

網路安全工具與技術的應用與實踐 Nmap



網路安全工具與技術的應用與實踐 Nmap 是一個用於網路掃描的工具，它可以用來發現網路中的設備、服務和漏洞。Nmap 是一個開放源碼工具，它可以用來進行網路掃描、端口掃描、服務識別、漏洞檢測等。Nmap 是一個非常強大的工具，它可以用來進行網路安全評估、網路監控、網路故障排除等。

網路安全工具與技術的應用與實踐 Nmap

網路安全工具與技術的應用與實踐 Nmap 是一個用於網路掃描的工具，它可以用來發現網路中的設備、服務和漏洞。Nmap 是一個開放源碼工具，它可以用來進行網路掃描、端口掃描、服務識別、漏洞檢測等。Nmap 是一個非常強大的工具，它可以用來進行網路安全評估、網路監控、網路故障排除等。

網路安全工具與技術的應用與實踐 Nmap 是一個用於網路掃描的工具，它可以用來發現網路中的設備、服務和漏洞。Nmap 是一個開放源碼工具，它可以用來進行網路掃描、端口掃描、服務識別、漏洞檢測等。Nmap 是一個非常強大的工具，它可以用來進行網路安全評估、網路監控、網路故障排除等。

網路安全工具與技術的應用與實踐 Nmap 是一個用於網路掃描的工具，它可以用來發現網路中的設備、服務和漏洞。Nmap 是一個開放源碼工具，它可以用來進行網路掃描、端口掃描、服務識別、漏洞檢測等。Nmap 是一個非常強大的工具，它可以用來進行網路安全評估、網路監控、網路故障排除等。

網路安全工具與技術的應用與實踐 Nmap 是一個用於網路掃描的工具，它可以用來發現網路中的設備、服務和漏洞。Nmap 是一個開放源碼工具，它可以用來進行網路掃描、端口掃描、服務識別、漏洞檢測等。Nmap 是一個非常強大的工具，它可以用來進行網路安全評估、網路監控、網路故障排除等。

```
31337
# nmap -A -T4 scanme.nmap.org d0ze

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

Nmap finished: 2 IP addresses (2 hosts up) scanned in 42.291 seconds
flog/home/fyodor/nmap-misc/Screenshots/042006#
```

Nmap 网络扫描利器

网络扫描是网络安全中的一项重要工作，它可以帮助我们了解网络中的主机和端口状态。Nmap 是一款强大的网络扫描工具，它可以帮助我们快速、准确地扫描网络中的主机和端口。Nmap 支持多种扫描方式，包括 TCP 扫描、SYN 扫描、FIN 扫描等。Nmap 还可以扫描主机的操作系统、服务版本等信息。Nmap 是一款非常实用的网络扫描工具，它可以帮助我们快速、准确地扫描网络中的主机和端口。

Nmap 使用 Transmission Control Protocol (TCP) 和 User Datagram Protocol (UDP) 进行扫描。TCP 扫描是通过发送 SYN 包来探测目标主机的端口是否开放。UDP 扫描是通过发送空包来探测目标主机的端口是否开放。Nmap 还支持其他多种扫描方式，如 FIN 扫描、Xmas 扫描等。Nmap 是一款非常实用的网络扫描工具，它可以帮助我们快速、准确地扫描网络中的主机和端口。

Nmap 还可以扫描主机的操作系统、服务版本等信息。Nmap 是一款非常实用的网络扫描工具，它可以帮助我们快速、准确地扫描网络中的主机和端口。Nmap 是一款非常实用的网络扫描工具，它可以帮助我们快速、准确地扫描网络中的主机和端口。

Nmap 是一款非常实用的网络扫描工具，它可以帮助我们快速、准确地扫描网络中的主机和端口。Nmap 是一款非常实用的网络扫描工具，它可以帮助我们快速、准确地扫描网络中的主机和端口。

Nmap 是一款非常实用的网络扫描工具，它可以帮助我们快速、准确地扫描网络中的主机和端口。Nmap 是一款非常实用的网络扫描工具，它可以帮助我们快速、准确地扫描网络中的主机和端口。

Nmap 是一款非常实用的网络扫描工具，它可以帮助我们快速、准确地扫描网络中的主机和端口。Nmap 是一款非常实用的网络扫描工具，它可以帮助我们快速、准确地扫描网络中的主机和端口。

