PortScan について

Eiji James Yoshida
zaddik@geocities.co.jp

penetration technique research site
http://www.geocities.co.jp/SiliconValley/1667/index.htm

June 30, 2000

1.0 Introduction

近年、不正侵入者によるホームページの書き換えが多発していますが、その前兆として異常としか思えない接続要求がログに記録されている時があります。
この不正侵入される前兆の異常な接続要求を侵入者がどのように行い、どのように利用してくるかを解説します。

1.1 PortScan とは何か？

PortScanとは複数のネットワークサービスポートに接続を試みることで、開いているポートを探すというものです。この開いているポートに接続して正規接続と同じ方法で情報収集を行うことや、接続後に異常な情報を流すことでサービスを混乱させることが出来ます。
また接続要求に対する返事の違いからフィルタの設定を調べることや、OSを推測することも出来るようになっています。
このようにPortScanから侵入者は多数の情報を集めることが出来ますので、不正侵入を行う際の事前調査や侵入方法を考える為に使われる場合が多いのです。
このPortScanを行うツールは多数ありますが、その中でも非常に実用的なPortScannerであるNMAPの仕組みを解説します。

1.2 NMAP(概要)

NMAPとはThe Network Mapperの略称であり http://www.insecure.org/nmap/ で取得できます。
フリーソフトウェアとして配布されており、多種のPortScanが行えるので実用的なPortScannerとして多くの技術者に愛用されています。
2000年1月現在の Nmap 2.3BETA14 は10種類のPortScanが可能であり、OPTIONを設定することで各種のScanを調整することが出来ます。

使い方 : nmap [PortScan の種類] [OPTION の種類] < host もしくは net list >

1.3 NMAP(PortScan の仕組み)

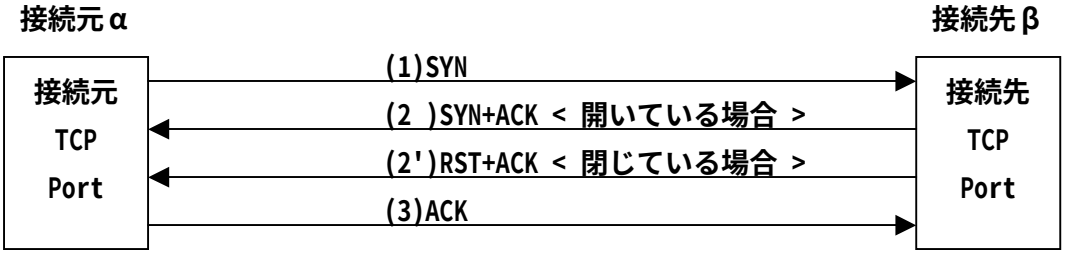
Nmap 2.3BETA14 は10種類のPortScanが可能ですが、大きく区分けすると次の２つが根本的な機能です。

・TCP PortScan(開いているTCP Portを捜査します)
・UDP PortScan(開いているUDP Portを捜査します)

この２つの機能はTCP PortやUDP Portに通常の接続を試みることで探すことが出来ます。
この通常接続の手順は次の通りです。

1.3.1 TCP Portへの接続(3Way HandShake)

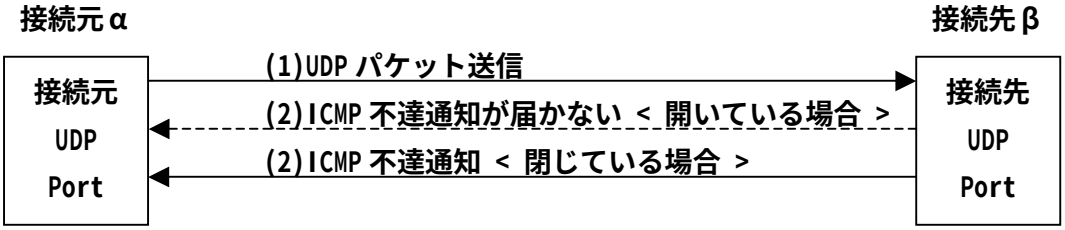
TCP Port への接続は次の手順で行われます。



(1)SYN: α→β への接続要求
(2)SYN+ACK: α→β の接続許可 ＋ α←β の接続要求
(2')RST: α→β の接続拒否
(3)ACK: α←β の接続許可(3Way HandShake完了)
処理(3)が終了することで接続完了となります。

1.3.2 UDP Port への接続

UDP Port への接続は次の手順で行われます。



※UDPパケットが届かない場合はICMP不達通知が返信されますがパケットロストも考えられるので、ICMP不達通知が届かない場合をUDPパケットが接続先に届いたと思わないでください。この場合、UDPパケットが接続先に届いた可能性があると推測できます。

1.4 NMAP(PortScan の種類)

通常接続によるPortScan以外にもNMAPは様々な接続要求を利用したPortScanが可能です。このNMAPの各種PortScanやOPTIONを使いながら、様々なPortScanの仕組みを解説します。

使用する PortScanner: Nmap 2.3BETA14

1.4.1 ディフォルトの設定

nmap < IP or NAME > ⇒ nmap -sT < IP or NAME>
host up check:あり(ICMP Echo + ACK Scan< Port 80 >)

NMAPのディフォルト設定は、対象ホストが起動しているかどうかをICMP EchoとACK SCAN(対象Port.80)を行うことで調べます。起動していればEcho replyかRSTが返ってくるので、その後に3Way HandShakeによるScanを行います。

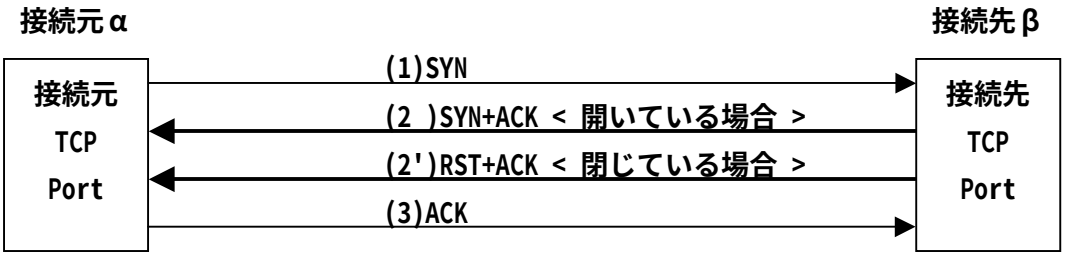
1.4.2 PortScan の種類

-sT : TCP connect() scan
-sS : TCP SYN scan

-sF : Stealth FIN scan
-sX : Stealth Xmas scan
-sN : Stealth Null scan
-sP : Ping scanning
-sU : UDP scans
-sR : RPC scan
-sW : ACK scan
-b <ftp relay host> : FTP bounce attack
--interactive : インタラクティブモード

1.4.3 -sT:TCP connect() scan

3Way HandShakeが完了するかどうかで対象ポートの開閉を調べます。接続できることでOPENと判断するので、このスキャンは非常に簡単にログを採取できます。



(3)の処理が完了で OPEN と判断します。

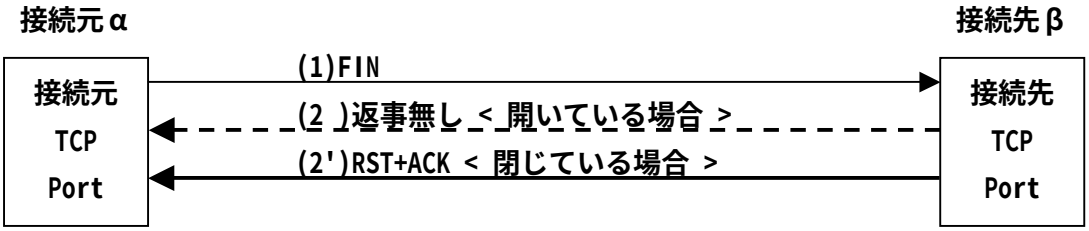
1.4.4 -sS:TCP SYN scan

SYN scan と呼ばれる方法で、half-open scan とも呼びます。この方法は接続を確立するのではなく、3Way HandShake の SYN に対する返事で対象 Port の開閉を調べます。接続は行わないので、接続のログには残りません。

(2)の返事は OPEN、(2')の返事は CLOSE と判断します。

1.4.5 -sF:Stealth FIN scan

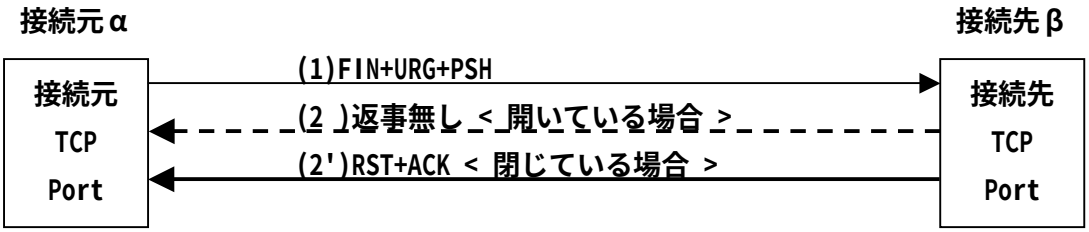
FIN scanとはTCPのBSDのネットコードバグを利用したPortScanです。元々FINフラグとはTCPの接続を終了させるのに使いますが、これを接続要求として使い返事の違いで対象Portの開閉を調べます。



