HackSheet ^{master}

Author: Matthias Vallentin
Web: https://github.com/mavam/hacksheet
License: Attribution-NonCommercial-ShareAlike 3.0 Unported

Terminology

Each command contains a list of flags that indicate the OS requirement: Linux (L), BSD (B), FreeBSD (F), Mac OS (M), UNIX (U), and Windows (W).

General Utility

Useful Powershell Commands

⋆ Download File from Internet
```
W #  Powershell
  $source = "http:www.download.com/file.txt"
  $destination = "c:\temp\file.txt"
  $wc = New-Object System.Net.WebClient
  $wc.DownloadFile(source,destination)
```

Reconnaissance

Scanning

⋆ Ping sweep of subnet and host range
```
U # nmap -sP 10.0.0.0/24 192.168.0.128-254
```
⋆ Scan specific TCP and UDP ports
```
U # nmap -pT:21-25,80,U:5000-6000 target
```
⋆ TCP SYN scan without connecting
```
U # nmap -P0 -sS target
```
⋆ Detect OS
```
U # nmap -O target
U # p0f -s trace.pcap
```
⋆ Grab application banners
```
U # nmap -sV target
U # echo QUIT | nc target 1-1024
```

Wireless

Vulnerability Scanning

Web

⋆ Look for web server vulnerabilities
```
U # nikto -host 10.0.0.1
```

Hardening

Physical

⋆ Check devices
  • Hardware keylogger (e.g., USB dongles)
  • Rogue WiFi cards

OS & Software

⋆ Check for package repositories
```
L # vi /etc/apt/sources.list (Ubuntu)
L # vi /etc/yum.repos.d/* (RHEL/Fedora)
```
⋆ Run package updates
```
L # yum upgrade package
L # apt-get upgrade package
```
⋆ Update Kernel
```
L # yum update kernel (RHEL/Fedora)
L # apt-cache search linux-image; apt-get
  install linux-image-x.x.x-xx (Debian)
```
⋆ Harden SSHD
```
U fail2ban
U # vi /etc/ssh/sshd_config
  Protocol 2
  AllowUsers root admin webmaster
  AllowGroup sshusers
  PasswordAuthentication no
  HostbasedAuthentication no
  RSAAuthentication yes
  PubkeyAuthentication yes
  PermitEmptyPasswords no
  PermitRootLogin no
  ServerKeyBits 2048
  IgnoreRhosts yes
  RhostsAuthentication no
  RhostsRSAAuthentication no
```

User Management

⋆ Show account security settings
```
U # passwd -l user
L # chage -l user
W # net accounts
W # net accounts /domain
```

⋆ View Users
```
W # wmic useraccount list brief
```

⋆ Look for users with root privileges
```
U # awk -F: '$3 == 0 {print $1}' /etc/passwd
W # net localgroup administratos
```

⋆ Look for users with empty passwords
```
U # awk -F: '$2 == "" {print $1}' /etc/shadow
```

⋆ Verify group memberships
```
U # vi /etc/group (admin, sudo, wheel)
```

⋆ Check sudo users
```
U # visudo
```

⋆ Check crontab users
```
U # for u in $(cut -f1 -d:  /etc/passwd); do
  crontab -u $u -l; done
```

⋆ Check remote authentication
```
U # vi ~/.rhosts
U # vi ~/.ssh/*
```

⋆ Change passwords
```
U # pwgen -sy (generate strong passwords)
U # passwd user
W # net user user *
```

File System

★ Secure mount points
  `U # mount -o nodev,noexec,nosuid /dev.. /tmp`

★ List file attributes
  `L # lsattr /var/log/foo`
  `B # ls -ol /var/log/foo`
  `W # cacls.exe file.txt`

★ File creation date
  `W # dir /tc /od`
  `U # ls -li /etc | sort -n`

★ System file checker
  `W # sfc /scannow`

★ File signature serification
  `W # sigverif`
  `W SIGCHECK`
  `W # sigcheck -e -u -s c:`

