

Red Team Field Manual (RTFM)

The Red Team Field Manual is a kind of reference guide to Linux, Windows, Cisco etc. It contains all the really useful information in a book small enough to carry around everywhere. Some of the really useful pages I will be keeping on here for 'my own' reference. You didn't see this page right (i'll fork bomb u if you did)

Linux Network Commands

```
watch ss -tp
netstat -ant
netstat -tulpn
lsof -i
smb:// ip /share
share user x.x.x.x c$
smbclient -U user\\\\ ip \\ share
ifconfig eth# ip I cidr
ifconfig eth0:l ip I cidr
route add default gw gw lp
ifconfig eth# mtu [size]
export MAC=xx: XX: XX: XX: XX
ifconfig int hw ether MAC
macchanger -m MAC int
iwlist int scan
dig -x ip
host ip
host -t SRV service tcp.url.com
dig @ ip domain -t AXFR
host -l domain namesvr
ip xfrm state list
ip addr add ip / cidr dev eth0
/var/log/messages | grep DHCP
tcpkill host ip and port port
echo "l" /proc/sys/net/ipv4/ip forward
echo 'nameserver x.x.x.x' /etc7resolv.conf
```

```
Network connections
Tcp connections -anu=udp
Connections with PIDs
Established connections
Access windows smb share
Mount Windows share
SMB connect
Set IP and netmask
Set virtual interface
Set GW
Change MTU size
Change MAC
Change MAC
Backtrack MAC changer
Built-in wifi scanner
Domain lookup for IP
Domain lookup for IP
Domain SRV lookup
DNS Zone Xfer
DNS Zone Xfer
Print existing VPN keys
Adds 'hidden' interface
List DHCP assignments
Block ip:port
Turn on IP Forwarding
Add DNS Server
```

Linux System Info

```
nbstat -A ip
id
w
who -a
last -a
ps -ef
df -h
uname -a
mount
getent passwd
PATH~$PATH:/home/mypath
kill pid
cat /etc/issue
cat /etc/'release'
cat /proc/version
rpm --query -all
rpm -ivh '.rpm
dpkg -get-selections
dpkg -I '.deb
pkginfo
which tscsh/csh/ksh/bash
chmod -5o tcsh/csh/ksh
```

```
Get hostname for IP
Current username
Logged on Users
User information
Last users logged on
Process listing (top)
Disk usage (free)
Kernel version/CPU Info
Mounted file systems
Show list of users
Add to PATH variable
Kill process with pid
Show OS info
Show OS Version info
Show Kernel info
Installed pkgs (Redhat)
Install RPM (-e=remove)
Installed pkgs (Ubuntu)
Install DEB (-r~remove)
Installed pkgs (Solaris)
Show location of executable
Disable shell , force bash
```

Linux Utility Commands

```
wget http:// url -O url.txt -o /dev/null
rdesktop ip
scp /tmp/file user@x.x.x.x:/tmp/file
scp user@ remoteip :/tmp/file /tmp/file
useradd -m user
passwd user
rmuser uname
script -a outfile
apropos subject
history
! num
```

```
Grab url
Remote Desktop to ip
Put file
Get file
Add user
Change user password
Remove user
Record shell : Ctrl-D stops
Find related command
View users command history
Executes line # in history
```

From:

<https://wiki.alanwalker.uk/> - WalkerWiki - wiki.alanwalker.uk

Permanent link:

<https://wiki.alanwalker.uk/doku.php?id=rtfm&rev=1469480709>

Last update: **2023/03/09 22:35**