返事が無い場合はOPEN、(2')の返事はCLOSEとなります。
※バグを利用するため、FIN scan は成功しない場合があります。

1.4.6 -sX:Stealth Xmas Tree scan

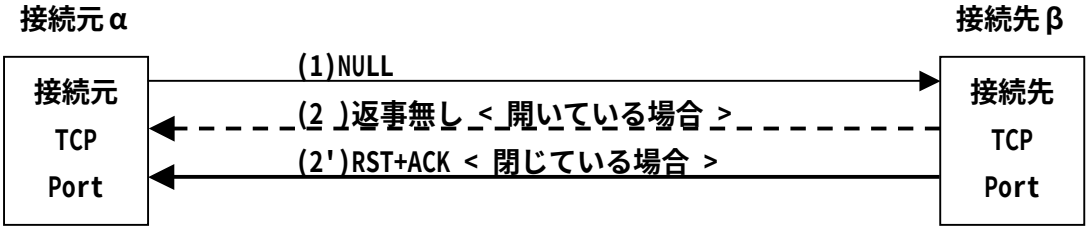
TCP のフラグを全てセットしたパケットを使い、返事の違いで対象 Port の開閉を調べます。NMAP は FIN+URG+PSH をセットしたパケットを使っています。



返事が無い場合はOPEN、(2')の返事はCLOSEとなります。
※OS によっては、Xmas scan は成功しない場合があります。

1.4.7 -sN:Stealth Null scan

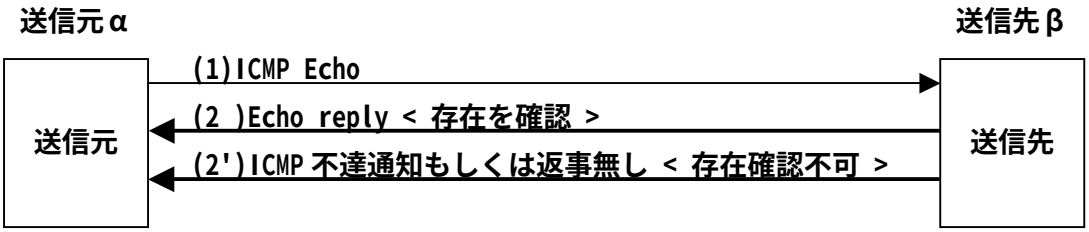
TCP の全てのフラグを降ろしたパケットを使い、対象ポートの開閉を調べます。TCP のフラグに対するフィルタを設定している場合は、このスキャンは検知されずに PortScan ができる可能性があります。



返事が無い場合はOPEN、(2 ’)の返事はCLOSEとなります。
※OS によっては、Null scan は成功しない場合があります。

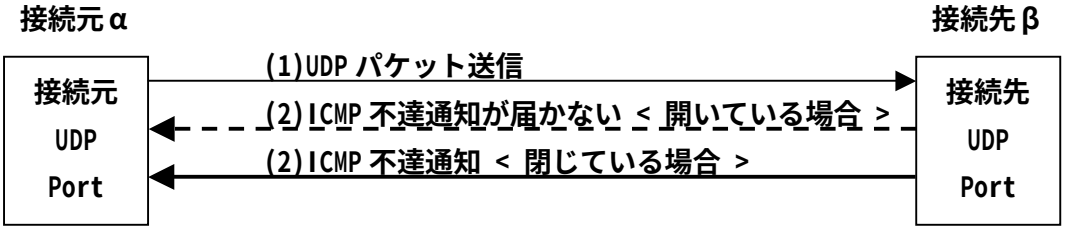
1.4.8 -sP:Ping scanning

広域なネットワークにPortScanをかけるときに、ホストの存在しないIPアドレスまでPortScanを行うと莫大な時間が必要となるので、このScanでホストの存在するIPアドレスを調べます。存在確認の方法はICMP Echo(Ping)によるものです。



1.4.9 -sU:UDP scans

UDP パケットを使い、返事の違いで対象 UDP Port の開閉を推測します。この Scan はコネクションレス型である UDP を使用するので、あくまでも PortScan の結果は推測でしかないことに注意してください。



※UDPパケットが届かない場合はICMP不達通知が返信されますがパケットロストも考えられるので、ICMP不達通知が届かない場合をUDPパケットが届いたと思わないでください。

1.4.10 -sR:RPC scan

このScanを選択するとPortScanを行い、開いているポート番号にRPC(リモート・プロシージャ・コール)サービスの番号が存在する場合は、RPCサービスからプログラム名とヴァージョン番号を取得します。

"rpcinfo"でも同じ結果を得ることが出来ます。

rpcinfo [-n portnum] -u host prognum [versnum]

rpcinfo [-n portnum] -t host prognum [versnum]

-n:ポート番号

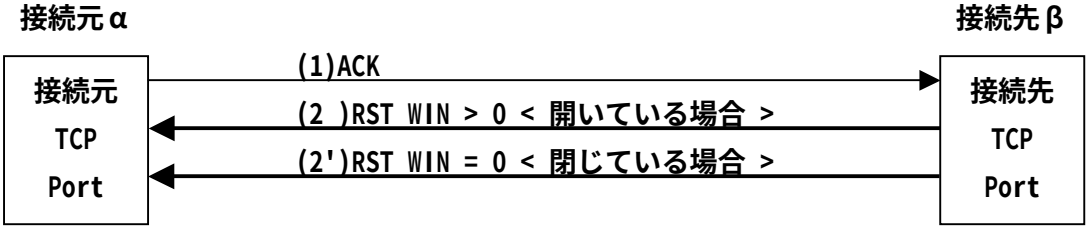
-t or -u:TCPかUDPを選択

prognum:ここで/etc/rpcに定義されている番号を使い総当たりします。

(例)rpcinfo -n 635 -t 192.168.0.45 100005

1.4.11 -sW:Stealth ACK scan

ACK scanとはACKフラグをセットしたパケットを使い、返事の違いで対象ポートの開閉を調べます。NMAPはhost up checkにこのScanを利用しています。



RSTパケットのWindowサイズが0ではない場合はOPEN、Windowサイズが0の場合はCLOSEになります。

※OS によっては、Window サイズが全て 0 にもなるので成功しない場合があります。

1.4.12 -b <ftp relay host>:FTP bounce attack

この Scan は古い FTP サーバへ PORT コマンドを使用し、任意のポートに FTP-DATA 転送用接続を試みることで PortScan を行います。

FTP bounce attackはFTPコマンドを使うことにより、手動で行うことが出来ます。

Scan対象サーバ：192.168.0.1

Scan対象ポート：2049

bounceサーバ：192.168.0.2

まず、telnetコマンドを使いFTPポート(21)に接続します。

telnet 192.168.0.2 21

次にログオンを行います。

user anonymous

pass hoge@hoge

ログオンが成功したのを確認して、PORTコマンドを入力します。

PORT 192,168,0,1,8,1

※後2つのフィールドは次の方法で導き出されます。(各フィールドは数値のみです。)

2049÷256=8余り1

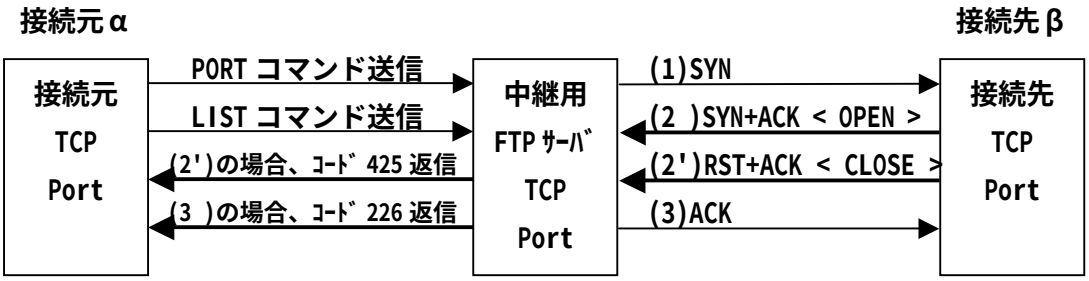
コマンド成功コード200が表示されるのを確認してLISTコマンドを入力します。

LIST

LIST入力後に表示されるコード番号から、対象ポートの開閉がわかります。

対象ポートが開いている場合：226 Transfer complete.

対象ポートが閉じている場合：425 Can't build data connection: Connection refused.



