **wirus overload memory**, jak działa?

Podsumowanie

1. Za pomocą jakiej komendy...

   poruszamy się między katalogami **cd**
   wyświetlamy zawartość katalogu **dir**
   kopiujemy katalog **copy**

2. Do czego używamy komendy

   ping ***sprawdzenie połączenia z innym komputerem / serwerem***
   ipconfig ***sprawdzenie konfiguracji karty sieciowej***

3. Czym jest **wirus overload memory**, jak działa?

   Rodzaj wirusa, który „zapycha" nam pamięć RAM, zwiększając jej zużycie. W efekcie, powoduje zawieszenie systemu co dawniej wywoływało słynny BLUE SCREEN

Polecam!

ŹRÓDŁO:
YouTube: https://youtu.be/oHknhhe4U6k?si=zfUBeRBF95MLoLjR

Polecam! Przydatne strony

https://niebezpiecznik.pl/

https://sekurak.pl/

https://zaufanatrzeciastrona.pl/

Polecam!

ŹRÓDŁO:
YouTube: https://youtu.be/wDGAkp1sHM4?si=tC1UXheJmj5vawn2