



**Daniel Österlin**  
**Patrick Wandelt**  
Säkerhet HT-03  
Martin Fahlgren

# NMAP= Network mapper

NMAP använder IP-paket för att ta reda på detta om nätverket :

1. Vilka datorer som finns
2. Vilka tjänster körs
3. Version av Operativsystem
4. Vilka brandväggar
5. Skanna stora och små nätverk
6. Upptäcka säkerhetsbrister

Det som skiljer NMAP från andra portskanners är att den innehåller flera olika funktioner. Ibland vill man kanske skanna något snabbt, ibland kanske man inte vill bli upptäckt (bra för att testa loggning på till exempel en brandvägg), och ibland kanske man vill specificera olika protokoll. För att göra detta behövs ofta flera olika skannerprogram, men inte i fallet NMAP, som klarar av att utföra flera olika typer av skanningar.

Kan köras med kommandon och grafiskt gränssnitt.

Avancerad skanning: Connect, SYN Stealth, FIN Stealth, Ping Scan, UDP Scan, Null Scan, Xmas Tree, IP Protocol Scan, ACK Scan, Windows Scan, RCP Scan, List Scan

För att undgå att upptäckas: Decoys, Stealth scanning. Programmet kör portar mot kända tjänster. Används ofta av mer användarvänliga program.

Mycket användbar om du t ex vill kontrollera dina brandväggsinställningar på din hemdator

## Installera nmap (Windows)

Hämta programmet på sidan :

[http://www.insecure.org/nmap/nmap\\_download.html](http://www.insecure.org/nmap/nmap_download.html)

- ➡ Kör installationsprogrammet, följ anvisningarna.
- ➡ Starta om.
- ➡ Klicka på Nmapwin ikonen.

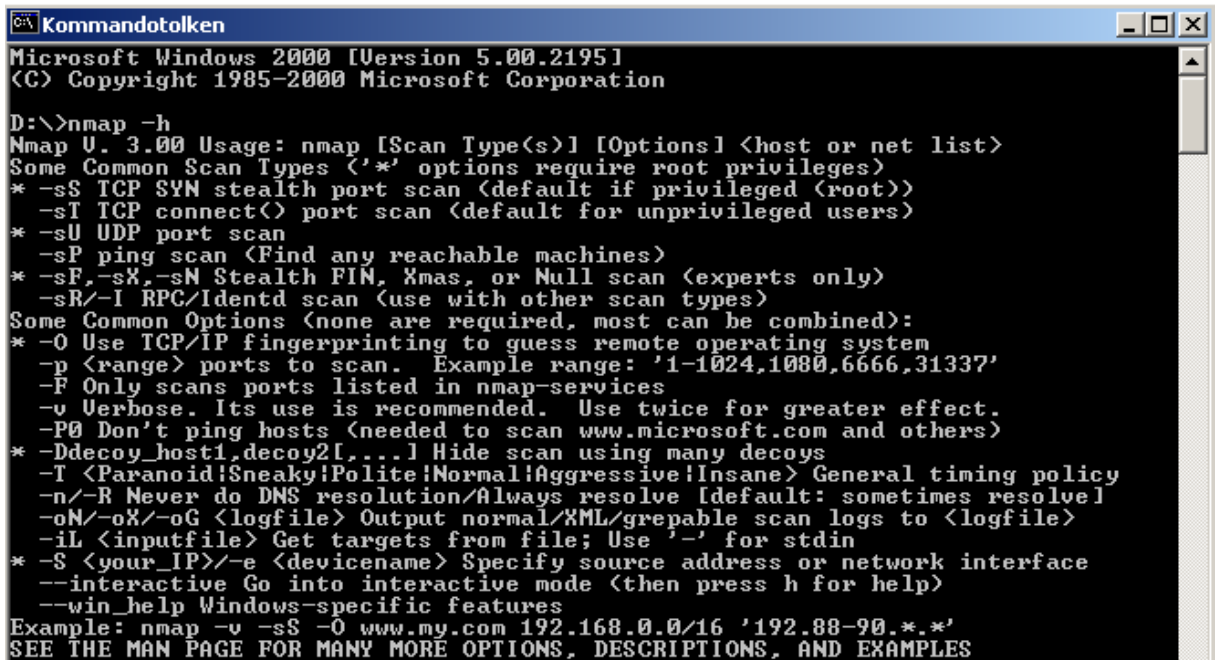
## Fördelarna med NMAP

- Flexibelt. Stödjer dussintals av avancerade tekniker för att kartlägga nätverk med IP-filtrer, brandväggar, routrar. Programmet innehåller många port skanners ( både TCP och UDP), Upptäcka operativsystem, upptäcka tjänster.

Programmet kan användas på alla OS.

- Gratis och öppen källkod så att man kan förbättra programmet.
- Support: . Vid problem med programmet kan man mejla [fyodor@nmap.org](mailto:fyodor@nmap.org).
- Mest nedladdade säkerhetsprogrammet och vunnit massa priser.
- Rekommenderas av Microsoft ! (Läs mer här. Längst ner på <http://www.microsoft.com/serviceproviders/security/tools.asp>

Öppna en dos prompt och skriv -h för att få hjälp angående växlarna:



```
Microsoft Windows [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corporation

D:\>nmap -h
Nmap U. 3.00 Usage: nmap [Scan Type(s)] [Options] <host or net list>
Some Common Scan Types ('*' options require root privileges)
* -sS TCP SYN stealth port scan (default if privileged (root))
* -sT TCP connect() port scan (default for unprivileged users)
* -sU UDP port scan
* -sP ping scan (Find any reachable machines)
* -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)
* -sR/-I RPC/Identd scan (use with other scan types)
Some Common Options (none are required, most can be combined):
* -O Use TCP/IP fingerprinting to guess remote operating system
* -p <range> ports to scan. Example range: '1-1024,1080,6666,31337'
* -F Only scans ports listed in nmap-services
* -v Verbose. Its use is recommended. Use twice for greater effect.
* -P0 Don't ping hosts (needed to scan www.microsoft.com and others)
* -Ddecoy_host1,decoy2[,...] Hide scan using many decoys
* -T <Paranoid!Sneaky!Polite!Normal!Aggressive!Insane> General timing policy
* -n/-R Never do DNS resolution/Always resolve [default: sometimes resolve]
* -oN/-oX/-oG <logfile> Output normal/XML/grepable scan logs to <logfile>
* -iL <inputfile> Get targets from file; Use '-' for stdin
* -S <your_IP>/-e <devicename> Specify source address or network interface
* --interactive Go into interactive mode (then press h for help)
* --win_help Windows-specific features
Example: nmap -v -sS -O www.my.com 192.168.0.0/16 '192.88-90.*.*'
SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES
```

## Tretton olika sorters skanningsalternativ

### TCP Connect:

Den enklaste skanningen är TCP connect. Bygger på metoden att upprätta en anslutning i TCP protokollet Man skickar

Ett connect packet till den skannade datorn och väntar på svar. Alla portar som lyssnar på connect kommer att svara. På så sätt kan man lätt avgöra vilka portar som är öppna för kommunikation.

Nackdelen med TCP connect är att den kan lätt upptäckas i den skannade datorns loggfiler. En annan nackdel är också att den är lätt att filtrera. Fördelen är att denna metod är snabb.

### **SYN Stealth:**

Det krävs rot privilegier (fulla rättigheter) för att använda denna skanning.

Vi skickar iväg ett SYN paket. En SYN/ACK indikerar att porten lyssnar.

En RST indikerar att ingen lyssnar. Om en SYN/ACK tas emot då skickas en RST för att avbryta anslutningen.

### **FIN Stealth, Xmas Tree, Null Scan:**

Det finns tillfällen när inte SYN skanning fungerar. Eftersom brandväggar och paketfilter kan upptäcka dessa sorters skanningar.

Det hela bygger på att portar måste svara på dina probes (stickprov) paket med en RST.

Medans öppna portar inte bryr sig om dina skickade paket.

FIN skanning använder ett FIN paket som stickprov.

Xmas tree sätter flaggorna på FIN, URG, PUSH.

Dessa tre skanningar funkar inte på Windows OS.

### **PING skanning:**

För att veta vilka datorer som fungerar skickar man ICMP eko förfrågningar.

### **UDP port skanning:**

Man skickar noll byte UDP paket till varje port. Om ICMP porten är onåbar då är porten stängd.

När vi vet vilka maskiner som är aktiva då är nästa steg att göra denna portskanning

### **IP protokoll:**

Denna metod tar reda på vilka IP protokoll som körs. Om ICMP porten är onåbar då är porten stängd.

### **Idle skanning:**

Gör en blind TCP port skanning. Med blind menas att inga paket skickas från vår riktiga IP adress

### **ACK Scan:**

Tar reda på om brandväggen endast är ett paketfilter (som endast hindrar SYN paket).

Metoden är att slumpmässiga ACK paket. Om RST kommer tillbaka då är portarna ofiltrerade.

### **Window skann:**

Samma som ACK skann förutom att den upptäcker öppna portar, filtrerade eller inte filtrerade.

### **RPC skann:**

Denna metod öppnar alla TCP/UDP portar och kontrollerar om det är RPC portar. Om så är fallet får man reda på vilken version som finns av programmen.

### **List skann:**

Denna metod skriver ut en lista på alla IP/Namn och gör DNS resolution.

### **FTP bounce:**

Skannar TCP portar från en Proxy ftp server. Då kan man kontakta en ftp server bakom en brandvägg.

## **Följande alternativ kan väljas**

### **Fragmentation:**

Man delar upp IP paketen i små bitar. Detta val används vid SYN, FIN, XMAS eller NULL skanningar. Tanken är att göra det svårare för paket-filters och andra program att se vad du gör.