1.5 NMAP(OPTION の種類)

1.5.1 OPTION の種類

-PO : host up check (ICMP Echo + ACK scan)を使用しない。
-PT : host up check の ICMP Echo を停止。ACK scan 対象ポートを指定。
-PS : host up check の ICMP Echo を停止。ACK scan をSYN scanに変更。
-PI : host up check の ACK scanを停止。
-PB : host up check (ICMP Echo + ACK scan)を使用。
-O : OS推測Scan。
-I : identを利用したサービス起動権限情報の収集。
-F : nmap-servicesに記述されたポート番号のみのScan。
-v : Scan中の情報を詳細表示。
-h : クイックリファレンス(ヘルプ)を表示。
-oN : 通常ログ出力。
-oM : マシン分析用ログ出力。
-oS : s|<ipTkiDd|3 fOrM に変換してログ出力。
-iL : ファイルによるScanの自動化。
-iR : ScanするホストのIPアドレスをランダムに生成。
-p <port ranges> : Scanするポートの範囲や番号を指定。
-f : 断片化したパケットを使用。
-D<decoy1[,decoy2][,ME],...> : 複数のおとりIPアドレスを使用。
-S <Source_IP> : 送信元IPアドレスの変更。
-e <interface> : ネットワークインターフェースの変更。
-g <Source_PORT> : 送信元ポートの変更。
-r : Scan するポートの順番を連番に変更。
--randomize_hosts : ScanするIPアドレスの順番をランダムに変更。
-M <max sockets> : 使用するソケットの数を設定。
-T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> : Scanの間隔変更。
--host_timeout <milliseconds> : 各IPアドレスに費やすScanの時間を設定。
--max_rtt_timeout <milliseconds> : 返事待ちの時間設定。(最長)
--min_rtt_timeout <milliseconds> : 返事待ちの時間設定。(最短)
--initial_rtt_timeout <milliseconds> : 返事待ちの時間設定。(初期値)

--max_parallelism <number> : 同時に行うScanの数を指定。
--scan_delay <milliseconds> : Scanの間隔を指定。
-n/-R : DNSの名前解決を停止。 / DNSの名前解決を使用。
-d : デバッグモードを使用。

1.5.2 -P<0,T,S,I,B>:host up check

この設定は、指定されたネットワークに効率良く高速に PortScan を行うためのものです。ICMP Echo に反応するホストに対して Scan を行うか、特定のポートに特定のパケットを送信して反応するホストに Scan を行うかを設定できます。

・host up check停止。
nmap -P0 host
・ICMP Echoを停止してACK Scanのポートを25番に設定。
nmap -PT25 host
・ICMP Echoを停止してSYN Scanのポートを25番に設定。
nmap -PS25 host
※P0 は Pzero なので注意してください。

1.5.3 -O:OS 推測 Scan

この設定は、使用される初期シーケンス番号の特徴や多種のパケットを送信した際の返信パケット種類とフラグの設定、windows サイズなどの情報を収集し OS を推測します。これは各 OS ごとに TCP/IP の実装が異なっている点を利用したものです。

TSeq(初期シーケンス番号テスト)
T1(OpenPortにSYNパケットを送った場合の返信内容テスト)
T2(OpenPortにNULLパケットを送った場合の返信内容テスト)
T3(OpenPortにSYN|FIN|URG|PSHパケットを送った場合の返信内容テスト)
T4(OpenPortにACKパケットを送った場合の返信内容テスト)
T5(ClosePortにSYNパケットを送った場合の返信内容テスト)
T6(ClosePortにACKパケットを送った場合の返信内容テスト)
T7(ClosePortにFIN|URG|PSHパケットを送った場合の返信内容テスト)
PU(UDPを利用した'port unreachable'messageテスト)

・TSeq(初期シーケンス番号テスト)

ISN(初期シーケンス番号)を収集し、番号生成の特徴を調べます。番号生成の種類は以下の通りです。

・constant sequence number(初期シーケンス番号が一定):旧式のUNIXなど

・trivial time dependency(初期シーケンス番号生成に時間が関係):Windowsなど

・random positive increments(初期シーケンス番号に乱数を含む):Solaris、IRIX、FreeBSDなど

・truly random(初期シーケンス番号が完全に乱数):Linux 2.0.*、OpenVMS、AIXなど

・T1〜T4(OpenPortに各種パケットを送った場合の返信内容テスト)

OpenPortに各種パケットを送った場合のレスポンスの有無とDon't fragmentフラグの有無、windowサイズ、ACKシーケンス番号、TCPフラグ、TCPオプションフラグを調べます。

・T5〜T7(ClosePortに各種パケットを送った場合の返信内容テスト)

ClosePortに各種パケットを送った場合のレスポンスの有無とDon't fragmentフラグの有無、windowサイズ、ACKシーケンス番号、TCPフラグ、TCPオプションフラグを調べます。

・PU(UDPを利用したICMP'port unreachable'messageテスト)

ClosePortにUDP Scanを行い、レスポンスの有無とDon't fragmentフラグの有無、TypeOfService、IPTotalLength、ICMPTotalLength、UDPパケットのコピーが正しいかのチェック、IPchecksumが正しいかのチェック、ICMPchecksumが正しいのかのチェック、UDPLengthの大きさが正しいかのチェックを行います。

1.5.4 -I:ident を利用したサービス起動権限情報収集

この設定は、113番ポート(auth)を利用して各サービスの起動権限情報を収集することが可能です。この情報からサービスを利用して悪意のあるコードを実行した場合の権限を推測することができます。

IdentScanを手動で行う方法は以下の通りです。

Scan対象IP:192.168.0.1

Scan対象Port:25

まずScan対象IPの対象Portに接続します。例ではNetCatを使用します。

nc -p 12321 192.168.0.1 25

上記コマンドは発信元Port:12321からScan対象IP:192.168.0.1の対象Port:25に対して接続します。

次に、Scan対象IP:192.168.0.1のPort:113(auth)に接続して、以下のコマンドを入力します。

25,12321

実行後の結果は以下のものです。

25 , 12321 : USERID : OTHER :root

この結果からPort:25**を使用しているサービスの起動権限は**root**である事が推測できます。**

この手法は netstat **と** telnet **で行うことも可能です。**

1.5.5 -F:nmap-services に記述されたポート番号のみの Scan

この設定をした場合は、nmap-services に記述されている well known ポートに対して Scan を行います。一般的に知られているポートのみを調査する際に設定することで、Scan を効率的に行うことができます。

1.5.6 -v:Scan 中の情報を詳細表示

この設定は Scan の進行状況を表示するものです。表示内容としては host up check の結果、PortScan の種類、Scan したポートの状況、Scan にかかった時間と Scan したポートの総数などです。選択した PortScan の種類や OPTION によって表示が異なります。

※小文字の v なので、大文字と間違えないようにしてください。

1.5.7 -h:クイックリファレンス(ヘルプ)を表示

この設定は簡易的な使用説明を表示します。詳細な使用説明については man nmap になります。

1.5.8 -V:ヴァージョン情報を表示

現在使用している NMAP のヴァージョン情報を表示します。

1.5.9 -oN:通常ログ出力

この設定は PortScan の結果をログ出力します。このログには Scan した日時と、使用した PortScan の種類や OPTION の種類が記録されます。

```
# Nmap (V. 2.3BETA14) scan initiated Wed Mar 22 10:43:31 2000 as: nmap -oN normal.log 192.168.0.48
Interesting ports on  (192.168.0.48):
Port    State       Protocol  Service
135     open        tcp       loc-srv
139     open        tcp       netbios-ssn

# Nmap run completed at Wed Mar 22 10:43:32 2000 -- 1 IP address (1 host up) scanned in 1 second
```

1.5.10 -oM:マシン分析用ログ出力

この設定は PortScan の結果をマシン分析用ログとして出力します。この設定によって出力されたログは他の SecurityScanner(whisker など)と連係を取るために使われます。

```
# Nmap (V. 2.3BETA14) scan initiated Wed Mar 22 10:52:51 2000 as: nmap -oM MP.log 192.168.0.48
Host: 192.168.0.48 ()   Ports: 135/open/tcp//loc-srv///, 139/open/tcp//netbios-ssn///
# Nmap run completed at Wed Mar 22 10:52:52 2000 -- 1 IP address (1 host up) scanned in 1 second
```

1.5.11 -oS:s|<ipTkiDd|3 fOrM に変換してログ出力

この設定は PortScan の結果を skript kiddie 形式でログ出力します。

```
$taRt|ng nmAp v. 2.383T414 6y fyOdor@|n$3cur3.ORg ( wwW.ins3cUr3.Org/nmaP/ )
IntErest|ng pOrtz On  (192.168.0.48):
POrt    $tat3       PrOtOcoL  Serv!c3
135     Op3n        tCp       lOc-SRv
139     Op3n        tcp       n3tbIOz-$sn
```

```
Nmap rUn compl3t3d -- 1 ip AddrE$s (1 ho$t up) $canned 1n 1 $3c0nd
```

1.5.12 -iL:ファイルによる Scan の自動化

この設定は Scan 対象の名前や IP アドレスを記入したリストを使用することで、PortScan を自動化します。

```
# more hostlist
192.168.0.110
192.168.0.48

# nmap -sS -iL hostlist
Reading target specifications from FILE: hostlist

Starting nmap V. 2.3BETA14 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Interesting ports on  (192.168.0.110):
Port    State       Protocol  Service
21      open        tcp       ftp
70      open        tcp       gopher
80      open        tcp       http
135     open        tcp       loc-srv
139     open        tcp       netbios-ssn
1031    open        tcp       iad2

Interesting ports on  (192.168.0.48):
Port    State       Protocol  Service
135     open        tcp       loc-srv
139     open        tcp       netbios-ssn

Nmap run completed -- 2 IP addresses (2 hosts up) scanned in 1 second
```

1.5.13 -iR:Scan するホストの IP アドレスをランダムに生成

この設定は無作為に選んだ IP アドレスに対して PortScan を行います。無作為に選ぶので使用時には十分注意してください。

1.5.14 -p <port ranges>:Scan するポートの範囲や番号を指定

この設定は Scan するポートの番号や範囲を指定できます。広域なネットワークで指定されたポートの開閉を調べるのに有効です。範囲は 1 から 65535 までの値です。