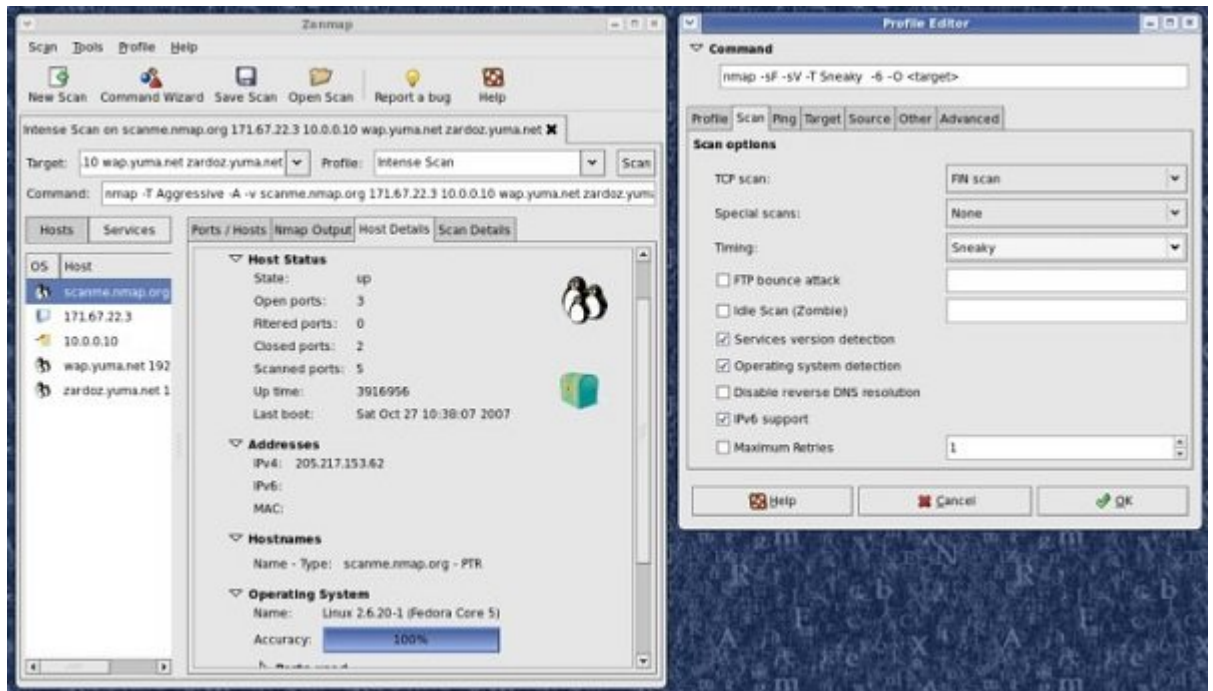
Nmap 是一款非常实用的网络扫描工具，它可以帮助我们快速、准确地扫描网络中的主机和端口。Nmap 是一款非常实用的网络扫描工具，它可以帮助我们快速、准确地扫描网络中的主机和端口。

«.Nmap 是一款非常实用的网络扫描工具，它可以帮助我们快速、准确地扫描网络中的主机和端口。Nmap 是一款非常实用的网络扫描工具，它可以帮助我们快速、准确地扫描网络中的主机和端口。

Networks and Nmap

.Linux, BSD, Solaris, AIX, HP-UX, IRIX, Mac OS, NetBSD, OpenBSD, OS/2, SGI IRIX, Sun Solaris, Tru64 UNIX, VxWorks, Windows, and many others. **Nmap** is also available for many other operating systems, including Red Hat, Debian, Ubuntu, Fedora, CentOS, Mandriva, SUSE, and many others. **Nmap** is also available for many other operating systems, including Red Hat, Debian, Ubuntu, Fedora, CentOS, Mandriva, SUSE, and many others. **Nmap** is also available for many other operating systems, including Red Hat, Debian, Ubuntu, Fedora, CentOS, Mandriva, SUSE, and many others.

□□□□ □□□□□□ **Nmap** □□ □□□□

[illegible]

00 000000 000000 000000000000 000 00 00000 00000 00 00000000 **Nmap** 0000000 00000 0000000000
 :0000 0000000 0000 000000 00 0000000000 0000 00000000 00 00 0000000000

0. 000000 00000000 0000 00 00 0000 00 00 000000 00000000 00000000 **Nmap** : 0000 000000000000 •
 (.000000 00000000 host discovery) 0000 00000000 000000 00 0000 000000 000000 0000 0 00000000

00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 Nmap :00000000 00000000 •
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 (.000000 OS fingerprint) 00000000
.000000 00000000 00000000 00000000 00000000 00000000

000000 00 00 0000 000 0 0000 00000000 00 0000 00 000000 0000000000 00000000 • **Nmap** :000000 00000000 0000 00 00 0000000000 0000 0 0000 000000000000 00000000 0 0000 000 00 00 0000000 00000 00000000 .000 00000000 00000000

□□□□ □□□□□□□□ □□ □□□□ □□ □□ □□□□□□□□□□ □ □□□□□□□□□□ □□□□ □□ □□□□ □□ □□ :□□□□□□ □□□□□□ •

