此文章已于 1:12:26 2015/12/25 发布到 Net | Linux | 安全

★Kali信息收集★8.Nmap ：端口扫描

* 1. **参数：（Zenmap是Nmap图形化工具，不想打指令的可以直接使用）**

详细：<https://nmap.org/man/zh/index.html>

计算机生成了可选文字:
/ home/ dnt# nmap - h 
Nmap 6. 49BETA4 ( 
https: //nmap. org ) 
Usage: nmap (Scan Type( s) I (Opt Ions) (target specificatioro 
TARGET 
SPEC 
CA ION 
Can pass hostnames, 
IP addresses, 
netwo rks, etc. 
ft. 
com/24, 192. 168. O. 1; 
10. o. 255. 1-254 
x: scanme. nmap. org, ml c roso 
-il_ cinputfilename»: 
Input from list 
f hosts/ netwo rks 
iR enum host": Choose random targets 
exclude chostl(, host21 1, host31 , 
Exclude hosts/ netwo rks 
-exclude file exclude 
file 
Exclude 
list from fil 
HOST DISCOVERY: 
st Scan 
simply list targets to scan 
sn: Ping Scan 
disable port scan 
-Pn: T reat all hosts as online 
skip host discovery 
PS/ PA/ PCI/ po rtlistl 
TCP S Y N/ ACK, UDP or SC TP discovery to given ports 
PE/ PM: ICMP echo, 
timestamp, and netmask request discovery probes 
POI protoco 
1 listl 
IP Protocol Ping 
-n/ -R: Never do DNS resolution/ Always resolve (default. 
sometimes) 
- dns- servers (servl(, serv21 , 
Spec 1 y custom DNS servers 
system- dns: 
Use OS' s DNS resolver 
Trace hop path to each host 
-trace route: 
SCAN TECHNIQUES 
- SS/ s /sA/ sW/ sM: TCP S Y N/ ACK/Window/ Maimon scans 
so: UDP Scan 
- SNI sF/ sX: 
TCP Null, FIN, and Xmas scans 
scan flags c flags»: Customize TCP scan flags 
-sl czombie host(: probeportl 
Idle scan 
sz: SCTP INIT/ COOKI 
CHO scans 
IP protocol scan 
b (FTP relay host»: 
FTP bounce scan 

Nmap 6.49BETA4 ( <https://nmap.org> )

Usage: nmap [Scan Type(s)] [Options] {target specification}

**TARGET SPECIFICATION:**

Can pass hostnames, IP addresses, networks, etc.

Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254

-iL <inputfilename>: Input from list of hosts/networks

-iR <num hosts>: Choose random targets

--exclude <host1[,host2][,host3],...>: Exclude hosts/networks

--excludefile <exclude\_file>: Exclude list from file

**HOST DISCOVERY**:

-sL: List Scan - simply list targets to scan

-sn: Ping Scan - disable port scan

-Pn: Treat all hosts as online -- skip host discovery

-PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports

-PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes

-PO[protocol list]: IP Protocol Ping

-n/-R: Never do DNS resolution/Always resolve [default: sometimes]

--dns-servers <serv1[,serv2],...>: Specify custom DNS servers

--system-dns: Use OS's DNS resolver

--traceroute: Trace hop path to each host

**SCAN TECHNIQUES:**

-sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans

-sU: UDP Scan

-sN/sF/sX: TCP Null, FIN, and Xmas scans

--scanflags <flags>: Customize TCP scan flags

-sI <zombie host[:probeport]>: Idle scan

-sY/sZ: SCTP INIT/COOKIE-ECHO scans

-sO: IP protocol scan

-b <FTP relay host>: FTP bounce scan

**PORT SPECIFICATION AND SCAN ORDER:**

-p <port ranges>: Only scan specified ports

Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9

--exclude-ports <port ranges>: Exclude the specified ports from scanning

-F: Fast mode - Scan fewer ports than the default scan

-r: Scan ports consecutively - don't randomize

--top-ports <number>: Scan <number> most common ports

--port-ratio <ratio>: Scan ports more common than <ratio>

**SERVICE/VERSION DETECTION:**

-sV: Probe open ports to determine service/version info

--version-intensity <level>: Set from 0 (light) to 9 (try all probes)

--version-light: Limit to most likely probes (intensity 2)

--version-all: Try every single probe (intensity 9)

--version-trace: Show detailed version scan activity (for debugging)

**SCRIPT SCAN:**

-sC: equivalent to --script=default

--script=<Lua scripts>: <Lua scripts> is a comma separated list of

directories, script-files or script-categories

--script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts

--script-args-file=filename: provide NSE script args in a file

--script-trace: Show all data sent and received

--script-updatedb: Update the script database.

--script-help=<Lua scripts>: Show help about scripts.

<Lua scripts> is a comma-separated list of script-files or

script-categories.

**OS DETECTION:**

-O: Enable OS detection

--osscan-limit: Limit OS detection to promising targets

--osscan-guess: Guess OS more aggressively

**TIMING AND PERFORMANCE:**

Options which take <time> are in seconds, or append 'ms' (milliseconds),

's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).

-T<0-5>: Set timing template (higher is faster)

--min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes

--min-parallelism/max-parallelism <numprobes>: Probe parallelization

--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies

probe round trip time.

--max-retries <tries>: Caps number of port scan probe retransmissions.

