nmap脚本使用总结

0x00 前言：

nmap的基本介绍和基本使用方法，在乌云知识库中已经有人提交过，讲的比较详细，在此文中就不再讲述。 具体链接：http://drops.wooyun.org/tips/2002

本文主要讲解nmap的众多脚本的使用，在内网渗透的时候尤其好用。

Nmap

nmap -T4 -A -v 192.168.10.100

nmap -A -v www.baidu.com/24

nmap -p22 192.168.53.1 -sV

nmap -p1-65535 192.16.53.1 -sV

nmap -p5000-6000 192.16.53.1 -sV

nmap -sV -O -T4 192.168.1.107

其他使用帮助

Nmap提供的命令行参数如下：

-sC: 等价于–script=default，使用默认类别的脚本进行扫描 可更换其他类别

–script=<Lua scripts>: <Lua scripts>使用某个或某类脚本进行扫描，支持通配符描述

–script-args=<n1=v1,[n2=v2,...]>: 为脚本提供默认参数

–script-args-file=filename: 使用文件来为脚本提供参数

–script-trace: 显示脚本执行过程中发送与接收的数据

–script-updatedb: 更新脚本数据库

–script-help=<scripts>: 显示脚本的帮助信息，其中<scripts>部分可以逗号分隔的文件或脚本类别

0x01 nmap按脚本分类扫描

nmap脚本主要分为以下几类，在扫描时可根据需要设置--script=类别这种方式进行比较笼统的扫描：

auth: 负责处理鉴权证书（绕开鉴权）的脚本

broadcast: 在局域网内探查更多服务开启状况，如dhcp/dns/sqlserver等服务

brute: 提供暴力破解方式，针对常见的应用如http/snmp等

default: 使用-sC或-A选项扫描时候默认的脚本，提供基本脚本扫描能力

discovery: 对网络进行更多的信息，如SMB枚举、SNMP查询等

dos: 用于进行拒绝服务攻击

exploit: 利用已知的漏洞入侵系统

external: 利用第三方的数据库或资源，例如进行whois解析

fuzzer: 模糊测试的脚本，发送异常的包到目标机，探测出潜在漏洞 intrusive: 入侵性的脚本，此类脚本可能引发对方的IDS/IPS的记录或屏蔽

malware: 探测目标机是否感染了病毒、开启了后门等信息

safe: 此类与intrusive相反，属于安全性脚本

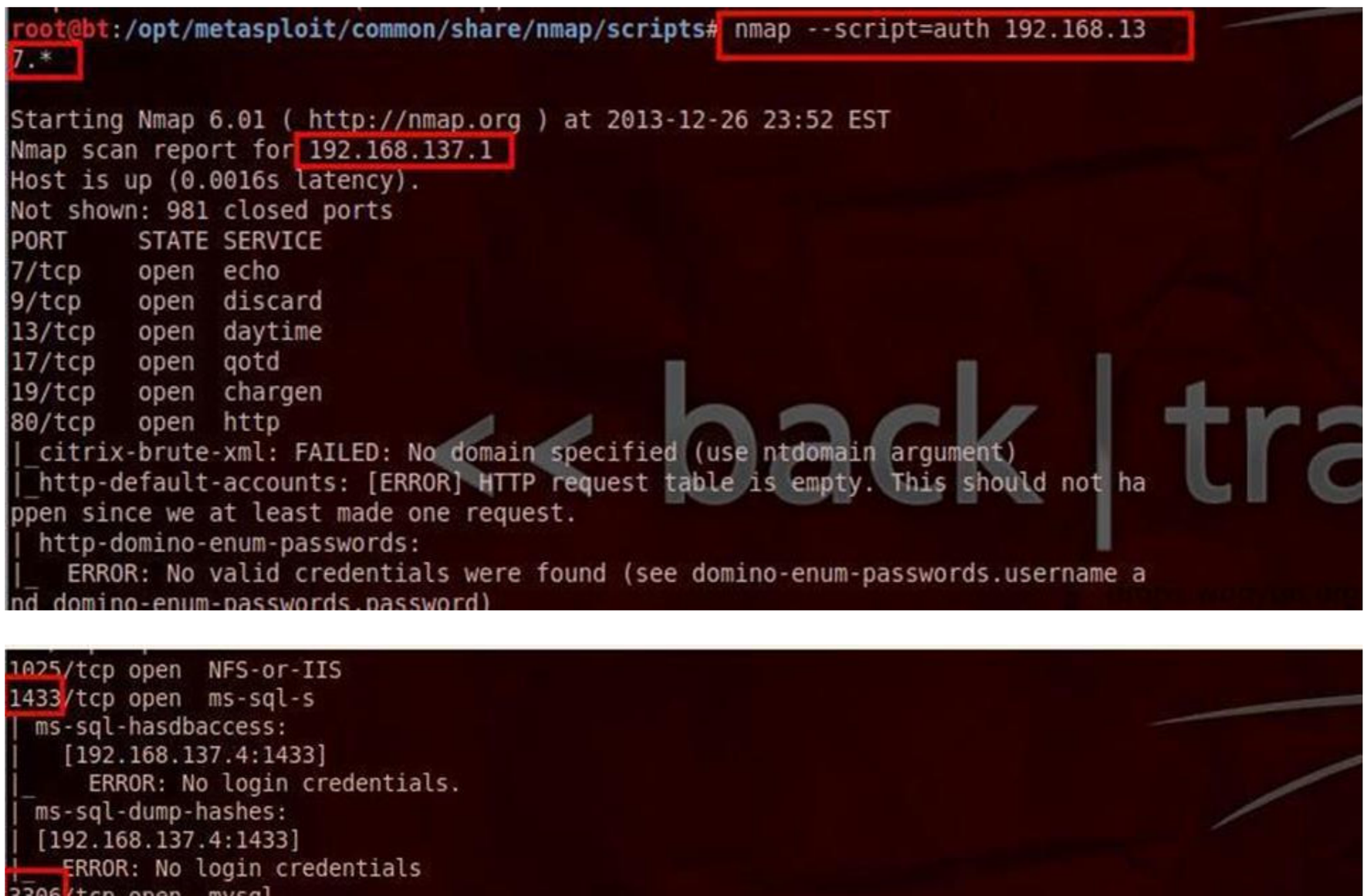
version: 负责增强服务与版本扫描（Version Detection）功能的脚本

vuln: 负责检查目标机是否有常见的漏洞（Vulnerability），如是否有MS08_067

部分使用截图：

（1） `nmap --script=auth 192.168.137.*`

负责处理鉴权证书（绕开鉴权）的脚本,也可以作为检测部分应用弱口令



（2）`nmap --script=brute 192.168.137.*`

提供暴力破解的方式 可对数据库，smb，snmp等进行简单密码的暴力猜解

```
root@bt:/opt/metasploit/common/share/nmap/scripts# nmap -sS --script=brute 192.168.137.*

Starting Nmap 6.01 ( http://nmap.org ) at 2013-12-27 01:19 EST
Nmap scan report for 192.168.137.1
Host is up (0.00067s latency).
Not shown: 981 closed ports
PORT     STATE SERVICE
7/tcp    open  echo
9/tcp    open  discard
13/tcp   open  daytime
17/tcp   open  qotd
19/tcp   open  chargen
80/tcp   open  http
| http-brute:
|_  ERROR: No path was specified (see http-brute.path)
| http-form-brute:
|_  ERROR: No passvar was specified (see http-form-brute.passvar)
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
| http-brute:
|_  ERROR: No path was specified (see http-brute.path)
| http-form-brute:
|_  ERROR: No passvar was specified (see http-form-brute.passvar)
```