00000 000000 00 000 .00000 00 000 00000 00 00000 00000000 00 0000000 0000 000000
 000 0000 0000 00 0000000 0000 000000 000000000 00 00 0000 0000 00 0000000000 0000 000000 000000
 000 000 0000 00 0000 000000 0000 0000 000 00 0000 000 00000000 00 000 0000 000 000 00000 00000 0
 0000 00 0000000 0000000 000000000 000 00 00000000000 00 00000000 00 .000 000000 000000000000 0
 .000 000000 0000000 000000 00 000 00000000000000 00000000

□□□□□□□□ □ □□□□□□□ □□□□ **Nmap** □□□□□□

000000 00000 0 000000 00000000 000 00000 00 000000 000000 00 000 0000 **Nmap** 00000 00000000 00 000
 00 000 00000 00 000 000000 00000 000000000 00000 00000 00000 00000000 00 00 000000 0000 00 000 0000000000
 00000000 000000 00 00 00000 000000000 000000000 00 0000000000 000000 00000000 00 000000000 00000000 00000000
 .000000 00000 00000 000000

[illegible]

በመጨረሻ ላይ ለጥያቄው ማስፈጸም የሚያስፈልጉትን ምንጮች ለመለየት ማስታወሻዎችን ያውቁ፡

[illegible]

65,535 (65,535) ... UDP 65,535 TCP
 :

(.00000 00000 00 0000 00000) sV •

$$(\text{version-intensity} \times \text{intensity}) < \text{version-intensity} < \text{intensity} \cdot$$
[illegible][illegible]

Nmap (NSE) □□□□□ □□□□□□□□ □□□□□

00 0 000000 000000 00000 Lua 0000000000000 0000 00 00 0000 00000000 000000 00 0000 **Nmap**
 0000 .000000 000000000000 00 000000 000000 000000 00 000000 000000000 000000000000
 0000 0000 0000 00000000 0000 000000000000 000000000000 000000000000 000000 0000 0000 0000000000
 .000 000000000000 00 0000 00 000000 00 0000000000

Nmap 与 Zenmap

[illegible]

Map to Nmap

[illegible]

0000 00 .000 00000000 0000 00 0000000000 000 00000000 00000000 00000000 0000 **Nmap** 0000000000
 000 0000 000000 000000 00 0000000 0 000000 0 000000 00000 0000 0 0000 0000 00 **Nmap** 00000000 000000
 000000 00000 .00000000 0000 00 000 00000000 00 00000000 000000 00 00 00 000 000 000000 00 000 000000
 00000000 000000000 .000000 00000 00000 000000 00 0000 000 0000000 0000 **Nmap** 0000000000 00 00000000 000000
 00000000 000000 000000 00000 0 0000000 000 00000 00000 0000000 00000000 00 000000 0000000000 00000 000000000
 .00000 000000 00000000 00000000000000000000 00000 00 0000000 00000 00 00 000000000 00000000 00

•

● □ □ □ □ □ □ □ □



● □ □ □ □ □ □ □ □ □ □

12:00 - 10/08/1397

•

□□□□□□□□ □□□□□□ - [Nmap](#) - [Network Mapper](#) - □□□□ □□□□□□ □□□□ - □□□□

□□□□□

[https://www.shabakeh-mag.com/networking-technology/14077/nmap-%DA%86%DB%8C%D8:B3%D8%AA-%D9%88-%DA%86%D8%B1%D8%A7-%D8%B4%D9%85%D8%A7-%D8%A8%D9%87-%DA%86%D9%86%DB%8C%D9%86-%D8%A7%D8%A8%D8%B2%D8%A7%D8%B1%DB%8C-%D8%A8%D8%B1%D8%A7%DB%8C-%D9%86%D9%82%D8%B4%D9%87%E2%80%8C%D8%A8%D8%B1%D8%AF%D8%A7%D8%B1%DB%8C-%D8%B4%D8%A8%DA%A9%D9%87-%D9%86%DB%8C%D8%A7%D8%B2-%D8%AF%D8%A7%D8%B1%DB%8C%D8%AF%D8%9F](https://www.shabakeh-mag.com/networking-technology/14077/nmap-%DA%86%DB%8C%D8%B3%D8%AA-%D9%88-%DA%86%D8%B1%D8%A7-%D8%B4%D9%85%D8%A7-%D8%A8%D9%87-%DA%86%D9%86%DB%8C%D9%86-%D8%A7%D8%A8%D8%B2%D8%A7%D8%B1%DB%8C-%D8%A8%D8%B1%D8%A7%DB%8C-%D9%86%D9%82%D8%B4%D9%87%E2%80%8C%D8%A8%D8%B1%D8%AF%D8%A7%D8%B1%DB%8C-%D8%B4%D8%A8%DA%A9%D9%87-%D9%86%DB%8C%D8%A7%D8%B2-%D8%AF%D8%A7%D8%B1%DB%8C%D8%AF%D8%9F)