### **Get Identd Info:**

Ger möjlighet att se användarnamn anslutna via TCP. Man kan även se om servern körs som rot.

### Resolve All:

Säger till NMAP att alltid köra (reverse DNS resolution) på målets IP adress. Detta gör man normalt bara om maskinen är online.

### Don't resolve:

Reverse DNS resolution körs inte.

### Fast Scan:

Du skannar bara de portar som finns i service filen som följer med programmet. Vilket är snabbare än att skanna alla 65535 portarna.

### OS Detection:

Ger möjlighet att identifiera en maskin med TCP/IP fingerprinting.

### Random Host:

Säger till NMAP att generera egna hostar att skanna. Genom att välja nummer slumpvis.

## Hastighet vid skanning

Finns sex olika alternativ

### Paranoid:

Långsam. Men ger möjlighet att skanna utan att bli upptäckt av Väntar 5 min innan den sänder nya paket.

### Sneaky:

Liknande men väntar 15 sekunder innan den sänder paket.

### Polite:

Minskar belastningen på nätverket och belastningen på datorerna.

### Normal :

Försöker att skanna så fort som möjligt utan att överbelasta och missa portar.

### Aggressive:

### Insane:

Används för snabba nätverk. Är inte lika noggran när den skannar

# SCREENSHOTS

## TCP Connect Skanning

Microsoft Windows 2000 [Version 5.00.2195]  
(C) Copyright 1985-2000 Microsoft Corporation

D:\> nmap -sT -PT -PI -O -v -T 3 62.88.181.34

Starting nmap V. 3.00 ( [www.insecure.org/nmap](http://www.insecure.org/nmap) )  
Host dator5889.161.gbgsd.se (62.88.181.34) appears to be up ... good.  
Initiating Connect() Scan against dator5889.161.gbgsd.se (62.88.181.34)  
Adding open port 139/tcp  
Adding open port 25/tcp  
Adding open port 1025/tcp  
Adding open port 110/tcp  
Adding open port 135/tcp  
Adding open port 445/tcp  
The Connect() Scan took 605 seconds to scan 1601 ports.  
For OSScan assuming that port 25 is open and port 1 is closed and neither are fi  
rewalled  
WARNING: RST from port 25 -- is this port really open?  
WARNING: RST from port 25 -- is this port really open?  
WARNING: RST from port 25 -- is this port really open?  
WARNING: RST from port 25 -- is this port really open?  
WARNING: RST from port 25 -- is this port really open?  
WARNING: RST from port 25 -- is this port really open?  
Insufficient responses for TCP sequencing (0), OS detection may be less accurate

For OSScan assuming that port 25 is open and port 1 is closed and neither are fi  
rewalled  
WARNING: RST from port 25 -- is this port really open?  
WARNING: RST from port 25 -- is this port really open?  
WARNING: RST from port 25 -- is this port really open?  
WARNING: RST from port 25 -- is this port really open?  
WARNING: RST from port 25 -- is this port really open?  
WARNING: RST from port 25 -- is this port really open?  
Insufficient responses for TCP sequencing (0), OS detection may be less accurate

For OSScan assuming that port 25 is open and port 1 is closed and neither are fi  
rewalled  
WARNING: RST from port 25 -- is this port really open?  
WARNING: RST from port 25 -- is this port really open?  
WARNING: RST from port 25 -- is this port really open?  
WARNING: RST from port 25 -- is this port really open?  
WARNING: RST from port 25 -- is this port really open?  
WARNING: RST from port 25 -- is this port really open?  
Insufficient responses for TCP sequencing (0), OS detection may be less accurate

Interesting ports on dator5889.161.gbgsd.se (62.88.181.34):  
(The 1595 ports scanned but not shown below are in state: closed)

Port	State	Service
25/tcp	open	smtp
110/tcp	open	pop-3
135/tcp	open	loc-srv

139/tcp open netbios-ssn  
445/tcp open microsoft-ds  
1025/tcp open NFS-or-IIS

No exact OS matches for host (If you know what OS is running on it, see <http://www.insecure.org/cgi-bin/nmap-submit.cgi>).

TCP/IP fingerprint:

SIInfo(V=3.00%P=i686-pc-windows-windows%D=12/4%Time=3FCF2907%O=25%C=1)

T1(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)

T2(Resp=Y%DF=N%W=0%ACK=S%Flags=AR%Ops=)

T3(Resp=Y%DF=N%W=0%ACK=O%Flags=AR%Ops=)

T4(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)

T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)

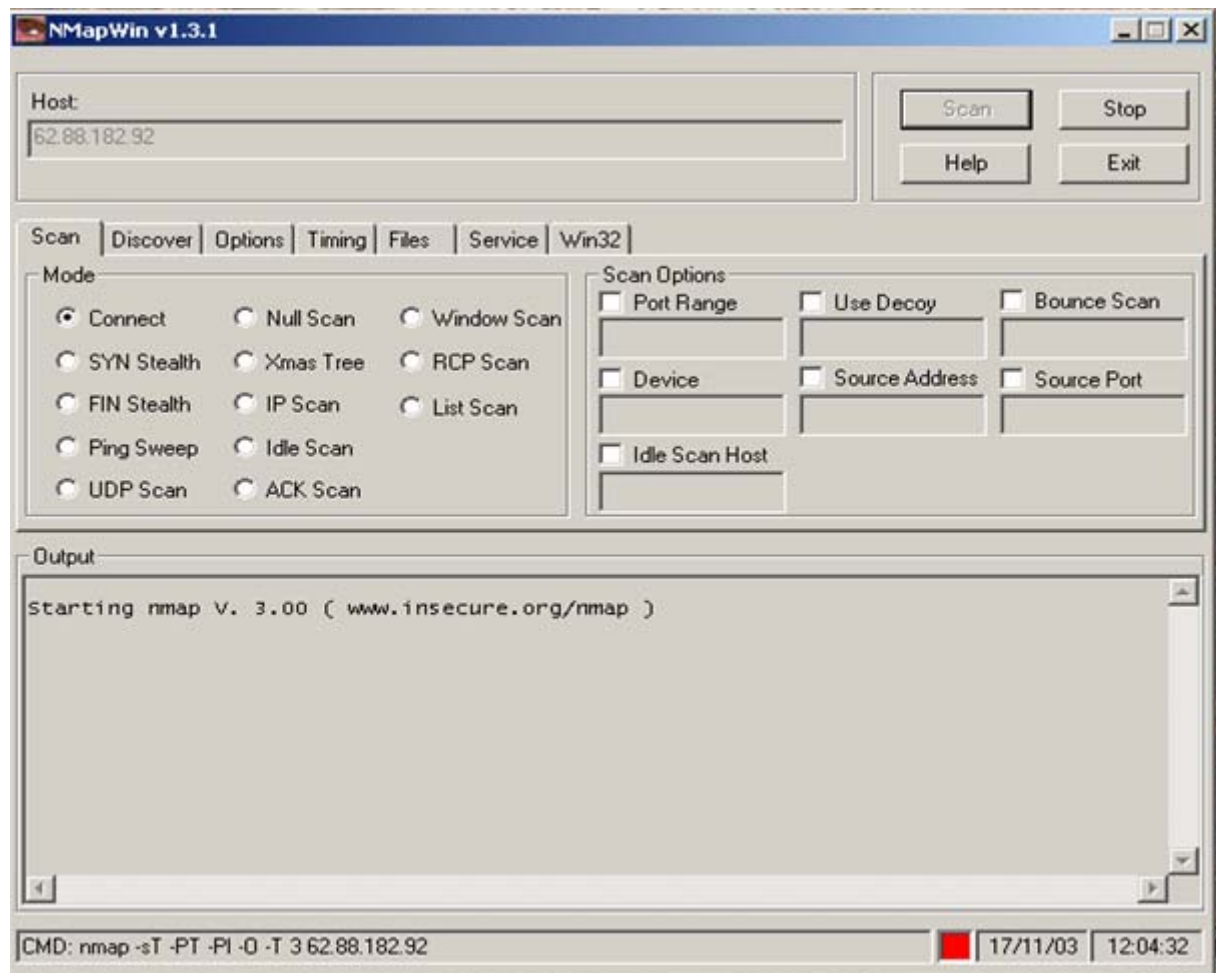
T6(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)

T7(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)

PU(Resp=Y%DF=N%TOS=0%IPLen=38%RIPTL=148%RIPCK=E%UCK=E%ULEN=134%DAT=E)