（3）`nmap --script=default 192.168.137.*` 或者 `nmap -sC 192.168.137.*`

默认的脚本扫描，主要是搜集各种应用服务的信息，收集到后，可再针对具体服务进行攻击

```
root@bt:/opt/metasploit/common/share/nmap/scripts# nmap -sC 192.168.137.*

Starting Nmap 6.01 ( http://nmap.org ) at 2013-12-27 00:39 EST
Nmap scan report for 192.168.137.1
Host is up (0.0042s latency).
Not shown: 981 closed ports
PORT     STATE SERVICE
7/tcp    open  echo
9/tcp    open  discard
13/tcp   open  daytime
17/tcp   open  qotd
19/tcp   open  chargen
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
|_http-methods: No Allow or Public header in OPTIONS response (status code 501)
| ssl-cert: Subject: commonName=VMware/countryName=US
| Not valid before: 2013-12-24 09:16:48
|_Not valid after:  2014-12-24 09:16:48
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
3306/tcp open  mysql
| mysql-info: Protocol: 10
| Version: 5.5.14
| Thread ID: 51175
| Some Capabilities: Long Passwords, Connect with DB, Compress, ODBC, Transactions, Secure Connection
| Status: Autocommit
|_Salt: +Jr#T\Q`
8009/tcp open  ajp13
8080/tcp open  http-proxy
| http-methods: Potentially risky methods: PUT DELETE
|_See http://nmap.org/nsedoc/scripts/http-methods.html
|_http-favicon: Apache Tomcat
MAC Address: 00:0C:29:5D:24:FB (VMware)

Host script results:
|_nbstat: NetBIOS name: USER-FW21F, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:5d:24:fb (VMware)
|_smbv2-enabled: Server doesn't support SMBv2 protocol
| smb-security-mode:
|   Account that was used for smb scripts: guest
|   User-level authentication
|   SMB Security: Challenge/response passwords supported
|_  Message signing disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows Server 2003 3790 Service Pack 2 (Windows Server 2003 5.2)
|   Computer name: user-fw21f
|   NetBIOS computer name: USER-FW21F
|   Workgroup: WORKGROUP
|_  System time: 2013-12-27 00:42:21 UTC+8
| ms-sql-info:
|   Windows server name: USER-FW21F
|   [192.168.137.4\MSSQLSERVER]
|     Instance name: MSSQLSERVER
|     Version: Microsoft SQL Server 2000 SP4
```

（4）`nmap --script=vuln 192.168.137.*`

检查是否存在常见漏洞

```
root@bt:/opt/metasploit/common/share/nmap/scripts# nmap --script=vuln 192.168.137.*

Starting Nmap 6.01 ( http://nmap.org ) at 2013-12-27 02:12 EST
Stats: 0:00:03 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.00% done
Nmap scan report for 192.168.137.1
Host is up (0.0037s latency).
Not shown: 981 closed ports
PORT     STATE SERVICE
7/tcp    open  echo
9/tcp    open  discard
13/tcp   open  daytime
17/tcp   open  qotd
19/tcp   open  chargen
80/tcp   open  http
| http-vuln-cve2011-3368:
|_  ERROR: Got no answers from pipelined queries
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
```

```
Nmap scan report for 192.168.137.4
Host is up (0.00049s latency).
Not shown: 978 closed ports
PORT     STATE SERVICE
23/tcp   open  telnet
80/tcp   open  http
| http-enum:
|   /fckeditor/editor/filemanager/connectors/test.html: phpmotion/FCKeditor File upload
|   /fckeditor/editor/filemanager/connectors/php/config.php: DM File Manager/FCKeditor File upload
|   /fckeditor/editor/filemanager/connectors/test.html: LightNEasy/FCKeditor File upload
|   /demo/: Potentially interesting folder
|_  /shop/: Potentially interesting folder
81/tcp   open  hosts2-ns
82/tcp   open  xfer
83/tcp   open  mit-ml-dev
84/tcp   open  ctf
85/tcp   open  mit-ml-dev
88/tcp   open  kerberos-sec
89/tcp   open  su-mit-tg
90/tcp   open  dnsix
99/tcp   open  metagram
100/tcp  open  newacct
```

```
8009/tcp open  ajp13
8080/tcp open  http-proxy
| http-vuln-cve2011-3192:
|   VULNERABLE:
|   Apache byterange filter DoS
|     State: VULNERABLE
|     IDs:  CVE:CVE-2011-3192  OSVDB:74721
|     Description:
|       The Apache web server is vulnerable to a denial of service attack when numerous
|       overlapping byte ranges are requested.
|     Disclosure date: 2011-08-19
|     References:
|       http://seclists.org/fulldisclosure/2011/Aug/175
|       http://nessus.org/plugins/index.php?view=single&id=55976
|       http://osvdb.org/74721
|_      http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
| http-enum:
|   /examples/: Sample scripts
|   /manager/html/upload: Apache Tomcat (401 Unauthorized)
|   /manager/html: Apache Tomcat (401 Unauthorized)
|_  /docs/: Potentially interesting folder
MAC Address: 00:0C:29:5D:24:FB (VMware)

Host script results:
| smb-check-vulns:
|_  MS08-067: VULNERABLE

Nmap done: 256 IP addresses (4 hosts up) scanned in 455.23 seconds
```

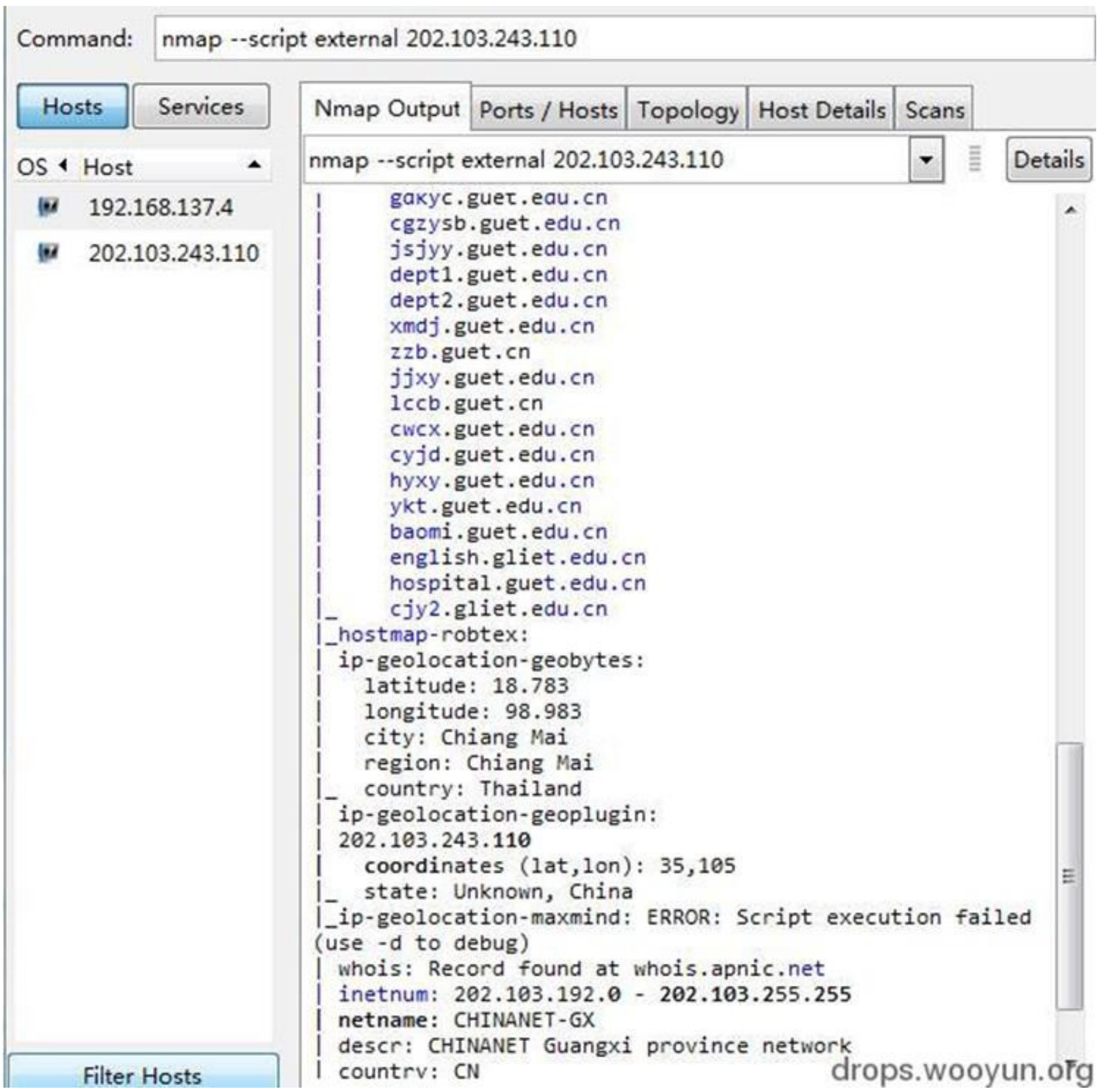
（5）`nmap -n -p445 --script=broadcast 192.168.137.4`

