

Nmap Scan durch die einzelnen Subnetze

```
bash-2.05a$ nmap -sP 172.16.0.*
```

```
Starting nmap V. 2.54BETA31 (
www.insecure.org/nmap/ )
Machine 172.16.0.2 MIGHT actually be listening on
probe port 80
Host (172.16.0.2) appears to be up.
Host (172.16.0.3) appears to be up.
```

```
Nmap run completed -- 256 IP addresses (2 hosts
up) scanned in 3 seconds
```

```
bash-2.05a$ nmap -sP 192.168.0-9.*
```

```
Starting nmap V. 2.54BETA31 (
www.insecure.org/nmap/ )
Warning: You are not root -- using TCP pingscan
rather than ICMP
Host GW-herr-der-ringe.student.com (192.168.0.5)
appears to be up.
Host security.student.com (192.168.0.10) appears
to be up.
Host grishnakh.fangorn.com (192.168.1.33) appears
to be up.
Host ents.fangorn.com (192.168.1.35) appears to
be up.
Host bambart.fangorn.com (192.168.1.57) appears
to be up.
Host sam.mordor.com (192.168.2.2) appears to be
up.
Host gollum.mordor.com (192.168.2.4) appears to
be up.
Host frodo.mordor.com (192.168.2.17) appears to
be up.
Host Shelob.mordor.com (192.168.2.25) appears to
be up.
Host Celeborn.lorien.com (192.168.3.1) appears to
be up.
Host arwen.lorien.com (192.168.3.2) appears to be
up.
Host haldir.lorien.com (192.168.3.99) appears to
be up.
Host merry.hobbits.com (192.168.5.12) appears to
be up.
Host pippin.hobbits.com (192.168.5.57) appears to
be up.
```

```
Nmap run completed -- 2560 IP addresses (14 hosts
up) scanned in 32 seconds
```

```
bash-2.05a$ nmap -sP 10.0.0.*
```

```
Starting nmap V. 2.54BETA31 (
www.insecure.org/nmap/ )
Warning: You are not root -- using TCP pingscan
rather than ICMP
Host gandalf.wizards.com (10.0.0.1) appears to
be up.
Host saruman.wizards.com (10.0.0.2) appears to
be up.
Host sauron.wizards.com (10.0.0.3) appears to be
up.
Host galadriel.com.wizards.com (10.0.0.4)
appears to be up.
Host (10.0.0.10) appears to be up.
Host radagast.wizards.com (10.0.0.100) appears
to be up.
```

```
Nmap run completed -- 256 IP addresses (6 hosts
up) scanned in 3 seconds
```

Portscans bei den einzelnen Rechnern

```
bash-2.05a$ nmap 172.16.0.2
```

```
Interesting ports on (172.16.0.2):
(The 1551 ports scanned but not shown below are
in state: closed)
Port      State      Service
21/tcp    open       ftp
25/tcp    open       smtp
80/tcp    open       http
```

LINUX Rechner weil:

```
Server: Apache/1.3.12 (Unix) (Red Hat/Linux) mod_ssl/2.6.6
OpenSSL/0.9.5a mod_perl/1.24
```

```
bash-2.05a$ nmap 172.16.0.3
```

```
Interesting ports on (172.16.0.3):
(The 1552 ports scanned but not shown below are
in state: closed)
Port      State      Service
23/tcp    open       telnet
25/tcp    open       smtp
```

LINUX Rechner, weil Sendmail nur auf Unix-Plattformen verfügbar ist

```
Interesting ports on GW-herr-der-
ringe.student.com (192.168.0.5):
(The 1550 ports scanned but not shown below are
in state: closed)
Port      State      Service
22/tcp    open       ssh
53/tcp    open       domain
111/tcp   open       sunrpc
1024/tcp  open       kdm
```

LINUX, weil KDM ist ein Unix Display Manager

```
Interesting ports on security.student.com
(192.168.0.10):
(The 1553 ports scanned but not shown below are
in state: closed)
Port      State      Service
22/tcp    open       ssh
```

Vermutlich Linux, wegen Openssh

```
Interesting ports on grishnakh.fangorn.com
(192.168.1.33):
(The 1552 ports scanned but not shown below are
in state: closed)
Port      State      Service
22/tcp    open       ssh
443/tcp   open       https
```