Nmap run completed -- 1 IP address (1 host up) scanned in 628 seconds

D:\>



## SYN Stealth

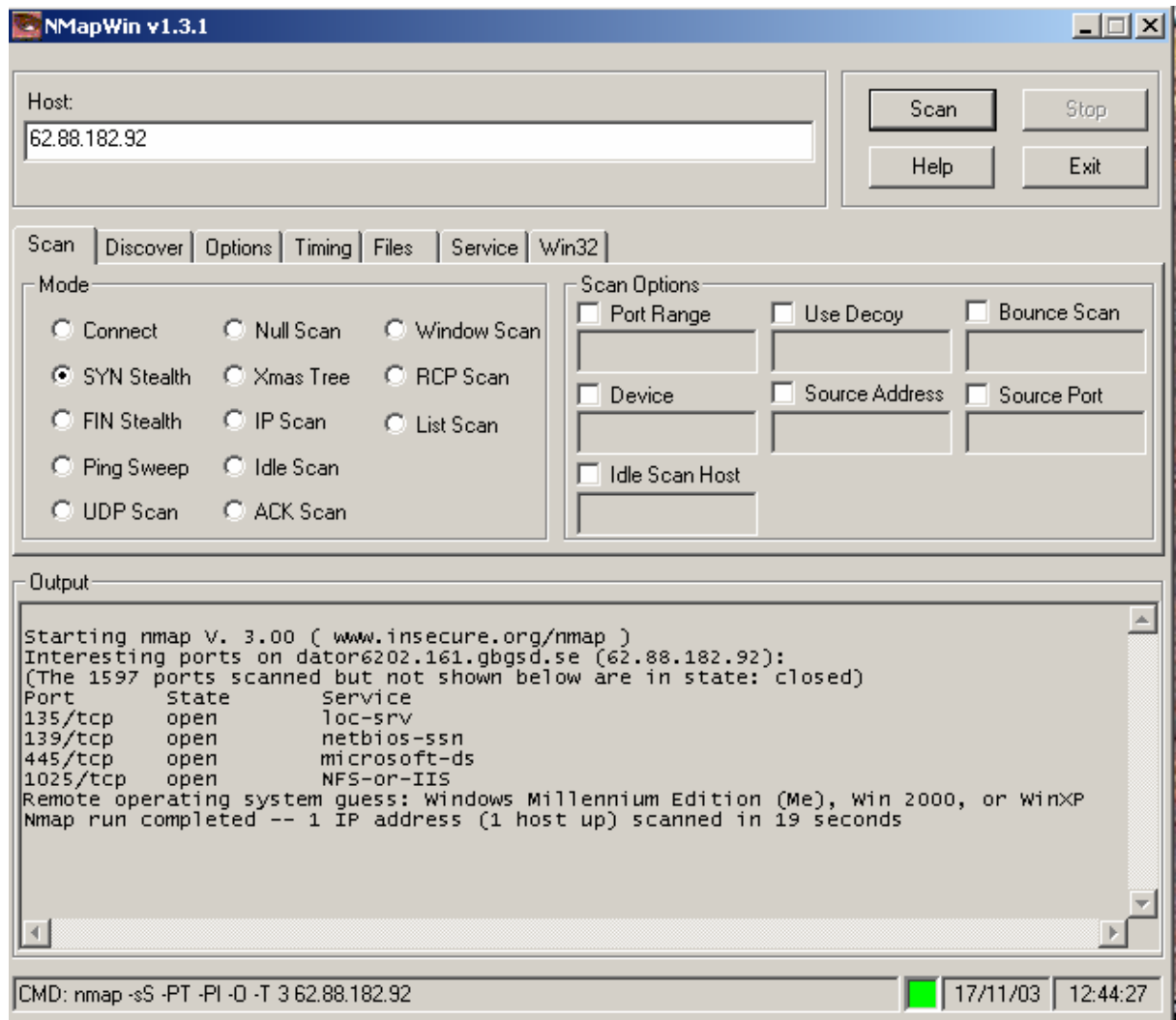
```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corporation

D:\>nmap -sS -PT -PI -O -v -T 3 62.88.181.34

Starting nmap U. 3.00 ( www.insecure.org/nmap )
Host dator5889.161.gbgsd.se (62.88.181.34) appears to be up ... good.
Initiating SYN Stealth Scan against dator5889.161.gbgsd.se (62.88.181.34)
Adding open port 135/tcp
Adding open port 139/tcp
Adding open port 445/tcp
Adding open port 1025/tcp
The SYN Stealth Scan took 3 seconds to scan 1601 ports.
For OSScan assuming that port 135 is open and port 1 is closed and neither are f
irewalled
Interesting ports on dator5889.161.gbgsd.se (62.88.181.34):
(The 1597 ports scanned but not shown below are in state: closed)
Port      State      Service
135/tcp   open       loc-srv
139/tcp   open       netbios-ssn
445/tcp   open       microsoft-ds
1025/tcp  open       NFS-or-IIS
Remote operating system guess: Windows Millennium Edition (Me), Win 2000, or Win
XP
TCP Sequence Prediction: Class=random positive increments
                          Difficulty=13252 (Worthy challenge)
IPID Sequence Generation: Incremental

Nmap run completed -- 1 IP address (1 host up) scanned in 4 seconds

D:\>_
```



## Fin Steal th

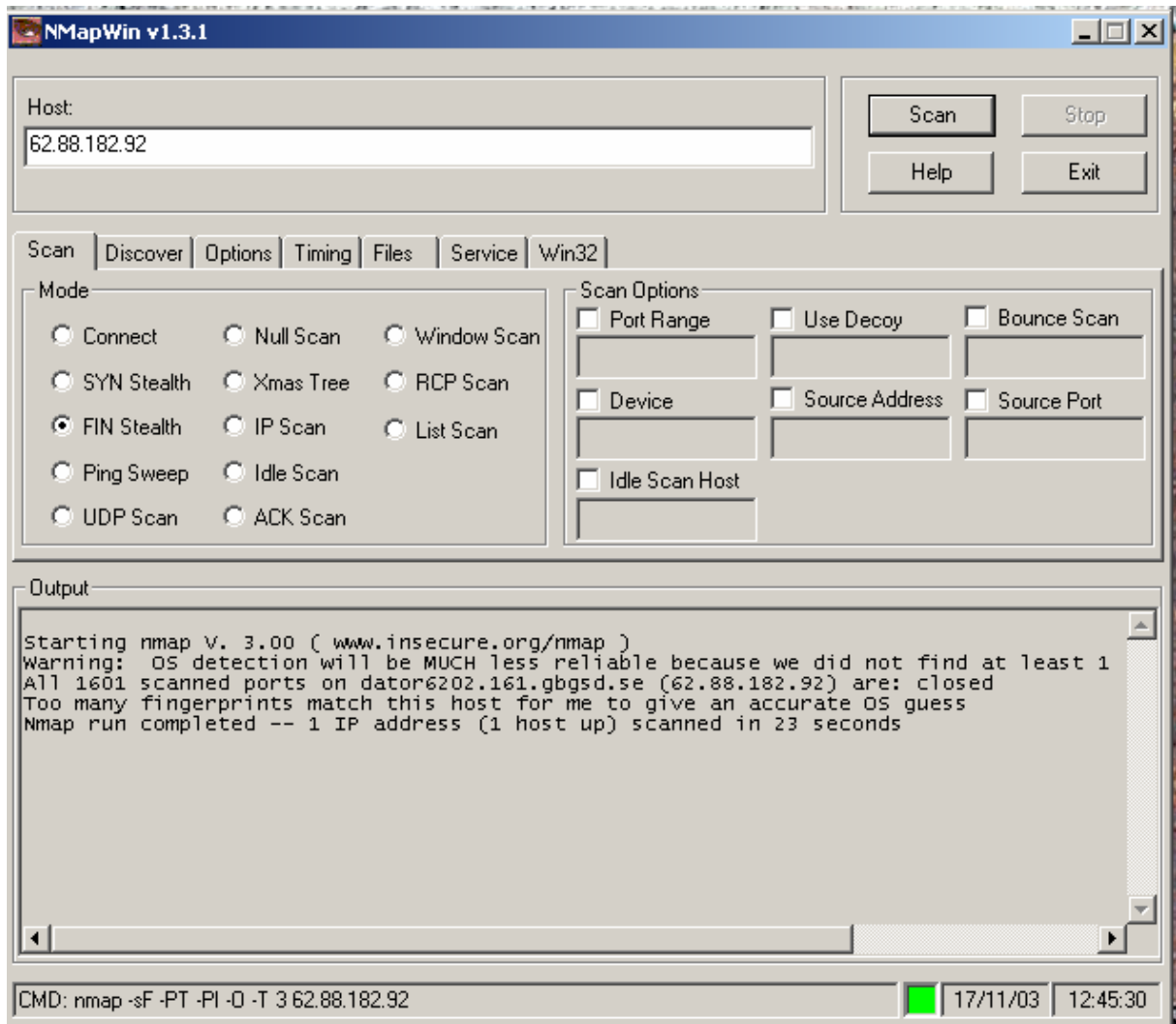
```
Microsoft Windows [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corporation

D:\>nmap -sF -PI -PI -O -v -T 3 62.88.181.34

Starting nmap U. 3.00 < www.insecure.org/nmap >
Host dator5889.161.gbgsd.se (62.88.181.34) appears to be up ... good.
Initiating FIN Scan against dator5889.161.gbgsd.se (62.88.181.34)
The FIN Scan took 4 seconds to scan 1601 ports.
Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1
closed TCP port
All 1601 scanned ports on dator5889.161.gbgsd.se (62.88.181.34) are: closed
Too many fingerprints match this host for me to give an accurate OS guess
TCP/IP fingerprint:
$Info(U=3.00%P=1686-pc-windows-windows%D=12/4%Time=3FCF2A06%O=-1%C=1)
T5<Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=>
T6<Resp=Y%DF=N%W=0%ACK=0%Flags=R%Ops=>
T7<Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=>
PU<Resp=Y%DF=N%IOS=0%IPLEN=38%RIPTL=148%RIPCK=E%UCK=E%ULEN=134%DAT=E>

Nmap run completed -- 1 IP address (1 host up) scanned in 8 seconds

D:\>_
```