--host-timeout <time>: Give up on target after this long

--scan-delay/--max-scan-delay <time>: Adjust delay between probes

--min-rate <number>: Send packets no slower than <number> per second

--max-rate <number>: Send packets no faster than <number> per second

**FIREWALL/IDS EVASION AND SPOOFING:**

-f; --mtu <val>: fragment packets (optionally w/given MTU)

-D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys

-S <IP\_Address>: Spoof source address

-e <iface>: Use specified interface

-g/--source-port <portnum>: Use given port number

--proxies <url1,[url2],...>: Relay connections through HTTP/SOCKS4 proxies

--data <hex string>: Append a custom payload to sent packets

--data-string <string>: Append a custom ASCII string to sent packets

--data-length <num>: Append random data to sent packets

--ip-options <options>: Send packets with specified ip options

--ttl <val>: Set IP time-to-live field

--spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address

--badsum: Send packets with a bogus TCP/UDP/SCTP checksum

**OUTPUT:**

-oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,

and Grepable format, respectively, to the given filename.

-oA <basename>: Output in the three major formats at once

-v: Increase verbosity level (use -vv or more for greater effect)

-d: Increase debugging level (use -dd or more for greater effect)

--reason: Display the reason a port is in a particular state

--open: Only show open (or possibly open) ports

--packet-trace: Show all packets sent and received

--iflist: Print host interfaces and routes (for debugging)

--append-output: Append to rather than clobber specified output files

--resume <filename>: Resume an aborted scan

--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML

--webxml: Reference stylesheet from Nmap.Org for more portable XML

--no-stylesheet: Prevent associating of XSL stylesheet w/XML output

**MISC:**

-6: Enable IPv6 scanning

-A: Enable OS detection, version detection, script scanning, and traceroute

--datadir <dirname>: Specify custom Nmap data file location

--send-eth/--send-ip: Send using raw ethernet frames or IP packets

--privileged: Assume that the user is fully privileged

--unprivileged: Assume the user lacks raw socket privileges

-V: Print version number

-h: Print this help summary page.

**EXAMPLES:**

nmap -v -A scanme.nmap.org

nmap -v -sn 192.168.0.0/16 10.0.0.0/8

nmap -v -iR 10000 -Pn -p 80

SEE THE MAN PAGE (<https://nmap.org/book/man.html>) FOR MORE OPTIONS AND EXAMPLES

离线下载：<http://pan.baidu.com/s/1dEiZdJV>

* 1. **应用：（常用的速度快点，完整的更详细但慢点~【主要就是全端口扫而导致慢的】）**
  + 重要 **识别系统：(先看看，后面有详解)**

**nmap -O -Pn ip地址**

计算机生成了可选文字:
rootMaLi: nmap -O 
Starting Nmap 6. 49 
BET 
Nmap scan report for 192. 
192. 168. 232. 134 
https: //nmap. org ) 
168. 232. 134 
at 2015. 12-23 15: 04 CS 
we could not find at least 1 
linux kernel: 3 
open and 1 
3. 10 
closed port 
Host is up (0. 0007 Is latency) _ 
Not shown: 999 
filtered ports 
SERVICE 
22/ t cp open ssh 
MAC Address: 00: CC: 29: 46: E9: EA (VMware) 
Wa rning: OSScan results may be unreliable because 
Device type: general purpose 
x 2.6. X13.x 
Running: 
Linu 
OS CPE. 
cpe: / o: linux: linux_kernel: 2. 6 cpe: / o: linux 
OS details: 
Linu 
x 2. 6.32 - 3. 10, 
Linux 2. 6. 32 - 3. 13 
Network Distance: 1 hop 
OS detection performed. Please report any incorrect 
Nmap done: 1 
IP address (1 host up) scanned in 7. 40 
Linu 
x 
resul ts 
seconds 
3. 10, 
Linux 3.4 - 
at https: //nmap. org/ submit 

计算机生成了可选文字:
host cnblogs. com 
cnblogs. com has address 42. 121. 252. 58 
-nmap -O 
PN 42. 121. 252. 58 
Starting Nmap 6. 49BETA4 ( 
https: //nmap. org ) at 2015- 12-23 15: 05 CS 
Stats: 0: 00: 41 elapsed; 0 hosts completed (1 up), 
undergoing SYN Stealth Scan 
SYN Stealth Scan Timing: About 99. 37% done; 
ET 
C: 15: 06 (0: 00: 00 remaining) 
Nmap scan report for 42. 121. 252. 58 
Host is up (0. 015s latency) _ 
Not shown: 998 
filtered ports 
PORT 
80/ tcp 
443/ tcp 
Wa rning: 
Device 
Running: 
OS CPE. 
SERVICE 
open http 
open https 
OSScan results may be unreliable because we could not find at least 1 open and 1 closed port 
ype: specialized I WAPI phone 
iPXE 1 X 
Linksys 
Linu 
Linux 2. 6. X, Sony Ericsson embedded 
cpe: / o: 1 pxe: 1 pxe: 1. O. 0BQb cpe: / o: linksys: linux_kernel: 2. 4 cpe: / o: linux: linux_kernel: 2. 6 cpe: / h: son 
Tomato 1.28 (Linu 
x 2. 4. 20), 
Tomato 
fi rmwa re 
Linux 2. 6. 22), Sony Ericsson C18i Viva 
Please report any incorrect results at https: //nmap. org/ submit 
(1 host up) scanned in 45. 96 seconds 
ericsson: u8i vivaz 
OS details: 
IPXE 1. O. 0+, 
z mobile phone 
OS detection performed. 
Nmap done: 1 
IP address 

