

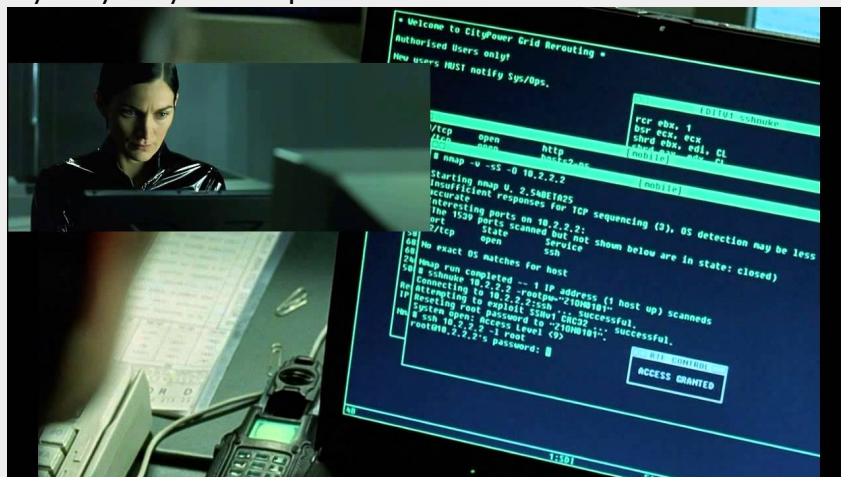
NARZĘDZIA DIAGNOSTYCZNE - wykorzystanie narzędzia Nmap w celu analizowania protokołów komunikacyjnych

WPROWADZENIE

Nmap (pełna nazwa „Network Mapper”) jest darmowym narzędziem do testowania sieci stworzonym przez Gordona Lyona w 1997 roku. Jest najpopularniejszym narzędziem do skanowania sieci komputerowych.

CIEKAWOSTKA

Program jest doceniany w szerokich kręgach umożliwiając m.in. wykrycie systemów, oprogramowania, usług jakie oferują hosty/serwery. Występuje na wszystkich systemach również w wersjach z GUI. Doceniono go również w kinematografii gdzie wykorzystany został np. w Matrixie.



Każdorazowo wynikiem działania aplikacji jest lista przeskanowanych adresów IP. Wyróżnić można kilka metod skanowania portów w ramach obranego adresu/ów IP:

- skanowanie oparte na pełnym połączeniu TCP (nmap -sT) – listuje porty, z którymi udało się nawiązać połączenie
- skanowanie SYN (tzw. półotwarte) (nmap -sS) – polega na wysyłaniu pakietów z ustawioną flagą SYN i oczekiwaniu na odpowiedź. Jeżeli serwer odpowie pakietem SYN-ACK oznacza to otwarty port. Serwer oczekuje na pakiet z bitem ACK, jednak nigdy go nie otrzymuje, a połączenie nie jest logowane w ramach warstwy aplikacji.
- metoda ACK (nmap -sA) – wykorzystywana jest najczęściej do poznania ustawień firewalla (rozpoznawania prostych filtrów pakietów). Nmap wysyła do wskazanych portów pakiety ACK. Jeśli otrzyma pakiet RST, port uznawany jest za niefiltrowany, jeżeli zaś nie otrzymuje odpowiedzi, uznaje go za filtrowany
- skanowanie FIN (nmap -sF) – korzysta z pakietów z ustawioną wyłącznie flagą FIN, czego host docelowy nie oczekuje. Porty niewykorzystane odpowiadają wówczas pakietem RST

- metoda Xmas Tree (nmap -sX) – wykorzystuje pakiety z bitami FIN, URG i PUSH, porty zamknięte odpowiadają pakietem z flagą RST
- skanowanie Null (nmap -sN) – korzysta z pakietów bez ustawionych żadnych flag
- skanowanie portów UDP (nmap -sU) – listuje otwarte porty, korzystające z protokołu UDP
- skanowanie ping (nmap -sP) – pozwala ono określić, które z hostów są aktywne w danym momencie
- skanowanie RPC (nmap -sR) – znajduje usługi dostępne przez RPC

ZALETY	WADY
Prosty w obsłudze	Skanowanie aktywne – duży ruch ułatwia jego wykrycie
Duża ilość metod skanowania	
Wysoka skuteczność	

I a. INSTALACJA Nmap



1. Należy pobrać najnowszą wersję aplikacji Zenmap ze strony www.nmap.org/zenmap/
2. Standardowa instalacja, po której narzędzie jest gotowe do pracy.

I b. INSTALACJA Nmap



1. Zaktualizowany system (komendy `update` i `upgrade`) powinien mieć prawidłowy dostęp do sieci (w ramach laboratoriów wirtualna karta sieciowa powinna być zmostkowana)
2. Należy zainstalować program – `apt-get install nmap`
3. Wykonywanie poleceń odbywa się w terminalu za pomocą komendy `nmap ...`

II. MANUAL



Wszelkie niezbędne informacje odnośnie opcji, parametrów można wywołać za pomocą komendy `nmap -help`. Znajdują się tam podstawowe polecenia, poszerzyć wiedzę można przez dokumentację znajdującą się w internecie. Odnośnik do oficjalnego manuala www.nmap.org/book/man.html

SKŁADADNIA !

nmap [Typ(y) skanowania] [Opcje] {specyfikacja celu}

POLECENIA

SOLO

1. Uruchom program.
2. Wykonaj podstawowe skanowanie (bez żadnych parametrów) konkretnego adresu IP.
3. Ten sam adres przeskanuj z wykorzystaniem parametru **-v**
4. Przeskanuj wybrany adres z parametrem umożliwiającym detekcję systemu operacyjnego.
5. Przeskanuj port z wykorzystaniem protokołu TCP.
6. Przeskanuj port z wykorzystaniem protokołu UDP.

PARA

1. Uruchom/zainstaluj usługę SSH.
 - a) Utwórz regułę firewalla która otworzy dostęp do terminala „z zewnątrz”.
 - b) Przetestuj czy SSH działa poprawnie (spróbuj się połączyć).
 - c) Wykonaj skanowanie portów w celu odnalezienia działającego SSH via nmap.
 - d) ZMIANA STRON – wykonanie całego punktu od nowa
2. Wykonaj zadanie identyczne jak powyższe jednak wymyślając własną usługę.
Udowodnij że działa!