## Ping Sweep

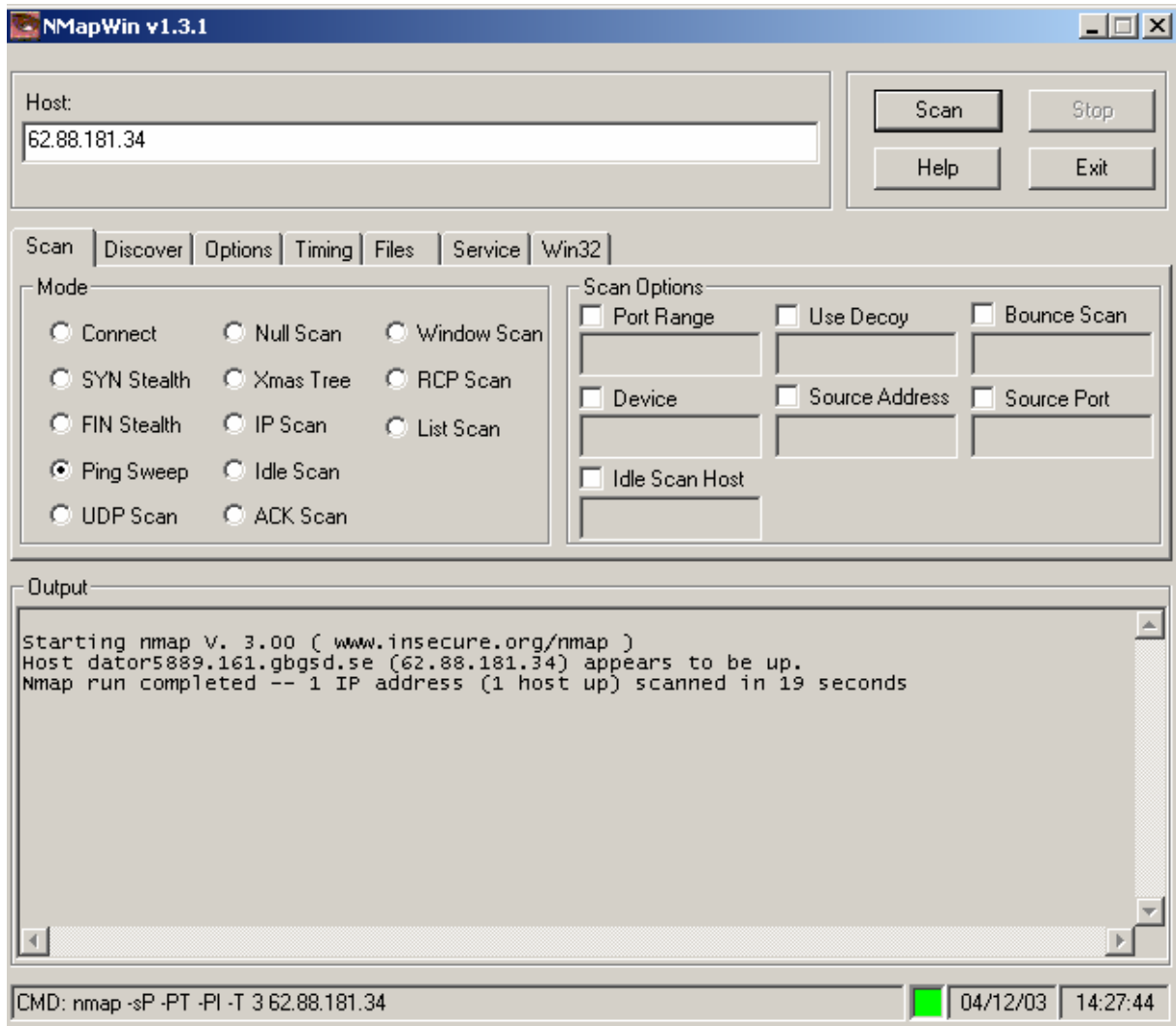
```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corporation

D:\>nmap sP -PT -PI -O -v -T 3 62.88.181.34

Starting nmap V. 3.00 ( www.insecure.org/nmap )
No tcp,udp, or ICMP scantype specified, assuming SYN Stealth scan. Use -sP if you really
want to portscan (and just want to see what hosts are up).
Failed to resolve given hostname/IP: sP. Note that you can't use '/mask' AND '[1-4,7,10]
le IP ranges
Host dator5889.161.gbgsd.se (62.88.181.34) appears to be up ... good.
Initiating SYN Stealth Scan against dator5889.161.gbgsd.se (62.88.181.34)
Adding open port 445/tcp
Adding open port 1025/tcp
Adding open port 139/tcp
Adding open port 135/tcp
The SYN Stealth Scan took 4 seconds to scan 1601 ports.
For OSScan assuming that port 135 is open and port 1 is closed and neither are firewalls
Interesting ports on dator5889.161.gbgsd.se (62.88.181.34):
(The 1597 ports scanned but not shown below are in state: closed)
Port      State      Service
135/tcp   open       loc-srv
139/tcp   open       netbios-ssn
445/tcp   open       microsoft-ds
1025/tcp  open       NFS-or-IIS
Remote operating system guess: Windows Millennium Edition (Me), Win 2000, or WinXP
TCP Sequence Prediction: Class=random positive increments
                        Difficulty=9733 (Worthy challenge)
IPID Sequence Generation: Incremental

Nmap run completed -- 1 IP address (1 host up) scanned in 6 seconds

D:\>
```



## UDP Scan

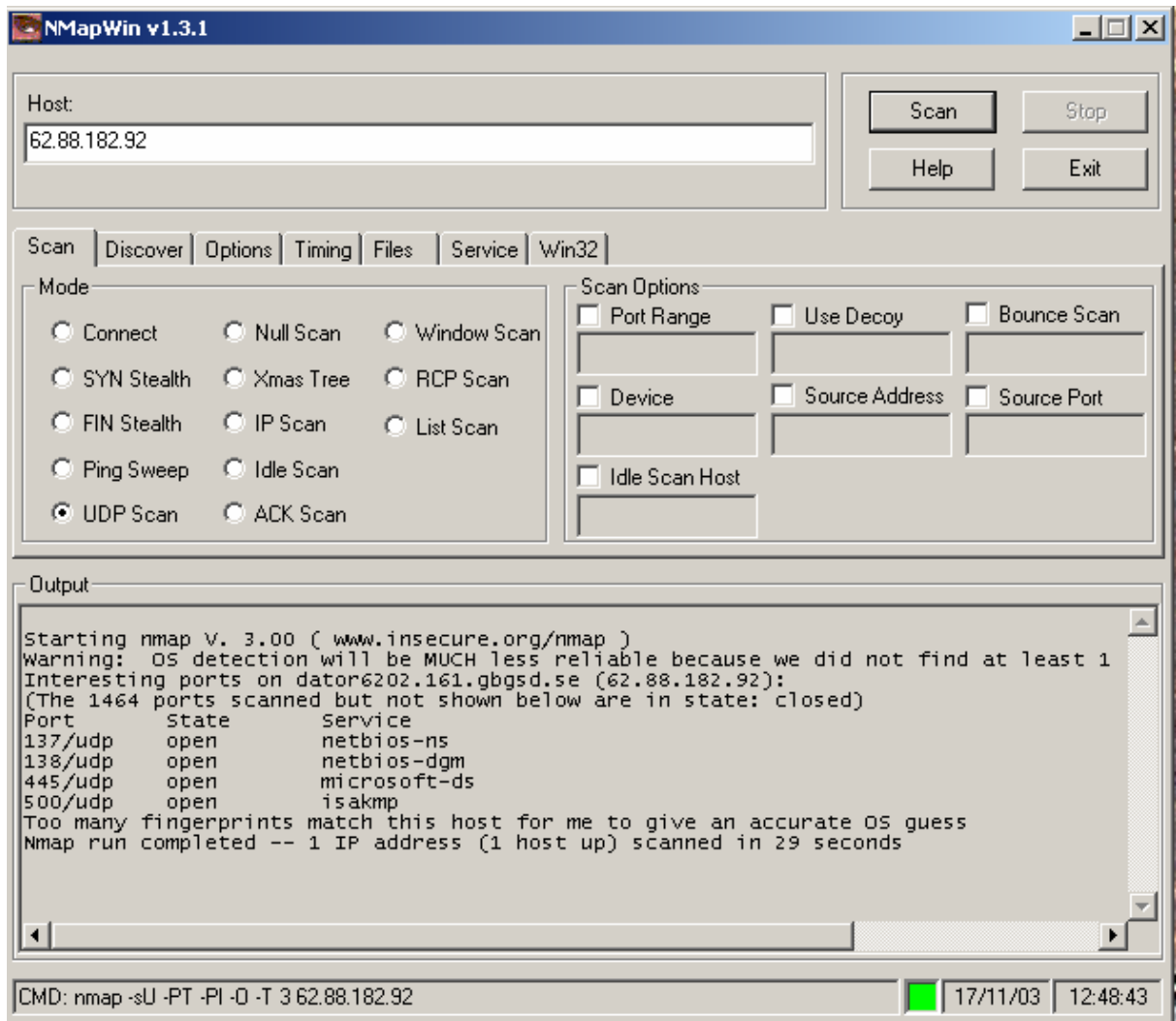
```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corporation

D:\>nmap sU -PT -PI -O -v -T 3 62.88.181.34

Starting nmap U. 3.00 ( www.insecure.org/nmap )
No tcp,udp, or ICMP scantype specified, assuming SYN Stealth scan. Use -sP if you really do
ant to portscan (and just want to see what hosts are up).
Failed to resolve given hostname/IP: sU. Note that you can't use '/mask' AND '[1-4,7,100-1
le IP ranges
Host dator5889.161.gbgsd.se (62.88.181.34) appears to be up ... good.
Initiating SYN Stealth Scan against dator5889.161.gbgsd.se (62.88.181.34)
Adding open port 139/tcp
Adding open port 1025/tcp
Adding open port 135/tcp
Adding open port 445/tcp
The SYN Stealth Scan took 3 seconds to scan 1601 ports.
For OSScan assuming that port 135 is open and port 1 is closed and neither are firewalled
Interesting ports on dator5889.161.gbgsd.se (62.88.181.34):
(The 1597 ports scanned but not shown below are in state: closed)
Port      State      Service
135/tcp   open      loc-srv
139/tcp   open      netbios-ssn
445/tcp   open      microsoft-ds
1025/tcp  open      NFS-or-IIS
Remote operating system guess: Windows Millennium Edition (Me), Win 2000, or WinXP
TCP Sequence Prediction: Class=random positive increments
                        Difficulty=7540 (Worthy challenge)
IPID Sequence Generation: Incremental

Nmap run completed -- 1 IP address (1 host up) scanned in 7 seconds

D:\>
```