计算机生成了可选文字:
: nmap h02. 168. 169. 105 
rootMati 
Starting Nmap 6.49BETAaq httbs: //nmab. Org ) 
Nmap scan report for 192. 168. 169. 105 
Host is up (0. 30s latency) _ 
Not shown: 988 closed po rte 
at 12-23 15: 10 CS 
PORT 
80/ tcp 
135/ tcp 
139/ tcp 
443/ tcp 
444/ tcp 
445/ tcp 
514/ tcp 
902,' tcp 
912,' tcp 
1433,' tcp 
2179,'tcp 
2383/ tcp 
STATE 
operi 
open 
open 
open 
open 
open 
filtered 
open 
open 
open 
open 
open 
SERVICE 
http 
ms rpc 
netbiog-esn 
https 
•npp 
mic de 
shell 
ss- reålkécura 
-apex- mesh 
ms- sql- s 
vm rdp 
ms- olap4 
Device type: general purpose 
Running: Mic rosoft Windows 7120121 XP 
OS CPE. 
cpe: / o: 
mic rosoft: windows_7 cpe: / o: 
mic rosoft: windows _ server 2012 cpe: / o: mic rosoft: windows_xp: : sp3 
OS details: Mic rosoft Windows 7 or Windows Server 2012, Mic rosoft Windows XP SP3 
OS detection performed. Please report any incorrect results at https: //nmap. org/ submit 
Nmap done: 1 
IP address (1 host up) scanned in 688. 18 seconds 

* + 重要 **TCP扫描**：端口扫描中最稳定的，**TCP三次握手**

**常用：nmap -sT -Pn ip地址**

计算机生成了可选文字:
nmap -S 
PN 42-121, 252. 58 
Starting Nmap 6. 49BETA4 ( 
https: //nmapargy at 2015. 1 Z. 23 11:37 CS 
Nmap scan report for 42. 121. 252. 58 
Host is up (O. 015s latency) . 
Not shown: 998 
filtered ports 
scanned in 47. 88 seconds 
PORT 
80/ t cp open 
443/ tcp open 
Nmap done: 1 
SERVICE 
http 
https 
IP address 
host u 

**完整：nmap -sT -p- -Pn ip地址**

计算机生成了可选文字:
cnblogs. com 
cnblogs. com 
cnblogs. com 
cnblogs. com 
cnblogs. com 
cnblogs. com 
cnblogs. com 
cnblogs. com 
host cnblogs. com 
has address 42. 121. 
252. 58 
30 aspmx3. googlemail. 
30 aspmx5. googlemail. 
20 altl. aspmx. l. google. com 
10 aspmx. l. google. com 
30 aspmx4. googlemail. 
20 alt2. aspmx. l. google. com 
30 aspmx2. googlemail. 
mail 
mail 
mail 
mail 
mail 
mail 
mail 
nmap 
is handled by 
is handled by 
is handled by 
is handled by 
is handled by 
is handled by 
is handled by 
PN 42. 121. 252. 58 
Starting Nmap 6. 49BETA4 ( 
https: //nmap. org ) at 2015- 12-22 23: 24 CS 

**-sT** TCP连接扫描（s=>哪种类型扫描？ ==>t TCP类型）

**-p-** 扫描所有端口 （不加就默认扫描1000个常用端口）

**-Pn** 禁用Nmap网络发现功能，假定所有系统都是活动的

**批量扫描 eg：nmap -sT -p- -Pn 192.168.1.1-254**

* + 重要 **SYN 扫描**：★端口扫描中用的最多的，**TCP两次握手**（隐形扫描，速度快）

**常用：nmap -sS -Pn ip地址**

计算机生成了可选文字:
fPN 42-121* 252. 58 
Starting Nmap 6. 49BE A4 ( 
https: // nnpapargy at 201512-23 Il; 35 CS 
Nmap scan report for 42. 121. 252. 58 
Host is up (O. 016s latency) 
Not shown: 998 
filtered ports 
scanned in 42. 99 seconds 
PORT 
80/ t cp open 
443/ tcp open 
Nmap done: 1 
SERVICE 
http 
https 
IP address (1 host up) 

**完整：nmap -sS -p- -Pn ip地址**

计算机生成了可选文字:
nmap -ss -p- 
Starting Nmaö 6' 49BETA4V ( 
PN 42. 121. 252. 58 
httos: LTriii1aKY.OfO ) 
at 201542' 23 
10: 37 cs 

**-sS** （-s => 哪种扫描类型？S=> SYN）

* + 重要 **UDP 扫描**：（DHCP,DNS,SNMP,TFTP等都使用了UDP协议）

**常用：nmap -sU ip地址**

计算机生成了可选文字:
rootMati. 
• nmap -slJ 192. 168. 169. 105 
2015.12' 23 
Starting Nmap 6. 49 
BET 
https: //nmap. 
Nmap scan report for 192. 168. 169. 105 
Org 
a 
11: 55 ICS 
12C._ 
Host is up (0. 0012s latency) . 
Not shown: 998 openl filtered ports 
PORT 
STATE 
137/ udp open 
4500/ udp closed 
Nmap done: 1 
IP 
SERVICE 
netbios- ns 
nat- t- ike 
address (1 
host 
up) 
17. 
86 
seconds 
scanned in 

**完整：nmap -sUV ip地址**

计算机生成了可选文字:
rootMati: nmap -SLIV 42. 
Starting Nmap 6. 49 
BET 
2015- 12- 23 
11: 13 
121.252. sg 
https: //nmap. 
org 
at 
cs 