在局域网内探查更多服务开启状况

```
rtt min/avg/max/mdev = 69.757/70.371/70.985/0.614 ms
root@bt:/usr/local/share/nmap/scripts# nmap -n -p445 --script=broadcast 192.168.137.
4

Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-30 00:07 EST
Pre-scan script results:
| broadcast-dhcp-discover:
|   IP Offered: 192.168.137.13
|   Server Identifier: 192.168.137.1
|   Subnet Mask: 255.255.255.0
|   Router: 192.168.137.1
|   Domain Name Server: 192.168.137.1
|_  Domain Name: mshome.net
| broadcast-eigrp-discovery:
|_ ERROR: Couldn't get an A.S value.
| broadcast-igmp-discovery:
|   192.168.137.1
|     Interface: eth1
|     Version: 2
|     Group: 239.255.255.250
|_  Use the newtargets script-arg to add the results as targets
| broadcast-listener:
|   ether
|       OSPF Hello
|
|       ARP Request
|_      sender ip      sender mac      target ip
```


（6）`nmap --script external 202.103.243.110`

利用第三方的数据库或资源，例如进行whois解析

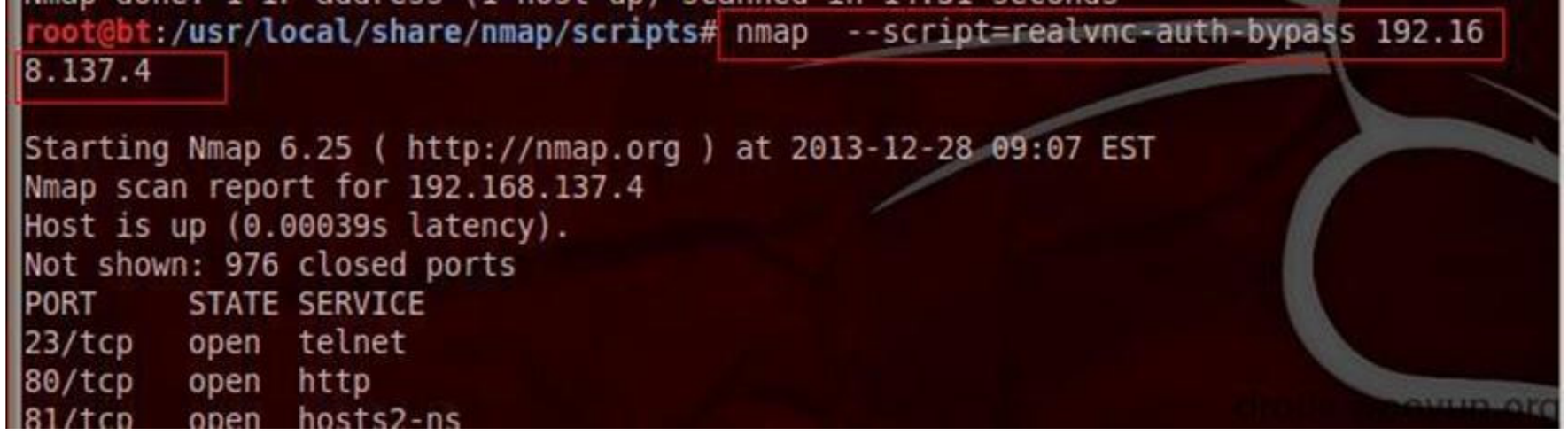


0x02 nmap按应用服务扫描

（1）vnc扫描：

检查vnc bypass

1	nmap --script=realvnc-auth-bypass 192.168.137.4



检查vnc认证方式

1	nmap --script=vnc-auth 192.168.137.4

获取vnc信息

1	nmap --script=vnc-info 192.168.137.4

（2）smb扫描：

smb破解

1	nmap --script=smb-brute.nse 192.168.137.4

smb字典破解

1	nmap --script=smb-brute.nse --script- args=userdb=/var/passwd,passdb=/var/passwd 192.168.137.4

smb已知几个严重漏

1	nmap --script=smb-check-vulns.nse --script-args=unsafe=1 192.168.137.4

```
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1433/tcp open  ms-sql-s
3306/tcp open  mysql
5800/tcp open  vnc-http
5900/tcp open  vnc
8009/tcp open  ajp13
8080/tcp open  http-proxy
MAC Address: 00:0C:29:5D:24:FB (VMware)

Host script results:
| smb-check-vulns:
|   MS08-067: VULNERABLE
|   Conficker: Likely CLEAN
|   SMBv2 DoS (CVE-2009-3103): NOT VULNERABLE
|   MS06-025: NO SERVICE (the Ras RPC service is inactive)
|_  MS07-029: NO SERVICE (the Dns Server RPC service is inactive)

Nmap done: 1 IP address (1 host up) scanned in 19.81 seconds
root@bt:/usr/local/share/nmap/scripts#
```

查看共享目录

```
1  nmap -p 445  --script smb-ls --script-args
   'share=e$,path=\,smbuser=test,smbpass=test' 192.168.137.4
```

查询主机一些敏感信息（注：需要下载nmap_service）

```
1  nmap -p 445 -n  – script=smb-psexec --script-args= smbuser=test,smbpass=test
   192.168.137.4
```

```
root@bt:/usr/local/share/nmap/scripts# nmap -n -p445 --script=smb-psexec --script-ar
gs=smbuser=test,smbpass=test 192.168.137.4

Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-29 22:29 EST
Nmap scan report for 192.168.137.4
Host is up (0.00024s latency).
PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:5D:24:FB (VMware)

Host script results:
| smb-psexec:
|   Windows version
|     Microsoft Windows [\xB0\xE6\xB1\xBE 5.2.3790]
|   IP Address and MAC Address from 'ipconfig.exe'
|     Ethernet adapter \xB1\xBE\xB5\xD8\xC1\xAC\xBD\xD3:
|       MAC Address: 00:0C:29:5D:24:FB
|       IP Address: 192.168.137.4
|   User list from 'net user'
|     \\ \xB5\xC4\xD3\xC3\xBB\xA7\xD5\xCA\xBB\xA7
|     123                  Administrator            ASPNET
|     Guest                IUSR_USER-FW21F          IWAM_USER-FW21F
|     SQLDebugger          SUPPORT_388945a0         test
```

查看会话

```
1  nmap -n -p445 --script=smb-enum-sessions.nse --script-
   args=smbuser=test,smbpass=test 192.168.137.4
```

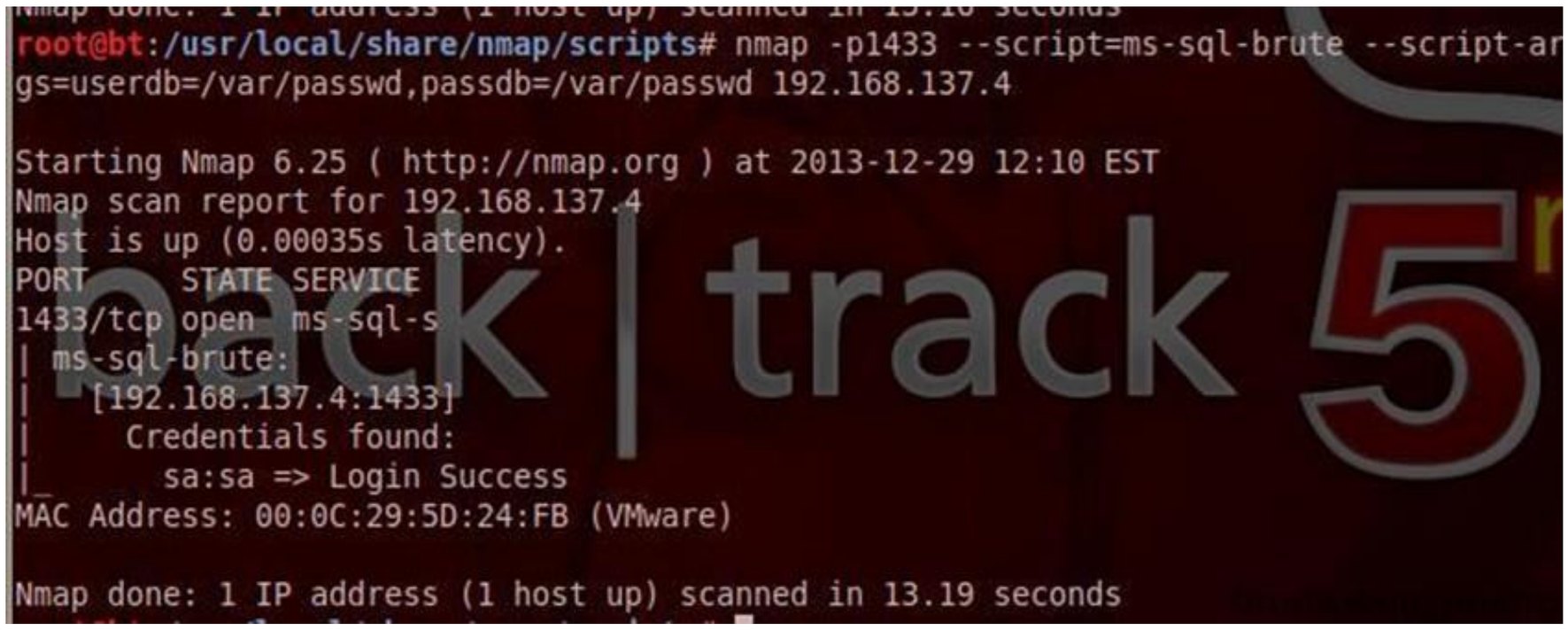
系统信息

```
1  nmap -n -p445 --script=smb-os-discovery.nse --script-
   args=smbuser=test,smbpass=test 192.168.137.4
```

（3）Mssql扫描：

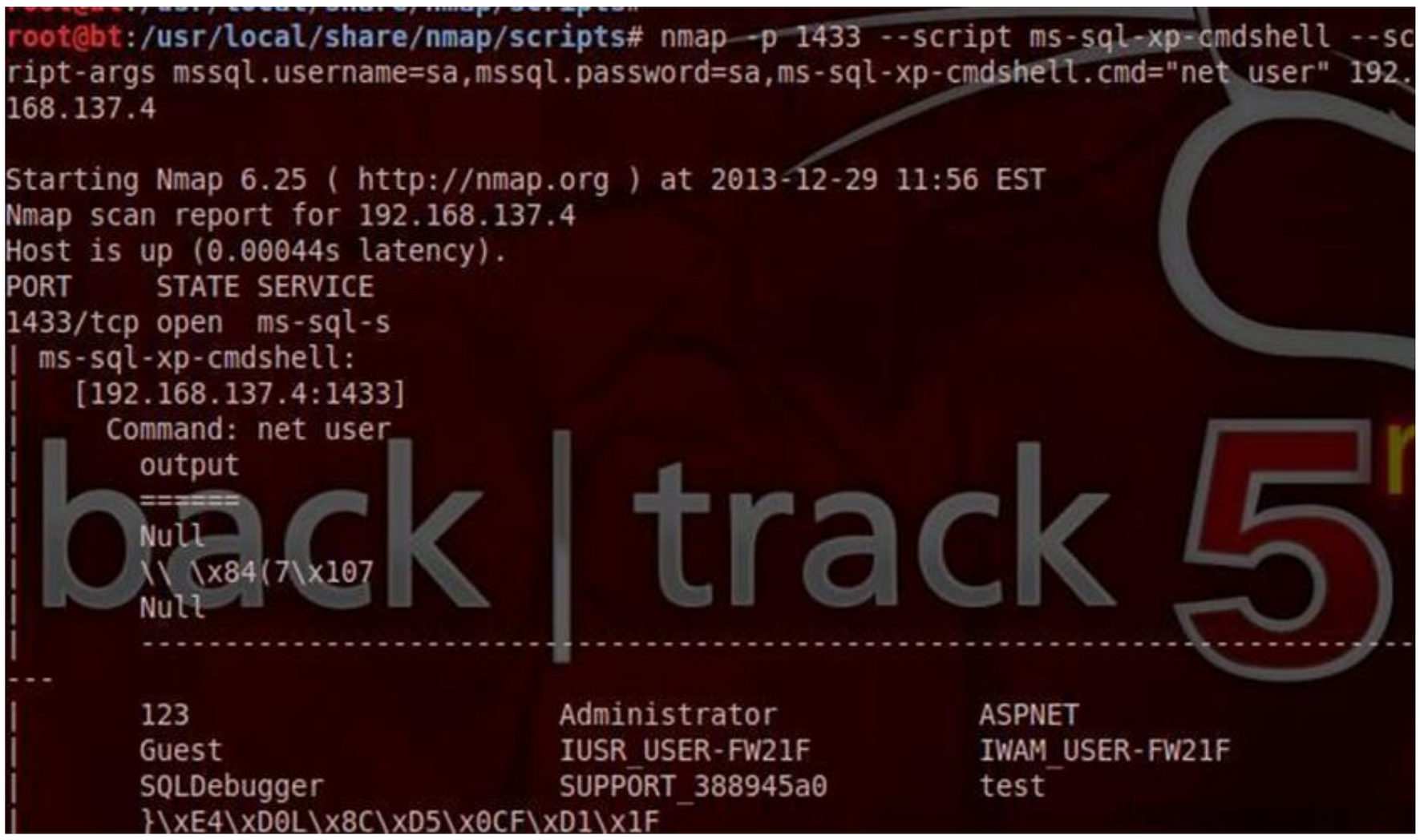
猜解mssql用户名和密码

1	nmap -p1433 --script=ms-sql-brute --script- args=userdb=/var/passwd,passdb=/var/passwd 192.168.137.4