- 192.168.0.0/24 で 80 番ポートの開閉を調べる場合

```
nmap 192.168.0.0/24 -p 80
```

- 192.168.0.0/24 で 135 番と 139 番のポート開閉を調べる場合

```
nmap 192.168.0.0/24 -p 135,139
```

- 192.168.0.0/24 で 1 番から 100 番までのポートの開閉を調べる場合

```
nmap 192.168.0.0/24 -p 1-100
```

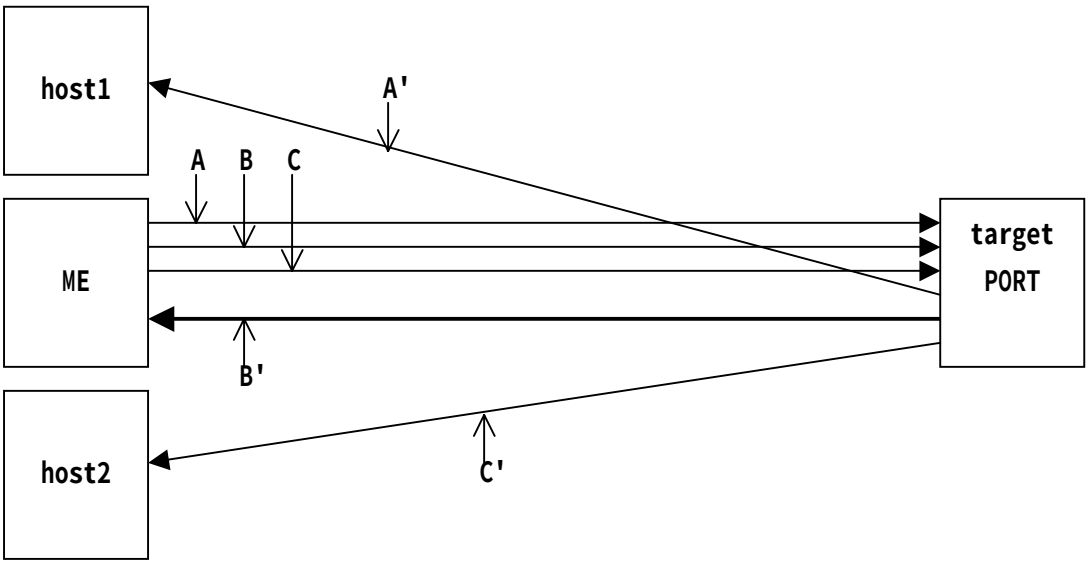
1.5.15 -f:断片化したパケットを使用

この設定は PortScan に使用するパケットをフラグメント(断片化)することで、フィルタの回避を試みます。フラグメントパケットは中継するルータでは再構築をしないで終点で再構築するのが一般的なので、ルータのフィルタを回避できる可能性があります。また、パケットの再構築が困難な旧式の侵入検知システムやファイアウォールに検知されずに、PortScan を行える可能性があります。

1.5.16 -D<decoy1[,decoy2][,ME],...>:複数のおとり IP を使用

この設定は自分の接続元 IP アドレスを複数の偽装した IP アドレス(おとり)に混ぜることで、接続元の特定を困難にするものです。おとりの IP アドレスの間に ME を指定しない場合は、無作為に自分の IP アドレスが挿入されます。

nmap -sS -Dhost1,ME,host2 target



A:発信元アドレス=host1、発信先アドレス=target
B:発信元アドレス=ME、発信先アドレス=target
C:発信元アドレス=host2、発信先アドレス=target
A':返信元アドレス=target、返信先アドレス=host1
B':返信元アドレス=target、返信先アドレス=ME
C':返信元アドレス=target、返信先アドレス=host2

※FTP bounce attack と TCP connect() scan には使用できません。

1.5.17 -S <Source_IP>:送信元 IP の変更

この設定は接続元 IP アドレスの偽装を行います。用途としては Scan 対象である企業に対して、敵対企業の IP アドレスを装って PortScan を行うことで争いの誘発を試みます。また、この設定を使用中は promiscuous mode(無差別受信)になるので、偽装した IP アドレスに帰ってきた返事を受信できれば結果が表示されます。

・接続元アドレスを 192.168.0.1 に偽装して、192.168.0.100 に Scan を行う場合

nmap -sS -P0 -e eth0 -S 192.168.0.1 192.168.0.100

※偽装を行う場合は host up check の停止と、使用するインターフェースの指定が必要です。

1.5.18 -e <interface>:ネットワークインターフェースの変更

この設定はパケットを送受信するインターフェースを選択します。複数のインターフェースがある場合や、送信元 IP アドレスを偽装する際に使用します。

1.5.19 -g <Source_PORT>:送信元ポートの変更

この設定は PortScan に使用する接続元ポートの変更を行います。ファイアウォールの内側から外側に対して、FTP や DNS を利用する際に行うフィルタの設定に誤りがある場合に有効です。

ファイアウォールの内側にあるクライアントから FTP を使用する場合、パッシブ・モードが選択されていないと、外側の FTP サーバの接続元 TCP ポート 20 番から FTP のデータ転送用の接続要求が送られます。この接続要求がファイアウォールの内側にあるクライアントに届かないとデータ転送用接続が確立できないので、正常な FTP の接続が出来ません。このような問題に対処するために、管理者は外側からの接続元 TCP ポート 20 番から送られてきた接続要求に、内側に入ることを許可するといった設定をしているかもしれません。

この場合、下のような設定をした NMAP で PortScan を行うと効果的です。

```
nmap -g 20 < HostName or IPaddress >
```

この設定で PortScan を行うと、全ての接続要求は接続元 TCP ポート 20 番から発信されるので、ファイアウォールはデータ転送用接続と誤認して PortScan の内側への透過を許可してしまいます。

同様に、ファイアウォールの内側にあるクライアントが DNS 名を IP アドレスに変換する場合、外側の DNS サーバに DNS-Query という UDP パケットを発信しています。この DNS-QUERY の返事として外側の DNS サーバは、接続元 UDP ポート番号 53 番から DNS-Response を内側のクライアントに返します。この DNS-Response が内側のクライアントに届かないと IP アドレスの変換に失敗します。このような問題に対処するために、管理者は外側から送られてきた接続元 UDP ポート 53 番のパケットに、内側に入ることを許可するといった設定をしているかもしれません。

この場合、下のような設定をした NMAP で PortScan を行うと効果的です。

```
nmap -sU -g 53 < HostName or IPaddress >
```

この設定で PortScan を行うと、全てのパケットは接続元 UDP ポート 53 番から発信されるので、ファイアウォールは DNS-Response と誤認して PortScan の内側への透過を許可してしまいます。

1.5.20 -r:Scan するポートの順番を連番に変更

ディフォルトの設定では侵入検知システムを回避するために、ポートの順番を無作為に選び PortScan を行います。この設定を行うと Scan するポートの順番を連番に変更します。そのため、侵入検知システムに検知される可能性が高くなります。

1.5.21 --randomize_hosts:Scan する IP の順番をランダムに変更

ディフォルトの設定では指定された IP の順番で Scan を行うため、連番の場合に侵入検知システムに検知される可能性があります。

この設定は IP アドレスを無作為な順番で選び Scan するので、侵入検知システムに検知される可能性が低くなります。

1.5.22 -M <max sockets>:使用するソケットの数を設定

この設定は使用するソケットの数を制限します。Scan の速度を緩める場合や、ソケットの使いすぎでサービス不能状態に陥るホストに対して有効です。

1.5.23 -T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane>:Scan の間隔変更

この設定は Scan の間隔を調整する際に使用します。各設定の間隔は次の通りです。

・Paranoid:短縮番号 0 番。各ポート毎に最低 5 分の間隔を空けて Scan を行います。
・Sneaky:短縮番号 1 番。各ポート毎に最低 15 秒の間隔を空けて Scan を行います。
・Polite:短縮番号 2 番。各ポート毎に最低 0.4 秒の間隔を空けて Scan を行います。

・Normal:短縮番号 3 番。ディフォルト設定です。
・Aggressive:短縮番号 4 番。各ポート毎に 1.25 秒までの間隔で Scan を行います。
ホスト一台につき 5 分のタイムアウトが設定されます。
・Insane:短縮番号 5 番。各ポート毎に 0.3 秒までの間隔で Scan を行います。
ホスト一台につき 75 秒のタイムアウトが設定されます。

Paranoid は送られてくる接続要求の間隔で、PortScan を検知する侵入検知システムを回避する際に有効となります。また、パケットの消失を抑える際にも使用します。

1.5.24 --host_timeout <milliseconds>:各 IP に費やす Scan の時間を設定

この設定は、各ホストに対しての Scan を何ミリ秒でタイムアウトするか指定します。

1.5.25 --max_rtt_timeout <milliseconds>:返事待ちの時間設定(最長)

この設定は接続要求に対する返事を最長で何ミリ秒待つか指定します。

1.5.26 --min_rtt_timeout <milliseconds>:返事待ちの時間設定(最短)

この設定は接続要求に対する返事を最短でも何ミリ秒待つか指定します。

1.5.27 --initial_rtt_timeout <milliseconds>:返事待ちの時間設定(初期値)

この設定は接続要求に対する返事待ちの初期時間を設定します。ディフォルトでは、host up check の際にかかった返事待ちの時間を初期値として設定しますが、-P0 などの host up check を行わない場合にこの設定を使用します。指定無しの場合は 6000 ミリ秒が設定されます。

1.5.28 --max_parallelism <number>:同時に行う Scan の数を指定

この設定は同ホストの複数のポートに、同時に Scan を行います。number に１を指定した場合は、同時に二つ以上のポートに PortScan を行うことが禁止されます。パケットの消失を減らす際に有効です。

1.5.29 --scan_delay <milliseconds>:Scan の間隔を指定

この設定は Scan の間隔を調整する際に使用します。-T と異なり任意の間隔を指定できます。間隔をおいた PortScan は、送られてくる接続要求の間隔で PortScan を検知する、侵入検知システムを回避する際に有効となります。また、パケットの消失を抑える際にも使用します。

1.5.30 -n/-R:DNS の名前解決を停止。 / DNS の名前解決を使用

DNS の名前解決を使用するかどうか設定します。ディフォルトは-R(使用する)です。

1.5.31 -d:デバッグモードを使用

この設定は、NMAP が行っている処理をデバッグ用に詳細表示するものです。
OS 推測 Scan により不明な OS を検出した際に、この設定で NMAP の接続要求に対する返事の有無や内容を詳細に調べることができます。また、PortScan の結果が NMAP の誤動作かどうか調べる際にも使用します。

1.5.32 --interactive:インタラクティブモード

この設定は NMAP で shell コマンドが使えるインタラクティブモードに切り替えます。

・n <nmap args> : nmap を nmap args の指定内容で実行します。
n -sS target
・! <command> : shell コマンドを実行します。
!cat /etc/passwd
・x : NMAP を終了します。
・n -h : NMAP のクイックリファレンス(ヘルプ)を表示します。
・h : インタラクティブモードのクイックリファレンス(ヘルプ)を表示します。
・f [--spoof <fakeargs>] [--nmap_path <path>] <nmap args> : バックグラウンドで NMAP を実行します。OPTION によりプロセス偽装や異なるヴァージョンの NMAP を実行することが出来ます。この設定は結果を画面表示しないので、ログ出力が必要です。
f --spoof "test" --nmap_path /home/tools/nmap-2.30BETA17/nmap -sS -oN /tmp/nmap.log target
この設定により、ps コマンドではプロセスは NMAP ではなく、test というプロセスで表示されます。また、実際に動作しているプロセスは/home/tools/nmap-2.30BETA17 にある nmap が使用されます。

1.6 NMAP(state について)

NMAP による PortScan の結果表示には、ポートの状態を表示する state があります。
この state には、次の 3 種類の状態が表示されます
・open
・filtered
・unfiltered
これら 3 種類の状態について解説します。

1.6.1 "open" state

state に open が表示されるのは次の場合です。
・接続要求 SYN に対して SYN+ACK の返信がある場合
・接続要求 FIN に対して返信が無い場合
・接続要求 FIN+URG+PSH に対して返信が無い場合
・フラグ無しの接続要求に対して返信が無い場合

・UDP パケットに対して ICMP 不達通知の返信が無い場合
・接続要求 ACK に対して RST WIN > 0 の返信がある場合

1.6.2 "filtered" state

state に filtered が表示されるのは次の場合です。
・接続要求 SYN に対して返信が無い場合
・接続要求 SYN に対して ICMP 管理上到達禁止通知(CODE13)が返信される場合
PortScan の結果を使い filtered を解説します。

```
# Nmap (V. 2.3BETA14) scan initiated Wed Mar 22 10:43:31 2000 as: nmap -sS 192.168.0.48
Interesting ports on  (192.168.0.48):
Port    State       Protocol  Service
21      open        tcp       ftp
80      open        tcp       http
135     filtered    tcp       loc-srv
139     filtered    tcp       netbios-ssn

# Nmap run completed at Wed Mar 22 10:43:32 2000 -- 1 IP address (1 host up) scanned in 1 second
```

上記の結果が表示されるには、接続要求に対して次のような返信が考えられます。

ポート番号	接続要求	返信内容	state
1〜20	SYN	RST+ACK	表示無し(close)
21	SYN	SYN+ACK	open
22〜79	SYN	RST+ACK	表示無し(close)
80	SYN	SYN+ACK	open
81〜134	SYN	RST+ACK	表示無し(close)
135	SYN	返信無し orCODE13	filtered
136〜138	SYN	RST+ACK	表示無し(close)
139	SYN	返信無し orCODE13	filtered
200〜65535	SYN	RST+ACK	表示無し(close)

この結果から、ポート番号 135 番と 139 番にフィルタが設定されていることがわかります。このように特定の番号だけにフィルタを設定している場合は、フィルタの後ろではポートが開いている可能性が推測されます。

1.6.3 "unfiltered" state

state に unfiltered が表示されるのは次の場合です。
・フィルタの設定されていないポートが閉じている場合
PortScan の結果を使い unfiltered を解説します。

```
# Nmap (V. 2.3BETA14) scan initiated Wed Mar 22 10:43:31 2000 as: nmap -sS 192.168.0.48
Interesting ports on  (192.168.0.48):
Port    State       Protocol  Service
21      unfiltered  tcp       ftp
80      open        tcp       http

# Nmap run completed at Wed Mar 22 10:43:32 2000 -- 1 IP address (1 host up) scanned in 1 second
```

上記の結果が表示されるには、接続要求に対して次のような返信が考えられます。

ポート番号	接続要求	返信内容	state
1～20	SYN	返信無し orCODE13	表示無し(filtered)
21	SYN	RST+ACK	unfiltered
22～79	SYN	返信無し orCODE13	表示無し(filtered)
80	SYN	SYN+ACK	open
81～65535	SYN	返信無し orCODE13	表示無し(filtered)

この結果から、ポート番号 21 番と 80 番を除いた全てのポート番号に、フィルタが設定されていることがわかります。このように特定の番号だけにフィルタを解除している場合は、任意のコードが実行可能な場合に unfiltered のポート番号でバックドアを仕掛けられる可能性があります。また、open と unfiltered のポート番号を利用して OS 推測が可能となります。

1.7 Conclusion

代表的な PortScanner である NMAP を使い、それぞれの PortScan について解説してきましたが、ここまでの内容でわかることは一概に PortScan と言っても様々なものがあるということです。単純に SYN を遮断するようなフィルタを設定するだけでは、侵入者に侵入するための情報を収集されてしまいます。侵入者は ACK や FIN を使った接続要求により対象ホ

ストの開いているポートを調べることで、侵入後の行動を模索したりブラインド・アタック(盲目的攻撃)の成功率を高めることが出来ます。

このように侵入者はあらゆる情報から的確な攻撃方法を探しだしてきますので、あらゆる PortScan の仕組みを知り適切なフィルタの設定を行い、侵入を困難なものにすることが望ましいです。