**U**=> UDP, **V**=>版本信息 (-sV UDP扫描中添加版本扫描信息)

不存在**-PN**参数（从UDP协议去理解，*你发了就ok管他收没收到*）

* + 重要 **Xmas扫描：**RFC文档描述了系统的技术细节，如果得到RFC文档，那么就可能找到系统的漏洞，xmas和null扫描的目的正是基于这一原因。***一般xmas针对unix或者linux系统比较有效***。

**常用：nmap -sX -Pn ip地址**

计算机生成了可选文字:
rootMati: nmap -sx - 
PN 192. 168. 232. 134 
Starting Nmap 6. 49 
BET 
https: //nmap. org 
2015- 12- 23 
at 
Nmap scan report for 192. 168. 232. 134 
Host is up (0. 00061s latency) . 
Not shown: 992 
filtered ports 
13:07 cs 
PORT 
Ill/tcp 
1025/ tcp 
1100/ tcp 
2004/ 
3283/ tcp 
5405/ tcp 
5900/ 
6839/ tcp 
STATE 
openl filtered 
openl filtered 
openl filtered 
openl filtered 
openl filtered 
openl filtered 
openl filtered 
openl filtered 
SERVICE 
rpcbind 
S- or- IIS 
mctp 
mailbox 
net assistant 
pcduo 
vnc 
unknown 
MAC Address: 00: CC: 29: 46: E9: EA (VMware) 
Nmap done: 1 
IP address (1 host u 
scanned in 997. 16 seconds 

**完整：nmap -sX -p- -Pn ip地址**

计算机生成了可选文字:
rootMati: nmap -sx -p- 
Starting Nmap 6. 49BETÅ4 
Éittp 
42. 121. 252. 58 
201512-23 IA: 

* + 重要 **Null 扫描**：和Xmas扫描相反,发送空数据包，打开端口不会返回相应信息关闭端口则返回一个RST数据包

**常用：nmap -sN -Pn ip地址**

计算机生成了可选文字:
rootMati: nmap - SN 
Starting Nmap 6. 49 
BET 
Stats: 0: 12: 44 elapsed; O 
192. 168. 232. 134 
https: //nmap. org ) 
at 
2015. 12-23 14: 36 cs 
hosts completed 
(1 
14: 
(1 
14: 
up) , 
undergoing NULL 
Scan 
52 
(O: 03: 37 remaining) 
up) , 
undergoing NULL 
Scan 
52 
O: 02: 30 remaining) 
NULL 
Scan Timing: About 77. 85% done; 
ETC: 
Stats: 0: 13: 57 elapsed; O hosts completed 
NULL 
Scan Timin 
About 84. 78% done• 
ETC: 
map scan report for 192. 168. 232. 134 
ost is up (O. 00064s latency) . 
ot shown: 994 
filtered ports 
Il/tcp 
13/ tcp 
43/ tcp 
54/ tcp 
81/tcp 
720/ tcp 
STATE 
SERVICE 
openl filtered rpcbind 
openl filtered ident 
openl filtered imap 
openl filtered rtsp 
openl filtered unknown 
openl filtered h323q931 
AC Address: 00: CC: 29: 46: E9: EA (VMware) 
ma done: 1 
IP address 1 host u 
scanned in 1011. 93 seconds 

**完整：nmap -sN -p- -Pn ip地址**

计算机生成了可选文字:
rootMati: nmap -SN -p- 
Starting Nmap 6. 49BETA4 ( 
2015- 12- 23 
• 49 cs 
PN 192. 168. 232. 134 
https: //nmap. org ) at 
14. 

* + **扩充：扫描的时候按d可以显示debug信息，按其他的键（比如X）可以显示当前进度 XX.XX%**

**Null扫描 和 Xmas扫描**

重要 如果系统遵循了TCP RFC文档，那么不用完成连接，在发起连接的时候namp就可以判断出目标系统的状态。(**PS：Xmas扫描和Null扫描都不会建立任何类型的通信通道。扫描目的就是为了判断哪些端口开或关**)

**扫描的其他指令**

-sV 参数用于版本扫描

-iL 批量扫描文件里面的ip

-F: 快速模式-扫描较少，扫描默认端口

-v 输出的时候更详细 (使用-vv 或更多的更大的作用)

-A 启用操作系统检测、 版本检测、 脚本扫描等

**-T** 速度设置（最慢0 - 最快5）**避免被检测到则降低速度，如果赶时间就提高速度**

* + **实战：（渗透中常用命令）**
  + 重要 **①快速扫描**

root@Kali:~# **nmap -T4 -F** 192.168.169.105

Starting Nmap 6.49BETA4 ( <https://nmap.org> ) at 2015-12-24 12:06 CST

Nmap scan report for 192.168.169.105

Host is up (1.7s latency).

Not shown: 92 closed ports

**PORT STATE SERVICE**

**80/tcp open http**

**135/tcp open msrpc**

**139/tcp open netbios-ssn**

**443/tcp open https**

**444/tcp open snpp**

**445/tcp open microsoft-ds**

**514/tcp filtered shell**

**1433/tcp open ms-sql-s**

Nmap done: 1 IP address (1 host up) scanned in 16.67 seconds

* + 重要 **②SYN迅速扫描：（TCP两次握手，隐蔽性高）**

root@Kali:~# **nmap -sS -T4 -A -v** cnblogs.com

Starting Nmap 6.49BETA4 ( <https://nmap.org> ) at 2015-12-23 17:00 CST

NSE: Loaded 122 scripts for scanning.

NSE: Script Pre-scanning.