xp_cmdshell 执行命令

1	nmap -p 1433 --script ms-sql-xp-cmdshell --script-args mssql.username=sa,mssql.password=sa,ms-sql-xp-cmdshell.cmd="net user" 192.168.137.4



dumphash值

1	nmap -p 1433 --script ms-sql-dump-hashes.nse --script-args mssql.username=sa,mssql.password=sa 192.168.137.4

```
root@bt:/usr/local/share/nmap/scripts# nmap -p 1433 --script ms-sql-dump-hashes.nse
--script-args mssql.username=sa,mssql.password=sa  192.168.137.4

Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-29 12:00 EST
Nmap scan report for 192.168.137.4
Host is up (0.00033s latency).
PORT     STATE SERVICE
1433/tcp open  ms-sql-s
| ms-sql-dump-hashes:
| [192.168.137.4:1433]
|     a0801170204:0x01009B1FC8315EABB138C52F70E4FCC14B221D04F8531E555D509B6E74653180
15BD06886F827CA22F78CD730072
|     sa:0x01007E03E85B91A9803D69004917618F2F265DE700D838F3801F426AECC60323DF5AC965D
993702BE5BAB3E3212F
|_    ycqy:0x0100DE2FE34DF7D5DDBAEC62987CF47961DA3750EF1C750CACB106B8725081D3AF500FA
CEF175E0522ECC4BC085B
MAC Address: 00:0C:29:5D:24:FB (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.16 seconds
```

（4）Mysql扫描：

扫描root空口令

1	nmap -p3306 --script=mysql-empty-password.nse 192.168.137.4

```
root@bt:/usr/local/share/nmap/scripts# nmap -p3306 --script=mysql-empty-password.nse
 192.168.137.4

Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-29 12:18 EST
Nmap scan report for 192.168.137.4
Host is up (0.00031s latency).
PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-empty-password:
|_   root account has empty password
MAC Address: 00:0C:29:5D:24:FB (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.13 seconds
```

列出所有mysql用户

1	nmap -p3306 --script=mysql-users.nse --script-args=mysqluser=root 192.168.137.4

支持同一应用的所有脚本扫描

1	nmap --script=mysql-* 192.168.137.4

```
3306/tcp open  mysql
| mysql-audit:
|   No audit rulebase file was supplied (see mysql-audit.filename)
| mysql-brute:
|   Accounts
|     root:<empty> - Valid credentials
|   Statistics
|     Performed 26079 guesses in 92 seconds, average tps: 702
|
|_ ERROR: Too many retries, aborted ...
| mysql-databases:
|   information_schema
|   cms4j2010
|   f1cms
|   gdfreenet
|   guangyang
|   ims
|   jeecms_2012_sp1
|   mydede
|   mysql
|   nwhgi
|   osphpsite
|   performance_schema
|   phpcms
```

（5）Oracle扫描：

oracle sid扫描

1	nmap --script=oracle-sid-brute -p 1521-1560 192.168.137.5

```
root@bt:/usr/local/share/nmap/scripts# nmap --script=oracle-sid-brute -p 1521-1560 192.168.137.5

Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-30 10:32 EST
Nmap scan report for 192.168.137.5
Host is up (0.00028s latency).
Not shown: 39 closed ports
PORT     STATE SERVICE
1521/tcp open  oracle
| oracle-sid-brute:
|_  ORCL
MAC Address: 00:0C:29:C4:12:5F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 25.38 seconds
```

oracle弱口令破解

1	nmap --script oracle-brute -p 1521 --script-args oracle-brute.sid=ORCL,userdb=/var/passwd,passdb=/var/passwd 192.168.137.5

```
root@bt:/usr/local/share/nmap/scripts# nmap --script oracle-brute -p 1521 --script-
rgs oracle-brute.sid=ORCL,userdb=/var/passwd,passdb=/var/passwd 192.168.137.5

Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-29 12:32 EST
Nmap scan report for 192.168.137.5
Host is up (0.00030s latency).
PORT     STATE SERVICE
1521/tcp open  oracle
| oracle-brute:
|   Accounts
|     system:system - Valid credentials
|   Statistics
|     Performed 49 guesses in 34 seconds, average tps: 1
|
|_  ERROR: Too many retries, aborted ...
MAC Address: 00:0C:29:C4:12:5F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 47.01 seconds
```

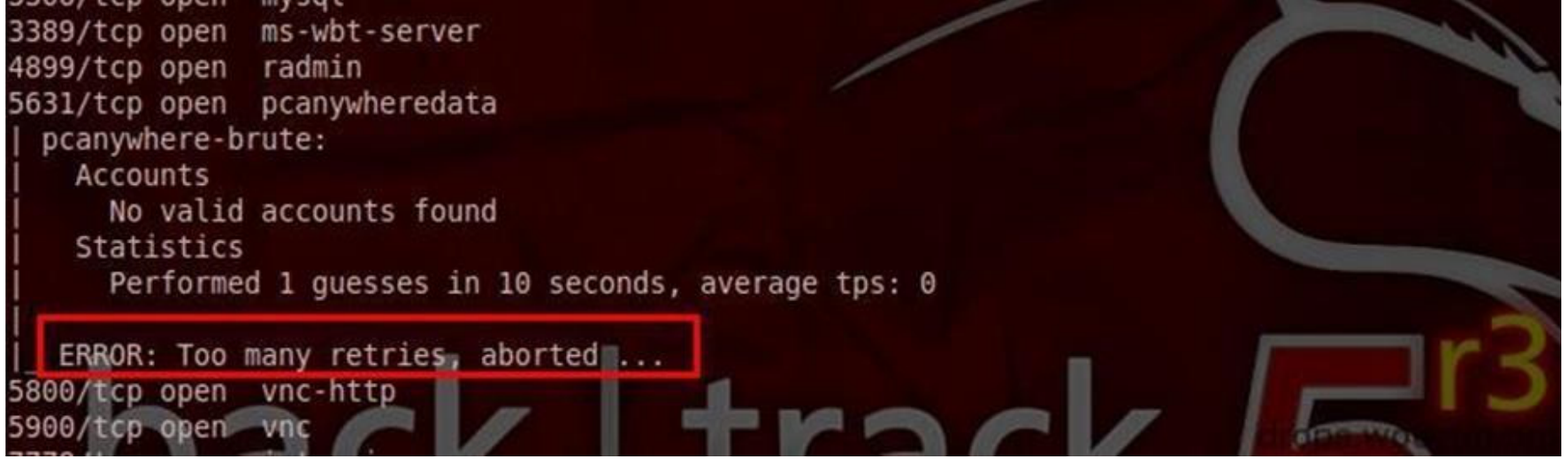
（6）其他一些比较好用的脚本

```
nmap --script=broadcast-netbios-master-browser 192.168.137.4   发现网关

nmap -p 873 --script rsync-brute --script-args 'rsync-brute.module=www'
192.168.137.4  破解rsync

nmap --script informix-brute -p 9088 192.168.137.4    informix数据库破解

nmap -p 5432 --script pgsql-brute 192.168.137.4       pgsql破解

nmap -sU --script snmp-brute 192.168.137.4            snmp破解

nmap -sV --script=telnet-brute 192.168.137.4          telnet破解

nmap --script=http-vuln-cve2010-0738 --script-args 'http-vuln-cve2010-0738.paths=
{/path1/,/path2/}' <target>  jboss autopwn

nmap --script=http-methods.nse 192.168.137.4 检查http方法

nmap --script http-slowloris --max-parallelism 400 192.168.137.4  dos攻击，对于处
理能力较小的站点还挺好用的 'half-HTTP' connections

nmap --script=samba-vuln-cve-2012-1182  -p 139 192.168.137.4
```

