|  |
| --- |
| Politechnika Wrocławska, Informatyka Stosowana |
| Rekonesans sieciowy |
| Cyberbezpieczeństwo, Laboratorium nr.11 - raport |

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

**4. Pytania**

**Pytanie 1;**

Te wyniki uzyskane przez nmap mogą być wiarygodne (w granicach możliwości narzędzia), ale zależy to od wielu czynników, między innymi od konfiguracji skanowania lub od tego czy system jest odpowiednio skonfigurowany, a także od poziomu zabezpieczeń badanego hosta lub sieci w której się znajduje. Dodatkowo jeżeli host posiada zabezpieczenia firewalla, to ochrona sieci może blokować dostęp do niektórych portów i pokazywać je fałszywie jako zamknięte. Ponadto usługi przypisane do określonych portów mogą różnic się od tych domyślnie rozpoznawanych przez bazę danych nmap.

**Pytanie 2;**

Uzyskane informacje o hoście docelowym mogą zależeć od opcji skanowania. Opcje które wymagają dostępu administratora umożliwiają bardziej szczegółowe analizy, ponieważ dostarczają więcej różnych danych o portach i usługach tam uruchomionych. Opcja skanowania SYN wykrywa otwarte porty bez pełnego ustanawiania połączenia. Z kolei opcje z wyborem konkretnych flag TCP nawiązują pełne połączenie, ale przez to takie które jest bardziej widoczne. Opcja skanowania wersji próbuje zidentyfikować usługę i jej wersję na danym porcie. Opcja skanowania systemu operacyjnego podejmuje próbę wykrycia systemu operacyjnego. Im bardziej szczegółowe skanowanie tym więcej informacji można uzyskać.

**Pytanie 3;**

Nie, skanowanie hostów bez pozwolenia może być nielegalne (zależnie od prawa w danym kraju) i traktowane jako próba włamania lub działanie nieautoryzowane. Jednak samo narzędzie nmap jest legalne i można go normalnie używać bez zewnętrznego pozwolenia, o ile nie zakłóca to w żaden sposób działania skanowanego systemu. Zależy to od prawa w danym kraju, ale w wielu miejscach takie działania mogą prowadzić do konsekwencji prawnych.

**5. Zadania**

**Zadanie 0;**

Adresy IP maszyn:

**Metasploitable**: 192.168.188.36

**Kali linux**: 192.168.188.35

Adres sieci: 192.168.188.0/24

**Zadanie 1;**

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Obraz zawierający tekst, zrzut ekranu, menu, Czcionka

Opis wygenerowany automatycznie

Obraz zawierający tekst, Czcionka, zrzut ekranu

Opis wygenerowany automatycznie

**Zadanie 2;**

a) Typy skanów TCP:

* –sT (skanowanie TCP connect):

Obraz zawierający tekst, zrzut ekranu, menu

Opis wygenerowany automatycznie

Obraz zawierający tekst, Czcionka, zrzut ekranu

Opis wygenerowany automatycznie

* –sS (skanowanie TCP SYN):

Obraz zawierający tekst, Czcionka, zrzut ekranu

Opis wygenerowany automatycznie

Obraz zawierający tekst, zrzut ekranu, menu, design

Opis wygenerowany automatycznie

* –sN (skanowanie null, brak flag tcp w nagłówku pakietów):

Obraz zawierający tekst, zrzut ekranu, design

Opis wygenerowany automatycznie

* –sM (skanowanie TCP Maimon FIN+ACK):

Obraz zawierający tekst, Czcionka, zrzut ekranu

Opis wygenerowany automatycznie

* –sA (skanowanie TCP ACK):

Obraz zawierający tekst, Czcionka, zrzut ekranu

Opis wygenerowany automatycznie

* –sW (skanowanie TCP Window):

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

* –sl (skanowanie Idle (z wykorzystaniem tzw. Zombie hosta)):

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

b) Opis różnic:

**-sT (TCP Connect Scan)**

* wykonuje pełne połączenie TCP (trzyetapowy handshake)
* jest najbardziej widoczny dla systemu docelowego, ale działa bez potrzeby uprawnień root