2.0 nmap-rpc

nmap に登録されている RPC のヴァージョン番号です。

```
# This was created by Vik Bajaj <vbajaj@sas.upenn.edu> with help
# from various members of the nmap-hackers list.
# To join nmap-hackers send mail to nmap-hackers-subscribe@insecure.org
# Nmap is available from http://www.insecure.org/nmap/
# All the rpc services we could find as of Feb22, 1999
# Tweaked a bit by Fyodor <fyodor@dhp.com>

3270_mapper          100013
NETlicense           100062
activity             100109 na.activity     # SunNet Manager
admind               100087
alis                 100018
amd                  300019 amq
arserverd            390600 arserverd              # Remedy AR System daemons
arservtcd            390604 arservtcd
aseagent             395176 aseagent
asedirector          395175 asedirector
asehsm               395177 asehsm
aselogger            395179 aselogger
autofsd              100099 autofsd
bootparamd           100026 bootparam
bssd                 300433 bss
bugtraqd             100071
bwnfsd            545580417
cachefsd             100235
cfsd              824395111
cfsd             1092830567
cluinfod             300527 # cluster information server
cmsd                 100068 dtcalendar
cnxagentd            300484 # cluster agent
cnxmond              300483 # cluster node monitor
database_svc         100016
debug_svc            100066 dbsrv
diskinfo             100105 na.diskinfo            # SunNet Manager
dmispd               300598
dmispd            805306368
drdd                 300434 drd
```

```
etherif             100118 na.etherif
etherif2            100135 na.etherif2            # SunNet Manager
etherstatd          100010 etherstat
event               100101 na.event        # SunNet Manager
exportmap           200023
fypxfrd          600100069 freebsd-ypxfrd
hostif              100117 na.hostif
hostmem             100112 na.hostmem
hostmem2            100136 na.hostmem2            # SunNet Manager
hostperf            100107 na.hostperf
inetray          555555555
inetray          555555556
inetray          555555557
inetray          555555558
inetray          555555559
inetray          555555560
inetray.start    555555554
ioadmd              100055 rpc.ioadmd
iostat              100106 na.iostat
iostat2             100137 na.iostat2             # SunNet Manager
ippath              100119 na.ippath              # SunNet Manager
iproutes            100120 na.iproutes
kcms                100221
kerbd               100078
keyserv             100029 keyserver
layers              100121 na.layers
layers2             100131 na.layers2             # SunNet Manager
llockmgr            100020
logger              100102 na.logger       # SunNet Manager
lpstat              100111 na.lpstat              # SunNet Manager
metad               100229 metad                  # rpc.metad
metamhd             100230 metamhd                # rpc.metamhd
mountd              100005 mount showmount
nf_snmd             120126 # SunNet Manager
nf_snmd             120127
nfs                 100003 nfsprog
nfs_acl             100227
nis_cache           100301
nis_callback        100302
nisd                100300 rpc.nisd
nisd_resolv         1073741824                    # chosen at run-time
nispasswd           100303 rpc.nispasswdd
nlockmgr            100021
nsed                100038
nsemntd             100039
ntserverd           390601 ntserverd
pcnfsd              150001 pcnfs
ping                100115 na.ping
portmapper          100000 portmap sunrpc rpcbind
prestoctl           390100 # Prestoserve
prpasswd            300632
rexd                100017 rex
rje_mapper          100014
rpcnfs              100116 na.rpcnfs
rquotad             100011 rquotaprog quota rquota
rstatd              100001 rstat rstat_svc rup perfmeter
```

```
rusersd             100002 rusers
sadmind             100232
sample              100113 na.sample
sched               100019
scopeux             805306352 # HP measureware scopeUX
seagent             20000777  # Memco/Platinum/CA SeOS security product
selection_svc       100015 selnsvc
sender              100139 cc_sender              # Cooperative Consoles
sgi.ha_ifa          391021 ha_ifa
sgi.ha_ifmx         391019 ha_ifmx
sgi.ha_orcl         391018 ha_orcl
sgi.ha_sybs         391020 ha_sybs
sgi_fam             391002
sgi_ha_appmon       391015 ha_appmon sgi.ha_appmon
sgi_ha_hb           391013 ha_heartbeat ha_hbeat sgi.ha_hbeat
sgi_ha_nc           391014 ha_nc sgi.ha_nc
sgi_iphone          391010
sgi_mediad          391017 mediad
sgi_mountd          391004 mount showmount
sgi_nfs             391007
sgi_notepad         391003 notepad
sgi_pcsd            391006 pcsd
sgi_pod             391009 pod
sgi_reserved        391022
sgi_reserved        391023
sgi_reserved        391024
sgi_reserved        391025
sgi_reserved        391026
sgi_reserved        391027
sgi_reserved        391028
sgi_reserved        391029
sgi_reserved        391030
sgi_reserved        391031
sgi_reserved        391032
sgi_reserved        391033
sgi_reserved        391034
sgi_reserved        391035
sgi_reserved        391036
sgi_reserved        391037
sgi_reserved        391038
sgi_reserved        391039
sgi_reserved        391040
sgi_reserved        391041
sgi_reserved        391042
sgi_reserved        391043
sgi_reserved        391044
sgi_reserved        391045
sgi_reserved        391046
sgi_reserved        391047
sgi_reserved        391048
sgi_reserved        391049
sgi_reserved        391050
sgi_reserved        391051
sgi_reserved        391052
sgi_reserved        391053
sgi_reserved        391054
```

```
sgi_reserved         391055
sgi_reserved         391056
sgi_reserved         391057
sgi_reserved         391058
sgi_reserved         391059
sgi_reserved         391060
sgi_reserved         391061
sgi_reserved         391062
sgi_reserved         391063
sgi_rfind            391008 rfind
sgi_smtd             391005 smtd
sgi_snoopd           391000 snoopd snoop
sgi_testcd           391012 testcd
sgi_toolkitbus       391001
sgi_videod           391011
sgi_xfsmd            391016
showfhd              100043 showfh
snmp                 100122 na.snmp snmp-cmc snmp-synoptics snmp-unisys snmp-utk
snmp-utk                  0
snmpXdmid            100249
snmpv2               100138 na.snmpv2              # SunNet Manager
sprayd               100012 spray
statmon              100023
status               100024
stdfm                300009 # Online help with
sunisamd             100065
sunlink_mapper       100033
sync                 100104 na.sync
tfsd                 100037
traffic              100123 na.traffic
ttdbserverd          100083 ttdbserverd tooltack ttdbserver rpc.ttdbserverd
ttsession         1342177279
ufsd                 100233 ufsd
walld                100008 rwall shutdown
x25                  100114 na.x25
x25.inr              100022
ypbind               100007
yppasswdd            100009 yppasswd
ypserv               100004 ypprog
ypupdated            100028 ypupdate
ypxfrd               100069 rpc.ypxfrd ypxfr
```

