Red Team Field Manual (RTFM)

2016

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                                    Network connections
netstat -ant                                    Tcp connections -anu=udp
netstat -tulpn                                  Connections with PIDs
lsof -i                                         Established connections
smb:// ip /share                                Access windows smb share
share user x.x.x.x c$                           Mount Windows share
smbclient -U user\\\\ ip \\ share               SMB connect
ifconfig eth# ip I cidr                         Set IP and netmask
ifconfig eth0:l ip I cidr                       Set virtual interface
route add default gw gw lp                      Set GW
ifconfig eth# mtu [size]                        Change MTU size
export MAC=xx: XX: XX: XX: XX: XX               Change MAC
ifconfig int hw ether MAC                       Change MAC
macchanger -m MAC int                           Backtrack MAC changer
iwlist int scan                                 Built-in wifi scanner
dig -x ip                                       Domain lookup for IP
host ip                                         Domain lookup for IP
host -t SRV service tcp.url.com                 Domain SRV lookup
dig @ ip domain -t AXFR                         DNS Zone Xfer
host -l domain namesvr                          DNS Zone Xfer
ip xfrm state list                              Print existing VPN keys
ip addr add ip / cidr dev eth0                  Adds 'hidden' interface
/var/log/messages | grep DHCP                   List DHCP assignments
tcpkill host ip and port port                   Block ip:port
echo "l" /proc/sys/net/ipv4/ip forward          Turn on IP Forwarding
echo ''nameserver x.x.x.x'' /etc7resolv.conf    Add DNS Server
```

Linux System Info

```
nbstat -A ip                                    Get hostname for IP
id                                              Current username
w                                               Logged on Users
who -a                                          User information
last -a                                         Last users logged on
ps -ef                                          Process listing (top)
df -h                                           Disk usage (free)
uname -a                                        Kernel version/CPU Info
mount                                           Mounted file systems
getent passwd                                   Show list of users
PATH~$PATH:/home/mypath                         Add to PATH variable
kill pid                                        Kill process with pid
cat /etc/issue                                  Show OS info
cat /etc/'release'                              Show OS Version info
cat /proc/version                               Show Kernel info
rpm --query -all                                Installed pkgs (Redhat)
rpm -ivh '.rpm                                  Install RPM (-e=remove)
dpkg -get-selections                            Installed pkgs (Obuntu)
dpkg -I '.deb                                   Install DEB (-r~remove)
pkginfo                                         Installed pkgs (Solaris)
which tscsh/csh/ksh/bash                        Show location of executable
```

```
chmod -5o tcsh/csh/ksh                          Disable shell , force bash
```

Linux Utility Commands

```
wget http:// url -O url.txt -o /dev/null        Grab url
rdesktop ip                                     Remote Desktop to ip
scp /tmp/file user@x.x.x.x:/tmp/file            Put file
scp user@ remoteip :/tmp/file /tmp/file         Get file
useradd -m user                                 Add user
passwd user                                     Change user password
rmuser uname                                    Remove user
script -a outfile                               Record shell : Ctrl-D stops
apropos subject                                 Find related command
history                                         View users command history
! num                                           Executes line # in history
```