Expt. No.: 8.

Date:

Page No

Aim ⇒ WAP to implement SHA-1 (Secure hash algo).

```
import hashlib

str = 'Hello world'
result = hashlib.sha256(str.encode())
result2 = hashlib.sha1(str.encode())

print("Original string is :- " + str)
print("SHA 256 Hashing code :- " + result.hexdigest())
print("SHA-1 Hashing code :- " + result2.hexdigest())
```

Output ⇒

Original string is :- Hello world

SHA 256 Hashing code :- 64ec88caa00b268e5ba1a3567
-8a1b5316d212f4f366b247724
-a8aeca37f3c

SHA 1 Hashing code :- 7b502c3a1f48c8609ae212cdfb639
dee39673f5e

Date:

Expt No: 9

Page No:

Aim ⇒ Installation of rootkits and study about the variety of options.

Root kit is a stealth type of malicious software designed to hide the existence of certain process from normal methods of detection and enables continued previleged access to a computer.

Introduction ⇒

Root is a UNIX/LINUX term that's equivalent to administrator in windows. The word kit denotes programs used to get root access.

This malicious software boots up before your OS, and allows installation of hidden files, processes, hidden user accounts and more.

The rootkit serves two primary function: remote command/control (back door) and evaesdropping. The presence of rootkit on Network was first documented in early 1990s. At that time, Sun and Linux OS were primary targets for a hacker looking to install a rootkit.

Teacher's Signature:

Date:

Expt. No:

Page No:

Procedure :-

Step1 ⇒ Download rootkit from "www.gmer.net"

Step2 ⇒ This displays the Processes, Modules, Services, Files, Registry, Rootkit / Malwares, Autostart, CMD of local host.

Step3 ⇒ Select process menu and kill any unwanted process.

Step4 ⇒ Modules menu displays various system files like .sys, .dll

Step5 ⇒ Services menu displays the complete services running with autostart, Enable, Disable, System, Boot.

Step6 ⇒ Files menu displays full files on HDD volumes.

Step7 ⇒ Registry displays HKey_Current_user and HKey_Local_Machine.

Step8 ⇒ Root kit / Malware scans the local drives selected.

Step9 ⇒ Autostart displays the registry base autostart applications.

Step10 ⇒ CMD allows the user to interact with command line utilities or Registry.

Teacher's Signature:

Expt. No. 10

Page No.

Aim ⇒ Working with SNORT TOOL To Demonstrate intrusion detection system.

Introduction ⇒

SNORT is an open source network intrusion detection system (NIDS) and it is a packet sniffer that monitors network traffic in real time.

SNORT Tool ⇒

Snort tool is based on libpcap (for library packet capture), a tool is widely used in TCP/IP traffic sniffers and analyzers.

SNORT can be configured in to run in three modes:-

1. Sniffer mode
   - → Sonort -v
   - → Snort -vd
2. Packet Logger mode
   - → Snort -dev -l c:\log
   - → Snort -dev -l c:\log -h ipaddress/24
3. Network intrusion detection system mode.

Teacher's Signature:

Date

Exp. No.

Page No.

Procedure :

Step 1 Sniffer mode snort -v Print out the TCP/IP packets header on the screen

Step 2 Snort -vd Show the TCP/IP ICMP header with application data in transit.

Step 3 Packet Logger mode snort -dev -l c:\log [create this directory in C drive] and snort will automatically know to go into packet logger mode, it collects every packet it sees and places it in log directory.

Step 4 snort -dev -l c:\log -h ipaddress/24 This rule tells snort that you want to print out the data link.

Step 5 snort -l c:\log -b this binary mode logs everything into a single file

Step 6 Network Intrusion Detection System mode snort -d c:\log -h ipaddress/24 -c snort.conf

Step 7 snort -d -h ip address/24 -l c:\log -c snort.conf

Step 8 Download SNORT from snort.org. Install snort with or without database support.

Step 9 Select all the components and click Next. Install and close

Step 10 Skip the Win Pcap driver installation.

Step 11 Add the path variable

Step 12 create a path variable and point it at snort.exe variable

Step 13 click OK button and then close all dialog boxes.

Teacher's Signature.

Expt. No.: 11 Page No.:

Aim: To study about ARP poisoning

Address resolution protocol (ARP) is used to convert IP address to physical address. The host sends an ARP broadcast on the network, and the recipient computer responds with its MAC address. The resolved IP/MAC address is then used to communication.

ARP poisoning is sending fake MAC addresses to the switch so that it can associate the attacker MAC address with the IP address of a computer on a network and hijack the traffic.

ARP poisoning:

- It is used to convert IP address to physical address
- Enter following in command: Arp -a
- -a is the parameter of to contents to the ARP caches.
- dynamic entries are added and deleted automatically during TCP/IP sessions.
- Static entries are added manually and deleted when computer restarts.
- Ipconfig/all command to get the IP and MAC address.
- arp -s 192.168.0.56 74-86.
- arp -a
- arp -d .... to delete an entry
- Download ettercap for windows.

Teacher's Signature: