

Forum:[Hack Forums](#)

Thread: [Linux Information Gathering and Situational Awareness](#)

CyberStrike - October 13, 2017, 7:09 pm

Linux Information Gathering and Situational Awareness

As with Windows getting a situational awareness is important. Having a familiarity with BASH is important in order to be confident with your enumeration skills. You must save these results for off line analysis, as this can be used for privilege escalation later. There are several different distributions of Linux as we all know, they can be broken down in a few major groups Debian/SlackWare/RHEL/Arch.

First we will want to find out the environment which we are in, since often times in production an Administrator and more over management is worried to say the least during patching especially when it comes to "critical infrastructure", so we often find that only major issues are patched at best, an operator should keep this in mind during this phase when landing on a machine.

Finding out about OS

Code `cat /etc/*-release`

`cat /etc/issue`

`uname -ar`

Finding out about the networks

Code `cat /etc/sysconfig/network`

`cat /etc/resolv.conf`

`cat /etc/nsswitch.conf`

`ifconfig -a`

Check Routing

Code `route`

`arp -a`

Checking active connections (TCP)

Code `netstat -antp`

Checking Active Ports and Services on those ports:

Code `netstat -p`

Disk enumeration

Code `df`

`mount`

`cat /etc/fstab`

Must be admin to view contents of shadow

View Passwords

Code `cat /etc/passwd`

`cat /etc/shadow`

Groups

Code `cat /etc/group`

Sudoers

Code `cat /etc/sudoers`

Sticky Bits Files (File Permissions)

Code `find / -perm -g=s -o -perm -4000 ! -type l -maxdepth 3 -exec ls -ld {} \; 2>/dev/null`

World Writable Directories & Files

Code `find / -perm -222 -type d 2>/dev/null`

`find / -type f -perm 0777 2>/dev/null`

Files owned by current user

Code `find / -user $(whoami) 2>/dev/null`

Permissions to root and home

Code `ls -ahlR /home/`

`ls -ahlR /root/`

[code]

Logged on users

[code]

w

Last logged on users

Code `last`

Processes running as root

Code `ps -ef | grep root`

Distribution Specific

Installed Packages for RHEL/Centos or Debian

Debian

Code `dpkg -l`

RHEL/CentOs

Code `rpm -qa`

RHEL/Centos startup processes

Code `chkconfig --list | grep $(runlevel | awk '{ print $2}'):on`

Debian startup (older pre-systemd)

Code `ls /etc/init.d/`

Debian Startup (Newer)

Code `systemctl list-units -t service --no-legend --all`

Checking Cron for user

Code crontab -u username -l

*Note: if you are in sudoers you can always change that password then start issuing commands and a super user.

Gathering information about the machine which you are currently on is important as applications installed can be exploited to give an operator privileges.

lwrist - October 13, 2017, 7:10 pm

Amazing thread with all the right details. Thanks for posting.

CyberStrike - October 13, 2017, 7:16 pm

(Oct 13, 2017 07:10 PM)oxid Wrote: [\[CITE\]](#) Amazing thread with all the right details. Thanks for posting.

Thank you ? (Wait was I supposed to put in wrong info?)

lwrist - October 13, 2017, 7:18 pm

(Oct 13, 2017 07:16 PM)sirru5h Wrote: [\[CITE\]](#) Thank you ? (Wait was I supposed to put in wrong info?)

lol

perhaps better wording would be that you got all the essential content out rather than fluff

CyberStrike - October 13, 2017, 7:25 pm

If people are following they should have an idea from the Windows tutorials as to why they are doing these things, so these next tutorials not much on fluff and the wordy stuff I will save that for Red Team Dirty Tricks and Tactics and Building up your Domain's Reputation (writing this right now btw)

lwrist - October 13, 2017, 7:35 pm

(Oct 13, 2017 07:25 PM)sirru5h Wrote: [\[CITE\]](#) If people are following they should have an idea from the Windows tutorials as to why they are doing these things, so these next tutorials not much on fluff and the wordy stuff I will save that for Red Team Dirty Tricks and Tactics and Building up your Domain's Reputation (writing this right now btw)

I'm very excited for the Red Team tnt

CyberStrike - October 13, 2017, 7:49 pm

It is the last tutorial but all of the tutorials that I posted and will post it will tie everything together with the technical and with social engineering.

Dimeblade - January 9, 2018, 10:45 am

IN MY OPINION The only person in HF that posts some valid decent and usefull stuff.

CyberStrike - January 9, 2018, 3:39 pm

DimeBlade, thanks I appreciate the positive comments. If you get a chance I also did OSX as well as various "infrastructure" give em a look

RedTeam Infrastructure/Structure

<https://hackforums.net/showthread.php?tid=5742945>

<https://hackforums.net/showthread.php?tid=5728866>

Windows Application Shimming : <https://hackforums.net/showthread.php?tid=5764027>

Windows Post Exploitation/ AD Hunting : <https://hackforums.net/showthread.php?tid=5732104>

OSX

<https://hackforums.net/showthread.php?tid=5751343>

It's been a bit hard getting feedback or a discussion going, although usually a different type of HF user does comment or read these types of threads.