Linux?

```
Interesting ports on ents.fangorn.com
(192.168.1.35):
(The 1552 ports scanned but not shown below are
in state: closed)
Port      State      Service
22/tcp    open       ssh
3306/tcp  open       mysql
```

Linux?

```

1024/tcp open kdm

Interesting ports on bambart.fangorn.com (192.168.1.57):
(The 1551 ports scanned but not shown below are in state: closed)
Port      State  Service
22/tcp    open  ssh
111/tcp   open  sunrpc
1024/tcp  open  kdm

Linux wegen KDM

Interesting ports on sam.mordor.com (192.168.2.2):
(The 1552 ports scanned but not shown below are in state: closed)
Port      State  Service
23/tcp    open  telnet
515/tcp   open  printer

??

Interesting ports on gollum.mordor.com (192.168.2.4):
(The 1549 ports scanned but not shown below are in state: closed)
Port      State  Service
23/tcp    open  telnet
135/tcp   open  loc-srv
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1025/tcp  open  listen

Windows Rechner

Interesting ports on frodo.mordor.com (192.168.2.17):
(The 1551 ports scanned but not shown below are in state: closed)
Port      State  Service
22/tcp    open  ssh
111/tcp   open  sunrpc
1024/tcp  open  kdm

Linux wegen KDM

Starting nmap V. 2.54BETA31 (
www.insecure.org/nmap/ )
Interesting ports on shelob.mordor.com (192.168.2.25):
(The 1550 ports scanned but not shown below are in state: closed)
Port      State  Service
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
3128/tcp  open  squid-http

Linux weil:
Server: Apache/1.3.23 (Unix) (Red-Hat/Linux) mod_ssl/2.8.7
OpenSSL/0.9.6b DAV/1.0.3 PHP/4.1.2 mod_perl/1.26
Server: Squid/2.4.STABLE6

Interesting ports on celebrorn.lorien.com (192.168.3.1):
(The 1551 ports scanned but not shown below are in state: closed)
Port      State  Service
22/tcp    open  ssh
111/tcp   open  sunrpc

1024/tcp  open  kdm

Linux wegen KDM

Interesting ports on arwen.lorien.com (192.168.3.2):
(The 1549 ports scanned but not shown below are in state: closed)
Port      State  Service
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
80/tcp    open  http

Linux weil Sendmail und weil:
Server: Apache/1.3.12 (Unix) (Red Hat/Linux) mod_ssl/2.6.6
OpenSSL/0.9.5a mod_perl/1.24

Interesting ports on haldir.lorien.com (192.168.3.99):
(The 1549 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  listen
1031/tcp  open  iad2

Windows!

Interesting ports on merry.hobbits.com (192.168.5.12):
(The 1544 ports scanned but not shown below are in state: closed)
Port      State  Service
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
79/tcp    open  finger
111/tcp   open  sunrpc
513/tcp   open  login
514/tcp   open  shell
587/tcp   open  submission
1024/tcp  open  kdm

Linux

Interesting ports on pippin.hobbits.com (192.168.5.57):
(The 1551 ports scanned but not shown below are in state: closed)
Port      State  Service
22/tcp    open  ssh
111/tcp   open  sunrpc
1024/tcp  open  kdm

Linux wegen KDM

Interesting ports on gandalf.wizards.com (10.0.0.1):
(The 1550 ports scanned but not shown below are in state: closed)
Port      State  Service
22/tcp    open  ssh
53/tcp    open  domain
111/tcp   open  sunrpc
1024/tcp  open  kdm

Linux wegen KDM

```

```
Interesting ports on saruman.wizards.com
(10.0.0.2):
(The 1551 ports scanned but not shown below are
in state: closed)
Port      State  Service
22/tcp    open  ssh
111/tcp   open  sunrpc
1024/tcp  open  kdm
```

Linux wegen KDM

```
Interesting ports on sauron.wizards.com
(10.0.0.3):
(The 1551 ports scanned but not shown below are
in state: closed)
Port      State  Service
22/tcp    open  ssh
111/tcp   open  sunrpc
1024/tcp  open  kdm
```