（7）不靠谱的脚本：

vnc-brute　次数多了会禁止连接

pcanywhere-brute　同上



0x03 学会脚本分析

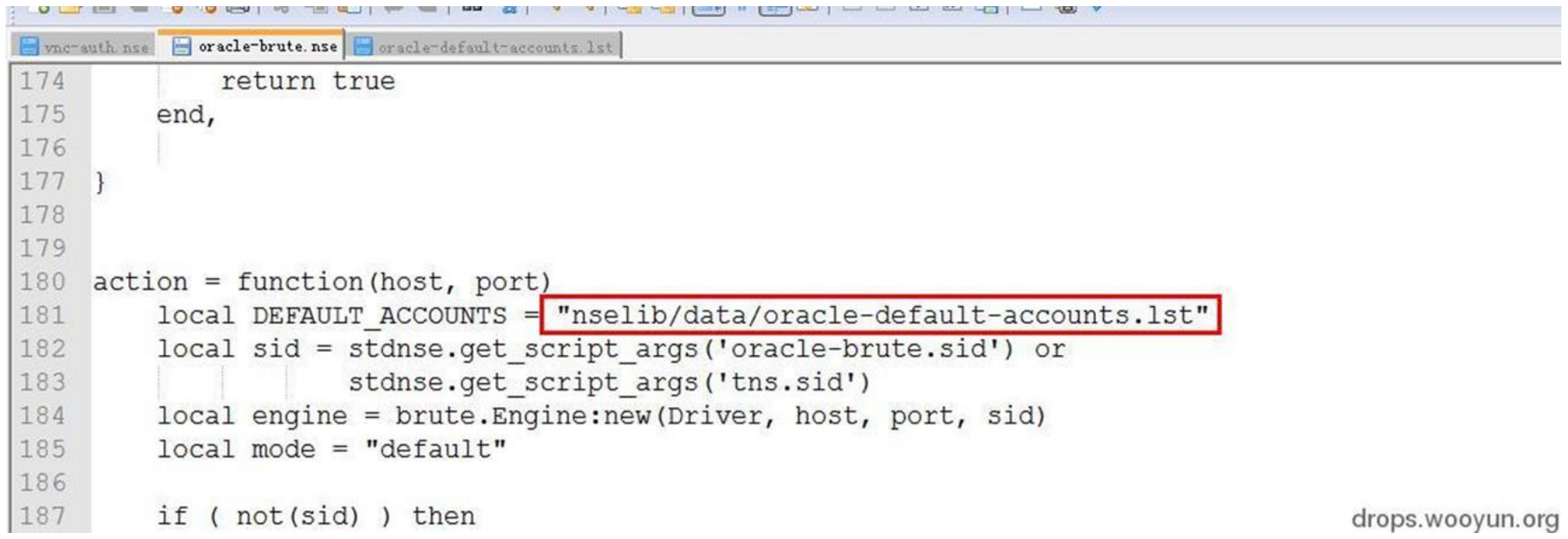
nmap中脚本并不难看懂，所以在使用时如果不知道原理可以直接看利用脚本即可，也可以修改其中的某些参数方便自己使用。

举例：

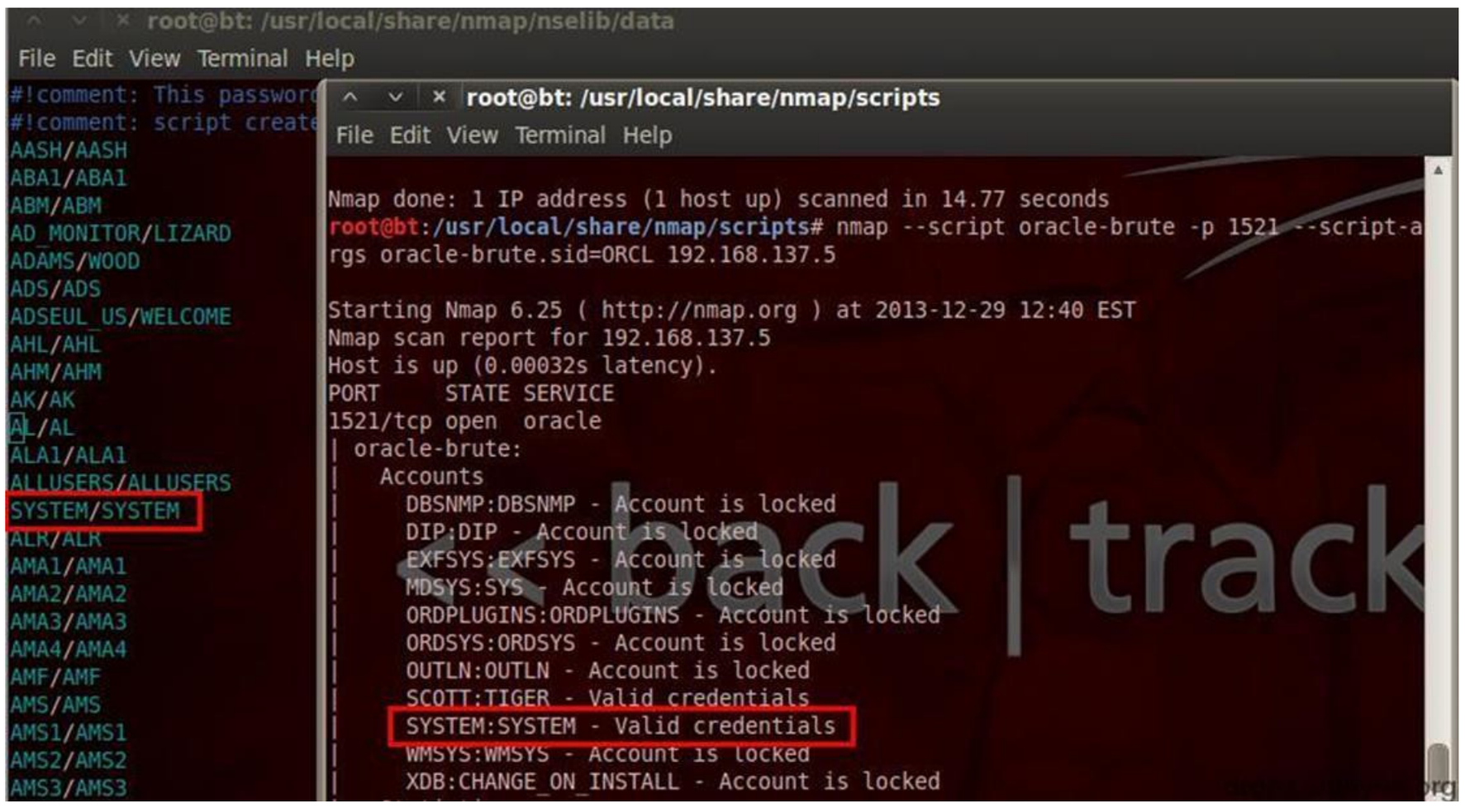
关于oracle的弱口令破解：

调用过程：oracle-brute.nse >> oracle-default-accounts.lst

首先是调用破解脚本：



根据脚本中字典的位置去查看默认字典，当然也可以将破解的字符自行添加其中，或者是修改脚本或参数改变破解字典：



附：

Nmap在实战中的高级用法

Nmap提供了四项基本功能（主机发现、端口扫描、服务与版本侦测、OS侦测）及丰富的脚本库。Nmap既能应用于简单的网络信息扫描，也能用在高级、复杂、特定的

环境中：例如扫描互联网上大量的主机；绕开防火墙/IDS/IPS；扫描Web站点；扫描路由器等等。

简要回顾Nmap简单的扫描方式：

Default

```
全面扫描：nmap-T4 -A targetip

主机发现：nmap-T4 -sn targetip

端口扫描：nmap-T4 targetip

服务扫描：nmap-T4 -sV targetip

操作系统扫描：nmap-T4 -O targetip
```

