|  |
| --- |
| Politechnika Wrocławska, Informatyka Stosowana |
| OSINT |
| Cyberbezpieczeństwo, Laboratorium nr.10 - raport |

|  |
| --- |
| Autor: Aleksander Stepaniuk  Nr. Indeksu: 272644 |

**4. Pytania**

**Pytanie 1;**

Tworzenie odcisków palców systemu operacyjnego polega na analizie charakterystycznych cech, takich jak odpowiedzi na pakiety TCP/IP, ustawienia TTL, znaczniki czasu, czy otwarte porty. Mogą one być tworzone przez użycie programów do skanowania systemu i zbierania informacji o wersji oprogramowania, zainstalowanych programach, analizie ruchu sieciowego oraz witryn internetowych otwieranych w systemie.

**Pytanie 2;**

Dzięki odciskom palców atakujący mogą dostosować swoje działania do konkretnego systemu, wykorzystując znane dla niego podatności, a także identyfikować użytkowników i urządzenia których używają. Z perspektywy ochrony, administratorzy mogą analizować takie informacje systemu i odpowiednio chronić przed różnego rodzaju atakami np. typu man in the middle.

**Pytanie 3;**

Aktywne techniki polegają na wysyłaniu zapytań do systemu i analizie odpowiedzi. Mogą wymagać one dodatkowej aktywności użytkownika poprzez zezwolenie na gromadzenie danych. Pasywne techniki, analizują ruch sieciowy bez ingerowania w komunikację oraz bez udziału użytkownika, co utrudnia ich wykrycie.

**Pytanie 4;**

Tak, można ograniczyć ujawniane informacje poprzez konfigurację firewalli, zmiany domyślnych ustawień protokołów, korzystanie z VPNa i korzystanie z przeglądarek chroniących prywatność.

**Pytanie 5;**

Tak, można użyć VPNa, który ukrywa niektóre dane użytkownika (między innymi jego lokalizację), albo odpowiednio skonfigurować firewalla, aby blokował lub zmieniał odpowiedzi na skanowania. Można też użyć honeypotów, które udają systemy lub serwery.

**Pytanie 6;**

Transfer stref DNS (AXFR) umożliwia pobranie pełnej zawartości strefy DNS. Atakujący mogą uzyskać listę subdomen i adresów IP, co ułatwia planowanie ataków. Ryzyko można ograniczyć, konfigurując serwery DNS tak, aby autoryzowały transfer tylko z zaufanych adresów.

**Pytanie 7;**

OSINT jest legalny, jeśli korzysta się z publicznie dostępnych informacji. Naruszenie prywatności lub zabezpieczeń może jednak prowadzić do łamania prawa. Należy więc zachowywać szczególną ostrożność w przypadku informacji, warto dowiadywać się czy nie są one poufne lub chronione jakiegoś rodzaju licencją.

**Pytanie 8;**

Największe zagrożenie to ujawnianie poufnych informacji w publicznie dostępnych źródłach, które mogą zostać wykorzystane przez atakujących do phishingu, inżynierii społecznej czy planowania ataków.

**Pytanie 9;**

Najlepiej ograniczyć ilość publicznie dostępnych danych, stosować polityki prywatności, przeszukiwać swoje informacje jak atakujący (audit OSINT), a także regularnie usuwać niepotrzebne treści i aktualizować zabezpieczenia.

**5. Zadania**

**Zadania 1-3ab;**

Wybrana przeze mnie domena to: wykop.pl

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

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

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Obraz zawierający tekst, zrzut ekranu

Opis wygenerowany automatycznie

**Zadanie 3c;**

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Obraz zawierający tekst, Czcionka, zrzut ekranu

Opis wygenerowany automatycznieObraz zawierający tekst, Czcionka, zrzut ekranu, typografia

Opis wygenerowany automatycznie Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie Obraz zawierający tekst, Czcionka, zrzut ekranu, typografia

Opis wygenerowany automatycznie

**Primary DNS:** cosmin.ns.cloudflare.com

**TTL:** 1800s, domena zapisana w pamięci podręcznej DNS:

**Czas żądania DNS:** Query time = 16msec – bardzo szybka odpowiedź, rekord prawdopodobnie był w pamięci podręcznej Google DNS, 12msec dla Cloudflare DNS (1.1.1.1), 8msec dla lokalnego DNS.

