KURS PENTESTERA 22/23

REKONESANS

ERNEST ŁATOSZYŃSKI

JAKIE ASPEKTY PORUSZYMY NA DZISIEJSZYCH ZAJĘCIACH

1. Czym jest OSINT?
2. Dlaczego go używamy?
3. Dlaczego też ważne jest przestrzeganie jego zasad?
4. Lista narzędzi, o której chcemy dzisiaj opowiedzieć.

WHITE HATS PWR

CZYM JEST OSINT?

Open **S**ource **INT**elligence (tzw. **Biały Wywiad)** – zdobywanie informacji o celu w legalny sposób. Informacje możliwe do zdobycia na stronach internetowych, mediach społecznościowych i wszystkim co ***publicznie*** udostępnione.

DLACZEGO GO UŻYWAMY?

Niesamowicie przydatny w socjotechnice i przygotowaniu do testu penetracyjnego!

Pozwala on na:

- Poznanie powierzchownej struktury
- Znalezienie części pracowników
- Poznanie ich sposobu życia, czy kompetencji - co może odbić się, np. na jakości haseł jakich używają wewnątrz firmowej infrastruktury
- Poznanie reputacji firmy (Czy często mają problemy? Czy mają rozwinięty i zaawansowany dział IT?)
- Rozpoznanie systemu, na jakim działa infrastruktura i/lub zdobycie informacji o jakości kodu, na którym się opiera – a także potencjalnych podatności jakich możemy się spodziewać w testowanym środowisku

WHITE HATS PWR

DLACZEGO WAŻNE JEST PRZESTRZEGANIE ZASAD OSINT'U?

Jedno słowo: **więzienie**

- **Nielegalny dostęp do systemu (*hacking*)** - art. 267 § 1 i 2 k.k. Przestępstwo to ścigane jest na wniosek poszkodowanego. Grozi za nie kara grzywny, kara ograniczenia wolności lub pozbawienie wolności do 2 lat.
- **Naruszenie tajemnicy korespondencji/komunikacji (*sniffing*)** - art. 267 § 3 k.k. Tego typu przestępstwo polega na uzyskaniu zastrzeżonej informacji, np. poprzez sniffery, czyli programy umożliwiające przechwytywanie danych (haseł i identyfikatorów użytkowników). Za taki czyn grozi maksymalnie do 2 lat pozbawienia wolności.
- **Naruszenie integralności danych (*wirusy, robaki, trojany*)**, 268 k.k., art. 268a k.k. Przestępstwo to dotyczy m.in. kradzieży danych osobowych, udostępniania ich podmiotom trzecim bez zgody właściciela, a także wykorzystywania ich w sposób do tego nieuprawniony. Za popełnienie tych czynów przewidziane są sankcje finansowe (maksymalnie do 100 000 zł).
- **Naruszenie integralności systemu** - art. 269 k.k. Przykładem takiego przestępstwa są np. ataki ***DoS/DDoS*** (***Ping flood***), które polegają na przeciążeniu łącza internetowego. Mogą one doprowadzić np. do niedostępności danych usług. Polski ustawodawca przewidział maksymalną karę za ten czyn do 8 lat pozbawienia wolności (w przypadku, gdy mowa jest o naruszeniu bezpieczeństwa państwa).
- **Wytwarzanie i/lub udostępnianie *„narzędzi hakerskich”*** - art. 269a k.k., art. 269b k.k. Za popełnienie tego przestępstwa grozi kara od 3 miesięcy do 5 lat pozbawienia wolności

WHITE HATS PWR

NARZĘDZIA OSINT'OWE

- **OSINT Framework**
- **Google Dorks** (specjalne operatory)
- **Temp-maile**
- **Shodan.io**
- **haveIbeenPWNed?**
- **CyberChief**
- **theHarvester**
- **findomain**
- **spiderFoot**

WHITE HATS PWR

DZIĘKI ZA UWAGĘ!

WHITE HATS
PWR