上述的扫描方式能满足一般的信息搜集需求。而若想利用Nmap探索出特定的场景中更详细的信息，则需仔细地设计Nmap命令行参数，以便精确地控制Nmap的扫描行为。

下面列举比较实用的高级应用场景和技巧。

1　Nmap高级选项

1.1 查看本地路由与接口

Nmap中提供了–iflist选项来查看本地主机的接口信息与路由信息。当遇到无法达到目标主机或想选择从多块网卡中某一特定网卡访问目标主机时，可以查看nmap –iflist中提供的网络接口信息。

nmap –iflist

1.2 指定网口与IP地址

在Nmap可指定用哪个网口发送数据，-e <interface>选项。接口的详细信息可以参考–iflist选项输出结果。

示例：

nmap -e eth0 targetip

Nmap也可以显式地指定发送的源端IP地址。使用-S <spoofip>选项，nmap将用指定的spoofip作为源端IP来发送探测包。

另外可以使用Decoy（诱骗）方式来掩盖真实的扫描地址，例如-D ip1,ip2,ip3,ip4,ME，这样就会产生多个虚假的ip同时对目标机进行探测，其中ME代表本机的真实地址，这样对方的防火墙不容易识别出是扫描者的身份。

nmap -T4 -F -n -Pn -D192.168.1.100,192.168.1.101,192.168.1.102,ME 192.168.1.1

1.3 定制探测包

Nmap提供–scanflags选项，用户可以对需要发送的TCP探测包的标志位进行完全的控制。可以使用数字或符号指定TCP标志位：URG, ACK, PSH,RST, SYN,and FIN。

例如,

nmap -sX -T4 –scanflags URGACKPSHRSTSYNFINtargetip

此命令设置全部的TCP标志位为1，可以用于某些特殊场景的探测。

另外使用–ip-options可以定制IP包的options字段。

使用-S指定虚假的IP地址，-D指定一组诱骗IP地址（ME代表真实地址）。-e指定发送探测包的网络接口，-g（–source- port）指定源端口，-f指定使用IP分片方式发送探测包，–spoof-mac指定使用欺骗的MAC地址。–ttl指定生存时间。

2　扫描防火墙

防火墙在今天网络安全中扮演着重要的角色，如果能对防火墙系统进行详细的探测，那么绕开防火墙或渗透防火墙就更加容易。所以，此处讲解利用Nmap获取防火墙基本信息典型的用法。

为了获取防火墙全面的信息，需尽可能多地结合不同扫描方式来探测其状态。在设计命令行参数时，可以综合网络环境来微调时序参数，以便加快扫描速度。

SYN扫描

首先可以利用基本的SYN扫描方式探测其端口开放状态。

nmap -sS -T4 www.91ri.org

扫描输出为:

Default

```
All 997 ports are filtered

PORT    STATE  SERVICE

80/tcp  open   http

113/tcp closed auth

507/tcp open   crs
```

我们可以看到SYN方式探测到3个端口开放，而有997个端口被过滤。Nmap默认扫描只扫描1000个最可能开放的端口，如果想扫描全部的端口.

使用命令nmap -sS -T4**-p-** www.91ri.org

FIN扫描

然后可以利用FIN扫描方式探测防火墙状态。FIN扫描方式用于识别端口是否关闭，收到RST回复说明该端口关闭，否则说明是open或filtered状态。

nmap -sF -T4 www.91ri.org

Default

```
1     PORT     STATE         SERVICE
2
3     7/tcp    open|filtered echo
4
5     9/tcp    open|filtered discard
6
7     11/tcp   open|filtered systat
8
9     13/tcp   open|filtered daytime
10
11    23/tcp   open|filtered telnet
12
13    25/tcp   open|filtered smtp
14
15    37/tcp   open|filtered time
16
17    79/tcp   open|filtered finger
18
19    80/tcp   open|filtered http
20
21    更多端口，此处省略
```

ACK扫描

然后利用ACK扫描判断端口是否被过滤。针对ACK探测包，未被过滤的端口（无论打开、关闭）会回复RST包。

nmap -sA -T4 www.91ri.org

扫描输出为：

Default

```
1     Not shown: 997 unfiltered ports
2
3     PORT      STATE    SERVICE
4
5     135/tcp   filtered msrpc
6
7     1434/tcp  filtered ms-sql-m
8
9     32777/tcp filtered sometimes-rpc17
```

从结果可以997个端口是未被过滤的（unfiltered），而3个（135/1434/32777）被过滤了。所以，将ACK与FIN扫描 的结果结合分析，我们可以找到很多开放的端口。例

如7号端口，FIN中得出的状态是:open或filtered，从ACK中得出的状态是 unfiltered，那么该端口只能是open的。

Window扫描

当然也可以利用Window扫描方式，得出一些端口信息，可以与之前扫描分析的结果相互补充。Window扫描方式只对某些TCPIP协议栈才有效。

window扫描原理与ACK类似，发送ACK包探测目标端口，对回复的RST包中的Window size进行解析。在某些TCPIP协议栈实现中，关闭的端口在RST中会将Window size设置为0；而开放的端口将Window size设置成非0的值。

nmap -sW -p- -T4 www.91ri.org

输出结果:

Default

```
PORT      STATE    SERVICE

7/tcp     open     echo

9/tcp     open     discard

11/tcp    open     systat

13/tcp    open     daytime

更多端口，此处省略
```

在采用多种方式获取出防火墙状态后，可以进一步进行应用程序与版本侦测及OS侦测。

此处不再赘述！91ri.org：小编这里份关于使用nmap突破防火墙的文章 推荐一下《Nmap绕过防火墙&脚本的使用》

3　扫描路由器

Nmap内部维护了一份系统与设备的数据库（nmap-os-db），能够识别数千种不同系统与设备。所以，可以用来扫描主流的路由器设备。

3.1 扫描思科路由器

nmap -p1-25,80,512-515,2001,4001,6001,9001 10.20.0.1/16

思科路由器会在上述端口中运行了常见的服务。列举出上述端口开放的主机，可以定位到路由器设备可能的IP地址及端口状态。

3.2 扫描路由器TFTP

nmap –sU –p69 –nvv target

大多数的路由器都支持TFTP协议（简单文件传输协议），该协议常用于备份和恢复路由器的配置文件，运行在UDP 69端口上。使用上述命令可以探测出路由器是否开放TFTP。

3.3 扫描路由器操作系统

与通用PC扫描方式类似，使用-O选项扫描路由器的操作系统。-F用于快速扫描最可能开放的100个端口，并根据端口扫描结果进一步做OS的指纹分析。

nmap -O -F -n 192.168.1.1

4 扫描互联网

Nmap内部的设计非常强大灵活，既能扫描单个主机、小型的局域网，也可以扫描成千上万台主机从中发掘用户关注的信息。扫描大量主机，需要对扫描时序等参数进行仔细的优化。