2.1 Nmap OS FingerPrint

Nmap 2.3BETA14 では 406 種類の OS を推測できます。

推測可能な OS は次の種類です。

```
3Com Access Builder 4000 7.2
3Com SuperStack II (OS v 2.0)
3Com SuperSTack II switch SW/NBSI-CF,11.1.0.00S38
```

```
3Com NetBuilder & NetBuilder II OS v8.1
3Com NetBuilder-II, OS version SW/NB2M-BR-5.1.0.27
3Com NetBuilder & NetBuilder II OS v 9.3
US Robotics Total Control NETServer Card
3COM / USR TotalSwitch Firmware: 02.02.00R
ACC Amazon 9.2.29 or Congo 9.2.35 WAN concentrator
Acorn Risc OS 3.6 (Acorn TCP/IP Stack 4.07)
Acorn RiscOS 3.7 using AcornNet TCP/IP stack  # Thanks to Chris Wilson
AGE Logic, Inc. IBM XStation
Aironet Wireless Bridge running firmware V5.0J
AIX 3.2
AIX 3.2 running on RS/6000
AIX 3.2.5 (Bull HardWare)
AIX 4.0 - 4.2
AIX 4.02.0001.0000
AIX v4.2
AIX 4.1
AIX v4.1 running on a C10
AIX 4.1
AIX 4.2
AIX 4.2
AIX 4.2
AIX 4.3.2.0 on an IBM RS/*
Alcatel 1000 ADSL (modem)
Alcatel 1000 DSL Router / unknown OS Rev.
Allied Telesyn AT-S10 version 3.0 on an AT-TS24TR hub
Allied Telesyn AT-3726 Ethernet Switch: 2.1cycleA
Alteon AceSwitch 110 (software 4.0.37)
AmigaOS Miami 2.1-3.0
AmigaOS Miami 3.0
AmigaOS Miami 3.1-3.2
AmigaOS Miami Deluxe 0.9 - Miami 3.2B
AmigaOS 3.1 running Miami Deluxe 0.9m
AmigaOS AmiTCP/IP 4.3
AmigaOS AmiTCP/IP Genesis 4.6
Amos 2.3A
AOS/VS on a Data General mainframe
Apollo Domain/OS SR10.4
AOS/VS or VSII
Apple Airport (Wireless Network Hub)
Ascend P130 Router
Ascend Max 1800 50Ap8+ or 2024
Ascend Max (HP,4000-6000) version 6.1.3 - 6.1.7
Ascend Pipeline 50 running 5.1A Firmware # Thanks to Jan Koum
Ascend GRF Router running Ascend Embedded/OS 2.1
Ascend Pipeline 50 rev 4.6C
Ascend P75
Ascend Pipeline P130 or 50
Ascend Pipeline 400/T1 (Software V 4.5B)
Ascend TNT OS +5.0Ap48+
Macintosh GS Server with MacOS 8.5.1 (Appleshare IP 6.0)
MacOS 8.1 running on a PowerPC G3 (iMac)
MacOS 8.6
Rhapsody 5.3 - 5.4 (Mac OS X Server 1.0 - 1.0-1)
Mac OS X (Rhapsody 5.5) on a G3
Apple Color LaserWrite 600 Printer # Thanks to Pluvius
```

```
Apple Color LaserWrite 600 Printer # Thanks to Pluvius
Apple LaserWriter 16/600 PS, HP 6P, or HP 5 Printer
Apple LaserWriter 8500 (PostScript version 3010.103)
AS5200  # Thanks to Michael Dodwell <mdodwell@vic.bigpond.net.au>
Asanta IntraStack Ethernet Switch (6014 DSB Versions: BP(2.06 ), FW(1.03 ))
Asanta IntraSwitch 5324
AsanteHub 2072 Ethernet Hub
Auspex Fileserver (AuspexOS 1.9.1/SunOS 4.1.4)
Assured Access Technology: ISAS Switch Release-2.3.0
Atari Mega STE running JIS-68k 3.0
ATT Unix SVR4.2 on a Lucent Definity voicemail system
A/UX 3.1.1 SVR2 or OpenStep 4.2
AXCENT Raptor Firewall running on Windows NT 4.0/SP3
AXIS NetEye Camera Server V1.20 # Thanks to Pluvius
AXIS Stack -- CD-ROM Server or Printer Server or Camera Server # Thanks to Pluvius
Axis 200+ Web Camera running OS v1.42
Bay Networks BLN-2 Network Router or ASN Processor revision 9
Bay Networks BayStack 310T switch
BayStack 28115/ADV Fast Ethernet Switch  # Thanks to Jan Koum!
BeOS 4 - 4.5
Bintec XS/XM ISDN access routers V. 4.9.1-4.9.3
Borderware 5.0 Firewall
Borderware 5.2 firewall
Borderware 6.0.2 firewall
BSDI BSD/OS 2.0 - 2.1  # Thanks to dmessiah & tacit@bigfoot.com
BSDI BSD/OS 3.0-3.1
BSDI 4.0  # Thanks to tom@bpf.promisc.org
BSDI BSD/OS 4.0.1 Kernel
BSDI Version 7.00LS
CacheOS (CacheFlow 2000 proxy cache)
Canon photocopier/fax/scanner/printer GP30F
Chase IOLan Terminal Server
Cisco 762 IOS 4.1(2) or 766 ISDN router
Cisco 7206 running IOS 11.1(24)
Cisco CacheEngine
Cisco CPA2500 (68030) or 2511 router
Cisco Localdirector 430, running OS 2.1
Cisco PIX 4.2(2) Internal Interface
Cisco 766 IOS4.2(3.5)
Cisco 3640 IOS 11.1(7)AX [KUONG(7)AX]
IOS Version 10.3(15) - 11.1(20)  # Thanks to Pluvius
Cisco 5260 or 5300 terminal server IOS 11.3.6(T1)
Cisco 4500-M running IOS 11.3(6) IP Plus
Cisco Catalyst 1900 switch or Netopia DSL/ISDN router
Cisco IOS 11.3 - 12.0(2)
Cisco 7206  (IOS 11.1(17)  # Thanks to jfesler@gigo.com
Cisco 1600/3640/7513 Router (IOS 11.2(14)P) #Thanks to Solar Designer
Cisco Local Director 420 version 2.1.1
Cisco Pix Firewall running PIX 4.1(5)
Cisco PIX v4.2 Firewall
Cisco IOS v11.14(CA)/12.0.2aT1/v12.0.3T
Cisco Router/Switch with IOS 11.2 # Thanks to Solar Designer
Cisco IOS 12.0(3.3)S  (perhaps a 7200)
Cisco 675 DSL router -- cbos 2.1
Cisco Secure PIX Firewall Version 5.0(2)
Cisco X.25/TCP/LAT Protocol Translator ver 8.2(4)
```

```
CLIX R3.1 Vr.7.6.20 6480
Compatible Systems (RISC Router, IntraPort)
Computone PowerRack IntelliServer Release 1.5.4d
ComOS - Livingston PortMaster or U.S. Robotics/3com Total Control system
Lucent Portmaster 4 running ComOS v4.0.3c2
Convex OS Release 10.1
Corporate IP/IPX ISDN Small Office ISDN router (version 9.9.9/8.0)
Cray UNICOS/mk 8.6
Cray Unicos 9.0 - 10.0 or Unicos/mk 1.5.1  # Thanks to Mea Culpa
Unicos 10.0.0 on Cray 90
Cray UNICOS 9.0.1ai - 10.0.0.2
Cyclades PathRouter V 1.2.4
Cyberguard 4.0 firewall
Cyclades PathRAS Remote Access Server v1.1.8 - 1.3.12
Cyclades PathRAS V 1.1.7
Datavoice TxPORT PRISM 3000 T1 CSU/DSU 6.22/2.06
DECbrouter90T1 Runs Cisco IOS 10.2(5)
DECNIS 600 V4.1.3B System
DECserver700-16, Network Access SW V2.2
DEC VNswitch900
DG/UX Release R4.11MU02
DG/UX Release R4.20MU02
Digital Link DL2001 Management Access Processor
Digital UNIX OSF1 V 3.0,3.2,3.2C  # Thanks to Lamont Granquist
Digital UNIX OSF1 V 4.0,4.0B,4.0D,4.0E  # Thanks to Mea Culpa & Lamont Grsnquist & Izar Tarandach
Compaq Tru64 UNIX (formerly Digital UNIX) 4.0e
Compaq Tru64 UNIX 5.0 on AlphaServer
DEC OSF/1 V1.3A - 2.0
OSF/1 5.60
Digital UNIX OSF1 V 4.0-4.0F
Epson Stylus 800n/EPSON Ethernet Ver. 4.20
X EPSON Ethernet Ver. 4.20 6.04, 13395E-98
Extreme Networks Black Diamond switch
Extreme Gigabit switch (unknown version)
NAT LANB/290 Console Program V4.00
NCR S26 (i386) running NCR MP-RAS SVR4 UNIX System
Farralon Netopia router or Compatible Systems 900i
Netopia DSL router
Nokia IPSO 3.2-fcs4 releng 783
Galacticomm WorldGroup BBS / Vircom TCP/IP stack
Gandalf LanLine Router
Compatible Systems MicroRouter 900i v3.0.9
Compatible Systems Microrouter 2220R w/ firmware v4.5
FlowPoint/2000 - 2200 SDSL Router (v1.2.3 - 3.0.4) or ASCOM Timeplex Access Router
Flowpoint 144 or 2200 SDSL [ATM] Router v3.0.8
FreeBSD 2.1.0 - 2.1.5  # Thanks to Jan Koum!
FreeBSD 2.2.1 - 3.2  # Thanks to David O'Brien
FreeBSD 2.2.1 - 4.0  #Thanks to Jan Koum
Gold Card Ethernet Interface Firmware Ver. 3.19 (95.01.16).  Apparently a MIO Network interface
  for HP LaserJets, etc.
Hitachi HI-UX/MPP (don't know version)
HP Advancestack Etherswitch 224T or 210
HP-BSD 2.0
HP Entria X station (running Netstation 7.x)  # Thanks t Zippy <seth@interport.net>
HP JetDirect Print Server
HP printer w/JetDirect card
```

```
HP LaserJet Printer # Thanks to Dmessiah
HP LaserJet 4000N Printer  # Thanks to David O'Brien
HP LaserJet 5  # Thanks to Pluvius
HP Procurve Routing Switch 9304M
HP-UX A.09.00 E 9000/817 - A.09.07 A 9000/777
HP-UX 9.01 - 9.07
HP-UX B.10.01 A 9000/715
HP-UX B.10.20 A 9000/715 or 9000/712 or 9000/871 or 9000/861 with tcp_random_seq = 0
HP-UX B.10.20 A 9000/715 or 9000/712 or 9000/871 with tcp_random_seq = 1 #Thanks to Lamont Granquist,
  David O'Brien
HP-UX 10.20 A 9000/715 or 9000/899
HP-UX B.10.20 9000/897
HP-UX 10.20 E 9000/777 or A 712/60 with tcp_random_seq = 0
HP-UX 10.20 # 9000/777 or A 712/60 with tcp_random_seq = 1 or 2
HP-UX B.11.00  # Thanks to root@knightmare.cc
HP-UX 11.00
HP-UX B11.00 U 9000/839
HP-UX 11.00  # Thanks to Jason Ledbetter <jason@colltech.com>
Hydra HydraWEB 5000
IBM 2210 router unknown patch level
IBM LAN RouteSwitch/Xylan OmniSwitch Version 3.2.5/NeXT
IBM OS/2 V 2.1
IBM OS/2 V.3  # Thanks to van Hauser (vh@reptile.rug.ac.be)