Initiating NSE at 17:00

Completed NSE at 17:00, 0.00s elapsed

Initiating NSE at 17:00

Completed NSE at 17:00, 0.00s elapsed

Initiating Ping Scan at 17:00

Scanning cnblogs.com (42.121.252.58) [4 ports]

Completed Ping Scan at 17:00, 0.20s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 17:00

Completed Parallel DNS resolution of 1 host. at 17:00, 2.01s elapsed

**Initiating SYN Stealth Scan at 17:00**

**Scanning cnblogs.com (42.121.252.58) [1000 ports]**

**Discovered open port 443/tcp on 42.121.252.58**

**Discovered open port 80/tcp on 42.121.252.58**

Increasing send delay for 42.121.252.58 from 0 to 5 due to 11 out of 20 dropped probes since last increase.

Increasing send delay for 42.121.252.58 from 5 to 10 due to 11 out of 11 dropped probes since last increase.

Completed SYN Stealth Scan at 17:01, 84.92s elapsed (1000 total ports)

Initiating Service scan at 17:01

Scanning 2 services on cnblogs.com (42.121.252.58)

Completed Service scan at 17:01, 5.01s elapsed (2 services on 1 host)

Initiating OS detection (try #1) against cnblogs.com (42.121.252.58)

Retrying OS detection (try #2) against cnblogs.com (42.121.252.58)

WARNING: OS didn't match until try #2

Initiating Traceroute at 17:01

Completed Traceroute at 17:01, 0.02s elapsed

Initiating Parallel DNS resolution of 2 hosts. at 17:01

Completed Parallel DNS resolution of 2 hosts. at 17:01, 0.15s elapsed

NSE: Script scanning 42.121.252.58.

Initiating NSE at 17:01

Completed NSE at 17:02, 6.16s elapsed

Initiating NSE at 17:02

Completed NSE at 17:02, 0.00s elapsed

Nmap scan report for cnblogs.com (42.121.252.58)

Host is up (0.0048s latency).

Not shown: 998 filtered ports

PORT STATE SERVICE VERSION

**80/tcp open tcpwrapped**

|\_http-favicon: Unknown favicon MD5: CDD795C4B3E1ED39250A6B1B1DB89E73

|\_http-methods: No Allow or Public header in OPTIONS response (status code 301)

| http-title: \xE5\x8D\x9A\xE5\xAE\xA2\xE5\x9B\xAD - \xE5\xBC\x80\xE5\x8F\x91\xE8\x80\x85\xE7\x9A\x84\xE7\xBD\x91\xE4\xB8\x8A\xE5\xAE\xB6\xE5\x9B\xAD

|\_Requested resource was <http://www.cnblogs.com/>

**443/tcp open tcpwrapped**

| http-cisco-anyconnect:

|\_ ERROR: Not a Cisco ASA or unsupported version

|\_http-methods: No Allow or Public header in OPTIONS response (status code 400)

|\_http-title: 400 The plain HTTP request was sent to HTTPS port

| ssl-cert: Subject: commonName=\*.cnblogs.com

| Issuer: commonName=Go Daddy Secure Certificate Authority - G2/organizationName=GoDaddy.com, Inc./stateOrProvinceName=Arizona/countryName=US

| Public Key type: rsa

| Public Key bits: 2048

| Signature Algorithm: sha256WithRSAEncryption

| Not valid before: 2015-09-28T08:12:38

| Not valid after: 2016-07-27T12:31:38

| MD5: 9b12 efe2 1f0c 7967 ca7c fe14 2a13 a200

|\_SHA-1: 29dd 13c4 11cd e03b de35 cad9 60ac e7e6 52de 8c44

|\_ssl-date: TLS randomness does not represent time

| tls-nextprotoneg:

|\_ http/1.1

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: WAP|general purpose

**Running: Actiontec Linux, Linux 2.4.X|3.X**

**OS CPE: cpe:/o:actiontec:linux\_kernel cpe:/o:linux:linux\_kernel:2.4 cpe:/o:linux:linux\_kernel:3**

**OS details: Actiontec MI424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2**

Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)

HOP RTT ADDRESS

1 0.04 ms 192.168.232.2

2 0.04 ms 42.121.252.58

NSE: Script Post-scanning.

Initiating NSE at 17:02

Completed NSE at 17:02, 0.00s elapsed

Initiating NSE at 17:02

Completed NSE at 17:02, 0.00s elapsed

Read data files from: /usr/bin/../share/nmap

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 108.48 seconds

Raw packets sent: 3196 (145.286KB) | Rcvd: 195 (9.170KB)

* + 重要 **③UDP迅速扫描**

root@Kali:~# **nmap -sU -v** 192.168.169.105

Starting Nmap 6.49BETA4 ( <https://nmap.org> ) at 2015-12-23 19:20 CST

Initiating Ping Scan at 19:20

Scanning 192.168.169.105 [4 ports]

Completed Ping Scan at 19:20, 0.20s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 19:20

Completed Parallel DNS resolution of 1 host. at 19:20, 2.01s elapsed

**Initiating UDP Scan at 19:20**

**Scanning 192.168.169.105 [1000 ports]**

**Discovered open port 137/udp on 192.168.169.105**

Completed UDP Scan at 19:20, 23.11s elapsed (1000 total ports)

Nmap scan report for 192.168.169.105

Host is up (0.0013s latency).