4.1 发现互联网上web服务器

nmap -iR 100000 -sS -PS80 -p 80 -oG nmap.txt

随机地产生10万个IP地址，对其80端口进行扫描。将扫描结果以greppable（可用grep命令提取）格式输出到nmap.txt文件。

可以使用grep命令从输出文件提取关心的细节信息。

4.2 统计互联网主机基本数据

Nmap的创始人Fyodor在2008年的Black Hat大会发表一篇演讲，讲的是如何使用Nmap来扫描互联网（Nmap: Scanning the Internet），资料地址：http://nmap.org/presentations/BHDC08/。

Fyodor进行互联网扫描的初衷是统计出网络经验数据并用之优化Nmap的性能。例如，根据统计出每个端口开放的概率，优先扫描常见端口，以节省用户的时间。

产生随机IP地址

产生100万个随机的IP地址，并将之保存到文件中，方便后续扫描时作为参数输入。

nmap -iR 1200000 -sL -n | grep “not scanned” | awk ‘{print $2}’ | sort -n | uniq >! tp; head -25000000 tp >! tcp-allports-1M-IPs; rm tp

上述命令含义：随机生成1200000个IP地址（-iR 120000），并进行列表扫描（-sL，列举出IP地址，不进行真正的扫描），不进行dns解析操作（-n），这样将产生Nmap列表扫描的结果。在此 结果中搜出未扫描的行（grep “not scanned”），打印出每一行的第二列内容（awk ‘{print $2}’，也就是IP地址），然后对获取到的IP地址进行排序（sort -n），然后剔除重复IP地址，将结果保存到临时文件tp，再取出前1000000

个IP地址保存到tcp-allports-1M-IPs文件中，删除 临时文件。

总之，此处产生了1000000个随机IP地址存放在tcp-allports-1M-IPs文件中。

优化主机发现

nmap -sP -PE -PP -PS21,22,23,25,80,113,31339-PA80,113,443,10042 –source-port 53 -T4 -iL tcp-allports-1M-IPs

上述命令进行主机发现：使用产生的IP地址（-iL tcp-allports-1M-IPs），指定发送包的源端口为53（–source-port 53，该端口是DNS查询端口，一般的防火墙都允许来自此端口的数据包），时序级别为4（-T4，探测速度比较快），以TCP SYN包方式探测目标机的21,22,23,25,80,113,31339端口，以TCP ACK包方式探测对方80,113,443,10042端口，另外也发送ICMP ECHO/ICMP TIMESTAMP包探测对方主机。只要上述的探测包中得到一个回复，就可以证明目标主机在线。

完整的扫描命令

在准备了必要的IP地址文件，并对主机发现参数优化后，我们就得到最终的扫描命令：

nmap -S [srcip] -d –max-scan-delay 10 -oAlogs/tcp-allports-%T-%D -iL tcp-allports-1M-IPs –max-retries 1–randomize-hosts -p- -PS21,22,23,25,53,80,443 -T4 –min-hostgroup 256 –min-rate175 –max-rate 300

上述命令用于扫描互联网上100万台主机全部的TCP端口的开放情况。

使用包含100万个IP地址的文件（-iL tcp-allports-1M-IPs），源端IP地址设置为srcip(指定一个IP地址，保证该IP地址位于统一局域网中，否则无法收到目标机的回复包)，主机发现过程使用TCP SYN包探测目标机的21,22,23,25,53,80,443，扫描过程将随机打乱主机顺序（–randomize-hosts，因为文件中的IP 已经排序，这里将之打乱，避免被防火墙检查出），端口扫描过程检查全部的TCP端口（-p-，端口1到65535），使用时序级别为4（-T4，速度比较 快），将结果以XML/grepable/普通格式输出到文件中（-oA logs/tcp-allports-%T-%D，其中%T表示扫描时间，%D表示扫描日期）。

-d表示打印调试出信息。

–max-scan-delay 10表示发包最多延时10秒，防止特殊情景下等待过长的时间。

–max-retries 1，表示端口扫描探测包最多被重传一次，防止Nmap在没有收到回复的情况下多次重传探测包，当然这样也会降低探测的准确性。

–min-host-group 256表示进行端口扫描与版本侦测时，同时进行探测的主机的数量，这里至少256个主机一组来进行扫描，可以加快扫描速度。

–min-rate 175和–max-rate 300，表示发包速率介于175和300之间，保证扫描速度不会太慢，也不会因为速率过高引起目标机的警觉。

扫描结果

Fyodor组织的此次扫描得出很多重要结论，统计出了互联网最有可能开放的10个TCP端口。

- 80 (http)
- 23 (telnet)
- 22 (ssh)
- 443 (https)
- 3389 (ms-term-serv)
- 445 (microsoft-ds)
- 139 (netbios-ssn)
- 21 (ftp)
- 135 (msrpc)
- 25 (smtp)

最有可能开放的10个UDP端口。

- 137 (netbios-ns)
- 161 (snmp)
- 1434 (ms-sql-m)
- 123 (ntp)
- 138 (netbios-dgm)
- 445 (microsoft-ds)
- 135 (msrpc)
- 67 (dhcps)
- 139 (netbios-ssn)
- 53 (domain)

5　扫描Web站点

Web是互联网上最广泛的应用，而且越来越多的服务倾向于以Web形式提供出来，所以对Web安全监管也越来越重要。目前安全领域有很多专门的 Web扫描软件（如AppScan、WebInspect、W3AF），能够提供端口扫描、漏洞扫描、漏洞利用、分析报表等诸多功能。而Nmap作为一款 开源的端口扫描器，对Web扫描方面支持也越来越强大，可以完成Web基本的信息探测：服务器版本、支持的Method、是否包含典型漏洞。功能已经远远 超过同领域的其他开源软件，如HTTPrint、Httsquash。

目前Nmap中对Web的支持主要通过Lua脚本来实现，NSE脚本库中共有50多个HTTP相关的脚本。

扫描实例：

nmap -sV -p 80 -T4 –script http*,defaultscanme.nmap.org

上面以扫描scanme.nmap.org的Web应用展示Nmap提供Web扫描能力，从图中可以看到扫描结果中提供了比较丰富的信息。

首先是应用程序及版本：**Apachehttpd 2.2.14 (Ubuntu)**

然后搜出了该站点的affiliate-id:该ID可用于识别同一拥有者的不同页面。

然后输出HTTP-headers信息，从中查看到基本配置信息。

从http-title中，可以看到网页标题。某些网页标题可能会泄漏重要信息，所以这里也应对其检查。

有想深入学习nmap的也可以参考：《渗透测试工具Nmap从初级到高级》文章

from:http://blog.csdn.net/aspirationflow/article/details/7983368

最新IT新闻:

· 天猫双11：人类历史上最大规模人机协同
· 免费看！《功守道》完整版上线：马云与功夫群星过招
· 乐视网再度否认放弃电视业务，称产量正在恢复
· 360回归记：从美国退市 再回中国上市
· 京东切入北京住房租赁平台：链家、我爱我家数据接入

» 更多新闻...

最新知识库文章:

· 关于编程，你的练习是不是有效的?
· 改善程序员生活质量的 3+10 习惯
· NASA的10条代码编写原则
· 为什么你参加了那么多培训，却依然表现平平?
· 写给初学前端工程师的一封信

» 更多知识库文章...