Scanning

discover hosts

```
netdiscover -r 10.0.0.0/24
```

scan subnet for hosts

```
nmap -v -sn 10.0.0.0/24
```

Syn-scan

```
nmap -sS INSERTIPADDRESS
```

Scan all ports, might take a while.

```
nmap INSERTIPADDRESS -p-
```

Service-version, default scripts, OS:

```
nmap INSERTIPADDRESS -sV -sC -O -p 111,222,333
```

Scan for UDP

```
nmap INSERTIPADDRESS -sU
```

Scan through proxychains

```
proxychains nmap -v -sT 10.3.3.34 -Pn
```

Unicornscan

```
unicornscan -mU -v -I INSERTIPADDRESS
```

Connect to udp if one is open

```
nc -u INSERTIPADDRESS 48772
```

Monster scan

```
nmap INSERTIPADDRESS -p- -A -T4 -sC
```

Wireshark

```
Check for traffic coming from or to host
```

Port 21 - FTP

```
• FTP-Name:
• FTP-version:
• Anonymous login:

nmap --script=ftp-anon,ftp-libopie,ftp-proftpd-backdoor,ftp-vsftpd-
backdoor,ftp-vuln-cve2010-4221,tftp-enum -p 21 INSERTIPADDRESS
```

Port 22 - SSH

```
• Name:
• Version:
• Takes-password:
• If you have usernames test login with username:username
```

Port 25 - SMTP

```
• Name:
• Version:
• VRFY:

nc -nvv INSERTIPADDRESS 25
HELO foo
telnet INSERTIPADDRESS 25
VRFY root
EXPN all
nmap --script=smtp-commands,smtp-enum-users,smtp-vuln-cve2010-
4344,smtp-vuln-cve2011-1720,smtp-vuln-cve2011-1764 -p 25
INSERTIPADDRESS
```

Port 53- DNS

```
gobuster -m dns -w subdomains.txt -u google.com
```

Port 110 - Pop3

```
• Name:
• Version:

telnet INSERTIPADDRESS 110
USER pelle@INSERTIPADDRESS
PASS admin
or:
USER pelle
PASS admin
# List all emails
list
# Retrieve email number 5, for example
retr 5
```

Port 111 - Rpcbind

```
rpcinfo -p INSERTIPADDRESS
```

Port 123-NTP

```
ntp-info and ntp-monlist
Check ntpd version for exploits
```

Port 139/445 - SMB

```
• Name:
• Version:
• Domain/workgroup name:
• Domain-sid:
• Allows unauthenticated login:
```

```
nmap --script=smb-enum-shares.nse,smb-ls.nse,smb-enum-users.nse,smb-
mbenum.nse,smb-os-discovery.nse,smb-security-mode.nse,smbv2-
enabled.nse,smb-vuln-cve2009-3103.nse,smb-vuln-ms06-025.nse,smb-vuln-
ms07-029.nse,smb-vuln-ms08-067.nse,smb-vuln-ms10-054.nse,smb-vuln-
ms10-061.nse,smb-vuln-regsvc-dos.nse,smbv2-enabled.nse INSERTIPADDRESS
-p 445
```

```
enum4linux -a INSERTIPADDRESS
rpcclient -U "" INSERTIPADDRESS
    -c options
        srvinfo
enumdomusers
getdompwinfo
querydominfo
netshareenum
netshareenumall
smbclient -L INSERTIPADDRESS
smbclient //INSERTIPADDRESS/tmp
smbclient \\\\INSERTIPADDRESS\\ipc$ -U john
smbclient //INSERTIPADDRESS/ipc$ -U john
nmblookup -A INSERTIPADDRESS
```

Log in with shell (psexec for linux):

```
winexe -U username //INSERTIPADDRESS "cmd.exe" --system
```

Port 161/162 UDP - SNMP

```
nmap -vv -sV -sU -Pn -p 161,162 --script=snmp-netstat,snmp-processes
INSERTIPADDRESS
snmp-check -t INSERTIPADDRESS -c public
# Common community strings
public
private
community
```

Port 1433 - MSSQL

SQL shell from Kali

```
sqsh -S IPADDRESS -U sa
    >SELECT * from Table;
    >GO
```

Useful MSSQL Commands

Version

```
SELECT @@version
```

Comments

```
SELECT 1 -- comment
SELECT /*comment*/1
```

Current User

```
SELECT user_name();
SELECT system_user;
SELECT user;
SELECT loginame FROM master..sysprocesses WHERE spid = @@SPID
```

List Users

```
SELECT name FROM master..syslogins;
```

List Databases

```
SELECT name FROM master.dbo.sysdatabases;
```

List Tables

```
SELECT * FROM INFORMATION_SCHEMA.TABLES WHERE TABLE_TYPE='BASE TABLE';
```

List Tables for specific database

```
SELECT TABLE_NAME FROM <DATABASE_NAME>.INFORMATION_SCHEMA.TABLES WHERE
TABLE_TYPE = 'BASE TABLE';
```

Port 1521 - Oracle

```
• Name:
• Version:
• Password protected:

tnscmd10g version -h INSERTIPADDRESS
tnscmd10g status -h INSERTIPADDRESS
```

Port 2049 - NFS

```
showmount -e INSERTIPADDRESS
```

```
If you find anything you can mount it like this:
```

```
mount INSERTIPADDRESS:/ /tmp/NFS
mount -t INSERTIPADDRESS:/ /tmp/NFS
```

3306 - MySQL

```
• Name:
• Version:

nmap --script=mysql-databases.nse,mysql-empty-password.nse,mysql-
enum.nse,mysql-info.nse,mysql-variables.nse,mysql-vuln-cve2012-2122.nse
INSERTIPADDRESS -p 3306
```

Remote MySQL shell

```
mysql --host=INSERTIPADDRESS -u root -p
```

Useful MySQL commands
Version

```
SELECT @@version
```

Comments

```
SELECT 1; #comment
SELECT /*comment*/1;
```

Current User

```
SELECT user();
SELECT system_user();
```

List Users

```
SELECT user FROM mysql.user;
```

List Password Hashes, must be privileged

```
SELECT host, user, password FROM mysql.user;
```

List Databases

```
show databases;
SELECT schema_name FROM information_schema.schemata; — for MySQL >= v5.0
```

List Columns

```
SELECT table_schema, table_name, column_name FROM
information_schema.columns WHERE table_schema != 'mysql' AND
table_schema != 'information_schema';
```

List Tables

```
show tables;
```

```
SELECT table_schema,table_name FROM information_schema.tables WHERE
table_schema != 'mysql' AND table_schema != 'information_schema';
```

List Stored Procedures

```
SHOW PROCEDURE STATUS;
SELECT name from mysql.proc;
```

Check for FILE privilege which allows users to access or create files on the system

```
SELECT user,file_priv FROM mysql.user WHERE FILE_PRIV='Y';
```

Port 3389 - Remote desktop

```
Test logging in to see what OS is running
rdesktop -u guest -p guest INSERTIPADDRESS -g 94%


# Brute force
ncrack -u administrator -P /usr/share/wordlists/rockyou.txt -p 3389
IPADDRESS
```