Linux wegen KDM

```
Interesting ports on galadriel.com.wizards.com
(10.0.0.4):
(The 1551 ports scanned but not shown below are
in state: closed)
Port      State  Service
22/tcp    open  ssh
111/tcp   open  sunrpc
1024/tcp  open  kdm
```

Linux wegen KDM

```
Interesting ports on (10.0.0.10):
(The 1552 ports scanned but not shown below are
in state: closed)
Port      State  Service
22/tcp    open  ssh
1241/tcp  open  msg
```

unser Nessus server → Linux

```
Interesting ports on radagast.wizards.com
(10.0.0.100):
(The 1551 ports scanned but not shown below are
in state: closed)
Port      State  Service
22/tcp    open  ssh
111/tcp   open  sunrpc
1024/tcp  open  kdm
```

Linux wegen KDM

Firewalk Scan auf Host 172.16.0.2

```
bash-2.05a$ firewalk-sec 192.168.3.2 172.16.0.2
Firewalk Interface for Security VU
SET Modus = restricted DONE

Firewalk 5.0 [gateway ACL scanner]
Firewalk state initialization completed
successfully.
TCP-based scan.
Ramping phase source port: 53, destination port:
33434
Hotfoot through 192.168.3.2 using 172.16.0.2 as a
metric.
Ramping Phase:
```

```
1 (TTL 1): expired [192.168.0.5]
2 (TTL 2): expired [10.0.0.100]
3 (TTL 3): expired [10.0.0.4]
4 (TTL 4): expired [192.168.3.2]
Binding host reached.
Scan bound at 5 hops.
df
Scanning Phase:
...
port 6: unknown (unreach ICMP_UNREACH_PORT)
[192.168.3.2]
port 7: *no response*
port 21: A! open (port listen) [172.16.0.2]
port 22: unknown (unreach ICMP_UNREACH_PORT)
[192.168.3.2]
port 23: A! open (port not listen)
[172.16.0.2]
port 24: *no response*
port 25: A! open (port listen) [172.16.0.2]
port 80: A! open (port listen) [172.16.0.2]
port 220: A! open (port not listen)
[172.16.0.2]
port 389: A! open (port not listen)
[172.16.0.2]
...
port 1024: unknown (unreach
ICMP_UNREACH_PORT) [192.168.3.2]

Scan completed successfully.

Total packets sent: 1028
Total packet errors: 0
Total packets caught 699
Total packets caught of interest 694
Total ports scanned 1024
Total ports open: 6
Total ports unknown: 684
```

Firewalk Scan auf Host 172.16.0.3

```
Firewalk Interface for Security VU
SET Modus = restricted DONE

Firewalk 5.0 [gateway ACL scanner]
Firewalk state initialization completed
successfully.
TCP-based scan.
Ramping phase source port: 53, destination port:
33434
Hotfoot through 192.168.3.2 using 172.16.0.3 as a
metric.
Ramping Phase:
1 (TTL 1): expired [192.168.0.5]
2 (TTL 2): expired [10.0.0.100]
3 (TTL 3): expired [10.0.0.4]
4 (TTL 4): expired [192.168.3.2]
Binding host reached.
Scan bound at 5 hops.

Scanning Phase:
...
port 21: A! open (port not listen)
[172.16.0.3]
port 22: unknown (unreach ICMP_UNREACH_PORT)
[192.168.3.2]
port 23: A! open (port listen) [172.16.0.3]
port 24: *no response*
port 25: A! open (port listen) [172.16.0.3]
port 80: A! open (port not listen)
[172.16.0.3]
port 220: A! open (port not listen)
[172.16.0.3]
port 1024: unknown (unreach
ICMP_UNREACH_PORT) [192.168.3.2]
```

Scan completed successfully.

Total packets sent:	1028
Total packet errors:	0
Total packets caught	702
Total packets caught of interest	695
Total ports scanned	1024
Total ports open:	6
Total ports unknown:	685

Nessus Vulnerability Scan, Output in nessus_security.txt

**Traceroute Ergebnisse wurden nicht vollständig
Aufgezeichnet, die Ergebnisse bilden sich in der Netzwerk-
Topologie ab.**