**Zadanie 4;**

Użycie komendy dnsenum:

**Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie**

**Zadanie 5;**

Użycie komendy fierce: (argument dns nie działał, więc użyłem –domain)

**Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie**

**Zadanie 6;**

Użycie komendy tcptraceroute:

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

**Zadanie 7;**

Narzędzia takie jak dig, traceroute, dnsenum, host i whois dostarczają informacji o domenach i infrastrukturze sieciowej. Dig i host są przydatne do analizowania rekordów typu DNS (A, MX, TXT), dnsenum automatyzuje wyszukiwanie subdomen oraz serwerów DNS, whois ujawnia informacje rejestrowe, takie jak dane właściciela domeny. Traceroute pokazuje trasę pakietów do celu, co pozwala na identyfikację węzłów sieciowych.

Złośliwy użytkownik może wykorzystać te dane do mapowania infrastruktury sieciowej, znajdowania potencjalnych punktów ataku, takich jak niechronione subdomeny czy słabe konfiguracje serwerów.

Najbardziej wszechstronnym narzędziem jest tutaj dnsenum, ponieważ automatyzuje on proces analizy DNS i odkrywa subdomeny i serwery, co daje dobry obraz infrastruktury docelowej domeny.

**Zadanie 8;**

(zamazane ze względu na niecenzuralne słownictwo)

Obraz zawierający zrzut ekranu, tekst, oprogramowanie, Oprogramowanie multimedialne

Opis wygenerowany automatycznie

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Czcionka

Opis wygenerowany automatycznie

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Strona internetowa

Opis wygenerowany automatycznie

Obraz zawierający tekst, Czcionka, zrzut ekranu, czarne

Opis wygenerowany automatycznieObraz zawierający tekst, zrzut ekranu, Czcionka, linia

Opis wygenerowany automatycznie

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Czcionka

Opis wygenerowany automatycznie

Obraz zawierający tekst, zrzut ekranu, Czcionka, oprogramowanie

Opis wygenerowany automatycznie

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Czcionka

Opis wygenerowany automatycznie

Statystyki dla domeny pwr.edu.pl (wykop.pl posiadał jedynie pojedyncze archaiczne rekordy)

Pdf: 50700

Doc: 1

Docx: 1

Txt: 1370

Xls: 1

Ppt: 1

**Zadanie 9;**

Narzędzie the Harvester dla bing:Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Yahoo:

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznieObraz zawierający tekst, zrzut ekranu, Czcionka, design

Opis wygenerowany automatycznie

Baidu:

Obraz zawierający tekst, zrzut ekranu, Czcionka, design

Opis wygenerowany automatycznie

Linkedin: (niestety nie zadziałał)

Obraz zawierający tekst, zrzut ekranu, Czcionka, design

Opis wygenerowany automatycznie

**Zadanie 10-11;**

Luki w zabezpieczeniach:

FTP:

Obraz zawierający tekst, zrzut ekranu, Czcionka, numer

Opis wygenerowany automatycznie

Tp-link router:

Obraz zawierający tekst, zrzut ekranu, Czcionka, numer

Opis wygenerowany automatycznie

Przykład luki

**CVE-2021-41617** - OpenSSH w wersji 6.2-8.7 oraz wcześniejszych zawierał błąd w mechanizmie uwierzytelniania publickey. Atakujący mógł zdalnie zalogować się bez uwierzytelnienia w określonych warunkach. Przykładowo shodan.io pokazuje, że dla wersji 7.7 mamy 54 systemy z tą podatniością z tego większość (23) z Włoch. <https://nvd.nist.gov/vuln/detail/CVE-2021-41617>

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Oprogramowanie multimedialne

Opis wygenerowany automatycznie