IBM OS/2 Warp 4.0
IBM OS/2 Warp Server for E-business (Aurora) Beta
IBM OS/2 Warp Server for E-business (Aurora) Beta
AS/400e 720 running OS/400 R4.4
IBM AS/400 V3 and V4
IBM VM/CMS (mainframe)
IBM VM/ESA 2.2.0 CMS Mainframe System
Cisco 760 Series (non IOS) or IBM Stackable Hub
D-Link Corp. DE-1800 Stackable Hub SNMP/Telnet Agent Software version 2.04B3 boot PROM 2.21
Intel Corporation, ER9100 Express Router 9100
Intel Express 510T switch
Interl Netport Express PRO V04.33a
Intel NetportExpress(tm) 10/100 3-port ROM: V05.10a
Lantronix EPS1 Version V3.5/1(970325)
Lantronix EPS2 Printer Version V3.5/2(970721)
MPE/iX 5.5
MultiTech CommPlete Controller
MVS TCP/IP TCPMVS 3.2
IBM MVS TCP/IP stack V. 3.2 or AIX 4.3.2
IBM MVS TCP/IP TCPOE 3.3  # Thanks to van Hauser
IBM MVS (unknown version)  # Thanks James W. Abendschan <jwa@jammed.com>
Instant Internet box
Intergraph Workstation (2000 Series) running CLiX R3.1
IPAD Model 5000 (see www.ipad-canada.com)
IRIX 5.2
IRIX 5.3  # Thanks to David O'Brien & Mea Culpa
IRIX 6.2 - 6.5  # Thanks to  Lamont Granquist
IRIX 6.2 - 6.5 # Thanks to Lamont Granquist
IRIX 6.4 - 6.5.3m  # Lamont Granquist (again :)
IRIX 6.5
Isolation Systems Infocrypt Enterprise
Juniper Router running JUNOS
Kentrox Datasmart 656 CSU/DSU or USR Netserver/16
```

```
Lantronix LSB4 Ethernet Switch
Router/Switch/Printer (LanPlex 2500/Cisco Catalyst 5505/Trancell Webramp/Xylan Omni
  Switch)/Epson Stylus (100BTX-NIC)
Lexmark Optra S Printer
Lexmark Optra R+ (4049-RA0) w. MarkNet XL card (firmware rev. 79.133.1
Linux 1.0.9
Linux 1.2.8 - 1.2.13
Linux 1.2.13
Linux 2.0.0
Linux 2.0.27 - 2.0.30
Linux 2.0.32-34
Linux 2.0.32-34
Linux 2.0.35-37
Linux 2.0.35 (S.u.S.E. Linux 5.3 (i386)
Linux 2.1.24 PowerPC
Linux 2.1.76
Linux Kernel 2.1.88
Linux 2.1.91 - 2.1.103
Linux 2.1.122 - 2.2.13
Linux 2.2.12
Linux kernel 2.2.13
Linux 2.3.12
Linux 2.3.28-31
MacOS 7.1   # Thanks to  Renaud Deraison
Mac OS 7.0-7.1 With MacTCP 1.1.1 - 2.0.6
MacOS 7.5.5 - 8.6 # Thanks to //Stany <stany@zerkalo.notbsd.org>
MacOS 8 running on an LC 475
MacOS 8.5  # Thanks to A.j. Effin ReznoR <spork@exo.com>
APC MasterSwitch Network Power Controller
ARLAN BR2000E V5.0E Radio Bridge
AXIS or Meridian Data Network CD-ROM server
AXIS 540/542Print ServerV5.30 Jan 24 1997
Axis 540 print server
Meridian Data Network CD-ROM Server (V4.20 Nov 26 1997)
Microplex Print Server
MiNT with MiNTnet 1.03 running on Atari TT
Minux 32-bit/Intel 2.0.0
Mirapoint M1000 (OS v 1.0.0)
MultiTech CommPlete (modem server) RAScard
NEC UX/4800
NCD X server (SNMP says: NCD16 server 2.3.0 03/12/91 downloaded)
NCR MP-RAS 3.0.x
NCR MP-RAS 3.01
NCSA Telnet (dos)
NCSA Telnet 2.3.08 for the PC
Neoware (was HDS) NetOS V. 2.0.1 or HP ENTRIA C3230A
NetApp OnTap 3.1.6
NetApp OnTap 5.1.2 - 5.2.2
NetBSD 1.0 little endian arch
NetBSD 1.0 big endian arch
NetBSD 1.1 - 1.2.1 litle endian arch
NetBSD 1.2 - 1.2.1 big endian arch
NetBSD 1.3 - 1.3.3 little endian arch
NetBSD 1.3 - 1.3.3 big endian arch
NetBSD 1.3H (after 19980919) or 1.3I (before 19990119) little endian arch
NetBSD 1.3H (after 19980919) or 1.3I (before 19990119) big endian arch
```

```
NetBSD 1.3I (after 19990119) to 1.4 x86
NetBSD 1.4 / Generic mac68k (Quadra 610)
NetJet Version 3.0 - 4.0 Printer
Network Systems router NS6614 (NSC 6600 series)
NeXT Mach
Nokia IPSO 3.2-fcs4 releng 783 (FreeBSD Based)
Nortel Networks CVX1800 RAS. Software version 2.02
Novell NetWare 3.12 - 5.00  # Thanks to Chris Wilson
NetWare 4.11 SP7- 5 SP3A BorderManager 3.5
Novell NetWare 5.0 with Border Manager
Novell NetWare 3.12 or 386 TCP/IP
Netware 5.0 SP 3a
OpenStep 4.0-4.2 or NextStep 1.0-3.3 (Intel)
OpenStep 4.1/NeXTStep 3.3
OpenStep 4.2/Intel
OpenBSD 2.1 - 2.3/SPARC
OpenBSD 2.1/X86
OpenBSD 2.2 - 2.3
OpenBSD Post 2.4 (November 1998) - 2.5
OpenBSD 2.6/X86
OpenVMS 6.1  # Thanks to Mcneil J <J.Mcneil@rhbnc.ac.uk>
OpenVMS V6.1 on Digital VAX 4000-105A
OpenVMS 6.2 on VAX
Digital OpenVMS AXP 6.2 running Attachmate Pathway 3.1 TCP stack
OpenVMS 6.2/Alpha
OpenVMS 7.1 using Process Software's TCPWare 5.3 TCP/IP package
OpenVMS 7.1 Alpha running Digital's UCX v4.1ECO2 TCP/IP package
OpenVMS v7.1 VAX running Process Software's TCPWare 5.1-5 TCP/IP package
OpenVMS Alpha V7.1-1H2 running DIGITAL TCP/IP Services (UCX) V4.2
OpenVMS V7.1 on VAX 6000-530
SEQUENT DYNIX/ptx(R) V4.2.1
SINIX-N 5.43C3002
SINIX-N 5.41C0005
SINIX-Y 5.43B0045
SINIX-Y 5.43C4001
SonicWall/10
SONY NEWS-OS 6.1.2
Sega Dreamcast
Stock OpenVMS 7.1
OpenVMS Alpha 6.2 running DIGITAL TCP/IP Services (UCX) v4.0
OS/390 V5R0M0
Packet Engines PowerRail 5200 Version 2.6.0r10 - 16 Sep, 1999
Packeteer IP-PacketShaper 2000 V3.1
Plan9 (can anyone give me a version number?)
Polycom ViewStation 512K videoconferencing system
Proteon OpenRoute 2.1 on a RBX200 Router
Proteon OpenRoute 3.0 gt series router
QNX 4.24
Raptor firewall 5.03 on NT 4
Raptor Firewall 6 on Solaris 2.6
Redback SMS 1000-2000 DSL Router
ReliantUNIX-Y 5.44 B0033 RM600 1/256 R10000
Ringdale RP21 Print server
SCO Release 5
SCO OpenServer(TM) Release 5
SCO OpenServer 5.0.5
```

```
UnixWare 2.01
SCO UnixWare 2.1        # Thanks to Digital Messiah
SCO UnixWare 2.1.2  # Thanks to Drew Morone <tdrew@cairn.org>
SCO UnixWare 7.0.0
SCO Open Desktop 2.0
Secure Computing Sidewinder firewall 3.2 update 4
Shiva AccessPort Bridge/Router Software V 2.1.0 or 3COM HiPer Access Router Card hardware V1.0.0
  software V4.1.59
Shiva LanRover/8E Version 3.5
Snap Network Box
Solaris 2.3 - 2.4  # Thanks to David O'Brien & Mea Culpa
Solaris 2.4 w/most Sun patches (jumbo cluster patch, security patches, etc)
Solaris 2.5, 2.5.1
Solaris 2.6 - 2.7
Solaris 2.6 - 2.7 X86
Solaris 2.6
Solaris 2.6 - 2.7 with tcp_strong_iss=0
Solaris 2.6 - 2.7 with tcp_strong_iss=2
Solaris 7
Sun Solaris 8 early acces beta (5.8) Beta_Refresh February 2000
SonicWall/10 Firewall
SPP-UX 5.2.1
SPP-UX 5.x on a Convex SPP-1600
SunOS 4.0.3
SunOS 4.1.3_U1 + ISI RFC1323 mods from ISI
SunOS 4.1.1 - 4.1.4 (or derivative) # Thanks to Renaud Deraison, Jericho, Lamont Granquist, and
  others
Tandem NSK D39
Tektronix Phaser 360 Extended
Tektronix Phaser(TM) Share Ethernet Card, firmware version 3.01
Telebit's NetBlazer 3.0
Telebit NetBlazer Version 3.05
Telebit NetBlazer Version 3.1, patch level 13
Teltrend (aka Securicor 3net) Router
TOPS-20 Monitor 7(102540)-1,TD-1
Toshiba TR650 ISDN Router
Ultrix 4.1
Ultrix 4.2 - 4.5
VersaNet ISP-Accelerator(TM) Remote Access Server
VNS V6.2
VxWorks 5.3.x bases system (usually an ethernet hub or switch)
Webwizard NuSwitch DS16, ver 1.10.03.
Windows 3.1 with Trumpet Winsock 2.0 revision B
Windows for Workgroups 3.11 / TCP/IP-32 3.11b stack
Windows NT4 / Win95 / Win98
Windows NT 4 SP3
Windows NT4 / Win95 / Win98
Microsoft NT 4.0 Server SP5 + 2047 Hotfixes
Windows NT 4.0 Server SP5-SP6
Windows 98
Windows 98 w/ Service Pack 1
Windows NT 5 Beta2 or Beta3
Windows 2000 RC1-RC3
Windows 2000 Professional, Build 2128
Windows 2000 Professional, Build 2183 (RC3)
MS Windows2000 Professional RC1
```

WNOS 5.0 on DOS 6.22
WorldGroup BBS (MajorBBS) w/TCP/IP
VAX/VMS 5.3 on a MicroVAX II
VAX/VMS v5.5, CMU-TEK TCP/IP stack
VAX 7000-610 or 4200/SPX OR 6000-430
XCD Xconnect print server, firmware version CC8S-3.58 (98.09.21)
Xerox 8830 Plotter
Xerox DocuPrint C55
Xerox DocuPrint N40
Xylan OmniSwitch 5x/9x ethernet switch, Annex3 Comm server R10.0, or Hitach HI-UX/WE2
Xyplex 1600 running MAXserver V6.0.2 firmware
LynxOS Realtime OS -- Could be MeetingPlace 3.4, Xylogics Remote Annex 4000 terminal server
CacheOS (CacheFlow 500-5000 webcache) CFOS 2.1.08 - 2.2.1
Xyplex Network9000
Xyplex Terminal Server v6.0.2S5
Zyxel P128imh router