Not shown: 998 open|filtered ports

**PORT STATE SERVICE**

**137/udp open netbios-ns**

**4500/udp closed nat-t-ike**

Read data files from: /usr/bin/../share/nmap

Nmap done: 1 IP address (1 host up) scanned in 25.39 seconds

Raw packets sent: 3006 (86.660KB) | Rcvd: 32 (1.654KB)

* + 重要 **④迅速扫描（NoPing）**

root@Kali:~# **nmap -T4 -A -v -Pn** 192.168.169.105

Starting Nmap 6.49BETA4 ( <https://nmap.org> ) at 2015-12-24 09:52 CST

NSE: Loaded 122 scripts for scanning.

NSE: Script Pre-scanning.

Initiating NSE at 09:52

Completed NSE at 09:52, 0.00s elapsed

Initiating NSE at 09:52

Completed NSE at 09:52, 0.00s elapsed

Initiating Parallel DNS resolution of 1 host. at 09:52

Completed Parallel DNS resolution of 1 host. at 09:52, 8.18s elapsed

Initiating SYN Stealth Scan at 09:52

Scanning 192.168.169.105 [1000 ports]

Discovered open port 80/tcp on 192.168.169.105

Increasing send delay for 192.168.169.105 from 0 to 5 due to 11 out of 15 dropped probes since last increase.

**Discovered open port 443/tcp on 192.168.169.105**

**Discovered open port 135/tcp on 192.168.169.105**

**Discovered open port 139/tcp on 192.168.169.105**

**Discovered open port 445/tcp on 192.168.169.105**

Increasing send delay for 192.168.169.105 from 5 to 10 due to max\_successful\_tryno increase to 5

Warning: 192.168.169.105 giving up on port because retransmission cap hit (6).

SYN Stealth Scan Timing: About 8.99% done; ETC: 09:58 (0:05:14 remaining)

SYN Stealth Scan Timing: About 14.66% done; ETC: 09:59 (0:05:55 remaining)

SYN Stealth Scan Timing: About 22.24% done; ETC: 09:59 (0:05:18 remaining)

SYN Stealth Scan Timing: About 29.91% done; ETC: 09:59 (0:04:43 remaining)

**Discovered open port 1433/tcp on 192.168.169.105**

SYN Stealth Scan Timing: About 37.97% done; ETC: 09:59 (0:04:07 remaining)

**Discovered open port 444/tcp on 192.168.169.105**

**Discovered open port 2383/tcp on 192.168.169.105**

SYN Stealth Scan Timing: About 54.17% done; ETC: 09:58 (0:02:33 remaining)

**Discovered open port 2179/tcp on 192.168.169.105**

SYN Stealth Scan Timing: About 76.10% done; ETC: 09:57 (0:01:06 remaining)

**Discovered open port 912/tcp on 192.168.169.105**

**Discovered open port 902/tcp on 192.168.169.105**

Completed SYN Stealth Scan at 09:57, 318.66s elapsed (1000 total ports)

Initiating Service scan at 09:57

Scanning 11 services on 192.168.169.105

Completed Service scan at 09:58, 33.60s elapsed (11 services on 1 host)

Initiating OS detection (try #1) against 192.168.169.105

Initiating Traceroute at 09:58

Completed Traceroute at 09:58, 1.01s elapsed

Initiating Parallel DNS resolution of 2 hosts. at 09:58

Completed Parallel DNS resolution of 2 hosts. at 09:58, 0.05s elapsed

NSE: Script scanning 192.168.169.105.

Initiating NSE at 09:58

Completed NSE at 09:58, 13.23s elapsed

Initiating NSE at 09:58

Completed NSE at 09:58, 0.00s elapsed

Nmap scan report for 192.168.169.105

Host is up (0.59s latency).

Not shown: 979 closed ports

**PORT STATE SERVICE VERSION**

**80/tcp open http Microsoft IIS httpd 10.0**

| http-methods: OPTIONS TRACE GET HEAD POST

| Potentially risky methods: TRACE

|\_See <http://nmap.org/nsedoc/scripts/http-methods.html>

|\_http-server-header: Microsoft-IIS/10.0

|\_http-title: IIS Windows

**135/tcp open msrpc Microsoft Windows RPC**

**139/tcp open netbios-ssn Microsoft Windows 98 netbios-ssn**

**443/tcp open ssl/http Apache httpd**

| http-auth:

| HTTP/1.1 401 Authorization Required

|\_ Basic realm=VisualSVN Server

| http-cisco-anyconnect:

|\_ ERROR: Not a Cisco ASA or unsupported version

|\_http-methods: No Allow or Public header in OPTIONS response (status code 401)

|\_http-server-header: Apache

|\_http-title: 401 Authorization Required

| ssl-cert: Subject: commonName=DESKTOP-PTACRF6

| Issuer: commonName=DESKTOP-PTACRF6

| Public Key type: rsa

| Public Key bits: 2048

| Signature Algorithm: sha256WithRSAEncryption

| Not valid before: 2015-12-06T14:04:50

| Not valid after: 2025-12-03T14:04:50

| MD5: c707 0eb2 71d6 5178 6687 9d2f 5594 dc01

|\_SHA-1: de83 b92f ad7d e0d0 125a 2f88 99d9 c741 6b51 bdcf

|\_ssl-date: TLS randomness does not represent time

**444/tcp open ssl/http VMware VirtualCenter Web service**

| http-cisco-anyconnect:

|\_ ERROR: Not a Cisco ASA or unsupported version

|\_http-methods: No Allow or Public header in OPTIONS response (status code 501)

|\_http-title: Site doesn't have a title (text; charset=plain).

