Lecture-4

Information Gathering and Digital Foot printing

Phases of hacking:

These phases are must to follow in order to perform any kind of hacking.

1. *Information Gathering (most crucial part of hacking)*
2. *Scanning*
3. *Gaining Access*
4. *Maintaining Access*
5. *Covering Traces /clearing tracks (Logs)*

Information Gathering:

To collect as much Information as possible about the target.
Information Gathering is divided into further

1. *Network Specific*
2. *Target Specific*

1. Network Specific :

To collect the information about the network
Number Of people Connected
IP Address allocated to the connected devices
MAC Address of devices connected etc.

Windows based tools:

1. *Soft Perfect Network Scanner (NetScan)*
2. *GFI Languard*

Linux based tool:

1. *Network Mapper (CLI NMap) Command Line Interface*
2. *Zenmap (GUI of NMap)*

2. Target Specific : Gathering information about the sources found.

i. Web site or web application
ii. Human Specific

Web site or web Application:

Some crucial information needs to be picked out about the target's website these information can be IP address, Server information, sub domains.

IP Address: Ping > "ip address"
Server Information

Dedicated or shared

https://www.yougetsignal.com --> reverse IP DOMAIN CHEKUP

Database Information

Name of the registrar

Technologies

White list and Black List

|--> robots.txt

*User-agent: **

Disallow: /

Informational websites :

https://whois.net/
https://whois.icann.org/en
https://mxtoolbox.com/

Human Specific:

Social Network
Social Networking Websites
Linkedin
Twitter
Facebook
Dating Websites
Matrimonial Websites
Job Portals
Fake Surveys
Spy Services

Websites:

Jantakhoj.com
pipl

Tools:

Maltego:

It is corporate level information gathering tool. It helps in gathering information about each and every aspect.

Community Edition ---> Free
All transformations does not work in free edition.
https://www.paterva.com/web7/downloads.php

OS Login Bypass:

When you log into the OS, then while starting the windows, you will be asked for password.

1. Online Method
2. Offline Method

1. Online Method:

When you need to crack or bypass the password, change the OS login password when the system is up, and you do not know the current password. It only works in windows ultimate or professional version.

1. *Right click on "My Computers"*
2. *Click on "Manage"*
3. *Click on "Local Users and Groups", in the left pane*
4. *Click on "Users"*
5. *Choose the user, for whom you want to change the password.*
6. *Right Click*
7. *Set Password*

Second method will be by replacing the SETHC(Syskey Password) by command prompt.

Demo...

2. Offline Method

This is the condition, when the device is in shut down mode and we cannot open the group editing policies.

SAM --> Security Account Manager

C:|Windows|System32|Config|SAM

Hiren Boot CD

Kon Boot CD

These are live bootable OS. We use tools like Rufus, to make the media bootable.

BIOS --> Basic Input Output System

Live OS ---> It replaces the BIOS of the Computer or the device from the one which is in the bootable media.

Created by: Vikram Solanki(Certified Ethical Hacker)