## Nul I Scan

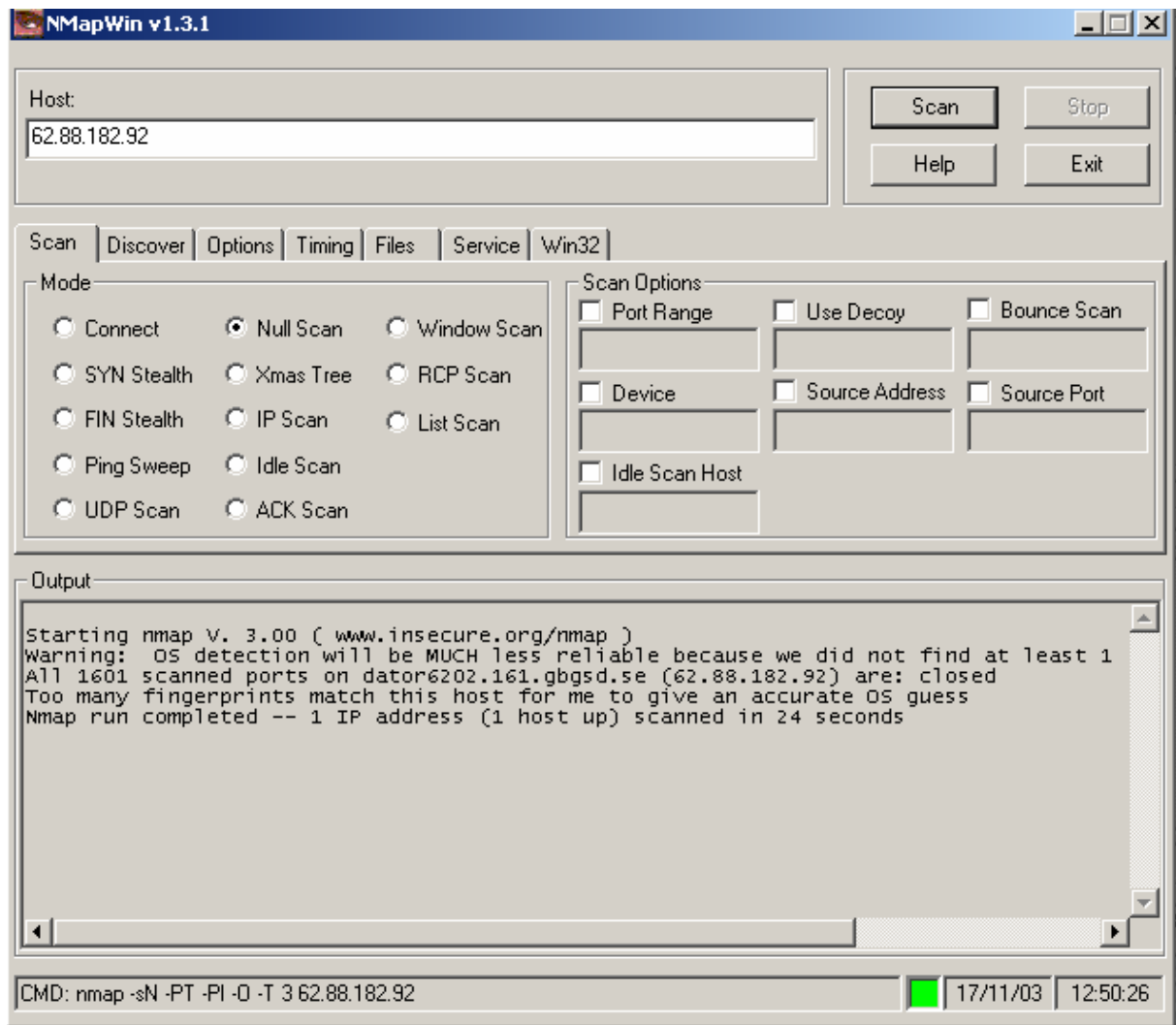
```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corporation

D:\>nmap sN -PT -PI -O -v -T 3 62.88.181.34

Starting nmap V. 3.00 ( www.insecure.org/nmap )
No tcp,udp, or ICMP scantype specified, assuming SYN Stealth scan. Use -sP if you really
n (and just want to see what hosts are up).
Failed to resolve given hostname/IP: sN. Note that you can't use '/mask' AND '[1-4,7,1
Host dator5889.161.gbgsd.se (62.88.181.34) appears to be up ... good.
Initiating SYN Stealth Scan against dator5889.161.gbgsd.se (62.88.181.34)
Adding open port 135/tcp
Adding open port 139/tcp
Adding open port 1025/tcp
Adding open port 445/tcp
The SYN Stealth Scan took 3 seconds to scan 1601 ports.
For OSScan assuming that port 135 is open and port 1 is closed and neither are firewall
Interesting ports on dator5889.161.gbgsd.se (62.88.181.34):
<The 1597 ports scanned but not shown below are in state: closed>
Port      State      Service
135/tcp   open       loc-srv
139/tcp   open       nethios-ssn
445/tcp   open       microsoft-ds
1025/tcp  open       NFS-or-IIS
Remote operating system guess: Windows Millennium Edition (Me), Win 2000, or WinXP
TCP Sequence Prediction: Class=random positive increments
                        Difficulty=12252 (Worthy challenge)
IPID Sequence Generation: Incremental

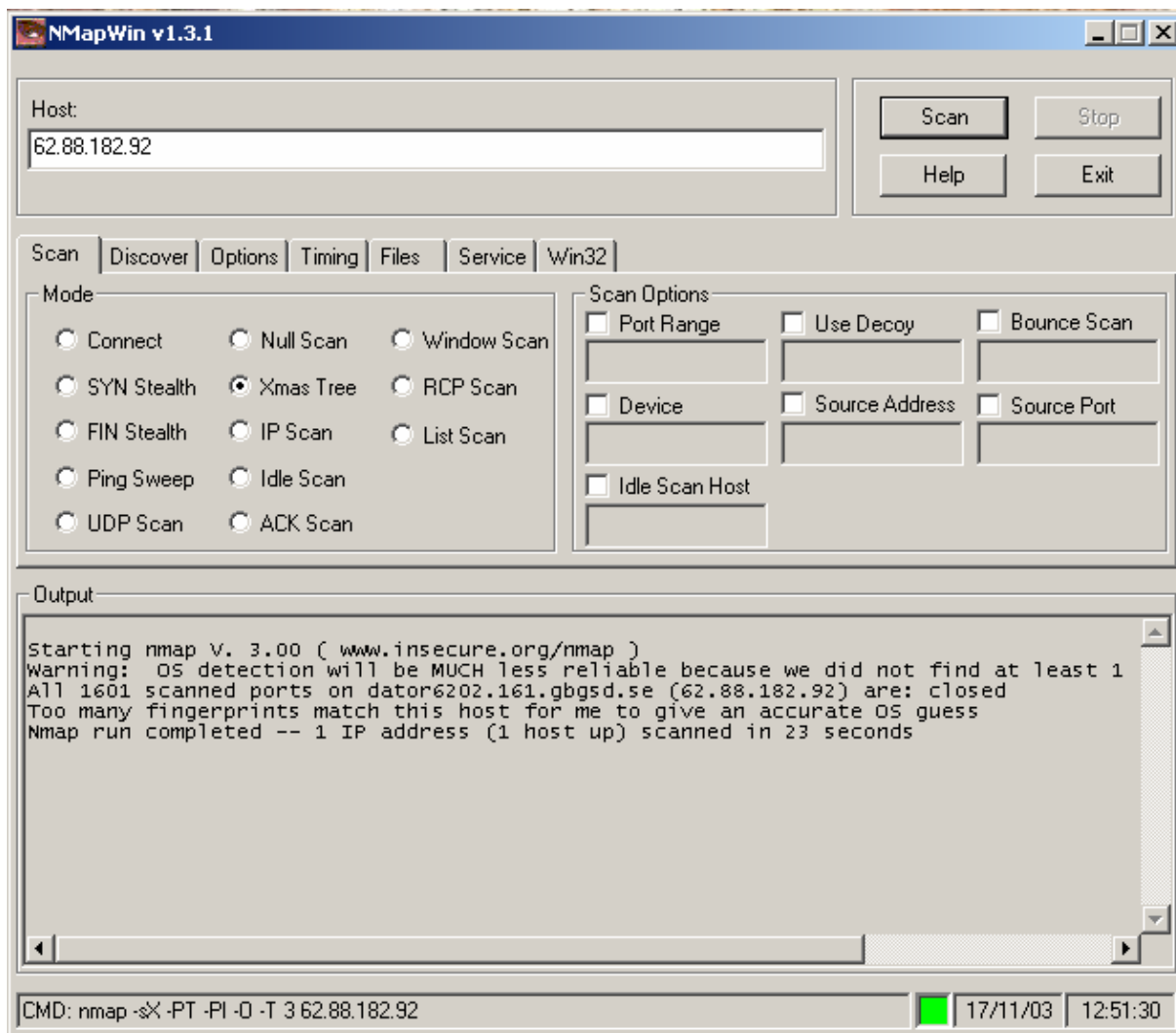
Nmap run completed -- 1 IP address (1 host up) scanned in 7 seconds

D:\>_
```