| ssl-cert: Subject: commonName=VMware/countryName=US

| Issuer: commonName=VMware/countryName=US

| Public Key type: rsa

| Public Key bits: 2048

| Signature Algorithm: sha256WithRSAEncryption

| Not valid before: 2015-12-06T15:04:18

| Not valid after: 2016-12-05T15:04:18

| MD5: 6634 afe2 c934 e412 653c ee79 8fbe c64f

|\_SHA-1: da6f aaeb 31b4 51a8 73b6 403a 728d c0e5 a1e9 7c08

|\_ssl-date: TLS randomness does not represent time

**445/tcp open microsoft-ds (primary domain: WORKGROUP)**

**514/tcp filtered shell**

**902/tcp open ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)**

**912/tcp open vmware-auth VMware Authentication Daemon 1.0 (Uses VNC, SOAP)**

**1198/tcp filtered cajo-discovery**

**1433/tcp open ms-sql-s Microsoft SQL Server 2014 12.00.4100.00; SP1+**

**1641/tcp filtered invision**

**2179/tcp open vmrdp?**

**2383/tcp open ms-olap4?**

**2717/tcp filtered pn-requester**

**2998/tcp filtered iss-realsec**

**3814/tcp filtered neto-dcs**

**5950/tcp filtered unknown**

**9944/tcp filtered unknown**

**10003/tcp filtered documentum\_s**

**44176/tcp filtered unknown**

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at <https://nmap.org/cgi-bin/submit.cgi?new-service> :

SF-Port445-TCP:V=6.49BETA4%I=7%D=12/24%Time=567B5124%P=i586-pc-linux-gnu%r

SF:(SMBProgNeg,85,"\0\0\0\x81\xffSMBr\0\0\0\0\x88\x01@\0\0\0\0\0\0\0\0\0\0

SF:\0\0\0\0@\x06\0\0\x01\0\x11\x07\0\x032\0\x01\0\x04\x11\0\0\0\0\x01\0\0\

SF:0\0\0\xfc\xe3\x01\0\xad\xb4\x16\x7f\xee=\xd1\x01\x20\xfe\x08<\0B2\xe4\^

SF:\xe0\xab\x91PW\0O\0R\0K\0G\0R\0O\0U\0P\0\0\0D\0E\0S\0K\0T\0O\0P\0-\0P\0

SF:T\0A\0C\0R\0F\x006\0\0\0");

**Device type: general purpose**

**Running: Microsoft Windows 7|2012|XP**

**OS CPE: cpe:/o:microsoft:windows\_7 cpe:/o:microsoft:windows\_server\_2012 cpe:/o:microsoft:windows\_xp::sp3**

**OS details: Microsoft Windows 7 or Windows Server 2012, Microsoft Windows XP SP3**

Network Distance: 2 hops

TCP Sequence Prediction: Difficulty=258 (Good luck!)

IP ID Sequence Generation: Incremental

Service Info: Host: DESKTOP-PTACRF6; OSs: Windows, Windows 98; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows\_98

Host script results:

| ms-sql-info:

| 192.168.169.105:1433:

| Version:

| Service pack level: SP1

| Post-SP patches applied: true

| name: Microsoft SQL Server 2014 SP1+

| number: 12.00.4100.00

|  **Product: Microsoft SQL Server 2014**

**|\_ TCP port: 1433**

| nbstat: NetBIOS name: DESKTOP-PTACRF6, NetBIOS user: <unknown>, NetBIOS MAC: ac:b5:7d:18:93:b9 (Liteon Technology)

| Names:

| DESKTOP-PTACRF6<00> Flags: <unique><active>

| WORKGROUP<00> Flags: <group><active>

|\_ DESKTOP-PTACRF6<20> Flags: <unique><active>

| smb-security-mode:

| authentication\_level: user

| challenge\_response: supported

|\_ message\_signing: disabled (dangerous, but default)

|\_smbv2-enabled: Server supports SMBv2 protocol

TRACEROUTE (using port 587/tcp)

HOP RTT ADDRESS

1 0.37 ms 192.168.232.2

2 1000.57 ms 192.168.169.105

NSE: Script Post-scanning.

Initiating NSE at 09:58

Completed NSE at 09:58, 0.00s elapsed

Initiating NSE at 09:58

Completed NSE at 09:58, 0.00s elapsed

Read data files from: /usr/bin/../share/nmap

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 382.58 seconds

Raw packets sent: 3582 (159.270KB) | Rcvd: 3259 (130.738KB)

* + 重要 **⑤快速扫描加强**

root@Kali:~# **nmap -sV -T4 -O -F --version-light** 192.168.169.105

Starting Nmap 6.49BETA4 ( <https://nmap.org> ) at 2015-12-24 12:10 CST

Nmap scan report for 192.168.169.105

Host is up (0.31s latency).

Not shown: 92 closed ports

**PORT STATE SERVICE VERSION**

**80/tcp open http Microsoft IIS httpd 10.0**

**135/tcp open msrpc Microsoft Windows RPC**

**139/tcp open netbios-ssn Microsoft Windows 98 netbios-ssn**

**443/tcp open ssl/http Apache httpd**

**444/tcp open ssl/http VMware VirtualCenter Web service**

**445/tcp open microsoft-ds (primary domain: WORKGROUP)**

**514/tcp filtered shell**

**1433/tcp open ms-sql-s Microsoft SQL Server 2014**

Device type: general purpose

**Running: Microsoft Windows 7|2012|XP**

**OS CPE: cpe:/o:microsoft:windows\_7 cpe:/o:microsoft:windows\_server\_2012 cpe:/o:microsoft:windows\_xp::sp3**

**OS details: Microsoft Windows 7 or Windows Server 2012, Microsoft Windows XP SP3**

Service Info: Host: DESKTOP-PTACRF6; OSs: Windows, Windows 98; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows\_98

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 47.93 seconds

* + 重要 **⑥SYN全端口扫描**

**[有些管理员端口不按常理来全端口扫才能发现好东西]**

root@Kali:~# **nmap -sS -p- -T4 -A -v** 192.168.169.105

Starting Nmap 6.49BETA4 ( <https://nmap.org> ) at 2015-12-24 09:07 CST

NSE: Loaded 122 scripts for scanning.

