

LAB ADVANCED – WINDOWS 1/1

WPROWADZENIE

Tematem głównym zadania jest uruchomienie na platformie Windows programu **Nmap** który jest jednym z najpopularniejszych skanerów sieciowych. Jest narzędziem open source do eksploracji sieci i audytów bezpieczeństwa. Został zaprojektowany do szybkiego skanowania dużych sieci, ale również działa dobrze w stosunku do pojedynczych adresów. Nmap wykorzystuje niskopoziomowe pakiety IP do wykrywania które adresy są dostępne w sieci, jakie udostępniają usługi (nazwa aplikacji i wersja), na jakich systemach operacyjnych pracują (wersja systemu), jakie typy systemów zaporowych (firewall) są wykorzystywane i dziesiątek innych cech. Nmap jest powszechnie wykorzystywany do audytów bezpieczeństwa, również wielu administratorów sieci i systemów wykorzystuje go wykonywania rutynowych czynności, takich jak inwentaryzacja zasobów sieci, zarządzanie aktualizacjami oprogramowania i monitorowania systemów oraz ich czasu działania (uptime).

```
Starting Nmap 4.01 ( http://www.insecure.org/nmap/ ) at 2006-03-20 15:53 PST
Interesting ports on scanme.nmap.org (205.217.153.62):
(The 1667 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 3.9p1 (protocol 1.99)
25/tcp    open  smtp      Postfix smtpd
53/tcp    open  domain    ISC Bind 9.2.1
70/tcp    closed gopher
80/tcp    open  http      Apache httpd 2.0.52 ((Fedora))
113/tcp   closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.0 - 2.6.11
Uptime 26.177 days (since Wed Feb 22 11:39:16 2006)

Interesting ports on d0ze.internal (192.168.12.3):
(The 1664 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp       Serv-U ftpd 4.0
25/tcp    open  smtp      IMail NT-ESMTP 7.15 2015-2
80/tcp    open  http      Microsoft IIS webserver 5.0
110/tcp   open  pop3      IMail pop3d 7.15 931-1
135/tcp   open  mstask     Microsoft mstask (task server - c:\winnt\system32\
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp  open  msrpc      Microsoft Windows RPC
5800/tcp  open  vnc-http   Ultr@VNC (Resolution 1024x800; VNC TCP port: 5900)
MAC Address: 00:A0:CC:51:72:7E (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows 2000 Professional
Service Info: OS: Windows
```

Wynikiem działania Nmap jest lista przeskanowanych adresów z dodatkowymi informacjami zależnymi od wykorzystanych opcji. Jedną z głównych informacji jest „lista interesujących portów”. Zawiera ona numery portów wraz z protokołami, nazwami usługi i wykrytym stanem. Stan może zostać opisany jako otwarty, filtrowany, zamknięty, lub niefiltrowany. Otwarty oznacza, że aplikacja na badanym adresie oczekuje na połączenia/pakiety przychodzące na ten port. Filtrowany oznacza, że system zaporowy lub inne urządzenie blokujące ruch sieciowy nie dopuszcza komunikacji do tego portu i z tego powodu Nmap nie jest w stanie określić czy badany port jest otwarty czy zamknięty. Zamknięty port nie posiada aplikacji, która obsługuje komunikację sieciową. Porty sklasyfikowane jako niefiltrowane odpowiadały na zapytania Nmap, jednak nie było możliwe określenie, czy były one otwarte czy zamknięte. Nmap raportuje kombinacje stanów otwarty|filtrowany i zamknięty|filtrowany jeśli nie jest w stanie określić, który z dwóch podanych stanów lepiej opisuje stan portu. Lista portów może również zawierać informacje o wykrytych wersjach oprogramowania, jeśli została włączona detekcja wersji. Jeśli została wybrana opcja skanowania dostępnych protokołów (-sO), Nmap zamiast listy portów dostarczy informacji na temat dostępności poszczególnych protokołów IP. (źródło www.nmap.org)

Nmap			
Windows		Linux	
<i>Terminal</i>	<i>GUI</i>	<i>Terminal</i>	<i>GUI</i>
	Zenmap		Zenmap

Powyżej znajduje się tabela która pokazuje w jaki sposób można korzystać z Nmap niezależnie od systemu oraz preferencji. Wszelkie tutoriale oraz pliki instalacyjne znajdują się na stronie:

www.nmap.org

Podsumowując program Nmap to skaner, głównym założeniem jest przeszukiwanie tych otwartych (TCP oraz UDP), jest w stanie zidentyfikować system na podstawie charakterystycznej budowy pakietu oraz usługi powiązane z routingiem.

BAZOWA SKŁADNIA

<i>Nmap</i>	<i><rodzaj skanowania></i>	<i><warunek></i>	<i><adres IP></i>
	Np.	Np.	
	-O (rozpoznawanie systemu)	-T (wprowadzenie ograniczenia 0 – 5 gdzie: 0 – najwolniej 5 – najszybciej)	
	-sV (rozpoznawanie usług)	-v (więcej informacji)	
	-sO (skanowanie IP)		
	-sT (skanowanie TCP)		
	-sU (skanowanie UDP)		
	-sS (skanowanie niewidzialne)		

POLECENIA

1. Zainstaluj program nmap.
2. Udowodnij że jesteś w stanie korzystać z wersji w terminalu oraz GUI.
3. Wykonaj skan strony WWW na której posiadasz skrzynkę pocztową.
4. Wykonaj skan wszystkich możliwych portów we własnym środowisku (localhost).
5. Wykonaj skan wykrywający usługę tj. jaką maszyną wirtualną pracujesz (localhost).
6. Stwórz blokadę portu (wcześniej skanowanego) w systemie który sprawdzasz, wykonaj ponowny skan innymi metodami – opisz rezultat.
7. Wykonaj skanowanie normalne oraz niewidzialne – opisz różnice w zależności od źródła.
8. Czy nmap umożliwia wykonywanie „ataków”?
9. Znajdź oparte na przykładzie ciekawe wykorzystanie programu.
10. Czy jesteś w stanie odnaleźć główny router szkolny (dlaczego tak/nie)?
11. Czy DNS ma jakikolwiek wpływ na wykonywane testy (dlaczego tak/nie)?