★ Make files append-only
  `L # chattr +a /var/log/foo`

Network

★ Show firewall rules
  `L # for t in nat mangle filter raw; do`
  `   iptables -t $t -nL; done`
  `W # netsh firewall show portopening`
  `W # netsh firewall show allowedprogram`
  `W # netsh firewall show config`

★ Close ports
  `W # netsh advfirewall firewall add rule`
  `   name="BlockAIM"`
  `   protocol=TCP`
  `   dir=out remoteport=4099 action=block`

★ Check DNS resolver
  `U # vi /etc/resolv.conf`

★ Disable IPv6
  `L # ipv6.disable=1` (add to kernel line)
  `L # vi /etc/sysctl.conf`
  `   net.ipv6.conf.all.disable_ipv6 = 1`
  `   net.ipv6.conf.<interface0>.disable_ipv6 = 1`
  `   net.ipv6.conf.<interfaceN>.disable_ipv6 = 1`
  `   vi /etc/hosts` (comment IPv6 hosts)
  `L # vi /etc/sysconfig/network`
  `   NETWORKING_IPV6=no`
  `   IPV6INIT=no`
  `   service network restart`
  `L # vi /etc/modprobe.conf`
  `   install ipv6 /bin/true` (append to file)
  `L # vi /etc/modprobe.conf` (RHEL/CentOS)
  `   alias net-pf-10 off`
  `L # vi /etc/modprobe.conf` (Debian/Ubuntu)
  `   alias net-pf-10 off`
  `   alias ipv6 off`
  `W # reg add hklm\system\currentcontrolset\services\`
  `   tcpip6\parameters /v DisabledComponents /t`
  `   REG_DWORD /d 255`

★ Check network configuration
  `L # vi /etc/network/interfaces` (Ubuntu)
  `L # vi /etc/sysconfig/network-scripts/ifcfg-eth*`
  `(RHEL)`

Forensics

Processes

★ Inspect startup items
  `L # initctl show-config` (upstart, Ubuntu)
  `F # less /etc/rc.local` (deprecated)
  `F # grep local_start /etc/defaults/rc.conf`
  `W AUTORUNS Everything`

★ Find SETUID and SETGID files and types
  `U # find / \( -perm -4000 -o -perm -2000 \)`
  `   -exec file \{\} \;`
  `U # crontab -e`
  `   0 4 * * * find / \( -perm -4000 -o -perm`
  `   -2000 \) -type f > /var/log/sidlog.new &&`
  `   diff /var/log/sidlog.new /var/log/sidlog &&`
  `   mv /var/log/sidlog.new /var/log/sidlog`

★ Find world/group writeable directories
  `U # find / \( -perm -g+w -o -perm -o+w \)`
  `   -type d -exec ls -ald \{\} \;`

★ Find all unsigned processes
  `W PROCESSEXPLORER Options → Verify Image Signatures`

★ Display listening TCP/UDP ports
  `LWU # netstat -tun`
  `W TCPVIEW`
  `B # netstat -p tcp -an | egrep`
  `   'Proto|LISTEN|udp'`
  `U # lsof -nPi | awk '/LISTEN/'`
  `F # sockstat -4 -l`

★ Check active connections to find backdoors
  `U # lsof -nPi | awk '/ESTABLISHED/'`

★ Currently Running Tasks/Processes
  `W # tasklist -svc`
  `LU # ps aux | less`
  `LU # top`
  `LU # ps -u user`

★ Kill Tasks/Processes
  `W # taskkill -pid pid`
  `LU # kill pid`

Users

⋆ Inspect logged in and past users

    U `# w`

    U `# last | head`

    U `# ps -ef | awk '$6 != "?"'` (interactive procs)

    W PsLoggedOn

    W Task Manager (open as administrator) -> Users
        Tab

Cleanup

⋆ Kill all processes accessing a mount point

    U `# fuser -k -c /mnt/secret`

Drivers

⋆ Driver query

windows `# driverquery (-v)`

References

- http://bit.ly/cmd-line-kung-fu
- http://www.robvanderwoude.com/ntadmincommands.php
- http://pubs.vmware.com/vsphere-50/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-50-security-guide.pdf

Very Useful Downloads

- http://technet.microsoft.com/en-us/sysinternals/bb842062