Akademia WSEI



**Technologie informatyczne i wzorce projektowe**

**Lab 4**

Wykonał:

Paweł Lorens

Lublin 2024

**Część 1**

1. Obraz zawierający tekst, elektronika, zrzut ekranu, Czcionka

   Opis wygenerowany automatycznie

Po skanowaniu nmapem widać, że mam otwarte porty, użycie konta administratora nie zmienia wyników:

80/tcp open http

135/tcp open msrpc

443/tcp open https

445/tcp open microsoft-ds

902/tcp open iss-realsecure

912/tcp open apex-mesh

3389/tcp open ms-wbt-server

5357/tcp open wsdapi

1. Obraz zawierający tekst, elektronika, zrzut ekranu, oprogramowanie

   Opis wygenerowany automatycznie
2. Istnieje pare opcji na unikniecie wykrycia przez ids  
   1. –spoof-mac czyli podrobienie naszego adresu mac dzięki czemu trudniej będzie namierzyć atakującego

2. –randomize-hosts czyli zmieniamy kolejność skanowania hostów na randomową dzięki czemu analiza ruchu sieciowego dla IDS będzie znacząco utrudniona

3. –scan-delay/--max-retries pozwalają na ustawienie opóźnień między wysyłanymi pakietami i pomaga zmienić tempo skanowania i utrudnić wykrywanie przec IDS.

1. Obraz zawierający tekst, zrzut ekranu, wyświetlacz

   Opis wygenerowany automatycznie

**Część 2**



* W celu wykrycia faktu ukrywania plików można poddać analizie metadane w poszukiwaniu anomalii i nieprawidłowości
* Badanie zawartości binarnej, skanowanie pliku pod kątem sekwencji lub wzorców wskazujących na ukryte dane

**Część 3**

1. Obraz zawierający tekst, zrzut ekranu, Czcionka

   Opis wygenerowany automatycznie

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

1. Obraz zawierający tekst, zrzut ekranu, Czcionka

   Opis wygenerowany automatycznie

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie  
Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

1. Obraz zawierający tekst, zrzut ekranu, Czcionka, oprogramowanie

   Opis wygenerowany automatycznie  
     
   hashcat ma problemy z działaniem i nie chce wpółpracować z jakiegoś powodu
2. Do skrócenia czasu łamania haseł przydatne może być użycie słowników najpopularniejszych haseł np. rockyou.txt