NSE: Script Pre-scanning.

Initiating NSE at 09:07

Completed NSE at 09:07, 0.00s elapsed

Initiating NSE at 09:07

Completed NSE at 09:07, 0.00s elapsed

Initiating Ping Scan at 09:07

Scanning 192.168.169.105 [4 ports]

Completed Ping Scan at 09:07, 0.20s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 09:07

Completed Parallel DNS resolution of 1 host. at 09:07, 0.06s elapsed

**Initiating SYN Stealth Scan at 09:07**

**Scanning 192.168.169.105 [65535 ports]**

**Discovered open port 135/tcp on 192.168.169.105**

**Discovered open port 443/tcp on 192.168.169.105**

**Discovered open port 80/tcp on 192.168.169.105**

**Discovered open port 445/tcp on 192.168.169.105**

**Discovered open port 139/tcp on 192.168.169.105**

Increasing send delay for 192.168.169.105 from 0 to 5 due to 45 out of 112 dropped probes since last increase.

Increasing send delay for 192.168.169.105 from 5 to 10 due to 397 out of 991 dropped probes since last increase.

SYN Stealth Scan Timing: About 5.11% done; ETC: 09:18 (0:09:35 remaining)

Warning: 192.168.169.105 giving up on port because retransmission cap hit (6).

SYN Stealth Scan Timing: About 8.41% done; ETC: 09:43 (0:32:52 remaining)

SYN Stealth Scan Timing: About 8.89% done; ETC: 09:47 (0:36:03 remaining)

**Discovered open port 1549/tcp on 192.168.169.105**

SYN Stealth Scan Timing: About 14.17% done; ETC: 10:19 (1:01:18 remaining)

SYN Stealth Scan Timing: About 14.89% done; ETC: 10:24 (1:04:57 remaining)

SYN Stealth Scan Timing: About 15.50% done; ETC: 10:29 (1:08:46 remaining)

**Discovered open port 1539/tcp on 192.168.169.105**

SYN Stealth Scan Timing: About 16.79% done; ETC: 10:35 (1:12:56 remaining)

SYN Stealth Scan Timing: About 17.95% done; ETC: 10:42 (1:17:19 remaining)

SYN Stealth Scan Timing: About 19.25% done; ETC: 10:49 (1:22:05 remaining)

SYN Stealth Scan Timing: About 20.88% done; ETC: 10:58 (1:27:13 remaining)

**Discovered open port 1553/tcp on 192.168.169.105**

SYN Stealth Scan Timing: About 22.52% done; ETC: 11:07 (1:32:45 remaining)

SYN Stealth Scan Timing: About 23.78% done; ETC: 11:17 (1:38:46 remaining)

Stats: 0:36:36 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan

SYN Stealth Scan Timing: About 26.11% done; ETC: 11:28 (1:43:32 remaining)

Stats: 0:36:39 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan

SYN Stealth Scan Timing: About 26.12% done; ETC: 11:28 (1:43:36 remaining)

**………………………………….比较耗时，就不详细输出了…………………………………**

* + 重要 **⑦大绝招：全面扫描**

**nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe)"** 192.168.169.105

Starting Nmap 6.49BETA4 ( <https://nmap.org> ) at 2015-12-24 12:28 CST

NSE: Loaded 243 scripts for scanning.

NSE: Script Pre-scanning.

Initiating NSE at 12:28

NSE: [mtrace] A source IP must be provided through fromip argument.

Completed NSE at 12:28, 10.50s elapsed

Initiating NSE at 12:28

Completed NSE at 12:28, 0.00s elapsed

Pre-scan script results:

| broadcast-eigrp-discovery:

|\_ ERROR: Couldn't get an A.S value.

| broadcast-igmp-discovery:

| 192.168.232.1

| Interface: eth0

| Version: 2

| Group: 224.0.0.251

| Description: mDNS

| 192.168.232.1

| Interface: eth0

| Version: 2

| Group: 224.0.0.252

| Description: Link-local Multicast Name Resolution (rfc4795)

| 192.168.232.1

| Interface: eth0

| Version: 2

| Group: 239.255.255.250

| Description: Organization-Local Scope (rfc2365)

|\_ Use the newtargets script-arg to add the results as targets

| broadcast-ping:

| IP: 192.168.232.2 MAC: 00:50:56:f5:1a:80

|\_ Use --script-args=newtargets to add the results as targets

| http-icloud-findmyiphone:

|\_ ERROR: No username or password was supplied

| http-icloud-sendmsg:

|\_ ERROR: No username or password was supplied

| targets-asn:

|\_ targets-asn.asn is a mandatory parameter

Initiating Ping Scan at 12:28

Scanning 192.168.169.105 [7 ports]

Completed Ping Scan at 12:28, 0.20s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 12:28

Completed Parallel DNS resolution of 1 host. at 12:28, 0.04s elapsed

Initiating SYN Stealth Scan at 12:28

Scanning 192.168.169.105 [1000 ports]

**………………………………….比较耗时，就不详细输出了…………………………………**