**-sS (SYN Scan)**

* wysyła pakiet SYN i czeka na odpowiedź (SYN-ACK oznacza otwarty port)
* bardziej dyskretny niż -sT, bo nie kończy pełnego połączenia (brak handshake)

**-sN (TCP Null Scan)**

* wysyła pakiety bez ustawionych flag TCP
* może wykrywać otwarte/filtrujące porty na systemach bez ścisłego RFC

**-sM (TCP Maimon Scan)**

* specjalna metoda, która działa podobnie do -sN, ale z flagą FIN+ACK
* służy do omijania słabo skonfigurowanych zapór sieciowych

**-sA (ACK Scan)**

* sprawdza odpowiedź na pakiety ACK, aby określić, czy port jest filtrowany
* nie identyfikuje otwartych portów, ale pomaga mapować reguły firewalla

**-sW (Window Scan)**

* podobny do -sA, ale wykorzystuje różnice w oknach TCP do rozpoznania stanu portów
* działa tylko na niektórych systemach

**-sI (Idle Scan)**

* ukryte skanowanie przy użyciu hosta zombie, aby ukryć adres atakującego
* bardzo dyskretne, ale wymaga odpowiedniego hosta zombie

**Zadanie 3;**

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Czcionka

Opis wygenerowany automatycznie

**Zadanie 4;**

* -T 5:

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

* -T 4:

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Obraz zawierający tekst, zrzut ekranu, Czcionka, design

Opis wygenerowany automatycznie

* -T 3:

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

* -T 2, 1, 0: czas oczekiwania dłuższy niż 15min

Wniosek: Czas oczekiwania na wykonanie procedury rośnie wraz ze spadkiem podawanej wartości argumentu „-T”.

**Zadanie 5;**

Port 21: (sSH)

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Port 22: FTP

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

**Zadanie 6;**

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Obraz zawierający tekst, Czcionka, zrzut ekranu

Opis wygenerowany automatycznieObraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Dla Metasploitable nie znaleziono

jednoznacznej informacji o OS, jedynie

mniej lub bardziej dokładne strzały.

(Linux 2.6.9 - 2.6.24)

**Zadanie 7;**

Obraz zawierający tekst, zrzut ekranu, menu, Czcionka

Opis wygenerowany automatycznie

Wybrane skrypty z folderu /usr/share/nmap/scripts/

* **http-traceroute.nse**: Wykonuje traceroute przez serwer HTTP, śledząc ścieżkę pakietów do hosta docelowego.
* **ssh-hostkey.nse**: Pobiera i wyświetla klucze hosta SSH z serwera, umożliwiając weryfikację tożsamości serwera.
* **dns-brute.nse**: Przeprowadza atak brute force na serwer DNS w celu odkrycia subdomen dla określonej domeny.
* **mysql-audit.nse**: Audytuje konfigurację bezpieczeństwa serwera MySQL zgodnie z wytycznymi CIS MySQL v1.0.2.

Obraz zawierający tekst, zrzut ekranu

Opis wygenerowany automatycznie

1. nmap -sC

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

http-enum

Obraz zawierający tekst, zrzut ekranu

Opis wygenerowany automatycznie

b)

Obraz zawierający tekst, zrzut ekranu, Czcionka, czarne i białe

Opis wygenerowany automatycznie

http-headers

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

http-methods

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Obraz zawierający tekst, zrzut ekranu, Czcionka, menu

Opis wygenerowany automatycznie

http-php-version

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

**Zadanie 8;**

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Oprogramowanie multimedialne

Opis wygenerowany automatycznie

Obraz zawierający tekst, zrzut ekranu

Opis wygenerowany automatycznie

Obraz zawierający tekst, zrzut ekranu, Czcionka, design

Opis wygenerowany automatycznie

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Oprogramowanie multimedialne

Opis wygenerowany automatycznie

**Zadanie 9;**

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Nmap skanuje sieć, wykrywa porty, usługi, wersje i systemy operacyjne. Amap skupia się bardziej na prostym rozpoznawaniu usług za pomocą „banner grabbing”, działa szybciej, ale dostarcza mniej szczegółowych danych. Nmap jest lepszy do ogólnych analiz sieci, a Amap sprawdza się przy identyfikacji usług na nietypowych portach lub w niestandardowych środowiskach.