## Xmas Tree

```
(C) Copyright 1985-2000 Microsoft Corporation
D:\>nmap sX -PT -PI -O -v -T 3 62.88.181.34
Starting nmap U. 3.00 ( www.insecure.org/nmap )
No tcp,udp, or ICMP scantype specified, assuming SYN Stealth scan. Use -sP if you really
n (and just want to see what hosts are up).
Failed to resolve given hostname/IP: sX. Note that you can't use '/mask' AND '[1-4,7,10
Host dator5889.161.gbgsd.se (62.88.181.34) appears to be up ... good.
Initiating SYN Stealth Scan against dator5889.161.gbgsd.se (62.88.181.34)
Adding open port 135/tcp
Adding open port 445/tcp
Adding open port 139/tcp
Adding open port 1025/tcp
The SYN Stealth Scan took 3 seconds to scan 1601 ports.
For OSScan assuming that port 135 is open and port 1 is closed and neither are firewall
Interesting ports on dator5889.161.gbgsd.se (62.88.181.34):
<The 1597 ports scanned but not shown below are in state: closed>
Port      State      Service
135/tcp   open      loc-srv
139/tcp   open      netbios-ssn
445/tcp   open      microsoft-ds
1025/tcp  open      NFS-or-IIS
Remote operating system guess: Windows Millennium Edition (Me), Win 2000, or WinXP
TCP Sequence Prediction: Class=random positive increments
                          Difficulty=9274 (Worthy challenge)
IPID Sequence Generation: Incremental
Nmap run completed -- 1 IP address (1 host up) scanned in 6 seconds
D:\>
```



## IP Scan

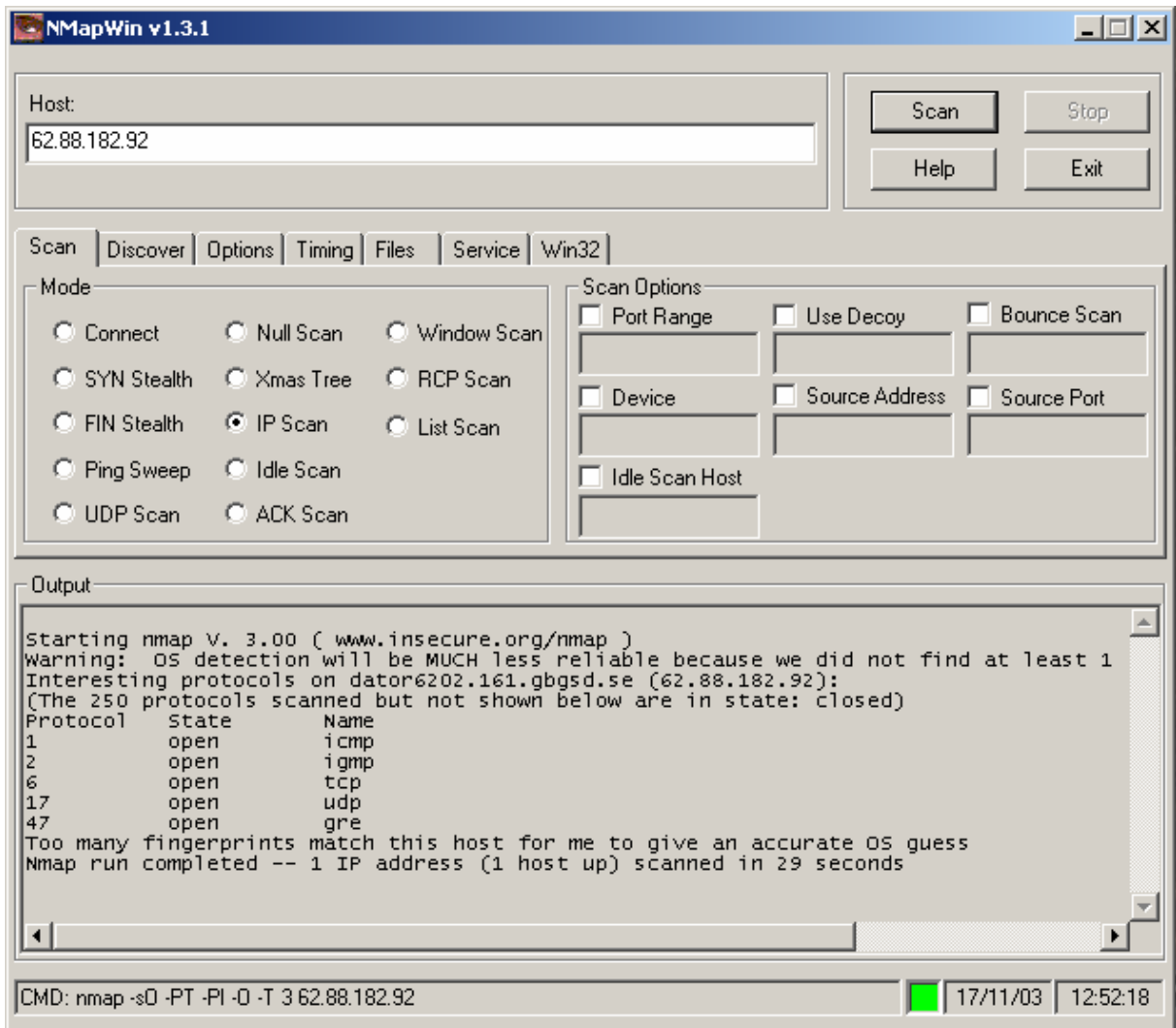
```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corporation

D:\>nmap s0 -PT -PI -O -v -T 3 62.88.181.34

Starting nmap V. 3.00 ( www.insecure.org/nmap )
No tcp,udp, or ICMP scantype specified, assuming SYN Stealth scan. Use -sP if you really
n (and just want to see what hosts are up).
Failed to resolve given hostname/IP: s0. Note that you can't use '/mask' AND '[1-4,7,10
Host dator5889.161.gbgsd.se (62.88.181.34) appears to be up ... good.
Initiating SYN Stealth Scan against dator5889.161.gbgsd.se (62.88.181.34)
Adding open port 445/tcp
Adding open port 139/tcp
Adding open port 1025/tcp
Adding open port 135/tcp
The SYN Stealth Scan took 3 seconds to scan 1601 ports.
For OSScan assuming that port 135 is open and port 1 is closed and neither are firewall
Interesting ports on dator5889.161.gbgsd.se (62.88.181.34):
(The 1597 ports scanned but not shown below are in state: closed)
Port      State      Service
135/tcp   open      loc-srv
139/tcp   open      netbios-ssn
445/tcp   open      microsoft-ds
1025/tcp  open      NFS-or-IIS
Remote operating system guess: Windows Millennium Edition (Me), Win 2000, or WinXP
TCP Sequence Prediction: Class=random positive increments
                        Difficulty=13798 (Worthy challenge)
IPID Sequence Generation: Incremental

Nmap run completed -- 1 IP address (1 host up) scanned in 6 seconds

D:\>_
```



## Idle Scan

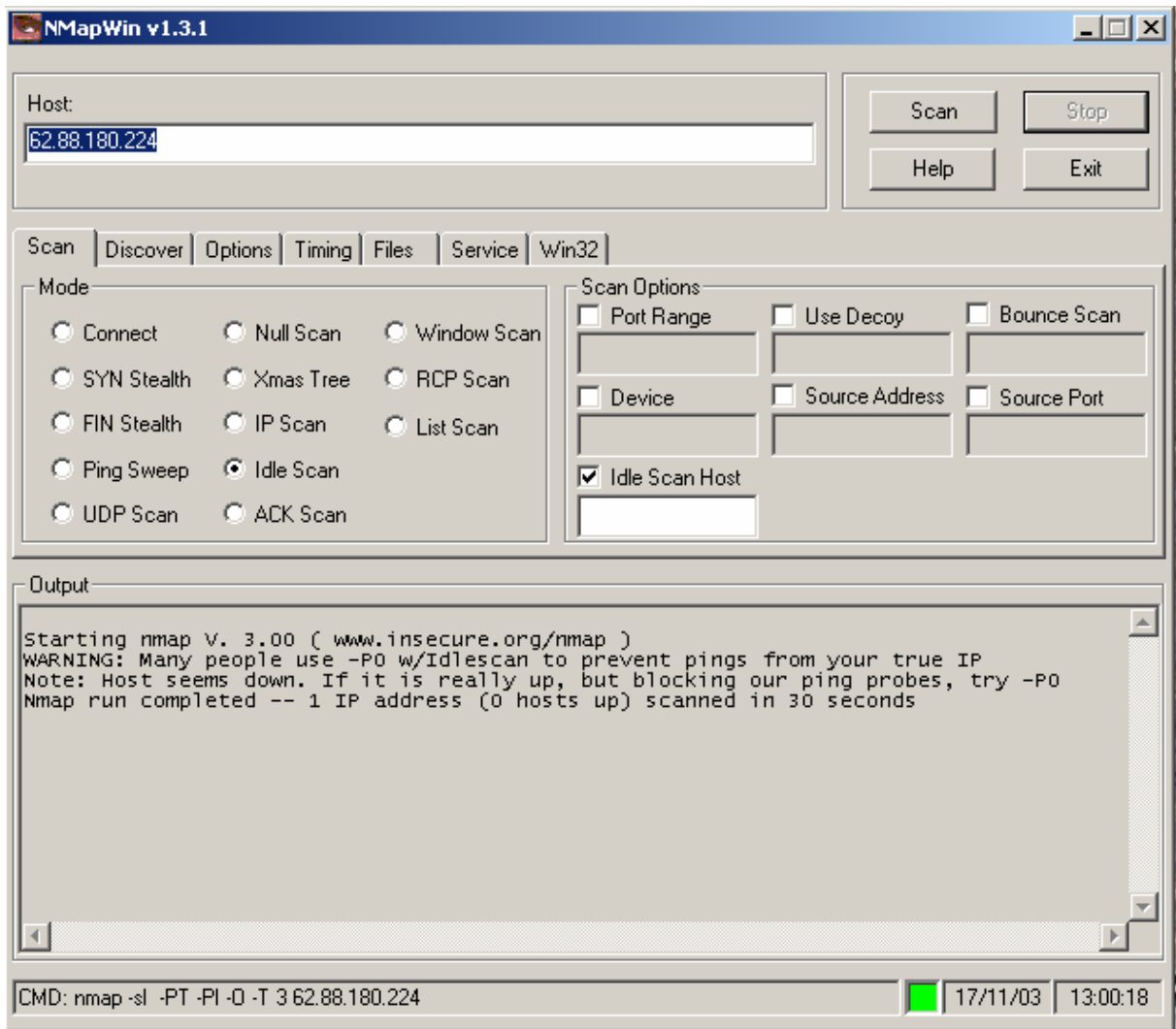
```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corporation

D:\>nmap sI -PT -PI -O -v -T 3 62.88.181.34

Starting nmap V. 3.00 ( www.insecure.org/nmap )
No tcp,udp, or ICMP scantype specified, assuming SYN Stealth scan. Use -sP if you really
n (and just want to see what hosts are up).
Failed to resolve given hostname/IP: sI. Note that you can't use '/mask' AND '[1-4,7,1
Host dator5889.161.gbgsd.se (62.88.181.34) appears to be up ... good.
Initiating SYN Stealth Scan against dator5889.161.gbgsd.se (62.88.181.34)
Adding open port 1025/tcp
Adding open port 135/tcp
Adding open port 139/tcp
Adding open port 445/tcp
The SYN Stealth Scan took 4 seconds to scan 1601 ports.
For OSScan assuming that port 135 is open and port 1 is closed and neither are firewall
Interesting ports on dator5889.161.gbgsd.se (62.88.181.34):
(The 1597 ports scanned but not shown below are in state: closed)
Port      State      Service
135/tcp   open       loc-srv
139/tcp   open       netbios-ssn
445/tcp   open       microsoft-ds
1025/tcp  open       NFS-or-IIS
Remote operating system guess: Windows Millennium Edition (Me), Win 2000, or WinXP
TCP Sequence Prediction: Class=random positive increments
                        Difficulty=6676 (Worthy challenge)
IPID Sequence Generation: Incremental

Nmap run completed -- 1 IP address (1 host up) scanned in 7 seconds

D:\>
```



