MUHAMMAD HAMAD - Project phase 4 – Digital forensics

STEP – I: ABSTRACT:

Now a days, a suspect may use a Web browser to collect information, to hide his/her crime, or to search for a new crime method. Searching for evidence left by Web browsing activity is typically a crucial component of investigations. Moreover, it is not sufficient to investigate a single log file from a single browser because the evidence may be spread over several log files. Second, existing research and tools remain at the level of simple parsing. In Web browser forensic investigation, it is necessary to extract more significant information related to digital forensics, such as search words and user activity. So an integrated browser analysis framework is required that can be able to unify the forensic related browser data in single software thus allow forensic analyst to create a timeline because criminal may have used multiple browsers to commit a crime , there should be an efficient data carving algorithms are required to reconstruct the browser deleted data. A primary point of hinderess in retrieval of information is related to private browsing option provided by many browsers. So a complete analysis framework that can find traces from deleted history, cookies, and password and carve the data related to forensics.

STEP – II: ATTACKS RELEVANT TO PROJECT

	Attack name	Weight (5 highly relevant)
1	Rootkit	5
2	Spy	4
3	Load module	3
4	Satan	2
5		

RELEVENCE TO THE PROJECT

Rootkit: Once installed it can hide its existence and mask the actual contents of disk/memory thus, Removal can be complicated or practically impossible, especially in cases where the rootkit resides in the kernel; As most of the project features are related to browser data extraction whose integrity can be compromised with rootkit.

Spy: Multi-day scenario in which a user breaks into a machine with the purpose of finding important information where the user tries to avoid detection. Uses several different exploit methods to gain access. In this way can get high value information can be compromised.

Load module: Non-stealthy load module attack which resets Internet Field Separator for a normal user and creates a root shell. If anyone get root access it will make all information on stake.

Satan: Network probing tool which looks for well-known weaknesses.

STEP III:

	Attack name	Feature name	Weight (5 highly relevant)
1	Rootkit	Source bytes,# of root access	5
2	Spy	Failed login, Count, dest bytes	4
3	Load module	Root shell, # of root access	3
4	Satan	Diff srv rate	2

Reason of feature selection:

Source bytes: Bytes sent from source to destination can be is important metric for rootkit detection because rootkit masks the actual data and acts as middle malicious layer and are not providing the necessary data.

No of root access: In some cases rootkit resides in kernel and have super user access to all system.

Failed login: As it is a multi-day scenario, so it may be possible that attacker for gaining initial access will try many logins that may fail initially.

Count: Number of connections that are made to the host as the current connection will possibly identify that someone is spying.

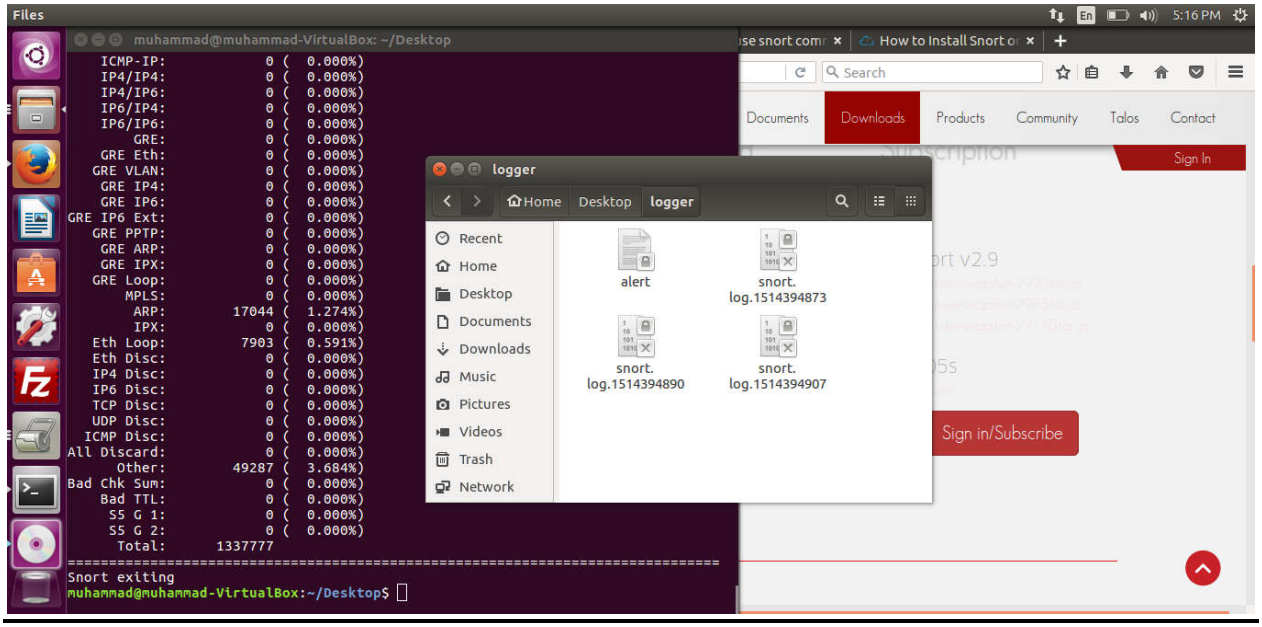
Root shell: As load module is basically trying to get shell access so I think this feature will help ids to detect load module

Diff srv rate: Is someone is probing we can check the number of connections to different services because for information gathering, attacker will definitely probe different services of system

---

I installed Ubuntu in virtual machine and installed snort in it and the downloaded some community rules from snort community rules website then I added those rules to snort directory and, downloaded outside.tcpdump from MIT website as link provided in research paper.

After configuration I run snort in packet sniffer mode and provided the outside.tcpdump file and some alerts were generated but they are saved with lock sign over them so I am not able to copy them. I am adding snap shot of that experiment in this.


Files
5:16 PM
muhammad@muhammad-VirtualBox: ~/Desktop
ICMP-IP: 0 (0.000%)
IP4/IP4: 0 (0.000%)
IP4/IP6: 0 (0.000%)
IP6/IP4: 0 (0.000%)
IP6/IP6: 0 (0.000%)
GRE: 0 (0.000%)
GRE Eth: 0 (0.000%)
GRE VLAN: 0 (0.000%)
GRE IP4: 0 (0.000%)
GRE IP6: 0 (0.000%)
GRE IP6 Ext: 0 (0.000%)
GRE PPTP: 0 (0.000%)
GRE ARP: 0 (0.000%)
GRE IPX: 0 (0.000%)
GRE Loop: 0 (0.000%)
MPLS: 0 (0.000%)
ARP: 17044 (1.274%)
IPX: 0 (0.000%)
Eth Loop: 7903 (0.591%)
Eth Disc: 0 (0.000%)
IP4 Disc: 0 (0.000%)
IP6 Disc: 0 (0.000%)
TCP Disc: 0 (0.000%)
UDP Disc: 0 (0.000%)
ICMP Disc: 0 (0.000%)
All Discard: 0 (0.000%)
Other: 49287 (3.684%)
Bad Chk Sum: 0 (0.000%)
Bad TTL: 0 (0.000%)
S5 G 1: 0 (0.000%)
S5 G 2: 0 (0.000%)
Total: 1337777
Snort exiting
muhammad@muhammad-VirtualBox:~/Desktop$
logger
Home
Desktop
logger
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
Network
alert
snort.log.1514394873
snort.log.1514394890
snort.log.1514394907
Search
Documents
Downloads
Products
Community
Talos
Contact
Sign In
Sign in/Subscribe

THE END