## ACK Scan

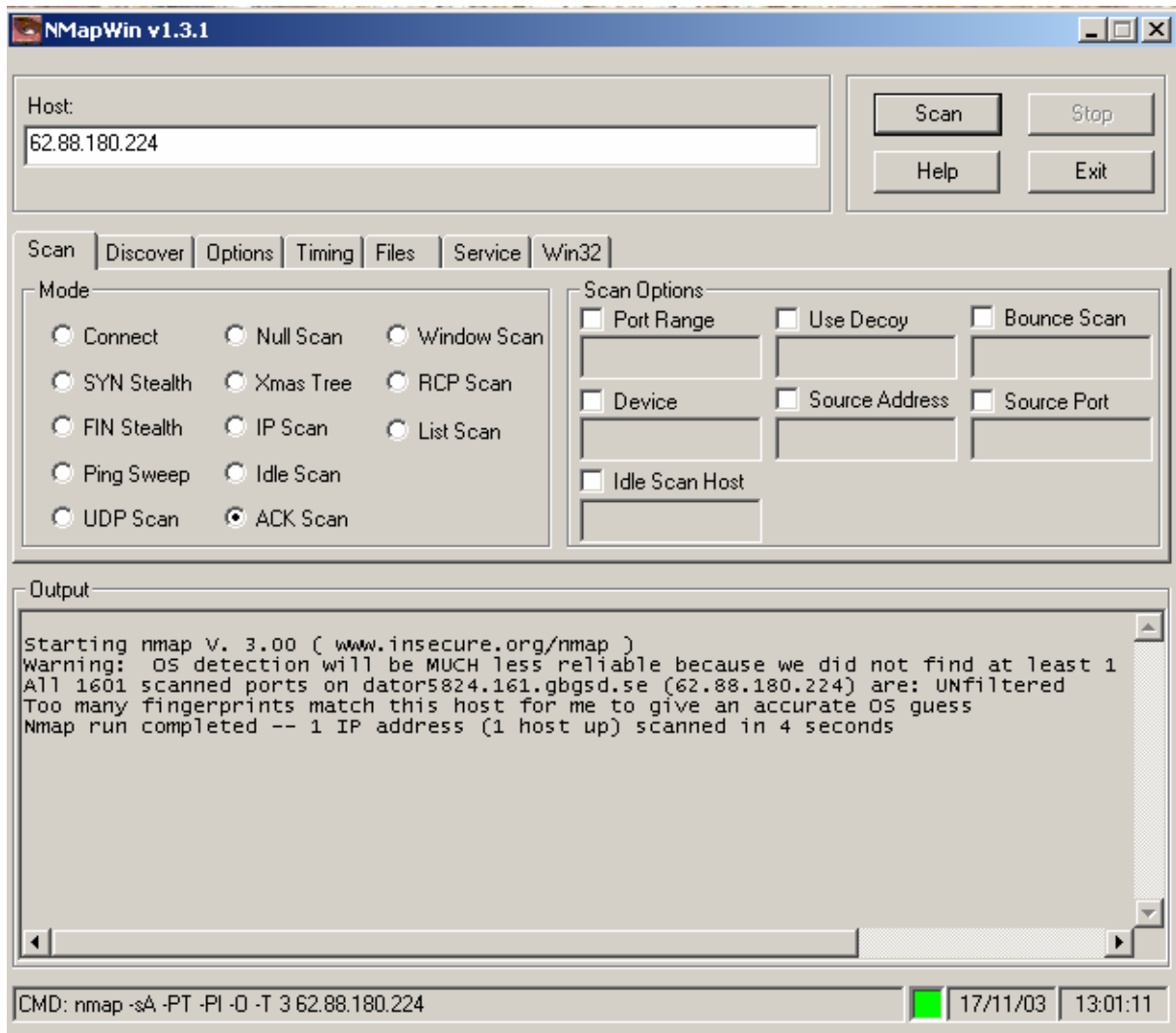
```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corporation

D:\>nmap -sA -PT -PI -O -v -T 3 62.88.181.34

Starting nmap V. 3.00 ( www.insecure.org/nmap )
Host dator5889.161.gbgsd.se (62.88.181.34) appears to be up ... good.
Initiating ACK Scan against dator5889.161.gbgsd.se (62.88.181.34)
The ACK Scan took 3 seconds to scan 1601 ports.
Warning: OS detection will be MUCH less reliable because we did not find at least 1 open port
All 1601 scanned ports on dator5889.161.gbgsd.se (62.88.181.34) are: UNfiltered
Too many fingerprints match this host for me to give an accurate OS guess
TCP/IP fingerprint:
SInfo(U=3.00%P=i686-pc-windows-windows%D=12/4%Time=3FCF3158%O=-1%C=-1)
T5(Resp=Y%DF=N%W=0%ACK=S+%Flags=AR%Ops=)
T6(Resp=Y%DF=N%W=0%ACK=0%Flags=R%Ops=)
T7(Resp=Y%DF=N%W=0%ACK=S+%Flags=AR%Ops=)
PU(Resp=Y%DF=N%TOS=0%IPLen=38%RIPTL=148%RIPCK=E%UCK=E%ULEN=134%DAT=E)

Nmap run completed -- 1 IP address (1 host up) scanned in 8 seconds

D:\>_
```



## Window Scan

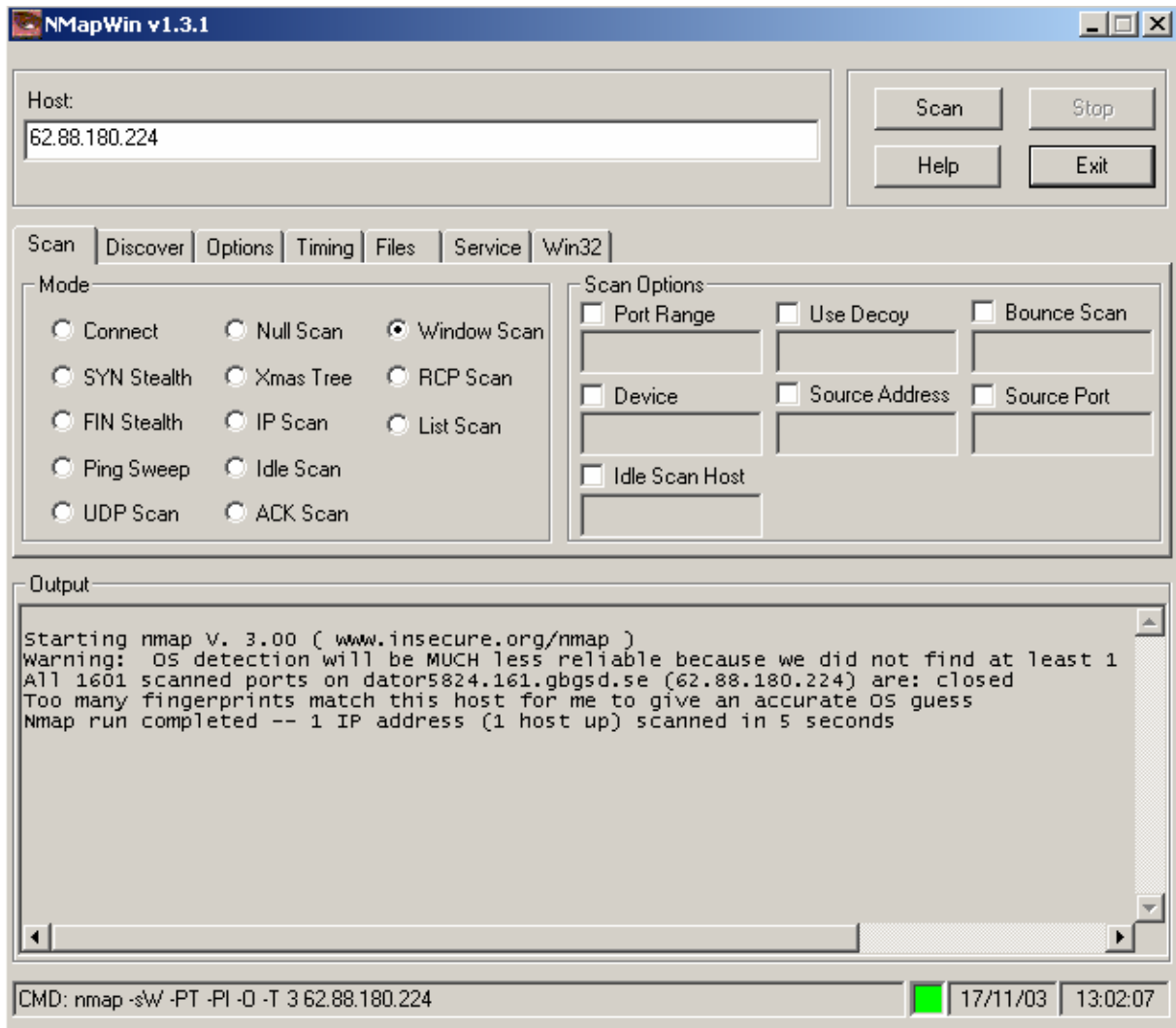
```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corporation

D:\>nmap sW -PT -PI -O -v -T 3 62.88.181.34

Starting nmap V. 3.00 ( www.insecure.org/nmap )
No tcp,udp, or ICMP scantype specified, assuming SYN Stealth scan. Use -sP if you really
n (and just want to see what hosts are up).
Failed to resolve given hostname/IP: sW. Note that you can't use '/mask' AND '[1-4,7,10
Host dator5889.161.gbgsd.se (62.88.181.34) appears to be up ... good.
Initiating SYN Stealth Scan against dator5889.161.gbgsd.se (62.88.181.34)
Adding open port 135/tcp
Adding open port 445/tcp
Adding open port 1025/tcp
Adding open port 139/tcp
The SYN Stealth Scan took 0 seconds to scan 1601 ports.
For OSScan assuming that port 135 is open and port 1 is closed and neither are firewall
Interesting ports on dator5889.161.gbgsd.se (62.88.181.34):
(The 1597 ports scanned but not shown below are in state: closed)
Port      State      Service
135/tcp   open      loc-srv
139/tcp   open      netbios-ssn
445/tcp   open      microsoft-ds
1025/tcp  open      NFS-or-IIS
Remote operating system guess: Windows Millennium Edition (Me), Win 2000, or WinXP
TCP Sequence Prediction: Class=random positive increments
                          Difficulty=10915 (Worthy challenge)
IPID Sequence Generation: Incremental

Nmap run completed -- 1 IP address (1 host up) scanned in 4 seconds

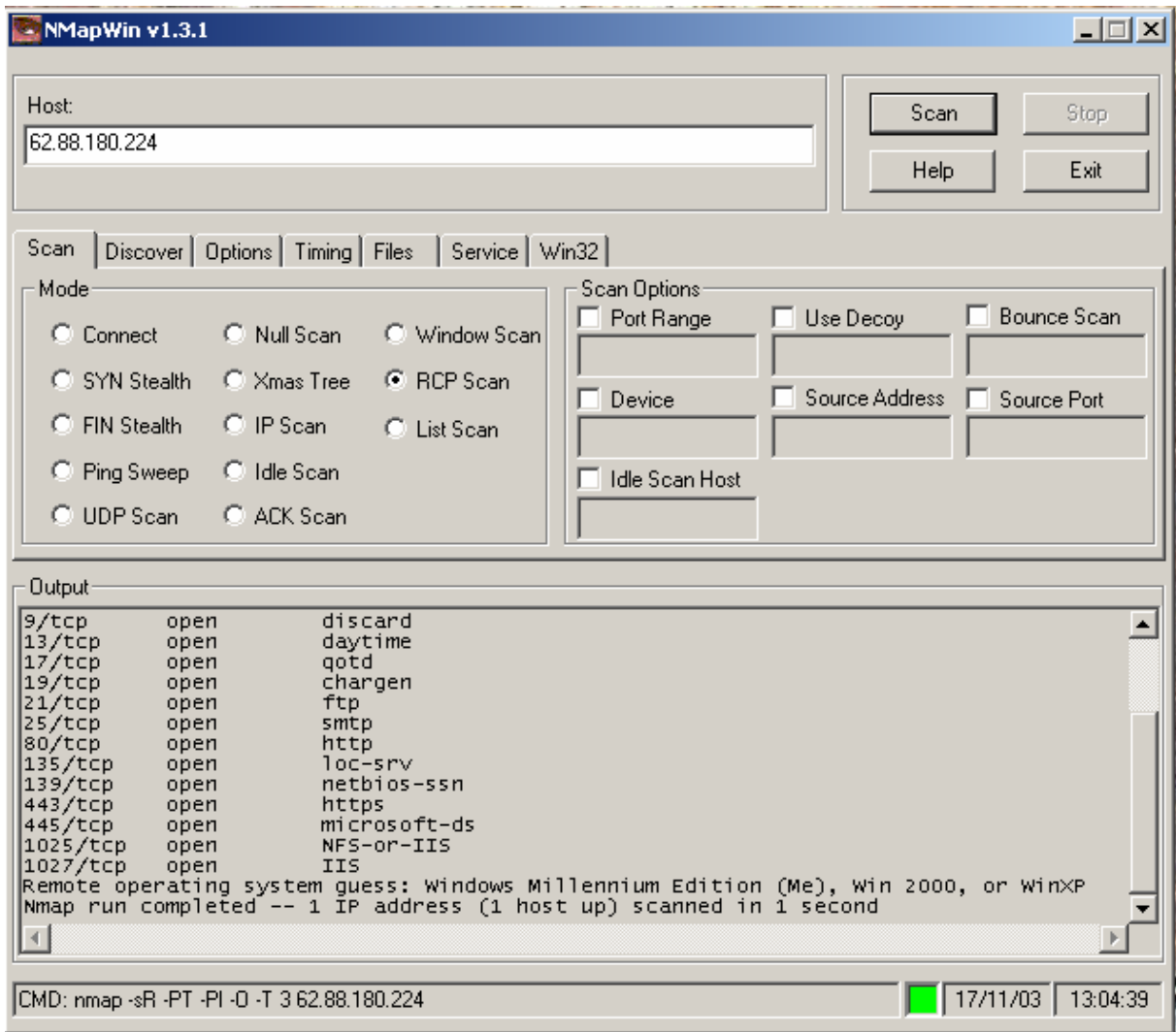
D:\>_
```



## RCP Scan

```
Starting nmap U. 3.00 ( www.insecure.org/nmap )
No tcp,udp, or ICMP scantype specified, assuming SYN Stealth scan. Use -sP if you really
n (and just want to see what hosts are up).
Host dator5889.161.gbgsd.se (62.88.181.34) appears to be up ... good.
Initiating SYN Stealth Scan against dator5889.161.gbgsd.se (62.88.181.34)
Adding open port 135/tcp
Adding open port 139/tcp
Adding open port 1025/tcp
Adding open port 445/tcp
The SYN Stealth Scan took 0 seconds to scan 1601 ports.
Initiating RPCGrind Scan against dator5889.161.gbgsd.se (62.88.181.34)
The RPCGrind Scan took 0 seconds to scan 0 ports.
For OSScan assuming that port 135 is open and port 1 is closed and neither are firewall
Interesting ports on dator5889.161.gbgsd.se (62.88.181.34):
<The 1597 ports scanned but not shown below are in state: closed>
Port      State      Service (RPC)
135/tcp   open       loc-srv
139/tcp   open       netbios-ssn
445/tcp   open       microsoft-ds
1025/tcp  open       NFS-or-IIS
Remote operating system guess: Windows Millennium Edition (Me), Win 2000, or WinXP
TCP Sequence Prediction: Class=random positive increments
                        Difficulty=8878 (Worthy challenge)
IPID Sequence Generation: Incremental

Nmap run completed -- 1 IP address (1 host up) scanned in 1 second
D:\>
```



## List Scan

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corporation

D:\>nmap sL -PT -PI -O -v -T 3 62.88.181.34

Starting nmap V. 3.00 ( www.insecure.org/nmap )
No tcp,udp, or ICMP scantype specified, assuming SYN Stealth scan. Use -sP if you really
n (and just want to see what hosts are up).
Failed to resolve given hostname/IP: sL. Note that you can't use '/mask' AND '[1-4,7,10
Host dator5889.161.gbgsd.se (62.88.181.34) appears to be up ... good.
Initiating SYN Stealth Scan against dator5889.161.gbgsd.se (62.88.181.34)
Adding open port 139/tcp
Adding open port 1025/tcp
Adding open port 135/tcp
Adding open port 445/tcp
The SYN Stealth Scan took 0 seconds to scan 1601 ports.
For OSScan assuming that port 135 is open and port 1 is closed and neither are firewall
Interesting ports on dator5889.161.gbgsd.se (62.88.181.34):
(The 1597 ports scanned but not shown below are in state: closed)
Port      State      Service
135/tcp   open       loc-srv
139/tcp   open       netbios-ssn
445/tcp   open       microsoft-ds
1025/tcp  open       NFS-or-IIS
Remote operating system guess: Windows Millennium Edition (Me), Win 2000, or WinXP
TCP Sequence Prediction: Class=random positive increments
                        Difficulty=7116 (Worthy challenge)
IPID Sequence Generation: Incremental

Nmap run completed -- 1 IP address (1 host up) scanned in 4 seconds

D:\>
```

